GUIDE D'ADMINISTRATION

Gamme Cisco Small Business

Appliances de sécurité intégrés de la gamme ISA500 (ISA550, ISA550W, ISA570, ISA570W)

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: **www.cisco.com/go/trademarks**. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2012 Cisco Systems, Inc. Tous droits réservés.

OL-23559-02

Déclaration sur les interférences de la FCC (Federal Communication Commission)

(Pour ISA570 et ISA570W)

Cet équipement a été testé et jugé conforme aux limites d'un périphérique numérique de classe A en vertu de la partie 15 des règlements de la FCC. Ces limites ont pour but de fournir une protection raisonnable contre les interférences nuisibles susceptibles de se produire, lorsque l'équipement est utilisé dans un environnement commercial. Cet équipement génère, utilise et peut émettre de l'énergie radioélectrique. S'il n'est pas installé et utilisé conformément au manuel d'instructions, il peut provoquer des interférences nuisibles aux communications radio. L'utilisation de cet équipement dans les zones résidentielles est susceptible de causer des interférences nuisibles. Le cas échéant, les utilisateurs devront corriger ces dernières à leurs frais.

(Pour ISA550 et ISA550W)

Cet équipement a été testé et jugé conforme aux limites des appareils numériques de Classe B en vertu de la Partie 15 des règlements de la FCC. L'objectif de ces normes est de fournir une protection raisonnable contre toute interférence nuisible dans une installation résidentielle. Cet équipement génère, utilise et peut émettre de l'énergie radioélectrique. S'il n'est pas installé et utilisé selon le manuel d'instructions, il peut provoquer des interférences nuisibles aux communications radio. Toutefois, rien ne garantit que son utilisation ne provoquera pas d'interférences dans une installation donnée. Si cet équipement provoque des interférences nuisibles pour la réception de la radio ou de la télévision (détectables par la mise hors tension et sous tension de l'équipement), l'utilisateur peut tenter d'y remédier de différentes façons :

- Réorientez ou déplacez l'antenne réceptrice.
- Augmentez la distance entre l'équipement et le récepteur.
- Branchez l'équipement sur une prise d'un circuit autre que celui auquel le récepteur est relié.
- Sollicitez l'aide du distributeur ou d'un technicien radio/télévision expérimenté.

Avertissement de la FCC : les changements ou modifications non approuvés expressément par la partie responsable de la conformité pourraient annuler le droit accordé à l'utilisateur d'exploiter cet équipement.

Cet appareil est conforme à la Partie 15 des règlements de la FCC. Son utilisation est sujette aux deux conditions suivantes : (1) il ne doit pas provoquer d'interférences dangereuses, et (2) il doit tolérer les interférences, notamment les interférences susceptibles de provoquer un fonctionnement indésirable.

REMARQUE IMPORTANTE :

Déclaration FCC sur l’exposition aux radiations : (Pour ISA550W et ISA570W)

Cet équipement est conforme aux normes d'exposition de la FCC en matière de radiations définies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé en respectant une distance minimale de 20 cm entre l'émetteur de radiations et vous-même.

Cet émetteur ne cohabitera pas ou ne fonctionnera pas conjointement avec toute autre antenne ou tout autre émetteur.

La disponibilité de certains canaux et/ou bandes de fréquences opérationnelles spécifiques dépend du pays et ils sont programmés dans le microprogramme à l'usine pour correspondre à la destination prévue. Le paramètre du microprogramme n'est pas accessible par l'utilisateur final.

Conformité à la réglementation canadienne :

Cet appareil est conforme à la norme CNR-210 des règlements d'Industrie Canada. Son utilisation est sujette aux deux conditions suivantes : (1) il ne doit pas provoquer d'interférences dangereuses, et (2) il doit tolérer les interférences, notamment les interférences susceptibles de provoquer un fonctionnement indésirable.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes : (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

REMARQUE IMPORTANTE :

Déclaration sur l’exposition aux radiations au Canada : (pour ISA550W et ISA570W)

Cet équipement est conforme aux normes d’exposition du Canada en matière de radiations définies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé en respectant une distance minimale de 20 cm entre l'émetteur de radiations et vous-même.

NOTE IMPORTANTE : (Pour l'utilisation de dispositifs mobiles)

Déclaration d'exposition aux radiations :

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Cet équipement a été conçu pour fonctionner avec une antenne dont le gain maximal est de 1,8 dBi. Conformément à la réglementation d'Industrie Canada, il est formellement proscrit d'utiliser une antenne de gain supérieur. L'impédance requise pour l'antenne est de 50 ohms.

Selon la réglementation d'Industrie Canada, cet émetteur radio peut fonctionner uniquement à l'aide d'une antenne d'un type et d'un gain maximal (ou inférieur) approuvés pour l'émetteur par Industrie Canada. Pour limiter les interférences radio potentielles avec les autres utilisateurs, le type d'antenne et son gain doivent être choisis de sorte que la puissance isotrope rayonnée équivalente (PIRE) ne soit pas supérieure à celle nécessaire pour une communication réussie.

(Le manuel d'utilisation de dispositifs émetteurs équipés d'antennes amovibles doit contenir les informations suivantes dans un endroit bien en vue :)

Ce dispositif a été conçu pour fonctionner avec une antenne ayant un gain maximal de 1,8 dBi. Une antenne à gain plus élevé est strictement interdite par les règlements d'Industrie Canada. L'impédance d'antenne requise est de 50 ohms.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peut fonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvés pour l'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectrique à l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que la puissance isotrope rayonnée équivalente (PIRE) ne dépasse pas l'intensité nécessaire à l'établissement d'une communication satisfaisante.

UL/CB

Instructions de montage sur bâti : les instructions suivantes ou similaires de montage sur bâti sont fournies avec les instructions d'installation :

A) Température ambiante de fonctionnement élevée : en cas d'installation dans un bâti fermé ou à plusieurs unités, la température ambiante de fonctionnement de l'environnement du bâti peut être supérieure à la température ambiante du local. Par conséquent, il est conseillé d'installer l'équipement dans un environnement compatible avec la température ambiante maximale (Tma) de 40 °C spécifiée par le fabricant.

B) Circulation d'air réduite : l'installation de l'équipement dans un bâti doit être telle que la quantité d'air requise pour un fonctionnement sûr de cet équipement ne soit pas compromise.

C) Charge mécanique : le montage de cet équipement dans le bâti ne doit pas générer de risque lié à un chargement mécanique inégal.

D) Surcharge des circuits : il convient de prendre en considération le raccordement de cet appareil au circuit d'alimentation et l'effet qu'une surcharge des circuits peut avoir sur la protection contre les surintensités et le câblage du module d'alimentation. À cet effet, veillez à tenir compte des caractéristiques nominales de la plaque signalétique de l'équipement.

Chapitre 1 : Démarrage 19

Introduction 20
Présentation du produit 21
Panneau avant 21
Panneau arrière 23
Mise en route à l'aide de l'utilitaire de configuration 25
Connexion à l'utilitaire de configuration 26
Navigation dans l'utilitaire de configuration 27
Utilisation du système d'aide 28
Icônes de l'utilitaire de configuration 28
Paramètres d'usine par défaut 30
Paramètres par défaut des fonctionnalités clés 30
Restauration des paramètres par défaut définis en usine 32
Exécution de tâches de configuration de base 33
Modification du mot de passe administrateur par défaut 33
Mise à niveau de votre microprogramme après votre première connexion 34
Sauvegarde de la configuration 35

Chapitre 2 : Assistants de configuration 36

Utilisation de l'assistant de configuration pour paramétrer la configuration initiale 37
Lancement de l'assistant de configuration 38
Configuration des informations d'identification du compte Cisco.com 39
Activation de la mise à niveau du microprogramme 40
Validation de la licence de sécurité 40
Activation des protocoles Bonjour et CDP (CDP Discovery Protocol) 41
Configuration de l'administration à distance 42
Configuration des ports physiques 43
Configuration du WAN principal 44
Configuration du WAN secondaire 44
Configuration de la redondance du WAN 44
Configuration des paramètres LAN par défaut 45

Configuration de la DMZ 47
Configuration des services DMZ 48
Configuration des paramètres de la radio sans fil 49
Configuration de l'accès WLAN Intranet 50
Configuration des services de sécurité 51
Affichage du résumé de la configuration 53
Utilisation de l'assistant double WAN pour configurer les paramètres de redondance WAN 53
Démarrage de l'assistant double WAN 54
Configuration d'un port configurable comme port WAN secondaire 54
Configuration du WAN principal 54
Configuration du WAN secondaire 54
Configuration de la redondance du WAN 55
Configuration de la détection des défaillances du réseau 56
Affichage du résumé de la configuration 56
Utilisation de l'assistant VPN d'accès à distance pour configurer l'accès à distance IPsec ou SSL 57
Utilisation de l'assistant VPN d'accès à distance pour configurer l'accès à distance IPsec 57
Lancement de l'assistant VPN d'accès à distance avec l'accès à distance IPsec 58
Configuration de la stratégie de groupe d'accès à distance IPsec 58
Configuration des paramètres WAN 59
Configuration du mode de fonctionnement 59
Configuration des paramètres de contrôle d'accès 60
Configuration des paramètres DNS et WINS 60
Configuration des serveurs de secours 61
Configuration de la transmission tunnel partagée 61
Affichage du résumé de la stratégie de groupe 62
Configuration des groupes d'utilisateurs d'accès à distance IPsec 62
Affichage du résumé de l'accès à distance IPsec 63
Utilisation de l'assistant VPN d'accès à distance pour configurer l'accès à distance SSL 63
Lancement de l'assistant VPN d'accès à distance avec l'accès à distance SSL 63
Configuration de la passerelle VPN SSL 64
Configuration de la stratégie de groupe VPN SSL 66

Configuration des groupes d'utilisateurs VPN SSL 69
Affichage du résumé VPN SSL 70
Utilisation de l'assistant VPN de site à site pour configurer le VPN de site à site 70
Lancement de l'assistant VPN de site à site 71
Configuration des paramètres des homologues VPN 71
Configuration des stratégies IKE 72
Configuration des stratégies de transformation 73
Configuration des réseaux locaux et distants 74
Affichage du résumé de la configuration 75
Utilisation de l'assistant DMZ pour configurer les paramètres DMZ 76
Lancement de l'assistant DMZ 76
Configuration des profils DDNS 76
Configuration du réseau DMZ 77
Configuration des services DMZ 79
Affichage du résumé de la configuration 80
Utilisation de l'assistant sans fil pour configurer les paramètres sans fil (pour l'ISA550W et l'ISA570W uniquement) 81
Lancement de l'assistant sans fil 81
Configuration des paramètres de la radio sans fil 81
Configuration des types de connectivité sans fil 82
Spécifier les paramètres de connectivité sans fil pour tous les SSID activés 83
Affichage du résumé de la configuration 83
Configuration du SSID pour l'accès WLAN Intranet 83
Configuration du SSID pour l'accès WLAN invité 85
Configuration du SSID pour l'accès au portail captif 86

Chapitre 3 : Status 89

Tableau de bord de l'état du périphérique 89
État du réseau 93
Récapitulatif de l'état 93
Statistiques de trafic 96
Rapports d'utilisation 97

Rapports de la bande passante WAN 99
Table ARP 100
Liaisons DHCP 100
État du STP 101
Voisinage CDP 103
État sans fil (pour l'ISA550W et l'ISA570W uniquement) 104
État du réseau sans fil 104
Client Status 105
NAT Status 105
État du VPN 106
IPsec VPN Status 106
SSL VPN Status 108
Active User Sessions 111
Security Services Reports 111
Rapport de sécurité Web 112
Rapport antivirus 113
Email Security Report 114
Rapport de réputation du réseau 115
IPS Report 116
Application Control Report 117
System Status 118
Processus 118
Utilisation des ressources 119

Chapitre 4 : Mise en réseau 120

Affichage de l'état du réseau 121
Configuration du routage IPv4 ou IPv6 121
Gestion des ports 122
Affichage de l'état des interfaces physiques 122
Configuration des ports physiques 123
Configuration de la mise en miroir des ports 125
Configuration du contrôle d'accès basé sur les ports (802.1x) 125

Configuration du WAN 128
Configuration des paramètres du WAN pour votre connexion internet 128
Configuration de la redondance du WAN 136
Équilibrage de charge pour la redondance du WAN 136
Configuration de la détection de basculement de liaison 138
Équilibrage de charge avec l'exemple de configuration du PBR 139
Configuration du DNS dynamique 140
Mesure et limitation du trafic avec l'utilitaire de contrôle du trafic 142
Configuration d'un VLAN 144
Configuration de la DMZ 147
Configuration des zones 152
Niveaux de sécurité des zones 152
Zones prédéfinies 153
Configuration des zones 154
Configuration des IP DHCP réservés 155
Configuration du routage 156
Affichage de la table de routage 156
Configuration du mode de routage 157
Configuration du routage statique 157
Configuration du routage dynamique - RIP 158
Configuration du PBR 159
Configuration de la qualité de service 161
Paramètres QoS généraux 162
Configuration de la QoS WAN 162
Gestion de la bande passante WAN pour le trafic en amont 163
Configuration des paramètres de file d'attente WAN 163
Configuration des sélecteurs de trafic 165
Configuration des profils de la stratégie QoS WAN 167
Configuration des règles de classe QoS WAN 167
Mappage des profils de stratégie QoS WAN aux interfaces WAN 168
Exemple de configuration de QoS WAN 169
Configuration de la QoS WAN pour le trafic voix du LAN au WAN 171
Configuration de la QoS WAN pour le trafic voix du WAN au LAN 173

Configuration de la QoS LAN 174
Configuration des paramètres de file d'attente LAN 174
Configuration des méthodes de classification QoS du LAN 175
Mappage de la CoS à la file LAN 175
Mappage du DSCP à la file LAN 176
Configuration de la CoS par défaut 176
Configuration de la QoS sans fil 176
Paramètres par défaut de la QoS sans fil 177
Configuration des méthodes de classification QoS sans fil 178
Mappage de la CoS à la file d'attente sans fil 178
Mappage du DSCP à la file d'attente sans fil 178
Configuration IGMP 179
Configuration VRRP 180
Gestion d'adresse 182
Configuration des adresses 182
Configuration des groupes d'adresses 183
Gestion des services 184
Configuration des services 184
Configuration des groupes de services 185
Configuration du portail captif 186

Chapitre 5 : Sans fil (pour ISA550W et ISA570W uniquement) 190

Affichage de l'état du réseau sans fil 191
Affichage des statistiques relatives aux réseaux sans fil 191
Affichage de l'état du client sans fil 192
Configuration des paramètres de base 192
Configuration des profils SSID 194
Configuration de la sécurité sans fil 195
Contrôle de l'accès sans fil par le biais des adresses MAC 202
Mappage du SSID au VLAN 203
Configuration de la programmation SSID 204

Configuration de Wi-Fi Protected Setup 205
Configuration du portail captif 207
Configuration de la détection des points d'accès indésirables sans fil 211
Advanced Radio Settings 212

Chapitre 6 : Pare-feu 215

Configuration des règles de pare-feu pour contrôler le trafic entrant et sortant 216
À propos des zones de sécurité 216
Paramètres du pare-feu par défaut 218
Priorités des règles de pare-feu 219
Tâches préliminaires de configuration des règles de pare-feu 220
Paramètres de pare-feu généraux 220
Configuration d'une règle de pare-feu 222
Configuration d'une règle de pare-feu pour autoriser le trafic de diffusion 224
Configuration des paramètres de consignation du pare-feu 225
Configuration des règles NAT pour accéder en toute sécurité à un réseau à distance 226
Affichage de l'état de la traduction NAT 227
Priorités des règles NAT 228
Configuration des règles de PAT dynamique 229
Configuration des règles NAT statiques 230
Configuration des règles de transfert de port 231
Configuration des règles de déclenchement de port 233
Configuration des règles NAT avancées 234
Configuration d'alias IP pour les règles NAT avancées 236
Configuration d'une règle NAT avancée pour prendre en charge la reconnexion NAT 238
Exemples de configuration d'une règle de pare-feu et NAT 239
Autorisation du trafic entrant vers un serveur FTP interne à l'aide de l'adresse IP WAN 240
Autorisation du trafic entrant vers un serveur RDP à l'aide d'une adresse IP publique spécifiée 241
Autorisation du trafic entrant en provenance de l'intervalle spécifié des hôtes externes 244

Blocage du trafic sortant par programmation et par plage d'adresses IP 246
Blocage du trafic sortant vers un serveur de messagerie hors site 246
Configuration du filtrage du contenu pour contrôler l'accès à internet 247
Configuration des profils de stratégie de filtrage du contenu 247
Configuration de la liste de contrôle d'accès aux sites Web 248
Mappage des profils de stratégie de filtrage du contenu aux zones 249
Configuration des paramètres avancés du filtrage du contenu 250
Configuration du filtrage des adresses MAC pour autoriser ou bloquer le trafic 251
Configuration de la liaison IP-MAC pour empêcher l'usurpation d'adresse 252
Configuration de la protection contre les attaques 253
Configuration des limites de session 255
Configuration de la passerelle de niveau application 255

Chapitre 7 : Services de sécurité 257

À propos des services de sécurité 258
Activation des services de sécurité 259
Priorité des services de sécurité 260
Tableau de bord des services de sécurité 260
Affichage des rapports de services de sécurité 262
Affichage du rapport de sécurité Web 262
Affichage du rapport antivirus 264
Affichage du rapport de sécurité de la messagerie 265
Affichage du rapport de réputation de réseau 266
Affichage du rapport IPS 267
Affichage du rapport de contrôle des applications 268
Configuration de l'antivirus 269
Paramètres antivirus généraux 270
Configuration des paramètres antivirus avancés 273
Configuration de la notification HTTP 274
Configuration de la notification par e-mail 275
Mise à jour des signatures antivirus 276

Configuration du contrôle des applications 277
Configuration des stratégies de contrôle des applications 277
Paramètres généraux de la stratégie de contrôle des applications 278
Ajout d'une stratégie de contrôle des applications 279
Autorisation ou blocage du trafic pour toutes les applications dans une catégorie 280
Autorisation ou blocage du trafic pour une application 282
Paramètres généraux du contrôle des applications 283
Activation du service de contrôle des applications 284
Mappage des stratégies de contrôle des applications aux zones 284
Configuration des règles de mappage de stratégie de contrôle des applications 285
Mise à jour la base de données de signatures des applications 286
Paramètres avancés du contrôle des applications 287
Configuration du filtre de courrier indésirable 289
Configuration de la prévention des intrusions 290
Configuration des actions de signature 293
Mise à jour de la base de données de signatures IPS 294
Configuration du filtrage par réputation Web 296
Configuration du filtrage URL Web 298
Configuration des profils de stratégie de filtrage URL Web 298
Configuration de la liste de contrôle d'accès aux sites Web 299
Mappage des profils de stratégie de filtrage URL Web aux zones 300
Configuration des paramètres avancés du filtrage URL Web 301
Réputation de réseau 302

Chapitre 8 : VPN 303

À propos des VPN 304
Affichage de l'état du VPN 305
Affichage de l'état du VPN IPsec 305
Affichage de l'état du VPN SSL 307
Configuration d'un VPN de site à site 309
Tâches de configuration pour établir un tunnel VPN de site à site 310
Paramètres VPN généraux de site à site 311
Configurer des stratégies VPN IPsec 312
Configuration des stratégies IKE 319

Configuration des ensembles de transformation 321
Exemples de configuration de télétravailleur distant 322
Configuration d'un accès à distance IPsec 325
Compatibilité du client VPN Cisco 326
Activation de l'accès à distance IPsec 327
Configuration des stratégies de groupe d'accès à distance IPsec 328
Configuration de règles NAT avancées pour permettre aux clients VPN distants d'accéder à Internet via les tunnels VPN 331
Configuration du client VPN pour télétravailleurs 334
Serveur VPN IPsec requis 335
Avantages de la fonctionnalité de client VPN pour télétravailleurs 336
Modes de fonctionnement 336
Mode Client 337
Mode NEM 338
Paramètres généraux de client VPN pour télétravailleurs 339
Configuration des stratégies de groupe de client VPN pour télétravailleurs 340
Configuration VPN SSL 344
Éléments du VPN SSL 346
Tâches de configuration pour l'établissement d'un tunnel VPN SSL 346
Installation du client à mobilité sécurisé Cisco AnyConnect 347
Certificats d'importation pour l'authentification des utilisateurs 348
Configuration des utilisateurs VPN SSL 348
Configuration de la passerelle VPN SSL 349
Configuration des stratégies de groupe VPN SSL 351
Accès au portail VPN SSL 354
Configuration des règles NAT avancées pour autoriser les clients VPN SSL à accéder à Internet via les tunnels VPN SSL 355
Configuration d'un serveur L2TP 357
Configuration du transfert VPN 359

Chapitre 9 : Gestion des utilisateurs 360

Affichage des sessions utilisateur actives 360

Configuration d'utilisateurs et de groupes d'utilisateurs 361
Groupe d'utilisateurs et utilisateur par défaut 361
Services disponibles pour les groupes d'utilisateurs 362
Préemption des administrateurs 362
Configuration des utilisateurs locaux 363
Configuration des groupes d'utilisateurs locaux 364
Configuration des paramètres d'authentification des utilisateurs 365
Utilisation d'une base de données locale pour l'authentification des utilisateurs 366
Utilisation d'un serveur RADIUS pour l'authentification utilisateur 367
Utilisation de la base de données locale et du serveur RADIUS pour l'authentification des utilisateurs 370
Utilisation du protocole LDAP pour l'authentification des utilisateurs 371
Utilisation de la base de données locale et du protocole LDAP pour l'authentification 374
Configuration de serveurs RADIUS 374

Chapitre 10 : Gestion des périphériques 376

Affichage de l'état du système 377
Affichage de l'état des processus 377
Affichage de l'utilisation des ressources 377
Administration 378
Configuration des paramètres d'administration 379
Configuration de l'administration à distance 380
Configuration des paramètres d'alerte par courriel 382
La configuration SNMP 389
Sauvegarde et restauration d'une configuration 391
Gestion des certificats pour l'authentification 393
Affichage de l'état et des détails des certificats 394
Exportation de certificats vers votre PC local 395
Exportation de certificats vers un périphérique USB 396
Importation de certificats depuis votre PC local 396
Importation de certificats depuis un périphérique USB 397
Génération de nouvelles demandes de signature de certificat 397

Importation d'un certificat signé pour CSR depuis votre PC local 398
Configuration des paramètres d'assistance et des services Cisco 399
Configuration d'un compte Cisco.com 399
Configuration de Cisco OnPlus 400
Configuration des paramètres d'assistance à distance 401
Envoi de contenus pour les diagnostics système 401
Configuration de l'heure système 402
Configuration des propriétés du périphérique 403
Utilitaires de diagnostic 404
Ping 404
Traceroute 405
DNS Lookup 405
Capture de paquet 406
Protocoles de détection de périphériques 406
UPnP Discovery 407
Bonjour Discovery 408
Détection CDP 409
Détection LLDP 410
Gestion du microprogramme 410
Affichage des informations sur le microprogramme 411
Utilisation du microprogramme secondaire 412
Mise à niveau de votre microprogramme à partir du site Cisco.com 413
Mise à niveau de votre microprogramme à partir d'une image de microprogramme stockée sur votre PC ou sur un périphérique USB 414
Mécanisme de basculement automatique du microprogramme 415
Utilisation du mode Rescue pour récupérer le système 416
Gestion de la licence de sécurité 417
Vérification de l'état de la licence de sécurité 417
Installation ou renouvellement de la licence de sécurité 418
Gestion des journaux 421
Affichage des journaux 421

Configuration des paramètres de journal 423
Configuration des composants journaux 426
Réamorçage et réinitialisation du périphérique 427
Restauration des paramètres par défaut définis en usine 427
Réinitialisation de l'appareil de sécurité 428
Configuration des programmations 429

Annexe A : Dépannage 431

Connexion Internet 431
Date et heure 434
Test ping pour tester la connectivité LAN 435
Évaluation du chemin LAN de votre PC à votre appareil de sécurité 435
Évaluation du chemin LAN de votre PC à un périphérique distant 436

Annexe B : Spécifications techniques et exigences environnementales 437

Annexe C : Paramètres d'usine par défaut 439

Gestion des périphériques 439
Gestion des utilisateurs 441
Mise en réseau 442
Sans fil 445
VPN 446
Services de sécurité 448
Pare-feu 449
Rapports 450
Objets de services par défaut 451
Objets d'adresse par défaut 455

Annexe D : Problèmes et solutions 456

1

Démarrage

Ce chapitre présente l'appareil de sécurité intégré de la gamme Cisco ISA500 et décrit les tâches de configuration de base pour vous permettre de configurer votre Cisco ISA500. Il comprend les sections suivantes :

- **Introduction, page 20**
- **Présentation du produit, page 21**
- **Mise en route à l'aide de l'utilitaire de configuration, page 25**
- **Paramètres d'usine par défaut, page 30**
- **Exécution de tâches de configuration de base, page 33**

REMARQUE Pour obtenir des informations sur la manière d'installer physiquement votre Cisco ISA500, reportez-vous au guide de démarrage rapide des Cisco ISA500 Integrated Security Appliances à l'adresse suivante : www.cisco.com/go/isa500resources.

Introduction

Nous vous remercions d'avoir choisi l'appareil de sécurité intégré de la gamme Cisco ISA 500, appartenant à la gamme Cisco Small Business. La gamme ISA500 est un ensemble d'appareils de sécurité de gestion unifiée des menaces (UTM). Ces appareils fournissent des solutions professionnelles de passerelle de sécurité avec une prise en charge des fonctionnalités de WAN double, DMZ, pare-feu par zone, VPN de site à site et d'accès à distance (y compris l'accès à distance IPsec, le client VPN pour télétravailleurs et VPN SSL), ainsi que la protection contre les menaces Internet (par exemple, le système de prévention des intrusions (IPS), un antivirus, le contrôle des applications, le filtrage URL Web, le filtrage par réputation des sites Web, un filtre de courrier indésirable et la réputation de réseau). Les modèles ISA550W et ISA570W incluent les fonctionnalités de point d'accès 802.11b/g/n.

Le tableau suivant répertorie les numéros de modèle disponibles.

Modèle	Description	Configuration
ISA550	Cisco ISA550 Integrated Security Appliance	1 port WAN, 2 ports LAN, 4 ports configurables et 1 port USB 2.0
ISA550W	Cisco ISA550 Integrated Security Appliance avec Wi-Fi	1 port WAN, 2 ports LAN, 4 ports configurables, 1 port USB 2.0 et 802.11b/g/n
ISA570	Cisco ISA570 Integrated Security Appliance	1 port WAN, 4 ports LAN, 5 ports configurables et 1 port USB 2.0
ISA570W	Cisco ISA570 Integrated Security Appliance avec Wi-Fi	1 port WAN, 4 ports LAN, 5 ports configurables, 1 port USB 2.0 et 802.11b/g/n

REMARQUE Chaque port configurable peut être configuré comme port WAN, DMZ ou LAN. Vous ne pouvez configurer qu'un seul port WAN à la fois. Vous pouvez configurer jusqu'à 4 ports DMZ en tout.

Présentation du produit

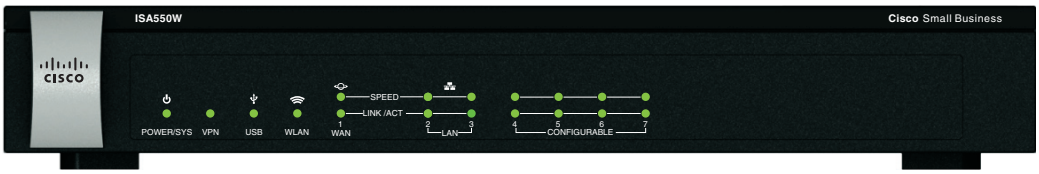
Avant d'utiliser l'Cisco ISA500, familiarisez-vous avec les voyants de la façade avant et les ports du panneau arrière.

- **Panneau avant, page 21**
- **Panneau arrière, page 23**

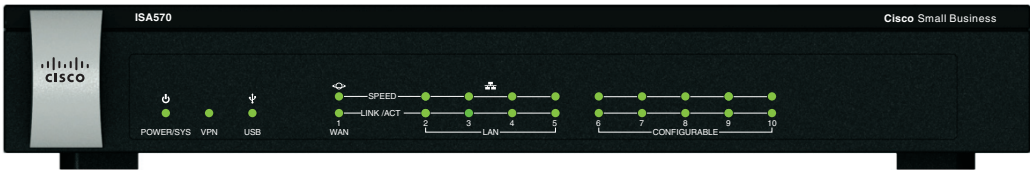
Panneau avant

ISA550 : façade

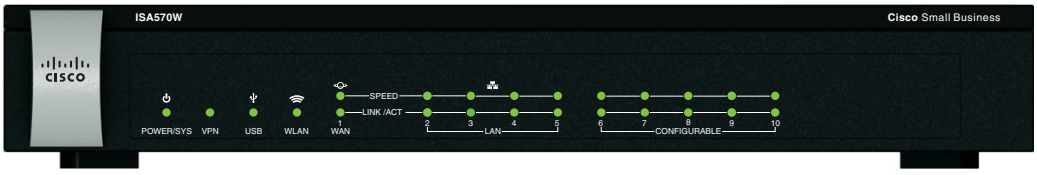
ISA550W : façade



ISA570 : façade



ISA570W : façade



Voyants du panneau avant

Le tableau suivant décrit les voyants de la façade du Cisco ISA500. Ces voyants permettent de surveiller l'activité du système.

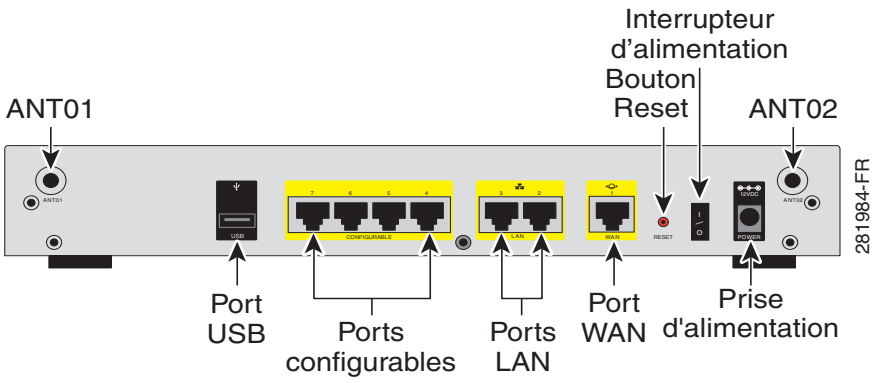
Voyant	Description
POWER/SYS	Indique l'état de l'alimentation et du système. ▪ Le voyant vert fixe indique que le système est sous tension et fonctionne normalement. ▪ Le voyant vert clignote lors du démarrage du système. ▪ Le voyant jaune fixe signale un problème de démarrage, une erreur de fonctionnement ou un problème relatif au système.
VPN	Indique l'état d'une connexion VPN site à site. ▪ Le voyant vert fixe indique que les connexions VPN site à site sont activées. ▪ Le voyant vert clignotant indique que le système tente d'établir un tunnel VPN site à site. ▪ Le voyant jaune clignotant indique que le système ne parvient pas à configurer la connexion VPN site à site ou qu'aucune connexion VPN site à site n'est disponible.
USB	Indique l'état d'un périphérique USB. ▪ Le voyant vert fixe indique qu'un périphérique USB est détecté et fonctionne normalement. ▪ Le voyant vert clignotant indique que l'appareil USB transfère et reçoit des données.
WLAN **(ISA550W et ISA570W uniquement)**	Indique l'état WLAN. ▪ Le voyant vert fixe indique que le WLAN fonctionne. ▪ Le voyant vert clignotant indique que le WLAN transfère et reçoit des données.

Voyant	Description
SPEED	Indique le débit du trafic du port associé. ▪ Désactivé lorsque le débit du trafic est de 10 ou 100 Mbit/s. ▪ Le voyant est vert fixe lorsque le débit de trafic est de 1 000 Mbit/s.
LINK/ACT	Indique qu'une connexion avec le port est en cours. ▪ Vert fixe lorsque la connexion est active. ▪ Le voyant vert clignotant indique que le port transfère et reçoit des données.

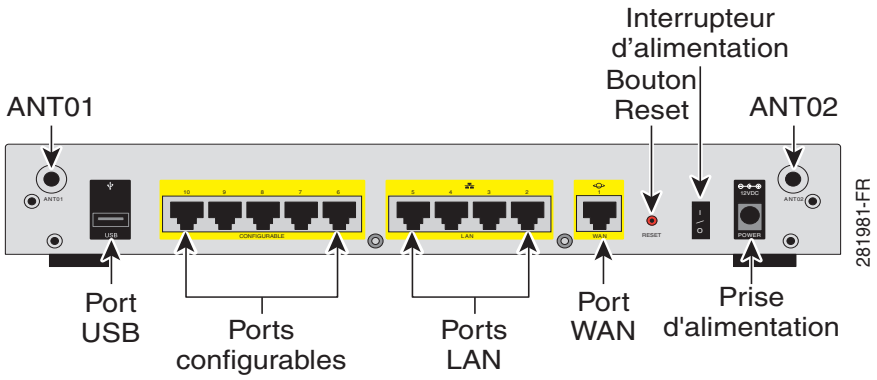
Panneau arrière

Le panneau arrière permet de connecter les périphériques réseau. Les ports situés sur le panneau peuvent varier en fonction du modèle.

ISA550 et ISA550W : panneau arrière



ISA570 et ISA570W : panneau arrière



Description du panneau arrière

Fonctionnalité	Description
ANT01/ANT02	Connecteurs filetés pour les antennes **(pour ISA550W et ISA570W uniquement)**.
Port USB	Permet de connecter un périphérique USB à l'appareil. Utilisez un périphérique USB pour enregistrer et rétablir la configuration du système ou mettre à jour le microprogramme.
Ports configurables	Peuvent être configurés comme ports WAN, LAN ou DMZ. Le ISA550 et le ISA550W disposent de 4 ports configurables. Le ISA570 et le ISA570W disposent de 5 ports configurables. **REMARQUE** : Vous ne pouvez configurer qu'un seul port WAN à la fois. Vous pouvez configurer jusqu'à 4 ports DMZ en tout.
Ports LAN	Connectent les ordinateurs et les autres appareils réseau à l'unité. Le ISA550 et le ISA550W disposent de 2 ports LAN dédiés. Le ISA570 et le ISA570W disposent de 4 ports LAN dédiés.
Port WAN	Permet de connecter l'appareil à un modem câble ou ADSL, ou à un appareil doté d'une connectivité WAN.

Fonctionnalité	Description
Bouton RESET	Pour redémarrer l'appareil, maintenez le bouton RESET enfoncé pendant moins de 3 secondes. Pour restaurer les paramètres d'usine par défaut de l'appareil, maintenez le bouton RESET enfoncé pendant plus de 3 secondes, Lorsque l'appareil est allumé et que le voyant POWER/SYS est vert fixe. Le voyant vert POWER/SYS clignotant indique que le système redémarre.
Interrupteur d'alimentation	Il permet de mettre l'unité sous tension ou hors tension.
Prise d'alimentation	Permet d'alimenter l'appareil à l'aide du cordon d'alimentation et de l'adaptateur fournis.

Mise en route à l'aide de l'utilitaire de configuration

L'utilitaire de configuration de la gamme ISA500 est un gestionnaire de périphériques Web permettant de mettre l'Cisco ISA500 en service. Pour utiliser cet utilitaire, vous devez pouvoir vous connecter à l'Cisco ISA500 depuis un PC ou un ordinateur portable. Vous pouvez accéder à l'utilitaire de configuration à l'aide des navigateurs web suivants :

- Microsoft Internet Explorer 8 et 9
- Mozilla Firefox 3.6.x, 5 et 6

REMARQUE La résolution d'écran minimale recommandée pour le PC exécutant le navigateur web utilisé pour accéder à l'utilitaire de configuration est 1 024 x 768.

Cette section comprend les rubriques suivantes :

- **Connexion à l'utilitaire de configuration, page 26**
- **Navigation dans l'utilitaire de configuration, page 27**
- **Utilisation du système d'aide, page 28**
- **Icônes de l'utilitaire de configuration, page 28**

Connexion à l'utilitaire de configuration

ÉTAPE 1 Connectez votre ordinateur à un port LAN disponible sur le panneau arrière.

Votre ordinateur devient un client DHCP du Cisco ISA500 et reçoit une adresse IP comprise dans la plage 192.168.75.x.

ÉTAPE 2 Ouvrez un navigateur Web. Dans la barre d'adresse, saisissez l'adresse IP par défaut du LAN de l'Cisco ISA500 : **192.168.75.1**.

REMARQUE : L'adresse ci-dessus est l'adresse LAN des paramètres d'usine par défaut. Si vous modifiez ce paramètre, saisissez la nouvelle adresse IP pour vous connecter à l'utilitaire de configuration.

ÉTAPE 3 Lorsque la page de connexion s'affiche, saisissez le nom d'utilisateur et le mot de passe.

Le nom d'utilisateur par défaut est **cisco**. Le mot de passe par défaut est **cisco**. Les noms d'utilisateurs et les mots de passe sont sensibles à la casse.

ÉTAPE 4 Cliquez sur **Login**.

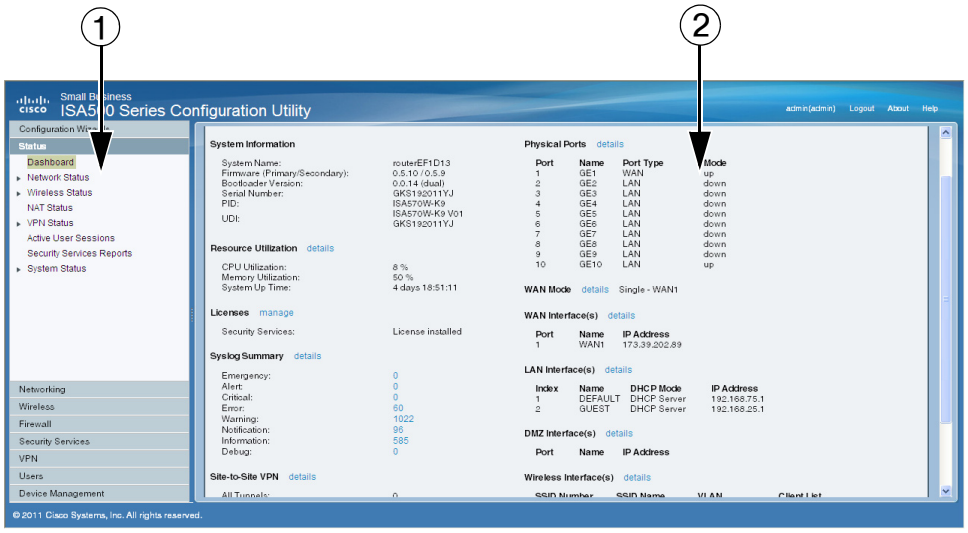
ÉTAPE 5 Pour des raisons de sécurité, vous devez changer le mot de passe par défaut du compte de l'administrateur par défaut. Définissez un nouveau mot de passe administrateur et cliquez sur **OK**.

ÉTAPE 6 Si vous pouvez accéder à Internet et qu'un microprogramme plus récent est détecté, la fenêtre Firmware Upgrade s'ouvre. Suivez les instructions affichées à l'écran pour télécharger et installer le microprogramme. Reportez-vous à la section **Mise à niveau de votre microprogramme après votre première connexion, page 34**.

ÉTAPE 7 Si vous ne pouvez pas accéder à Internet ou si vous utilisez la dernière version du microprogramme, l'assistant de configuration démarre. Suivez les invites affichées à l'écran pour effectuer la configuration initiale. Reportez-vous à la section **Utilisation de l'assistant de configuration pour paramétrer la configuration initiale, page 37**.

Navigation dans l'utilitaire de configuration

Utilisez le volet de navigation gauche pour effectuer les tâches dans l'utilitaire de configuration.



Numéro	Component	Description
1	Volet de navigation gauche	Le volet de navigation gauche permet de naviguer facilement entre les différentes fonctionnalités configurables. Vous pouvez développer les branches principales pour afficher les fonctionnalités. Cliquez sur le titre de la branche principale pour développer son contenu. Cliquez sur le triangle en regard d'une fonctionnalité pour développer ou réduire ses sous-fonctionnalités. Cliquez sur le titre d'une fonctionnalité ou d'une sous-fonctionnalité pour l'ouvrir.
2	Contenu principal	Le contenu principal de la fonctionnalité ou sous-fonctionnalité s'affiche dans cette zone.

Utilisation du système d'aide

L'utilitaire de configuration fournit un fichier d'aide contextuelle pour toutes les tâches de configuration. Pour afficher la page d'aide, cliquez sur le lien **Help** dans l'angle supérieur droit de l'écran. Une nouvelle fenêtre s'ouvre et fournit des informations sur la page que vous consultez actuellement.

Icônes de l'utilitaire de configuration

L'utilitaire de configuration dispose d'icônes pour les options de configuration couramment utilisées. Le tableau suivant décrit ces icônes :

Icône	Description	Action
	Icône d'ajout	Permet d'ajouter une entrée.
	Icône de modification	Permet de modifier une entrée.
	Icône de doublon	Permet de créer une copie d'une entrée existante.
	Icône de suppression	Permet de supprimer une entrée ou plusieurs entrées sélectionnées.
	Icône de déplacement	Permet de déplacer un élément à un emplacement spécifique.
	Icône de déplacement vers le bas	Permet de déplacer un élément d'une place vers le bas.
	Icône de déplacement vers le haut	Permet de déplacer un élément d'une place vers le haut.
	Icône de développement en forme de triangle	Permet de développer les sous-fonctionnalités d'une fonctionnalité dans le volet de navigation gauche ou de développer les éléments sous une catégorie.
	Icône de réduction en forme de triangle	Permet de réduire les sous-fonctionnalités d'une fonctionnalité dans le volet de navigation gauche ou de réduire les éléments sous une catégorie.
	Icône de connexion	Permet d'établir une connexion VPN.

Icône	Description	Action
	Icône de déconnexion	Permet de mettre fin à une connexion VPN ou à une session utilisateur active.
	Icône d'autorisation forcée	Permet de désactiver le contrôle d'accès 802.1x et entraîne la transition du port à l'état autorisé sans qu'aucun échange d'authentification ne soit requis.
	Icône d'interdiction forcée	Entraîne le maintien du port à l'état non-autorisé, en ignorant toutes les tentatives d'authentification effectuées par le client.
	Icône Auto	Permet d'activer le contrôle d'accès 802.1x et entraîne le démarrage du port à l'état non-autorisé, en autorisant uniquement l'envoi et la réception de trames EAPOL via le port.
	Icône d'importation depuis un PC	Permet d'importer un certificat local ou un certificat CA depuis un PC.
	Icône d'exportation vers USB ou d'importation depuis USB	Permet l'exportation d'un certificat local, d'un certificat CA ou d'une demande de signature de certificat vers une clé USB ou l'importation d'un certificat local ou d'un certificat CA depuis une clé USB.
	Icône Détails	Permet l'affichage des détails d'un certificat ou d'une demande de signature de certificat.
	Icône de téléchargement (sur)	Permet de télécharger un certificat local, un certificat CA ou une demande de signature de certificat sur un PC.
	Icône de téléchargement (vers)	Permet de télécharger un certificat signé pour la demande de signature de certificat depuis un PC.
	Icône d'installation ou de renouvellement	Permet d'installer la licence de sécurité.
	Icône d'actualisation	Permet d'actualiser les données.
	Icône de réinitialisation	Permet de réinitialiser le périphérique sur les paramètres d'usine par défaut ou de renouveler la licence de sécurité.

Icône	Description	Action
	Icône de recherche des mises à jour	Permet de rechercher immédiatement les nouvelles mises à jour de signatures à partir du serveur de signatures Cisco.
	Icône des références	Permet d'afficher les informations d'identification du périphérique.
	Icône d'alerte par courriel	Permet d'afficher ou de configurer les paramètres des alertes par courriel.

Paramètres d'usine par défaut

L'Cisco ISA500 est préconfiguré avec certains paramètres pour permettre de commencer à l'utiliser avec des modifications minimes. Selon les exigences de votre fournisseur de services Internet (FAI) et les besoins de votre entreprise, vous serez peut-être amené à modifier certains paramètres. Vous pouvez utiliser l'utilitaire de configuration pour personnaliser tous les paramètres, si nécessaire.

Cette section comprend les rubriques suivantes :

- **Paramètres par défaut des fonctionnalités clés, page 30**
- **Restauration des paramètres par défaut définis en usine, page 32**

Paramètres par défaut des fonctionnalités clés

Les paramètres par défaut des fonctionnalités clés sont décrits ci-dessous. Pour obtenir une liste complète de tous les paramètres d'usine par défaut, reportez-vous à la section **Paramètres d'usine par défaut, page 439**.

- **Mode de routage IP** : par défaut, seul le mode IPv4 est activé. Pour prendre en charge les adressages IPv6 et IPv4, activez le mode IPv4/IPv6. Reportez-vous à la section **Configuration du routage IPv4 ou IPv6, page 121**.
- **Configuration WAN** : par défaut, l'Cisco ISA500 est configuré pour obtenir une adresse IP auprès de votre FAI à l'aide du protocole DHCP (Dynamic Host Configuration Protocol). Selon les exigences de votre FAI, configurez le mode d'adressage réseau du WAN principal. Vous pouvez également modifier les autres paramètres WAN. Reportez-vous à la section **Configuration des paramètres du WAN pour votre connexion internet, page 128**.

- **Configuration LAN** : par défaut, le LAN de l'Cisco ISA500 est configuré dans le sous-réseau 192.168.75.0 et l'adresse IP LAN est 192.168.75.1. L'Cisco ISA500 agit comme un serveur DHCP pour les hôtes du réseau LAN. Il peut automatiquement attribuer des adresses IP et des adresses de serveur DNS aux ordinateurs et aux autres périphériques du LAN. Pour la plupart des scénarios de déploiement, les paramètres DHCP et TCP/IP par défaut doivent être satisfaisants. Toutefois, vous pouvez modifier l'adresse de sous-réseau ou l'adresse IP par défaut. Reportez-vous à la section **Configuration d'un VLAN, page 144**.
- **VLAN Configuration** : l'Cisco ISA500 prédéfinit un VLAN natif (DEFAULT) et un VLAN invité (GUEST). Vous pouvez personnaliser les VLAN prédéfinis ou en créer de nouveaux pour répondre à vos besoins professionnels spécifiques. Reportez-vous à la section **Configuration d'un VLAN, page 144**.
- **Ports configurables** : chaque port configurable peut être configuré comme port WAN, DMZ ou LAN. Par défaut, tous les ports configurables sont configurés comme ports LAN. Vous ne pouvez configurer qu'un seul port WAN à la fois (reportez-vous à la section **Configuration du WAN, page 128**). Vous pouvez configurer jusqu'à quatre ports DMZ en tout (reportez-vous à la section **Configuration de la DMZ, page 147**).
- **Réseau sans fil (pour ISA550W et ISA570W uniquement)** : les modèles ISA550W et ISA570W sont configurés avec quatre SSID. Par défaut, tous les SSID sont désactivés. Pour des raisons de sécurité, nous vous recommandons vivement de configurer les SSID avec les paramètres de sécurité appropriés. Reportez-vous à la section **Sans fil (pour ISA550W et ISA570W uniquement), page 190**.
- **Accès administratif** : vous pouvez accéder à l'utilitaire de configuration en utilisant un navigateur web côté LAN et en entrant l'adresse IP LAN par défaut (192.168.75.1). Vous pouvez ouvrir une session en saisissant le nom d'utilisateur (**cisco**) et le mot de passe (**cisco**) du compte d'administrateur par défaut. Pour éviter tout accès non autorisé, vous devez immédiatement changer le mot de passe administrateur à la première connexion et êtes encouragé à modifier le nom d'utilisateur du compte d'administrateur par défaut. Reportez-vous à la section **Modification du mot de passe administrateur par défaut, page 33**.
- **Services de sécurité** : par défaut, les services de sécurité, tels que le système de prévention des intrusions (IPS), l'antivirus, le contrôle des applications, le filtrage URL Web, le filtrage par réputation des sites Web et le filtre de courrier indésirable, sont désactivés. Reportez-vous au **Chapitre 7, « Services de sécurité. »**

- **Pare-feu** : par défaut, le pare-feu bloque le trafic entrant et autorise tout le trafic sortant. Si vous souhaitez autoriser une partie du trafic entrant ou bloquer une partie du trafic sortant, vous devez personnaliser des règles de pare-feu. Jusqu'à 100 règles personnalisées de pare-feu peuvent être configurées sur l'Cisco ISA500. Reportez-vous à la section **Configuration des règles de pare-feu pour contrôler le trafic entrant et sortant, page 216**.
- **VPN** : cette fonctionnalité est désactivée par défaut. L'Cisco ISA500 peut fonctionner comme serveur VPN IPsec, client VPN pour télétravailleurs ou comme passerelle VPN SSL afin que les utilisateurs distants puissent accéder en toute sécurité aux ressources réseau de l'entreprise via des tunnels VPN. Vous pouvez également établir un tunnel VPN IPsec sécurisé entre deux sites physiquement séparés à l'aide de la fonctionnalité VPN de site à site. Reportez-vous au chapitre **VPN, page 303**.

Restauration des paramètres par défaut définis en usine

Pour rétablir les paramètres d'usine par défaut, effectuez l'une des actions suivantes :

- Lorsque l'appareil est allumé et que le voyant POWER/SYS est vert fixe, maintenez le bouton **RESET** enfoncé sur le panneau arrière de l'appareil pendant plus de 3 secondes. Relâchez le bouton et attendez le redémarrage de l'appareil. Le voyant vert POWER/SYS clignotant indique que le système redémarre.
- Sinon, lancez l'utilitaire de configuration et connectez-vous. Cliquez sur **Gestion de périphériques > Redémarrage/Réinitialisation** dans le volet de navigation gauche. Dans la zone **Reset Device**, cliquez sur **Reset to Factory Defaults**.

Après la restauration des paramètres d'usine par défaut, les paramètres suivants s'appliquent :

Paramètres	Valeur par défaut
Nom d'utilisateur	cisco
Mot de passe	cisco
LAN IP	192.168.75.1
DHCP Range	192.168.75.100 à 200

Exécution de tâches de configuration de base

Nous vous conseillons d'effectuer les tâches suivantes avant de configurer l'Cisco ISA500 :

- **Modification du mot de passe administrateur par défaut, page 33**
- **Mise à niveau de votre microprogramme après votre première connexion, page 34**
- **Sauvegarde de la configuration, page 35**

Modification du mot de passe administrateur par défaut

Le compte d'administrateur par défaut (« cisco ») dispose de privilèges complets pour définir la configuration et lire l'état du système. Pour des raisons de sécurité, vous devez changer le mot de passe administrateur par défaut à la première connexion.

ÉTAPE 1 Saisissez les informations suivantes :

- **User name** : saisissez le nom d'utilisateur actuel ou entrez-en un nouveau si vous souhaitez modifier le nom d'utilisateur par défaut.
- **New password** : saisissez un nouveau mot de passe administrateur. Les mots de passe sont sensibles à la casse.

  REMARQUE : Un mot de passe doit comporter au minimum 8 caractères et au moins trois des classes de caractères suivantes : lettres majuscules et minuscules, chiffres et caractères spéciaux. Ne répétez aucun mot de passe plus de trois fois sur une ligne. Ne définissez pas le nom d'utilisateur ou « cisco » comme mot de passe. Ne mettez pas ces mots en majuscule et ne les écrivez pas à l'envers.
- **Confirm password** : saisissez à nouveau le mot de passe administrateur pour le confirmer.

ÉTAPE 2 Cliquez sur **OK** pour enregistrer vos paramètres.

Mise à niveau de votre microprogramme après votre première connexion

L'Cisco ISA500 utilise un client IDA intégré pour interroger le microprogramme depuis le serveur Cisco IDA. Si un microprogramme plus récent est détecté lorsque vous vous connectez à l'utilitaire de configuration pour la première fois, nous vous recommandons d'effectuer une mise à niveau de votre microprogramme vers la version la plus récente avant d'exécuter une autre tâche. Cette fonctionnalité requiert une connexion WAN active permettant d'accéder à Internet.

ÉTAPE 1 Connectez-vous à l'utilitaire de configuration pour la première fois et modifiez le mot de passe administrateur par défaut. Reportez-vous à la section **Connexion à l'utilitaire de configuration, page 26**.

Si un microprogramme plus récent est détecté, la fenêtre Firmware Upgrade s'ouvre. Le numéro de version du microprogramme que vous utilisez actuellement et le numéro de la dernière version du microprogramme qui est détecté s'affichent.

ÉTAPE 2 Saisissez vos informations d'identification de compte Cisco.com dans les champs **Username** et **Password**.

Un compte Cisco.com valide est requis pour télécharger et installer le microprogramme depuis le site Cisco.com. Si vous n'en disposez pas, accédez à la page https:// tools.cisco.com/RPF/register/register.do en cliquant sur le lien **Create a Cisco.com Account** pour enregistrer un compte Cisco.com.

REMARQUE : Ignorez cette étape si vos identifiants de compte Cisco.com sont déjà configurés sur l'Cisco ISA500.

ÉTAPE 3 Cliquez sur **Continue**.

REMARQUE : vous pouvez cliquer sur **Install Later** pour mettre à niveau le microprogramme ultérieurement. Un lien **Upgrade Available** s'affiche dans le coin supérieur droit de l'écran et l'assistant de configuration démarre alors. Nous vous recommandons fortement de mettre à niveau le microprogramme immédiatement.

ÉTAPE 4 Validez vos identifiants de compte Cisco.com via Internet. Si vos identifiants de compte Cisco.com sont valides, l'Cisco ISA500 lance le téléchargement et l'installation du microprogramme. Ce processus peut prendre quelques minutes.

ÉTAPE 5 L'Cisco ISA500 redémarre une fois le microprogramme mis à niveau. Vous serez redirigé vers l'écran de connexion lorsque l'Cisco ISA500 redémarre.

ÉTAPE 6 Connectez-vous à nouveau à l'utilitaire de configuration. L'assistant de configuration démarre. Suivez les invites affichées à l'écran pour effectuer la configuration initiale. Reportez-vous à la section **Utilisation de l'assistant de configuration pour paramétrer la configuration initiale, page 37**.

REMARQUE Autres options pour mettre à niveau le microprogramme :

- Si vous ne parvenez pas à accéder à Internet lorsque vous vous connectez à l'utilitaire de configuration pour la première fois, vous pouvez utiliser l'assistant de configuration pour configurer votre connexion internet, puis rechercher automatiquement les mises à jour du microprogramme après l'exécution de l'assistant de configuration. L'assistant de configuration vous permet également de mettre à niveau le microprogramme manuellement à partir d'une image du microprogramme stockée sur votre PC local. Reportez-vous à la section **Utilisation de l'assistant de configuration pour paramétrer la configuration initiale, page 37**.
- Vous pouvez effectuer manuellement la mise à niveau du microprogramme à partir d'une image du microprogramme stockée sur votre PC ou sur un périphérique USB. Vous devez tout d'abord télécharger la dernière image du microprogramme depuis le site Cisco.com et l'enregistrer sur votre PC local ou sur un périphérique USB. Reportez-vous à la section **Mise à niveau de votre microprogramme à partir d'une image de microprogramme stockée sur votre PC ou sur un périphérique USB, page 414**.
- L'Cisco ISA500 recherche automatiquement les mises à jour du microprogramme à partir du serveur Cisco IDA toutes les 24 heures. Vous pouvez mettre à niveau votre microprogramme vers la dernière version si un microprogramme plus récent est disponible sur le site Web Cisco.com. Cette fonctionnalité requiert une connexion WAN active et nécessite qu'un compte Cisco.com valide soit configuré sur l'Cisco ISA500 au préalable. Reportez-vous à la section **Mise à niveau de votre microprogramme à partir du site Cisco.com, page 413**.

Sauvegarde de la configuration

Vous pouvez, à tout moment du processus, sauvegarder votre configuration. Si vous apportez ultérieurement des modifications que vous souhaitez abandonner, vous pouvez facilement rétablir la configuration sauvegardée. Reportez-vous à la section **Sauvegarde et restauration d'une configuration, page 391**.

2

Assistants de configuration

Ce chapitre explique comment utiliser les assistants de configuration pour configurer l'Cisco ISA500. Il comprend les sections suivantes :

- **Utilisation de l'assistant de configuration pour paramétrer la configuration initiale, page 37**
- **Utilisation de l'assistant double WAN pour configurer les paramètres de redondance WAN, page 53**
- **Utilisation de l'assistant VPN d'accès à distance pour configurer l'accès à distance IPsec ou SSL, page 57**
- **Utilisation de l'assistant VPN de site à site pour configurer le VPN de site à site, page 70**
- **Utilisation de l'assistant DMZ pour configurer les paramètres DMZ, page 76**
- **Utilisation de l'assistant sans fil pour configurer les paramètres sans fil (pour l'ISA550W et l'ISA570W uniquement), page 81**

Pour accéder aux pages des assistants de configuration, cliquez sur **Configuration Wizards** dans le volet de navigation de gauche.

Utilisation de l'assistant de configuration pour paramétrer la configuration initiale

Utilisez l'assistant de configuration pour configurer rapidement les fonctionnalités principales de l'Cisco ISA500, telles que les informations d'identification de compte Cisco.com, la licence de sécurité, l'administration à distance, les ports, les réseaux WAN et LAN, DMZ, la redondance WAN, WLAN (pour ISA550W et ISA570W uniquement) et les services de sécurité. Reportez-vous aux étapes suivantes :

- Lancement de l'assistant de configuration, page 38
- Configuration des informations d'identification du compte Cisco.com, page 39
- Activation de la mise à niveau du microprogramme, page 40
- Validation de la licence de sécurité, page 40
- Activation des protocoles Bonjour et CDP (CDP Discovery Protocol), page 41
- Configuration de l'administration à distance, page 42
- Configuration des ports physiques, page 43
- Configuration du WAN principal, page 44
- Configuration du WAN secondaire, page 44
- Configuration de la redondance du WAN, page 44
- Configuration des paramètres LAN par défaut, page 45
- Configuration de la DMZ, page 47
- Configuration des services DMZ, page 48
- Configuration des paramètres de la radio sans fil, page 49
- Configuration de l'accès WLAN Intranet, page 50
- Configuration des services de sécurité, page 51
- Affichage du résumé de la configuration, page 53

REMARQUE Avant d'utiliser l'assistant de configuration pour configurer l'Cisco ISA500, nous vous conseillons de disposer des éléments requis suivants :

- Une connexion WAN active pour vérifier les informations d'identification de compte Cisco.com, valider la licence de sécurité et mettre à niveau le microprogramme vers la dernière version obtenue à partir de Cisco.com.
- Un compte Cisco.com valide pour valider la licence de sécurité et mettre à niveau le microprogramme vers la dernière version obtenue à partir de Cisco.com. Pour souscrire à un compte Cisco.com, consultez le site https:// tools.cisco.com/RPF/register/register.do.
- La clé d'autorisation de produit (CAP) ou le code de licence, pour valider la licence de sécurité et activer les services de sécurité. Vous pouvez trouver le code de licence sur le certificat de demande de licence logicielle que Cisco fournit à l'achat de l'appliance de sécurité.

Lancement de l'assistant de configuration

ÉTAPE 1 Lorsque vous vous connectez à l'utilitaire de configuration pour la première fois, l'assistant de configuration peut démarrer automatiquement. Pour lancer l'assistant de configuration à tout moment, cliquez sur **Configuration Wizards > Setup Wizard**.

La page Getting Started apparaît. Si vous avez appliqué une configuration, le message d'avertissement suivant s'affiche : « Continuing with the Setup Wizard will overwrite some of your previously modified parameters ». Lisez attentivement ce message d'avertissement avant de commencer la configuration.

ÉTAPE 2 Cliquez sur **Next**.

Configuration des informations d'identification du compte Cisco.com

ÉTAPE 3 Reportez-vous à la page Cisco.com Credentials pour configurer vos informations d'identification de compte Cisco.com.

Un compte Cisco.com valide est requis pour télécharger la dernière image du microprogramme à partir de Cisco.com, valider la licence de sécurité, ainsi que rechercher les mises à jour des signatures à partir du serveur de signatures Cisco pour IPS, le contrôle des applications et l'antivirus. Si vous n'en possédez pas encore, accédez à la page https:// tools.cisco.com/RPF/register/register.do en cliquant sur le lien **Create a Cisco.com Account** pour souscrire à un compte Cisco.com.

- **Username** : entrez le nom d'utilisateur de votre compte Cisco.com.
- **Password** : entrez le mot de passe de votre compte Cisco.com.

ÉTAPE 4 Cliquez sur **Next**.

Si vous pouvez accéder à Internet, l'assistant de configuration valide vos informations d'identification de compte Cisco.com via Internet une fois que vous avez cliqué sur **Next**.

Si vous ne pouvez pas accéder à Internet, l'assistant de configuration suppose que vos informations d'identification de compte Cisco.com sont valides et vous permet de passer à l'étape suivante.

REMARQUE : vous pouvez configurer vos informations d'identification de compte Cisco.com à la page Device Management > Cisco Services & Support > Cisco.com Account une fois que vous avez fini d'exécuter l'assistant de configuration. Reportez-vous à la **Configuration d'un compte Cisco.com, page 399**.

ÉTAPE 5 Si vos informations d'identification de compte Cisco.com sont incorrectes, cliquez sur **OK** pour retourner à la page Cisco.com Credentials. Corrigez vos informations d'identification de compte Cisco.com, puis cliquez sur **Next** pour les vérifier à nouveau.

ÉTAPE 6 Si vos informations d'identification de compte Cisco.com sont valides, passez à la page Upgrade Firmware.

Activation de la mise à niveau du microprogramme

ÉTAPE 7 Reportez-vous à la page Upgrade Firmware pour permettre au périphérique de rechercher des mises à jour du microprogramme ou pour mettre à niveau manuellement le microprogramme.

- Pour rechercher automatiquement des mises à jour du microprogramme, cochez la case en regard de **Check for firmware update when Setup Wizard completes**. L'Cisco ISA500 recherche immédiatement des mises à jour du microprogramme une fois l'exécution de l'assistant de configuration terminée. Cette fonctionnalité nécessite que vous disposiez d'une connexion WAN active.
- Pour mettre à niveau manuellement le microprogramme à partir d'une image du microprogramme stockée sur votre PC, désactivez la case en regard de **Check for firmware update when Setup Wizard completes**. Désactivez cette case à cocher lorsque vous ne disposez pas d'une connexion WAN active et que vous avez déjà téléchargé la dernière image du microprogramme à partir de Cisco.com sur votre PC local.

ÉTAPE 8 Si vous désactivez cette case à cocher, cliquez sur **Browse** pour localiser et sélectionner l'image du microprogramme à partir de votre PC, puis cliquez sur **Upgrade**.

Une fois que vous avez cliqué sur Upgrade, l'Cisco ISA500 commence à installer le microprogramme. Ce processus peut prendre quelques minutes. Ne débranchez pas le périphérique et ne le réinitialisez pas. Cela annulerait le processus de mise à niveau du microprogramme et pourrait éventuellement endommager ce dernier. L'Cisco ISA500 redémarre une fois le microprogramme mis à niveau. Vous serez redirigé vers l'écran de connexion lorsque l'Cisco ISA500 redémarre.

ÉTAPE 9 Si vous choisissez de rechercher automatiquement les mises à jour du microprogramme, cliquez sur **Next**.

Validation de la licence de sécurité

ÉTAPE 10 Reportez-vous à la page License Installation pour valider la licence de sécurité, qui est utilisée pour activer les services de sécurité sur le périphérique.

ÉTAPE 11 Si la licence de sécurité est déjà installée sur l'Cisco ISA500, cliquez sur **Next** pour passer à l'étape suivante.

ÉTAPE 12 Si la licence de sécurité n'est pas installée sur l'Cisco ISA500, entrez les informations suivantes pour valider la licence de sécurité :

- **Email Address** : entrez l'adresse e-mail enregistrée pour recevoir l'ID de clé d'autorisation de produit.
- **PAK ID** : entrez votre clé d'autorisation du produit dans ce champ. Vous pouvez trouver le code de licence sur le certificat de demande de licence logicielle que Cisco fournit à l'achat de l'appliance de sécurité.

  REMARQUE : un compte Cisco.com valide est requis pour valider la licence de sécurité. Si vos informations d'identification de compte Cisco.com ne sont pas configurées, revenez à la page Cisco.com Credentials pour les configurer.

REMARQUE : si vous souhaitez poursuivre la configuration de l'assistant de configuration sans installer la licence de sécurité, cochez la case en regard de **Continue without installing license (not recommended)**. Les services de sécurité ne peuvent pas être activés sans l'installation de la licence de sécurité.

ÉTAPE 13 Lorsque vous avez terminé, cliquez sur **Next**.

Activation des protocoles Bonjour et CDP (CDP Discovery Protocol)

ÉTAPE 14 Reportez-vous à la page Discovery pour activer les protocoles Bonjour et/ou CDP sur l'Cisco ISA500. Pour une prise en charge optimale de la topologie et de la détection de périphériques, via le portail OnPlus, activez les deux protocoles de détection.

- **Enable Bonjour Discovery Protocol** : cochez cette case pour activer le protocole Bonjour Discovery Protocol ou désélectionnez-la pour le désactiver.
- **Enable Cisco Discovery Protocol (CDP)** : cochez cette case pour activer le protocole Cisco Discovery Protocol ou désactivez-la.

  REMARQUE : les protocoles de détection sont opérationnels uniquement sur les ports LAN de l'Cisco ISA500.

ÉTAPE 15 Lorsque vous avez terminé, cliquez sur **Next**.

Configuration de l'administration à distance

ÉTAPE 16 Reportez-vous à la page Remote Administration pour configurer les paramètres de gestion à distance. L'Cisco ISA500 permet une gestion à distance sécurisée via les protocoles HTTPS et HTTP, comme par exemple https://xxx.xxx.xxx.xxx:8080.

- **Remote Administration** : cliquez sur **On** pour activer la gestion à distance via HTTPS ou cliquez sur **Off** pour la désactiver. Nous vous recommandons d'utiliser HTTPS pour la gestion à distance sécurisée.
- **HTTPS Listen Port Number** : si vous activez la gestion à distance via le protocole HTTPS, entrez le numéro de port. Par défaut, le numéro du port d'écoute pour HTTPS est 8080.
- **HTTP Enable** : cliquez sur **On** pour activer la gestion à distance via HTTP ou cliquez sur **Off** pour la désactiver.
- **HTTP Listen Port Number** : si vous activez la gestion à distance via le protocole HTTP, entrez le numéro de port. Par défaut, le numéro du port d'écoute pour HTTP est 80.
- **Allow Address** : pour spécifier les périphériques qui peuvent accéder à l'utilitaire de configuration par l'intermédiaire de l'interface WAN, choisissez un objet d'adresse ou entrez une adresse.
  - **Address Objects** : ces objets représentent les adresses IP et plages d'adresses connues, telles que le VLAN GUEST et le pool DHCP. Une fois l'exécution de l'assistant terminée, vous pouvez afficher les informations sur les objets d'adresse sur la page Networking > Address Management.
  - **Create new address** : choisissez cette option pour entrer une adresse IP ou une plage d'adresses. Dans la fenêtre contextuelle, renseignez le champ **Name** et spécifiez le **Type** (hôte ou plage). Pour un hôte unique, entrez l'adresse IP. Pour une plage, renseignez les champs **Starting IP Address** et **Ending IP Address**.
- **Remote SNMP** : cliquez sur **On** pour activer SNMP pour la connexion à distance ou cliquez sur **Off** pour désactiver SNMP. L'activation de SNMP permet aux utilisateurs distants d'utiliser le protocole SNMP pour accéder à l'utilitaire de configuration.

ÉTAPE 17 Lorsque vous avez terminé, cliquez sur **Next**.

Configuration des ports physiques

ÉTAPE 18 Reportez-vous à la page Port Configuration pour spécifier la configuration des ports.

Si vous utilisez l'ISA570 ou l'ISA570W, choisissez l'une des options suivantes :

- **1 WAN, 9 LAN switch** : un port WAN (WAN1) et neuf ports LAN sont configurés.
- **1 WAN, 1 DMZ, 8 LAN switch** : un port WAN (WAN1), un port DMZ et huit ports LAN sont configurés. Le port configurable GE10 est défini en tant que port DMZ.
- **1 WAN, 1 WAN backup, 8 LAN switch** : deux ports WAN (WAN1 est le WAN principal et WAN2 le WAN secondaire) et huit ports LAN sont configurés. Le port configurable GE10 est défini en tant que port WAN secondaire.
- **1 WAN, 1 WAN backup, 1 DMZ, 7 LAN switch** : deux ports WAN (WAN1 est le WAN principal et WAN2 le WAN secondaire), un port DMZ et sept ports LAN sont configurés. Le port configurable GE10 est défini en tant que port WAN secondaire et le port configurable GE9 est défini en tant que port DMZ.

Si vous utilisez l'ISA550 ou l'ISA550W, choisissez l'une des options suivantes :

- **1 WAN, 6 LAN switch** : un port WAN (WAN1) et six ports LAN sont configurés.
- **1 WAN, 1 DMZ, 5 LAN switch** : un port WAN (WAN1), un port DMZ et cinq ports LAN sont configurés. Le port configurable GE7 est défini en tant que port DMZ.
- **1 WAN, 1 WAN backup, 5 LAN switch** : deux ports WAN (WAN1 est le WAN principal et WAN2 le WAN secondaire) et cinq ports LAN sont configurés. Le port configurable GE7 est défini en tant que port WAN secondaire.
- **1 WAN, 1 WAN backup, 1 DMZ, 4 LAN switch** : deux ports WAN (WAN1 est le WAN principal et WAN2 le WAN secondaire), un port DMZ et quatre ports LAN sont configurés. Le port configurable GE7 est défini en tant que port WAN secondaire et le port configurable GE6 est défini en tant que port DMZ.

REMARQUE : si vous avez deux liaisons ISP, nous vous recommandons de définir un WAN de secours afin de pouvoir fournir une connexion de secours ou assurer l'équilibrage de charge. Si vous devez héberger des services publics, nous vous recommandons de définir un port DMZ.

ÉTAPE 19 Lorsque vous avez terminé, cliquez sur **Next**.

Configuration du WAN principal

ÉTAPE 20 Reportez-vous à la page Primary WAN Connection pour configurer la connexion WAN principale à l'aide des informations de compte fournies par votre ISP.

- **WAN Name** : nom du port WAN principal.
- **IP Address Assignment** : en fonction des exigences de votre ISP, choisissez le mode d'adressage réseau et configurez les champs correspondants pour le port WAN principal. L'Cisco ISA500 prend en charge le client DHCP, l'IP statique, PPPoE, PPTP et L2TP. Pour plus d'informations, reportez-vous à la section **Mode d'adressage réseau, page 131**.

ÉTAPE 21 Lorsque vous avez terminé, cliquez sur **Next**.

Configuration du WAN secondaire

ÉTAPE 22 Si un seul port WAN est configuré, allez à la section **Configuration des paramètres LAN par défaut, page 45**. Si deux ports WAN sont configurés, reportez-vous à la page Secondary WAN Connection pour configurer la connexion WAN secondaire à l'aide des informations de compte fournies par votre ISP.

- **WAN Name** : nom du port WAN secondaire.
- **IP Address Assignment** : en fonction des exigences de votre ISP, choisissez le mode d'adressage réseau et configurez les champs correspondants pour le port WAN secondaire. Pour plus d'informations, reportez-vous à la section **Mode d'adressage réseau, page 131**.

ÉTAPE 23 Lorsque vous avez terminé, cliquez sur **Next**.

Configuration de la redondance du WAN

ÉTAPE 24 Si vous avez deux liaisons WAN, reportez-vous à la page WAN Redundancy pour déterminer comment les deux liaisons ISP sont utilisées.

- **Equal Load Balancing (Round Robin)** : sélectionnez cette option si vous souhaitez réordonner les ports WAN pour la sélection Round Robin. L'ordre est le suivant : WAN1 et WAN2. La sélection revient ensuite au WAN1 et continue l'ordre.
- **Weighted Load Balancing** : sélectionnez cette option si vous voulez répartir la bande passante sur deux ports WAN en fonction du pourcentage pondéré ou de la bande passante de liaison pondérée. Les deux liaisons acheminent des données pour les protocoles auxquels elles sont liées.

- **Weighted By Percentage** : si vous sélectionnez cette option, spécifiez le pourcentage ou la bande passante pour chaque WAN, courriel 80 % pour WAN1 et 20 % pour WAN2.
- **Weighted by Link Bandwidth** : si vous sélectionnez cette option, spécifiez la quantité de bande passante pour chaque WAN, comme par exemple 80 Mbits/s pour WAN1 et 20 Mbits/s pour WAN2.

REMARQUE : L'option Weighted by Link Bandwidth produit le même effet que l'option Weighted by Percentage. Toutefois, elle fournit davantage d'options de pourcentage que dans le champ Weighted by Percentage.

- **Failover** : sélectionnez cette option si vous souhaitez utiliser une liaison ISP en tant que liaison de secours. Si une défaillance est détectée sur la liaison principale, l'Cisco ISA500 dirige l'ensemble du trafic Internet vers la liaison de secours. Lorsque la liaison principale récupère la connectivité, l'ensemble du trafic Internet est dirigé vers la liaison principale et la liaison de secours devient inactive.
  - **Select WAN Precedence** : choisissez l'une des options suivantes :

    Primary : WAN1; Secondary : WAN2 : si vous choisissez cette option, le WAN1 est défini comme liaison principale et le WAN2 comme liaison de secours.

    Primary : WAN2; Secondary : WAN1 : si vous choisissez cette option, le WAN1 est défini comme liaison principale et le WAN2 comme liaison de secours.
  - **Preempt Delay Timer** : entrez l'heure en secondes à laquelle l'Cisco ISA500 mettra en priorité la liaison principale par rapport à la liaison de secours une fois la liaison principale de nouveau active. La valeur par défaut est 5 secondes.

ÉTAPE 25 Lorsque vous avez terminé, cliquez sur **Next**.

Configuration des paramètres LAN par défaut

ÉTAPE 26 Reportez-vous à la page LAN Configuration pour configurer les paramètres LAN par défaut.

- **IP Address** : entrez l'adresse IP de sous-réseau du LAN par défaut.
- **Netmask** : entrez le masque de sous-réseau pour le LAN par défaut.

- **DHCP Mode** : choisissez l'un des modes DHCP suivants :
  - **Disable** : choisissez cette option si les ordinateurs du LAN sont configurés avec des adresses IP statiques ou pour utiliser un autre serveur DHCP.
  - **DHCP Server** : permet à l'Cisco ISA500 d'agir en tant que serveur DHCP et attribue les adresses IP à tous les périphériques connectés au LAN. Tout nouveau client DHCP se connectant au LAN reçoit une adresse IP du pool DHCP.
  - **DHCP Relay** : permet à l'Cisco ISA500 d'utiliser un relais DHCP. Si vous choisissez le relais DHCP, entrez l'adresse IP du serveur DHCP distant dans le champ **Relay IP**.

ÉTAPE 27 Si vous choisissez **DHCP Server** comme mode DHCP, entrez les informations suivantes :

- **Start IP** : entrez l'adresse IP de début du pool DHCP.
- **Start IP** : entrez l'adresse IP de début du pool DHCP.

  REMARQUE : l'adresse IP de début et l'adresse IP de fin doivent être dans le même sous-réseau que l'adresse IP du LAN.
- **Lease Time** : entrez la durée de connexion maximale de « location » d'une adresse IP dynamique à un utilisateur du réseau. Lorsque le temps s'est écoulé, l'adresse IP dynamique de l'utilisateur est automatiquement renouvelée.
- **DNS1** : entrez l'adresse IP du serveur DNS principal.
- **DNS2** : entrez éventuellement l'adresse IP du serveur DNS secondaire.
- **WINS1** : entrez éventuellement l'adresse IP du serveur WINS principal.
- **WINS2** : entrez éventuellement l'adresse IP du serveur WINS secondaire.
- **Domain Name** : éventuellement, entrez le nom de domaine pour le LAN par défaut.
- **Default Gateway** : entrez l'adresse IP de la passerelle par défaut.

ÉTAPE 28 Lorsque vous avez terminé, cliquez sur **Next**.

Configuration de la DMZ

ÉTAPE 29 Si vous n'avez pas configuré un port DMZ, allez à la section **Configuration des paramètres de la radio sans fil, page 49**. Si vous avez configuré un port DMZ, reportez-vous à la page DMZ Configuration pour configurer un réseau DMZ.

- **IP Address** : entrez l'adresse IP de sous-réseau de la DMZ.
- **Netmask** : entrez le masque de sous-réseau de la DMZ.
- **DHCP Mode** : choisissez l'un des modes DHCP suivants :
  - **Disable** : choisissez cette option si les ordinateurs de la DMZ sont configurés avec des adresses IP statiques ou pour utiliser un autre serveur DHCP.
  - **DHCP Server** : permet à l'Cisco ISA500 d'agir en tant que serveur DHCP et affecte les adresses IP à tous les périphériques connectés à la DMZ. Tout nouveau client DHCP se connectant au DMZ reçoit une adresse IP du pool DHCP.
  - **DHCP Relay** : permet à l'Cisco ISA500 d'utiliser un relais DHCP. Si vous choisissez le relais DHCP, entrez l'adresse IP du serveur DHCP distant dans le champ **Relay IP**.

ÉTAPE 30 Si vous choisissez **DHCP Server** comme mode DHCP, entrez les informations suivantes :

- **Start IP** : entrez l'adresse IP de début du pool DHCP.
- **Start IP** : entrez l'adresse IP de début du pool DHCP.

  REMARQUE : l'adresse IP de début et l'adresse IP de fin doivent être dans le même sous-réseau que l'adresse IP du DMZ.
- **Lease Time** : entrez la durée de connexion maximale de « location » d'une adresse IP dynamique à un utilisateur du réseau. Lorsque le temps s'est écoulé, l'adresse IP dynamique de l'utilisateur est automatiquement renouvelée.
- **DNS1** : entrez l'adresse IP du serveur DNS principal.
- **DNS2** : entrez éventuellement l'adresse IP du serveur DNS secondaire.
- **WINS1** : entrez éventuellement l'adresse IP du serveur WINS principal.
- **WINS2** : entrez éventuellement l'adresse IP du serveur WINS secondaire.
- **Domain Name** : entrez éventuellement le nom de domaine de la DMZ.
- **Default Gateway** : entrez l'adresse IP de la passerelle par défaut.

ÉTAPE 31 Lorsque vous avez terminé, cliquez sur **Next**.

Configuration des services DMZ

ÉTAPE 32 Reportez-vous à la page DMZ Service pour configurer les services DMZ.

ÉTAPE 33 Cliquez sur **Add** pour créer un service DMZ.

Autres options : pour modifier une entrée, cliquez sur l'icône de **modification** (crayon). Pour supprimer une entrée, cliquez sur l'icône de **suppression** (x). Pour supprimer plusieurs entrées, cochez-les et cliquez sur **Delete**.

ÉTAPE 34 Dans la fenêtre DMZ Service - Add/Edit, entrez les informations suivantes :

- **Original Service** : sélectionnez un service comme service entrant.
- **Translated Service** : sélectionnez un service en tant que service traduit ou sélectionnez **Original** si le service traduit est le même que le service entrant. Si le service de votre choix ne figure pas dans la liste, sélectionnez **Create a new service** pour créer un nouvel objet Service. Pour conserver les objets Service, accédez à la page Networking > Service Management. Reportez-vous à la **Gestion des services, page 184**.

  REMARQUE : La traduction un-à-un sera exécutée pour le transfert de plage de ports. Par exemple, si vous souhaitez traduire un service TCP original avec la plage de ports 50000 à 50002 en un service TCP avec la plage de ports 60000 à 60002, le port 50000 sera traduit en port 60000, le port 50001 sera traduit en port 60001 et le port 50002 sera traduit en port 60002.
- **Translated IP** : sélectionnez l'adresse IP de votre serveur local qui doit être traduit. Si l'adresse IP de votre choix ne figure pas dans la liste, sélectionnez **Create a new address** pour créer un nouvel objet Adresse IP. Pour conserver les objets Adresse IP, accédez à la page Networking > Address Management. Reportez-vous à la **Gestion d'adresse, page 182**.
- **WAN** : sélectionnez WAN1 ou WAN2, ou les deux, comme port WAN entrant.
- **WAN IP** : spécifiez l'adresse IP publique du serveur. Vous pouvez utiliser l'adresse IP du port WAN sélectionné ou une adresse IP publique fournie par votre ISP. Lorsque vous sélectionnez **Both** en tant que port WAN entrant, cette option est grisée.
- **Enable DMZ Service** : cliquez sur **On** pour activer le service DMZ ou cliquez sur **Off** pour créer uniquement le service DMZ.
- **Create Firewall Rule** : cochez cette case pour créer automatiquement une règle de pare-feu permettant d'autoriser l'accès pour ce service DMZ. Vous devez créer manuellement une règle de pare-feu si vous désactivez cette case à cocher.

REMARQUE : Si vous sélectionnez Both en tant que port WAN entrant, une règle de pare-feu de n'importe quelle zone à n'importe quelle zone est alors créée.

- **Description** : entrez le nom du service DMZ.

  Par exemple, vous hébergez un serveur RDP (192.168.12.101) dans la DMZ. Votre ISP vous a fourni une adresse IP statique (172.39.202.102) que vous souhaitez exposer au public comme votre adresse de serveur RDP. Vous pouvez créer un service DMZ comme suit pour permettre à l'utilisateur Internet d'accéder au serveur RDP à l'aide de l'adresse IP publique spécifiée.

Original Service	RDP
Translated Service	RDP
Translated IP	RDPServer
WAN	WAN1
WAN IP	PublicIP
Enable DMZ Service	On
Create Firewall Rule	On

REMARQUE : dans cet exemple, vous devez créer manuellement deux objets Adresse (RDPServer et PublicIP) et un objet Service TCP avec le port 3389 appelé « RDP ».

ÉTAPE 35 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 36 Lorsque vous avez terminé, cliquez sur **Next**.

Configuration des paramètres de la radio sans fil

ÉTAPE 37 Si vous utilisez l'ISA550 ou l'ISA570, allez à la section **Affichage du résumé de la configuration, page 53**. Si vous utilisez l'ISA550W ou ISA570W, reportez-vous à la page Wireless Radio Setting pour configurer les paramètres de transmission de données par liaison sans fil.

- **Wireless Radio** : cliquez sur **On** pour activer la transmission radio sans fil et par conséquent activer le SSID appelé « cisco-data », ou cliquez sur **Off** pour désactiver cette option.

- **Wireless Network Mode** : choisissez la technique de modulation 802.11.
  - **802.11b/g mixed** : sélectionnez ce mode si certains périphériques du réseau sans fil utilisent 802.11b et que d'autres utilisent 802.11g. Les clients 802.11b et 802.11g peuvent se connecter au point d'accès.
  - **802.11g/n mixed** : sélectionnez ce mode si certains périphériques du réseau sans fil utilisent 802.11g et que d'autres utilisent 802.11n. Les clients 802.11g et 802.11n peuvent se connecter au point d'accès.
  - **802.11b/g/n mixed** : sélectionnez ce mode pour autoriser les clients 802.11b, 802.11g et 802.11n utilisant la fréquence 2,4 GHz à se connecter au point d'accès.
  - **802.11n only** : sélectionnez ce mode si tous les périphériques du réseau sans fil peuvent prendre en charge 802.11n. Seuls les clients 802.11n qui utilisent la fréquence 2.4 GHz peuvent se connecter au point d'accès.
- **Wireless Channel** : sélectionnez un canal dans une liste de canaux ou sélectionnez l'option **Auto** pour permettre au système de déterminer le canal optimal à utiliser en fonction des niveaux sonores environnementaux des canaux disponibles.

ÉTAPE 38 Lorsque vous avez terminé, cliquez sur **Next**.

Configuration de l'accès WLAN Intranet

ÉTAPE 39 Si vous avez désactivé la transmission de données par liaison sans fil, allez à la section **Affichage du résumé de la configuration, page 53**. Si vous avez activé la transmission de données par liaison sans fil, reportez-vous à la page Intranet WLAN Access pour configurer les paramètres de connectivité sans fil pour le SSID appelé « cisco-data ».

- **SSID Name** : nom du SSID.
- **Security Mode** : sélectionnez l'algorithme de cryptage pour le cryptage des données pour ce SSID et configurez les paramètres correspondants. Pour plus d'informations, reportez-vous à la section **Configuration de la sécurité sans fil, page 195**.
- **VLAN Name** : sélectionnez le VLAN auquel ce SSID est mappé. Tout le trafic en provenance des clients sans fil connectés à ce SSID est dirigé vers le VLAN sélectionné. Pour l'accès VLAN Intranet, vous devez sélectionner un VLAN mappé à une zone approuvée.

REMARQUE : l'ISA550W et l'ISA570W prennent en charge quatre SSID. Pour configurer les paramètres de connectivité sans fil pour les autres SSID, accédez à la page Wireless > Basic Settings page (voir **Configuration des profils SSID, page 194**) ou utilisez l'assistant sans fil (voir **Utilisation de l'assistant sans fil pour configurer les paramètres sans fil (pour l'ISA550W et l'ISA570W uniquement), page 81**).

ÉTAPE 40 Lorsque vous avez terminé, cliquez sur **Next**.

Configuration des services de sécurité

ÉTAPE 41 Reportez-vous à la page Security Services pour activer les services de sécurité et spécifier comment gérer le trafic affecté lorsque les services de sécurité basés sur la réputation ne sont pas disponibles.

REMARQUE :

- L'activation d'un service de sécurité appliquera ses paramètres par défaut sur l'Cisco ISA500 pour fournir un niveau modéré de protection. Nous vous recommandons fortement de personnaliser les paramètres de chaque service de sécurité activé une fois l'exécution de l'assistant de configuration terminée. Pour plus d'informations, reportez-vous à la section **Chapitre 7, « Services de sécurité. »**
- Le contrôle des applications et le filtrage URL Web nécessitent une configuration supplémentaire dans les pages Security Services.
- Une licence de sécurité valide est nécessaire pour activer les services de sécurité. Si la licence de sécurité n'est pas encore installée, retournez à la page License Installation pour entrer la clé d'autorisation de produit (CAP) et l'adresse électronique. Une fois l'exécution de l'assistant de configuration terminée, l'Cisco ISA500 commence par valider la licence de sécurité via Internet, puis active les services de sécurité.

Les fonctionnalités suivantes sont disponibles :

- **Anti-Virus** : l'antivirus empêche les virus et les programmes malveillants d'entrer dans votre réseau par le biais des applications de messagerie électronique, Web, FTP, CIFS et Netbios. Cochez cette case pour activer la fonctionnalité d'antivirus sur l'Cisco ISA500, ou décochez-la pour la désactiver.
- **Intrusion Prevention (IPS)** : IPS surveille les protocoles réseau et empêche les attaques contre les périphériques client en analysant certains types de trafics réseau et en y répondant. Cochez cette case pour activer la fonctionnalité IPS sur l'Cisco ISA500, ou décochez-la pour la désactiver.

- **Network Reputation** : la réputation de réseau bloque le trafic entrant provenant des adresses IP connues pour lancer des attaques sur Internet. Cochez cette case pour activer la fonctionnalité de réputation de réseau sur l'Cisco ISA500, ou décochez-la pour la désactiver. Par défaut, la réputation de réseau est activée.
- **Spam Filter** : le filtre de courrier indésirable détecte et bloque le courrier électronique indésirable. Cochez cette case pour activer le filtre de courrier indésirable sur l'Cisco ISA500, ou décochez-la pour le désactiver. Si vous activez le filtre de courrier indésirable, entrez l'adresse IP ou le nom de domaine de votre serveur SMTP interne dans le champ **Local SMTP Server IP Address**. Le trafic Internet du serveur SMTP doit être acheminé via l'Cisco ISA500. Le serveur SMTP ou les clients qui utilisent ce serveur SMTP peuvent être configurés pour répondre aux balises de courrier indésirable et de suspicion de courrier indésirable que l'Cisco ISA500 applique aux courriels.
- **Web Reputation Filtering** : le filtrage par réputation Web empêche les périphériques client d'accéder à des sites Web dangereux contenant des virus, des logiciels espions, des programmes malveillants ou des liens d'hameçonnage. Cochez cette case pour activer la fonctionnalité de filtrage par réputation Web sur l'Cisco ISA500, ou décochez-la pour la désactiver.

  REMARQUE : cliquer sur le lien **Details** pour un service de sécurité peut ouvrir la page d'aide qui fournit des détails complets pour le service de sécurité.

ÉTAPE 42 Le filtre de courrier indésirable, la réputation de réseau, le filtrage par réputation Web et le filtrage URL Web sont des services de sécurité basés sur la réputation. Vous pouvez spécifier comment traiter le trafic affecté lorsque ces services de réputation ne sont pas disponibles. Sélectionnez l'une des options suivantes :

- **Prevent affected network traffic** : tout le trafic affecté est bloqué jusqu'à ce que les services de sécurité basés sur la réputation soient disponibles.
- **Allow affected network traffic** : tout le trafic affecté est autorisé jusqu'à ce que les services de sécurité basés sur la réputation soient disponibles.

ÉTAPE 43 Lorsque vous avez terminé, cliquez sur **Next**.

Affichage du résumé de la configuration

ÉTAPE 44 Reportez-vous à la page Summary pour afficher les informations relatives à la configuration.

ÉTAPE 45 Pour modifier des paramètres, cliquez sur **Back**. Si la configuration est correcte, cliquez sur **Apply** pour appliquer les paramètres.

Une fois que la configuration a été correctement appliquée, l'assistant de configuration recherche immédiatement des mises à jour du microprogramme.

ÉTAPE 46 Si la fenêtre Firmware Upgrade apparaît, suivez les instructions affichées à l'écran pour télécharger et installer le microprogramme. Reportez-vous à la **Mise à niveau de votre microprogramme après votre première connexion, page 34**. Si vous utilisez le microprogramme le plus récent, cliquez sur **Finish**.

Utilisation de l'assistant double WAN pour configurer les paramètres de redondance WAN

Si vous disposez de deux liaisons ISP, un WAN de secours est requis pour que vous puissiez fournir une connexion de secours ou assurer l'équilibrage de charge. Utilisez l'assistant double WAN pour configurer les paramètres de redondance WAN. Reportez-vous aux étapes suivantes :

- **Démarrage de l'assistant double WAN, page 54**
- **Configuration d'un port configurable comme port WAN secondaire, page 54**
- **Configuration du WAN principal, page 54**
- **Configuration du WAN secondaire, page 54**
- **Configuration de la redondance du WAN, page 55**
- **Configuration de la détection des défaillances du réseau, page 56**
- **Affichage du résumé de la configuration, page 56**

Démarrage de l'assistant double WAN

ÉTAPE 1 Cliquez sur **Configuration Wizards > Dual WAN Wizard**.

ÉTAPE 2 Cliquez sur **Next**.

Configuration d'un port configurable comme port WAN secondaire

ÉTAPE 3 Sur la page Port Configuration, spécifiez un port configurable (de GE6 à GE10) en tant que port WAN secondaire. Le port physique GE1 est réservé pour le port WAN principal.

ÉTAPE 4 Lorsque vous avez terminé, cliquez sur **Next**.

Configuration du WAN principal

ÉTAPE 5 Reportez-vous à la page Primary WAN Connection pour configurer la connexion WAN principale à l'aide des informations de compte fournies par votre ISP.

- **WAN Name** : nom du port WAN principal.
- **IP Address Assignment** : en fonction des exigences de votre ISP, choisissez le mode d'adressage réseau et configurez les champs correspondants pour le port WAN principal. L'Cisco ISA500 prend en charge le client DHCP, l'IP statique, PPPoE, PPTP et L2TP. Pour plus d'informations, reportez-vous à la section **Mode d'adressage réseau, page 131**.

ÉTAPE 6 Lorsque vous avez terminé, cliquez sur **Next**.

Configuration du WAN secondaire

ÉTAPE 7 Reportez-vous à la page Secondary WAN Connection pour configurer la connexion WAN secondaire à l'aide des informations de compte fournies par votre ISP.

- **WAN Name** : nom du port WAN secondaire.
- **IP Address Assignment** : en fonction des exigences de votre ISP, choisissez le mode d'adressage réseau et configurez les champs correspondants pour le port WAN secondaire. Pour plus d'informations, reportez-vous à la section **Mode d'adressage réseau, page 131**.

ÉTAPE 8 Lorsque vous avez terminé, cliquez sur **Next**.

Configuration de la redondance du WAN

ÉTAPE 9 Reportez-vous à la page WAN Redundancy pour déterminer comment les deux liaisons ISP sont utilisées.

- **Dual WAN Settings** : sélectionnez cette option si vous souhaitez utiliser les deux liaisons ISP simultanément. L'équilibrage de charge répartit la bande passante sur deux ports WAN en fonction du pourcentage pondéré ou de la bande passante de liaison pondérée. Les deux liaisons acheminent des données pour les protocoles auxquels elles sont liées.
  - **Weighted by percentage** : si vous sélectionnez cette option, spécifiez le pourcentage pour chaque WAN, comme par exemple 80 % de bande passante pour WAN1 et au moins 20 % de bande passante pour WAN2.
  - **Weighted by Link Bandwidth** : si vous choisissez cette option, spécifiez la quantité de bande passante pour chaque WAN, telle que 80 Mbit/s pour le WAN1 et 20 Mbit/s pour le WAN2, ce qui signifie que 80 % de la bande passante est distribuée au WAN1 et au moins 20 % au WAN2.

  REMARQUE : L'option Weighted by Link Bandwidth produit le même effet que l'option Weighted by Percentage. Elle propose seulement davantage d'options de pourcentage que l'option Weighted by Percentage qui n'en propose que trois.
- **Failover** : sélectionnez cette option si vous souhaitez utiliser une liaison ISP en tant que liaison de secours. Le mode Failover dirige tout le trafic Internet vers la liaison secondaire si la liaison principale est en panne. Lorsque la liaison principale récupère la connectivité, l'ensemble du trafic Internet est dirigé vers la liaison principale et la liaison secondaire devient inactive.
  - **Select WAN Precedence** : choisissez l'une des options suivantes :

    Primary : WAN1; Secondary : WAN2 : si vous choisissez cette option, le WAN1 est défini comme liaison principale et le WAN2 comme liaison de secours.

    Primary : WAN2; Secondary : WAN1 : si vous choisissez cette option, le WAN1 est défini comme liaison principale et le WAN2 comme liaison de secours.
  - **Preempt Delay Timer** : entrez l'heure en secondes à laquelle l'Cisco ISA500 mettra en priorité la liaison principale par rapport à la liaison de secours une fois la liaison principale de nouveau active. La valeur par défaut est de 5 secondes.

ÉTAPE 10 Lorsque vous avez terminé, cliquez sur **Next**.

Configuration de la détection des défaillances du réseau

ÉTAPE 11 Reportez-vous à la page Network Detection pour configurer la détection des défaillances du réseau.

- **Retry Count** : entrez le nombre de tentatives. L'Cisco ISA500 essaie à plusieurs reprises de se connecter à l'ISP après la détection de la défaillance du réseau.
- **Retry Timeout** : entrez la valeur de l'intervalle entre deux paquets de détection (détection Ping ou DNS).
- **Ping Detection-Ping using WAN Default Gateway** : si vous sélectionnez cette option, envoyez une requête ping à l'adresse IP de la passerelle WAN par défaut. Si la passerelle WAN par défaut peut être détectée, la connexion réseau est active.
- **DNS Detection-DNS lookup using WAN DNS Servers** : si vous sélectionnez cette option, l'Cisco ISA500 envoie la requête DNS pour www.cisco.com au serveur DNS WAN par défaut. Si le serveur DNS peut être détecté, la connexion réseau est active.

ÉTAPE 12 Lorsque vous avez terminé, cliquez sur **Next**.

Affichage du résumé de la configuration

ÉTAPE 13 Reportez-vous à la page Summary pour afficher les informations relatives à la configuration.

ÉTAPE 14 Pour modifier des paramètres, cliquez sur **Back**. Si la configuration est correcte, cliquez sur **Finish** pour appliquer les paramètres.

Utilisation de l'assistant VPN d'accès à distance pour configurer l'accès à distance IPsec ou SSL

Utilisez l'assistant VPN d'accès à distance pour configurer l'Cisco ISA500 en tant que serveur VPN IPsec ou passerelle VPN SSL, afin que les utilisateurs distants puissent accéder en toute sécurité aux ressources du réseau d'entreprise via les tunnels VPN. L'assistant VPN d'accès à distance prend en charge les types de réseaux VPN suivants :

- **IPsec Remote Access** : activez la fonctionnalité d'accès à distance IPsec et définissez ainsi l'Cisco ISA500 comme serveur VPN IPsec. Si vous sélectionnez cette option, suivez les instructions affichées à l'écran pour configurer une stratégie de groupe d'accès à distance IPsec et spécifier les utilisateurs et les groupes d'utilisateurs pour l'accès à distance IPsec. Pour plus d'informations, reportez-vous à la section **Utilisation de l'assistant VPN d'accès à distance pour configurer l'accès à distance IPsec, page 57**.
- **SSL Remote Access** : activez la fonctionnalité d'accès à distance SSL et définissez ainsi l'Cisco ISA500 comme serveur VPN SSL. Si vous sélectionnez cette option, suivez les instructions affichées à l'écran pour configurer les stratégies de groupe VPN SSL et spécifier les utilisateurs et les groupes d'utilisateurs pour l'accès à distance SSL. Pour plus d'informations, reportez-vous à la section **Utilisation de l'assistant VPN d'accès à distance pour configurer l'accès à distance SSL, page 63**.

Utilisation de l'assistant VPN d'accès à distance pour configurer l'accès à distance IPsec

Cette section explique comment utiliser l'assistant VPN d'accès à distance pour configurer une stratégie de groupe d'accès à distance IPsec et spécifier les utilisateurs et les groupes d'utilisateurs pour l'accès à distance IPsec. Reportez-vous aux étapes suivantes :

- **Lancement de l'assistant VPN d'accès à distance avec l'accès à distance IPsec, page 58**
- **Configuration de la stratégie de groupe d'accès à distance IPsec, page 58**
- **Configuration des paramètres WAN, page 59**
- **Configuration du mode de fonctionnement, page 59**

- Configuration des paramètres de contrôle d'accès, page 60
- Configuration des paramètres DNS et WINS, page 60
- Configuration des serveurs de secours, page 61
- Configuration de la transmission tunnel partagée, page 61
- Affichage du résumé de la stratégie de groupe, page 62
- Configuration des groupes d'utilisateurs d'accès à distance IPsec, page 62
- Affichage du résumé de l'accès à distance IPsec, page 63

Lancement de l'assistant VPN d'accès à distance avec l'accès à distance IPsec

ÉTAPE 1 Cliquez sur **Configuration Wizards > Remote Access VPN Wizard**.

ÉTAPE 2 Sur la page Getting Started, choisissez **IPsec Remote Access** dans la liste déroulante **VPN Tunnel Type**.

ÉTAPE 3 Cliquez sur **Next**.

Configuration de la stratégie de groupe d'accès à distance IPsec

ÉTAPE 4 Reportez-vous à la page IPsec Group Policy pour configurer les paramètres suivants de la stratégie de groupe d'accès à distance IPsec :

- **Group Name** : entrez le nom de la stratégie de groupe.
- **IKE Authentication Method** : spécifiez la méthode d'authentification.
  - **Pre-shared Key** : utilise une clé unique, basée sur votre mot de passe, pour l'authentification. Si vous sélectionnez cette option, entrez la valeur souhaitée que les clients VPN distants doivent fournir pour établir les connexions VPN. La clé prépartagée PSK (Pre-Shared Key) doit être entrée de façon parfaitement identique ici et sur les clients VPN distants.
  - **Certificate** : utilise un certificat numérique d'une autorité de certification (CA) tierce pour l'authentification. Si vous choisissez cette option, sélectionnez un certificat CA comme certificat local dans la liste déroulante **Local Certificate** et sélectionnez un certificat CA comme certificat distant dans la liste déroulante **Peer Certificate**, pour l'authentification. Le certificat distant sélectionné sur le serveur VPN IPsec doit être configuré comme certificat local sur les clients VPN distants.

REMARQUE : vous devez posséder des certificats CA valides importés sur votre Cisco ISA500 avant d'utiliser les certificats numériques pour l'authentification. Accédez à la page Device Management > Certificate Management pour importer les certificats CA. Reportez-vous à la **Gestion des certificats pour l'authentification, page 393**.

ÉTAPE 5 Lorsque vous avez terminé, cliquez sur **Next**.

Configuration des paramètres WAN

ÉTAPE 6 Reportez-vous à la page WAN pour sélectionner le port WAN que le trafic traverse par le biais du tunnel VPN. Si vous disposez de deux liaisons, vous pouvez activer le basculement WAN pour rediriger le trafic vers la liaison secondaire lorsque la liaison principale est défaillante.

- **WAN Failover** : cliquez sur **On** pour activer le basculement WAN ou sur **Off** pour le désactiver.

  REMARQUE : Pour activer le basculement WAN pour l'accès à distance IPsec, vérifiez que le port WAN secondaire a été configuré et que la redondance WAN a été définie comme mode d'équilibrage de charge ou de basculement. L'Cisco ISA500 met automatiquement à jour la passerelle WAN locale pour le tunnel VPN en fonction des configurations de la liaison WAN de secours. À cet effet, le DNS dynamique doit être configuré, car l'adresse IP va changer en raison du basculement. Dans ce cas, les clients VPN distants doivent utiliser le nom de domaine du serveur VPN IPsec pour établir les connexions VPN.

- **WAN Interface** : sélectionnez le port WAN que le trafic traverse par le biais du tunnel VPN.

ÉTAPE 7 Lorsque vous avez terminé, cliquez sur **Next**.

Configuration du mode de fonctionnement

ÉTAPE 8 Reportez-vous à la page Network pour configurer le mode de fonctionnement. Le client matériel VPN Cisco prend en charge le mode NEM (Network Extension Mode, mode d'extension de réseau) et le mode client. La stratégie de groupe d'accès à distance IPsec doit être configurée avec le mode correspondant pour autoriser uniquement la connexion des clients matériels VPN Cisco au mode de fonctionnement identique.

Par exemple, si vous sélectionnez le mode client pour la stratégie de groupe d'accès à distance IPsec, seuls les clients matériels VPN Cisco en mode client peuvent être connectés à l'aide de cette stratégie de groupe. Pour obtenir plus d'informations sur le mode de fonctionnement, reportez-vous à la section **Modes de fonctionnement, page 336**.

- **Mode** : sélectionnez l'un des modes suivants :
  - **Client** : sélectionnez ce mode pour la stratégie de groupe qui est utilisée à la fois pour le PC exécutant le logiciel Client VPN Cisco et le périphérique Cisco qui prend en charge le client matériel VPN Cisco en mode client. En mode « Client », le serveur VPN IPsec peut attribuer des adresses IP aux interfaces externes des clients VPN distants. Pour définir la plage du regroupement pour les clients VPN distants, entrez les adresses IP de début et de fin dans les champs **Start IP** et **End IP**.
  - **NEM** : sélectionnez ce mode pour la stratégie de groupe qui est utilisée uniquement pour le périphérique Cisco qui prend en charge le client matériel VPN Cisco en mode NEM.
- **Client Internet Access** : cochez cette case pour créer automatiquement des règles NAT avancées afin de permettre aux clients VPN distants d'accéder à Internet via les tunnels VPN. Si vous désactivez cette case, vous pouvez créer manuellement des règles NAT avancées. Pour plus d'informations, reportez-vous à la section **Configuration de règles NAT avancées pour permettre aux clients VPN distants d'accéder à Internet via les tunnels VPN, page 331**.

ÉTAPE 9 Lorsque vous avez terminé, cliquez sur **Next**.

Configuration des paramètres de contrôle d'accès

ÉTAPE 10 Reportez-vous à la page Access Control pour contrôler l'accès à partir du PC exécutant le logiciel Client VPN Cisco ou du réseau privé du client matériel VPN Cisco aux zones par le biais du tunnel VPN. Cliquez sur **Permit** pour permettre l'accès ou sur **Deny** pour le refuser.

REMARQUE : Les règles de pare-feu VPN qui sont automatiquement générées par les paramètres de contrôle d'accès aux zones seront ajoutées à la liste des règles de pare-feu avec une priorité supérieure aux règles de pare-feu par défaut, mais inférieure aux règles de pare-feu personnalisées.

ÉTAPE 11 Lorsque vous avez terminé, cliquez sur **Next**.

Configuration des paramètres DNS et WINS

ÉTAPE 12 Éventuellement, utilisez la page DNS/WINS pour spécifier les paramètres DNS et de domaine.

- **Primary DNS Server** : entrez l'adresse IP du serveur DNS principal.
- **Secondary DNS Server** : entrez l'adresse IP du serveur DNS secondaire.
- **Primary WINS Server** : entrez l'adresse IP du serveur WINS principal.

- **Secondary WINS Server** : entrez l'adresse IP du serveur WINS secondaire.
- **Default Domain** : entrez le nom de domaine par défaut qui doit être envoyé aux clients VPN distants.

ÉTAPE 13 Lorsque vous avez terminé, cliquez sur **Next**.

Configuration des serveurs de secours

ÉTAPE 14 Reportez-vous à la page Backup Server pour spécifier en option jusqu'à trois serveurs VPN IPsec comme serveurs de secours. En cas de défaillance de la connexion au serveur principal, les clients VPN distants peuvent tenter de se connecter aux serveurs de secours.

Backup Server 1/2/3 : entrez l'adresse IP ou le nom de domaine du serveur de secours. Le serveur de secours 1 bénéficie de la priorité la plus élevée et le serveur de secours 3, de la priorité la plus faible.

REMARQUE : Les serveurs de secours que vous avez spécifiés sur le serveur VPN IPsec sont envoyés aux clients VPN distants à l'établissement des connexions VPN. Les clients VPN distants les mettent en mémoire cache.

ÉTAPE 15 Lorsque vous avez terminé, cliquez sur **Next**.

Configuration de la transmission tunnel partagée

ÉTAPE 16 Reportez-vous à la page Split Tunnel pour spécifier les paramètres de transmission tunnel partagée :

- **Split Tunnel** : cliquez sur **On** pour activer la fonctionnalité de transmission tunnel partagée ou sur **Off** pour la désactiver. La transmission tunnel partagée autorise uniquement le trafic spécifié par les routes du client VPN vers les ressources de l'entreprise via le tunnel VPN. Si vous activez la fonctionnalité de transmission tunnel partagée, vous devez définir les sous-réseaux fractionnés. Pour ajouter un sous-réseau, entrez l'adresse IP et le masque de réseau dans les champs **IP Address** et **Netmask**, puis cliquez sur **Add**. Pour supprimer un sous-réseau, sélectionnez-le dans la liste et cliquez sur **Delete**.
- **Split DNS** : le DNS fractionné dirige les paquets DNS en texte clair à travers le tunnel VPN pour les domaines desservis par le DNS d'entreprise. Pour ajouter un domaine, entrez le nom de domaine qui doit être résolu par le serveur DNS de votre réseau dans le champ **Domain Name** et cliquez sur **Add**. Pour supprimer un domaine, sélectionnez-le dans la liste et cliquez sur **Delete**.

  Pour utiliser le DNS fractionné, vous devez également activer la fonctionnalité de transmission tunnel partagée et spécifier les domaines. La fonctionnalité de DNS fractionné prend en charge jusqu'à 10 domaines.

ÉTAPE 17 Lorsque vous avez terminé, cliquez sur **Next**.

Affichage du résumé de la stratégie de groupe

ÉTAPE 18 Reportez-vous à la page Group Policy Summary pour consulter les informations relatives aux paramètres de stratégie de groupe.

ÉTAPE 19 Cliquez sur **Next**.

Configuration des groupes d'utilisateurs d'accès à distance IPsec

ÉTAPE 20 Reportez-vous à la page IPsec Remote Access - User Group pour configurer les utilisateurs et les groupes d'utilisateurs pour l'accès à distance IPsec. Le service d'accès à distance IPsec doit être activé pour chaque groupe d'utilisateurs. Tous les membres des groupes d'utilisateurs peuvent utiliser la stratégie de groupe spécifiée pour établir les connexions VPN.

ÉTAPE 21 Cliquez sur **Add** pour ajouter un groupe d'utilisateurs.

Autres options : pour modifier une entrée, cliquez sur l'icône de **modification** (crayon). Pour supprimer une entrée, cliquez sur l'icône de **suppression** (x). Pour supprimer plusieurs entrées, cochez-les et cliquez sur **Delete**.

ÉTAPE 22 Dans l'onglet **Group Settings**, entrez les informations suivantes :

- **Name** : entrez le nom du groupe d'utilisateurs.
- **Services** : spécifiez la stratégie de service du groupe d'utilisateurs. Le service **Accès à distance IPsec** doit être activé pour ce groupe d'utilisateurs, afin que tous les membres du groupe puissent établir le tunnel VPN pour accéder en toute sécurité à vos ressources réseau.

ÉTAPE 23 Dans l'onglet **Membership**, spécifiez les membres du groupe d'utilisateurs. Vous devez ajouter au moins un utilisateur dans le groupe d'utilisateurs avant de continuer.

- Pour ajouter un membre, sélectionnez un utilisateur existant dans la liste **User** et cliquez sur la flèche droite. Les membres du groupe apparaissent dans la liste **Membership**.
- Pour supprimer un membre du groupe, sélectionnez le membre dans la liste **Membership** et cliquez sur la flèche gauche.
- Pour créer un nouvel utilisateur, entrez le nom d'utilisateur dans le champ **User Name** et le mot de passe dans le champ **Password**, entrez le même mot de passe dans le champ **Password Confirm** pour confirmer, puis cliquez sur **Create**.

ÉTAPE 24 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 25 Lorsque vous avez terminé, cliquez sur **Next**.

Affichage du résumé de l'accès à distance IPsec

ÉTAPE 26 Reportez-vous à la page IPsec Remote Access - Summary pour consulter les informations relatives à la stratégie de groupe d'accès à distance IPsec et aux groupes d'utilisateurs spécifiés.

ÉTAPE 27 Pour modifier des paramètres, cliquez sur **Back**. Si la configuration est correcte, cliquez sur **Finish** pour appliquer les paramètres.

Une fois les paramètres enregistrés, l'Cisco ISA500 est configuré en tant que serveur VPN IPsec. Les utilisateurs distants qui appartiennent aux groupes d'utilisateurs spécifiés peuvent utiliser la stratégie de groupe spécifiée pour établir les connexions VPN. Si vous cochez l'option **Client Internet Access**, les règles NAT avancées correspondantes sont créées automatiquement pour permettre aux clients VPN distants d'accéder à Internet via les tunnels VPN.

Utilisation de l'assistant VPN d'accès à distance pour configurer l'accès à distance SSL

Cette section explique comment utiliser l'assistant VPN d'accès à distance pour configurer les stratégies de groupe VPN SSL et spécifier les utilisateurs et les groupes d'utilisateurs pour l'accès à distance SSL. Reportez-vous aux étapes suivantes :

- **Lancement de l'assistant VPN d'accès à distance avec l'accès à distance SSL, page 63**
- **Configuration de la passerelle VPN SSL, page 64**
- **Configuration de la stratégie de groupe VPN SSL, page 66**
- **Configuration des groupes d'utilisateurs VPN SSL, page 69**
- **Affichage du résumé VPN SSL, page 70**

Lancement de l'assistant VPN d'accès à distance avec l'accès à distance SSL

ÉTAPE 1 Cliquez sur **Configuration Wizards > Remote Access VPN Wizard**.

ÉTAPE 2 Sélectionnez **SSL Remote Access** dans la liste déroulante **VPN Tunnel Type**.

ÉTAPE 3 Cliquez sur **Next**.

Configuration de la passerelle VPN SSL

ÉTAPE 4 Reportez-vous à la page SSL VPN - Configuration pour configurer les paramètres de la passerelle VPN SSL.

ÉTAPE 5 Dans la zone **Gateway (Basic)**, entrez les informations suivantes :

- **Gateway Interface** : sélectionnez le port WAN que le trafic traverse par le biais du tunnel VPN SSL.
- **Gateway Port** : saisissez le numéro de port utilisé pour la passerelle VPN SSL. Par défaut, SSL fonctionne sur le port 443. Toutefois, la passerelle VPN SSL doit être suffisamment flexible pour fonctionner sur un port défini par l'utilisateur. Le pare-feu doit permettre au port d'assurer la livraison des paquets destinés à la passerelle VPN SSL. Les clients VPN SSL doivent entrer la paire d'adresses complète « Adresse IP de la passerelle : numéro de port de la passerelle » pour permettre la connexion.
- **Certificate File** : sélectionnez le certificat par défaut ou un certificat importé pour authentifier les utilisateurs qui tentent d'accéder à votre ressource réseau via les tunnels VPN SSL. Pour plus d'informations sur l'importation des certificats, reportez-vous à la section **Gestion des certificats pour l'authentification, page 393**.
- **Client Address Pool** : la passerelle VPN SSL dispose d'un pool d'adresses configurable d'une taille maximale de 255, qui permet d'allouer des adresses IP aux clients distants. Saisissez le groupement d'adresses IP pour tous les clients distants. Le client se voit attribuer une adresse IP via la passerelle VPN SSL.

  REMARQUE : configurez une plage d'adresses IP qui ne couvre directement aucune autre adresse de votre réseau local.
- **Client Netmask** : entrez l'adresse IP du masque réseau utilisé pour les clients VPN SSL. Le masque réseau du client peut uniquement être IP 255.255.255.0, 255.255.255.128 et 255.255.255.192.

  Le groupement d'adresses du client est utilisé avec le masque réseau du client. Le tableau suivant montre les paramètres valides pour la saisie du groupement d'adresses du client et du masque réseau du client.

Masque réseau du client	Groupement d'adresses du client
255.255.255.0	x.x.x.0
255.255.255.128	x.x.x.0 ou x.x.x.128
255.255.255.192	x.x.x.0, x.x.x.64, x.x.x.128 ou x.x.x.192

Par exemple, s'ils sont définis comme suit, le client VPN SSL obtiendra une adresse VPN comprise entre 10.10.10.1 et 10.10.10.254.

- Pool d'adresses du client = 10.10.10.0
- Masque réseau du client = 255.255.255.0

- **Client Internet Access** : cochez cette case pour créer automatiquement des règles NAT avancées afin de permettre aux clients VPN SSL d'accéder à Internet via les tunnels VPN SSL. Si vous désactivez cette case, vous pouvez créer manuellement des règles NAT avancées. Pour plus d'informations, reportez-vous à la section **Configuration des règles NAT avancées pour autoriser les clients VPN SSL à accéder à Internet via les tunnels VPN SSL, page 355**.
- **Client Domain** : entrez le nom de domaine qui doit être envoyé aux clients VPN SSL.
- **Login Banner** : une fois l'utilisateur VPN SSL connecté, une bannière de connexion configurable s'affiche. Saisissez le texte du message à afficher avec la bannière.

ÉTAPE 6 Dans la zone **Gateway (Advanced)**, entrez les informations suivantes :

- **Idle Timeout** : entrez le délai en secondes pendant lequel la session VPN SSL peut rester inactive. La valeur par défaut est de 2 100 secondes.
- **Session Timeout** : entrez le délai en secondes pendant lequel une session VPN SSL peut rester active. La valeur par défaut est de 0 seconde, ce qui indique que la session VPN SSL peut toujours être active.
- **Client DPD Timeout** : la détection DPD (Dead Peer Detection) permet la détection des homologues morts. Saisissez le délai de DPD pendant lequel une session sera maintenue avec un client distant inactif. La valeur par défaut est de 300 secondes.

- **Gateway DPD Timeout** : saisissez le délai de détection DPD pendant lequel une session sera maintenue avec une passerelle VPN SSL inactive. La valeur par défaut est de 300 secondes.

  REMARQUE : Si la passerelle VPN SSL n'a pas de réponse deux ou trois fois au cours du délai de détection DPD, la session VPN SSL prend fin.

- **Keep Alive** : saisissez l'intervalle en secondes, auquel le client VPN SSL va envoyer des messages keepalive. Ces messages garantissent que la connexion VPN SSL reste ouverte, même si le délai d'inactivité maximal du client est limité par un périphérique intermédiaire, par exemple un proxy, un pare-feu ou un périphérique NAT.

- **Lease Duration** : entrez la durée après laquelle le client VPN SSL doit envoyer une requête de renouvellement de validité de l'adresse IP sur le serveur. La valeur par défaut est de 43 200 secondes.

- **Max MTU** : entrez l'unité de transfert maximum pour la session. La valeur par défaut est de 1 406 octets.

- **Rekey Interval** : entrez la fréquence de renouvellement des clés dans ce champ. La valeur par défaut est de 3 600 secondes.

ÉTAPE 7 Lorsque vous avez terminé, cliquez sur **Next**.

Configuration de la stratégie de groupe VPN SSL

ÉTAPE 8 Reportez-vous à la page Group Policy pour configurer les stratégies de groupe VPN SSL.

REMARQUE : jusqu'à 32 stratégies de groupe VPN SSL peuvent être configurées sur l'Cisco ISA500.

ÉTAPE 9 Cliquez sur **Add** pour ajouter une nouvelle stratégie de groupe VPN SSL.

Autres options : pour modifier une entrée, cliquez sur l'icône de **modification** (crayon). Pour supprimer une entrée, cliquez sur l'icône de **suppression** (x). Pour supprimer plusieurs entrées, cochez-les et cliquez sur **Delete**.

ÉTAPE 10 Dans l'onglet **Basic Settings**, entrez les informations suivantes :

- **Policy Name** : entrez le nom de la stratégie de groupe VPN SSL.

- **Primary DNS** : entrez éventuellement l'adresse IP du serveur DNS principal.

- **Secondary DNS** : entrez éventuellement l'adresse IP du serveur DNS secondaire.

- **Primary WINS** : entrez éventuellement l'adresse IP du serveur WINS principal.
- **Secondary WINS** : entrez éventuellement l'adresse IP du serveur WINS secondaire.

ÉTAPE 11 Dans l'onglet **IE Proxy Settings**, entrez les informations suivantes :

La passerelle VPN SSL peut spécifier plusieurs proxys de Microsoft Internet Explorer (MSIE) pour les PC clients. Si ces paramètres sont activés, IE est automatiquement configuré sur le PC client avec ces paramètres.

- **IE Proxy Policy** : sélectionnez l'une des options suivantes :
  - **None** : permet au navigateur de n'utiliser aucun paramètre de proxy.
  - **Auto** : permet au navigateur de détecter automatiquement les paramètres de proxy.
  - **Bypass-Local** : permet au navigateur de contourner les paramètres de proxy qui sont configurés sur l'utilisateur distant.
  - **Disable** : désactive les paramètres de proxy de MSIE.
- **Address** : si vous choisissez « Bypass-Local » ou « Auto », entrez l'adresse IP ou le nom de domaine du serveur proxy de MSIE.
- **Port** : entrez le numéro de port du serveur proxy de MSIE.
- **IE Proxy Exception** : vous pouvez spécifier les hôtes d'exception pour les paramètres de proxy d'Internet Explorer. Cette option permet au navigateur de ne pas envoyer de trafic via le proxy pour le nom d'hôte ou l'adresse IP fournis. Pour ajouter une entrée, saisissez l'adresse IP ou le nom de domaine d'un hôte et cliquez sur **Add**.

ÉTAPE 12 Dans la zone **Split Tunneling Settings**, entrez les informations suivantes :

La transmission tunnel partagée permet qu'un trafic spécifique soit acheminé en dehors du tunnel VPN SSL. Le trafic est soit inclus (résolu dans le tunnel) ou exclu (résolu par le biais de la connexion WAN ou FAI). Les options de la configuration de la résolution du tunnel s'excluent mutuellement. Une adresse IP ne peut pas être à la fois inclue et exclue.

- **Enable Split Tunneling** : par défaut, tout le trafic en provenance de l'hôte est acheminé via le tunnel. Cochez cette case pour activer la fonctionnalité de transmission tunnel partagée afin que le tunnel soit utilisé uniquement pour le trafic spécifié par les routes du client.

- **Split Selection** : si vous activez la transmission tunnel partagée, sélectionnez l'une des options suivantes :
  - **Include Traffic** : vous permet d'ajouter les routes du client sur le client VPN SSL de telle sorte que seul le trafic vers les réseaux de destination puisse être redirigé via les tunnels VPN SSL. Pour ajouter une route de client, saisissez le sous-réseau de destination auquel une route est ajoutée sur le client VPN SSL dans le champ **Address** et le masque de sous-réseau du réseau de destination dans le champ **Netmask,** puis cliquez sur **Add**.
  - **Exclude Traffic** : vous permet d'exclure les réseaux de destination sur le client VPN SSL. Le trafic vers les réseaux de destination est redirigé à l'aide de l'interface réseau native du client VPN SSL (résolu par le biais de la connexion WAN ou FAI). Pour ajouter une route de client, saisissez le sous-réseau de destination auquel une route est ajoutée sur le client VPN SSL dans le champ **Address** et le masque de sous-réseau du réseau de destination dans le champ **Netmask,** puis cliquez sur **Add**.

    REMARQUE : pour exclure les réseaux de destination, vérifiez que la fonctionnalité d'exclusion des LAN locaux est activée sur les clients à mobilité sécurisé Cisco AnyConnect.
  - **Exclude Local LANs** : si vous choisissez d'exclure du traffic, cochez cette case pour permettre aux utilisateurs distants d'accéder à leurs réseaux LAN sans passer par le tunnel VPN ou décochez-la pour empêcher les utilisateurs distants d'accéder à leurs réseaux LAN sans passer par le tunnel VPN.

    REMARQUE : pour exclure des réseaux LAN, veillez à ce que la fonctionnalité d'exclusion des LAN soit activée sur le serveur VPN SSL et sur les clients à mobilité sécurisés Cisco AnyConnect.
- **Split DNS** : le DNS fractionné peut diriger les paquets DNS en texte clair via Internet pour des domaines desservis via un DNS externe (servant votre ISP) ou via un tunnel VPN SSL vers des domaines desservis par le DNS d'entreprise. Pour ajouter un domaine pour la transmission tunnel des demandes DNS vers des destinations dans le réseau privé, entrez l'adresse IP ou le nom de domaine dans le champ et cliquez sur **Add**. Pour supprimer un domaine, sélectionnez-le dans la liste et cliquez sur **Delete**.

ÉTAPE 13 Dans la zone **Zone-based Firewall Settings**, vous pouvez contrôler l'accès des clients VPN SSL aux zones via les tunnels VPN SSL. Cliquez sur **Permit** pour permettre l'accès ou sur **Deny** pour le refuser.

REMARQUE : Les règles de pare-feu VPN qui sont automatiquement générées par les paramètres de contrôle d'accès aux zones seront ajoutées à la liste des règles de pare-feu avec une priorité supérieure aux règles de pare-feu par défaut, mais inférieure aux règles de pare-feu personnalisées.

ÉTAPE 14 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 15 Lorsque vous avez terminé, cliquez sur **Next**.

Configuration des groupes d'utilisateurs VPN SSL

ÉTAPE 16 Reportez-vous à la page User Group pour configurer les utilisateurs et les groupes d'utilisateurs pour l'accès à distance SSL. Le service VPN SSL doit être activé pour les groupes d'utilisateurs. Tous les membres d'un groupe d'utilisateurs peuvent utiliser la stratégie de groupe VPN SSL sélectionnée pour établir les connexions VPN SSL.

ÉTAPE 17 Cliquez sur **Add** pour ajouter un groupe d'utilisateurs.

Autres options : pour modifier une entrée, cliquez sur l'icône de **modification** (crayon). Pour supprimer une entrée, cliquez sur l'icône de **suppression** (x). Pour supprimer plusieurs entrées, cochez-les et cliquez sur **Delete**.

ÉTAPE 18 Dans l'onglet **Group Settings**, entrez les informations suivantes :

- **Name** : entrez le nom du groupe d'utilisateurs.
- **Services** : spécifiez la stratégie de service du groupe d'utilisateurs. Le service **VPN SSL** doit être activé pour ce groupe d'utilisateurs afin que tous les membres du groupe d'utilisateurs puissent établir les tunnels VPN SSL basés sur la stratégie de groupe VPN SSL sélectionnée pour accéder aux ressources du réseau.

ÉTAPE 19 Dans l'onglet **Membership**, spécifiez les membres du groupe d'utilisateurs. Vous devez ajouter au moins un utilisateur dans le groupe d'utilisateurs avant de continuer.

- Pour ajouter un membre, sélectionnez un utilisateur existant dans la liste **User** et cliquez sur la flèche droite. Les membres du groupe apparaissent dans la liste **Membership**.
- Pour supprimer un membre du groupe, sélectionnez le membre dans la liste **Membership** et cliquez sur la flèche gauche.
- Pour créer un nouveau membre, entrez le nom d'utilisateur dans le champ **User Name** et le mot de passe dans le champ **Password**, entrez le même mot de passe dans le champ **Password Confirm** pour confirmer, puis cliquez sur **Create**.

ÉTAPE 20 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 21 Lorsque vous avez terminé, cliquez sur **Next**.

Affichage du résumé VPN SSL

ÉTAPE 22 Reportez-vous à la page SSL VPN Summary pour consulter des informations pour toutes les stratégies de groupe VPN SSL et tous les groupes d'utilisateurs configurés.

ÉTAPE 23 Pour modifier des paramètres, cliquez sur **Back**. Si la configuration est correcte, cliquez sur **Finish** pour appliquer les paramètres.

Une fois les paramètres enregistrés, l'Cisco ISA500 est configuré en tant que serveur VPN SSL. Les utilisateurs VPN SSL qui appartiennent aux groupes d'utilisateurs spécifiés peuvent utiliser les stratégies de groupe sélectionnées pour établir les connexions VPN SSL. Si vous cochez l'option **Client Internet Access**, les règles NAT avancées sont créées automatiquement afin de permettre aux clients VPN SSL d'accéder à Internet via les tunnels VPN SSL.

Utilisation de l'assistant VPN de site à site pour configurer le VPN de site à site

Utilisez l'assistant VPN de site à site pour configurer une stratégie VPN de site à site pour établir une connexion sécurisée entre deux routeurs physiquement distincts. Reportez-vous aux étapes suivantes :

- **Lancement de l'assistant VPN de site à site, page 71**
- **Configuration des paramètres des homologues VPN, page 71**
- **Configuration des stratégies IKE, page 72**
- **Configuration des stratégies de transformation, page 73**
- **Configuration des réseaux locaux et distants, page 74**
- **Affichage du résumé de la configuration, page 75**

Lancement de l'assistant VPN de site à site

ÉTAPE 1 Cliquez sur **Configuration Wizards > Site-to-Site VPN Wizard**.

ÉTAPE 2 Cliquez sur **Next**.

Configuration des paramètres des homologues VPN

ÉTAPE 3 Reportez-vous à la page VPN Peer Settings pour configurer une stratégie VPN IPsec afin d'établir la connexion VPN avec un routeur distant.

- **Profile Name** : entrez le nom de la stratégie VPN IPsec.
- **WAN Interface** : sélectionnez le port WAN que le trafic traverse par le biais du tunnel VPN.
- **Remote Type** : spécifiez le type de l'homologue distant :
  - **Static IP** : sélectionnez cette option si l'homologue distant utilise une adresse IP statique. Entrez l'adresse IP du périphérique distant dans le champ **Remote Address**.
  - **Dynamic IP** : sélectionnez cette option si l'homologue distant utilise une adresse IP dynamique.
  - **FQDN (Fully Qualified Domain Name)** : sélectionnez cette option si vous voulez utiliser le nom de domaine du réseau distant, tel que vpn.company.com. Entrez le nom de domaine du périphérique distant dans le champ **Remote Address**.
- **Authentication Method** : spécifiez la méthode d'authentification.
  - **Pre-Shared Key** : utilise une clé unique, basée sur un mot de passe, pour l'authentification. Si vous choisissez cette option, saisissez la valeur que le périphérique homologue doit fournir pour établir une connexion dans le champ **Key**. La clé prépartagée PSK (Pre-Shared Key) saisie doit être exactement identique ici et sur l'homologue distant.
  - **Certificate** : utilise un certificat numérique d'une autorité de certification (CA) tierce pour l'authentification. Si vous choisissez cette option, sélectionnez un certificat CA comme certificat local dans la liste déroulante **Local Certificate** et sélectionnez un certificat CA comme certificat distant dans la liste déroulante **Remote Certificate**. Le certificat distant sélectionné sur la passerelle locale doit être configuré comme certificat local sur l'homologue distant.

REMARQUE : vous devez posséder des certificats CA valides importés sur votre Cisco ISA500 avant d'utiliser les certificats numériques pour l'authentification. Accédez à la page Device Management > Certificate Management pour importer les certificats CA. Reportez-vous à la **Gestion des certificats pour l'authentification, page 393**.

ÉTAPE 4 Lorsque vous avez terminé, cliquez sur **Next**.

Configuration des stratégies IKE

ÉTAPE 5 Reportez-vous à la page IKE Policies pour configurer les stratégies IKE et spécifier une stratégie IKE pour la stratégie VPN IPsec. Vous pouvez choisir la stratégie par défaut ou une stratégie IKE personnalisée.

ÉTAPE 6 Cliquez sur **Add** pour ajouter une stratégie IKE.

Autres options : pour modifier une entrée, cliquez sur **Edit**. Pour supprimer une entrée, sélectionnez-la et cliquez sur **Delete**. La stratégie IKE par défaut (**DefaultIke**) ne peut être ni modifiée, ni supprimée.

ÉTAPE 7 Saisissez les informations suivantes :

- **Name** : entrez le nom de la stratégie IKE.
- **Encryption** : sélectionnez l'algorithme utilisé pour négocier l'association de sécurité. Quatre algorithmes sont pris en charge par l'Cisco ISA500 : ESP_3DES, ESP_AES_128, ESP_AES_192 et ESP_AES_256.
- **HASH** : spécifiez l'algorithme d'authentification pour l'en-tête VPN. Deux algorithmes de hachage sont pris en charge par l'Cisco ISA500 : SHA1 et MD5. Veillez à ce que l'algorithme d'authentification soit configuré de manière identique des deux côtés.
- **Authentication** : spécifiez la méthode d'authentification utilisée par l'Cisco ISA500 pour établir l'identité de chaque homologue IPsec.
  - **PRE_SHARE** : utilisez une clé unique, basée sur un mot de passe, pour l'authentification. La clé alphanumérique est partagée avec l'homologue IKE. L'évolutivité des clés prépartagées PSK (Pre-Shared Key) face à un réseau en expansion est insuffisante, mais elles sont plus faciles à configurer dans un petit réseau.
  - **RSA_SIG** : utilisez un certificat numérique pour l'authentification. RSA_SIG est un certificat numérique avec des clés générées par l'algorithme de signatures RSA. Dans ce cas, un certificat doit être configuré pour que la signature RSA fonctionne.

- **D-H Group** : sélectionnez l'identifiant de groupe Diffie-Hellman. L'identifiant est utilisé par deux homologues IPsec pour dériver un secret partagé sans qu'ils se le transmettent entre eux. Le groupe D-H définit la puissance de l'algorithme en bits. Le paramètre par défaut est Group 5. Plus le numéro du groupe Diffie-Hellman est bas, moins il a besoin de temps CPU pour être exécuté. Plus le numéro de groupe D-H est élevé, plus le niveau de sécurité est important.
  - Groupe 2 (1 024 bits)
  - Groupe 5 (1 536 bits)
  - Groupe 14 (2 048 bits)
- **Lifetime** : saisissez le nombre de secondes pendant lesquelles l'association de sécurité IKE reste valide. En règle générale, une durée de vie plus courte garantit des négociations ISAKMP plus sécurisées. Toutefois, avec des durées de vie plus courtes, l'Cisco ISA500 configure plus rapidement des associations de sécurité IKE futures.

ÉTAPE 8 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 9 Lorsque vous avez terminé, cliquez sur **Next**.

Configuration des stratégies de transformation

ÉTAPE 10 Reportez-vous à la page Transform Policies pour configurer les stratégies de transformation et spécifier un ensemble de transformation pour la stratégie VPN IPsec. Vous pouvez choisir le paramètre par défaut ou un ensemble de transformation personnalisé.

ÉTAPE 11 Cliquez sur **Add** pour ajouter un ensemble de transformation.

Autres options : pour modifier une entrée, cliquez sur **Edit**. Pour supprimer une entrée, sélectionnez-la et cliquez sur **Delete**. L'ensemble de transformation par défaut (**DefaultTrans**) ne peut être ni modifié, ni supprimé.

ÉTAPE 12 Saisissez les informations suivantes :

- **Name** : saisissez le nom de l'ensemble de transformation.
- **Integrity** : sélectionnez l'algorithme de hachage utilisé pour assurer l'intégrité des données. L'algorithme de hachage garantit qu'un paquet provient d'où il dit provenir et qu'il n'a pas été modifié en chemin.

- **ESP_SHA1_HMAC** : authentification avec SHA1 (160 bits).
- **ESP_MD5_HMAC** : authentification avec MD5 (128 bits). MD5 a une empreinte plus petite et est considéré comme étant un peu plus rapide que SHA1. Une attaque réussie (mais extrêmement difficile) contre MD5 est survenue ; cependant, la variante HMAC utilisée par IKE empêche cette attaque.

▪ **Encryption** : sélectionnez l'algorithme de cryptage symétrique qui protège la transmission des données entre deux homologues IPsec. Le paramètre par défaut est ESP_3DES. La norme AES (Advanced Encryption Standard) prend en charge des longueurs de clé de 128, 192 et 256 bits.

- **ESP_3DES** : cryptage avec 3DES (168 bits).
- **ESP_AES_128** : cryptage avec AES (128 bits).
- **ESP_AES_192** : cryptage avec AES (192 bits).
- **ESP_AES_256** : cryptage avec AES (256 bits).

ÉTAPE 13 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 14 Lorsque vous avez terminé, cliquez sur **Next**.

Configuration des réseaux locaux et distants

ÉTAPE 15 Reportez-vous à la page Local and Remote VPN Networks pour configurer les réseaux locaux et distants.

▪ **Local Subnet** : sélectionnez l'adresse IP pour votre réseau local. Sélectionnez **Any** si vous voulez activer les paramètres de contrôle d'accès de zone afin de pouvoir contrôler le trafic entrant provenant du réseau VPN distant dans les zones via les tunnels VPN.

▪ **Remote Subnet** : sélectionnez l'adresse IP pour le réseau distant. Vous devez connaître l'adresse IP du réseau distant avant de connecter le tunnel VPN.

Si l'objet Adresse IP que vous souhaitez ne figure pas dans la liste, sélectionnez **Create a new address** pour ajouter un nouvel objet Adresse ou sélectionnez **Create a new address group** pour ajouter un nouvel objet Groupe d'adresses. Pour gérer les objets d'adresses et de groupes d'adresses, accédez à la page Networking > Address Management. Reportez-vous à la **Gestion d'adresse, page 182**.

REMARQUE : L'Cisco ISA500 peut prendre en charge plusieurs sous-réseaux pour établir les tunnels VPN. Vous devez sélectionner un objet Groupe d'adresses incluant plusieurs sous-réseaux pour les réseaux locaux et distants.

ÉTAPE 16 Lorsque vous avez terminé, cliquez sur **Next**.

Affichage du résumé de la configuration

ÉTAPE 17 Reportez-vous à la page Summary pour consulter les informations relatives à la stratégie VPN IPsec.

ÉTAPE 18 Pour modifier des paramètres, cliquez sur **Back**. Si la configuration est correcte, cliquez sur **Finish** pour appliquer les paramètres.

ÉTAPE 19 Une fois que vous avez cliqué sur Finish, le message d'avertissement suivant apparaît : « Do you want to make this connection active when the settings are saved? (Only one connection can be active at a time.) » [(Souhaitez-vous activer cette connexion une fois les paramètres enregistrés ? (Vous ne pouvez activer qu'une seule connexion VPN à la fois)]

- Si vous souhaitez activer la connexion immédiatement après l'enregistrement des paramètres, cliquez sur **Activate Connection**. Une fois que vous avez enregistré vos paramètres, l'Cisco ISA500 tente immédiatement d'établir la connexion VPN.
- Si vous souhaitez uniquement créer la stratégie VPN IPsec et ne souhaitez pas activer la connexion immédiatement après l'enregistrement des paramètres, cliquez sur **Do Not Activate**. La connexion sera déclenchée par tout trafic correspondant à cette stratégie VPN IPsec et le tunnel VPN sera configuré automatiquement. Vous pouvez également accéder à la page VPN > Site-to-Site > IPsec Policies pour établir manuellement la connexion VPN en cliquant sur l'icône **de connexion**.

Utilisation de l'assistant DMZ pour configurer les paramètres DMZ

Utilisez l'assistant DMZ pour configurer DMZ et les services DMZ si vous devez héberger des services publics. Reportez-vous aux étapes suivantes :

- Lancement de l'assistant DMZ, page 76
- Configuration des profils DDNS, page 76
- Configuration du réseau DMZ, page 77
- Configuration des services DMZ, page 79
- Affichage du résumé de la configuration, page 80

Lancement de l'assistant DMZ

ÉTAPE 1 Cliquez sur **Configuration Wizards > DMZ Wizard**.

ÉTAPE 2 Cliquez sur **Next**.

Configuration des profils DDNS

ÉTAPE 3 Éventuellement, reportez-vous à la page DDNS Setup pour configurer les profils DDNS pour la gestion à distance du réseau DMZ.

REMARQUE : jusqu'à 16 stratégies de groupe VPN DDNS peuvent être configurées sur l'Cisco ISA500.

ÉTAPE 4 Cliquez sur **Add** pour créer un profil DDNS.

Autres options : pour modifier une entrée, cliquez sur l'icône de **modification** (crayon). Pour supprimer une entrée, cliquez sur l'icône de **suppression** (x).

ÉTAPE 5 Saisissez les informations suivantes :

- **Service** : sélectionnez DynDNS ou No-IP service.

  REMARQUE : Vous devez souscrire un compte auprès de l'un de ces fournisseurs avant de pouvoir utiliser ce service.

- **Active On Startup** : cliquez sur **On** pour activer le paramètre DDNS au démarrage de l'Cisco ISA500.

- **WAN Interface** : sélectionnez le port WAN pour le service DDNS. Le trafic des services DDNS passera par le port WAN spécifié.

  REMARQUE : Si la redondance WAN est définie comme mode de basculement, cette option est grisée. Lorsque le basculement du WAN se produit, le DDNS bascule le trafic sur le port WAN actif.

- **User Name** : entrez le nom d'utilisateur du compte que vous avez enregistré dans le fournisseur DDNS.
- **Password** : entrez le mot de passe du compte que vous avez enregistré dans le fournisseur DDNS.
- **Host and Domain Name** : spécifiez le nom d'hôte et le nom de domaine complets pour le service DDNS.
- **Use wildcards** : cochez cette case pour permettre à tous les sous-domaines de votre nom d'hôte DDNS de partager la même adresse IP publique comme nom d'hôte.
- **Update every week** : cochez cette case pour mettre à jour les informations de l'hôte chaque semaine.

ÉTAPE 6 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 7 Lorsque vous avez terminé, cliquez sur **Next**.

Configuration du réseau DMZ

ÉTAPE 8 Reportez-vous à la page DMZ Configuration pour configurer les réseaux DMZ.

REMARQUE : jusqu'à 4 stratégies de groupe VPN DMZ peuvent être configurées sur l'Cisco ISA500. Vous devez configurer au moins un réseau DMZ pour terminer l'assistant DMZ.

ÉTAPE 9 Cliquez sur **Add** pour créer un réseau DMZ.

Autres options : pour modifier une entrée, cliquez sur l'icône de **modification** (crayon). Pour supprimer une entrée, cliquez sur l'icône de **suppression** (x).

ÉTAPE 10 Dans l'onglet **Basic Setting**, entrez les informations suivantes :

- **Name** : entrez le nom de la DMZ.
- **IP** : entrez l'adresse IP de sous-réseau de la zone DMZ.
- **Netmask** : entrez le masque de sous-réseau de la DMZ.
- **Spanning Tree** : cochez cette case pour activer la fonctionnalité Spanning Tree afin de déterminer s'il existe des boucles dans la topologie de réseau.

- **Port** : sélectionnez un port configurable dans la liste **Port** et ajoutez-le dans la liste **Member**. Le port configurable sélectionné est défini comme port DMZ en mode d'accès.
- **Zone** : choisissez la zone DMZ par défaut ou une zone DMZ personnalisée à laquelle la DMZ est mappée.

ÉTAPE 11 Dans l'onglet **DHCP Pool Settings**, choisissez le mode DHCP dans la liste déroulante **DHCP Mode**.

- **Disable** : choisissez cette option si les ordinateurs de la DMZ sont configurés avec des adresses IP statiques ou sont configurés pour utiliser un autre serveur DHCP.
- **DHCP Server** : permet à l'Cisco ISA500 d'agir en tant que serveur DHCP et affecte les adresses IP à tous les périphériques connectés à la DMZ. Tout nouveau client DHCP se connectant à la DMZ reçoit une adresse IP du pool DHCP.
- **DHCP Relay** : permet à l'Cisco ISA500 d'utiliser un relais DHCP. Si vous choisissez le relais DHCP, entrez l'adresse IP du serveur DHCP distant dans le champ **Relay IP**.

ÉTAPE 12 Si vous choisissez **DHCP Server** comme mode DHCP, entrez les informations suivantes :

- **Start IP** : entrez l'adresse IP de début du pool DHCP.
- **Start IP** : entrez l'adresse IP de début du pool DHCP.

  REMARQUE : l'adresse IP de début et l'adresse IP de fin doivent être dans le même sous-réseau que l'adresse IP du DMZ.
- **Lease Time** : entrez la durée de connexion maximale de « location » d'une adresse IP dynamique à un utilisateur du réseau. Lorsque le temps s'est écoulé, une nouvelle adresse IP dynamique est automatiquement attribuée à l'utilisateur.
- **DNS1** : entrez l'adresse IP du serveur DNS principal.
- **DNS2** : en option, entrez l'adresse IP d'un serveur DNS secondaire.
- **WINS1** : entrez éventuellement l'adresse IP du serveur WINS principal.
- **WINS2** : entrez éventuellement l'adresse IP d'un serveur WINS secondaire.
- **Domain Name** : entrez éventuellement le nom de domaine de la DMZ.
- **Default Gateway** : entrez l'adresse IP de la passerelle par défaut.

ÉTAPE 13 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 14 Lorsque vous avez terminé, cliquez sur **Next**.

Configuration des services DMZ

ÉTAPE 15 Reportez-vous à la page DMZ Service pour configurer les services DMZ.

ÉTAPE 16 Cliquez sur **Add** pour créer un service DMZ.

Autres options : pour modifier une entrée, cliquez sur l'icône de **modification** (crayon). Pour supprimer une entrée, cliquez sur l'icône de **suppression** (x). Pour supprimer plusieurs entrées, cochez-les et cliquez sur **Delete**.

ÉTAPE 17 Saisissez les informations suivantes :

- **Original Service** : sélectionnez un service comme service entrant.
- **Translated Service** : sélectionnez un service en tant que service traduit ou sélectionnez **Original** si le service traduit est le même que le service entrant. Si le service de votre choix ne figure pas dans la liste, sélectionnez **Create a new service** pour créer un nouvel objet Service. Pour conserver les objets Service, accédez à la page Networking > Service Management. Reportez-vous à la **Gestion des services, page 184**.

  REMARQUE : La traduction un-à-un sera exécutée pour le transfert de plage de ports. Par exemple, si vous souhaitez traduire un service TCP original avec la plage de ports 50000 à 50002 en un service TCP avec la plage de ports 60000 à 60002, le port 50000 sera traduit en port 60000, le port 50001 sera traduit en port 60001 et le port 50002 sera traduit en port 60002.
- **Translated IP** : sélectionnez l'adresse IP de votre serveur local qui doit être traduit. Si l'adresse IP de votre choix ne figure pas dans la liste, sélectionnez **Create a new address** pour créer un nouvel objet Adresse IP. Pour conserver les objets Adresse IP, accédez à la page Networking > Address Management. Reportez-vous à la **Gestion d'adresse, page 182**.
- **WAN** : sélectionnez WAN1 ou WAN2, ou les deux, comme port WAN entrant.
- **WAN IP** : spécifiez l'adresse IP publique du serveur. Vous pouvez utiliser l'adresse IP du port WAN sélectionné ou une adresse IP publique fournie par votre ISP. Lorsque vous sélectionnez **Both** en tant que port WAN entrant, cette option est grisée.
- **Enable DMZ Service** : cliquez sur **On** pour activer le service DMZ ou cliquez sur **Off** pour créer uniquement le service DMZ.

- **Create Firewall Rule** : cochez cette case pour créer automatiquement une règle de pare-feu permettant d'autoriser l'accès pour ce service DMZ. Vous devez créer manuellement une règle de pare-feu si vous désactivez cette case à cocher.

  REMARQUE : Si vous sélectionnez Both en tant que port WAN entrant, une règle de pare-feu de n'importe quelle zone à n'importe quelle zone est alors créée.

- **Description** : entrez le nom du service DMZ.

  Par exemple, vous hébergez un serveur RDP (192.168.12.101) dans la DMZ. Votre ISP vous a fourni une adresse IP statique (172.39.202.102) que vous souhaitez exposer au public comme votre adresse de serveur RDP. Vous pouvez créer un service DMZ comme suit pour permettre à l'utilisateur Internet d'accéder au serveur RDP à l'aide de l'adresse IP publique spécifiée.

Original Service	RDP
Translated Service	RDP
Translated IP	RDPServer
WAN	WAN1
WAN IP	PublicIP
Enable DMZ Service	On
Create Firewall Rule	On

REMARQUE : dans cet exemple, vous devez créer manuellement deux objets Adresse (RDPServer et PublicIP) et un objet Service TCP avec le port 3389 appelé « RDP ».

ÉTAPE 18 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 19 Lorsque vous avez terminé, cliquez sur **Next**.

Affichage du résumé de la configuration

ÉTAPE 20 Reportez-vous à la page Summary pour afficher les informations relatives à la configuration.

ÉTAPE 21 Pour modifier des paramètres, cliquez sur **Back**. Si la configuration est correcte, cliquez sur **Finish** pour appliquer les paramètres.

Utilisation de l'assistant sans fil pour configurer les paramètres sans fil (pour l'ISA550W et l'ISA570W uniquement)

Si vous utilisez l'ISA550W ou l'ISA570W, vous pouvez utiliser l'assistant sans fil pour configurer le réseau sans fil. Reportez-vous aux étapes suivantes :

- **Lancement de l'assistant sans fil, page 81**
- **Configuration des paramètres de la radio sans fil, page 81**
- **Configuration des types de connectivité sans fil, page 82**
- **Spécifier les paramètres de connectivité sans fil pour tous les SSID activés, page 83**
- **Affichage du résumé de la configuration, page 83**

Lancement de l'assistant sans fil

ÉTAPE 1 Cliquez sur **Configuration Wizards > Wireless Wizard**.

ÉTAPE 2 Cliquez sur **Next**.

Configuration des paramètres de la radio sans fil

ÉTAPE 3 Reportez-vous à la page Wireless Radio pour configurer les paramètres de transmission de données par liaison sans fil.

- **Wireless Mode** : choisissez la technique de modulation 802.11.
  - **802.11b/g mixed** : sélectionnez ce mode si certains périphériques du réseau sans fil utilisent 802.11b et que d'autres utilisent 802.11g. Les clients 802.11b et 802.11g peuvent se connecter au point d'accès.
  - **802.11g/n mixed** : sélectionnez ce mode si certains périphériques du réseau sans fil utilisent 802.11g et que d'autres utilisent 802.11n. Les clients 802.11g et 802.11n peuvent se connecter au point d'accès.
  - **802.11b/g/n mixed** : sélectionnez ce mode pour autoriser les clients 802.11b, 802.11g et 802.11n utilisant la fréquence 2,4 GHz à se connecter au point d'accès.

- **802.11n only** : sélectionnez ce mode si tous les périphériques du réseau sans fil peuvent prendre en charge 802.11n. Seuls les clients 802.11n qui utilisent la fréquence 2.4 GHz peuvent se connecter au point d'accès.

- **Wireless Channel** : sélectionnez un canal dans une liste de canaux ou sélectionnez l'option **Auto** pour permettre au système de déterminer le canal optimal à utiliser en fonction des niveaux sonores environnementaux des canaux disponibles.

ÉTAPE 4 Lorsque vous avez terminé, cliquez sur **Next**.

Configuration des types de connectivité sans fil

ÉTAPE 5 Reportez-vous à la page Choose SSIDs pour activer et configurer les SSID que vous souhaitez utiliser.

- **Enable** : cochez cette case pour activer le SSID.

- **Mode** : sélectionnez le type de connectivité sans fil pour chaque SSID activé.

  - **Intranet WLAN Access** : permet aux utilisateurs sans fil d'accéder au réseau d'entreprise via le réseau sans fil. Par défaut, le WLAN est mappé sur le VLAN DEFAULT.

  - **Guest WLAN Access** : autorise uniquement les utilisateurs sans fil qui se connectent au SSID invité pour accéder au réseau d'entreprise via le réseau sans fil. Par défaut, le WLAN est mappé sur le VLAN GUEST.

  - **Captive Portal Access** : autorise uniquement les utilisateurs qui se sont authentifiés à accéder au réseau d'entreprise via le réseau sans fil. Les utilisateurs sans fil sont dirigés vers une page de connexion de zone d'accès sans fil spécifique pour s'authentifier, puis ils sont dirigés vers un portail Web spécifié après connexion avant de pouvoir accéder à Internet.

REMARQUE : vous ne pouvez définir qu'un seul SSID à la fois pour l'accès au portail captif.

ÉTAPE 6 Lorsque vous avez terminé, cliquez sur **Next**.

Spécifier les paramètres de connectivité sans fil pour tous les SSID activés

ÉTAPE 7 Spécifiez les paramètres de connectivité sans fil pour tous les SSID activés.

- Pour plus d'informations pour configurer les paramètres de connectivité pour l'accès WLAN Intranet, reportez-vous à la section **Configuration du SSID pour l'accès WLAN Intranet, page 83**.
- Pour plus d'informations pour configurer les paramètres de connectivité pour l'accès WLAN invité, reportez-vous à la section **Configuration du SSID pour l'accès WLAN invité, page 85**.
- Pour plus d'informations pour configurer les paramètres de connectivité pour l'accès au portail captif, reportez-vous à la section **Configuration du SSID pour l'accès au portail captif, page 86**.

ÉTAPE 8 Lorsque vous avez terminé, cliquez sur **Next**.

Affichage du résumé de la configuration

ÉTAPE 9 Reportez-vous à la page Summary pour afficher les informations relatives à la configuration.

ÉTAPE 10 Pour modifier des paramètres, cliquez sur **Back**. Si la configuration est correcte, cliquez sur **Finish** pour enregistrer les paramètres.

Configuration du SSID pour l'accès WLAN Intranet

Suivez ces étapes pour configurer les paramètres de connectivité pour l'accès WLAN Intranet.

ÉTAPE 1 Saisissez les informations suivantes :

- **SSID** : entrez le nom du SSID.
- **Broadcast SSID** : cochez cette case pour diffuser le SSID dans ses trames de balise. Tous les périphériques sans fil à portée peuvent voir le SSID lorsqu'ils recherchent des réseaux disponibles. Décochez cette case pour empêcher la détection automatique du SSID. Dans ce cas, les utilisateurs doivent connaître le SSID pour configurer une connexion sans fil à ce SSID.
- **Station Isolation** : cochez cette option afin que les clients sans fil sur le même SSID ne puissent pas se voir entre eux.

ÉTAPE 2 Dans la zone **Security Settings**, spécifiez les paramètres de sécurité sans fil.

- **Security Mode** : sélectionnez le mode de sécurité et configurez les paramètres de sécurité correspondants. Pour des raisons de sécurité, nous vous recommandons vivement d'utiliser WPA2 pour la sécurité sans fil. Par exemple, si vous sélectionnez WPA2-Personal, entrez les informations suivantes :
  - **Encryption** : WPA2-Personal utilise toujours AES pour le cryptage des données.
  - **Shared Secret** : la clé prépartagée PSK (Pre-Shared Key) est la clé secrète partagée pour WPA. Saisissez une chaîne comprenant entre 8 et 63 caractères.
  - **Key Renewal Timeout** : entrez une valeur pour définir l'intervalle d'actualisation de la clé pour les clients associés à ce SSID. La valeur zéro (0) indique que la clé n'est pas actualisée. La valeur par défaut est 3 600 secondes.

  REMARQUE : pour obtenir des informations sur la configuration d'autres modes de sécurité, reportez-vous à la section **Configuration de la sécurité sans fil, page 195**.

ÉTAPE 3 Dans la zone **Advanced Settings**, entrez les informations suivantes :

- **VLAN Mapping** : sélectionnez le VLAN auquel le SSID est mappé. Tout le trafic en provenance des clients sans fil connectés à ce SSID est dirigé vers le VLAN sélectionné. Pour l'accès VLAN Intranet, vous devez sélectionner un VLAN mappé à une zone approuvée.
- **User Limit** : spécifiez le nombre maximal d'utilisateurs pouvant se connecter simultanément à ce SSID. Entrez une valeur comprise entre 0 et 200. La valeur par défaut est 0 (zéro), ce qui indique qu'il n'y a pas de limite pour ce SSID.

  REMARQUE : Le nombre maximal d'utilisateurs pouvant se connecter simultanément à tous les SSID activés est 200.

Configuration du SSID pour l'accès WLAN invité

Suivez ces étapes pour configurer les paramètres de connectivité pour l'accès WLAN invité.

ÉTAPE 1 Saisissez les informations suivantes :

- **SSID** : entrez le nom du SSID.
- **Broadcast SSID** : cochez cette case pour diffuser le SSID dans ses trames de balise. Tous les périphériques sans fil à portée peuvent voir le SSID lorsqu'ils recherchent des réseaux disponibles. Décochez cette case pour empêcher la détection automatique du SSID. Dans ce cas, les utilisateurs doivent connaître le SSID pour configurer une connexion sans fil à ce SSID.
- **Station Isolation** : cochez cette option afin que les clients sans fil sur le même SSID ne puissent pas se voir entre eux.

ÉTAPE 2 Dans la zone **Security Settings**, spécifiez les paramètres de sécurité sans fil.

- **Security Mode** : sélectionnez le mode de sécurité et configurez les paramètres de sécurité correspondants. Pour plus d'informations sur la configuration du mode de sécurité, reportez-vous à la section **Configuration de la sécurité sans fil, page 195**.

ÉTAPE 3 Dans la zone **Advanced Settings**, entrez les informations suivantes :

- **VLAN Mapping** : sélectionnez le VLAN auquel le SSID est mappé. Tout le trafic en provenance des clients sans fil connectés à ce SSID est dirigé vers le VLAN sélectionné. Pour l'accès VLAN invité, vous devez sélectionner un VLAN mappé à une zone invitée.
- **User Limit** : spécifiez le nombre maximal d'utilisateurs pouvant se connecter simultanément à ce SSID. Entrez une valeur comprise entre 0 et 200. La valeur par défaut est 0 (zéro), ce qui indique qu'il n'y a pas de limite pour ce SSID.

  REMARQUE : Le nombre maximal d'utilisateurs pouvant se connecter simultanément à tous les SSID activés est 200.

Configuration du SSID pour l'accès au portail captif

Suivez ces étapes pour configurer les paramètres de connectivité pour l'accès au portail captif. Dans cette configuration, le réseau sans fil permet l'accès uniquement par les utilisateurs sans fil qui se sont authentifiés correctement. Lors d'une tentative d'accès à Internet, les utilisateurs sans fil sont dirigés vers une page de connexion de zone d'accès sans fil spécifique pour s'authentifier, puis ils sont dirigés vers un portail Web spécifié.

ÉTAPE 1 Saisissez les informations suivantes :

- **SSID** : entrez le nom du SSID.
- **Broadcast SSID** : cochez cette case pour diffuser le SSID dans ses trames de balise. Tous les périphériques sans fil à portée peuvent voir le SSID lorsqu'ils recherchent des réseaux disponibles. Décochez cette case pour empêcher la détection automatique du SSID. Dans ce cas, les utilisateurs doivent connaître le SSID pour configurer une connexion sans fil à ce SSID.
- **Station Isolation** : cochez cette option afin que les clients sans fil sur le même SSID ne puissent pas se voir entre eux.

ÉTAPE 2 Dans la zone **Security Settings**, sélectionnez le **mode de sécurité** et configurez les paramètres correspondants. Pour plus d'informations sur la configuration du mode de sécurité, reportez-vous à la section **Configuration de la sécurité sans fil, page 195**.

ÉTAPE 3 Dans la zone **Authentication**, la méthode d'authentification utilisée pour authentifier les utilisateurs sans fil s'affiche. Ce paramètre est dérivé des paramètres d'authentification des utilisateurs. Reportez-vous à la page Users > User Authentication pour configurer la méthode d'authentification. Pour plus d'informations, reportez-vous à la section **Configuration des paramètres d'authentification des utilisateurs, page 365**.

ÉTAPE 4 Dans la zone **Captive Portal Authentication Type**, spécifiez la méthode d'authentification Web et configurez les paramètres correspondants :

- **Web Authentication Type** : sélectionnez l'une des méthodes suivantes :
  - **Internal** : utilise la page de connexion de zone d'accès sans fil par défaut pour authentifier les utilisateurs sans fil. Pour se connecter, le nom d'utilisateur et le mot de passe sont nécessaires.
  - **Internal, no auth with accept button** : permet aux utilisateurs sans fil d'accéder au réseau sans fil sans saisir le nom d'utilisateur et le mot de passe. Si vous choisissez cette option, cliquez sur le bouton **Accept** sur la page de connexion de zone d'accès sans fil par défaut pour accéder au réseau sans fil sans authentification.

- **External** : utilise une page de connexion de zone d'accès sans fil personnalisée sur un serveur Web externe pour authentifier les utilisateurs sans fil. Pour se connecter, le nom d'utilisateur et le mot de passe sont nécessaires.
- **External, no auth with accept button** : permet aux utilisateurs sans fil d'accéder au réseau sans fil sans saisir le nom d'utilisateur et le mot de passe. Si vous choisissez cette option, cliquez sur le bouton **Accept** sur la page de connexion de zone d'accès sans fil personnalisée pour accéder au réseau sans fil sans authentification.

▪ **Redirect URL After Login** : entrez l'URL souhaitée, incluant http:// ou https:// dans ce champ (telle que l'URL de votre entreprise : http://www.cisco.com). Si vous ne spécifiez pas le portail (champ vide), les utilisateurs sans fil accéderont directement au site Web d'origine.

Supposons, par exemple, que vous sélectionniez **Internal** pour l'authentification et que le portail Web défini soit http://www.ABcompanyC.com. Ensuite, lorsqu'un utilisateur sans fil tente d'accéder à un site Web externe, tel que http://www.google.com, la page de connexion de zone d'accès sans fil par défaut s'affiche.

Saisissez le nom d'utilisateur et le mot de passe, puis cliquez sur **Login**. Une fois que l'utilisateur sans fil est connecté, il est dirigé vers le portail Web (http://www.ABcompanyC.com). Le temps passé en ligne par l'utilisateur sans fil connecté apparaît dans la barre de titre de la page de connexion. Cliquez sur **Logout** pour vous déconnecter.

▪ **Authentication Web Server** : si vous sélectionnez **External** ou **External, no auth with accept button** comme méthode d'authentification Web, entrez l'URL complète du serveur Web externe (incluant https://) dans ce champ, par exemple https://172.24.10.10/cgi-bin/PortalLogin.cgi.

▪ **Authentication Web Key** : si vous sélectionnez **External** ou **External, no auth with accept button** comme méthode d'authentification Web, entrez la clé utilisée pour protéger le nom d'utilisateur et le mot de passe que le serveur Web externe envoie à l'Cisco ISA500 pour son authentification.

▪ **Monitored HTTP Port List** : spécifiez les ports pour surveiller les requêtes HTTP. Les requêtes HTTP qui transitent par les ports HTTP surveillés sont dirigées vers la page de portail Web spécifiée. Pour ajouter un port HTTP surveillé, cliquez sur **Add**. Pour modifier une entrée, cliquez sur l'icône de **modification** (crayon). Pour supprimer une entrée, cliquez sur l'icône de **suppression** (x).

REMARQUE : le portail captif surveille uniquement les requêtes HTTPS qui transitent par le port 443.

ÉTAPE 5 Dans la zone **Advanced Settings**, spécifiez les informations suivantes :

- **VLAN Mapping** : sélectionnez le VLAN auquel le SSID est mappé. Tout le trafic en provenance des clients sans fil connectés à ce SSID est dirigé vers le VLAN sélectionné.
- **User Limit** : spécifiez le nombre maximal d'utilisateurs pouvant se connecter simultanément à ce SSID. Entrez une valeur comprise entre 0 et 200. La valeur par défaut est 0 (zéro), ce qui indique qu'il n'y a pas de limite pour ce SSID.

  REMARQUE : le nombre maximal d'utilisateurs pouvant se connecter simultanément à tous les SSID activés est 200.

3

Status

Ce chapitre explique comment afficher l'état de l'Cisco ISA500. Il comprend les sections suivantes :

- **Tableau de bord de l'état du périphérique, page 89**
- **État du réseau, page 93**
- **État sans fil (pour l'ISA550W et l'ISA570W uniquement), page 104**
- **NAT Status, page 105**
- **État du VPN, page 106**
- **Active User Sessions, page 111**
- **Security Services Reports, page 111**
- **System Status, page 118**

Pour accéder aux pages relatives aux états, cliquez sur **Status** dans le volet de navigation de gauche.

Tableau de bord de l'état du périphérique

Reportez-vous à la page Status > Dashboard pour consulter les informations relatives à l'Cisco ISA500 et ses paramètres actuels.

Status > Dashboard

Champ	Description
Informations sur le système	
Nom du système	Nom de l'unité du périphérique

Champ	Description
Firmware (Primary/Secondary)	Version du microprogramme que l'Cisco ISA500 utilise actuellement (Primary) et version du microprogramme qui était utilisé précédemment (Secondary). Par défaut, l'Cisco ISA500 s'initialise en exécutant le microprogramme principal.
Bootloader Version	Version du chargeur d'amorçage de l'Cisco ISA500.
Numéro de série	Numéro de série de l'Cisco ISA500.
PID	Identifiant de produit (PID) de l'Cisco ISA500, également connu en tant que nom de produit, nom de modèle et numéro de produit.
UDI	Identifiant unique de périphérique (UDI) de l'Cisco ISA500. L'UDI correspond au standard d'identification des produits Cisco pour les produits matériels.
Utilisation des ressources Pour afficher tous les détails de l'utilisation des ressources, cliquez sur **details**.	
Utilisation de l'UC	Utilisation actuelle du CPU.
CPU Utilization Over 1 Minute	Utilisation moyenne du CPU au cours de la dernière minute
Memory Utilization	Utilisation totale de la mémoire après le démarrage de l'Cisco ISA500.
System Up Time	Durée pendant laquelle l'Cisco ISA500 s'est exécuté.
Current Time	Date et heure actuelles du système.
Licences Affiche l'état de la licence de sécurité qui est utilisée pour activer les services de sécurité. Pour gérer la licence de sécurité, cliquez sur **manage**.	
Résumé Syslog Affiche le récapitulatif des journaux d'événements du système. Les entrées Syslog peuvent avoir différents niveaux de gravité. Pour afficher les journaux complets, cliquez sur **details**.	
Emergency	Nombre total de journaux d'urgence. Cliquez sur le lien pour afficher tous les détails.

Champ	Description
Alert	Nombre total de journaux d'alertes. Cliquez sur le lien pour afficher tous les détails.
Critical	Nombre total de journaux critiques. Cliquez sur le lien pour afficher tous les détails.
Error	Nombre total de journaux d'erreurs. Cliquez sur le lien pour afficher tous les détails.
Attention	Nombre total de journaux d'avertissements. Cliquez sur le lien pour afficher tous les détails.
Notification	Nombre total de journaux de notifications. Cliquez sur le lien pour afficher tous les détails.
Information	Nombre total de journaux d'informations. Cliquez sur le lien pour afficher tous les détails.
Debug	Nombre total de journaux de débogage. Cliquez sur le lien pour afficher tous les détails.
Site-to-Site VPN Affiche le nombre total de tunnels VPN de site à site actifs. Pour afficher tous les détails, cliquez sur **details**.	
VPN d'accès distant	
SSL Users	Nombre total d'utilisateurs VPN SSL actifs. Cliquez sur le lien **SSL Users** pour afficher tous les détails.
IPsec Users	Nombre total d'utilisateurs VPN IPsec actifs. Cliquez sur le lien **IPsec Users** pour afficher tous les détails. Cette option est disponible uniquement lorsque l'Cisco ISA500 agit en tant que serveur VPN IPsec.
Mode de routage Affiche le mode de routage (NAT ou routage) entre les réseaux WAN et LAN. Par défaut, le mode NAT est activé. Pour activer ou désactiver le mode de routage (Routing), cliquez sur **details**.	
Ports physiques	
Name	Nom du port physique.
Port Type	Type de port physique, par exemple WAN, LAN, ou DMZ.

Champ	Description
Mode	État de la liaison du port physique
Mode WAN Affiche le mode de fonctionnement WAN, tel que Single - WAN1 (simple), Failover (basculement) ou Load Balancing (équilibrage de charge). Pour afficher tous les détails de redondance WAN, cliquez sur **details.**	
Interface(s) WAN Pour afficher tous les détails de tous les ports WAN, cliquez sur **details.**	
Name	Nom du port WAN.
IP Address	Adresse IP du port WAN
Interfaces LAN Pour afficher tous les détails de tous les réseaux VLAN, cliquez sur **details.**	
Index	ID du VLAN.
Name	Nom du VLAN.
DHCP Mode	Mode DHCP du VLAN
IP Address	Adresse IP de sous-réseau du VLAN.
Interface DMZ Pour afficher tous les détails de toutes les zones DMZ, cliquez sur **details.**	
Port	Port configurable qui est défini comme port DMZ
Name	Nom du port DMZ
IP Address	Adresse IP de sous-réseau du port DMZ.
Interfaces sans fil (pour l'ISA550W et l'ISA570W uniquement) Pour afficher tous les détails de tous les SSID, cliquez sur **details.**	
SSID Number	Numéro du SSID.
SSID Name	Nom du SSID.
VLAN	Réseaux VLAN auxquels le SSID est mappé
Client List	Nombre de stations clientes connectées au SSID.

État du réseau

Reportez-vous aux pages sur l'état du réseau pour afficher les informations concernant les différentes interfaces, les rapports d'utilisation du réseau, les rapports de la bande passante WAN, toutes les entrées du protocole ARP (Address Resolution Protocol) et l'affectation d'adresses DHCP. Reportez-vous aux rubriques suivantes :

- **Récapitulatif de l'état, page 93**
- **Statistiques de trafic, page 96**
- **Rapports d'utilisation, page 97**
- **Rapports de la bande passante WAN, page 99**
- **Table ARP, page 100**
- **Liaisons DHCP, page 100**
- **État du STP, page 101**
- **Voisinage CDP, page 103**

Récapitulatif de l'état

Reportez-vous à la page Network Status > Status Summary pour afficher les informations concernant les différentes interfaces.

Network Status > Status Summary

Champ	Description
Ethernet	
Port	Numéro du port physique.
Name	Nom du port physique.
Enable	Indique si le port physique est activé ou désactivé.
Port Type	Type de port physique, par exemple WAN, LAN, ou DMZ.
Line Status	Indique si le port physique est connecté ou non.
Speed/Duplex	Mode duplex (paramètre de vitesse et duplex) du port physique.

Champ	Description
Mode	Mode d'accès du port physique. Un port WAN ou DMZ est toujours défini en mode d'accès et un port LAN peut être défini en mode d'accès ou de liaison.
VLAN	VLAN auxquels le port physique est mappé.
PVID	ID de VLAN du port (PVID) à utiliser pour transférer ou filtrer les paquets non marqués arrivant sur le port. Le PVID d'un port de liaison est fixé sur le DEFAULT VLAN (1).
WAN	
Name	Nom du port WAN.
Type de WAN	Mode d'adressage réseau utilisé pour la connexion à Internet du port WAN.
Connection Time	Durée de connexion du port WAN, en secondes.
Connection Status	Indique si le port WAN obtient une adresse IP avec succès ou non. Si oui, l'état de la connexion est « Connected ».
WAN State	Indique si le port WAN est actif ou inactif pour le routage. Si le port WAN est actif pour le routage, l'état du WAN est « Up ». Si le port WAN est inactif pour le routage, l'état du WAN est « Down ». **REMARQUE** : L'état « Down » signifie que la détection des réseaux est défaillante. Même si l'état du WAN est « Down » en raison d'une défaillance de détection des réseaux, les services WAN (tels que VPN SSL et l'administration à distance) peuvent toujours être connectés à l'exception du service d'accès VPN IPsec.
MAC Address	Adresse MAC du port WAN.
IP Address	Adresse IP du port WAN accessible à partir d'Internet
Subnet Mask/Prefix Length	Longueur du masque de sous-réseau ou du préfixe IPv6 pour le port WAN.
Gateway	Passerelle par défaut pour le port WAN.
DNS Server	Serveur DNS pour le port WAN.

Champ	Description
Physical Port	Port physique associé au port WAN.
Line Status	Indique si le câble est inséré dans le port WAN ou non. Si l'état de la ligne indique « Not Connected », le câble peut être desserré, débranché ou ne pas fonctionner correctement. **REMARQUE** : Si le champ Line Status indique « Not Connected », le champ Connection Status indique « Not Connected » et le champ WAN State indique « Down ».
Zone	Zone à laquelle le port WAN est attribué.
VLAN	
LAN MAC Address	Adresse MAC du LAN par défaut.
Name	Nom du VLAN.
VID	ID du VLAN.
IP Address	Adresse IP de sous-réseau du VLAN.
Subnet Mask/Prefix Length	Longueur du masque de sous-réseau ou du préfixe IPv6 du VLAN.
Physical Port	Ports physiques attribués au VLAN.
Zone	Zone à laquelle le VLAN est mappé.
DMZ	
Physical Port	Port physique attribué à la DMZ.
Zone	Zone à laquelle la DMZ est mappée.
Name	Nom de la DMZ.
VID	ID du VLAN.
IP Address	Adresse IP de sous-réseau du DMZ.
Subnet Mask/Prefix Length	Longueur du masque de sous-réseau ou du préfixe IPv6 de la DMZ.

Statistiques de trafic

Reportez-vous à la page Network Status > Traffic Statistics pour afficher les données de trafic pour les différentes interfaces. Cette page est automatiquement mise à jour toutes les 10 secondes. Cliquez sur **Refresh** pour actualiser manuellement les données. Cliquez sur **Reset** pour réinitialiser les valeurs de la table Ethernet à zéro.

Network Status > Traffic Statistics

Champ	Description
Ethernet	
Port	Nom du port physique.
Link Status	Indique si le port est connecté ou non.
Tx Packets	Nombre de paquets IP transmis par le port.
Rx Packets	Nombre de paquets IP reçus par le port.
Collisions	Nombre de collisions de signal qui se sont produites sur ce port. Une collision se produit lorsque le port tente d'envoyer des données en même temps qu'un port sur un autre routeur ou ordinateur connecté à ce port.
Tx Bytes/Sec	Nombre d'octets transmis par le port par seconde.
Rx Bytes/Sec	Nombre d'octets reçus par le port par seconde.
Uptime	Durée pendant laquelle le port a été actif. La disponibilité est remise à zéro lorsque l'Cisco ISA500 ou le port est redémarré.
WAN	
Name	Nom du port WAN.
Tx Packets	Nombre de paquets IP transmis par le port WAN.
Rx Packets	Nombre de paquets IP reçus par le port WAN.
Collisions	Nombre de collisions de signal qui se sont produites sur ce port WAN.
Tx Bytes/Sec	Nombre d'octets transmis par le port WAN par seconde.

Champ	Description
Rx Bytes/Sec	Nombre d'octets reçus par le port WAN par seconde.
Uptime	Durée pendant laquelle le port WAN a été actif. La disponibilité est remise à zéro lorsque l'Cisco ISA500 ou le port est relancé.
VLAN	
Name	Nom du VLAN.
Tx Packets	Nombre de paquets IP transmis par le VLAN.
Rx Packets	Nombre de paquets IP reçus par le VLAN.
Collisions	Nombre de collisions de signal qui se sont produites sur ce VLAN.
Tx Bytes/Sec	Nombre d'octets transmis par le VLAN par seconde.
Rx Bytes/Sec	Nombre d'octets reçus par le VLAN par seconde.
Uptime	Durée pendant laquelle le port LAN a été actif.
DMZ	
Name	Nom de la DMZ.
Tx Packets	Nombre de paquets IP transmis par la DMZ.
Rx Packets	Nombre de paquets IP reçus par la DMZ.
Collisions	Nombre de collisions de signal qui se sont produites sur la DMZ.
Tx Bytes/Sec	Nombre d'octets transmis par la DMZ par seconde.
Rx Bytes/Sec	Nombre d'octets reçus par la DMZ par seconde.
Uptime	Durée pendant laquelle le port DMZ a été actif.

Rapports d'utilisation

Reportez-vous à la page Network Status > Usage Reports pour afficher les 25 premiers sites Web le plus souvent consultés, les 25 premiers utilisateurs de la bande passante Internet par adresse IP et les 25 premiers services et applications qui consomment le plus de bande passante.

ÉTAPE 1 Cliquez sur **Network Status > Usage Reports**.

ÉTAPE 2 Dans la zone **Data Collection**, entrez les informations suivantes :

- **Enable Bandwidth Usage Report by IP Address** : cochez cette case pour activer le rapport d'utilisation de la bande passante trié pour commencer avec les 25 adresses IP qui consomment le plus de bande passante.
- **Enable Bandwidth Usage Report by Internet Service** : cochez cette case pour activer le rapport d'utilisation de la bande passante trié pour commencer avec les 25 services et applications qui consomment le plus de bande passante.
- **Enable Website Visits Report** : cochez cette case pour activer le rapport des sites Web consultés, trié pour commencer avec les 25 URL qui ont été le plus souvent visitées.

ÉTAPE 3 Cliquez sur **Save** pour enregistrer vos paramètres.

ÉTAPE 4 Dans la zone **Statistics Report**, choisissez le rapport que vous souhaitez afficher dans la liste déroulante **Type**.

- **Bandwidth Usage by IP Address** : ce rapport affiche l'adresse IP des 25 premiers utilisateurs qui consomment le plus de bande passante et la somme des octets reçus et transmis par adresse IP.
- **Bandwidth Usage by Internet Service** : ce rapport affiche les informations suivantes pour les 25 premiers services et applications qui consomment le plus de bande passante :
  - **Application** : nom d'un service ou d'une application connus ou le numéro de port d'un service ou d'une application inconnus. Si, par exemple, SMTP (6, 25) est affiché, SMTP correspond au nom du service, 6 au numéro du protocole et 25 au numéro de port du service.
  - **Sessions** : nombre total de sessions pour le service ou l'application.
  - **Total Bandwidth (TX/RX)** : nombre total d'octets reçus et transmis par le service ou l'application pendant la période.
  - **Average Bandwidth (TX/RX)** : nombre moyen d'octets reçus et transmis par seconde.

  Ce rapport est utile pour déterminer si les services et les applications utilisés sont appropriés pour votre organisation. Vous pouvez bloquer les services et les applications qui consomment une grande partie de la bande passante disponible. Pour plus d'informations sur le blocage des applications, reportez-vous à la section **Configuration du contrôle des applications, page 277**.

- **Website Visits** : ce rapport affiche les URL des 25 premiers sites Web le plus souvent consultés et le nombre de visites pour chaque site.

  Ce rapport contrôle uniquement les visites de sites Web via le port HTTP spécifié dans les paramètres avancés de filtrage de contenu du pare-feu ou de filtrage URL Web. Vous pouvez bloquer les sites Web si des sites Web inappropriés figurent dans ce rapport. Pour plus d'informations sur le blocage des sites Web, reportez-vous à la section **Configuration du filtrage du contenu pour contrôler l'accès à internet, page 247**, ou **Configuration du filtrage URL Web, page 298**.

ÉTAPE 5 Cliquez sur **Refresh** pour mettre à jour les données à l'écran ou sur **Reset** pour réinitialiser les valeurs à zéro.

- **Statistics Start Time** : affiche l'heure à laquelle le rapport commence à collecter les données.

  REMARQUE : Lorsqu'un rapport est activé ou désactivé, ou si vous cliquez sur **Reset**, la période d'échantillonnage pour le rapport est réinitialisée.

- **Last Refresh Time** : affiche l'heure de votre dernière opération d'actualisation.

Rapports de la bande passante WAN

Reportez-vous à la page Network Status > WAN Bandwidth pour afficher l'utilisation de la bande passante WAN en temps réel par heure au cours des dernières 24 heures. Cette page est automatiquement mise à jour toutes les 10 secondes.

ÉTAPE 1 Cliquez sur **Network Status > WAN Bandwidth**.

ÉTAPE 2 Pour activer les rapports de la bande passante WAN, cochez la case à côté de **Collect and Display WAN Bandwidth Statistics**.

ÉTAPE 3 Cliquez sur **Save** pour enregistrer vos paramètres.

ÉTAPE 4 Dans l'onglet **Primary WAN**, vous pouvez voir l'utilisation de la bande passante en temps réel par heure au cours des dernières 24 heures du port WAN principal.

ÉTAPE 5 Dans l'onglet **Secondary WAN**, vous pouvez voir l'utilisation de la bande passante en temps réel par heure au cours des dernières 24 heures du port WAN secondaire si un port WAN secondaire est configuré.

ÉTAPE 6 Cliquez sur **Refresh** pour actualiser manuellement les données.

ÉTAPE 7 Cliquez sur **Reset** pour réinitialiser les données d'utilisation de la bande passante WAN sur les ports du WAN principal et du WAN secondaire.

Table ARP

Le protocole de résolution d'adresse (ARP) est un protocole de réseau informatique qui détermine l'adresse de couche de liaison ou l'adresse matérielle d'un hôte du réseau lorsque seule l'adresse de la couche Internet (IP) ou de la couche réseau est connue.

Utilisez la page Network Status > ARP Table pour afficher les informations de toutes les entrées ARP. Cette page est automatiquement mise à jour toutes les 10 secondes. Cliquez sur **Refresh** pour actualiser manuellement les données.

Network Status > ARP Table

Champ	Description
IP Address	Adresse IP du périphérique.
Flag	Type d'indicateur du périphérique.
MAC Address	Adresse MAC du périphérique associé à l'adresse IP.
Device	Type d'interface du périphérique.

Liaisons DHCP

Utilisez la page Network Status > DHCP Bindings pour afficher les informations concernant l'attribution d'adresses DHCP. Cette page est automatiquement mise à jour toutes les 10 secondes. Cliquez sur **Refresh** pour actualiser manuellement les données.

Network Status > DHCP Bindings

Champ	Description
IP Address	Adresse IP attribuée à l'hôte ou au périphérique à distance.
MAC Address	Adresse MAC de l'hôte ou du périphérique à distance.

Champ	Description
Heure de début de location	Heure de début de location de l'adresse IP.
Lease End Time	Heure de fin de location de l'adresse IP.

État du STP

Reportez-vous à la page Network Status > STP Status pour afficher des informations sur les VLAN ayant le protocole STP (Protocole Spanning Tree) activé. STP est un protocole réseau de couche liaison qui permet une topologie sans boucle pour les LAN avec ponts. Aucune information n'est affichée pour les VLAN pour lesquels STP n'est pas activé.

En haut de la page, utilisez la liste **Check the STP status in this VLAN** pour choisir un VLAN.

Network Status > STP Status > Global Status

Champ	Description
Bridge ID	ID unique pour les autres équipements du réseau afin d'identifier ce périphérique.
Root Bridge ID	ID de pont du pont racine.
Root Port	ID de port du port racine. Le port racine est le port qui présente le coût de chemin le plus faible vers le pont racine. Le pont racine ne dispose pas de port racine.
Root Path Cost	Coût du chemin le plus court de l'appareil de sécurité vers le pont racine. La valeur 0 indique que cet appareil de sécurité est le pont racine.

Tableau d'état de l'interface

Champ	Description
Interfaces	Nom de l'interface.

Champ	Description
Port Role	Rôle attribué à ce port. ▪ Root port : port qui présente le coût de chemin le plus faible vers le pont racine. ▪ Designated port : port qui présente le coût de chemin le plus faible sur un segment LAN. Le segment LAN utilise le port désigné pour atteindre le pont racine. ▪ Blocked port : port qui n'est ni un port racine ni un port désigné.
Path Cost	Coût du chemin vers le pont racine via ce port.
Priority	Priorité du port.
Port State	État du port : ▪ Disabled : ce port est désactivé. Il ne transmettra ou ne recevra aucun trafic. ▪ Blocking : ce port est activé mais bloqué par le protocole STP. Il ne transmettra ou ne recevra aucun trafic. ▪ Listening : ce port reçoit et traite les BPDU (Bridge Protocol Data Units) STP (Spanning Tree Protocol), mais ne transmet aucun trafic de données. ▪ Learning : ce port commence à apprendre les adresses MAC à partir des paquets reçus. Il reçoit et traite également les BPDU STP, mais ne transmet pas de trafic de données. ▪ Forwarding : ce port transmet le trafic de données, traite les BPDU et apprend l'adresse MAC.
Designated Bridge ID	ID du pont désigné du segment LAN. Le pont désigné est utilisé par tous les autres équipements du segment LAN pour atteindre le pont racine.
Designated Port ID	ID du port désigné du segment LAN. Le port désigné est utilisé par tous les autres équipements du segment LAN pour atteindre le pont racine.
Designated Cost	Coût du chemin vers le pont désigné du segment LAN.

Voisinage CDP

Reportez-vous à la page Network Status > CDP Neighbors pour afficher des informations d'état sur les périphériques voisins qui ont été détectés par le protocole CDP (Cisco Discovery Protocol) (s'il est activé). Ces informations peuvent s'avérer utiles pour le dépannage.

Les informations de cette page sont automatiquement actualisées toutes les 15 secondes. Si le CDP est désactivé, un message apparaît en haut de la page et la liste est vide. Pour activer CDP, consultez la section **Détection CDP, page 409**.

Champ	Description
Device ID	Nom d'hôte de l'équipement voisin.
Local Port	Port sortant que l'appareil de sécurité utilise pour cette connexion.
Duration	Intervalle (en secondes) pendant lequel l'appareil de sécurité conserve les informations CDP d'un périphérique voisin.
Fonction	Type de périphérique voisin : R - routeur, T - pont transparent, B - pont de routage de source, S - commutateur, H - hôte, I - IGMP ou r - répéteur.
Platform	Numéro de modèle de l'équipement voisin.
Interface ID	Interface utilisée par le périphérique voisin utilise pour la connexion.
IP Address	Adresse IP de l'équipement voisin.
Duplex	Mode duplex de la connexion.
Voice VLAN	ID du VLAN voix de l'équipement voisin.

État sans fil (pour l'ISA550W et l'ISA570W uniquement)

Reportez-vous aux pages sur l'état sans fil pour afficher des informations sur votre réseau sans fil. Reportez-vous aux rubriques suivantes :

- **État du réseau sans fil, page 104**
- **Client Status, page 105**

État du réseau sans fil

Reportez-vous à la page Wireless Status pour consulter le total cumulé des statistiques sans fil appropriées pour tous les SSID. Cette page est automatiquement mise à jour toutes les 10 secondes. Cliquez sur **Refresh** pour actualiser manuellement les données.

Wireless Status > Wireless Status

Champ	Description
Wireless Status	
SSID Number	Numéro du SSID.
SSID Name	Nom du SSID.
MAC Address	Adresse MAC du SSID.
VLAN	VLAN auquel le SSID est mappé.
Client List	Nombre de stations clientes connectées au SSID.
Wireless Statistics	
Name	Nom du SSID.
Tx Packets	Nombre de paquets transmis sur le SSID.
Rx Packets	Nombre de paquets reçus sur le SSID.
Collisions	Nombre de collisions de paquets signalées au SSID.
Tx Bytes/Sec	Nombre d'octets d'informations transmis sur le SSID.
Rx Bytes/Sec	Nombre d'octets d'informations reçus sur le SSID.
Uptime	Durée pendant laquelle le SSID était actif.

Client Status

Reportez-vous à la page Wireless Status > Client Status pour consulter les informations relatives à toutes les stations clientes qui sont déjà connectées à chaque SSID. L'adresse MAC et l'adresse IP sont affichées pour toutes les stations clientes connectées pour chaque SSID. Cette page est automatiquement mise à jour toutes les 10 secondes. Cliquez sur **Refresh** pour actualiser manuellement les données.

NAT Status

Reportez-vous à la page NAT Status pour consulter les informations relatives à toutes les règles NAT.

État du NAT

Champ	Description
Original Source Address	Adresse IP source d'origine dans le paquet.
Original Destination Address	Adresse IP de destination d'origine dans le paquet.
Source Port	Interface source d'où provient le trafic.
Destination Port	Interface de destination où le trafic s'achemine.
Translated Destination Address	Adresse IP vers laquelle l'adresse de destination d'origine spécifiée est traduite.
Translated Source Address	Adresse IP vers laquelle l'adresse source d'origine spécifiée est traduite.
Translated Destination Port	Interface vers laquelle l'interface de destination spécifiée est traduite.
Translated Source Port	Interface vers laquelle l'interface source spécifiée est traduite.
Tx Packets	Nombre de paquets transmis.
Rx Packets	Nombre de paquets reçus.

Champ	Description
Tx Bytes/Sec	Volume en octets du trafic transmis.
Rx Bytes/Sec	Volume en octets du trafic reçu.

État du VPN

Reportez-vous aux pages sur l'état du VPN pour consulter les informations relatives à toutes les sessions VPN. Reportez-vous aux rubriques suivantes :

- **IPsec VPN Status, page 106**
- **SSL VPN Status, page 108**

IPsec VPN Status

Reportez-vous à la page VPN Status > IPsec VPN Status pour consulter les informations relatives à toutes les sessions VPN IPsec. Cette page est automatiquement mise à jour toutes les 10 secondes. Cliquez sur **Refresh** pour actualiser manuellement les données.

VPN Status > IPsec VPN Status

Champ	Description
Sessions actives	
	Pour mettre fin manuellement à une session VPN IPsec, cliquez sur l'icône de **déconnexion** dans la colonne **Connect**. Pour mettre fin manuellement à plusieurs sessions VPN IPsec actives, sélectionnez-les et cliquez sur le bouton **Disconnect**. Si une session VPN IPsec est terminée, vous pouvez établir manuellement la connexion VPN en cliquant sur l'icône de **connexion** dans la colonne **Connect**.
Name	Stratégie VPN utilisée pour une session VPN IPsec.
Status	État de connexion d'une session VPN IPsec.
VPN Type	Type de connexion VPN pour une session VPN IPsec, tel que Site-to-Site, IPsec Remote Access ou Teleworker VPN Client.

Champ	Description
Interface WAN	Port WAN utilisé pour une session VPN IPsec.
Remote Gateway	Adresse IP de l'homologue distant. **REMARQUE** : Pour une session VPN de site à site, ce champ indique l'adresse IP de la passerelle distante. Pour une session VPN IPsec entre le client VPN pour télétravailleurs et un serveur VPN IPsec distant, ce champ indique l'adresse IP du serveur VPN IPsec. Pour une session VPN IPsec entre le serveur VPN IPsec et un client VPN distant, ce champ indique l'adresse IP du client VPN distant.
Local Network	Adresse IP de sous-réseau et masque réseau du réseau local.
Remote Network	Adresse IP de sous-réseau et masque réseau du réseau distant.
Statistics	
Name	Stratégie VPN utilisée pour une session VPN IPsec.
VPN Type	Type de connexion VPN pour une session VPN IPsec
WAN Interface	Port WAN utilisé pour une session VPN IPsec.
Remote Gateway	Adresse IP de l'homologue distant.
Local Network	Adresse IP de sous-réseau et masque réseau du réseau local.
Remote Network	Adresse IP de sous-réseau et masque réseau du réseau distant.
Tx Bytes	Volume du trafic en kilo-octets transmis à partir du tunnel VPN.
Rx Bytes	Volume du trafic en kilo-octets reçu à partir du tunnel VPN.
Tx Packets	Nombre de paquets IP transmis à partir du tunnel VPN.
Rx Packets	Nombre de paquets IP reçus à partir du tunnel VPN

Champ	Description
Teleworker VPN Client	
Si la fonctionnalité de client VPN pour télétravailleurs (Teleworker VPN Client) est activée et que l'Cisco ISA500 agit en tant que client matériel VPN Cisco, les informations ci-dessous sont affichées.	
Status	Indique si la fonctionnalité Teleworker VPN Client est activée ou désactivée.
Primary DNS	Adresse IP du serveur DNS principal.
Secondary DNS	Adresse IP du serveur DNS secondaire.
Primary WINS	Adresse IP du serveur WINS principal.
Secondary WINS	Adresse IP du serveur WINS secondaire.
Default Domain	Nom de domaine par défaut.
Split Tunnel	Adresse IP et masque réseau pour les sous-réseaux fractionnés spécifiés
Split DNS	Adresse IP ou nom de domaine pour le DNS fractionné spécifié
Backup Server 1/2/3	Adresse IP ou nom d'hôte pour les serveurs de sauvegarde spécifiés.

SSL VPN Status

Reportez-vous à la page VPN Status > SSL VPN Status pour consulter les informations relatives à toutes les sessions VPN SSL actives. Cette page est automatiquement mise à jour toutes les 10 secondes. Cliquez sur **Refresh** pour actualiser manuellement les données.

VPN Status > SSL VPN Status

Champ	Description
Sessions actives	
Pour mettre fin manuellement à une session VPN SSL active, cliquez sur l'icône de **déconnexion** dans la colonne **Configure**. Pour mettre fin manuellement à plusieurs sessions VPN SSL actives, sélectionnez-les et cliquez sur le bouton **Disconnect**.	
Session ID	ID de la session VPN SSL.
User Name	Nom de l'utilisateur VPN SSL connecté.
Client IP (Actual)	Adresse IP réelle utilisée par le client VPN SSL
Client IP (VPN)	Adresse IP virtuelle du client VPN SSL attribuée par la passerelle VPN SSL
Connect Time	Temps écoulé depuis que l'utilisateur VPN SSL a établi la connexion pour la première fois.
Statistiques VPN SSL	
Les informations statistiques globales sont affichées dans la zone **Global Status**. Pour effacer les informations statistiques globales, cliquez sur **Clear**.	
Active Users	Nombre total d'utilisateurs VPN SSL connectés
In CSTP Frames	Nombre de trames CSTP reçues de tous les clients.
In CSTP Bytes	Nombre total d'octets dans les trames CSTP reçues de tous les clients
In CSTP Data	Nombre de trames de données CSTP reçues de tous les clients
In CSTP Control	Nombre de trames de contrôle CSTP reçues de tous les clients.
Out CSTP Frames	Nombre de trames CSTP envoyées à tous les clients.
Out CSTP Bytes	Nombre total d'octets dans les trames CSTP envoyées à tous les clients
Out CSTP Data	Nombre de trames de données CSTP envoyées à tous les clients.
Out CSTP Control	Nombre de trames de contrôle CSTP envoyées à tous les clients.

Champ	Description
Dans le tableau **Session Statistics**, les informations répertoriées ci-dessous sont affichées pour chaque session VPN SSL. Pour effacer les informations statistiques pour une session VPN SSL simple, cliquez sur **Clear** dans la colonne **Configure**. Pour effacer les informations statistiques pour plusieurs sessions VPN SSL, sélectionnez-les et cliquez sur **-Clear**.	
Session ID	ID de la session VPN SSL.
In CSTP Frames	Nombre de trames CSTP reçues du client.
In CSTP Bytes	Nombre total d'octets dans les trames CSTP reçues du client.
In CSTP Data	Nombre de trames de données CSTP reçues du client.
In CSTP Control	Nombre de trames de contrôle CSTP reçues du client.
Out CSTP Frames	Nombre de trames CSTP envoyées au client
Out CSTP Bytes	Nombre total d'octets dans les trames CSTP envoyées au client.
Out CSTP Data	Nombre de trames de données CSTP envoyées au client.
Out CSTP Control	Nombre de trames de contrôle CSTP envoyées au client

REMARQUE CSTP est un protocole propriétaire Cisco pour la tunnellisation VPN SSL. « In » indique que le paquet provient du client. « Out » indique que le paquet est envoyé au client. Le client est le PC exécutant le logiciel client à mobilité sécurisé Cisco AnyConnect qui se connecte à l'Cisco ISA500 exécutant le serveur VPN SSL. Une trame CSTP est un paquet transportant des informations de protocole CSTP. Il existe deux principaux types de trames, les trames de contrôle et les trames de données. Les trames de contrôle implémentent des fonctions de contrôle au sein du protocole. Les trames de données transportent les données client, telles que la charge utile tunnellisée.

Active User Sessions

Reportez-vous à la page Active User Sessions pour consulter les informations relatives à toutes les sessions utilisateur actives qui sont actuellement connectées à l'Cisco ISA500. Cette page est automatiquement mise à jour toutes les 10 secondes. Cliquez sur **Refresh** pour actualiser manuellement les données. Cliquez sur l'icône de **déconnexion** pour mettre fin à une session utilisateur Web ou à une session utilisateur VPN.

Active User Sessions

Champ	Description
User Name	Nom de l'utilisateur connecté.
IP Address	Adresse IP d'hôte à partir de laquelle l'utilisateur a accédé à l'Cisco ISA500.
Login Method	Méthode utilisée par l'utilisateur pour se connecter à l'Cisco ISA500, telle que le Web, VPN SSL, l'accès à distance IPsec ou le portail captif.
Session Time	Heure à laquelle l'utilisateur s'est connecté à l'Cisco ISA500.

Security Services Reports

Reportez-vous aux pages sur les rapports de services de sécurité pour consulter les rapports relatifs à tous les services de sécurité. Cette page est automatiquement mise à jour toutes les 10 secondes. Cliquez sur **Refresh** pour actualiser manuellement les données. Reportez-vous aux rubriques suivantes :

- **Rapport de sécurité Web, page 112**
- **Rapport antivirus, page 113**
- **Email Security Report, page 114**
- **Rapport de réputation du réseau, page 115**
- **IPS Report, page 116**
- **Application Control Report, page 117**

REMARQUE Les rapports de services de sécurité sont actifs uniquement une fois que la licence de sécurité a été validée. Avant de choisir un rapport de service de sécurité à afficher, vérifiez que le service de sécurité correspondant est activé.

Rapport de sécurité Web

Ce rapport indique le nombre de demandes d'accès Web consignées et le nombre de sites Web bloqués par le filtrage URL Web, le filtrage par réputation Web, ou les deux.

ÉTAPE 1 Dans l'onglet **Web Security**, indiquez les informations suivantes :

- **Enable** : cochez cette case pour activer le rapport de sécurité Web ou décochez-la pour la désactiver.
- **Blocked Requests** : cochez cette case pour afficher le nombre de sites Web bloqués par le filtrage URL Web et/ou le filtrage par réputation Web dans le graphique. Pour obtenir plus d'informations sur les requêtes bloquées, cliquez sur la barre rouge dans le graphique. Une fenêtre contextuelle affiche les informations suivantes pour chaque requête bloquée : la date et l'heure, l'adresse IP et l'adresse MAC de l'hôte qui a émis la demande, le site Web, l'URL bloquée, le filtre qui a bloqué la requête, et le nombre de fois que la connexion a été bloquée.
- **Processed Requests** : cochez cette case pour afficher le nombre de demandes d'accès Web consignées par le filtrage URL Web et/ou le filtrage par réputation Web dans le graphique.

Champ	Description
System Date	Heure système actuelle.
Total Since Activated	Nombre total de demandes d'accès Web traitées et nombre total de sites Web bloqués depuis l'activation des services de filtrage URL Web et de filtrage par réputation Web.
Total Last 7 Days	Nombre total de demandes d'accès Web traitées et nombre total de sites Web bloqués au cours des sept derniers jours.
Total Today	Nombre total de demandes d'accès Web traitées et nombre total de sites Web bloqués en une journée.

Champ	Description
Graph	Nombre total de demandes d'accès Web traitées et nombre total de sites Web bloqués par jour au cours des sept derniers jours.

Rapport antivirus

Ce rapport indique le nombre de fichiers vérifiés et le nombre de virus détectés par le service antivirus.

ÉTAPE 1 Dans l'onglet **Anti-Virus**, indiquez les informations suivantes :

- **Enable** : cochez cette case pour activer le rapport antivirus ou décochez-la pour le désactiver.
- **Detected Requests** : cochez cette case pour afficher le nombre de virus détectés par le service antivirus dans le graphique. Pour afficher des informations supplémentaires sur les requêtes détectées, cliquez sur la barre rouge dans le graphique. Une fenêtre contextuelle affiche les informations suivantes pour chaque requête détectée : la date et l'heure, l'adresse IP et l'adresse MAC de la source et de la destination, le protocole utilisé pour la connexion, la mesure prise et le nombre de fois qu'un virus a été trouvé.
- **Processed Requests** : cochez cette case pour afficher le nombre de fichiers vérifiés par le service antivirus dans le graphique.

ÉTAPE 2 Cliquez sur **Save** pour enregistrer vos paramètres.

Champ	Description
System Date	Heure système actuelle.
Total Since Activated	Nombre total de fichiers vérifiés et nombre total de virus détectés depuis l'activation du service antivirus.
Total Last 7 Days	Nombre total de fichiers vérifiés et nombre total de virus détectés au cours des sept derniers jours.

Champ	Description
Total Today	Nombre total de fichiers vérifiés et nombre total de virus détectés en une journée.
Graph	Nombre total de fichiers vérifiés et nombre total de virus détectés par jour au cours des sept derniers jours.

Email Security Report

Ce rapport indique le nombre de courriels vérifiés et le nombre de courriels indésirables ou suspectés d'être indésirables détectés par le service de filtre de courrier indésirable.

ÉTAPE 1 Dans l'onglet **Email Security**, indiquez les informations suivantes :

- **Enable** : cochez cette case pour activer le rapport de sécurité de la messagerie ou décochez-la pour le désactiver.
- **Blocked Requests** : cochez cette case pour afficher dans le graphique le nombre de courriels indésirables ou suspectés d'être indésirables, détectés par le service de filtre de courrier indésirable.
- **Processed Requests** : cochez cette case pour afficher dans le graphique le nombre de courriels vérifiés par le service de filtre de courrier indésirable.

ÉTAPE 2 Cliquez sur **Save** pour enregistrer vos paramètres.

Champ	Description
System Date	Heure système actuelle.
Total Since Activated	Nombre total de courriels vérifiés et nombre total de courriels indésirables ou suspectés d'être indésirables détectés par jour depuis l'activation du service de filtre de courrier indésirable.
Total Last 7 Days	Nombre total de courriels vérifiés et nombre total de courriels indésirables ou suspectés d'être indésirables détectés au cours des sept derniers jours.

Champ	Description
Total Today	Nombre total de courriels vérifiés et nombre total de courriels indésirables ou suspectés d'être indésirables détectés au cours des sept derniers jours.
Graph	Nombre total de courriels vérifiés et nombre total de courriels indésirables ou suspectés d'être indésirables détectés au cours des sept derniers jours.

Rapport de réputation du réseau

Ce rapport indique le nombre de paquets vérifiés et le nombre de paquets bloqués par le service de réputation de réseau.

ÉTAPE 1 Dans l'onglet **Network Reputation**, indiquez les informations suivantes :

- **Enable** : cochez cette case pour activer le rapport de réputation de réseau ou décochez-la pour le désactiver.
- **Blocked Requests** : cochez cette case pour afficher dans le graphique le nombre de paquets bloqués par le service de réputation de réseau.
- **Processed Requests** : cochez cette case pour afficher dans le graphique le nombre de paquets vérifiés par le service de réputation de réseau.

ÉTAPE 2 Cliquez sur **Save** pour enregistrer vos paramètres.

Champ	Description
System Date	Heure système actuelle.
Total Since Activated	Nombre total de paquets vérifiés et nombre total de paquets bloqués depuis l'activation du service de réputation de réseau.
Total Last 7 Days	Nombre total de paquets vérifiés et nombre total de paquets bloqués au cours des sept derniers jours.
Total Today	Nombre total de paquets vérifiés et nombre total de paquets bloqués en une journée.

Champ	Description
Graph	Nombre total de paquets vérifiés et nombre total de paquets bloqués par jour au cours des sept derniers jours.

IPS Report

Ce rapport indique le nombre de paquets détectés et le nombre de paquets abandonnés par le service IPS de prévention des intrusions.

ÉTAPE 1 Dans l'onglet **IPS**, indiquez les informations suivantes :

- **Enable** : cochez cette case pour activer le rapport IPS ou décochez-la pour le désactiver.
- **Blocked Requests** : cochez cette case pour afficher dans le graphique le nombre de paquets abandonnés par le service IPS. Pour afficher des informations supplémentaires sur les requêtes bloquées, cliquez sur la barre rouge dans le graphique. Une fenêtre contextuelle affiche les informations suivantes pour chaque requête bloquée : la date et l'heure, l'adresse IP et l'adresse MAC de la source et de la destination, la mesure prise et le nombre de fois que cet événement a été détecté.
- **Processed Requests** : cochez cette case pour afficher dans le graphique le nombre de paquets détectés par le service IPS.

ÉTAPE 2 Cliquez sur **Save** pour enregistrer vos paramètres.

Champ	Description
System Date	Heure système actuelle.
Total Since Activated	Nombre total de paquets détectés et nombre total de paquets abandonnés depuis l'activation du service IPS.
Total Last 7 Days	Nombre total de paquets détectés et nombre total de paquets abandonnés au cours des sept derniers jours.

Champ	Description
Total Today	Nombre total de paquets détectés et nombre total de paquets abandonnés en une journée.
Graph	Nombre total de paquets détectés et nombre total de paquets abandonnés par jour au cours des sept derniers jours.

Application Control Report

Ce rapport indique le nombre de paquets détectés et le nombre de paquets bloqués par le service de contrôle des applications.

ÉTAPE 1 Dans l'onglet **Application Control**, indiquez les informations suivantes :

- **Enable** : cochez cette case pour activer le rapport de contrôle des applications ou décochez-la pour le désactiver.
- **Blocked Requests** : cochez cette case pour afficher dans le graphique le nombre de paquets abandonnés par le service de contrôle des applications. Pour afficher des informations supplémentaires sur les requêtes bloquées, cliquez sur la barre rouge dans le graphique. Une fenêtre contextuelle affiche les informations suivantes pour chaque requête bloquée : la date et l'heure, l'adresse IP et l'adresse MAC de l'hôte qui a émis la demande, l'application bloquée et le nombre de fois que l'application a été bloquée.
- **Processed Requests** : cochez cette case pour afficher dans le graphique le nombre de paquets détectés par le service de contrôle des applications.

ÉTAPE 2 Cliquez sur **Save** pour enregistrer vos paramètres.

Champ	Description
System Date	Heure système actuelle.
Total Since Activated	Nombre total de paquets détectés et nombre total de paquets bloqués depuis l'activation du service de contrôle des applications.
Total Last 7 Days	Nombre total de paquets détectés et nombre total de paquets bloqués au cours des sept derniers jours.

Champ	Description
Total Today	Nombre total de paquets détectés et nombre total de paquets bloqués en une journée.
Graph	Nombre total de paquets détectés et nombre total de paquets bloqués par jour au cours des sept derniers jours.

System Status

Reportez-vous aux pages d'état du système pour afficher des informations pour tous les processus en cours d'exécution, l'utilisation du processeur et la consommation de la mémoire du système. Reportez-vous aux rubriques suivantes :

- **Processus, page 118**
- **Utilisation des ressources, page 119**

Processus

Reportez-vous à la page System Status > Processes pour consulter les informations relatives à tous les processus en cours. Cette page est automatiquement mise à jour toutes les 10 secondes. Cliquez sur **Refresh** pour actualiser manuellement les données.

System Status > Processes

Champ	Description
Name	Nom du processus en cours d'exécution sur l'Cisco ISA500.
Description	Brève description du processus en cours d'exécution.
Protocol	Protocole utilisé par le connecteur.
Port	Numéro de port de l'extrémité locale du connecteur.
Local Address	Adresse IP de l'extrémité locale du connecteur.
Foreign Address	Adresse IP de l'extrémité distante du connecteur.

Utilisation des ressources

Reportez-vous à la page System Status > Resource Utilization pour consulter les informations relatives à l'utilisation de la mémoire et du processeur du système.

System Status > Resource Utilization

Champ	Description
CPU Utilization	
CPU Usage by User	Pourcentage de la ressource de CPU actuellement utilisée par les processus d'espace utilisateur.
CPU Usage by Kernel	Pourcentage de la ressource de CPU actuellement utilisée par les processus d'espace noyau.
CPU Idle	Pourcentage de la ressource de CPU inactive à l'heure actuelle.
CPU Waiting for I/O	Pourcentage de la ressource de CPU actuellement en attente d'E/S.
Memory Utilization	
Total Memory	Espace mémoire total disponible sur l'Cisco ISA500
Memory Used	Espace mémoire total actuellement utilisé par les processus
Free Memory	Espace mémoire total actuellement non utilisé par les processus
Cached Memory	Espace mémoire total actuellement utilisé comme cache.
Buffer Memory	Espace mémoire total actuellement utilisé en tant que tampon.

4

Mise en réseau

Utilisation du module de mise en réseau pour configurer votre connexion internet, VLAN, DMZ, zones, routage, qualité de service (QoS) et fonctionnalités associées. Il comprend les sections suivantes :

- **Affichage de l'état du réseau, page 121**
- **Configuration du routage IPv4 ou IPv6, page 121**
- **Gestion des ports, page 122**
- **Configuration du WAN, page 128**
- **Configuration d'un VLAN, page 144**
- **Configuration de la DMZ, page 147**
- **Configuration des zones, page 152**
- **Configuration des IP DHCP réservés, page 155**
- **Configuration du routage, page 156**
- **Configuration de la qualité de service, page 161**
- **Configuration IGMP, page 179**
- **Configuration VRRP, page 180**
- **Gestion d'adresse, page 182**
- **Gestion des services, page 184**

Pour accéder aux pages relatives à la mise en réseau, cliquez sur **Networking** dans le volet de navigation de gauche.

Affichage de l'état du réseau

Utilisez les pages Networking > Network Status pour afficher les statistiques de trafic, les rapports d'utilisation, les rapports de la bande passante WAN, toutes les d'entrées ARP (Address Resolution Protocol, Protocole de résolution d'adresse) et l'affectation d'adresse DHCP. Pour obtenir une description de ces rapports d'état, voir **État du réseau, page 93**.

Configuration du routage IPv4 ou IPv6

Utilisez la page Networking > IPv4 or IPv6 Routing pour choisir le mode de routage IP pour votre réseau. Le protocole Internet version 6 (IPv6) est un nouveau protocole IP conçu pour remplacer IPv4, le protocole Internet largement déployé et utilisé de façon intensive dans le monde entier. IPv6 quadruple le nombre de bits des adresses réseau et passe de 32 bits (dans IPv4) à 128 bits, permettant ainsi d'accroître l'espace d'adressage de façon exponentielle. Vous pouvez configurer l'Cisco ISA500 pour prendre en charge l'adressage IPv6 sur le WAN, le LAN et la DMZ.

ATTENTION ISA500 prend actuellement en charge des fonctionnalités IPv6 limitées. ISA500 ne prend pas en charge le pare-feu, VPN ni d'autres services de sécurité pour IPv6 dans ce microprogramme. Nous recommandons d'activer IPv6 pour le laboratoire de test uniquement avec ce microprogramme. Pour les mises à jour possibles, s'il vous plaît voir avenir microprogramme et notes de version.

ÉTAPE 1 Cliquez sur **IPv4 or IPv6** pour activer l'adressage IPv4 et IPv6 ou sur **IPv4 only** pour activer uniquement l'adressage IPv4. Par défaut, seul l'adressage IPv4 est pris en charge.

ÉTAPE 2 Cliquez sur **Save** pour enregistrer vos paramètres.

Gestion des ports

Utilisez les pages Networking > Ports pour configurer les ports physiques, la mise en miroir des ports et les paramètres de contrôle d'accès basés sur les ports. Reportez-vous aux rubriques suivantes :

- **Affichage de l'état des interfaces physiques, page 122**
- **Configuration des ports physiques, page 123**
- **Configuration de la mise en miroir des ports, page 125**
- **Configuration du contrôle d'accès basé sur les ports (802.1x), page 125**

Affichage de l'état des interfaces physiques

Utilisez la page Networking > Ports > Physical Interface pour afficher des informations sur tous les ports physiques sur l'appliance de sécurité.

Pour tous les modèles, les informations suivantes s'affichent :

- **Name** : nom du port physique.
- **Enable** : indique si le port physique est activé ou désactivé.
- **Port Type** : type de port physique, par exemple WAN, LAN ou DMZ.
- **Mode** : mode d'accès du port physique. Un port WAN ou DMZ est toujours défini en mode d'accès. Un port LAN peut être défini en mode d'accès ou de liaison.
- **VLAN** : VLAN auxquels le port physique est mappé.
- **PVID** : ID de VLAN du port (PVID) utilisé pour transférer ou filtrer les paquets non marqués arrivant sur le port. Le PVID d'un port de liaison est fixé sur le DEFAULT VLAN (1).
- **Speed/Duplex** : mode duplex (paramètre de vitesse et duplex) du port physique.
- **Link Status** : indique si le port physique est connecté ou déconnecté.

Pour ISA570W et ISA550W, la zone Wireless Interfaces affiche les informations suivantes pour tous les SSID :

- **SSID Name** : nom du SSID.
- **VLAN** : VLAN auquel le SSID est mappé.
- **Client Associated** : nombre de stations clientes connectées au SSID.

REMARQUE : Pour configurer votre réseau sans fil, accédez aux pages Wireless. Voir **Sans fil (pour ISA550W et ISA570W uniquement), page 190**.

ÉTAPE 1 Procédez comme suit :

- Cochez la case de la colonne **Enable** pour activer un port physique, ou décochez-la pour le désactiver.
- Pour modifier les paramètres d'un port physique, cliquez sur l'icône **Edit** (crayon). Voir **Configuration des ports physiques, page 123**.

ÉTAPE 2 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration des ports physiques

Lorsque vous cliquez sur l'icône Edit (crayon) dans la page Networking > Ports > Physical Interface, utilisez la page Ethernet Configuration - Add/Edit pour activer ou désactiver le port physique sélectionné, attribuez-la à un ou plusieurs VLAN, et configurez-le mode duplex.

ÉTAPE 1 Entrez les informations suivantes :

- **Name** : nom du port physique.
- **Port Type** : type de port physique, par exemple WAN, LAN ou DMZ.
- **Mode** : choisissez le mode **Access** ou **Trunk** pour un port LAN, ou **Access** pour un port WAN ou DMZ. Par défaut, tous les ports sont définis en mode d'accès.
  - **Access** : toutes les données en direction et en provenance du port d'accès sont non marquées. Le mode d'accès est recommandé si le port est connecté à un seul périphérique d'utilisateur final non sensible au VLAN.
  - **Trunk** : toutes les données en direction et en provenance du port de liaison sont marquées. Les données non marquées arrivant dans le port ne sont pas transférées, à l'exception du DEFAULT VLAN, qui est non marqué. Le mode de liaison est recommandé si le port est connecté à un commutateur ou à un routeur sensible au VLAN.
- **Port** : cliquez sur **On** pour activer le port, ou sur **Off** pour le désactiver. Par défaut, tous les ports sont activés.

- **VLAN** : vous pouvez affecter le port physique aux VLAN.
  - Pour affecter le port à un VLAN, choisissez un VLAN existant dans la liste de VLAN disponibles et cliquez sur les flèches droites. Les VLAN associés figurent dans la liste des VLAN.
  - Pour libérer le port d'un VLAN, choisissez un VLAN de la liste de VLAN et cliquez sur les flèches gauches.

  REMARQUE : Un port LAN peut être affecté à plusieurs VLAN, mais un port LAN d'accès ne peut être affecté qu'à un VLAN. Un port DMZ doit être affecté à un réseau DMZ.

  REMARQUE : Vous pouvez cliquer sur le lien **Create VLAN** pour créer de nouveaux VLAN. Pour plus d'informations sur la configuration du VLAN, consultez la section **Configuration d'un VLAN, page 144**.
- **Flow Control** : cliquez sur **On** pour contrôler le flux sur le port ou sur **Off** pour le désactiver.

  REMARQUE : le contrôle de flux Gigabit Ethernet est fourni par un mécanisme de trame PAUSE. Un port encombré envoie une trame XON PAUSE, qui entraîne l'arrêt de l'envoi de données par le port source jusqu'à ce qu'une trame XOFF PAUSE soit reçue. Pour que ce mécanisme fonctionne, le contrôle de flux doit être activé sur le port source et le port de destination. Même lorsque le contrôle de flux est activé, des abandons de paquets peuvent se produire si le port de réception manque de tampons.
- **Speed** : choisissez l'une des options suivantes : AUTO, 10M, 100M et 1000M. L'option par défaut est AUTO pour tous les ports. L'option AUTO permet au système et au réseau de déterminer la vitesse optimale du port.
- **Duplex** : choisissez Half ou Full en fonction du paramètre de vitesse du port. La valeur par défaut est Full Duplex pour tous les ports.
  - **Full** : le port prend en charge les transmissions entre le périphérique et le client dans les deux sens simultanément.
  - **Half** : le port prend en charge les transmissions entre le périphérique et le client dans un seul sens à la fois.

ÉTAPE 2 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 3 Dans la page Networking > Ports > Physical Interface, cliquez sur **Save** pour appliquer vos paramètres.

Configuration de la mise en miroir des ports

Utilisez la page Networking > Ports > Port Mirroring pour autoriser que le trafic sur un port soit visible sur d'autres ports. Cette fonctionnalité est utile pour le débogage ou la surveillance du trafic.

REMARQUE Le port WAN dédié (GE1) ne peut pas être défini comme port de destination ou port surveillé.

ÉTAPE 1 Cliquez sur **On** pour activer la mise en miroir des ports ou sur **Off** pour la désactiver.

ÉTAPE 2 Si vous activez la mise en miroir des ports, entrez les informations suivantes :

- **TX Destination** : choisissez le port qui surveille le trafic transmis pour d'autres ports.
- **TX Monitored Ports** : sélectionnez les ports surveillés. Le port que vous avez défini comme port de destination du trafic transmis ne peut pas être sélectionné comme port surveillé.
- **RX Destination** : choisissez le port qui surveille le trafic reçu pour d'autres ports.
- **RX Monitored Ports** : sélectionnez les ports surveillés. Le port que vous avez défini comme port RX Destination ne peut pas être sélectionné comme port surveillé.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration du contrôle d'accès basé sur les ports (802.1x)

Utilisez la page Networking > Ports > Port-Based Access Control pour configurer l'authentification basée sur le port IEEE 802.1x, qui empêche les périphériques non-autorisés (clients compatibles avec la norme 802.1x) d'accéder au réseau.

La norme IEEE 802.1x définit un protocole de contrôle d'accès et d'authentification basé sur un serveur client qui empêchent les périphériques non autorisés de se connecter à un VLAN via des ports d'accès public. Le serveur d'authentification authentifie chaque client demandeur (sous Windows 2000, XP, Vista, Windows 7 et Mac OS) connecté à un port avant de mettre à disposition les services proposés par l'Cisco ISA500 ou le VLAN.

Une fois le client authentifié, le contrôle d'accès 802.1x autorise uniquement le protocole EAP (Extensible Authentication Protocol) sur le trafic LAN (EAPOL) via le port auquel le client est connecté. Une fois l'authentification réussie, le trafic normal peut passer par le port.

Cette fonctionnalité simplifie la gestion de la sécurité en vous permettant de contrôler l'accès à partir d'une base de données principale d'un serveur unique. Vous pouvez néanmoins utiliser jusqu'à trois serveurs RADIUS pour fournir des sauvegardes en cas de problème d'accès au serveur principal. L'utilisateur peut également entrer la même paire nom d'utilisateur/mot de passe RADIUS autorisée pour l'authentification, quel que soit le commutateur correspondant au point d'accès dans le VLAN.

ÉTAPE 1 Dans la zone **RADIUS Settings**, spécifiez les serveurs RADIUS pour l'authentification.

L'Cisco ISA500 prédéfinit trois groupes RADIUS. Choisissez un groupe RADIUS prédéfini dans la liste déroulante **RADIUS Index** pour authentifier les utilisateurs sur les clients compatibles avec la norme 802.1x. Les paramètres du serveur RADIUS du groupe sélectionné s'affichent. Vous pouvez modifier les paramètres du serveur RADIUS, mais les paramètres que vous spécifiez remplaceront les paramètres par défaut du groupe sélectionné. Pour plus d'informations sur la configuration des serveurs RADIUS, voir **Configuration de serveurs RADIUS, page 374**.

ÉTAPE 2 Dans la zone **Port-Based Access Control Settings**, effectuez les actions suivantes :

- **Access Control** : cochez cette case pour activer la fonctionnalité de contrôle d'accès 802.1x ou décochez-la pour la désactiver. Cette fonctionnalité n'est pas disponible pour les ports de liaison.
- **Guest Authentication** : une fois que vous avez activé la fonctionnalité de contrôle d'accès 802.1x, cochez cette case pour activer la fonctionnalité Guest Authentication ou décochez-la pour la désactiver.
- **Authorization Mode** : spécifiez le mode d'autorisation pour chaque port physique en cliquant sur l'une des icônes suivantes :
  - **Forced Authorized** : désactiver la fonctionnalité de contrôle d'accès 802.1x et passer le port à l'état autorisé sans qu'aucun échange d'authentification ne soit requis. Le port transmet et reçoit le trafic normal sans l'authentification 802.1x du client.
  - **Forced Unauthorized** : passer le port à l'état non autorisé, en ignorant toutes les tentatives d'authentification effectuées par le client. L'Cisco ISA500 n'est pas en mesure de fournir des services d'authentification au client via le port.

- **Auto :** activer la fonctionnalité de contrôle d'accès 802.1x et entraîner le démarrage du port à l'état non autorisé, en autorisant uniquement l'envoi et la réception de trames EAPOL via le port. Le processus d'authentification commence lorsque l'état des liaisons du port passe de bas en haut, ou lorsqu'une trame de départ EAPOL est reçue. L'Cisco ISA500 demande l'identité du client et commence par relayer les messages d'authentification entre le client et le serveur d'authentification. Chaque client qui tente d'accéder au réseau est identifié de façon unique par l'Cisco ISA500 à l'aide de l'adresse MAC du client.

ÉTAPE 3 Pour spécifier les VLAN authentifiés sur un port physique, cliquez sur l'icône **Edit** (crayon).

ÉTAPE 4 Entrez les informations suivantes dans la page Port-Base Access Control - Edit :

- **Access Control** : cochez cette case pour activer la fonctionnalité de contrôle d'accès 802.1x.
- **Authenticated VLAN** : si vous activez la fonctionnalité de contrôle d'accès 802.1x, choisissez le VLAN authentifié auquel ce port est affecté. Les utilisateurs qui se sont authentifiés peuvent accéder au VLAN authentifié via le port. En cas d'échec d'authentification, bloquez l'accès via le port.
- **Guest Authenticated** : si vous activez la fonctionnalité de contrôle d'accès 802.1x, cochez cette case pour activer la fonctionnalité Guest Authentication.
- **Authenticated VLAN** : si vous activez la fonctionnalité Guest Authentication, choisissez le VLAN invité à associer au port. En cas d'échec d'authentification, le port est affecté au VLAN invité sélectionné au lieu de s'arrêter. Pour les clients non compatibles avec la norme 802.1x, le port est également affecté au VLAN invité sélectionné lorsque Guest Authentication est activé.

ÉTAPE 5 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 6 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration du WAN

Par défaut, l'Cisco ISA500 est configurée pour recevoir une adresse IP publique de votre FAI automatiquement via le protocole DHCP. En fonction des exigences de votre FAI, vous devrez peut-être utiliser les pages Networking > WAN pour modifier les paramètres du réseau WAN afin d'assurer la connectivité Internet. Reportez-vous aux rubriques suivantes :

- **Configuration des paramètres du WAN pour votre connexion internet, page 128**
- **Configuration de la redondance du WAN, page 136**
- **Configuration de la détection de basculement de liaison, page 138**
- **Configuration du DNS dynamique, page 140**

Configuration des paramètres du WAN pour votre connexion internet

Utilisez la page Networking > WAN > WAN Settings pour configurer les paramètres du WAN à l'aide des informations de compte fournies par votre FAI. Si vous disposez de deux liaisons FAI, vous pouvez configurer l'une pour WAN1 et l'autre pour WAN2.

Procédez comme suit :

- **Publication ou renouvellement d'une connexion WAN par DHCP, page 128**
- **Configuration du WAN principal, page 129**
- **Configuration d'un WAN secondaire, page 130**

Publication ou renouvellement d'une connexion WAN par DHCP

Lorsque l'interface WAN est configurée pour obtenir une adresse IP du FAI à l'aide du protocole DHCP (Dynamic Host Configuration Protocol), vous pouvez cliquer sur l'icône **Release** pour publier son adresse IP ou sur l'icône **Renew** pour obtenir une nouvelle adresse IP.

Configuration du WAN principal

Pour configurer les paramètres du WAN principal, cliquez sur l'icône **Edit** (crayon). Utilisez ensuite la page WAN - Add/Edit pour configurer la connexion. Si vous avez activé le mode du routage IPv4/IPv6, remplissez les deux pages avec onglets. Cliquez sur **OK** pour enregistrer vos paramètres. Cliquez sur **Save** pour appliquer vos paramètres à l'appliance de sécurité.

Pour le mode de routage IPv4, entrez les informations suivantes dans l'onglet **IPv4** :

- **Physical Port** : port physique associé au WAN principal.
- **WAN Name** : nom du WAN principal (WAN1).
- **IP Address Assignment** : en fonction des exigences de votre FAI, choisissez le mode d'adressage réseau et complétez les paramètres correspondants. L'Cisco ISA500 prend en charge le client DHCP, l'IP statique, PPPoE, PPTP et L2TP. Pour obtenir des informations sur la configuration du mode d'adressage réseau, voir **Mode d'adressage réseau, page 131**.
- **DNS Server Source** : les serveurs DNS établissent une correspondance entre les noms de domaines Internet et les adresses IP. Vous pouvez obtenir les adresses des serveurs DNS automatiquement auprès de votre FAI ou utiliser les adresses spécifiées par votre FAI.
  - **Get Dynamically from ISP :** choisissez cette option si une adresse IP statique DNS ne vous a pas été attribuée.
  - **Use these DNS Servers :** choisissez cette option si une adresse IP statique DNS vous a été attribuée. Entrez également les adresses dans les champs **DNS1** et **DNS2**.
- **MAC Address Source** : spécifiez l'adresse MAC pour le WAN principal. En général, vous pouvez utiliser l'adresse Ethernet locale unique de 48 bits de l'Cisco ISA500 en tant qu'adresse MAC source.
  - **Use Default MAC Address** : choisissez cette option pour utiliser l'adresse MAC par défaut.
  - **Use the following MAC address** : si votre FAI requiert l'authentification MAC et qu'une autre adresse MAC a été enregistrée précédemment auprès de ce dernier, choisissez cette option et entrez l'adresse MAC requise par votre FAI pour cette connexion.
- **MAC Address** : entrez l'adresse MAC, par exemple 01:23:45:67:89:ab.

- **Zone** : choisissez la zone WAN par défaut ou une zone non fiable pour le WAN principal. Vous pouvez cliquer sur le lien **Create Zone** pour afficher, modifier ou ajouter des zones sur l'appliance de sécurité.

Pour le mode de routage IPv4/IPv6, entrez les informations suivantes dans l'onglet **IPv6** :

- **IP Address Assignment** : choisissez **Static IP** si votre FAI a attribué une adresse IP fixe (statique ou permanente) ou **SLAAC** si aucune adresse IP statique ne vous a été attribuée. Par défaut, votre Cisco ISA500 est configuré comme client DHCPv6 du FAI, avec la configuration automatique des adresses sans état (SLAAC).
  - **SLAAC** : la SLAAC fournit une méthode très pratique pour attribuer des adresses IP aux nœuds IPv6. Cette méthode ne requiert aucune intervention de la part d'un utilisateur IPv6. Si vous choisissez la SLAAC, l'Cisco ISA500 peut générer ses propres adresses à l'aide d'une combinaison d'informations localement disponibles et d'informations annoncées par les routeurs.
  - **Static IP** : si votre FAI a affecté une adresse IPv6 statique, configurez la connexion WAN IPv6 dans les champs suivants :

    IPv6 Address : entrez l'adresse IP statique fournie par votre FAI.

    IPv6 Prefix Length : le réseau IPv6 (sous-réseau) est identifié par les bits initiaux de l'adresse appelés préfixe. Tous les hôtes du réseau possèdent des bits initiaux identiques pour leur adresse IPv6. Entrez le nombre de bits initiaux communs dans les adresses du réseau. La longueur du préfixe par défaut est 64.

    Default IPv6 Gateway : entrez l'adresse IPv6 de la passerelle de votre FAI. Elle est généralement fournie par le FAI ou votre administrateur réseau.

    Primary DNS Server : entrez une adresse IP valide du serveur DNS principal.

    Secondary DNS Server (Optional) : en option, entrez une adresse IP valide du serveur DNS secondaire.

Configuration d'un WAN secondaire

Pour configurer un WAN secondaire (WAN2), cliquez sur **Add**. Utilisez ensuite la page WAN - Add/Edit pour configurer la connexion. Si vous avez activé le mode du routage IPv4/IPv6, remplissez les deux pages avec onglets, comme décrit pour l'interface WAN principale. Cliquez sur **OK** pour enregistrer vos paramètres dans

la fenêtre contextuelle. Cliquez sur **Save** pour appliquer vos paramètres à l'appliance de sécurité. Pour déterminer la manière dont les deux liaisons FAI sont utilisées, configurez les paramètres de redondance du WAN. Voir **Configuration de la redondance du WAN, page 136**.

- Si vous rencontrez des problèmes avec votre connexion WAN, voir **Connexion Internet, page 431**.

Mode d'adressage réseau

L'Cisco ISA500 prend en charge cinq types de modes d'adressage réseau. Vous devez spécifier le mode d'adressage réseau pour le WAN principal et le WAN secondaire en fonction des exigences de votre FAI.

REMARQUE Faites-vous confirmer auprès de votre FAI ou d'un routeur homologue que vous disposez bien des informations réseau permettant de configurer l'Cisco ISA500 pour accéder à Internet.

Mode d'adressage réseau	Configuration
Client DHCP	Type de connexion souvent utilisé avec les modems câbles. Choisissez cette option si votre FAI attribue dynamiquement une adresse IP lors de la connexion. **REMARQUE** : Sauf indication contraire de la part de votre FAI, il est recommandé de ne pas modifier les valeurs MTU. ▪ **MTU** : l'unité de transmission maximale correspond à la taille, en octets, du plus grand paquet pouvant être transmis. Choisissez **Auto** pour utiliser la taille MTU par défaut ou **Manual** si vous souhaitez spécifier une autre taille. ▪ **MTU Value** : si vous choisissez **Manual**, entrez la taille MTU personnalisée en octets.

Mode d'adressage réseau	Configuration
Adresse IP statique	Choisissez cette option si le FAI vous fournit une adresse IP statique (permanente) et ne l'attribue pas dynamiquement. Utilisez les informations correspondantes de votre FAI pour compléter les champs suivants : ▪ **IP Address** : entrez l'adresse IP du port WAN pouvant être accessible à partir d'Internet. ▪ **Subnet Mask** : entrez l'adresse IP du masque de sous-réseau. ▪ **Gateway** : entrez l'adresse IP de la passerelle par défaut. ▪ **MTU** : l'unité de transmission maximale correspond à la taille, en octets, du plus grand paquet pouvant être transmis. Choisissez **Auto** pour utiliser la taille MTU par défaut ou **Manual** si vous souhaitez spécifier une autre taille. ▪ **MTU Value** : si vous choisissez **Manual**, entrez la taille MTU personnalisée en octets.

Mode d'adressage réseau	Configuration
PPPoE	PPPoE utilise le protocole PPPoE (Point to Point Protocol over Ethernet) pour la connexion à Internet. Choisissez cette option si votre FAI vous fournit un logiciel client, un nom d'utilisateur et un mot de passe. Utilisez les informations PPPoE nécessaires fournies par votre FAI pour terminer la configuration PPPoE. ▪ **User Name** : entrez le nom d'utilisateur requis pour vous connecter au FAI. ▪ **Password** : entrez le mot de passe requis pour vous connecter au FAI. ▪ **Authentication Type** : sélectionnez le type d'authentification spécifié par votre FAI. ▪ **Connect Idle Time** : choisissez cette option pour permettre à l'Cisco ISA500 de se déconnecter d'Internet après une période d'inactivité donnée (délai d'inactivité). Ce choix est recommandé si votre connexion Internet est facturée au temps passé en ligne. ▪ **Keep alive** : choisissez cette option pour que la connexion soit permanente, quel que soit le niveau de l'activité. Ce choix est recommandé si vous payez un abonnement fixe pour votre service Internet. ▪ **MTU** : choisissez **Auto** pour utiliser la taille MTU par défaut, ou **Manual** si vous souhaitez spécifier une autre taille. ▪ **MTU Value** : si vous choisissez **Manual**, entrez la taille MTU personnalisée en octets. ▪ **Add VLAN Tag** : cliquez sur **Yes** pour prendre en charge le marquage VLAN (802.1q) sur le port WAN, ou sur **No** pour le désactiver. ▪ **VLAN Tag ID** : spécifiez la balise VLAN (ID) sur le port WAN. ▪ **Reset Timer** : vous pouvez réinitialiser la connexion PPPoE à un moment donné de la journée et à un jour donné de la semaine. Les événements de réinitialisation sont consignés si vous activez cette fonctionnalité. Choisissez l'une des options suivantes dans la liste déroulante **Frequency** et spécifiez les paramètres correspondants : - **Never** : choisissez cette option pour désactiver cette fonctionnalité. - **Daily** : choisissez cette option pour réinitialiser la connexion PPPoE à un moment donné de la journée. Spécifiez l'heure de la journée dans les champs **Time**. - **Weekly** : choisissez cette option pour réinitialiser la connexion PPPoE à un jour donné de la semaine. Spécifiez ensuite le jour de la semaine et de l'heure de la journée.

Mode d'adressage réseau	Configuration
PPTP	Le protocole PPTP est généralement utilisé pour la connexion VPN. Utilisez les informations nécessaires fournies par votre FAI pour terminer la configuration PPTP : ▪ **IP Address** : entrez l'adresse IP du port WAN pouvant être accessible à partir d'Internet. ▪ **Subnet Mask** : entrez le masque de sous-réseau. ▪ **Gateway** : entrez l'adresse IP de la passerelle par défaut. ▪ **User Name** : entrez le nom d'utilisateur requis pour vous connecter au serveur PPTP. ▪ **Password** : entrez le mot de passe requis pour vous connecter au serveur PPTP. ▪ **PPTP Server IP Address** : entrez l'adresse IP du serveur PPTP. ▪ **MPPE Encryption** : le cryptage point à point de Microsoft (MPPE) crypte les données dans les connexions à distance basées sur PPP ou les connexions VPN PPTP. Cochez cette case afin de permettre au cryptage MPPE de fournir la sécurité des données pour la connexion PPTP entre le client VPN et le serveur VPN. ▪ **Connect Idle Time** : choisissez cette option pour permettre à l'Cisco ISA500 de se déconnecter d'Internet après une période d'inactivité donnée (délai d'inactivité). Ce choix est recommandé si votre connexion Internet est facturée au temps passé en ligne. ▪ **Keep alive** : choisissez cette option pour que la connexion soit permanente, quel que soit le niveau de l'activité. Ce choix est recommandé si vous payez un abonnement fixe pour votre service Internet. ▪ **MTU** : choisissez **Auto** pour utiliser la taille MTU par défaut ou **Manual** si vous souhaitez spécifier une autre taille. ▪ **MTU Value** : si vous choisissez **Manual**, entrez la taille MTU personnalisée en octets.

Mode d'adressage réseau	Configuration
L2TP	Choisissez cette option si vous souhaitez utiliser l'IPsec pour connecter un serveur L2TP (Layer 2 Tunneling Protocol) et crypter toutes les données transmises du client au serveur. Cependant, il ne crypte pas le trafic réseau vers d'autres destinations. Utilisez les informations nécessaires fournies par votre FAI pour terminer la configuration L2TP : ▪ **IP Address** : entrez l'adresse IP du port WAN pouvant être accessible à partir d'Internet. ▪ **Subnet Mask** : entrez le masque de sous-réseau. ▪ **Gateway** : entrez l'adresse IP de la passerelle par défaut. ▪ **User Name** : entrez le nom d'utilisateur requis pour vous connecter au serveur L2TP. ▪ **Password** : entrez le mot de passe requis pour vous connecter au serveur L2TP. ▪ **L2TP Server IP Address** : entrez l'adresse IP du serveur L2TP. ▪ **Secret (Optional)** : L2TP intègre un système d'authentification des tunnels simple, optionnel et de type CHAP lors de l'établissement de la connexion de contrôle. Entrez le secret pour l'authentification du tunnel si nécessaire. ▪ **Connect Idle Time** : choisissez cette option pour permettre à l'Cisco ISA500 de se déconnecter d'Internet après une période d'inactivité donnée (délai d'inactivité). Ce choix est recommandé si votre connexion Internet est facturée au temps passé en ligne. ▪ **Keep alive** : choisissez cette option pour que la connexion soit permanente, quel que soit le niveau de l'activité. Ce choix est recommandé si vous payez un abonnement fixe pour votre service Internet. ▪ **MTU** : choisissez **Auto** pour utiliser la taille MTU par défaut ou **Manual** si vous souhaitez spécifier une autre taille. ▪ **MTU Value** : si vous choisissez **Manual**, entrez la taille MTU personnalisée en octets.

Configuration de la redondance du WAN

Si vous disposez de deux liaisons FAI, l'une pour WAN1 et l'autre pour WAN2, utilisez les pages Networking > WAN Redundancy pour configurer la redondance du WAN afin de déterminer comment les deux liaisons FAI sont utilisées. Reportez-vous aux rubriques suivantes :

- **Équilibrage de charge pour la redondance du WAN, page 136**
- **Équilibrage de charge avec l'exemple de configuration du PBR, page 139**

REMARQUE Avant de configurer les paramètres de redondance du WAN, vous devez tout d'abord configurer la connexion WAN secondaire. Voir **Configuration d'un WAN secondaire, page 130**.

REMARQUE Lorsque l'Cisco ISA500 fonctionne en mode Dual WAN Settings ou Failover, si une liaison WAN est en panne (par exemple, le câble est déconnecté), les paramètres de redondance du WAN et de PBR (Policy Based Routing) sont ignorés et l'ensemble du trafic est traité par le port WAN actif.

Équilibrage de charge pour la redondance du WAN

Utilisez la page Networking > WAN Redundancy > Dual WAN Settings pour isoler le trafic entre les liaisons qui ne sont pas de la même vitesse. Par exemple, vous pouvez lier les services de gros volume via le port connecté à la liaison haut débit et lier les services de faible volume au port connecté à la liaison bas débit.

Le mode Dual WAN Settings est mis en œuvre pour le trafic sortant et non pour le trafic entrant. Pour garder un meilleur contrôle du trafic du port WAN, pensez à rendre l'adresse Internet du port WAN publique et à conserver l'autre privée.

REMARQUE Pour configurer le mode Dual WAN Settings, vérifiez que vous avez configuré les deux ports WAN de façon à les maintenir actifs. Si le port WAN est configuré pour s'arrêter après une période d'inactivité spécifiée, le mode Dual WAN Settings ne s'applique pas.

ÉTAPE 1 Sélectionnez une option dans la section Dual WAN Settings pour préciser la façon dont les deux liaisons FAI sont utilisées. Les deux liaisons acheminent des données pour les protocoles auxquels elles sont liées.

- **Weighted Load Balancing** : répartit la bande passante sur deux ports WAN en fonction du pourcentage pondéré ou de la bande passante de liaison pondérée. Si vous choisissez ce mode, choisissez l'une des options suivantes et terminez en spécifiant les paramètres suivants :
  - **Weighted by Percentage** : si vous choisissez cette option, spécifiez le pourcentage de chaque WAN, tel que 80 % de la bande passante pour le WAN1 et au moins 20 % de la bande passante pour le WAN2.
  - **Weighted by Link Bandwidth** : si vous choisissez cette option, spécifiez la quantité de bande passante pour chaque WAN, telle que 80 Mbit/s pour le WAN1 et 20 Mbit/s pour le WAN2, ce qui signifie que 80 % de la bande passante est distribuée au WAN1 et au moins 20 % au WAN2.

  REMARQUE : L'option Weighted by Link Bandwidth produit le même effet que l'option Weighted by Percentage. Elle propose seulement davantage d'options de pourcentage que l'option Weighted by Percentage qui n'en propose que trois. Par exemple, vous pouvez définir 60 Mbits/s pour le WAN1 et 40 Mbits/s pour le WAN2, ce qui signifie que 60 % de la bande passante est distribuée au WAN1 et le restante 40 % est distribuée au WAN2.
- **Based on Real-time Bandwidth** : envoie du trafic sur la liaison dont la bande passante en temps réel est la plus élevée. Utilisez les informations fournies par votre prestataire de services pour spécifier la bande passante de base pour chaque liaison dans les champs **WAN1** et **WAN2**.
- **Failover** : si une défaillance est détectée sur la liaison principale, l'appliance de sécurité dirige l'ensemble du trafic Internet vers la liaison de secours. Lorsque la liaison principale récupère la connectivité, l'ensemble du trafic Internet est dirigé vers la liaison principale et la liaison de secours devient inactive. Par défaut, WAN1 est défini comme liaison principale et WAN2 comme liaison de secours.

  REMARQUE : Lorsque l'Cisco ISA500 fonctionne en mode Failover, les paramètres PBR (Policy-Based Routing) sont ignorés.
  - **Select WAN Precedence** : sélectionnez la liaison à utiliser comme liaison principale et de secours. L'option par défaut est principal : WAN1 ; secondaire : WAN2.

- **Preempt Delay Timer** : entrez l'heure en secondes à laquelle l'Cisco ISA500 attendra avant d'envoyer le trafic de la liaison de secours vers la liaison principale une fois cette dernière de nouveau active. La valeur par défaut est 5 de secondes.

- **Routing Table** : utilise les stratégies de routage statique pour déterminer les types de trafic qui traversent les deux liaisons WAN. Pour obtenir des informations sur la configuration du routage statique, voir **Configuration du routage statique, page 157**.

ÉTAPE 2 Activez **Policy Based Routing** si vous souhaitez utiliser des stratégies pour spécifier l'IP et/ou le service interne passant par chaque port du WAN afin de fournir un trafic plus souple et plus granuleux prenant en charge des fonctionnalités. Cliquez sur **On** pour activer cette fonctionnalité ou sur **Off** pour la désactiver. Après avoir activé cette fonctionnalité, cliquez sur **Configure** pour définir les stratégies. Voir **Configuration du PBR, page 159**.

REMARQUE : Si vous activez le PBR, ses paramètres sont prioritaires par rapport aux paramètres de Dual WAN Settings. Le trafic correspondant aux stratégies PBR sera acheminé en fonction de ces paramètres. Le trafic ne correspondant pas aux stratégies PBR est acheminé selon les paramètres de Dual WAN Settings.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration de la détection de basculement de liaison

Utilisez la page Networking > WAN > WAN Redundancy > Link Failover Detection pour détecter la défaillance de la liaison. Si une défaillance se produit, le trafic de la liaison non disponible est transféré vers le lien actif.

ÉTAPE 1 Entrez les informations suivantes :

- **Failover Detection** : cliquez sur **On** pour activer la fonctionnalité Link Failover Detection ou sur **Off** pour la désactiver.
- **Retry Count** : entrez le nombre de tentatives. L'Cisco ISA500 cherche à plusieurs reprises de se connecter au FAI après la détection de la défaillance de liaison. La valeur par défaut est de 5.
- **Retry Timeout** : si la connexion au FAI est en panne, l'Cisco ISA500 essaie de se connecter au FAI après un délai spécifié. Entrez le délai, en secondes, avant de se reconnecter au FAI. La valeur par défaut est 5 secondes.

- **Ping Detection** : choisissez cette option pour détecter la défaillance du WAN en effectuant un test ping sur l'adresse IP que vous spécifiez dans les champs suivants :
  - **Default IP Gateways** : effectuez un test ping sur l'adresse IP de la passerelle WAN par défaut. Si la passerelle WAN par défaut peut être détectée, la connexion réseau est active.
  - **Specify the IP Gateways** : effectuez un test ping sur les hôtes à distance. Entrez les adresses IP dans les champs **Primary IP Gateway** et **Secondary IP Gateway**. En mode de basculement, si l'hôte à distance du WAN principal peut être détecté, la connexion réseau est active. En mode d'équilibrage de charge, si les hôtes à distance des deux ports WAN peuvent être détectés, la connexion WAN est active.
- **DNS Detection** : choisissez cette option pour détecter la défaillance du WAN en recherchant les serveurs DNS que vous spécifiez dans les champs suivants :
  - **Default DNS Servers** : envoyez la requête DNS de www.cisco.com au serveur DNS du WAN par défaut. Si le serveur DNS peut être détecté, la connexion réseau est active.
  - **Specify DNS Servers** : envoyez la requête DNS de www.cisco.com aux serveurs DNS spécifiés. Entrez les adresses IP dans les champs **Primary WAN DNS Server** et **Secondary WAN DNS Server**. Si le serveur DNS principal ou secondaire peut être détecté, la connexion réseau est active.

ÉTAPE 2 Cliquez sur **Save** pour appliquer vos paramètres.

Équilibrage de charge avec l'exemple de configuration du PBR

Use Case : un client dispose de deux lignes, une liaison par câble et une liaison DSL. La majorité du trafic passe par la liaison par câble puisque la bande passante est plus importante et le reste du trafic passe par la liaison DSL. Puisqu'un bon nombre de sites Web sécurisés (les sites bancaires ou de commerce en ligne par exemple) sont sensibles au basculement de l'adresse IP source, autorisez le trafic pour https, ftp, les vidéos et les jeux à passer via la liaison par câble.

Solution : effectuez les tâches de configuration suivantes :

- Configurez un port configurable comme WAN secondaire (WAN2). Voir **Configuration d'un WAN secondaire, page 130**.

- Connectez le modem câble au port WAN principal (WAN1) et connectez le modem DSL au port WAN secondaire (WAN2).
- Activez le mode Weighted Dual WAN Settings, puis définissez la valeur pondérée du WAN1 sur 80 % et la valeur pondérée du WAN2 sur 20 %. Voir **Équilibrage de charge pour la redondance du WAN, page 136**.
- Activez la fonctionnalité PBR et configurez les règles PBR de façon à rediriger le trafic pour HTTPS, FTP, les vidéos et les jeux vers le WAN1. Voir **Configuration du PBR, page 159**.
- (Facultatif) Activez les rapports d'utilisation et les rapports de la bande passante WAN de façon à afficher l'utilisation de la bande passante. Reportez-vous aux sections **Rapports d'utilisation, page 97** et **Rapports de la bande passante WAN, page 99**.

Configuration du DNS dynamique

Utilisez la page Networking > WAN > DDNS pour configurer le DNS dynamique (DDNS). Le DDNS est un service Internet qui permet aux routeurs possédant des adresses IP publiques variables d'être localisés à l'aide de noms de domaine Internet. Si votre FAI ne vous a pas fourni d'adresse IP statique et que votre connexion WAN est configurée pour utiliser le protocole DHCP et obtenir une adresse IP de manière dynamique, le DDNS fournit le nom de domaine pour mapper l'adresse IP dynamique de votre site Web. Pour utiliser le DDNS, vous devez configurer un compte avec un fournisseur DDNS tel que DynDNS.com.

Table des services DDNS

La colonne **Status** affiche l'état du service DDNS. Cliquez sur **Active** pour mettre à jour manuellement l'adresse IP de l'interface WAN avec le nom de domaine spécifié par l'utilisateur.

- **Non-active** : le service DDNS n'est pas actif (le daemon DDNS ne s'amorce pas).
- **Active (initial)** : le daemon DDNS s'amorce, mais le processus de mise à jour du DDNS n'est pas encore terminé.
- **Active (updated WAN**x**) :** le processus de mise à jour du DDNS est terminé et l'adresse de l'interface WAN est mise à jour avec le nom de domaine spécifié par l'utilisateur.

Ajout ou modification d'un service DDNS

Cliquez sur **Add** pour ajouter un nouveau service DDNS. Pour modifier une entrée, cliquez sur l'icône **Edit** (crayon). Pour supprimer une entrée, cliquez sur l'icône **Delete** (x).

ÉTAPE 1 Entrez les informations suivantes :

- **Service** : spécifiez le fournisseur de votre service DDNS. Vous pouvez choisir DynDNS ou No-IP service.

  REMARQUE : Vous devez souscrire un compte auprès de l'un de ces fournisseurs avant de pouvoir utiliser ce service.

- **Active on Startup** : cochez cette case pour activer le service DDNS lorsque l'Cisco ISA500 démarre.

- **WAN Interface** : choisissez le port WAN du service DDNS. Le trafic des services DDNS passe par le port WAN spécifié.

  REMARQUE : Si la redondance du WAN est définie comme mode de basculement, cette option est grisée. Lorsque le basculement du WAN se produit, le DDNS bascule le trafic sur le port WAN actif.

- **User Name** : entrez le nom d'utilisateur du compte que vous avez enregistré dans le fournisseur DDNS.

- **Password** : entrez le mot de passe du compte que vous avez enregistré dans le fournisseur DDNS.

- **Host and Domain Name** : entrez le nom d'hôte et le nom de domaine complets du service DDNS, par exemple : name.dyndns.org.

- **Wildcards** : cochez cette case pour permettre à tous les sous-domaines de votre nom d'hôte DDNS de partager la même adresse IP publique comme nom d'hôte.

- **Update** : cochez cette case pour mettre à jour les informations de l'hôte chaque semaine.

ÉTAPE 2 Cliquez sur **OK** pour enregistrer vos paramètres et fermer la fenêtre contextuelle.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Mesure et limitation du trafic avec l'utilitaire de contrôle du trafic

Utilisez les pages Networking > WAN > Traffic Metering pour mesurer et limiter le trafic acheminé par l'Cisco ISA500. Si vous avez activé une liaison WAN secondaire, utilisez l'arborescence de navigation pour choisir Primary WAN Metering ou Secondary WAN Metering.

ÉTAPE 1 Dans la zone **Traffic Meter**, entrez les informations suivantes :

- **Enable** : cliquez sur **On** pour activer la mesure du trafic sur le port, ou sur **Off** pour la désactiver. Le fait d'activer cette fonctionnalité sur le port permet de conserver un enregistrement du volume de trafic acheminé depuis ce port.
- **Traffic Limit** : spécifiez la restriction sur le volume de données transférées par le port.
  - **No Limit** : option par défaut, aucune limite de transfert de données n'est imposée.
  - **Download Only** : limitez la quantité de trafic de téléchargement. Entrez le volume de données maximal autorisé en mégaoctets pouvant être téléchargé pour un mois donné dans le champ **Monthly Limit**. Une fois la limite atteinte, aucun trafic n'est autorisé côté WAN.
  - **Both Directions** : calculez le trafic du chargement et du téléchargement. La limite de trafic entrée dans le champ **Monthly Limit** est partagée par le trafic de chargement et le trafic de téléchargement. Par exemple, pour une limite de 1 Go, si un fichier de 700 Mo est téléchargé, les 300 Mo restants doivent être partagés entre le trafic de chargement et le trafic de téléchargement. Le volume de trafic téléchargé réduit le volume de trafic pouvant être chargé et vice-versa.
- **Monthly Limit** : entrez la limite de volume qui s'applique pour ce mois. Cette limite s'applique au type de direction (Download Only ou Both Directions) sélectionné ci-dessus. La valeur zéro (0) indique que l'ensemble du trafic via le port sera bloqué.

ÉTAPE 2 Dans la zone **Traffic Counter,** entrez les informations suivantes :

- **Traffic Counter** : spécifiez l'action à entreprendre sur le compteur de trafic.
  - **Restart Now** : choisissez cette option, puis cliquez sur **Save** pour réinitialiser immédiatement le compteur.
  - **Specific Time** : choisissez cette option si vous souhaitez que le compteur reparte à un jour et une heure précis. Entrez ensuite l'heure en heures (hh) et en minutes (mm) et sélectionnez le jour du mois dans la zone **Reset Time.**

- **Send Email Report** : cliquez sur **On** pour envoyer un e-mail d'alerte à l'adresse e-mail spécifiée avant la réinitialisation du compteur de trafic, ou sur **Off** pour le désactiver. Cette fonctionnalité requiert l'activation de la fonctionnalité d'alerte de mesure du trafic et la configuration des paramètres du serveur de messagerie sur la page Email Alert Settings. Voir **Configuration des paramètres d'alerte par courriel, page 382**.

ÉTAPE 3 Dans la zone **When Limit is Reached**, spécifiez l'action à entreprendre lorsque la limite de trafic est atteinte.

- **Traffic Block** : choisissez l'une des options suivantes :
  - **All Traffic** : bloquez l'ensemble du trafic via le port WAN lorsque la limite de trafic est atteinte.
  - **All Traffic Except Email** : bloquez l'ensemble du trafic excepté le courrier électronique via le port WAN lorsque la limite de trafic est atteinte.
- **Email Alert** : Cliquez sur **On** pour envoyer un message d'alerte à l'adresse électronique spécifiée lorsque la limite de trafic est atteinte ou sur **Off** pour désactiver cette fonctionnalité. Cette fonctionnalité requiert l'activation de la fonctionnalité d'alerte de mesure du trafic et la configuration des paramètres du serveur de messagerie sur la page Email Alert Settings. Voir **Configuration des paramètres d'alerte par courriel, page 382**.

ÉTAPE 4 Dans la zone **Internet Traffic**, les informations suivantes s'affichent après l'activation de la mesure du trafic :

Start Date/Time	Date à laquelle l'utilitaire de contrôle du trafic a été lancé ou dernière fois que le compteur de trafic a été réinitialisé.
Outgoing Traffic Volume	Volume du trafic, en mégaoctets, qui a été chargé par ce port.
Incoming Traffic Volume	Volume du trafic, en mégaoctets, qui a été téléchargé par ce port.
Average per day	Volume du trafic moyen acheminé via ce port.
Traffic Utilized	Volume du trafic, en pourcentage, acheminé via ce port par rapport à la limite mensuelle.

ÉTAPE 5 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration d'un VLAN

Utilisez la page Networking > WAN > VLAN pour configurer un LAN virtuel (VLAN). Les VLAN vous permettent de compartimenter et d'isoler le trafic. Un ordinateur d'un VLAN ne peut pas accéder aux ressources réseau d'autres VLAN.

L'Cisco ISA500 prédéfinit trois VLAN :

- Un VLAN natif (PAR DÉFAUT), avec l'ID de VLAN 1 et l'adresse IP 192.168.75.1. Par défaut, ce VLAN se trouve dans la zone LAN.
- Un VLAN invité (INVITÉ), avec l'ID de VLAN 2 et l'adresse IP 192.168.25.1. Par défaut, ce VLAN est dans la zone INVITÉ.
- Un VLAN voix (VOICE) avec l'ID de VLAN 100 et l'adresse 10.1.1.2. Par défaut, ce VLAN se trouve dans la zone VOICE.

Vous pouvez modifier les paramètres des VLAN prédéfinis ou ajouter de nouveaux VLAN pour répondre à vos besoins professionnels.

REMARQUE Vous pouvez configurer jusqu'à 16 VLAN sur l'Cisco ISA500.

ÉTAPE 1 Pour ajouter un nouveau VLAN, cliquez sur **Add**. Pour modifier les paramètres d'un VLAN, cliquez sur l'icône **Edit** (crayon).

Autres options : pour supprimer un VLAN, cliquez sur l'icône **Delete** (x). Les VLAN par défaut ne peuvent pas être supprimés.

ÉTAPE 2 Dans l'onglet **Basic Settings**, entrez les informations suivantes :

- **Name** : entrez le nom du VLAN.
- **VLAN ID** : entrez un numéro d'identification unique pour le VLAN, qui peut être n'importe quel numéro entre 3 et 4089. L'ID de VLAN 1 est réservé au VLAN PAR DÉFAUT et l'ID de VLAN 2 est réservé au VLAN INVITÉ.
- **IP Address** : entrez l'adresse IP de sous-réseau du VLAN.
- **Netmask** : entrez le masque de sous-réseau du VLAN.
- **Spanning Tree** : cochez cette case pour activer la fonctionnalité Spanning Tree afin de déterminer s'il existe des boucles dans la topologie de réseau. Le protocole STP (Spanning Tree Protocol) est un protocole réseau de couche de liaison qui garantit une topologie sans boucle pour les LAN avec ponts. Il est utilisé pour éviter les boucles de pont et garantir le rayonnement de la diffusion.
- **Voice VLAN** : cochez la case si vous souhaitez que les applications vocales utilisent ce VLAN.

- **Port** : affectez les ports LAN au VLAN. Le trafic via les ports LAN sélectionnés est dirigé vers le VLAN. Tous les ports disponibles, notamment les ports LAN dédiés et les ports configurables apparaissent dans la liste **Port**.

  Choisissez les ports dans la liste **Port** et cliquez sur **Access** pour les ajouter à la liste **Member** et définir les ports sélectionnés en mode d'accès. Vous pouvez également choisir les ports de la liste **Port** et cliquer sur **Trunk** pour les ajouter à la liste **Member** et définir les ports sélectionnés en mode Trunk.

  REMARQUE : Ce paramètre modifie le type de port et le mode d'accès des ports physiques sélectionnés. Par exemple, sélectionnez un port qui a été configuré comme port DMZ et ajoutez-le à la liste des membres. Le port DMZ est configuré comme un port LAN. La modification du type de port élimine l'ensemble de la configuration relative au port physique.

- **Zone** : choisissez la zone à laquelle le VLAN est mappé. Par défaut, le VLAN PAR DÉFAUT est mappé à la zone LAN, le VLAN INVITÉ est mappé à la zone INVITÉ, et le VLAN VOIX est mappé à la zone VOIX. Vous pouvez cliquer sur le lien **Create Zone** pour afficher, modifier ou ajouter des zones sur l'appliance de sécurité.

ÉTAPE 3 Dans l'onglet **DHCP Pool Settings**, choisissez le mode DHCP dans la liste déroulante **DHCP Mode**.

- **Disable** : choisissez cette option si les ordinateurs du VLAN sont configurés avec des adresses IP statiques ou pour utiliser un autre serveur DHCP.
- **DHCP Server** : permet à l'Cisco ISA500 d'agir en tant que serveur DHCP et attribue les adresses IP à tous les périphériques connectés au VLAN. Tout nouveau client DHCP se connectant au VLAN reçoit une adresse IP du pool DHCP.
- **DHCP Relay** : permet à l'Cisco ISA500 d'utiliser un relais DHCP. Si vous choisissez le relais DHCP, entrez l'adresse IP du serveur DHCP distant dans le champ **Relay IP**.

ÉTAPE 4 Si vous choisissez **DHCP Server** comme mode DHCP, entrez les informations suivantes :

- **Start IP** : entrez l'adresse IP de début du pool DHCP.
- **End IP** : entrez l'adresse IP de fin du pool DHCP.

  REMARQUE : L'adresse IP de début et l'adresse IP de fin doivent être dans le même sous-réseau que l'adresse IP du VLAN.

- **Lease Time** : entrez la durée de connexion maximale de « location » d'une adresse IP dynamique à un utilisateur du réseau. Lorsque le temps s'est écoulé, l'adresse IP dynamique de l'utilisateur est automatiquement renouvelée.
- **DNS1** : entrez l'adresse IP du serveur DNS principal.
- **DNS2** : entrez éventuellement l'adresse IP du serveur DNS secondaire.
- **WINS1** : entrez éventuellement l'adresse IP du serveur WINS principal.
- **WINS2** : entrez éventuellement l'adresse IP du serveur WINS secondaire.
- **Domain Name** : entrez éventuellement le nom de domaine du VLAN.
- **Default Gateway** : entrez l'adresse IP de la passerelle par défaut.
- **Option 66** : fournit les informations d'adresse du serveur de mise en service aux hôtes qui en font la demande. Prend en charge uniquement l'adresse IP ou le nom d'hôte d'un seul serveur TFTP. Entrez l'adresse IP du serveur TFTP unique du VLAN.
- **Option 67** : fournit un nom de fichier de configuration ou d'amorçage aux hôtes qui en font la demande. Cette option est utilisée conjointement avec l'option 66 pour permettre au client de formuler une demande TFTP appropriée pour le fichier. Entrez le nom de fichier de configuration ou d'amorçage sur le serveur TFTP spécifié.
- **Option 150** : prend en charge une liste de serveurs TFTP (2 serveurs TFTP). Entrez les adresses IP des serveurs TFTP. Vous pouvez indiquer plusieurs entrées séparées par une virgule (,).

  REMARQUE : Les entreprises ayant des petites filiales qui mettent en œuvre une solution de voix sur IP de téléphonie IP Cisco mettent généralement en œuvre Cisco CallManager dans un bureau central pour contrôler les Cisco IP Phone dans les petites filiales. Cette mise en œuvre permet le traitement centralisé des appels, réduit l'équipement nécessaire et élimine l'administration d'un Cisco CallManager supplémentaire et d'autres serveurs dans les filiales. Les Cisco IP Phone téléchargent leur configuration à partir d'un serveur TFTP. Lorsqu'un Cisco IP Phone entre en fonction, si l'adresse IP et l'adresse IP du serveur TFTP ne sont pas préconfigurées, il envoie une requête avec l'option 150 ou 66 au serveur DHCP pour obtenir ces informations.

ÉTAPE 5 Dans l'onglet **IPv6**, spécifiez l'adressage IPv6 pour le VLAN si vous activez le mode IIPv4 ou Pv6.

- **IPv6 Address** : entrez l'adresse IPv6 en fonction des exigences de votre réseau.
- **IPv6 Prefix Length** : entrez le nombre de caractères du préfixe IPv6.

  Le réseau IPv6 (sous-réseau) est identifié par le préfixe, qui est composé des bits initiaux de l'adresse. La longueur du préfixe par défaut est de 64 bits. Tous les hôtes du réseau possèdent des bits initiaux identiques pour l'adresse IPv6. Le nombre de bits initiaux communs des adresses est défini par le champ de longueur du préfixe.

ÉTAPE 6 Cliquez sur **OK** pour enregistrer vos paramètres et fermer la fenêtre contextuelle.

ÉTAPE 7 Cliquez sur **Save** pour appliquer vos paramètres.

ÉTAPE 8 Si vous souhaitez réserver certaines adresses IP pour des périphériques spécifiés, accédez à la page Networking > DHCP Reservations**.** Voir **Configuration des IP DHCP réservés, page 155**. Vous devez activer le mode DHCP Server ou DHCP Relay à cet effet.

Configuration de la DMZ

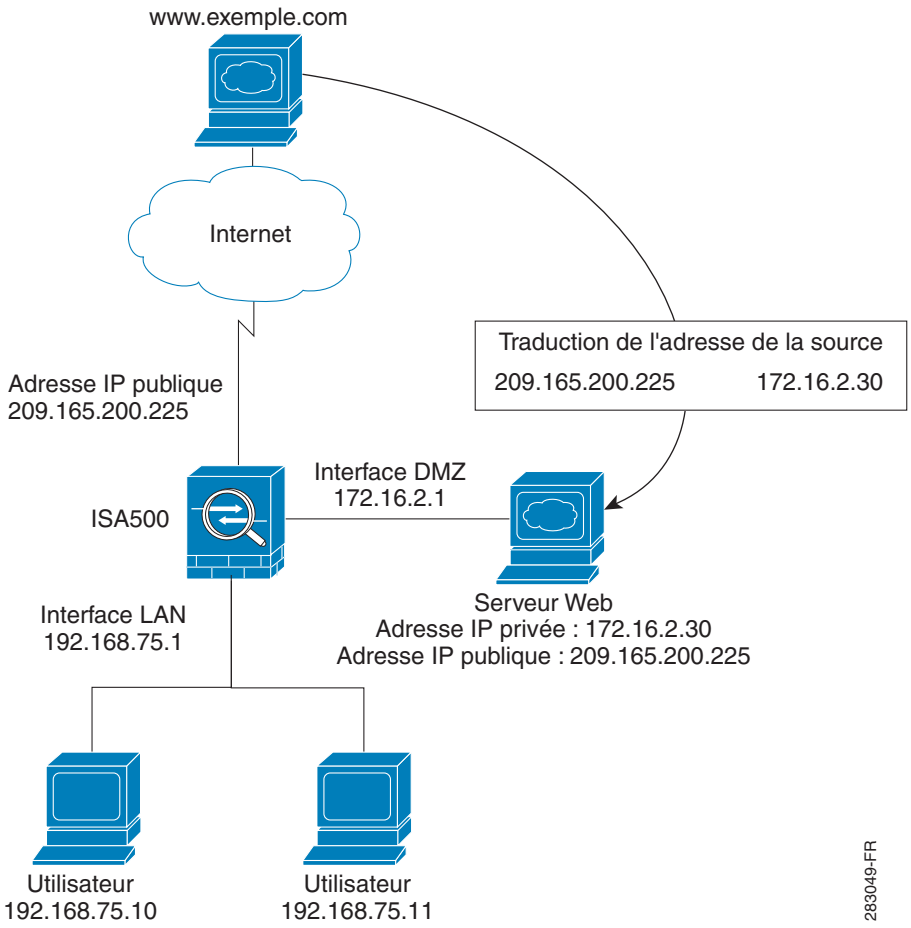
Utilisez la page Networking > DMZ pour configurer une zone de démarcation ou une zone démilitarisée (DMZ). Une DMZ est un sous-réseau qui se trouve derrière le pare-feu, mais qui est ouverte au public. En plaçant vos services publics sur une DMZ, vous pouvez ajouter une couche de sécurité supplémentaire au LAN. Le public peut se connecter aux services de la DMZ mais ne peut pas pénétrer le LAN. Vous devez configurer votre DMZ afin d'inclure tous les hôtes qui doivent être exposés au WAN (tels que les serveurs Web ou de messagerie).

À propos des réseaux DMZ

Cette section décrit comment configurer les réseaux DMZ. La configuration DMZ est identique à la configuration VLAN. Il n'existe aucune restriction sur l'adresse ou le sous-réseau IP attribués au port DMZ. Cependant, ils ne peuvent pas être identiques à l'adresse IP donnée aux VLAN prédéfinis.

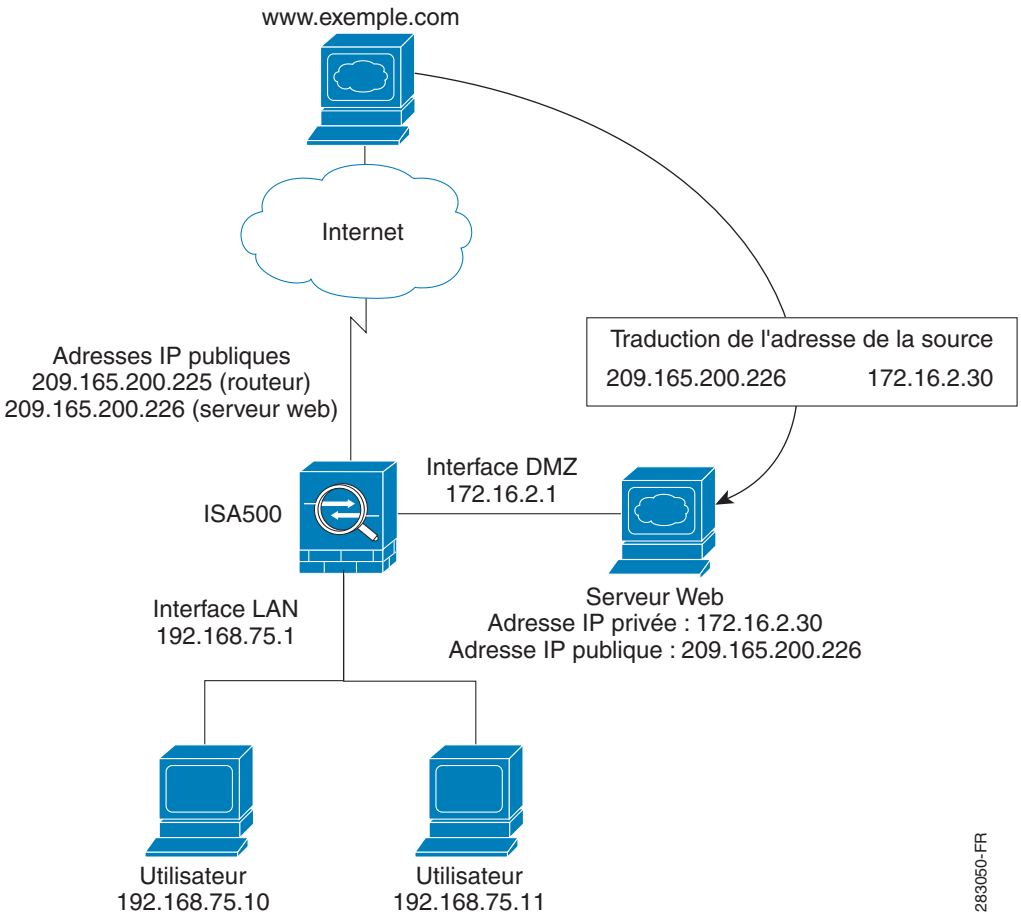
REMARQUE Jusqu'à 4 DMZ peuvent être configurées sur l'Cisco ISA500.

Figure 1 Exemple d'une DMZ avec une adresse IP publique pour le WAN et la DMZ



Dans ce scénario, l'entreprise dispose d'une adresse IP publique, 209.165.200.225, utilisée pour l'adresse IP publique de l'appliance de sécurité et du serveur Web. L'administrateur configure le port configurable à utiliser comme port DMZ. Une règle de pare-feu autorise le trafic HTTP entrant sur le serveur Web à l'adresse 172.16.2.30. Les utilisateurs d'Internet entrent le nom de domaine associé à l'adresse IP 209.165.200.225 et peuvent alors se connecter au serveur Web. La même adresse IP est utilisée pour l'interface WAN.

Figure 2 Exemple de DMZ avec deux adresses IP publiques



Dans ce scénario, le FAI a émis deux adresses IP statiques : 209.165.200.225 et 209.165.200.226. L'adresse 209.165.200.225 est utilisée pour l'adresse IP publique de l'appliance de sécurité. L'administrateur configure le port configurable à utiliser comme port DMZ et crée une règle de pare-feu pour autoriser le trafic HTTP entrant sur le serveur Web à l'adresse 172.16.2.30. La règle de pare-feu spécifie l'adresse IP externe 209.165.200.226. Les utilisateurs d'Internet entrent le nom de domaine associé à l'adresse IP 209.165.200.226 et peuvent alors se connecter au serveur Web.

Configuration d'une DMZ

ÉTAPE 1 Pour ajouter une nouvelle DMZ, cliquez sur **Add**. Pour modifier les paramètres d'une DMZ, cliquez sur l'icône **Edit** (crayon).

Autres options : pour supprimer une DMZ, cliquez sur l'icône **Delete** (x).

ÉTAPE 2 Dans l'onglet **Basic Settings,** entrez les informations suivantes :

- **Name** : entrez le nom de la DMZ.
- **IP Address** : entrez l'adresse IP de sous-réseau de la DMZ.
- **Netmask** : entrez le masque de sous-réseau de la DMZ.
- **Spanning Tree** : cochez cette case pour activer la fonctionnalité Spanning Tree afin de déterminer s'il existe des boucles dans la topologie de réseau.
- **Port** : spécifiez un port configurable comme port DMZ. Le trafic via le port DMZ est dirigé vers la DMZ. Tous les ports configurables disponibles apparaissent dans la liste **Port**. Choisissez un port dans la liste **Port** et ajoutez-le à la liste **Member**. Le port configurable sélectionné sera défini comme port DMZ.

  REMARQUE : Ce paramètre modifie le type de port et le mode d'accès du port configurable sélectionné. La modification du type de port élimine l'ensemble de la configuration relative au port physique.
- **Zone** : choisissez la zone DMZ par défaut ou une zone DMZ personnalisée à laquelle la DMZ est mappée. Vous pouvez cliquer sur le lien **Create Zone** pour afficher, modifier ou ajouter les zones sur l'Cisco ISA500.

ÉTAPE 3 Dans l'onglet **DHCP Pool Settings**, choisissez le mode DHCP dans la liste déroulante **DHCP Mode**.

- **Disable** : choisissez cette option si les ordinateurs de la DMZ sont configurés avec des adresses IP statiques ou pour utiliser un autre serveur DHCP.
- **DHCP Server** : permet à l'Cisco ISA500 d'agir en tant que serveur DHCP et affecte les adresses IP à tous les périphériques connectés à la DMZ. Tout nouveau client DHCP se connectant à la DMZ reçoit une adresse IP du pool DHCP.
- **DHCP Relay** : permet à l'Cisco ISA500 d'utiliser un relais DHCP. Si vous choisissez le relais DHCP, entrez l'adresse IP du serveur DHCP distant dans le champ **Relay IP**.

ÉTAPE 4 Si vous choisissez **DHCP Server** comme mode DHCP, entrez les informations suivantes :

- **Start IP** : entrez l'adresse IP de début de la plage DHCP.
- **End IP** : entrez l'adresse IP de fin de la plage DHCP.

  REMARQUE : Les adresses IP de départ et de fin doivent être dans le même sous-réseau que l'adresse IP de la DMZ.

- **Lease Time** : entrez la durée de connexion maximale de « location » d'une adresse IP dynamique à un utilisateur du réseau. Lorsque le temps s'est écoulé, l'adresse IP dynamique de l'utilisateur est automatiquement renouvelée.
- **DNS 1** : entrez l'adresse IP du serveur DNS principal.
- **DNS 2** : entrez éventuellement l'adresse IP du serveur DNS secondaire.
- **WINS 1** : entrez éventuellement l'adresse IP du serveur WINS principal.
- **WINS 2** : entrez éventuellement l'adresse IP du serveur WINS secondaire.
- **Domain Name** : entrez éventuellement le nom de domaine de la DMZ.
- **Default Gateway** : entrez l'adresse IP de la passerelle par défaut.
- **Option 66** : fournit les informations d'adresse du serveur de mise en service aux hôtes qui en font la demande. Prend en charge uniquement l'adresse IP ou le nom d'hôte d'un seul serveur TFTP. Entrez l'adresse IP du serveur TFTP du DMZ.
- **Option 67** : fournit un nom de fichier de configuration ou d'amorçage aux hôtes qui en font la demande. Cette option est utilisée conjointement avec l'option 66 pour permettre au client de formuler une demande TFTP appropriée pour le fichier. Entrez le nom de fichier de configuration ou d'amorçage sur le serveur TFTP spécifié.
- **Option 150** : prend en charge une liste de serveurs TFTP (2 serveurs TFTP). Entrez les adresses IP des serveurs TFTP. Vous pouvez indiquer plusieurs entrées séparées par une virgule (,).

ÉTAPE 5 Dans l'onglet **IPv6 Setting**, spécifiez l'adressage IPv6 de la DMZ si vous activez le mode IPv4/IPv6.

- **IPv6 Address** : entrez l'adresse IPv6 en fonction des exigences de votre réseau.
- **IPv6 Prefix Length** : entrez le nombre de caractères du préfixe IPv6.

  Le réseau IPv6 (sous-réseau) est identifié par le préfixe, qui est composé des bits initiaux de l'adresse. La longueur du préfixe par défaut est de 64 bits. Tous les hôtes du réseau possèdent des bits initiaux identiques pour l'adresse IPv6. Le nombre de bits initiaux communs des adresses est défini par le champ de longueur du préfixe.

ÉTAPE 6 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 7 Cliquez sur **Save** pour appliquer vos paramètres.

ÉTAPE 8 Si vous souhaitez réserver certaines adresses IP pour des périphériques spécifiés, accédez à la page Networking > DHCP Reservations. Voir **Configuration des IP DHCP réservés, page 155**. Vous devez activer le mode DHCP Server ou DHCP Relay à cet effet.

Configuration des zones

Utilisez la page Networking > Zones pour configurer une zone de sécurité, qui est un groupe d'interfaces auxquelles une politique de sécurité peut être appliquée. Les interfaces d'une zone partagent des fonctionnalités communes. Par exemple, deux interfaces connectées au LAN local peuvent être placées dans une zone de sécurité et les interfaces connectées à Internet peuvent être placées dans une autre zone de sécurité.

Les interfaces sont des interfaces basées sur IP (VLAN, WAN1, WAN2, etc.). Chaque interface ne peut se connecter qu'à une zone, mais chaque zone avec un niveau de sécurité spécifique peut avoir plusieurs interfaces.

Reportez-vous aux rubriques suivantes :

- **Niveaux de sécurité des zones, page 152**
- **Zones prédéfinies, page 153**
- **Configuration des zones, page 154**

REMARQUE Nous vous recommandons de configurer les zones avant de configurer le WAN, le VLAN, la DMZ, le pare-feu basé sur les zones et les services de sécurité.

Niveaux de sécurité des zones

Le niveau de sécurité de la zone définit le niveau de confiance accordée à cette zone. L'Cisco ISA500 prend en charge cinq niveaux de sécurité pour les zones comme indiqué ci-dessous. Plus la valeur est grande, plus le niveau d'autorisation est élevé. Les zones VPN et SSLVPN prédéfinies ont le même niveau de sécurité.

- **Trusted(100)** : propose le niveau de confiance le plus élevé. La zone LAN est toujours fiable.
- **VPN(75)** : propose un niveau de confiance plus élevé qu'une zone publique, mais plus bas qu'une zone fiable, utilisé exclusivement par les zones VPN et SSLVPN prédéfinies. L'ensemble du trafic à destination et en provenance d'une zone VPN est chiffré.

- **Public(50)** : propose un niveau de confiance plus élevé qu'une zone invitée, mais plus bas qu'une zone VPN. La zone DMZ est une zone publique.
- **Guest(25)** : propose un niveau de confiance plus élevé qu'une zone non fiable, mais plus bas qu'une zone publique. Les zones invitées ne peuvent être utilisées que pour l'accès invité.
- **Untrusted(0)** : propose le niveau de confiance le plus de bas. Il est utilisé par le WAN et les zones virtuelles de multidiffusion. Vous pouvez mapper le port WAN à une zone non fiable.

Zones prédéfinies

L'Cisco ISA500 prédéfinit les zones suivantes avec différents niveaux de sécurité :

- **WAN** : la zone WAN est une zone non fiable. Par défaut, le port WAN1 est mappé à la zone WAN. Si le WAN (WAN2) secondaire s'applique, il peut être mappé à la zone WAN ou à toute autre zone non fiable.
- **LAN** : la zone LAN est une zone fiable. Vous pouvez mapper un ou plusieurs VLAN à une zone fiable. Par défaut, le VLAN PAR DÉFAUT est mappé à la zone LAN.
- **DMZ** : la zone DMZ est une zone publique utilisée pour les serveurs publics que vous hébergez dans les réseaux DMZ.
- **SSLVPN** : la zone SSLVPN est une zone virtuelle utilisée pour simplifier les connexions VPN SSL sécurisées et à distance. Cette zone n'a pas de port physique attribué.
- **VPN** : la zone VPN est une zone virtuelle utilisée pour simplifier les connexions VPN IPsec sécurisées. Cette zone n'a pas de port physique attribué.
- **INVITÉ** : la zone INVITÉ ne peut être utilisée que pour l'accès invité. Par défaut, le VLAN INVITÉ est mappé à cette zone.
- **VOICE** : la zone VOIX est une zone de sécurité conçue pour le trafic voix. Le trafic entrant et sortant de cette zone est optimisé pour les opérations de voix. Si vous possédez des périphériques de voix, tels que le Cisco IP Phone, il est souhaitable de placer les périphériques dans la zone VOIX.

Configuration des zones

Cette section décrit comment configurer sur les zones sur l'Cisco ISA500. Vous pouvez restaurer la configuration des zones et revenir aux paramètres d'usine par défaut, modifier les paramètres des zones prédéfinies (sauf pour les zones VPN et SSLVPN), ou personnaliser de nouvelles zones pour répondre à vos besoins professionnels spécifiques.

REMARQUE Vous pouvez cliquer sur **Reset** pour restaurer la configuration des zones et revenir aux paramètres d'usine par défaut. Une fois cette opération effectuée, toutes les zones personnalisées sont supprimées et les paramètres relatifs à ces zones personnalisées sont effacés.

ÉTAPE 1 Pour ajouter une nouvelle zone, cliquez sur **Add**. Pour modifier une entrée, cliquez sur l'icône **Edit** (crayon).

Autres options : pour supprimer une entrée, cliquez sur l'icône **Delete** (x). Pour supprimer plusieurs entrées, cochez-les et cliquez sur **Delete**.

REMARQUE : Toutes les zones prédéfinies (à l'exception de la zone VOIX) ne peuvent pas être supprimées. Seuls les ports et les VLAN associés des zones prédéfinies (à l'exception des zones VPN et SSLVPN) peuvent être modifiés.

ÉTAPE 2 Entrez les informations suivantes :

- **Name** : entrez le nom de la zone.
- **Security Level** : spécifiez le niveau de sécurité de la zone.
  - Pour les VLAN, tous les niveaux de sécurité peuvent être sélectionnés.
  - Pour les DMZ, choisissez Public(50).
  - Pour les ports WAN, choisissez Untrusted(0).
- **Map interfaces to this zone** : choisissez les VLAN ou les ports WAN existants dans la liste **Available Interfaces** et cliquez sur la flèche droite pour les ajouter à la liste **Mapped to Zone**. Vous pouvez mapper jusqu'à 16 VLAN à une zone.

ÉTAPE 3 Cliquez sur **OK** pour enregistrer vos paramètres et fermer la fenêtre contextuelle.

ÉTAPE 4 Cliquez sur **Save** pour appliquer vos paramètres.

REMARQUE Étapes suivantes :

- Une fois que vous avez créé une nouvelle zone, un certain nombre de règles de pare-feu est automatiquement généré afin d'autoriser ou de bloquer le trafic de la nouvelle zone vers d'autres zones ou d'autres zones vers la nouvelle zone. L'action d'autorisation ou de blocage est déterminée par le niveau de sécurité de la nouvelle zone. Par défaut, le pare-feu bloque l'ensemble du trafic entrant et autorise l'ensemble du trafic sortant. Pour personnaliser les règles de pare-feu de la nouvelle zone, accédez à la page Firewall > Access Control > ACL Rules. Pour obtenir des informations sur la configuration des règles de pare-feu, voir **Configuration des règles de pare-feu pour contrôler le trafic entrant et sortant, page 216**.
- Appliquez les services de sécurité aux zones si vous activez les services de sécurité tels que la prévention des intrusions (IPS), l'antivirus et le contrôle des applications sur l'Cisco ISA500. Pour plus d'informations, voir **Chapitre?7, « Services de sécurité. »**

Configuration des IP DHCP réservés

Utilisez la page Networking > DHCP Reservations pour réserver certaines adresses IP pour les périphériques spécifiés, identifiés par leurs adresses MAC. Dès que le serveur DHCP reçoit une demande d'un périphérique, l'adresse matérielle est comparée à la base de données. Si le périphérique est détecté, l'adresse IP réservée est utilisée. Sinon, une adresse IP est attribuée automatiquement depuis le pool DHCP.

ÉTAPE 1 Pour ajouter une règle DHCP Reservation, cliquez sur **Add**. Pour modifier une entrée, cliquez sur l'icône **Edit** (crayon).

Autres options : pour supprimer une entrée, cliquez sur l'icône **Delete** (x).

La fenêtre DHCP IP Reservation - Add/Edit s'ouvre.

ÉTAPE 2 Entrez les informations suivantes :

- **Name** : entrez le nom de la règle DHCP Reservation.
- **MAC Address** : entrez l'adresse MAC de l'hôte sous un VLAN.
- **IP Address** : Entrez l'adresse IP attribuée à l'hôte. Cette adresse doit se situer dans le pool DHCP du VLAN.

ÉTAPE 3 Cliquez sur **OK** pour enregistrer vos paramètres et fermer la fenêtre contextuelle.

ÉTAPE 4 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration du routage

Cette section fournit des informations sur la configuration du mode de routage entre les réseaux WAN et LAN, l'affichage de la table de routage et la configuration du routage statique, du routage dynamique et des paramètres PBR. Reportez-vous aux rubriques suivantes :

- **Affichage de la table de routage, page 156**
- **Configuration du mode de routage, page 157**
- **Configuration du routage statique, page 157**
- **Configuration du routage dynamique - RIP, page 158**
- **Configuration du PBR, page 159**

Affichage de la table de routage

Utilisez la page **Networking > Routing > Routing Table** pour afficher les informations suivantes :

- **Destination Address** : adresse IP de l'hôte ou du réseau vers laquelle la route mène.
- **Subnetwork Mask** : masque de sous-réseau du réseau de destination.
- **Gateway** : adresse IP de la passerelle via laquelle l'hôte ou le réseau de destination sont accessibles.
- **Flags** : indicateur d'état de la route.
- **Metric** : coût d'une route. Les mesures de routage sont affectées aux routes par des protocoles de routage afin de fournir des valeurs mesurables qui peuvent être utilisées pour apprécier l'utilité (ou le faible coût) d'une route.
- **Interface** : port physique via lequel cette route est accessible.

Cette page est automatiquement mise à jour toutes les 10 secondes. Cliquez sur **Refresh** pour actualiser manuellement la table de routage.

Configuration du mode de routage

Utilisez la page **Networking > Routing > Routing Mode** pour activer ou désactiver le mode de routage, en fonction des exigences de votre FAI. Par défaut, le mode de routage est désactivé.

ÉTAPE 1 Activez ou désactivez le mode de routage :

- Si votre FAI attribue une adresse IP pour chaque ordinateur que vous utilisez, cliquez sur **On** pour activer le mode de routage.
- Si vous partagez des adresses IP sur plusieurs périphériques tels que votre LAN et que vous utilisez d'autres périphériques dédiés pour la DMZ, cliquez sur **Off** pour désactiver le mode de routage.

ÉTAPE 2 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration du routage statique

Utilisez la page Networking > Routing > Static Routing pour configurer des routes statiques. Vous pouvez également affecter une priorité, qui détermine la sélection de la route lorsqu'il existe plusieurs routes se déplaçant vers la même destination.

REMARQUE Vous pouvez configurer jusqu'à 150 règles de routage statique sur l'Cisco ISA500.

ÉTAPE 1 Pour ajouter une route statique, cliquez sur **Add**. Pour modifier une entrée, cliquez sur l'icône **Edit** (crayon).

Autres options : pour supprimer une entrée, cliquez sur l'icône **Delete** (x). Pour supprimer plusieurs entrées, cochez-les et cliquez sur **Delete**.

ÉTAPE 2 Entrez les informations suivantes :

- **Destination Address** : choisissez un objet d'adresse existant pour l'hôte ou pour le réseau vers lequel la route mène. Si l'objet d'adresse que vous souhaitez ne figure pas dans la liste, choisissez **Create a new address** pour créer un nouvel objet d'adresse. Pour gérer les objets d'adresse, accédez à la page Networking > Address Management. Voir **Gestion d'adresse, page 182**.
- **Setting as default route** : cochez cette case pour configurer cette route statique comme route par défaut.

- **Next Hop** : choisissez un port ou une adresse IP comme saut suivant pour cette route statique.
  - **Interface** : choisissez le WAN1 ou le WAN2 comme saut suivant.
  - **IP Address** : choisissez une adresse IP de la passerelle via laquelle l'hôte de destination ou du réseau peuvent être atteints.
- **Metric** : entrez éventuellement un numéro pour gérer la priorité de la route. S'il existe plusieurs routes pour la même destination, la route avec la plus petite mesure est sélectionnée.

ÉTAPE 3 Cliquez sur **OK** pour enregistrer vos paramètres et fermer la fenêtre contextuelle.

ÉTAPE 4 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration du routage dynamique - RIP

Utilisez la page Networking > Routing > Dynamic - RIP pour configurer le routage dynamique ou le RIP. Le RIP est un protocole IGP (Interior Gateway Protocol) qui est généralement utilisé dans les réseaux internes. Il permet à un routeur d'échanger automatiquement ses informations de routage avec d'autres routeurs et de régler de manière dynamique ses tables de routage en s'adaptant aux modifications du réseau.

ÉTAPE 1 En haut de la page, entrez les informations suivantes :

- **RIP Enable** : cliquez sur **On** pour activer le protocole RIP ou sur **Off** pour le désactiver. Par défaut, le protocole RIP est désactivé.
- **RIP Version** : si vous activez le protocole RIP, spécifiez la version. L'Cisco ISA500 prend en charge les versions 1 et 2 du protocole RIP.
  - **RIP Version 1** est une version de routage basée sur les classes qui n'inclut pas les informations de sous-réseau. C'est la version la plus souvent prise en charge.
  - **RIP Version 2** inclut toutes les fonctionnalités de RIPv1 et prend en charge les informations de sous-réseau.
  - **Default** : les données sont envoyées au format de la version 1 du protocole RIP et reçues au format de la version 1 et 2. Il s'agit du paramètre par défaut.

ÉTAPE 2 Dans le tableau, spécifiez les paramètres du protocole RIP pour chaque interface disponible :

- **RIP Enable** : cochez cette case pour activer les paramètres du protocole RIP sur le port ou le VLAN.
- **Authentication** : si vous utilisez la version 2 du protocole RIP, cliquez sur l'icône **Edit** (crayon) pour indiquer la méthode d'authentification du port ou du VLAN.
  - **None** : choisissez cette option pour invalider l'authentification.
  - **Simple Password Authentication** : choisissez cette option pour valider l'authentification par mot de passe simple. Entrez le mot de passe dans le champ.
  - **MD5 Authentication** : choisissez cette option pour valider l'authentification MD5. Entrez l'ID de clé unique dans le champ **MD5 Key ID** et la clé dans le champ **MD5 Auth Key**.
- **Port Passive** : détermine comment l'Cisco ISA500 reçoit les paquets RIP. Cochez cette case pour activer cette fonctionnalité sur le port ou le VLAN.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration du PBR

Utilisez la page Networking > Routing > Policy Based Routing pour configurer le PBR. Ce dernier spécifie l'IP et/ou le service interne passant via un port WAN spécifié pour fournir des capacités de traitement du trafic plus souples et plus granulaires. Vous pouvez configurer jusqu'à 100 règles de PBR sur l'Cisco ISA500.

Cette fonctionnalité peut être utilisée pour isoler le trafic entre des liaisons avec des vitesses différentes. Le trafic de gros volume peut être acheminé via le port connecté à une liaison à haut débit et le trafic de faible volume via le port connecté à la liaison lente. Par exemple, même si le trafic HTTP est généralement acheminé via le WAN1, à l'aide du PBR vous pouvez lier le protocole HTTP au WAN1 et le protocole FTP au WAN2. Dans ce cas, l'Cisco ISA500 transporte automatiquement les données FTP via le WAN2.

Si plusieurs fonctionnalités de routage fonctionnent simultanément, l'Cisco ISA500 fait correspondre en premier les règles de PBR, puis les règles de Static Routing et celles de routage par défaut. Par exemple, si la redondance du WAN est définie comme mode Weighted Dual WAN Settings et que les règles de PBR et de Static Routing sont configurées, la priorité de routage fonctionne comme suit :

1. Si le trafic ne peut pas correspondre aux règles de routage basé sur les stratégies ou celles de routage statique, le trafic suit les paramètres d'équilibrage de charge pondéré.
2. Si le trafic A correspond aux règles de PBR ou de Static Routing, il est tout d'abord géré par les règles de PBR ou de Static Routing, alors que le reste du trafic suit les paramètres de Weighted Dual WAN Settings.

REMARQUE Veillez à configurer une connexion WAN secondaire et à définir la redondance du WAN comme mode Dual WAN Settings ou Routing Table avant de configurer les paramètres de PBR.

ÉTAPE 1 Cliquez sur **On** pour activer le PBR ou sur **Off** pour le désactiver.

ÉTAPE 2 Pour ajouter une nouvelle règle de PBR, cliquez sur **Add**. Pour modifier une entrée, cliquez sur l'icône **Edit** (crayon).

Autres options : pour supprimer une entrée, cliquez sur l'icône **Delete** (x).

ÉTAPE 3 Entrez les informations suivantes :

- **From** : choisissez le VLAN d'où provient le trafic.
- **Service** : pour la liaison de service uniquement, sélectionnez un service existant. Pour la liaison IP uniquement, sélectionnez **All Traffic**. Si le service que vous souhaitez ne figure pas dans la liste, sélectionnez **Create a new service** pour créer un nouvel objet de service. Pour gérer les objets de service, accédez à la page Networking > Service Management. Voir **Gestion des services, page 184**.
- **Source IP** : pour la liaison de service uniquement, sélectionnez **Any**. Pour la liaison IP uniquement, sélectionnez l'adresse IP source pour le trafic sortant. Si l'objet d'adresse que vous souhaitez ne figure pas dans la liste, choisissez **Create a new address** pour créer un nouvel objet d'adresse. Pour gérer les objets d'adresse, accédez à la page Networking > Address Management. Voir **Gestion d'adresse, page 182**.
- **Destination IP** : pour la liaison de service uniquement, sélectionnez **Any**. Pour la liaison IP uniquement, sélectionnez l'adresse IP de destination pour le trafic sortant.
- **DSCP** : choisissez la valeur DSCP pour définir le niveau de priorité du trafic.

- **Route to** : choisissez le port WAN vers lequel le trafic sortant est acheminé.
- **Failover** : cliquez sur **On** pour activer le basculement WAN ou sur **Off** pour le désactiver. Lorsque le port WAN sélectionné pour le routage est en panne, l'activation du basculement transfère le trafic au WAN de secours.

  REMARQUE : Lorsqu'une connexion WAN est en panne (une défaillance de connexion est détectée par le test ping ou la requête DNS) et que la fonctionnalité de basculement du PBR est désactivée, le trafic est abandonné.

ÉTAPE 4 Cliquez sur **OK** pour enregistrer vos paramètres et fermer la fenêtre contextuelle.

ÉTAPE 5 Cliquez sur **Save** pour appliquer vos paramètres.

REMARQUE : Après l'application de vos paramètres, les paramètres PBR modifiés prennent immédiatement effet pour toutes les nouvelles sessions, mais pas pour les sessions existantes. Vous pouvez effacer manuellement les sessions existantes sur la page Firewall > Session Limits pour appliquer immédiatement les paramètres PBR à toutes les nouvelles sessions.

Configuration de la qualité de service

La fonctionnalité Qualité de service (QoS) est appliquée à l'ensemble du réseau afin de garantir que le trafic réseau soit hiérarchisé en fonction des critères requis et qu'il fasse l'objet d'un traitement préférentiel.

Les garanties de la QoS sont importantes si la capacité du réseau est insuffisante. C'est le cas pour les applications multimédias de diffusion en continu et en temps réel telles que la voix sur IP, les jeux en ligne et l'IPTV, qui sont sensibles aux retards et nécessitent souvent un débit binaire fixe.

Reportez-vous aux rubriques suivantes :

- **Paramètres QoS généraux, page 162**
- **Configuration de la QoS WAN, page 162**
- **Configuration de la QoS LAN, page 174**
- **Configuration de la QoS sans fil, page 176**

Paramètres QoS généraux

Utilisez la page General Settings pour activer ou désactiver les fonctionnalités de QoS WAN, du LAN et du WLAN.

ÉTAPE 1 Cliquez sur **Networking > QoS > General Settings**.

ÉTAPE 2 Entrez les informations suivantes :

- **WAN QoS** : cochez cette case pour activer la fonctionnalité QoS WAN. Par défaut, la QoS WAN est désactivée.
- **LAN QoS** : cochez cette case pour activer la fonctionnalité QoS LAN. La QoS LAN spécifie les valeurs de priorité qui peuvent être utilisées pour différencier le trafic et donner la préférence au trafic de priorité plus élevée, par exemple les appels téléphoniques. Par défaut, la QoS LAN est désactivée.
- **Wireless QoS** : cochez cette case pour activer le QoS sans fil. La QoS sans fil contrôle la différenciation de priorité pour les paquets de données dans le sens de sortie sans fil. Par défaut, la QoS sans fil est désactivée. La QoS sans fil ne s'applique qu'à l'ISA550W et l'ISA570W.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration de la QoS WAN

Cette section décrit comment configurer la QoS WAN. Reportez-vous aux rubriques suivantes :

- **Gestion de la bande passante WAN pour le trafic en amont, page 163**
- **Configuration des paramètres de file d'attente WAN, page 163**
- **Configuration des sélecteurs de trafic, page 165**
- **Configuration des profils de la stratégie QoS WAN, page 167**
- **Configuration des règles de classe QoS WAN, page 167**
- **Mappage des profils de stratégie QoS WAN aux interfaces WAN, page 168**
- **Exemple de configuration de QoS WAN, page 169**

- Configuration de la QoS WAN pour le trafic voix du LAN au WAN, page 171
- Configuration de la QoS WAN pour le trafic voix du WAN au LAN, page 173

Gestion de la bande passante WAN pour le trafic en amont

Utilisez la page Bandwidth pour spécifier la bande passante maximale autorisée pour le trafic en amont sur chaque interface WAN.

ÉTAPE 1 Cliquez sur **Networking > QoS > WAN QoS > Bandwidth**.

ÉTAPE 2 Entrez la quantité de bande passante maximale autorisée pour le trafic en amont sur chaque interface WAN. La valeur par défaut est de 0 kbit/s, ce qui signifie qu'il n'y a aucune limite pour le trafic en amont.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration des paramètres de file d'attente WAN

Utilisez la page Queue Settings pour déterminer comment gérer le trafic des files d'attente pour chaque port WAN. L'Cisco ISA500 prend en charge six files d'attente pour les ports WAN, Q1 à Q6. Il existe trois façons de déterminer comment gérer le trafic des files d'attente :

Strict Priority (SP)	Le trafic de sortie de la file d'attente avec le niveau de priorité le plus élevé (Q1) est transmis en premier. Le trafic des files d'attente avec un niveau de priorité plus faible est traité uniquement après la transmission de la file d'attente avec le niveau de priorité le plus élevé. De cette façon, le niveau de priorité de trafic le plus élevé est donné à la file d'attente portant le numéro le plus élevé.

Weighted Round Robin (WRR)	Distribue la bande passante entre les classes en utilisant le schéma de Round Robin pondérée. Les pondérations décident du rythme avec lequel chaque file d'attente peut envoyer les paquets. En mode WRR, le nombre de paquets envoyés depuis la file d'attente est proportionnel à la pondération de la file d'attente. Plus la pondération est élevée, plus le nombre de trames envoyées est important.
Low Latency Queuing (LLQ)	Intègre les files d'attente SP et WRR pour fournir une Strict Priority Queuing (PQ) à la Class-Based Weighted Fair Queuing (CBWFQ). Grâce à la LLQ, les données sensibles aux retards (telles que le trafic voix) bénéficient d'un traitement préférentiel par rapport à d'autres trafics et peuvent être retirées de la file d'attente et envoyées en premier.

ÉTAPE 1 Cliquez sur **Networking > QoS > WAN QoS > Queue Settings**.

ÉTAPE 2 Spécifiez comment gérer le trafic des files d'attente pour chaque port WAN.

- **Strict Priority (SP)** : définissez l'ordre de traitement des files d'attente. La planification du trafic pour la file d'attente sélectionnée et pour toutes files d'attente avec un niveau de priorité plus élevé est strictement basée sur la priorité de la file d'attente. Elle commence par Q1 (file d'attente avec le niveau de priorité le plus élevé) et passe à la file d'attente suivante avec un niveau de priorité plus faible lorsque chaque file d'attente est terminée.
- **Weighted Round Robin (WRR)** : entrez la pondération WRR, en pourcentage, attribué aux files d'attente que vous souhaitez utiliser. La planification du trafic pour la file d'attente sélectionnée est basée sur la WRR.
- **Latency Queuing (LLQ)** : appliquez le mode SP à Q1 et le mode WRR à d'autres files d'attente (Q2 à Q6). Q1 a le niveau de priorité le plus élevé et est toujours traitée pour se terminer avant les files d'attente avec des niveaux de priorité inférieurs. Si vous choisissez la LLQ, entrez la quantité de bande passante affectée à Q1 et les pondérations WRR des autres files d'attente que vous souhaitez utiliser.

ÉTAPE 3 Si nécessaire, entrez une brève description de chaque file d'attente dans le champ de la colonne **Queue Description**.

ÉTAPE 4 Dans la zone **Random Early Detection**, cliquez sur **On** pour activer le mécanisme de détection précoce aléatoire (RED) ou sur **Off** pour le désactiver. RED est un mécanisme permettant d'éviter la congestion et tire parti du mécanisme de contrôle de congestion du protocole TCP. En abandonnant les paquets de façon aléatoire avant les périodes de forte congestion, RED indique à la source du paquet de diminuer sa vitesse de transmission. En supposant que la source du paquet utilise le protocole TCP, il réduit sa vitesse de transmission jusqu'à ce que tous les paquets atteignent leur destination, indiquant que la congestion est effacée.

ÉTAPE 5 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration des sélecteurs de trafic

Le sélecteur de trafic (ou la classification du trafic) est utilisé pour le classement du trafic via des interfaces WAN dans une classe de trafic donnée afin d'identifier le trafic qui doit être géré.

REMARQUE Vous pouvez configurer jusqu'à 256 sélecteurs de trafic sur l'Cisco ISA500.

ÉTAPE 1 Cliquez sur **Networking > QoS > WAN QoS > Traffic Selector (Classification)**.

La fenêtre Traffic Selector (Classification) s'ouvre.

ÉTAPE 2 Pour ajouter un nouveau sélecteur de trafic, cliquez sur **Add**.

Autres options : pour modifier une entrée, cliquez sur l'icône **Edit** (crayon). Pour supprimer une entrée, cliquez sur l'icône **Delete** (x).

La fenêtre Traffic Selector - Add/Edit s'ouvre.

ÉTAPE 3 Entrez les informations suivantes :

- **Class Name** : entrez un nom descriptif pour la classe de trafic.
- **Source Address** : choisissez **Any** ou une adresse ou un groupe d'adresse (réseau) existant d'où provient le trafic.
- **Destination Address** : choisissez **Any** ou une adresse ou un groupe d'adresses (réseau) existant où le trafic est dirigé.

  Si les objets d'adresse que vous souhaitez ne figurent pas dans la liste, sélectionnez **Create a new address group** pour créer un nouvel objet de groupe d'adresses ou **Create a new address** pour créer un nouvel objet

d'adresse. Pour gérer les objets d'adresses ou de groupes d'adresses, accédez à la page Networking > Address Management. Voir **Gestion d'adresse, page 182**.

- **Source Service** sélectionnez **Any** ou un service existant dans la liste déroulante.
- **Destination Service** sélectionnez **Any** ou un service existant dans la liste déroulante.

  Si les objets de service que vous souhaitez ne figurent pas dans la liste, sélectionnez **Create a new service** pour créer un nouvel objet de service. Pour gérer les objets de service, accédez à la page Networking > Service Management. Voir **Gestion des services, page 184**.
- **DSCP** : DSCP est un champ dans un paquet IP qui permet d'attribuer différents niveaux de service au trafic réseau. Sélectionnez les valeurs DSCP pour la classe de trafic et cliquez sur la flèche droite.
- **CoS** : la classe de service (CoS) IEEE 802.1p basée sur la QoS indique une valeur de priorité entre 0 et 7, qui peut être utilisée pour différencier le trafic et donner la préférence au trafic avec un niveau de priorité plus élevé. Choisissez la valeur CoS pour la classe de trafic.
- **VLAN** : choisissez le VLAN d'identification de l'hôte auquel doit s'appliquer le sélecteur de trafic.

  REMARQUE : le trafic correspondant aux paramètres ci-dessus est classé dans une classe à des fins de gestion.

ÉTAPE 4 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration des profils de la stratégie QoS WAN

Utilisez la page QoS Policy Profile pour configurer les profils de stratégie basés sur les classes afin de gérer le trafic via les interfaces WAN.

REMARQUE Jusqu'à 32 profils de stratégie QoS WAN peuvent être configurés sur l'Cisco ISA500.

ÉTAPE 1 Cliquez sur **Networking > QoS > WAN QoS > QoS Policy Profile**.

ÉTAPE 2 Pour ajouter un nouveau profil de stratégie QoS WAN, cliquez sur **Add**.

Autres options : pour modifier une entrée, cliquez sur l'icône **Edit** (crayon). Pour supprimer une entrée, cliquez sur l'icône **Delete** (x).

La fenêtre QoS Policy - Add/Edit s'ouvre.

ÉTAPE 3 Entrez les informations suivantes :

- **Policy Name** : entrez le nom du profil de stratégie QoS WAN.
- **Apply this policy to** : cliquez sur **Inbound Traffic** pour appliquer ce profil de stratégie au trafic entrant ou sur **Outbound Traffic** pour l'appliquer au trafic sortant.

ÉTAPE 4 Spécifiez les paramètres QoS des classes de trafic que vous voulez associer au profil de stratégie. Pour plus d'informations, voir **Configuration des règles de classe QoS WAN, page 167**.

ÉTAPE 5 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 6 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration des règles de classe QoS WAN

Cette section décrit comment configurer les règles de classe QoS que vous voulez associer au profil de stratégie QoS WAN.

REMARQUE Vous pouvez associer jusqu'à 64 classes de trafic à un profil de stratégie QoS WAN.

ÉTAPE 1 Dans la zone **QoS Class Rules**, cliquez sur **Add** pour ajouter une règle de classe QoS WAN.

La fenêtre QoS Class Rule - Add/Edit s'ouvre.

ÉTAPE 2 Entrez les informations suivantes :

- **Class** : choisissez un sélecteur de trafic existant (classe de trafic) à associer au profil de stratégie.
- **Queue** : pour un profil de stratégie de trafic sortant, choisissez la file d'attente pour l'envoi de paquets appartenant à la classe de trafic sélectionnée. Cette option est désactivée pour un profil de stratégie de trafic entrant.
- **DSCP Marking** : choisissez la valeur de marquage DSCP pour attribuer la priorité au trafic.
- **CoS Marking** : pour un profil de stratégie de trafic entrant, choisissez la valeur de marquage CoS pour attribuer la priorité au trafic entrant. Cette option est désactivée pour un profil de stratégie de trafic sortant.
- **Rate-limiting** : entrez la quantité de limitation de bande passante en kbits/s pour la classe de trafic sélectionnée. Par exemple, si le profil de stratégie est appliqué au trafic entrant, le paramètre de limite de débit ne s'applique qu'au trafic entrant appartenant à la classe sélectionnée. La valeur par défaut est 0 kbits/s, ce qui signifie qu'il n'y a aucune limite.

ÉTAPE 3 Cliquez sur **OK** pour enregistrer vos paramètres.

Mappage des profils de stratégie QoS WAN aux interfaces WAN

Utilisez la page Policy Profile to Interface Mapping pour affecter les profils de stratégie QoS WAN aux interfaces WAN.

ÉTAPE 1 Cliquez sur **Networking > QoS > WAN QoS > Policy Profile to Interface Mapping**.

La fenêtre Policy Profile to Interface Mapping s'ouvre.

ÉTAPE 2 Pour modifier les paramètres de profil de stratégie associés à l'interface WAN, cliquez sur l'icône **Edit** (crayon).

La fenêtre Policy Profile to Interface Mapping - Edit s'ouvre.

ÉTAPE 3 Entrez les informations suivantes :

- **Interface** : nom de l'interface WAN à laquelle les profils de stratégie sont associés.
- **Inbound Policy Name** : sélectionnez un profil de stratégie entrant pour gérer le trafic entrant via l'interface WAN sélectionnée.
- **Outbound Policy Name** : sélectionnez un profil de stratégie sortant pour gérer le trafic sortant via l'interface WAN sélectionnée.

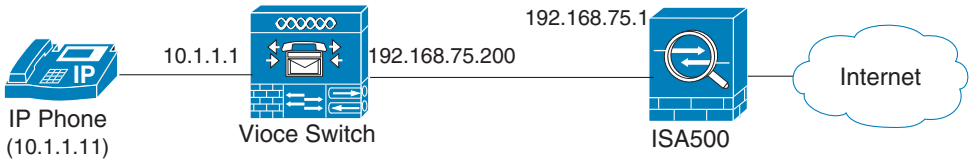
ÉTAPE 4 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 5 Cliquez sur **Save** pour appliquer vos paramètres.

Exemple de configuration de QoS WAN

Cette section présente un exemple de configuration de QoS WAN pour attribuer au trafic voix une priorité plus élevée à un système téléphonique ou aux téléphones SPA via l'Cisco ISA500.

Use Case : un téléphone IP est connecté directement au commutateur de voix derrière l'Cisco ISA500 ou au port LAN de l'Cisco ISA500. Le trafic voix et de données est envoyé via le port WAN de l'Cisco ISA500.



Solution : pour le trafic voix du LAN au WAN (trafic voix sortant), vérifiez que le trafic voix sortant est bien traité par la file d'attente avec le niveau de priorité le plus élevé (Q1) et que l'autre trafic sortant, tel que le trafic de données, est traité par les files d'attente avec des niveaux de priorité inférieurs (Q2 à Q6). Pour le trafic voix du WAN au LAN (trafic voix entrant), la CoS et le DSCP sont marqués afin que le commutateur de voix puisse hiérarchiser le trafic voix entrant par la CoS ou le DSCP entrant.

Effectuez les tâches de configuration suivantes pour donner au trafic voix un niveau de priorité plus élevé :

- Accédez à la page Networking > Routing > Static Routing pour ajouter une règle de routage statique comme suit :

Destination Address	voice_phone_ip **REMARQUE** : Dans ce cas, vous pouvez créer manuellement un objet d'adresse IP appelé « voice_phone_ip »avec l'adresse IP 10.1.1.11 en sélectionnant l'option **Create a new address**.
IP Address	voice_switch_ip **REMARQUE** : Dans ce cas, vous pouvez créer manuellement un objet d'adresse IP appelé « voice_switch_ip »avec l'adresse IP 192.168.75.200 en sélectionnant l'option **Create a new address**.
Metric	1

- Accédez à la page Firewall > NAT > Advanced NAT pour ajouter une règle NAT avancée comme suit pour autoriser le trafic voix et de données via le port WAN (WAN1) de l'appliance de sécurité :

Name	voice_traffic_nat
Enable	On
From	Any
To	WAN1
Original Source Address	voice_phone_ip
Translated Source Address	WAN1_IP

- Accédez à la page Networking > QoS > General Settings pour activer la QoS WAN sur l'Cisco ISA500.
- Accédez à la page Networking > QoS > WAN QoS > Bandwidth pour spécifier la bande passante en amont pour le port WAN.

- Configurez la QoS WAN pour le trafic voix sortant. Pour plus d'informations, voir **Configuration de la QoS WAN pour le trafic voix du LAN au WAN, page 171**.
- Configurez la QoS WAN pour le trafic voix entrant. Pour plus d'informations, voir **Configuration de la QoS WAN pour le trafic voix du WAN au LAN, page 173**.

Configuration de la QoS WAN pour le trafic voix du LAN au WAN

Pour configurer la QoS WAN pour gérer le trafic voix sortant du LAN au WAN, procédez comme suit :

ÉTAPE 1 Accédez à la page Networking > QoS > WAN QoS > Queue Settings pour déterminer comment gérer le trafic des files d'attente pour le port WAN.

a. Sélectionnez la case d'option **Low Latency Queuing (LLQ)**. Grâce à la LLQ, les données sensibles aux retards (telles que le trafic voix) bénéficient d'un traitement préférentiel par rapport à d'autres trafics et peuvent être retirées de la file d'attente et envoyées en premier.

b. Entrez la quantité de bande passante affectée à Q1. Q1 a le niveau de priorité le plus élevé et est toujours traitée pour se terminer avant les files d'attente avec des niveaux de priorité inférieurs.

c. Entrez le pourcentage attribué aux autres files d'attente (Q2 à Q6) que vous souhaitez utiliser.

ÉTAPE 2 Accédez à la page Networking > QoS > WAN QoS > Traffic Selector (Classification) pour ajouter deux sélecteurs de trafic utilisés pour classer le trafic voix et de données sortant.

a. Ajoutez un sélecteur de trafic pour classer le trafic de données sortant en procédant comme suit :

Class Name	data-outbound-class
VLAN	VLAN par défaut

b. Ajoutez un sélecteur de trafic pour classer le trafic voix sortant en procédant comme suit :

Class Name	voice-outbound-class
Source Address	voice_phone_ip

ÉTAPE 3 Accédez à la page Networking > QoS > WAN QoS > QoS Policy Profile pour ajouter un profil de stratégie QoS basé sur les classes afin de gérer le trafic voix et de données sortant via le port WAN.

a. Ajoutez un profil de stratégie de QoS WAN en procédant comme suit :

Policy Name	voice-outbound-profile
Apply this policy to	Outbound Traffic

b. Ajoutez deux règles de classe QoS pour associer les classes de trafic spécifiées au profil de stratégie QoS en procédant comme suit :

Règle 1 de classe QoS	
Classe	Choisissez la classe de trafic appelée « voice-outbound-class ».
File d'attente	Choisissez le niveau de priorité le plus élevé (Q1) pour le trafic voix sortant.
Règle 2 de classe QoS	
Classe	Choisissez la classe de trafic appelée « data-outbound-class ».
File d'attente	Choisissez une file d'attente de Q6 à Q6 pour le trafic de données sortant.

ÉTAPE 4 Accédez à la page Networking > QoS > WAN QoS > Policy Profile to Interface Mapping pour appliquer ce profil de stratégie QoS sur le port WAN. Dans ce cas, sélectionnez le profil de stratégie « voice-outbound-profile » dans la liste déroulante **Outbound Policy Name**.

Configuration de la QoS WAN pour le trafic voix du WAN au LAN

Pour configurer la QoS WAN pour gérer le trafic voix entrant du WAN au LAN, procédez comme suit :

ÉTAPE 1 Accédez à la page Networking > QoS > WAN QoS > Traffic Selector (Classification) pour ajouter un sélecteur de trafic afin de classer le trafic voix entrant en procédant comme suit :

Class Name	voice-inbound-class
Destination Address	voice_phone_ip

ÉTAPE 2 Accédez à la page Networking > QoS > WAN QoS > QoS Policy Profile pour ajouter un profil de stratégie QoS basé sur les classes afin de gérer le trafic voix entrant via le port WAN en procédant comme suit :

Policy Name	voice-inbound-profile
Apply this policy to	Inbound Traffic
Règle de classe QoS	Ajoutez une règle de classe QoS avec les paramètres suivants : ▪ **Class** : choisissez la classe de trafic appelée « voice-inbound-class ». ▪ **DSCP Marking** : choisissez la valeur de marquage DSCP (par exemple, 46) pour le trafic voix entrant selon les paramètres QoS de votre commutateur de voix. ▪ **CoS Marking** : choisissez la valeur de marquage CoS (par exemple, 6) pour le trafic voix entrant selon les paramètres QoS de votre commutateur de voix.

ÉTAPE 3 Accédez à la page Networking > QoS > WAN QoS > Policy Profile to Interface Mapping pour appliquer le profil de stratégie QoS entrant sur le port WAN. Dans ce cas, sélectionnez le profil de stratégie QoS « voice-inbound-profile » dans la liste déroulante **Inbound Policy Name**.

Configuration de la QoS LAN

La QoS LAN spécifie les valeurs de priorité qui peuvent être utilisées pour différencier le trafic et donner la préférence au trafic de priorité plus élevée, par exemple les appels téléphoniques. Reportez-vous aux rubriques suivantes :

- **Configuration des paramètres de file d'attente LAN, page 174**
- **Configuration des méthodes de classification QoS du LAN, page 175**
- **Mappage de la CoS à la file LAN, page 175**
- **Mappage du DSCP à la file LAN, page 176**
- **Configuration de la CoS par défaut, page 176**

Configuration des paramètres de file d'attente LAN

Utilisez la page Queue Settings pour configurer si la planification du trafic sur les interfaces Ethernet est basée sur le SP ou le WRR, ou une combinaison des deux. L'Cisco ISA500 prend en charge quatre files d'attente pour le trafic LAN, Q1 à Q4.

ÉTAPE 1 Cliquez sur **Networking > QoS > LAN QoS > Queue Settings**.

ÉTAPE 2 Indiquez comment déterminer le trafic LAN dans les files d'attente.

- **Strict Priority (SP)** : indique que la planification du trafic pour la file d'attente sélectionnée est strictement basée sur la priorité de la file d'attente.
- **Weighted Round Robin (WRR)** : indique que la planification du trafic de la file d'attente sélectionnée est strictement basée sur les pondérations WRR. Si le WRR est sélectionné, les pondérations prédéterminées 8, 4, 2 et 1 sont affectées respectivement aux files d'attente 1, 2, 3 et 4.
- **SP et WRR** : intègre les files d'attente SP et WRR. Il applique le SP à Q1 et WRR à d'autres files d'attente à (Q2 à Q4). Si vous choisissez SP+WRR, le PQ est attribué à Q1 et les pondérations prédéfinies 4, 2 et 1 sont attribuées à Q2, Q3 et Q4 respectivement. Il n'y a pas de limite pour le PQ, ce qui signifie que les files d'attente WRR peuvent être sous-alimentées si le PQ envoie toujours un trafic plus important que la bande passante maximale des ports LAN.

ÉTAPE 3 Si nécessaire, entrez une brève description de chaque file d'attente dans le champ de la colonne **Queue Description**.

ÉTAPE 4 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration des méthodes de classification QoS du LAN

La classification du trafic est utilisée pour le classement du trafic via les interfaces LAN dans une classe de trafic donnée afin d'identifier le trafic qui doit être géré.

ÉTAPE 1 Cliquez sur **Networking > QoS > LAN QoS > Classification Methods**.

ÉTAPE 2 En fonction de la conception de votre réseau, choisissez la méthode de marquage du trafic Differentiated Services Code Point (DSCP) ou Class of Service (CoS) via toutes les interfaces LAN. Lorsque vous choisissez le DSCP comme méthode de classification, la fonctionnalité Mapping CoS to LAN Queue est grisée. Dans ce cas, la relation de mappage entre les files d'attente LAN et la CoS se définit comme suit :

File d'attente LAN	Valeur CoS
1	6
2	4
3	2
4	0

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Mappage de la CoS à la file LAN

ÉTAPE 1 Cliquez sur **Networking > QoS > LAN QoS > Mapping CoS to Queue**.

ÉTAPE 2 Choisissez la file d'attente de transfert du trafic vers laquelle la valeur de marquage de priorité CoS est mappée. Quatre files d'attente de trafic hiérarchisées sont prises en charge, dans lesquelles Q4 est le niveau de priorité le plus bas et Q1 le plus élevé.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Mappage du DSCP à la file LAN

ÉTAPE 1 Cliquez sur **Networking > QoS > LAN QoS > Mapping DSCP to Queue**.

ÉTAPE 2 Choisissez la file d'attente de transfert du trafic vers laquelle la valeur de marquage de priorité DSCP est mappée. Quatre files d'attente de trafic hiérarchisées sont prises en charge, dans lesquelles Q4 est le niveau de priorité le plus bas et Q1 le plus élevé.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration de la CoS par défaut

Utilisez la page Default CoS pour configurer les valeurs CoS par défaut des paquets entrants via chaque interface LAN. Les valeurs de champ possibles sont comprises entre 0 et 7. La valeur par défaut est de 0.

ÉTAPE 1 Cliquez sur **Networking > QoS > LAN QoS > Default CoS**.

ÉTAPE 2 Entrez les informations suivantes :

- **Default CoS** : choisissez la valeur de marquage de priorité CoS par défaut pour les interfaces LAN, 0 étant le niveau de priorité le plus faible et 7 le plus élevé.
- **Trust** : choisissez **Yes** pour garder la valeur de marquage CoS des paquets via les interfaces LAN ou **No** pour la modifier.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration de la QoS sans fil

La QoS sans fil contrôle la différenciation de priorité pour les paquets de données dans le sens de sortie sans fil. Reportez-vous aux rubriques suivantes :

- **Paramètres par défaut de la QoS sans fil, page 177**
- **Configuration des méthodes de classification QoS sans fil, page 178**
- **Mappage de la CoS à la file d'attente sans fil, page 178**
- **Mappage du DSCP à la file d'attente sans fil, page 178**

Paramètres par défaut de la QoS sans fil

La QoS sans fil utilise la méthode de mise en file d'attente par défaut pour le trafic sans fil. Le trafic sans fil est toujours fiable. Les tableaux ci-dessous affichent les paramètres de mappage par défaut entre 802.1p et 802.1e.

Mappage de 802.1p à IEEE 802.11e

Priorité de 802.1p	Priorité de 802.11e
0	0 (priorité « Au mieux »)
1	1 (priorité d'arrière-plan)
2	2 (priorité d'arrière-plan)
3	4 (priorité de la vidéo)
4	5 (priorité de la vidéo)
5	6 (priorité de la voix)
6	7 (priorité de la voix)
7	7 (priorité de la voix)

Mappage de IEEE 802.11e à 802.1p

Priorité de 802.11e	Priorité de 802.1p
0 (priorité « Au mieux »)	0
1 (priorité d'arrière-plan)	1
2 (priorité d'arrière-plan)	2
3 (priorité « Au mieux »)	0
4 (priorité de la vidéo)	3
5 (priorité de la vidéo)	4
6 (priorité de la voix)	5
7 (priorité de la voix)	6

Configuration des méthodes de classification QoS sans fil

La classification du trafic est utilisée pour le classement du trafic via les SSID dans une classe de trafic donnée afin d'identifier le trafic qui doit être géré.

ÉTAPE 1 Cliquez sur **Networking > QoS > Wireless QoS > Classification Methods**.

ÉTAPE 2 En fonction de la conception de votre réseau, choisissez la méthode de marquage DSCP ou CoS pour le trafic via chaque SSID.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Mappage de la CoS à la file d'attente sans fil

ÉTAPE 1 Cliquez sur **Networking > QoS > Wireless QoS > Mapping CoS to Queue**.

ÉTAPE 2 Choisissez la file d'attente de transfert du trafic vers laquelle la valeur de marquage de priorité CoS est mappée.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Mappage du DSCP à la file d'attente sans fil

ÉTAPE 1 Cliquez sur **Networking > QoS > Wireless QoS > Mapping DSCP to Queue**.

ÉTAPE 2 Choisissez la file d'attente de transfert du trafic vers laquelle la valeur de marquage de priorité DSCP est mappée.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration IGMP

Le protocole IGMP (Internet Group Management Protocol) est un protocole de communication utilisé par les hôtes et les routeurs adjacents sur les réseaux IP pour établir les appartenances aux groupes de multidiffusion. Le protocole IGMP peut être utilisé pour le flux vidéo et les jeux en ligne et permet d'utiliser de façon plus efficace les ressources lors de la prise en charge de ces types d'applications.

Le proxy IGMP active les hôtes qui ne sont pas directement connectés à un routeur en aval pour se connecter à un groupe de multidiffusion provenant d'un réseau en amont. La surveillance IGMP restreint le trafic de diffusion IPv4 à la couche 2 en configurant les ports LAN de la couche 2 de façon dynamique pour transférer le trafic de diffusion IPv4 uniquement vers les ports qui le souhaitent. La surveillance IGMP s'exécute sur le protocole IGMP version 3, qui est rétrocompatible avec les versions précédentes.

REMARQUE Par défaut, le trafic de diffusion de n'importe quelle zone vers n'importe quelle zone est bloqué par le pare-feu. Lorsque vous activez le proxy IGMP et que vous souhaitez recevoir des paquets de multidiffusion du WAN au LAN, vous devez d'abord décocher la case **Block Multicast Packets** dans la page Firewall > Attack Protection, puis créer une règle de pare-feu pour autoriser la multidiffusion du WAN au LAN. Pour obtenir des informations sur la configuration des règles de pare-feu pour autoriser ou refuser le trafic multidiffusion, voir **Configuration d'une règle de pare-feu pour autoriser le trafic de diffusion, page 224** .

ÉTAPE 1 Cliquez sur **Networking > IGMP**.

La fenêtre IGMP s'ouvre.

ÉTAPE 2 Entrez les informations suivantes :

- **IGMP Proxy** : cliquez sur **On** pour activer le proxy IGMP pour que l'Cisco ISA500 puisse servir de proxy pour toutes les requêtes IGMP et communiquer avec les serveurs IGMP du FAI ou sur **Off** pour le désactiver.
- **IGMP Version** : choisissez IGMP version 1 et 2 ou IGMP version 3.
  - **IGMP Version 1** : les hôtes peuvent se connecter à des groupes de multidiffusion. Aucun message de départ. Les routeurs utilisent un mécanisme basé sur le délai d'expiration pour détecter les groupes sans intérêt pour les membres.

- **IGMP Version 2** : les messages de départ sont ajoutés au protocole. La terminaison de l'appartenance au groupe peut donc être signalée rapidement au protocole de routage, ce qui est important pour les groupes et/ou les sous-réseaux de multidiffusion à forte consommation de bande passante appartenant au groupe très volatile.
- **IGMP Version 3** : protocole ayant fait l'objet d'une révision majeure. Il permet aux hôtes de spécifier les listes des hôtes à partir desquels ils souhaitent recevoir du trafic. Le trafic provenant d'autres hôtes est bloqué au sein du réseau. Il permet également aux hôtes de bloquer au sein du réseau les paquets provenant de sources qui envoient du trafic indésirable.

▪ **IGMP Snooping :** la surveillance rationalise le traitement du trafic de diffusion pour les VLAN. En examinant les messages de rapport d'appartenance au groupe IGMP (surveillance) des hôtes intéressés, le trafic de diffusion est limité au sous-réseau des interfaces VLAN sur lesquelles l'hôte réside. La surveillance IGMP permet de réduire la consommation de bande passante pour éviter d'inonder le VLAN entier. Cliquez sur **On** pour activer la surveillance IGMP ou sur **Off** pour la désactiver.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration VRRP

Le protocole de redondance du routeur virtuel (VRRP) est un protocole de redondance pour l'unité d'accès LAN. Il configure un groupe de routeurs (comprenant un routeur principal et plusieurs routeurs de secours) comme routeur virtuel.

ÉTAPE 1 Cliquez sur **Networking > VRRP**.

La fenêtre VRRP s'ouvre.

ÉTAPE 2 Cochez la case à côté de **Enable Virtual Router Redundancy Protocol (VRRP)** pour activer le protocole VRRP ou décochez-la pour la désactiver.

ÉTAPE 3 Si vous activez le protocole VRRP, entrez les informations suivantes :

- **Interface** : port par défaut du routeur virtuel principal (votre Cisco ISA500).
- **Source IP** : adresse IP source du routeur virtuel principal.

REMARQUE : Si un routeur VRRP possède l'adresse IP du routeur virtuel et celle de l'interface physique, il fonctionne comme un routeur virtuel principal.

- **VRID** : ID du routeur virtuel principal. Un routeur virtuel possède un ID unique qui est présenté en tant qu'adresse MAC virtuelle unique. Entrez une valeur comprise entre 1 et 255.
- **Priority** : priorité du routeur virtuel principal. La priorité détermine le rôle que chaque routeur VRRP joue et ce qui se passe si le routeur virtuel principal est défaillant. Entrez une valeur comprise entre 1 et 254.
- **Advertisement Interval** : spécifiez l'intervalle en secondes entre les annonces successives par le routeur virtuel principal dans un groupe VRRP. Par défaut, les annonces sont envoyées toutes les secondes. Les annonces envoyées par le routeur virtuel principal communiquent l'état et la priorité du routeur virtuel principal actuel.

  REMARQUE : Tous les routeurs d'un groupe VRRP doivent utiliser la même valeur d'intervalle d'annonce. Si les valeurs d'intervalles ne sont pas identiques, les routeurs du groupe VRRP ne communiquent pas entre eux et n'importe quel routeur mal configuré modifie son état pour les rétablir.
- **Verify** : cliquez sur **On** pour activer l'authentification ou sur **Off** pour la désactiver. L'Cisco ISA500 ignore les paquets VRRP entrants depuis les routeurs qui n'ont pas la même configuration d'authentification pour un groupe VRRP. Le protocole VRRP prend en charge les schémas d'authentification en texte brut et IPsec-AH. Choisissez le mot de passe ou l'en-tête d'authentification (AH) comme système d'authentification et spécifiez les paramètres.
- **Virtual IP Address** : entrez l'adresse IP virtuelle utilisée pour tous les routeurs virtuels de secours d'un même groupe.
- **Status** : affiche l'état de la vérification VRRP.

ÉTAPE 4 Cliquez sur **Save** pour appliquer vos paramètres.

Gestion d'adresse

Utilisez la page Address Management pour gérer les objets d'adresse et de groupes d'adresses. L'Cisco ISA500 est configurée avec une longue liste d'objets d'adresse courants que vous pouvez utiliser pour configurer les règles de pare-feu, les règles de transfert de ports, ou d'autres fonctions. Voir **Objets d'adresse par défaut, page 455**.

Reportez-vous aux rubriques suivantes :

- **Configuration des adresses, page 182**
- **Configuration des groupes d'adresses, page 183**

Configuration des adresses

ÉTAPE 1 Cliquez sur **Networking > Address Management**.

ÉTAPE 2 Dans la zone **Address Objects**, cliquez sur **Add Address** pour ajouter un nouvel objet d'adresse.

Autres options : pour modifier une entrée, cliquez sur l'icône **Edit** (crayon). Pour supprimer une entrée, cliquez sur l'icône **Delete** (x). Pour supprimer plusieurs entrées, cochez-les et cliquez sur **Delete**. Les objets d'adresse par défaut ne peuvent pas être modifiés et supprimés.

La fenêtre Address Object - Add/Edit s'ouvre.

ÉTAPE 3 Entrez les informations suivantes :

- **Name** : entrez le nom de l'objet d'adresse.
- **Type** : spécifiez le type d'adresse et entrez les informations correspondantes.
  - **Host** : définit un hôte unique par son adresse IP. Le masque de réseau d'un objet d'adresse d'hôte est automatiquement défini sur 32 bits (255.255.255.255) pour l'identifier en tant qu'hôte unique. Si vous choisissez l'hôte, entrez l'adresse IP de l'hôte dans le champ **IP Address.**
  - **Range** : définit une plage d'adresses IP contiguës. Aucun masque de réseau n'est associé à l'objet d'adresse Range, mais la logique interne traite généralement chaque membre de la plage spécifiée en tant qu'objet d'hôte masqué de 32 bits. Si vous choisissez Range, entrez l'adresse IP de début dans le champ **Starting IP Address** et l'adresse IP de fin dans le champ **Ending IP Address.**

- **Network** : l'objet d'adresse réseau tel que l'objet Range comprend plusieurs hôtes, mais plutôt que d'être lié par les délimiteurs de plage inférieure et supérieure spécifiés, les limites sont définies par un masque de réseau valide. Les objets d'adresse réseau doivent être définis par l'adresse réseau et le masque de réseau correspondant. En règle générale, la première (l'adresse réseau) et la dernière adresse d'un réseau (l'adresse de diffusion) sont inutilisables. Si vous choisissez Network, entrez l'adresse IP de sous-réseau dans le champ **IP Address** et l'adresse de diffusion dans le champ **Netmask**.
- **MAC** : identifie un hôte par son adresse matérielle ou son adresse MAC (Media Access Control). Les adresses MAC sont attribuées de manière unique aux périphériques de réseau filaires ou sans fil par les fabricants de matériel. Les adresses MAC sont des valeurs de 48 bits qui sont exprimées en notation hexadécimale de 6 octets. Si vous choisissez MAC, entrez l'adresse MAC dans le champ **MAC**.

ÉTAPE 4 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 5 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration des groupes d'adresses

Un objet de groupe d'adresses est associé à plusieurs objets d'adresse. L'Cisco ISA500 prend en charge jusqu'à 64 objets de groupe d'adresses. Un groupe d'adresses peut comporter jusqu'à 100 membres d'adresses.

ÉTAPE 1 Cliquez sur **Networking > Address Management**.

ÉTAPE 2 Dans la zone **Address Groups**, cliquez sur **Add Group** pour ajouter un nouvel objet de groupe d'adresses.

Autres options : pour modifier une entrée, cliquez sur l'icône **Edit** (crayon). Pour supprimer une entrée, cliquez sur l'icône **Delete** (x). Pour supprimer plusieurs entrées, cochez-les et cliquez sur **Delete**.

La fenêtre Address Group - Add/Edit s'ouvre.

ÉTAPE 3 Entrez le nom de l'objet de groupe d'adresses dans le champ **Group Name.**

ÉTAPE 4 Pour ajouter les objets d'adresse au groupe, sélectionnez les objets d'adresse dans la liste de gauche, puis cliquez sur la flèche droite.

ÉTAPE 5 Pour supprimer les objets d'adresse du groupe, sélectionnez les objets d'adresse de la liste de droite, puis cliquez sur la flèche gauche.

ÉTAPE 6 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 7 Cliquez sur **Save** pour appliquer vos paramètres.

Gestion des services

Utilisez la page Service Management pour gérer les objets de service ou de groupe de services. L'Cisco ISA500 est configurée avec une longue liste de services standards que vous pouvez utiliser pour configurer les règles de pare-feu, les règles de transfert de ports, ou d'autres fonctions. Voir **Objets de services par défaut, page 451**.

Reportez-vous aux rubriques suivantes :

- **Configuration des services, page 184**
- **Configuration des groupes de services, page 185**

Configuration des services

Si vous devez configurer une fonctionnalité pour un service personnalisé ne figurant pas dans la liste standard, vous devez d'abord définir l'objet de service.

ÉTAPE 1 Cliquez sur **Networking > Service Management**.

ÉTAPE 2 Dans la zone **Services**, cliquez sur **Add Service** pour ajouter un nouveau service.

Autres options : pour modifier une entrée, cliquez sur l'icône **Edit** (crayon). Pour supprimer une entrée, cliquez sur l'icône **Delete** (x). Pour supprimer plusieurs entrées, cochez-les et cliquez sur **Delete**. Les services par défaut ne peuvent pas être supprimés. Seule la plage de ports des services par défaut peut être modifiée.

La fenêtre Service Object - Add/Edit s'ouvre.

ÉTAPE 3 Entrez les informations suivantes :

- **Name** : entrez le nom du service.
- **Protocol** : spécifiez le protocole et la plage de ports pour le service :
  - **IP** : utilisez le type d'IP prédéfini. Si vous choisissez cette option, entrez le numéro du protocole dans le champ **IP Type**.
  - **ICMP** : le protocole ICMP (Internet Control Message Protocol) est un protocole TCP/IP utilisé pour envoyer des messages d'erreur et de contrôle. Si vous choisissez cette option, entrez le type de protocole ICMP dans le champ **ICMP Type**.
  - **TCP** : le protocole TCP (Transmission Control Protocol) est un protocole de transport dans TCP/IP. Le protocole TCP garantit l'envoi d'un message avec exactitude et dans son intégralité. Si vous choisissez cette option, entrez le numéro du port de début dans le champ **Port Range Start** et celui du port de fin dans le champ **Port Range End**.
  - **UDP** : le protocole UDP (User Datagram Protocol) est un protocole de la suite de protocoles TCP/IP utilisé à la place de TCP lorsqu'un acheminement fiable n'est pas requis. Si vous choisissez cette option, entrez le numéro du port de début dans le champ **Port Range Start** et celui du port de fin dans le champ **Port Range End**.
  - **Both (TCP/UDP)** : si vous choisissez cette option, entrez le numéro du port de début dans le champ **Port Range Start** et celui du port de fin dans le champ **Port Range End**.

ÉTAPE 4 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 5 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration des groupes de services

Les services qui s'appliquent aux applications courantes sont regroupés en tant qu'objet de groupe de services. Le groupe de services est traité comme un service unique. L'Cisco ISA500 prend en charge jusqu'à 64 groupes de services. Un groupe de services peut comprendre jusqu'à 64 membres de service.

ÉTAPE 1 Cliquez sur **Networking > Service Management**.

ÉTAPE 2 Dans la zone **Address Groups**, cliquez sur **Add Group** pour ajouter un nouvel objet de groupe d'adresses.

Autres options : pour modifier une entrée, cliquez sur l'icône **Edit** (crayon). Pour supprimer une entrée, cliquez sur l'icône **Delete** (x). Pour supprimer plusieurs entrées, cochez-les et cliquez sur **Delete**.

La fenêtre Service Group - Add/Edit s'ouvre.

ÉTAPE 3 Entrez le nom du groupe de services dans le champ **Group Name**.

ÉTAPE 4 Pour ajouter des services au groupe, sélectionnez-les dans la liste de gauche, puis cliquez sur la flèche droite.

ÉTAPE 5 Pour supprimer des services du groupe, sélectionnez-les dans la liste de droite, puis cliquez sur la flèche gauche.

ÉTAPE 6 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 7 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration du portail captif

Le portail captif permet aux utilisateurs authentifiés d'être dirigés vers une page Web spécifiée (portail) avant de pouvoir accéder à Internet. Les utilisateurs sont dirigés vers une page de connexion d'authentification Web spécifiée afin qu'ils s'authentifient, puis envoyés sur le portail Web spécifié après la connexion.

ÉTAPE 1 Cliquez sur **Wireless > Captive Portal** ou **Networking > Captive Portal**.

La fenêtre Captive Portal s'ouvre.

ÉTAPE 2 Dans la zone **Captive Portal**, entrez les informations suivantes :

- **Enable Captive Portal** : cliquez sur **On** pour activer la fonctionnalité Captive Portal ou sur **Off** pour la désactiver.
- **Apply on** : sélectionnez le SSID, le VLAN ou l'interface DMZ sur lequel appliquer les paramètres Captive Portal.

  REMARQUE : Vous ne pouvez définir qu'une seule interface à la fois pour l'accès au portail captif.

- **Web Authentication Type** : choisissez l'une des méthodes suivantes pour l'authentification Web. L'Cisco ISA500 peut authentifier les utilisateurs sans fil à l'aide de la base de données locale et du serveur externe d'AAA (tel que RADIUS, AD et LDAP). La méthode d'authentification est dérivée des paramètres d'authentification de l'utilisateur que vous avez spécifiés sur la page Users > User Authentication**.**
  - **Internal** : utilise la page de connexion de zone d'accès par défaut pour authentifier les utilisateurs. Pour se connecter, le nom d'utilisateur et le mot de passe sont nécessaires.
  - **Internal, no auth with accept button** : permet aux utilisateurs d'accéder au réseau sans entrer le nom d'utilisateur et le mot de passe. Si vous choisissez cette option, cliquez sur le bouton **Accept** sur la page de connexion de zone d'accès par défaut pour accéder au réseau sans authentification.
  - **External** : utilise une page de connexion de zone d'accès personnalisée sur le serveur Web externe spécifié pour authentifier les utilisateurs. Pour se connecter, le nom d'utilisateur et le mot de passe sont nécessaires.
  - **External, no auth with accept button** : permet aux utilisateurs d'accéder au réseau sans fil sans entrer le nom d'utilisateur et le mot de passe. Si vous choisissez cette option, cliquez sur le bouton **Accept** sur la page de connexion de zone d'accès personnalisée pour accéder au réseau sans fil sans authentification.
- **Redirected URL After Login** : choisissez l'une des options suivantes :
  - **Redirect Client to Customer URL** : dirige les utilisateurs vers une URL particulière (comme l'URL de votre société) après qu'ils se soient connectés. Si vous choisissez cette option, entrez l'URL souhaitée dans le champ, en indiquant notamment http:// ou https://.
  - **Redirect Client to Original URL** : dirige les utilisateurs vers l'URL d'origine.

  Supposons, par exemple, que vous sélectionniez **Internal** pour l'authentification et que le portail Web défini soit http://www.ABcompanyC.com. Lorsqu'un utilisateur sans fil tente d'accéder à un site Web externe, tel que http://www.google.com, la page de connexion de zone d'accès par défaut s'ouvre.

  Entrez le nom d'utilisateur et le mot de passe, puis cliquez sur **Login**. Une fois que l'utilisateur sans fil est connecté, il est dirigé vers le portail Web http://www.ABcompanyC.com. Le temps passé en ligne par l'utilisateur sans fil connecté s'affiche dans la barre de titre de la page de connexion. Cliquez sur **Logout** pour vous déconnecter.

- **Session Timeout** : entrez le délai d'attente (en minutes) pendant lequel la session sans fil peut rester connectée. Une fois ce délai expiré, la session se termine et le client doit s'authentifier à nouveau. Une valeur égale à zéro (0) indique que les utilisateurs peuvent se connecter et rester connectés aussi longtemps qu'ils le souhaitent. La valeur par défaut est de 60 minutes.
- **Idle Timeout** : entrez le délai d'attente (en minutes) pendant lequel la session sans fil peut rester inactive. Une session inactive prend fin à l'expiration du délai d'inactivité. La valeur par défaut est de 5 minutes.

ÉTAPE 3 Selon la méthode d'authentification Web sélectionnée, indiquez les informations suivantes dans la zone **Configuration** :

- Si vous choisissez **Internal** ou **Internal, no auth with accept button** comme méthode d'authentification Web, vous pouvez personnaliser les informations suivantes sur la page de connexion de zone d'accès par défaut :
  - **Logo File :** vous pouvez importer une image, telle que votre logo d'entreprise, pour qu'elle s'affiche sur la page de connexion. Cliquez sur **Browse** pour localiser et sélectionner un fichier d'image de votre PC local, puis cliquez sur **Upload**. Pour supprimer le fichier téléchargé, cliquez sur **Delete**.
  - **Background File** : vous pouvez importer une image afin de l'afficher comme arrière-plan de la page de connexion. Cliquez sur **Browse** pour localiser et sélectionner un fichier d'image (jpg, gif, or png) de votre PC local, puis cliquez sur **Upload**. Pour supprimer le fichier téléchargé, cliquez sur **Delete**.

    REMARQUE : Lorsque vous chargez un fichier, sélectionnez un fichier bmp, jpg, gif ou png de 200 Ko ou moins. Le champ Current Logo File affiche le nom du fichier qui est en cours d'utilisation, ou *par défaut* si aucun dossier n'a été chargé à cet effet.
  - **Cisco Logo** : si vous souhaitez masquer le logo Cisco qui apparaît sur la page de connexion, sélectionnez **Hide**. Dans le cas contraire, sélectionnez **Show**.
  - **Headline** : si vous souhaitez créer votre propre titre sur la page de connexion, entrez le texte souhaité dans ce champ.
  - **Message** : si vous souhaitez créer votre propre message sur la page de connexion, entrez le texte souhaité dans ce champ.
- Si vous choisissez **External** ou **External, no auth with accept button** comme méthode d'authentification Web, entrez les informations suivantes :

- **Authentication Web Server** : entrez l'URL complète du serveur Web externe (y compris https://), par exemple https://172.24.10.10/cgi-bin/PortalLogin.cgi.
- **Authentication Web Key** : entrez la clé utilisée pour protéger le nom d'utilisateur et le mot de passe que le serveur Web externe envoie à l'Cisco ISA500 pour l'authentification.

ÉTAPE 4 Dans la zone **Advanced Settings > Monitored HTTP Ports**, spécifiez les ports pour surveiller les requêtes HTTP. Les requêtes HTTP qui transitent par les ports HTTP surveillés sont dirigées vers la page Web spécifiée (portail).

REMARQUE : Le portail captif surveille uniquement les requêtes HTTPS qui transitent par le port 443.

a. Pour ajouter un port HTTP surveillé, cliquez sur **Add**. La fenêtre Port Configuration - Add/Edit s'ouvre.

b. Entrez un numéro de port dans le champ **Port**.

c. Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 5 Dans la zone **Advanced Settings > Open Domains**, indiquez l'adresse IP ou le nom de domaine des sites Web que vous souhaitez ouvrir. Les utilisateurs peuvent accéder à ces sites Web directement sans authentification.

a. Pour ajouter un domaine ouvert, **c**liquez sur **Add**. La fenêtre Domain Configuration - Add/Edit s'ouvre.

b. Entrez l'adresse IP ou le nom de domaine dans le champ **Domain**.

c. Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 6 Cliquez sur **Save** pour appliquer vos paramètres.

5

Sans fil (pour ISA550W et ISA570W uniquement)

Ce chapitre décrit comment configurer votre réseau sans fil. Il comprend les sections suivantes :

- **Affichage de l'état du réseau sans fil, page 191**
- **Configuration des paramètres de base, page 192**
- **Configuration des profils SSID, page 194**
- **Configuration de Wi-Fi Protected Setup, page 205**
- **Configuration du portail captif, page 207**
- **Configuration de la détection des points d'accès indésirables sans fil, page 211**
- **Advanced Radio Settings, page 212**

Pour accéder aux pages relatives au réseau sans fil, cliquez sur **Wireless** dans le volet de navigation gauche.

Affichage de l'état du réseau sans fil

Cette section explique comment afficher les informations relatives à votre réseau sans fil. Reportez-vous aux rubriques suivantes :

- **Affichage des statistiques relatives aux réseaux sans fil, page 191**
- **Affichage de l'état du client sans fil, page 192**

Affichage des statistiques relatives aux réseaux sans fil

Reportez-vous à la page Wireless Status pour consulter le total cumulé des statistiques sans fil appropriées pour tous les SSID. Cette page est automatiquement mise à jour toutes les 10 secondes. Cliquez sur Refresh pour actualiser manuellement les données.

Wireless > Wireless Status > Wireless Status

Champ	Description
Wireless Status	
SSID Number	Numéro du SSID.
SSID Name	Nom du SSID.
MAC Address	Adresse MAC du SSID.
VLAN	VLAN auquel le SSID est mappé.
Client List	Nombre de stations clientes connectées au SSID.
Wireless Statistics	
Name	Nom du SSID.
Tx Packets	Nombre de paquets transmis sur le SSID.
Rx Packets	Nombre de paquets reçus sur le SSID.
Collisions	Nombre de collisions de paquets signalées au SSID.
Tx Bytes/Sec	Nombre d'octets d'informations transmis sur le SSID.
Rx Bytes/Sec	Nombre d'octets d'informations reçus sur le SSID.
Uptime	Durée pendant laquelle le SSID était actif.

Affichage de l'état du client sans fil

Reportez-vous à la page Client Status pour consulter les informations relatives à toutes les stations clientes qui sont déjà connectées à chaque SSID. L'adresse MAC et l'adresse IP sont affichées pour toutes les stations clientes connectées pour chaque SSID. Pour ouvrir cette page, cliquez sur **Wireless > Wireless Status > Client Status**. Cette page est automatiquement mise à jour toutes les 10 secondes. Cliquez sur **Refresh** pour actualiser manuellement les données.

Configuration des paramètres de base

Utilisez la page Basic Settings pour modifier le mode sans fil en fonction des périphériques de votre réseau, spécifier le canal et la bande passante à utiliser pour résoudre les problèmes d'interférences avec d'autres points d'accès dans la zone ou activer l'isolation U-APSD et SSID si nécessaire.

ÉTAPE 1 Cliquez sur **Wireless > Basic Settings**.

ÉTAPE 2 Saisissez les informations suivantes :

- **Wireless Radio** : cliquez sur **On** pour activer la transmission radio sans fil et par conséquent activer le SSID appelé « cisco-data », ou cliquez sur **Off** pour désactiver cette option. L'activation d'un SSID activera la transmission de données par liaison sans fil. La désactivation de tous les SSID entraîne la mise hors tension de la radio sans fil.
- **Wireless Mode** : choisissez la technique de modulation 802.11.
  - **802.11b/g mixed** : sélectionnez ce mode si certains périphériques du réseau sans fil utilisent 802.11b et que d'autres utilisent 802.11g. Les clients 802.11b et 802.11g peuvent se connecter au point d'accès.
  - **802.11b/g/n mixed** : sélectionnez ce mode pour autoriser les clients 802.11b, 802.11g et 802.11n utilisant la fréquence 2,4 GHz à se connecter au point d'accès.
  - **802.11n only** : sélectionnez ce mode si tous les périphériques du réseau sans fil peuvent prendre en charge 802.11n. Seuls les clients 802.11n qui utilisent la fréquence 2.4 GHz peuvent se connecter au point d'accès.
- **Wireless Channel** : sélectionnez un canal dans une liste de canaux ou sélectionnez l'option **Auto** pour permettre au système de déterminer le canal optimal à utiliser en fonction des niveaux sonores environnementaux des canaux disponibles.

- **Bandwidth Channel** : choisissez l'agrégation de canaux 20 MHz (espacement) ou sélectionnez l'option **Auto** pour permettre au système de déterminer l'espacement optimal à utiliser entre les canaux. Ce paramètre est propre au trafic 802.11n.
- **Extension Channel** : sélectionnez l'option « Lower » ou « Upper » si vous choisissez l'option « Auto » pour l'espacement entre les canaux.
- **Unscheduled Automatic Power Save Delivery (U-APSD)** : cliquez sur **Enable** pour activer U-APSD pour réduire la consommation d'énergie ou sur **Disable** pour désactiver cette option.
- **SSID Isolation** : cliquez sur **Enable** pour activer la fonctionnalité d'isolation SSID isolation afin que les SSID ne puissent se voir entre eux lorsqu'ils appartiennent au même VLAN ou cliquez sur **Disable** pour désactiver cette option. Lorsque vous activez l'isolation SSID (entre les SSID), le trafic sur un SSID n'est pas acheminé vers un autre SSID.

ÉTAPE 3 Dans la zone **des SSID**, tous les SSID prédéfinis sur l'Cisco ISA500 apparaissent dans le tableau. Vous pouvez configurer les propriétés suivantes pour chaque SSID prédéfini :

- **Enable** : cochez cette case pour activer un SSID, décochez-la pour désactiver un SSID. Par défaut, tous les SSID sont désactivés.
- **SSID Name** : saisissez le nom d'un SSID.
- **SSID Broadcast** : cochez cette case pour diffuser le SSID dans ses trames de balise. Tous les périphériques sans fil à portée peuvent voir le SSID lorsqu'ils recherchent des réseaux disponibles. Décochez cette case pour empêcher la détection automatique du SSID. Dans ce cas, les utilisateurs doivent connaître le SSID pour configurer une connexion sans fil à ce SSID.

  REMARQUE : la désactivation de la diffusion SSID est suffisante pour éviter que les clients se connectent accidentellement à votre réseau, mais pas pour faire échouer la moindre tentative de connexion ou de surveillance du trafic non crypté de la part d'un pirate informatique. La suppression de la diffusion SSID offre un niveau de protection des plus faibles sur les réseaux exposés d'une autre manière (comme les réseaux invités) pour lesquels la priorité facilite l'obtention d'une connexion pour les clients et aucune information confidentielle n'est disponible.
- **Security Mode** : affiche le mode de sécurité actuellement utilisé pour le SSID. Pour configurer les paramètres de sécurité du SSID, cliquez sur l'icône de **modification** (crayon). Voir **Configuration de la sécurité sans fil, page 195**.

- **MAC Filtering** : indique si la fonctionnalité de filtrage MAC est activée ou désactivée sur le SSID. Le filtrage MAC permet d'autoriser ou de bloquer l'accès au SSID par l'adresse MAC (matérielle) du périphérique qui envoie la demande. Pour configurer les paramètres de filtrage MAC du SSID, cliquez sur l'icône de **modification** (crayon). Voir **Contrôle de l'accès sans fil par le biais des adresses MAC, page 202**.
- **VLAN Mapping** : affiche le VLAN auquel le SSID est mappé. L'ensemble du trafic en provenance des clients sans fil connectés à ce SSID est dirigé vers le VLAN sélectionné. Pour associer à un SSID à un VLAN spécifique, cliquez sur l'icône de **modification** (crayon). Voir **Mappage du SSID au VLAN, page 203**.
- **Wi-Fi Multimedia** : cochez cette case pour activer le Wi-Fi Multimedia (WMM), conçu pour améliorer l'expérience utilisateur pour les applications audio, vidéo et vocales via une connexion sans fil Wi-Fi. WMM fait référence à la QoS sur Wi-Fi. La QoS permet aux points d'accès Wi-Fi d'attribuer des priorités au trafic et optimise la manière dont les ressources réseau partagées sont allouées aux différentes applications. Par défaut, WMM est activé lorsque vous choisissez un mode de communication sans fil qui inclut la norme 802.11n.
- **Station Isolation** : cochez cette option afin que les clients sans fil sur le même SSID ne puissent pas se voir entre eux.

ÉTAPE 4 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration des profils SSID

ISA550W et ISA570W prennent en charge quatre SSID. Par défaut, tous les SSID sont désactivés. Pour des raisons de sécurité, nous vous recommandons vivement de configurer chaque SSID avec le niveau de sécurité maximal pris en charge par les périphériques de votre réseau sans fil.

Plusieurs SSID peuvent segmenter le LAN sans fil en plusieurs domaines de diffusion. Cette configuration vous permet de garder un meilleur contrôle sur le trafic de diffusion, qui affecte les performances réseau.

Reportez-vous aux rubriques suivantes :

- **Configuration de la sécurité sans fil, page 195**
- **Contrôle de l'accès sans fil par le biais des adresses MAC, page 202**
- **Mappage du SSID au VLAN, page 203**
- **Configuration de la programmation SSID, page 204**

Configuration de la sécurité sans fil

Cette section décrit comment configurer le mode de sécurité du SSID. Tous les équipements sur ce réseau doivent utiliser le même mode et des paramètres de sécurité identiques pour fonctionner correctement. Cisco recommande l'utilisation du niveau de sécurité maximal pris en charge par les périphériques de votre réseau.

REMARQUE Si le mode de sécurité est défini sur WEP ou WPA avec l'algorithme de cryptage TKIP pour le SSID prenant en charge la norme 802.11n, le débit de transmission de ses stations clientes associées ne dépassera pas 54 Mbit/s.

ÉTAPE 1 Cliquez sur **Wireless > Basic Settings**.

ÉTAPE 2 Dans la zone **des SSID**, cliquez sur l'icône de **modification** (crayon) pour modifier les paramètres du SSID.

La fenêtre SSID - Edit s'ouvre.

ÉTAPE 3 Dans l'onglet **Security Mode**, indiquez les informations suivantes :

- **SSID Name** : nom du SSID sur lequel les paramètres de sécurité sont appliqués.
- **User Limit** : spécifiez le nombre maximal d'utilisateurs pouvant se connecter simultanément à ce SSID. Entrez une valeur comprise entre 0 et 200. La valeur zéro (0) indique qu'il n'y a pas de limite pour ce SSID.

  REMARQUE : Le nombre maximal d'utilisateurs pouvant se connecter simultanément à tous les SSID activés est 200.
- **Security Mode** : sélectionnez le type de sécurité.

Security Mode	Description
Open	Tout périphérique sans fil qui se trouve à portée peut se connecter au SSID. Il s'agit du paramètre par défaut, mais il n'est pas recommandé.

Security Mode	Description
WEP	Le protocole WEP (Wired Equivalent Privacy) est un protocole de cryptage de données pour les réseaux sans fil 802.11. Les stations sans fil et les SSID du réseau sont tous configurés avec une clé partagée 64 bits ou 128 bits statique pour le cryptage des données. Plus le débit binaire pour le cryptage des données est élevé, plus votre réseau est sûr. Le cryptage WEP est une ancienne méthode de cryptage qui n'est pas considérée comme sûre et qui peut aisément être piratée. Ne sélectionnez cette option que si vous voulez autoriser l'accès aux périphériques ne prenant pas en charge WPA ou WPA2.

Security Mode	Description
WPA	L'accès protégé par Wi-Fi (WPA, Wi-Fi Protected Access) offre une meilleure sécurité que le cryptage WEP, car il utilise une méthode de cryptage par clé dynamique. Cette norme a été mise en œuvre comme mesure intermédiaire pour remplacer le WEP, en attendant la finalisation totale de la norme 802.11i pour le WPA2. L'Cisco ISA500 prend en charge les modes de sécurité WPA suivants. Choisissez l'un d'entre eux si vous avez besoin d'autoriser l'accès à des périphériques qui ne prennent pas en charge le WPA2. ▪ **WPA-Personal** : prend en charge les méthodes de cryptage TKIP (Temporal Key Integrity Protocol) ou AES (Advanced Encryption System) pour le cryptage des données (la valeur par défaut est TKIP). La méthode TKIP fait appel à des clés dynamiques et intègre un code MIC (Message Integrity Code) de protection contre le piratage. La méthode AES utilise un cryptage symétrique des données par blocs de 128 bits. ▪ **WPA-Enterprise** : utilise WPA avec l'authentification RADIUS. Ce mode prend en charge les mécanismes de cryptage TKIP et AES (la valeur par défaut est TKIP) et nécessite l'utilisation d'un serveur RADIUS pour authentifier les utilisateurs.

Security Mode	Description
WPA2	WPA2 fournit la meilleure sécurité en matière de transmissions sans fil. Cette méthode met en œuvre les normes de sécurité spécifiées dans la version finale de 802.11i. L'Cisco ISA500 prend en charge les modes de sécurité WPA2 suivants : ▪ **WPA2-Personal** : utilise toujours le mécanisme de cryptage AES pour le cryptage des données. ▪ **WPA2-Enterprise** : utilise WPA2 avec l'authentification RADIUS. Ce mode utilise toujours le mécanisme de cryptage AES pour le cryptage des données et nécessite l'utilisation d'un serveur RADIUS pour authentifier les utilisateurs.
WPA + WPA2	Permet aux clients WPA et WPA2 de se connecter simultanément. Le SSID sélectionne automatiquement l'algorithme de cryptage utilisé par chaque périphérique client. Choisissez ce mode de sécurité pour activer un plus haut niveau de sécurité tout en autorisant l'accès aux périphériques qui ne prennent pas en charge WPA2. L'Cisco ISA500 prend en charge les modes de sécurité WPA+WPA2 suivants : ▪ **WPA/WPA2-Personal mixed** : prend en charge la transition entre les modes WPA-Personal et WPA2-Personal. Vous disposez peut-être de périphériques clients utilisant WPA-Personal ou WPA2-Personal. ▪ **WPA/WPA2-Enterprise mixed** : prend en charge la transition entre les modes WPA-Enterprise et WPA2-Enterprise. Vous disposez peut-être de périphériques clients utilisant WPA-Enterprise ou WPA2-Enterprise.
RADIUS	Utilise des serveurs RADIUS pour l'authentification client et la génération dynamique de clé WEP pour le cryptage des données.

ÉTAPE 4 Si vous sélectionnez le mode de sécurité **Open**, aucune autre option n'est configurable. Dans ce mode, aucune donnée transférée vers ou depuis le SSID n'est cryptée. Il peut être utile lors de la configuration réseau initiale ou pour la résolution de problèmes, mais il n'est pas recommandé pour une utilisation régulière sur le réseau interne, car il n'est pas sécurisé.

ÉTAPE 5 Si vous sélectionnez le mode de sécurité **WEP**, entrez les informations suivantes :

- **Authentication Type** : choisissez soit **Open System**, soit **Shared key**, ou sélectionnez **Auto** pour permettre à l'Cisco ISA500 d'accepter les schémas de système ouvert et de clés partagées.
- **Default Transmit Key** : sélectionner un index de clé comme clé de transmission par défaut. Les index de clé 1 à 4 sont disponibles.
- **Encryption** : sélectionnez le type de cryptage : 64 bits (10 chiffres hexadécimaux), 64 bits (5 ASCII), 128 bits (26 chiffres hexadécimaux) ou 128 bits (13 ASCII). La valeur par défaut est 64 bits (64 bits (10 chiffres hexadécimaux)). Les clés de plus grande taille fournissent un meilleur cryptage, la clé est plus difficile à pirater.
- **Passphrase** : si vous souhaitez générer des clés WEP en utilisant une phrase de passe, saisissez n'importe quelle phrase alphanumérique (comprise entre 4 et 63 caractères), puis cliquez sur **Generate** pour générer 4 clés WEP uniques. Sélectionnez une clé qui sera indispensable aux périphériques pour utiliser le réseau sans fil.
- **Key 1-4** : si la phrase de passe WEP n'est pas spécifiée, vous pouvez saisir une clé directement dans l'une des cases « Key ». La clé doit se composer de 5 caractères ASCII (ou 10 caractères hexadécimaux) pour le cryptage 64 bits et 13 caractères ASCII (ou 26 caractères hexadécimaux) pour le cryptage 128 bits.

ÉTAPE 6 Si vous sélectionnez le mode de sécurité **WPA-Personal**, entrez les informations suivantes :

- **Encryption** : choisissez TKIP ou TKIP_CCMP (AES) comme algorithme de cryptage pour le cryptage des données. La valeur par défaut est TKIP.
- **Shared Secret** : la clé prépartagée PSK (Pre-Shared Key) est la clé secrète partagée pour WPA. Saisissez une chaîne comprenant entre 8 et 63 caractères.
- **Key Renewal Timeout** : entrez une valeur pour définir l'intervalle d'actualisation de la clé pour les clients associés à ce SSID. La plage valide est comprise entre 0 et 4 194 303 secondes. La valeur zéro (0) indique que la clé n'est pas actualisée. La valeur par défaut est de 3 600 secondes.

ÉTAPE 7 Si vous sélectionnez le mode de sécurité **WPA2-Personal**, entrez les informations suivantes :

- **Encryption** : utilisez toujours AES pour le cryptage des données.
- **Shared Secret** : la clé prépartagée PSK (Pre-Shared Key) est la clé secrète partagée pour WPA. Saisissez une chaîne comprenant entre 8 et 63 caractères.
- **Key Renewal Timeout** : entrez une valeur pour définir l'intervalle d'actualisation de la clé pour les clients associés à ce SSID. La plage valide est comprise entre 0 et 4 194 303 secondes. La valeur zéro (0) indique que la clé n'est pas actualisée. La valeur par défaut est de 3 600 secondes.

ÉTAPE 8 Si vous sélectionnez le mode de sécurité **WPA/WPA2-Personal mixed**, entrez les informations suivantes :

- **Encryption** : sélectionnez automatiquement TKIP ou AES pour le cryptage des données.
- **Shared Secret** : la clé prépartagée PSK (Pre-Shared Key) est la clé secrète partagée pour WPA. Saisissez une chaîne comprenant entre 8 et 63 caractères.
- **Key Renewal Timeout** : entrez une valeur pour définir l'intervalle d'actualisation de la clé pour les clients associés à ce SSID. La plage valide est comprise entre 0 et 4 194 303 secondes. La valeur zéro (0) indique que la clé n'est pas actualisée. La valeur par défaut est de 3 600 secondes.

ÉTAPE 9 Si vous sélectionnez le mode de sécurité **WPA-Enterprise**, entrez les informations suivantes :

- **Encryption** : choisissez TKIP ou AES comme algorithme de cryptage pour le cryptage des données. La valeur par défaut est TKIP.
- **Key Renewal Timeout** : entrez une valeur pour définir l'intervalle d'actualisation de la clé pour les clients associés à ce SSID. La plage valide est comprise entre 0 et 4 194 303 secondes. La valeur zéro (0) indique que la clé n'est pas actualisée. La valeur par défaut est de 3 600 secondes.
- **RADIUS Server ID** : l'Cisco ISA500 prédéfinit trois groupes RADIUS. Sélectionnez un groupe RADIUS existant pour l'authentification client. Les paramètres du serveur RADIUS suivant du groupe sélectionné s'affichent.
  - **Primary RADIUS Server IP Address** : adresse IP du serveur RADIUS principal.
  - **Primary RADIUS Server Port** : numéro de port du serveur RADIUS principal.

- **Primary RADIUS Server Shared Secret** : clé secrète partagée du serveur RADIUS principal.
- **Secondary RADIUS Server IP Address** : adresse IP du serveur RADIUS secondaire.
- **Secondary RADIUS Server Port** : numéro de port du serveur RADIUS secondaire.
- **Secondary RADIUS Server Shared Secret** : clé secrète partagée du serveur RADIUS secondaire.

  REMARQUE : Vous pouvez modifier les paramètres dans les champs ci-dessus, mais les paramètres du serveur RADIUS que vous spécifiez remplaceront les paramètres par défaut du groupe sélectionné. Pour maintenir les serveurs RADIUS, accédez à la page Users > RADIUS Servers. Voir **Configuration de serveurs RADIUS, page 374**.

ÉTAPE 10 Si vous sélectionnez le mode de sécurité **WPA2-Enterprise**, entrez les informations suivantes :

- **Encryption** : utilisez toujours l'algorithme de cryptage AES pour le cryptage des données.
- **Key Renewal Timeout** : entrez une valeur pour définir l'intervalle d'actualisation de la clé pour les clients associés à ce SSID. La plage valide est comprise entre 0 et 4 194 303 secondes. La valeur zéro (0) indique que la clé n'est pas actualisée. La valeur par défaut est de 3 600 secondes.
- **RADIUS Server ID** : choisissez un groupe RADIUS existant pour l'authentification client. Les paramètres du serveur RADIUS du groupe sélectionné s'affichent. Vous pouvez changer les paramètres du serveur RADIUS, mais les paramètres que vous spécifiez remplaceront les paramètres par défaut du groupe sélectionné. Pour maintenir les serveurs RADIUS, accédez à la page Users > RADIUS Servers. Voir **Configuration de serveurs RADIUS, page 374**.

ÉTAPE 11 Si vous sélectionnez le mode de sécurité **WPA/WPA2-Enterprise Mixed**, entrez les informations suivantes :

- **Encryption** : choisit automatiquement l'algorithme de cryptage AES ou TKIP pour le cryptage des données.
- **Key Renewal Timeout** : entrez une valeur pour définir l'intervalle d'actualisation de la clé pour les clients associés à ce SSID. La plage valide est comprise entre 0 et 4 194 303 secondes. La valeur zéro (0) indique que la clé n'est pas actualisée. La valeur par défaut est de 3 600 secondes.

- **RADIUS Server ID** : choisissez un groupe RADIUS existant pour l'authentification client. Les paramètres du serveur RADIUS du groupe sélectionné s'affichent. Vous pouvez changer les paramètres du serveur RADIUS, mais les paramètres que vous spécifiez remplaceront les paramètres par défaut du groupe sélectionné. Pour maintenir les serveurs RADIUS, accédez à la page Users > RADIUS Servers. Voir **Configuration de serveurs RADIUS, page 374**.

ÉTAPE 12 Si vous sélectionnez le mode de sécurité **RADIUS**, choisissez un groupe RADIUS existant pour l'authentification client dans la liste déroulante **RADIUS Server ID**. Les paramètres du serveur RADIUS du groupe sélectionné s'affichent. Vous pouvez changer les paramètres du serveur RADIUS, mais les paramètres que vous spécifiez remplaceront les paramètres par défaut du groupe sélectionné. Pour maintenir les serveurs RADIUS, accédez à la page Users > RADIUS Servers. Voir **Configuration de serveurs RADIUS, page 374**.

ÉTAPE 13 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 14 Cliquez sur **Save** pour appliquer vos paramètres.

Contrôle de l'accès sans fil par le biais des adresses MAC

Le filtrage MAC autorise ou bloque l'accès au SSID par l'adresse MAC (matérielle) du périphérique qui envoie la demande. Par défaut, le filtrage MAC est désactivé pour chaque SSID.

Le filtrage MAC fournit une sécurité supplémentaire, mais il augmente également la complexité et la maintenance. Vous devez spécifier la liste d'adresses MAC que vous souhaitez bloquer ou autoriser. Veillez à saisir chaque adresse MAC correctement pour que la stratégie soit appliquée comme prévu. Généralement il est plus facile et plus sûr d'utiliser cette fonctionnalité pour autoriser l'accès aux adresses MAC spécifiées, refusant de ce fait l'accès aux adresses MAC inconnues.

ÉTAPE 1 Cliquez sur **Wireless > Basic Settings**.

ÉTAPE 2 Dans la zone **des SSID**, cliquez sur l'icône de **modification** (crayon) pour modifier les paramètres du SSID.

La fenêtre SSID - Edit s'ouvre.

ÉTAPE 3 Dans l'onglet **MAC Filtering**, entrez les informations suivantes :

- **SSID Name** : nom du SSID sur lequel les paramètres de filtrage MAC sont appliqués.
- **Connection Control** : choisissez l'une des options suivantes comme stratégie de filtrage MAC :
  - **Disable** : désactive le filtrage MAC pour le SSID.
  - **Allow only the following MAC addresses to connect to the wireless network** : la connexion à ce SSID est autorisée à tous les périphériques figurant dans la liste d'adresses MAC. Tous les autres périphériques sont bloqués.
  - **Prevent the following MAC addresses from connecting to the wireless network** : la connexion à ce SSID est refusée à tous les périphériques figurant dans la liste d'adresses MAC. Tous les autres périphériques sont autorisés.

ÉTAPE 4 Dans la zone **Connection Control List**, spécifiez la liste d'adresses MAC que vous souhaitez bloquer ou autoriser. Vous pouvez ajouter jusqu'à 16 adresses MAC.

ÉTAPE 5 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 6 Cliquez sur **Save** pour appliquer vos paramètres.

Mappage du SSID au VLAN

ÉTAPE 1 Cliquez sur **Wireless > Basic Settings**.

ÉTAPE 2 Dans la zone **des SSID**, cliquez sur l'icône de **modification** (crayon) pour modifier les paramètres du SSID.

La fenêtre SSID - Edit s'ouvre.

ÉTAPE 3 Dans l'onglet **des VLAN**, entrez les informations suivantes :

- **SSID Name** : nom du SSID auquel le VLAN est mappé.
- **VLAN** : choisissez le VLAN dans la liste déroulante. Le SSID est mappé au VLAN sélectionné. L'ensemble du trafic en provenance des clients sans fil connectés à ce SSID est dirigé vers le VLAN sélectionné.

ÉTAPE 4 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 5 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration de la programmation SSID

Cette section décrit comment spécifier la programmation permettant de maintenir le SSID actif à une plage horaire spécifique de la journée.

ÉTAPE 1 Cliquez sur **Wireless > Basic Settings**.

ÉTAPE 2 Dans la zone **des SSID**, cliquez sur l'icône de **modification** (crayon) pour modifier les paramètres du SSID.

La fenêtre SSID - Edit s'ouvre.

ÉTAPE 3 Dans l'onglet **Scheduling**, spécifiez la période de la journée pendant laquelle le SSID restera actif :

- **SSID Name** : nom du SSID sur lequel le paramètre de programmation est appliqué.
- **Active Time** : cliquez sur **On** pour activer la fonctionnalité de programmation pour le SSID ou sur **Off** pour la désactiver. La désactivation de la fonctionnalité de programmation permet de maintenir le SSID actif 24 heures par jour. Si vous activez cette fonctionnalité, configurez la plage horaire journalière pendant laquelle le SSID restera actif.
  - **Start Time** : entrez les valeurs dans les champs de l'heure et des minutes et sélectionnez AM (matin) ou PM (après-midi) dans la liste déroulante.
  - **Stop Time** : entrez les valeurs dans les champs de l'heure et des minutes et sélectionnez AM (matin) ou PM (après-midi) dans la liste déroulante.

ÉTAPE 4 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 5 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration de Wi-Fi Protected Setup

Utilisez la page Wi-Fi Protected Setup pour paramétrer la configuration protégée par Wi-Fi (WPS) sur l'Cisco ISA500 afin de permettre une connexion plus facile des périphériques WPS au réseau sans fil.

ÉTAPE 1 Cliquez sur **Wireless > Wi-Fi Protected Setup**.

La fenêtre Wi-Fi Protected Setup s'ouvre.

ÉTAPE 2 Cliquez sur **On** pour activer le protocole WPS ou sur **Off** pour le désactiver.

ÉTAPE 3 Si vous activez WPS, spécifiez les paramètres WPS suivants :

- **WPS Configuration Status** : détermine s'il faut démarrer une nouvelle configuration sur le SSID avant que le client sans fil établisse une connexion WPS.
  - **Configured** : si vous sélectionnez cette option, les clients sans fil s'associent au SSID en respectant les paramètres de sécurité d'origine du SSID ; ceci est susceptible d'entraîner une connexion non sécurisée si le SSID n'est pas correctement configuré à l'avance, par exemple si le mode de sécurité est défini sur « Open ». Pour fournir une connexion sécurisée sous l'état « Configured », vous pouvez modifier manuellement à l'avance le mode de sécurité du SSID, puis établir la connexion WPS.
  - **Unconfigured** : si vous sélectionnez cette option, le SSID configure automatiquement ses paramètres de sécurité, tels que le nom de SSID et le mode de sécurité, avant que les clients sans fil soient associés pour assurer une connexion sécurisée. Une fois que les clients sans fil sont connectés, l'état passe automatiquement à « Configured ». Tout changement apporté au nom de SSID, au mode de sécurité ou à la phrase de passe ou clé WEP entraîne le passage de l'état à « Configured ».
- **Network Name (SSID)** : choisissez le SSID sur lequel les paramètres WPS sont appliqués.
- **Security** : mode de sécurité actuellement utilisé pour le SSID sélectionné.
- **Encryption** : méthode de cryptage actuellement utilisée pour le SSID sélectionné.

ÉTAPE 4 Si le périphérique client sans fil dispose d'un bouton-poussoir WPS, procédez comme suit pour établir la connexion WPS :

a. Activez WPS sur l'Cisco ISA500.

b. Cliquez sur le bouton **WPS** sur cette page.

c. Appuyez sur le bouton poussoir **WPS** sur le périphérique client sans fil, dans un délai de 2 minutes.

d. Vérifiez que le client sans fil est connecté au SSID.

ÉTAPE 5 Si le périphérique client sans fil dispose d'un code PIN WPS, procédez comme suit pour établir la connexion WPS :

a. Obtenez le code PIN utilisé sur le périphérique client sans fil.

b. Activez WPS sur l'Cisco ISA500.

c. Saisissez le code PIN dans le champ et cliquez sur **Apply** pour l'enregistrer.

d. Activez WPS sur le périphérique client sans fil dans un délai de 2 minutes.

e. Vérifiez que le client sans fil est connecté au SSID.

ÉTAPE 6 Si le périphérique client sans fil demande le code PIN de l'Cisco ISA500, procédez comme suit pour établir la connexion WPS :

a. Activez WPS sur l'Cisco ISA500.

b. Cliquez sur**Generate** pour générer un code PIN.

c. Suivez les instructions sur le périphérique client sans fil pour configurer WPS dans un délai de 2 minutes à l'aide du code PIN enregistré.

d. Vérifiez que le périphérique client sans fil est connecté au SSID.

REMARQUE : Si le périphérique client sans fil ne se connecte pas au SSID après 2 minutes, désactivez manuellement WPS sur l'Cisco ISA500 pour empêcher une attaque en force WPS.

ÉTAPE 7 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration du portail captif

Le portail captif permet aux utilisateurs authentifiés d'être dirigés vers une page Web spécifiée (portail) avant de pouvoir accéder à Internet. Les utilisateurs sont dirigés vers une page de connexion d'authentification Web spécifiée afin qu'ils s'authentifient, puis envoyés sur le portail Web spécifié après la connexion.

ÉTAPE 1 Cliquez sur **Wireless > Captive Portal** ou **Networking > Captive Portal**.

La fenêtre Captive Portal s'ouvre.

ÉTAPE 2 Dans la zone **Captive Portal**, entrez les informations suivantes :

- **Enable Captive Portal** : cliquez sur **On** pour activer la fonctionnalité Captive Portal ou sur **Off** pour la désactiver.
- **Apply on :** sélectionnez le SSID, le VLAN ou l'interface DMZ sur lequel appliquer les paramètres Captive Portal.

  REMARQUE : Vous ne pouvez définir qu'une seule interface à la fois pour l'accès au portail captif.

- **Web Authentication Type** : choisissez l'une des méthodes suivantes pour l'authentification Web. L'Cisco ISA500 peut authentifier les utilisateurs sans fil à l'aide de la base de données locale et du serveur externe d'AAA (tel que RADIUS, AD et LDAP). La méthode d'authentification est dérivée des paramètres d'authentification de l'utilisateur que vous avez spécifiés sur la page Users > User Authentication**.**
  - **Internal** : utilise la page de connexion de zone d'accès par défaut pour authentifier les utilisateurs. Pour se connecter, le nom d'utilisateur et le mot de passe sont nécessaires.
  - **Internal, no auth with accept button** : permet aux utilisateurs d'accéder au réseau sans entrer le nom d'utilisateur et le mot de passe. Si vous choisissez cette option, cliquez sur le bouton **Accept** sur la page de connexion de zone d'accès par défaut pour accéder au réseau sans authentification.
  - **External** : utilise une page de connexion de zone d'accès personnalisée sur le serveur Web externe spécifié pour authentifier les utilisateurs. Pour se connecter, le nom d'utilisateur et le mot de passe sont nécessaires.
  - **External, no auth with accept button** : permet aux utilisateurs d'accéder au réseau sans fil sans entrer le nom d'utilisateur et le mot de passe. Si vous choisissez cette option, cliquez sur le bouton **Accept** sur la page de connexion de zone d'accès personnalisée pour accéder au réseau sans fil sans authentification.
- **Redirected URL After Login** : choisissez l'une des options suivantes :
  - **Redirect Client to Customer URL** : dirige les utilisateurs vers une URL particulière (comme l'URL de votre société) après qu'ils se soient connectés. Si vous choisissez cette option, entrez l'URL souhaitée dans le champ, en indiquant notamment http:// ou https://.
  - **Redirect Client to Original URL** : dirige les utilisateurs vers l'URL d'origine.

  Supposons, par exemple, que vous sélectionniez **Internal** pour l'authentification et que le portail Web défini soit http://www.ABcompanyC.com. Lorsqu'un utilisateur sans fil tente d'accéder à un site Web externe, tel que http://www.google.com, la page de connexion de zone d'accès par défaut s'ouvre.

Saisissez le nom d'utilisateur et le mot de passe, puis cliquez sur **Login**. Une fois que l'utilisateur sans fil est connecté, il est dirigé vers le portail Web http://www.ABcompanyC.com. Le temps passé en ligne par l'utilisateur sans fil connecté s'affiche dans la barre de titre de la page de connexion. Cliquez sur **Logout** pour vous déconnecter.

- **Session Timeout** : entrez le délai d'attente (en minutes) pendant lequel la session sans fil peut rester connectée. Une fois ce délai expiré, la session se termine et le client doit s'authentifier à nouveau. Une valeur égale à zéro (0) indique que les utilisateurs peuvent se connecter et rester connectés aussi longtemps qu'ils le souhaitent. La valeur par défaut est de 60 minutes.
- **Idle Timeout** : entrez le délai d'attente (en minutes) pendant lequel la session sans fil peut rester inactive. Une session inactive prend fin à l'expiration du délai d'inactivité. La valeur par défaut est de 5 minutes.

ÉTAPE 3 Selon la méthode d'authentification Web sélectionnée, indiquez les informations suivantes dans la zone **Configuration** :

- Si vous choisissez **Internal** ou **Internal, no auth with accept button** comme méthode d'authentification Web, vous pouvez personnaliser les informations suivantes sur la page de connexion de zone d'accès par défaut :
  - **Logo File** : vous pouvez importer une image, telle que votre logo d'entreprise, pour qu'elle s'affiche sur la page de connexion. Cliquez sur **Browse** pour localiser et sélectionner un fichier d'image de votre PC local, puis cliquez sur **Upload**. Pour supprimer le fichier téléchargé, cliquez sur **Delete**.
  - **Background File** : vous pouvez importer une image afin de l'afficher comme arrière-plan de la page de connexion. Cliquez sur **Browse** pour localiser et sélectionner un fichier d'image (jpg, gif, or png) de votre PC local, puis cliquez sur **Upload**. Pour supprimer le fichier téléchargé, cliquez sur **Delete**.

    REMARQUE : Lorsque vous chargez un fichier, sélectionnez un fichier bmp, jpg, gif ou png de 200 Ko ou moins. Le champ Current Logo File affiche le nom du fichier qui est en cours d'utilisation, ou *par défaut* si aucun dossier n'a été chargé à cet effet.
  - **Cisco Logo** : si vous souhaitez masquer le logo Cisco qui apparaît sur la page de connexion, sélectionnez **Hide**. Dans le cas contraire, sélectionnez **Show**.
  - **Headline** : si vous souhaitez créer votre propre titre sur la page de connexion, entrez le texte souhaité dans ce champ.
  - **Message** : si vous souhaitez créer votre propre message sur la page de connexion, entrez le texte souhaité dans ce champ.

- Si vous choisissez **External** ou **External, no auth with accept button** comme méthode d'authentification Web, entrez les informations suivantes :
  - **Authentication Web Server** : entrez l'URL complète du serveur Web externe (y compris https://), par exemple https://172.24.10.10/cgi-bin/PortalLogin.cgi.
  - **Authentication Web Key** : entrez la clé utilisée pour protéger le nom d'utilisateur et le mot de passe que le serveur Web externe envoie à l'Cisco ISA500 pour l'authentification.

ÉTAPE 4 Dans la zone **Advanced Settings > Monitored HTTP Ports**, spécifiez les ports pour surveiller les requêtes HTTP. Les requêtes HTTP qui transitent par les ports HTTP surveillés sont dirigées vers la page Web spécifiée (portail).

REMARQUE : Le portail captif surveille uniquement les requêtes HTTPS qui transitent par le port 443.

a. Pour ajouter un port HTTP surveillé, cliquez sur **Add**. La fenêtre Port Configuration - Add/Edit s'ouvre.

b. Saisissez un numéro de port dans le champ **Port**.

c. Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 5 Dans la zone **Advanced Settings > Open Domains**, indiquez l'adresse IP ou le nom de domaine des sites Web que vous souhaitez ouvrir. Les utilisateurs peuvent accéder à ces sites Web directement sans authentification.

a. Pour ajouter un domaine ouvert, **c**liquez sur **Add**. La fenêtre Domain Configuration - Add/Edit s'ouvre.

b. Entrez l'adresse IP ou le nom de domaine dans le champ **Domain**.

c. Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 6 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration de la détection des points d'accès indésirables sans fil

Un point d'accès indésirable est un point d'accès connecté à votre réseau sans autorisation. Il n'est pas soumis à la gestion de vos administrateurs réseau et n'est pas nécessairement conforme à vos politiques de sécurité réseau.

L'Cisco ISA500 assure la détection proactive des points d'accès indésirables dans la bande 2,4 GHz. La détection des points d'accès indésirables permet de localiser, détecter et signaler les points d'accès non autorisés. Vous pouvez spécifier un point d'accès autorisé par le biais de son adresse MAC.

ÉTAPE 1 Cliquez sur **Wireless > Rogue AP Detection**.

La fenêtre Rogue AP Detection s'ouvre.

ÉTAPE 2 Cliquez sur **On** pour activer la détection des points d'accès indésirables ou sur **Off** pour la désactiver.

ÉTAPE 3 Si vous activez la détection des points d'accès indésirables, tous les points d'accès non autorisés détectés par l'Cisco ISA500 à proximité de réseau apparaissent dans la liste des points d'accès indésirables détectés. L'adresse MAC du point d'accès détecté s'affiche. Vous pouvez localiser les points d'accès non autorisés par le biais de leur adresse MAC et l' les surveille jusqu'à ce qu'ils soient autorisés ou éliminés. Cliquez sur **Refresh** pour mettre à jour les données.

ÉTAPE 4 Si un point d'accès répertorié comme non autorisé est en fait un point d'accès légitime, vous pouvez cliquer sur **Grant Access** pour le configurer comme point d'accès autorisé. Le point d'accès auquel vous venez d'autoriser est déplacé vers la liste des points d'accès autorisé.

ÉTAPE 5 L'Cisco ISA500 ne détecte pas les points d'accès autorisés.

- Pour ajouter un point d'accès autorisé, cliquez sur **Add**. Saisissez l'adresse MAC du point d'accès et cliquez sur **OK**. Vous pouvez spécifier jusqu'à 128 points d'accès autorisés.
- Pour supprimer un point d'accès autorisé dans la liste, cliquez sur l'icône de **suppression** (x).
- Pour modifier l'adresse MAC d'un point d'accès autorisé, cliquez sur l'icône de **modification** (crayon).
- Pour exporter la liste des points d'accès autorisés vers un dossier, cliquez sur **Export**.

- Pour importer la liste des points d'accès autorisés à partir d'un fichier, cliquez sur **Import**.

  Choisissez de remplacer la liste existante de points d'accès autorisé ou d'ajouter les entrées figurant dans le fichier importé à la liste des points d'accès autorisés.

  - Cliquez sur **Replace** pour importer la liste et remplacer la totalité du contenu de la liste des points d'accès autorisés. Cliquez sur **Browse** pour localiser le fichier et cliquez sur **OK**.
  - Cliquez sur **Merge** pour importer la liste et ajouter les points d'accès figurant dans le fichier importé aux points d'accès actuellement affichés dans la liste des points d'accès autorisés. Cliquez sur **Browse** pour localiser le fichier et cliquez sur **OK**.

  Une fois l'importation terminée, l'écran se met à jour et les adresses MAC des points d'accès importés apparaissent dans la liste des points d'accès autorisés.

ÉTAPE 6 Cliquez sur **Save** pour appliquer vos paramètres.

Advanced Radio Settings

Utilisez la page Advanced Settings pour spécifier les paramètres de transmission radio avancés.

REMARQUE Cette page est disponible si la transmission de données par liaison sans fil est activée dans la page Basic Settings.

ÉTAPE 1 Cliquez sur **Wireless > Advanced Settings**.

ÉTAPE 2 Saisissez les informations suivantes :

- **Guard Interval** : sélectionnez l'option « Long » (800 ns) ou « Short » (400 ns) de l'intervalle pour l'Cisco ISA500 qui doit retenter la transmission d'une trame qui échoue.

  REMARQUE : la trame courte est disponible uniquement lorsque le mode sans fil spécifié inclut le mode 802.11n.

- **CTS Protection Mode** : la fonctionnalité de mode de protection CTS (Clear-To-Send, prêt à émettre) renforce la capacité du SSID à capter toutes les transmissions sans fil G, mais réduit considérablement les performances.
  - Sélectionnez la case d'option **AUTO** si vous souhaitez que l'Cisco ISA500 établisse une liaison CTS avant d'émettre un paquet. Ce mode peut de réduire les collisions entre les stations masquées.
  - Sélectionnez la case d'option **Disabled** pour désactiver définitivement cette fonctionnalité.
- **Power Output** : vous pouvez régler la puissance de sortie du point d'accès pour obtenir une couverture adéquate pour votre réseau sans fil. Choisissez le niveau qui convient à votre environnement. Si vous n'êtes pas sûr du paramètre à sélectionner, utilisez le paramètre par défaut, 100 %.
- **Beacon Interval** : Les trames de balise sont transmises à intervalles réguliers par le point d'accès pour annoncer l'existence du réseau sans fil. Définissez l'intervalle en saisissant une valeur en millisecondes. Entrez une valeur comprise entre 20 et 999 ms. La valeur par défaut est 100 ms, ce qui signifie que ces trames de balise sont envoyées toutes les 100 ms.
- **DTIM Interval** : le message DTIM (Delivery Traffic Information Map) est un élément inclus dans certaines trames de balise. Il indique que les stations clientes se trouvent actuellement en veille en mode bas-régime et ont stocké des données en attente d'utilisation dans la mémoire tampon sur le point d'accès. Définissez l'intervalle en saisissant une valeur en trames de balise. Entrez une valeur comprise entre 1 et 255. La valeur par défaut est 1, ce qui signifie que le message DTIM est inclus dans chaque deuxième trame de balise.
- **RTS Threshold** : le seuil RTS détermine la taille de paquet qui nécessite une liaison RTS (Request To Send)/CTS (Clear To Send) avant l'envoi. Un paramètre de seuil bas peut être utile dans les zones où de nombreux périphériques client s'associent au périphérique sans fil ou dans les zones où les clients sont éloignés et qu'ils ne peuvent détecter que le point d'accès et non les autres clients. Bien qu'une valeur de seuil faible consomme davantage de bande passante et réduise le débit du paquet, les paquets RTS fréquents peuvent permettre un rétablissement du réseau suite à une interférence ou à des collisions. Définissez le seuil en saisissant la taille de paquet en octets. Entrez une valeur comprise entre 1 et 2 347. La valeur par défaut est 2 347, ce qui désactive le RTS de manière efficace.

- **Fragmentation Threshold** : le seuil de fragmentation est la longueur de trame qui nécessite la division (fragmentation) des paquets en deux trames ou plus. Une valeur minimale peut réduire les collisions, car ces dernières se produisent plus fréquemment lors de la transmission de longues trames, lesquelles occupent le canal plus longtemps. Utilisez un paramètre bas dans les zones où la communication est médiocre ou dans les zones où il existe de nombreuses interférences radio. Définissez le seuil en saisissant la longueur de trame en octets. Entrez une valeur comprise entre 256 et 2 346. La valeur par défaut est 2 346, ce qui désactive la fragmentation de manière efficace.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

6

Pare-feu

Ce chapitre décrit comment configurer les règles de pare-feu qui contrôlent le trafic entrant et sortant et comment définir d'autres paramètres pour protéger votre réseau. Il comprend les sections suivantes :

- **Configuration des règles de pare-feu pour contrôler le trafic entrant et sortant, page 216**
- **Configuration des règles NAT pour accéder en toute sécurité à un réseau à distance, page 226**
- **Exemples de configuration d'une règle de pare-feu et NAT, page 239**
- **Configuration du filtrage du contenu pour contrôler l'accès à internet, page 247**
- **Configuration du filtrage des adresses MAC pour autoriser ou bloquer le trafic, page 251**
- **Configuration de la liaison IP-MAC pour empêcher l'usurpation d'adresse, page 252**
- **Configuration de la protection contre les attaques, page 253**
- **Configuration des limites de session, page 255**
- **Configuration de la passerelle de niveau application, page 255**

Pour accéder aux pages de pare-feu, cliquez sur **Firewall** dans le volet de navigation gauche.

Configuration des règles de pare-feu pour contrôler le trafic entrant et sortant

Le pare-feu par zone peut autoriser ou refuser le trafic entrant ou sortant en fonction de la zone, du service, de l'adresse source et de destination et de la programmation.

Reportez-vous aux rubriques suivantes :

- **Paramètres du pare-feu par défaut, page 218**
- **Priorités des règles de pare-feu, page 219**
- **Tâches préliminaires de configuration des règles de pare-feu, page 220**
- **Paramètres de pare-feu généraux, page 220**
- **Configuration d'une règle de pare-feu, page 222**
- **Configuration d'une règle de pare-feu pour autoriser le trafic de diffusion, page 224**
- **Configuration des paramètres de consignation du pare-feu, page 225**

À propos des zones de sécurité

Une zone de sécurité est un groupe d'interfaces auxquelles une politique de sécurité peut être appliquée pour contrôler le trafic entre les zones. Pour faciliter le déploiement, le Cisco ISA500 a plusieurs zones prédéfinies avec des paramètres de sécurité par défaut pour protéger votre réseau. Vous pouvez créer des zones supplémentaires en fonction des besoins.

Chaque zone est associée à un niveau de sécurité. Le niveau de sécurité représente le niveau de confiance, du moins élevé (0) au plus élevé (100). Des règles de pare-feu par défaut sont créées pour toutes les zones prédéfinies et vos nouvelles zones en fonction de ces niveaux de sécurité. Par exemple, par défaut l'ensemble du trafic de la zone LAN (avec un niveau de sécurité Trusted) vers la zone WAN (avec un niveau de sécurité Untrusted) est autorisé, mais le trafic de la zone WAN (Untrusted) vers la zone LAN (Trusted) est bloqué. Vous pouvez créer et modifier des règles de pare-feu pour spécifier l'action d'autorisation ou de blocage pour des services, des adresses source ou de destination et des programmations spécifiés.

Pour en savoir plus, reportez-vous au tableau **Niveaux de sécurité et zones prédéfinies**.

Niveaux de sécurité et zones prédéfinies

Niveau de sécurité	Description	Zones prédéfinies
Trusted (100)	Niveau de confiance le plus élevé. Par défaut, le DEFAULT VLAN est mappé à la zone LAN prédéfinie. Vous pouvez regrouper un ou plusieurs VLAN dans une zone fiable.	LAN
VPN (75)	Niveau de confiance plus élevé qu'une zone publique, mais plus bas qu'une zone fiable. Ce niveau de sécurité est utilisé exclusivement pour les connexions VPN. L'ensemble du trafic est chiffré.	VPN SSLVPN
Public (50)	Niveau de confiance plus élevé qu'une zone invitée, mais plus bas qu'une zone VPN.	DMZ
Guest (25)	Niveau de confiance plus élevé qu'une zone non fiable, mais plus bas qu'une zone publique.	GUEST
Untrusted (0)	Le plus bas niveau de confiance. Par défaut, l'interface WAN1 est mappée à la zone WAN. Si vous utilisez le WAN (WAN2) secondaire, vous pouvez le mapper à la zone WAN ou à toute autre zone non fiable.	Réseau WAN
Voice	Conçu exclusivement pour le trafic voix. Le trafic entrant et sortant est optimisé pour les opérations de voix. Par exemple, affectez des téléphones IP Cisco à la zone VOICE.	VOICE

Paramètres du pare-feu par défaut

Par défaut, le pare-feu bloque l'ensemble du trafic d'une zone de sécurité inférieure à une zone de sécurité plus élevée (généralement appelé entrant) et autorise tout le trafic d'une zone de sécurité élevée vers une zone de sécurité plus faible (généralement appelée sortant).

Par exemple, il autorise l'ensemble du trafic provenant du LAN (zone fiable) vers le WAN (zone non fiable), et le trafic WAN (zone non fiable) vers la DMZ (zone publique) est bloqué.

Lorsque vous créez une nouvelle zone, telle qu'une zone de données, des règles de pare-feu sont automatiquement générées afin d'autoriser ou de bloquer le trafic entre cette zone et d'autres zones en fonction des niveaux de sécurité pour les zones **From** et **To**.

Le tableau suivant indique les paramètres de contrôle d'accès par défaut pour le trafic entre les zones de niveaux de sécurité identiques ou différents.

From/To	Trusted(100)	VPN(75)	Public(50)	Guest(25)	Untrusted(0)
Trusted(100)	Refuser	Autoriser	Autoriser	Autoriser	Autoriser
VPN(75)	Refuser	Refuser	Autoriser	Autoriser	Autoriser
Public(50)	Refuser	Refuser	Refuser	Autoriser	Autoriser
Guest(25)	Refuser	Refuser	Refuser	Refuser	Autoriser
Untrusted(0)	Refuser	Refuser	Refuser	Refuser	Refuser

Si vous souhaitez modifier les comportements par défaut afin, par exemple, de permettre l'accès entrant à votre réseau (WAN vers LAN) ou de bloquer le trafic sortant de votre réseau (LAN vers WAN), vous devez créer des règles de pare-feu.

Consultez la page Default Policies pour afficher les comportements de pare-feu par défaut pour toutes les zones nouvelles et prédéfinies.

ÉTAPE 1 Cliquez sur **Firewall > Access Control > Default Policies**.

ÉTAPE 2 Cliquez sur le triangle pour développer ou réduire les paramètres de contrôle d'accès par défaut d'une zone spécifique. Les comportements suivants sont définis pour toutes les zones prédéfinies.

From/To	LAN	VOICE	VPN	SSLVPN	DMZ	GUEST	WAN
LAN	S/O	Refuser	Autoriser	Autoriser	Autoriser	Autoriser	Autoriser
VOICE	Refuser	S/O	Autoriser	Autoriser	Autoriser	Autoriser	Autoriser
VPN	Refuser	Refuser	S/O	Refuser	Autoriser	Autoriser	Autoriser
SSLVPN	Refuser	Refuser	Refuser	S/O	Autoriser	Autoriser	Autoriser
DMZ	Refuser	Refuser	Refuser	Refuser	S/O	Autoriser	Autoriser
GUEST	Refuser	Refuser	Refuser	Refuser	Refuser	S/O	Autoriser
WAN	Refuser	Refuser	Refuser	Refuser	Refuser	Refuser	S/O

REMARQUE Les règles ACL s'appliquent pour le trafic entre réseaux locaux virtuels, dans une zone ou entre les zones. Vous ne pouvez pas définir de règles de liste de contrôle d'accès pour le trafic Intra-VLAN, par exemple LAN à LAN.

Priorités des règles de pare-feu

L'Cisco ISA500 comprend trois types de règles de pare-feu :

- **Règles de pare-feu par défaut** : règles de pare-feu définies sur l'Cisco ISA500 pour toutes les zones nouvelles et prédéfinies. Les règles de pare-feu par défaut ne peuvent pas être modifiées ni supprimées.
- **Règles de pare-feu personnalisées** : règles de pare-feu configurées par les utilisateurs. L'Cisco ISA500prend en charge jusqu'à 100 règles de pare-feu personnalisées.
- **Règles de pare-feu VPN** : règles de pare-feu automatiquement générées par les paramètres de contrôle d'accès aux zones dans vos configurations VPN. Les règles de pare-feu VPN ne peuvent pas être modifiées dans la page Firewall > Access Control > ACL Rules. Pour modifier les paramètres de contrôle d'accès de vos configurations VPN, allez sur les pages VPN.

Toutes les règles de pare-feu sont triées par priorité. Les règles personnalisées de pare-feu ont la priorité la plus élevée. Les règles de pare-feu VPN ont des priorités plus élevées que les règles de pare-feu par défaut, mais inférieures à celles des règles personnalisées de pare-feu.

Tâches préliminaires de configuration des règles de pare-feu

Selon les paramètres de pare-feu que vous souhaitez utiliser, vous pouvez être amené à effectuer les tâches suivantes avant de configurer les règles de pare-feu :

- Pour créer une règle de pare-feu qui s'applique uniquement à une zone spécifique à l'exception des zones prédéfinies, commencez par créer la zone. Voir **Configuration des zones, page 152**.
- Pour créer une règle de pare-feu qui s'applique à un service ou à un groupe de services spécifique, commencez par créer le service ou le groupe de services. Voir **Gestion des services, page 184**.
- Pour créer une règle de pare-feu qui s'applique uniquement à une adresse spécifique ou un groupe d'adresses, commencez par créer l'adresse ou le groupe d'adresses. Voir **Gestion d'adresse, page 182**.
- Pour créer une règle de pare-feu qui s'applique uniquement à un jour et à une heure spécifiques, commencez par créer la programmation. Voir **Configuration des programmations, page 429**.

Paramètres de pare-feu généraux

ÉTAPE 1 Cliquez sur **Firewall > Access Control > ACL Rules**.

La fenêtre ACL Rules s'ouvre. Les règles de pare-feu apparaissent dans le tableau de la liste de contrôle d'accès (ACL). Ce tableau contient toutes les règles de pare-feu pour le contrôle du trafic d'une zone particulière vers une destination spécifique.

ÉTAPE 2 Les règles de pare-feu sont triées par priorité. Vous pouvez réorganiser les règles personnalisées de pare-feu par priorité. Vous pouvez déplacer une règle vers le haut ou vers le bas, ou la déplacer vers un emplacement spécifié de la liste.

- Pour déplacer la règle d'une position vers le haut, cliquez sur l'icône de **déplacement vers le haut**.
- Pour déplacer la règle d'une position vers le bas, cliquez sur l'icône de **déplacement vers le bas**.
- Pour déplacer la règle vers un emplacement spécifique, cliquez sur l'icône de **déplacement** et entrez le numéro d'index cible vers lequel déplacer la règle sélectionnée.

  Par exemple : un index cible 2 déplace la règle en position 2 et déplace les autres règles en position 3 dans la liste.

REMARQUE : vous ne pouvez pas réorganiser les règles de pare-feu par défaut et les règles de pare-feu VPN. Les règles de pare-feu personnalisées ne peuvent pas être déplacées au-delà des règles de pare-feu par défaut et des règles de pare-feu VPN.

ÉTAPE 3 Pour afficher la liste des règles de pare-feu qui appartiennent au même groupe, choisissez la source et la destination dans les listes déroulantes **From Zone** et **To Zone** et cliquez sur **Apply**. Seules les règles correspondant aux zones spécifiées s'affichent.

Par exemple : si vous choisissez WAN dans la liste déroulante **From Zone** et LAN dans la liste déroulante **To Zone**, seules les règles de pare-feu du WAN au LAN apparaissent.

ÉTAPE 4 Vous pouvez effectuer d'autres tâches pour les règles de pare-feu :

- Cochez la case **Enable** pour activer une règle de pare-feu, ou décochez-la pour désactiver cette règle de pare-feu. Par défaut, toutes les règles de pare-feu par défaut sont activées.
- Pour ajouter une nouvelle entrée, cliquez sur le bouton **Add**.
- Pour modifier une entrée, cliquez sur l'icône de **modification** (crayon).
- Pour supprimer une entrée, cliquez sur l'icône de **suppression** (x).
- Pour supprimer plusieurs entrées, cochez-les et cliquez sur le bouton **Delete**.
- Cochez **Log** pour enregistrer l'événement lorsqu'une règle de pare-feu est survenue. Pour obtenir des informations sur la configuration des paramètres de consignation du pare-feu, reportez-vous à la section **Configuration des paramètres de consignation du pare-feu, page 225**.
- Pour autoriser l'accès du trafic, sélectionnez **Permit**. Pour refuser l'accès du trafic, sélectionnez **Deny**. Pour augmenter le nombre d'occurrences d'un lorsque le paquet correspond à la règle de pare-feu, sélectionnez **Accounting**.
- Pour afficher le type d'une règle de pare-feu, pointez votre curseur sur l'icône **Detail**.
- Pour définir les valeurs de la colonne Hit Count sur zéro pour toutes les règles de pare-feu, cliquez sur **Reset**.
- Pour actualiser manuellement les données du tableau, cliquez sur **Refresh**.

REMARQUE : les règles de pare-feu par défaut ne peuvent être ni désactivées, ni supprimées, ni modifiées, ni déplacées.

Configuration d'une règle de pare-feu

Cette section décrit comment configurer une règle de pare-feu pour contrôler le trafic entrant ou sortant.

REMARQUE Pour obtenir des exemples détaillés de configuration du pare-feu, reportez-vous à la section **Exemples de configuration d'une règle de pare-feu et NAT, page 239**.

ÉTAPE 1 Cliquez sur **Firewall > Access Control > ACL Rules**.

La fenêtre ACL Rules s'ouvre.

ÉTAPE 2 Pour ajouter une nouvelle règle de pare-feu, cliquez sur **Add**.

La fenêtre Rule - Add/Edit s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **Enable** : cliquez sur **On** pour activer la règle de pare-feu ou sur **Off** pour créer uniquement la règle de pare-feu.
- **From Zone** : sélectionnez la zone source du trafic qui est couverte par cette règle de pare-feu. Par exemple, sélectionnez **DMZ** si le trafic provient d'un serveur sur votre DMZ.
- **To Zone** : sélectionnez la zone de destination du trafic qui est couverte par cette règle de pare-feu. Par exemple, sélectionnez **WAN** si le trafic est à destination d'Internet.

  REMARQUE : seules les zones existantes peuvent être sélectionnées. Pour créer de nouvelles zones, allez sur la page **Networking > Zone**. Pour obtenir des informations sur la configuration des zones, reportez-vous à la section **Configuration des zones, page 152**.
- **Services** : sélectionnez un service ou un groupe de services existant qui est couvert par cette règle de pare-feu. Si le service ou le groupe de services que vous souhaitez ne figure pas dans la liste, choisissez **Create a new service** pour créer un nouvel objet de service ou **Create a new service group** pour créer un nouvel objet de groupe de services. Pour gérer les objets de service ou de groupe de services, allez à la page **Networking > Service Management**. Voir **Gestion des services, page 184**.
- **Source Address** : choisissez une adresse ou un groupe d'adresses existant comme adresse source ou comme réseau qui est couvert par cette règle de pare-feu.

- **Destination Address** : choisissez une adresse ou un groupe d'adresses existant comme adresse de destination ou comme réseau qui est couvert par cette règle de pare-feu.

  Si l'adresse ou le groupe d'adresses que vous souhaitez ne figure pas dans la liste, sélectionnez **Create a new address** pour créer un objet d'adresse ou **Create a new address group** pour créer un nouvel objet de groupe d'adresses. Pour gérer les objets d'adresses et de groupes d'adresses, accédez à la page **Networking > Address Management**. Voir **Gestion d'adresse, page 182**.

- **Schedule** : par défaut, la règle de pare-feu est toujours active. Si vous souhaitez conserver la règle de pare-feu active à un jour et à une heure spécifiques, choisissez la programmation pour la règle de pare-feu. Si la programmation que vous souhaitez ne figure pas dans la liste, choisissez **Create a new schedule** pour créer un objet de programmation. Pour gérer les programmations, accédez à la page **Device Management > Schedules**. Voir **Configuration des programmations, page 429**.

- **Log** : cliquez sur **On** pour enregistrer l'événement lorsqu'une règle de pare-feu est survenue. Pour obtenir des informations sur la configuration des paramètres de consignation du pare-feu, reportez-vous à la section **Configuration des paramètres de consignation du pare-feu, page 225**.

- **Match Action** : sélectionnez l'action pour le trafic lorsque le paquet correspond à la règle de pare-feu.

  - **Deny** : refuse l'accès.
  - **Permit** : accorde l'accès.
  - **Accounting** : augmente le nombre d'occurrences d'un lorsque le paquet correspond à la règle de pare-feu.

ÉTAPE 4 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 5 Cliquez sur **Save** pour appliquer vos paramètres.

REMARQUE Outre des règles de pare-feu, vous pouvez utiliser les méthodes suivantes pour contrôler le trafic :

- Empêcher les types d'attaques communs. Voir **Configuration de la protection contre les attaques, page 253**.
- Autoriser ou bloquer le trafic provenant des adresses MAC spécifiées. Voir **Configuration du filtrage des adresses MAC pour autoriser ou bloquer le trafic, page 251**

- Associer les adresses IP aux adresses MAC pour éviter l'usurpation d'adresse. Voir **Configuration de la liaison IP-MAC pour empêcher l'usurpation d'adresse, page 252**
- Autoriser ou bloquer des sites Web contenant des domaines ou des mots-clés d'URL spécifiques. Voir **Configuration du filtrage du contenu pour contrôler l'accès à internet, page 247**.

Configuration d'une règle de pare-feu pour autoriser le trafic de diffusion

Par défaut, le trafic de diffusion de n'importe quelle zone vers n'importe quelle zone est bloqué par le pare-feu. Pour activer le trafic de diffusion, vous devez désélectionner **Block Multicast Packets** sur la page **Firewall > Attack Protection** puis créer manuellement des règles de pare-feu pour autoriser le transfert multidiffusion d'une zone spécifique vers d'autres zones. L'Cisco ISA500 prédéfinit une adresse de multidiffusion (**IPv4_Multicast**) à cet effet.

Par exemple, le proxy IGMP peut être activé de la zone WAN à la zone LAN. Lorsque vous activez le proxy IGMP et que vous souhaitez recevoir des paquets de multidiffusion de la zone WAN vers la zone LAN, vous devez décocher la case **Block Multicast Packets** de la page **Firewall > Attack Protection**, puis créer une règle de pare-feu pour autoriser le trafic de diffusion de la zone WAN vers la zone LAN.

Cette section donne un exemple de configuration sur la façon de créer une règle de pare-feu du WAN au LAN pour autoriser le trafic de diffusion à l'aide de l'objet prédéfini d'adresse de multidiffusion.

ÉTAPE 1 Cliquez sur **Firewall > Access Control > ACL Rules**.

ÉTAPE 2 Cliquez sur **Add** pour ajouter une nouvelle règle de pare-feu.

La fenêtre Rule - Add/Edit s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **Enable** : cliquez sur **On** pour activer la règle de pare-feu.
- **From Zone** : sélectionnez **WAN** comme zone source du trafic.
- **To Zone** : sélectionnez **LAN** comme zone de destination du trafic.
- **Services** : sélectionnez **ANY** pour cette règle de pare-feu.
- **Source Address** : sélectionnez **ANY** comme adresse source.

- **Destination Address** : choisissez l'adresse de multidiffusion prédéfinie appelée **IPv4_Multicast** comme adresse de destination.
- **Schedule** : sélectionnez **Always On** pour cette règle de pare-feu.
- **Log** : cliquez sur **Off** pour cette règle de pare-feu. Nous vous conseillons de désactiver la fonctionnalité de fichier journal pour une règle de pare-feu de multidiffusion.
- **Match Action** : sélectionnez **Permit** pour autoriser l'accès.

ÉTAPE 4 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 5 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration des paramètres de consignation du pare-feu

Procédez comme suit pour consigner les événements de pare-feu et afficher les journaux de pare-feu :

ÉTAPE 1 Activez la fonctionnalité de fichier journal pour les règles de pare-feu. Voir **Configuration d'une règle de pare-feu, page 222**.

ÉTAPE 2 Allez sur la page **Device Management > Logs > Log Settings** pour configurer les paramètres de consignation. Vous devez activer la fonctionnalité Log, définir la taille de la mémoire tampon de journal et spécifier les paramètres Email Alert, Remote Logs et Local Log si vous voulez envoyer les journaux du pare-feu à une adresse courriel spécifique, enregistrer les journaux du pare-feu sur votre démon syslog local et sur un serveur syslog distant spécifié. Voir **Configuration des paramètres de journal, page 423**.

ÉTAPE 3 Allez sur la page **Device Management > Logs > Log Facilities** pour activer l'alerte par courriel, le journal local et/ou le fichier journal distant pour l'installation de pare-feu.

- Pour envoyer les journaux du pare-feu à une adresse courriel indiquée, cochez la case d'alerte par courriel pour l'installation de **pare-feu**.
- Pour enregistrer les journaux du pare-feu dans le démon syslog local, cochez la case du journal local pour l'installation de **pare-feu**.
- Pour enregistrer les journaux du pare-feu dans le serveur syslog distant, cochez la case du journal distant pour l'installation de **pare-feu**.

ÉTAPE 4 Après avoir configuré les paramètres de consignation du pare-feu, allez sur la page **Device Management > Logs > View Logs** pour afficher les journaux du pare-feu. Choisissez **Firewall** dans la liste déroulante Log Facility pour afficher les journaux du pare-feu. Vous pouvez filtrer les journaux du pare-feu par niveau de gravité ou par adresses IP source et de destination. Voir **Affichage des journaux, page 421**.

Configuration des règles NAT pour accéder en toute sécurité à un réseau à distance

La traduction d'adresses de réseau (NAT) permet aux réseaux IP privés de se connecter à Internet. Le NAT remplace une adresse IP privée par une adresse IP publique, traduisant les adresses privées du réseau interne privé en véritables adresses routables, qui peuvent être utilisées sur l'Internet public. De cette manière, le NAT conserve les adresses publiques, car il peut être configuré pour annoncer uniquement une adresse publique pour le réseau entier au monde extérieur.

Le NAT peut également offrir les avantages suivants :

- **Sécurité** : le fait de laisser les adresses IP internes masquées décourage des attaques directes.
- **Solutions de routage IP** : la superposition d'adresses IP n'est pas un problème lorsque vous utilisez le NAT.
- **Flexibilité** : vous pouvez modifier les schémas d'adressage IP internes, sans affecter les adresses publiques disponibles en externe. Par exemple, pour un serveur accessible à Internet, vous pouvez conserver une adresse IP fixe pour l'utilisation d'Internet, mais en interne, vous pouvez modifier l'adresse du serveur.

Reportez-vous aux rubriques suivantes :

- **Affichage de l'état de la traduction NAT, page 227**
- **Priorités des règles NAT, page 228**
- **Configuration des règles de PAT dynamique, page 229**
- **Configuration des règles NAT statiques, page 230**
- **Configuration des règles de transfert de port, page 231**

- Configuration des règles de déclenchement de port, page 233
- Configuration des règles NAT avancées, page 234
- Configuration d'alias IP pour les règles NAT avancées, page 236
- Configuration d'une règle NAT avancée pour prendre en charge la reconnexion NAT, page 238

REMARQUE Pour des exemples détaillés de configuration NAT, reportez-vous à la section Exemples de configuration d'une règle de pare-feu et NAT, page 239.

Affichage de l'état de la traduction NAT

Reportez-vous à la page NAT Status pour consulter les informations relatives à toutes les règles NAT. Si une page ne peut pas afficher toutes les entrées NAT, choisissez le numéro de page dans la liste déroulante pour afficher les entrées NAT sur une autre page.

Firewall > NAT > NAT Status

Champ	Description
Original Source Address	Adresse IP source d'origine dans le paquet.
Original Destination Address	Adresse IP de destination d'origine dans le paquet.
Source Port	Interface source d'où provient le trafic.
Destination Port	Interface de destination où le trafic s'achemine.
Translated Destination Address	Adresse IP vers laquelle l'adresse de destination d'origine spécifiée est traduite.
Translated Source Address	Adresse IP vers laquelle l'adresse source d'origine spécifiée est traduite.
Translated Destination Port	Interface vers laquelle l'interface de destination spécifiée est traduite.
Translated Source Port	Interface vers laquelle l'interface source spécifiée est traduite.
Tx Packets	Nombre de paquets transmis.

Champ	Description
Rx Packets	Nombre de paquets reçus.
Tx Bytes/Sec	Volume en octets du trafic transmis.
Rx Bytes/Sec	Volume en octets du trafic reçu.

Priorités des règles NAT

S'il existe un conflit entre NAT avancé, NAT statique ou les règles de transfert de port, l'appareil de sécurité traite les règles comme indiqué ci-dessous.

Trafic entrant

Pour un paquet entrant, l'appareil de sécurité exécute NAT avant qu'une décision de transmission soit prise et utilise l'ordre de priorité suivant pour les différents types de règles :

1. NAT avancé
2. NAT statique
3. Transfert de port
4. Déclenchement de port

Trafic sortant

Pour un paquet entrant, l'appareil de sécurité exécute NAT avant qu'une décision de transmission soit prise et utilise l'ordre de priorité suivant pour les différents types de règles :

1. NAT avancé
2. NAT statique
3. Dynamic PAT

Par exemple, si une règle NAT avancée et une règle de transfert de port sont en conflit, alors la règle NAT avancée a priorité sur la règle de transfert de port et la règle de transfert de port n'est pas appliquée.

Configuration des règles de PAT dynamique

La traduction d'adresses de ports (PAT dynamique) peut uniquement être utilisée pour établir des connexions du réseau privé au réseau public. La PAT dynamique traduit les adresses privées multiples en une ou plusieurs adresses IP publiques.

REMARQUE Pendant la durée de la traduction, un hôte distant peut établir une connexion vers l'hôte traduit si une règle de pare-feu le permet. Étant donné que l'adresse du port (vrai et mappé) est imprévisible, une connexion vers l'hôte est peu probable. Néanmoins, dans ce cas, vous pouvez compter sur la sécurité des règles de pare-feu.

ÉTAPE 1 Cliquez sur **Firewall > NAT > Dynamic PAT**.

ÉTAPE 2 Indiquez l'adresse IP de PAT pour chaque port WAN.

- **Auto** : utilisez automatiquement l'adresse IP du port WAN comme adresse IP traduite.
- **Manual** : choisissez manuellement une adresse IP publique unique ou une adresse réseau comme adresse IP à partir de la liste déroulante **IP Address**. Si l'objet d'adresse que vous souhaitez ne figure pas dans la liste, choisissez **Create a new address** pour créer un nouvel objet d'adresse. Pour gérer les objets d'adresse, accédez à la page **Networking > Address Management**. Voir **Gestion d'adresse, page 182**.

ÉTAPE 3 Convertissez les adresses IP privées d'un VLAN en une ou plusieurs adresses IP mappées.

- **Enable WAN1** : cochez cette case pour traduire toutes les adresses IP du VLAN sélectionné en une adresse IP publique spécifiée sur le port WAN1.
- **Enable WAN2** : cochez cette case pour traduire toutes les adresses IP du VLAN sélectionné en une adresse IP publique spécifiée sur le port WAN2.
- **VLAN IP Address** : adresse IP de sous-réseau et masque de réseau du VLAN sélectionné.

ÉTAPE 4 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration des règles NAT statiques

La NAT statique crée une traduction fixe d'une adresse réelle en une adresse associée. Étant donné que l'adresse mappée est la même pour chaque connexion consécutive, le NAT statique autorise la demande de connexion bidirectionnelle, à la fois vers et à partir de l'hôte (si une règle de pare-feu le permet). En outre, avec la PAT dynamique, chaque hôte utilise une adresse ou un port distinct pour chaque traduction suivante, l'initiation bidirectionnelle n'est donc pas prise en charge.

Jusqu'à 64 règles NAT statiques peuvent être configurées sur l'Cisco ISA500. Vous devez créer des règles de pare-feu pour autoriser l'accès de sorte que les règles NAT statiques puissent fonctionner correctement.

REMARQUE La gestion à distance de l'appareil de sécurité ne fonctionne pas si vous configurez une règle NAT statique qui mappe un serveur interne vers l'adresse IP WAN. Par exemple, si vous créez une règle NAT statique qui mappe l'adresse 192.168.75.100 vers l'adresse IP WAN, 173.39.202.68, les utilisateurs distants n'ont pas accès à l'utilitaire de configuration via http://173.39.202.68:8080.

ÉTAPE 1 Cliquez sur **Firewall > NAT > Static NAT**.

ÉTAPE 2 Pour ajouter une règle NAT statique, cliquez sur **Add**.

Autres options : pour modifier une entrée, cliquez sur l'icône de **modification** (crayon). Pour supprimer une entrée, cliquez sur l'icône de **suppression** (x). Pour supprimer plusieurs entrées, cochez-les et cliquez sur **Delete**.

La fenêtre Static NAT Rule - Add/Edit s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **WAN** : choisissez WAN1 ou WAN2 comme port WAN.
- **Public IP** : sélectionnez un objet d'adresse IP comme adresse IP publique.
- **Private IP** : sélectionnez un objet d'adresse IP comme adresse IP privée.

  Si l'adresse IP de votre choix ne figure pas dans la liste, sélectionnez **Create a new address** pour créer un nouvel objet Adresse IP. Pour gérer les objets Adresse IP, accédez à la page **Networking > Address Management**. Voir **Gestion d'adresse, page 182**.

  REMARQUE : les règles de pare-feu doivent être configurées pour autoriser l'accès. Vous pouvez accéder à la page **Firewall > Access Control > ACL Rules** ou cliquez sur le lien **Create Rule** pour effectuer cette opération, mais devez d'abord enregistrer vos paramètres sur cette page.

ÉTAPE 4 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 5 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration des règles de transfert de port

Le transfert de port transmet un paquet TCP/IP traversant une passerelle de traduction d'adresses de réseau (NAT) à un port de réseau prédéfini sur un hôte au sein d'un réseau NAT usurpé, en général basé sur le réseau privé sur le numéro de port sur lequel il a été reçu à la passerelle de l'hôte émetteur.

Utilisez la page de transfert de port pour attribuer un numéro de port à un service associé à l'application que vous souhaitez exécuter, comme les serveurs Web, les serveurs FTP, les serveurs de messagerie ou d'autres applications Internet spécialisées.

REMARQUE

- Jusqu'à 64 règles de transfert de port peuvent être configurées sur l'Cisco ISA500. Vous devez créer des règles de pare-feu pour autoriser l'accès, de sorte que les règles de transfert de port puissent fonctionner correctement.
- Pour ouvrir un serveur FTP interne sur Internet, vérifiez que le serveur FTP écoute sur le port TCP 21 ou qu'à la fois le serveur FTP et le client doivent utiliser le mode actif lorsque le serveur FTP écoute sur un autre port TCP. Sinon le client FTP ne parvient pas à accéder au serveur FTP.

ÉTAPE 1 Cliquez sur **Firewall > NAT > Port Forwarding**.

ÉTAPE 2 Pour activer une règle de transfert de port, sélectionnez la case de la colonne **Enable.**

ÉTAPE 3 Pour ajouter une règle de transfert de port, cliquez sur **Add**.

Autres options : pour modifier une entrée, cliquez sur l'icône de **modification** (crayon). Pour supprimer une entrée, cliquez sur l'icône de **suppression** (x). Pour supprimer plusieurs entrées, cochez-les et cliquez sur **Delete**.

La fenêtre Port Forwarding Rule - Add/Edit s'ouvre.

ÉTAPE 4 Saisissez les informations suivantes :

- **Original Service** : sélectionnez un service existant en tant que service entrant.

- **Translated Service** : sélectionnez un service en tant que service traduit ou sélectionnez **Original** si le service traduit est le même que le service entrant. Si le service de votre choix ne figure pas dans la liste, sélectionnez **Create a new service** pour créer un nouvel objet Service. Pour gérer les objets de service, accédez à la page **Networking > Service Management**. Voir **Gestion des services, page 184**.

  REMARQUE : La traduction un-à-un sera exécutée pour le transfert de plage de ports. Par exemple, si vous souhaitez traduire un service TCP original avec la plage de ports 50000 à 50002 en un service TCP avec la plage de ports 60000 à 60002, le port 50000 sera traduit en port 60000, le port 50001 sera traduit en port 60001 et le port 50002 sera traduit en port 60002.

- **Translated IP** : sélectionnez l'adresse IP de votre serveur local qui doit être traduit. Si l'adresse IP de votre choix ne figure pas dans la liste, sélectionnez **Create a new address** pour créer un nouvel objet Adresse IP. Pour gérer les objets Adresse IP, accédez à la page **Networking > Address Management**. Voir **Gestion d'adresse, page 182**.

- **WAN** : sélectionnez WAN1 ou WAN2, ou les deux, comme port WAN entrant.

- **WAN IP** : spécifiez l'adresse IP publique du serveur. Vous pouvez utiliser l'adresse IP du port WAN sélectionné ou une adresse IP publique fournie par votre ISP. Lorsque vous sélectionnez Both en tant que port WAN entrant, cette option est grisée.

- **Enable Port Forwarding** : cliquez sur **On** pour activer la règle de redirection de port ou cliquez sur **Off** pour créer uniquement la règle de transfert de port.

- **Create Firewall Rule** : cochez cette case pour créer automatiquement une règle de pare-feu pour autoriser l'accès de sorte que la règle de transfert de port puisse fonctionner correctement. Vous devez créer manuellement une règle de pare-feu si vous désactivez cette case à cocher.

  REMARQUE : Si vous sélectionnez Both en tant que port WAN entrant, une règle de pare-feu de n'importe quelle zone à n'importe quelle zone est alors créée.

- **Description** : entrez le nom de la règle de transfert de port.

ÉTAPE 5 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 6 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration des règles de déclenchement de port

Le déclenchement de port ouvre un port entrant pour un type de trafic spécifié sur un port sortant défini. Lorsqu'un périphérique LAN établit une connexion sur l'un des ports sortants définis, l'Cisco ISA500 ouvre le port entrant spécifié pour prendre en charge l'échange de données. Les ports ouverts seront fermés à nouveau au bout de 600 secondes une fois l'échange des données terminé.

Le déclenchement de port est plus flexible et sécurisé que le transfert de port. En effet, les ports entrants ne sont pas ouverts tout le temps. Ils sont ouverts uniquement lorsqu'un programme utilise activement le port de déclenchement.

Certaines applications peuvent requérir le déclenchement de port. Pour fonctionner correctement, ces applications nécessitent de recevoir, lorsque des périphériques externes se connectent à elles, des données sur un port ou une plage de ports spécifique. L'Cisco ISA500 nécessite l'envoi de toutes les données entrantes pour cette application uniquement sur le port ou la plage de ports requis. Vous pouvez spécifier une règle de déclenchement de port en définissant le type de trafic (TCP ou UDP) et la plage des ports entrants et sortants à ouvrir en cas d'activation.

REMARQUE Jusqu'à 15 règles de déclenchement de port peuvent être configurées sur l'Cisco ISA500. Le déclenchement de port n'est pas adapté aux serveurs sur le LAN, puisque le périphérique LAN doit établir une connexion sortante avant qu'un port entrant soit ouvert. Dans ce cas, vous pouvez créer des règles de transfert de port à cet effet.

ÉTAPE 1 Cliquez sur **Firewall > NAT > Port Triggering**.

ÉTAPE 2 Pour activer une règle de transfert de port, sélectionnez la case de la colonne **Enable.**

ÉTAPE 3 Pour ajouter une nouvelle règle de déclenchement, cliquez sur **Add**.

Autres options : pour modifier une entrée, cliquez sur l'icône de **modification** (crayon). Pour supprimer une entrée, cliquez sur l'icône de **suppression** (x). Pour supprimer plusieurs entrées, cochez-les et cliquez sur **Delete**.

La fenêtre Port Triggering Rule - Add/Edit s'ouvre.

ÉTAPE 4 Saisissez les informations suivantes :

- **Description** : entrez le nom de la règle de déclenchement.
- **Triggered Service** : sélectionnez un service TCP ou UDP sortant.
- **Opened Service** : sélectionnez un service TCP ou UDP entrant.

Si le service de votre choix ne figure pas dans la liste, sélectionnez **Create a new service** pour créer un nouvel objet Service. Pour gérer les objets de service, accédez à la page **Networking > Service Management**. Voir **Gestion des services, page 184**.

- **Enable Port Triggering** : cliquez sur **On** pour activer la règle de déclenchement de port ou sur **Off** pour créer uniquement la règle de déclenchement de port.

ÉTAPE 5 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 6 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration des règles NAT avancées

Le NAT avancé vous permet d'identifier de vraies adresses et de vrais ports pour la traduction d'adresses en indiquant les adresses source et de destination.

REMARQUE Il est possible de configurer jusqu'à 32 règles NAT avancées sur l'Cisco ISA500. Vous devez créer des règles de pare-feu pour autoriser l'accès de sorte que les règles NAT avancées puissent fonctionner correctement.

ÉTAPE 1 Cliquez sur **Firewall > NAT > Advanced NAT**.

ÉTAPE 2 Pour activer une règle de transfert de port, sélectionnez la case de la colonne **Enable.**

ÉTAPE 3 Pour ajouter une nouvelle règle NAT avancée, cliquez sur **Add**.

Autres options : pour modifier une entrée, cliquez sur l'icône de **modification** (crayon). Pour supprimer une entrée, cliquez sur l'icône de **suppression** (x). Pour supprimer plusieurs entrées, cochez-les et cliquez sur **Delete**.

La fenêtre Advanced NAT Rule - Add/Edit s'ouvre.

ÉTAPE 4 Saisissez les informations suivantes :

- **Name** : entrez le nom de la règle NAT avancée.
- **Enable** : cliquez sur **On** pour activer la NAT avancée ou sur **Off** pour uniquement créer la règle NAT avancée.
- **From** : sélectionnez **Any** ou sélectionnez une interface (un port WAN ou un VLAN) d'où provient ce trafic.

- **To** : sélectionnez **Any** ou sélectionnez une interface (un VLAN ou un port WAN) vers lequel le trafic sera acheminé.

  REMARQUE : Lorsque l'adresse de destination initiale est différente de l'adresse de destination traduite, vous devez choisir **Any** pour cette option. Lorsque l'adresse de destination initiale est la même que l'adresse de destination traduite, vous pouvez choisir un port VLAN ou WAN spécifique pour cette option.

- **Original Source Address** : choisissez l'adresse source d'origine pour le paquet.
- **Original Destination Address** : choisissez l'adresse de destination d'origine pour le paquet.
- **Original Services** : sélectionnez le service TCP ou UDP d'origine.
- **Translated Source Address** : choisissez l'adresse source traduite pour le paquet.
- **Translated Destination Address** : choisissez l'adresse de destination traduite pour le paquet.
- **Translated Services** : sélectionnez le service TCP ou UDP traduit.

  Si l'adresse de votre choix ne figure pas dans la liste, sélectionnez **Create a new address** pour créer un nouvel objet Adresse IP. Pour gérer les objets Adresse IP, accédez à la page **Networking > Address Management**. Voir **Gestion d'adresse, page 182**.

  Si le service de votre choix ne figure pas dans la liste, sélectionnez **Create a new service** pour créer un nouvel objet Service. Pour gérer les objets de service, accédez à la page **Networking > Service Management**. Voir **Gestion des services, page 184**.

ÉTAPE 5 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 6 Cliquez sur **Save** pour appliquer vos paramètres.

ÉTAPE 7 Les règles de pare-feu doivent être configurées pour autoriser l'accès de sorte que les règles NAT avancées puissent fonctionner correctement. Une fois avoir enregistré vos paramètres, rendez-vous sur la page **Firewall > Access Control > ACL Rules** pour effectuer cette opération. Voir **Configuration d'une règle de pare-feu, page 222**.

Configuration d'alias IP pour les règles NAT avancées

Un port WAN unique est accessible via des adresses IP multiples en ajoutant un alias IP au port. Lorsque vous configurez une règle NAT avancée, l'Cisco ISA500 crée automatiquement un alias IP dans les cas suivants :

Exemple d'utilisation : l'interface entrante (**From**) est définie sur un port WAN, mais l'adresse IP de destination d'origine (**Original Destination Address**) est différente de l'adresse IP publique du port WAN sélectionné.

Par exemple, vous hébergez un hôte HTTP (192.168.75.20) sur votre LAN. Votre ISP vous a fourni une adresse IP statique (1.1.1.3) que vous souhaitez exposer au public comme votre adresse de serveur HTTP. Vous souhaitez autoriser les utilisateurs Internet à accéder au serveur HTTP interne à l'aide de l'adresse IP publique spécifiée.

Solution : en supposant que l'adresse IP du port WAN1 est 1.1.1.2 et qu'une autre adresse IP publique 1.1.1.3 vous est affectée. Vous pouvez tout d'abord créer un objet d'adresse d'hôte avec l'adresse 192.168.75.20 nommé HTTPServer et un objet d'adresse d'hôte avec l'adresse 1.1.1.3 nommé PublicIP, puis configurer une règle NAT avancée comme suit pour ouvrir le serveur HTTP sur Internet.

From	WAN1 **REMARQUE** : Elle doit en être définie en tant que port WAN et ne peut pas être définie sur Any.
To	Any
Original Source Address	Any
Original Destination Address	PublicIP
Original Services	HTTP
Translated Source Address	Any
Translated Destination Address	HTTPServer
Translated Services	HTTP

Exemple d'utilisation : l'interface sortante (**To**) est définie sur un port WAN, mais l'adresse IP source traduite (**Translated Source Address**) est différente de l'adresse IP publique du port WAN sélectionné.

Par exemple, vous avez fourni une adresse IP statique (1.1.1.3). L'Cisco ISA500est définie en tant que VPN SSL. Vous souhaitez traduire les adresses IP des clients VPN SSL en adresse IP publique spécifique lorsque les clients VPN SSL accèdent à Internet.

Solution : en supposant que l'adresse IP du port WAN1 soit 1.1.1.2 et que le pool d'adresses du client VPN SSL soit défini sur 192.168.200.0 /24. Vous pouvez tout d'abord créer un objet d'adresse d'hôte avec l'adresse 1.1.1.3 PublicIP nommé PublicIP et ensuite créer une règle NAT avancée comme suit pour permettre aux clients de VPN SSL d'accéder à Internet :

From	Any
To	WAN1 **REMARQUE** : Elle doit en être définie en tant que port WAN et ne peut pas être définie sur Any.
Original Source Address	SSLVPNPool
Original Destination Address	Any
Original Services	Any
Translated Source Address	PublicIP
Translated Destination Address	Any
Translated Services	Any

Configuration d'une règle NAT avancée pour prendre en charge la reconnexion NAT

La reconnexion NAT permet aux hôtes du côté LAN d'accéder aux serveurs internes à l'aide de leurs adresses IP externes respectives (adresses IP publiques). Cette section fournit un exemple de configuration sur la façon de créer une règle NAT avancée pour prendre en charge la reconnexion NAT.

ÉTAPE 1 Allez à la page **Networking > Address Management** pour créer un objet d'adresse d'hôte avec l'adresse 192.168.10.100 appelé FTPServer. Le serveur FTP effectue des recherches dans la zone LAN.

ÉTAPE 2 Accédez à la page **Firewall > NAT > Port Forwarding** pour créer une règle de transfert de port comme suit.

Original Service	FTP-CONTROL
Translated Service	FTP-CONTROL
Translated IP	FTPServer
WAN	WAN1
WAN IP	WAN1_IP
Enable Port Forwarding	On
Create Firewall Rule	On

ÉTAPE 3 Une règle de pare-feu est automatiquement créée comme suit pour autoriser l'accès.

From Zone	WAN
To Zone	LAN
Services	FTP-CONTROL
Source Address	ANY
Destination Address	FTPServer
Match Action	Permit

ÉTAPE 4 Passez ensuite à la page **Firewall > NAT > Advanced NAT** pour créer une règle NAT avancée comme suit.

From	DEFAULT
To	Any
Original Source Address	DEFAULT_NETWORK
Original Destination Address	WAN1_IP
Original Services	FTP-CONTROL
Translated Source Address	WAN1_IP
Translated Destination Address	FTPServer
Translated Services	FTP-CONTROL

Exemples de configuration d'une règle de pare-feu et NAT

Cette section fournit des exemples de configuration sur l'ajout de règles de pare-feu et NAT.

- **Autorisation du trafic entrant vers un serveur FTP interne à l'aide de l'adresse IP WAN, page 240**
- **Autorisation du trafic entrant vers un serveur RDP à l'aide d'une adresse IP publique spécifiée, page 241**
- **Autorisation du trafic entrant en provenance de l'intervalle spécifié des hôtes externes, page 244**
- **Blocage du trafic sortant par programmation et par plage d'adresses IP, page 246**
- **Blocage du trafic sortant vers un serveur de messagerie hors site, page 246**

Autorisation du trafic entrant vers un serveur FTP interne à l'aide de l'adresse IP WAN

Exemple d'utilisation : vous hébergez un serveur FTP sur votre LAN. Vous souhaitez ouvrir le serveur FTP à Internet à l'aide de l'adresse IP du port WAN1. Le trafic entrant est adressé à l'adresse IP WAN1 mais est dirigé vers le serveur FTP.

Solution : procédez comme suit pour réaliser la configuration :

ÉTAPE 1 Allez sur la page **Networking > Address Management** pour créer un objet d'adresse d'hôte avec l'adresse 192.168.75.100 nommé InternalFTP.

ÉTAPE 2 Accédez à la page **Firewall > NAT > Port Forwarding** pour créer une règle de transfert de port comme suit.

Original Service	FTP-CONTROL
Translated Service	FTP-CONTROL
Translated IP	InternalFTP
WAN	WAN1
WAN IP	WAN1_IP
Enable Port Forwarding	On

ÉTAPE 3 Passez ensuite à la page **Firewall > NAT > Advanced NAT** pour créer une règle NAT avancée comme suit.

From	WAN1
To	DEFAULT
Original Source Address	ANY
Original Destination Address	WAN1_IP
Original Services	FTP-CONTROL

Translated Source Address	ANY
Translated Destination Address	InternalFTP
Translated Services	FTP-CONTROL

ÉTAPE 4 Passez ensuite à la page **Firewall > Access Control > ACL Rules** pour créer une règle de pare-feu de la façon suivante pour autoriser l'accès :

From Zone	WAN
To Zone	LAN
Services	FTP-CONTROL
Source Address	ANY
Destination Address	InternalFTP
Match Action	Permit

REMARQUE Lorsque vous créez une règle de transfert de port, cochez **Create Firewall Rule** pour générer automatiquement la règle de pare-feu.

Autorisation du trafic entrant vers un serveur RDP à l'aide d'une adresse IP publique spécifiée

Exemples d'utilisation : vous hébergez un serveur RDP sur le DMZ. Votre ISP vous a fourni une adresse IP statique que vous souhaitez exposer au public comme votre adresse de serveur RDP. Vous souhaitez autoriser les utilisateurs Internet à accéder au serveur RDP à l'aide de l'adresse IP publique spécifiée.

Solution 1 : procédez comme suit pour réaliser la configuration :

ÉTAPE 1 Accédez à la page Networking > Address Management pour créer un objet d'adresse d'hôte avec l'adresse 192.168.12.101 nommé « RDPServer » et un objet d'adresse d'hôte avec l'adresse 172.39.202.102 nommé « PublicIP ».

ÉTAPE 2 Accédez à la page Networking > Service Management pour créer un objet service TCP avec le port 3389 nommé « RDP ».

ÉTAPE 3 Accédez à la page Firewall > NAT > Port Forwarding pour créer une règle de transfert de port comme suit.

Original Service	RDP
Translated Service	RDP
Translated IP	RDPServer
WAN	WAN1
WAN IP	PublicIP
Enable Port Forwarding	On
Create Firewall Rule	On

ÉTAPE 4 Ou passez à la page Firewall > NAT > Advanced NAT pour créer une règle NAT avancée comme suit.

From	WAN1
To	DMZ
Original Source Address	ANY
Original Destination Address	PublicIP
Original Services	RDP
Translated Source Address	ANY
Translated Destination Address	RDPServer
Translated Services	RDP

ÉTAPE 5 Passez ensuite à la page Firewall > Access Control > ACL Rules pour créer une règle de pare-feu de la façon suivante pour autoriser l'accès :

From Zone	WAN
To Zone	DMZ
Services	RDP
Source Address	ANY
Destination Address	RDPServer
Match Action	Permit

REMARQUE Lorsque vous créez une règle de transfert de port, cochez **Create Firewall Rule** pour générer automatiquement la règle de pare-feu.

Solution 2 : pour cet exemple d'utilisation, vous pouvez utiliser l'assistant DMZ pour effectuer la configuration.

ÉTAPE 1 Cliquez sur **Configuration Wizards > DMZ Wizard**.

ÉTAPE 2 Dans la page DMZ Configuration, configurez un réseau DMZ, comme suit :

Name	DMZ
IP	192.168.12.1
Netmask	255.255.255.0
Port	GE6
Zone	DMZ

ÉTAPE 3 Dans la page DMZ Service, créez un service DMZ de la manière suivante :

Original Service	RDP
Translated Service	RDP
Translated IP	RDPServer

WAN	WAN1
WAN IP	PublicIP
Enable DMZ Service	On
Create Firewall Rule	On

ÉTAPE 4 Cliquez sur **Finish** pour appliquer vos paramètres.

ÉTAPE 5 Une règle de pare-feu est automatiquement générée comme suit pour autoriser l'accès.

From Zone	WAN
To Zone	DMZ
Services	RDP
Source Address	ANY
Destination Address	RDPServer
Match Action	Permit

Autorisation du trafic entrant en provenance de l'intervalle spécifié des hôtes externes

Exemples d'utilisation : vous souhaitez autoriser l'exécution de la vidéoconférence entrante à partir d'une plage limitée d'adresses IP externes (132.177.88.2 à 132.177.88.254). Dans l'exemple, les connexions pour CU-SeeMe (client de vidéoconférence Internet) sont autorisées uniquement si elles proviennent d'une plage spécifiée d'adresses IP externes.

Solution : procédez comme suit pour réaliser la configuration :

ÉTAPE 1 Accédez à la page Networking > Address Management pour créer un objet d'adresse avec la plage 132.177.88.2 à 132.177.88.254 nommé « OutsideNetwork » et un objet d'adresse d'hôte avec l'adresse 192.168.75.110 nommé « InternalIP ».

ÉTAPE 2 Accédez à la page Firewall > NAT > Port Forwarding pour créer une règle de transfert de port comme suit.

Original Service	CU-SEEME
Translated Service	CU-SEEME
Translated IP	InternalIP
WAN	WAN1
WAN IP	WAN1_IP
Enable Port Forwarding	On
Create Firewall Rule	Off

ÉTAPE 3 Accédez à la page Firewall > Access Control > ACL Rules et créez une règle d'ACL comme il est décrit ci-dessous.

From Zone	WAN
To Zone	LAN
Services	CU-SEEME
Source Address	OutsideNetwork
Destination Address	InternalIP
Match Action	Permit

Blocage du trafic sortant par programmation et par plage d'adresses IP

Exemple d'utilisation : bloquez toute utilisation d'Internet pendant le week-end si la requête provient d'une plage spécifiée d'adresses IP.

Solution : créez un objet d'adresse avec la plage 10.1.1.1 à 10.1.1.100 nommé « TempNetwork » et une programmation appelée « Weekend » pour définir la période pendant laquelle la règle de pare-feu est en vigueur. Créez ensuite une règle de pare-feu comme suit :

From Zone	LAN
To Zone	WAN
Services	HTTP
Source Address	TempNetwork
Destination Address	Any
Schedule	Weekend
Match Action	Deny

Blocage du trafic sortant vers un serveur de messagerie hors site

Exemples d'utilisation : blocage de l'accès au service SMTP pour empêcher un utilisateur d'envoyer des courriels via un serveur de messagerie hors site.

Solution : créez un objet d'adresse d'hôte avec l'adresse IP 10.64.173.20 nommé « OffsiteMail », puis créez une règle de pare-feu comme suit :

From Zone	LAN
To Zone	WAN
Services	SMTP
Source Address	Any
Destination Address	OffsiteMail
Match Action	Deny

Configuration du filtrage du contenu pour contrôler l'accès à internet

Le filtrage du contenu bloque ou autorise l'accès HTTP aux sites Web contenant des mots clés ou des domaines spécifiques. Il contrôle l'accès à certains sites Internet en fonction de l'analyse de son contenu (mot-clé d'URL ou de domaine), plutôt que de sa source ou d'autres critères. Il est largement utilisé sur Internet pour filtrer l'accès Web.

Reportez-vous aux rubriques suivantes :

- **Configuration des profils de stratégie de filtrage du contenu, page 247**
- **Configuration de la liste de contrôle d'accès aux sites Web, page 248**
- **Mappage des profils de stratégie de filtrage du contenu aux zones, page 249**
- **Configuration des paramètres avancés du filtrage du contenu, page 250**

REMARQUE L'activation du filtrage du contenu de pare-feu désactive le filtrage URL Web. L'activation du filtrage URL Web désactive le filtrage du contenu du pare-feu.

Configuration des profils de stratégie de filtrage du contenu

Un profil de stratégie de filtrage du contenu est utilisé pour indiquer quels sites Web sont bloqués ou autorisés.

REMARQUE Jusqu'à 16 profils de stratégie de filtrage du contenu peuvent être configurés sur l'Cisco ISA500.

ÉTAPE 1 Cliquez sur **Firewall > Content Filtering > Content Filtering Policies**.

ÉTAPE 2 Pour ajouter un profil de stratégie de filtrage du contenu, cliquez sur **Add**.

Autres options : pour modifier une entrée, cliquez sur l'icône de **modification** (crayon). Pour supprimer une entrée, cliquez sur l'icône de **suppression** (x).

La page Content Filtering Policies - Add/Edit s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **Policy Profile** : entrez le nom profil de stratégie de filtrage du contenu.
- **Description** : entrez une courte description du profil de stratégie de filtrage du contenu.

ÉTAPE 4 Dans la zone **Website Access Control List**, spécifiez la liste des sites Web que vous souhaitez autoriser ou bloquer. Voir **Configuration de la liste de contrôle d'accès aux sites Web, page 248**.

ÉTAPE 5 Dans la zone **For URLs not specified above**, spécifiez comment traiter les sites Web qui ne sont pas spécifiés dans la liste.

- **Permit them** : si vous choisissez cette option, tous les sites Web non spécifiés dans la liste sont autorisés.
- **Deny them** : si vous choisissez cette option, tous les sites Web non spécifiés dans la liste sont bloqués.

ÉTAPE 6 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 7 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration de la liste de contrôle d'accès aux sites Web

Cette section décrit comment spécifier la liste de contrôle d'accès aux sites Web pour contrôler l'accès à des sites Web spécifiques.

REMARQUE Il est possible de configurer jusqu'à 32 règles d'accès au site Web pour chaque profil de stratégie de filtrage du contenu.

ÉTAPE 1 Dans la zone **Website Access Control List**, cliquez sur **Add** pour ajouter une règle d'accès au site Web.

Autres options : pour modifier une entrée, cliquez sur l'icône de **modification** (crayon). Pour supprimer une entrée, cliquez sur l'icône de **suppression** (x). Pour supprimer toutes les entrées, cliquez sur **Delete All**.

La fenêtre Website Access Control List - Add/Edit s'ouvre.

ÉTAPE 2 Saisissez les informations suivantes :

- **Enable Content Filter URL** : cliquez sur **On** pour activer la règle d'accès au site Web, ou sur **Off** pour créer uniquement la règle d'accès au site Web.
- **URL** : entrez le nom de domaine ou le mot-clé d'URL d'un site Web que vous souhaitez autoriser ou bloquer.

- **Match Type** : indiquez comment faire correspondre cette règle :
  - **Web Site** : si vous choisissez cette option, vous autorisez ou bloquez l'accès HTTP d'un site Web qui correspond parfaitement au domaine que vous avez entré dans le champ **URL**.

    Par exemple, si vous entrez example.com dans le champ URL, cela peut alors correspondre au site Web http://example.com/*, mais ne peut pas correspondre au site Web http://*.example.com.uk/*.
  - **URL Keyword** : si vous choisissez cette option, vous autorisez ou bloquez l'accès HTTP d'un site Web qui contient le mot clé que vous avez entré dans le champ **URL**.

    Par exemple, si vous entrez example dans le champ URL, cela peut alors correspondre aux sites tels que www.example.com, tw.example.com, www.example.com.uk et www.example.co.jp.
- **Action** : choisissez **Permit** pour autoriser l'accès, ou choisissez **Block** pour bloquer l'accès.

ÉTAPE 3 Cliquez sur **OK** pour enregistrer vos paramètres.

Mappage des profils de stratégie de filtrage du contenu aux zones

Utilisez la page Policy to Zone Mapping pour appliquer le profil de stratégie de filtrage du contenu à chaque zone. Le profil de stratégie de filtrage du contenu affecté à chaque zone détermine s'il faut bloquer ou transférer les requêtes HTTP à partir des hôtes de la zone. Les demandes bloquées seront consignées.

ÉTAPE 1 Cliquez sur **Firewall > Content Filtering > Policy to Zone Mapping**.

La fenêtre Policy to Zone Mapping s'ouvre.

ÉTAPE 2 Cliquez sur **On** pour activer la fonctionnalité de filtrage du contenu ou sur **Off** pour la désactiver.

ÉTAPE 3 Spécifiez le profil de stratégie pour chaque zone. Par défaut, le profil par défaut qui autorise tous les sites Web est sélectionné pour toutes les zones nouvelles et prédéfinies.

ÉTAPE 4 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration des paramètres avancés du filtrage du contenu

ÉTAPE 1 Cliquez sur **Firewall > Content Filtering > Advanced Settings**.

ÉTAPE 2 Saisissez les informations suivantes :

- **Filter Traffic on HTTP Port** : entrez le numéro de port utilisé pour filtrer le trafic HTTP. Le filtrage du contenu surveille et contrôle uniquement les visites de sites Web via le port HTTP spécifié. La valeur par défaut est 80.
- **Filter Traffic on HTTPS port** : entrez le numéro de port utilisé pour filtrer le trafic HTTPS. Le filtrage URL Web surveille et contrôle uniquement les visites de sites Web via le port HTTPS spécifié. La valeur par défaut est 443.
- **Blocked Web Components** : vous pouvez bloquer des composants Web comme le proxy, Java, ActiveX et les témoins. Par défaut, tous sont autorisés.
  - **Proxy** : cochez cette case pour bloquer les serveurs proxy, qui peuvent être utilisés pour contourner certaines règles de pare-feu et présenter d'éventuelles failles de sécurité.
  - **Java** : cochez cette case pour bloquer les applets Java pouvant être téléchargées à partir de pages qui les contiennent.
  - **ActiveX** : cochez cette case pour empêcher le téléchargement des applets ActiveX via Internet Explorer.
  - **Cookies** : cochez cette case pour bloquer les cookies, qui contiennent généralement des sessions.
- **Action** : choisissez l'une des actions suivantes lorsqu'une page Web est bloquée :
  - **Display Default Blocked Page when the requested page is blocked** : affiche la page de blocage par défaut si une page Web est bloquée. Si vous choisissez cette option, le message que vous spécifiez dans le champ **Block Message** s'affichera sur la page de blocage par défaut.
  - **Redirect URL** : redirige vers une page Web spécifiée si une page Web est bloquée. Si vous choisissez cette option, entrez l'URL de redirection souhaitée. Vérifiez que l'URL spécifiée est bien autorisée par la liste de contrôle d'accès aux sites Web.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration du filtrage des adresses MAC pour autoriser ou bloquer le trafic

Le filtrage d'adresses MAC autorise et bloque l'accès au réseau à partir de périphériques spécifiques, grâce à l'utilisation d'une liste d'adresse MAC. Les paramètres de filtrage d'adresses MAC s'appliquent pour l'ensemble du trafic excepté le trafic Intra-VLAN et Intra-SSID.

ÉTAPE 1 Cliquez sur **Firewall > MAC Filtering > MAC Address Filtering**.

La fenêtre MAC Address Filtering s'ouvre.

ÉTAPE 2 Cliquez sur **On** pour activer la fonctionnalité de filtrage d'adresses MAC ou sur **Off** pour la désactiver.

ÉTAPE 3 Si vous activez le filtrage d'adresses MAC, choisissez l'une des options suivantes comme stratégie de filtrage d'adresses MAC :

- **Block MAC Addresses (and allow all others)** : les adresses MAC de la liste sont bloquées et toutes les autres adresses MAC non incluses dans la liste sont autorisées.
- **Allow MAC Addresses (and block all others)** : seules les adresses MAC de la liste sont autorisées et toutes les autres adresses MAC non incluses dans la liste sont bloquées.

ÉTAPE 4 Dans la zone **MAC Address Filtering Rules**, spécifiez la liste d'adresses MAC. Pour ajouter une adresse MAC, cliquez sur **Add**. Pour modifier une entrée, cliquez sur l'icône de **modification** (crayon). Pour supprimer une entrée, cliquez sur l'icône de **suppression** (x). Pour supprimer plusieurs entrées, cochez-les et cliquez sur **Delete**.

Par exemple, si vous cliquez sur **Add**, la fenêtre MAC Address Filtering Rule - Add/Edit s'ouvre. Sélectionnez l'objet d'adresse MAC dans la liste déroulante **MAC Address** et cliquez sur **OK**. Si l'objet d'adresse MAC que vous souhaitez ne figure pas dans la liste, choisissez **Create a new address** pour créer un nouvel objet d'adresse MAC. Pour gérer les objets d'adresse MAC, accédez à la page Networking > Address Management. Voir **Gestion d'adresse, page 182**.

ÉTAPE 5 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration de la liaison IP-MAC pour empêcher l'usurpation d'adresse

L'association IP/MAC vous permet de lier une adresse IP à une adresse MAC, et vice-versa. Elle autorise uniquement le trafic lorsque l'adresse IP hôte correspond à une adresse de MAC spécifiée. En demandant à la passerelle de valider l'adresse IP du trafic source avec l'adresse MAC unique du périphérique, cela garantit que le trafic de l'adresse IP spécifiée n'est pas frauduleux. En case de violation (l'adresse IP source du trafic ne correspond pas à l'adresse MAC attendue avec la même adresse IP), les paquets sont abandonnés et peuvent être consignés à des fins le diagnostic.

REMARQUE Il est possible de configurer jusqu'à 100 règles de liaison IP-MAC sur l'Cisco ISA500.

ÉTAPE 1 Cliquez sur **Firewall > MAC Filtering > IP - MAC Binding Rules**.

La fenêtre IP - MAC Binding Rules s'ouvre.

ÉTAPE 2 Pour ajouter une règle de liaison IP-MAC, cliquez sur **Add**.

Autres options : pour modifier une entrée, cliquez sur l'icône de **modification** (crayon). Pour supprimer une entrée, cliquez sur l'icône de **suppression** (x). Pour supprimer plusieurs entrées, cochez-les et cliquez sur **Delete**.

La fenêtre IP&MAC Binding Rule - Add/Edit s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **Name** : entrez le nom de la règle de liaison IP-MAC.
- **MAC Address** : sélectionnez un objet d'adresse MAC existant. Si l'objet d'adresse MAC que vous souhaitez ne figure pas dans la liste, choisissez **Create a new address** pour ajouter un nouvel objet d'adresse MAC. Pour gérer les objets d'adresse MAC, accédez à la page Networking > Address Management. Voir **Gestion d'adresse, page 182**.
- **IP Address** : sélectionnez l'objet d'adresse IP existant à lier avec l'adresse MAC sélectionnée. Si l'objet d'adresse IP que vous souhaitez ne figure pas dans la liste, choisissez **Create a new address** pour ajouter un nouvel objet d'adresse IP. Pour gérer les objets Adresse IP, accédez à la page Networking > Address Management. Voir **Gestion d'adresse, page 182**.
- **Log Dropped Packet** : sélectionnez **Enable** pour consigner tous les paquets qui sont abandonnés. Sinon, sélectionnez **Disable**.

ÉTAPE 4 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 5 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration de la protection contre les attaques

Utilisez la page Attack Protection pour spécifier comment protéger votre réseau contre les principaux types d'attaques, notamment la détection, l'inondation et les orages d'écho.

ÉTAPE 1 Cliquez sur **Firewall > Attack Protection**.

ÉTAPE 2 Dans la zone **WAN Security Checks**, entrez les informations suivantes :

- **Block Ping WAN Interface** : cochez cette option pour empêcher les agresseurs d'utiliser les demandes d'écho (ping) ICMP pour accéder à votre réseau. Nous vous conseillons de désactiver cette fonctionnalité uniquement si vous devez laisser l'Cisco ISA500 répondre aux requêtes ping à des fins de diagnostic.
- **Stealth Mode** : cochez cette case pour empêcher l'Cisco ISA500 de répondre aux demandes de connexion entrante en provenance des ports WAN. En mode furtif, l'Cisco ISA500 ne répond pas aux demandes de connexion entrantes bloquées et votre réseau est moins exposé à la détection et aux attaques.
- **Block TCP Flood** : cochez cette case pour abandonner tous les paquets TCP non valides. Cette fonctionnalité protège votre réseau contre une attaque de type inondation SYN, dans laquelle un pirate envoie une succession de requêtes SYN (synchronize) à un système cible. Elle bloque les attaques de type inondation TCP SYN (plus de 200 paquets simultanés de TCP par seconde) à partir des ports WAN.

ÉTAPE 3 Dans la section **LAN Security Checks**, entrez les informations suivantes :

- **Block UDP Flood :** cochez cette case pour limiter le nombre de connexions UDP actives simultanées à partir d'un seul ordinateur sur le LAN. Si vous activez cette fonctionnalité, entrez également le nombre de connexions à autoriser par hôte par seconde. La valeur par défaut est 500 et la plage valide est comprise entre 100 et 10 000. Lorsque cette limite est atteinte, l'Cisco ISA500 la considère comme une attaque par inondation UDP et abandonne toutes les connexions à partir de l'hôte.

ÉTAPE 4 Dans la zone **Firewall Settings**, entrez les informations suivantes :

- **Block ICMP Notification** : cochez cette case pour activer le blocage automatique sans envoyer de notification ICMP à l'expéditeur. Certains protocoles, tels que la découverte du MTU de chemin, nécessitent des notifications ICMP.
- **Block Fragmented Packets** : cochez cette case pour bloquer les paquets fragmentés de ANY à ANY.
- **Block Multicast Packets** : cochez cette case pour bloquer les paquets de multidiffusion. Par défaut, le pare-feu bloque tous les paquets de multidiffusion. Cette fonctionnalité a une priorité plus élevée que les règles de pare-feu, ce qui signifie que les règles de pare-feu qui autorisent le trafic de diffusion sont ignorées si vous activez cette fonctionnalité.

ÉTAPE 5 Dans la zone **DoS Attacks**, saisissez les informations suivantes :

- **SYN Flood Detect Rate** : entrez le nombre maximal de paquets SYN par seconde qui permettra à l'Cisco ISA500 de déterminer qu'une intrusion de type inondation SYN est en train de se produire. Entrez une valeur entre 0 et 65535 paquets de SYN par seconde. La valeur par défaut est de 128 paquets SYN par seconde. Une valeur égale à zéro (0) indique que la fonctionnalité SYN Flood Detect est désactivée.
- **Echo Storm** : entrez le nombre de commandes Ping par seconde qui permettra à l'Cisco ISA500 de déterminer qu'un événement d'intrusion de type orage d'écho est en train de se produire. Entrez une valeur entre 0 et 65535 paquets de requêtes ping par seconde. La valeur par défaut est de 15 paquets de requêtes ping par seconde. Une valeur égale à zéro (0) indique que la fonctionnalité Echo Storm est désactivée.
- **ICMP Flood** : saisissez le nombre de paquets ICMP par seconde, y compris les paquets PING, qui permettra à l'Cisco ISA500 de déterminer qu'un événement d'intrusion de type inondation ICMP est en train de se produire. Entrez une valeur entre 0 et 65535 de paquets ICMP par seconde. La valeur par défaut est de 100 paquets ICMP par seconde. Une valeur égale à zéro (0) indique que la fonctionnalité ICMP Flood est désactivée.

  REMARQUE : lorsque l'un des niveaux d'attaque DoS est dépassé, ce type de trafic est abandonné.

ÉTAPE 6 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration des limites de session

Utilisez la page Session Limits pour configurer le nombre maximal de sessions de connexion. Lorsque la table de connexion est pleine, les nouvelles sessions qui accèdent à l'Cisco ISA500 sont abandonnées.

ÉTAPE 1 Cliquez sur **Firewall > Session Limits**.

ÉTAPE 2 Saisissez les informations suivantes :

- **Current All Connections** : affiche le nombre total de connexions actuelles. Cliquez sur **Disconnect All** pour nettoyer toutes les sessions connectées.
- **Maximum Connections** : Limite le nombre de connexions TCP et UDP. Entrez une valeur comprise entre 1000 et 60000. La valeur par défaut est 60000.
- **TCP Timeout** : entrez la durée d'expiration en secondes pour la session TCP. Les sessions TCP inactives sont supprimées de la table de session après cette période. La plage valide est comprise entre 5 et 3600 secondes. La valeur par défaut est 1200 secondes.
- **UDP Timeout** : entrez la durée d'expiration en secondes pour la session UDP. Les sessions UDP inactives sont supprimées de la table de session après cette période. La plage valide est comprise entre 5 et 3600 secondes. La valeur par défaut est de 180 secondes.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration de la passerelle de niveau application

L'Cisco ISA500 peut fonctionner comme une Application Level Gateway (ALG) pour autoriser certaines applications incompatibles NAT (telles que SIP ou H.323) de fonctionner correctement avec l'Cisco ISA500.

Si le service VoIP (Voice over IP) est utilisé dans votre organisation, vous devez activer H.323 ALG ou SIP ALG pour ouvrir les ports nécessaires pour permettre la VoIP via votre périphérique vocal. Les ALG sont créées pour fonctionner dans un environnement NAT pour maintenir la sécurité pour l'équipement privé de conférence protégé par votre périphérique vocal.

Vous pouvez utiliser H.323 ALG et SIP ALG en même temps, si nécessaire. Pour déterminer quelle ALG utiliser, reportez-vous à la documentation fournie avec vos périphériques ou applications de voix sur IP.

ÉTAPE 1 Cliquez sur **Firewall > Application Level Gateway**.

La fenêtre Application Level Gateway s'ouvre.

ÉTAPE 2 Saisissez les informations suivantes :

- **SIP Support** : SIP ALG peut réécrire les informations dans les messages SIP (en-têtes SIP et corps SDP) pour permettre le trafic audio et la signalisation entre le client situé derrière le périphérique NAT et le point d'extrémité SIP. Sélectionnez ou désélectionnez cette case pour activer ou désactiver la prise en charge d'une passerelle de couche Application SIP (Session Initiation Protocol).

  REMARQUE : Activez SIP ALG lorsque les périphériques vocaux, tels que des téléphones UC500, UC300 ou SIP sont connectés au réseau derrière l'Cisco ISA500.

- **Prise en charge de H.323** : H.323 est une suite de protocoles standard de téléconférence qui fournit de l'audio, des données et de la vidéoconférence. Elle permet la communication point à point et multipoint en temps réel entre les ordinateurs clients sur un réseau à base de paquets qui n'offre pas une qualité de service garantie. Sélectionnez ou désélectionnez cette case pour activer ou désactiver la prise en charge d'une passerelle de couche Application H.323.

- **FTP Support on TCP port** : cochez la case pour activer la prise en charge de FTP ou décochez la case pour désactiver cette fonctionnalité. Choisissez ensuite un port d'écoute. Le port par défaut est FTP-CONTROL (21).

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

7

Services de sécurité

Ce chapitre décrit comment configurer les services de sécurité de la gestion unifiée des menaces (UTM) pour assurer une protection contre les menaces Internet. Il comprend les sections suivantes :

- **À propos des services de sécurité, page 258**
- **Activation des services de sécurité, page 259**
- **Priorité des services de sécurité, page 260**
- **Tableau de bord des services de sécurité, page 260**
- **Affichage des rapports de services de sécurité, page 262**
- **Configuration de l'antivirus, page 269**
- **Configuration du contrôle des applications, page 277**
- **Configuration du filtre de courrier indésirable, page 289**
- **Configuration de la prévention des intrusions, page 290**
- **Configuration du filtrage par réputation Web, page 296**
- **Configuration du filtrage URL Web, page 298**
- **Réputation de réseau, page 302**

Pour accéder aux pages de services de sécurité, cliquez sur **Security Services** dans le volet de navigation de gauche.

À propos des services de sécurité

L'Cisco ISA500 prend en charge divers services de sécurité UTM pour assurer la protection de votre réseau contre les menaces Internet. Par défaut, tous les services de sécurité, à l'exception de la réputation de réseau sont désactivés.

Le tableau suivant présente tous les services de sécurité disponibles sur l'Cisco ISA500.

Service de sécurité	Description
Antivirus	L'antivirus empêche les menaces envers le réseau sur de nombreux protocoles, tels que HTTP, FTP, POP3, SMTP, CIFS, NETBIOS et IMAP. Voir **Configuration de l'antivirus, page 269**.
Contrôle des applications	Le contrôle des applications surveille et contrôle l'utilisation d'applications sur votre réseau. Voir **Configuration du contrôle des applications, page 277**.
Filtre de courrier indésirable	Le filtre de courrier indésirable détecte le score de réputation de l'expéditeur de l'e-mail. Si le score de réputation est situé sous le seuil, l'e-mail est bloqué ou marqué comme courrier indésirable ou suspecté de courrier indésirable. Voir **Configuration du filtre de courrier indésirable, page 289**.
Prévention des intrusions (IPS)	L'IPS surveille le trafic réseau pour détecter les comportements malveillants ou indésirables et peut répondre, en temps réel, en bloquant ou en empêchant ces activités. Voir **Configuration de la prévention des intrusions, page 290**.
Réputation de réseau	La réputation de réseau bloque le trafic entrant provenant des adresses IP connues pour lancer des attaques sur Internet. Voir **Réputation de réseau, page 302**.

Service de sécurité	Description
Filtrage par réputation Web	Le filtrage par réputation Web empêche les périphériques clients d'accéder à des sites Web dangereux contenant des virus, des logiciels espions, des programmes malveillants ou des liens d'hameçonnage. Voir **Configuration du filtrage par réputation Web, page 296**.
Filtrage URL Web	Le filtrage URL Web vous permet de bloquer l'accès HTTP aux sites Web malveillants en fonction des catégories d'URL. Voir **Configuration du filtrage URL Web, page 298**.

L'antivirus, le contrôle des applications et l'IPS sont des services de sécurité basés sur les signatures. Vous devez mettre à jour régulièrement les signatures pour vous assurer que ces services de sécurité vous apportent la meilleure protection.

Le filtre de courrier indésirable, la réputation de réseau, le filtrage par réputation Web et le filtrage URL Web sont des services de sécurité basés sur la réputation. Ils obtiennent les données de sécurité des serveurs SecApps et déterminent quel trafic est autorisé ou bloqué. Vérifiez que les serveurs SecApps sont bien en ligne après l'activation de ces services de sécurité ; dans le cas contraire, ils ne seront pas disponibles.

Activation des services de sécurité

Les services de sécurité sont sous licence. Vous devez installer une licence de sécurité valide sur l'Cisco ISA500 pour activer les services de sécurité. Une licence de sécurité valide est également requise pour la prise en charge de SSLVPN avec les périphériques mobiles, tels que les téléphones intelligents et les tablettes. La clé d'autorisation de produit (PAK) est nécessaire pour valider la licence de sécurité. Vous pouvez trouver le code de licence sur le certificat de demande de licence logicielle que Cisco fournit à l'achat de l'appliance de sécurité.

Vérifiez que la licence de sécurité est bien installée et n'expire pas avant la configuration des services de sécurité. Accédez à la page Device Management > License Management pour valider la licence de sécurité ou pour la renouveler avant qu'elle arrive à expiration. Voir **Installation ou renouvellement de la licence de sécurité, page 418**.

Priorité des services de sécurité

Plusieurs services de sécurité peuvent fonctionner simultanément pour protéger votre réseau. Le filtrage par réputation Web est plus prioritaire que le filtrage URL Web. Vous pouvez ajouter les exceptions de site Web dans la liste de contrôle d'accès aux sites Web lorsque vous configurez un profil de stratégie de filtrage URL Web. Les exceptions de site Web peuvent ignorer les paramètres de catégorie d'URL du profil, mais ne peuvent pas remplacer les paramètres de filtrage par réputation Web.

Par exemple, un site Web en tant qu'exception dispose d'une autorisation d'accès par filtrage URL Web, mais a un score de réputation inférieur au seuil de réputation Web spécifié dans le filtrage par réputation Web. Le filtrage par réputation Web bloquera l'accès à ce site Web même s'il s'agit d'une exception de la liste de contrôle d'accès aux sites Web, sauf si vous avez modifié le seuil de réputation Web.

Tableau de bord des services de sécurité

Utilisez la page Dashboard pour afficher l'état de la licence de sécurité, pour activer ou désactiver les services de sécurité, et pour rechercher les mises à jour de signatures pour tous les services de sécurité basés sur les signatures.

ÉTAPE 1 Cliquez sur **Security Services > Dashboard**.

La fenêtre Dashboard s'ouvre.

ÉTAPE 2 Dans la zone **License Status**, l'état de la licence de sécurité s'affiche. Si la licence de sécurité arrive à expiration, accédez à la page Device Management > License Management pour la renouveler. Voir **Installation ou renouvellement de la licence de sécurité, page 418**.

ÉTAPE 3 Dans la zone **Settings Summary**, vous pouvez effectuer les tâches suivantes :

- Pour activer un service de sécurité, cochez la case dans la colonne **Enable**. Par défaut, seule la réputation de réseau est activée.
- Pour configurer les paramètres d'un service de sécurité, cliquez sur **Configure**.

- Pour rechercher immédiatement de nouvelles mises à jour de services de sécurité, cliquez sur **Check for Updates Now**.
  - Pour les services de sécurité basés sur les signatures tels que l'antivirus, le contrôle des applications et l'IPS, cliquez sur ce bouton pour rechercher les mises à jour de signatures à partir du serveur de signatures Cisco. L'antivirus et l'IPS utilisent des bases de données de signatures différentes, mais l'IPS et le contrôle des applications utilisent la même base de données de signatures. Cette opération lancera une recherche de toutes les mises à jour de signatures à la fois. Si un nouveau fichier de signatures plus récent que le fichier actuel est disponible sur le serveur, le nouveau fichier de signatures est téléchargé sur votre périphérique.

    REMARQUE : Un compte Cisco.com valide est requis pour rechercher les mises à jour de signatures à partir du serveur de signatures Cisco. Accédez à la page Device Management > Cisco.com Account pour configurer vos informations d'identification de compte Cisco.com sur l'Cisco ISA500. Voir **Configuration d'un compte Cisco.com, page 399**.
  - Pour les services de sécurité basés sur la réputation, tels que le filtre de courrier indésirable, le filtrage URL Web, le filtrage par réputation Web et la réputation de réseau, cliquez sur ce bouton pour rechercher de nouvelles mises à jour de la réputation de réseau. Cette opération ne lance pas de recherche de nouvelles mises à jour pour le filtre de courrier indésirable, le filtrage URL Web et le filtrage par réputation Web.

  La date et l'heure de votre dernière vérification sont affichées dans la colonne **Last Check**. Lorsqu'un fichier de signatures a bien été mis à jour, la date et l'heure de la dernière mise à jour réussie s'affichent dans la colonne **Last Update**.
- Le filtre de courrier indésirable, le filtrage URL Web, le filtrage par réputation Web et la réputation de réseau obtiennent les données de sécurité des serveurs SecApps et déterminent quel trafic est autorisé ou bloqué. La colonne **Server Status** affiche l'état des serveurs SecApps. Vérifiez que les serveurs SecApps sont bien en ligne après l'activation de ces services de sécurité ; dans le cas contraire, ils ne seront pas disponibles.

ÉTAPE 4 Dans la zone **External Web Proxy Settings**, spécifiez un proxy Web externe utilisé pour rediriger le trafic HTTP si nécessaire :

- **External Web Proxy** : cliquez sur **On** pour prendre en charge un proxy Web externe, par exemple Scansafe et un proxy Web sortant tiers, ou cliquez sur **Off** pour le désactiver.

REMARQUE : Lorsque la fonctionnalité de proxy Web externe est activée, les paramètres de pare-feu, de la QoS, de filtrage URL Web et de filtrage par réputation Web ne fonctionnent pas ou sont ignorés pour le trafic HTTP.

- **Redirected Web Proxy IP Address** : entrez l'adresse IP du proxy Web externe utilisé pour rediriger le trafic HTTP.
- **Redirected HTTP Ports** : indiquez les ports de proxy. Pour ajouter une entrée, cliquez sur **Add**. Pour modifier une entrée, cliquez sur l'icône de **modification** (crayon). Pour supprimer une entrée, cliquez sur l'icône de **suppression** (x).

ÉTAPE 5 Cliquez sur **Save** pour appliquer vos paramètres.

Affichage des rapports de services de sécurité

Reportez-vous à la page Security Services Reports pour consulter les rapports relatifs à tous les services de sécurité. Pour ouvrir la page, cliquez sur **Security Services > Security Services Reports**. Cette page est automatiquement mise à jour toutes les 10 secondes. Cliquez sur **Refresh** pour actualiser manuellement les données. Reportez-vous aux rubriques suivantes :

- **Affichage du rapport de sécurité Web, page 262**
- **Affichage du rapport antivirus, page 264**
- **Affichage du rapport de sécurité de la messagerie, page 265**
- **Affichage du rapport de réputation de réseau, page 266**
- **Affichage du rapport IPS, page 267**
- **Affichage du rapport de contrôle des applications, page 268**

REMARQUE Les rapports de services de sécurité sont actifs uniquement après l'installation de la licence de sécurité. Avant de choisir un rapport à afficher, vérifiez que le service de sécurité correspondant est activé.

Affichage du rapport de sécurité Web

Ce rapport indique le nombre de demandes d'accès Web consignées et le nombre de sites Web bloqués par le filtrage URL Web, le filtrage par réputation Web, ou les deux.

ÉTAPE 1 Dans l'onglet **Web Security**, indiquez les informations suivantes :

- **Enable** : cochez cette case pour activer le rapport de sécurité Web ou décochez-la pour le désactiver.
- **Blocked Requests** : cochez cette case pour afficher le nombre de sites Web bloqués par le filtrage URL Web et/ou le filtrage par réputation Web dans le graphique. Pour afficher des informations supplémentaires sur les requêtes bloquées, cliquez sur la barre rouge dans le graphique. Une fenêtre contextuelle affiche les informations suivantes pour chaque requête bloquée : la date et l'heure, l'adresse IP et l'adresse MAC de l'hôte qui a émis la demande, le site Web, l'URL bloquée, le filtre qui a bloqué la requête, et le nombre de fois que la connexion a été bloquée.
- **Processed Requests** : cochez cette case pour afficher le nombre de demandes d'accès Web consignées par le filtrage URL Web et/ou le filtrage par réputation Web dans le graphique.

ÉTAPE 2 Cliquez sur **Save** pour appliquer vos paramètres.

Champ	Description
System Date	Heure système actuelle.
Total Since Activated	Nombre total de demandes d'accès Web traitées et nombre total de sites Web bloqués depuis l'activation du filtrage URL Web et du filtrage par réputation Web.
Total Last 7 Days	Nombre total de demandes d'accès Web traitées et nombre total de sites Web bloqués au cours des sept derniers jours.
Total Today	Nombre total de demandes d'accès Web traitées et nombre total de sites Web bloqués en une journée.
Graph	Nombre total de demandes d'accès Web traitées et nombre total de sites Web bloqués par jour au cours des sept derniers jours.

Affichage du rapport antivirus

Ce rapport indique le nombre de fichiers vérifiés et le nombre de virus détectés par le service antivirus.

ÉTAPE 1 Dans l'onglet **Anti-Virus**, indiquez les informations suivantes :

- **Enable** : cochez cette case pour activer le rapport antivirus ou décochez-la pour le désactiver.
- **Detected Requests** : cochez cette case pour afficher le nombre de virus détectés par le service antivirus dans le graphique. Pour afficher des informations supplémentaires sur les requêtes détectées, cliquez sur la barre rouge dans le graphique. Une fenêtre contextuelle affiche les informations suivantes pour chaque requête détectée : la date et l'heure, l'adresse IP et l'adresse MAC de la source et de la destination, le protocole utilisé pour la connexion, la mesure prise et le nombre de fois qu'un virus a été trouvé.
- **Processed Requests** : cochez cette case pour afficher le nombre de fichiers vérifiés par le service antivirus dans le graphique.

ÉTAPE 2 Cliquez sur **Save** pour appliquer vos paramètres.

Champ	Description
System Date	Heure système actuelle.
Total Since Activated	Nombre total de fichiers vérifiés et nombre total de virus détectés depuis l'activation du service antivirus.
Total Last 7 Days	Nombre total de fichiers vérifiés et nombre total de virus détectés au cours des sept derniers jours.
Total Today	Nombre total de fichiers vérifiés et nombre total de virus détectés en une journée.
Graph	Nombre total de fichiers vérifiés et nombre total de virus détectés par jour au cours des derniers sept jours.

Affichage du rapport de sécurité de la messagerie

Ce rapport indique le nombre d'e-mails vérifiés et le nombre d'e-mails indésirables ou suspectés d'être indésirables détectés par le service de filtre de courrier indésirable.

ÉTAPE 1 Dans l'onglet **Email Security**, indiquez les informations suivantes :

- **Enable** : cochez cette case pour activer le rapport de sécurité de la messagerie ou décochez-la pour le désactiver.
- **Blocked Requests** : cochez cette case pour afficher dans le graphique le nombre d'e-mails indésirables ou suspectés d'être indésirables, détectés par le service de filtre de courrier indésirable.
- **Processed Requests** : cochez cette case pour afficher dans le graphique le nombre d'e-mails vérifiés par le service de filtre de courrier indésirable.

ÉTAPE 2 Cliquez sur **Save** pour appliquer vos paramètres.

Champ	Description
System Date	Heure système actuelle.
Total Since Activated	Nombre total d'e-mails vérifiés et nombre total d'e-mails indésirables ou suspectés d'être indésirables détectés depuis l'activation du service de filtre de courrier indésirable.
Total Last 7 Days	Nombre total d'e-mails vérifiés et nombre total d'e-mails indésirables ou suspectés d'être indésirables détectés au cours des sept derniers jours.
Total Today	Nombre total d'e-mails vérifiés et nombre total d'e-mails indésirables ou suspectés d'être indésirables détectés en une journée.
Graph	Nombre total d'e-mails vérifiés et nombre total d'e-mails indésirables ou suspectés d'être indésirables détectés par jour au cours des sept derniers jours.

Affichage du rapport de réputation de réseau

Ce rapport indique le nombre de paquets vérifiés et le nombre de paquets bloqués par le service de réputation de réseau.

ÉTAPE 1 Dans l'onglet **Network Reputation**, indiquez les informations suivantes :

- **Enable** : cochez cette case pour activer le rapport de réputation de réseau ou décochez-la pour le désactiver.
- **Blocked Requests** : cochez cette case pour afficher dans le graphique le nombre de paquets bloqués par le service de réputation de réseau.
- **Processed Requests** : cochez cette case pour afficher dans le graphique le nombre de paquets vérifiés par le service de réputation de réseau.

ÉTAPE 2 Cliquez sur **Save** pour appliquer vos paramètres.

Champ	Description
System Date	Heure système actuelle.
Total Since Activated	Nombre total de paquets vérifiés et nombre total de paquets bloqués depuis l'activation du service de réputation de réseau.
Total Last 7 Days	Nombre total de paquets vérifiés et nombre total de paquets bloqués au cours des sept derniers jours.
Total Today	Nombre total de paquets vérifiés et nombre total de paquets bloqués en une journée.
Graph	Nombre total de paquets vérifiés et nombre total de paquets bloqués par jour au cours des sept derniers jours.

Affichage du rapport IPS

Ce rapport indique le nombre de paquets détectés et le nombre de paquets abandonnés par le service IPS.

ÉTAPE 1 Dans l'onglet **IPS**, indiquez les informations suivantes :

- **Enable** : cochez cette case pour activer le rapport IPS ou décochez-la pour le désactiver.
- **Blocked Requests** : cochez cette case pour afficher dans le graphique le nombre de paquets abandonnés par le service IPS. Pour afficher des informations supplémentaires sur les requêtes bloquées, cliquez sur la barre rouge dans le graphique. Une fenêtre contextuelle affiche les informations suivantes pour chaque requête bloquée : la date et l'heure, l'adresse IP et l'adresse MAC de la source et de la destination, la mesure prise et le nombre de fois que cet événement a été détecté.
- **Processed Requests** : cochez cette case pour afficher dans le graphique le nombre de paquets détectés par le service IPS.

ÉTAPE 2 Cliquez sur **Save** pour appliquer vos paramètres.

Champ	Description
System Date	Heure système actuelle.
Total Since Activated	Nombre total de paquets détectés et nombre total de paquets abandonnés depuis l'activation du service IPS.
Total Last 7 Days	Nombre total de paquets détectés et nombre total de paquets abandonnés au cours des sept derniers jours.
Total Today	Nombre total de paquets détectés et nombre total de paquets abandonnés en une journée.
Graph	Nombre total de paquets détectés et nombre total de paquets abandonnés par jour au cours des sept derniers jours.

Affichage du rapport de contrôle des applications

Ce rapport indique le nombre de paquets détectés et le nombre de paquets bloqués par le service de contrôle des applications.

ÉTAPE 1 Dans l'onglet **Application Control**, indiquez les informations suivantes :

- **Enable** : cochez cette case pour activer le rapport de contrôle des applications ou décochez-la pour le désactiver.
- **Blocked Requests** : cochez cette case pour afficher dans le graphique le nombre de paquets abandonnés par le service de contrôle des applications. Pour afficher des informations supplémentaires sur les requêtes bloquées, cliquez sur la barre rouge dans le graphique. Une fenêtre contextuelle affiche les informations suivantes pour chaque requête bloquée : la date et l'heure, l'adresse IP et l'adresse MAC de l'hôte qui a émis la demande, l'application bloquée et le nombre de fois que l'application a été bloquée.
- **Processed Requests** : cochez cette case pour afficher dans le graphique le nombre de paquets détectés par le service de contrôle des applications.

ÉTAPE 2 Cliquez sur **Save** pour appliquer vos paramètres.

Champ	Description
System Date	Heure système actuelle.
Total Since Activated	Nombre total de paquets détectés et nombre total de paquets bloqués depuis l'activation du service de contrôle des applications.
Total Last 7 Days	Nombre total de paquets détectés et nombre total de paquets bloqués au cours des sept derniers jours.
Total Today	Nombre total de paquets détectés et nombre total de paquets bloqués en une journée.
Graph	Nombre total de paquets détectés et nombre total de paquets bloqués par jour au cours des sept derniers jours.

Configuration de l'antivirus

L'antivirus protège votre réseau contre les virus et programmes malveillants. L'antivirus recherche les virus sur de nombreux protocoles, tels que HTTP, FTP, POP3, SMTP, CIFS, NETBIOS et IMAP.

REMARQUE L'antivirus protège contre les menaces les plus récentes et répandues, mais n'est pas en mesure de détecter tous les virus connus (notamment, les virus rares). Il offre une " défense de première couche ", gère efficacement les attaques par programmes malveillants et détecte les plus répandus et dangereux (communément appelés les programmes malveillants " in-the-wild "). Actuellement, les types de programmes malveillants les plus répandus sont les vers, les chevaux de Troie, les exploits, les virus et les dissimulateurs d'activité. Au fur et à mesure que de nouvelles menaces font leur apparition, l'antivirus est mis à jour pour inclure les plus dangereuses.

Vous pouvez appliquer le service antivirus aux zones. L'antivirus examine l'ensemble du trafic entrant et sortant pour les zones sélectionnées et exécute l'action que vous spécifiez pour les différents types de trafic. Vous pouvez choisir d'abandonner la connexion, de supprimer les fichiers infectés et/ou d'envoyer une alerte par e-mail au destinataire des e-mails si les virus sont détectés.

Les fichiers contenant le code malveillant et les virus peuvent être compressés. Un antivirus peut donc automatiquement décompresser les fichiers compressés et analyser ensuite les virus. L'antivirus prend en charge l'analyse des fichiers compressés à niveau unique pour les types de fichiers suivants : zip, gzip, tar, rar 2.0 et bz2 (Bzip).

L'antivirus utilise les signatures pour identifier les fichiers infectés. Vous devez mettre à jour régulièrement les signatures pour que la protection reste à jour. Voir **Mise à jour des signatures antivirus, page 276**.

Vous pouvez activer le rapport antivirus à partir de la page Security Services > Security Services Reports ou de la page Status > Security Services Reports pour afficher le nombre de fichiers vérifiés et le nombre de virus détectés par le service antivirus. Voir **Affichage du rapport antivirus, page 264**.

Vous pouvez activer la fonctionnalité d'alerte antivirus pour envoyer un e-mail d'alerte à une adresse e-mail indiquée lors d'événements de virus et selon un intervalle spécifié. Voir **Configuration des paramètres d'alerte par courriel, page 382**.

Reportez-vous aux rubriques suivantes :

- **Paramètres antivirus généraux, page 270**

- Configuration des paramètres antivirus avancés
- Configuration de la notification HTTP, page 274
- Configuration de la notification par e-mail, page 275
- Mise à jour des signatures antivirus, page 276

Paramètres antivirus généraux

Utilisez la page General Settings pour activer ou désactiver l'antivirus, spécifier les zones de recherche de virus, configurer les actions de prévention pour les différents types de trafic et choisir la taille de fichier maximale à analyser.

ÉTAPE 1 Cliquez sur **Security Services > Anti-Virus > General Settings**.

ÉTAPE 2 Cliquez sur **On** pour activer l'antivirus ou sur **Off** pour le désactiver.

ÉTAPE 3 Dans la zone **Zone to Scan**, spécifiez les zones d'analyse de virus :

- **WAN Zone** : choisissez cette option pour analyser les virus sur l'ensemble du trafic entrant et sortant de la zone WAN.
- **WAN+VPN Zone** : choisissez cette option pour analyser les virus sur l'ensemble du trafic entrant et sortant des zones WAN et VPN.
- **All Zone** : sélectionnez cette option pour analyser les virus sur l'ensemble du trafic entrant et sortant de toutes les zones.

ÉTAPE 4 Dans la zone **Applications to Scan**, effectuez les tâches suivantes pour rechercher les virus sur votre réseau :

- **Enable** : cochez la case dans cette colonne pour rechercher les virus sur un protocole.
- **Logging** : cochez la case dans cette colonne pour consigner les événements lorsque les virus sont détectés.

  Pour consigner les événements d'antivirus, vous devez d'abord cocher la case **Logging** pour les protocoles, puis accéder aux pages Device Management > Logs pour configurer les paramètres et les utilitaires du journal. Voir Gestion des journaux, page 421.

- Pour enregistrer les journaux d'antivirus dans le daemon syslog local, vous devez activer la fonctionnalité de journal, définir la taille de la mémoire tampon du journal et le niveau de gravité pour les journaux locaux, puis activer les paramètres des journaux locaux pour l'utilitaire d'antivirus.
- Pour enregistrer les journaux d'antivirus dans le serveur syslog à distance si vous disposez d'une assistance de serveur syslog à distance, vous devez activer la fonctionnalité de journal, spécifier les paramètres de journal à distance et activer les paramètres de journal à distance pour l'utilitaire d'antivirus.

▪ **Action** : spécifiez l'action de prévention pour les différents types de trafic lorsque les virus sont détectés. Le tableau suivant répertorie toutes les actions disponibles pour chaque protocole.

Protocol	Action
HTTP	**None** : aucune action n'est requise lorsque les virus sont détectés. **Notify** : envoyer un message d'alerte à l'utilisateur lorsque les virus sont détectés dans les pages Web ou dans les fichiers auxquels l'utilisateur tente d'accéder. **Notify + Drop Connection** : abandonner la connexion et envoyer un message d'alerte à l'utilisateur lorsque les virus sont détectés dans les pages Web ou dans les fichiers auxquels l'utilisateur tente d'accéder. **Disable HTTP Resume** : en option, cochez la case pour désactiver la reprise du transfert de fichiers basé sur le Web à l'aide du protocole HTTP lorsque les virus sont détectés. **REMARQUE** : Si vous choisissez Notify ou Notify + Drop Connection, accédez à la page HTTP Notification pour configurer le message de notification. Voir **Configuration de la notification HTTP, page 274**.

Protocol	Action
FTP	**None** : aucune action n'est requise lorsque les virus sont détectés. **Drop Connection** : abandonner la connexion lorsque les virus sont détectés. **Disable FTP Resume** : en option, cochez la case pour désactiver la reprise du transfert de fichiers à l'aide du protocole FTP lorsque les virus sont détectés.
Pièces jointes de la messagerie SMTP	**None** : aucune action n'est requise lorsque les virus sont détectés. **Notify** : envoyer l'e-mail d'origine et un e-mail d'alerte au destinataire de l'e-mail lorsque les virus sont détectés dans les pièces jointes des e-mails. **Notify + Destruct File** : supprimer les fichiers infectés et envoyer l'e-mail d'origine et un e-mail d'alerte au destinataire de l'e-mail lorsque les virus sont détectés dans les pièces jointes des e-mails. **REMARQUE** : Si vous choisissez Notify ou Notify + Destruct File, accédez à la page Email Notification pour configurer les paramètres de notification par e-mail. Voir **Configuration de la notification par e-mail, page 275**.
Pièces jointes de la messagerie POP3	**None** : aucune action n'est requise lorsque les virus sont détectés. **Notify** : envoyer l'e-mail d'origine et un e-mail d'alerte au destinataire de l'e-mail lorsque les virus sont détectés dans les pièces jointes des e-mails. **Notify + Destruct File** : supprimer les fichiers infectés et envoyer l'e-mail d'origine et un e-mail d'alerte au destinataire de l'e-mail lorsque les virus sont détectés dans les pièces jointes des e-mails. **REMARQUE** : Si vous choisissez Notify ou Notify + Destruct File, accédez à la page Email Notification pour configurer les paramètres de notification par e-mail. Voir **Configuration de la notification par e-mail, page 275**.

Protocol	Action
Pièces jointes de la messagerie IMAP	**None** : aucune action n'est requise lorsque les virus sont détectés. **Destruct File** : supprimer les fichiers infectés lorsque les virus sont détectés dans les pièces jointes des e-mails.
NETBIOS/ CIFS	**None** : aucune action n'est requise lorsque les virus sont détectés. **Drop Connection** : abandonner la connexion lorsque les virus sont détectés.

ÉTAPE 5 Dans la zone **Update Virus Database**, spécifiez comment mettre à jour les signatures antivirus. Vous pouvez rechercher automatiquement les mises à jour de signatures à partir du serveur de signatures Cisco toutes les 24 heures ou rechercher manuellement ces mises à jour à tout moment en cliquant sur **Update**. Voir **Mise à jour des signatures antivirus, page 276**.

ÉTAPE 6 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration des paramètres antivirus avancés

Utilisez la page Advanced Settings pour configurer les paramètres de l'analyse.

ÉTAPE 1 Cliquez sur **Security Services > Anti-Virus > Advanced Settings**.

ÉTAPE 2 **Maximum File Size to Scan** : saisissez la taille maximale de fichier, de 0 à 10 240 kilo-octets. Les fichiers de taille supérieure à cette taille sont transmis sans analyse. Utilisez le paramètre par défaut « 0 » pour indiquer qu'il n'y a pas de limite pour la taille du fichier.

REMARQUE : Pour les fichiers compressés, l'antivirus analyse chaque fichier après la décompression et ignore l'analyse antivirus pour les fichiers dont la taille est supérieure à la taille de fichier maximale.

ÉTAPE 3 Pour chaque protocole, effectuer les sélections souhaitées :

- **HTTP :**
  - Cochez la case **Optimize Performance** pour interrompre l'analyse antivirus pour les sites Web ayant une bonne réputation. Décochez la case pour analyser tous les sites. Cette option est disponible uniquement

si le filtrage par réputation Web est activé. Pour obtenir plus d'informations, voir **Configuration du filtrage par réputation Web, page 296**.

- Cochez la case **Disable HTTP Resume** pour désactiver la reprise du transfert de fichiers basé sur le Web à l'aide du protocole HTTP lorsque les virus sont détectés. Décochez la case pour autoriser la reprise du transfert de fichiers basé sur le Web dans ce cas.

- **FTP** : cochez la case **Disable FTP Resume** pour désactiver la reprise du transfert de fichiers à l'aide du protocole FTP lorsque les virus sont détectés. Décochez la case pour activer la reprise du transfert de fichiers dans ce cas.

ÉTAPE 4 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration de la notification HTTP

La notification HTTP informe les utilisateurs que les virus sont détectés dans les pages Web ou dans les dossiers auxquels ils tentent d'accéder. Utilisez la page HTTP Notification pour personnaliser le message de notification à envoyer à l'utilisateur lorsque les virus sont détectés.

ÉTAPE 1 Cliquez sur **Security Services > Anti-Virus > HTTP Notification**.

ÉTAPE 2 Entrez le message d'alerte dans le champ **Notification Content**.

- Si vous sélectionnez l'action Notify pour le protocole HTTP, le message d'alerte est envoyé à l'utilisateur.

- Si vous sélectionnez l'action Notify + Drop Connection pour le protocole HTTP, la connexion est abandonnée et le message d'alerte est envoyé à l'utilisateur.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration de la notification par e-mail

La fonctionnalité de notification par e-mail vous permet d'envoyer un e-mail d'alerte au destinataire de l'e-mail lorsque les virus sont détectés dans les pièces jointes des e-mails. Utilisez la page Email Notification pour personnaliser la balise et le message de notification affichés dans l'e-mail d'alerte.

ÉTAPE 1 Cliquez sur **Security Services > Anti-Virus > Email Notification**.

La fenêtre Email Notification s'ouvre. Les informations suivantes sont affichées :

- **Email Notification Status** : indique si l'action de notification ou de notification + destruction du fichier est activée ou désactivée pour le protocole SMTP ou POP3.
  - Si vous choisissez Notify comme action de prévention, le message d'origine et un e-mail d'alerte sont envoyés au destinataire de l'e-mail.
  - Si vous choisissez Notify + Destruct File comme action de prévention, les fichiers infectés sont supprimés et le message d'origine et un e-mail d'alerte sont envoyés au destinataire de l'e-mail.
- **From Email Address** : adresse e-mail utilisée pour envoyer l'e-mail d'alerte.
- **SMTP Server** : adresse IP ou nom Internet du serveur SMTP.
- **SMTP Authentication** : indique si l'authentification SMTP est activée ou désactivée.

  REMARQUE : Les paramètres du serveur de messagerie mentionnés ci-dessus sont en lecture seule. Ils sont utilisés pour envoyer l'e-mail d'alerte au destinataire de l'e-mail d'origine. Vous pouvez cliquer sur le lien **Edit** pour configurer les paramètres du serveur de messagerie, mais enregistrez d'abord vos paramètres sur cette page. Voir **Configuration des paramètres d'alerte par courriel, page 382**.

ÉTAPE 2 Si la fonctionnalité de notification par e-mail est activée et que les paramètres du serveur de messagerie sont configurés, entrez les informations suivantes :

- **Mail Tag** : entrez la balise qui s'affiche dans l'objet de l'e-mail d'alerte. La balise s'insère dans l'objet de l'alerte par e-mail au format **[Tag] Email Subject**.
- **Mail Content** : entrez le contenu de la notification qui apparaît dans l'e-mail d'alerte.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Mise à jour des signatures antivirus

Vous pouvez rechercher automatiquement les mises à jour des signatures antivirus à partir du serveur de signatures Cisco toutes les 24 heures ou rechercher manuellement ces mises à jour à tout moment en cliquant sur **Update**. Si un nouveau fichier de signatures plus récent est disponible sur le serveur, le nouveau fichier de signatures est téléchargé sur votre périphérique.

REMARQUE Un compte Cisco.com valide est requis pour rechercher les mises à jour de signatures à partir du serveur de signatures Cisco. Accédez à la page Device Management > Cisco Services & Support > Cisco.com Account ou cliquez sur le lien **Edit Cisco.com Account Settings** pour configurer vos informations d'identification de compte Cisco.com sur l'Cisco ISA500. Voir **Configuration d'un compte Cisco.com, page 399**.

ÉTAPE 1 Cliquez sur **Security Services > Anti-Virus > General Settings**.

ÉTAPE 2 Dans la zone **Update Virus Database**, vous pouvez afficher l'état du fichier de signatures antivirus. Les informations suivantes sont affichées :

- **Last Check** : date et heure de votre dernière vérification.
- **Last Update** : date et heure de la dernière mise à jour réussie.
- **Version** : numéro de version du fichier de signatures antivirus.
- **Virus Pattern Number** : nombre total de types de virus dans le fichier de signatures antivirus.

ÉTAPE 3 Pour mettre à jour automatiquement les signatures antivirus, procédez comme suit :

a. Dans la zone **Auto Update Virus Database**, cliquez sur **On** pour rechercher automatiquement les mises à jour de signatures à partir du serveur de signatures Cisco toutes les 24 heures.

b. Cliquez sur **Save** pour appliquer vos paramètres.

ÉTAPE 4 Pour mettre à jour manuellement les signatures antivirus à tout moment, cliquez sur **Update** pour rechercher immédiatement les mises à jour de signatures à partir du serveur de signatures Cisco.

Vous pouvez également cliquer sur **Check for Updates Now** à partir de la page Security Services > Dashboard pour mettre à jour manuellement les signatures antivirus.

Configuration du contrôle des applications

Le contrôle des applications surveille le trafic traité via le Cisco ISA500 afin d'autoriser ou de bloquer ce trafic pour certaines applications et catégories d'applications. Pour certaines applications, vous pouvez autoriser ou bloquer certaines fonctionnalités de l'application.

Important : Lisez les informations de ce guide pour comprendre les fonctionnalités, les tâches requises et les recommandations avant de procéder à la mise en œuvre de ce service.

Pour configurer le contrôle des applications, reportez-vous aux rubriques suivantes :

- **Configuration des stratégies de contrôle des applications, page 277**
- **Paramètres généraux du contrôle des applications, page 283**
- **Paramètres avancés du contrôle des applications, page 287**

Pour configurer les rapports et les alertes de messagerie électronique, reportez-vous aux rubriques suivantes :

- **Affichage du rapport de contrôle des applications, page 268**
- **Configuration des paramètres d'alerte par courriel, page 382**

Pour vous assurer que le contrôle des applications peut identifier les dernières applications, consultez la rubrique : **Mise à jour la base de données de signatures des applications, page 286**

Configuration des stratégies de contrôle des applications

Utilisez la page Application Control Policies pour configurer les stratégies de contrôle des applications. Une stratégie de contrôle des applications vous permet d'autoriser ou de bloquer le trafic pour les applications par programmation.

Conseils importants :

- Gardez à l'esprit que le Cisco ISA500 peut contrôler l'accès uniquement pour le trafic qu'il traite. Par exemple, si un PC et un serveur sont directement connectés aux ports LAN du Cisco ISA500, les stratégies de contrôle des applications s'appliquent au trafic entre ces périphériques. Cependant, si un commutateur établit une liaison montante avec le Cisco ISA500, l'appliance de sécurité ne traite pas le trafic passant par les ports de ce commutateur et, par conséquent, les stratégies de contrôle des applications ne s'appliquent pas.
- Le contrôle des applications utilise les signatures pour identifier et bloquer les applications. Vous devez mettre à jour les signatures des applications régulièrement afin que le contrôle des applications puisse identifier les dernières applications. Voir **Mise à jour la base de données de signatures des applications, page 286**.

Reportez-vous aux rubriques suivantes :

- **Paramètres généraux de la stratégie de contrôle des applications, page 278**
- **Ajout d'une stratégie de contrôle des applications, page 279**
- **Autorisation ou blocage du trafic pour toutes les applications dans une catégorie, page 280**
- **Autorisation ou blocage du trafic pour une application, page 282**

Paramètres généraux de la stratégie de contrôle des applications

ÉTAPE 1 Cliquez sur **Security Services > Application Control > Application Control Policies**.

ÉTAPE 2 Vous pouvez effectuer les actions suivantes :

- Cliquez sur **Add Policy** pour ajouter une nouvelle stratégie de contrôle des applications. Voir **Ajout d'une stratégie de contrôle des applications, page 279**.
- Cliquez sur l'icône de **modification** (crayon) pour modifier une stratégie de contrôle des applications existante.
- Cliquez sur l'icône **Duplicate** pour créer une copie d'une stratégie de contrôle des applications existante. Cette fonctionnalité vous permet d'apporter une modification mineure à une stratégie de contrôle des applications existante pour créer une nouvelle stratégie.

- Cliquez sur l'icône de **suppression** (x) pour supprimer une stratégie de contrôle des applications existante. La stratégie de contrôle des applications par défaut ne peut pas être supprimée.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Ajout d'une stratégie de contrôle des applications

Une stratégie de contrôle des applications est utilisée pour autoriser ou bloquer le trafic pour les applications par programmation.

REMARQUE Jusqu'à 80 stratégies de contrôle des applications personnalisées peuvent être configurées sur l'Cisco ISA500. Jusqu'à 8 stratégies de contrôle des applications peuvent être appliquées à chaque zone.

ÉTAPE 1 Cliquez sur **Add Policy** pour créer une nouvelle stratégie de contrôle des applications.

La fenêtre Policy Profile - Add/Edit s'ouvre.

ÉTAPE 2 Saisissez les informations suivantes :

- **Policy Name** : entrez le nom de la stratégie de contrôle des applications.
- **Schedule** : choisissez **Always on** pour maintenir la stratégie de contrôle des applications toujours active ou choisissez une programmation pour autoriser ou bloquer les applications à un moment donné de la journée ou à des jours spécifiés de la semaine. Si la programmation que vous souhaitez ne figure pas dans la liste, choisissez **Create a new schedule** pour ajouter un nouvel objet de programmation. Pour conserver les programmations, accédez à la page Device Management > Schedules. Voir **Configuration des programmations, page 429**.

ÉTAPE 3 L'Cisco ISA500 prend en charge une longue liste d'applications. Vous pouvez utiliser les paramètres de filtre du tableau pour filtrer les applications et indiquer ensuite les paramètres pour les applications sélectionnées.

- **Category** : vous permet de filtrer les applications par catégorie. Choisissez **All** pour afficher toutes les catégories dans le tableau ou choisissez une catégorie pour n'afficher que les applications qui appartiennent à la catégorie choisie. Vous pouvez cliquer sur le triangle en regard d'une catégorie pour développer ou réduire toutes les applications de cette catégorie.

- **Application** : vous permet de filtrer l'application par le nom. Entrez le nom de l'application dans ce champ. Seule l'application que vous avez spécifiée est affichée dans le tableau.
- **Current Action** : vous permet de filtrer les applications par action. Choisissez **Deny** pour afficher toutes les applications bloquées ou choisissez **Permit** pour afficher toutes les applications autorisées.

  REMARQUE : Par défaut, les paramètres de filtre du tableau sont masqués. Vous pouvez cliquer sur le triangle à côté des **Hide Table Filter Settings** pour afficher ou masquer les paramètres de filtre du tableau.

ÉTAPE 4 Une fois que vous avez défini les paramètres de filtre du tableau, cliquez sur **Refresh Table** pour actualiser les données du tableau. Seules les applications que vous avez spécifiées sont affichées dans le tableau.

ÉTAPE 5 Spécifiez l'action de prévention pour une seule application ou pour toutes les applications dans une catégorie :

- Pour autoriser ou bloquer le trafic pour toutes les applications dans une catégorie, cliquez sur l'icône de **modification** (crayon) dans la colonne **Configure** de la catégorie. Pour plus d'informations, reportez-vous à la section **Autorisation ou blocage du trafic pour toutes les applications dans une catégorie, page 280**.
- Si les paramètres d'action, de programmation ou de consignation varient entre les applications dans une catégorie, vous pouvez configurer les paramètres pour chaque application de la catégorie. Vous devez d'abord choisir **keep application-level settings** pour les options d'action et de consignation, puis cliquer sur l'icône de **modification** (crayon) dans la colonne **Configure** de l'application. Pour plus d'informations, reportez-vous à la section **Autorisation ou blocage du trafic pour une application, page 282**.

ÉTAPE 6 Cliquez sur **OK** pour enregistrer vos paramètres.

Autorisation ou blocage du trafic pour toutes les applications dans une catégorie

Cette section explique comment configurer les paramètres par défaut de la catégorie. Les paramètres par défaut de la catégorie sont appliqués à toutes les applications dans une catégorie.

ÉTAPE 1 Cliquez sur l'icône de **modification** (crayon) dans la colonne **Configure** de la catégorie.

La fenêtre Policy Profile - Add/Edit s'ouvre.

ÉTAPE 2 Spécifiez les paramètres par défaut de la catégorie :

- **Category** : nom de la catégorie.
- **Action** : choisissez **Permit** pour autoriser le trafic ou choisissez **Deny** pour le bloquer. Si les paramètres d'action varient entre les applications de la catégorie, vous devez d'abord choisir l'option **keep application-level settings**, puis configurer l'action pour chaque application dans la catégorie. Voir **Autorisation ou blocage du trafic pour une application, page 282**.
- **Logging** : choisissez **Enable** pour consigner l'événement lorsqu'une application est bloquée, ou choisissez **Disable** pour désactiver la fonctionnalité de consignation. Si les paramètres de consignation varient entre les applications d'une catégorie, vous devez d'abord choisir l'option **keep application-level settings**, puis configurer les paramètres de consignation pour chaque application dans la catégorie. Voir **Autorisation ou blocage du trafic pour une application, page 282**.

  Pour consigner les événements de blocage d'application, vous devez activer les paramètres de consignation des applications, puis accéder aux pages Device Management > Logs pour configurer les paramètres et les utilitaires du journal. Voir **Gestion des journaux, page 421**.

  - Pour enregistrer les journaux de blocage d'application dans le daemon syslog local, vous devez activer la fonctionnalité de journal, définir la taille de la mémoire tampon du journal et le niveau de gravité pour les journaux locaux, puis activer les paramètres des journaux locaux pour l'utilitaire de contrôle des applications.
  - Pour enregistrer les journaux de blocage d'application dans le serveur syslog à distance si vous disposez d'une assistance de serveur syslog à distance, vous devez activer la fonctionnalité de journal, spécifier les paramètres de journal à distance et activer les paramètres de journal à distance pour l'utilitaire de contrôle des applications.

  REMARQUE : La modification des paramètres par défaut de la catégorie remplace les paramètres au niveau des applications pour toutes les applications de la catégorie.

ÉTAPE 3 Cliquez sur **OK** pour enregistrer vos paramètres.

Autorisation ou blocage du trafic pour une application

Si les paramètres d'action, de programmation ou de consignation varient entre les applications dans une catégorie, vous pouvez configurer les paramètres d'action et de consignation pour chaque application de la catégorie. Les paramètres au niveau des applications sont appliqués à une seule application dans une catégorie.

REMARQUE Pour modifier les paramètres d'une application dont la détection est désactivée, vous devez d'abord activer la détection à partir de la page Advanced Settings.

REMARQUE Avant de configurer les paramètres au niveau des applications pour chaque application dans une catégorie, choisissez bien **keep application-level settings** pour les options d'action et de consignation de la catégorie.

ÉTAPE 1 Cliquez sur l'icône de **modification** (crayon) dans la colonne **Configure** d'une application.

La fenêtre Policy Profile - Add/Edit s'ouvre.

ÉTAPE 2 Spécifiez les paramètres de contrôle au niveau des applications :

- **Application** : entrez le nom de l'application.
- **Action** : choisissez **Permit** afin d'autoriser le trafic pour l'application ou choisissez **Deny** afin de le bloquer pour l'application.
- **Logging** : choisissez **Enable** pour consigner l'événement lorsqu'une application est bloquée, ou choisissez **Disable** pour désactiver la fonctionnalité de consignation.

  Pour consigner les événements de blocage d'application, vous devez d'abord activer les paramètres de consignation des applications, puis accéder aux pages Device Management > Logs pour configurer les paramètres et les utilitaires du journal. Voir **Gestion des journaux, page 421**.
- **Configure feature-specific access control** : pour certaines applications, vous pouvez autoriser ou bloquer certaines fonctionnalités de l'application. Par exemple, pour l'application Google Talk, vous pouvez activer la fonctionnalité de chat mais bloquer la fonctionnalité de transfert de fichiers multimédia. Cochez cette case, puis spécifiez l'action pour chaque fonctionnalité de l'application.

REMARQUE : Lorsque l'action de l'application est définie sur « Deny », cette fonctionnalité est grisée.

ÉTAPE 3 Cliquez sur **OK** pour enregistrer vos paramètres.

Paramètres généraux du contrôle des applications

Utilisez la page Application Control Settings pour activer la fonctionnalité de contrôle des applications, pour appliquer les stratégies de contrôle des applications à différentes zones et pour mettre à jour la base de données de signatures des applications.

Conseils importants :

- Gardez à l'esprit que le Cisco ISA500 peut contrôler l'accès uniquement pour le trafic qu'il traite. Par exemple, si un PC et un serveur sont directement connectés aux ports LAN du Cisco ISA500, les stratégies de contrôle des applications s'appliquent au trafic entre ces périphériques. Cependant, si un commutateur établit une liaison montante avec le Cisco ISA500, l'appliance de sécurité ne traite pas le trafic passant par les ports de ce commutateur et, par conséquent, les stratégies de contrôle des applications ne s'appliquent pas.
- Vous devez mettre à jour les signatures des applications régulièrement afin que le contrôle des applications puisse identifier les dernières applications.

Reportez-vous aux rubriques suivantes :

- **Activation du service de contrôle des applications, page 284**
- **Mappage des stratégies de contrôle des applications aux zones, page 284**
- **Configuration des règles de mappage de stratégie de contrôle des applications, page 285**
- **Mise à jour la base de données de signatures des applications, page 286**

Activation du service de contrôle des applications

ÉTAPE 1 Cliquez sur **Security Services > Application Control > Application Control Settings**.

ÉTAPE 2 Cliquez sur **On** pour activer la fonctionnalité de contrôle des applications, ou sur **Off** pour la désactiver. Si vous activez le contrôle des applications, par défaut toutes les applications sont autorisées sauf si elles sont spécifiquement bloquées par une stratégie de contrôle des applications.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Mappage des stratégies de contrôle des applications aux zones

Vous pouvez appliquer des stratégies de contrôle des applications différentes à différentes zones. Vous pouvez avoir plusieurs stratégies au sein d'une zone donnée pour un ensemble d'utilisateurs différent. Par défaut, la stratégie de contrôle des applications par défaut qui autorise le trafic de toutes les applications est sélectionnée pour toutes les zones.

ÉTAPE 1 Cliquez sur **Security Services > Application Control > Application Control Settings**.

ÉTAPE 2 Dans la zone **Zone Mapping**, vous pouvez effectuer les actions suivantes :

- Cliquez sur le triangle en regard d'une zone pour développer ou réduire les règles de mappage de stratégie de contrôle des applications de la zone sélectionnée.
- Cliquez sur **Add Mapping Rule** pour ajouter une nouvelle règle de mappage de stratégie de contrôle des applications. Voir **Configuration des règles de mappage de stratégie de contrôle des applications, page 285**.
- Cliquez sur l'icône de **modification** (crayon) pour modifier une règle de mappage de stratégie de contrôle des applications existante.
- Cliquez sur l'icône de **suppression** (x) pour supprimer une règle de mappage de stratégie de contrôle des applications. La règle de mappage de stratégie de contrôle des applications par défaut pour chaque zone ne peut pas être supprimée.
- Réorganisez les priorités de plusieurs règles de mappage de stratégie de contrôle des applications au sein d'une zone donnée. Pour déplacer la règle d'une position vers le haut, cliquez sur l'icône **Move up**. Pour déplacer la

règle d'une position vers le bas, cliquez sur l'icône **Move down**. La règle de mappage de stratégie de contrôle des applications par défaut doit être la dernière stratégie avec la priorité la plus faible pour une zone.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration des règles de mappage de stratégie de contrôle des applications

Une règle de mappage de stratégie de contrôle des applications s'applique à une stratégie de contrôle des applications spécifique pour une zone donnée afin de contrôler le trafic des applications en provenance et à destination de la zone. Vous pouvez également appliquer une stratégie de contrôle des applications sélectionnée à un ensemble d'utilisateurs différent.

Par exemple, vous pouvez contrôler le trafic entrant et sortant pour une zone donnée d'un hôte spécifique ou des hôtes au sein d'une plage IP spécifique.

REMARQUE Vérifiez que vous avez bien configuré les stratégies de contrôle des applications avant de configurer les règles de mappage de stratégie. Voir **Configuration des stratégies de contrôle des applications, page 277**.

ÉTAPE 1 Cliquez sur **Add Mapping Rule** pour ajouter une nouvelle règle de mappage de stratégie de contrôle des applications.

La fenêtre Application Control Policy Mapping - Add/Edit s'ouvre.

ÉTAPE 2 Saisissez les informations suivantes :

- **Zone** : choisissez une zone existante pour contrôler le trafic des applications en provenance et à destination de la zone sélectionnée. Cette règle de mappage sera répertoriée sous la zone sélectionnée.
- **Policy** : choisissez une stratégie de contrôle des applications existante pour appliquer la stratégie sélectionnée à la zone.
- **Matching Condition** : vous pouvez appliquer la stratégie de contrôle des applications sélectionnée à tous les utilisateurs, à un hôte spécifique ou aux hôtes au sein d'une plage IP donnée. Sélectionnez l'une des options suivantes :
  - **All IP Addresses and Users** : applique la stratégie de contrôle des applications sélectionnée à tous les utilisateurs.

- **Specific IP Address Object** : applique la stratégie de contrôle des applications sélectionnée à un hôte spécifique ou aux hôtes au sein d'une plage IP donnée. Le trafic de l'hôte spécifique ou des hôtes au sein de la plage IP sera détecté. Le trafic des autres utilisateurs sera ignoré. L'objet d'adresses IP peut être un hôte ou une plage d'adresses IP. Si l'objet d'adresse que vous souhaitez ne figure pas dans la liste, choisissez **Create a new address** pour créer un nouvel objet d'adresse. Pour conserver les objets d'adresse, accédez à la page Networking > Address Management. Voir **Gestion d'adresse, page 182**.

ÉTAPE 3 Cliquez sur **OK** pour enregistrer vos paramètres.

Mise à jour la base de données de signatures des applications

Le contrôle des applications utilise les signatures pour identifier et bloquer les applications. Vous devez mettre à jour les signatures des applications régulièrement afin que le contrôle des applications puisse identifier les dernières applications. Vous pouvez rechercher automatiquement les mises à jour de signatures à partir du serveur de signatures Cisco une fois par semaine ou rechercher manuellement les mises à jour de signatures à tout moment en cliquant sur **Check for Update Now**. Si un nouveau fichier de signatures plus récent est disponible sur le serveur, le nouveau fichier de signatures est automatiquement téléchargé sur votre périphérique.

Vous pouvez également en premier lieu télécharger le dernier fichier de signatures à partir du serveur de signatures Cisco sur votre ordinateur local, puis mettre à jour manuellement les signatures des applications via l'utilitaire de configuration.

Un compte Cisco.com valide est requis pour rechercher les mises à jour de signatures à partir du serveur de signatures Cisco. Accédez à la page Device Management > Cisco Services & Support > Cisco.com Account pour configurer vos informations d'identification de compte Cisco.com sur l'Cisco ISA500. Voir **Configuration d'un compte Cisco.com, page 399**.

REMARQUE Le contrôle des applications et l'IPS utilisent la même base de données de signatures. La mise à jour des signatures des applications mettra à jour également les signatures IPS au même moment.

ÉTAPE 1 Cliquez sur **Security Services > Application Control > Application Control Settings**.

ÉTAPE 2 Dans la zone **Update Signature Database**, les informations suivantes sont affichées :

- **Last Check** : date et heure de la dernière vérification.
- **Last Update** : date et heure de la dernière mise à jour réussie lorsque le fichier de signatures a bien été mis à jour.
- **Version** : numéro de version du fichier de signatures des applications actuellement utilisé sur l'appliance de sécurité.

ÉTAPE 3 Pour mettre à jour automatiquement les signatures des applications, procédez comme suit :

a. Dans la zone **Auto Update**, cliquez sur **On** pour rechercher automatiquement les mises à jour de signatures à partir du serveur de signatures Cisco chaque lundi à 0h00.

b. Cliquez sur **Save** pour appliquer vos paramètres.

ÉTAPE 4 Pour mettre à jour manuellement les signatures des applications à tout moment, cliquez sur **Check for Update Now** pour rechercher immédiatement les mises à jour de signatures à partir du serveur de signatures Cisco.

Vous pouvez également cliquer sur **Check for Updates Now** à partir de la page Security Services > Dashboard pour mettre à jour manuellement les signatures des applications.

ÉTAPE 5 Pour mettre à jour manuellement les signatures des applications à partir de votre ordinateur local, procédez comme suit :

a. Vous devez en premier lieu télécharger le fichier de signatures des applications à partir du serveur de signatures Cisco sur votre ordinateur local.

b. Dans la zone **Manually Update Signature Database**, cliquez sur **Browse** pour localiser et sélectionner le fichier de signatures à partir de votre ordinateur local.

c. Cliquez sur **Update Database**.

Paramètres avancés du contrôle des applications

Utilisez la page Application Control Advanced Settings pour activer ou désactiver la détection pour chaque application.

ÉTAPE 1 Cliquez sur **Security Services > Application Control > Application Control Advanced Settings**.

La fenêtre Application Control Advanced Settings s'ouvre.

ÉTAPE 2 L'Cisco ISA500 prend en charge une longue liste d'applications. Vous pouvez utiliser les paramètres de filtre du tableau pour filtrer les applications dans le tableau, puis spécifier les paramètres de détection pour toutes les applications sélectionnées :

- **Category** : vous permet de filtrer les applications par catégorie. Choisissez la catégorie que vous souhaitez dans la liste déroulante. Seules les applications qui appartiennent à la catégorie sélectionnée s'affichent. Vous pouvez cliquer sur le triangle en regard d'une catégorie pour développer ou réduire toutes les applications sous cette catégorie.
- **Application** : vous permet de filtrer l'application par le nom. Entrez le nom de l'application dans ce champ. Seule l'application que vous avez spécifiée est affichée dans le tableau.
- **Detection** : vous permet de filtrer les applications par état de détection. Choisissez **Enable** pour afficher toutes les applications dont la détection est activée ou choisissez **Disable** pour afficher toutes les applications dont la détection est désactivée.

  REMARQUE : Par défaut, les paramètres de filtre du tableau sont masqués. Vous pouvez cliquer sur le triangle en regard de **Show Table Filter Settings** pour afficher ou masquer les paramètres de filtre du tableau.

ÉTAPE 3 Une fois que vous avez défini les paramètres de filtre du tableau, cliquez sur **Refresh Table** pour actualiser les données du tableau.

ÉTAPE 4 Vous pouvez activer ou désactiver la détection pour les applications sélectionnées dans le tableau. Dans la colonne **Detection**, choisissez **Enable** afin d'activer la détection pour une application ou **Disable** afin de désactiver la détection pour une application.

ÉTAPE 5 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration du filtre de courrier indésirable

Le filtre de courrier indésirable détecte le score de réputation de l'expéditeur de l'e-mail. Les scores de réputation vont de - 10 (mauvais) à + 10 (bon). Un e-mail est classé comme indésirable si la réputation de l'expéditeur se trouve sous le seuil de courrier indésirable ou est classé comme suspecté d'être indésirable si la réputation de l'expéditeur se trouve entre le seuil de courrier indésirable et le seuil de suspicion de courrier indésirable. Un e-mail n'est pas classé comme indésirable si la réputation de l'expéditeur dépasse le seuil de suspicion de courrier indésirable.

Le filtre de courrier indésirable détecte les e-mails indésirables en fonction du score de réputation de l'adresse IP de l'expéditeur. L'adresse de l'expéditeur correspond à l'adresse de l'hôte qui se connecte au serveur SMTP pour remettre un e-mail et non à une adresse figurant dans l'en-tête d'e-mail.

ÉTAPE 1 Cliquez sur **Security Services > Spam Filter**.

ÉTAPE 2 Cliquez sur **On** pour activer le filtre de courrier indésirable ou sur **Off** pour le désactiver.

ÉTAPE 3 Si vous activez le filtre de courrier indésirable, entrez les informations suivantes :

- **SMTP Server Address/Domain** : entrez l'adresse IP ou le nom de domaine de votre serveur SMTP interne. Le trafic Internet du serveur SMTP doit être acheminé via l'Cisco ISA500. Le serveur SMTP ou les clients qui utilisent ce serveur SMTP peuvent être configurés pour répondre aux balises de courrier indésirable et de suspicion de courrier indésirable que l'Cisco ISA500 applique à l'e-mail.
- **Action when Spam Detected** : choisissez **Block Email** pour bloquer l'e-mail ou **Tag Email with [Spam]** pour que l'e-mail soit marqué avec [Spam].
- **Action when Suspect Spam Detected** : choisissez **Block Email** pour bloquer l'e-mail ou **Tag Email with [Suspect Spam]** pour que l'e-mail soit marqué avec [Suspect Spam].
- **Reputation Threshold** : spécifiez la sensibilité du bloc comme Low, Medium ou High, ou sous la forme d'un seuil numérique (Custom).
  - **Low** : bloque moins d'e-mails indésirables avec un faible risque de faux positifs. La valeur de seuil pour le courrier indésirable est -4 et celle pour le courrier suspecté d'être indésirable est -2.

- **Medium** : bloque davantage d'e-mails indésirables avec un risque modéré de faux positifs. La valeur de seuil pour le courrier indésirable est -3 et celle pour le courrier suspecté d'être indésirable est -1.
- **High** : bloque la plupart des e-mails indésirables avec un risque élevé de faux positifs. La valeur de seuil pour le courrier indésirable est -2 et celle pour le courrier suspecté d'être indésirable est -0.5.
- **Custom** : définissez manuellement le seuil de réputation de courrier indésirable. Lorsque la case d'option Custom est sélectionnée, choisissez les valeurs de seuil pour le courrier indésirable et le courrier suspecté d'être indésirable. Les valeurs autorisées pour le seuil sont des nombres entiers sur une échelle de -10 à -1 et la valeur -0,5.

ÉTAPE 4 Dans la zone **Allowed Senders**, vous pouvez spécifier les exceptions d'expéditeur d'e-mail en fonction de vos paramètres de filtre de courrier indésirable. Le trafic en provenance de noms d'hôte ou d'adresses IP spécifiées ne sera pas examiné par le filtre de courrier indésirable.

- Pour ajouter une exception, entrez le nom d'hôte ou l'adresse IP de l'expéditeur dans le champ **Hostname/IP Address** et cliquez sur **Add**.
- Pour supprimer une exception, sélectionnez-la dans la liste **Allowed Senders** et cliquez sur **Remove**.

ÉTAPE 5 Dans la zone **Service Outage**, choisissez l'une des actions suivantes lorsque le filtre de courrier indésirable n'est pas disponible :

- **Do Not Accept Emails when spam reputation services are not available** : tous les e-mails sont retardés jusqu'à ce que le filtre de courrier indésirable soit disponible.
- **Accept Emails even when spam reputation services are not available** : tous les e-mails sont reçus sans recherche de courrier indésirable.

ÉTAPE 6 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration de la prévention des intrusions

Le système de prévention des intrusions (IPS) est une plate-forme réseau qui inspecte le trafic réseau à la recherche d'activités malveillantes ou indésirables, telles que les vers, les logiciels espions et les violations de règles. Lorsque le service IPS détecte une menace, il répond en temps réel en effectuant des

actions, comme le blocage ou la suppression des connexions, la consignation des activités détectées et l'envoi de notifications sur ces activités. Vous pouvez utiliser les actions par défaut pour chaque signature ou personnaliser les actions pour répondre à vos attentes.

IMPORTANT : L'IPS utilise les signatures pour identifier les attaques en cours. Vous devez mettre à jour régulièrement les signatures IPS pour que la protection reste à jour. Voir **Mise à jour de la base de données de signatures IPS, page 294**.

Après avoir configuré l'IPS, vous disposez des options suivantes pour surveiller l'activité :

- Activez le rapport IPS à partir de la page Security Services > Security Services Reports ou de la page Status > Security Services Reports pour afficher le nombre de paquets détectés et le nombre de paquets abandonnés par le service IPS. Voir **Affichage du rapport IPS, page 267**.
- Activez la fonctionnalité d'alerte IPS pour envoyer un e-mail d'alerte à une adresse e-mail donnée si une attaque est détectée par le service IPS. Voir **Configuration des paramètres d'alerte par courriel, page 382**.

REMARQUE Vous devez installer des licences sur la page License Management avant de pouvoir configurer l'IPS.

ÉTAPE 1 Cliquez sur **Security Services > Intrusion Prevention (IPS) > IPS Policy and Protocol Inspection**.

La fenêtre IPS Policy and Protocol Inspection s'ouvre.

ÉTAPE 2 En haut de la page, activez ou désactivez l'IPS en cliquant sur **On** ou **Off**.

ÉTAPE 3 Dans la zone **Zone**, sélectionnez les zones à inspecter. L'IPS inspecte uniquement le trafic interzone.

- **Pour ajouter une zone** : dans la liste Zones Available, cliquez sur une zone, puis cliquez sur **Add** pour la déplacer vers la liste Selected Zones. L'ensemble du trafic entrant et sortant pour les zones sélectionnées est inspecté.
- **Pour supprimer une zone** : dans la liste Selected Zones, cliquez sur une zone, puis cliquez sur **Remove** pour la déplacer vers la liste Zones Available.

REMARQUE : Vous pouvez bloquer une intrusion en fonction des zones source ou des zones de destination. Par exemple, si vous sélectionnez les zones LAN et DMZ, l'IPS inspecte l'ensemble du trafic des zones LAN et DMZ, quelle que soit sa source. Le trafic entre le LAN et le DMZ est inspecté une seule fois, pas deux. Si vous sélectionnez la zone WAN, l'IPS inspecte l'ensemble du trafic de la zone WAN, quelle que soit sa destination.

ÉTAPE 4 Dans la zone **IPS Signature**, utilisez les options ci-dessous pour filtrer la liste des signatures dans la table Selected Signature. La liste non filtrée des milliers de signatures IPS qui permettent d'identifier les attaques. Après avoir sélectionné les filtres, cliquez sur **Refresh** pour afficher à nouveau la table Selected en affichant uniquement les signatures sélectionnées.

- **Severity Level** : sélectionnez un niveau de gravité, du plus élevé au plus faible : Critical, High, Medium, Low et Information.
- **Operating System Type** : sélectionnez **All** pour inclure toutes les signatures quel que soit le type de système d'exploitation, ou **Selected OS Types Only** pour inclure uniquement les signatures correspondant aux types de systèmes d'exploitation spécifiés.
- **Host Type** : choisissez un type d'hôte.
- **Category** : sélectionnez **All** pour inclure toutes les signatures indépendamment de la catégorie ou **Selected Categories Only** pour inclure uniquement les signatures correspondant aux catégories spécifiées.

La table Selected Signature affiche les informations suivantes :

- **Name** : nom de la signature.
- **ID** : identificateur unique de la signature. Pour afficher les informations détaillées d'une signature, cliquez sur le lien dans la colonne ID.
- **Severity** : niveau de gravité de la menace que la signature peut identifier.
- **Category** : catégorie à laquelle la signature appartient.
- **Default Action** : action de prévention par défaut pour la signature.
  - **Block and Log** : refuser la demande, abandonner la connexion et consigner l'événement lorsqu'une signature est détectée par le moteur IPS.
  - **Log Only** : consigner l'événement uniquement lorsqu'une signature est détectée par le moteur IPS.
- **Current Action** : action de prévention actuelle de la signature.
- **Edit Action** : cliquez sur l'icône en forme de crayon pour activer, désactiver ou définir les actions préventives pour une signature. Pour obtenir plus d'informations, voir **Configuration des actions de signature, page 293**.

  REMARQUE : Pour faciliter l'utilisation, vous pouvez modifier les actions préventives pour un groupe de signatures. Cochez la case pour chaque signature à modifier, ou sélectionnez toutes les signatures en cochant la

case dans le coin supérieur gauche de la table. Pour modifier les paramètres pour les signatures sélectionnées, cliquez sur l'icône de **modification** (crayon) dans la partie supérieure de la table.

- **Block Threshold** : spécifiez un seuil à partir duquel le blocage se produit ; si l'action actuelle est le blocage et la consignation, ou la consignation uniquement, le trafic est bloqué après le nombre indiqué d'occurrences. Entrez 0 pour appliquer l'action actuelle immédiatement après la détection.

  REMARQUE : Le compteur est réinitialisé à 0 chaque fois que les paramètres IPS sont enregistrés dans l'utilitaire de configuration ou que l'appliance de sécurité est redémarré.

ÉTAPE 5 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration des actions de signature

Après avoir sélectionné une ou plusieurs signatures sur la page Security Services > Intrusion Prevention (IPS) > IPS Policy and Protocol Inspection, utilisez la page Edit Selected Signature Actions pour activer ou désactiver les signatures sélectionnées et pour configurer les actions.

ÉTAPE 1 Saisissez les informations suivantes :

- **Enable detection of selected signatures** : cochez cette case pour activer la détection des intrusions pour cette signature, ou décochez-la pour désactiver l'option.
- **Name** : nom de la signature.
- **ID** : identificateur unique de la signature.
- **Severity** : niveau de gravité de la menace que la signature peut identifier.
- **Default Action** : action de prévention par défaut pour la signature.
- **Action on Detect** : choisissez l'une des actions suivantes pour la signature :
  - **Block and Log** : refuser la demande, abandonner la connexion et consigner l'événement lorsque la signature est détectée par le moteur IPS.
  - **Log only** : consigner l'événement uniquement lorsque la signature de sécurité est détectée par le moteur IPS. Cette option est principalement utilisée à des fins de dépannage.

Pour consigner les événements IPS, vous devez d'abord spécifier l'action pour les signatures, puis accéder aux pages Device Management > Logs pour configurer les paramètres et les utilitaires du journal. Voir **Gestion des journaux, page 421**.

Pour enregistrer les journaux IPS dans le daemon syslog local, vous devez activer la fonctionnalité de journal, définir la taille de la mémoire tampon du journal et le niveau de gravité pour les journaux locaux, puis activer les paramètres des journaux locaux pour l'utilitaire de prévention des intrusions (IPS).

Pour enregistrer les journaux IPS sur un serveur syslog distant, vous devez activer la fonctionnalité de fichier journal, spécifier les paramètres de journal à distance et activer les paramètres de journal à distance pour l'utilitaire de prévention des intrusions (IPS).

ÉTAPE 2 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Mise à jour de la base de données de signatures IPS

Vous pouvez rechercher automatiquement les mises à jour de signatures à partir du serveur de signatures Cisco une fois par semaine ou rechercher manuellement les mises à jour de signatures à tout moment en cliquant sur **Check for Update Now**. Si un fichier de signatures plus récent est disponible, le nouveau fichier de signatures est automatiquement téléchargé sur votre périphérique.

Vous pouvez également en premier lieu télécharger le dernier fichier de signatures à partir du serveur de signatures Cisco sur votre ordinateur local, puis mettre à jour manuellement les signatures IPS via l'utilitaire de configuration.

Un compte Cisco.com valide est requis pour rechercher les mises à jour de signatures et télécharger le fichier de signatures IPS à partir du serveur de signatures Cisco. Accédez à la page Device Management > Cisco Services & Support > Cisco.com Account pour configurer vos informations d'identification de compte Cisco.com sur l'Cisco ISA500. Voir **Configuration d'un compte Cisco.com, page 399**.

REMARQUE L'IPS et le contrôle des applications utilisent la même base de données de signatures. La mise à jour des signatures IPS mettra à jour également les signatures des applications au même moment.

ÉTAPE 1 Cliquez sur **Security Services > Intrusion Prevention (IPS) > IPS Policy and Protocol Inspection**.

La fenêtre IPS Policy and Protocol Inspection s'ouvre.

ÉTAPE 2 Dans la zone **Automatic Update Signature Database** les informations suivantes sont affichées :

- **Last Check** : date et heure de la dernière vérification.
- **Last Update** : date et heure de la dernière mise à jour réussie lorsque le fichier de signatures a bien été mis à jour.
- **Version** : numéro de version du fichier de signatures IPS actuellement utilisé sur l'appliance de sécurité.

ÉTAPE 3 Pour mettre à jour automatiquement les signatures IPS, procédez comme suit :

a. Dans la zone **Auto Update**, cliquez sur **On** pour rechercher automatiquement les mises à jour de signatures à partir du serveur de signatures Cisco chaque lundi à 0h00.

b. Cliquez sur **Save** pour appliquer vos paramètres.

ÉTAPE 4 Pour mettre à jour manuellement les signatures IPS à tout moment, cliquez sur **Check for Update Now** pour rechercher immédiatement les mises à jour de signatures à partir du serveur de signatures Cisco.

Vous pouvez également cliquer sur **Check for Updates Now** à partir de la page Security Services > Dashboard pour mettre à jour manuellement les signatures IPS.

ÉTAPE 5 Pour mettre à jour manuellement les signatures IPS à partir de votre ordinateur local, procédez comme suit :

a. Vous devez d'abord télécharger le fichier de signatures à partir du serveur de signatures Cisco sur votre ordinateur local.

b. Dans la zone **Manually Update Signature Database**, cliquez sur **Browse** pour localiser et sélectionner le fichier de signatures à partir de votre ordinateur local.

c. Cliquez sur **Update Database**.

Configuration du filtrage par réputation Web

Le filtrage par réputation Web empêche les périphériques clients d'accéder à des sites Web dangereux contenant des virus, des logiciels espions, des programmes malveillants ou des liens d'hameçonnage. Le filtrage par réputation Web permet de détecter les menaces Web en fonction du score de réputation d'une page Web. Les scores de réputation vont de -10 (mauvais) à + 10 (bon). Les pages Web avec des scores de réputation inférieurs à un seuil spécifique sont considérées comme des menaces et sont bloquées.

Le filtrage par réputation Web surveille et contrôle uniquement les visites de sites Web via le port HTTP spécifié. Accédez à la page Security Services > Web URL Filtering > Advanced Settings pour afficher ou spécifier le port HTTP. Voir **Configuration des paramètres avancés du filtrage URL Web, page 301**.

Vous pouvez créer une " liste blanche " des sites de confiance et inclure 16 sites Web autorisés au maximum. Les sites Web spécifiés ne seront pas examinés par le filtrage par réputation Web.

ÉTAPE 1 Cliquez sur **Security Services > Web Reputation Filtering**.

ÉTAPE 2 Cliquez sur **On** pour activer le filtrage par réputation Web ou sur **Off** pour le désactiver.

ÉTAPE 3 Spécifiez la sensibilité du bloc comme Low, Medium ou High, ou sous la forme d'un seuil numérique (Custom). Les valeurs de seuils Low, Medium ou High sont prédéfinies et ne peuvent pas être modifiées.

- **Low** : bloque moins de menaces Web avec un faible risque de faux positifs. La valeur du seuil est -8.
- **Medium** : bloque davantage de menaces Web avec un risque modéré de faux positifs. La valeur du seuil est -6.
- **High** : bloque la plupart des menaces Web avec un risque élevé de faux positifs. La valeur du seuil est -4.
- **Custom** : définissez manuellement le seuil de réputation Web. Lorsque la case d'option Custom est sélectionnée, choisissez la valeur du seuil à partir de la liste déroulante. Les valeurs disponibles pour le seuil sont des nombres entiers sur une échelle de -10 à -1 et la valeur -0,5.

ÉTAPE 4 Dans la zone Allowed Web Sites, vous pouvez spécifier les exceptions de site Web en fonction de vos paramètres de filtrage par réputation Web. Les sites Web

spécifiés ne seront pas examinés par le filtrage par réputation Web. La liste peut comporter jusqu'à 16 sites Web.

- Pour ajouter une nouvelle exception de site Web, entrez les informations suivantes :
  - **Matching Domain** : vous permet d'autoriser l'accès HTTP d'un site Web qui correspond exactement à un nom de domaine spécifique. Si vous choisissez cette option, entrez le nom de domaine sans http:// dans le champ **Site URL** et cliquez sur **Add**.
  - **Containing Keyword** : vous permet d'autoriser l'accès HTTP d'un site Web qui contient un mot-clé spécifique. Si vous choisissez cette option, entrez le mot-clé d'URL sans http:// dans le champ **Site URL** et cliquez sur **Add**.
- Pour supprimer une exception de site Web, sélectionnez-la dans la liste des **Allowed Sites** et cliquez sur **Remove**.

ÉTAPE 5 Dans la zone **Service Outage**, vous pouvez spécifier comment gérer le trafic Web lorsque le filtrage par réputation Web n'est pas disponible. Sélectionnez l'une des actions suivantes :

- **Block Web Traffic when web reputation filter services are not available** : l'ensemble du trafic Web est bloqué jusqu'à ce que le filtrage par réputation Web soit disponible. La page de blocage par défaut s'affiche lorsqu'une page Web est bloquée. Le message que vous spécifiez dans le champ **Blocked Web Filter Message** s'affichera sur la page de blocage par défaut.
- **Allow Web Traffic even when web reputation filter services are not available** : l'ensemble du trafic Web est autorisé jusqu'à ce que le filtrage par réputation Web soit disponible.

ÉTAPE 6 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration du filtrage URL Web

Le filtrage URL Web vous permet de bloquer l'accès HTTP aux sites Web malveillants en fonction des catégories d'URL. Vous pouvez autoriser ou bloquer une catégorie complète d'URL pour simplifier la configuration. Vous pouvez également spécifier les exceptions de site Web en fonction des paramètres de catégorie d'URL. Par exemple, vous pouvez bloquer les sites Web autorisés généralement par le filtrage URL Web, ou autoriser les sites Web bloqués généralement par le filtrage URL Web.

Vous pouvez activer l'alerte de filtrage URL Web pour envoyer des alertes par e-mail à une adresse e-mail spécifique lorsque les catégories d'URL Web ont été modifiées. Voir **Configuration des paramètres d'alerte par courriel, page 382**.

Le filtrage URL Web surveille et contrôle uniquement les visites de sites Web via le port HTTP spécifié dans la page Web URL Filtering > Advanced Settings.

Reportez-vous aux rubriques suivantes :

- **Configuration des profils de stratégie de filtrage URL Web, page 298**
- **Configuration de la liste de contrôle d'accès aux sites Web, page 299**
- **Mappage des profils de stratégie de filtrage URL Web aux zones, page 300**
- **Configuration des paramètres avancés du filtrage URL Web, page 301**

Configuration des profils de stratégie de filtrage URL Web

Un profil de stratégie de filtrage URL Web est utilisé pour spécifier quelles sont les catégories d'URL autorisées ou bloquées.

REMARQUE Jusqu'à 32 profils de stratégie de filtrage URL Web peuvent être configurés sur l'Cisco ISA500.

ÉTAPE 1 Cliquez sur **Security Services > Web URL Filtering > Policy Profile**.

ÉTAPE 2 Pour ajouter un nouveau profil de stratégie de filtrage URL Web, cliquez sur **Add**.

Other Options : pour modifier une entrée, cliquez sur l'icône de **modification** (crayon). Pour supprimer une entrée, cliquez sur l'icône de **suppression** (x). Le profil par défaut ne peut pas être supprimé.

La fenêtre Policy Profile - Add/Edit s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **Policy Name** : entrez le nom du profil de stratégie.
- **Description** : entrez une courte description du profil de stratégie.
- **Select URL Categories to Block** : sélectionnez une catégorie d'URL pour la bloquer, ou décochez cette case pour l'autoriser. Si une catégorie d'URL est bloquée (ou autorisée), tous les sites Web appartenant à cette catégorie sont bloqués (ou autorisés).

ÉTAPE 4 Spécifiez les exceptions de site Web si nécessaire. Les exceptions de site Web vous permettent d'autoriser ou de bloquer des sites Web spécifiques en fonction des paramètres de catégorie d'URL. Toutes les exceptions de site Web peuvent être ajoutées à la liste de contrôle d'accès aux sites Web. La liste de contrôle d'accès aux sites Web a une priorité plus élevée que les paramètres de catégorie d'URL. Voir **Configuration de la liste de contrôle d'accès aux sites Web, page 299**.

Par exemple, si la catégorie Sports et loisirs est bloquée, mais que vous voulez autoriser le site Web : www.sports.com, vous pouvez l'ajouter à la liste de contrôle d'accès aux sites Web comme exception.

ÉTAPE 5 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration de la liste de contrôle d'accès aux sites Web

Le blocage d'une catégorie d'URL bloquera tous les sites Web appartenant à cette catégorie. Vous pouvez spécifier les exceptions de site Web dans la liste de contrôle d'accès aux sites Web. Les exceptions de site Web remplaceront les paramètres de catégorie d'URL dans le même profil.

REMARQUE Jusqu'à 32 exceptions de site Web peuvent être configurées pour chaque profil de stratégie de filtrage URL Web.

ÉTAPE 1 Dans la zone **Specify URLs or URL keywords you want to permit or deny**, cliquez sur **Edit**.

La fenêtre Policy Profile - Add/Edit s'ouvre.

ÉTAPE 2 Pour ajouter une règle d'accès au site Web, cliquez sur **Add**.

Autres options : pour modifier une entrée, cliquez sur l'icône de **modification** (crayon). Pour supprimer une entrée, cliquez sur l'icône de **suppression** (x). Pour supprimer toutes les entrées, cliquez sur **Delete All**.

La fenêtre Website Access Control Rule - Add/Edit s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **Enable Content Filter URL** : cliquez sur **On** pour activer la règle d'accès au site Web, ou sur **Off** pour créer uniquement la règle d'accès au site Web.
- **URL** : entrez le nom de domaine ou le mot-clé d'URL d'un site Web que vous souhaitez autoriser ou bloquer.
- **Match Type** : spécifiez la méthode pour appliquer cette règle :
  - **Domain** : autoriser ou refuser l'accès HTTP d'un site Web qui correspond exactement au nom de domaine que vous avez entré dans le champ **URL**.

    Par exemple, si vous entrez example.com dans le champ URL, cela peut alors correspondre au site Web http://example.com/*, mais ne peut pas correspondre au site Web http://*.example.com.uk/*.
  - **URL Keyword** : autoriser ou refuser l'accès HTTP d'un site Web qui contient le mot-clé que vous avez entré dans le champ **URL**.

    Par exemple, si vous entrez example dans le champ URL, cela peut alors correspondre aux sites tels que www.example.com, tw.example.com, www.example.com.uk et www.example.co.jp.
- **Action** : choisissez **Permit** pour autoriser l'accès, ou choisissez **Block** pour bloquer l'accès.

ÉTAPE 4 Cliquez sur **OK** pour enregistrer vos paramètres.

Mappage des profils de stratégie de filtrage URL Web aux zones

Utilisez la page Policy to Zone Mapping pour appliquer le profil de stratégie de filtrage URL Web à chaque zone. La stratégie de filtrage URL Web affectée à chaque zone détermine s'il faut bloquer ou transférer les requêtes HTTP à partir des hôtes de la zone. Par défaut, le profil par défaut qui autorise toutes les catégories d'URL est affecté à toutes les zones prédéfinies et aux nouvelles zones.

ÉTAPE 1 Cliquez sur **Security Services > Web URL Filtering > Policy to Zone Mapping**.

La fenêtre Policy to Zone Mapping s'ouvre.

ÉTAPE 2 Cliquez sur **On** pour activer le filtrage URL Web ou sur **Off** pour le désactiver.

REMARQUE : L'activation du filtrage URL Web désactivera le filtrage du contenu du pare-feu et vice-versa.

ÉTAPE 3 Dans la zone **Zone Policy Map**, choisissez une stratégie de filtrage URL Web pour chaque zone.

ÉTAPE 4 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration des paramètres avancés du filtrage URL Web

ÉTAPE 1 Cliquez sur **Security Services > Web URL Filtering > Advanced Settings**.

ÉTAPE 2 Saisissez les informations suivantes :

- **Filter Traffic on HTTP port** : entrez le numéro de port utilisé pour filtrer le trafic HTTP. Le filtrage URL Web surveille et contrôle uniquement les visites de sites Web via le port HTTP spécifié. La valeur par défaut est 80.
- **Filter Traffic on HTTPS port** : entrez le numéro de port utilisé pour filtrer le trafic HTTPS. Le filtrage URL Web surveille et contrôle uniquement les visites de sites Web via le port HTTPS spécifié. La valeur par défaut est 443.
- **Blocked Web Components** : vous pouvez bloquer ou autoriser les composants Web tels que Proxy, Java, ActiveX et les cookies. Par défaut, tous sont autorisés.
  - **Proxy** : cochez cette case pour bloquer les serveurs proxy, qui peuvent être utilisés pour contourner certaines règles de pare-feu et présenter d'éventuelles failles de sécurité.
  - **Java** : cochez cette case pour bloquer les applets Java pouvant être téléchargées à partir de pages qui les contiennent.
  - **ActiveX** : cochez cette case pour empêcher le téléchargement des applets ActiveX via Internet Explorer.
  - **Cookies** : cochez cette case pour bloquer les cookies, qui contiennent généralement des sessions.

ÉTAPE 3 Choisissez l'une des actions suivantes lorsque le filtrage URL Web n'est pas disponible :

- **Block Web Traffic when web URL filter services are not available** : l'ensemble du trafic Web est bloqué jusqu'à ce que le filtrage URL Web soit disponible.
- **Allow Web Traffic even when web URL filter services are not available** : l'ensemble du trafic Web est autorisé jusqu'à ce que le filtrage URL Web soit disponible.

ÉTAPE 4 Choisissez l'une des actions suivantes lorsqu'une page Web est bloquée :

- **Display Blocked URL Message when the requested page is blocked** : affiche la page de blocage par défaut lorsqu'une page Web est bloquée. Si vous choisissez cette option, le message que vous spécifiez dans le champ **Blocked URL Message** s'affichera sur la page de blocage par défaut.
- **Redirect URL** : redirige vers une page Web spécifiée lorsqu'une page Web est bloquée. Si vous choisissez cette option, entrez l'URL de redirection souhaitée. Vérifiez que l'URL spécifiée est bien autorisée par la liste de contrôle d'accès aux sites Web.

ÉTAPE 5 Cliquez sur **Save** pour appliquer vos paramètres.

Réputation de réseau

La réputation de réseau bloque le trafic entrant provenant des adresses IP connues pour lancer des attaques sur Internet. La réputation de réseau vérifie les adresses source et de destination de chaque paquet en fonction de la liste noire d'adresses pour déterminer s'il faut traiter ou abandonner le paquet. Les données de la liste noire sont automatiquement mises à jour toutes les six heures. Vous pouvez cliquer sur **Check for Updates Now** sur la page Security Services > Dashboard pour rechercher immédiatement de nouvelles mises à jour de la réputation de réseau.

REMARQUE Aucune configuration n'est requise pour la réputation de réseau. Il vous suffit d'activer ou de désactiver cette fonctionnalité à partir de la page Security Services > Dashboard.

8

VPN

Ce chapitre décrit la procédure de configuration de réseaux privés virtuels (VPN) pour permettre à d'autres sites et aux travailleurs distants d'accéder à vos ressources réseau. Il comprend les sections suivantes :

- **À propos des VPN, page 304**
- **Affichage de l'état du VPN, page 305**
- **Configuration d'un VPN de site à site, page 309**
- **Configuration d'un accès à distance IPsec, page 325**
- **Configuration du client VPN pour télétravailleurs, page 334**
- **Configuration VPN SSL, page 344**
- **Configuration d'un serveur L2TP, page 357**
- **Configuration du transfert VPN, page 359**

Pour accéder aux pages relatives aux VPN, cliquez sur **VPN** dans le volet de navigation gauche.

À propos des VPN

Un VPN fournit un canal de communication sécurisé (également appelé « tunnel ») entre deux routeurs de passerelle ou entre un PC distant et un routeur de passerelle. L'Cisco ISA500 prend en charge les solutions VPN suivantes :

- **Site-to-Site VPN** : connecte deux routeurs pour sécuriser le trafic entre deux sites physiquement séparés. Voir **Configuration d'un VPN de site à site, page 309**.
- **IPsec Remote Access** : permet à l'Cisco ISA500 d'agir en tant que périphérique de tête de réseau dans les VPN d'accès à distance. Votre Cisco ISA500 sera défini comme serveur VPN IPsec et enverra les politiques de sécurité aux clients VPN distants, afin que ceux-ci disposent de stratégies actualisées avant d'établir les connexions VPN. Le serveur VPN IPsec peut également aussi interrompre les connexions VPN lancées par les clients VPN distants. Cette souplesse permet aux utilisateurs distants et mobiles d'accéder à des données et applications critiques sur l'intranet. Voir **Configuration d'un accès à distance IPsec, page 325**.
- **Teleworker VPN Client** : réduit les exigences de configuration sur les sites distants en permettant à l'Cisco ISA500 de fonctionner comme un client matériel VPN Cisco pour recevoir des politiques de sécurité sur le tunnel VPN à partir d'un serveur VPN IPsec distant. Voir **Configuration du client VPN pour télétravailleurs, page 334**.
- **VPN SSL** : permet aux utilisateurs distants d'accéder au réseau d'entreprise à l'aide du logiciel client à mobilité sécurisé Cisco AnyConnect. L'accès à distance est assuré par une passerelle VPN SSL. Voir **Configuration VPN SSL, page 344**.
- **L2TP** : permet aux clients distants d'utiliser un réseau IP public pour sécuriser la communication avec les serveurs de réseau d'entreprise privé. Voir **Configuration d'un serveur L2TP, page 357**.

REMARQUE L'Cisco ISA500 peut faire office soit de serveur VPN IPsec, soit de client matériel VPN Cisco, mais pas les deux simultanément.

Affichage de l'état du VPN

Cette section explique comment afficher les informations relatives à toutes les sessions VPN. Reportez-vous aux rubriques suivantes :

- **Affichage de l'état du VPN IPsec, page 305**
- **Affichage de l'état du VPN SSL, page 307**

Affichage de l'état du VPN IPsec

Utilisez la page IPSec VPN Status pour afficher l'état de toutes les sessions VPN IPsec. Cette page est automatiquement mise à jour toutes les 10 secondes. Cliquez sur **Refresh** pour actualiser manuellement les données.

VPN > VPN Status > IPsec VPN Status

Champ	Description
Sessions actives Pour mettre fin manuellement à une session VPN IPsec, cliquez sur l'icône de **déconnexion** dans la colonne **Connect**. Pour mettre fin manuellement à plusieurs sessions VPN IPsec actives, sélectionnez-les et cliquez sur le bouton **Disconnect**. Si une session VPN IPsec est terminée, vous pouvez établir manuellement la connexion VPN en cliquant sur l'icône de **connexion** dans la colonne **Connect**.	
Name	Stratégie VPN utilisée pour une session VPN IPsec.
Status	État de connexion d'une session VPN IPsec.
VPN Type	Type de connexion VPN pour une session VPN IPsec, tel que Site-to-Site (site à site), IPsec Remote Access ou Teleworker VPN Client.
WAN Interface	Port WAN utilisé pour une session VPN IPsec.

Champ	Description
Remote Gateway	Adresse IP de l'homologue distant. **REMARQUE** : Pour une session VPN de site à site, ce champ indique l'adresse IP de la passerelle distante. Pour une session VPN IPsec entre le client VPN pour télétravailleurs et un serveur VPN IPsec distant, ce champ indique l'adresse IP du serveur VPN IPsec. Pour une session VPN IPsec entre le serveur VPN IPsec et un client VPN distant, ce champ indique l'adresse IP du client VPN distant.
Local Network	Adresse IP de sous-réseau et masque réseau du réseau local.
Remote Network	Adresse IP de sous-réseau et masque réseau du réseau distant.
Statistics	
Name	Stratégie VPN utilisée pour une session VPN IPsec.
VPN Type	Type de connexion VPN pour une session VPN IPsec.
Interface WAN	Port WAN utilisé pour une session VPN IPsec.
Remote Gateway	Adresse IP de l'homologue distant.
Local Network	Adresse IP de sous-réseau et masque réseau du réseau local.
Remote Network	Adresse IP de sous-réseau et masque réseau du réseau distant.
Tx Bytes	Volume du trafic en kilo-octets transmis à partir du tunnel VPN.
Rx Bytes	Volume du trafic en kilo-octets reçu à partir du tunnel VPN.
Tx Packets	Nombre de paquets IP transmis à partir du tunnel VPN.
Rx Packets	Nombre de paquets IP reçus à partir du tunnel VPN.
Teleworker VPN Client Si la fonctionnalité de client VPN pour télétravailleurs (Teleworker VPN Client) est activée et que l'Cisco ISA500 agit en tant que client matériel VPN Cisco, les informations ci-dessous sont affichées.	

Champ	Description
Status	Indique si la fonctionnalité Teleworker VPN Client est activée ou désactivée.
Primary DNS	Adresse IP du serveur DNS principal.
Secondary DNS	Adresse IP du serveur DNS secondaire.
Primary WINS	Adresse IP du serveur WINS principal.
Secondary WINS	Adresse IP du serveur WINS secondaire.
Default Domain	Nom de domaine par défaut.
Split Tunnel	Adresse IP et masque réseau pour les sous-réseaux fractionnés spécifiés.
Split DNS	Nom de domaine pour le DNS fractionné spécifié.
Backup Server 1/2/3	Adresse IP ou nom d'hôte pour les serveurs de sauvegarde spécifiés.

Affichage de l'état du VPN SSL

Reportez-vous à la page SSL VPN Status pour consulter les informations relatives à toutes les sessions VPN SSL actives. Cette page est automatiquement mise à jour toutes les 10 secondes. Cliquez sur **Refresh** pour actualiser manuellement les données.

VPN > VPN Status > SSL VPN Status

Champ	Description
Sessions actives Pour mettre fin manuellement à une session VPN SSL active, cliquez sur l'icône de **déconnexion** dans la colonne **Configure**. Pour mettre fin manuellement à plusieurs sessions VPN SSL actives, sélectionnez-les et cliquez sur le bouton **Disconnect**.	
Session ID	ID de la session VPN SSL.
User Name	Nom de l'utilisateur VPN SSL connecté.
Client IP (Actual)	Adresse IP réelle utilisée par le client VPN SSL.
Client IP (VPN)	Adresse IP virtuelle du client VPN SSL attribuée par la passerelle VPN SSL.

Champ	Description
Connect Time	Temps écoulé depuis que l'utilisateur VPN SSL a établi la connexion pour la première fois.

Statistiques VPN SSL

Les informations statistiques globales sont affichées dans la zone **Global Status**. Pour effacer les informations statistiques globales, cliquez sur **Clear**.

Active Users	Nombre total d'utilisateurs VPN SSL connectés.
In CSTP Frames	Nombre de trames CSTP reçues de tous les clients.
In CSTP Bytes	Nombre total d'octets dans les trames CSTP reçues de tous les clients.
In CSTP Data	Nombre de trames de données CSTP reçues de tous les clients.
In CSTP Control	Nombre de trames de contrôle CSTP reçues de tous les clients.
Out CSTP Frames	Nombre de trames CSTP envoyées à tous les clients.
Out CSTP Bytes	Nombre total d'octets dans les trames CSTP envoyées à tous les clients.
Out CSTP Data	Nombre de trames de données CSTP envoyées à tous les clients.
Out CSTP Control	Nombre de trames de contrôle CSTP envoyées à tous les clients.

Dans le tableau **Session Statistics**, les informations répertoriées ci-dessous sont affichées pour chaque session VPN SSL.

Pour effacer les informations statistiques pour une session VPN SSL simple, cliquez sur **Clear** dans la colonne **Configure**. Pour effacer les informations statistiques pour plusieurs sessions VPN SSL, sélectionnez-les et cliquez sur **-Clear**.

Session ID	ID de la session VPN SSL.
In CSTP Frames	Nombre de trames CSTP reçues du client.
In CSTP Bytes	Nombre total d'octets dans les trames CSTP reçues du client.
In CSTP Data	Nombre de trames de données CSTP reçues du client.
In CSTP Control	Nombre de trames de contrôle CSTP reçues du client.

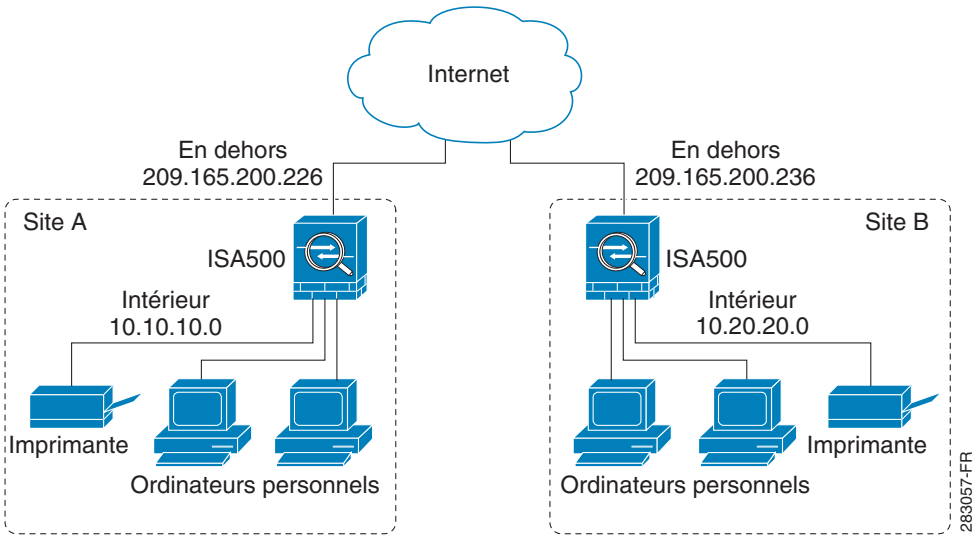
Champ	Description
Out CSTP Frames	Nombre de trames CSTP envoyées au client.
Out CSTP Bytes	Nombre total d'octets dans les trames CSTP envoyées au client.
Out CSTP Data	Nombre de trames de données CSTP envoyées au client.
Out CSTP Control	Nombre de trames de contrôle CSTP envoyées au client.

REMARQUE CSTP est un protocole propriétaire Cisco pour la tunnellisation VPN SSL. « In » indique que le paquet provient du client. « Out » indique que le paquet est envoyé au client. Le client est le PC exécutant le logiciel client à mobilité sécurisé Cisco AnyConnect qui se connecte à l'Cisco ISA500 exécutant le serveur VPN SSL. Une trame CSTP est un paquet transportant les informations de protocole CSTP. Il existe deux principaux types de trames, les trames de contrôle et les trames de données. Les trames de contrôle implémentent des fonctions de contrôle au sein du protocole. Les trames de données transportent les données client, telles que la charge utile tunnellisée.

Configuration d'un VPN de site à site

Un tunnel VPN de site à site connecte deux routeurs pour sécuriser le trafic entre deux sites physiquement séparés.

Figure 3 VPN de site à site



Cette section explique comment configurer les tunnels VPN de site à site. Reportez-vous aux rubriques suivantes :

- **Tâches de configuration pour établir un tunnel VPN de site à site, page 310**
- **Paramètres VPN généraux de site à site, page 311**
- **Configurer des stratégies VPN IPsec, page 312**
- **Configuration des stratégies IKE, page 319**
- **Configuration des ensembles de transformation, page 321**
- **Exemples de configuration de télétravailleur distant, page 322**

Tâches de configuration pour établir un tunnel VPN de site à site

Pour établir un tunnel VPN de site à site, exécutez les tâches de configuration suivantes :

- Ajouter les objets d'adresse IP de sous-réseau de votre réseau local et du réseau distant. Voir **Gestion d'adresse, page 182**.
- (Facultatif) Importez les certificats pour l'authentification entre deux homologues. Ignorez cette étape si vous souhaitez utiliser une clé

pré-partagée pour l'authentification. Voir **Gestion des certificats pour l'authentification, page 393**.

- Activez la fonctionnalité VPN de site à site sur l'Cisco ISA500. Voir **Paramètres VPN généraux de site à site, page 311**.
- Configurez des stratégies IKE. Voir **Configuration des stratégies IKE, page 319**.
- Configurez des stratégies de transformation. Voir **Configuration des ensembles de transformation, page 321**.
- Configurez les stratégies VPN IPsec. Voir **Configurer des stratégies VPN IPsec, page 312**.
- (Facultatif) Cochez une stratégie VPN IPsec activée et cliquez sur l'icône de **connexion** pour établir la connexion VPN.

  Lorsqu'une stratégie VPN IPsec site à site est en place et activée, une connexion est déclenchée par tout trafic correspondant à la stratégie. Dans ce cas, le tunnel VPN est configuré automatiquement. Toutefois, pour une stratégie VPN IPsec dans laquelle le réseau distant du routeur est configuré sur Any (un tunnel site à site), la connexion ne peut pas être configurée automatiquement. Vous devez alors établir la connexion VPN manuellement en cliquant sur l'icône de **connexion**.
- Affichez les informations sur l'état et les statistiques pour toutes les sessions VPN IPsec. Voir **Affichage de l'état du VPN IPsec, page 305**.

Paramètres VPN généraux de site à site

ÉTAPE 1 Cliquez sur **VPN > Site-to-Site > IPsec Policies**.

La fenêtre IPSec Policies s'ouvre. Toutes les stratégies VPN IPsec existantes sont répertoriées dans le tableau. Les informations suivantes sont affichées :

- **Name** : nom de la stratégie VPN IPsec.
- **Enable** : indique si la stratégie VPN IPsec est activée ou désactivée.
- **Status** : indique si le tunnel VPN IPsec est connecté ou déconnecté.
- **WAN Interface** : port WAN que le trafic utilise sur le tunnel VPN IPsec.
- **Peers** : adresse IP de l'homologue distant.
- **Local** : réseau local de l'homologue local.

- **Remote** : réseau distant de l'homologue distant.
- **IKE** : stratégie IKE utilisée pour la stratégie VPN IPsec.
- **Transform** : ensemble de transformation utilisé pour la stratégie VPN IPsec.

ÉTAPE 2 Cliquez sur **On** pour activer le VPN de site à site ou sur **Off** pour le désactiver.

REMARQUE : L'activation de la fonctionnalité VPN de site à site entraîne la désactivation de la fonctionnalité de client VPN pour télétravailleurs.

ÉTAPE 3 Si vous activez le VPN de site à site, effectuez les actions suivantes :

- Pour ajouter une nouvelle stratégie VPN IPsec, cliquez sur **Add**. Voir **Configurer des stratégies VPN IPsec, page 312**.
- Pour modifier une stratégie VPN IPsec existante, cliquez sur l'icône de **modification** (x).
- Pour supprimer une stratégie VPN IPsec, cliquez sur l'icône de **suppression** (x).
- Pour supprimer plusieurs stratégies VPN IPsec, cochez-les et cliquez sur **Delete**.
- Pour activer une stratégie VPN IPsec, cochez la case correspondante dans la colonne **Enable**.
- Pour établir manuellement un tunnel VPN, cliquez sur l'icône de **connexion** pour une stratégie VPN IPsec activée.
- Pour mettre fin manuellement à une connexion VPN, cliquez sur l'icône de **déconnexion**.
- Pour actualiser les données de VPN de site à site, cliquez sur **Refresh**.

ÉTAPE 4 Cliquez sur **Save** pour appliquer vos paramètres.

Configurer des stratégies VPN IPsec

Les stratégies VPN IPsec sont utilisées pour établir une connexion VPN entre deux homologues. ISA550 et ISA550W prennent en charge jusqu'à 50 tunnels VPN IPsec. ISA570 et ISA570W prennent en charge jusqu'à 100 tunnels VPN IPsec.

REMARQUE Avant de créer une stratégie VPN IPsec, assurez-vous que les stratégies IKE et de transformation sont configurées. Ensuite, vous pouvez appliquer les stratégies IKE et de transformation à la stratégie VPN IPsec.

ÉTAPE 1 **Cliquez sur VPN > Site-to-Site > IPsec Policies.**

ÉTAPE 2 Pour ajouter une nouvelle stratégie VPN IPsec, cliquez sur **Add**.

Autres options : pour modifier une entrée, cliquez sur l'icône de **modification** (crayon). Pour supprimer une entrée, cliquez sur l'icône de **suppression** (x). Pour supprimer plusieurs entrées, cochez-les et cliquez sur **Delete**.

La fenêtre IPsec Policies - Add/Edit s'ouvre.

ÉTAPE 3 Dans l'onglet **Basic Settings**, entrez les informations suivantes :

- **Description** : entrez le nom de la stratégie VPN IPsec.
- **IPsec Policy Enable** : cliquez sur **On** pour activer la stratégie VPN IPsec ou sur **Off** pour uniquement créer la stratégie VPN IPsec.
- **Remote Type** : spécifiez l'homologue distant :
  - **Static IP :** sélectionnez cette option si l'homologue distant utilise une adresse IP statique. Entrez l'adresse IP de l'homologue distant dans le champ **Remote Address**.
  - **Dynamic IP** : sélectionnez cette option si l'homologue distant utilise une adresse IP dynamique.
  - **FQDN (Fully Qualified Domain Name)** : sélectionnez cette option pour utiliser le nom de domaine du réseau distant, tel que vpn.company.com. Entrez le nom de domaine de l'homologue distant dans le champ **Remote Address**.

  Pour l'exemple illustré à la **Figure 3**, le site distant, Site B, possède l'adresse IP publique 209.165.200.236. Vous devez sélectionner **Static IP** et entrer 209.165.200.236 dans le champ **Remote Address**.
- **Authentication Method** : choisissez l'une des méthodes d'authentification suivantes :
  - **Pre-shared Key** : utilise une clé unique, basée sur votre mot de passe, pour l'authentification. Si vous choisissez cette option, saisissez la valeur que le périphérique homologue doit fournir pour établir une connexion dans le champ **Key**. La clé prépartagée PSK (Pre-Shared Key) saisie doit être exactement identique ici et sur l'homologue distant.
  - **Certificate** : utilise un certificat numérique d'une autorité de certification (CA) tierce pour l'authentification. Si vous choisissez cette option, sélectionnez un certificat CA comme certificat local dans la liste déroulante **Local Certificate** et sélectionnez un certificat CA comme

certificat distant dans la liste déroulante **Remote Certificate**. Le certificat distant sélectionné sur la passerelle locale doit être configuré comme certificat local sur l'homologue distant.

REMARQUE : Vous devez avoir les certificats CA valides importés sur votre Cisco ISA500 avant de choisir cette option. Accédez à la page Device Management > Certificate Management pour importer les certificats CA. Voir **Gestion des certificats pour l'authentification, page 393**.

- **WAN Interface** : sélectionnez le port WAN que le trafic utilise sur le tunnel VPN IPsec.
- **Local Network** : sélectionnez l'adresse IP du réseau local. Si vous souhaitez configurer les paramètres de contrôle d'accès aux zones pour le VPN de site à site, sélectionnez **Any** pour le réseau local. Ensuite, vous pourrez contrôler le trafic entrant à partir du réseau VPN distant vers les zones sur les tunnels VPN.
- **Remote Network** : sélectionnez l'adresse IP du réseau distant. Vous devez connaître l'adresse IP du réseau distant avant de connecter le tunnel VPN.

  Pour l'exemple illustré à la **Figure 3**, le site A a l'adresse IP LAN 10.10.10.0 LAN et le site B a l'adresse IP LAN 10.20.20.0. Lorsque vous configurez le VPN de site à site sur le site A, le réseau local est 10.10.10.0 et le réseau distant est 10.20.20.0.

  Si l'objet d'adresse que vous souhaitez n'est pas dans la liste, sélectionnez **Create a new address** pour ajouter un nouvel objet d'adresse ou sélectionnez **Create a new address group** pour ajouter un nouvel objet de groupe d'adresses. Pour gérer les objets d'adresses et de groupes d'adresses, accédez à la page Networking > Address Management. Voir **Gestion d'adresse, page 182**.

  REMARQUE : L'Cisco ISA500 peut prendre en charge plusieurs sous-réseaux pour établir les tunnels VPN. Sélectionnez un objet de groupe d'adresses incluant plusieurs sous-réseaux pour les réseaux locaux et/ou distants.

ÉTAPE 4 Dans l'onglet **Advanced Settings**, entrez les informations suivantes :

- **PFS Enable** : cliquez sur **On** pour activer Perfect Forward Secrecy (PFS) afin d'améliorer la sécurité ou cliquez sur **Off** pour désactiver cette option. Si vous activez PFS, un échange Diffie-Hellman est effectué pour chaque négociation de phase 2. PFS est souhaitable sur le canal de génération de clé de la connexion VPN.

- **DPD Enable** : cliquez sur **On** pour activer la détection DPD (Dead peer detection) ou sur **Off** pour la désactiver. DPD est une méthode de détection d'homologues IKE (Internet Key Exchange) morts. Cette méthode utilise des modèles de trafic IPsec afin de réduire le nombre de messages requis pour confirmer la disponibilité d'un homologue. La détection DPD est utilisée pour récupérer les ressources perdues au cas où un homologue serait trouvé mort, ainsi que pour effectuer un basculement d'homologue IKE. Si vous activez DPD, saisissez les informations suivantes :
  - **Delay Time** : saisissez la valeur du délai d'attente, en secondes, entre des messages DPD R-U-THERE consécutifs. Les messages DPD R-U-THERE sont envoyés uniquement lorsque le trafic IPsec est inactif. La valeur par défaut est de 10 secondes.
  - **Detection Timeout** : saisissez la valeur du délai de détection, en secondes. S'il n'y a aucune réponse et aucun trafic au cours de ce délai, déclarez l'homologue mort. La valeur par défaut est de 30 secondes.
  - **DPD Action** : choisissez l'une des actions suivantes au cours du délai de détection :

    Hold : le trafic de votre réseau local vers le réseau distant peut déclencher l'Cisco ISA500 pour relancer la connexion VPN au cours du délai de détection. Nous vous recommandons d'utiliser l'option « Hold » lorsque l'homologue distant utilise une adresse IP statique.

    Clean : mettez fin à la connexion VPN au cours du délai de détection. Vous devez relancer manuellement la connexion VPN. Nous vous recommandons d'utiliser l'option « Clean » lorsque l'homologue distant utilise une adresse IP dynamique.

    Restart : relance la connexion VPN trois fois au cours du délai de détection.
- **Windows Networking (NetBIOS) Broadcast** : cliquez sur **On** pour permettre d'accéder à des ressources réseau à distance à l'aide de son nom NetBIOS, par exemple, en parcourant le voisinage de Windows. La diffusion Netbios peut résoudre un nom NetBIOS en une adresse réseau. Cette option permet aux diffusions NetBIOS de se déplacer via le tunnel VPN.
- **Access Control** : lorsque le réseau local est défini sur « Any », vous pouvez contrôler le trafic entrant du réseau VPN distant vers les zones. Cliquez sur **Permit** pour permettre l'accès ou sur **Deny** pour le refuser. Par défaut, le trafic entrant du réseau distant vers toutes les zones est autorisé.

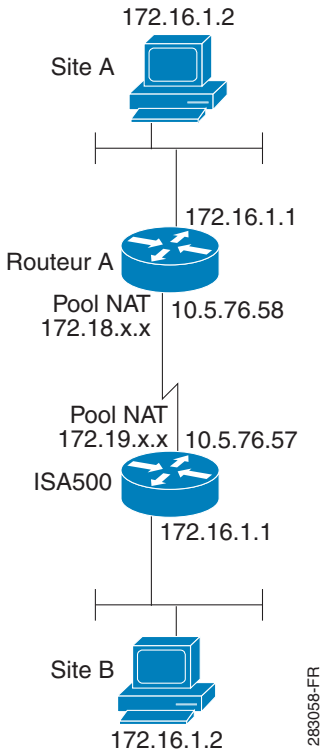
REMARQUE : Les règles de pare-feu VPN qui sont automatiquement générées par les paramètres de contrôle d'accès aux zones seront ajoutées à la liste des règles de pare-feu avec une priorité supérieure aux règles de pare-feu par défaut, mais inférieure aux règles de pare-feu personnalisées.

- **Apply NAT Policies** : cliquez sur **On** pour appliquer les paramètres NAT au réseau local et au réseau distant qui communiquent sur le tunnel VPN. Cette option est particulièrement utile dans les cas où les deux côtés d'un tunnel utilisent des sous-réseaux identiques ou qui se chevauchent.
  - **Translates Local Network** : pour traduire le réseau local, sélectionnez un objet d'adresse traduit pour le réseau local.
  - **Translates Remote Network** : pour traduire le réseau distant, sélectionnez un objet d'adresse traduit pour le réseau distant.

  Si l'objet d'adresse que vous souhaitez n'est pas dans la liste, sélectionnez **Create a new address** pour ajouter un nouvel objet d'adresse ou sélectionnez **Create a new address group** pour ajouter un nouvel objet de groupe d'adresses. Pour gérer les objets d'adresses ou de groupes d'adresses, accédez à la page Networking > Address Management. Voir **Gestion d'adresse, page 182**.

  La **Figure 4** présente un exemple de mise en réseau simulant deux sociétés qui fusionnent avec le même système d'adressage IP. Deux routeurs sont connectés avec un tunnel VPN et les réseaux derrière chaque routeur sont identiques. Pour qu'un site accède aux hôtes sur l'autre site, la traduction d'adresses de réseau (NAT) est utilisée sur les routeurs pour modifier les adresses source et de destination en sous-réseaux différents.

Figure 4 Exemple de mise en réseau simulant deux sociétés qui fusionnent avec le même système d'adressage IP



Dans cet exemple, lorsque l'hôte 172.16.1.2 sur le site A accède à l'hôte dont l'adresse IP est identique sur le site B, il se connecte à une adresse 172.19.1.2 au lieu de l'adresse réelle 172.16.1.2. Lorsque l'hôte sur le site B veut accéder au site A, il se connecte à une adresse 172.18.1.2. La traduction d'adresses de réseau sur le routeur A traduit toute adresse 172.16.x.x pour qu'elle ressemble à l'entrée de l'hôte correspondante 172.18.x.x. La traduction d'adresses de réseau sur l'ISA500 modifie l'adresse 172.16.x.x pour qu'elle ressemble à 172.19.x.x.

REMARQUE : Cette configuration permet uniquement aux deux réseaux de communiquer. Elle ne permet pas la connectivité Internet. Vous avez besoin de chemins supplémentaires à Internet pour la connectivité à des sites autres que ces deux sites ; en d'autres termes, vous devez ajouter un routeur ou un pare-feu supplémentaire de chaque côté, avec plusieurs routes configurées sur les hôtes.

- **IKE Policy** : sélectionnez la stratégie IKE utilisée pour la stratégie VPN IPsec. Vous pouvez cliquer sur **IKE Policy Link** pour maintenir les stratégies IKE, mais enregistrez vos paramètres sur cette page en premier lieu.

- **Transform** : sélectionnez l'ensemble de transformation utilisé pour la stratégie VPN IPsec. Vous pouvez cliquer sur **Transform Link** pour maintenir les stratégies de transformation, mais enregistrez vos paramètres sur cette page en premier lieu.
- **SA-Lifetime** : saisissez la durée de vie de l'association de sécurité (SA) IPsec. La durée de vie de l'association de sécurité IPsec représente l'intervalle de temps après lequel l'association de sécurité IPsec devient non valide. Une fois cet intervalle écoulé, l'association de sécurité IPsec est renégociée. La valeur par défaut est d'1 heure.

ÉTAPE 5 Dans l'onglet **VPN Failover**, entrez les informations suivantes :

- **WAN Failover Enable** : cliquez sur **On** pour activer le basculement WAN pour le VPN de site à site ou sur **Off** pour le désactiver. Si vous activez le basculement WAN, le port WAN de secours garantit que le trafic VPN bascule sur la liaison de sauvegarde à chaque fois que la liaison principale tombe en panne. L'Cisco ISA500 met automatiquement à jour la passerelle WAN locale pour le tunnel VPN en fonction des configurations de la liaison WAN de secours. À cet effet, le DNS dynamique doit être configuré, car l'adresse IP est modifiée par le basculement, ou autorisez la passerelle distante utiliser l'adresse IP dynamique.

  REMARQUE : Pour activer le basculement WAN pour le VPN de site à site, vérifiez que le port WAN secondaire a été configuré et que la redondance WAN a été définie comme mode de basculement ou d'équilibrage de charge.

- **Redundant Gateway** : cliquez sur **On** pour activer la passerelle redondante ou sur **Off** pour la désactiver. Si vous activez la passerelle redondante, lorsque la connexion de la passerelle distante tombe en panne, la connexion de secours devient automatiquement active. Une stratégie de secours prend effet uniquement si la stratégie primaire échoue.

  - **Select Backup Policy** : choisissez une stratégie de secours pour cette stratégie.
  - **Fallback Time to switch from back-up to primary** : saisissez le nombre de secondes nécessaires avant la confirmation du rétablissement d'un tunnel principal après une défaillance. Si le tunnel principal est actif pendant le nombre de secondes spécifié, l'Cisco ISA500 bascule sur le tunnel principal en désactivant le tunnel de secours. Saisissez une valeur comprise entre 3 et 59 secondes. La valeur par défaut est de 5 secondes.

REMARQUE : La détection DPD doit être activée si vous souhaitez utiliser la fonctionnalité de passerelle redondante pour la connexion VPN IPsec.

ÉTAPE 6 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 7 Lorsque la fonctionnalité VPN de site à site et la stratégie VPN IPsec sont activées, le message d'avertissement suivant apparaît à l'écran : « Do you want to make this connection active when the settings are saved? » (Voulez-vous rendre cette connexion active lorsque les paramètres sont enregistrés ?)

- Si vous souhaitez activer la connexion immédiatement après l'enregistrement des paramètres, cliquez sur le bouton **Activate Connection**. Une fois que vous avez enregistré vos paramètres, l'Cisco ISA500 tente immédiatement d'établir la connexion VPN. Vous pouvez consulter son état de connexion dans la colonne Status.
- Si vous souhaitez uniquement créer la stratégie VPN IPsec et ne souhaitez pas activer la connexion immédiatement après l'enregistrement des paramètres, cliquez sur le bouton **Do Not Activate**. La connexion sera déclenchée par tout trafic correspondant à la stratégie VPN IPsec et le tunnel VPN sera configuré automatiquement. Vous pouvez également cliquer sur l'icône de **connexion** pour établir manuellement la connexion VPN.

ÉTAPE 8 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration des stratégies IKE

Le protocole IKE (Internet Key Exchange) est un protocole de négociation comprenant une méthode de cryptage pour protéger les données et garantir la confidentialité. Il s'agit également d'une méthode d'authentification pour vérifier l'identité des périphériques qui tentent de se connecter au réseau.

Vous pouvez créer des stratégies IKE pour définir les paramètres de sécurité (tels que l'authentification de l'homologue, les algorithmes de cryptage, etc.) à utiliser pour un tunnel VPN.

REMARQUE Jusqu'à 16 stratégies IKE peuvent être configurées sur l'Cisco ISA500.

ÉTAPE 1 Cliquez sur **VPN > Site-to-Site > IKE Policies**.

La fenêtre IKE Policies s'ouvre. Les stratégies IKE par défaut et personnalisées sont répertoriées dans le tableau.

ÉTAPE 2 Pour ajouter une nouvelle stratégie, cliquez sur **Add**.

Autres options : pour modifier une entrée, cliquez sur l'icône de **modification** (crayon). Pour supprimer une entrée, cliquez sur l'icône de **suppression** (x). Pour supprimer plusieurs entrées, cochez-les et cliquez sur **Delete**. La stratégie IKE par défaut (DefaultIke) ne peut être ni modifiée, ni supprimée.

La fenêtre IKE Policy - Add/Edit s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **Name** : entrez le nom de la stratégie IKE.
- **Encryption** : sélectionnez l'algorithme utilisé pour négocier l'association de sécurité. Quatre algorithmes sont pris en charge par l'Cisco ISA500 : ESP_3DES, ESP_AES_128, ESP_AES_192 et ESP_AES_256.
- **Hash** : spécifiez l'algorithme d'authentification pour l'en-tête VPN. Deux algorithmes de hachage sont pris en charge par l'Cisco ISA500 : SHA1 et MD5.

  REMARQUE : Vérifiez que l'algorithme d'authentification est configuré de manière identique des deux côtés.
- **Authentication** : spécifiez la méthode d'authentification utilisée par l'Cisco ISA500 pour établir l'identité de chaque homologue IPsec.
  - **Pre-shared Key** : utilise une clé unique, basée sur votre mot de passe, pour l'authentification. La clé alphanumérique est partagée avec l'homologue IKE. L'évolutivité des clés pré-partagée face à un réseau en expansion est insuffisante, mais elles sont plus faciles à configurer dans un petit réseau.
  - **RSA_SIG** : utilise un certificat numérique pour l'authentification. RSA_SIG est un certificat numérique avec des clés générées par l'algorithme de signatures RSA. Dans ce cas, un certificat doit être configuré pour que la signature RSA fonctionne.
- **D-H Group** : sélectionnez l'identifiant de groupe Diffie-Hellman que les deux homologues IPsec utilisent pour dériver un secret partagé sans se le transmettre. Le groupe D-H définit la puissance de l'algorithme en bits. Plus le numéro du groupe Diffie-Hellman est bas, moins il a besoin de temps CPU pour être exécuté. Plus le numéro du groupe Diffie-Hellman est élevé, plus la sécurité est élevée.
  - Groupe 2 (1 024 bits)
  - Groupe 5 (1 536 bits)

- Groupe 14 (2 048 bits)

- **Lifetime** : saisissez le nombre de secondes pendant lesquelles l'association de sécurité IKE reste valide. En règle générale, une durée de vie plus courte permet des négociations ISAKMP (Internet Security Association and Key Management Protocol) mieux sécurisées (jusqu'à un certain point). Toutefois, les durées de vie plus courtes permettent à l'Cisco ISA500 de configurer les associations de sécurité IPsec futures plus rapidement. La valeur par défaut est de 24 heures.

ÉTAPE 4 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 5 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration des ensembles de transformation

Un ensemble de transformation détermine les algorithmes d'intégrité et de cryptage que l'homologue utilisera pour protéger les communications de données. Deux homologues doivent utiliser le même algorithme pour communiquer.

REMARQUE Jusqu'à 16 ensembles de transformation peuvent être configurés sur l'Cisco ISA500.

ÉTAPE 1 Cliquez sur **VPN > Site-to-Site > Transform Policies**.

La fenêtre Transform Sets s'ouvre. Les ensembles de transformation par défaut et personnalisés sont répertoriés dans le tableau.

ÉTAPE 2 Pour ajouter un nouvel ensemble de transformation, cliquez sur **Add**.

Autres options : pour modifier une entrée, cliquez sur l'icône de **modification** (crayon). Pour supprimer une entrée, cliquez sur l'icône de **suppression** (x). Pour supprimer plusieurs entrées, cochez-les et cliquez sur **Delete**. L'ensemble de transformation par défaut (DefaultTrans) ne peut être ni modifié, ni supprimé.

La fenêtre Transform Set - Add/Edit s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **Name** : saisissez le nom de l'ensemble de transformation.

- **Integrity** : sélectionnez l'algorithme de hachage utilisé pour assurer l'intégrité des données. Il garantit que la provenance d'un paquet est bien celle qu'il indique et que ce dernier n'a pas été modifié pendant le transit.

- **ESP_SHA1_HMAC** : authentification avec SHA1 (160 bits).
- **ESP_MD5_HMAC** : authentification avec MD5 (128 bits). MD5 a une empreinte plus petite et est considéré comme étant un peu plus rapide que SHA1. Une attaque réussie (mais extrêmement difficile) contre MD5 est survenue ; cependant, la variante HMAC utilisée par IKE empêche cette attaque.

▪ **Encryption** : sélectionnez l'algorithme de cryptage symétrique qui protège la transmission des données entre deux homologues IPsec. Le paramètre par défaut est ESP_3DES. La norme AES (Advanced Encryption Standard) prend en charge des longueurs de clé de 128, 192 et 256 bits.

- **ESP_3DES** : cryptage avec 3DES (168 bits).
- **ESP_AES_128** : cryptage avec AES (128 bits).
- **ESP_AES_192** : cryptage avec AES (192 bits).
- **ESP_AES_256** : cryptage avec AES (256 bits).

ÉTAPE 4 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 5 Cliquez sur **Save** pour appliquer vos paramètres.

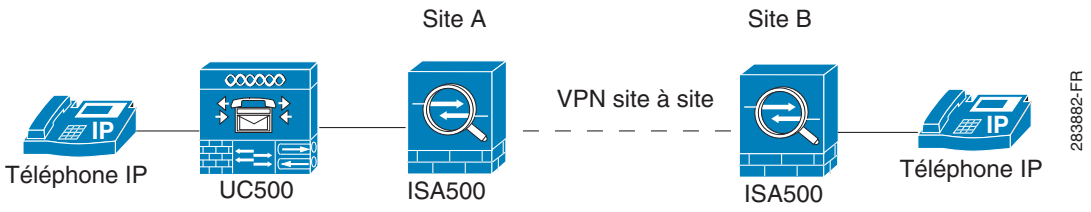
Exemples de configuration de télétravailleur distant

Exemple d'utilisation : vous souhaitez établir un tunnel VPN de site à site entre l'Cisco ISA500 et un UC500 distant pour fournir des services voix et données sur les téléphones d'un site distant.

Solution : lorsque vous utilisez la fonctionnalité Multisite Manager (MSM) du CCA (Cisco Configuration Assistant) pour configurer les paramètres VPN de site à site de l'UC500, MSM du CCA utilise l'ensemble de transformation par défaut et la stratégie IKE. Dans ce cas, l'Cisco ISA500 doit créer une stratégie VPN IPsec comme suit pour établir le tunnel VPN de site à site avec l'UC500.

Champ	Paramètre
Remote Network	Choisissez un groupe d'adresses comprenant plusieurs sous-réseaux sur l'UC500. **REMARQUE** : Par défaut, trois VLAN (192.168.10.0/24, 10.1.1.0/24 et 10.1.10.0/24) sont prédéfinis sur l'UC500.
IKE Policy	Encryption = ESP_3DES Hash = SHA1 D-H Group = Group 2 **REMARQUE** : La stratégie IKE par défaut utilisée sur l'UC500 ne peut être modifiée via le CCA. Les paramètres IKE ci-dessus doivent être configurés sur l'Cisco ISA500.
Transform	Intégrité = ESP_SHA1_HMAC Encryption = ESP_3DES **REMARQUE** : L'ensemble de transformation par défaut utilisé sur l'UC500 ne peut pas être modifié via le CCA. Les paramètres de transformation ci-dessus doivent être configurés sur l'Cisco ISA500.

Exemple d'utilisation : le périphérique UC500 est derrière l'Cisco ISA500. Vous souhaitez établir un tunnel VPN de site à site entre deux appareils de sécurité pour fournir des services voix et données sur les téléphones d'un site distant.



Solution : lorsque vous configurez le VPN de site à site sur les dispositifs de sécurité, assurez-vous que le réseau local sur l'Cisco ISA500 du site A est défini sur « Any » et que le réseau distant sur l'Cisco ISA500 du site B est défini sur « Any ».

Étant donné que l'Cisco ISA500 fournit le pare-feu, la traduction d'adresses de réseau (NAT) et la passerelle de couche Application SIP (SIP ALG, SIP Application Level Gateway) pour votre réseau, vous devez désactiver ces fonctions sur l'UC500. Pour toute instruction, reportez-vous à la documentation ou l'aide en ligne du CCA (Cisco Configuration Assistant).

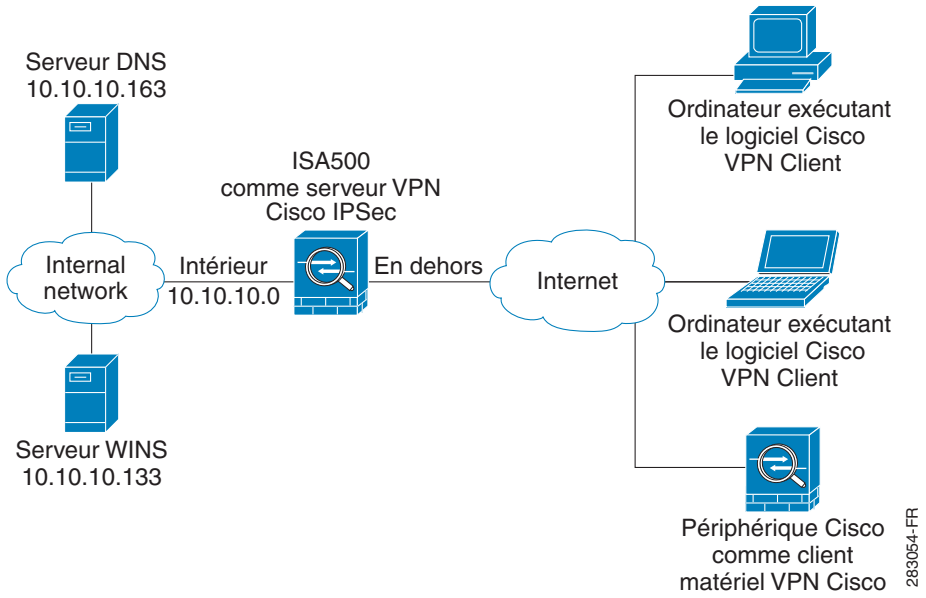
Pour permettre aux hôtes de sous-réseaux non natifs du Cisco ISA500 d'accéder à Internet via des tunnels VPN, vous devez créer manuellement des règles NAT avancées sur votre Cisco ISA500. Accédez à la page Firewall > NAT > Advanced NAT pour effectuer cette opération. Par exemple, vous pouvez créer une règle NAT avancée, comme suit, pour permettre aux hôtes du LAN de données (10.25.1.0/24) derrière l'UC500 d'accéder à Internet :

Name	datalan-behinduc500
Enable	On
From	Any
To	WAN1
Original Source Address	uc540-datalan **REMARQUE** : Vous pouvez sélectionner l'option **Create a new address** dans la liste déroulante pour créer un objet d'adresse pour le LAN de données (10.25.1.0/24) derrière l'UC500, puis le sélectionner comme adresse source d'origine.
Original Destination Address	Any
Original Services	Any
Translated Source Address	WAN1_IP
Translated Destination Address	Any
Translated Services	Any

Configuration d'un accès à distance IPsec

La fonctionnalité d'accès à distance IPsec introduit la prise en charge du serveur pour les clients logiciels Client VPN Cisco (version 4.x et 5.x) et les clients matériels VPN Cisco. Cette fonctionnalité permet aux utilisateurs distants d'établir les tunnels VPN afin d'accéder en toute sécurité aux ressources réseau de l'entreprise. Les stratégies IPsec gérées de manière centralisée sont « envoyées » aux clients VPN distants de VPN par le serveur VPN, ce qui réduit la configuration par les utilisateurs finaux.

Figure 5 Accès à distance IPsec avec le logiciel Client VPN Cisco ou un périphérique Cisco comme un client matériel VPN Cisco



REMARQUE Lorsque l'Cisco ISA500 agit en tant que serveur VPN IPsec, la stratégie IKE et l'ensemble de transformation ci-dessous sont utilisés par défaut. La stratégie IKE et l'ensemble de transformation utilisés sur l'Cisco ISA500 sont inconfigurables.

Champ	Paramètre
IKE Policy	Encryption = ESP_AES_256 Hash = SHA Authentication = Pre-shared Key D-H Group = Group 2
Transform	Integrity = SHA Encryption = ESP_AES_256

Cette section décrit la procédure de configuration de la fonctionnalité d'accès à distance IPsec. Reportez-vous aux rubriques suivantes :

- **Compatibilité du client VPN Cisco, page 326**
- **Activation de l'accès à distance IPsec, page 327**
- **Configuration des stratégies de groupe d'accès à distance IPsec, page 328**
- **Configuration de règles NAT avancées pour permettre aux clients VPN distants d'accéder à Internet via les tunnels VPN, page 331**

Compatibilité du client VPN Cisco

Le client VPN distant peut être un périphérique Cisco qui sert de client matériel VPN Cisco ou un PC qui exécute le logiciel Client VPN Cisco (version 4.x ou 5.x).

Le logiciel Client VPN Cisco est un logiciel client IPsec destiné aux utilisateurs Windows, Mac ou Linux. Le logiciel Client Cisco VPN est compatible avec les plates-formes suivantes :

- Windows 7 (32 bits et 64 bits)
- Windows Vista (32 bits et 64 bits)
- Windows XP (32 bits)
- Linux Intel (noyau 2.6.x)
- Mac OS X 10.5 et 10.6

Vous pouvez trouver les programmes d'installation du logiciel Client VPN Cisco sur le CD qui est joint à la livraison du périphérique. Ce CD inclut les packages de client VPN pour Windows, Mac OS X et Linux. Sélectionnez le package du client VPN correspondant à votre système d'exploitation sur le CD afin de procéder à son téléchargement.

Vous pouvez également télécharger le logiciel Client VPN Cisco via ce lien : http://www.cisco.com/cisco/software/navigator.html?mdfid=278875403 Sélectionnez ensuite **Client VPN Cisco**.

REMARQUE Vous devez vous connecter et posséder un contrat de service cisco valide afin d'avoir accès au logiciel Client VPN Cisco. Un contrat de service d'assistance Cisco Small Business de 3 ans (CON-SBS-SVC2) est requis pour télécharger le logiciel client sur le site Cisco.com. Si vous n'en disposez pas, contactez votre partenaire, votre revendeur ou l'assistance CISCO pour en savoir plus.

Pour plus d'informations sur le téléchargement, l'installation et la configuration du logiciel Client VPN Cisco, consultez le site http://www.cisco.com/en/US/products/sw/secursw/ps2308/index.html.

Activation de l'accès à distance IPsec

ÉTAPE 1 Cliquez sur **VPN > IPsec Remote Access**.

ÉTAPE 2 Cliquez sur **On** pour activer la fonctionnalité d'accès à distance IPsec et, par conséquent, définir l'Cisco ISA500 comme serveur VPN IPsec, ou sur **Off** pour la désactiver.

REMARQUE : L'activation de la fonctionnalité d'accès à distance IPsec désactive la fonctionnalité de client VPN pour télétravailleurs.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration des stratégies de groupe d'accès à distance IPsec

Une stratégie de groupe d'accès à distance IPsec est utilisée par les clients VPN distants pour établir les connexions VPN.

REMARQUE Jusqu'à 16 stratégies de groupe d'accès à distance IPsec peuvent être configurées sur l'Cisco ISA500.

ÉTAPE 1 Cliquez sur **VPN > IPsec Remote Access**.

ÉTAPE 2 Pour ajouter une stratégie de groupe d'accès à distance, cliquez sur **Add**.

Other Options : pour modifier une entrée, cliquez sur l'icône de **modification** (crayon). Pour supprimer une entrée, cliquez sur l'icône de **suppression** (x). Pour supprimer plusieurs entrées, cochez-les et cliquez sur **Delete**.

La fenêtre IPsec Remote Access - Add/Edit s'ouvre.

ÉTAPE 3 Dans l'onglet **Basic Settings**, entrez les informations suivantes :

- **Group Name** : entrez le nom de la stratégie de groupe.
- **WAN Interface** : sélectionnez le port WAN que le trafic utilise sur le tunnel VPN IPsec.
- **IKE Authentication Method** : sélectionnez la méthode d'authentification.
  - **Pre-shared Key** : utilise une clé unique, basée sur votre mot de passe, pour l'authentification. Si vous sélectionnez cette option, saisissez la valeur souhaitée que les clients VPN distants doivent fournir pour établir les connexions VPN dans le champ **Password**. La clé prépartagée saisie doit être exactement identique ici et sur les clients distants.
  - **Certificate** : utilise un certificat numérique d'une autorité de certification (CA) tierce pour l'authentification. Si vous choisissez cette option, sélectionnez un certificat CA comme certificat local dans la liste déroulante **Local Certificate** et sélectionnez un certificat CA comme certificat distant dans la liste déroulante **Peer Certificate** pour l'authentification. Le certificat distant sélectionné sur le serveur VPN IPsec doit être configuré comme certificat local sur les clients VPN distants.

    REMARQUE : Vous devez avoir les certificats CA valides importés sur votre Cisco ISA500 avant de choisir cette option. Accédez à la page Device Management > Certificate Management pour importer les certificats CA. Voir **Gestion des certificats pour l'authentification, page 393**.

- **Mode** : le client matériel VPN Cisco prend en charge le mode « NEM » (Network Extension Mode) et le mode « Client ». La stratégie de groupe d'accès à distance IPsec doit être configurée avec le mode correspondant pour autoriser uniquement la connexion des clients matériels VPN Cisco au mode de fonctionnement identique. Par exemple, si vous choisissez le mode « Client » pour la stratégie de groupe, seuls les clients matériels VPN Cisco en mode « Client » peuvent être connectés à l'aide de cette stratégie de groupe. Pour obtenir plus d'informations sur le mode de fonctionnement, voir **Modes de fonctionnement, page 336**.

  - Sélectionnez **Client** pour la stratégie de groupe qui est utilisée à la fois pour le PC exécutant le logiciel Client VPN Cisco et le périphérique Cisco qui sert de client matériel VPN Cisco en mode « Client ». En mode « Client », le serveur VPN IPsec peut attribuer des adresses IP aux interfaces externes des clients VPN distants. Pour définir la plage du regroupement pour les clients VPN distants, entrez les adresses IP de début et de fin dans les champs **Start IP** et **End IP**.

  - Sélectionnez **NEM** pour la stratégie de groupe qui est utilisée uniquement pour le périphérique Cisco qui sert de client matériel VPN Cisco en mode « NEM ».

- **Client Internet Access** : cochez cette case pour créer automatiquement des règles NAT avancées afin de permettre aux clients VPN distants d'accéder à Internet via les tunnels VPN. Si vous désactivez cette case, vous pouvez créer manuellement des règles NAT avancées. Voir **Configuration de règles NAT avancées pour permettre aux clients VPN distants d'accéder à Internet via les tunnels VPN, page 331**.

- **WAN Failover** : cliquez sur **On** pour activer le basculement WAN ou sur **Off** pour le désactiver. Si vous activez le basculement WAN, le trafic est automatiquement redirigé vers la liaison secondaire lorsque la liaison principale est en panne.

  REMARQUE : Pour activer le basculement WAN pour l'accès à distance IPsec, vérifiez que le port WAN secondaire a été configuré et que la redondance WAN a été définie comme mode d'équilibrage de charge ou de basculement.

  REMARQUE : L'Cisco ISA500 met automatiquement à jour la passerelle WAN locale pour le tunnel VPN en fonction des configurations de la liaison WAN de secours. À cet effet, le DNS dynamique doit être configuré, car l'adresse IP est modifiée par le basculement et les clients VPN distants doivent utiliser le nom de domaine du serveur VPN IPsec pour établir les connexions VPN.

ÉTAPE 4 Dans l'onglet **Zone Access Control**, vous pouvez contrôler l'accès à partir du PC exécutant le logiciel Client VPN Cisco ou du réseau privé du client matériel VPN Cisco aux zones sur les tunnels VPN. Cliquez sur **Permit** pour permettre l'accès ou sur **Deny** pour le refuser.

REMARQUE : Les règles de pare-feu VPN qui sont automatiquement générées par les paramètres de contrôle d'accès aux zones seront ajoutées à la liste des règles de pare-feu avec une priorité supérieure aux règles de pare-feu par défaut, mais inférieure aux règles de pare-feu personnalisées.

ÉTAPE 5 Dans l'onglet **Mode Configuration Settings**, entrez les informations suivantes :

- **Primary DNS Server** : entrez l'adresse IP du serveur DNS principal.
- **Secondary DNS Server** : entrez l'adresse IP du serveur DNS secondaire.
- **Primary WINS Server** : entrez l'adresse IP du serveur WINS principal.
- **Secondary WINS Server** : entrez l'adresse IP du serveur WINS secondaire.
- **Default Domain** : entrez le nom de domaine par défaut qui doit être envoyé aux clients VPN distants.
- **Backup Server 1/2/3** : entrez l'adresse IP ou le nom d'hôte du serveur de secours. Vous pouvez spécifier jusqu'à trois serveurs VPN IPsec de secours. Lorsque la connexion au serveur principal échoue, les clients VPN peuvent tenter de se connecter aux serveurs de secours. Le serveur de secours 1 bénéficie de la priorité la plus élevée et le serveur de secours 3, de la priorité la plus faible.

  REMARQUE : Les serveurs de secours que vous avez spécifiés sur le serveur VPN IPsec sont envoyés aux clients VPN distants à l'établissement des connexions VPN. Les clients VPN distants les mettent en mémoire cache.

- **Split Tunnel** : cliquez sur **On** pour activer la fonctionnalité de transmission tunnel partagée ou sur **Off** pour la désactiver. La transmission tunnel partagée autorise uniquement le trafic spécifié par les routes du client VPN vers les ressources de l'entreprise via le tunnel VPN. Si vous activez la transmission tunnel partagée, vous devez définir les sous-réseaux partagés. Pour ajouter un sous-réseau, saisissez l'adresse IP et le masque de réseau dans les champs **Protected Network** et **Netmask**, puis cliquez sur **Add**. Pour supprimer un sous-réseau, sélectionnez-le dans la liste et cliquez sur **Delete**.

- **Split DNS** : le DNS fractionné dirige les paquets DNS en texte clair à travers le tunnel VPN vers des domaines desservis par le DNS d'entreprise. Pour ajouter un domaine, entrez le **nom de domaine** qui doit être résolu par le serveur DNS de votre réseau, puis cliquez sur **Add**. Pour supprimer un domaine, sélectionnez-le dans la liste et cliquez sur **Delete**.

  REMARQUE : Pour utiliser le DNS fractionné, vous devez également activer la fonctionnalité de transmission tunnel partagée et spécifier les domaines. La fonctionnalité de DNS fractionné prend en charge jusqu'à 10 domaines.

ÉTAPE 6 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 7 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration de règles NAT avancées pour permettre aux clients VPN distants d'accéder à Internet via les tunnels VPN

L'activation de l'accès du client à Internet crée automatiquement des règles NAT avancées afin de permettre aux clients VPN distants d'accéder à Internet via les tunnels VPN. Cette section fournit un exemple de configuration manuelle des règles NAT avancées afin de permettre aux clients VPN distants d'accéder à Internet via les tunnels VPN.

ÉTAPE 1 Partons du principe que vous activez la fonctionnalité d'accès à distance IPsec et que vous créez une stratégie de groupe comme suit :

Champ	Paramètre
Group Name	VPNGroup1
WAN Interface	WAN1
IKE Authentication Method	Pre-shared key
Mode	Client
Pool Range for Client LAN	Start IP : 192.168.3.2 End IP : 192.168.3.254

Champ	Paramètre
Client Internet Access	Disable
WAN Failover	On

REMARQUE : Un objet d'adresse compris entre 192.168.3.2 et 192.168.3.254 appelé « EZVPN_VPNGroup1 » est créé automatiquement.

ÉTAPE 2 Si une seule interface WAN unique est configurée, accédez à la page Firewall > NAT > Advanced NAT pour créer une règle NAT avancée comme suit.

Champ	Paramètre
Name	VPNClient_to_WAN1
Enable	On
From	Any
To	WAN1
Original Source Address	EZVPN_VPNGroup1
Original Destination Address	Any
Original Services	Any
Translated Source Address	WAN1_IP
Translated Destination Address	Any
Translated Services	Any

ÉTAPE 3 Si deux interfaces WAN sont configurées, accédez à la page Firewall > NAT > Advanced NAT pour créer deux règles NAT avancées comme suit.

Champ	Paramètre
Name	VPNClient_to_WAN1
Enable	On
From	Any
To	WAN1
Original Source Address	EZVPN_VPNGroup1
Original Destination Address	Any
Original Services	Any
Translated Source Address	WAN1_IP
Translated Destination Address	Any
Translated Services	Any

Champ	Paramètre
Name	VPNClient_to_WAN2
Enable	On
From	Any
To	WAN2
Original Source Address	EZVPN_VPNGroup1
Original Destination Address	Any
Original Services	Any
Translated Source Address	WAN2 IP

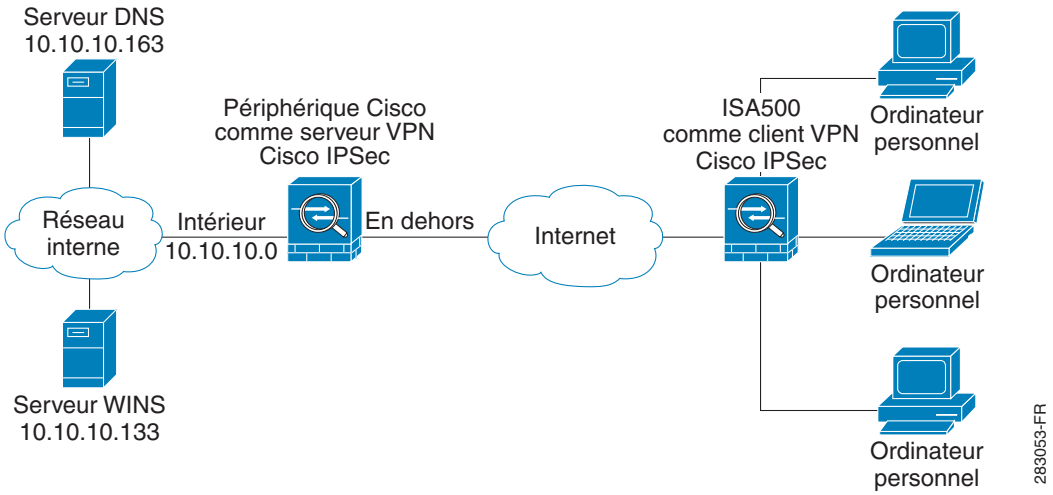
Champ	Paramètre
Translated Destination Address	Any
Translated Services	Any

Configuration du client VPN pour télétravailleurs

La fonctionnalité de client VPN pour télétravailleurs réduit les exigences de configuration sur les sites distants en permettant à l'Cisco ISA500 de fonctionner comme un client matériel VPN Cisco pour recevoir les politiques de sécurité sur le tunnel VPN à partir d'un serveur VPN IPsec distant.

Une fois le serveur VPN IPsec configuré, une connexion VPN peut être créée avec une configuration minimale sur le client VPN pour télétravailleurs. Lorsque le client VPN télétravailleurs lance la connexion VPN, le serveur VPN IPsec envoie les stratégies IPsec au client VPN pour télétravailleurs et crée le tunnel VPN correspondant. Cette solution est idéale pour les bureaux distants disposant de peu d'assistance informatique ou pour les grands déploiements CPE (Customer Premises Equipment, Équipement des locaux du client), pour lesquels il est impossible de configurer individuellement les périphériques distants.

Figure 6 Accès à distance IPsec avec un serveur VPN IPsec



REMARQUE Lorsque l'Cisco ISA500 sert de client matériel VPN Cisco, la stratégie IKE et l'ensemble de transformation ci-dessous sont utilisés par défaut. La stratégie IKE et l'ensemble de transformation utilisés sur l'Cisco ISA500 sont inconfigurables.

Champ	Paramètre
IKE Policy	Encryption = ESP_AES_256 Hash = SHA Authentication = Pre-shared Key D-H Group = Group 2
Transform Set	Integrity = SHA Encryption = ESP_AES_256

Cette section décrit comment configurer la fonctionnalité de client VPN pour télétravailleurs. Reportez-vous aux rubriques suivantes :

- **Serveur VPN IPsec requis, page 335**
- **Avantages de la fonctionnalité de client VPN pour télétravailleurs, page 336**
- **Modes de fonctionnement, page 336**
- **Paramètres généraux de client VPN pour télétravailleurs, page 339**
- **Configuration des stratégies de groupe de client VPN pour télétravailleurs, page 340**

Serveur VPN IPsec requis

La fonctionnalité de client VPN pour télétravailleurs nécessite que l'homologue de destination soit un périphérique ISA500 qui serve de serveur VPN IPsec ou un routeur Cisco IOS (tel que C871, C1801, C1812, C1841 et C2821), ou une plate-forme Cisco ASA5500 qui prenne en charge la fonctionnalité de serveur VPN IPsec.

La fonctionnalité de client VPN pour télétravailleur prend en charge la configuration d'un seul homologue de destination. Si votre application nécessite plusieurs tunnels VPN, vous devez configurer manuellement les paramètres du tunnel VPN et de traduction d'adresses de réseau/traduction d'adresses d'homologue (NAT/PAT) sur le client et le serveur.

Avantages de la fonctionnalité de client VPN pour télétravailleurs

- Permet une configuration dynamique de la stratégie d'utilisateur final, en exigeant moins de configuration manuelle par les utilisateurs et les techniciens sur site, ce qui réduit le nombre d'erreurs et d'appels de service ultérieurs.
- Permet au fournisseur de modifier les configurations des équipements et réseau suivant les besoins, en limitant (ou supprimant) le travail de reconfiguration de l'équipement de l'utilisateur final.
- Permet une gestion centralisée des politiques de sécurité.
- Permet des déploiements à grande échelle avec l'approvisionnement rapide d'utilisateurs.
- Évite aux utilisateurs finaux de devoir acheter et configurer des périphériques VPN externes.
- Évite aux utilisateurs finaux de devoir installer et configurer le logiciel Client VPN Cisco sur leur PC.
- Déleste la création et la maintenance des connexions VPN du PC vers le routeur.
- Réduit les problèmes d'interopérabilité entre les différents clients VPN logiciels basés sur PC, les solutions VPN matérielles externes et les autres applications VPN.
- Configure un tunnel IPsec unique, quel que soit le nombre de sous-réseaux multiples qui sont pris en charge et la taille de la liste de fractionnement ou d'inclusion (split-include).

Modes de fonctionnement

La fonctionnalité de client VPN pour télétravailleurs définit l'Cisco ISA500 en tant que client matériel VPN Cisco. Le client matériel VPN Cisco prend en charge deux modes de fonctionnement : le mode « Client » ou le mode « NEM » (Network Extension Mode, mode d'extension de réseau). Le mode de fonctionnement détermine si les hôtes internes relatives proches du client matériel VPN Cisco sont accessibles à partir du réseau de l'entreprise via le tunnel VPN. Il est obligatoire de spécifier le mode de fonctionnement avant d'établir une connexion, car le client matériel VPN Cisco ne dispose pas d'un mode par défaut.

Tous les modes de fonctionnement prennent également en charge la transmission tunnel partagée ; celle-ci qui permet un accès sécurisé aux ressources de l'entreprise via le tunnel VPN tout en permettant également un accès Internet via une connexion à un FAI ou à un autre service (éliminant ainsi le réseau d'entreprise du chemin d'accès au Web).

Reportez-vous aux rubriques suivantes :

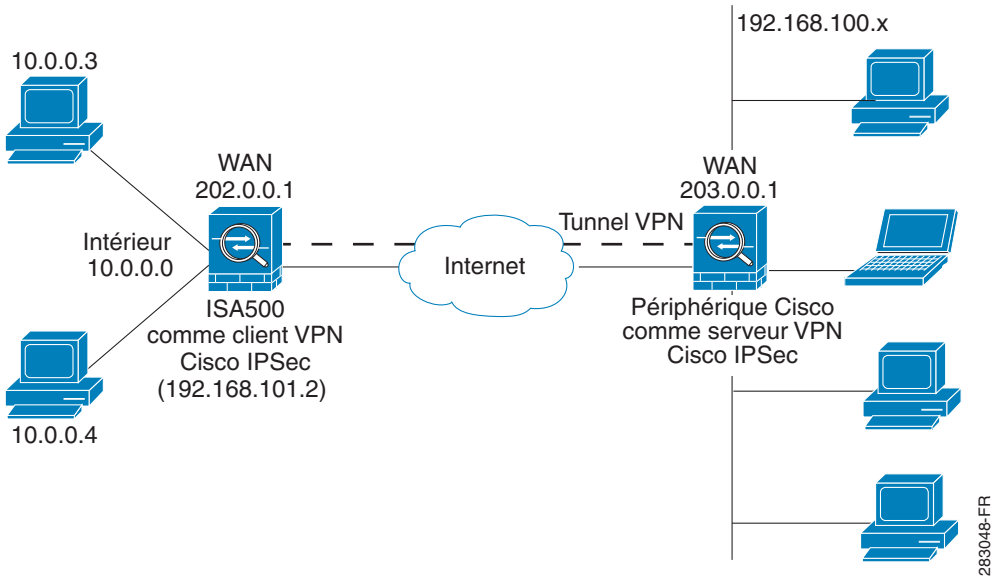
- **Mode Client, page 337**
- **Mode NEM, page 338**

Mode Client

Le mode client indique que la traduction d'adresse de réseau (NAT) ou de port (PAT) doit être effectuée pour que les PC et autres hôtes à l'extrémité distante du tunnel VPN forment un réseau privé qui n'utilise pas les adresses IP dans l'espace d'adressage IP du serveur de destination. En mode « Client », l'interface externe du client matériel VPN Cisco peut se voir attribuer une adresse IP par le serveur distant.

La **Figure 7** illustre le mode de fonctionnement du client. Dans cet exemple, l'Cisco ISA500 permet d'accéder à deux PC qui possèdent des adresses IP dans l'espace de réseau privé 10.0.0.0. Ces ordinateurs se connectent à l'interface Ethernet sur le Cisco ISA500, et le serveur attribue une adresse IP 192.168.101.2 à l'Cisco ISA500. Le Cisco ISA500 effectue la traduction NAT ou PAT sur le tunnel VPN afin que les PC puissent accéder au réseau de destination. Lorsque de l'accès au réseau distant 192.168.100.x, les hôtes 10.0.0.3 et 10.0.04 seront traduites vers 192.168.101.2, mais aux hôtes du réseau distant 192.168.100.x ne peut accéder aux hôtes 10.0.0.3 et 10.0.04.

Figure 7 Connexion au client VPN IPsec



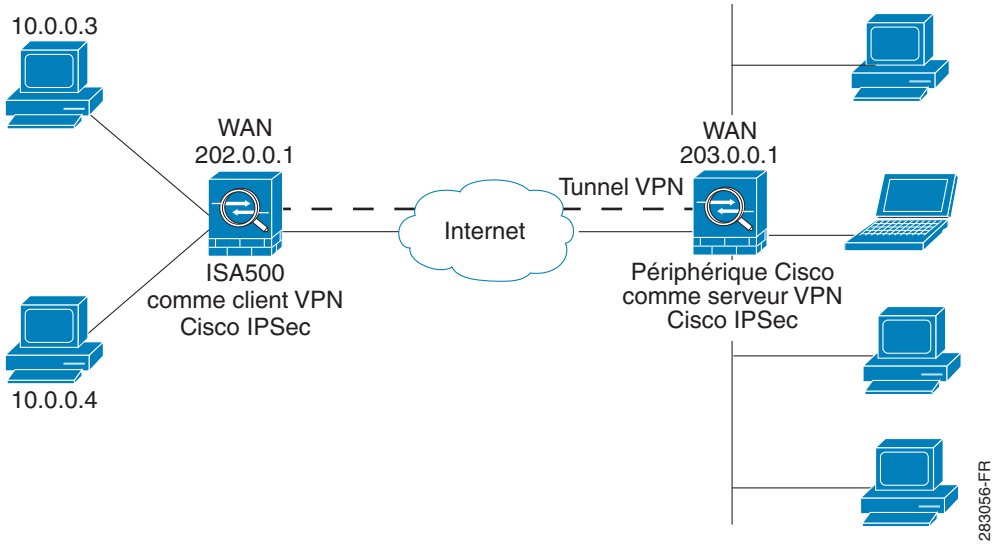
Mode NEM

Le mode d'extension de réseau (NEM) indique que les PC et autres hôtes à l'extrémité Client du tunnel VPN se voient attribuer des adresses IP entièrement routables et accessibles par le réseau de destination sur le réseau tunnellisé afin de former un réseau logique. La traduction PAT n'est pas utilisée, ce qui permet aux hôtes et aux PC clients d'avoir un accès direct aux PC et aux hôtes sur le réseau de destination. En mode « NEM », le client matériel VPN Cisco obtient une adresse IP privée d'un server DHCP local ou est configuré avec une adresse IP statique.

La **Figure 8** illustre le fonctionnement du mode d'extension de réseau. Dans cet exemple, le Cisco ISA500 sert de client matériel VPN Cisco, en se connectant à un serveur VPN IPsec distant. Les hôtes reliés au Cisco ISA500 ont des adresses IP dans l'espace de réseau privé 10.0.0.0. Le serveur n'attribue pas d'adresse IP au Cisco ISA500, et le Cisco ISA500 n'effectue pas de traduction NAT ou PAT sur le tunnel VPN. Lorsque de l'accès au réseau distant 192.168.100.x, les hôtes 10.0.0.3 et 10.0.04 ne sont pas traduits, et les hôtes du réseau distant 192.168.100.x peuvent accéder directement aux hôtes 10.0.0.3 et 10.0.04.

Les hôtes clients se voient attribuer des adresses IP qui sont entièrement routables par le réseau de destination sur le tunnel de VPN. Ces adresses IP peuvent se trouver sur le même espace de sous-réseau que le réseau de destination ou sur des sous-réseaux séparés, à condition que les routeurs de destination soient configurés pour acheminer correctement ces adresses IP sur le tunnel VPN.

Figure 8 Connexion d'extension de réseau VPN IPsec



Paramètres généraux de client VPN pour télétravailleurs

Cette section explique comment activer la fonctionnalité de client VPN pour télétravailleurs, configurer les paramètres de tentative de lancement automatique, connecter ou déconnecter manuellement les connexions VPN.

ÉTAPE 1 Cliquez sur **VPN > Teleworker VPN Client**.

ÉTAPE 2 Saisissez les informations suivantes :

- **Teleworker VPN Client** : cliquez sur **On** pour activer la fonctionnalité de client VPN pour télétravailleurs et, par conséquent, définir le Cisco ISA500 en tant que client matériel VPN Cisco, ou sur **Off** pour la désactiver.

  REMARQUE : L'activation de la fonctionnalité de client VPN pour télétravailleurs désactive les fonctionnalités de VPN de site à site et d'accès à distance IPsec, et met fin à leurs sessions VPN connectées.

- **Auto Initiation Retry** : cliquez sur **On** pour activer la fonctionnalité de tentative automatique de lancement ou sur **Off** pour la désactiver.

  Lorsque vous activez Auto Initiation Retry (tentative automatique de lancement), l'Cisco ISA500 (défini en tant que client matériel VPN Cisco) lance tout d'abord la connexion VPN au serveur principal. S'il n'y a pas de réponse du serveur principal après le délai défini dans le champ **Retry Interval**, le Cisco ISA500 relance alors la connexion VPN au serveur

principal. Cela continue le nombre de fois que vous avez défini dans le champ **Retry Limit** (ou jusqu'à ce que le serveur principal soit connecté). Si le serveur principal ne peut pas être connecté après le nombre de fois spécifié, le Cisco ISA500 tente à nouveau d'établir la connexion VPN aux serveurs de secours en suivant le délai et le nombre de tentatives spécifiés. Si les trois serveurs de secours ne peuvent pas être connectés, répétez le processus de tentative de lancement plusieurs fois jusqu'à ce qu'un serveur VPN IPsec puisse être connecté.

Lorsque vous désactivez Auto Initiation Retry (tentative automatique de lancement), le Cisco ISA500 lance en premier lieu la connexion VPN au serveur principal. S'il n'y a pas de réponse du serveur principal en 120 secondes, le Cisco ISA500 relance alors la connexion VPN aux serveurs de secours. Si les trois serveurs de secours ne peuvent pas être connectés, répétez le processus de tentative de lancement plusieurs fois jusqu'à ce qu'un serveur VPN IPsec puisse être connecté.

- **Retry Interval** : indiquez la fréquence, en secondes, selon laquelle le Cisco ISA500 relance la connexion VPN au serveur principal et aux serveurs de secours. La valeur par défaut est de 120 secondes.
- **Retry Limit** : entrez le nombre de fois que le Cisco ISA500 doit tenter d'établir une connexion VPN. La valeur par défaut est 2.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

ÉTAPE 4 Pour exécuter manuellement la connexion VPN, cliquez sur l'icône de **connexion** dans la colonne **Configure**. Par défaut, la stratégie de groupe que le paramètre « Activate Connection on Startup » a activé lancera automatiquement la connexion VPN au démarrage du Cisco ISA500. Vous ne pouvez activer qu'une seule connexion VPN à la fois.

ÉTAPE 5 Pour mettre fin manuellement à la connexion VPN, cliquez sur l'icône de **déconnexion**.

Configuration des stratégies de groupe de client VPN pour télétravailleurs

Pour pouvoir terminer la configuration d'une stratégie de groupe de client VPN pour télétravailleurs, vous devez avoir les informations suivantes à portée de main.

- Adresse IP ou nom d'hôte du serveur VPN IPsec.
- Nom de la stratégie de groupe du serveur VPN IPsec.
- Clé prépartagée ou certificats numériques pour l'authentification IKE.

REMARQUE Jusqu'à 16 stratégies de groupe de client VPN pour télétravailleurs peuvent être configurées sur le Cisco ISA500. Vous pouvez créer plusieurs stratégies de groupe pour vous connecter à différents serveurs VPN, mais vous ne pouvez activer qu'une seule connexion VPN à la fois.

ÉTAPE 1 Cliquez sur **VPN > Teleworker VPN Client**.

ÉTAPE 2 Pour ajouter une stratégie de groupe, cliquez sur **Add**.

Other Options : pour modifier une entrée, cliquez sur l'icône de **modification** (crayon). Pour supprimer une entrée, cliquez sur l'icône de **suppression** (x). Pour supprimer plusieurs entrées, cochez-les et cliquez sur **Delete**.

La fenêtre Teleworker VPN Client - Add/Edit s'ouvre.

ÉTAPE 3 Dans l'onglet **Basic Settings**, entrez les informations suivantes :

- **Description** : entrez le nom de la stratégie de groupe.
- **Server (Remote Address)** : entrez l'adresse IP ou le nom de domaine du serveur VPN IPsec.
- **Activate Connection on Startup** : cliquez sur **On** pour lancer automatiquement la connexion VPN au démarrage du Cisco ISA500 ou sur **Off** pour désactiver cette option. Vous ne pouvez activer qu'une seule connexion VPN à la fois au démarrage.
- **IKE Authentication Method** : le client VPN doit être correctement authentifié avant de pouvoir accéder au réseau distant. Choisissez l'une des méthodes d'authentification suivantes :
  - **Pre-shared Key** : sélectionnez cette option si le serveur VPN IPsec utilise une clé unique basée sur un mot de passe pour l'authentification, puis saisissez les informations suivantes :

    Group Name : entrez le nom de la stratégie de groupe d'accès à distance IPsec qui est définie sur le serveur VPN IPsec. Le Cisco ISA500 utilise cette stratégie de groupe pour établir la connexion VPN avec le serveur VPN IPsec. Le serveur VPN IPsec envoie les paramètres de sécurité via le tunnel VPN au Cisco ISA500.

    Password : entrez la clé pré-partagée indiquée dans la stratégie de groupe sélectionné pour établir une connexion VPN. La clé prépartagée saisie doit être exactement identique ici et sur le serveur VPN IPsec.

- **Certificate** : sélectionnez cette option si le serveur VPN IPsec utilise le certificat numérique d'une autorité de certification (CA) tierce pour l'authentification. Sélectionnez un certificat CA en tant que certificat local dans la liste déroulante **Local Certificate** et sélectionnez le certificat CA utilisé sur le serveur VPN IPsec distant en tant que certificat distant dans la liste déroulante **Peer Certificat**, pour l'authentification.

  REMARQUE : Vous devez avoir les certificats CA valides importés sur votre Cisco ISA500 avant de choisir cette option. Accédez à la page Device Management > Certificate Management pour importer les certificats CA. Voir **Gestion des certificats pour l'authentification, page 393**.

- **Mode** : le mode de fonctionnement détermine si les hôtes internes relatives proches du client matériel VPN Cisco sont accessibles à partir du réseau de l'entreprise via le tunnel VPN. Il est obligatoire de spécifier un mode de fonctionnement avant d'établir une connexion VPN, car le client matériel VPN Cisco ne dispose pas d'un mode par défaut. Pour obtenir plus d'informations sur le mode de fonctionnement, voir **Modes de fonctionnement, page 336**.

  - Sélectionnez le mode **Client** si vous souhaitez que les PC ou les autres dispositifs se trouvant au niveau du réseau interne du routeur forment un réseau privé et disposent d'adresses IP réservées. Les fonctionnalités de traduction d'adresses de réseau (NAT) et de traduction d'adresses de port (PAT) seront utilisées. Les périphériques se trouvant à l'extérieur du LAN ne pourront pas envoyer une requête ping aux périphériques du LAN, ni les atteindre directement.

  - Sélectionnez le mode **NEM** (Extension du réseau) si vous souhaitez que les périphériques connectés aux interfaces internes disposent d'adresses IP routables et accessibles à partir du réseau de destination. Les périphériques se trouvant à chaque extrémité de la liaison formeront un réseau logique. La fonctionnalité PAT sera automatiquement désactivée afin de permettre aux PC et aux hôtes se trouvant à chaque extrémité de la liaison d'avoir un accès mutuel direct.

- **VLAN** : si vous choisissez le mode NEM, spécifiez le VLAN qui autorise l'accès à partir de et au réseau privé du serveur VPN IPsec.

- **User Name** : saisissez le nom d'utilisateur utilisé par le client VPN pour télétravailleurs afin d'établir une connexion VPN.

- **User Password** : entrez le mot de passe utilisé par le client VPN pour télétravailleurs afin d'établir une connexion VPN.

ÉTAPE 4 Dans l'onglet **Zone Access Control**, vous pouvez contrôler l'accès des zones de votre réseau au réseau distant si le client VPN pour télétravailleurs fonctionne en mode « Client ». Cliquez sur **Permit** pour permettre l'accès ou sur **Deny** pour le refuser.

REMARQUE : Les règles de pare-feu VPN qui sont automatiquement générées par les paramètres de contrôle d'accès aux zones seront ajoutées à la liste des règles de pare-feu avec une priorité supérieure aux règles de pare-feu par défaut, mais inférieure aux règles de pare-feu personnalisées.

ÉTAPE 5 Dans l'onglet **Advanced Settings**, entrez les informations suivantes.

- **Backup Server 1/2/3** : entrez l'adresse IP ou le nom d'hôte du serveur de secours. Vous pouvez spécifier jusqu'à trois serveurs de secours. Lorsque la connexion au serveur VPN IPsec principal échoue, le Cisco ISA500, lance la connexion VPN aux serveurs de secours. Le serveur de secours 1 bénéficie de la priorité la plus élevée et le serveur de secours 3, de la priorité la plus faible.

  REMARQUE : Le client VPN pour télétravailleurs peut obtenir les serveurs de secours depuis le serveur VPN IPsec lors de la négociation de tunnel. La priorité des serveurs de secours spécifiés sur le serveur VPN IPsec est plus élevée que celle des serveurs de secours spécifiés sur le client VPN pour télétravailleurs. Lorsque la connexion principale échoue, tentez en premier lieu de vous connecter aux serveurs de secours spécifié sur le serveur VPN IPsec, puis tentez de vous connecter aux serveurs de secours spécifiés sur le client VPN pour télétravailleurs.

- **Peer Timeout** : saisissez la valeur du délai de détection, en secondes. S'il n'y a aucune réponse et aucun trafic du serveur principal ou du serveur de secours au cours de ce délai, déclarez l'homologue mort. La valeur par défaut est de 120 secondes.

ÉTAPE 6 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 7 Le message d'avertissement suivant s'affiche : « Do you want to make this connection active when the settings are saved? (Only one connection can be active at a time.) » [(Souhaitez-vous activer cette connexion une fois les paramètres enregistrés ? (Vous ne pouvez activer qu'une seule connexion VPN à la fois)]

- Si vous souhaitez activer la connexion immédiatement après l'enregistrement des paramètres, cliquez sur le bouton **Activate Connection**. Lorsque vous créez plusieurs stratégies de groupe de client VPN pour télétravailleurs à la fois, vous ne pouvez activer qu'une seule connexion après l'enregistrement de vos paramètres. Le Cisco ISA500 utilise la dernière stratégie de groupe qui a été créée ou modifiée pour établir la connexion VPN.

- Si vous souhaitez uniquement créer la stratégie de groupe de client VPN pour télétravailleurs et ne souhaitez pas activer la connexion immédiatement après l'enregistrement des paramètres, cliquez sur le bouton **Do Not Activate**. Vous pouvez cliquer sur l'icône de **connexion** pour établir manuellement la connexion VPN.

  REMARQUE : Cette fonctionnalité est différente de la fonctionnalité de connexion active au démarrage. Elle permet d'activer la connexion dès que les paramètres sont enregistrés, alors que la fonctionnalité de connexion active au démarrage permet d'activer la connexion lorsque le Cisco ISA500 démarre.

ÉTAPE 8 Cliquez sur **Save** pour appliquer vos paramètres.

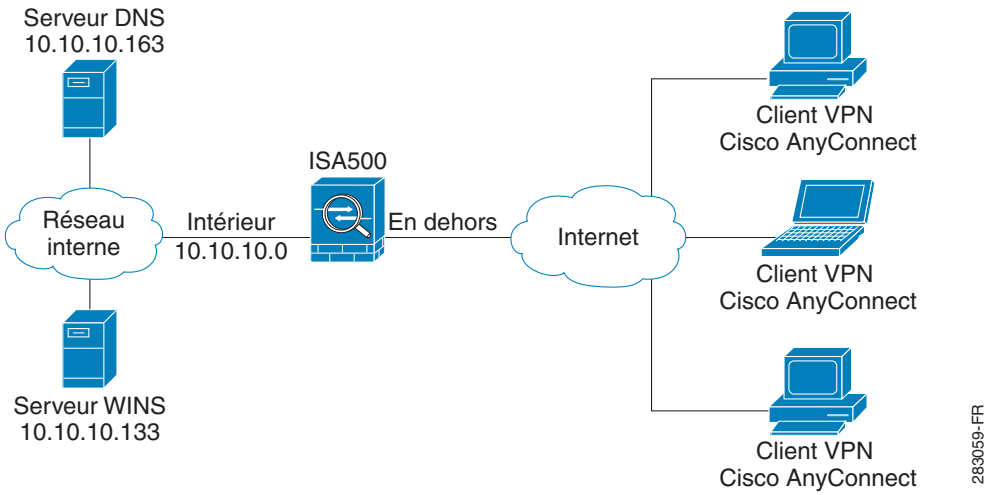
Configuration VPN SSL

SSL VPN est un moyen souple et sécurisé d'étendre les ressources réseau à pratiquement n'importe quel utilisateur distant. L'Cisco ISA500 prend en charge la fonctionnalité VPN SSL et fonctionne avec le logiciel client à mobilité sécurisé Cisco AnyConnect.

Une licence de sécurité valide est également requise pour la prise en charge de SSLVPN avec les périphériques mobiles, tels que les smartphones et les tablettes. Pour obtenir plus d'informations, voir **Activation des services de sécurité, page 259**.

La **Figure 9** montre un exemple de VPN SSL. Les utilisateurs peuvent accéder à distance au réseau à l'aide du logiciel client sécurisé de mobilité Cisco AnyConnect. Une fois que le tunnel VPN SSL est établi, chaque utilisateur dispose d'une adresse IP sur le réseau interne.

Figure 9 Accès utilisateur distant SSL



Cette section décrit comment configurer la fonctionnalité SSL VPN. Reportez-vous aux rubriques suivantes :

- **Éléments du VPN SSL, page 346**
- **Tâches de configuration pour l'établissement d'un tunnel VPN SSL, page 346**
- **Installation du client à mobilité sécurisé Cisco AnyConnect, page 347**
- **Certificats d'importation pour l'authentification des utilisateurs, page 348**
- **Configuration des utilisateurs VPN SSL, page 348**
- **Configuration de la passerelle VPN SSL, page 349**
- **Configuration des stratégies de groupe VPN SSL, page 351**
- **Accès au portail VPN SSL, page 354**
- **Configuration des règles NAT avancées pour autoriser les clients VPN SSL à accéder à Internet via les tunnels VPN SSL, page 355**

REMARQUE Nous vous recommandons de ne pas connecter un PC ou un téléphone directement à un port WAN de l'Cisco ISA500 pour établir une connexion VPN SSL entre eux.

Éléments du VPN SSL

Plusieurs éléments fonctionnent ensemble pour prendre en charge le VPN SSL.

- **SSL VPN Users** : créez vos utilisateurs VPN SSL et activez le service VPN SSL pour les groupes d'utilisateurs auxquels les utilisateurs VPN SSL appartiennent. La sélection d'une stratégie de groupe VPN SSL permet d'activer le service VPN SSL pour un groupe d'utilisateurs. Tous les membres du groupe d'utilisateurs sur les sites distants peuvent établir les tunnels VPN SSL en fonction de la stratégie de groupe VPN SSL sélectionnée. Voir **Configuration des utilisateurs VPN SSL, page 348**.
- **SSL VPN Group Policies** : créez vos stratégies de groupe VPN SSL. La stratégie de groupe VPN SSL sert à établir le tunnel VPN SSL permettant d'accéder aux ressources réseau. Voir **Configuration des stratégies de groupe VPN SSL, page 351**.
- **Cisco AnyConnect Secure Mobility Client** : le client à mobilité sécurisé Cisco AnyConnect est le client VPN de nouvelle génération. Il fournit aux utilisateurs distants des connexions VPN sécurisées à la passerelle VPN SSL. Voir **Installation du client à mobilité sécurisé Cisco AnyConnect, page 347**.

Tâches de configuration pour l'établissement d'un tunnel VPN SSL

Vous devez effectuer les tâches de configuration suivantes pour établir le tunnel VPN SSL.

- Téléchargez et installez le logiciel client à mobilité sécurisé Cisco AnyConnect sur le PC de l'utilisateur distant. Voir **Installation du client à mobilité sécurisé Cisco AnyConnect, page 347**.
- (Facultatif) Importez les certificats sur votre Cisco ISA500 utilisé pour l'authentification des utilisateurs. Voir **Certificats d'importation pour l'authentification des utilisateurs, page 348**.
- Activez la fonctionnalité VPN SSL et configurez les paramètres de passerelle VPN SSL. Voir **Configuration de la passerelle VPN SSL, page 349**.
- Définissez les stratégies de groupe VPN SSL. Voir **Configuration des stratégies de groupe VPN SSL, page 351**.
- Créez vos utilisateurs et groupes d'utilisateurs VPN SSL, et spécifiez la stratégie de groupe VPN SSL de chaque groupe d'utilisateurs VPN SSL. Voir **Configuration des utilisateurs VPN SSL, page 348**.

- Lancez le logiciel client à mobilité sécurisé Cisco AnyConnect sur le PC de l'utilisateur, entrez la paire d'adresses « Adresse IP de passerelle : Numéro de port de passerelle » pour vous connecter à la passerelle VPN SSL distante, puis saisissez les identifiants d'authentification pour établir une connexion VPN SSL.
- Affichez les informations pour toutes les sessions VPN SSL actives. Voir **Affichage de l'état du VPN SSL, page 307**.

Installation du client à mobilité sécurisé Cisco AnyConnect

Vous pouvez configurer un PC pour qu'il exécute le logiciel client à mobilité sécurisé Cisco AnyConnect en installant le logiciel client correspondant au système d'exploitation adéquat directement sur le PC de l'utilisateur. L'utilisateur lance le logiciel client à mobilité sécurisé Cisco AnyConnect et fournit les identifiants d'authentification pour établir la connexion VPN.

L'Cisco ISA500 prend en charge la version 3.0 du client à mobilité sécurisé Cisco AnyConnect (utilisation pour SSL uniquement). Le client à mobilité sécurisé Cisco AnyConnect est compatible avec les plates-formes suivantes :

- Windows 7 (32 bits et 64 bits)
- Windows Vista (32 bits et 64 bits)
- Windows XP SP2+ (32 bits et 64 bits)
- Linux Intel (noyau 2.6.x)
- Mac OS X 10,5, 10.6.x et 10,7

Vous pouvez trouver les programmes d'installation du logiciel sur le CD qui est livré avec l'Cisco ISA500. Le CD inclut les packages AnyConnect pour Windows, Mac OS X et Linux. Sélectionnez le package AnyConnect correspondant à votre système d'exploitation sur le CD afin de procéder à son téléchargement.

Vous pouvez également télécharger le logiciel Client à mobilité sécurisé Cisco AnyConnect en vous rendant sur ce site :
http://www.cisco.com/cisco/software/type.html?mdfid=283000185&catid=null

Vous devez vous connecter et posséder un contrat de service cisco valide afin d'avoir accès au logiciel client à mobilité sécurisé Cisco AnyConnect. Un contrat de service d'assistance Cisco Small Business de 3 ans (CON-SBS-SVC2) est requis pour télécharger le logiciel client sur le site Cisco.com. Si vous n'en disposez pas, contactez votre partenaire, votre revendeur ou l'assistance CISCO pour en savoir plus.

Pour plus d'informations sur la façon de télécharger, installer et configurer le logiciel client à mobilité sécurisé Cisco AnyConnect, allez sur ce site : http://www.cisco.com/en/US/products/ps10884/tsd_products_support_series_home.html

REMARQUE Le client à mobilité sécurisé Cisco AnyConnect conserve l'état de reconnexion après que le câble de l'interface WAN sur le serveur ait été débranché, puis rebranché. Dans ce cas, vous devez tout d'abord mettre fin à la reconnexion du client, puis vous connecter manuellement au serveur VPN SSL.

Certificats d'importation pour l'authentification des utilisateurs

La passerelle VPN SSL détient un certificat CA qui est présenté aux clients VPN SSL lorsque ceux-ci se connectent pour la première fois à la passerelle. L'objectif de ce certificat est de permettre d'authentifier le serveur. Vous pouvez utiliser le certificat par défaut ou un certificat importé pour l'authentification. Pour plus d'informations sur l'importation des certificats, voir **Gestion des certificats pour l'authentification, page 393**.

Configuration des utilisateurs VPN SSL

ISA550 et ISA550W prennent en charge 25 utilisateurs VPN SSL. ISA570 et ISA570W prennent en charge 50 utilisateurs VPN SSL. Pour configurer les utilisateurs et les groupes d'utilisateurs pour l'accès VPN SSL, accédez à la page Users > Users and Groups.

Vous pouvez affecter tous les utilisateurs VPN SSL à un seul groupe d'utilisateurs. Toutefois, si vous avez plusieurs stratégies de groupe VPN SSL, vous pouvez créer plusieurs groupes d'utilisateurs et spécifier des stratégies de groupe VPN SSL différentes pour chacun d'entre eux. La définition d'une stratégie de groupe VPN SSL pour un groupe d'utilisateurs permet d'activer le service VPN SSL pour tous les membres du groupe d'utilisateurs. Pour plus d'informations, voir **Configuration d'utilisateurs et de groupes d'utilisateurs, page 361**.

Selon les paramètres d'authentification des utilisateurs spécifiés sur l'Cisco ISA500, les utilisateurs VPN SSL peuvent être authentifiés par la base de données locale ou par un serveur AAA externe (Active Directory, LDAP ou RADIUS, par exemple). Pour obtenir des informations sur la configuration des paramètres d'authentification des utilisateurs, voir **Configuration des paramètres d'authentification des utilisateurs, page 365**.

Configuration de la passerelle VPN SSL

Utilisez la page SSL VPN Configuration pour activer la fonctionnalité VPN SSL et pour configurer les paramètres de passerelle VPN SSL.

ÉTAPE 1 Cliquez sur **VPN > SSL Remote User Access > SSL VPN Configuration**.

La fenêtre SSL VPN Configuration s'ouvre.

ÉTAPE 2 Cliquez sur **On** pour activer la fonctionnalité VPN SSL et, par conséquent, définir l'Cisco ISA500 comme serveur VPN SSL, ou sur **Off** pour la désactiver.

ÉTAPE 3 Dans la zone **Mandatory Gateway**, entrez les informations suivantes :

- **Gateway Interface** : sélectionnez le port WAN par lequel passe le trafic sur les tunnels SSL VPN.
- **Gateway Port** : saisissez le numéro de port utilisé pour la passerelle VPN SSL. Par défaut, SSL fonctionne sur le port 443. Cependant, la passerelle VPN SSL doit être flexible pour fonctionner sur un port défini par l'utilisateur. Le pare-feu doit permettre au port d'assurer la livraison des paquets destinés à la passerelle VPN SSL. Les clients VPN SSL doivent saisir la paire d'adresses complète « Adresse IP de passerelle : Numéro de port de passerelle » pour permettre la connexion.
- **Certificate File** : sélectionnez le certificat par défaut ou un certificat importé pour authentifier les utilisateurs qui tentent d'accéder à votre ressource réseau via les tunnels VPN SSL. Pour plus d'informations sur l'importation des certificats, voir **Gestion des certificats pour l'authentification, page 393**.
- **Client Address Pool** : la passerelle VPN SSL dispose d'un groupement d'adresses configurable qui permet d'attribuer des adresses IP aux clients VPN distants. Saisissez le groupement d'adresses IP pour tous les clients distants. Le client se voit attribuer une adresse IP via la passerelle VPN SSL.

  REMARQUE : Configurez une plage d'adresses IP qui ne se superpose avec aucune adresse de votre réseau local.
- **Client Netmask** : entrez l'adresse IP du masque réseau utilisé pour les clients VPN SSL. Le masque réseau du client peut uniquement être IP 255.255.255.0, 255.255.255.128 et 255.255.255.192.

Le groupement d'adresses du client est utilisé avec le masque réseau du client. Le tableau suivant montre les paramètres valides pour la saisie du groupement d'adresses du client et du masque réseau du client.

Client Netmask	Client Address Pool
255.255.255.0	x.x.x.0
255.255.255.128	x.x.x.0 ou x.x.x.128
255.255.255.192	x.x.x.0, x.x.x.64, x.x.x.128 ou x.x.x.192

S'ils sont définis comme suit, le client VPN SSL obtiendra une adresse VPN comprise entre 10.10.10.1 et 10.10.10.254.

- Groupement d'adresses du client = 10.10.10.0
- Masque réseau du client = 255.255.255.0

- **Client Internet Access** : cochez cette case pour créer automatiquement des règles NAT avancées afin d'autoriser les clients VPN SSL à accéder à Internet. Si vous désactivez cette case, vous pouvez créer manuellement des règles NAT avancées. Voir **Configuration des règles NAT avancées pour autoriser les clients VPN SSL à accéder à Internet via les tunnels VPN SSL, page 355**.
- **Client Domain** : entrez le nom de domaine qui doit être envoyé aux clients VPN SSL.
- **Login Banner** : une fois les utilisateurs connectés, une bannière configurable s'affiche. Saisissez le texte du message à afficher avec la bannière.

ÉTAPE 4 Dans la zone **Optional Gateway**, entrez les informations suivantes :

- **Idle Timeout** : entrez le délai en secondes pendant lequel la session VPN SSL peut rester inactive. La valeur par défaut est de 2 100 secondes.
- **Session Timeout** : entrez le délai en secondes pendant lequel une session VPN SSL peut rester active. La valeur par défaut est de 0 seconde, ce qui indique que la session VPN SSL peut toujours être active.
- **Client DPD Timeout** : la détection DPD (Dead Peer Detection) permet la détection des homologues morts. Saisissez le délai de DPD pendant lequel une session sera maintenue avec un client distant inactif. La valeur par défaut est de 300 secondes.

- **Gateway DPD Timeout** : saisissez le délai de détection DPD pendant lequel une session sera maintenue avec une passerelle VPN SSL inactive. La valeur par défaut est de 300 secondes.

  REMARQUE : Si la passerelle VPN SSL n'a pas de réponse deux ou trois fois au cours du délai de détection DPD, la session VPN SSL prend fin.

- **Keep Alive** : saisissez l'intervalle en secondes, auquel le client VPN SSL va envoyer des messages keepalive. Ces messages garantissent que la connexion VPN SSL reste ouverte, même si le délai d'inactivité maximal du client est limité par un périphérique intermédiaire, par exemple un proxy, un pare-feu ou un périphérique NAT.
- **Lease Duration** : entrez la durée après laquelle le client VPN SSL doit envoyer une requête de renouvellement de validité de l'adresse IP sur le serveur. La valeur par défaut est de 43 200 secondes.
- **Max MTU** : entrez l'unité de transfert maximum pour la session. La valeur par défaut est de 1 406 octets.
- **Rekey Method** : spécifiez la méthode de renouvellement des clés de session (SSL ou nouveau tunnel). Le renouvellement de clés permet la renégociation des clés SSL après l'établissement de la session.
- **Rekey Interval** : entrez la fréquence de renouvellement des clés dans ce champ. La valeur par défaut est de 3 600 secondes.

ÉTAPE 5 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration des stratégies de groupe VPN SSL

Tous les membres du groupe d'utilisateurs VPN SSL peuvent établir les tunnels VPN SSL en fonction de la stratégie de groupe de VPN SSL spécifiée pour accéder aux ressources réseau.

REMARQUE Jusqu'à 32 stratégies de groupe VPN SSL peuvent être configurées sur l'Cisco ISA500.

ÉTAPE 1 Cliquez sur **VPN > SSL Remote User Access > SSL VPN Group Policies**.

La fenêtre SSL VPN Group Policies s'ouvre. Les stratégies de groupe VPN SSL par défaut et personnalisées sont répertoriées dans le tableau.

ÉTAPE 2 Pour ajouter une nouvelle stratégie de groupe VPN, cliquez sur **Add**.

Autres options : pour modifier une entrée, cliquez sur l'icône de **modification** (crayon). Pour supprimer une entrée, cliquez sur l'icône de **suppression** (x). Pour supprimer plusieurs entrées, cochez-les et cliquez sur **Delete**. La stratégie de groupe VPN SSL par défaut (SSLVPNDefaultPolicy) ne peut pas être supprimée.

La fenêtre SSL VPN Group Policy - Add/Edit s'ouvre.

ÉTAPE 3 Dans l'onglet **Basic Settings**, entrez les informations suivantes :

- **Policy Name** : entrez le nom de la stratégie de groupe VPN SSL.
- **Primary DNS** : entrez l'adresse IP du serveur DNS principal.
- **Secondary DNS** : saisissez l'adresse IP du serveur DNS secondaire.
- **Primary WINS** : entrez l'adresse IP du serveur WINS principal.
- **Secondary WINS** : saisissez l'adresse IP du serveur WINS secondaire.

ÉTAPE 4 Dans l'onglet **IE Proxy Settings**, entrez les informations suivantes :

La passerelle VPN SSL peut spécifier plusieurs proxys de Microsoft Internet Explorer (MSIE) pour les PC clients. Si ces paramètres sont activés, IE est automatiquement configuré sur le PC client avec ces paramètres.

- **IE Proxy Policy** : sélectionnez l'une des stratégies de proxy d'IE suivantes :
  - **None** : permet au navigateur de n'utiliser aucun paramètre de proxy.
  - **Auto** : permet au navigateur de détecter automatiquement les paramètres de proxy.
  - **Bypass-Local** : permet au navigateur de contourner les paramètres de proxy qui sont configurés sur l'utilisateur distant.
  - **Disable** : désactive les paramètres de proxy de MSIE.
- **Address** : si vous choisissez « Bypass-Local » ou « Auto », entrez l'adresse IP ou le nom de domaine du serveur proxy de MSIE.
- **Port** : saisissez le numéro de port du serveur proxy de MSIE.
- **IE Proxy Exception** : vous pouvez spécifier les hôtes d'exception pour les paramètres de proxy d'Internet Explorer. Cette option permet au navigateur de ne pas envoyer de trafic via le proxy pour le nom d'hôte ou adresse IP indiqués. Pour ajouter une entrée, saisissez l'adresse IP ou le nom de domaine d'un hôte et cliquez sur **Add**. Pour supprimer une entrée, sélectionnez-la et cliquez sur **Delete**.

ÉTAPE 5 Dans la zone **Split Tunneling Settings**, entrez les informations suivantes :

La transmission tunnel partagée permet qu'un trafic spécifique soit acheminé en dehors du tunnel VPN SSL. Le trafic est soit inclus (résolu dans le tunnel) ou exclu (résolu par le biais de la connexion WAN ou FAI). Les options de la configuration de la résolution du tunnel s'excluent mutuellement. Une adresse IP ne peut pas être à la fois inclue et exclue.

- **Enable Split Tunneling** : par défaut, tout le trafic en provenance de l'hôte est acheminé via le tunnel VPN. Cochez cette case pour activer la fonctionnalité de transmission tunnel partagée afin que le tunnel VPN soit utilisé uniquement pour le trafic spécifié par les routes du client.
- **Split Selection** : sélectionnez l'une des options suivantes :
  - **Include Traffic** : vous permet d'ajouter les routes du client sur le client VPN SSL de telle sorte que seul le trafic vers les réseaux de destination puisse être redirigé via le tunnel VPN. Pour ajouter une route de client, saisissez le sous-réseau de destination auquel une route est ajoutée sur le client VPN SSL dans le champ **Address** et le masque de sous-réseau du réseau de destination dans le champ **Netmask,** puis cliquez sur **Add**.
  - **Exclude Traffic** : vous permet d'exclure les réseaux de destination sur le client VPN SSL. Le trafic vers les réseaux de destination est redirigé à l'aide de l'interface réseau native du client VPN SSL (résolu par le biais de la connexion WAN ou FAI). Pour ajouter une route de client, saisissez le sous-réseau de destination auquel une route est ajoutée sur le client VPN SSL dans le champ **Address** et le masque de sous-réseau du réseau de destination dans le champ **Netmask,** puis cliquez sur **Add**.

    REMARQUE : Pour exclure les réseaux de destination, vérifiez que la fonctionnalité d'exclusion de LAN local est activée sur les clients à mobilité sécurisé Cisco AnyConnect.
  - **Exclude Local LAN** : si vous choisissez « Exclude Traffic », cochez cette case pour permettre aux utilisateurs distants d'accéder à leurs réseaux LAN sans passer par le tunnel VPN ou décochez-la pour empêcher les utilisateurs distants d'accéder à leurs réseaux LAN sans passer par le tunnel VPN.

    REMARQUE : Pour exclure des réseaux LAN, vérifiez que la fonctionnalité d'exclusion de LAN local est activée sur le serveur VPN SSL et les clients AnyConnect.

- **Split DNS** : le DNS fractionné permet de diriger les paquets DNS en texte clair via Internet vers des domaines desservis par un DNS externe (servant votre FAI) ou via le tunnel VPN vers des domaines desservis par le DNS d'entreprise.

  Par exemple, la requête d'un paquet destiné à corporate.com serait acheminée par le tunnel VPN sur le DNS qui dessert le réseau privé, alors que la requête d'un paquet destiné à myfavoritesearch.com serait gérée par le DNS du FAI. Pour utiliser le DNS fractionné, vous devez également avoir configuré la transmission tunnel partagée.

  Pour ajouter un domaine pour la transmission tunnel de paquets à des destinations sur le réseau privé, saisissez l'adresse IP ou le nom de domaine dans le champ et cliquez sur **Add**. Pour supprimer un domaine, sélectionnez-le et cliquez sur **Delete**.

ÉTAPE 6 Dans la zone **Zone-based Firewall Settings**, vous pouvez contrôler l'accès des clients VPN SSL aux zones sur les tunnels VPN. Cliquez sur **Permit** pour permettre l'accès ou sur **Deny** pour le refuser.

REMARQUE : Les règles de pare-feu VPN qui sont automatiquement générées par les paramètres de contrôle d'accès aux zones seront ajoutées à la liste des règles de pare-feu avec une priorité supérieure aux règles de pare-feu par défaut, mais inférieure aux règles de pare-feu personnalisées.

ÉTAPE 7 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 8 Cliquez sur **Save** pour appliquer vos paramètres.

Accès au portail VPN SSL

Le portail VPN SSL présente un message afin de rappeler aux utilisateurs d'installer le logiciel client à mobilité sécurisé Cisco AnyConnect pour se connecter au serveur VPN SSL. Vous pouvez trouver les programmes d'installation sur le CD qui est joint à la livraison du périphérique ou les télécharger sur le site Web Cisco.com. Voir **Installation du client à mobilité sécurisé Cisco AnyConnect, page 347**.

Vous pouvez accéder au portail VPN SSL via un navigateur Web côté WAN à l'aide du protocole HTTPS. Vous devez tout d'abord activer la fonctionnalité VPN SSL sur l'Cisco ISA500, puis saisir la paire d'adresses complète « Adresse IP de passerelle : Numéro de port de passerelle » dans la barre d'adresse pour accéder au portail VPN SSL.

Configuration des règles NAT avancées pour autoriser les clients VPN SSL à accéder à Internet via les tunnels VPN SSL

L'activation de l'accès du client à Internet crée automatiquement des règles NAT avancées afin de permettre aux clients VPN SSL d'accéder à Internet via les tunnels VPN SSL. Cette section fournit un exemple de configuration manuelle des règles NAT avancées afin de permettre aux clients VPN SSL d'accéder à Internet via les tunnels VPN SSL.

ÉTAPE 1 Partons du principe que vous activez la fonctionnalité VPN SSL et que vous configurez les paramètres de passerelle comme suit.

Champ	Paramètre
Gateway Interface	WAN1
Gateway Port	443
Certificate File	Par défaut
Client Address Pool	192.168.200.0
Client Netmask	255.255.255.0

ÉTAPE 2 Si une seule interface WAN unique est configurée, accédez à la page Firewall > NAT > Advanced NAT pour créer une règle NAT avancée comme suit.

Champ	Paramètre
Name	SSLVPN_to_WAN1
Enable	On
From	Any
To	WAN1
Original Source Address	SSLVPN_ADDRESS_POOL
Original Destination Address	Any
Original Services	Any

Champ	Paramètre
Translated Source Address	WAN1_IP
Translated Destination Address	Any
Translated Services	Any

ÉTAPE 3 Si deux interfaces WAN sont configurées et si la redondance WAN est définie sur le mode « Load Balancing », accédez à la page Firewall > NAT > Advanced NAT pour créer deux règles NAT avancées comme suit.

Champ	Paramètre
Name	SSLVPN_to_WAN1
Enable	On
From	Any
To	WAN1
Original Source Address	SSLVPN_ADDRESS_POOL
Original Destination Address	Any
Original Services	Any
Translated Source Address	WAN1_IP
Translated Destination Address	Any
Translated Services	Any

Champ	Paramètre
Name	SSLVPN_to_WAN2
Enable	On
From	Any

Champ	Paramètre
To	WAN2
Original Source Address	SSLVPN_ADDRESS_POOL
Original Destination Address	Any
Original Services	Any
Translated Source Address	WAN2 IP
Translated Destination Address	Any
Translated Services	Any

Configuration d'un serveur L2TP

Le protocole L2TP (Layer 2 Tunneling Protocol) est un protocole de tunnellisation VPN qui permet aux utilisateurs distants d'utiliser le réseau IP public en toute sécurité pour communiquer avec des serveurs de réseau d'entreprise privés. L2TP utilise le protocole PPP sur UDP (port 1701) pour la transmission tunnel des données.

Le protocole L2TP est basé sur le modèle client-serveur. L'Cisco ISA500 peut mettre fin aux connexions L2TP-sur-IPsec des clients Microsoft Windows entrants.

ÉTAPE 1 Cliquez sur **VPN > L2TP Server**.

ÉTAPE 2 Cliquez sur **On** pour activer le serveur L2TP ou sur **Off** pour le désactiver.

ÉTAPE 3 Si vous activez le serveur L2TP, entrez les informations suivantes :

- **Listen WAN Interface** : choisissez l'interface WAN sur laquelle le serveur L2TP écoute pour accepter la connexion VPN L2TP entrante.
- **User Name** : entrez le nom d'utilisateur que tous les clients L2TP utilisent pour accéder au serveur L2TP.

- **Password** : entrez le mot de passe que tous les clients L2TP utilisent pour accéder au serveur L2TP.

  REMARQUE : Tous les clients L2TP utilisent les mêmes nom d'utilisateur et mot de passe pour se connecter au serveur L2TP.

- **MTU** : saisissez la taille de MTU, en octets, pouvant être envoyée sur le réseau. La plage correcte est comprise entre 128 et 1 400 octets. La valeur par défaut est 1400 octets.
- **Authentication Method** : choisissez le protocole CHAP Challenge Handshake Authentication Protocol) ou PAP (Password Authentication Protocol), ou les deux, pour authentifier les clients L2TP. Cliquez sur **On** pour activer le protocole CHAP ou PAP ou sur **Off** pour le désactiver.
- **Address Pool** : le serveur L2TP attribue des adresses IP à tous les clients L2TP. Entrez l'adresse IP de début dans le champ **Start IP Address** et l'adresse IP de fin dans le champ **End IP Address**.
- **DNS1 IP Address** : entrez l'adresse IP du serveur DNS principal.
- **DNS2 IP Address** : éventuellement, entrez l'adresse IP du serveur DNS secondaire.
- **IPsec** : cliquez sur **On** pour activer le cryptage des données sur le tunnel VPN IPsec ou sur **Off** pour le désactiver.
- **Pre-shared Key** : le cryptage des données sur le tunnel VPN utilise une clé pré-partagée pour l'authentification. Si vous activez **IPsec**, saisissez la valeur souhaitée que le client L2TP doit fournir pour établir une connexion. La clé prépartagée saisie doit être exactement identique ici et sur les clients L2TP.

ÉTAPE 4 Cliquez sur **Save** pour appliquer vos paramètres.

ÉTAPE 5 Par défaut, le pare-feu refuse l'accès depuis la zone VPN aux zones LAN et voix. Si vous souhaitez autoriser les clients L2TP à accéder à votre VLAN par défaut, vous devez accéder la page Firewall > Access Control > ACL Rules pour créer manuellement une règle de pare-feu comme suit :

Champ	Paramètre
From Zone	VPN
To Zone	LAN
Service	Any

Champ	Paramètre
Source Address	l2tp_clients **REMARQUE** : Sélectionnez **Create a new address** dans la liste déroulante pour créer un objet d'adresse « l2tp_clients » avec la plage d'adresses IP du groupement d'adresses du serveur L2TP.
Destination Address	DEFAULT_NETWORK
Schedule	Always on
Match Action	Permit

Configuration du transfert VPN

Reportez-vous à la page VPN Passthrough pour configurer le transfert VPN afin d'autoriser le trafic VPN qui provient de clients VPN à traverser votre Cisco ISA500. Utilisez cette fonctionnalité s'il existe des périphériques derrière votre Cisco ISA500 qui ont besoin des tunnels IPsec pour être configurés indépendamment, comme la connexion à un autre routeur sur le réseau WAN.

ÉTAPE 1 Cliquez sur **VPN > VPN Passthrough**.

La fenêtre VPN Passthrough s'ouvre.

ÉTAPE 2 Spécifiez le type de trafic qui peut traverser l'appareil de sécurité :

- **Layer-2 Tunneling Protocol (L2TP)** : cliquez sur **On** pour permettre aux tunnels L2TP de traverser l'Cisco ISA500 ou sur **Off** pour désactiver cette option.
- **Point-to-Point Tunneling Protocol (PPTP)** : cliquez sur **On** pour permettre aux tunnels PPTP de traverser l'Cisco ISA500 ou sur **Off** pour désactiver cette option.
- **Internet Protocol Security (IPsec)** : cliquez sur **On** pour permettre aux tunnels de sécurité IP de traverser l'Cisco ISA500 ou sur **Off** pour désactiver cette option.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

9

Gestion des utilisateurs

Ce chapitre décrit comment gérer les utilisateurs et groupes d'utilisateurs, et configurer des paramètres d'authentification des utilisateurs. Il comprend les sections suivantes :

- **Affichage des sessions utilisateur actives, page 360**
- **Configuration d'utilisateurs et de groupes d'utilisateurs, page 361**
- **Configuration des paramètres d'authentification des utilisateurs, page 365**
- **Configuration de serveurs RADIUS, page 374**

Pour accéder aux pages relatives aux utilisateurs, cliquez sur **Users** dans le volet de navigation de gauche.

Affichage des sessions utilisateur actives

Reportez-vous à la page Active User Sessions pour consulter les informations relatives à toutes les sessions utilisateur actives qui sont actuellement connectées à l'Cisco ISA500. Cette page est automatiquement mise à jour toutes les 10 secondes. Cliquez sur **Refresh** pour actualiser manuellement les données. Cliquez sur l'icône de **déconnexion** pour mettre fin à une session utilisateur Web ou à une session utilisateur VPN.

Users > Active User Sessions

Champ	Description
User Name	Nom de l'utilisateur connecté.
IP Address	Adresse IP d'hôte à partir de laquelle l'utilisateur a accédé à l'Cisco ISA500.

Champ	Description
Login Method	Méthode utilisée par l'utilisateur pour se connecter à l'Cisco ISA500, telle que le Web, VPN SSL, l'accès à distance IPsec ou le portail captif.
Session Time	Heure à laquelle l'utilisateur s'est connecté à l'Cisco ISA500.

Configuration d'utilisateurs et de groupes d'utilisateurs

Cette section décrit comment maintenir les utilisateurs et les groupes d'utilisateurs dans la base de données locale. Reportez-vous aux rubriques suivantes :

- **Groupe d'utilisateurs et utilisateur par défaut, page 361**
- **Services disponibles pour les groupes d'utilisateurs, page 362**
- **Préemption des administrateurs, page 362**
- **Configuration des utilisateurs locaux, page 363**
- **Configuration des groupes d'utilisateurs locaux, page 364**

Groupe d'utilisateurs et utilisateur par défaut

L'Cisco ISA500 conserver les informations sur l'utilisateur et le groupe d'utilisateurs dans la base de données locale. La base de données locale prend en charge jusqu'à 100 utilisateurs et 50 groupes d'utilisateurs. Un groupe d'utilisateurs peut comporter jusqu'à 100 utilisateurs. Tout utilisateur doit être membre d'un groupe d'utilisateurs.

Le compte d'administrateur par défaut (« cisco ») dispose de privilèges complets pour définir la configuration et lire l'état du système. Le compte d'administrateur par défaut ne peut pas être supprimé. Pour des raisons de sécurité, vous devez changer le mot de passe administrateur par défaut à la première connexion. Voir **Modification du mot de passe administrateur par défaut, page 33**.

Le groupe d'utilisateurs par défaut (« admin ») a la capacité d'accès administratif de connexion Web et active les services VPN SSL, d'accès à distance IPsec et de portail captif (pour ISA550W et ISA570W uniquement). Le groupe d'utilisateurs par défaut ne peut pas être supprimé, mais sa stratégie de service peut être modifiée.

Services disponibles pour les groupes d'utilisateurs

Un utilisateur ne peut appartenir qu'à un seul groupe d'utilisateurs. Les utilisateurs faisant partie d'un même groupe d'utilisateurs partagent la même stratégie de service. Un groupe d'utilisateurs n'a qu'une seule stratégie de service. Les services disponibles pour un groupe d'utilisateurs sont les suivants :

- **Web Login** : ce service permet aux membres du groupe d'utilisateurs de se connecter à l'utilitaire de configuration par le biais du navigateur web pour afficher la configuration ou pour la définir.
- **SSL VPN** : ce service permet aux membres du groupe d'utilisateurs qui se trouvent sur des sites distants d'établir les tunnels VPN SSL en fonction de la stratégie de groupe VPN SSL sélectionnée pour accéder aux ressources du réseau. Le logiciel client à mobilité sécurisé Cisco AnyConnect doit être installé sur le PC de l'utilisateur.
- **IPsec Remote Access** : ce service permet aux membres du groupe d'utilisateurs qui se trouvent sur des sites distants d'établir les tunnels VPN pour accéder en toute sécurité à vos ressources réseau.
- **Captive Portal** : ce service permet aux utilisateurs qui se sont authentifiés d'être dirigés vers une page Web spécifiée (portail) avant de pouvoir accéder à Internet. Ce service s'applique uniquement à ISA550W et à ISA570W.

REMARQUE L'Cisco ISA500 peut effectuer les authentifications en parallèle lorsque plusieurs services doivent authentifier en même temps.

Préemption des administrateurs

Lorsqu'un administrateur tente de se connecter tandis qu'un autre administrateur est déjà connecté, le message d'avertissement suivant s'affiche : « Another administrative user is logged into the application. Do you want to take control of the session? (The other user will be logged out.) » [Un autre utilisateur administratif est connecté à l'application. Voulez-vous prendre le contrôle de la session ? (L'autre utilisateur sera déconnecté)]. Cliquez sur **Yes** pour être prioritaire par rapport à l'administrateur actuel ou cliquez sur **No** pour revenir à l'écran de connexion.

Configuration des utilisateurs locaux

Utilisez la page Users and Groups pour afficher, ajouter, modifier ou supprimer des utilisateurs locaux. La base de données locale prend en charge jusqu'à 100 utilisateurs.

ÉTAPE 1 Cliquez sur **Users > Users and Groups**.

La fenêtre Users and Groups s'ouvre. Tous les utilisateurs locaux existants sont répertoriés dans la table des utilisateurs locaux (Local Users).

ÉTAPE 2 Dans la zone **Local Users**, cliquez sur **Add** pour ajouter un utilisateur.

Autres options : pour modifier une entrée, cliquez sur l'icône de **modification** (crayon). Pour supprimer une entrée, cliquez sur l'icône de **suppression** (x). Pour supprimer plusieurs entrées, cochez-les et cliquez sur **Delete**.

La fenêtre Local User - Add/Edit s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **User** : saisissez le nom d'utilisateur correspondant à l'utilisateur.
- **New Password** : entrez le mot de passe de l'utilisateur. Les mots de passe sont sensibles à la casse.

  REMARQUE : Un mot de passe doit comporter au minimum 8 caractères et au moins trois des classes de caractères suivantes : lettres majuscules et minuscules, chiffres et caractères spéciaux. Ne répétez aucun mot de passe plus de trois fois sur une ligne. Ne définissez pas le nom d'utilisateur ou « cisco » comme mot de passe. Ne mettez pas ces mots en majuscule et ne les écrivez pas à l'envers.
- **New Password Confirm** : saisissez à nouveau le mot de passe pour le confirmer.
- **Group** : sélectionnez le groupe d'utilisateurs auquel l'utilisateur appartient.

  REMARQUE : Pour un utilisateur VPN SSL, assurez-vous que le groupe d'utilisateurs sélectionné active le service VPN SSL. Pour un utilisateur VPN IPsec, assurez-vous que le groupe d'utilisateurs sélectionné active le service d'accès à distance IPsec.

ÉTAPE 4 Cliquez sur **OK** pour enregistrer vos paramètres.

Configuration des groupes d'utilisateurs locaux

Un groupe d'utilisateurs est utilisé pour créer un regroupement logique d'utilisateurs qui partagent la même stratégie de service. Utilisez la page Users and Groups pour afficher, ajouter, modifier ou supprimer des groupes d'utilisateurs locaux. La base de données locale prend en charge jusqu'à 50 groupes d'utilisateurs.

ÉTAPE 1 Cliquez sur **Users > Users and Groups**.

La fenêtre Users and Groups s'ouvre. Tous les groupes d'utilisateurs existants sont répertoriés dans la table des groupes (Groups).

ÉTAPE 2 Dans la zone **Groups**, cliquez sur **Add** pour ajouter un groupe d'utilisateurs.

Autres options : pour modifier une entrée, cliquez sur l'icône de **modification** (crayon). Pour supprimer une entrée, cliquez sur l'icône de **suppression** (x). Pour supprimer plusieurs entrées, cochez-les et cliquez sur **Delete**.

La fenêtre Group - Add/Edit s'ouvre.

ÉTAPE 3 Dans l'onglet **Group Settings**, entrez les informations suivantes :

- **Name** : entrez le nom du groupe d'utilisateurs.
- **Services** : spécifiez la stratégie de service du groupe d'utilisateurs. Vous pouvez activer plusieurs services pour un groupe d'utilisateurs.
  - **Web Login** : choisissez l'une des stratégies suivantes de connexion Web pour le groupe d'utilisateurs.

    Disable : aucun membre du groupe d'utilisateurs ne peut se connecter à l'utilitaire de configuration par le biais du navigateur Web.

    Read Only : tous les membres du groupe d'utilisateurs peuvent uniquement lire l'état du système après s'être connectés. Ils ne peuvent modifier aucune configuration.

    Administrator : tous les membres du groupe d'utilisateurs disposent de privilèges complets pour définir la configuration et lire l'état du système.

    REMARQUE : Vous ne pouvez pas désactiver le service de connexion Web, ni modifier son niveau de service pour le groupe d'utilisateurs par défaut (« admin »).

- **SSL VPN** : sélectionnez une stratégie de groupe VPN SSL pour activer le service VPN SSL pour le groupe d'utilisateurs, ou sélectionnez **Disable** pour le désactiver. Si vous activez VPN SSL, tous les membres du groupe d'utilisateurs peuvent établir les tunnels VPN SSL en fonction de la stratégie de groupe VPN SSL sélectionnée pour accéder en toute sécurité à vos ressources réseau. Pour plus d'informations sur la stratégie de groupe VPN SSL, reportez-vous à la section **Configuration des stratégies de groupe VPN SSL, page 351**.
- **IPsec Remote Access** : cliquez sur **Enable** pour activer le service d'accès à distance IPsec pour le groupe d'utilisateurs ou sur **Disable** pour le désactiver. Si vous activez l'accès à distance IPsec, tous les membres du groupe d'utilisateurs peuvent établir les tunnels VPN pour accéder en toute sécurité à vos ressources réseau.
- **Captive Portal** : cliquez sur **Enable** pour activer le service de portail captif pour le groupe d'utilisateurs ou sur **Disable** pour le désactiver. Si vous activez le portail captif, les membres sans fil du groupe d'utilisateurs qui se sont authentifiés seront redirigés vers une page Web spécifiée (portail) avant de pouvoir accéder à Internet. Ce service s'applique uniquement à ISA550W et à ISA570W.

ÉTAPE 4 Dans l'onglet **Membership**, spécifiez les membres du groupe d'utilisateurs.

- Pour ajouter un membre, sélectionnez un utilisateur existant dans la liste **User** et cliquez sur la flèche droite. Les membres du groupe d'utilisateurs apparaissent dans la liste **Membership**.
- Pour supprimer un membre du groupe d'utilisateurs, sélectionnez-le dans la liste **Membership** et cliquez sur la flèche gauche.

ÉTAPE 5 Cliquez sur **OK** pour enregistrer vos paramètres.

Configuration des paramètres d'authentification des utilisateurs

L'authentification des utilisateurs est un moyen d'identifier l'utilisateur et de vérifier qu'il est autorisé à accéder à certains services limités. Par exemple, un utilisateur peut être identifié en tant qu'utilisateur de VPN SSL afin qu'il accède à vos ressources réseau via des tunnels VPN SSL.

L'Cisco ISA500 authentifie tous les utilisateurs lorsqu'ils tentent d'accéder à vos ressources réseau dans différentes zones. Les utilisateurs des VLAN effectuent uniquement des tâches locales et n'ont pas besoin d'être authentifiés par l'Cisco ISA500.

L'Cisco ISA500 prend en charge une base de données locale qui est stockée sur l'Cisco ISA500 et divers types de serveur AAA, tels que RADIUS, le protocole LDAP (LDAP) et Active Directory (AD). Vous pouvez utiliser la base de données locale, un serveur AAA, ou les deux, pour l'authentification des utilisateurs. La base de données locale prend en charge jusqu'à 100 utilisateurs. Vous devez donc utiliser le serveur AAA pour l'authentification si le nombre d'utilisateurs accédant au réseau est supérieur à 100.

REMARQUE La stratégie de service des groupes d'utilisateurs peut uniquement être configurée localement. Tous les groupes d'utilisateurs sur un serveur AAA doivent être dupliqués localement.

Reportez-vous aux rubriques suivantes :

- **Utilisation d'une base de données locale pour l'authentification des utilisateurs, page 366**
- **Utilisation d'un serveur RADIUS pour l'authentification utilisateur, page 367**
- **Utilisation de la base de données locale et du serveur RADIUS pour l'authentification des utilisateurs, page 370**
- **Utilisation du protocole LDAP pour l'authentification des utilisateurs, page 371**
- **Utilisation de la base de données locale et du protocole LDAP pour l'authentification, page 374**

Utilisation d'une base de données locale pour l'authentification des utilisateurs

Utilisez la base de données locale pour authentifier les utilisateurs lorsque le nombre d'utilisateurs accédant au réseau est inférieur à 100.

La base de données locale vérifie les informations d'identification de l'utilisateur. Seuls les utilisateurs locaux valides sont autorisés à accéder au réseau. Pour obtenir des informations sur la configuration des utilisateurs locaux dans la base de données locale, reportez-vous à la section **Configuration des utilisateurs locaux, page 363**.

ÉTAPE 1 Cliquez sur **Users > User Authentication**.

ÉTAPE 2 Choisissez **Local Database** comme méthode d'authentification.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Utilisation d'un serveur RADIUS pour l'authentification utilisateur

L'Cisco ISA500 peut utiliser des serveurs RADIUS pour l'authentification des utilisateurs afin d'accéder au réseau. Le serveur RADIUS utilise l'attribut Framed-Filter-ID pour stocker les informations sur l'utilisateur et le groupe d'utilisateurs, et vérifie les informations d'identification de l'utilisateur à l'aide du système d'authentification PAP (Password Authentication Protocol, protocole d'authentification de mot de passe).

Lorsqu'un utilisateur s'authentifie, l'Cisco ISA500 vérifie les informations d'identification de l'utilisateur via le serveur RADIUS. Le serveur RADIUS renvoie les résultats de l'authentification à l'Cisco ISA500. En cas d'utilisateur RADIUS valide, l'Cisco ISA500 contrôle sa stratégie de service de groupe d'utilisateurs à partir de la base de données locale et autorise l'accès. En cas d'utilisateur RADIUS non valide, l'Cisco ISA500 bloque l'accès.

ÉTAPE 1 Cliquez sur **Users > User Authentication**.

ÉTAPE 2 Choisissez **RADIUS** comme méthode d'authentification.

ÉTAPE 3 Cliquez sur **Configure** pour configurer les paramètres RADIUS.

ÉTAPE 4 Dans l'onglet **Settings**, sélectionnez le groupe RADIUS pour l'authentification et configurez la valeur d'expiration globale, puis testez à nouveau les paramètres.

- **Global RADIUS Settings** : spécifiez la valeur d'expiration globale et testez à nouveau les paramètres pour les serveurs RADIUS sélectionnés :
  - **RADIUS Server Timeout** : entrez le nombre de secondes pendant lesquelles la connexion peut exister avant qu'une nouvelle authentification ne soit requise. La plage est comprise entre 1 et 60 secondes. La valeur par défaut est de 3 secondes.
  - **Retries** : entrez le nombre de fois que l'Cisco ISA500 tentera de contacter le serveur RADIUS. La plage de valeurs se situe entre 0 et 10 tentatives. La valeur par défaut est 2.

L'Cisco ISA500 envoie tout d'abord un message de requête au serveur RADIUS principal. S'il n'y a pas de réponse du serveur RADIUS principal, l'Cisco ISA500 attend le nombre de secondes que vous avez défini dans le champ **RADIUS Server Timeout**, puis envoie un autre message de requête. Cela continue le nombre de fois que vous avez défini dans le champ **Retries** (ou jusqu'à ce qu'il y ait une réponse valide). S'il n'y a pas de réponse valide du serveur RADIUS principal après le nombre de tentatives spécifié, l'Cisco ISA500 utilise le serveur RADIUS secondaire pour la prochaine tentative d'authentification. Si le serveur secondaire ne répond pas non plus après le nombre de tentatives spécifié, la connexion est interrompue.

- **RADIUS Servers** : sélectionnez l'index de groupe RADIUS dans la liste déroulante. Les paramètres du serveur RADIUS du groupe sélectionné s'affichent. Vous pouvez modifier ces paramètres ici, mais les paramètres que vous spécifiez remplaceront ceux par défaut du groupe sélectionné. Pour conserver les paramètres de serveur RADIUS, accédez à la page Users > RADIUS Servers**.** Voir **Configuration de serveurs RADIUS, page 374**.

ÉTAPE 5 Dans l'onglet **RADIUS Users**, entrez les informations suivantes :

- **Allow Only Users Listed Locally** : cliquez sur **On** pour n'autoriser que les utilisateurs RADIUS qui sont également présents dans la base de données locale à se connecter ou sur **Off** pour désactiver cette option.
- **Mechanism for Setting User Group Memberships for RADIUS Users** : sélectionnez l'un des mécanismes suivants pour configurer les appartenances à des groupes d'utilisateurs pour les utilisateurs RADIUS :
  - **Use RADIUS Filter-ID** : recherchez les informations sur le groupe d'utilisateurs à l'aide de l'attribut Framed-Filter-ID depuis le serveur RADIUS.

    Par exemple, le serveur RADIUS comporte trois groupes d'utilisateurs (Group1, Group2 et Group3) et la base de données locale comprend deux groupes d'utilisateurs (Group1 et Group2). Le tableau suivant montre les paramètres d'appartenance des groupes d'utilisateurs.

Paramètres de la base de données locale	**Paramètres du serveur Radius**		
	User1 dans Group1	User1 dans Group2	User1 dans Group3

User1 dans Group1	Group1	Group2	Groupe par défaut
User1 dans Group2	Group1	Group2	Groupe par défaut
User1 n'existe pas.	Group1	Group2	Groupe par défaut

Dans le tableau ci-dessus, si l'utilisateur User1 dans le serveur RADIUS appartient au Group1 mais que l'utilisateur User1 de la base de données locale appartient au Group2, alors l'utilisateur User1 appartiendra au Group1 une fois qu'il aura passé l'authentification RADIUS. Si l'utilisateur User1 dans le serveur RADIUS appartient au Group3, mais que la base de données locale n'a pas de Group3, alors l'utilisateur User1 sera défini sur le groupe par défaut spécifié.

- **Local Configuration Only** : recherchez les informations sur le groupe d'utilisateurs à partir de la base de données locale uniquement.

  Par exemple, le serveur RADIUS comporte trois groupes d'utilisateurs (Group1, Group2 et Group3) et la base de données locale comprend deux groupes d'utilisateurs (Group1 et Group2). Le tableau suivant montre les paramètres d'appartenance des groupes d'utilisateurs.

Paramètres de la base de données locale	**Paramètres du serveur Radius**		
	User1 dans Group1	User1 dans Group2	User1 dans Group3
User1 dans Group1	Group1	Group1	Group1
User1 dans Group2	Group2	Group2	Group2
User1 n'existe pas.	Groupe par défaut	Groupe par défaut	Groupe par défaut

Dans le tableau ci-dessus, si l'utilisateur User1 dans le serveur RADIUS appartient au Group1, mais que l'utilisateur User1 dans la base de données locale appartient au Group2, alors l'utilisateur User1 appartiendra au Group2 une fois que l'utilisateur aura passé l'authentification RADIUS. Si l'utilisateur User1 n'existe pas dans la base de données locale, il sera défini sur le groupe par défaut spécifié.

- **Default User Group to Which All RADIUS Users Belong** : choisissez un groupe d'utilisateurs local comme groupe par défaut auquel les utilisateurs RADIUS appartiennent. Si le groupe n'existe pas dans la base de données locale lors de l'obtention des informations sur le groupe d'utilisateurs à partir du serveur RADIUS, l'utilisateur RADIUS sera défini automatiquement sur le groupe d'utilisateurs local spécifié.

ÉTAPE 6 Dans l'onglet **Test**, entrez les informations d'identification dans les champs **User** et **Password**, puis cliquez sur le bouton **Test** pour vérifier si l'utilisateur RADIUS est valide.

ÉTAPE 7 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 8 Cliquez sur **Save** pour appliquer vos paramètres.

Utilisation de la base de données locale et du serveur RADIUS pour l'authentification des utilisateurs

Vous pouvez utiliser à la fois la base de données locale et le serveur RADIUS pour authentifier les utilisateurs qui tentent d'accéder au réseau.

Lorsqu'un utilisateur s'authentifie, l'Cisco ISA500 vérifie en premier lieu les informations d'identification de l'utilisateur via le serveur RADIUS. Le serveur RADIUS renvoie les résultats de l'authentification à l'Cisco ISA500. En cas d'utilisateur RADIUS valide, l'Cisco ISA500 contrôle sa stratégie de service de groupe d'utilisateurs à partir de la base de données locale et autorise l'accès. Pour un utilisateur RADIUS non valide, l'Cisco ISA500 utilise ensuite la base de données locale pour le vérifier à nouveau. Pour un utilisateur local valide, l'Cisco ISA500 contrôle sa stratégie de service de groupe d'utilisateurs à partir de la base de données locale et autorise l'accès. Pour un utilisateur local non valide, l'Cisco ISA500 bloque l'accès.

ÉTAPE 1 Cliquez sur **Users > User Authentication**.

ÉTAPE 2 Sélectionnez **RADIUS + Local Database** comme méthode d'authentification.

ÉTAPE 3 Cliquez sur **Configure** pour configurer les paramètres RADIUS pour l'authentification des utilisateurs. Pour plus d'informations, reportez-vous à la section **Utilisation d'un serveur RADIUS pour l'authentification utilisateur, page 367**.

ÉTAPE 4 Cliquez sur **Save** pour appliquer vos paramètres.

Utilisation du protocole LDAP pour l'authentification des utilisateurs

L'Cisco ISA500 peut utiliser l'annuaire LDAP pour l'authentification des utilisateurs, avec prise en charge de trois schémas incluant Microsoft Active Directory, InterOrgPerson RFC2798 et le service NIS (Network Information Service) RFC2307.

ÉTAPE 1 Cliquez sur **Users > User Authentication**.

ÉTAPE 2 Choisissez **LDAP** comme méthode d'authentification.

ÉTAPE 3 Cliquez sur **Configure** pour configurer les paramètres LDAP.

ÉTAPE 4 Dans l'onglet **Settings**, entrez les informations suivantes :

- **IP Address** : saisissez l'adresse IP du serveur LDAP.
- **Port Number** : saisissez le numéro de port d'écoute IP utilisé sur le serveur LDAP. En général, les connexions non sécurisées utilisent 389 et les connexions sécurisées utilisent 636. La valeur par défaut est 389.
- **Server Timeout** : entrez la durée, en secondes, pendant laquelle l'Cisco ISA500 attendra une réponse du serveur LDAP avant l'expiration du délai. La valeur par défaut est de 5 secondes.

  L'Cisco ISA500 tentera à nouveau de se connecter au serveur LDAP s'il n'y a pas de réponse de ce dernier après l'expiration du délai. Par exemple, si le délai de serveur est défini sur 5 secondes et qu'il n'y a pas de réponse du serveur LDAP après 5 secondes, l'Cisco ISA500 tentera à nouveau de se connecter au serveur LDAP 5 secondes plus tard.
- **Login Method** : choisissez l'une des méthodes de connexion suivantes :
  - **Anonymous Login** : sélectionnez cette option si le serveur LDAP permet d'accéder à l'arborescence d'utilisateur de manière anonyme.
  - **Give Login Name or Location in Tree** : sélectionnez cette option si le nom distinctif qui est utilisé pour la liaison au serveur LDAP est constitué à partir des champs **Primary Domain** et de **User Tree for Login to Server** dans l'onglet **Directory**.
  - **Give Bind Distinguished Name** : sélectionnez cette option si le nom de destination est connu. Vous devez fournir le nom de destination à utiliser explicitement pour la liaison au serveur LDAP.

- **Login User Name** : si vous choisissez **Give Login Name or Location in Tree** ou **Give Bind Distinguished Name** comme méthode de connexion, entrez le nom distinctif de l'utilisateur du compte qui est autorisé à se connecter au serveur LDAP.
- **Login Password** : si vous choisissez **Give Login Name or Location in Tree** ou **Give Bind Distinguished Name** comme méthode de connexion, entrez le mot de passe du compte pouvant se connecter au serveur LDAP.
- **Protocol Version** : sélectionnez la version du protocole LDAP dans la liste déroulante. L'Cisco ISA500 prend en charge les versions 2 et 3 du protocole LDAP. La plupart des annuaires LDAP, y compris Active Directory, utilisent la version 3 du protocole LDAP.

ÉTAPE 5 Dans l'onglet **Schema**, entrez les informations suivantes :

- **LDAP Schema** : choisissez l'un des schémas suivants :
  - Microsoft Active Directory
  - RFC2798 InetOrgPerson
  - RFC2307 Network Information Service
- **User Objects** : les champs suivants affichent les valeurs correctes utilisées par le schéma sélectionné. Les champs qui apparaissent en grisé ne peuvent pas être modifiés, mais vous pouvez spécifier les champs modifiables si vous disposez d'une configuration spécifique de schéma LDAP.
  - **Object Class** : classe d'objet du compte d'utilisateur individuel.
  - **Login Name Attribute** : attribut utilisé pour l'authentification de connexion.
  - **Qualified Login Name Attribute** : attribut d'un objet utilisateur qui définit un nom de connexion secondaire pour l'utilisateur, au format name@domain.
  - **User Group Membership Attribute** : attribut d'appartenance qui contient des informations sur le groupe auquel l'objet utilisateur appartient. Cette option est uniquement disponible pour Microsoft Active Directory.
  - **Framed IP Address Attribute** : attribut permettant de récupérer une adresse IP statique qui est attribuée à un utilisateur dans l'annuaire.

- **User Group Objects** : les champs suivants affichent les valeurs correctes utilisées par le schéma sélectionné.
  - **Object Class** : nom associé au groupe d'attributs.
  - **Member Attribute** : attribut associé à un membre.

ÉTAPE 6 Dans l'onglet **Directory**, entrez les informations sur la direction de l'utilisateur dans les champs suivants :

- **Primary Domain** : entrez le domaine utilisateur utilisé par votre mise en œuvre de LDAP. Tous les composants du domaine utilisent « dc= ». Le domaine est au format « dc=ExampleCorporation, dc=com ».
- **User Tree for Login to Server** : si vous choisissez **Give Login Name or Location in Tree** comme méthode de connexion dans l'onglet **Settings**, indiquez l'arborescence d'utilisateur utilisée pour se connecter au serveur LDAP.
- **Trees Containing Users** : spécifiez les arborescences d'utilisateurs qui se trouvent dans l'annuaire LDAP. Pour ajouter une entrée, cliquez sur **Add**. Pour modifier une entrée, cliquez sur l'icône de **modification** (crayon). Pour supprimer une entrée, cliquez sur **Remove**. Pour modifier la priorité d'une entrée dans l'arborescence, cliquez sur la flèche orientée vers le haut ou celle orientée vers le bas.
- **Trees Containing User Groups** : spécifiez les arborescences d'utilisateurs qui se trouvent dans l'annuaire LDAP. Celles-ci s'appliquent uniquement lorsqu'il n'y a aucun attribut d'appartenance au groupe d'utilisateurs dans l'objet utilisateur du schéma et ne sont pas utilisées avec AD. Pour ajouter une entrée, cliquez sur **Add**. Pour modifier une entrée, cliquez sur **Edit**. Pour supprimer une entrée, cliquez sur **Remove**. Pour modifier la priorité d'une entrée dans l'arborescence, cliquez sur la flèche orientée vers le haut ou celle orientée vers le bas.

  REMARQUE : Toutes les arborescences ci-dessus sont fournies dans le format des noms distinctifs (« cn=Users, dc=ExampleCorporation, dc=com »).

ÉTAPE 7 Dans l'onglet **LDAP Users**, entrez les informations suivantes :

- **Allow Only Users Listed Locally** : cliquez sur **On** pour autoriser uniquement les utilisateurs LDAP qui sont également présents dans la base de données locale à se connecter ou sur **Off** pour désactiver cette option.

- **Default LDAP User Group** : choisissez un groupe d'utilisateurs local en tant que groupe par défaut auquel les utilisateurs LDAP appartiennent. Si le groupe n'existe pas dans la base de données locale lors de l'obtention des informations sur le groupe d'utilisateurs à partir du serveur LDAP, l'utilisateur LDAP sera défini automatiquement sur le groupe d'utilisateurs local spécifié.

ÉTAPE 8 Dans l'onglet **Test,** entrez les informations d'identification dans les champs **User** et **Password**, puis cliquez sur **Test** pour vérifier si l'utilisateur LDAP est valide.

ÉTAPE 9 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 10 Cliquez sur **Save** pour appliquer vos paramètres.

Utilisation de la base de données locale et du protocole LDAP pour l'authentification

Vous pouvez utiliser à la fois la base de données locale et LDAP pour authentifier les utilisateurs qui tentent d'accéder au réseau.

ÉTAPE 1 Cliquez sur **Users > User Authentication**.

ÉTAPE 2 Choisissez **LDAP + Local Database** comme méthode d'authentification.

ÉTAPE 3 Cliquez sur **Configure** pour configurer les paramètres LDAP pour l'authentification des utilisateurs. Pour plus d'informations, reportez-vous à la section **Utilisation du protocole LDAP pour l'authentification des utilisateurs, page 371**.

ÉTAPE 4 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration de serveurs RADIUS

Utilisez la page RADIUS Servers pour configurer les serveurs RADIUS qui sont utilisés pour authentifier les utilisateurs qui tentent d'accéder aux ressources réseau. Un groupe RADIUS inclut un serveur RADIUS principal et un serveur RADIUS de secours. L'Cisco ISA500 prédéfinit trois groupes RADIUS.

ÉTAPE 1 Cliquez sur **Users > RADIUS Servers**.

La fenêtre RADIUS Servers s'ouvre. Tous les groupes RADIUS prédéfinis sont répertoriés dans la table.

ÉTAPE 2 Pour modifier les paramètres d'un groupe RADIUS prédéfini, cliquez sur l'icône de **modification** (crayon).

La fenêtre RADIUS Group - Edit s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **Primary RADIUS Server IP** : entrez l'adresse IP du serveur RADIUS principal.
- **Primary RADIUS Server Port** : saisissez le numéro de port du serveur RADIUS principal qui est utilisé pour envoyer le trafic RADIUS. La valeur par défaut est 1812.
- **Primary RADIUS Server Pre-shared Key** : entrez la clé pré-partagée configurée sur le serveur RADIUS principal.
- **Secondary RADIUS Server IP** : entrez l'adresse IP du serveur RADIUS secondaire.
- **Secondary RADIUS Server Port** : saisissez le numéro de port du serveur RADIUS secondaire utilisé pour envoyer le trafic RADIUS. La valeur par défaut est 1812.
- **Secondary RADIUS Server Pre-shared Key** : entrez la clé pré-partagée configurée sur le serveur RADIUS secondaire.

ÉTAPE 4 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 5 Répétez les étapes ci-dessus pour modifier les paramètres d'autres groupes RADIUS si nécessaire.

ÉTAPE 6 Cliquez sur **Save** pour appliquer vos paramètres.

10

Gestion des périphériques

Ce chapitre explique la marche à suivre pour effectuer les tâches suivantes : maintenir la configuration et le microprogramme, redémarrer ou réinitialiser l'Cisco ISA500, gérer la licence de sécurité et les certificats numériques, et configurer d'autres fonctionnalités permettant de faciliter la gestion de l'Cisco ISA500. Il comprend les sections suivantes :

- **Affichage de l'état du système, page 377**
- **Administration, page 378**
- **Sauvegarde et restauration d'une configuration, page 391**
- **Gestion des certificats pour l'authentification, page 393**
- **Configuration des paramètres d'assistance et des services Cisco, page 399**
- **Sauvegarde et restauration d'une configuration, page 391**
- **Configuration de l'heure système, page 402**
- **Configuration des propriétés du périphérique, page 403**
- **Utilitaires de diagnostic, page 404**
- **Protocoles de détection de périphériques, page 406**
- **Gestion du microprogramme, page 410**
-
- **Gestion de la licence de sécurité, page 417**
- **Gestion des journaux, page 421**
- **Réamorçage et réinitialisation du périphérique, page 427**
- **Configuration des programmations, page 429**

Pour accéder aux pages relatives à la gestion des périphériques, cliquez sur **Device Management** dans le volet de navigation gauche.

Affichage de l'état du système

Cette section explique comment afficher les informations relatives à tous les processus en cours d'exécution, ainsi qu'à l'utilisation de la mémoire et du processeur du système. Reportez-vous aux rubriques suivantes :

- **Affichage de l'état des processus, page 377**
- **Affichage de l'utilisation des ressources, page 377**

Affichage de l'état des processus

Reportez-vous à la page Processes pour consulter les informations relatives à tous les processus en cours. Cette page est automatiquement mise à jour toutes les 10 secondes. Cliquez sur **Refresh** pour actualiser manuellement les données.

Device Management > System Status > Processes

Champ	Description
Name	Nom du processus en cours d'exécution sur l'Cisco ISA500.
Description	Brève description du processus en cours d'exécution.
Protocol	Protocole utilisé par le connecteur.
Port	Numéro de port de l'extrémité locale du connecteur.
Local Address	Adresse IP de l'extrémité locale du connecteur.
Foreign Address	Adresse IP de l'extrémité distante du connecteur.

Affichage de l'utilisation des ressources

Reportez-vous à la page Resource Utilization pour consulter les informations relatives à l'utilisation de la mémoire et du CPU du système.

Device Management > System Status > Resource Utilization

Champ	Description
CPU Utilization	
CPU Usage by User	Pourcentage de la ressource de CPU actuellement utilisée par les processus d'espace utilisateur.

Champ	Description
CPU Usage by Kernel	Pourcentage de la ressource de CPU actuellement utilisée par les processus d'espace noyau.
CPU Idle	Pourcentage de la ressource de CPU inactive à l'heure actuelle.
CPU Waiting for I/O	Pourcentage de la ressource de CPU actuellement en attente d'E/S.
Memory Utilization	
Total Memory	Espace mémoire total disponible sur l'Cisco ISA500
Memory Used	Espace mémoire total actuellement utilisé par les processus.
Free Memory	Espace mémoire total actuellement non utilisé par les processus.
Cached Memory	Espace mémoire total actuellement utilisé comme cache.
Buffer Memory	Espace mémoire total actuellement utilisé en tant que tampon.

Administration

Utilisez les pages Administration pour modifier le nom d'utilisateur et le mot de passe du compte d'administrateur par défaut, configurer les paramètres de session utilisateur, configurer de manière centralisée les paramètres d'alerte par courriel et configurer la gestion à distance et SNMP.

Cette section comprend les rubriques suivantes :

- **Configuration des paramètres d'administration, page 379**
- **Configuration de l'administration à distance, page 380**
- **Configuration des paramètres d'alerte par courriel, page 382**
- **La configuration SNMP, page 389**

Configuration des paramètres d'administration

Utilisez la page Administrator Settings pour modifier le nom d'utilisateur et le mot de passe du compte d'administrateur par défaut, et pour configurer les paramètres de session utilisateur. Les paramètres de session utilisateur s'appliquent à toutes les méthodes d'authentification.

REMARQUE À la première connexion, vous devez changer le mot de passe administrateur par défaut, pour des raisons de sécurité. La page Administrator Settings propose une autre approche permettant de modifier le nom d'utilisateur et le mot de passe du compte d'administrateur par défaut, mais pas à la première connexion.

ÉTAPE 1 Cliquez sur **Device Management > Administration > Administrator Settings**.

ÉTAPE 2 Pour mettre à jour votre mot de passe, entrez les informations suivantes dans la zone **Administrator Name and Password** :

- **User Name** : saisissez le nom d'utilisateur actuel du compte d'administrateur par défaut ou entrez un nouveau nom d'utilisateur si vous souhaitez le modifier.
- **Current Password** : entrez le mot de passe administrateur actuel.
- **New password** : saisissez un nouveau mot de passe administrateur. Les mots de passe sont sensibles à la casse.

  REMARQUE : Un mot de passe doit comporter au minimum 8 caractères et au moins trois des classes de caractères suivantes : lettres majuscules et minuscules, chiffres et caractères spéciaux. Ne répétez aucun mot de passe plus de trois fois sur une ligne. Ne définissez pas le nom d'utilisateur ou « cisco » comme mot de passe. Ne mettez pas ces mots en majuscule et ne les écrivez pas à l'envers.
- **Confirm New Password** : ressaisissez le nouveau mot de passe pour le confirmer.

ÉTAPE 3 Pour modifier les paramètres de session utilisateur, entrez les informations suivantes dans la zone **Session** :

- **Inactivity Timeout** : entrez la durée, en minutes, pendant laquelle l'utilisateur peut être inactif avant que la session ne soit déconnectée. La valeur par défaut est de 15 minutes. Une valeur égale à zéro (0) indique que l'utilisateur est toujours actif avant que la session ne soit déconnectée.
- **Limit Login Session for Web Logins** : cliquez sur **On** pour limiter la durée pendant laquelle l'utilisateur peut être connecté à l'Cisco ISA500 via un navigateur web. Entrez la durée en minutes dans le champ **Login Session Limit**. La valeur par défaut est de 10 minutes. Une valeur égale à zéro (0) indique qu'il n'y a pas de limite pour les sessions de connexion au Web.

- **Web Server SSL Certificate** : sélectionnez un certificat pour authentifier les utilisateurs qui tentent d'accéder à l'utilitaire de configuration au moyen d'un navigateur web via le protocole HTTPS. Le serveur d'authentification Web utilise systématiquement le certificat par défaut pour l'authentification. Vous pouvez choisir un certificat importé pour l'authentification. Le serveur d'authentification Web redémarrera pour charger le certificat sélectionné.
- **Management** : cochez cette case pour activer l'accès à l'utilitaire de configuration via HTTP ou HTTPS. Le protocole HTTP est activé par défaut.

  REMARQUE : Si les deux cases sont décochées, l'accès à l'utilitaire de configuration est désactivé.
- **Allow Address** : choisissez d'accorder l'accès à l'utilitaire de configuration à partir de **n'importe quelle** adresse IP ou d'une adresse ou d'une plage d'adresses particulière. Le paramètre par défaut est « Any ».

ÉTAPE 4 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration de l'administration à distance

Vous pouvez activer l'administration à distance pour permettre à un administrateur de se connecter à l'utilitaire de configuration à partir d'un autre réseau que le réseau local (LAN) de l'appareil de sécurité. Vous pouvez autoriser les connexions via HTTPS (HTTP sur SSL) et HTTP.

Lorsque cette fonction est activée, un utilisateur peut accéder à l'utilitaire de configuration en lançant un navigateur Web et en entrant le protocole, l'adresse IP WAN de l'appareil de sécurité et le numéro de port d'écoute spécifié, comme illustré dans cet exemple : `https://209.165.201.1:8080`

REMARQUE Pour accéder en local ou à distance à l'utilitaire de configuration à partir d'un PC exécutant Windows Server 2008 et Internet Explorer 9 via le protocole HTTP, ajoutez l'URL (telle que http://192.168.75.1:80/login.htm) comme site de confiance. Pour ajouter un site de confiance dans Internet Explorer 9, vous pouvez tout d'abord ouvrir le navigateur et accéder à la page Outils > Options Internet > Sécurité, puis sélectionner la zone **Sites de confiance** et ajouter votre URL comme site de confiance.

ÉTAPE 1 Cliquez sur **Device Management > Administration > Remote Administration.**

ÉTAPE 2 Indiquez les informations suivantes :

- **Remote Administration** : cliquez sur **On** pour activer la gestion à distance via HTTPS ou cliquez sur **Off** pour la désactiver. Nous vous recommandons d'utiliser HTTPS pour la gestion à distance sécurisée.
- **HTTPS Listen Port Number** : si vous activez la gestion à distance via le protocole HTTPS, entrez le numéro de port. Par défaut, le numéro du port d'écoute pour HTTPS est 8080.
- **HTTP** : cliquez sur **On** pour activer la gestion à distance via HTTP ou sur **Off** pour la désactiver.
- **HTTP Listen Port Number** : si vous activez la gestion à distance via le protocole HTTP, entrez le numéro de port. Par défaut, le numéro du port d'écoute pour HTTP est 80.
- **Allow Address** : pour spécifier les périphériques qui peuvent accéder à l'utilitaire de configuration par l'intermédiaire de l'interface WAN, choisissez un objet d'adresse ou entrez une adresse.
  - **Address Objects** : ces objets représentent les adresses IP et plages d'adresses connues, telles que le VLAN GUEST et le pool DHCP. Pour obtenir des informations sur les objets d'adresse répertoriés, consultez la page Networking > Address Management.
  - **Create new address** : choisissez cette option pour entrer une adresse IP ou une plage d'adresses. Dans la fenêtre contextuelle, renseignez le champ **Name** et spécifiez le **Type** (hôte ou plage). Pour un hôte unique, entrez l'adresse IP. Si vous choisissez la plage, entrez l'**adresse IP de début** et l'**adresse IP de fin**.
- **Remote SNMP** : cliquez sur **On** pour activer SNMP pour la connexion à distance ou sur **Off** pour désactiver SNMP. L'activation de SNMP permet aux utilisateurs distants d'utiliser le protocole SNMP pour gérer l'Cisco ISA500 du côté WAN.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration des paramètres d'alerte par courriel

Utilisez la page Email Alert pour configurer de manière centralisée la procédure d'envoi des courriels d'alerte à l'opérateur ou à l'administrateur pour des événements ou comportements spécifiques susceptibles d'avoir une incidence sur les performances, le fonctionnement et la sécurité de votre Cisco ISA500 ou pour le débogage.

Lorsque cette fonctionnalité est activée, une alerte est envoyée aux trois conditions suivantes :

- Les catégories URL Web sont modifiées.
- L'état du serveur d'applications des services de sécurité est défini sur No Authentication (aucune authentification) car le serveur est hors ligne.
- La résolution DNS du nom du serveur d'applications des services de sécurité échoue car le serveur est hors ligne.

ÉTAPE 1 Cliquez sur **Device Management > Administration > Email Alert**.

ÉTAPE 2 Dans la zone **Email Server**, spécifiez le serveur de messagerie SMTP qui est utilisée pour envoyer les courriels d'alerte.

- **SMTP Server** : entrez l'adresse IP ou le nom Internet du serveur SMTP.
- **Port** : saisissez le port pour la communication SMTP. La plage des numéros de port valide est comprise entre 1 et 65535.
  - Si vous choisissez le port 25 (le paramètre par défaut), vous pouvez sélectionner le protocole TLS (Transport Layer Security) ou SSL (Secure Sockets Layer) pour sécuriser la communication SMTP, ou l'option « None » pour une connexion non sécurisée.
  - Si vous choisissez le port 465, vous pouvez sélectionner l'option TLS ou SSL pour sécuriser la communication SMTP.
  - Si vous choisissez le port 587, vous pouvez sélectionner l'option TLS ou SSL pour sécuriser la communication SMTP.
- **Secure Connectivity Method** : sélectionnez l'option **TLS** ou **SSL** pour sécuriser la communication SMTP, ou sélectionnez l'option **None** pour une connexion non sécurisée. Si vous sélectionnez TLS ou SSL, l'authentification SMTP sera activée.

- **SMTP Authentication** : cliquez sur **On** si le serveur SMTP nécessite une authentification avant d'accepter les connexions. Les utilisateurs doivent fournir les identifiants de compte SMTP pour l'authentification.
- **Account** : entrez le nom d'utilisateur du compte de messagerie SMTP.
- **Password** : entrez le mot de passe du compte de messagerie SMTP.
- **From Email Address** : saisissez l'adresse courriel d'envoi des courriels d'alertes.
- **From Email Address** : saisissez l'adresse courriel d'envoi des courriels d'alertes. Cette adresse courriel est utilisée pour recevoir des courriels d'alerte pour tous les événements. Si vous souhaitez envoyer les courriels d'alerte appartenant à différents événements à différentes adresses courriel, décochez l'option **All Alerts**, puis spécifiez individuellement l'adresse courriel pour chaque événement.

ÉTAPE 3 Pour vérifier les paramètres, cliquez sur **Test Connectivity to Email Server**. Les résultats s'affichent dans une fenêtre contextuelle.

ÉTAPE 4 Dans la zone **Event Alerts**, indiquez les paramètres d'alerte par courriel pour chaque événement. Lorsque les événements associés seront détectés, les courriels d'alertes seront envoyés à l'adresse courriel spécifiée.

Le tableau suivant fournit des informations sur la manière d'activer la fonctionnalité d'alerte par courriel pour chaque événement.

Événement	Description
CPU Overload Alert	Envoie un courriel d'alerte si l'utilisation du processeur est plus élevée que le seuil pendant plus d'une minute et envoie un autre courriel d'alerte lorsque l'utilisation du processeur revient à la normale pendant une minute. ▪ **CPU Threshold Setting** : saisissez une valeur comprise entre 10 et 100 % pour le seuil d'utilisation du processeur. La valeur par défaut est 90 %. ▪ **From Email Address** : saisissez l'adresse courriel d'envoi des courriels d'alertes. Pour activer l'alerte de surcharge du processeur, vous devez effectuer les tâches suivantes : ▪ Configurez les paramètres de serveur de messagerie utilisés pour envoyer des courriels d'alerte. ▪ Cochez l'option **CPU Overload Alert** dans la colonne **Enable** et spécifiez le seuil d'utilisation du processeur et l'adresse courriel utilisée pour recevoir les courriels d'alertes.
New Firmware Alert	Envoie un courriel d'alerte à l'adresse courriel spécifiée si un microprogramme plus récent est détecté sur le site Cisco.com. ▪ **From Email Address** : saisissez l'adresse courriel d'envoi des courriels d'alertes. Pour activer l'alerte de nouvelle version du microprogramme, vous devez effectuer les tâches suivantes : ▪ Configurez les paramètres de serveur de messagerie utilisés pour envoyer des courriels d'alerte. ▪ Cochez l'option **New Firmware Alert** dans la colonne **Enable** et spécifiez l'adresse courriel utilisée pour recevoir les courriels d'alertes. **REMARQUE** : Vérifiez que vous disposez d'une connexion WAN active et d'un compte Cisco.com valide pour télécharger la dernière image du microprogramme depuis le site Cisco.com, puis installez-la sur votre Cisco ISA500. Pour plus d'informations, reportez-vous à la section **Mise à niveau de votre microprogramme à partir du site Cisco.com, page 413**.

Événement	Description
License Expiration Alert	Envoie un courriel d'alerte quelques jours avant l'expiration de la licence de sécurité. ▪ **Days** : entrez le nombre de jours devant précéder l'expiration de la licence pour l'envoi du courriel d'alerte. La valeur par défaut est de 15 jours. ▪ **From Email Address** : saisissez l'adresse courriel d'envoi des courriels d'alertes. Pour activer l'alerte avant l'expiration de la licence, vous devez effectuer les tâches suivantes : ▪ Valider la licence de sécurité dans l'Cisco ISA500 sur la page Device Management > License Management**.** Voir **Installation ou renouvellement de la licence de sécurité, page 418**. ▪ Configurez les paramètres de serveur de messagerie utilisés pour envoyer des courriels d'alerte. ▪ Cochez l'option **License Expiration Alert** dans la colonne **Enable**, définissez le nombre de jours devant précéder l'expiration de la licence pour l'envoi des courriels d'alertes et spécifiez l'adresse courriel utilisée pour recevoir les courriels d'alertes.

Événement	Description
Syslog Email	Envoie les messages syslog selon une programmation à l'adresse courriel spécifiée à des fins de dépannage. ▪ **Send to Email Address** : saisissez l'adresse courriel de réception des messages syslog. Pour activer les messages syslog, vous devez effectuer les tâches suivantes : ▪ Activez la fonctionnalité de fichier journal et spécifiez le sous-titre et le niveau de gravité des messages syslog que vous souhaitez envoyer, ainsi que la programmation de l'envoi des messages syslog sur la page Device Management > Logs > Log Settings. Voir **Configuration des paramètres de journal, page 423**. ▪ Activez la fonctionnalité **Email Alert** pour les composants sur la page Device Management > Logs > Log Facilities. Les messages syslog générés par les composants sélectionnés peuvent être envoyés à l'adresse courriel spécifiée. Voir **Configuration des composants journaux, page 426**. ▪ Configurez les paramètres du serveur de messagerie utilisés pour envoyer les messages syslog. ▪ Cochez l'option **Syslog Email** dans la colonne **Enable** et spécifiez l'adresse courriel utilisée pour recevoir les messages syslog.
Site-to-Site VPN Up/Down Alert	Envoie un courriel d'alerte lorsqu'un tunnel VPN est établi, qu'un tunnel VPN est inactif ou que la négociation de tunnel VPN échoue. ▪ **From Email Address** : saisissez l'adresse courriel d'envoi des courriels d'alertes. Pour activer l'alerte de VPN de site à site actif/inactif, vous devez effectuer les tâches suivantes : ▪ Activez la fonctionnalité VPN de site à site et spécifiez les stratégies VPN IPsec utilisées pour établir les tunnels VPN sur la page VPN > Site-to-Site > IPsec Policies. Voir **Configuration d'un VPN de site à site, page 309**. ▪ Configurez les paramètres de serveur de messagerie utilisés pour envoyer des courriels d'alerte. ▪ Cochez l'option **Site-to-Site VPN Up/Down Alert** dans la colonne **Enable** et spécifiez l'adresse courriel utilisée pour recevoir les courriels d'alertes.

Événement	Description
WAN Up/Down Alert	Envoie un courriel d'alerte si la liaison WAN est active ou inactive. ▪ **Alert Interval** : spécifiez la fréquence (en minutes) à laquelle l'Cisco ISA500 doit envoyer les courriels d'alertes. Saisissez une valeur comprise entre 3 et 1 440 minutes. La valeur par défaut est de 5 minutes. ▪ **From Email Address** : saisissez l'adresse courriel d'envoi des courriels d'alertes. Pour activer l'alerte de WAN actif/inactif, vous devez effectuer les tâches suivantes : ▪ Configurez les paramètres de serveur de messagerie utilisés pour envoyer des courriels d'alerte. ▪ Cochez l'option **WAN Up/Down Up/Down Alert** dans la colonne **Enable** et spécifiez l'adresse courriel utilisée pour recevoir les courriels d'alertes.
Traffic Meter Alert	Envoie un courriel d'alerte lorsque la limite du trafic est atteinte ou avant la réinitialisation du compteur de trafic. ▪ **From Email Address** : saisissez l'adresse courriel d'envoi des courriels d'alertes. Pour activer l'alerte de mesure du trafic, vous devez effectuer les tâches suivantes : ▪ Activez la fonctionnalité de mesure du trafic pour le WAN principal et le WAN secondaire (le cas échéant) et spécifiez les paramètres correspondants sur les pages Networking > WAN > Traffic Metering**.** Voir **Mesure et limitation du trafic avec l'utilitaire de contrôle du trafic, page 142**. ▪ Configurez les paramètres de serveur de messagerie utilisés pour envoyer des courriels d'alerte. ▪ Cochez l'option **New Firmware Alert** dans la colonne **Enable** et spécifiez l'adresse courriel utilisée pour recevoir les courriels d'alertes.

Événement	Description
Anti-Virus Alert	Envoie un courriel d'alerte à l'intervalle spécifié à une adresse courriel spécifiée si des virus sont détectés. ▪ **Alert Interval** : spécifiez la fréquence (en minutes) d'envoi par l'Cisco ISA500 d'un courriel d'alerte pour les événements de virus. Saisissez une valeur comprise entre 1 et 1 440 minutes. La valeur par défaut est de 30 minutes. L'Cisco ISA500 générera des fichiers journaux d'événements de virus entre les intervalles d'alerte et les enverra dans un courriel d'alerte à l'adresse courriel spécifiée. ▪ **From Email Address** : saisissez l'adresse courriel d'envoi des courriels d'alertes. Pour activer l'alerte antivirus, vous devez effectuer les tâches suivantes : ▪ Activez la fonctionnalité d'antivirus et spécifiez les protocoles de recherche des virus sur la page Security Services > Anti-Virus > General Settings. Voir **Configuration de l'antivirus, page 269**. ▪ Configurez les paramètres de serveur de messagerie utilisés pour envoyer des courriels d'alerte. ▪ Cochez l'option **Anti-Virus VPN Up/Down Alert** dans la colonne **Enable** et spécifiez l'adresse courriel utilisée pour recevoir les courriels d'alertes.
IPS Alert	Envoie un courriel d'alerte toutes les 30 minutes à l'adresse courriel spécifiée si une attaque est détectée par le service IPS ou si une application est bloquée par le service de contrôle des applications. ▪ **From Email Address** : saisissez l'adresse courriel d'envoi des courriels d'alertes. Pour activer la fonctionnalité d'alerte IPS, vous devez effectuer les tâches suivantes : ▪ Activez IPS et configurez les paramètres IPS. Voir **Configuration de la prévention des intrusions, page 290**. ▪ Activez le contrôle des applications et configurez les paramètres de contrôle des applications. Voir **Configuration du contrôle des applications, page 277**. ▪ Configurez les paramètres de serveur de messagerie utilisés pour envoyer des courriels d'alerte. ▪ Cochez l'option **New Firmware Alert** dans la colonne **Enable** et spécifiez l'adresse courriel utilisée pour recevoir les courriels d'alertes.

Événement	Description
Web URL Filtering Alert	Envoie un courriel d'alerte à l'adresse courriel spécifiée lorsque des catégories d'URL Web sont modifiées. ▪ **From Email Address** : saisissez l'adresse courriel d'envoi des courriels d'alertes. Pour activer la fonctionnalité d'alerte de filtrage URL Web, vous devez effectuer les tâches suivantes : ▪ Activez le filtrage URL Web sur la page Security Services > Web URL Filtering > Policy to Zone Mapping. Voir **Configuration du filtrage URL Web, page 298**. ▪ Configurez les paramètres de serveur de messagerie utilisés pour envoyer des courriels d'alerte. ▪ Cochez l'option **New Firmware Alert** dans la colonne **Enable** et spécifiez l'adresse courriel utilisée pour recevoir les courriels d'alertes.

REMARQUE : Si une adresse courriel globale destinée à la réception de tous les courriels d'alertes est configurée dans le champ **To Email Address**, elle est affichée dans le champ **Send to Email Address** de toutes les catégories.

ÉTAPE 5 Cliquez sur **Save** pour appliquer vos paramètres.

La configuration SNMP

Le protocole SNMP (Simple Network Management Protocol) est un protocole réseau utilisé sur le protocole UDP (User Datagram Protocol). Il permet de surveiller et de gérer l'Cisco ISA500 à partir d'un gestionnaire SNMP. Le protocole SNMP permet de surveiller et de contrôler les périphériques réseau à distance et de gérer la configuration, la collecte des statistiques, les performances et la sécurité.

ÉTAPE 1 Cliquez sur **Device Management > Administration > SNMP**.

ÉTAPE 2 Cliquez sur **On** pour activer SNMP ou sur **Off** pour désactiver SNMP. Par défaut, le protocole SNMP est désactivé.

ÉTAPE 3 Si vous activez SNMP, spécifiez la version SNMP. L'Cisco ISA500 prend en charge la surveillance de réseau via SNMP Versions 1, 2c et 3. Par défaut, SNMP Versions 1 et 2 est sélectionné.

ÉTAPE 4 Une fois que vous avez activé SNMP et sélectionné la version SNMP, entrez les informations suivantes :

- **System Contact** : entrez le nom du contact pour votre Cisco ISA500.
- **Device** : saisissez le nom du périphérique pour faciliter l'identification de votre Cisco ISA500.
- **System Location** : entrez l'emplacement physique de votre Cisco ISA500.
- **Security User Name** : entrez le nom du compte d'administrateur disposant de la capacité d'accéder et de gérer les objets MIB SNMP. Ceci est uniquement disponible pour SNMPv3.
- **Authentication Password** : entrez le mot de passe du compte d'administrateur pour l'authentification (la longueur minimale du mot de passe est de 8 caractères). Ceci est uniquement disponible pour SNMPv3.
- **Encrypted Password** : entrez le mot de passe pour le cryptage des données (la longueur minimale du mot de passe est de 8 caractères). Ceci est uniquement disponible pour SNMPv3.
- **SNMP Engine ID** : ID du moteur de l'entité SNMP. L'ID du moteur est utilisé comme ID unique entre deux entités SNMP. Ceci est uniquement disponible pour SNMPv3.

ÉTAPE 5 Pour activer un déroutement SNMP, entrez les informations suivantes :

- **SNMP Read-Only Community** : entrez la communauté en lecture seule qui est utilisée pour accéder à l'entité SNMP.
- **SNMP Read-Write Community** : entrez la communauté en lecture-écriture qui est utilisé pour accéder à l'entité SNMP.
- **Trap Community** : entrez la communauté de laquelle l'hôte récepteur d'interruption distant reçoit les déroutements ou les notifications envoyés par l'entité SNMP.
- **SNMP Trusted Host** : entrez l'adresse IP ou le nom de domaine de l'hôte auquel l'entité SNMP fait confiance. L'hôte de confiance peut accéder à l'entité SNMP. Entrer 0.0.0.0 dans ce champ permet à n'importe quel hôte d'accéder à l'entité SNMP.
- **Trap Receiver Host** : entrez l'adresse IP ou le nom de domaine de l'hôte distant qui est utilisé pour recevoir les déroutements SNMP.

ÉTAPE 6 Cliquez sur **Save** pour appliquer vos paramètres.

Sauvegarde et restauration d'une configuration

Reportez-vous à la page Device Management > Backup/Restore pour gérer votre configuration.

Vous pouvez sauvegarder vos paramètres actuels sous la forme d'un fichier de configuration sur votre PC local ou sur un périphérique USB, le cas échéant. Vous pouvez restaurer ultérieurement la configuration enregistrée si nécessaire. Sauvegardez votre configuration à chaque fois que vous apportez des modifications à la configuration des périphériques ou que vous effectuez des mises à jour du microprogramme.

REMARQUE Lors de l'enregistrement de la configuration dans un fichier, la licence de sécurité et les certificats auto-signés ne sont pas enregistrés dans ce fichier de configuration.

ÉTAPE 1 Cliquez sur **Device Management > Backup/Restore**.

ÉTAPE 2 Pour sauvegarder les paramètres actuels sur votre PC local, procédez comme suit :

a. Dans la zone **Configuration Backup**, sélectionnez la case d'option **Save Configuration to PC** et cliquez sur **Backup**. La fenêtre Encryption s'ouvre.

b. Si vous souhaitez crypter la configuration, cochez l'option **Encrypt** et entrez le mot de passe dans le champ **Key**, puis cliquez sur **OK**. Déterminez l'emplacement où vous souhaitez enregistrer le fichier de configuration (configure.bin) et cliquez sur **Save**.

c. Si vous ne souhaitez pas crypter la configuration, cliquez sur **OK**. Déterminez l'emplacement où vous souhaitez enregistrer le fichier de configuration (configure.xml) et cliquez sur **Save**.

ÉTAPE 3 Pour sauvegarder les paramètres actuels sur un périphérique USB, procédez comme suit :

a. Insérez un périphérique USB dans le port USB situé sur le panneau arrière. Vérifiez que l'état du périphérique USB s'affiche sous la forme « Device Attached ». Cliquez sur **Refresh** pour actualiser l'état immédiatement.

b. Dans la zone **Configuration Backup**, sélectionnez la case d'option **Save Configuration to USB** et cliquez sur **Backup**. La fenêtre Encryption s'ouvre.

c. Si vous souhaitez crypter la configuration, cochez l'option **Encrypt** et entrez le mot de passe dans le champ **Key**, puis cliquez sur **OK**. Les paramètres actuels seront enregistrés sous la forme d'un fichier de configuration (configure.bin) sur le périphérique USB.

d. Si vous ne cryptez pas la configuration, cliquez sur **OK**. Les paramètres actuels seront enregistrés sous la forme d'un fichier de configuration (configure.xml) sur le périphérique USB.

REMARQUE : Définissez le mot de passe avec soin et notez-le ; sans mot de passe correct, il vous sera impossible de charger le fichier de configuration par la suite.

ÉTAPE 4 Pour restaurer les paramètres à partir d'un fichier de configuration enregistré sur votre PC local, procédez comme suit :

a. Dans la zone **Configuration Restore**, sélectionnez la case d'option **Restore Configuration From PC**.

b. Cliquez sur **Browse** pour sélectionner le fichier de configuration enregistré sur votre PC local et cliquez sur **Restore**.

c. Si le fichier de configuration sélectionné est crypté, la fenêtre Encryption s'ouvre. Entrez le mot de passe dans le champ **Key** et cliquez sur **OK**. L'Cisco ISA500 se réinitialise avec les paramètres enregistrés du fichier de configuration sélectionné.

ÉTAPE 5 Pour restaurer les paramètres à partir d'un fichier de configuration enregistré sur un périphérique USB, procédez comme suit :

a. Insérez un périphérique USB dans le port USB situé sur le panneau arrière.

b. Dans la zone **Configuration Restore**, sélectionnez la case d'option **Restore Configuration From USB**. Vérifiez que l'état du périphérique USB affiche « Device Attached ». Cliquez sur **Refresh** pour actualiser l'état.

c. Dans la zone **Configuration files on USB device**, tous les fichiers de configuration enregistrés qui se trouvent sur le périphérique USB apparaissent dans la liste. Sélectionnez un fichier de configuration et cliquez sur **Restore**.

d. Si le fichier de configuration sélectionné est crypté, la fenêtre Encryption s'ouvre. Entrez le mot de passe dans le champ **Key** et cliquez sur **OK**. L'Cisco ISA500 se réinitialise avec les paramètres enregistrés du fichier de configuration sélectionné.

Gestion des certificats pour l'authentification

Utilisez la page Certificate Management pour gérer les certificats requis pour l'authentification. Vous pouvez effectuer les tâches suivantes :

- Afficher l'état et les détails des certificats. Voir **Affichage de l'état et des détails des certificats, page 394**.
- Pour exporter un certificat local ou une demande de signature de certificat (CSR) vers votre PC, cochez-les et cliquez sur l'icône de **téléchargement** dans la colonne **Configure**. Voir **Exportation de certificats vers votre PC local, page 395**.
- Pour exporter un certificat local ou une demande de signature de certificat vers un périphérique USB installé, cochez-les et cliquez sur l'icône d'**exportation vers USB** dans la colonne **Configure**. Voir **Exportation de certificats vers un périphérique USB, page 396**.
- Pour importer un certificat CA ou un certificat local depuis votre PC local, cliquez sur **Import PC**. Voir **Importation de certificats depuis votre PC local, page 396**.
- Pour importer un certificat CA ou un certificat local depuis un périphérique USB installé, cliquez sur **Import USB**. Voir **Importation de certificats depuis un périphérique USB, page 397**.
- Pour générer une demande de signature de certificat, cliquez sur **Request Signing**. Voir **Génération de nouvelles demandes de signature de certificat, page 397**.
- Pour importer un certificat signé pour une demande de signature de certificat depuis un PC local, cliquez sur l'icône de **téléchargement** dans la colonne **Configure**. Voir **Importation d'un certificat signé pour CSR depuis votre PC local, page 398**.
- Pour supprimer un certificat ou une demande de signature de certificat, cliquez sur l'icône de **suppression** (x) dans la colonne **Configure**.
- Pour supprimer plusieurs certificats, cochez-les et cliquez sur **Delete**.

Affichage de l'état et des détails des certificats

ÉTAPE 1 Cliquez sur **Device Management > Certificate Management**.

La fenêtre Certificate Management s'ouvre. Tous les certificats existants sont répertoriés dans le tableau. Les informations suivantes relatives aux certificats sont affichées :

- **Certificate** : nom du certificat.
- **Type** : type du certificat. L'Cisco ISA500 prend en charge trois types de certificats :
  - **Certificate Signing Request** : demande de certificat générée par votre Cisco ISA500 qui doit être envoyée à l'autorité de certification (CA) pour signature. Le CSR contient toutes les informations nécessaires à la création de votre certificat numérique.
  - **Local Certificate** : le certificat local est délivré par une autorité de certification fiable et utilisé dans les applications telles que la gestion à distance et VPN SSL. Pour utiliser un certificat local, vous devez d'abord demander un certificat à l'autorité de certification et après importer le certificat vers votre Cisco ISA500.
  - **CA Certificate** : le certificat CA est délivré par des autorités de certification intermédiaires, telles que GoDaddy ou VeriSign. Le certificat CA permet de vérifier la validité des certificats générés et signés par l'autorité de certification.

ÉTAPE 2 Pour afficher les informations détaillées d'un certificat, cliquez sur l'icône de **détails** dans la colonne **Details**.

Type de certificat	Details
CA Certificate ou Local Certificate	▪ **Name** : nom utilisé pour identifier ce certificat. ▪ **Issuer** : nom de l'autorité de certification qui a délivré le certificat. ▪ **Subject** : nom du titulaire (propriétaire) de ce certificat affiché aux autres organisations. ▪ **Serial number** : numéro de série géré par l'autorité de certification et utilisé à des fins d'identification. ▪ **Valid from** : date à partir de laquelle le certificat est valide. ▪ **Expires on** : date à laquelle le certificat expire. Il est recommandé de renouveler le certificat avant qu'il arrive à expiration.
Certification Signing Request (CSR)	▪ **Name** : nom utilisé pour identifier ce CSR. ▪ **Subject** : nom du titulaire (propriétaire) de ce certificat affiché aux autres organisations.

Exportation de certificats vers votre PC local

Vous pouvez exporter un certificat local ou une demande de signature de certificat vers votre PC local. L'exportation du certificat CA n'est pas autorisée.

ÉTAPE 1 Cliquez sur **Device Management > Certificate Management**.

ÉTAPE 2 Pour exporter un certificat local ou une demande de signature de certificat vers votre PC local, cliquez sur l'icône de **téléchargement** dans la colonne **Configure**.

- Si vous téléchargez une demande de signature de certificat, la fenêtre Download Certificate Signing Request s'ouvre. Cliquez sur **Download**. Le fichier de certificat est enregistré au format .pem.
- Si vous téléchargez un certificat local, la fenêtre Download Certificate s'ouvre. Entrez un mot de passe dans le champ **Enter Export Password** pour protéger le fichier de certificat et cliquez sur **Download**. Le fichier de certificat est enregistré au format .p12.

Exportation de certificats vers un périphérique USB

Pour exporter un certificat local ou une demande de signature de certificat vers un périphérique USB, vous devez en premier lieu insérer le périphérique USB dans le port USB situé sur le panneau arrière. L'exportation du certificat CA n'est pas autorisée.

ÉTAPE 1 Cliquez sur **Device Management > Certificate Management**.

ÉTAPE 2 Pour exporter un certificat local ou une demande de signature de certificat vers le périphérique USB, cliquez sur l'icône d'**exportation vers USB** dans la colonne **Configure**.

- Si vous téléchargez une demande de signature de certificat, la fenêtre Export Certificate Signing Request to USB s'ouvre. Cliquez sur **Export**. Le fichier CSR est enregistré sur le périphérique USB au format .pem.
- Si vous téléchargez un certificat local, la fenêtre Export Certificate to USB s'ouvre. Entrez un mot de passe dans le champ **Enter Export Password** pour protéger le fichier de certificat et cliquez sur **Export**. Le fichier de certificat est enregistré sur le périphérique USB au format .p12.

Importation de certificats depuis votre PC local

Vous pouvez importer un certificat local ou un certificat CA depuis votre PC local.

ÉTAPE 1 Cliquez sur **Device Management > Certificate Management**.

ÉTAPE 2 Pour importer un certificat local ou un certificat CA depuis votre PC local, cliquez sur **Import PC**.

ÉTAPE 3 Saisissez les informations suivantes :

- **Import a local end-user certificate with private key from a PKCS#12 (.p12) encoded file** : si vous sélectionnez cette option, cliquez sur **Browse** pour localiser et sélectionner un fichier de certificat local à partir de votre ordinateur local, entrez le nom du certificat dans le champ **Certificate Name** field et le mot de passe de protection dans le champ **Import Password**, puis cliquez sur **Import**.
- **Import a CA certificate from a PEM (.pem or .crt) encoded file** : si vous sélectionnez cette option, cliquez sur **Browse** pour localiser et sélectionner un fichier certificat CA à partir de votre PC local et cliquez sur **Import**.

Importation de certificats depuis un périphérique USB

Pour importer des certificats locaux ou CA depuis un périphérique USB, vous devez en premier lieu insérer le périphérique USB dans le port USB situé sur le panneau arrière.

ÉTAPE 1 Cliquez sur **Device Management > Certificate Management**.

ÉTAPE 2 Pour importer un certificat local ou un certificat CA depuis un périphérique USB, cliquez sur **Import USB**.

La fenêtre Import Certificate s'ouvre. Tous les certificats locaux et CA disponibles apparaissent dans la liste.

ÉTAPE 3 Vérifiez le fichier de certificat, entrez le nom du certificat dans le champ **Certificate Name** et le mot de passe de protection dans le champ **Import Password**, puis cliquez sur **Import**.

Génération de nouvelles demandes de signature de certificat

ÉTAPE 1 Cliquez sur **Device Management > Certificate Management**.

ÉTAPE 2 Cliquez sur **Request Signing** pour générer une nouvelle demande de signature de certificat.

La fenêtre Generate Certificate Signing Request s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **Certificate Alias** : entrez un nom d'alias pour le certificat.
- **Country Name** : choisissez un pays dans la liste déroulante.
- **State or Province Name** : saisissez le nom de l'état ou de la province de l'endroit où vous vous situez.
- **Locality Name** : saisissez l'adresse de l'endroit où vous vous situez.
- **Organization Name** : entrez le nom de votre organisation.
- **Organization Unit Name** : saisissez le nom de votre service.
- **Common Name** : entrez le nom commun du certificat.
- **E-mail Address** : entrez votre adresse électronique.

- **Subject Distinguished Name** : une fois que vous avez entré les informations ci-dessus, le nom unique (DN) est créé dans ce champ.
- **Subject Key Type** : affiche l'algorithme de signature (RSA) utilisé pour signer le certificat. RSA est un algorithme cryptographique de clé publique utilisé pour le cryptage des données.
- **Subject Key Size** : choisissez la longueur de la signature : 502 bits, 1 024 bits ou 2 048 bits.

ÉTAPE 4 Cliquez sur **Generate** pour créer un dossier de demande de signature de certificat.

Une fois qu'un fichier de demande de signature de certificat a été généré, vous devez exporter ce fichier vers votre PC local pour le soumettre à un enregistrement ou à une autorité de certification. Le fichier CSR est enregistré au format .pem.

Importation d'un certificat signé pour CSR depuis votre PC local

Vous pouvez télécharger le certificat signé pour une demande de signature de certification depuis votre PC local.

ÉTAPE 1 Cliquez sur **Device Management > Certificate Management**.

ÉTAPE 2 Pour importer le certificat signé pour une demande de signature de certificat depuis un PC local, cliquez sur l'icône de **téléchargement** dans la colonne **Configure**.

ÉTAPE 3 Cliquez sur **Browse** pour localiser et sélectionnez le fichier de certificat signé pour la demande de signature de certificat depuis votre PC local, puis cliquez sur **Upload**.

REMARQUE : Le fichier de certificat signé doit être au format PEM (fichier .pem ou .crt) codé.

Configuration des paramètres d'assistance et des services Cisco

Cette section décrit la marche à suivre pour configurer votre compte Cisco.com sur l'Cisco ISA500, activer ou désactiver Cisco OnPlus, configurer les paramètres d'assistance à distance et envoyer les contenus pour les diagnostics système. Reportez-vous aux rubriques suivantes :

- **Configuration d'un compte Cisco.com, page 399**
- **Configuration de Cisco OnPlus, page 400**
- **Configuration des paramètres d'assistance à distance, page 401**
- **Envoi de contenus pour les diagnostics système, page 401**

Configuration d'un compte Cisco.com

Utilisez la page Cisco.com Account pour configurer vos identifiants de compte Cisco.com sur l'Cisco ISA500.

Un compte Cisco.com valide est requis pour télécharger la dernière image du microprogramme depuis le site Cisco.com, ainsi que pour rechercher les mises à jour des signatures à partir du serveur de signature Cisco pour IPS, le contrôle des applications et l'antivirus. Si vous n'en disposez pas, accédez à la page https:// tools.cisco.com/RPF/register/register.do en cliquant sur le lien **Create a Cisco.com Account** figurant sur cette page pour enregistrer un compte Cisco.com.

REMARQUE Vous pouvez également configurer vos identifiants de compte Cisco.com à l'aide de l'assistant de configuration. Voir **Configuration des informations d'identification du compte Cisco.com, page 39**.

ÉTAPE 1 Cliquez sur **Device Management > Cisco Services & Support > Cisco.com Account**.

La fenêtre Cisco.com Account s'ouvre.

ÉTAPE 2 Saisissez les informations suivantes :

- **User Name :** entrez le nom de votre compte Cisco.com.
- **Password :** entrez le mot de passe de votre compte Cisco.com.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration de Cisco OnPlus

Utilisez la page Cisco OnPlus pour activer ou désactiver le service de sécurité avancée Cisco sur OnPlus sur l'Cisco ISA500. Activer le service de sécurité avancée Cisco OnPlus permet à votre Cisco ISA500 d'envoyer les données de notification et de signalement de sécurité via le service OnPlus. Si aucun périphérique OnPlus n'est présent sur votre réseau, ce paramètre n'a aucun effet.

Vous pouvez, par exemple, sauvegarder et restaurer la configuration, effectuer la mise à niveau du microprogramme et afficher les rapports d'utilisation du réseau, ceux de la bande passante WAN et l'utilisation du périphérique relative à Cisco ISA500 par le biais du service OnPlus. L'Cisco ISA500 peut lancer une connexion HTTP ou HTTPS avec l'agent.

Pour plus d'informations sur Cisco OnPlus, accédez à l'URL www.cisco.com/go/onplus.

ÉTAPE 1 Cliquez sur **Device Management > Cisco Services & Support > Cisco OnPlus**.

ÉTAPE 2 Cochez la case en regard de **Enable Cisco OnPlus Advanced Security Service** pour activer Cisco OnPlus sur votre Cisco ISA500 ou décochez cette case pour le désactiver. Par défaut, Cisco OnPlus est activé. Ce paramètre est fourni principalement à des fins d'assistance et de dépannage. Si vous désactivez OnPlus sur l'Cisco ISA500, le service Cisco OnPlus ne pourra pas communiquer avec l'Cisco ISA500, et la gestion, la surveillance et la création de rapports seront affectées de manière globale.

REMARQUE : L'Cisco ISA500 commence à collecter les données de session uniquement lorsque le périphérique OnPlus est connecté.

ÉTAPE 3 Si Cisco OnPlus est activé, nous vous recommandons d'activer les protocoles de détection suivants sur votre Cisco ISA500 pour une détection de périphériques et une prise en charge de la topologie optimales via le portail OnPlus :

- **Cisco Discovery Protocol (CDP)** : s'affiche si CDP est activé ou désactivé. Vous pouvez cliquer sur le lien pour afficher ou modifier les paramètres. Voir **Détection CDP, page 409**.
- **Bonjour Discovery Protocol** : s'affiche si Bonjour est activé ou désactivé. Vous pouvez cliquer sur le lien pour afficher ou modifier les paramètres. Voir **Bonjour Discovery, page 408**.

ÉTAPE 4 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration des paramètres d'assistance à distance

Utilisez la page Remote Support pour activer le serveur SSHv2 à des fins de débogage. Cette fonctionnalité permet aux ingénieurs d'utiliser un mot de passe racine unique de console pour se connecter à l'Cisco ISA500 afin d'effectuer des opérations de débogage.

ÉTAPE 1 Cliquez sur **Device Management > Cisco Services & Support > Remote Support**.

ÉTAPE 2 Saisissez les informations suivantes :

- **SSHv2 Server** : cliquez sur **On** pour activer le serveur SSHv2 pour le débogage ou sur **Off** pour le désactiver.
- **Remote Support Password** : entrez le mot de passe racine pour l'assistance à distance dans ce champ. Le mot de passe racine expire au bout de 24 heures. Vous devez donc en demander un nouveau une fois qu'il est arrivé à expiration.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Envoi de contenus pour les diagnostics système

Utilisez la page Send Diagnostics pour sélectionner les contenus, tels que le fichier de configuration, le fichier syslog et les données d'état du système, pour les compresser dans un fichier au format zip, puis pour envoyer le fichier compressé à l'adresse courriel spécifiée pour les diagnostics système. Vous pouvez définir un mot de passe pour protéger le fichier compressé, pour des raisons de sécurité.

ÉTAPE 1 Cliquez sur **Device Management > Cisco Services& Support > Send Diagnostics**.

ÉTAPE 2 Dans la zone **Content (compressed)**, choisissez le contenu que vous souhaitez utiliser pour diagnostiquer le système. Les fichiers sélectionnés sont compressés en un seul fichier.

- **Configuration File** : cliquez sur **On** pour compresser la configuration pour les diagnostics système.
- **Syslog File** : cliquez sur **On** pour compresser les messages syslog pour les diagnostics système.
- **System Status** : cliquez sur **On** pour compresser les données d'état du système pour les diagnostics système.

ÉTAPE 3 Dans la zone **Password Protection**, vous pouvez définir un mot de passe pour sécuriser le fichier compressé.

- **Password Protection** : cliquez sur **On** pour activer la protection par mot de passe ou sur **Off** pour la désactiver.
- **Password** : si vous activez la protection par mot de passe, entrez le mot de passe dans ce champ.

ÉTAPE 4 Dans la zone **Email**, indiquez l'adresse courriel de réception du fichier compressé.

- Vous pouvez envoyer le fichier compressé à l'adresse courriel spécifiée sur la page Email Alert en sélectionnant la première case d'option.
- Si vous souhaitez envoyer temporairement le fichier compressé à une adresse courriel spécifique pour effectuer des diagnostics système, sans changer les paramètres de la page Email Alert, sélectionnez la case d'option **Other Address** et entrez l'adresse courriel dans le champ.

ÉTAPE 5 Cliquez sur **Save** pour appliquer vos paramètres.

ÉTAPE 6 Cliquez sur **Send Now** pour envoyer immédiatement le fichier compressé à l'adresse courriel spécifiée.

ÉTAPE 7 Cliquez sur **Download** pour enregistrer le fichier compressé sur votre PC local.

Configuration de l'heure système

Utilisez la page Date and Time pour configurer manuellement l'heure système, ou pour synchroniser de façon dynamique l'heure système avec le serveur NTP (Network Time Protocol).

ÉTAPE 1 Cliquez sur **Device Management > Date and Time**.

ÉTAPE 2 Spécifiez le fuseau horaire à partir de la liste déroulante **Time zone**.

ÉTAPE 3 Sélectionnez la case d'option **Manually Set System Time** pour régler manuellement la date et l'heure. Entrez les valeurs dans les champs **Date** et **Time**.

ÉTAPE 4 Sélectionnez la case d'option **Dynamically Set System Time** pour synchroniser automatiquement la date et l'heure avec le serveur NTP spécifié :

- **Daylight Saving Time Adjustment** : cliquez sur **On** pour régler automatiquement l'heure d'été ou sur **Off** pour désactiver cette option.
- **Default NTP Servers** : cliquez sur cette option pour utiliser le serveur NTP par défaut.
- **Custom NTP Servers :** cliquez sur cette option pour utiliser un serveur NTP personnalisé. Entrez les adresses IP ou les noms de domaine de deux serveurs NTP personnalisés maximum dans les champs **Server 1 Name/IP Address** et **Server 2 Name/IP Address**. Le serveur 1 est le serveur NTP principal et le serveur 2 est le serveur NTP secondaire.
- **Current Time** : affiche la date et l'heure actuelles synchronisées avec le serveur NTP configuré.

ÉTAPE 5 Cliquez sur **Save** pour appliquer vos paramètres.

Configuration des propriétés du périphérique

Utilisez la page Device Properties pour configurer le nom d'hôte et le nom de domaine afin d'identifier votre Cisco ISA500 sur le réseau.

ÉTAPE 1 Cliquez sur **Device Management > Device Properties**.

ÉTAPE 2 Saisissez les informations suivantes :

- **Host Name** : entrez le nom d'hôte de votre Cisco ISA500. Celui-ci est affiché sur le réseau afin d'identifier votre périphérique.
- **Domain Name** : entrez un nom de domaine unique afin d'identifier votre réseau.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Utilitaires de diagnostic

Utilisez les utilitaires de diagnostic suivants pour accéder à la configuration de l'Cisco ISA500 et pour surveiller la santé globale du réseau.

- **Ping, page 404**
- **Traceroute, page 405**
- **DNS Lookup, page 405**
- **Capture de paquet, page 406**

REMARQUE Ces fonctionnalités nécessitent une connexion WAN active.

Ping

Utilisez la page Ping pour tester la connectivité entre l'Cisco ISA500 et un périphérique connecté sur le réseau.

ÉTAPE 1 Cliquez sur **Device Management > Diagnostic Utilities > Ping**.

La fenêtre Ping s'ouvre.

ÉTAPE 2 Saisissez les informations suivantes :

- **IP Address or URL** : entrez l'adresse IP ou l'URL pour le test Ping.
- **Packet Size :** saisissez une taille de paquet comprise entre 32 à 65 500 octets pour le test ping. L'Cisco ISA500 enverra un paquet de la taille définie à la destination.
- **Number of Pings** : saisissez le nombre de tests Ping. L'Cisco ISA500 enverra le paquet le nombre de fois qui est spécifié pour vérifier la connectivité avec la destination.

ÉTAPE 3 Cliquez sur **Start** pour envoyer une requête ping à l'adresse IP ou à l'URL, ou sur **Stop** pour cesser d'envoyer une requête ping.

Traceroute

Utilisez la page Traceroute pour afficher le routage entre l'Cisco ISA500 et une destination.

ÉTAPE 1 Cliquez sur **Device Management > Diagnostic Utilities > Traceroute**.

La fenêtre Traceroute s'ouvre.

ÉTAPE 2 Saisissez les informations suivantes :

- **IP Address or URL :** entrez l'adresse IP ou l'URL de la destination.
- **Maximum Number of Hops :** choisissez le nombre maximal de sauts.

ÉTAPE 3 Cliquez sur **Start** pour tracer le routage de l'adresse IP ou de l'URL, ou sur **Stop** pour arrêter le traçage.

DNS Lookup

Utilisez la page DNS Lookup pour récupérer l'adresse IP d'un serveur sur Internet.

ÉTAPE 1 Cliquez sur **Device Management > Diagnostic Utilities > DNS Lookup**.

ÉTAPE 2 Entrez l'adresse IP ou le nom de domaine que vous souhaitez rechercher dans le champ **IP Address or Domain Name**.

ÉTAPE 3 Cliquez sur **Run** pour interroger le serveur sur Internet. Si le nom de l'hôte ou du domaine existe, une réponse s'affiche avec l'adresse IP.

ÉTAPE 4 Cliquez sur **Clear** pour nettoyer les résultats de la requête.

Capture de paquet

Utilisez la page Packet Capture pour capturer tous les paquets qui passent par une interface sélectionnée.

ÉTAPE 1 Cliquez sur **Device Management > Diagnostic Utilities > Packet Capture**.

ÉTAPE 2 Choisissez une interface ou un réseau (tel que DEFAULT VLAN) dont vous souhaitez capturer les paquets dans la liste déroulante **Network.**

REMARQUE : Sélectionner WAN1 ou WAN2 (le cas échéant) signifie capturer des paquets via une interface logique. Sélectionner GEx signifie capturer des paquets via une interface physique. Si vous choisissez un VLAN, seul le trafic entre les réseaux locaux virtuels est capturé.

ÉTAPE 3 Cliquez sur **Start** pour commencer à capturer les paquets, sur **Stop** pour arrêter de les capturer ou sur **Save** pour enregistrer les paquets capturés.

Protocoles de détection de périphériques

L'Cisco ISA500 prend en charge les protocoles suivants pour détecter les périphériques :

- **UPnP Discovery, page 407**
- **Bonjour Discovery, page 408**
- **Détection CDP, page 409**
- **Détection LLDP, page 410**

UPnP Discovery

UPnP (Universal Plug and Play) permet la détection automatique des périphériques qui peuvent communiquer avec votre Cisco ISA500. La table UPnP Portmaps affiche les entrées de mappage de port des périphériques UPnP qui ont accédé à votre Cisco ISA500.

ÉTAPE 1 Cliquez sur **Device Management > Discovery Protocols > UPnP**.

ÉTAPE 2 Saisissez les informations suivantes :

- **Universal Plug-n-Play (UPnP)** : cliquez sur **On** pour activer la fonctionnalité UPnP ou sur **Off** pour la désactiver. Si la fonctionnalité UPnP est désactivée, l'Cisco ISA500 ne permettra pas la configuration automatique des périphériques.
- **LAN** : choisissez un VLAN existant sur lequel les informations UPnP sont diffusées et écoutées.
- **Advertisement Period** : entrez une valeur en secondes pour la fréquence à laquelle l'Cisco ISA500 diffuse ses informations UPnP à tous les périphériques dans la zone de portée. La valeur par défaut est de 1 800 secondes.
- **Advertisement Time to Live** : entrez une valeur exprimée en nombre de sauts pour chaque paquet UPnP. Il s'agit du nombre d'étapes qu'un paquet est autorisé à propager avant d'être rejeté. Les petites valeurs limiteront la portée de diffusion UPnP. La valeur par défaut est 4.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

ÉTAPE 4 Une fois que vous avez activé UPnP, les informations de la table UPnP Portmaps sont immédiatement actualisées. Cliquez sur **Refresh** pour actualiser manuellement les données.

Bonjour Discovery

Bonjour est un protocole de détection et d'annonces de service. Bonjour annonce uniquement les services par défaut configurés sur l'Cisco ISA500 lorsque Bonjour est activé.

ÉTAPE 1 Cliquez sur **Device Management > Discovery Protocols > Bonjour**.

ÉTAPE 2 Cliquez sur **On** pour activer Bonjour ou sur **Off** pour le désactiver. Si vous activez Bonjour, tous les services par défaut, tels que CSCO-SB, HTTP et HTTPS sont activés. Vous ne pouvez pas désactiver un service particulier. Vous pouvez seulement activer ou désactiver Bonjour.

ÉTAPE 3 Dans la zone **VLAN Association**, vous pouvez associer les VLAN pour les services par défaut. Les services par défaut sont visibles uniquement aux hôtes appartenant aux VLAN associés. Par défaut, le domaine de diffusion est DEFAULT VLAN.

- Pour associer un VLAN, choisissez un VLAN dans la liste déroulante **VLAN** et cliquez sur **Apply**.
- Pour dissocier les VLAN des services par défaut, cochez les cases en regard du VLAN approprié et cliquez sur **Delete**.

ÉTAPE 4 Cliquez sur **Save** pour appliquer vos paramètres.

Détection CDP

Cisco Discovery Protocol (CDP) est un protocole de détection de périphériques qui s'exécute sur tous les équipements conçus par Cisco. Chaque périphérique compatible CDP envoie des messages périodiques à une adresse de multidiffusion et écoute également les messages périodiques envoyés par d'autres afin d'en savoir plus sur les périphériques voisins et déterminer l'état de ces périphériques. Voir **Détection CDP, page 409**.

ÉTAPE 1 Cliquez sur **Device Management > Discovery Protocols > CDP**.

ÉTAPE 2 Dans la zone **CDP Configuration**, saisissez les informations suivantes :

- **Cisco Discovery Protocol (CDP)** : contrôlez si CDP fonctionne sur certaines, toutes ou aucune des interfaces Ethernet. Sélectionnez l'une des options suivantes :
  - **Enable All** : activez CDP sur tous les ports pris en charge par l'Cisco ISA500.
  - **Disable All** : désactivez CDP sur tous les ports.
  - **Per Port** : configurez CDP sur des ports sélectionnés. Nous recommandons l'option CDP per port.
- **CDP Timer** : saisissez la valeur de l'intervalle entre deux paquets CDP successifs envoyés par l'Cisco ISA500. La valeur par défaut est de 60 secondes.
- **CDP Hold Timer** : le temps de garde est le laps de temps pendant lequel les informations envoyées dans le paquet CDP doivent être mises en cache par l'Cisco ISA500 qui reçoit ce paquet CDP et à l'issue duquel les informations expirent. La valeur par défaut est de 180 secondes.

Remarque : Le champ Voice VLAN ID est en lecture seule. Vous pouvez configurer le VLAN voix sur la page Networking > VLAN. Pour obtenir plus d'informations, reportez-vous à la **Configuration d'un VLAN, page 144**.

ÉTAPE 3 Dans la zone **Enable CDP**, spécifiez quelles interfaces exécuteront CDP. Cliquez sur **On** pour activer CDP sur une interface ou sur **Off** pour désactiver CDP. Cela est nécessaire si vous choisissez **Per Port** dans la liste déroulante **CDP**.

ÉTAPE 4 Cliquez sur **Save** pour appliquer vos paramètres.

Détection LLDP

Le protocole LLDP (Link Layer Discovery Protocol) permet aux gestionnaires de réseau de dépanner et d'améliorer la gestion du réseau en détectant et en maintenant des topologies de réseau sur des environnements multi-fournisseurs. LLDP détecte les voisins du réseau en normalisant les méthodes via lesquelles les périphériques réseau se présentent à d'autres systèmes et stockent les informations détectées.

LLDP permet à un périphérique d'annoncer son ID, sa configuration et ses fonctionnalités aux périphériques voisins qui stockent les données dans une base des informations de gestion (MIB). Le système de gestion du réseau modélise la topologie du réseau en interrogeant ses bases de données MIB.

ÉTAPE 1 Cliquez sur **Device Management > Discovery Protocols > LLDP**.

ÉTAPE 2 Cliquez sur **On** pour activer le protocole LLDP ou sur **Off** pour le désactiver. Si vous activez LLDP, les voisins LLDP apparaissent dans la table des voisins LLDP.

ÉTAPE 3 Pour afficher les détails sur un voisin LLDP, cochez cette option et cliquez sur **Details**.

ÉTAPE 4 Pour actualiser les données de la table des voisins LLDP, cliquez sur **Refresh**.

ÉTAPE 5 Cliquez sur **Save** pour appliquer vos paramètres.

Gestion du microprogramme

Vous pouvez effectuer les tâches suivantes de maintenir le microprogramme :

- Afficher l'état du microprogramme. Voir **Affichage des informations sur le microprogramme, page 411**.
- Basculer vers le microprogramme secondaire via l'utilitaire de configuration. Voir **Utilisation du microprogramme secondaire, page 412**.
- Mettre à niveau votre microprogramme vers la dernière version depuis le site Cisco.com. Voir **Mise à niveau de votre microprogramme à partir du site Cisco.com, page 413**.

- Mettre à niveau votre microprogramme à partir d'une image de microprogramme se trouvant sur votre PC local ou sur un périphérique USB. Voir **Mise à niveau de votre microprogramme à partir d'une image de microprogramme stockée sur votre PC ou sur un périphérique USB, page 414**.
- Basculer automatiquement sur le microprogramme secondaire. Voir **Mécanisme de basculement automatique du microprogramme, page 415**.
- Utiliser le mode Rescue pour récupérer le système. Voir **Utilisation du mode Rescue pour récupérer le système, page 416**.

ATTENTION Lors d'une mise à niveau du microprogramme, vous ne devez EN AUCUN CAS effectuer les actions suivantes : fermer la fenêtre du navigateur, naviguer à partir de la page de mise à niveau, mettre le périphérique hors tension, arrêter le PC, retirer le câble ou interrompre le processus de quelque manière que ce soit jusqu'à ce que l'opération soit terminée. Ce processus prend normalement quelques minutes, y compris le processus de réinitialisation. L'interruption de la mise à niveau à des moments particuliers, lors de l'enregistrement de la mémoire flash, corrompt cette dernière et rend l'Cisco ISA500 inutilisable.

Affichage des informations sur le microprogramme

ÉTAPE 1 Cliquez sur **Device Management > Firmware**.

La fenêtre Firmware s'ouvre.

ÉTAPE 2 Dans la zone **Firmware Version**, les informations suivantes relatives au microprogramme s'affichent :

- **Primary Firmware Version** : version du microprogramme principal que vous utilisez.
- **Secondary Firmware Version** : version du microprogramme secondaire que vous utilisiez précédemment.

Utilisation du microprogramme secondaire

Si le microprogramme principal n'est pas stable, vous pouvez définir manuellement comme microprogramme principal le microprogramme secondaire qui était utilisé. Le microprogramme primaire initial devient alors le microprogramme secondaire. Nous vous conseillons de sauvegarder vos paramètres actuels pour une utilisation ultérieure avant de basculer sur le microprogramme secondaire.

ATTENTION N'essayez pas de commuter le microprogramme si aucune image de microprogramme secondaire n'est présente. Cela peut empêcher la réinitialisation de l'Cisco ISA500.

ÉTAPE 1 Cliquez sur **Device Management > Firmware**.

La fenêtre Firmware s'ouvre.

ÉTAPE 2 Dans la zone **Firmware Version**, cliquez sur **Switch Firmware**.

Un message d'avertissement apparaît indiquant la préparation « Preparing to reboot. Do you want to continue? WARNING : All current sessions will be closed and the system will be down for approximately 180 seconds. » (Préparation de la réinitialisation. Voulez-vous continuer? AVERTISSEMENT : toutes les sessions en cours seront fermées et le système sera arrêté pendant environ 180 secondes)

ÉTAPE 3 Cliquez sur **Yes** pour réinitialiser l'Cisco ISA500 à l'aide de l'image du microprogramme secondaire.

Mise à niveau de votre microprogramme à partir du site Cisco.com

L'Cisco ISA500 recherche automatiquement les mises à jour du microprogramme sur le site Cisco.com toutes les 24 heures. Vous pouvez mettre à niveau votre microprogramme vers la dernière version si un microprogramme plus récent est disponible sur le site Web Cisco.com. Un compte Cisco.com valide est requis pour télécharger l'image de microprogramme depuis le site Cisco.com.

REMARQUE Cette fonctionnalité nécessite une connexion WAN active.

ÉTAPE 1 Cliquez sur **Device Management > Firmware**.

La fenêtre Firmware s'ouvre.

ÉTAPE 2 Dans la zone **Upgrade Firmware**, les informations suivantes s'affichent sous la case d'option **Upgrade Firmware from Cisco.com** :

- **Your firmware is up to date** : affiche le message si vous utilisez la dernière version du microprogramme. La case d'option **Upgrade Firmware from Cisco.com** sera grisée.
- **Last checked** : affiche la date et l'heure de la dernière requête.
- **Unable to check firmware status** : affiche ce message si l'Cisco ISA500 ne peut pas accéder au serveur Cisco IDA en raison d'une connexion WAN non valide ou pour tout autre motif.
- **New Firmware Available** : affiche le numéro de version de la dernière image du microprogramme sur le serveur Cisco IDA si un microprogramme plus récent est disponible après la requête. La case d'option **Upgrade Firmware from Cisco.com** sera activée.

ÉTAPE 3 Si un microprogramme plus récent est disponible sur le site Cisco.com, sélectionnez la case d'option **Upgrade Firmware from Cisco.com**, puis effectuez l'une des actions suivantes :

- Pour mettre à niveau le microprogramme et continuer à utiliser les paramètres actuels, cliquez sur **Upgrade**.
- Pour mettre à niveau le microprogramme et restaurer les paramètres d'usine par défaut, cliquez sur **Upgrade and Factory Reset**.

ÉTAPE 4 La fenêtre Firmware Upgrade s'ouvre. Suivez les instructions affichées à l'écran pour télécharger et installer le microprogramme sur votre Cisco ISA500. Pour plus d'informations, reportez-vous à la section **Mise à niveau de votre microprogramme après votre première connexion, page 34**.

Mise à niveau de votre microprogramme à partir d'une image de microprogramme stockée sur votre PC ou sur un périphérique USB

Cette section explique comment mettre à niveau le microprogramme manuellement à partir d'une image de microprogramme se trouvant sur votre PC local ou sur un périphérique USB. Vous devez tout d'abord télécharger la dernière image du microprogramme depuis le site Cisco.com et l'enregistrer sur votre PC local ou sur un périphérique USB.

ÉTAPE 1 Cliquez sur **Device Management > Firmware**.

La fenêtre Firmware s'ouvre.

ÉTAPE 2 Pour mettre à niveau le microprogramme manuellement à partir votre PC local, procédez comme suit :

a. Dans la zone **Upgrade Firmware**, sélectionnez la case d'option **Upgrade Firmware from PC**.

b. Cliquez sur **Browse** pour localiser et sélectionner l'image du microprogramme sur votre PC local.

c. Pour mettre à niveau le microprogramme et continuer à utiliser les paramètres actuels, cliquez sur **Upgrade**.

d. Pour mettre à niveau le microprogramme et restaurer les paramètres d'usine par défaut, cliquez sur **Upgrade and Factory Reset**.

ÉTAPE 3 Pour mettre à niveau le microprogramme via un périphérique USB, procédez comme suit :

a. Insérez le périphérique USB contenant les images du microprogramme dans le port USB situé sur le panneau arrière.

b. Dans la zone **Upgrade Firmware**, sélectionnez la case d'option **Upgrade Firmware from USB**. Vérifiez que l'état du périphérique USB s'affiche sous la forme « Device Attached ». Cliquez sur **Refresh** pour actualiser l'état.

c. Dans la zone **Firmware images on USB device**, toutes les images de microprogramme qui figurent sur le périphérique USB apparaissent dans la liste. Sélectionnez une image de microprogramme dans la liste pour effectuer la mise à niveau.

d. Pour mettre à niveau le microprogramme et continuer à utiliser les paramètres actuels, cliquez sur **Upgrade**.

e. Pour mettre à niveau le microprogramme et restaurer les paramètres d'usine par défaut, cliquez sur **Upgrade and Factory Reset**.

Mécanisme de basculement automatique du microprogramme

L'Cisco ISA500 comprend deux images de microprogramme logiciel dans le même flash NAND pour fournir un mécanisme de basculement automatique du microprogramme afin que l'Cisco ISA500 puisse basculer automatiquement sur le microprogramme secondaire lorsque le microprogramme principal rencontre une erreur CRC ou ne parvient pas à démarrer correctement cinq fois.

- **CRC Error** : erreur indiquant que le microprogramme n'arrive pas à réussir la validation CRC (Cyclic Redundancy Check, Contrôle de redondance cyclique). Télécharger un microprogramme incomplet ou enregistrer incomplètement le microprogramme sur la mémoire flash peut provoquer l'erreur CRC.
- **Boot Failure** : défaillance indiquant que le microprogramme ne parvient pas réinitialiser correctement cinq fois.

Le mécanisme de basculement automatique du microprogramme fonctionne comme suit :

ÉTAPE 1 L'Cisco ISA500 s'initialise tout d'abord avec le microprogramme principal.

ÉTAPE 2 Le programme d'amorçage vérifie le CRC pour le microprogramme principal.

ÉTAPE 3 Si l'erreur CRC ou l'échec d'amorçage se produit pour le microprogramme principal, le programme d'amorçage bascule sur le microprogramme secondaire.

ÉTAPE 4 Le programme d'amorçage vérifie le CRC pour le microprogramme secondaire.

ÉTAPE 5 Si l'erreur CRC ou l'échec d'amorçage se produit pour le microprogramme secondaire, le mode Rescue s'exécute. En mode Rescue, l'Cisco ISA500 fonctionne comme un serveur TFTP. Vous pouvez utiliser un client TFTP pour charger l'image de microprogramme afin de mettre à niveau le microprogramme. Pour obtenir plus d'informations sur le mode Rescue, reportez-vous à la section **Utilisation du mode Rescue pour récupérer le système, page 416**.

Utilisation du mode Rescue pour récupérer le système

Lorsque le système a un problème d'initialisation, qu'une erreur de périphérique se produit ou que le système a un problème, le voyant POWER/SYS situé sur la façade avant est orange fixe. Procédez comme suit pour lancer le mode Rescue directement, puis récupérer le système.

ÉTAPE 1 Appuyez sur le bouton RESET situé sur le panneau arrière de l'appliance de sécurité et maintenez-le enfoncé pendant plus de 3 secondes, puis mettez simultanément l'unité sous tension.

Le mode Rescue s'exécute. La DEL Status est vert clignotant, puis devient orange fixe. En mode Rescue, l'appliance de sécurité comme un serveur TFTP.

ÉTAPE 2 Retirez tous les câbles des ports WAN et LAN.

ÉTAPE 3 Connectez votre ordinateur au port LAN.

ÉTAPE 4 Configurez votre PC avec une adresse IP statique 192.168.75.100 et un masque de sous-réseau 255.255.255.0.

ÉTAPE 5 Sur votre ordinateur, démarrez votre client TFTP, tel que tftpd32. Spécifiez l'adresse IP hôte 192.168.75.1 et transférez le fichier de microprogramme ISA500 de votre ordinateur vers l'appliance de sécurité.

L'appliance de sécurité effectuera la mise à niveau du microprogramme une fois l'image téléchargée. Ce processus prend normalement quelques minutes, y compris le processus de réinitialisation.

IMPORTANT : Lors d'une mise à niveau du microprogramme, vous ne devez en aucun cas mettre le périphérique hors tension, arrêter le PC, interrompre le processus ou retirer le câble avant que l'opération soit terminée.

Lorsque le voyant POWER/SYS sur la façade avant est vert fixe, le système fonctionne normalement.

Gestion de la licence de sécurité

Les services de sécurité sont sous licence. Une licence de sécurité valide est requise pour la prise en charge de SSLVPN avec les périphériques mobiles, tels que les téléphones intelligents et les tablettes. La clé d'autorisation de produit (PAK) et un compte Cisco.com valide sont nécessaires pour valider la licence de sécurité. Vous pouvez trouver le code de licence sur la licence imprimée fournie avec l'unité.

Utilisez la page License Management pour gérer la licence de sécurité. Reportez-vous aux rubriques suivantes :

- **Vérification de l'état de la licence de sécurité, page 417**
- **Installation ou renouvellement de la licence de sécurité, page 418**

Vérification de l'état de la licence de sécurité

Vous pouvez afficher les informations concernant la licence de sécurité, notamment la date d'expiration, les identifiants de périphérique utilisés pour renouveler la licence et les paramètres d'alerte par courriel pour les événements d'expiration de licence.

ÉTAPE 1 Cliquez sur **Device Management > License Management**.

La fenêtre License Management s'ouvre. Les informations suivantes sont affichées.

- **Feature** : nom de la licence de sécurité.
- **Status** : indique si la licence de sécurité est installée ou non. Une fois installée, la licence de sécurité ne peut être transmise, ni révoquée.
- **Expiration :** date à laquelle la licence de sécurité expire.

ÉTAPE 2 Cliquez sur **Credentials** pour afficher l'ID de produit, le numéro de série du périphérique et les identifiants de périphérique. Les identifiants de périphérique

peuvent être demandés par le service commercial ou l'assistance Cisco pour terminer ou dépanner les licences.

ÉTAPE 3 Cliquez sur **Email Alerts** pour définir ou afficher les paramètres d'alerte par courriel pour les événements d'expiration de licence.

La fenêtre Email Alerts s'ouvre. Les informations suivantes sont affichées.

- **Email Alert :** cliquez sur **On** pour activer les alertes par courriel pour l'expiration de la licence, ou cliquez sur **Off** pour désactiver cette fonctionnalité.
- **From Email Address :** adresse électronique à utiliser pour expédier les courriels d'alerte.
- **Send to Email Address :** 'adresse électronique à laquelle les alertes seront envoyées.
- **SMTP Server** : adresse IP ou nom Internet du serveur SMTP.
- **SMTP Authentication :** cliquez sur **On** pour activer l'authentification SMTP ou sur **Off** pour désactiver cette fonctionnalité.
- **Alert when it is :** saisissez un numéro pour spécifier à quel moment l'alerte sera envoyée. Par exemple, entrez 14 pour envoyer l'courriel deux semaines avant l'expiration de la licence.

ÉTAPE 4 Nous vous recommandons d'activer la fonctionnalité d'alerte avant l'expiration de la licence de manière à ce que le système puisse envoyer une alerte pour vous rappeler de renouveler la licence de sécurité avant qu'elle arrive à expiration. Cliquez sur le lien qui se trouve sur la page ou accédez à la page Device Management > Administration > Email Alert pour activer la fonctionnalité d'alerte avant l'expiration de la licence et pour configurer les paramètres du serveur de messagerie. Voir **Configuration des paramètres d'alerte par courriel, page 382**.

Installation ou renouvellement de la licence de sécurité

Cette section explique comment installer la licence de sécurité ou comment la renouveler avant qu'elle arrive à expiration. Une licence de sécurité valide est requise pour la prise en charge de SSLVPN avec les périphériques mobiles, tels que les téléphones intelligents et les tablettes.

REMARQUE Vous pouvez également valider la licence de sécurité à l'aide de l'assistant de configuration. Voir **Validation de la licence de sécurité, page 40**.

ÉTAPE 1 Contactez votre revendeur Cisco pour acheter une licence. Le numéro de série, le PID et l'UDI de votre périphérique sont requis pour faire une demande de licence. Vous trouverez ces informations sur les pages Status > Dashboard ou Device Management > License Management.

ÉTAPE 2 Connectez-vous à l'utilitaire de configuration.

ÉTAPE 3 Cliquez sur **Device Management > License Management**.

ÉTAPE 4 Pour installer la licence de sécurité, cliquez sur l'icône d'**installation**. **Autre option :** si la licence de sécurité est installée, vous pouvez cliquer sur l'icône de **renouvellement** pour renouveler la licence de sécurité avant qu'elle arrive à expiration. Choisissez le type de licence dans la liste déroulante **License Type** :

- **License Code (PAK) from Cisco.com** : récupère et installe automatiquement la licence sur l'Cisco ISA500 à partir du serveur Cisco. Si vous choisissez cette option, saisissez les informations suivantes. Ces identifiants sont requis afin que l'Cisco ISA500 s'authentifie sur le serveur Cisco.
  - **License Code :** entrez le code de licence (PAK).
  - **Cisco.com Login :** saisissez le nom d'utilisateur de votre compte Cisco.com.
  - **Cisco.com Password :** entrez le mot de passe de votre compte Cisco.com.
  - **Email Address :** saisissez l'adresse courriel enregistrée pour recevoir le PAK.
- **License File download from Cisco.com** : installe une licence de sécurité qui a été précédemment téléchargée sur votre PC. Si vous sélectionnez cette option, cliquez sur **Browse** pour localiser et sélectionnez le fichier de licence de votre PC.

  REMARQUE : Vérifiez que l'Cisco ISA500 est réglé sur l'heure actuelle, sinon la licence ne sera pas correctement installée. Voir **Configuration de l'heure système, page 402**.

ÉTAPE 5 Cochez la case **Click here if you accept with SEULA** pour accepter les conditions du contrat de licence logicielle de l'utilisateur final (SEULA). Vous

pouvez cliquer sur le lien **SEULA** pour consulter les conditions détaillées du contrat de licence logicielle de l'utilisateur final sur le site Cisco.com.

ÉTAPE 6 Cliquez sur **Validate License** pour valider la licence de sécurité sur votre Cisco ISA500.

Une fois la licence installée ou renouvelée, la date d'expiration de la licence de sécurité est mise à jour immédiatement. Les services de sécurité sont activés par la licence de sécurité.

Gestion des journaux

Vous pouvez configurer les journaux pour différents événements se produisant sur votre réseau. Les journaux d'événements peuvent être utilisés pour le suivi des risques de sécurité potentiels. Différents événements peuvent être capturés et consignés pour vérification. Ces journaux peuvent être enregistrés dans le daemon syslog local ou sur un serveur syslog distant spécifié, ou être envoyés par courrier électronique à une adresse courriel spécifiée.

Cette section explique comment afficher les journaux d'événements et configurer les paramètres et les composants journaux. Reportez-vous aux rubriques suivantes :

- **Affichage des journaux, page 421**
- **Configuration des paramètres de journal, page 423**
- **Configuration des composants journaux, page 426**

Affichage des journaux

Utilisez la page View Logs pour afficher les journaux afin de consulter un niveau de gravité, un composant journaux ou une adresse IP source et/ou de destination spécifique, ou pour rechercher les journaux par mot clé.

REMARQUE Veillez à activer la fonctionnalité de fichier journal local avant d'afficher les fichiers journaux. Voir **Configuration des paramètres de journal, page 423**.

ÉTAPE 1 Cliquez sur **Device Management > Logs > View Logs**.

ÉTAPE 2 Spécifiez les journaux à afficher :

- **Log Severity** : sélectionnez le niveau de gravité pour le filtrage des journaux. Par exemple : si vous sélectionnez « Critical », tous les journaux répertoriés sous les catégories « Critical », « Emergency » et « Alert » sont affichés.
- **Log Facility** : choisissez le composant pour le filtrage des journaux. Tous les journaux qui appartiennent au composant sélectionné et qui correspondent aux paramètres de gravité spécifiés sont affichés.
- **Keyword** : entrez le mot clé pour la recherche dans les fichiers journaux. Tous les journaux qui contiennent le mot clé spécifié sont affichés.

- **Source IP Address** : saisissez l'adresse IP source pour le filtrage des journaux du pare-feu. Tous les journaux du pare-feu qui correspondent à cette adresse IP source sont affichés.
- **Destination IP Address :** entrez l'adresse IP de destination pour le filtrage des journaux du pare-feu. Tous les journaux du pare-feu qui correspondent à cette adresse IP de destination sont affichés.

ÉTAPE 3 Cliquez sur **Query**.

Les résultats de la requête apparaissent dans la table **Logs**. Les informations suivantes sont affichées.

- **Date** : date de l'événement.
- **Severity** : niveau de gravité de l'événement.
- **Facility** : type de composant journaux.
- **Log Data** : brève description de l'événement.
- **Source IP Address** : adresse IP source de l'événement du pare-feu.
- **Destination IP Address** : adresse IP de destination de l'événement du pare-feu.

ÉTAPE 4 Vous pouvez également effectuer les actions suivantes :

- Trier les entrées de journal. Les journaux peuvent être triés en cliquant sur l'en-tête de colonne. Par défaut, les journaux sont triés par date et heure, dans l'ordre décroissant. Par exemple, si vous cliquez sur **Severity**, les journaux sont triés par niveau de gravité dans l'ordre croissant. Si vous cliquez deux fois sur **Severity**, les journaux sont triés par niveau de gravité, dans l'ordre décroissant.
- Parcourir les entrées du journal. Lorsque vous affichez un grand nombre de journaux, vous pouvez préciser combien de journaux s'affichent dans le tableau par page, ou vous pouvez parcourir ces journaux en utilisant les boutons de navigation si une page ne peut pas afficher tous les journaux.
- Cliquez sur **Clear** pour nettoyer tous les journaux qui sont enregistrés dans le daemon syslog local.
- Cliquez sur **Refresh** pour actualiser les données du journal.
- Cliquez sur **Export** pour exporter les journaux vers une destination définie pour le débogage.

Configuration des paramètres de journal

Utilisez la page Log Settings pour activer la fonctionnalité de fichier journal et pour configurer les paramètres de journal. Vous pouvez définir la taille de la mémoire tampon des journaux, enregistrer tout le trafic de monodiffusion ou le trafic de diffusion acheminé vers votre périphérique à des fins de dépannage, spécifier quels messages syslog seront envoyés à une adresse courriel indiquée selon une programmation et définir le niveau de gravité des événements qui sont consignés. Si vous disposez d'une assistance de serveur syslog à distance, vous pouvez enregistrer des journaux sur le serveur syslog distant.

ÉTAPE 1 Cliquez sur **Device Management > Logs > Log Settings**.

ÉTAPE 2 Dans la zone **Log Settings**, saisissez les informations suivantes :

- **Log :** cliquez sur **On** pour activer la fonctionnalité de fichier journal ou sur **Off** pour la désactiver.
- **Log Buffer :** si vous activez la fonctionnalité de fichier journal, indiquez la taille du tampon de journal local. La valeur par défaut est de 409 600 octets.

  REMARQUE : Une fois que vous avez activé la fonctionnalité de fichier journal et défini la taille de la mémoire tampon des journaux, indiquez le niveau de gravité des événements que vous souhaitez enregistrer. Ces journaux seront enregistrés dans le daemon de journal local. Voir **Étape 7**.

ÉTAPE 3 Dans la zone **System Logs,** si vous souhaitez surveiller l'Cisco ISA500 avec plus de données de trafic, vous pouvez choisir d'enregistrer tout le trafic de monodiffusion et/ou tout le trafic de diffusion ou multidiffusion dirigé vers votre Cisco ISA500 en vue de dépannage. Les journaux pour le trafic de monodiffusion et le trafic de diffusion ou de multidiffusion se trouvent au niveau de gravité Information.

- **Unicast Traffic :** cliquez sur **On** pour enregistrer tous les paquets de monodiffusion dirigé vers l'Cisco ISA500. Le trafic de monodiffusion de tous les composants sera consigné, quel que soit le trafic interne ou externe.
- **Broadcast/Multicast Traffic :** cliquez sur **On** pour enregistrer tous les paquets diffusion ou multidiffusion dirigés vers l'Cisco ISA500. Le trafic de diffusion ou de multidiffusion de tous les composants sera consigné, quel que soit le trafic interne ou externe.

  Si aucune des deux options n'est sélectionnée, l'Cisco ISA500 enregistre uniquement les événements basés sur les paramètres de votre composant. Les composants journaux sont utilisés pour la consignation d'événements intéressants, tels que l'association de clients, le blocage de paquets par les règles de pare-feu, la détection de virus le service d'antivirus, etc.

ÉTAPE 4 Dans la zone **Email Server**, précisez quels messages syslog doivent être envoyés à une adresse courriel indiquée suivant une programmation.

- **Email Alert** : indique si la fonctionnalité courriel Syslog est activée ou désactivée.
- **From Email Address** : adresse courriel utilisée pour envoyer les journaux.
- **From Email Address** : adresse courriel utilisée pour envoyer les journaux.
- **SMTP Server** : adresse IP ou nom Internet du serveur SMTP.
- **SMTP Authentication :** indique si l'authentification SMTP est activée ou désactivée.

  REMARQUE : Les paramètres du serveur de messagerie mentionnés ci-dessus sont en lecture seule. Vous devez activer la fonctionnalité courriel Syslog et configurer les paramètres du serveur de messagerie pour envoyer les messages syslog à une adresse courriel spécifiée. Pour cela, vous pouvez soit cliquer sur le lien **Set Email Alert**, soit accéder à la page Device Management > Administration > Email Alert. Voir **Configuration des paramètres d'alerte par courriel, page 382**.
- **Mail Subtitle :** entrez le sous-titre qui s'affiche dans le courriel. Par exemple, si vous définissez le nom du périphérique comme sous-titre, le destinataire du courriel peut identifier rapidement de quel périphérique proviennent les fichiers journaux ou les alertes.
- **Severity** : sélectionnez le niveau de gravité des fichiers journaux que vous souhaitez envoyer.

Niveau de gravité	Description
Emergency (niveau 0, gravité la plus élevée)	Système inutilisable.
Alert (niveau 1)	Intervention immédiate requise.
Critical (niveau 2)	Conditions critiques.
Error (niveau 3)	Conditions d'erreur.
Warning (niveau 4)	Avertissements.
Notification (niveau 5)	Événements normaux, mais importants.
Information (niveau 6)	Message d'information uniquement.

Niveau de gravité	Description
Debug (niveau 7, la gravité la plus faible)	Messages de débogage.

Par exemple : si vous sélectionnez « Critical », tous les journaux répertoriés sous les catégories « Critical », « Emergency » et « Alert » sont envoyés.

ÉTAPE 5 Dans la zone **Email Schedule**, spécifiez la programmation de l'envoi des journaux.

- **Frequency :** sélectionnez la fréquence d'envoi des journaux.
  - **Hourly :** permet l'envoi des journaux toutes les heures.
  - **Daily :** permet l'envoi des journaux tous les jours. Si vous choisissez cette option, spécifiez l'heure d'envoi dans le champ **Time**.
  - **Weekly** : permet l'envoi des journaux toutes les semaines. Si vous choisissez cette option, spécifiez le jour de la semaine dans le champ **Day** et l'heure dans le champ **Time**.
- **Day :** si les fichiers journaux sont envoyés toutes les semaines, choisissez le jour de la semaine
- **Time** : choisissez l'heure à laquelle les journaux doivent être envoyés.

ÉTAPE 6 Dans la zone **Remote Logs**, spécifiez comment enregistrer les journaux sur un serveur syslog distant.

- **Remote Logs :** cliquez sur **On** pour enregistrer les journaux sur le serveur syslog distant spécifié ou sur **Off** pour désactivez l'option.
- **Syslog Server :** entrez l'adresse IP ou le nom de domaine du serveur syslog distant exécutant un démon syslog.
- **Severity** : sélectionnez le niveau de gravité des journaux que vous voulez enregistrer sur le serveur syslog distant.

  Par exemple : si vous sélectionnez « Critical », les journaux répertoriés dans les catégories « Critical », « Emergency » et « Alert » sont enregistrées sur le serveur syslog distant.

ÉTAPE 7 Dans la zone **Local Log**, sélectionnez le niveau de gravité pour les événements que vous souhaitez enregistrer. Les journaux seront enregistrés dans le daemon syslog local.

Par exemple : si vous sélectionnez « Critical », les messages de journal répertoriés dans les catégories « Critical », « Emergency » et « Alert » sont enregistrées sur le démon syslog local.

ÉTAPE 8 Cliquez sur **Save** pour appliquer vos paramètres.

REMARQUE Étapes suivantes :

- Pour spécifier les messages système devant être consignés en fonction du composant, accédez à la page Log Facilities. Voir **Configuration des composants journaux, page 426**.
- (Facultatif) Pour activer la fonctionnalité courriel Syslog et configurer les paramètres du serveur de messagerie pour envoyer les messages syslog à une adresse courriel spécifiée, accédez à la page Device Management > Administration > Email Alert. Voir **Configuration des paramètres d'alerte par courriel, page 382**.

Configuration des composants journaux

Utilisez la page Log Facilities pour spécifier les messages système devant être consignés en fonction du composant, déterminer où enregistrer les messages syslog et indiquer s'il faut les envoyer à une adresse courriel selon une programmation.

REMARQUE Avant de configurer les composants journaux, veillez à activer la fonctionnalité de fichier journal, définissez la taille de la mémoire tampon du journal et spécifiez les paramètres « Email Alert », « Remote Log » et « Local Log ». Voir **Configuration des paramètres de journal, page 423**.

ÉTAPE 1 Cliquez sur **Device Management > Logs > Logs Facilities**.

La fenêtre Log Facilities s'ouvre. Tous les composants pris en charge sont répertoriés dans le tableau.

ÉTAPE 2 Indiquez les informations suivantes :

- **Email Alert :** cochez l'option **Email Alert** pour activer les paramètres d'alerte par courriel pour tous les composants ou cochez la case correspondant à un composant spécifique pour activer les paramètres d'alerte par courriel pour le composant sélectionné.

  Les événements qui appartiennent au composant sélectionné et qui correspondent au niveau de gravité spécifié pour les courriels Syslog sont consignés et les messages syslog enregistrés sont envoyés à l'adresse courriel spécifiée selon une programmation.

- **Remote Log :** cochez l'option **Remote Log** pour activer les paramètres de journal à distance pour tous les composants, ou cochez la case correspondant à un composant spécifique pour activer les paramètres de journal à distance pour le composant sélectionné.

  Les événements qui appartiennent aux composants sélectionnés et qui correspondent au niveau de gravité spécifié pour les journaux à distance sont consignés et les messages syslog enregistrés sont sauvegardés sur le serveur syslog distant spécifié.

- **Local Log** : cochez l'option **Local Log** pour activer les paramètres de journal local pour tous les composants, ou cochez la case correspondant à un composant spécifique pour activer les paramètres de journal local pour le composant sélectionné.

  Les événements qui appartiennent aux composants sélectionnés et qui correspondent au niveau de gravité spécifié pour le journal local sont consignés et les messages syslog enregistrés sont sauvegardés sur le daemon syslog local.

  REMARQUE : Pour obtenir des informations sur la configuration des paramètres Email Alert, Remote Log et Local Log à distance, reportez-vous à la section **Configuration des paramètres de journal, page 423**.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Réamorçage et réinitialisation du périphérique

Utilisez la page Reboot/Reset pour réamorcer l'Cisco ISA500 ou pour réinitialiser les paramètres d'usine par défaut de l'Cisco ISA500 (s'il y a lieu) depuis l'utilitaire de configuration. Reportez-vous aux rubriques suivantes :

- **Restauration des paramètres par défaut définis en usine, page 427**
- **Réinitialisation de l'appareil de sécurité, page 428**

Restauration des paramètres par défaut définis en usine

Pour restaurer les paramètres d'usine par défaut de l'Cisco ISA500, vous pouvez appuyer sur le bouton **RESET** situé sur le panneau arrière pendant plus de 3 secondes ou effectuer l'opération **Reset to Factory Defaults** depuis l'utilitaire de configuration.

ATTENTION La réinitialisation des paramètres d'usine par défaut éliminera les paramètres actuellement utilisés sur l'Cisco ISA500 (y compris les certificats importés). Nous vous conseillons de sauvegarder vos paramètres actuels avant de restaurer les paramètres d'usine par défaut.

ÉTAPE 1 Cliquez sur **Device Management > Reboot/Reset**.

La fenêtre Reboot/Reset s'ouvre.

ÉTAPE 2 Dans la zone **Reset Device**, cliquez sur **Reset to Factory Defaults**.

Le message d'avertissement suivant s'affiche : « Preparing to restore the factory default settings. Do you want to continue? WARNING : The current configuration will be overwritten » (Préparation de la restauration des paramètres d'usine par défaut. Voulez-vous continuer? AVERTISSEMENT : la configuration actuelle sera remplacée).

ÉTAPE 3 Cliquez sur **Yes** pour réamorcer l'Cisco ISA500 avec les paramètres d'usine par défaut.

Réinitialisation de l'appareil de sécurité

Pour réinitialiser l'Cisco ISA500, vous pouvez appuyez sur le bouton **RESET** situé sur le panneau arrière pendant moins de 3 secondes ou effectuer l'opération **Reboot** depuis l'utilitaire de configuration.

ÉTAPE 1 Cliquez sur **Device Management > Reboot/Reset**.

La fenêtre Reboot/Reset s'ouvre.

ÉTAPE 2 Dans la zone **Reboot Device**, cliquez sur **Reboot**.

Un message d'avertissement apparaît indiquant la préparation « Preparing to reboot. Do you want to continue? WARNING : All current sessions will be closed and the system will be down for approximately 180 seconds. » (Préparation de la réinitialisation. Voulez-vous continuer? AVERTISSEMENT : toutes les sessions en cours seront fermées et le système sera arrêté pendant environ 180 secondes)

ÉTAPE 3 Cliquez sur **Yes** pour réinitialiser l'Cisco ISA500.

Configuration des programmations

La programmation indique quand la règle de pare-feu ou la stratégie de contrôle des applications sont actives. Par exemple, si vous souhaitez qu'une règle de pare-feu fonctionne uniquement le week-end, vous pouvez créer une programmation appelée « Weekend » qui sera active uniquement le samedi et le dimanche.

ÉTAPE 1 Cliquez sur **Device Management > Schedules**.

La fenêtre Schedules s'ouvre.

ÉTAPE 2 Pour créer une programmation, cliquez sur **Add**.

Autres options : pour modifier une entrée, cliquez sur l'icône de **modification** (crayon). Pour supprimer une entrée, cliquez sur l'icône de **suppression** (x). Pour supprimer plusieurs entrées, cochez-les et cliquez sur **Delete**.

La fenêtre Schedule - Add/Edit s'ouvre.

ÉTAPE 3 Saisissez les informations suivantes :

- **Schedule Name** : entrez le nom de la programmation.
- **Schedule Days** : planifie la règle de pare-feu ou la stratégie de contrôle des applications (tous les jours ou certains jours uniquement).
  - **All Days** : sélectionnez cette option si vous souhaitez que la règle de pare-feu ou la stratégie de contrôle des applications reste active en permanence.
  - **Specific Days** : sélectionnez cette option, puis cochez les jours pendant lesquels vous souhaitez que la règle de pare-feu ou la stratégie de contrôle des applications reste active.
- **Schedule Time** : planifie la règle de pare-feu ou la stratégie de contrôle des applications (tous les jours ou à un moment précis de la journée).
  - **All Days** : sélectionnez cette option si vous souhaitez que la règle de pare-feu ou la stratégie de contrôle des applications reste active en permanence.
  - **Specific Times :** sélectionnez cette option si vous souhaitez que la règle de pare-feu ou la stratégie de contrôle des applications reste active à certaines heures spécifiques. Définissez les options **Start Time** (heure de début) et **End Time** (heure de fin) en entrant les heures et minutes et en choisissant AM (matin) ou PM (après-midi).

ÉTAPE 4 Cliquez sur **OK** pour enregistrer vos paramètres.

ÉTAPE 5 Cliquez sur **Save** pour appliquer vos paramètres.

A

Dépannage

Ce chapitre explique comment résoudre certains problèmes courants que vous pouvez rencontrer lors de l'utilisation de l'Cisco ISA500. Il comprend les sections suivantes :

- **Connexion Internet, page 431**
- **Date et heure, page 434**
- **Test ping pour tester la connectivité LAN, page 435**

Connexion Internet

Symptôme : Vous ne pouvez pas accéder à l'utilitaire de configuration à partir d'un PC sur votre réseau LAN.

Actions recommandées :

ÉTAPE 1 Vérifiez la connexion Ethernet entre le PC et l'Cisco ISA500.

ÉTAPE 2 Assurez-vous que l'adresse IP de votre PC se trouve sur le même sous-réseau que l'Cisco ISA500. Si vous utilisez le schéma d'adressage recommandé, l'adresse de votre PC doit être comprise entre 192.168.75.100 et 192.168.75.200.

ÉTAPE 3 Vérifiez l'adresse IP de votre PC. Si le PC ne peut pas accéder à un serveur DHCP, certaines versions de Windows et de MacOS génèrent et attribuent une adresse IP. Ces adresses sont générées automatiquement dans la plage 169.254.x.x. Si votre adresse IP se trouve dans cette plage, vérifiez la connexion du PC à l'Cisco ISA500 et redémarrez votre PC.

ÉTAPE 4 Si votre adresse IP a changé et que vous ne la connaissez pas, réinitialisez l'Cisco ISA500 aux paramètres d'usine par défaut.

Si vous ne souhaitez pas rétablir les paramètres d'usine par défaut et perdre votre configuration, redémarrez l'Cisco ISA500 et utilisez un outil de surveillance des paquets (par exemple Ethereal™) pour capturer les paquets envoyés au cours du redémarrage. Regardez les paquets ARP pour localiser l'adresse d'interface LAN.

ÉTAPE 5 Lancez le navigateur Web et vérifiez que Java, JavaScript ou ActiveX est activé. Si vous utilisez Internet Explorer, cliquez sur **Actualiser** pour vous assurer que l'applet Java est chargé. Fermez le navigateur et relancez-le.

ÉTAPE 6 Vérifiez que vous utilisez les informations de connexion appropriées. Le nom de connexion par défaut est « cisco » et le mot de passe est « cisco ». Vérifiez que VERR. MAJ est désactivé lorsque vous saisissez ces informations.

Symptôme : L'Cisco ISA500 n'enregistre pas mes modifications de configuration.

Actions recommandées :

ÉTAPE 1 Lorsque vous entrez des paramètres de configuration, cliquez sur **OK** ou sur **Save** avant de passer à une autre page ou à un autre onglet ; sinon, vos modifications sont perdues.

ÉTAPE 2 Cliquez sur **Actualiser** ou **Recharger** dans le navigateur, ce qui effacera une copie de l'ancienne configuration dans le cache.

Symptôme : L'Cisco ISA500 ne parvient pas à accéder à Internet.

Cause possible : Si vous utilisez des adresses IP dynamiques, votre Cisco ISA500 ne demande pas d'adresse IP au FAI.

Actions recommandées :

ÉTAPE 1 Lancez le navigateur et vérifiez si vous pouvez vous connecter à un site externe tel que www.cisco.com.

ÉTAPE 2 Lancez l'utilitaire de configuration et connectez-vous.

ÉTAPE 3 Cliquez sur **Status > Dashboard**.

ÉTAPE 4 Dans la zone **WAN Interface(s)**, recherchez l'adresse WAN1. Si 0.0.0.0 est affiché, votre Cisco ISA500 n'a pas obtenu d'adresse IP de votre FAI. Reportez-vous au symptôme suivant.

Symptôme : L'Cisco ISA500 ne parvient pas à obtenir une adresse IP du FAI.

Actions recommandées :

ÉTAPE 1 Mettez hors tension le câble ou le modem DSL.

ÉTAPE 2 Mettez la plate-forme Cisco ISA500 hors tension.

ÉTAPE 3 Rétablissez l'alimentation du câble ou du modem DSL.

ÉTAPE 4 Lorsque les voyants du modem indiquent qu'il est resynchronisé avec le FAI, rétablissez l'alimentation de l'Cisco ISA500. Si l'Cisco ISA500 ne peut toujours pas obtenir d'adresse d'ISP, reportez-vous au symptôme suivant.

Symptôme : L'Cisco ISA500 ne parvient toujours pas à obtenir une adresse IP du FAI.

Actions recommandées :

ÉTAPE 1 Cliquez sur **Networking > WAN > WAN Settings**.

ÉTAPE 2 Cliquez sur l'icône de **modification** (crayon) pour configurer le port WAN principal.

La fenêtre WAN - Add/Edit s'ouvre.

ÉTAPE 3 Posez les questions suivantes à votre FAI :

- Quel type de mode d'adressage réseau est nécessaire pour votre connexion internet ? Dans l'onglet **IPv4**, sélectionnez la connexion FAI adéquate dans la liste déroulante **IP Address Assignment**, puis entrez les informations de compte spécifiées par le FAI.
- Votre FAI s'attend-il à ce que vous vous connectiez à partir d'une adresse MAC Ethernet particulière ? Si oui, dans l'onglet **IPv4**, sélectionnez **Use the following MAC address** dans la liste déroulante **MAC Address Source**, puis saisissez l'adresse MAC requise dans le champ **MAC Address**.

Symptôme : L'Cisco ISA500 peut obtenir une adresse IP, mais le PC ne parvient pas à charger les pages Internet.

Actions recommandées :

ÉTAPE 1 Demandez à votre FAI les adresses de ses serveurs DNS désignés. Configurez votre PC pour qu'il identifie ces adresses. Pour plus de détails, reportez-vous à la documentation de votre système d'exploitation.

ÉTAPE 2 Sur votre PC, configurez l'Cisco ISA500 en tant que passerelle TCP/IP.

Date et heure

Symptôme : La date affichée est le 1er janvier 2000.

Cause possible : L'Cisco ISA500 n'a pas encore pu atteindre de serveur NTS (Network Time Server).

Actions recommandées :

ÉTAPE 1 Si vous venez de configurer l'Cisco ISA500, cliquez sur **Device Management > Date and Time**.

ÉTAPE 2 Passez en revue les paramètres de date et heure.

ÉTAPE 3 Vérifiez vos paramètres d'accès à Internet.

Symptôme : L'heure de l'appareil retarde d'une heure.

Cause possible : L'Cisco ISA500 ne se règle pas automatiquement sur l'heure d'été.

Actions recommandées :

ÉTAPE 1 Cliquez sur **Device Management > Date and Time**.

ÉTAPE 2 Activez la fonctionnalité **Daylight Saving Time Adjustment**.

ÉTAPE 3 Cliquez sur **Save** pour appliquer vos paramètres.

Test ping pour tester la connectivité LAN

L'Cisco ISA500 et la plupart des périphériques de terminal TCP/IP contiennent un utilitaire de ping qui envoie un paquet de demande d'écho ICMP au périphérique désigné. Le périphérique répond par un écho. Le dépannage d'un réseau TCP/IP est grandement facilité par l'utilitaire de ping de votre PC ou station de travail.

Cette section comprend les rubriques suivantes :

- **Évaluation du chemin LAN de votre PC à votre appareil de sécurité, page 435**
- **Évaluation du chemin LAN de votre PC à un périphérique distant, page 436**

Évaluation du chemin LAN de votre PC à votre appareil de sécurité

ÉTAPE 1 Sur votre PC, cliquez sur le bouton **Démarrer** de Windows, puis cliquez sur **Exécuter**.

ÉTAPE 2 Saisissez ping <IP_address>, <IP_address> étant l'adresse IP de l'Cisco ISA500. Exemple : ping 192.168.75.1.

ÉTAPE 3 Cliquez sur **OK**.

ÉTAPE 4 Observez le résultat qui s'affiche :

- Si le chemin fonctionne, cette séquence de message s'affiche :
```
Pinging <IP address> with 32 bytes of data
Reply from <IP address>: bytes=32 time=NN ms TTL=xxx
```
- Si le chemin ne fonctionne pas, cette séquence de message s'affiche :
```
Pinging <IP address> with 32 bytes of data
Request timed out
```
- Si le chemin ne fonctionne pas, vérifiez les connexions physiques entre le PC et l'Cisco ISA500. Si le voyant du port LAN est éteint, vérifiez que les voyants de liaison correspondants sont allumés pour votre carte d'interface réseau et pour tous les ports du concentrateur qui sont connectés à votre station de travail et à l'Cisco ISA500.

- Si le chemin n'est toujours pas actif, testez la configuration réseau.
  - Vérifiez que le logiciel du pilote de carte Ethernet et le logiciel TCP/IP sont installés et configurés sur le PC.
  - Assurez-vous que les adresses IP de l'Cisco ISA500 et du PC sont correctes et se trouvent sur le même sous-réseau.

Évaluation du chemin LAN de votre PC à un périphérique distant

ÉTAPE 1 Sur votre PC, cliquez sur le bouton **Démarrer** de Windows, puis cliquez sur **Exécuter**.

ÉTAPE 2 Saisissez ping -n10 <IP_address>, où -n10 spécifie un maximum de 10 essais et <IP address> est l'adresse IP d'un périphérique distant, par exemple le serveur DNS de votre FAI. Exemple : ping -n 10 10.1.1.1.

ÉTAPE 3 Cliquez sur **OK** puis observez le résultat qui s'affiche (reportez-vous à la procédure précédente).

ÉTAPE 4 Si le chemin ne fonctionne pas, effectuez les tâches suivantes :

- Vérifiez que l'adresse IP de votre Cisco ISA500 est répertoriée comme passerelle par défaut. (Si la configuration IP de votre PC est attribuée par DHCP, ces informations ne sont pas visibles dans le panneau de configuration réseau de votre PC.)
- Vérifiez que l'adresse réseau (sous-réseau) de votre PC est différente de l'adresse réseau du périphérique distant.
- Vérifiez que le câble ou le modem DSL est connecté et fonctionne.
- Contactez votre FAI et posez-lui les questions répertoriées dans **L'Cisco ISA500 ne parvient pas à obtenir une adresse IP du FAI.**
- Demandez à votre FAI s'il rejette les adresses MAC Ethernet de tous vos ordinateurs sauf un. De nombreux FAI de haut débit limitent l'accès en acceptant le trafic uniquement de l'adresse MAC de votre modem haut débit. Certains FAI restreignent encore l'accès à l'adresse MAC d'un seul PC connecté à ce modem. Dans ce cas, configurez votre Cisco ISA500 pour cloner ou usurper l'adresse MAC du PC autorisé. Voir **Configuration des paramètres du WAN pour votre connexion internet, page 128**.

B

Spécifications techniques et exigences environnementales

Le tableau suivant présente les spécifications techniques et les exigences environnementales de l'Cisco ISA500.

Fonctionnalité	ISA550	ISA550W	ISA570	ISA570W
Interfaces physiques	2 connecteurs RJ-45 pour les ports LAN 1 connecteur RJ-45 pour le port WAN 4 connecteurs RJ-45 pour les ports LAN, WAN ou DMZ 1 connecteur USB pour USB 2.0 1 commutateur d'alimentation	2 connecteurs RJ-45 pour les ports LAN 1 connecteur RJ-45 pour le port WAN 4 connecteurs RJ-45 pour les ports LAN, WAN ou DMZ 1 connecteur USB pour USB 2.0 1 commutateur d'alimentation 2 antennes externes	4 connecteurs RJ-45 pour les ports LAN 1 connecteur RJ-45 pour le port WAN 5 connecteurs RJ-45 pour les ports LAN, WAN ou DMZ 1 connecteur USB pour USB 2.0 1 commutateur d'alimentation	4 connecteurs RJ-45 pour les ports LAN 1 connecteur RJ-45 pour le port WAN 5 connecteurs RJ-45 pour les ports LAN, WAN ou DMZ 1 connecteur USB pour USB 2.0 1 commutateur d'alimentation 2 antennes externes
Température de fonctionnement	De 0 °C à 40 °C	De 0 °C à 40 °C	De 0 °C à 40 °C	De 0 °C à 40 °C
Température de stockage	De -20 °C à 70 °C (-4 °F à 158 °F)	De -20 °C à 70 °C (-4 °F à 158 °F)	De -20 °C à 70 °C (de -4 °F à 158 °F)	De -20 °C à 70 °C (-4 °F à 158 °F)
Humidité de fonctionnement	Humidité relative de 10 à 90 %, sans condensation	Humidité relative de 10 à 90 %, sans condensation	Humidité relative de 10 à 90 %, sans condensation	Humidité relative de 10 à 90 %, sans condensation

Fonctionnalité	ISA550	ISA550W	ISA570	ISA570W
Humidité de stockage	Humidité relative de 5 à 95 %, sans condensation	Humidité relative de 5 à 95 %, sans condensation	Humidité relative de 5 à 95 %, sans condensation	Humidité relative de 5 à 95 %, sans condensation
Alimentation électrique interne				
Gamme de tensions	Tension normale : 100 à 240 V CA Plage de variation de tension : 90 à 264 V CA	Tension normale : 100 à 240 V CA Plage de variation de tension : 90 à 264 V CA	Tension normale : 100 à 240 V CA Plage de variation de tension : 90 à 264 V CA	Tension normale : 100 à 240 V CA Plage de variation de tension : 90 à 264 V CA
Plage de fréquence d'entrée	Fréquence normale : 50 à 60 Hz Plage de variation de fréquence : 47 Hz à 63 Hz	Fréquence normale : 50 à 60 Hz Plage de variation de fréquence : 47 Hz à 63 Hz	Fréquence normale : 50 à 60 Hz Plage de variation de fréquence : 47 Hz à 63 Hz	Fréquence normale : 50 à 60 Hz Plage de variation de fréquence : 47 Hz à 63 Hz
Régulation de la tension de sortie	11,4 à 12,6 V	11,4 à 12,6 V	11,4 à 12,6 V	11,4 à 12,6 V
Courant en sortie	2,5 A max.	2,5 A max.	1,667 A max.	1,667 A max.
Caractéristiques physiques				
Format	1 RU, montage sur bâti de 19 pouces	1 RU, montage sur bâti de 19 pouces	1 RU, montage sur bâti de 19 pouces	1 RU, montage sur bâti de 19 pouces
Dimensions (H x L x P)	44 x 308 x 185,5 mm (1,73 x 12,1 x 7,30 pouces)	44 x 308 x 185,5 mm (1,73 x 12,1 x 7,30 pouces) Les antennes ajoutent environ 31,6 mm (1,24 pouces) de profondeur.	44 x 308 x 185,5 mm (1,73 x 12,1 x 7,30 pouces)	44 x 308 x 185,5 mm (1,73 x 12,1 x 7,30 pouces) Les antennes ajoutent environ 31,6 mm (1,24 pouces) de profondeur.
Poids (avec alimentation électrique)	1,20 kg (3,22 livres)	1,26 kg (3,38 livres)	1,3 kg (3,48 livres)	1,36 kg (3,64 livres)

C

Paramètres d'usine par défaut

Ce chapitre décrit les paramètres d'usine par défaut des principales fonctionnalités et fournit les listes d'objets d'adresse et de service prédéfinis. Il comprend les sections suivantes :

- Gestion des périphériques, page 439
- Gestion des utilisateurs, page 441
- Mise en réseau, page 442
- Sans fil, page 445
- VPN, page 446
- Services de sécurité, page 448
- Pare-feu, page 449
- Rapports, page 450
- Objets de services par défaut, page 451
- Objets d'adresse par défaut, page 455

Gestion des périphériques

Fonctionnalité	Paramètre
Remote Administration	Désactiver
Remote management using HTTPS	Désactiver
Access type	All IP addresses
HTTPS listen port number	8080

Fonctionnalité	Paramètre
Remote management using HTTP	Désactiver
HTTP listen port number	80
Remote SNMP	Désactiver
User Session Settings	
Inactivity timeout	15 minutes (0 to 1000 minutes)
Limit login session for web logins	Désactiver
Login session limit	10 minutes (0 to 1000 minutes)
SNMP	Désactiver
SNMP Versions	SNMP versions 1 et 2, SNMP version 3
Maximum number of certificates	128
Remote Support	Désactiver
Cisco OnPlus	Activer
Send Diagnostics	Désactiver
Date and Time	Dynamically set system time
Daylight saving time adjustment	Désactiver
Default NTP servers	Activer
Host Name	« routeur » et les trois premiers octets de l'adresse MAC
UPnP	Désactiver
Bonjour	Activer
CDP	Désactiver
LLDP	Désactiver
Syslog Settings	Désactiver
Email Alert Settings	
CPU Overload Alert	Désactiver
CPU threshold setting	90 % (10 à 100 %)
New Firmware Alert	Désactiver

Fonctionnalité	Paramètre
License Expiration Alert	Désactiver
Alert before the license expires	15 jours
Syslog Email	Désactiver
Site-to-Site VPN Up/Down Alert	Désactiver
WAN Up/Down Alert	Désactiver
WAN Up/Down alert interval	5 minutes (3 to 1440 minutes)
Traffic Meter Alert	Désactiver
Anti-Virus Alert	Désactiver
Anti-Virus alert interval	30 minutes (de 1 à 1440 minutes)
IPS Alert	Désactiver
Web URL Filtering Alert	Désactiver

Gestion des utilisateurs

Fonctionnalité	Paramètre
User Groups (groupes d'utilisateurs)	
Default administrator user group	admin
Services disponibles pour les groupes d'utilisateurs	Web Login, SSL VPN, IPsec Remote Access et Captive Portal (pour ISA550W et ISA570W uniquement)
Maximum number of user groups	50
Utilisateurs locaux	
Default administrator username	cisco
Default administrator password	cisco
Maximum number of local users	100

Fonctionnalité	Paramètre
User Authentication Methods	Local Database (par défaut) RADIUS RADIUS+Local Database LDAP LDAP+Local Database

Mise en réseau

Fonctionnalité	Paramètre
IPv4 or IPv6 Routing	IPv4 only
WAN Interfaces	
Maximum number of WAN interfaces	2
WAN1-Physical Port	GE1
WAN1-IP Address Assignment	Client DHCP
WAN1-MTU	Auto-
WAN1-MTU Value	1500
WAN1-DNS Server Source	Get Dynamically from ISP
WAN1-MAC Address Source	Use Default MAC address
WAN1-Zone Mapping	Réseau WAN
Network Addressing Modes	DHCP Client, L2TP, PPTP, PPPoE et Static IP
Port Mirroring	Désactiver
Port-based Access Control (contrôle d'accès basés sur les ports)	Désactiver

Fonctionnalité	Paramètre
WAN Redundancy Operation Modes	Equal Load Balancing (par défaut) Load Balancing Failover Routing Table
VLAN	
Maximum number of VLANs	16
DEFAULT VLAN	VID=1 IP Address=192.168.75.1 Subnet=255.255.255.0 Spanning Tree=Disable DHCP Mode=DHCP Server DHCP Pool = 192.168.75.100 à 200 Lease Time=1 day Default Gateway=192.168.75.1 Mapped Zone=LAN
GUEST VLAN	VID=2 IP Address=192.168.25.1 Subnet=255.255.255.0 Spanning Tree=Disable DHCP Mode=DHCP Server DHCP Pool = 192.168.25.100 à 200 Lease Time=1 day Default Gateway=192.168.25.1 Mapped Zone=GUEST

Fonctionnalité	Paramètre
VOICE VLAN	VID=100 IP Address=10.1.1.2 Subnet=255.255.255.0 Spanning Tree=Enable Mapped Zone=VOICE DHCP Mode=Disable
Zones	
Maximum number of zones	32
Predefined zones	WAN, LAN, DMZ, VPN, GUEST, SSLVPN, VOICE
Routing	
Routing mode	Désactiver
Maximum number of Static Routing rules	150
Dynamic Routing (RIP)	Désactiver
Policy-Based Routing	Désactiver
Maximum number of Policy-Based Routing rules	100
WAN QoS	Désactiver
Maximum number of traffic selectors	256
Maximum number of WAN QoS policy profiles	32
Maximum number of traffic selectors associated with one WAN QoS policy profile	64
LAN QOS (QoS LAN)	Désactiver
WLAN QoS	Désactiver

Fonctionnalité	Paramètre
Service Management	
Maximum number of service groups	64
Maximum number of services	150
Maximum number of services in one service group	64
Address Management	
Maximum number of address groups	64
Maximum number of addresses	150
Maximum number of addresses in one address group	100
Maximum number of DDNS profiles	16
VRRP	Désactiver
IGMP Proxy	Activer
IGMP Snooping	Activer
Version IGMP (par défaut)	IGMP Version 3

Sans fil

Fonctionnalité	Paramètre
Wireless Radio	Désactiver
Basic Radio Settings	
Wireless mode	802.11b/g/n mixed
Wireless channel	Auto-
Bandwidth channel	Auto-
Extension channel	Lower
U-APSD	Désactiver
SSID isolation (entre des SSID)	Désactiver

Fonctionnalité	Paramètre
SSID par défaut (cisco-data, cisco-guest, cisco3, cisco4)	Désactiver
SSID broadcast	Activer
Station isolation (between clients)	Désactiver
Security Mode	Open
Wi-Fi Multimedia (WMM)	Activer
Wireless MAC Filtering	Désactiver
Advanced Radio Settings	
Guard interval	Long (800 ns)
CTS protection mode	Auto-
Beacon interval	100 ms (20 to 999 ms)
DTIM interval	1 ms (1 to 255 ms)
RTS threshold	2347 ms (1 to 2347 ms)
Fragmentation threshold	2346 ms (256 to 2346 ms)
Power output	100 %
Wi-Fi Protected Setup (WPS)	Désactiver
Rogue AP Detection	Désactiver
Captive Portal	Désactiver
Session timeout	60 minutes (0 to 480 minutes)
Idle timeout	5 minutes (de 0 à 480 minutes)

VPN

Fonctionnalité	Paramètre
Site-to-Site VPN	Désactiver
Maximum number of Site-to-Site VPN tunnels	100 pour ISA570 et ISA570W 50 pour ISA550 et ISA550W

Fonctionnalité	Paramètre
IKE Policies	
Maximum number of IKE policies	16
DefaultIke, Hash	SHA1
DefaultIke, Authentication	Pre-shared Key
DefaultIke, D-H Group	Group 2
DefaultIke, Encryption	ESP_AES_256
DefaultIke, Lifetime	24 heures
Transform Policies	
Maximum number of transform policies	16
DefaultTrans, Integrity	ESP_SHA1_HMAC
DefaultTrans, Encryption	ESP_AES_256
IPsec Remote Access	Désactiver
Maximum number of group policies	16
Teleworker VPN Client	Désactiver
Maximum number of group policies	16
Auto initiation retry	Désactiver
Retry interval	120 seconds (120 to 1800 seconds)
Retry limit	0 (0 to 16)
VPN SSL	Désactiver
Maximum number of group policies	32
Gateway Interface	WAN1
Gateway port number	443
Certificate file	Par défaut
Client address pool	192.168.200.0
Client netmask	255.255.255.0
Idle timeout	2 100 secondes (de 60 à 86 400 secondes)

Fonctionnalité	Paramètre
Session timeout	0 secondes (de 0, 60 à 120 9600 secondes)
Client DPD timeout	300 secondes (de 0 à 3 600 secondes)
Gateway DPD timeout	300 secondes (de 0 à 3 600 secondes)
Keep alive	30 secondes (de 0 à 600 secondes)
Lease duration	43 200 secondes (de 600 à 1 209 600 secondes)
Max MTU	1406 bytes (256 to 1406 bytes)
Rekey method	SSL
Rekey interval	3600 seconds (0 to 43200 seconds)
L2TP Server	Désactiver
IPsec Passthrough	Activer
PPTP Passthrough	Activer
L2TP Passthrough	Activer

Services de sécurité

Fonctionnalité	Paramètre
Antivirus	Désactiver
Application Control	Désactiver
Spam Filter	Désactiver
Intrusion Prevention (IPS)	Désactiver
Web Reputation Filtering	Désactiver
Web URL Filtering	Désactiver
Network Reputation	Activer

Pare-feu

Fonctionnalités	Paramètre
Default Firewall Rules	Prevent all inbound traffic and allow all outbound traffic
Maximum number of custom firewall rules	100
NAT	
Dynamic PAT	Activer
Maximum number of Static NAT rules	64
Maximum number of Port Forwarding rules	64
Maximum number of Port Triggering rules	15
Maximum number of Advanced NAT rules	32
Content Filtering	Désactiver
MAC Address Filtering	Désactiver
Maximum number of MAC Address Filtering rules	100
IP - MAC Binding	
Maximum number of IP - MAC Binding rules	100
Attack Protection	
Block Ping WAN Interface	Activer
Stealth Mode	Activer
Block TCP Flood	Activer
Block UDP Flood	Activer
Block ICMP Notification	Activer

Fonctionnalités	Paramètre
Block Fragmented Packets	Désactiver
Block Multicast Packets	Activer
SYN Flood Detect Rate	128 max/sec (0 to 65535)
Echo Storm	15 packets/sec (0 to 65535)
ICMP Flood	100 packets/sec (0 to 65535)
Session Limits	
Maximum number of connections	60000 (1000 to 60000)
TCP timeout	1200 seconds (5 to 3600 seconds)
UDP timeout	180 secondes (de 5 à 3 600 secondes)
Application Level Gateway (ALG)	
SIP ALG	Activer
H.323 ALG	Activer

Rapports

Fonctionnalité	Paramètre
Bandwidth Usage Reports	
Bandwidth Usage Report by IP Address	Désactiver
Bandwidth Usage Report by Internet Service	Désactiver
Website Visits Report	Désactiver
WAN Bandwidth Reports	Désactiver
Security Services Reports	
Anti-Virus Report	Désactiver
Application Control Report	Désactiver

Fonctionnalité	Paramètre
Email Security Report	Désactiver
IPS Report	Désactiver
Network Reputation Report	Activer
Web Security Report	Désactiver

Objets de services par défaut

Le tableau suivant présente tous les objets de services prédéfinis sur l'Cisco ISA500.

Nom du service	Protocoles	Début de port	Fin de port	Description
AIM-CONNECT	TCP	4443	4443	AOL Instant Messenger, direct connect
AIM-CHAT	TCP	5 190	5 190	AOL Instant Messenger, transfert de fichiers et discussion
BGP	TCP	179	179	Protocole BGP
BOOTP_client	UDP	68	68	Protocole Bootstrap
BOOTP_server	UDP	67	67	Protocole Bootstrap
CU-SEEME	TCP/UDP	7648	7652	Protocole de vidéoconférence Internet
DHCP	UDP	67	67	Protocole DHCP (Dynamic Host Configuration Protocol)
DNS	TCP/UDP	53	53	Système de noms de domaine (DNS)
ESP	Communications			Protocole 50
FINGER	TCP	79	79	Echange d'informations sur les utilisateurs et l'état destiné aux utilisateurs

Nom du service	Protocoles	Début de port	Fin de port	Description
FTP-DATA	TCP	20	20	Protocole de transfert de fichiers (FTP), transfert de données
FTP-CONTROL	TCP	21	21	Protocole de transfert de fichiers (FTP), commande control
HTTP	TCP	80	80	Protocole de transfert hypertexte (HTTP)
HTTPS	TCP	443	443	HTTP sur·SSL/TLS
ICMP Destination Unreachable	ICMP	3	0	
ICMP Ping Reply	ICMP	0	0	
ICMP Ping Request	ICMP	8	0	
ICMP Redirect Message	ICMP	5	0	
ICMP Router Advertisement	ICMP	9	0	
ICMP Router Solicitation	ICMP	10	0	
ICMP Source Quench	ICMP	4	0	
ICMP Time Exceeded	ICMP	11	0	
ICMP Timestamp	ICMP	13	0	
ICMP Type-6	ICMP	6	0	Adresse d'hôte secondaire
ICMP Type-7	ICMP	7	0	Réservé
ICQ	TCP	5 190	5 190	Messagerie instantanée
IDENT	TCP	113	113	Service d'authentification/protocole d'identification
IKE	UDP	500	500	Échange de clés IPsec

Nom du service	Protocoles	Début de port	Fin de port	Description
Interface IMAP	TCP	143	143	Internet Message Access Protocol
IMAP2	TCP	143	143	Internet Message Access Protocol Version 2
IMAP3	TCP	220	220	Internet Message Access Protocol Version 3
IPSEC-UDP-ENCAP	UDP	4 500	4 500	IPsec sur·UDP
IRC	TCP	6660	6660	IRC (Internet Relay Chat), port de facto : 6660 à 6669
ISAKMP	UDP	500	500	
L2TP	UDP	1701	1701	Protocole de tunnellisation couche 2 (L2TP)
NEWS	TCP	144	144	
NFS	UDP	2049	2049	Système de fichiers en réseau
NNTP	TCP	119	119	Protocole NNTP (Network News Transfer Protocol), NNTP sur SSL utilise le port 563
POP3	TCP	110	110	Protocole POP (Post Office Protocol) version 3
PPTP	TCP	1723	1723	Protocole de tunnellisation point à point Microsoft
RCMD	TCP	512	512	
REAL-AUDIO	TCP	7070	7070	
REXEC	TCP	512	512	Exécution de processus à distance
RIP	UDP	520	520	Protocole RIP (Routing Information Protocol, protocole d'informations de routage)

Nom du service	Protocoles	Début de port	Fin de port	Description
RLOGIN	TCP	513	513	
RTELNET	TCP	107	107	Service Telnet à distance
RTSP	TCP/UDP	554	554	Protocole RTSP (Real Time Streaming Protocol)
SFTP	TCP	115	115	Protocole SFTP (Simple File Transfer Protocol, protocole de transfert de fichiers simple)
SHTTPD	TCP	8080	8080	HTTPD simple
SHTTPDS	TCP	443	443	HTTPD simple sur SSL
SIP	TCP/UDP	5060	5060	Protocole SIP
SMTP	TCP	25	25	Simple Mail Transfer Protocol
SNMP	TCP/UDP	161	161	SNMP : protocole
SNMP-TRAPS	TCP/UDP	162	162	Simple Network Management Protocol - Trap
SQL-NET	TCP	1521	1521	
SSH	TCP/UDP	22	22	Protocole SSH (Secure Shell)
STRMWORKS	UDP	1558	1558	
TACACS	TCP	49	49	Protocole LHP (Login Host Protocol)
TELNET	TCP	23	23	
TELNET secondaire	TCP	8023	8023	
TELNET SSL	TCP	992	992	
TFTP	UDP	69	69	Trivial FTP
VDOLIVE	TCP	650	650	Protocole VDOLive

Objets d'adresse par défaut

Le tableau suivant présente tous les objets d'adresse prédéfinis sur l'Cisco ISA500. L'adresse IP, l'adresse IP et le masque réseau, ou la plage IP de ces objets seront automatiquement modifiés en fonction de votre configuration ou de votre connexion réseau.

Nom d'adresse	Type	IP, IP/Masque réseau ou plage IP
WAN1_IP	Hôte	0.0.0.0
WAN1_GW	Hôte	0.0.0.0
WAN1_DNS1	Hôte	0.0.0.0
WAN1_DNS2	Hôte	0.0.0.0
WAN1_USER_DNS1	Hôte	0.0.0.0
WAN1_USER_DNS2	Hôte	0.0.0.0
WAN1_NETWORK	Réseau	0.0.0.0/255.255.255.255
WAN1_MAC	MAC	S/O
DEFAULT_IP	Hôte	192.168.75.1
DEFAULT_Network	Réseau	192.168.75.0/255.255.255.0
DEFAULT_DHCP_POOL	Plage	192.168.75.100 à 192.168.75.200
GUEST_IP	Hôte	192.168.25.1
GUEST_Network	Réseau	192.168.25.0/255.255.255.0
GUEST_DHCP_POOL	Plage	192.168.25.100 à 192.168.25.200
IPv4_Multicast	Plage	224.0.0.0 à 239.255.255.255
SSLVPN_ADDRESS_POOL	Réseau	192.168.200.0/255.255.255.0

D

Problèmes et solutions

Cisco propose une vaste gamme de ressources pour vous aider, ainsi que vos clients, à tirer pleinement parti des Cisco ISA500 Integrated Security Appliances.

Ressources sur les produits	
Assistance	
Communauté d'assistance Cisco Small Business	www.cisco.com/go/smallbizsupport
Ressources et assistance Cisco Small Business	www.cisco.com/go/smallbizhelp
Coordonnées de l'assistance téléphonique	www.cisco.com/go/sbsc
Téléchargement de microprogrammes	www.cisco.com/go/isa500software
Documentation sur les produits	
Cisco ISA500 Integrated Security Appliances	www.cisco.com/go/isa500resources
Gamme Cisco Small Business	
Partenaires et revendeurs Cisco pour les PME (identification partenaire obligatoire)	www.cisco.com/web/partners/sell/smb
Accueil Cisco Small Business	www.cisco.com/smb