Guide Cisco pour renforcer les périphériques Cisco IOS

Contenu

Chiffrez les sessions de Gestion
SSHv2
Améliorations SSHv2 pour des clés RSA
Console et ports AUX
Contrôle des lignes vty et tty
Contrôle du transport pour les lignes vty et tty
Messages d'avertissement
Authentification, autorisation, et comptabilité
Authentification TACACS+
Authentification de secours
Utilisation des mots de passe de type 7
Autorisation de commande avec TACACS+
Comptabilité de commandes TACACS+
Serveurs AAA redondants
Enrichissez le protocole SNMP
Chaînes de caractères de la communauté SNMP
Chaînes de caractères de la communauté SNMP avec ACL
Les ACL d´infrastructure
SNMP Views
SNMP Version 3
Protection du plan de gestion
Les meilleures pratiques de journalisation
Envoyer les journaux à un emplacement central
Niveau de journalisation
N´enregistrez pas à la console ou aux sessions de surveillance
Utiliser la journalisation mise en mémoire
Configurer l´interface de la source de journalisation
Configurer les horodatages des journalisations
Gestion de la configuration du logiciel Cisco IOS
Configuration Replace et Configuration Rollback
Exclusive Configuration Change Access
Cisco IOS Software Resilient Configuration
Logiciel de Cisco signé par Digital
Configuration Change Notification and Logging
Plan de contrôle
Durcissement général du plan de contrôle
Redirections ICMP IP
ICMP inaccessibles
ARP Proxy
Incidence CPU de limite du trafic d'avion de contrôle
Comprenez le trafic d'avion de contrôle
Les ACL d´infrastructure
Listes de contrôle d'accès de réception
CoPP
Protection du plan de contrôle

Limiteurs matériels de débit
BGP sécurisé
Protections de sécurité basées sur TTL
Authentification d´homologue de BGP avec MD5
Configurez les préfixes maximum
Préfixes BGP de filtre avec des listes de préfixes
Préfixes BGP de filtre avec des Listes d'accès de chemin d'Autonomous System
Protocoles sécurisés d'Interior Gateway
Authentification et vérification du protocole de routage avec Message Digest 5
Commandes Passive-Interface
Filtrage de route
Consommation des ressources liées au processus de routage
Sécurisez les premiers protocoles de Redondance de saut
Plan de données
Durcissement général du plan de données
Options IP de rejet sélectif
Désactiver le routage de la source IP
Désactiver les redirections ICMP
Désactiver ou limiter les diffusions dirigées par IP
Le trafic de transit de filtre avec le transit ACLs
Filtrage des paquets ICMP
Fragments IP de filtre
Support d'ACL pour le filtrage des options IP
Protections anti-spoofing
Unicast RPF
Protection de la source IP
Sécurité de port
Inspection dynamique d'ARP
ACL anti-spoofing
Incidence CPU de limite du trafic de plan de données
Fonctionnalités et types de trafic qui affectent le CPU
Filtre sur la valeur de TTL
Filtre sur la présence des options IP
Protection du plan de contrôle
Identification du trafic et retour arrière
Netflow
ACL de classification
Contrôle d'accès avec des VLAN Maps et des listes de contrôle d'accès de port
Contrôle d'accès avec VLAN Maps
Contrôle d'accès avec des PACL
Contrôle d'accès avec MAC
Utilisation de VLAN privé
VLAN isolés
VLAN de communauté
Ports proches

Introduction

Ce document décrit les informations pour vous aider à sécuriser vos périphériques du système de Cisco IOS®, qui augmente la Sécurité globale de votre réseau. Structuré autour des trois plans dans lesquels des fonctions d'un périphérique réseau peuvent être classées par catégorie, ce document fournit un aperçu de chaque fonctionnalité incluse et des références à la documentation apparentée.

Conditions préalables

Exigences

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Les trois plans fonctionnels d´un réseau, le plan de gestion, le plan de contrôle, et le plan de données, fournissent chacun une fonctionnalité différente qui doit être protégée.

- **Avion de Gestion** - L'avion de Gestion gère le trafic qui est envoyé au Cisco IOS périphérique et se compose des applications et des protocoles tels que le Protocole Secure Shell (SSH) et le Protocole SNMP (Simple Network Management Protocol).

- **Avion de contrôle** - Le plan de contrôle d'un périphérique de réseau traite le trafic qui est primordial pour mettre à jour la fonctionnalité de l'infrastructure réseau. Le plan de contrôle se compose des applications et des protocoles entre les périphériques réseau, qui inclut le Border Gateway Protocol (BGP), ainsi que les Interior Gateway Protocols (IGP) comme l'Enhanced Interior Gateway Routing Protocol (EIGRP) et l'Open Shortest Path First (OSPF).

- **Plan de données** - De plan de données les données en avant par un périphérique de réseau. Le plan de données n'inclut pas le trafic qui est envoyé au périphérique Cisco IOS local.

La couverture des fonctions de sécurité dans ce document fournit souvent assez de détails pour que vous configuriez la fonctionnalité. Cependant, dans les cas où elle ne le fait pas, la fonctionnalité est expliquée de telle manière que vous puissiez évaluer si une attention supplémentaire à la fonctionnalité est requise. Si possible et approprié, ce document contient des recommandations qui, si mises en application, aident à sécuriser un réseau.

Opérations sécurisées

Les opérations sécurisées du réseau sont un sujet substantiel. Bien que la majeure partie de ce document soit consacrée à la configuration sécurisée d'un périphérique Cisco IOS, les configurations à elles seules ne sécurisent pas complètement un réseau. Les procédures opérationnelles en service sur le réseau contribuent autant à la sécurité que la configuration des périphériques sous-jacents.

Ces sujets contiennent les recommandations opérationnelles que vous êtes avisé de mettre en application. Ces sujets mettent en valeur des domaines critiques spécifiques des fonctionnements du réseau et ne sont pas complets.

Surveiller les avis et les réponses de la sécurité Cisco

L'équipe de résolution d´incidents de sécurité des produits Cisco (PSIRT) crée et maintient des publications, généralement désignées sous le nom d´Avis PSIRT, pour les problèmes liés à la sécurité des Produits Cisco. La méthode utilisée pour la transmission des questions moins graves est Cisco Security Response. Les avis et les réponses de sécurité sont disponibles à http://www.cisco.com/go/psirt .

Des informations supplémentaires au sujet de ces véhicules de transmission sont disponibles dans Politique de vulnérabilité de la sécurité Cisco.

Afin de maintenir un réseau sécurisé, vous devez être au courant des avis et réponses de la sécurité Cisco qui ont été publiés. Vous devez avoir la connaissance d'une vulnérabilité avant que la menace qu'elle peut constituer au réseau puisse être évaluée. Référez-vous au Triage du risque pour des annonces de vulnérabilité de sécurité pour assistance dans cette évaluation.

Exploiter Authentication, Authorization, and Accounting (AAA)

Le cadre d'Authentification, autorisation et comptabilité (AAA) est essentiel aux périphériques de réseau sécurisé. Le cadre AAA fournit l'authentification des sessions de gestion et peut également limiter les utilisateurs à des commandes spécifiques définies par l´administrateur et enregistrer toutes les commandes saisies par tous les utilisateurs. Voyez la section d'authentification, d'autorisation, et de comptabilité de ce document pour plus d'informations sur la façon accroître l'AAA.

Centraliser la collection et la surveillance du journal

Afin d'acquérir des connaissances au sujet d'exister, émergeant, et les événements historiques ont associé aux incidents de sécurité, votre organisation doit avoir une stratégie unifiée pour se connecter et corrélation d'événement. Cette stratégie doit exploiter la journalisation de tous les périphériques réseau et utiliser les capacités de corrélation pré-packaged et personnalisables.

Après que la journalisation centralisée soit mise en application, vous devez développer une approche structurée pour l'analyse du journal et le suivi des incidents. Basé sur les besoins de votre organisation, cette approche peut aller d'un examen diligent simple des données de journal jusqu´à l'analyse avancée basée sur des règles.

Voir la section Meilleures pratiques de journalisation de ce document pour plus d'informations sur la façon mettre en application la journalisation sur les périphériques réseau Cisco IOS.

Utiliser les protocoles sécurisés quand c'est possible

Beaucoup de protocoles sont utilisés afin de transporter des données sensibles de gestion de réseau. Vous devez utiliser des protocoles sécurisés chaque fois que c´est possible. Un choix de protocole sécurisé inclut l'utilisation de SSH au lieu de Telnet de sorte que les données d'authentification et les informations de gestion soient chiffrées. En outre, vous devez utiliser des protocoles de transfert de fichiers sécurisés quand vous copiez des données de configuration. Un exemple est l'utilisation du Secure Copy Protocol (SCP) au lieu de FTP ou TFTP.

Voyez la section interactive sécurisée de sessions de Gestion de ce document pour plus d'informations sur la Gestion sécurisée des périphériques de Cisco IOS.

Obtenir la visibilité du trafic avec Netflow

Netflow vous permet de surveiller les flux de trafic du réseau. Initialement destiné à exporter les informations de trafic vers des applications de gestion de réseau, Netflow peut également être utilisé afin de montrer les informations de flux sur un routeur. Cette capacité vous permet de voir quel trafic traverse le réseau en temps réel. Que les informations de flux soient exportées ou non vers un collecteur distant, vous êtes avisés de configurer les périphériques de réseau pour Netflow de sorte qu'il puisse être utilisé réactivement si nécessaire.

D´autres informations sur cette fonctionnalité sont disponibles dans la section Identification du trafic et retour arrière de ce document et à http://www.cisco.com/go/netflow (clients enregistrés seulement).

Gestion de la configuration

La gestion de la configuration est un processus par lequel des modifications de configuration sont proposées, passées en revue, approuvées et déployées. Dans le contexte de configuration de périphérique Cisco IOS, deux aspects supplémentaires de gestion de la configuration sont critiques : archivage et sécurité de la configuration.

Vous pouvez employer les archives de configuration pour abandonner les modifications qui sont apportées aux périphériques de réseau. Dans un contexte de sécurité, les archives de configuration peuvent également être utilisées afin de déterminer quelles modifications de la sécurité ont été apportées et quand ces modifications se sont produites. En même temps que les données du journal de l'AAA, ces informations peuvent aider aux audits de sécurité des périphériques de réseau.

La configuration d'un périphérique Cisco IOS contient beaucoup de détails sensibles. Les noms d'utilisateur, les mots de passe et le contenu des listes de contrôle d'accès sont des exemples de ce type d'information. Le référentiel que vous utilisez pour archiver des configurations de périphérique Cisco IOS doit être sécurisé. Un accès non sécurisé à ces informations peut nuire à

la sécurité de tout le réseau.

Plan de gestion

Le plan de gestion se compose de fonctions qui accomplissent les buts de gestion du réseau. Ceci inclut les sessions interactives de Gestion qui utilisent le SSH, aussi bien que la statistiques-collecte avec le SNMP ou le NetFlow. Quand vous considérez la sécurité d'un périphérique de réseau, il est critique que le plan de gestion soit protégé. Si un incident lié à la sécurité peut miner les fonctions du plan de gestion, il peut vous être impossible de rétablir ou de stabiliser le réseau.

Ces sections de ce document détaillent les fonctions et les configurations de sécurité disponibles dans le logiciel Cisco IOS, qui aident à renforcer le plan de gestion.

Durcissement général du plan de gestion

Le plan de gestion est utilisé afin d'accéder, configurer et gérer un périphérique, ainsi que pour surveiller ses opérations et le réseau sur lequel il est déployé. Le plan de gestion est le plan qui reçoit et envoie le trafic pour les opérations de ces fonctions. Vous devez sécuriser le plan de Gestion et le plan de contrôle d'un périphérique, parce que les fonctionnements de l'avion de contrôle affectent directement des fonctionnements de l'avion de Gestion. Cette liste des protocoles est utilisée par le plan de gestion :

- Protocole SNMP
- Telnet
- Secure Shell Protocol
- Protocole de transfert de fichiers
- Trivial File Transfer Protocol
- Secure Copy Protocol
- TACACS+
- RADIUS
- Netflow
- Network Time Protocol
- Syslog

Des mesures doivent être prises pour assurer la survie des plans de gestion et de contrôle pendant les incidents liés à la sécurité. Si un de ces plans est exploité avec succès, tous les plans peuvent être compromis.

Gestion des mots de passe

Accès par contrôle de mots de passe aux ressources ou aux périphériques. Ceci est accompli par la définition d´un mot de passe ou secret qui est utilisé afin d'authentifier les demandes. Quand une demande est reçue pour l'accès à une ressource ou à un périphérique, la demande est contestée pour la vérification du mot de passe et de l'identité, et l'accès peut être accordé, refusé ou limité basé sur le résultat. Comme meilleure pratique de sécurité, les mots de passe doivent être gérés avec un serveur d'authentification TACACS+ ou RADIUS. Cependant, notez qu'un mot de passe localement configuré pour l'accès privilégié est nécessaire toujours en cas de la panne du TACACS+ ou des services RADIUS. Un périphérique peut également avoir d'autres informations relatives au mot de passe présentes dans sa configuration, comme une clé NTP, la chaîne de communauté SNMP ou la clé du protocole de routage.

La commande **enable secret** est utilisée pour définir le mot de passe qui accorde l'accès administratif privilégié au système Cisco IOS. La commande **enable secret** doit être utilisée, plutôt que la commande plus ancienne **enable password**. La commande **enable password** utilise un algorithme de chiffrement faible.

Si aucune enable secret n'est défini et un mot de passe est configuré pour la ligne tty de la console, le mot de passe de la console peut être utilisé afin de recevoir l'accès privilégié, même d'une session du téléscripteur virtuel distant (vty). Cette action est presque certainement non désirée et est une autre raison d'assurer la configuration d'une enable secret.

La commande de configuration globale **service password-encryption** instruit le logiciel Cisco IOS de chiffrer les mots de passe, les secrets du protocole d'authentification CHAP (Challenge Handshake Authentication Protocol), et les données semblables qui sont enregistrées dans son fichier de configuration. Un tel chiffrement est utile afin d'empêcher les observateurs occasionnels de lire les mots de passe, comme lorsqu´ils regardent l'écran au-dessus du rassemblement d'un administrateur. Cependant, l'algorithme utilisé par la **commande service password-encryption** est un Vigen simple au sujet de chiffrement. L'algorithme n'est pas conçu pour protéger les fichiers de configuration contre une analyse sérieuse par même des attaquants légèrement sophistiqués et ne doit pas être utilisé à cet effet. N'importe quel fichier de configuration de Cisco IOS qui contient des mots de passe chiffrés doit être traité avec le même soin qui est utilisé pour une liste en libellé de ces mêmes mots de passe.

Bien que cet algorithme de chiffrement faible ne soit pas utilisé par la commande **enable secret**, il est utilisé par la commande de configuration globale **enable password**, ainsi que par la commande **password line configuration**. On doit éliminer les mots de passe de ce type et la commande **enable secret** ou la fonctionnalité Enhanced Password Security doivent être utilisées.

La commande **enable secret** et la fonctionnalité Enhanced Password Security utilisent Message Digest 5 (MD5) pour le hachage du mot de passe. Cet algorithme a eu une revue publique considérable et n'est pas connu pour être réversible. Cependant, l'algorithme est sujet à des attaques de dictionnaire. Dans une attaque de dictionnaire, un attaquant essaye chaque mot d´un dictionnaire ou autre liste de mots de passe candidats afin de rechercher une correspondance. Par conséquent, les fichiers de configuration doivent être stockés de manière sécurisée et seulement partagés avec des personnes de confiance.

Enhanced Password Security

La fonctionnalité Enhanced Password Security, introduite dans le Logiciel Cisco IOS Version 12.2(8)T, permet à un administrateur de configurer le hachage MD5 des mots de passe pour la commande **username**. Avant cette fonctionnalité, il y avait deux types de mots de passe : Type 0, qui est un mot de passe de libellé, et type 7, qui utilise l'algorithme du Vigen au sujet du

chiffrement. La fonctionnalité Enhanced Password Security ne peut pas être utilisée avec les protocoles qui exigent du mot de passe libellé d'être recouvrable, comme le protocole CHAP.

Afin de chiffrer un mot de passe utilisateur avec le hachage MD5, émettez la commande de configuration globale **username secret**.

```
!

username <name> secret <password>

!
```

Référez-vous à Enhanced Password Security pour plus d'informations sur cette fonctionnalité.

Login Password Retry Lockout

La fonctionnalité Login Password Retry Lockout, ajoutée dans le Logiciel Cisco IOS version 12.3(14)T, te permet pour verrouiller un compte d'utilisateur local après qu'un nombre configuré de tentatives infructueuses de procédure de connexion. Une fois qu'un utilisateur est bloqué, son compte est verrouillé jusqu'à ce que vous le déverrouilliez. Un utilisateur autorisé qui est configuré avec le niveau de privilège 15 ne peut pas être verrouillé avec cette fonction. Le nombre d'utilisateurs avec le niveau de privilège 15 doit être maintenu à un minimum.

Notez que les utilisateurs autorisés peuvent se verrouiller eux-mêmes en dehors d'un périphérique si le nombre de tentatives de connexion infructueuses est atteint. En outre, un utilisateur malveillant peut créer un état de déni de service (DoS) avec des tentatives répétées d'authentification avec un nom d'utilisateur valide.

Cet exemple montre comment activer la fonctionnalité Login Password Retry Lockout :

```
!

aaa new-model
aaa local authentication attempts max-fail <max-attempts>
aaa authentication login default local

!

username <name> secret <password>

!
```

Cette fonctionnalité s'applique également aux méthodes d´authentification telles que les protocoles CHAP et PAP (Password Authentication Protocol).

Aucune récupération de mot de passe de service

Dans le Logiciel Cisco IOS Versions 12.3(14)T et ultérieure, la fonctionnalité No Service Password-Recovery empêche quiconque avec accès par console d´accéder de façon non sécurisée à la configuration du périphérique et d´effacer le mot de passe. Elle également ne permet pas aux utilisateurs malveillants de changer la valeur du registre de configuration et d'accéder NVRAM.

```
!

no service password-recovery

!
```

Le logiciel de Cisco IOS fournit une procédure de récupération de mot de passe qui compte lors de l'accès au mode moniteur ROM (ROMMON) utilisant la touche d'interruption pendant le démarrage du système. Dans ROMMON, le logiciel de périphérique peut être rechargé afin d'inciter une nouvelle configuration de système qui inclut un nouveau mot de passe.

La procédure de récupération de mot de passe actuelle permet à n'importe qui avec l'accès par console pour accéder au périphérique et son réseau. La caractéristique de No Service Password-Recovery empêche la fin de la séquence de touche d'interruption et entrer de ROMMON pendant le démarrage du système.

Si **no service password-recovery** est activé sur un périphérique, il est recommandé qu'une copie hors ligne de la configuration du périphérique soit enregistrée et qu'une solution d´archivage de configuration soit mise en application. S'il est nécessaire de récupérer le mot de passe d'un périphérique Cisco IOS une fois que cette fonctionnalité est activée, la configuration entière est supprimée.

*Référez-vous à l'*exemple sécurisé de configuration ROMMON pour plus d'informations sur cette caractéristique.

Désactiver les services inutilisés

Comme meilleure pratique de sécurité, n'importe quel service inutile doit être désactivé. Ces services inutiles, particulièrement ceux qui utilisent le Protocole UDP (User Datagram Protocol), sont rarement utilisés pour les raisons légitimes mais peuvent être utilisés afin de lancer le DOS et d'autres attaques qui sont autrement empêchées par filtrage des paquets.

Les petits services TCP et UDP doivent être désactivés. Ces services incluent :

- écho (numéro de port 7)
- jeter (numéro de port 9)
- journée (numéro de port 13)
- chargen (numéro de port 19)

Bien que l'abus des petits services puisse être évité ou être rendu moins dangereux par des listes d'accès anti-spoofing, les services doivent être désactivés sur n'importe quel périphérique accessible dans le réseau. Les petits services sont désactivés par défaut dans le logiciel Cisco IOS versions 12.0 et ultérieures. Dans les logiciels antérieurs, les commandes de configuration globale **no service tcp-small-servers** et **no service udp-small-servers** peuvent être émis afin de les désactiver.

Ceci est une liste des services supplémentaires qui doivent être désactivés si pas en service :

- Émettez la commande de configuration globale **no ip finger** afin de désactiver le service Finger. Les versions ultérieures à 12.1(5) et 12.1(5)T du logiciel Cisco IOS désactivent ce service par défaut.

- Émettez la commande de configuration globale **no ip bootp server** afin de désactiver le protocole Bootstrap (BOOTP).

- Dans les versions 12.2(8)T et ultérieures du logiciel Cisco IOS, émettez la commande en mode de configuration globale **ip dhcp bootp ignore** afin de désactiver BOOTP. Ceci laisse activés les services DHCP (Dynamic Host Configuration Protocol).

- Les services DHCP peuvent être désactivés si les services de relais DHCP ne sont pas requis. Émettez la commande **no service dhcp** dans le mode de configuration globale.

- Émettez la commande **no mop enabled** dans le mode de configuration de l'interface afin de désactiver le service MOP (Maintenance Operation Protocol).

- Émettez la commande de configuration globale **no ip domain-lookup** afin de désactiver les services de résolution DNS (Domain Name System).

- Émettez la commande de configuration globale **no service pad** afin de désactiver le service PAD (Packet Assembler/Disassembler), qui est utilisé pour des réseaux X.25.

- Le serveur HTTP peut être désactivé avec l'**aucune** commande d'**ip http server** en mode de configuration globale, et le serveur sécurisé du HTTP (HTTPS) peut être désactivé avec l'**aucune** commande de configuration globale d'**ip http secure-server**.

- Àmoins que les périphériques Cisco IOS récupèrent des configurations du réseau pendant le démarrage, la commande de configuration globale **no service config** doit être utilisée. Ceci empêche le périphérique de Cisco IOS d'une tentative de localiser un fichier de configuration sur le réseau avec le TFTP.

- Le protocole CDP (Cisco Discovery Protocol) est un protocole de réseau qui est utilisé pour découvrir d'autres périphériques activés par CDP pour la contiguïté de voisins et la topologie du réseau. Le CDP peut être utilisé par NMS (Network Management Systems) ou pendant le dépannage. Le CDP doit être désactivé sur toutes les interfaces qui sont connectées aux réseaux non sécurisés. Ceci est accompli avec la commande d´interface **no cdp enable**. Alternativement, CDP peut être désactivé globalement avec la commande de configuration globale **no cdp run**. Notez que le CDP peut être utilisé par un utilisateur malveillant pour la reconnaissance et le mappage de réseau.

- Le protocole LLDP (Link Layer Discovery Protocol) est un protocole IEEE qui est défini dans 802.1AB. Le LLDP est semblable à CDP. Cependant, ce protocole permet l'interopérabilité entre d'autres périphériques qui ne supportent pas CDP. Le LLDP doit être traité de la même manière que le CDP et être désactivé sur toutes les interfaces qui se connectent aux réseaux non sécurisés. Afin d'accomplir ceci, émettez les commandes de configuration d'interface **no lldp transmettent** et **no lldp receive**. Émettez la commande de configuration globale **no lldp run** afin de désactiver le LLDP globalement. Le LLDP peut également être utilisé par un utilisateur malveillant pour la reconnaissance et le mappage d´un réseau.

- Pour les Commutateurs qui prennent en charge l'initialisation du sdflash, la Sécurité peut être

améliorée en amorçant de l'éclair et en désactivant le sdflash avec la commande de configuration de « aucun sdflash ».

EXEC Timeout

Afin de définir l'intervalle que l'interpréteur de commande EXEC attend pour une entrée de l´utilisateur avant de terminer la session, émettez la commande de configuration de ligne **exec-timeout**. La commande **exec-timeout** doit être utilisée afin de fermer des sessions sur les lignes vty ou tty qui sont inactives. Par défaut, des sessions sont déconnectées après dix minutes d'inactivité.

```
!

line con 0
exec-timeout <minutes> [seconds]
line vty 0 4
exec-timeout <minutes> [seconds]
!
```

Keepalives pour les sessions TCP

Le service tcp-keepalives-in et les commandes de configuration globale de **service tcp-keepalives-out** permettent à un périphérique d'envoyer le Keepalives de TCP pour des sessions TCP. Cette configuration doit être utilisée afin d'activer des TCP keepalives sur des connexions en entrée au périphérique et aux connexions en partance du périphérique. Ceci assure que le périphérique à l´extrémité distante de la connexion est encore accessible et que les connexions semi-ouvertes ou orphelines sont supprimées du périphérique local Cisco IOS.

```
!

service tcp-keepalives-in
service tcp-keepalives-out
!
```

Utilisation d'interface de gestion

Le plan de gestion d'un périphérique est accédé intrabande ou hors bande sur une interface de gestion physique ou logique. Dans le meilleur des cas, l'accès de gestion in-band et out-of-band existe pour chaque périphérique réseau de sorte que le plan de gestion puisse être accédé pendant les pannes du réseau.

Une des interfaces les plus communes qui est utilisée pour l'accès in-band à un périphérique est l'interface de bouclage logique. Les interfaces de bouclage sont toujours actives, tandis que les interfaces physiques peuvent changer d'état, et l´interface peut ne pas être accessible. Il est recommandé d'ajouter une interface de bouclage à chaque périphérique comme interface de gestion et qu´elle soit utilisée exclusivement pour le plan de gestion. Ceci permet à l'administrateur d'appliquer les politiques dans tout le réseau pour le plan de gestion. Une fois que l'interface de bouclage est configurée sur un périphérique, elle peut être utilisée par les protocoles du plan de gestion, tels que SSH, SNMP et Syslog, afin d'envoyer et de recevoir du trafic.

```
!
interface Loopback0
```

```
 ip address 192.168.1.1 255.255.255.0
!
```

Memory Threshold Notifications

La fonctionnalité Memory Threshold Notification, ajoutée au logiciel Cisco IOS Version 12.3(4)T, vous permet d´atténuer les états de mémoire saturée sur un périphérique. Cette caractéristique emploie deux méthodes afin d'accomplir ceci : Memory Threshold Notification et Memory Reservation.

Memory Threshold Notification produit un message du journal afin d'indiquer que la mémoire libre sur un périphérique est tombée plus bas qu´un seuil configuré. Cet exemple de configuration montre comment activer cette fonctionnalité avec la commande de configuration globale **memory free low-watermark**. Ceci permet à un périphérique de produire une notification quand la mémoire libre disponible tombe plus bas qu´un seuil spécifié, et de nouveau quand la mémoire libre disponible remonte à cinq pour cent du seuil spécifié.

```
!

memory free low-watermark processor <threshold>
memory free low-watermark io <threshold>
!
```

Memory Reservation est utilisé de sorte que la mémoire suffisante soit disponible pour des notifications critiques. Cet exemple de configuration explique comment activer cette fonctionnalité. Ceci s'assure que les processus de gestion continuent à fonctionner quand la mémoire du périphérique est épuisée.

```
!
memory reserve critical <value> !
```

Référez-vous à Memory Threshold Notifications pour plus d'informations sur cette fonctionnalité.

CPU Thresholding Notification

Introduit dans le Logiciel Cisco IOS Version 12.3(4)T, la fonctionnalité CPU Thresholding Notification vous permet de détecter et d´être notifié quand la charge CPU sur un périphérique dépasse un seuil configuré. Quand le seuil est franchi, le périphérique produit et envoie un message de déroutement SNMP. Deux méthodes de seuillage d'utilisation du CPU sont supportées sur le logiciel Cisco IOS : Rising Threshold et Falling Threshold.

Cet exemple de configuration montre comment activer les Rising et Falling Thresholds qui déclenchent un message de notification de seuil CPU :

```
!

snmp-server enable traps cpu threshold
!

snmp-server host <host-address> <community-string> cpu
!

process cpu threshold type <type> rising <percentage> interval <seconds>
[falling <percentage> interval <seconds>]
```

```
process cpu statistics limit entry-percentage <number> [size <seconds>]
!
```

Référez-vous à CPU Thresholding Notification pour plus d'informations sur cette fonctionnalité.

&

Reserve Memory for Console Access

Dans le Logiciel Cisco IOS Versions 12.4(15)T et ultérieure, la fonctionnalité Reserve Memory for Console Access peut être utilisée afin de réserver assez de mémoire pour assurer l'accès par console à un périphérique Cisco IOS pour des buts administratifs et de dépannage. Cette fonctionnalité est particulièrement bénéfique quand le périphérique fonctionne sur mémoire basse. Vous pouvez émettre la commande de configuration globale **memory reserve console** afin d'activer cette fonctionnalité. Cet exemple configure un périphérique Cisco IOS pour réserver 4096 kilo-octets à cet effet.

```
!
memory reserve console 4096
!
```

Référez-vous à Reserve Memory for Console Access pour plus d'informations sur cette fonctionnalité.

Memory Leak Detector

Introduite dans le logiciel Cisco IOS version 12.3(8)T1, la fonctionnalité Memory Leak Detector vous permet de détecter les fuites de mémoire sur un périphérique. Memory Leak Detector peut rechercher des fuites dans tous les pools de mémoire, tampons de paquets et blocs. Les fuites de mémoire sont des affectations statiques ou dynamiques de la mémoire qui n'atteignent aucun objectif utile. Cette fonctionnalité se concentre sur les allocations de mémoire qui sont dynamiques. Vous pouvez employer la commande EXEC **show memory debug leaks** afin de détecter si une fuite de mémoire existe.

Buffer Overflow : Détection et correction de la corruption de Redzone

Dans le logiciel Cisco IOS Versions 12.3(7)T et ultérieure, le Buffer Overflow : La détection et la correction de la fonctionnalité Redzone Corruption peut être activée sur un périphérique afin de détecter et corriger un débordement de bloc mémoire et de continuer les opérations.

Ces commandes de configuration globale peuvent être utilisées afin d'activer cette fonctionnalité. Une fois configurée, la commande **show memory overflow** peut être utilisée afin d'afficher les statistiques de détection et de correction d´un dépassement de mémoire tampon.

```
!
exception memory ignore overflow io
exception memory ignore overflow processor
!
```

Enhanced Crashinfo File Collection

La fonctionnalité Enhanced Crashinfo File Collection supprime automatiquement les vieux fichiers crashinfo. Cette caractéristique, ajoutée dans le Logiciel Cisco IOS version 12.3(11)T, permet à un

périphérique pour reprendre l'espace afin de créer de nouveaux fichiers crashinfo quand le périphérique tombe en panne. Cette fonctionnalité autorise également la configuration du nombre de fichiers crashinfo à enregistrer.

```
!
exception crashinfo maximum files <number-of-files>
!
```

Network Time Protocol

Le Network Time Protocol (NTP) n'est pas un service particulièrement dangereux, mais n'importe quel service inutile peut représenter un vecteur d'attaque. Si le NTP est utilisé, il est important de configurer explicitement une source temporelle de confiance et d'utiliser l'authentification appropriée. Une heure précise et fiable est requise pour Syslog, comme pendant les investigations légales d´attaques potentielles, ainsi que pour la connectivité réussie de VPN en cas de dépendance sur les certificats pour l´authentification de phase 1.

- **Fuseau horaire de NTP** - Quand vous configurez le NTP, le fuseau horaire doit être configuré de sorte que des horodateurs puissent être exactement corrélés. Il y a habituellement deux approches pour configurer le fuseau horaire pour des périphériques dans un réseau avec une présence globale. Une méthode est de configurer tous les périphériques réseau avec l´UTC (Coordinated Universal Time) (précédemment heure GMT (Greenwich Mean Time)). L'autre approche est de configurer les périphériques réseau avec le fuseau horaire local. Plus d'informations sur cette fonctionnalité peuvent être trouvées dans « clock timezone » dans la documentation du produit Cisco.

- **Authentification de NTP** - Si vous configurez l'authentification de NTP, elle fournit l'assurance que des messages de NTP sont permutés entre les pairs de confiance de NTP.

Configuration d'échantillon utilisant l'authentification de NTP :

Client :

```
(config)#ntp authenticate
(config)#ntp authentication-key 5 md5 ciscotime
(config)#ntp trusted-key 5
(config)#ntp server 172.16.1.5 key 5
```

Serveur :

```
(config)#ntp authenticate
(config)#ntp authentication-key 5 md5 ciscotime
(config)#ntp trusted-key 5
```

Le débronchement intelligent installent

Les pratiques recommandées de Sécurité autour de Cisco Smart installent la caractéristique (SMI) dépendent de la façon dont la caractéristique est utilisée dans un environnement spécifique de client. Cisco différencie ces cas d'utilisation :

- Les clients qui n'utilisent pas l'intelligent installent la caractéristique.
- Les clients qui accroissent l'intelligent installent la caractéristique seulement pour le

déploiement sans intervention.
- Les clients qui accroissent l'intelligent installent la caractéristique pour plus que le déploiement sans intervention (Gestion de configuration et d'image).

Ces sections décrivent chaque scénario en détail :

- Les clients qui n'utilisent pas l'intelligent installent la caractéristique.
- Les clients qui n'utilisent pas Cisco Smart installent la caractéristique, et exécutent une release de Cisco IOS et le Logiciel Cisco IOS XE version 2 où la commande est disponible, devrait désactiver l'intelligent installent la caractéristique avec l'**aucune** commande de **vstack**.

Note: La commande de **vstack** a été introduite dans la Cisco IOS version 12.2(55)SE03.

C'est sortie témoin de la commande de **vstack d'exposition** sur un commutateur Cisco Catalyst avec l'intelligent installent la fonctionnalité client désactivée :

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Les clients qui accroissent l'intelligent installent la caractéristique seulement pour le déploiement sans intervention

Désactivez l'intelligent installent la fonctionnalité de client après que l'installation de zéro-toucher soit complète ou n'utilisent l'**aucune** commande de **vstack**.

Afin de ne propager l'**aucune** commande de **vstack** dans le réseau, utilisez une de ces méthodes :

- Ne sélectionnez l'**aucune** commande de **vstack** sur tous les commutateurs client manuellement ou avec un script.
- N'ajoutez l'**aucune** commande de **vstack** en tant qu'élément de la configuration Cisco IOS qui est poussée dans chaque intelligent installent le client en tant qu'élément de l'installation de zéro-toucher.
- Dans les versions qui ne prennent en charge pas la commande de **vstack** (versions de Cisco IOS version 12.2(55)SE02 et antérieures), appliquez une liste de contrôle d'accès (ACL) sur des commutateurs client afin de bloquer le trafic sur le port 4786 de TCP.

Afin d'activer l'intelligent installez la fonctionnalité de client plus tard, sélectionnez la commande de **vstack** sur tous les commutateurs client manuellement ou avec un script.

Les clients qui accroissent l'intelligent installent la caractéristique pour plus que le déploiement sans intervention

Dans la conception d'un intelligent installez l'architecture, soin devrait être pris tels que l'espace d'adresse IP d'infrastructure n'est pas accessible aux interlocuteurs non approuvés. Dans des releases qui ne prennent en charge pas la commande de **vstack**, assurez-vous que seulement les intelligents installent le directeur font installer la Connectivité de TCP à tout l'intelligent des clients sur le port 4786.

Les administrateurs peuvent utiliser ces pratiques recommandées de Sécurité pour Cisco Smart installent des déploiements sur les périphériques affectés :

- Interface ACLs
- Réglementation du plan de commande (CoPP). Cette caractéristique n'est pas disponible

dans des toutes les versions logicielles de Cisco IOS.

Cet exemple affiche qu'un ACL d'interface avec l'intelligent installent l'adresse IP de directeur comme 10.10.10.1 et les intelligents installent l'adresse IP de client comme 10.10.10.200 :

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Cet ACL doit être déployé sur toutes les interfaces IP sur tous les clients. Il peut également être poussé par l'intermédiaire du directeur quand des Commutateurs sont d'abord déployés.

Afin de limiter plus loin l'accès à tous les clients dans l'infrastructure, les administrateurs peuvent employer ces pratiques recommandées de Sécurité sur d'autres périphériques dans le réseau :

- Listes de contrôle d'accès d'infrastructure (iACLs)
- Listes de contrôle d'accès VLAN (VACLs)

Limite Access au réseau avec l'infrastructure ACLs

Conçu pour empêcher la communication directe non autorisée aux équipements réseau, les listes de contrôle d'accès d'infrastructure (iACL) sont l'un des contrôles de sécurité les plus critiques qui peuvent être mis en application dans les réseaux. Les ACL d'infrastructure exploitent l'idée que presque tout le trafic sur le réseau traverse le réseau et n'est pas destiné au réseau lui-même.

Un iACL est construit et appliqué afin de spécifier des connexions des hôtes ou des réseaux qui doivent être permis aux périphériques de réseau. Des exemples communs de ces types de connexions sont eBGP, SSH et SNMP. Après avoir permis les connexions requises, tout autre trafic à l'infrastructure est explicitement refusé. Tout trafic de transit qui croise le réseau et n'est pas destiné aux périphériques d'infrastructure est alors explicitement autorisé.

Les protections fournies par les iACL sont pertinentes aux plans de gestion et de contrôle. La mise en place des iACL peut être facilitée par l'utilisation de l'adressage distinct pour des périphériques d'infrastructure réseau. Référez-vous à Une approche orientée sécurité de l'adressage IP pour plus d'informations sur les implications en matière de sécurité de l'adressage IP.

Cet exemple de configuration d´iACL illustre la structure qui doit être utilisée comme point de départ quand vous commencez le processus d'implémentation d'iACL :

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Une fois créé, l'iACL doit être appliqué à toutes les interfaces qui font face à des périphériques de non-infrastructure. Ceci inclut les interfaces qui se connectent à d'autres organismes, les segments d'accès à distance, les segments utilisateur et les segments aux centres de données.

Reportez-vous à Protection de votre noyau : Listes de contrôle d'accès de protection d'infrastructure pour plus d'informations sur les ACL d'infrastructure.

Filtrage des paquets ICMP

L'ICMP (Internet Control Message Protocol) est conçu comme protocole de contrôle IP. En tant

que tels, les messages qu´il transporte peuvent avoir des ramifications de grande envergure pour les protocoles TCP et IP en général. Tandis que les outils de dépannage de réseau **ping et traceroute** utilisent ICMP, la connectivité externe d'ICMP est nécessaire rarement pour l'opération appropriée d'un réseau.

Le logiciel de Cisco IOS fournit la fonctionnalité afin de filtrer spécifiquement des messages ICMP de nom ou taper et les coder. Cet exemple d´ACL, qui doit être utilisé avec les entrées de contrôle d'accès (ACE) des exemples précédents, permet des pings des stations de gestion et serveurs NMS de confiance et bloque tous les autres paquets ICMP :

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Fragments IP de filtre

Le procédé de filtration pour les paquets IP fragmentés peut lancer un défi aux périphériques de sécurité. C'est parce que l'information de couche 4 qui est utilisée afin de filtrer les paquets TCP et UDP est seulement présente dans le fragment initial. Le logiciel de Cisco IOS emploie une méthode spécifique afin de vérifier des fragments non initiaux contre les Listes d'accès configurées. Le logiciel Cisco IOS évalue ces fragments non initiaux contre l'ACL et ignore n'importe quelle information de filtrage de la couche 4. Ceci cause des fragments non initiaux d'être évalués seulement sur la portion couche 3 de tout ACE configuré.

Dans cet exemple de configuration, si un paquet TCP destiné à 192.168.1.1 sur le port 22 est réduit en fragments en transit, le fragment initial est abandonné comme prévu par le second ACE basé sur l'information de la couche 4 dans le paquet. Cependant, tous les fragments restant (non-initiaux) sont autorisés par le premier ACE basé complètement sur l'information de la couche 3 dans le paquet et l´ACE. Ce scénario est montré dans cette configuration :

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

En raison de la nature non intuitive du traitement des fragments, les fragments IP sont souvent autorisés par mégarde par les ACL. La fragmentation est également souvent employée dans les tentatives d'éluder la détection par les systèmes de détection des intrusions. C'est pour ces raisons que les fragments IP sont employés souvent dans les attaques, et pourquoi ils doivent être explicitement filtrés en tête de tous les iACL configurés. Cet exemple d´ACL inclut le filtrage complet des fragments d'IP. La fonctionnalité de cet exemple doit être utilisée en même temps que la fonctionnalité des exemples précédents.

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Référez-vous aux listes de contrôle d'accès et aux fragments IP pour plus d'informations sur la façon dont l'ACL manipule les paquets IP fragmentés.

Support d'ACL pour le filtrage des options IP

Le logiciel Cisco IOS Version 12.3(4)T a ajouté le support pour l'utilisation des ACL pour filtrer les paquets IP basé sur les options d'IP qui sont contenues dans le paquet. Les options IP présentent

un défi de sécurité pour les équipements réseau parce que ces options doivent être traitées comme des paquets d´exception. Ceci exige un niveau d'effort du CPU qui n'est pas requis pour les paquets typiques qui traversent le réseau. La présence des options d'IP dans un paquet peut également indiquer une tentative de corrompre les contrôles de sécurité dans le réseau ou de modifier autrement les caractéristiques de transit d'un paquet. C´est pour ces raisons que les paquets avec des options d'IP doivent être filtrés à la frontière du réseau.

Cet exemple doit être utilisé avec les ACE des exemples précédents afin d'inclure le filtrage complet des paquets IP qui contiennent des options IP :

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Support d'ACL à filtrer sur la valeur de TTL

Le Logiciel Cisco IOS version 12.4(2)T a ajouté le support d'ACL pour filtrer des paquets IP basés sur la valeur du Time to Live (TTL). La valeur de TTL d'un datagramme IP est décrémentée par chaque périphérique réseau lorsqu´un paquet passe de la source à la destination. Bien que les valeurs initiales varient par le système d'exploitation, quand le TTL d'un paquet atteint zéro, le paquet doit être abandonné. Le périphérique qui décrémente le TTL à zéro, et relâche donc le paquet, est exigé afin de générer et envoyer un message de temps expiré de l'ICMP à la source du paquet.

La production et la transmission de ces messages est un processus d'exception. Les Routeurs peuvent remplir cette fonction quand le nombre de paquets IP qui doivent expirer est bas, mais si le nombre de paquets devant expirer est élevé, la production et la transmission de ces messages peuvent consommer toutes les ressources disponibles CPU. Ceci présente un vecteur d'attaque DoS. C'est pour cette raison que des périphériques doivent être durcis contre les attaques DoS qui utilisent un haut débit de paquets IP qui doivent expirer.

Il est recommandé que les organismes filtrent les paquets IP avec des valeurs basses de TTL à la périphérie du réseau. Un filtrage complet des paquets avec des valeurs de TTL insuffisantes pour traverser le réseau atténue la menace des attaques basées sur TTL.

Cet exemple d´ACL filtre les paquets avec des valeurs de TTL inférieures à six. Ceci assure la protection contre les attaques d'échéance de TTL pour des réseaux jusqu'à cinq sauts de largeur.

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

> **Note**: Quelques protocoles font l'utilisation légitime des paquets avec des valeurs de TTL basses. L'eBGP est l´un de tels protocoles. Référez-vous à TTL Expiry Attack Identification and Mitigation pour plus d'informations sur l´atténuation des attaques basées sur l´échéance de TTL.

Référez-vous à Support d´ACL pour le filtrage sur la valeur de TTL pour plus d'informations sur cette fonction.

Sessions interactives sécurisées de Gestion

Les sessions de gestion de périphériques vous permettent d'afficher et collecter des informations au sujet d'un périphérique et de ses opérations. Si ces informations sont révélées à un utilisateur malveillant, le périphérique peut devenir la cible d'une attaque, compromis, et utilisé afin d'exécuter des attaques supplémentaires. N'importe qui avec l'accès privilégié à un périphérique a la capacité de plein contrôle administratif de ce périphérique. Il est impératif de sécuriser des sessions de Gestion afin d'empêcher la divulgation d'informations et l'accès non autorisé.

Protection du plan de gestion

Dans le Logiciel Cisco IOS version 12.4(6)T et plus tard, le Management Plane Protection de caractéristique (MPP) permet à un administrateur pour limiter sur quel trafic d'administration d'interfaces peut être reçu par un périphérique. Ceci permet à l'administrateur le contrôle supplémentaire d'un périphérique et comment le périphérique est accédé.

Cet exemple affiche comment permettre au MPP afin de permettre seulement le SSH et HTTPS sur le GigabitEthernet0/1 relient :

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Référez-vous à Protection du plan de gestion pour plus d'informations sur le MPP.

Protection du plan de contrôle

CPPr (Control Plane Protection) se base sur la fonctionnalité de Surveillance du panneau de contrôle afin de restreindre et de contrôler le trafic du plan de contrôle qui est destiné au processeur de routage du périphérique IOS. CPPr, ajouté dans le Logiciel Cisco IOS Version 12.4(4)T, divise le plan de contrôle en catégories distinctes du plan de contrôle qui sont connues comme sous-interfaces. Trois sous-interfaces de plan de contrôle existent : Hôte, Transit et CEF-Exception. En outre, CPPr inclut ces fonctionnalités de protection supplémentaires du plan de contrôle :

- **Fonctionnalité Port-filtering** - Cette caractéristique prévoit le maintien de l'ordre ou la baisse des paquets qui vont aux ports fermés ou non-écoutants de TCP et UDP.

- **Caractéristique de Queue-threshold policy** - Cette caractéristique limite le nombre de paquets pour un protocole spécifié qui sont permis dans la file d'attente d'entrée IP d'avion de contrôle.

CPPr permet à un administrateur pour classifier, maintenir l'ordre, et limiter le trafic qui est envoyé à un périphérique pour la Gestion avec la sous-interface d'hôte. Des exemples de paquets qui sont classifiés pour la catégorie de sous-interface de l´hôte incluent le trafic de gestion tel que SSH ou Telnet et les protocoles de routage.

> **Note**: CPPr ne prend en charge pas l'IPv6 et est limité au chemin d'entrée d'ipv4.

Référez-vous à Guide de la fonctionnalité Protection du plan de contrôle - 12.4T et Comprendre la Protection du plan de contrôle pour plus d'informations sur la fonctionnalité CPPr de Cisco.

Chiffrez les sessions de Gestion

Puisque les informations peuvent être révélées en session interactive de Gestion, ce trafic doit être chiffré de sorte qu'un utilisateur malveillant ne puisse pas accéder aux données qui sont transmises. Le cryptage du trafic permet une connexion d'accès distant sécurisé au périphérique. Si trafic pour une gestion session est envoyé au-dessus du réseau en libellé, un attaquant peut obtenir des informations confidentielles au sujet du périphérique et du réseau.

Un administrateur peut établir une connexion chiffré et d'accès distant sécurisé de Gestion à un périphérique avec les configurations de SSH ou HTTPS (protocole de transfert hypertexte sécurisé). Version SSH 1.0 (SSHv1) de supports logiciels de Cisco IOS, version SSH 2.0 (SSHv2), et HTTPS qui utilise Secure Sockets Layer (SSL) et le Transport Layer Security (TLS) pour l'authentification et le chiffrement de données. SSHv1 et SSHv2 ne sont pas compatibles. SSHv1 est non sécurisé et non normalisé, ainsi il n'est pas recommandé si SSHv2 est une option.

Le logiciel de Cisco IOS prend en charge également le Secure Copy Protocol (SCP), qui permet chiffré et une connexion sécurisée afin de copier des configurations ou des images logicielles de périphérique. SCP se fonde sur SSH. Cet exemple de configuration active SSH sur un périphérique Cisco IOS :

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Cet exemple de configuration active les services SCP :

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

C'est un exemple de configuration pour les services HTTPS :

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Référez-vous à FAQ sur la configuration de Secure Shell sur routeurs et commutateurs exécutant Cisco IOS et Secure Shell (SSH) pour plus d'informations sur la fonctionnalité SSH du logiciel Cisco IOS.

SSHv2

La fonctionnalité introduite du support SSHv2 dans le Logiciel Cisco IOS version 12.3(4)T permet à un utilisateur pour configurer SSHv2. (Le support SSHv1 a été mis en application dans une version antérieure de logiciel de Cisco IOS.) les passages de SSH sur un transport fiable posent et fournissent des capacités d'authentification poussée et de cryptage. Le seul transport fiable qui est défini pour le SSH est TCP. Le SSH fournit des moyens d'accéder à sécurisé et exécuter sécurisé des commandes sur un ordinateur ou un périphérique différent au-dessus d'un réseau. La caractéristique de Secure Copy Protocol (SCP) qui est percée un tunnel au-dessus du SSH tient compte du transfert sécurisé des fichiers.

Si la commande du **verson 2 d'ip ssh** n'est pas explicitement configurée, alors le Cisco IOS active la version SSH 1.99. La version SSH 1.99 permet les connexions SSHv1 et SSHv2. SSHv1 est considéré non sécurisé et peut exercer des effets inverses sur le système. Si le SSH est activé, il est recommandé de désactiver SSHv1 à l'aide de la commande de l'**ip ssh version 2**.

Cet exemple de configuration active SSHv2 (le SSHv1 étant désactivé) sur un périphérique de Cisco IOS :

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Référez-vous au support sécurisé de version 2 de shell pour plus d'informations sur l'utilisation de SSHv2.

Améliorations SSHv2 pour des clés RSA

Le Cisco IOS SSHv2 prend en charge des méthodes d'authentification clavier-interactives et basées sur mot de passe. Les améliorations SSHv2 pour la caractéristique de clés RSA prend en charge également l'authentification basée sur RSA de clé publique pour le client et serveur.

Pour l'authentification de l'utilisateur, l'authentification de l'utilisateur basée sur RSA utilise paire de clés privée/publique associée avec chaque utilisateur pour l'authentification. L'utilisateur doit générer paire de clés privée/publique sur le client et configurer une clé publique sur le serveur de SSH de Cisco IOS afin de se terminer l'authentification.

Un utilisateur de SSH qui essaye d'établir les qualifications fournit à une signature chiffrée la clé privée. La signature et la clé publique de l'utilisateur sont envoyées au serveur de SSH pour l'authentification. Le serveur de SSH calcule des informations parasites au-dessus de la clé publique fournie par l'utilisateur. Les informations parasites sont utilisées afin de déterminer si le serveur a une entrée qui s'assortit. Si une correspondance est trouvée, la vérification basée sur RSA de message est exécutée avec la clé publique. Par conséquent, l'utilisateur est authentifié ou accès basé sur refusé sur la signature chiffrée.

Pour l'authentification de serveur, le client SSH de Cisco IOS doit assigner une clé de hôte pour chaque serveur. Quand les essais de client pour établir une session de SSH avec un serveur, il reçoit la signature du serveur en tant qu'élément du message d'échange principal. Si la clé de hôte stricte vérifiant l'indicateur est activée sur le client, le client vérifie s'il a l'entrée de clé de hôte qui correspond au serveur préconfiguré. Si une correspondance est trouvée, les essais de client pour valider la signature avec la clé d'hôte de serveur. Si le serveur est avec succès authentifié, l'établissement de session continue ; autrement il est terminé et affiche un message d'**échec de l'authentification de serveur**.

Cet exemple de configuration active l'utilisation des clés RSA avec SSHv2 sur un périphérique de Cisco IOS :

```
switch# show vstack
config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Référez-vous aux améliorations sécurisées de version 2 de shell pour des clés RSA pour plus d'informations sur l'utilisation des clés RSA avec SSHv2.

Cet exemple de configuration permet au serveur de SSH de Cisco IOS d'exécuter l'authentification de l'utilisateur basée sur RSA. L'authentification de l'utilisateur est réussie si la clé publique RSA enregistrée sur le serveur est vérifiée avec le public ou la paire de clés privée enregistrée sur le

client.

```
!
! Configure a hostname for the device
!

hostname router
!
! Configure a domain name
!

ip domain-name cisco.com
!
! Generate RSA key pairs using a modulus of 2048 bits
!

crypto key generate rsa modulus 2048
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Configure the SSH username
!

username ssh-user
!
! Specify the RSA public key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash command (followed by the SSH key type and version.)
!
```

Référez-vous à configurer le serveur de SSH de Cisco IOS pour exécuter l'authentification de l'utilisateur basée sur RSA pour plus d'informations sur l'utilisation des clés RSA avec SSHv2.

Cet exemple de configuration permet au client SSH de Cisco IOS d'exécuter l'authentification de serveur basée sur RSA.

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!
```

```
server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

Référez-vous à configurer le client SSH de Cisco IOS pour exécuter l'authentification de serveur basée sur RSA pour plus d'informations sur l'utilisation des clés RSA avec SSHv2.

Console et ports AUX

Dans les périphériques Cisco IOS, console et ports auxiliaires (AUX) sont des lignes asynchrones qui peuvent être utilisées pour l'accès local et à distance à un périphérique. Vous devez vous rendre compte que les ports de console sur les périphériques Cisco IOS ont des privilèges spéciaux. En particulier, ces privilèges permettent à un administrateur d´exécuter la procédure de récupération de mot de passe. Afin d'exécuter la récupération de mot de passe, un attaquant non authentifié devrait avoir accès au port de console et la capacité d'interrompre l´alimentation du périphérique ou de faire tomber en panne le périphérique.

N'importe quelle méthode utilisée afin d'accéder au port de console d'un périphérique doit être sécurisée d´une manière qui est égale à la sécurité qui est imposée pour l'accès privilégié à un périphérique. Les méthodes utilisées afin de sécuriser l'accès doivent inclure l'utilisation de l'AAA, de l´exec-timeout et des mots de passe du modem si un modem est attaché à la console.

Si la récupération de mot de passe n'est pas requise, alors un administrateur peut retirer la capacité d'exécuter la procédure de récupération de mot de passe en utilisant la commande de configuration globale **no service password-recovery** ; cependant, une fois que la commande **no service password-recovery** a été activée, un administrateur ne peut plus exécuter la récupération de mot de passe sur un périphérique.

Dans la plupart des situations, le port auxiliaire d'un périphérique doit être désactivé afin d'empêcher l'accès non autorisé. Un port auxiliaire peut être désactivé avec ces commandes :

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!
```

```
ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

Contrôle des lignes vty et tty

Les sessions de gestion interactive dans le logiciel Cisco IOS utilisent un téléscripteur ou téléscripteur virtuel (vty). Un téléscripteur est une ligne locale asynchrone à laquelle un terminal peut être attaché pour l'accès local au périphérique ou un modem pour l'accès commuté au périphérique. Notez que des téléscripteurs peuvent être utilisés pour des connexions aux ports de console d'autres périphériques. Cette fonction permet à un périphérique avec des lignes tty d´agir en tant que serveur de console où des connexions peuvent être établies à travers le réseau aux ports de console des périphériques connectés aux lignes tty. Les lignes tty pour ces connexions inversées sur le réseau doivent également être contrôlées.

Une ligne vty est utilisée pour toutes les autres connexions réseau à distance supportées par le périphérique, indépendamment du protocole (SSH, SCP ou Telnet sont des exemples). Afin de s'assurer qu'un périphérique peut être accédé par l'intermédiaire d'une session de gestion locale ou à distance, des contrôles appropriés doivent être imposés sur les lignes vty et tty. Les périphériques Cisco IOS ont un nombre limité de lignes vty ; le nombre de lignes disponibles peut être déterminé avec la commande EXEC de show line. Quand toutes les lignes vty sont en service, de nouvelles sessions de Gestion ne peuvent pas être établies, qui crée une condition DOS pour l'accès au périphérique.

La forme la plus simple du contrôle d'accès à un vty ou un téléscripteur d'un périphérique est par l'utilisation de l'authentification sur toutes les lignes, indépendamment de l´emplacement du périphérique dans le réseau. C'est critique pour les lignes vty parce qu'elles sont accessibles par l'intermédiaire du réseau. Une ligne TTY qui est connectée à un modem qui est utilisé pour l'Accès à distance au périphérique, ou une ligne TTY qui est connectée au port de console d'autres périphériques sont également accessibles par l'intermédiaire du réseau. D'autres formes des contrôles d'accès vty et téléscripteur peuvent être imposées avec les commandes de configuration de **transport input** ou d'**access-class**, avec l'utilisation des caractéristiques de CoPP et de CPPr, ou si vous appliquez des Listes d'accès aux interfaces sur le périphérique.

L'authentification peut être imposée par l'utilisation de l'AAA, qui est la méthode recommandée pour l'accès authentifié à un périphérique, avec l'utilisation de la base de données locale des utilisateurs, ou par l'authentification de mot de passe simple configurée directement sur la ligne vty ou tty.

La commande **exec-timeout** doit être utilisée afin de fermer des sessions sur les lignes vty ou tty qui sont inactives. La commande de **service tcp-keepalives-in** doit également être utilisée afin d'activer le Keepalives de TCP sur les connexions entrantes au périphérique. Ceci assure que le périphérique à l´extrémité distante de la connexion est encore accessible et que les connexions semi-ouvertes ou orphelines sont supprimées du périphérique IOS local.

Contrôle du transport pour les lignes vty et tty

Un vty et un téléscripteur devraient être configurés afin de recevoir des connexions seulement chiffré et d'accès distant sécurisé de Gestion au périphérique ou par le périphérique s'il est utilisé en tant que serveur de console. Ce section a trait aux téléscripteurs parce que de telles lignes peuvent être connectées aux ports de console sur d'autres périphériques, qui permettent au téléscripteur d´être accessible sur le réseau. Dans un effort d'empêcher la révélation d'informations ou l'accès non autorisé aux données qui sont transmises entre l'administrateur et le périphérique, **transport input ssh** devrait être utilisé au lieu des protocoles en libellé, tels que Telnet et rlogin. **Le transport input aucun** configuration peut être activé sur un téléscripteur, qui désactive en effet l'utilisation de la ligne TTY pour des connexions d'inverse-console.

Les lignes vty et tty permettent toutes les deux à un administrateur de se connecter à d'autres périphériques. Afin de limiter le type de transport qu'un administrateur peut utiliser pour les connexions sortantes, utilisez la commande de configuration de ligne **transport output.** Si les connexions sortantes ne sont pas nécessaires, alors **transport output none** devrait être utilisé. Cependant, si les connexions sortantes sont permises, une méthode d'accès à distance chiffrée et sécurisée pour la connexion devrait alors être imposée par l'utilisation de **transport output ssh**.

> **Note**: IPSec peut être utilisé pour les connexions chiffré et d'accès distant sécurisé à un périphérique, si pris en charge. Si vous utilisez IPSec, il provoque une charge supplémentaire du CPU au périphérique. Cependant, SSH doit encore être imposé comme transport même lorsqu'IPSec est utilisé.

Messages d'avertissement

Dans quelques juridictions juridiques, il peut être impossible à poursuivre et illégal pour surveiller les utilisateurs malveillants à moins qu'on les ait annoncé qu'ils ne sont pas permis pour utiliser le système. Une méthode pour donner cette notification est de placer cette information dans un message de bannière qui est configuré avec la commande banner login du logiciel Cisco IOS.

Les exigences de notification légale sont complexes, varient par juridiction et situation, et devraient être discutées avec le conseiller juridique. Même dans des juridictions, les avis juridiques peuvent différer. En coopération avec l'avocat-conseil, une bannière peut fournir certaines ou toutes ces informations :

- Notice qu´il faut se connecter au système ou qu´il soit utilisé seulement par un personnel spécifiquement autorisé et peut-être des informations sur qui peut autoriser l'utilisation.
- Notez que n'importe quelle utilisation non autorisée du système est illégale et peut être sujette à des pénalités civiles et criminelles.
- Notez que n'importe quelle utilisation du système peut être enregistrée ou surveillée sans autre communication préalable et que les journaux en résultant peuvent être utilisés comme

preuves devant le tribunal.

- Avis spécifiques requis par les lois locales.

D'un point de vue de la sécurité, plutôt que juridique, une bannière d'ouverture de connexion ne devrait contenir aucune information spécifique sur le nom du routeur, le modèle, le logiciel ou la propriété. Ces informations peuvent être abusées par des utilisateurs malveillants.

Authentification, autorisation, et comptabilité

Le cadre d'Authentification, autorisation et comptabilité (AAA) est essentiel afin de sécuriser l'accès interactif aux périphériques de réseau. Le cadre d'AAA fournit un environnement fortement configurable qui peut être travaillé a basé sur les besoins du réseau.

Authentification TACACS+

TACACS+ est un protocole d'authentification que les périphériques de Cisco IOS peuvent utiliser pour l'authentification des utilisateurs de Gestion contre un serveur distant d'AAA. Ces utilisateurs de gestion peuvent accéder au périphérique IOS par l'intermédiaire de SSH, HTTPS, Telnet ou HTTP.

L'authentification TACACS+, ou plus généralement l´authentification AAA, fournit la capacité d'utiliser les comptes d'utilisateurs individuels pour chaque administrateur réseau. Quand vous ne dépendez pas d'un mot de passe partagé simple, la Sécurité du réseau est améliorée et votre responsabilité est renforcée.

RADIUS est un protocole semblable dans le but à TACACS+ ; cependant, il chiffre seulement le mot de passe envoyé à travers le réseau. En revanche, TACACS+ chiffre la charge utile entière de TCP, qui inclut chacun des deux le nom d'utilisateur et mot de passe. Pour cette raison, TACACS+ devrait être utilisé de préférence à RADIUS quand TACACS+ est supporté par le serveur AAA. Référez-vous à Comparaison de TACACS+ et RADIUS pour une comparaison plus détaillée de ces deux protocoles.

L'authentification TACACS+ peut être activée sur un périphérique de Cisco IOS avec une configuration semblable à cet exemple :

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!
```

```
server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

La configuration précédente peut être utilisée comme point de départ pour un modèle d´authentification AAA spécifique à une organisation. Référez-vous au protocole Authentication, Authorization, and Accounting pour plus d´informations sur la configuration d'AAA.

Une liste de méthode est une liste séquentielle qui décrit les méthodes d'authentification à questionner afin d'authentifier un utilisateur. Les listes de méthode te permettent d'indiquer un ou plusieurs protocoles de Sécurité à utiliser pour l'authentification, et assurent ainsi un système de sauvegarde pour l'authentification au cas où la méthode initiale échouerait. Le logiciel de Cisco IOS utilise la première méthode répertoriée qui avec succès reçoit ou rejette un utilisateur. Les méthodes subséquentes sont seulement essayées dans les cas où les méthodes précédentes échouent en raison de l'indisponibilité ou de la configuration incorrecte du serveur.

Référez-vous à Listes de méthodes nommées pour authentification pour plus d'informations sur configuration des listes de méthodes nommées.

Authentification de secours

Si tous les serveurs TACACS+ configurés deviennent indisponibles, alors un périphérique Cisco IOS peut se fonder sur des protocoles d'authentification secondaires. Les configurations typiques incluent l'utilisation de l'authentification locale ou activée si tous les serveurs TACACS+ configurés sont indisponibles.

La liste complète d'options pour l'authentification sur périphérique inclut activée, locale et ligne. Chacune de ces options a des avantages. L'utilisation de l'enable secret est préférée parce que le secret est haché avec un algorithme à sens unique qui est en soi plus sécurisés que l'algorithme de chiffrement qui est utilisé avec les mots de passe du type 7 pour la ligne ou l'authentification locale.

Cependant, sur les versions du logiciel Cisco IOS qui supportent l'utilisation de mots de passe secrets pour les utilisateurs localement définis, un recours à l'authentification locale peut être desirable. Ceci permet de créer un utilisateur localement défini pour un ou plusieurs administrateurs réseau. Si TACACS+ devenait complètement indisponible, chaque administrateur peut utiliser son nom d'utilisateur local et son mot de passe. Bien que cette action améliore la responsabilité des administrateurs réseau dans des pannes TACACS+, elle augmente de manière significative la charge administrative parce que des comptes d'utilisateur local sur tous les périphériques de réseau doivent être mis à jour.

Constructions de cet exemple de configuration sur l'exemple précédent d'authentification TACACS+ afin d'inclure l'authentification de retour au mot de passe qui est configuré localement

avec la **commande enable secret** :

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

Référez-vous à Configuration de l´authentification pour plus d'informations sur l'utilisation de l'authentification de secours avec AAA.

Utilisation des mots de passe de type 7

Initialement conçu afin de permettre le déchiffrement rapide des mots de passe enregistrés, les mots de passe du type 7 ne sont pas une forme sécurisée de mémoire de mot de passe. Il y a beaucoup d'outils disponibles qui peuvent facilement déchiffrer ces mots de passe. L'utilisation des mots de passe du type 7 devrait être évitée à moins que requise par une fonctionnalité qui est en service sur un périphérique Cisco IOS.

Le type 9 (scrypt) devrait être utilisé autant que possible :

```
!
!

hostname router
!
ip domain-name cisco.c
!
```

```
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

La suppression des mots de passe de ce type peut être facilitée par l'authentification AAA et l'utilisation de la fonctionnalité Enhanced Password Security, qui permet d´utiliser des mots de passe secrets avec les utilisateurs qui sont localement définis par l'intermédiaire de la commande de configuration globale **username**. Si vous ne pouvez pas entièrement empêcher l'utilisation des mots de passe du type 7, considérez ces mots de passe brouillés mais non chiffrés.

Voyez la section durcissante plate du Général Gestion de ce document pour plus d'informations sur la suppression des mots de passe du type 7.

Autorisation de commande avec TACACS+

L´autorisation de commande avec TACACS+ et AAA fournit un mécanisme qui accepte ou refuse chaque commande qui est entrée par un utilisateur administratif. Quand l'utilisateur entre des commandes EXEC, Cisco IOS envoie chaque commande au serveur AAA configuré. Le serveur AAA utilise alors ses politiques configurées afin d´accepter ou refuser la commande pour cet utilisateur particulier.

Cette configuration peut être ajoutée à l'exemple précédent d´authentification AAA afin de mettre en application l´autorisation de commande :

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!
```

```
crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

Référez-vous à Autorisation de configuration pour plus d'informations sur l´autorisation de commande.

Comptabilité de commandes TACACS+

Une fois configurée, la comptabilité des commandes AAA envoie des informations sur chaque commande EXEC qui est entrée aux serveurs TACACS+ configurés. Les informations envoyées au serveur TACACS+ incluent la commande exécutée, la date où elle a été exécutée, et le nom d'utilisateur de l'utilisateur qui sélectionne la commande. La comptabilité des commandes n'est pas prise en charge avec RADIUS.

Cet exemple de configuration active la comptabilité des commandes AAA pour les commandes EXEC entrées aux niveaux de privilège zéro, un et 15. Cette configuration se base sur les exemples précédents qui incluent la configuration des serveurs TACACS.

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!
```

```
server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

Référez-vous à configurer en expliquant plus d'informations sur la configuration de l'aaa accounting.

Serveurs AAA redondants

Les serveurs AAA qui sont exploités dans un environnement devraient être redondants et déployés d'une façon insensible aux défaillances. Ceci aide à s'assurer que l'accès à la gestion interactive, tel que SSH, est possible si un serveur AAA est indisponible.

Quand vous concevez ou implémentez une solution redondante de serveur d'AAA, souvenez-vous ces considérations :

- Disponibilité des serveurs AAA pendant les pannes de réseau potentielles
- Emplacement géographiquement dispersé des serveurs AAA
- Chargez sur différents serveurs d'AAA dans équilibré et des conditions de panne
- Latence de réseau entre les serveurs d'accès au réseau et les serveurs AAA
- Synchronisation des bases de données de serveur AAA

Référez-vous à Déployer les serveurs de contrôle d'accès pour plus d'informations.

Enrichissez le protocole SNMP

Cette section met en valeur plusieurs méthodes qui peuvent être utilisées afin de sécuriser le déploiement de SNMP dans des périphériques IOS. Il est essentiel que le SNMP soit correctement sécurisé afin de protéger la confidentialité, l'intégrité, et la Disponibilité des données de réseau et des périphériques de réseau par lesquels ces données transitent. SNMP vous fournit une grande quantité d'informations sur la santé des périphériques réseau. Ces informations devraient être protégées contre les utilisateurs malveillants qui veulent accroître ces données afin d'exécuter des attaques contre le réseau.

Chaînes de caractères de la communauté SNMP

Les chaînes de caractères de la communauté sont des mots de passe qui sont appliqués à un périphérique IOS pour limiter l'accès, en lecture seule et en lecture-écriture, aux données SNMP

sur le périphérique. Ces chaînes de caractères de la communauté, comme avec tous les mots de passe, devraient être soigneusement choisies pour assurer qu'elles ne sont pas insignifiantes. Les chaînes de caractères de la communauté devraient être changées à intervalles réguliers et conformément aux stratégies de sécurité du réseau. Par exemple, les chaînes de caractères devraient être changées quand un administrateur réseau change des rôles ou quitte la société.

Ces lignes de configuration configurent une chaîne de caractères de la communauté en lecture seule READONLY, et une chaîne de caractères de la communauté en lecture-écriture *READWRITE* :

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

> **Note**: Les exemples précédents de chaîne de la communauté ont été choisis afin d'expliquer clairement l'utilisation de ces chaînes. Pour des environnements de production, les chaînes de caractères de la communauté devraient être choisies avec prudence et devraient se composer d'une série de symboles alphabétiques, numériques et non-alphanumériques. Référez-vous à Recommandations pour la création de mots de passe forts pour plus d'informations sur la sélection de mots de passe non triviaux.

Référez-vous à Guide de référence des commandes pour IOS SNMP pour plus d'informations sur cette fonctionnalité.

Chaînes de caractères de la communauté SNMP avec ACL

En plus de la chaîne de caractères de la communauté, il faut appliquer une ACL qui limite encore plus l'accès SNMP à un groupe choisi d´adresses IP source. Cette configuration limite l'accès SNMP en lecture seule aux périphériques d'hôte qui résident dans l'espace d'adresses 192.168.100.0/24 et limite l'accès SNMP en lecture-écriture seulement au périphérique d'hôte d'extrémité à 192.168.100.1.

> **Note**: Les périphériques qui sont permis par des ces ACLs exigent de la chaîne appropriée de la communauté afin d'accéder aux informations demandées SNMP.

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

Référez-vous au snmp-server community dans la référence de commande de gestion de réseau Cisco IOS pour plus d'informations sur cette caractéristique.

Les ACL d´infrastructure

L'infrastructure ACLs (iACLs) peut être déployée afin de s'assurer que seulement les hôtes d'extrémité avec les adresses IP de confiance peuvent envoyer le trafic SNMP à un périphérique IOS. Une iACL devrait contenir une politique qui refuse les paquets SNMP non autorisés sur le port UDP 161.

Voir la section Limitation de l'accès au réseau avec ACL d'infrastructure de ce document pour plus d'informations sur l'utilisation des iACL.

SNMP Views

SNMP Views est une fonctionnalité de sécurité qui peut permettre ou refuser l'accès à certains MIB SNMP. Une fois qu´un affichage est créé et appliqué à une chaîne de caractères de la communauté avec les commandes de configuration globale **snmp-server community** *community-string view*, si vous accédez à des données MIB, vous êtes limité aux autorisations qui sont définies par l'affichage. Quand approprié, vous êtes informé d´employer des affichages pour limiter les utilisateurs de SNMP aux données dont ils ont besoin.

Cet exemple de configuration limite l'accès SNMP avec la chaîne de caractères de la communauté *LIMITED* aux données MIB qui sont situées dans le groupe *system* :

```
!
!

hostname router
!
ip domain-name cisco.c
!
! Generate RSA key pairs
!

crypto key generate rsa
!
! Configure SSH-RSA keys for user and server authentication on the SSH server
!

ip ssh pubkey-chain
!
! Enable the SSH server for public-key authentication on the router
!

server SSH-server-name
!
! Specify the RSA public-key of the remote peer
!
! You must then configure either the key-string command
! (followed by the RSA public key of the remote peer) or the
! key-hash <key-type> <key-name> command (followed by the SSH key
! type and version.)
!
! Ensure that server authentication takes place - The connection will be
! terminated on a failure
!

ip ssh stricthostkeycheck
!
```

Référez-vous à Configuration du support SNMP pour plus d'informations.

SNMP Version 3

SNMP version 3 (SNMPv3) est défini par RFC3410 , RFC3411 , RFC3412 , RFC3413 , RFC3414 et RFC3415 et est un protocole basé sur des normes interopérables pour la gestion de réseau. SNMPv3 permet d'accéder l'accès sécurisé aux périphériques parce qu'il authentifie et chiffre sur option des paquets au-dessus du réseau. Là où pris en charge, SNMPv3 peut être utilisé afin d'ajouter une autre couche de Sécurité quand vous déployez le SNMP. SNMPv3 se compose de trois options principales de configuration :

- **no auth** - Ce mode n'exige aucune authentification ni aucun cryptage des paquets SNMP
- **authentique** - Ce mode exige l'authentification du paquet SNMP sans cryptage
- **priv** - Ce mode exige l'authentification et le cryptage (intimité) de chaque paquet SNMP

Un ID de moteur principal doit exister afin d'utiliser les mécanismes de sécurité SNMPv3 - authentification ou authentification et cryptage - pour manipuler des paquets SNMP ; par défaut, l'ID du moteur est produite localement. L'ID du moteur peut être affichée avec la commande **show snmp engineID** comme illustré dans cet exemple :

```
router#show snmp engineID
Local SNMP engineID: 80000009030000152BD35496
Remote Engine ID IP-addr Port
```

Note: Si l'engineID est changé, tous les comptes utilisateurs SNMP doivent être modifiés.

L'étape suivante est de configurer un groupe SNMPv3. Cette commande configure un périphérique de Cisco IOS pour SNMPv3 avec un groupe de serveurs AUTHGROUP SNMP et l'authentification d'enables seulement pour ce groupe avec le mot clé **authentique** :

```
router#show snmp engineID
Local SNMP engineID: 80000009030000152BD35496
Remote Engine ID IP-addr Port
```

Cette commande configure un périphérique de Cisco IOS pour SNMPv3 avec un groupe de serveurs PRIVGROUP SNMP et active l'authentification et le cryptage pour ce groupe avec le mot clé de **priv** :

```
router#show snmp engineID
Local SNMP engineID: 80000009030000152BD35496
Remote Engine ID IP-addr Port
```

Cette commande configure un utilisateur SNMPv3 *snmpv3user* avec un mot de passe d'authentification MD5 de *authpassword* et le chiffrement 3DES du mot de passe de *privpassword* :

```
router#show snmp engineID
Local SNMP engineID: 80000009030000152BD35496
Remote Engine ID IP-addr Port
```

Notez que les commandes de configuration **snmp-server user** ne sont pas affichées dans la sortie de configuration du périphérique selon les exigences de RFC 3414 ; donc, le mot de passe utilisateur n'est pas visualisable dans la configuration. Afin d'afficher les utilisateurs configurés, saisissez la commande **show snmp user** comme illustré dans cet exemple :

```
router#show snmp user
User name: snmpv3user
Engine ID: 80000009030000152BD35496
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: 3DES
Group-name: PRIVGROUP
```

Référez-vous à Configuration du support SNMP pour plus d'informations sur cette fonctionnalité.

Protection du plan de gestion

La caractéristique du Management Plane Protection (MPP) en logiciel de Cisco IOS peut être utilisée afin d'aider le SNMP sécurisé parce qu'elle limite les interfaces par lesquelles le trafic SNMP peut se terminer sur le périphérique. La fonctionnalité MPP permet à un administrateur de désigner une ou plusieurs interfaces comme interfaces de gestion. La gestion du trafic est autorisée à entrer dans un périphérique seulement par ces interfaces de gestion. Après que MPP soit activé, aucune interface, sauf les interfaces de gestion désignées, n'accepte de trafic de gestion du réseau qui est destiné au périphérique.

Notez que le MPP est un sous-ensemble de la caractéristique de CPPr et exige une version de l'IOS qui prend en charge CPPr. Référez-vous à Comprendre la Protection du plan de contrôle pour plus d'informations sur CPPr.

Dans cet exemple, MPP est utilisé afin de limiter l´accès SNMP et SSH à seulement l´interface FastEthernet 0/0 :

```
router#show snmp user
User name: snmpv3user
Engine ID: 80000009030000152BD35496
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: 3DES
Group-name: PRIVGROUP
```

Référez-vous au Guide de la fonctionnalité Gestion du plan de contrôle pour plus d´informations.

Les meilleures pratiques de journalisation

La journalisation des événements vous fournit la visibilité dans le fonctionnement d'un périphérique Cisco IOS et du réseau dans lequel il est déployé. Le logiciel Cisco IOS fournit plusieurs options flexibles de journalisation qui peuvent aider à atteindre les buts de gestion du réseau et de visibilité d'une organisation.

Ces sections fournissent quelques meilleures pratiques de journalisation de base qui peuvent aider un administrateur à exploiter la journalisation avec succès tout en réduisant au minimum son incidence sur un périphérique Cisco IOS.

Envoyer les journaux à un emplacement central

Vous êtes informé d´envoyer les informations de journalisation à un serveur Syslog distant. Ceci permet pour corréler et des événements de réseau et de Sécurité d'audit à travers des périphériques de réseau plus efficacement. Notez que les messages Syslog sont transmis de manière peu fiable par UDP et en libellé. Pour cette raison, toutes les protections qu'un réseau a les moyens au trafic d'administration (par exemple, cryptage ou accès hors bande) devraient être étendues afin d'inclure le trafic de Syslog.

Cet exemple de configuration configure un périphérique de Cisco IOS afin d'envoyer les informations de journalisation à un serveur distant de Syslog :

```
router#show snmp user
User name: snmpv3user
```

```
Engine ID: 80000009030000152BD35496
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: 3DES
Group-name: PRIVGROUP
```

Référez-vous à Identification des incidents à l´aide de pare-feu et des événements Syslog du routeur IOS pour plus d'informations sur la corrélation de journal.

Intégré dans 12.4(15)T et initialement introduit dans 12.0(26)S, se connecter aux messages locaux de journalisation système d'enables de caractéristique de mémoire permanente (disque ATA) à enregistrer sur un disque Flash de la connexion de technologie avancée (ATA). Les messages enregistrés sur un lecteur ATA persistent après qu'un routeur soit redémarré.

Cette configuration raye configurent 134,217,728 octets (128 Mo) de messages de journalisation au répertoire de Syslog de l'éclair ATA (disk0), spécifiant une taille de fichier de 16,384 octets :

```
router#show snmp user
User name: snmpv3user
Engine ID: 80000009030000152BD35496
storage-type: nonvolatile active
Authentication Protocol: MD5
Privacy Protocol: 3DES
Group-name: PRIVGROUP
```

Avant que des messages de journalisation soient écrits à un fichier sur le disque ATA, le logiciel de Cisco IOS vérifie s'il y a suffisamment d'espace disque. Sinon, le fichier le plus ancien des messages de journalisation (par l'horodateur) est supprimé, et le fichier en cours est enregistré. Le format de nom du fichier est **log_month : jour : année : : temps**.

> **Note**: Un lecteur flash ATA a limité l'espace disque et ainsi les besoins d'être mis à jour pour éviter de remplacer des données stockées.

Cet exemple affiche comment copier des messages de journalisation à partir du disque Flash du routeur ATA sur un disque externe sur 192.168.1.129 serveur ftp en tant qu'élément des procédures de maintenance :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Référez-vous à se connecter à la mémoire permanente locale (disque ATA) pour plus d'informations sur cette caractéristique.

Niveau de journalisation

Chaque message du journal qui est produit par un périphérique Cisco IOS est assigné une de huit gravités qui vont du niveau 0, urgences, jusqu´au niveau 7, débogage. À moins que spécifiquement requis, vous êtes informé éviter de se connecter au niveau 7. se connectant au niveau 7 produit un chargement élevé CPU sur le périphérique qui peut mener au périphérique et à l'instabilité de réseau.

Le niveau de **logging trap de** commande de configuration globale est utilisé afin de spécifier quels messages de journalisation sont envoyés aux serveurs distants de Syslog. Le *niveau* spécifié indique le message de plus basse gravité qui est envoyé. Pour une journalisation mise en mémoire tampon, la commande **logging buffered** *level* est utilisée.

Cet exemple de configuration limite les messages du journal qui sont envoyés aux serveurs Syslog distants et à la mémoire tampon locale du journal aux gravités allant de 6 (informationnelles) à 0 (urgences) :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Référez-vous à Dépannage, gestion des pannes et journalisation pour plus d'informations.

N´enregistrez pas à la console ou aux sessions de surveillance

Avec le logiciel de Cisco IOS, il est possible d'envoyer des messages de log aux sessions de surveillance - les sessions de surveillance sont des sessions interactives de Gestion dans lesquelles le **terminal monitor de** commande EXEC a été émis - et à la console. Cependant, ceci peut élever le chargement CPU d'un périphérique IOS et donc n'est pas recommandé. Au lieu de cela, vous êtes informé envoyer les informations de journalisation à la mémoire tampon de log locale, qui peut être visualisée avec la commande de **show logging**.

N'utilisez le **no logging console de** commandes de configuration globale et **aucun moniteur se connectant** afin de désactiver se connecter à la console et aux sessions de surveillance. Cet exemple de configuration montre l'utilisation de ces commandes :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Référez-vous à Référence des commandes de gestion de réseau Cisco IOS pour plus d'informations sur les commandes de configuration globale.

Utiliser la journalisation mise en mémoire

Le logiciel Cisco IOS supporte l'utilisation d'une mémoire tampon locale du journal, de sorte qu'un administrateur puisse afficher les messages du journal localement produits. L'utilisation de mettre en mémoire tampon la journalisation est fortement recommandée contre la journalisation à la console ou aux sessions de surveillance.

Il y a deux configuration options qui sont pertinentes en configurant la journalisation mise en mémoire tampon : la taille de tampon de journalisation et les gravités des messages qui sont stockées dans la mémoire tampon. La taille du **tampon de journalisation** est configurée avec la commande de configuration globale **logging buffered** size. La plus basse sévérité incluse dans la mémoire tampon est configurée avec la commande de sévérité de logging buffered. Un administrateur peut afficher le contenu du tampon de journalisation au moyen de la commande **show logging exec**.

Cet exemple de configuration inclut la configuration d'un tampon de journalisation de 16384 octets, aussi bien qu'une sévérité de 6, informationnelle, qui indique que des messages aux niveaux 0 (urgences) par 6 (informationnel) est enregistrés :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Référez-vous à Référence de commandes de gestion de réseau Cisco IOS pour plus d'informations sur la journalisation mise en mémoire tampon.

Configurer l´interface de la source de journalisation

Afin de fournir un plus grand niveau de la cohérence quand vous collectez et passez en revue des messages de log, vous êtes informé configurer statiquement une interface se connectante de source. Accompli par l'intermédiaire de la commande d´interface **logging source-interface**, configurer statiquement une interface de source de journalisation assure que la même adresse IP apparaît dans tous les messages de journalisation qui sont envoyés d'un périphérique Cisco IOS individuel. Pour plus de stabilité, il est recommandé d´utiliser une interface de bouclage comme source de journalisation.

Cet exemple de configuration montre l'utilisation de la commande de configuration globale d'interface de **logging source-interface** afin de spécifier que l'adresse IP du bouclage 0 interfaces soit utilisée pour tous les messages de log :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Pour plus d'informations, référez-vous à Référence des commandes Cisco IOS.

Configurer les horodatages des journalisations

La configuration des horodatages des journalisations vous aide à corréler des événements à travers les périphériques réseau. Il est important de mettre en application une configuration d´horodatage correct et cohérent des journalisations pour assurer que vous pouvez corréler les données de journalisation. Les horodatages des journalisations devraient être configurés pour inclure la date et l´heure avec une précision de milliseconde et pour inclure le fuseau horaire en service sur le périphérique.

Cet exemple inclut la configuration de l´horodatage des journalisations avec une précision de milliseconde dans la zone UTC (Coordinated Universal Time) :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Si vous préférez ne pas enregistrer les heures relativement à l´UTC, vous pouvez configurer un fuseau horaire local spécifique et configurer cette information pour être présente dans les messages du journal produits. Cet exemple montre une configuration de périphérique pour la zone Heure standard du Pacifique (PST) :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Gestion de la configuration du logiciel Cisco IOS

Le logiciel Cisco IOS inclut plusieurs fonctionnalités qui peuvent activer une forme de gestion de configuration sur un périphérique Cisco IOS. De telles fonctions incluent une fonctionnalité pour archiver des configurations et retourner la configuration à une précédente version ainsi que pour créer un journal détaillé des modifications de configuration.

Configuration Replace et Configuration Rollback

Dans le Logiciel Cisco IOS version 12.3(7)T et plus tard, les caractéristiques de Configuration Replace et de Configuration Rollback te permettent pour archiver la configuration de périphérique de Cisco IOS sur le périphérique. Enregistré manuellement ou automatiquement, les configurations dans ces archives peuvent être utilisées afin de remplacer la configuration en cours d'exécution par la **commande configure replace filename**. Ceci contraste avec la commande **copy** *filename* **running-config**. La commande **configure replace** *filename* remplace la configuration en

cours par opposition à la fusion exécutée par la commande copy.

Il est recommandé d´activer cette fonctionnalité sur tous les périphériques Cisco IOS du réseau. Une fois qu'activé, un administrateur peut causer la configuration en cours d'exécution d'être ajouté aux archives avec la commande de privileged exec d'**archive config**. Les configurations archivées peuvent être visualisées avec la commande EXEC de **show archive**.

Cet exemple illustre la configuration de l'archivage automatique de configuration. Cet exemple instruit le périphérique Cisco IOS de stocker les configurations archivées en tant que fichiers nommés *archived-config-N* sur le disk0 : système de fichier, pour maintenir un maximum de 14 copies de sauvegarde, et pour l'archiver une fois par jour (1440 minutes) et quand un administrateur émet la commande EXEC **write memory**.

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Bien que la fonctionnalité d'archives de configuration puisse enregistrer jusqu'à 14 configurations de sauvegarde, vous êtes informé considérer espace requis avant que vous utilisiez la commande **maximum**.

Exclusive Configuration Change Access

Ajouté au Logiciel Cisco IOS Version 12.3(14)T, la fonctionnalité Exclusive Configuration Change Access assure que seulement un administrateur apporte des modifications de configuration à un périphérique Cisco IOS à un moment donné. Cette fonctionnalité aide à éliminer l'incidence indésirable de modifications simultanées apportées à des composants de configuration apparentés. Cette caractéristique est configurée avec le mode de **configuration mode exclusive de** commande de configuration globale et fonctionne dans un de deux modes : auto et manuel. En mode automatique, la configuration se verrouille automatiquement quand un administrateur émet la commande EXEC **configure terminal**. En mode manuel, l'administrateur emploie la **commande configure terminal lock** afin de verrouiller la configuration quand elle écrit le mode de configuration.

Cet exemple illustre la configuration de cette fonctionnalité pour le verrouillage automatique de la configuration :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Cisco IOS Software Resilient Configuration

Ajouté dans le Logiciel Cisco IOS version 12.3(8)T, la caractéristique de Resilient Configuration permet pour enregistrer sécurisé une copie de l'image de logiciel Cisco IOS et de la configuration de périphérique qui est actuellement utilisée par un périphérique de Cisco IOS. Quand cette fonctionnalité est activée, il n´est pas possible de modifier ou supprimer ces fichiers de sauvegarde. Vous êtes informé permettre à cette caractéristique afin d'empêcher des tentatives négligentes et malveillantes de supprimer ces fichiers.

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Une fois que cette fonctionnalité est activée, il est possible de rétablir une configuration supprimée ou l´image du logiciel Cisco IOS. L'état courant en cours de cette caractéristique peut être affiché avec la commande EXEC **sécurisée de démarrage d'exposition**.

Logiciel de Cisco signé par Digital

Ajouté dans le Logiciel Cisco IOS version 15.0(1)M pour Cisco 1900, 2900, et des Routeurs de gamme 3900, la caractéristique de logiciel signée par Digital de Cisco facilite l'utilisation du logiciel de Cisco IOS qui est digitalement signé et fait confiance ainsi, avec l'utilisation du chiffrement asymétrique sécurisé (de public-clé).

Une image digitalement signée porte (avec une clé privée) des informations parasites chiffrées de elle-même. Sur le contrôle, le périphérique déchiffre les informations parasites avec la clé publique correspondante des clés qu'elle a dans sa mémoire principale et calcule également ses propres informations parasites de l'image. Si les informations parasites déchiffrées apparient les informations parasites calculées d'image, l'image n'a pas été trifouillée et peut sont de confiance.

Des clés de logiciel de Cisco signées par Digital sont identifiées par le type et la version de la clé. Une clé peut être une offre spéciale, une production, ou un type principal inversé. Les types de clé de production et d'offre spéciale ont une version principale associée qui incrémente alphabétiquement toutes les fois que la clé est retirée et remplacée. ROMMON et images régulières de Cisco IOS sont signés avec une clé d'offre spéciale ou de production quand vous utilisez la caractéristique de logiciel signée par Digital de Cisco. L'image ROMmon est évolutive et doit être signée avec la même clé que l'image d'offre spéciale ou de production qui est chargée.

Cette commande vérifie l'intégrité de l'image c3900-universalk9-mz.SSA dans l'éclair avec les clés dans la mémoire de clé de périphérique :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

La caractéristique de logiciel signée par Digital de Cisco a été également intégrée dans la release 3.1.0.SG de Cisco IOS XE pour les Commutateurs de gamme E de Cisco Catalyst 4500.

Référez-vous au logiciel de Cisco signé par Digital pour plus d'informations sur cette caractéristique.

Dans le Logiciel Cisco IOS version 15.1(1)T et plus tard, le remplacement principal pour le logiciel de Cisco signé par Digital a été introduit. Le remplacement et la révocation principaux remplace et retire une clé qui est utilisée pour un chèque signé par Digital de logiciel de Cisco de la mémoire principale d'une plate-forme. Seulement des clés spéciales et de production peuvent être retirées en cas d'une compromission principale.

Une nouvelle (offre spéciale ou production) clé pour l'image a (offre spéciale ou production) est livré dans l'image a (production ou révocation) qui est utilisée afin de retirer la clé précédente d'offre spéciale ou de production. L'intégrité d'image de révocation est vérifiée avec une clé inversée qui est livré préenregistré sur la plate-forme. Une clé inversée ne change pas. Quand vous retirez une clé de production, après que l'image de révocation soit chargée, la nouvelle clé qu'elle porte est ajoutée à la mémoire principale et la vieille clé correspondante peut être retirée tant que l'image ROMmon est mise à jour et la nouvelle image de production est amorcée. Quand vous retirez une clé spéciale, une image de production est chargée. Cette image ajoute la nouvelle clé spéciale et peut retirer la vieille clé spéciale. Après que vous upgrade rommon, la nouvelle image spéciale puissiez être amorcé.

Cet exemple décrit la révocation d'une clé spéciale. Ces commandes ajoutent la nouvelle clé spéciale à la mémoire principale de l'image en cours de production, copient une nouvelle image ROMmon (C3900_rom-monitor.srec.SSB) sur la zone de stockage (usbflash0 :), améliorent le fichier ROMMON, et retirent la vieille clé spéciale :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Une nouvelle image spéciale (c3900-universalk9-mz.SSB) peut alors être copiée sur l'éclair à charger et la signature de l'image est vérifiée avec la clé spéciale nouvellement ajoutée (.SSB) :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

La révocation et le remplacement principaux n'est pas prise en charge sur le Catalyst les Commutateurs de 4500 gamme E qui exécutent le Logiciel Cisco IOS XE version 2, bien que ces Commutateurs prennent en charge la caractéristique de logiciel signée par Digital de Cisco.

Référez-vous à la section de révocation et de rechange de clé de logiciel de Cisco signée par Digital du guide de logiciel de Cisco signé par Digital pour plus d'informations sur cette caractéristique.

Configuration Change Notification and Logging

La fonctionnalité Configuration Change Notification and Logging, ajoutée dans le logiciel Cisco IOS Version 12.3(4)T, permet d´enregistrer les modifications de configuration apportées à un périphérique Cisco IOS. Le journal est mis à jour sur le périphérique Cisco IOS et contient les informations utilisateur de la personne qui a effectué la modification, la commande de configuration entrée et l´heure à laquelle la modification a été apportée. Cette fonctionnalité est activée avec le **commande logging enable change logger configuration mode**. **Les hidekeys** et le **logging size entries** facultatifs de commandes sont utilisés afin d'améliorer la configuration par défaut parce qu'ils empêchent se connecter des données de mot de passe et augmentent la longueur du log de modification.

Il est recommandé d´activer cette fonctionnalité de sorte que l'historique de modification de configuration d'un périphérique Cisco IOS puisse être plus facilement compréhensible. Supplémentaire, vous êtes informé employer la commande de configuration de **notify syslog** afin d'activer la génération des messages de Syslog quand une modification de configuration est apportée.

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Après que la fonctionnalité Configuration Change Notification and Logging ait été activée, la commande EXEC privilégiée **show archive log config all** peut être utilisée afin d'afficher le journal de configuration.

Plan de contrôle

Les fonctions plates de contrôle comprennent les protocoles et les processus qui communiquent entre les périphériques de réseau afin de déplacer des données de la source à la destination. Ceci inclut les protocoles de routage tels que Border Gateway Protocol, ainsi que des protocoles comme ICMP et Resource Reservation Protocol (RSVP).

Il est important que les événements dans les plans de gestion et de données ne compromettent pas le plan de contrôle. Si un événement de plan de données comme une attaque DoS affecte le plan de contrôle, l´ensemble du réseau peut devenir instable. Ces informations sur les fonctionnalités et les configurations du logiciel Cisco IOS peuvent aider à assurer la résilience du plan de contrôle.

Durcissement général du plan de contrôle

La protection du plan de contrôle d'un équipement réseau est critique parce que le plan de contrôle assure que les plans de gestion et de données sont mis à jour et opérationnels. Si le plan de contrôle devenait instable pendant un incident lié à la sécurité, il peut vous être impossible de rétablir la stabilité du réseau.

Dans de nombreux cas, vous pouvez désactiver la réception et la transmission de certains types de messages sur une interface afin de réduire la quantité de chargement CPU qui est exigé pour traiter les paquets inutiles.

Redirections ICMP IP

Un message de redirection ICMP peut être produit par un routeur quand un paquet est reçu et transmis sur la même interface. Dans cette situation, le routeur expédie le paquet et envoie un message de redirection ICMP à l'expéditeur du paquet original. Ce comportement permet à l'expéditeur de contourner le routeur et d´expédier les paquets futurs directement à la destination (ou à un routeur plus près de la destination). Dans un réseau IP fonctionnant correctement, un routeur envoie des redirections seulement aux hôtes sur ses propres sous-réseaux locaux. En d'autres termes, les redirections ICMP ne devraient jamais dépasser une limite de couche 3.

Il y a deux types de messages de redirection ICMP : redirection pour une adresse d´hôte et redirection pour un sous-réseau entier. Un utilisateur malveillant peut exploiter la capacité du routeur d'envoyer l'ICMP réoriente en envoyant continuellement des paquets au routeur, qui force le routeur pour répondre avec l'ICMP réoriente des messages, et des résultats dans une incidence défavorable sur la CPU et la représentation du routeur. Afin d'empêcher le routeur d'envoyer des redirections ICMP, utilisez la commande de configuration d'interface **no ip redirects**.

ICMP inaccessibles

Le filtrage avec une liste d´accès d´interface provoque la retransmission des messages ICMP inaccessibles à la source du trafic filtré. La génération de ces messages peut augmenter l'utilisation du processeur sur le périphérique. Dans le logiciel Cisco IOS, la génération d´ICMP inaccessible est limitée à un paquet toutes les 500 millisecondes par défaut. La génération de message ICMP inaccessible peut être désactivée avec la commande de configuration d'interface **aucun ip unreachables**. La limitation de débit inaccessible d'ICMP peut être changée du par défaut avec l'intervalle-dans-ms d'**ip icmp rate-limit unreachable de** commande de configuration globale.

ARP Proxy

Le proxy ARP est la technique selon laquelle un périphérique, habituellement un routeur, répond aux requêtes ARP qui sont destinées à un autre périphérique. En « truquant » son identité, le routeur accepte la responsabilité du routage de paquets vers la destination « réelle ». Le proxy ARP peut aider des machines sur un sous-réseau d´atteindre des sous-réseaux distants sans configurer le routage ou la passerelle par défaut. Le proxy ARP est défini dans RFC 1027 .

Il y a plusieurs inconvénients à l'utilisation de proxy ARP. Il peut avoir comme conséquence une augmentation de la quantité du trafic ARP sur l'épuisement de segment et de ressource de réseau et des attaques homme-dans-le-moyennes. Le proxy ARP présente un vecteur d'attaque d'épuisement de ressource parce que chaque requête de proxy ARP consomme une petite quantité de mémoire. Un attaquant peut pouvoir épuiser toute la mémoire disponible s'il envoie un

grand nombre de demandes d'ARP.

les attaques Homme-dans-le-moyennes permettent à un hôte sur le réseau de charrier l'adresse MAC du routeur, qui des résultats dans des hôtes confiants envoyant le trafic à l'attaquant. Le proxy ARP peut être désactivé avec la commande de configuration d'interface **aucun ip proxy-arp**.

Référez-vous à Activer le proxy ARP pour plus d'informations sur cette fonctionnalité.

Incidence CPU de limite du trafic d'avion de contrôle

La protection du plan de contrôle est critique. Puisque la performance de l'application et l'expérience de l'utilisateur peuvent souffrir sans la présence de données et du trafic de gestion, l'aptitude à la survie du plan de contrôle assure que les deux autres plans sont mis à jour et opérationnels.

Comprenez le trafic d'avion de contrôle

Afin de protéger correctement le plan de contrôle du périphérique de Cisco IOS, il est essentiel de comprendre les types de trafic qui est commuté par processus par la CPU. Le trafic commuté par processus se compose normalement de deux types différents de trafic. Le premier type de trafic est dirigé vers le périphérique Cisco IOS et doit être traité directement par le CPU du périphérique Cisco IOS. Ce trafic comprend la catégorie du *trafic de contiguïté de réception*. Ce trafic contient une entrée dans la table de Technologie Cisco Express Forwarding (CEF) par lequel le prochain saut de routeur soit le périphérique lui-même, qui est indiqué par le terme reçoit dans la sortie CLI de **show ip cef**. Cette indication est le cas pour toute adresse IP qui exige un traitement direct par le CPU du périphérique Cisco IOS, qui inclut l´interface des adresses IP, l´espace d´adressage de multicast et l´espace d'adressage de diffusion.

Le deuxième type de trafic qui est manipulé par la CPU est le trafic de plan de données - trafiquez avec une destination au delà du périphérique de Cisco IOS elle-même - qui exige l'offre spéciale traitant par la CPU. Bien que n´étant pas une liste exhaustive du CPU ayant un impact sur le trafic du plan de données, ces types de trafic sont commutés par processus et peuvent donc affecter le fonctionnement du plan de contrôle :

- **Se connecter de liste de contrôle d'accès** - L'ACL se connectant le trafic se compose de tous les paquets qui sont dus généré à une correspondance (l'autorisation ou refusent) d'ACE sur lequel le mot clé de journal est utilisé.
- **Unicast Reverse Path Forwarding (Unicast RPF)** - Unicast RPF, utilisé en même temps qu'un ACL, peut avoir comme conséquence la commutation de processus de certains paquets.
- **Options IP** - Tous les paquets IP avec des options incluses doivent être traités par la CPU.
- **Fragmentation** - Tout paquet IP qui exige la fragmentation doit être passé à la CPU pour le traitement.
- **Échéance du Time to Live (TTL)** - Les paquets qui ont une valeur de TTL inférieur ou égal à une avoir besoin de le temps d'Internet Control Message Protocol ont dépassé (type ICMP 11, code 0) des messages à envoyer, qui a comme conséquence le traitement CPU.

- **ICMP Unreachables** - Des paquets qui ont comme conséquence les messages ICMP inaccessibles dus à l'acheminement, le MTU, ou le filtrage est traités par la CPU.

- **Le trafic exigeant une demande d'ARP** - Les destinations pour lesquelles une entrée d'ARP n'existe pas exigent le traitement par la CPU.

- **Le trafic Non-IP** - Tout le trafic non-IP est traité par la CPU.

Cette liste détaille plusieurs méthodes pour déterminer quels types de trafic sont traités par le CPU du périphérique Cisco IOS :

- La commande **show ip cef** fournit les informations de saut suivant pour chaque préfixe IP qui est contenu dans le tableau CEF. Comme indiqué précédemment, les entrées qui contiennent receive comme « Next Hop » sont considérées comme des contiguïtés de receive et indiquent que le trafic doit être envoyé directement au CPU.

- La commande de **commutation d'interface d'exposition** fournit des informations sur le nombre de paquets qui sont commutés par processus par un périphérique.

- La commande **show ip traffic** fournit des informations sur le nombre de paquets IP :

  avec une destination locale (c'est-à-dire, recevoir la juxtaposition trafic)avec des optionsqui exigent la fragmentationqui sont envoyés pour diffuser l'espace d'adressagequi sont envoyés à l'espace d'adressage multicast

- Recevoir la juxtaposition trafic peut être identifié à l´aide de la commande **show ip cache flow** . Tous les flux qui sont destinés au périphérique Cisco IOS ont une interface de destination (DstIf) *locale*.

- **Surveillance du plan de contrôle** peut être utilisé afin d'identifier le type et le débit du trafic qui atteint le plan de contrôle du périphérique Cisco IOS. La Surveillance du plan de contrôle peut être effectuée par l'utilisation des ACL de classification granulaire, de la journalisation et de la commande **show policy-map control-plane** .

Les ACL d´infrastructure

Les ACL d'infrastructure (iACL) limitent la communication externe aux périphériques du réseau. L'infrastructure ACLs sont intensivement couvertes dans la limite Access au réseau de section d'ACLs d'infrastructure de ce document.

Vous êtes informé implémenter des iACLs afin de protéger le plan de contrôle de tous les périphériques de réseau.

Listes de contrôle d'accès de réception

Pour les plates-formes distribuées, les ACL de réception (rACL) peuvent être une option pour le logiciel Cisco IOS Versions 12.0(21)S2 pour le 12000 (GSR), 12.0(24)S pour le 7500 et 12.0(31)S pour le 10720. Le rACL protège le périphérique du trafic néfaste avant que le trafic n´affecte le processeur de routage. Les ACL de réception sont conçus pour protéger seulement les

périphériques sur lesquels ils sont configurés et le trafic de transit n'est pas affecté par un rACL. En conséquence, l´adresse IP de destination qui est utilisée dans l´exemple d´ACL ci-dessous se rapporte seulement aux adresses IP physiques ou virtuelles du routeur. Les ACL de réception sont également considérées comme une meilleure pratique de sécurité du réseau et devraient être considérées comme un ajout à long terme à une bonne sécurité du réseau.

C'est l'ACL du chemin de réception qui est écrit pour autoriser le trafic SSH (port TCP 22) des serveurs de confiance sur le réseau 192.168.100.0/24 :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Reportez-vous à GSR : Listes de contrôle d'accès de réception afin d´aider à identifier et permettre un trafic légitime à un périphérique et refuser tous les paquets non désirés.

CoPP

La caractéristique de CoPP peut également être utilisée afin de limiter les paquets IP qui sont destinés au périphérique d'infrastructure. Dans cet exemple, seul le trafic SSH d´hôtes de confiance est autorisé à atteindre le CPU du périphérique Cisco IOS.

> **Note**: Le trafic chutant des adresses IP inconnues ou non approuvées peut empêcher des hôtes avec les adresses IP dynamique-assignées de connecter au Cisco IOS le périphérique.

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Dans l'exemple précédent de CoPP, les rubriques de liste ACL qui s'assortissent les paquets non autorisés avec l'action d'autorisation ont comme conséquence un écart de ces paquets par la fonction de baisse de policy-map, alors que des paquets qui apparient l'action de refuser ne sont pas affectés par la fonction de baisse de policy-map.

CoPP est disponible dans le logiciel Cisco IOS séries de versions 12.0S, 12.2SX, 12.2S, 12.3T, 12,4 et 12.4T.

Référez-vous à Déploiement de la surveillance du panneau de contrôle pour plus d'informations sur la configuration et l'utilisation de la fonctionnalité CoPP.

Protection du plan de contrôle

Control Plane Protection (CPPr), introduit dans le logiciel Cisco IOS Version 12.4(4)T, peut être utilisé pour limiter ou surveiller le trafic du plan de contrôle qui est destiné au CPU du périphérique Cisco IOS. Bien que semblable à CoPP, CPPr a la capacité de limiter le trafic avec une granularité plus fine. CPPr divise le plan de contrôle global en trois catégories distinctes de plan de contrôle connues sous le nom de sous-interfaces. Les sous-interfaces existent pour les catégories de trafic hôte, transit et CEF-Exception. En outre, CPPr inclut ces fonctionnalités de protection du plan de contrôle :

- **Fonctionnalité Port-filtering** - Cette caractéristique prévoit le maintien de l'ordre et la baisse des paquets qui sont envoyés au TCP ou aux ports UDP fermés ou non-écoutants.

- **Fonctionnalité Queue-thresholding** - Cette caractéristique limite le nombre de paquets pour un protocole spécifié qui sont permis dans la file d'attente d'entrée IP de contrôle-avion.

Référez-vous à Protection du plan de contrôle et à Comprendre la Protection du plan de contrôle (CPPr) pour plus d'informations sur la configuration et l'utilisation de la fonctionnalité CPPr.

Limiteurs matériels de débit

Les Supervisor Engine 32 et 720 de la gamme Cisco Catalyst 6500 assurent l'assistance de limiteurs matériels de débit (HWRL) spécifiques à une plate-forme pour les scénarios particuliers de réseautique. Ces limiteurs matériels de débit sont désignés comme cas spécial de limiteurs de débit parce qu'ils recouvrent un ensemble prédéfini spécifique de scénarios DoS d´ipv4, IPv6, unicast et multicast. Les HWRL peuvent protéger le périphérique Cisco IOS d'un grand choix d'attaques qui exigent que les paquets soient traités par le CPU.

Il y a plusieurs HWRL qui sont activés par défaut. Référez-vous à Configurations par défaut des limiteurs matériels de débit PFC3 pour plus d'informations.

Référez-vous à Limiteurs matériels de débit sur PFC3 pour plus d'informations sur les HWRL.

BGP sécurisé

Le protocole Border Gateway Protocol (BGP) est la base du routage d´Internet. En soi, n'importe quelle organisation avec des exigences de connectivité plus que modestes utilise souvent le BGP. Le BGP est souvent visé par des attaquants en raison de son ubiquité et de la nature de *configurer et oublier des* configurations BGP dans de plus petits organismes. Cependant, il y a beaucoup de fonctions de sécurité spécifiques au BGP qui peuvent être exploitées pour augmenter la sécurité de la configuration d´un BGP.

Ceci fournit un aperçu des fonctions de sécurité du BGP les plus importantes. Le cas échéant, des recommandations de configuration sont faites.

Protections de sécurité basées sur TTL

Chaque paquet IP contient un champ de 1 octet connu sous le nom de Time to Live (TTL). Chaque périphérique qu'un paquet IP traverse décrémente cette valeur de un. La valeur de départ varie par le système d'exploitation et s'étend typiquement de 64 à 255. Un paquet est lâché quand sa valeur de TTL atteint zéro.

Connu comme les deux entaille basée sur TTL généralisée du mécanisme de sécurité (GTSM) et de la Sécurité BGP TTL (BTSH), une protection de Sécurité basée sur TTL accroît la valeur de TTL des paquets IP afin de s'assurer que les paquets BGP qui sont reçus sont d'un pair directement connecté. Cette fonctionnalité exige souvent la coordination des routeurs d´appairage ; cependant, une fois activée, elle peut complètement annihiler beaucoup d'attaques basées sur TCP contre le BGP.

GTSM pour le BGP est activé avec l'option de **ttl-security** pour la commande de configuration **voisine de** routeur BGP. Cet exemple illustre la configuration de cette fonctionnalité :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Àmesure que les paquets BGP sont reçus, la valeur de TTL est vérifiée et doit être supérieure ou

égale à 255, moins le *nombre de sauts* spécifiés.

Authentification d´homologue de BGP avec MD5

L'authentification de pair avec le MD5 crée un condensé de MD5 de chaque paquet envoyé en tant qu'élément d'une session BGP. Spécifiquement, des portions des en-têtes d'IP et de TCP, de la charge utile de TCP, et une clé secrète sont utilisées afin de produire le condensé.

Le condensé créé est alors stocké dans l´option TCP Kind 19, qui a été créée spécifiquement à cet effet par RFC 2385. Le speaker BGP de réception emploie la même clé d'algorithme et de secret afin de régénérer le condensé de message. Si les condensés reçus et calculés ne sont pas identiques, le paquet est rejeté.

L'authentification de pair avec le MD5 est configurée avec l'option de **mot de passe à la** commande de configuration **voisine de** routeur BGP. L'utilisation de cette commande est illustrée comme suit :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Référez-vous à Authentification du routeur voisin pour plus d'informations sur l'authentification d´homologue BGP avec MD5.

Configurez les préfixes maximum

Les préfixes BGP sont stockés en mémoire par a routeur. Plus un routeur doit se tenir préfixes, plus le BGP doit consommer mémoire. Dans quelques configurations, un sous-ensemble de tous les préfixes d'Internet peut être stocké, comme dans les configurations qui exploitent seulement une ou plusieurs routes par défaut pour les réseaux du client d'un fournisseur.

Afin d'empêcher l'épuisement de la mémoire, il est important de configurer le nombre maximal de préfixes qui est accepté par homologue. On lui recommande qu'une limite soit configurée pour chaque homologue BGP.

Quand vous configurez cette caractéristique avec la commande de configuration de routeur BGP de **neighbor maximum-prefix**, un argument est exigé : le nombre maximal de préfixes qui sont acceptés avant qu'un homologue soit arrêté. Sur option, un chiffre de 1 à 100 peut également être saisi. Ce chiffre représente le pourcentage de la valeur maximale de préfixes auquel un message du journal est envoyé.

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Référez-vous à Configurer la fonctionnalité maximum-prefix de BGP pour plus d'informations sur le maximum de préfixes par homologue.

Préfixes BGP de filtre avec des listes de préfixes

Les listes de préfixes permettent à un administrateur réseau d´accepter ou de refuser des préfixes spécifiques qui sont envoyés ou reçus par l'intermédiaire de BGP. Des listes de préfixes devraient être utilisées si possible afin de s'assurer que le trafic réseau est envoyé au-dessus des chemins destinés. Les listes de préfixes devraient être appliquées à chaque eBGP homologue dans les directions entrantes et sortantes.

Les listes de préfixes configurées limitent les préfixes qui sont envoyés ou reçus à ceux spécifiquement permis par la politique de routage d'un réseau. Si ce n'est pas faisable en raison du grand nombre de préfixes reçus, une liste de préfixes devrait être configurée pour bloquer spécifiquement les mauvais préfixes connus. Ces mauvais préfixes connus incluent l'espace d'adressage IP non affecté et les réseaux qui sont réservés à des fins internes ou de tests par RFC 3330. Les listes de préfixes sortants devraient être configurées pour permettre spécifiquement seulement les préfixes qu'une organisation a l´intention d´annoncer.

Cet exemple de configuration emploie des listes de préfixes pour limiter les routes qui sont apprises et annoncées. Spécifiquement, seulement une route par défaut est permise en entrée par la liste de préfixes BGP-PL-INBOUND, et le préfixe 192.168.2.0/24 est la seule route permise d´être annoncée par BGP-PL-OUTBOUND.

copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog

Référez-vous à Connexion à un prestataire de services à l´aide de BGP externe pour la couverture complète du filtrage des préfixes BGP.

Préfixes BGP de filtre avec des Listes d'accès de chemin d'Autonomous System

Les listes d'accès BGP au chemin du système autonome (AS) permettent à l'utilisateur de filtrer les préfixes reçus et annoncés en fonction de l'attribut AS-path d'un préfixe. Ceci peut être utilisé en même temps que des listes de préfixes afin d'établir un ensemble robuste de filtres.

Les utilisations de cet exemple de configuration COMME Listes d'accès de chemin afin de limiter des préfixes d'arrivée à ceux ont commencé par le distant COMME et les préfixes sortants à ceux ont commencé par l'Autonomous System local. Les préfixes qui sont originaires de tout autre système autonome sont filtrés et ne sont pas installés dans le tableau de routage.

copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog

Protocoles sécurisés d'Interior Gateway

La capacité d'un réseau à expédier correctement le trafic et à se rétablir à la suite de modifications ou d´erreurs de topologie dépend d'une vue précise de la topologie. Vous pouvez souvent exécuter un Protocole IGP (Interior Gateway Protocol) dans la commande fournissez cette vue. Par défaut, les IGP sont dynamiques et découvrent des routeurs supplémentaires qui communiquent avec l'IGP en service. Les IGP découvrent également des routes qui peuvent être utilisées pendant une panne de liaison réseau.

Ces sous-sections fournissent un aperçu des fonctions de sécurité les plus importantes de l'IGP. Des recommandations et des exemples qui recouvrent le Routing Information Protocol Version 2 (RIPv2), l'Enhanced Interior Gateway Routing Protocol (EIGRP), et l'Open Shortest Path First (OSPF) sont fournis selon besoins.

Authentification et vérification du protocole de routage avec Message Digest 5

Le manque de sécuriser l'échange des informations de routage permet à un attaquant d´introduire des informations de routage fausses dans le réseau. À l'aide de l´authentification de mot de passe avec des protocoles de routage entre les routeurs, vous pouvez renforcer la sécurité du réseau. Cependant, parce que cette authentification est envoyée en libellé, il peut être simple pour un

attaquant de corrompre ce contrôle de sécurité.

En ajoutant des capacités de hachage MD5 au processus d'authentification, les mises à jour du routage ne contiennent plus de mots de passe en libellé, et le contenu entier de la mise à jour du routage est plus résistant aux falsifications. Cependant, l'authentification MD5 est encore susceptible aux attaques de force brute et par dictionnaire si des mots de passe faibles sont choisis. Il est recommandé d´utiliser des mots de passe avec une randomisation suffisante. Puisque l'authentification MD5 est beaucoup plus sécurisée par comparaison à l´authentification par mot de passe, ces exemples sont spécifiques à l'authentification MD5. IPSec peut également être utilisé afin de valider et sécuriser les protocoles de routage, mais ces exemples ne détaillent pas son utilisation.

EIGRP et RIPv2 utilisent des clés en tant qu'élément de la configuration. Référez-vous à key pour plus d'informations sur la configuration et l'utilisation des clés.

Ceci est un exemple de configuration pour l'authentification de routeur EIGRP utilisant MD5 :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Ceci est un exemple de configuration pour l´authentification de routeur MD5 pour RIPv2. RIPv1 ne prend pas en charge l'authentification.

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Ceci est un exemple de configuration pour l'authentification de routeur OSPF utilisant MD5. OSPF n'utilise pas de clés.

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Référez-vous à Configuration du protocole OSPF pour plus d'informations.

Commandes Passive-Interface

Les fuites d'information, ou l'introduction d'informations fausses dans un IGP, peuvent être atténuées par l'utilisation de la commande **passive-interface** qui aide à contrôler l´annonce des informations de routage. Il est recommandé de ne pas annoncer d´informations aux réseaux qui sont en dehors de votre contrôle administratif.

Cet exemple démontre l'utilisation de cette fonctionnalité :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Filtrage de route

Afin de réduire la possibilité que vous introduisez les informations de routage fausses dans le réseau, vous devez utiliser le filtrage d'artère. À la différence de la commande **passive-interface** de configuration de routeur, le routage se produit sur des interfaces une fois que le filtrage de routeur est activé, mais les informations qui sont annoncées ou traitées sont limitées.

Pour l'EIGRP et le RIP, utilisation de la commande de **distribute-list** avec les limites de mot clé de **sortie** quelles informations sont annoncées, alors que l'utilisation du **dans le** mot clé limite quelles mises à jour sont traitées. La commande **distribute-list** est disponible pour OSPF, mais elle

n'empêche pas un routeur de propager des routes filtrées. Au lieu de cela, la commande **area filter-list** peut être utilisée.

Cet exemple d´EIGRP filtre les annonces sortantes avec la commande **distribute-list** et une liste de préfixes :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Cet exemple d´EIGRP filtre les mises à jour entrantes avec une liste de préfixes :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Référez-vous à configurer des caractéristiques de Protocol-indépendant de Routage IP pour plus d'informations sur la façon contrôler la publicité et au traitement des mises à jour de routage.

Cet exemple OSPF utilise une liste de préfixes avec la commande d'**area filter-list d'OSPF-** particularité :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Consommation des ressources liées au processus de routage

Les préfixes du protocole de routage sont enregistrés en mémoire par un routeur, et la consommation des ressources augmente avec les préfixes supplémentaires que le routeur doit contenir. Afin d'empêcher l'épuisement des ressources, il est important de configurer le protocole de routage pour limiter la consommation des ressources. C'est possible avec l'OSPF si vous utilisez la caractéristique de protection de surcharge de base de données d'État de lien.

Cet exemple démontre la configuration de la fonctionnalité OSPF Protection de surcharge de la base de données d'état de liaison :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Référez-vous à Limitation du nombre de LSA autogénérateurs pour un processus d'OSPF pour plus d'informations sur l´OSPF Protection de surcharge de la base de données d'état de liaison.

Sécurisez les premiers protocoles de Redondance de saut

Les premiers protocoles de Redondance de saut (FHRPs) fournissent la résilience et la Redondance pour les périphériques qui agissent en tant que passerelles par défaut. Cette situation et ces protocoles sont courants dans les environnements où une paire de périphériques de couche 3 fournit la fonctionnalité de passerelle par défaut pour un segment de réseau ou définit des VLAN qui contiennent des serveurs ou des postes de travail.

Le Gateway Load-Balancing Protocol (GLBP), le Hot Standby Router Protocol (HSRP) et le Virtual Router Redundancy Protocol (VRRP) sont tous des FHRP. Par défaut, ces protocoles communiquent avec des transmissions unauthenticated. Ce genre de transmission peut permettre à un attaquant de poser comme périphérique de FHRP-parler pour assumer le rôle de passerelle par défaut sur le réseau. Cette prise de contrôle permettrait à un attaquant d´exécuter une attaque homme du milieu et d´intercepter tout le trafic utilisateur qui quitte le réseau.

Afin d'empêcher ce type d'attaque, tout le FHRPs qui sont pris en charge par le logiciel de Cisco

IOS incluent une capacité d'authentification avec le MD5 ou les chaînes de texte. En raison de la menace constituée par les FHRP non authentifiés, il est recommandé que les instances de ces protocoles utilisent l'authentification MD5. Cet exemple de configuration démontre l'utilisation de l´authentification MD5 GLBP, HSRP et VRRP :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Plan de données

Bien que le plan de données soit responsable du transport des données de source à la destination, dans le contexte de la sécurité, le plan de données est le moins important des trois plans. C'est pour cette raison que il est important de protéger les avions de Gestion et de contrôle dans la préférence au-dessus du plan de données quand vous sécurisez un périphérique de réseau.

Cependant, dans le plan de données lui-même, il y a beaucoup de fonctionnalités et d'options de configuration qui peuvent aider à sécuriser le trafic. Ces sections précisent ces fonctionnalités et options afin que vous puissiez plus facilement sécuriser votre réseau.

Durcissement général du plan de données

La grande majorité du trafic des plans de données passe à travers le réseau tel que déterminé par la configuration de routage du réseau. Cependant, la fonctionnalité du réseau IP existe pour modifier le chemin des paquets à travers le réseau. Les fonctionnalités telles que les options IP, spécifiquement l'option de routage de la source, constituent un défi de sécurité dans les réseaux actuels.

L'utilisation des ACL de transit est également pertinente au durcissement du plan de données.

Voyez le trafic de transit de filtre avec la section d'ACLs de transit de ce pour en savoir plus de document.

Options IP de rejet sélectif

Il y a deux préoccupations en matière de sécurité présentées par les options d'IP. Le trafic qui contient des options IP doit être changé par processus par les périphériques Cisco IOS, ce qui peut mener à une élévation de la charge du CPU. Les options IP incluent également la fonctionnalité pour modifier le chemin qui trafiquent des prises par le réseau, qui lui permet potentiellement pour renverser des contrôles de sécurité.

En raison de ces préoccupations, la commande de configuration globale ip options {drop **| ignore}** a été ajoutée au logiciel Cisco IOS Versions 12.3(4)T, 12.0(22)S et 12.2(25)S. Sous la première forme de cette commande, les **options d'IP chutent**, tous les paquets IP qui contiennent les options IP qui sont reçues par le Cisco IOS que le périphérique sont abandonnés. Ceci empêche d´élever la charge CPU et la subversion possible des contrôles de sécurité que les options IP peuvent activer.

La deuxième forme de cette commande, **ip options ignore**, configure le périphérique Cisco IOS pour ignorer les options IP qui sont contenues dans les paquets reçus. Tandis que ceci atténue les menaces liées aux options IP pour le périphérique local, il est possible que des périphériques en aval puissent être affectés par la présence des options IP. C'est pour cette raison que la forme

drop de cette commande est fortement recommandée. Ceci est démontré dans l'exemple de configuration :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Notez que quelques protocoles, par exemple RSVP, font un usage légitime des options IP. La fonctionnalité de ces protocoles est affectée par cette commande.

Une fois qu´Options IP de rejet sélectif a été activée, la commande EXEC **show ip traffic** peut être utilisé afin de déterminer le nombre de paquets qui sont rejetés en raison de la présence des options IP. Cette information est présente dans le compteur *rejet obligatoire*.

Référez-vous à Rejet sélectif des options IP ACL pour plus d'informations sur cette fonction.

Désactiver le routage de la source IP

Le routage de la source IP exploite les options Loose Source Route et Record Route en tandem ou la Strict Source Route avec l´option Record Route, afin d'activer la source du datagramme IP pour spécifier le chemin de réseau pris par un paquet. Cette fonctionnalité peut être utilisée dans les tentatives de router le trafic autour des contrôles de sécurité dans le réseau.

Si les options IP n'ont pas été complètement F6485désactivées par l'intermédiaire de la fonctionnalité Options IP de rejet sélectif, il est important que le routage de la source IP soit désactivé. Le routage de la source IP, qui est activé par défaut dans toutes les versions du logiciel Cisco IOS, est désactivé par l'intermédiaire de la commande de configuration globale **no ip source-route**. Cet exemple de configuration illustre l'utilisation de cette commande :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Désactiver les redirections ICMP

Les redirections ICMP sont utilisées afin d'informer un périphérique réseau d'un meilleur chemin à une destination IP. Par défaut, le logiciel Cisco IOS envoie une redirection s'il reçoit un paquet qui doit être routé par l´interface selon laquelle il a été reçu.

Dans certaines situations, il pourrait être possible que un attaquant fasse envoyer le périphérique de Cisco IOS à beaucoup l'ICMP réorientent des messages, qui a comme conséquence un chargement élevé CPU. Pour cette raison, il est recommandé que la transmission des redirections d'ICMP soit désactivée. L'ICMP réoriente sont désactivés avec la configuration d'interface **aucune** commande d'**ip redirects**, suivant les indications de l'exemple de configuration :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Désactiver ou limiter les diffusions dirigées par IP

Les diffusions dirigées par IP rendent possible d´envoyer un paquet de diffusion IP à un sous-réseau IP distant. Une fois qu'il atteint le réseau distant, le périphérique IP d'expédition envoie le paquet comme diffusion de couche 2 à toutes les stations sur le sous-réseau. Ceci fonctionnalité de diffusion dirigée a été exploitée comme une aide d'amplification et de réflexion dans plusieurs attaques, y compris l'attaque smurf.

Les versions actuelles du logiciel Cisco IOS ont cette fonctionnalité désactivée par défaut ; cependant, elle peut être activée par l'intermédiaire de la commande de configuration d'interface **ip directed-broadcast**. Les versions du logiciel Cisco IOS antérieures à 12.0 ont cette fonctionnalité activée par défaut.

Si un réseau exige absolument la fonctionnalité de diffusion dirigée, son utilisation devrait être contrôlée. C'est possible avec l'utilisation d'une liste de contrôle d'accès comme option à la commande d'**ip directed-broadcast**. Cet exemple de configuration limite des diffusions dirigées dans ces paquets UDP qui commencent à un réseau de confiance, 192.168.1.0/24 :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Le trafic de transit de filtre avec le transit ACLs

Il est possible de contrôler quel trafic transite le réseau avec l'utilisation du transit ACLs (tACLs). Ceci contraste avec les ACL d'infrastructure qui recherchent à filtrer le trafic qui est destiné au réseau lui-même. Le filtrage fourni par des tACLs est salutaire quand il est desirable de filtrer le trafic à un groupe particulier de périphériques ou de trafiquer que transite le réseau.

Ce type de filtrage est traditionnellement exécuté par les pare-feux. Cependant, il y a des instances où il peut être avantageux d'exécuter ce filtrage sur un périphérique Cisco IOS dans le réseau, par exemple, là où le filtrage doit être exécuté mais aucun pare-feu n'est présent.

Les ACL de transit sont également un endroit approprié dans lequel mettre en application des protections anti-spoofing statiques.

Voyez la section de protections anti-spoofing de ce pour en savoir plus de document.

Reportez-vous à Listes de contrôle d'accès de transit : Filtrage au niveau de votre périphérie pour plus d'informations sur les tACL.

Filtrage des paquets ICMP

L'Internet Control Message Protocol (ICMP) a été conçu comme protocole de contrôle pour IP. En tant que tels, les messages qu´il transporte peuvent avoir des ramifications de grande envergure sur les protocoles TCP et IP en général. L'ICMP est utilisé par les outils de dépannage réseau **ping et traceroute**, ainsi que par la découverte de MTU de la voie d'accès ; cependant, la connectivité externe d'ICMP est nécessaire rarement pour l'opération appropriée d'un réseau.

Le logiciel Cisco IOS fournit la fonctionnalité pour filtrer spécifiquement des messages ICMP par nom ou type et code. Cet ACL d'exemple permet l'ICMP des réseaux de confiance tandis qu'il bloque tous les paquets d'ICMP d'autres sources :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Fragments IP de filtre

Comme détaillé précédemment dans la limite Access au réseau avec la section d'ACLs d'infrastructure de ce document, le filtrage des paquets IP fragmentés peut lancer un défi aux périphériques de sécurité.

En raison de la nature non intuitive du traitement des fragments, les fragments IP sont souvent autorisés par mégarde par les ACL. La fragmentation est également souvent employée dans les tentatives d'éluder la détection par les systèmes de détection des intrusions. C'est pour ces raisons que les fragments IP sont employés souvent dans les attaques, et pourquoi ils doivent être explicitement filtrés en tête de tous les tACL configurés. L'ACL ci-dessous inclut le filtrage complet des fragments d'IP. La fonctionnalité illustrée dans cet exemple doit être utilisée en même temps que la fonctionnalité des exemples précédents :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Référez-vous aux listes de contrôle d'accès et aux fragments IP pour plus d'informations sur la manipulation d'ACL des paquets IP fragmentés.

Support d'ACL pour le filtrage des options IP

Dans le Logiciel Cisco IOS version 12.3(4)T et plus tard, supports logiciels de Cisco IOS l'utilisation d'ACLs de filtrer des paquets IP basés sur les options IP qui sont contenues dans le paquet. La présence des options IP dans un paquet pourrait indiquer une tentative de renverser des contrôles de sécurité dans le réseau ou de modifier autrement les caractéristiques de transit d'un paquet. C´est pour ces raisons que les paquets avec des options d'IP doivent être filtrés au bord du réseau.

Cet exemple doit être utilisé avec le contenu des exemples précédents afin d'inclure le filtrage complet des paquets IP qui contiennent des options IP :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Protections anti-spoofing

Beaucoup d'attaques utilisent l'adresse IP source charriant pour être efficaces ou pour cacher la source vraie d'attaque et pour gêner le retour arrière précis. Le logiciel de Cisco IOS fournit Unicast RPF et protection de source IP (IPSG) afin de décourager les attaques qui se fondent sur charrier d'adresse IP source. En outre, les ACL et le routage null sont souvent déployés en tant que moyens manuels de prévention du spoofing.

La protection de source IP travaille pour réduire la mystification pour les réseaux qui sont sous le contrôle administratif direct en exécutant le port de commutateur, l'adresse MAC, et la vérification d'adresse source. Unicast RPF fournit la vérification du réseau source et peut réduire les attaques de spoofing dans les réseaux qui ne sont pas sous contrôle administratif direct. La Sécurité de port peut être utilisée afin de valider les adresses MAC à la couche d'accès. L'inspection dynamique de Protocole ARP (Address Resolution Protocol) (DAI) atténue les vecteurs d'attaque qui utilisent l'empoisonnement d'ARP sur des segments locaux.

Unicast RPF

Unicast RPF permet à un périphérique de vérifier que l´adresse source d'un paquet expédié peut être atteinte par l´interface qui a reçu le paquet. Vous ne devez pas compter sur Unicast RPF comme seule protection contre la spoofing. Les paquets usurpés pourraient entrer dans le réseau par une interface activée par Unicast RPF si une route de retour appropriée à l'adresse IP de la source existe. Unicast RPF se fonde sur vous pour activer Cisco Express Forwarding sur chaque périphérique et est par interface configuré.

Unicast RPF peut être configuré dans l´un de deux modes : lâche ou strict. Dans les cas de routage asymétrique, le mode lâche est préféré parce que le mode strict est connu pour rejeter des paquets dans ces situations. Pendant la configuration de la commande de configuration d'interface **ip verify**, le mot clé **any** configure le mode lâche tandis que le mot clé **rx** configure le mode strict.

Cet exemple illustre la configuration de cette fonctionnalité :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Référez-vous à Comprendre la retransmission par le chemin inverse d'Unicast pour plus d'informations sur configuration et l'utilisation d'Unicast RPF.

Protection de la source IP

La Protection de la source IP est un moyen efficace de prévention du spoofing qui peut être utilisé si vous avez le contrôle des interfaces de couche 2. La Protection de la source IP utilise des informations d´espionnage DHCP pour configurer dynamiquement une liste de contrôle d'accès de port (PACL) sur l'interface de couche 2, refusant tout trafic des adresses IP qui ne sont pas associées dans la table de liaison de la source ip.

La Protection de la source IP peut être appliqué aux interface de couche 2 appartenant aux VLAN activés par l´espionnage DHCP. Ces commandes activent le snooping DHCP :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Après que le spoofing DHCP soit activé, ces commandes activent IPSG :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

La sécurité de port peut être activée avec la commande de configuration d'interface **ip verify source port security**. Ceci exige la commande de configuration globale **ip dhcp snooping information option** ; en outre, le serveur DHCP doit prendre en charge l'option 82 de DHCP.

Référez-vous à Configuration des fonctionnalités DHCP et protection de la source IP pour plus d'information sur cette fonctionnalité.

Sécurité de port

La Sécurité de port est utilisée afin d'atténuer le spoofing des adresses MAC à l'interface d'accès. La Sécurité de port peut utiliser les adresses MAC apprises dynamiquement (rémanent) pour faciliter la configuration initiale. Une fois que la Sécurité de port a déterminé une violation de MAC, elle peut utiliser un de quatre modes de violation. Ces modes sont protect, restrict, shutdown et shutdown VLAN. Dans les exemples quand un port fournit seulement à l'accès pour un seul poste de travail l'utilisation des protocoles standard, un nombre maximal d'un peut être suffisant. Les protocoles qui exploitent les adresses virtuelles MAC, tel que HSRP, ne fonctionnent pas quand le nombre maximal est égal à un.

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Référez-vous à configurer la Sécurité de port pour plus d'informations sur le confuration de Sécurité de port.

Inspection dynamique d'ARP

L'inspection dynamique d'ARP (DAI) peut être utilisée afin d'atténuer des attaques d'empoisonnement d'ARP sur des segments locaux. Une attaque d'empoisonnement d'ARP est une méthode dans laquelle un attaquant envoie des informations ARP falsifiées à un segment local. Ces informations sont conçues afin de corrompre le cache d'ARP d'autres périphériques. Souvent, un attaquant utilise l'empoisonnement d´ARP afin d'exécuter une attaque de l´homme du milieu.

DAI intercepte et valide le rapport IP à adresse MAC de tous les paquets ARP sur les ports non sécurisés. Dans des environnements DHCP, DAI utilise les données qui sont générées par la caractéristique de surveillance DHCP. Les paquets ARP qui sont reçus sur des interfaces de confiance ne sont pas validés et les paquets non valides sur des interfaces non sécurisées sont rejetés. Dans les environnements non-DHCP, l'utilisation des ACL d'ARP est requis.

Ces commandes activent le snooping DHCP :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Une fois que le spoofing DHCP a été activé, ces commandes activent DAI :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Dans les environnements non DHCP, les ACL ARP sont requis d'activer DAI. Cet exemple démontre la configuration de base de DAI avec les ACL ARP :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Dai peut également être activé en fonction par base d'interface là où prise en charge.

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Référez-vous à Configuration de l'inspection dynamique d'ARP pour plus d'informations sur la façon de configurer DAI.

ACL anti-spoofing

ACLs manuellement configuré peut assurer la protection anti-spoofing statique contre les attaques qui utilisent l'espace d'adressage inutilisé et non approuvé connu. Généralement, ces ACL anti-spoofing sont appliquées au trafic entrant aux frontières du réseau comme composants d'une plus grande ACL. l'Anti-mystification ACLs exigent la surveillance régulière parce qu'ils peuvent fréquemment changer. La mystification peut être réduite dans le trafic qui provient du réseau local si vous appliquez ACLs sortant qui limitent le trafic aux adresses locales valides.

Cet exemple démontre comment les ACL peut être utilisées afin de limiter l'usurpation d'adresse IP. Cette ACL est appliquée dans la direction entrante sur l´interface désirée. Les ACE qui composent cette ACL ne sont pas exhaustives. Si vous configurez ces types d'ACL, recherchez une référence à jour qui est concluante.

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Référez-vous à Configuration des ACL IP fréquemment utilisées pour plus d'informations sur la

façon de configurer les listes de contrôle d'accès.

La liste officielle des adresses Internet non affectées est mise à jour par l'équipe Cymru. Des informations supplémentaires au sujet du filtrage d´adresses inutilisées sont disponibles à la page de référence de Bogon.

Incidence CPU de limite du trafic de plan de données

L'objectif principal des routeurs et des commutateurs est de transférer les paquets et trames par le périphérique vers les destinations finales. Ces paquets, qui transitent les périphériques déployées dans tout le réseau, peuvent affecter le fonctionnement du CPU d'un périphérique. Le plan de données, qui se compose du trafic qui transite le périphérique de réseau, devrait être sécurisé pour assurer le fonctionnement des avions de Gestion et de contrôle. Si le trafic de transit peut faire traiter le trafic de commutateur par un périphérique, le plan de contrôle d'un périphérique peut être affecté, ce qui peut mener à une interruption opérationnelle.

Fonctionnalités et types de trafic qui affectent le CPU

Bien que non exhaustive, cette liste inclut les types de trafic de plans de données qui exigent un traitement CPU spécial et qui sont commutés par processus par le CPU :

- **Se connecter d'ACL** - L'ACL se connectant le trafic se compose de tous les paquets qui sont dus généré à une correspondance (l'autorisation ou refusent) d'ACE sur lequel le **mot clé de journal** est utilisé.
- **Unicast RPF** - Unicast RPF utilisé en même temps qu'un ACL pourrait avoir comme conséquence la commutation de processus de certains paquets.
- **Options IP** - Tous les paquets IP avec des options incluses doivent être traités par la CPU.
- **Fragmentation** - Tout paquet IP qui exige la fragmentation doit être passé à la CPU pour le traitement.
- **Échéance du Time to Live (TTL)** - Les paquets qui ont une valeur de TTL inférieur ou égal à 1 avoir besoin de le temps d'Internet Control Message Protocol ont dépassé (type ICMP 11, code 0) des messages à envoyer, qui a comme conséquence le traitement CPU.
- **ICMP Unreachables** - Des paquets qui ont comme conséquence les messages ICMP inaccessibles dus à l'acheminement, au MTU ou au filtrage sont traités par la CPU.
- **Le trafic exigeant une demande d'ARP** - Les destinations pour lesquelles une entrée d'ARP n'existe pas exigent le traitement par la CPU.
- **Le trafic Non-IP** - Tout le trafic non-IP est traité par la CPU.

Voir la section Durcissement général du plan de données de ce document pour plus d'informations sur le durcissement du plan de données.

Filtre sur la valeur de TTL

Vous pouvez utiliser le soutien ACL pour le filtrage sur la fonctionnalité Valeur de TTL, introduit dans le Logiciel Cisco IOS Version 12.4(2)T, dans une liste d'accès IP étendue pour filtrer les paquets basés sur la valeur de TTL. Cette fonctionnalité peut être utilisée afin de protéger un périphérique recevant le trafic de transit où la valeur de TTL est zéro ou un. Le filtrage de paquets basé sur les valeurs de TTL peut également être utilisé afin d'assurer que la valeur de TTL ne soit pas inférieure au diamètre du réseau, de ce fait protégeant le plan de contrôle des périphériques d'infrastructure en aval contre les attaques d'échéance de TTL.

Notez que certaines applications et outils tels que **traceroute** utilisent l'échéance TTL de paquets dans des buts de tests et de diagnostiques. Quelques protocoles, tels qu'IGMP, utilisent légitimement une valeur de TTL égale à un.

Cet exemple d´ACL crée une politique qui filtre les paquets IP où la valeur de TTL est inférieure à 6.

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Référez-vous à Identification et atténuation d'attaques d'échéance TTL pour plus d'informations sur le filtrage de paquets basé sur la valeur de TTL.

Référez-vous à Support d´ACL pour le filtrage sur la valeur de TTL pour plus d'informations sur cette fonctionnalité.

Dans le Logiciel Cisco IOS version 12.4(4)T et le plus défunt, flexible Packet Matching (FPM) permet à un administrateur pour apparier sur les bits arbitraires d'un paquet. Cette politique de FPM rejette les paquets avec une valeur de TTL inférieure à six.

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Référez-vous à Flexible Packet Matching, situé sur la page d'accueil Cisco IOS Flexible Packet Matching, pour plus d'informations sur la fonctionnalité.

Filtre sur la présence des options IP

Dans le Logiciel Cisco IOS version 12.3(4)T et plus tard, vous pouvez employer le soutien d'ACL de la caractéristique de filtrage d'options IP dans une liste d'accès IP Désignée et étendue afin de filtrer des paquets IP en présence des options IP. Le filtrage de paquets IP qui est basé sur la présence d´options IP peut également être utilisé afin d'empêcher le plan de contrôle des périphériques d'infrastructure de devoir traiter ces paquets au niveau du CPU.

Notez que le soutien ACL pour la fonctionnalité Filtrage des options IP peut seulement être utilisé avec des ACL nommées et étendues. Il devrait également noter que le RSVP, l'Ingénierie de trafic MPLS (commutation multiprotocole par étiquette), les IGMP version 2 et 3, et d'autres protocoles qui utilisent des paquets d'options IP ne pourraient pas pouvoir fonctionner correctement si des paquets pour ces protocoles sont lâchés. Si ces protocoles sont en service dans le réseau, alors le soutien ACL pour le filtrage des options IP peut être utilisé ; cependant, la caractéristique sélective de baisse d'options IP d'ACL pourrait relâcher ce trafic et ces protocoles ne pourraient pas fonctionner correctement. S'il n'y a aucun protocole en service qui exigent des options IP, la baisse sélective d'options IP d'ACL est la méthode préférée pour relâcher ces paquets.

Cet exemple d´ACL crée une politique qui filtre les paquets IP qui contiennent des options IP :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Cet exemple d´ACL démontre une politique qui filtre les paquets IP avec cinq options IP spécifiques. Les paquets qui contiennent ces options sont refusés :

- 0 Fin de la liste d´options (eool)
- 7 Enregistrement de route (record-route)
- 68 Horodatage
- 131 - Route source lâche (lsr)
- 137 - Route source stricte (ssr)

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Voir la section Durcissement général du plan de données de ce document pour plus d'informations sur le Rejet sélectif des options IP ACL.

Reportez-vous à Listes de contrôle d'accès de transit : Filtrage au niveau de votre périphérie pour plus d'informations sur le filtrage du trafic de transit et du trafic périphérique.

Une autre fonctionnalité du logiciel Cisco IOS qui peut être utilisée afin de filtrer les paquets avec options IP est CoPP. Dans le Logiciel Cisco IOS version 12.3(4)T et plus tard, CoPP permet à un administrateur pour filtrer l'ordre d'exécution du trafic des paquets d'avion. Un périphérique qui prend en charge CoPP et le soutien d'ACL pour le filtrage des options IP, introduit dans le Logiciel Cisco IOS Version 12.3(4)T, peut employer une politique de liste d´accès pour filtrer les paquets qui contiennent des options IP.

Cette politique de CoPP rejette les paquets de transit qui sont reçus par un périphérique quand des options IP sont présentes :

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Cette politique de CoPP rejette les paquets de transit qui sont reçus par un périphérique quand ces options IP sont présentes :

- 0 Fin de la liste d´options (eool)
- 7 Enregistrement de route (record-route)
- 68 Horodatage
- 131 - Route source+F7461 lâche (lsr)
- 137 - Route source stricte (ssr)

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Dans les politiques précédentes de CoPP, les entrées de la liste de contrôle d'accès (ACE) qui correspondent aux paquets avec l'action *permettre* ont pour résultat le rejet de ces paquets par la

fonction policy-map *rejeter*, tandis que les paquets qui correspondent à l'action *refuser* (non montrée) ne sont pas affectés par la fonction de policy-map *rejeter*.

Référez-vous à déployer la Réglementation du plan de commande pour plus d'informations sur la caractéristique de CoPP.

Protection du plan de contrôle

Dans le Logiciel Cisco IOS version 12.4(4)T et plus tard, le Control Plane Protection (CPPr) peut être utilisé afin de limiter ou le trafic d'avion de contrôle de police par la CPU d'un périphérique de Cisco IOS. Tandis que semblable à CoPP, CPPr a la capacité de limiter ou contrôler le trafic avec une granularité plus fine que CoPP. CPPr divise le plan de contrôle global en trois catégories distinctes de plan de contrôle connues sous le nom de sous-interfaces : Des sous-interfaces d´hôte, de transit et de CEF-Exception existent.

Cette politique de CPPr rejette les paquets en transit reçus par un périphérique où la valeur de TTL est moins de 6 et les paquets en transit ou non reçus par un périphérique où la valeur de TTL est zéro ou un. La politique de CPPr rejette également les paquets avec options IP sélectionnées reçus par le périphérique.

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Dans la stratégie précédente de CPPr, les entrées de liste de contrôle d'accès qui s'assortissent des paquets avec l'action d'autorisation ont comme conséquence ces paquets jeté par la fonction de baisse de policy-map, alors que des paquets qui apparient l'action de refuser (non affichée) ne sont pas affectés par la fonction de baisse de policy-map.

Référez-vous à Comprendre la Protection du plan de contrôle et Protection du plan de contrôle pour plus d'informations sur la fonctionnalité CPPr.

Identification du trafic et retour arrière

Parfois, vous pouvez devoir identifier rapidement le trafic sur le réseau et revenir en arrière, particulièrement pendant une réponse d'incident ou des mauvaises performances du réseau. Le NetFlow et la classification ACLs sont les deux méthodes primaires pour accomplir ceci avec le logiciel de Cisco IOS. Le Netflow peut fournir la visibilité dans tout le trafic du réseau. En outre, le Netflow peut être mis en application avec des collecteurs qui peuvent fournir les tendances à long terme et une analyse automatisée. Les ACL de classification sont un composant des ACL qui exigent une pré-planification pour identifier un trafic donné et une intervention manuelle pendant l'analyse. Ces sections fournissent une brève présentation générale de chaque fonctionnalité.

Netflow

Netflow identifie l'activité réseau anormale et liée à la sécurité en suivant les débits du réseau. Des données de NetFlow peuvent être visualisées et analysées par l'intermédiaire du CLI, ou les données peuvent être exportées à un collecteur de NetFlow de message publicitaire ou de logiciel gratuit pour l'agrégation et l'analyse. Les collecteurs Netflow, par tendance à long terme, peuvent fournir le comportement du réseau et l'analyse de l'utilisation. Netflow fonctionne en exécutant l'analyse sur des attributs spécifiques dans les paquets IP et en créant des flux. Version 5 est la version la plus utilisée généralement du Netflow ; cependant, le version 9 est plus extensible. Des écoulements de NetFlow peuvent être créés avec des données de trafic échantillonnées dans les

environnements à fort débit.

Le CEF, ou le CEF distribué, est une condition préalable à activer le NetFlow. Netflow peut être configuré sur des routeurs et des commutateurs.

Cet exemple illustre la configuration de base de cette fonctionnalité. Dans les versions précédentes du logiciel Cisco IOS, la commande pour activer Netflow sur une interface est **ip route-cache flow** au lieu de **ip flow {ingress | de sortie}**.

```
copy disk0:/syslog ftp://myuser/mypass@192.168.1.129/syslog
```

Ceci est un exemple de sortie Netflow du CLI. L'attribut SrcIf peut faciliter le retour arrière.

```
router#show ip cache flow
IP packet size distribution (26662860 total packets):
1-32 64 96 128 160 192 224 256 288 320 352 384 416 448 480
.741 .124 .047 .006 .005 .005 .002 .008 .000 .000 .003 .000 .001 .000 .000

512 544 576 1024 1536 2048 2560 3072 3584 4096 4608
.000 .000 .001 .007 .039 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
55 active, 65481 inactive, 1014683 added
41000680 ager polls, 0 flow alloc failures
Active flows timeout in 2 minutes
Inactive flows timeout in 60 seconds
IP Sub Flow Cache, 336520 bytes
110 active, 16274 inactive, 2029366 added, 1014683 added to flow
0 alloc failures, 0 force free
1 chunk, 15 chunks added
last clearing of statistics never
Protocol Total Flows Packets Bytes Packets Active(Sec) Idle(Sec)
-------- Flows /Sec /Flow /Pkt /Sec /Flow /Flow
TCP-Telnet 11512 0.0 15 42 0.2 33.8 44.8
TCP-FTP 5606 0.0 3 45 0.0 59.5 47.1
TCP-FTPD 1075 0.0 13 52 0.0 1.2 61.1
TCP-WWW 77155 0.0 11 530 1.0 13.9 31.5
TCP-SMTP 8913 0.0 2 43 0.0 74.2 44.4
TCP-X 351 0.0 2 40 0.0 0.0 60.8
TCP-BGP 114 0.0 1 40 0.0 0.0 62.4
TCP-NNTP 120 0.0 1 42 0.0 0.7 61.4
TCP-other 556070 0.6 8 318 6.0 8.2 38.3
UDP-DNS 130909 0.1 2 55 0.3 24.0 53.1
UDP-NTP 116213 0.1 1 75 0.1 5.0 58.6
UDP-TFTP 169 0.0 3 51 0.0 15.3 64.2
UDP-Frag 1 0.0 1 1405 0.0 0.0 86.8
UDP-other 86247 0.1 226 29 24.0 31.4 54.3
ICMP 19989 0.0 37 33 0.9 26.0 53.9
IP-other 193 0.0 1 22 0.0 3.0 78.2
Total: 1014637 1.2 26 99 32.8 13.8 43.9

SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts
Gi0/1 192.168.128.21 Local 192.168.128.20 11 CB2B 07AF 3
Gi0/1 192.168.150.60 Gi0/0 10.89.17.146 06 0016 101F 55
Gi0/0 10.89.17.146 Gi0/1 192.168.150.60 06 101F 0016 9
Gi0/1 192.168.150.60 Local 192.168.206.20 01 0000 0303 11
Gi0/0 10.89.17.146 Gi0/1 192.168.150.60 06 07F1 0016 1
```

Référez-vous à Netflow Cisco IOS pour plus d'informations sur les capacités de Netflow.

Référez-vous à Introduction à Netflow Cisco IOS - Un aperçu technique pour un aperçu technique de Netflow.

ACL de classification

Les ACL de classification fournissent la visibilité dans le trafic qui traverse l´interface. Les ACL de classification ne modifient pas la stratégie de sécurité d'un réseau et sont typiquement construites pour classifier des protocoles individuels, des adresses source ou des destinations. Par exemple, un ACE qui permet tous les trafics pourrait être séparé en protocoles ou ports spécifiques. Cette classification plus granulaire du trafic dans des ACE spécifiques peut aider à comprendre le trafic du réseau parce que chaque catégorie de trafic a son propre compteur de coups. Un administrateur pourrait également séparer l'implicite refusent à la fin d'un ACL dans les as granulaires pour aider à identifier les types de trafic refusé.

Un administrateur peut accélérer une résolution d'incidents à l'aide des ACL de classification avec les commandes EXEC **show access-list** et **clear ip access-list counters**.

Cet exemple illustre la configuration d'une ACL de classification pour identifier le trafic SMB avant un refus par défaut :

```
router#show ip cache flow
IP packet size distribution (26662860 total packets):
1-32 64 96 128 160 192 224 256 288 320 352 384 416 448 480
.741 .124 .047 .006 .005 .005 .002 .008 .000 .000 .003 .000 .001 .000 .000

512 544 576 1024 1536 2048 2560 3072 3584 4096 4608
.000 .000 .001 .007 .039 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 4456704 bytes
55 active, 65481 inactive, 1014683 added
41000680 ager polls, 0 flow alloc failures
Active flows timeout in 2 minutes
Inactive flows timeout in 60 seconds
IP Sub Flow Cache, 336520 bytes
110 active, 16274 inactive, 2029366 added, 1014683 added to flow
0 alloc failures, 0 force free
1 chunk, 15 chunks added
last clearing of statistics never
Protocol Total Flows Packets Bytes Packets Active(Sec) Idle(Sec)
-------- Flows /Sec /Flow /Pkt /Sec /Flow /Flow
TCP-Telnet 11512 0.0 15 42 0.2 33.8 44.8
TCP-FTP 5606 0.0 3 45 0.0 59.5 47.1
TCP-FTPD 1075 0.0 13 52 0.0 1.2 61.1
TCP-WWW 77155 0.0 11 530 1.0 13.9 31.5
TCP-SMTP 8913 0.0 2 43 0.0 74.2 44.4
TCP-X 351 0.0 2 40 0.0 0.0 60.8
TCP-BGP 114 0.0 1 40 0.0 0.0 62.4
TCP-NNTP 120 0.0 1 42 0.0 0.7 61.4
TCP-other 556070 0.6 8 318 6.0 8.2 38.3
UDP-DNS 130909 0.1 2 55 0.3 24.0 53.1
UDP-NTP 116213 0.1 1 75 0.1 5.0 58.6
UDP-TFTP 169 0.0 3 51 0.0 15.3 64.2
UDP-Frag 1 0.0 1 1405 0.0 0.0 86.8
UDP-other 86247 0.1 226 29 24.0 31.4 54.3
ICMP 19989 0.0 37 33 0.9 26.0 53.9
IP-other 193 0.0 1 22 0.0 3.0 78.2
Total: 1014637 1.2 26 99 32.8 13.8 43.9
```

```
SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts
Gi0/1 192.168.128.21 Local 192.168.128.20 11 CB2B 07AF 3
Gi0/1 192.168.150.60 Gi0/0 10.89.17.146 06 0016 101F 55
Gi0/0 10.89.17.146 Gi0/1 192.168.150.60 06 101F 0016 9
Gi0/1 192.168.150.60 Local 192.168.206.20 01 0000 0303 11
Gi0/0 10.89.17.146 Gi0/1 192.168.150.60 06 07F1 0016 1
```

Afin d'identifier le trafic qui utilise une ACL de classification, utiliser la commande EXEC **show access-list** *acl-name*. Les compteurs d'ACL peuvent être effacés par avec la commande EXEC d'acl-nom de **clear ip access-list counters**.

```
router#show access-list ACL-SMB-CLASSIFY
Extended IP access list ACL-SMB-CLASSIFY
10 deny tcp any any eq 139 (10 matches)
20 deny tcp any any eq 445 (9 matches)
30 deny ip any any (184 matches)
```

Référez-vous à Comprendre la journalisation de la liste de contrôle d'accès pour plus d'informations sur la façon d'activer les capacités de journalisation dans les ACL.

Contrôle d'accès avec des VLAN Maps et des listes de contrôle d'accès de port

Les listes de contrôle d'accès VLAN (VACL), ou VLAN maps et ACL de port (PACL), fournissent la capacité d´imposer le contrôle d'accès sur le trafic non routé qui est plus près des périphériques d'extrémité que des listes de contrôle d'accès qui sont appliquées aux interfaces routées.

Ces sections fournissent un aperçu des fonctionnalités, des avantages et des scénarios d'utilisation potentiels des VACL et des PACL.

Contrôle d'accès avec VLAN Maps

Les VACL, ou VLAN maps qui s'appliquent à tous les paquets qui entrent dans le VLAN, fournissent la capacité d´imposer le contrôle d'accès sur le trafic intra-VLAN. Ce n'est pas possible avec ACLs sur les interfaces conduites. Par exemple, une carte VLAN pourrait être utilisée afin d'empêcher les hôtes qui sont contenus dans le même VLAN de la transmission les uns avec les autres, qui réduit des occasions pour que les attaquants locaux ou les vers exploitent un hôte sur le même segment de réseau. Afin d´empêcher des paquets d'utiliser un VLAN map, vous pouvez créer une liste de contrôle d'accès (ACL) qui correspond au trafic et, dans le VLAN map, définir l'action pour rejeter. Une fois qu'un VLAN map est configuré, tous les paquets qui entrent dans le LAN sont séquentiellement évalués contre le VLAN map configuré. Les VLAN access maps prennent en charge IPv4 et les listes d'accès MAC ; cependant, ils ne prennent pas en charge la journalisation ou les ACL IPv6.

Cet exemple utilise une liste d'accès Désignée étendue qui montre la configuration de cette caractéristique :

```
router#show access-list ACL-SMB-CLASSIFY
Extended IP access list ACL-SMB-CLASSIFY
10 deny tcp any any eq 139 (10 matches)
20 deny tcp any any eq 445 (9 matches)
30 deny ip any any (184 matches)
```

Cet exemple explique l'utilisation d'une carte VLAN afin de refuser des ports TCP 139 et 445 aussi bien que le protocole vigne-IP :

```
router#show access-list ACL-SMB-CLASSIFY
Extended IP access list ACL-SMB-CLASSIFY
10 deny tcp any any eq 139 (10 matches)
20 deny tcp any any eq 445 (9 matches)
30 deny ip any any (184 matches)
```

Référez-vous à Configuration de la sécurité réseau avec des ACL pour plus d'informations sur la configuration des VLAN maps.

Contrôle d'accès avec des PACL

Les PACL peuvent seulement être appliqués à la direction entrante sur des interfaces physiques de la couche 2 d'un commutateur. Semblable aux VLAN maps, les PACL fournissent le contrôle d'accès sur trafic non-routé ou de couche 2 . La syntaxe pour la création de PACLs, qui a la priorité au-dessus des cartes et du routeur ACLs VLAN, est identique que le routeur ACLs. Si un ACL est appliqué à une interface de couche 2, il est alors désigné sous le nom de PACL. La configuration comporte la création d'un ipv4, IPv6, ou ACL de MAC et application de elle à l'interface de couche 2.

Cet exemple emploie une liste d'accès Désignée étendue afin de montrer la configuration de cette caractéristique :

```
router#show access-list ACL-SMB-CLASSIFY
Extended IP access list ACL-SMB-CLASSIFY
10 deny tcp any any eq 139 (10 matches)
20 deny tcp any any eq 445 (9 matches)
30 deny ip any any (184 matches)
```

Référez-vous à la section ACL de port de Configuration de la sécurité réseau avec des ACL pour plus d'informations sur la configuration des PACL.

Contrôle d'accès avec MAC

Les listes de contrôle d'accès MAC ou les listes étendues peuvent être appliquées sur un réseau IP avec l'utilisation de cette commande en mode de configuration d'interface :

```
Cat6K-IOS(config-if)#mac packet-classify
```

> **Note**: C´est pour classifier les paquets de couche 3 comme paquets de couche 2. La commande est prise en charge dans le Logiciel Cisco IOS Version 12.2(18)SXD (pour Sup 720) et le Logiciel Cisco IOS Versions 12.2(33)SRA ou ultérieures.

Cette commande d´interface doit être appliquée sur l'interface d'entrée et elle demande au moteur de transfert de ne pas inspecter l'en-tête IP. Le résultat est que vous pouvez utiliser une liste d'accès de MAC sur l'environnement IP.

Utilisation de VLAN privé

Les VLAN privés (PVLAN) sont une fonction de sécurité de la couche 2 qui limite la connectivité entre les postes de travail ou les serveurs dans un VLAN. Sans PVLANs, tous les périphériques sur une couche 2 VLAN peuvent communiquer librement. Des situations de réseau existent où la

sécurité peut être facilitée en limitant la communication entre les périphériques sur un seul VLAN. Par exemple, des PVLAN sont employés souvent afin d'interdire la communication entre les serveurs dans un sous-réseau publiquement accessible. Si un serveur unique deviennent compromis, le manque de Connectivité à d'autres serveurs dus à l'application de PVLANs pourrait aider à limiter la compromission à l'un serveur.

Il y a trois types de VLAN privés : VLAN isolés, VLAN de communauté et VLAN principaux. La configuration des PVLAN se sert des VLAN principaux et secondaires. Le VLAN principal contient tous les ports proches, qui sont décrits plus tard, et inclut un ou plusieurs VLAN secondaires, qui peuvent être des VLAN isolés ou de communauté.

VLAN isolés

La configuration d'un VLAN secondaire en tant que VLAN isolé empêche complètement la communication entre les périphériques dans le VLAN secondaire. Il pourrait seulement y avoir un VLAN d'isolement par VLAN primaire, et seulement les ports proches peuvent communiquer avec des ports dans un VLAN d'isolement. Les VLAN isolés devraient être utilisés sur des réseaux non sécurisés comme les réseaux qui prennent en charge des invités.

Cet exemple de configuration configure VLAN 11 en tant que VLAN isolé et l´associe au VLAN principal, VLAN 20. L´exemple ci-dessous configure également l´interface FastEthernet 1/1 en tant que port isolé dans le VLAN 11 :

```
Cat6K-IOS(config-if)#mac packet-classify
```

VLAN de communauté

Un VLAN secondaire qui est configuré en tant que VLAN de communauté permet la communication entre les membres du VLAN aussi bien qu'avec tous les ports proches dans le VLAN principal. Cependant, aucune communication n'est possible entre deux VLAN de communauté quelconques ou entre un VLAN de communauté et un VLAN isolé. Les VLAN de communauté doivent être utilisés afin de grouper des serveurs qui ont besoin de connectivité entre eux, mais où la connectivité à tous les autres périphériques dans le VLAN n'est pas requise. Ce scénario est commun dans un réseau accessible publiquement ou partout où des serveurs fournissent un contenu aux clients non sécurisés.

Cet exemple configure un VLAN de communauté seul et configure le port de commutation FastEthernet 1/2 en tant que membre de ce VLAN. Le VLAN de communauté, VLAN 12, est un VLAN secondaire du VLAN principal 20.

```
Cat6K-IOS(config-if)#mac packet-classify
```

Ports proches

Les ports de commutation qui sont placés dans le VLAN principal sont connus comme ports proches. Les ports proches peuvent communiquer avec tous les autres ports dans les VLAN principaux et secondaires. Les interfaces de routeurs ou de pare-feux sont les périphériques les plus communs de ces VLAN.

Cet exemple de configuration combine les exemples précédents de VLAN isolés et de communauté et ajoute la configuration de l´interface FastEthernet 1/12 comme port proche :

```
Cat6K-IOS(config-if)#mac packet-classify
```

Quand vous implémentez PVLANs, il est important de s'assurer que la configuration de la couche 3 en place prend en charge les restrictions qui sont imposées par PVLANs et ne tient pas compte pour que la configuration PVLAN soit renversée. La couche 3 filtrant avec un ACL de routeur ou Pare-feu peut empêcher la subversion de la configuration PVLAN.

Référez-vous à VLAN privés (PVLAN) - proches, isolés, de communauté, situé sur la page d´accueil de Sécurité LAN, pour plus d'informations sur l´utilisation-et la configuration des VLAN privés.

Conclusion

Ce document vous donne un large aperçu des méthodes qui peuvent être utilisées afin de sécuriser un périphérique du système Cisco IOS. Si vous sécurisez les périphériques, il augmente la sécurité globale des réseaux que vous gérez. Dans cet aperçu, la protection de la gestion, du contrôle et des plans de données est discutée, et des recommandations pour la configuration sont fournies. Dans la mesure du possible, suffisamment de détails sont donnés pour la configuration de chaque fonctionnalité associée. Cependant, dans tous les cas, des références complètes sont fournies pour vous fournir les informations nécessaires à une évaluation complémentaire.

Remerciements

Quelques descriptions de la fonction dans ce document ont été écrites par des équipes de développement de l'information de Cisco.

Annexe : Périphérique de Cisco IOS durcissant la liste de contrôle

Cette liste de contrôle est une collection de toutes les étapes durcissantes qui sont présentées de ce guide. Les administrateurs peuvent l'utiliser pendant qu'un rappel de tout le durcissement comporte utilisé et considéré pour un périphérique de Cisco IOS, même si une caractéristique n'a pas été mise en application parce qu'elle ne s'est pas appliquée. Des administrateurs sont informés évaluer chaque option pour son risque potentiel avant qu'ils implémentent l'option.

Plan de gestion

- Mots de passe

  Activez le MD5 hachant (option secrète) pour des mots de passe d'enable et d'utilisateur localConfigurez le verrouillage de relance de mot de passeReprise de mot de passe de débronchement (considérez le risque)

- Services inutilisés de débronchement

- Configurez le Keepalives de TCP pour des sessions de Gestion
- Placez les notifications de mémoire et de seuil CPU
- Configurer

  Notifications de seuil de mémoire et CPUMémoire de réserve pour l'accès de consoleDétecteur de fuite de mémoireDétection de débordement de tamponCollection améliorée de crashinfo
- IACLs d'utilisation pour limiter l'accès de Gestion
- Filtre (considérez le risque)

  Paquets d'ICMPFragments IPOptions IPValeur de TTL en paquets
- Protection du plan de contrôle

  Configurez le filtrage de portConfigurez les seuils de file d'attente
- Accès de Gestion

  Management Plane Protection d'utilisation pour limiter des interfaces de gestionPlacez le délai d'attente d'exécutifUtilisez un protocole de transport chiffré (tel que le SSH) pour l'accès CLIContrôlez le transport pour des lignes vty et tty (l'option de classe d'accès)Avertissez en utilisant des bannières
- AAA

  AAA d'utilisation pour l'authentification et le retourUtilisez l'AAA (TACACS+) pour l'autorisation de commandeAAA d'utilisation pour la comptabilitéServeurs redondants d'AAA d'utilisation
- SNMP

  Configurez les communautés SNMPv2 et appliquez ACLsConfigurez SNMPv3
- Se connecter

  Configure a centralisé se connecterSets logging level pour tous les composants appropriésPlacez le logging source-interfaceConfigurez la finesse de logging timestamp
- Gestion de la configuration

  Remplacez et repositionnementExclusive Configuration Change AccessConfiguration de résilience de logicielNotifications de modification de configuration

Plan de contrôle

- Débronchement (considérez le risque)

  L'ICMP réorienteUnreachables d'ICMPARP Proxy

- Configurez l'authentification de NTP si le NTP est utilisé
- Configurez la Réglementation du plan de commande/protection (filtrage de port, les seuils de file d'attente)
- Protocoles de routage sécurisés

  BGP (TTL, MD5, préfixes maximum, listes de préfixes, chemin ACLs de système)IGP (MD5, interface passive, filtrage d'artère, consommation de ressource)

- Configurez les bornes de débit de matériel
- Sécurisez les premiers protocoles de Redondance de saut (GLBP, HSRP, le VRRP)

Plan de données

- Configurez la baisse sélective d'options IP
- Débronchement (considérez le risque)

  Acheminement de source IPDiffusions dirigées IPL'ICMP réoriente

- Diffusions dirigées IP de limite
- Configurez les tACLs (considérez le risque)

  ICMP de filtreFragments IP de filtreOptions IP de filtreValeurs de TTL de filtre

- Configure a exigé des protections anti-spoofing

  ACLsProtection de la source IPInspection dynamique d'ARPUnicast RPFSécurité de port

- Control Plane Protection (cef-exception de contrôle-avion)
- Configurez le NetFlow et la classification ACLs pour l'identification du trafic
- Configure a exigé le contrôle d'accès ACLs (cartes VLAN, PACLs, le MAC)
- Configurez les VLAN privés