Mise en correspondance des fonctionnalités de Cisco Secure Firewall ASA et Threat Defense

Dernière modification : 2025-07-25

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

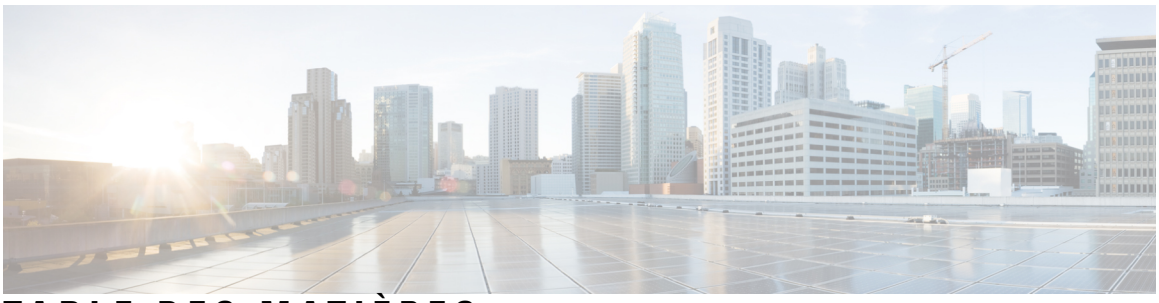


TABLE DES MATIÈRES

À propos de ce guide

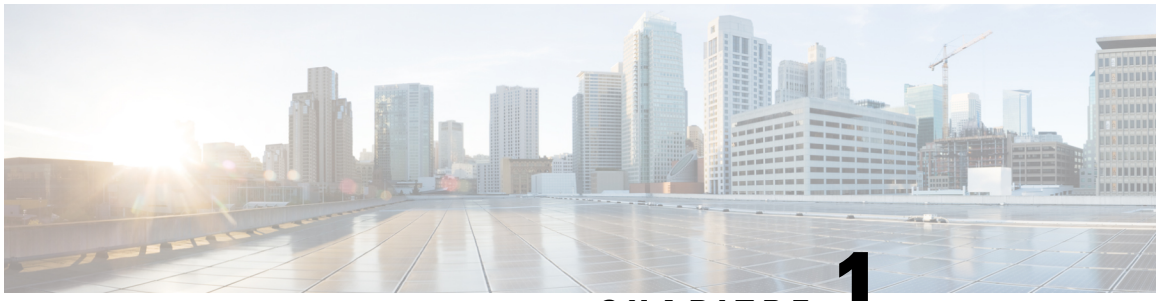
Ce document présente les fonctionnalités ASA couramment utilisées et les capacités équivalentes de la défense contre les menaces . Pour chaque fonctionnalité ASA (qui correspond à un chapitre ou une section du guide de configuration ASA), nous indiquons la fonctionnalité équivalente dans la défense contre les menaces , ainsi que le chemin d'accès de l'interface utilisateur permettant de configurer la fonctionnalité dans le Cisco Secure Firewall Management Center ou dans le Cisco Defense Orchestrator (CDO), le centre de gestion de pare-feu offert en mode infonuagique. Nous fournissons également des liens vers la documentation du centre de gestion, afin que vous puissiez en savoir plus sur la mise en œuvre de chaque fonctionnalité. Pour chaque fonctionnalité, nous précisons les limitations connues ou les différences, le cas échéant.

Le centre de gestion est un gestionnaire multipériphériques qui vous permet d'appliquer des stratégies de sécurité à plusieurs périphériques.

La défense contre les menaces comprend de nombreuses fonctionnalités de sécurité utiles qui ne sont pas disponibles avec l'ASA, ainsi que des fonctionnalités de gestion offertes par le centre de gestion qui ne sont pas accessibles avec les méthodes de gestion ASA. Ce guide ne présente pas les fonctionnalités de la défense contre les menaces qui ne sont pas disponibles dans ASA.

Remarque Le centre de gestion prend en charge certaines fonctionnalités ASA à l'aide d'un outil CLI appelé FlexConfig.

À propos de ce guide



CHAPITRE 1

Fonctionnalités générales d'exploitation

Pour commencer

Tableau 1 : Pour commencer

Fonctionnalité ASA	Fonctionnalité Défense contre les menaces (Threat Defense) dans Cisco Secure Firewall Management Center	Notes
ASA interface de ligne de commande pour la configuration	**Interface de ligne de commande limitée Défense contre les menaces (Threat Defense) pour la configuration, configuration complète via l'interface graphique** Consultez les sections : Guides de démarrage (accès à la console), Référence des commandes, Guide de configuration des périphériques	L'interface de ligne de commande défense contre les menaces comprend des commandes *limitées* pour la configuration initiale uniquement et certaines opérations spéciales. La configuration doit être effectuée dans le centre de gestion qui offre des fonctionnalités limitées de détection de configuration des appareils.

Fonctionnalité ASA	Fonctionnalité Défense contre les menaces (Threat Defense) dans Cisco Secure Firewall Management Center	Notes
ASA interface de ligne de commande pour la surveillance	**Interface de ligne de commande Défense contre les menaces (Threat Defense) pour la surveillance** Chemin de l'interface utilisateur : **System (Système)** (⚙) > **Health (Intégrité)** > **Monitor (Moniteur)> Advanced Troubleshooting (Dépannage avancé)** > **Threat Defense CLI (Interface de commande en ligne de défense contre les menaces)** Consultez les sections : Guides de démarrage (accès à la console), Référence des commandes, Utilisation de l'interface de ligne de commande de défense contre les menaces à partir de l'interface Web	Vous pouvez utiliser les mêmes commandes **show** qui sont disponibles sur les ASA. Vous pouvez accéder à l'interface de ligne de commande via la console, en SSH ou en utilisant l'outil Web de l'interface de ligne de commande.
Configuration initiale	**Configuration initiale** Consultez la section : Guides de démarrage (accès à la console)	Utilisez l'interface de ligne de commande ou le gestionnaire d'appareil pour définir les paramètres réseau et enregistrer le périphérique auprès du centre de gestion.
Changements de configuration	**Déploiement de la configuration** Chemin de l'interface utilisateur : **Deploy (Déployer)** Consultez la section : Déploiement de la configuration	Vous devez déployer toutes les modifications à partir du centre de gestion.
Licences Smart	**Licences Smart** Chemin de l'interface utilisateur : **System (Système)** > **Licenses** > **Smart Licenses (Licences Smart)** Consultez la section : Licences Instructions : enregistrer le centre de gestion auprès d'un compte Cisco Smart	Les licences sont utilisées et attribuées par le centre de gestion.
Mode pare-feu transparent ou routé	**Mode pare-feu transparent ou routé** Consultez la section : Mode pare-feu transparent ou routé	Comme avec les ASA, vous devez changer le mode du pare-feu en utilisant l'interface de ligne de commande avant d'enregistrer le périphérique auprès du centre de gestion.

Fonctionnalités de haute disponibilité et d'évolutivité

Tableau 2 : Fonctionnalités de haute disponibilité et d'évolutivité

Fonctionnalité ASA	Fonctionnalité Défense contre les menaces (Threat Defense) dans Cisco Secure Firewall Management Center	Notes
Mode contexte multiple	**Mode multi-instances** ou **routeurs virtuels** Chemin de l'interface utilisateur : • Firepower 4100/9300 Multi-Instances : **Logical Devices (Périphériques logiques)** > **Add (Ajouter)** (chassis manager (gestionnaire de châssis)) • Routeurs virtuels : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Edit (Modifier)** > **Routing (Routage)** > **Manage Virtual Routers (Gérer les routeurs virtuels)** Consultez les sections : Utilisation de la capacité multi-instances sur le périphérique Firepower 4100/9300, Routeurs virtuels Comment faire pour : créer un routeur virtuel, affecter des interfaces aux routeurs virtuels, configurer la NAT pour un routeur virtuel, fournir un accès Internet avec des espaces d'adressage superposés, configurer la politique de routage	Dans de nombreux cas, vos clients peuvent n'avoir besoin que de tableaux de routage distincts plutôt que d'une séparation complète. Dans ce cas, vous pouvez utiliser des routeurs virtuels. Pour une séparation complète de la configuration, utilisez le mode multi-instances sur les plateformes prises en charge. Cette mise en œuvre est différente du mode de contexte multiple d'ASA, mais la fonctionnalité est similaire.
Basculement actif/de secours	**haute disponibilité** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Add** > **High Availability (Ajouter la haute disponibilité)** Voir : Haute disponibilité Instructions : Créer une paire à haute disponibilité	

Fonctionnalité ASA	Fonctionnalité Défense contre les menaces (Threat Defense) dans Cisco Secure Firewall Management Center	Notes
Mise en grappes	**Mise en grappes** Chemin de l'interface utilisateur : • Firepower 4100/9300 : **Logical Devices (Périphériques logiques)** > **Add (Ajouter)** (chassis manager (gestionnaire de châssis)) **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Add (Ajouter)** > **Device (Périphérique)** (centre de gestion) • Défense contre les menaces virtuelles pour le nuage public : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Add (Ajouter)** > **Device (Périphérique)** • Cisco Secure Firewall 3100 : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Add (Ajouter)** > **Cluster (Grappe)** • Défense contre les menaces virtuelles pour le nuage privé : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Add (Ajouter)** > **Cluster (Grappe)** Consultez les sections : Déployer une grappe pour Threat Defense sur Cisco Secure Firewall 3100, Déployer une grappe pour Threat Defense sur Firepower 4100/9300, Déployer une grappe pour Threat Defense Virtual dans un nuage public, Déployer une grappe pour Threat Defense Virtual dans un nuage privé Instructions : créer une grappe, modifier une grappe existante, ajouter des nœuds à une grappe existante, retirer un nœud de données d'une grappe, dissocier une grappe, supprimer une grappe, dissocier un nœud de la grappe, supprimer un nœud de données de la grappe.	La mise en grappe intersite et le VPN de site à site distribué ne sont pas pris en charge.

Interfaces

Pour la défense contre les menaces , les interfaces sont configurées par périphérique. Cependant, pour la plupart des fonctionnalités, vous affectez des interfaces aux périmètres de sécurité, puis appliquez les politiques aux *zones*, et non directement aux interfaces. Les zones, comme la politique de sécurité elle-même, sont configurées en tant qu'objets pouvant être partagés sur plusieurs périphériques.

Remarque La défense contre les menaces prend en charge les interfaces de pare-feu normales comme ASA, mais elle prend également en charge un autre type d'interface réservée à l'IPS.

Tableau 3 : Interfaces

Fonctionnalité ASA	Fonctionnalité Défense contre les menaces (Threat Defense) dans Cisco Secure Firewall Management Center	Notes
Interface de gestion	**Interface de gestion** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Edit (Modifier)** > **Devices (Périphériques)** > **Management (Gestion)** Consultez la section : Compléter la configuration initiale de la défense contre les menaces	L'ASA a une interface réservée à la gestion qui a sa propre table de routage, mais fonctionne pour la plupart comme des interfaces de données. La défense contre les menaces a une interface de gestion distincte des interfaces de données. Elle est utilisée pour configurer et enregistrer les périphériques dans le centre de gestion. Il utilise sa propre adresse IP et le routage statique.
Interfaces physiques	**Interfaces physiques** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Edit (Modifier)** > **Interfaces** Consultez la section : Présentation de l'interface Instructions : Configurer les paramètres d'interface	
Ports de commutation Firepower 1010	**Ports de commutation Firepower 1010** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Edit (Modifier)** > **Interfaces** Consultez la section : Configurer les ports de commutation de Firepower 1010	
EtherChannels	**EtherChannels** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Edit (Modifier)** > **Interfaces** Consultez la section : Configurer les interfaces EtherChannel	
Interfaces de boucle avec retour	**Interfaces de boucle avec retour** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Edit (Modifier)** > **Interfaces** Consultez la section : Configurer les interfaces de boucle avec retour	

Fonctionnalité ASA	Fonctionnalité Défense contre les menaces (Threat Defense) dans Cisco Secure Firewall Management Center	Notes
Sous-interfaces VLAN	**Sous-interfaces VLAN** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Edit (Modifier)** > **Interfaces** Consultez la section : Configurer les sous-interfaces VLAN et la jonction 802.1Q	
Interfaces VXLAN	**Interfaces VXLAN** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Edit (Modifier)** > **Interfaces** Consultez la section : Configurer les interfaces VXLAN	
Interfaces en mode routage et en mode transparent	**Interfaces en mode routage et en mode transparent** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Edit (Modifier)** > **Interfaces** Consultez la section : Configurer les interfaces en mode routage et en mode transparent	
Configuration avancée de l'interface	**Configuration avancée de l'interface** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Edit (Modifier)** > **Interfaces** Consultez la section : Configurer les paramètres avancés de l'interface	
Zones de circulation	**ECMP** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Edit (Modifier)** > **Routing (Routage)** > **ECMP** Consultez la section : ECMP	

Paramètres de base

Tableau 4 : Paramètres de base

Fonctionnalité ASA	Fonctionnalité Défense contre les menaces (Threat Defense) dans Cisco Secure Firewall Management Center	Notes
Serveur DNS	**Serveur DNS** Chemin de l'interface utilisateur : • **Objects (Objets) > Object Management (Gestion des objets) > DNS Server Group (Groupe de serveurs DNS)** • **Devices (Périphériques) > Platform Settings (Paramètres de plateforme) > DNS** Consultez les sections : Groupe de serveurs DNS, Configurer le DNS, Politiques FlexConfig.	Les serveurs DNS font partie des paramètres de plateforme qui peuvent être appliqués à plusieurs périphériques. **Remarque** Le serveur DNS pour l'interface de gestion dédiée défense contre les menaces est configuré au niveau de l'interface de ligne de commande à l'aide des commandes **configure network dns servers** et **configure network dns searchdomains**
ISA 3000, contournement matériel (Hardware Bypass)	**ISA 3000, contournement matériel(Hardware Bypass)** Chemin de l'interface utilisateur : • **Objects (Objets) > Object Management (Gestion d'objets) > FlexConfig > FlexConfig Objects (Objets FlexConfig)** • **Devices (Périphériques) > FlexConfig** Consultez la section : Comment configurer le contournement matériel automatique en cas de panne d'alimentation (ISA 3000)	Cette fonctionnalité peut être configurée à l'aide de FlexConfig.
ISA 3000, protocole PTP (Precision Time Protocol)	**ISA 3000, protocole PTP (Precision Time Protocol)** Chemin de l'interface utilisateur : • **Objects (objets) > Object Management (gestion d'objets) > FlexConfig > FlexConfig Objects (objets FlexConfig)** • **Devices (Périphériques) > FlexConfig** Consultez la section : Comment configurer le protocole PTP (Precision Time Protocol) (ISA 3000)	Cette fonctionnalité peut être configurée à l'aide de FlexConfig.

Fonctionnalité ASA	Fonctionnalité Défense contre les menaces (Threat Defense) dans Cisco Secure Firewall Management Center	Notes
ISA 3000, alimentation électrique redondante (Precision Dual Power Supply)	**ISA 3000, alimentation électrique redondante (Precision Dual Power Supply)** Chemin de l'interface utilisateur : • **Objects (objets)** > **Object Management (gestion d'objets)** > **FlexConfig** > **FlexConfig Objects (objets FlexConfig)** • **Devices (Périphériques)** > **FlexConfig** Consultez la section : Politiques FlexConfig:	Cette fonctionnalité peut être configurée à l'aide de FlexConfig.
Serveur DHCP	**Serveur DHCP** Chemin de l'interface utilisateur : • IPv4 : **Devices (Périphériques)** > **Device Management (Gestion des périphériques** > **Edit (Modifier)** > **DHCP** > **DHCP Server (Serveur DHCP)** • IPv6 : Devices (Périphériques)**Device Management (Gestion des périphériques** > **Edit (Modifier)** > **Interfaces** > **IPv6** > **DHCP** Consultez les sections : Configurer le serveur DHCPv4, Configurer le serveur sans état DHCPv6	
Agent de relais DHCP	**Agent de relais DHCP** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Edit (Modifier)** > **DHCP** > **DHCP Relay (Relais DHCP)** Consultez la section : Configurer l'agent de relais DHCP	
Système de nom de domaine dynamique (DDNS)	**Système de nom de domaine dynamique (DDNS)** Chemin de l'interface utilisateur : **Devices(Périphériques)** > **Device Management (Gestion des périphériques)** > **Edit (Modifier)** > **DHCP** > **DDNS** Consultez la section : Configure Dynamic DNS	

Fonctionnalité ASA	Fonctionnalité Défense contre les menaces (Threat Defense) dans Cisco Secure Firewall Management Center	Notes
Certificats numériques	**Certificats, PKI** Chemin de l'interface utilisateur : • **Objects (Objets)** > **Object Management (Gestion des objets)** > **PKI** • **Devices (Périphériques)** > **Certificates (Certificats)** Consultez la section : PKI, Certificates Instructions : • Authentifier un VPN d'accès à distance (RA VPN) à l'aide d'un certificat : créer une table de correspondance des certificats pour l'authentification dans le VPN RA et associer une table de correspondance à un profil de connexion. • Créer et installer un certificat d'identité sur le périphérique pour la configuration d'un VPN d'accès à distance : utiliser un objet d'inscription de certificat PKCS12, un objet d'inscription manuel, un objet d'inscription autosigné ou SCEP, installer un certificat manuel, PKCS12, SCEP ou autosigné, puis configurer le VPN d'accès à distance. • Configuration du VPN : renouveler un certificat à l'aide d'une réinscription manuelle, renouveler un certificat à l'aide d'un certificat autosigné, SCEP ou EST.	Créez des objets de certificat réutilisables, puis appliquez-les par périphérique.
Inspection ARP et table des adresses MAC	**Inspection ARP et table des adresses MAC** Chemin de l'interface utilisateur : • **Devices (Périphériques)** > **Device Management (Gestion des périphériques** > **Edit (Modifier)** > **Interfaces** > **Advanced (Avancé)** > **ARP and MAC(ARP et MAC)** • **Devices (Périphériques)** > **Platform Settings (Paramètres de la plateforme)** > **ARP Inspection (Inspection ARP)** Consultez les sections : Advanced Interface Settings, Configure ARP Inspection	L'inspection ARP fait partie des paramètres de la plateforme qui peuvent être appliqués à plusieurs périphériques.
WCCP	**WCCP** Chemin de l'interface utilisateur : • **Objects (objets)** > **Object Management (gestion d'objets)** > **FlexConfig** > **FlexConfig Objects (objets FlexConfig)** • **Devices (Périphériques)** > **FlexConfig** Consultez la section : Politiques FlexConfig	Cette fonctionnalité peut être configurée à l'aide de FlexConfig.

Routage

Le routage est configuré par périphérique.

Tableau 5 : Routage

Fonctionnalité ASA	Fonctionnalité Défense contre les menaces (Threat Defense) dans Cisco Secure Firewall Management Center	Notes
Tableaux de routage des données et de gestion	**Tableaux de routage des données et de gestion** Consultez la section : Référence pour le routage Instructions : Configurer la politique de routage	L'ASA et la défense contre les menaces utilisent des valeurs par défaut différentes pour déterminer si le trafic est dirigé vers le tableau de routage de gestion ou vers le tableau de routage des données. **Remarque** L'interface de gestion dédiée possède une table de routage Linux distincte que vous pouvez configurer à l'interface CLI.
Routages statiques et par défaut	**Routages statiques et par défaut** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Edit (Modifier)** > **Routing (Routage)** > **Static Route (Route statique)** Consultez la section : Routes statiques et par défaut Instructions : configurer une route statique pour VTI	
Routage basé sur une stratégie	**Routage basé sur une stratégie** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Edit (Modifier)** > **Routing (Routage)** > **Policy Based Routing (Routage basé sur des politiques)** Consultez la section : Routage basé sur des politiques	
Cartes de routage	**Cartes de routage** Chemin de l'interface utilisateur : **Objects (Objets)** > **Object Management (Gestion des objets)** > **Route Map (Carte de routage)** Consultez la section : Carte de routage	
Routage par détection de transfert bidirectionnel (BFD)	**Routage par détection de transfert bidirectionnel (BFD)** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Edit (Modifier)** > **Routing (Routage)** > **BFD** Consultez la section : Routage avec BFD	

Fonctionnalité ASA	Fonctionnalité Défense contre les menaces (Threat Defense) dans Cisco Secure Firewall Management Center	Notes
BGP	**BGP** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Edit (Modifier)** > **Routing (Routage)** > **BGP** Consultez la section : BGP. Instructions : configurer le routage BGP pour VTI	
OSPF	**OSPF** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Edit (Modifier)** > **Routing (Routage)** > **OSPF** Consultez la section : OSPF	
ISIS	**ISIS** Chemin de l'interface utilisateur : • **Objects (objets)** > **Object Management (gestion d'objets)** > **FlexConfig** > **FlexConfig Objects (objets FlexConfig)** • **Devices (Périphériques)** > **FlexConfig** Consultez la section : Politiques FlexConfig	Cette fonctionnalité peut être configurée à l'aide de FlexConfig
EIGRP	**EIGRP** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Edit (Modifier)** > **Routing (Routage)** > **EIGRP** Consultez la section : EIGRP	
Routage multidiffusion	**Routage multidiffusion** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Edit (Modifier)** > **Routing (Routage)** > **Multicast Routing (Routage multidiffusion)** Consultez la section : Multidiffusion	
RIP	**RIP** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **Edit (Modifier)** > **Routing (Routage)** > **RIP** Consultez la section : RIP	

Serveurs AAA

Sur le défense contre les menaces , les serveurs AAA peuvent être utilisés pour l'accès VPN. Pour les serveurs AAA et la base de données locale pour l'accès de gestion, consultez Administration système, à la page 13.

Tableau 6 : Serveurs AAA

Fonctionnalité ASA	Fonctionnalité Défense contre les menaces (Threat Defense) dans Cisco Secure Firewall Management Center	Notes
RADIUS pour le VPN	**RADIUS pour le VPN** Chemin de l'interface utilisateur : **Objects (Objets)** > **Object Management (Gestion des objets)** > **AAA Server (Serveur AAA)** > **RADIUS Server Group (Groupe de serveurs RADIUS)** Consultez la section : Ajouter un groupe de serveurs RADIUS	
LDAP pour le VPN	**LDAP pour le VPN** Chemin de l'interface utilisateur : **Integration (Intégration)** > **Other Integrations (Autres intégrations)** > **Realms (Domaines)** Consultez la section : Créer un domaine Active Directory et un répertoire de domaine Instructions : Configurer la carte des attributs LDAP pour le VPN d'accès à distance.	
Authentification de connexion unique SAML pour le VPN	**Authentification de connexion unique SAML pour le VPN** Chemin de l'interface utilisateur : **Objects (Objets)** > **Object Management (Gestion des objets)** > **AAA Server (Serveur AAA)** > **Single Sign-On Server (Serveur de connexion unique)** Consultez la section : Ajouter un serveur de connexion unique Instructions : Créer un objet serveur de connexion unique SAML.	

Administration système

Tableau 7 : Administration système

Fonctionnalité ASA	Fonctionnalité Défense contre les menaces (Threat Defense) dans Cisco Secure Firewall Management Center	Notes
Base de données locale pour la gestion des périphériques	**Utilisateur interne (centre de gestion)** Chemin de l'interface utilisateur : **System (Système)** (⚙) > **Utilisateurs** Consultez la section : Ajouter un utilisateur interne **Utilisateurs (défense contre les menaces)** Consultez la section : Ajouter un utilisateur interne au niveau de l'interface de ligne de commande	Le centre de gestion et la défense contre les menaces maintiennent des bases de données d'utilisateurs distinctes. Vous pouvez configurer les utilisateurs du centre de gestion pour l'accès Web et l'accès CLI. Pour ajouter des utilisateurs à la défense contre les menaces , vous devez utiliser l'interface CLI. Les utilisateurs de la défense contre les menaces disposent d'un accès SSH.
RADIUS pour la gestion des périphériques	**RADIUS (centre de gestion)** Chemin de l'interface utilisateur : **System (Système)** (⚙) > **Users (utilisateurs)** > **External Authentication (authentification externe)** Consultez la section : Ajouter un objet d'authentification externe RADIUS pour le centre de gestion des objets **RADIUS (défense contre les menaces)** Chemin de l'interface utilisateur : • **System (Système)** (⚙) > **Users (utilisateurs)** > **External Authentication (authentification externe)** • **Devices (Périphériques)** > **Platform Settings (Paramètres de la plateforme)** > **Edit (Modifier)** > **External Authentication (Authentification extérieure)** Consultez la section : Configurer l'authentification externe pour SSH	Pour les utilisateurs défense contre les menaces , vous activez l'objet d'authentification RADIUS dans le cadre de la configuration des paramètres de la plateforme.

Fonctionnalité ASA	Fonctionnalité Défense contre les menaces (Threat Defense) dans Cisco Secure Firewall Management Center	Notes
LDAP pour la gestion des périphériques	**LDAP (centre de gestion)** Chemin de l'interface utilisateur : **System (Système)** (⚙) > **Users (utilisateurs)** > **External Authentication (authentification externe)** Consultez la section : Ajouter un objet d'authentification externe LAPD pour le centre de gestion des objets **LDAP (défense contre les menaces)** Chemin de l'interface utilisateur : • **System (Système)** (⚙) > **Users (utilisateurs)** > **External Authentication (authentification externe)** • **Devices (Périphériques)** > **Platform Settings (Paramètres de la plateforme)** > **Edit (Modifier)** > **External Authentication (Authentification extérieure)** Consultez la section : Configurer l'authentification externe pour SSH	Pour les utilisateurs défense contre les menaces , vous activez l'objet d'authentification LDAP dans les paramètres de la plateforme.
SSH	**Liste de contrôle d'accès (centre de gestion)** Chemin de l'interface utilisateur : **System (Système)** (⚙) > **Configuration** > **Access List (liste d'accès)** Consultez la section : Liste d'accès **Protocole Secure Shell (défense contre les menaces)** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **Platform Settings (Paramètres de la plateforme)** > **Secure Shell** Consultez la section : Configurer le protocole SSH (Secure Shell)	Pour le centre de gestion, SSH est activé par défaut. Vous pouvez restreindre l'accès dans la configuration du système. Pour la défense contre les menaces , SSH est activé par défaut pour l'interface de gestion dédiée. Vous pouvez restreindre l'accès en utilisant la commande **configure ssh-access-list**. Pour SSH sur les interfaces de données, activez-le dans les paramètres de la plateforme. Ces paramètres peuvent s'appliquer à plusieurs périphériques.
HTTPS	**Liste d'accès** Chemin de l'interface utilisateur : **System (Système)** (⚙) > **Configuration** > **Access List (liste d'accès)** Consultez la section : Liste d'accès	Vous pouvez contrôler l'accès HTTPS au centre de gestion dans la configuration du système. La défense contre les menaces ne prend pas en charge l'accès HTTPS lorsqu'il est géré par le centre de gestion.

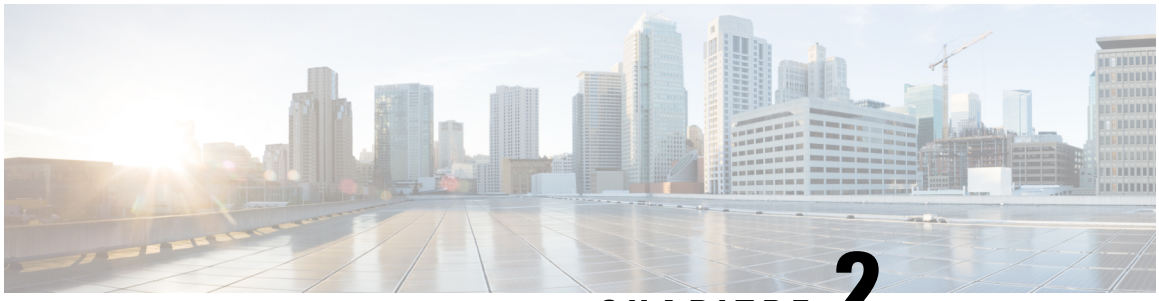
Fonctionnalité ASA	Fonctionnalité Défense contre les menaces (Threat Defense) dans Cisco Secure Firewall Management Center	Notes
Mise à jour du logiciel	**Mise à jour du logiciel** Chemin de l'interface utilisateur : **System (Système)** (⚙) > **Mises à jour** Consultez la section : Guide de mise à niveau de Cisco Secure Firewall Threat Defense pour Management Center Instructions : Mettre à niveau Secure Firewall Threat Defense	Effectuez toutes les mises à niveau à l'aide de centre de gestion.
Rétrogradation	**Rétablissement** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > **More (Plus)** > **Revert Upgrade (Annuler la mise à niveau)** Consultez la section : Annuler la mise à niveau	
Backup and Restore	**Backup and Restore** Chemin de l'interface utilisateur : **System (Système)** (⚙) > **Tools (outils)** > **Backup/Restore (sauvegarde et restauration)** Consultez la section : Sauvegarder et restaurer	
Échange à chaud d'un SSD (Secure Firewall 3100)	**Échange à chaud d'un SSD (Secure Firewall 3100)** Consultez la section : Échange à chaud d'un SSD sur le Cisco Secure Firewall 3100	Utilisez l'interface CL pour effectuer l'échange à chaud.
Messages de débogage	**Messages de débogage** Consultez la section : commande debug dans la référence des commandes	
Capture de paquets	**Capture de paquets** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **Packet Capture (Capture de paquets)** Consultez la section : Utiliser la trace de capture Instructions : Recueillir la capture de paquets pour le périphérique de défense contre les menaces.	
Packet Tracer	**Packet Tracer** Chemin de l'interface utilisateur : **Devices (périphériques)** > **Packet Tracer (traceur de paquets)** Consultez la section : Utiliser l'outil de trace de paquets Packet Tracer Instructions : Recueillir la capture de paquets pour dépanner le périphérique de défense contre les menaces.	

Fonctionnalité ASA	Fonctionnalité Défense contre les menaces (Threat Defense) dans Cisco Secure Firewall Management Center	Notes
Ping	**Ping** Chemin de l'interface utilisateur : **System (Système)** (⚙) > **Health (Intégrité)** > **Monitor (Moniteur)> Advanced Troubleshooting (Dépannage avancé)** > **Threat Defense CLI (Interface de commande en ligne de défense contre les menaces)** Consultez la section : commande ping dans la référence des commandes	
Traceroute	**Traceroute** Chemin de l'interface utilisateur : **System (Système)** (⚙) > **Health (Intégrité)** > **Monitor (Moniteur)> Advanced Troubleshooting (Dépannage avancé)** > **Threat Defense CLI (Interface de commande en ligne de défense contre les menaces)** Consultez la section : commande traceroute dans la référence des commandes	
Supervision des connexions	**Supervision des connexions** Chemin de l'interface utilisateur : **System (Système)** (⚙) > **Health (Intégrité)** > **Monitor (Moniteur)> Advanced Troubleshooting (Dépannage avancé)** > **Threat Defense CLI (Interface de commande en ligne de défense contre les menaces)** Consultez la section : commande show conn dans la référence des commandes	
show asp drop	**Supprimer l'ASP** Chemin de l'interface utilisateur : **System (Système)** (⚙) > **Politique** > **d'intégrité** Consultez la section : Modules d'intégrité	

Surveillance

Tableau 8 : Surveillance

Fonctionnalité ASA	Fonctionnalité Défense contre les menaces (Threat Defense) dans Cisco Secure Firewall Management Center	Notes
Logging (journalisation)	**Syslog** Chemin de l'interface utilisateur : • Syslog de type ASA : **Devices (Périphériques)** > **Platform Settings (Paramètres de plateforme)** > **Syslog** • Alertes pour les fichiers et les programmes malveillants, les connexions, les renseignements de sécurité et les incidents d'intrusion : **(Politiques)** > **(Contrôle d'accès)** > **Edit (Modifier)** > **logging (Journalisation)** • Alertes pour les règles de contrôle d'accès, les règles de prévention des intrusions et d'autres services avancés : **Policies (Politiques)** > **Actions** > **Alerts (Alertes)** Consultez les sections : Configurer Syslog, À propos de l'envoi de messages Syslog pour les événements de sécurité, Création d'une réponse d'alerte Syslog	La défense contre les menaces prend en charge la même capacité syslog que l'ASA. Mais elle prend également en charge la journalisation et les alertes générées par la prise en charge IPS de nouvelle génération que seule la défense contre les menaces fournit. Les paramètres Syslog font partie des paramètres de plateforme qui peuvent être appliqués à plusieurs périphériques.
SNMP	**SNMP** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **Platform Settings (Paramètres de plateforme** > **) SNMP** Consultez la section : Configurer le SNMP	Les paramètres SNMP font partie des paramètres de plateforme qui peuvent être appliqués à plusieurs périphériques.
Cisco Success Network	**Cisco Success Network** Chemin de l'interface utilisateur : **Integration (Intégration)** > **SecureX** > **Cisco Cloud Support** Consultez la section : Configurer l'inscription au Cisco Success Network	
Alarmes pour Cisco ISA 3000	**Alarmes pour Cisco ISA 3000** Chemin de l'interface utilisateur : **Objects (Objets)** > **Object Management (Gestion des objets)** > **FlexConfig** > **FlexConfig Object (Objet FlexConfig)** Consultez la section : Alarmes pour Cisco ISA 3000	Cette fonctionnalité peut être configurée à l'aide de FlexConfig



CHAPITRE 2

Fonctionnalités de pare-feu

Les rubriques suivantes expliquent comment configurer les fonctionnalités du pare-feu ASA, ou leurs équivalents, dans le Cisco Secure Firewall Threat Defense à l'aide du Cisco Secure Firewall Management Center ou du Cisco Firewall Management Center en nuage. Les fonctionnalités sont regroupées de façon approximative selon l'organisation de la documentation dans le *livre 2 de la CLI/ASDM : Guide de configuration de la CLI/ASDM pour les pare-feu de la gamme Cisco Secure Firewall ASA* .

Contrôle d'accès

Lorsque vous utilisez l'interface de ligne de commande ASA ou ADSM pour configurer un ASA, vous configurez toujours un seul périphérique à la fois.

En comparaison, la politique de contrôle d'accès dans Cisco Secure Firewall Management Center est toujours une politique partagée. Vous créez la politique, puis vous l'affectez à un ou plusieurs périphériques.

Généralement, vous devez créer une politique de contrôle d'accès pour plusieurs périphériques. Par exemple, vous pouvez affecter la même politique à tous les pare-feu de lieu éloigné (qui connectent les sites distants au réseau principal de l'entreprise). Ensuite, vous pourriez avoir une politique différente pour les pare-feu qui résident dans votre centre de données principal. Vous pouvez bien sûr créer des politiques distinctes pour chaque périphérique, mais ce n'est pas une utilisation efficace d'un gestionnaire d'appareils multiples.

L'application d'une règle de contrôle d'accès donnée à un périphérique est contrôlée par les interfaces spécifiées dans la règle :

- Si vous spécifiez aucune interface, la règle s'applique à tous les périphériques auxquels la politique est affectée.
- Si vous précisez des zones de sécurité, qui sont des objets composés d'une liste d'interfaces de périphériques spécifiques, la règle s'applique et est déployée uniquement aux périphériques qui ont des interfaces dans les zones spécifiées. Les périmètres de sécurité ne se limitent pas simplement aux noms d'interface, mais aux paires « interface sur périphérique ». Par exemple, « inside on device1 » pourrait se trouver dans une zone qui ne contient pas inside on device2 ».

Le tableau suivant présente les principales fonctionnalités de contrôle d'accès pour les ASA, ainsi que l'endroit où vous devez les configurer, ou leurs équivalents, sur un périphérique Cisco Secure Firewall Threat Defense.

Tableau 9 : Fonctionnalités de contrôle d'accès

Fonctionnalité ASA	Fonctionnalité Défense contre les menaces (Threat Defense) dans Cisco Secure Firewall Management Center	Notes
Objets pour le contrôle d'accès.	**Objets** Chemin de l'interface utilisateur : **Objects (Objets)** > **Object Management (Gestion des objets)**. Consultez la section : Gestion des objets. Instructions : configurer les objets dynamiques	Vous pouvez également créer des objets de réseau et de port (service) lors de la modification de la politique de contrôle d'accès. Les balises de groupes de sécurité et les plages de temps sont également prises en charge. Les groupes d'utilisateurs locaux et de service en réseau ne sont pas pris en charge (ou sont nécessaires). Objets supplémentaires que vous pouvez utiliser dans les règles de contrôle d'accès : filtres d'application, géolocalisation, périmètres de sécurité d'interface, URL et balise VLAN. Ces objets s'appliquent aux fonctionnalités non disponibles sur les ASA.
Listes de contrôle d'accès (ACL) pour les groupes et les règles de contrôle qui ne sont pas des éléments de contrôle d'accès.	**Listes de contrôle d'accès (ACL)** Chemin de l'interface utilisateur : ACL standard et ACL étendues : **Objects (objets)** > **Object Management (Gestion des objets)**. Ethertype ACLs (ACL) : **Devices (Périphériques)** > **FlexConfig**. Consultez les sections : Gestion des objets et Politiques FlexConfig. Instructions : • Configurer le filtrage du trafic pour les connexions VPN d'accès à distance (RA) : créer une liste d'accès étendue pour filtrer le trafic sur une connexion VPN RA, ajouter une liste d'accès étendue à une stratégie de groupe pour filtrer le trafic sur une connexion VPN RA.	Vous créez des objets pour les listes de contrôle d'accès standard ou étendues, puis utilisez ces objets lors de la configuration du routage ou d'autres fonctionnalités qui nécessitent des listes de contrôle d'accès.

Fonctionnalité ASA	Fonctionnalité Défense contre les menaces (Threat Defense) dans Cisco Secure Firewall Management Center	Notes
Règles de contrôle d'accèsde base (réseau, port, protocole, ICMP).	**Règles de contrôle d'accès** Chemin de l'interface utilisateur : **Policies (Politiques)** > **Access Control (Contrôle d'accès)**. Consultez la section : Règles de contrôle d'accès. Instructions : • Configurer votre périphérique. Ajouter une règle de contrôle d'accès. Entrer une procédure pas à pas de fonctionnalité. Créer une politique de contrôle d'accès. • Configurer un tunnel VTI : configurer une règle de contrôle d'accès afin de permettre le trafic chiffré via VTI • La nouvelle interface utilisateur Access Control Policy UI (Interface utilisateur de la politique de contrôle d'accès) — A Feature Walkthrough (Visite virtuelle des fonctionnalités), Accessing the New AC Policy UI (Accès à la nouvelle interface utilisateur de la politique AC), Rules Table (Tableau des règles), Rule Creation (Création de règles), Rule Editing (Modification de règles).	La politique de contrôle d'accès prend en charge les règles de contrôle d'accès de type 5-tuple de base et VLAN. De plus, vous pouvez utiliser des objets de géolocalisation pour cibler des adresses IP associées à des emplacements géographiques particuliers. Vous pouvez également utiliser des règles de préfiltrage pour contrôler le trafic en tunnel (comme GRE) et d'autres trafics de type 5-tuple. Les règles de préfiltrage sont traitées avant les règles de contrôle d'accès et ne sont pas disponibles sur les ASA. Consultez les sections**Politiques** > **Préfiltre**.
Règles de contrôle d'accès; contrôle basé sur l'utilisateur	**Règles de contrôle d'accès** Chemin de l'interface utilisateur : pour configurer les règles d'obtention des correspondances entre le nom d'utilisateur et les groupes, accédez à **Policies (Politiques)** > **Identity (Identité)**. Vous pouvez ensuite sélectionner des noms d'utilisateur et des groupes dans les règles de contrôle d'accès ; **Policies (Politiques)** > **Access Control (Contrôle d'accès**. Consultez les sections : Règles de contrôle d'accès et Politiques d'identité de l'utilisateur. Instructions : configurer une règle de politique de contrôle d'accès pour un objet dynamique	Il existe davantage d'options pour obtenir des informations sur l'appartenance des utilisateurs ou des groupes par rapport aux ASA.
Règles de contrôle d'accès – groupe de sécurité et Trustsec	**Règles de contrôle d'accès** Chemin de l'interface utilisateur : Pour configurer le moteur de services de vérification des identités (ISE) de Cisco, accédez à **Integration (Intégration)** > **Other Integrations (Autres intégrations)** > **Identity Sources (Sources d'identité)**. Vous pouvez ensuite sélectionner les balises de groupe de sécurité dans les règles de contrôle d'accès ; **Policies (Politiques)** > **Access Control (Contrôle d'accès)**. Consultez les sections : Règles de contrôle d'accès et Contrôle utilisateur avec ISE/ISE-PIC.	Vous pouvez également utiliser le moteur du service de vérification des identités pour recueillir des informations sur le nom d'utilisateur ou le groupe d'utilisateurs à des fins de contrôle basé sur l'utilisateur.

Fonctionnalité ASA	Fonctionnalité Défense contre les menaces (Threat Defense) dans Cisco Secure Firewall Management Center	Notes
(Non disponible sur les ASA.) Règles de contrôle d'accès : contrôle des applications de couche 7.	**Règles de contrôle d'accès** Chemin de l'interface utilisateur : **Policies (Politiques)** > **Access Control (Contrôle d'accès)**. Consultez la section : Règles de contrôle d'accès.	Vous pouvez écrire des règles de contrôle d'accès pour des applications qui utilisent autrement le même protocole et le même port, ce qui vous permet de différencier différents types de trafic HTTP/HTTPS, par exemple Le filtrage des applications peut vous aider à appliquer un contrôle plus granulaire que ce qui est disponible sur les ASA.
Règles de contrôle d'accès– filtrage des URL.	**Règles de contrôle d'accès** Chemin de l'interface utilisateur : **Policies (Politiques)** > **Access Control (Contrôle d'accès)**. Consultez la section : Filtrage des URL.	Nécessite une licence de filtrage des URL pour contrôler l'accès en fonction de la catégorie et de la réputation de l'URL. Vous pouvez également utiliser la politique de renseignements de sécurité définie dans une politique de contrôle d'accès pour effectuer un filtrage anticipé en fonction de l'URL ou d'un objet réseau. La stratégie DNS peut faire la même chose pour les demandes de consultation de systèmes de noms de domaine.
Règles d'accès ICMP pour le trafic adressé au périphérique (commandes **icmp permit/deny** et **ipv6 icmp permit/deny**.)	**Règles d'accès ICMP** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **Platform Settings (Paramètres de plateforme)** , page **ICMP Access** (Accès ICMP) . . Consultez la section : Paramètres de la plateforme.	Tout comme la politique de contrôle d'accès, la politique des paramètres de la plateforme est partagée et vous pouvez l'appliquer à plusieurs appareils.
Cisco Umbrella	**Cisco Umbrella** Chemin de l'interface utilisateur : **Integration (Intégration)** > **Other Integrations (Autres intégrations)** > **Cloud Services (Services Cloud)** **Policies (Politiques)** > **DNS** **Devices (Périphériques)** > **VPN : Site-to-Site (Site à site)** > **SASE Topology (+Topologie SASE)**. Consultez les sections : Politiques DNS et VPN de site à site pour Cisco Secure Firewall Threat Defense.	Vous pouvez créer des politiques DNS Cisco Umbrella et des topologies VPN Cisco Umbrella SASE.

NAT (Network Address Translation; Translation d'adresses de réseau)

Tout comme la stratégie de contrôle d'accès, la stratégie de traduction d'adresses réseau (NAT) est partagée. Vous créez la stratégie NAT, puis vous l'affectez à un ou plusieurs périphériques. La stratégie FlexConfig est également partagée.

Le déploiement d'une règle NAT donnée sur un périphérique dépend du fait que vous limitiez la règle par interface ou que vous l'appliquiez à toutes les interfaces.

- Si vous ne spécifiez aucune interface, la règle s'applique à tous les périphériques auxquels la stratégie est assignée.
- Si vous spécifiez des objets d'interface, la règle s'applique uniquement aux périphériques qui possèdent ces interfaces et elle est déployée sur ceux-ci.

Le tableau suivant présente les principales fonctionnalités de traduction d'adresses réseau pour l'ASA et précise où vous pouvez les configurer, ou leurs équivalents, sur un périphériqu Cisco Secure Firewall Threat Defense.

Tableau 10 : Fonctionnalités de traduction d'adresses réseau

Fonctionnalité ASA	Fonctionnalité Défense contre les menaces (Threat Defense) dans Cisco Secure Firewall Management Center	Notes
Traduction d'adresses réseau (NAT) :NAT dynamique/NAT PAT, NAT statique, NAT d'identité.	**Traduction d'adresses réseau (NAT)** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **NAT**. Consultez la section : Traduction d'adresse réseau (NAT). Instructions : • Configurer votre périphérique : créer une stratégie NAT de fonction : guide fonctionnel • Configurer le routage virtuel : fournir un accès Internet avec des espaces d'adressag superposés, configurer la NAT pour un routeur virtuel	Vous pouvez configurer à la fois l'objet et deux fois la NAT. Cependant, elles sont appelées NAT automatique et NAT manuelle dans Cisco Secure Firewall Threat Defense.
Traduction d'adresses de port (PAT) avec allocation de blocs de ports.	**Traduction d'adresses de port (PAT) avec allocation de blocs de ports**. Chemin de l'interface utilisateur : pour configurer les paramètres d'allocation de port PAT global (commande **xlate block-allocation**), utilisez **Devices (Périquériques)** > **FlexConfig**. Vous pouvez ensuite configurer les règles PAT via **Devices (Périphériques)** > **NAT** Consultez la section : Politiques de traduction d'adresses réseau (NAT) et FlexConfig.	Cette fonctionnalité est utilisée pour la PAT à grande échelle ou de niveau opérateur.

Fonctionnalité ASA	Fonctionnalité Défense contre les menaces (Threat Defense) dans Cisco Secure Firewall Management Center	Notes
PAT par session ou PAT multisession (la commande **xlate per-session**).	**PAT par session ou PAT multisession** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **FlexConfig**. Consultez la section : Politiques FlexConfig.	La configuration par défaut de Cisco Secure Firewall Threat Defense comprend les mêmes règles de session prédéfinies que l'ASA. La configuration est nécessaire uniquement si vous souhaitez un comportement personnalisé.
Mappage de l'adresse et du port (MAP)	**Mappage de l'adresse et du port (MAP)** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **FlexConfig**. Consultez la section : Politiques FlexConfig.	Le mappage de l'adresse et du port (MAP) est conçu pour la traduction d'adresses IPv4 vers IPv6 à l'échelle opérateur.

Inspection des applications

Snort est le principal moteur d'inspection sur un périphérique Cisco Secure Firewall Threat Defense. Toutefois, les inspections ASA continuent de s'exécuter et sont appliquées avant l'inspection Snort.

Comme Snort effectue une grande partie de l'inspection HTTP, le moteur d'inspection HTTP de l'ASA n'est pas du tout pris en charge et vous ne pouvez pas le configurer.

De nombreux moteurs d'inspection ASA sont activés par défaut avec leurs paramètres par défaut. Dans les cas où le moteur d'inspection ASA prend en charge une configuration supplémentaire, vous devez utiliser FlexConfig (une politique partagée) pour configurer ces paramètres. Si vous utilisez les mêmes paramètres sur plusieurs périphériques, vous pouvez créer une seule politique FlexConfig pour vos paramètres d'inspection et l'appliquer à tous les périphériques concernés.

Si vous souhaitez simplement activer ou désactiver une inspection, vous pouvez utiliser la commande **configure inspection** dans l'interface CLI du périphérique, comme alternative à FlexConfig. Cependant, toutes les inspections de protocoles possibles ne sont pas offertes avec cette commande.

Le tableau suivant présente les différents moteurs d'inspection ASA et indique ceux qui sont activés par défaut sur un périphérique Cisco Secure Firewall Threat Defense.

Tableau 11 : Fonctionnalités d'inspection des applications

Fonctionnalité ASA	Fonctionnalité Défense contre les menaces (Threat Defense) dans Cisco Secure Firewall Management Center	Notes
Inspection des protocoles Internet de base	**Inspection** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **FlexConfig**. Consultez la section : Politiques FlexConfig.	Voici les inspections prises en charge. Le texte en gras indique que l'inspection est activée dans la configuration par défaut. • DCERPC • **DNS** • **FTP** • **ICMP** • **Erreur ICMP** • ILS • **Options d'adresse IP** • Intercommunication IPsec • IPv6 • Lisp • **NetBIOS** • PPTP • **RSH** • SMTP/ESMTP • **SNMP** • **SQL*Net** • **Sun RPC** • **TFTP** • WAAS • XDMCP • VXLAN Non pris en charge (par Snort) : HTTP, IM (Messagerie instantanée), .

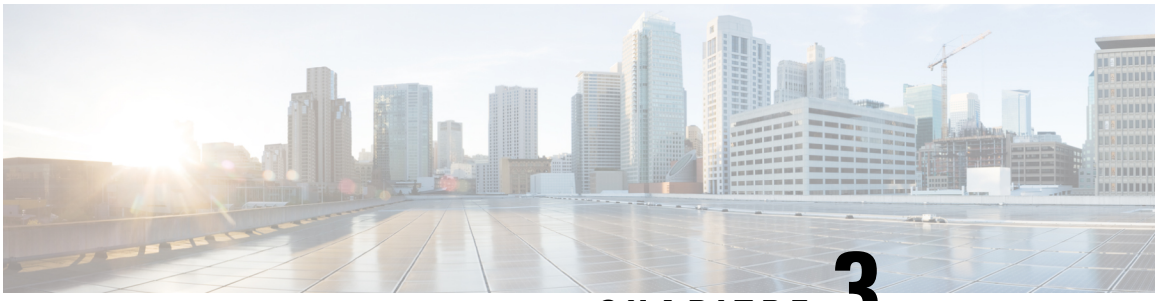
Fonctionnalité ASA	Fonctionnalité Défense contre les menaces (Threat Defense) dans Cisco Secure Firewall Management Center	Notes
Inspection des protocoles vocaux et vidéo	**Inspection** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **FlexConfig**. Consultez la section : Politiques FlexConfig.	Voici les inspections prises en charge. Le texte en gras indique que l'inspection est activée dans la configuration par défaut. • CTIQBE • **H.323 H.225** • **H.323 RAS** • MGCP • **RTSP** • **SIP** • **Skinny** • STUN
Inspection des réseaux mobiles.	**Inspection** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **FlexConfig**. Consultez la section : Politiques FlexConfig.	Voici les inspections prises en charge. Ces inspections nécessitent la licence Carrier. Aucune n'est activée par défaut. • Diamètre • GTP/GPRS • M3UA • SCTP • Comptabilité RADIUS (cette inspection ne nécessite pas la licence Carrier)

Politique de service, paramètres de connexion, détection des menaces

Le tableau suivant répertorie certaines fonctionnalités faiblement liées qui contrôlent certains aspects des connexions qui passent par le périphérique. La plupart de ces paramètres ont des valeurs par défaut qui fonctionnent dans la plupart des cas.

Tableau 12 : Politique de service, paramètres de connexion, fonctionnalités de détection des menaces

Fonctionnalité ASA	Fonctionnalité Défense contre les menaces (Threat Defense) dans Cisco Secure Firewall Management Center	Notes
Délais d'expiration globaux	**Délais d'expiration globaux** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **Platform Settings (Paramètres de plateforme)**, page **Timeouts** (Délai d'expiration). Consultez la section : Paramètres de la plateforme.	Les paramètres de plateforme constituent une politique partagée. Ces paramètres sont appliqués à chaque appareil auquel la politique est attribuée.
Politique de service pour les paramètres de connexion	**Politique du service Threat Defense** Chemin de l'interface utilisateur : **Policies (Politiques)** > **Access Control (Contrôle d'accès)**, puis lors de la modification d'une politique, recherchez **Threat Defense Service Policy (Politique de service de défense contre les menaces)** dans **Advanced Settings (Paramètres avancés)**. Consultez la section : Politiques de service.	Ces paramètres incluent **le contournement de l'état TCP**, **la randomisation des séquences TCP**, **l'interception TCP**, **la détection des connexions inactives (DCD)**, **la normalisation TCP** et les limites générales de connexion et délais d'expiration par classe de trafic. La politique de service de défense contre les menaces est définie dans le cadre de la politique de contrôle d'accès, qui est une politique partagée que vous affectez à un ou plusieurs périphériques. Toutes les règles que vous limitez à des interfaces précises ne sont configurées que sur les périphériques qui incluent cette interface. Les règles globales sont appliquées à chaque périphérique auquel la politique de contrôle d'accès est affectée.
Qualité de service (QoS)	**Qualité de service (QoS)** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **QoS**. Conslutez la section : Qualité de service.	La politique de QoS est partagée, mais chaque règle de la politique doit spécifier une ou plusieurs interfaces. Une règle est configurée sur un périphérique uniquement si cette règle inclut une interface présente sur le périphérique.
Détection des menaces (la commande **threat-detection**).	**Détection des menaces** Chemin de l'interface utilisateur : **Policies (Politiques)** > **Access Control (Contrôle d'accès)**, puis, lors de la modification d'une politique, recherchez **Threat Detection (Détection de menaces)** dans **Advanced Settings (Paramètres avancés)**. Conslutez la section : Détection des menaces.	La fonctionnalité Cisco Secure Firewall Threat Defense ne correspond pas exactement à la fonctionnalité ASA, mais elle inclut de nouvelles capacités. Vous pouvez également utiliser FlexConfig pour déployer les versions de commande ASA.



CHAPITRE 3

Fonctionnalités de réseau privé virtuel (VPN)

Ce chapitre fournit des informations générales pour configurer les fonctionnalités de réseau privé virtuel ASA dans Cisco Secure Firewall Threat Defense à l'aide de Cisco Secure Firewall Management Center.

VPN de site à site

Tableau 13 : VPN de site à site

Fonctionnalité ASA	Fonctionnalité Défense contre les menaces (Threat Defense) dans Cisco Secure Firewall Management Center	Notes
IPsec de LAN à LAN	**VPN basé sur des politiques** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **Site To Site (Site à site)** > **Policy Based (Basé sur une stratégie) (Crypto Map (Carte crypto))**. Consultez la section : Configurer un VPN de site à site basé sur une politique. Instructions : configurer un VPN de site à site basé sur des politiques, personnaliser les options IKE pour un déploiement VPN de site à site existant, personnaliser les options IPsec pour un déploiement VPN de site à site existant, personnaliser les paramètres avancés pour un déploiement VPN de site à site	Le centre de gestion fournit un seul assistant pour configurer le VPN sur les homologues.

Fonctionnalité ASA	Fonctionnalité Défense contre les menaces (Threat Defense) dans Cisco Secure Firewall Management Center	Notes
Virtual Tunnel Interface (VTI)	**VPN basé sur le routage** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **Site To Site (Site à site)** > **Route Based (VTI) (Basé sur le routage (VTI))**. Consultez la section : Créer un VPN de site à site basé sur le routage. Instructions : créer un VPN basé sur le routage (VTI), configurer une route statique pour VTI, configurer le routage BGP pour VTI, configurer une règle de contrôle d'accès pour autoriser le trafic chiffré sur VTI	La création d'un VPN entre un concentrateur avec un VTI dynamique et des rayons avec des VTI statiques est beaucoup plus facile dans centre de gestion à l'aide de l'assistant. Il n'y a pas d'assistant dans ASDM.
Cisco Umbrella SASE	**Déployer un tunnel SASE sur Umbrella** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **VPN** > **Site To Site (Site à site)** > **+SASE Topology (+Topologie SASE)**. Consultez la section : Déployer un tunnel SASE sur Cisco Umbrella.	
Superviser le VPN de site à site	**Superviser le VPN de site à site** Chemin de l'interface utilisateur : **Overview (Survol)** > **Dashboards (Tableaux de bord)** > **Site to Site VPN (VPN site à site)**. Consultez la section : Superviser le VPN de site à site.	

VPN d'accès à distance

Tableau 14 : VPN d'accès à distance

Fonctionnalité ASA	Fonctionnalité Défense contre les menaces (Threat Defense) dans Cisco Secure Firewall Management Center	Notes
VPN d'accès à distance IPsec – IKE v2	**Stratégie de VPN sur l'accès à distance** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **VPN** > **Remote Access (Accès à distance)** > **Policy Assignment (Attribution des politiques)** > **VPN Protocols (Protocoles VPN)** > **IPsec-IKEv2**. Consultez la section : Configuration d'une nouvelle connexion de VPN d'accès à distance. Instructions : • Configurer le filtrage du trafic pour les connexions VPN d'accès à distance (RA) : créer une liste d'accès étendue pour filtrer le trafic sur une connexion VPN RA, ajouter une liste d'accès étendue à une stratégie de groupe pour filtrer le trafic sur une connexion VPN RA. • Authentifier un VPN d'accès à distance (RA VPN) à l'aide d'un certificat : créer une table de correspondance des certificats pour l'authentification dans le VPN RA et associer une table de correspondance à un profil de connexion. • Créer et installer un certificat d'identité sur le périphérique pour la configuration d'un VPN d'accès à distance : utiliser un objet d'inscription de certificat PKCS12, un objet d'inscription manuel, un objet d'inscription autosigné ou SCEP, installer un certificat manuel, PKCS12, SCEP ou autosigné, puis configurer le VPN d'accès à distance. • Configurer le VPN : renouveler un certificat à l'aide d'un réenrôlement manuel, renouveler un certificat autosigné, SCEP ou EST, configurer une carte d'attributs LDAP pour le VPN d'accès à distance, ajouter un serveur d'authentification unique (SSO), configurer une stratégie d'accès dynamique pour le VPN d'accès à distance	La configuration d'un profil de connexion et d'un objet de stratégie de groupe reste identique dans le centre de gestion et dans l'ASA. Vous devez créer un objet de domaine pour créer des utilisateurs locaux et établir des connexions avec Active Directory/LDAP. Les domainess sont des connexions entre le centre de gestion et les comptes utilisateur sur les serveurs.
VPN SSL d'accès à distance	**Stratégie de VPN sur l'accès à distance** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **VPN** > **Remote Access (Accès à distance)** > **Policy Assignment (Attribution des politiques)** > **VPN Protocols (Protocoles VPN)** > **SSL**. Consultez la section : Configuration d'une nouvelle connexion de VPN d'accès à distance. Instructions : Configurer l'accès à distance au VPN	

Fonctionnalité ASA	Fonctionnalité Défense contre les menaces (Threat Defense) dans Cisco Secure Firewall Management Center	Notes
Équilibrage de la charge VPN	**Équilibrage de la charge VPN** Chemin de l'interface utilisateur : modifier le protocole VPN d'accès à distance. **Advanced (Avancé)** > **Load Balancing (Équilibreur de charge)**. Consultez la section : Configuration de l'équilibrage de charge du VPN.	L'équilibrage de charge VPN est un mécanisme permettant de distribuer équitablement le trafic VPN d'accès à distance entre les périphériques d'un groupe d'équilibrage de charge VPN.
Politiques d'accès dynamique	**Politiques d'accès dynamique** Chemin de l'interface utilisateur : **Devices (Périphériques)** > **Dynamic Access Policy (Politique d'accès dynamique)** . Consultez la section : Politiques d'accès dynamique. Instructions : Configurer la politique d'accès dynamique pour le VPN d'accès à distance.	Vous permet de configurer des autorisations qui tiennent compte de la dynamique des environnements VPN.
Surveillance du VPN	**Tableau de bord du VPN d'accès à distance** Chemin de l'interface utilisateur : **Overview (Survol)** > **Dashboards (Tableaux de bord)** > **Remote Access VPN (VPN d'accès à distance)** Consultez la section : Surveillance du VPN d'accès à distance.	
Analyse de l'hôte du Secure Client (services client sécurisés)	**Objets de fichiers VPN** Chemin de l'interface utilisateur : **Objects (Objets)** > **Object Management (Gestion des objets)** > **VPN** > **Secure Client File (Fichier client sécurisé)**. Consultez la section : Objets de fichier.	
Attributs personnalisés du Secure Client (services client sécurisés)	**Secure Client (services client sécurisés)Ajouter des objets attributs personnalisés AnyConnect** Chemin de l'interface utilisateur : **Objects (Objets)** > **Object Management(Gestion des objets)** > **VPN** > **Custom Attribute (Attributs personnalisés)**. Objets d'attributs personnalisés du client sécurisé.	

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.