# Guide Cisco pour renforcer les périphériques Cisco IOS

## Table des matières

# Introduction

Le document fournit de l'information qui vous aidera à sécuriser vos périphériques système Cisco IOS®, rehaussant ainsi 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 exigence spécifique n'est associée à ce document.

## Composants utilisés

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

# 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.

- Plan de gestion : Le plan de gestion gère le trafic qui est envoyé au périphérique Cisco IOS et est constitué d'applications et de protocoles comme le protocole SSH (Secure Shell) et SNMP (Simple Network Management Protocol).

- Plan de contrôle : Le plan de contrôle d'un périphérique réseau traite le trafic qui est primordial pour le maintien de 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 : Le plan de données achemine les données par un périphérique 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 AAA (authentification, autorisation et administration) est essentiel pour sécuriser les périphériques réseau. 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. Consultez la section Authentification, autorisation et administration du présent document pour savoir comment tirer parti du modèle AAA.

## Centraliser la collection et la surveillance du journal

Afin d’acquérir des connaissances sur les événements existants, émergents et historiques liés à des incidents de sécurité, votre entreprise doit disposer d’une stratégie unifiée pour la journalisation et la corrélation des événements. 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.

Consultez la section Sessions de gestion interactive sécurisée du présent document pour en savoir plus sur la gestion sécurisée des périphériques 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 la configuration d’un périphérique Cisco IOS, deux aspects supplémentaires de la gestion de la configuration sont essentiels : l’archivage de la configuration et la sécurité.

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. Il s'agit notamment des sessions de gestion interactives qui utilisent SSH, ainsi que la collecte de statistiques avec SNMP ou 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, car les activités du plan de contrôle affectent directement celles du plan de gestion. Cette liste des protocoles est utilisée par le plan de gestion :

- Protocole SNMP (Simple Network Management Protocol)
- Telnet
- Secure Shell Protocol
- Protocole FTP (File Transfer Protocol)
- Protocole HTTP (HyperText Transfer Protocol) / Protocole S-HTTP (Secure Hypertext Transfer Protocol)
- Protocole TFTP (Trivial File Transfer Protocol)
- Secure Copy Protocol
- TACACS+
- RADIUS
- NetFlow
- Protocole NTP
- 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. Notez toutefois qu'un mot de passe configuré localement pour l'accès privilégié est toujours nécessaire en cas de panne des services TACACS+ ou 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. L'algorithme qu'utilise la commande service password-encryption est simplement le chiffre de Vigenère. 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 : le type 0, qui est un mot de passe en texte clair, et le type 7, qui utilise l'algorithme du chiffrement Vigen re. 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

Ajoutée à la version logicielle 12.3(14)T de Cisco IOS, la fonction de verrouillage des nouvelles tentatives pour la saisie du mot de passe vous permet de verrouiller un compte utilisateur local après un nombre donné de tentatives de connexion infructueuses. 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
!
```

Cisco IOS fournit une procédure de récupération du mot de passe qui repose sur le mode d’accès au moniteur ROM (ROMmon) au moyen de la touche d’arrêt lors du démarrage du système. Dans le ROMmon, le logiciel du périphérique peut être rechargé afin de demander une nouvelle configuration du système, y compris 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 fonction « No Service Password-Recovery » (absence du service-récupération de mot de passe) empêche l’exécution de la séquence de la touche d’arrêt et l’entrée de ROMmon lors du 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.

Examinez l’exemple de configuration sécurisée de ROMmon pour en savoir plus sur cette fonction.

Désactiver les services inutilisés

Comme meilleure pratique de sécurité, n'importe quel service inutile doit être désactivé. Ces services inutiles, en particulier ceux qui utilisent le protocole UDP (User Datagram Protocol), servent rarement à des fins légitimes, mais peuvent servir au lancement d’attaques DoS ou autres, qui seraient autrement bloquées par le filtre 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.
- Il est possible de désactiver le serveur HTTP grâce à la commande no ip http server [serveur HTTP sans IP] en mode de configuration globale, et le serveur HTTPS peut être désactivé au moyen de la commande de configuration globale no ip http secure-server [serveur HTTP sécurisé sans IP].
- À moins que les périphériques Cisco IOS récupèrent des configurations du réseau pendant le démarrage, la commande de configuration globale no service config doit être utilisée.

Ainsi, le périphérique Cisco IOS ne peut tenter de localiser un fichier de configuration sur le réseau avec 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 le démarrage à partir de sdflash, la sécurité peut être renforcée par un démarrage à partir de la mémoire flash et par la désactivation de sdflash grâce à la commande de configuration « no 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, les sessions sont interrompues 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

Les commandes service tcp-keepalives-in et service tcp-keepalives-out permettent à un périphérique d’envoyer des messages keepalive 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 de l’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 fonctionnalité utilise deux méthodes pour accomplir ceci : Notification de seuil de mémoire et Réservation de mémoire.

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. Le logiciel Cisco IOS prend en charge deux méthodes de seuil d'utilisation du CPU : 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 Redzone

Dans le logiciel Cisco IOS Version 12.3(7)T et ultérieure, la fonctionnalité Buffer Overflow : Detection and Correction of Redzone Corruption peut être activée par sur un périphérique afin de détecter et de corriger un débordement de bloc de 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. Ajoutée à la version logicielle 12.3(11)T de Cisco IOS, cette fonction permet à un périphérique de récupérer, en cas de panne, de l’espace pour créer de nouveaux fichiers crashinfo. Cette fonctionnalité autorise également la configuration du nombre de fichiers crashinfo à enregistrer.

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

Protocole NTP

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.

- NTP Time Zone [fuseau horaire NTP] : Lorsque vous configurez le protocole NTP, le fuseau horaire doit être configuré de sorte que les horodatages puissent être corrélés avec précision. En général, deux approches peuvent servir à configurer le fuseau horaire pour les périphériques d’un réseau ayant 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.

- NTP Authentication [authentification NTP] : Si vous configurez l’authentification NTP, celle-ci garantit que les messages NTP seront échangés entre les homologues NTP de confiance.

Exemple de configuration au moyen de l’authentification NTP :

Client :

<#root>

```
(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 :

<#root>

```
(config)#
ntp authenticate

(config)#
ntp authentication-key 5 md5 ciscotime

(config)#
ntp trusted-key 5
```

Désactiver Smart Install

Les pratiques exemplaires en matière de sécurité avec la fonction Cisco Smart Install (SMI) dépendent de la façon dont la fonction est utilisée dans un environnement client en particulier. Cisco fait une distinction pour ces cas d'utilisation :

- Les clients qui n'utilisent pas la fonction Smart Install;
- Les clients qui tirent profit de la fonction Smart Install seulement pour un déploiement à distance;
- Les clients qui tirent profit de la fonction Smart Install pour plus que le déploiement à distance (configuration et gestion d'image).

Ces sections décrivent en détail chaque scénario :

- Les clients qui n'utilisent pas la fonction Smart Install.
- Les clients qui ne se servent pas de la fonction Cisco Smart Install et qui utilisent une version de Cisco IOS et de Cisco IOS XE offrant la commande doivent désactiver la fonction Smart Install au moyen de la commande no vstack.

---

 Remarque : la commande vstack a été introduite dans Cisco IOS version 12.2(55)SE03.

---

Voici un exemple de résultat de la commande show vstack sur un commutateur Cisco Catalyst dont la fonction Smart Install client est désactivée :

<#root>

```
switch#
show vstack


config Role: Client (SmartInstall disabled)
Vstack Director IP address: 0.0.0.0
```

Les clients qui tirent profit de la fonction Smart Install seulement pour un déploiement à distance

Désactivez la fonction Smart Install client après l'installation à distance ou utilisez la commande no vstack.

Pour propager la commande no vstack dans le réseau, utilisez une des méthodes suivantes :

- Saisissez la commande no vstack sur tous les commutateurs clients, manuellement ou au moyen d'un script.
- Ajoutez la commande no vstack dans le cadre de la configuration de Cisco IOS, intégrée à chaque client Smart Install lors d'une installation à distance.
- Dans les versions qui ne prennent pas en charge la commande vstack [Cisco IOS, versions 12.2(55)SE02 et antérieures], appliquez une ACL sur les commutateurs clients afin de bloquer le trafic sur le port TCP 4786.

Afin d'activer ultérieurement la fonction Smart Install client, saisissez la commande vstack sur tous les commutateurs clients, manuellement ou au moyen d'un script.

Les clients qui tirent profit de la fonction Smart Install pour plus que le déploiement à distance

Dans la conception d'une architecture Smart Install, veillez à ce que l'espace destiné à l'adresse IP de l'infrastructure ne soit pas accessible aux parties non fiables. Dans les versions qui ne prennent pas en charge la commande vstack, assurez-vous que seul le directeur Smart Install dispose d'une connectivité TCP aux clients Smart Install sur le port 4786.

Les administrateurs peuvent utiliser ces pratiques exemplaires en matière de sécurité pour les déploiements de Cisco Smart Install sur les périphériques touchés :

- ACL de l'interface
- Régulation de plan de contrôle (CoPP). Cette fonction n'est pas offerte dans toutes les versions logicielles de Cisco IOS.

Cet exemple présente une ACL d'interface dont l'adresse IP du directeur Smart Install est 10.10.10.1 et celle du client de Smart Install est 10.10.10.200 :

```
ip access-list extended SMI_HARDENING_LIST
Permit tcp host 10.10.10.1 host 10.10.10.200 eq 4786
deny tcp any any eq 4786
permit ip any any
```

Cette ACL doit être déployée sur toutes les interfaces IP des clients. Elle peut également être transmise par le directeur lors du déploiement initial des commutateurs.

Afin de limiter l'accès aux clients dans l'infrastructure, les administrateurs peuvent utiliser ces pratiques exemplaires en matière de sécurité sur d'autres périphériques du réseau :

- Listes de contrôle d'accès d'infrastructure (iACL)
- Listes de contrôle d'accès VLAN (VACL)

## Limiter l'accès au réseau assorti de listes de contrôle d'accès (ACL) d'infrastructure

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.

Une iACL est construite, puis appliquée afin de préciser les connexions à partir des hôtes ou des réseaux qui doivent être autorisés à accéder aux périphériques 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 :

```
!

ip access-list extended ACL-INFRASTRUCTURE-IN
!
!--- Permit required connections for routing protocols and
!--- network management
!

 permit tcp host <trusted-ebgp-peer> host <local-ebgp-address> eq 179
 permit tcp host <trusted-ebgp-peer> eq 179 host <local-ebgp-address>
 permit tcp host <trusted-management-stations> any eq 22
 permit udp host <trusted-netmgmt-servers> any eq 161
!
!--- Deny all other IP traffic to any network device
!
```

```
 deny ip any <infrastructure-address-space> <mask>
!
!--- Permit transit traffic
!

 permit ip any any
!
```

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.

Référez-vous à Protection de votre coeur : 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.

Cisco IOS fournit des fonctions qui permettent de filtrer précisément les messages ICMP par noms ou par types et par codes. 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 :

```
!

ip access-list extended ACL-INFRASTRUCTURE-IN
!
!--- Permit ICMP Echo (ping) from trusted management stations and servers
!

 permit icmp host <trusted-management-stations> any echo
 permit icmp host <trusted-netmgmt-servers> any echo
!
!--- Deny all other IP traffic to any network device
!

 deny ip any <infrastructure-address-space> <mask>
!
!--- Permit transit traffic
!

 permit ip any any
!
```

Filtrer les fragments IP

Le processus de filtre des paquets IP fragmentés peut poser problème en ce qui a trait 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. Cisco IOS utilise une méthode particulière afin de comparer les fragments non initiaux aux 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 :

```
!

ip access-list extended ACL-FRAGMENT-EXAMPLE
 permit tcp any host 192.168.1.1 eq 80
 deny tcp any host 192.168.1.1 eq 22
!
```

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.

```
!

ip access-list extended ACL-INFRASTRUCTURE-IN
!
!--- Deny IP fragments using protocol-specific ACEs to aid in
!--- classification of attack traffic
!

 deny tcp any any fragments
 deny udp any any fragments
 deny icmp any any fragments
 deny ip any any fragments
!
!--- Deny all other IP traffic to any network device
!

 deny ip any <infrastructure-address-space> <mask>
```

```
!
!--- Permit transit traffic
!

 permit ip any any
!
```

Consultez les listes de contrôle d’accès et les fragments IP pour en savoir plus sur le traitement par l’ACL des 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 :

```
!

ip access-list extended ACL-INFRASTRUCTURE-IN
!
!--- Deny IP packets containing IP options
!

 deny ip any any option any-options
!
!--- Deny all other IP traffic to any network device
!

 deny ip any <infrastructure-address-space> <mask>
!
!--- Permit transit traffic
!

 permit ip any any
!
```

Soutien ACL pour filtrer la valeur TTL

Cisco IOS de version 12.4(2)T prend désormais en charge l’ACL pour filtrer les paquets IP selon la valeur TTL (Time to Live). 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. L'appareil qui réduit la valeur TTL à zéro et abandonne ainsi le paquet est nécessaire pour générer et envoyer un message de dépassement de délai ICMP à la source du paquet.

La production et la transmission de ces messages est un processus d'exception. Les routeurs peuvent exécuter cette fonction lorsque peu de paquets IP sont sur le point d'expirer, mais s'ils sont nombreux, la génération et la transmission de ces messages peuvent consommer toutes les ressources utilisables du CPU. Ceci présente un vecteur d'attaque DoS. C'est pourquoi la protection de ces périphériques doit être renforcée contre les attaques DoS qui utilisent un taux élevé de paquets IP arrivant à expiration.

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.

```
!

ip access-list extended ACL-INFRASTRUCTURE-IN
!
!--- Deny IP packets with TTL values insufficient to traverse the network
!

 deny ip any any ttl lt 6
!
!--- Deny all other IP traffic to any network device
!

 deny ip any <infrastructure-address-space> <mask>
!
!--- Permit transit traffic
!

 permit ip any any
!
```

Remarque : certains protocoles font un usage légitime des paquets avec des valeurs TTL faibles. eBGP est un de ces 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 de gestion interactive sécurisée

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 les sessions de gestion pour éviter la divulgation d'informations et l'accès non autorisé.

Protection du plan de gestion

Dans les versions 12.4(6)T et ultérieures de Cisco IOS, le protocole MPP (Management Plane Protection) permet à un administrateur de limiter les interfaces pouvant recevoir le trafic de gestion par un périphérique. Ceci permet à l'administrateur le contrôle supplémentaire d'un périphérique et comment le périphérique est accédé.

Cet exemple montre comment activer le protocole MPP afin d'autoriser uniquement les protocoles SSH et HTTPS sur l'interface GigabitEthernet0/1 :

```
!

control-plane host
  management-interface GigabitEthernet 0/1 allow ssh https
!
```

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. Il existe trois sous-interfaces de plan de contrôle : Host, Transit et CEF-Exception. En outre, CPPr inclut ces fonctionnalités de protection supplémentaires du plan de contrôle :

- Filtrer les ports : Cette fonction permet de rejeter les paquets connectés aux ports TCP et UDP qui sont fermés ou qui ne sont pas à l'écoute ou d'appliquer une politique les concernant.

- Politique du seuil de la file d'attente : Cette fonction limite le nombre de paquets, pour un protocole précis, qui sont autorisés dans la file d'attente d'entrées IP du plan de contrôle.

CPPr autorise un administrateur à classer, à surveiller et à limiter le trafic qui est envoyé vers un périphérique aux fins de gestion grâce à la sous-interface 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.

---

Remarque : CPPr ne prend pas en charge IPv6 et est limité au chemin d'entrée 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.

Chiffrer les sessions de gestion

Étant donné que les informations peuvent être divulguées dans une session de gestion interactive, le trafic doit être chiffré de sorte qu'un utilisateur malveillant ne puisse pas accéder aux données transmises. Le chiffrement du trafic permet une connexion sécurisée pour accéder à distance 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 de gestion sécurisée et chiffrée pour accéder à distance à un périphérique grâce aux fonctions SSH ou HTTPS. Cisco IOS prend en charge les versions 1.0 (SSHv1) et 2.0 (SSHv2) de SSH ainsi que le protocole HTTPS, qui utilisent SSL (Secure Sockets Layer) et TLS (Transport Layer Security) pour l'authentification et le chiffrement des données. SSHv1 et SSHv2 ne sont pas compatibles. SSHv1 n'est ni sécurisé ni normalisé. Il n'est donc pas recommandé de l'utiliser si la version SSHv2 est offerte en option.

Cisco IOS prend également en charge le protocole SCP (Secure Copy Protocol), qui permet une connexion chiffrée et sécurisée pour copier les configurations du périphérique ou les images logicielles. SCP se fonde sur SSH. Cet exemple de configuration active SSH sur un périphérique Cisco IOS :

```
!

ip domain-name example.com
!

crypto key generate rsa modulus 2048
!

ip ssh time-out 60
ip ssh authentication-retries 3
ip ssh source-interface GigabitEthernet 0/1
!

line vty 0 4
 transport input ssh
!
```

Cet exemple de configuration active les services SCP :

```
!
```

```
ip scp server enable
!
```

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

```
!

crypto key generate rsa modulus 2048
!

ip http secure-server
!
```

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

Grâce à la fonction de prise en charge correspondante introduite dans la version 12.3(4)T de Cisco IOS, l'utilisateur peut configurer la version SSHv2 du logiciel. (La prise en charge SSHv1 a été implémentée dans une version antérieure du logiciel Cisco IOS.) SSH s'exécute au-dessus d'une couche transport fiable et fournit des fonctionnalités d'authentification et de cryptage puissantes. TCP est le seul transport fiable défini pour SSH. SSH permet un accès sûr à un autre ordinateur ou périphérique du réseau, en plus de l'exécution sécurisée des commandes sur l'ordinateur ou le périphérique. La fonction SCP (Secure Copy Protocol), pour la tunnellisation vers SSH, contribue au transfert sécurisé des fichiers.

Si la commande ip ssh version 2 n'est pas configurée explicitement, Cisco IOS active alors le protocole SSH 1.99. La version 1.99 de SSH autorise les connexions SSHv1 et SSHv2. La version SSHv1 est considérée comme non sécurisée et peut avoir des effets négatifs sur le système. Si SSH est activé, il est plutôt recommandé de désactiver SSHv1 à l'aide de la commande ip ssh version 2.

Cet exemple de configuration vient activer SSHv2 (tandis que le logiciel SSHv1 est désactivé) sur un périphérique Cisco IOS :

```
!

hostname router

!

ip domain-name example.com

!
```

```
crypto key generate rsa modulus 2048

!

ip ssh time-out 60
ip ssh authentication-retries 3
ip ssh source-interface GigabitEthernet 0/1

!

ip ssh version 2

!

line vty 0 4
transport input ssh

!
```

Pour plus d'informations sur l'utilisation de SSHv2, consultez la section sur la prise en charge de SSHv2 [Secure Shell version 2].

Amélioration de SSHv2 pour les clés RSA

Cisco IOS SSHv2 prend en charge les méthodes d'authentification par clavier interactif et par mot de passe. La fonction d'améliorations de SSHv2 pour clés RSA (SSHv2 Enhancements for RSA Keys) prend également en charge l'authentification par clé publique RSA pour le client et le serveur.

L'authentification des utilisateurs qui repose sur RSA utilise quant à elle une paire de clés privées ou publiques associées à chaque utilisateur. L'utilisateur doit générer une paire de clés privées et publiques sur le client et configurer une clé publique sur le serveur SSH de Cisco IOS pour procéder à l'authentification.

Un utilisateur SSH qui tente d'établir les informations d'authentification fournit une signature chiffrée avec la clé privée. La signature et la clé publique de l'utilisateur sont envoyées au serveur SSH aux fins d'authentification. Le serveur SSH calcule un hachage à l'aide de la clé publique fournie par l'utilisateur. Ce hachage est utilisé pour déterminer si une entrée du serveur correspond. Le cas échéant, la vérification des messages reposant sur RSA est réalisée avec la clé publique. L'utilisateur est donc authentifié ou refusé selon la signature chiffrée.

Pour l'authentification du serveur, le client SSH de Cisco IOS doit octroyer une clé d'hôte à chaque serveur. Lorsque le client tente d'établir une session SSH avec un serveur, il reçoit la signature du serveur dans le message d'échange de clés. Si l'option de vérification stricte des clés de l'hôte est activée sur le client, ce dernier vérifie alors si l'entrée de la clé d'hôte qui correspond au serveur est préconfigurée. Si une correspondance est établie, le client tente de valider la signature à l'aide de la clé d'hôte du serveur. Si le serveur est authentifié avec succès, l'établissement de session continue ; sinon, il est interrompu et affiche un message Server Authentication Failed.

La configuration donnée en exemple permet l'utilisation de clés RSA avec SSHv2 sur un périphérique Cisco IOS :

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

hostname router
!
! Configure a domain name
!

ip domain-name cisco.com
!
! Specify the name of the RSA key pair (in this case, "sshkeys") to use for SSH
!

 ip ssh rsa keypair-name sshkeys
!
! Enable the SSH server for local and remote authentication on the router using
! the "crypto key generate" command
! For SSH version 2, the modulus size must be at least 768 bits
!

 crypto key generate rsa usage-keys label sshkeys modulus 2048
!
! Configure an ssh timeout (in seconds)
!
! The following enables a timeout of 120 seconds for SSH connections
!

ip ssh time-out 120
!
! Configure a limit of five (5) authentication retries
!

ip ssh authentication-retries 5
!
! Configure SSH version 2
!

ip ssh version 2
!
```

Consultez la section sur les améliorations de SSHv2 pour les clés RSA si vous voulez en savoir plus sur l'utilisation des clés RSA avec SSHv2.

La configuration illustrée dans cet exemple permet au serveur SSH de Cisco IOS d'authentifier un utilisateur au moyen de la clé RSA. L'utilisateur est authentifié avec succès si la clé publique RSA enregistrée sur le serveur est vérifiée grâce à la paire de clés publiques ou privées enregistrées 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.)
!
```

Pour en savoir plus sur l'utilisation des clés RSA avec SSHv2, consultez la section sur la [configuration du serveur SSH de Cisco IOS pour authentifier un utilisateur au moyen des clés RSA.]

La configuration illustrée dans cet exemple permet au client SSH de Cisco IOS d'authentifier un serveur au moyen des clés 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
!
```

Pour en savoir plus sur l'utilisation des clés RSA avec SSHv2, consultez la section sur la configuration du client SSH de Cisco IOS pour authentifier un serveur au moyen des clés RSA.

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, un administrateur peut supprimer la possibilité d'effectuer la procédure de récupération de mot de passe à l'aide de 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 effectuer de récupération de mot de passe sur un périphérique.

Très souvent, le port auxiliaire (AUX) d'un périphérique doit être désactivé afin d'empêcher tout accès non autorisé. Un port AUX peut être désactivé à l'aide des commandes suivantes :

```
!

line aux 0
```

```
 transport input none
 transport output none
 no exec
 exec-timeout 0 1
 no password
!
```

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 à l’aide de la commande EXEC show line. Lorsque toutes les lignes VTY sont utilisées, l’établissement de nouvelles sessions de gestion est impossible, ce 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 utilisé pour l’accès à distance au périphérique ou qui est connectée au port de console d’un autre périphérique est également accessible par le réseau. D’autres formes de contrôles d’accès VTY et TTY sont possibles grâce aux commandes de configuration transport input [entrée de transport] ou access-class [classe d’accès], et à l’aide des fonctions CoPP et CPPr, ou si vous appliquez des listes d’accès aux interfaces sur le périphérique.

L’authentification peut se faire à l’aide du protocole AAA – soit la méthode recommandée pour l’accès authentifié à un périphérique –, au moyen de la base de données des utilisateurs locaux, ou par une simple authentification par mot de passe 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. Il faut aussi utiliser la commande service tcp-keepalives-in pour activer les messages keepalive TCP sur les connexions entrantes vers le 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

Les lignes VTY et TTY sont configurées pour accepter seulement les connexions de gestion d’accès à distance chiffrées et sécurisées vers le périphérique ou par celui-ci 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. La configuration transport input none peut être activée sur un TTY, ce qui désactive l’utilisation de la ligne TTY pour les connexions de console inverse.

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.

---

Remarque : IPSec peut être utilisé pour des connexions d'accès à distance chiffrées et sécurisées à un périphérique, s'il est 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 certaines régions, il peut être impossible de poursuivre en justice les utilisateurs malveillants, ou illégal de les surveiller, sauf s’ils ont été informés qu’ils n’étaient pas autorisés à 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 administration (AAA)

Le cadre AAA est essentiel pour sécuriser l'accès interactif aux périphériques réseau. Ce cadre offre un environnement grandement configurable qui peut être adapté en fonction des besoins du réseau.

### Authentification TACACS+

TACACS+ est un protocole d'authentification que les périphériques Cisco IOS peuvent utiliser pour authentifier les utilisateurs de gestion par rapport à un serveur AAA distant. 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. Si vous n'êtes pas dépendant d'un mot de passe unique partagé, la sécurité du réseau est alors améliorée, et votre responsabilité est renforcée.

RADIUS est un protocole dont l'objectif est similaire à TACACS+ ; toutefois, il ne chiffre que le mot de passe envoyé sur le réseau. En revanche, TACACS+ chiffre l'intégralité de la charge utile TCP, y compris le nom d'utilisateur et le 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 Cisco IOS avec une configuration comparable à celle illustrée ici :

```
!

aaa new-model
aaa authentication login default group tacacs+
!

tacacs-server host <ip-address-of-tacacs-server>
tacacs-server key <key>
!
```

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 méthodes consiste en une liste séquentielle expliquant les méthodes à utiliser pour l'authentification d'un utilisateur. Ces listes vous permettent de déterminer un ou plusieurs protocoles de sécurité qui serviront pour l'authentification, et de garantir ainsi un système d'authentification de rechange en cas d'échec de la méthode initiale. Cisco IOS utilise la première méthode répertoriée, qui permet d'accepter ou de refuser 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. Il est préférable d'utiliser la fonction « enable secret » [activer le secret], car le secret est haché au moyen d'un algorithme à sens unique qui est fondamentalement plus sûr que l'algorithme de chiffrement employé avec les mots de passe de type 7 pour l'authentification locale ou en ligne.

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 accroisse la responsabilité des administrateurs réseau quant aux pannes TACACS+, elle augmente considérablement la charge administrative, étant donné que les comptes utilisateurs locaux des périphériques réseau doivent être conservés.

La configuration illustrée repose sur l'exemple d'authentification TACACS+ précédent afin d'intégrer une solution de rechange à l'authentification par mot de passe qui est configuré localement avec la commande enable secret :

```
!

enable secret <password>
!

aaa new-model
aaa authentication login default group tacacs+ enable
!

tacacs-server host <ip-address-of-tacacs-server>
```

```
tacacs-server key <key>
!
```

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

Conçus au départ pour favoriser le décodage rapide des mots de passe enregistrés, les mots de passe de type 7 ne sont toutefois pas sûrs. 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) doit être utilisé dans la mesure du possible :

```
username <username> privilege 15 algorithm-type scrypt secret <secret>
```

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.

Consultez la section sur le renforcement du plan de gestion général du présent document pour en savoir plus sur la suppression des mots de passe de 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 :

```
!

aaa authorization exec default group tacacs none
aaa authorization commands 0 default group tacacs none
aaa authorization commands 1 default group tacacs none
aaa authorization commands 15 default group tacacs none
!
```

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 de l'exécution et le nom d'utilisateur de celui qui saisit la commande. L'administration des commandes n'est pas prise en charge par 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.

```
!

aaa accounting exec default start-stop group tacacs
aaa accounting commands 0 default start-stop group tacacs
aaa accounting commands 1 default start-stop group tacacs
aaa accounting commands 15 default start-stop group tacacs
!
```

Consultez la section sur la configuration de l'administration pour en savoir plus sur la configuration du protocole AAA.

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.

Lorsque vous élaborez ou mettez en œuvre une solution pour le serveur AAA redondant, tenez compte de ce qui suit :

- Disponibilité des serveurs AAA pendant les pannes de réseau potentielles
- Emplacement géographiquement dispersé des serveurs AAA
- Charger chaque serveur AAA qui se trouve dans un état stable et en situation 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.

## Renforcer le protocole SNMP (Simple Network Management Protocol)

Cette section met en valeur plusieurs méthodes qui peuvent être utilisées afin de sécuriser le déploiement de SNMP dans des périphériques IOS. Il faut absolument que le protocole SNMP soit correctement sécurisé pour protéger la confidentialité, l'intégrité et la disponibilité des données du réseau et des périphériques réseau par où transitent ces données. SNMP vous fournit une grande quantité d'informations sur la santé des périphériques réseau. Ces informations doivent être protégées des utilisateurs malveillants qui souhaitent se servir de ces données pour lancer 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 :

```
!

snmp-server community READONLY RO
snmp-server community READWRITE RW
!
```

---

Remarque : les exemples de chaînes de communauté précédents 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.

---

Remarque : les périphériques autorisés par ces listes de contrôle d'accès nécessitent la chaîne de communauté appropriée pour accéder aux informations SNMP demandées.

---

```
!

access-list 98 permit 192.168.100.0 0.0.0.255
access-list 99 permit 192.168.100.1
!

snmp-server community READONLY RO 98
snmp-server community READWRITE RW 99
!
```

Consultez la section sur la communauté du serveur SNMP figurant dans la référence de la commande Cisco IOS Network Management pour en savoir plus.

Les ACL d´infrastructure

Les iACL peuvent être déployées pour que seuls les hôtes finaux ayant une adresse IP fiable puissent acheminer du 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 :

```
!
```

```
snmp-server view VIEW-SYSTEM-ONLY system include
!

snmp-server community LIMITED view VIEW-SYSTEM-ONLY RO
!
```

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. Le protocole SNMPv3 fournit un accès sécurisé aux périphériques, car il authentifie et peut chiffrer les paquets sur le réseau. Lorsqu'il est pris en charge, le protocole SNMPv3 peut être utilisé pour ajouter une couche de sécurité lors du déploiement du protocole SNMP. SNMPv3 se compose de trois options principales de configuration :

- no auth : Ce mode ne requiert aucune authentification et aucun chiffrement des paquets SNMP.
- auth : Ce mode requiert l'authentification du paquet SNMP sans chiffrement.
- priv : Ce mode requiert l'authentification et le chiffrement (confidentialité) de chaque paquet SNMP.

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

<#root>

```
router#
show snmp engineID


   Local SNMP engineID: 800000090300000152BD35496
   Remote Engine ID          IP-addr    Port
```

Remarque : si l'ID de moteur est modifié, tous les comptes utilisateur SNMP doivent être reconfigurés.

L'étape suivante est de configurer un groupe SNMPv3. Cette commande configure un périphérique Cisco IOS pour le protocole SNMPv3 avec un groupe de serveurs SNMP AUTHGROUP et active seulement l'authentification pour ce groupe au moyen du mot clé auth :

```
!
snmp-server group AUTHGROUP v3 auth
!
```

Cette commande configure un périphérique Cisco IOS pour le protocole SNMPv3 avec un groupe de serveurs SNMP PRIVGROUP et active l'authentification et le chiffrement pour ce groupe au moyen du mot clé priv :

```
!
snmp-server group PRIVGROUP v3 priv
!
```

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 :

```
!

snmp-server user snmpv3user PRIVGROUP v3 auth md5 authpassword priv 3des
     privpassword
!
```

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

<#root>

```
router#

show snmp user


User name: snmpv3user
Engine ID: 800000090300000152BD35496
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 fonction de protection du plan de gestion (MPP) du logiciel Cisco IOS peut servir à sécuriser le protocole SNMP, car il limite les interfaces où prend fin le trafic SNMP 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.

Soulignons que le fichier MPP est un sous-ensemble de la fonction CPPr et qu'il nécessite une version d'IOS qui prend en charge cette fonction. 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 :

```
!
control-plane host
 management-interface FastEthernet0/0 allow ssh snmp
!
```

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. Ainsi, la corrélation et la vérification des événements du réseau et de sécurité peuvent être réalisées plus efficacement sur les périphériques réseau. Notez que les messages Syslog sont transmis de manière peu fiable par UDP et en libellé. C'est pourquoi les protections qu'offre un réseau pour le trafic de gestion (p. ex., le chiffrement ou l'accès hors bande) doivent être élargies afin d'intégrer le trafic syslog.

La configuration donnée en exemple illustre comment configurer un périphérique Cisco IOS pour l'envoi d'informations de journalisation à un serveur syslog distant :

```
!
```

```
logging host <ip-address>
!
```

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.

Intégrée dans la version 12.4(15)T et présentée initialement dans la version 12.0(26)S, la fonction de journalisation de la mémoire non volatile (disque ATA) permet de consigner les messages de journalisation du système sur un disque flash ATA (Advanced Technology Attachment). Les messages enregistrés sur un disque ATA persistent après le redémarrage du routeur.

Ces lignes configurent 134 217 728 octets (128 Mo) de messages de journalisation dans le répertoire syslog du disque flash ATA (disk0), donnant au fichier une taille de 16 384 octets :

```
logging buffered
logging persistent url disk0:/syslog size 134217728 filesize 16384
```

Avant que les messages de journalisation soient écrits dans un fichier sur le disque ATA, Cisco IOS vérifie si le disque possède suffisamment d'espace. Faute d'espace sur le disque, le fichier le plus ancien contenant les messages de journalisation (selon l'horodatage) est supprimé, permettant au fichier actuel d'être enregistré. Le format du nom de fichier est log_month:day:year::time.

---

Remarque : un lecteur flash ATA dispose d'un espace disque limité et doit donc être conservé pour éviter d'écraser les données stockées.

---

Ici, l'exemple explique comment copier des messages de journalisation à partir du disque flash ATA du routeur vers un disque externe sur le serveur FTP 192.168.1.129 dans le cadre des procédures de maintenance :

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

Consultez la section sur la journalisation dans la mémoire vive non volatile (disque ATA) pour en savoir plus sur cette fonction.

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. Sauf si cela est spécifiquement requis, il est conseillé d'éviter la journalisation au niveau 7. La journalisation au niveau 7 génère une charge CPU élevée sur le périphérique, ce qui peut entraîner une instabilité

du périphérique et du réseau.

La commande de configuration générale logging trap est utilisée pour indiquer quels messages de journalisation sont envoyés aux serveurs syslog distants. 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) :

```
!

logging trap 6
logging buffered 6
!
```

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 Cisco IOS, il est possible d'envoyer des messages de journalisation aux sessions de surveillance – des sessions de gestion interactives dans lesquelles la commande EXEC terminal monitor est formulée – et à la console. Toutefois, la charge du CPU d'un périphérique IOS peut se voir augmenter, ce qui n'est pas recommandé. Nous vous conseillons plutôt de transmettre les informations de journalisation à la mémoire tampon locale, qui s'affiche grâce à la commande show logging.

Utilisez les commandes de configuration générales no logging console et no logging monitor pour désactiver la journalisation sur la console et les sessions de surveillance. Cet exemple de configuration montre l'utilisation de ces commandes :

```
!

no logging console
no logging monitor
!
```

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.

Deux options de configuration sont pertinentes lors de la configuration de la journalisation en mémoire tampon : la taille de la mémoire tampon de journalisation et la gravité des messages qui est stockée dans la mémoire tampon. La taille du tampon de journalisation est configurée avec la commande de configuration globale logging buffered size. La plus faible gravité dans la mémoire tampon est configurée grâce à la commande « logging buffered severity ». Un administrateur peut afficher le contenu du tampon de journalisation au moyen de la commande show logging exec.

L'exemple qui suit illustre la configuration d'une mémoire tampon de 16 384 octets pour la journalisation, d'une gravité de niveau 6 (information). Cela signifie que les messages de niveaux 0 (urgences) à 6 (information) sont enregistrés :

```
!

logging buffered 16384 6
!
```

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 d'accroître la cohérence lorsque vous collectez et examinez les messages du journal, vous devriez configurer de façon statique une interface source de journalisation. 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.

Ici, l'exemple de configuration illustre l'utilisation de la commande de configuration générale de l'interface logging source-interface pour indiquer que l'adresse IP de l'interface de la boucle avec retour 0 doit être utilisée pour l'ensemble des messages du journal :

```
!
logging source-interface Loopback 0
!
```

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) :

```
!
service timestamps log datetime msec show-timezone
!
```

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) :

```
!

clock timezone PST -8
service timestamps log datetime msec localtime show-timezone
!
```

## 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 les versions 12.3(7)T et ultérieures de Cisco IOS, les fonctions de remplacement et de restauration de la configuration vous permettent d’archiver la configuration sur le périphérique Cisco IOS. Enregistrées manuellement ou automatiquement, les configurations de ces archives peuvent remplacer la configuration actuelle à l’aide de 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.

Après l’activation, un administrateur peut ajouter la configuration actuelle à l’archive à l’aide de la commande EXEC privilégiée archive config. Les configurations archivées peuvent être affichées à l’aide de la commande EXEC show archive.

Cet exemple illustre la configuration de l'archivage automatique de configuration. Cet exemple montre comment demander au périphérique Cisco IOS de stocker les configurations archivées sous forme de fichiers nommés archived-config-N sur le système de fichiers disk0: , de conserver un maximum de 14 sauvegardes et de les archiver une fois par jour (1 440 minutes) lorsqu'un administrateur exécute la commande EXEC write memory.

```
!

archive
 path disk0:archived-config
 maximum 14
 time-period 1440
 write-memory
!
```

Bien que la fonction d’archivage de la configuration puisse enregistrer 14 configurations de rechange, vous devriez tenir compte des exigences d’espace avant d’utiliser 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 fonction est configurée avec la commande de configuration globale mode de configuration exclusive mode et fonctionne dans l'un des deux modes suivants : auto et manual. En mode automatique, la configuration se verrouille automatiquement quand un administrateur émet la commande EXEC configure terminal. En mode manuel, l’administrateur utilise la commande configure terminal lock afin de verrouiller la configuration lorsqu’elle passe en mode de configuration.

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

```
!
configuration mode exclusive auto
!
```

Cisco IOS Software Resilient Configuration

Ajoutée à la version 12.3(8)T du logiciel Cisco IOS, la fonction de configuration résiliente permet l'enregistrement sûr d'une copie de l'image logicielle de Cisco IOS et d'une copie de la configuration du périphérique utilisée actuellement par un périphérique Cisco IOS. Quand cette fonctionnalité est activée, il n´est pas possible de modifier ou supprimer ces fichiers de sauvegarde. Vous devriez idéalement activer cette fonction pour éviter les suppressions accidentelles et malveillantes de ces fichiers.

```
!
secure boot-image
secure boot-config!
```

Une fois que cette fonctionnalité est activée, il est possible de rétablir une configuration supprimée ou l´image du logiciel Cisco IOS. L'état d'exécution actuel de cette fonction peut être affiché grâce à la commande EXEC show secure boot.

Logiciel Cisco à signature numérique

Ajoutée à la version 15.0(1)M du logiciel Cisco IOS pour les routeurs Cisco de séries 1900, 2900 et 3900, la fonction du logiciel Cisco à signature numérique facilite l'utilisation du logiciel Cisco IOS qui est signé, et donc approuvé, numériquement. Ce peut être fait à l'aide d'un chiffrement asymétrique sécurisé (clé publique).

Une image à signature numérique est assortie d'un hachage chiffré (avec clé privée). Après vérification, le périphérique déchiffre le hachage avec la clé publique correspondante parmi les clés contenues dans sa mémoire principale, puis calcule son propre hachage de l'image. Si le hachage déchiffré correspond à celui qui a été calculé pour l'image, cette dernière n'a donc pas été falsifiée et peut être approuvée.

Les clés du logiciel Cisco à signature numérique sont identifiées selon le type et la version de la clé. Une clé peut être de trois types : clé spéciale, clé de production et clé inversée. Les clés de production et les clés spéciales sont assorties à une version de clé connexe qui se présente par ordre alphabétique chaque fois que la clé est révoquée et remplacée. Les images standard de Cisco IOS et les images ROMmon sont signées à l'aide d'une clé spéciale ou d'une clé de production lorsque vous utilisez le logiciel Cisco à signature numérique. L'image ROMmon peut être mise à niveau et doit être signée à l'aide de la même clé que celle utilisée pour l'image spéciale ou de production téléversée.

Cette commande permet la vérification de l'intégrité de l'image c3900-universalk9-mz.SSA dans la mémoire flash avec les clés comprises dans l'ensemble de clés du périphérique :

```
show software authenticity file flash0:c3900-universalk9-mz.SSA
```

La fonction du logiciel Cisco à signature numérique a également été intégrée à la version 3.1.0.SG

de Cisco IOS XE pour les commutateurs Cisco Catalyst de série 4500 E.

Pour en savoir plus sur la fonction du logiciel Cisco à signature numérique, consultez la section à cet effet.

Le remplacement de clés pour la fonction du logiciel Cisco à signature numérique a été introduit aux versions 15.1(1)T et ultérieures du logiciel Cisco IOS. Le remplacement et la révocation des clés se font pour les clés utilisées aux fins de vérification de la fonction du logiciel Cisco à signature numérique à partir de l'enregistrement de clés d'une plateforme. Seules les clés spéciales et les clés de production peuvent être révoquées si elles étaient compromises.

Une nouvelle clé (spéciale ou de production) pour une image (spéciale ou de production) est fournie dans une image (de production ou de révocation) utilisée pour révoquer la clé spéciale ou de production précédente. L'intégrité de l'image de révocation est vérifiée au moyen d'une clé inversée, qui est déjà enregistrée sur la plateforme. Une telle clé ne change pas. Si vous révoquez une clé de production après le chargement de l'image de révocation, la nouvelle clé est ajoutée à l'ensemble de clés, et l'ancienne clé correspondante peut alors être révoquée, pourvu que l'image ROMmon soit mise à niveau et que la nouvelle image de production soit démarrée. Si vous révoquez une clé spéciale, une image de production est à ce moment chargée. Cette image ajoute la nouvelle clé spéciale et peut révoquer l'ancienne. Après la mise à niveau de ROMmon, la nouvelle image spéciale peut être démarrée.

Cet exemple montre la révocation d'une clé spéciale. Ces commandes ajoutent la nouvelle clé spéciale dans l'ensemble de clés à partir de l'image de production actuelle, copient une nouvelle image ROMmon (C3900_rom-monitor.srec.SSB) dans la zone de stockage (usbflash0:), mettent à niveau le fichier ROMmon et révoquent l'ancienne clé spéciale :

```
software authenticity key add special
copy tftp://192.168.1.129/C3900_rom-monitor.srec.SSB usbflash0:
upgrade rom-monitor file usbflash0:C3900_PRIV_RM2.srec.SSB
software authenticity key revoke special
```

Une nouvelle image spéciale (c3900-universalk9-mz.SSB) peut ensuite être copiée dans la mémoire flash à téléverser, et la signature de l'image est vérifiée au moyen de la clé spéciale que vous venez d'ajouter (.SSB) :

```
copy /verify tftp://192.168.1.129/c3900-universalk9-mz.SSB flash:
```

La révocation et le remplacement de la clé ne sont pas pris en charge par les commutateurs Catalyst de série 4500 E qui utilisent le logiciel Cisco IOS XE, même s'ils prennent en charge la fonction du logiciel Cisco à signature numérique.

Consultez la section sur la révocation et le remplacement des clés du logiciel Cisco à signature

numérique du guide du logiciel Cisco à signature numérique pour de plus amples renseignements sur ces fonctions.

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 fonction est activée à l'aide de la commande logging enable configuration change logger configuration mode. Les commandes facultatives hidekeys et logging size entries sont utilisées pour améliorer la configuration par défaut. En effet, elles empêchent la journalisation des données du mot de passe et prolongent le journal des modifications.

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. En outre, vous devriez idéalement employer la commande de configuration notify syslog afin d'activer la génération des messages syslog si une modification est apportée à la configuration.

```
!

archive
 log config
  logging enable
  logging size 200
  hidekeys
  notify 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 du plan de contrôle se composent des protocoles et des processus qui communiquent entre les périphériques réseau pour transférer les données de la source vers 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 au minimum la charge du CPU qui est nécessaire 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 existe deux types de messages de redirection ICMP : la redirection pour une adresse hôte et la redirection pour un sous-réseau entier. Un utilisateur malveillant peut exploiter la capacité du routeur à transmettre des messages de redirections ICMP en envoyant continuellement des paquets au routeur, forçant ce dernier à répondre à l’aide de messages de redirection ICMP. Cette situation a des répercussions négatives sur le CPU et le rendement 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 tels messages peut accroître l’utilisation du CPU 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 messages ICMP inaccessibles peut être désactivée grâce à la commande no ip unreachables. La restriction du débit ICMP inaccessible peut être modifiée par défaut avec la commande de configuration générale ip icmp rate-limit unreachable interval-in-ms.

### 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.

L’utilisation du protocole proxy ARP présente plusieurs inconvénients. Mentionnons notamment l’augmentation du trafic ARP sur le segment de réseau ainsi que l’épuisement des ressources et des attaques de l’homme du milieu. 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. L’agresseur peut parvenir à épuiser toute la mémoire disponible s’il envoie un grand nombre de requêtes ARP.

Les attaques de l’homme du milieu permettent à un hôte du réseau d’usurper l’adresse MAC du routeur, ce qui se traduit par l’envoi du trafic à l’agresseur par des hôtes sans méfiance. Le proxy ARP peut être désactivé au moyen de la commande de configuration no ip proxy-arp.

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

## Limiter l’incidence du trafic du plan de contrôle sur le CPU

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.

### Comprendre le trafic du plan de contrôle

Afin de protéger correctement le plan de contrôle du périphérique Cisco IOS, il est essentiel de comprendre les types de trafics qui sont acheminés par le 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 consiste en la catégorie visant à recevoir le trafic de contiguïté. Il contient une entrée dans le tableau CEF (Cisco Express Forwarding) par lequel le saut de routage suivant s’avère être le périphérique lui-même, indiqué par le terme « Receive » dans la sortie show ip cef CLI. 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 que gère le CPU est le trafic du plan de données – un trafic dont la destination dépasse le périphérique Cisco IOS –, ce qui requiert un traitement spécial de la part du 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 :

- Journalisation des listes de contrôle d’accès : Le trafic de journalisation des listes de contrôle d’accès (ACL) est constitué de tout paquet généré à la suite d’une correspondance (« permit » ou « deny ») d’ACE où est utilisé le mot clé « log ».

- Transfert de chemin inverse (RPF) en monodiffusion : L’utilisation du RPF en monodiffusion, conjointement avec une ACL, peut entraîner la commutation de certains paquets.

- Options IP : Tout paquet IP ayant des options intégrées doit être traité par le CPU.

- Fragmentation : Tout paquet IP nécessitant une fragmentation doit être transmis au CPU aux fins de traitement.

- Expiration de la durée de vie (TTL) : Les paquets dont la valeur TTL est inférieure ou égale à 1 nécessitent l'envoi de messages ICMP « time-exceeded » [délai expiré] (type 11, code 0), entraînant ainsi le traitement du CPU.

- Messages ICMP inaccessibles : Les paquets qui génèrent des messages ICMP inaccessibles en raison du routage, de la MTU ou du filtre sont traités par le CPU.

- Trafic nécessitant une requête ARP : Les destinations n'ayant aucune entrée ARP n'ont pas besoin d'être traitées par le CPU.

- Trafic non IP : Tout trafic non IP est traité par le 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 show interface switching fournit des informations sur le nombre de paquets qui sont traités 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 options
    - qui exigent la fragmentation
    - qui sont envoyés pour diffuser l'espace d'adressage
    - qui 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. Les ACL d’infrastructure (iACL) sont vues en profondeur dans la section Limit Access to the Network with Infrastructure ACLs [limiter l’accès au réseau avec les ACL d’infrastructure] du présent document.

Vous devriez idéalement mettre en œuvre les iACL pour protéger le plan de contrôle des périphériques 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 :

```
!
!--- Permit SSH from trusted hosts allowed to the device.
!

access-list 151 permit tcp 192.168.100.0 0.0.0.255 any eq 22
!
!--- Deny SSH from all other sources to the RP.
!

access-list 151 deny tcp any any eq 22
!
!--- Permit all other traffic to the device.
!--- according to security policy and configurations.
!

access-list 151 permit ip any any
!
!--- Apply this access list to the receive path.
!

ip receive access-list 151
!
```

Référez-vous à GSR : Receive Access Control Lists afin d'aider à identifier et autoriser le trafic légitime vers un périphérique et refuser tous les paquets indésirables.

CoPP

La fonction CoPP peut également être utilisée pour limiter les paquets IP 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.

---

Remarque : l'abandon du trafic provenant d'adresses IP inconnues ou non approuvées peut empêcher les hôtes disposant d'adresses IP attribuées dynamiquement de se connecter au périphérique Cisco IOS.

---

```
!

access-list 152 deny tcp <trusted-addresses> <mask> any eq 22
access-list 152 permit tcp any any eq 22
access-list 152 deny ip any any
!

class-map match-all COPP-KNOWN-UNDESIRABLE
 match access-group 152
!

policy-map COPP-INPUT-POLICY
 class COPP-KNOWN-UNDESIRABLE
  drop
!

control-plane
 service-policy input COPP-INPUT-POLICY
!
```

Dans l'exemple CoPP précédent, les entrées des ACL qui correspondent aux paquets non autorisés avec l'action « permit » viennent supprimer les paquets au moyen de la fonction de suppression de la liste des politiques, tandis que les paquets qui correspondent à l'action « deny » ne sont quant à eux pas touchés par cette fonction.

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 :

- Fonction de filtrage des ports : Cette fonction permet le contrôle et la suppression des paquets envoyés aux ports TCP ou UDP qui sont fermés ou qui ne sont pas à l'écoute.

- Fonction de seuil de la file d'attente : Cette fonction limite, pour un protocole en particulier, le nombre de paquets qui sont autorisés dans la file d'attente liée à l'entrée IP du plan de contrôle.

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. À ce titre, toute entreprise ayant des exigences plus que modestes en matière de connectivité utilise souvent le protocole BGP. Le protocole BGP est souvent la cible d'agresseurs en raison de son omniprésence et de la nature « préréglage absolu » des configurations BGP dans les petites entreprises. 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.

Connue à la fois comme le mécanisme GTSM (Generalized TTL-based Security Mechanism) et le protocole BTSH (BGP TTL Security Hack), une protection de la sécurité basée sur la durée de vie

(TTL) tire profit de la valeur de durée de vie des paquets IP afin de s’assurer que les paquets BGP reçus proviennent d’un homologue connecté directement. Cette fonctionnalité nécessite souvent la coordination des routeurs d'appairage ; cependant, une fois activée, elle peut complètement vaincre de nombreuses attaques basées sur TCP contre BGP.

Le mécanisme GTSM pour BGP est activé à l’aide de l’option ttl-security pour la commande de configuration du routeur BGP neighbor. Cet exemple illustre la configuration de cette fonctionnalité :

```
!

router bgp <asn>
 neighbor <ip-address> remote-as <remote-asn>
 neighbor <ip-address> ttl-security hops <hop-count>
!
```

À mesure 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 l’homologue avec MD5 entraîne une authentification MD5 pour chaque paquet envoyé lors 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 haut-parleur BGP qui reçoit le message utilise le même algorithme et la même clé secrète pour régénérer l’authentification MD5. Si les condensés reçus et calculés ne sont pas identiques, le paquet est rejeté.

L’authentification de l’homologue avec MD5 est configurée avec l’option mot de passe pour la commande de configuration du routeur BGP neighbor. L'utilisation de cette commande est illustrée comme suit :

```
!

router bgp <asn>
 neighbor <ip-address> remote-as <remote-asn>
 neighbor <ip-address> password <secret>
!
```

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

Configurer le nombre maximal de préfixes

Les préfixes BGP sont stockés en mémoire par a routeur. Plus le nombre de préfixes qu'un routeur doit contenir est élevé, plus la mémoire que doit consommer le protocole BGP est grande. 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.

Lorsque vous configurez cette fonctionnalité avec la commande de configuration de routeur neighbor maximum-prefix, un argument est requis : 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.

```
!

router bgp <asn>
 neighbor <ip-address> remote-as <remote-asn>
 neighbor <ip-address> maximum-prefix <shutdown-threshold> <log-percent>
!
```

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

Filtrer les préfixes BGP avec les 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. Les listes de préfixes doivent être utilisées dans la mesure du possible afin de garantir l'envoi du trafic réseau sur les chemins prévus. 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.

```
!

ip prefix-list BGP-PL-INBOUND seq 5 permit 0.0.0.0/0
ip prefix-list BGP-PL-OUTBOUND seq 5 permit 192.168.2.0/24
!

router bgp <asn>
 neighbor <ip-address> prefix-list BGP-PL-INBOUND in
 neighbor <ip-address> prefix-list BGP-PL-OUTBOUND out
!
```

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

Filtrer les préfixes BGP avec les listes d’accès au chemin du système autonome

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. Il est possible d’utiliser cette fonction conjointement avec les listes de préfixes afin d’établir un ensemble robuste de filtres.

Cet exemple de configuration utilise les listes d’accès au chemin d’AS pour que les préfixes entrants soient limités à ceux générés par le système AS distant, et les préfixes sortants, à ceux provenant du système autonome local. Les préfixes qui sont originaires de tout autre système autonome sont filtrés et ne sont pas installés dans le tableau de routage.

```
!

ip as-path access-list 1 permit ^65501$
ip as-path access-list 2 permit ^$
!

router bgp <asn>
 neighbor <ip-address> remote-as 65501
 neighbor <ip-address> filter-list 1 in
 neighbor <ip-address> filter-list 2 out
!
```

## Protocoles sécurisés de passerelle intérieure

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 utiliser un protocole IGP (Interior Gateway Protocol) pour obtenir cet affichage. 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 :

```
!

key chain <key-name>
 key <key-identifier>
 key-string <password>
!

interface <interface>
 ip authentication mode eigrp <as-number> md5
 ip authentication key-chain eigrp <as-number> <key-name>
!
```

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

```
!

key chain <key-name>
 key <key-identifier>
 key-string <password>
!

interface <interface>
 ip rip authentication mode md5
 ip rip authentication key-chain <key-name>
!
```

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

```
!

interface <interface>
 ip ospf message-digest-key <key-id> md5 <password>
!

router ospf <process-id>
 network 10.0.0.0 0.255.255.255 area 0
 area 0 authentication message-digest
!
```

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 :

```
!

router eigrp <as-number>
 passive-interface default
 no passive-interface <interface>
!
```

Filtrage de route

Afin de réduire la possibilité d’introduire de fausses informations de routage dans le réseau, vous devez utiliser le filtre de routage. 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 EIGRP et RIP, l’utilisation de la commande distribute-list au moyen du mot clé out limite les informations diffusées, tandis que l’utilisation du mot clé in limite le traitement des mises à jour. 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 :

```
!

ip prefix-list <list-name> seq 10 permit <prefix>
!

router eigrp <as-number>
 passive-interface default
 no passive-interface <interface>
 distribute-list prefix <list-name> out <interface>
!
```

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

```
!

ip prefix-list <list-name> seq 10 permit <prefix>
!

router eigrp <as-number>
 passive-interface default
 no passive-interface <interface>
 distribute-list prefix <list-name> in <interface>
!
```

Consultez la section sur la [configuration des fonctions indépendantes du protocole de routage IP pour savoir comment contrôler la divulgation et le traitement des mises à jour de routage.]

Le présent exemple du protocole OSPF emploie une liste de préfixes avec la commande area filter-list axée sur OSPF :

```
!

ip prefix-list <list-name> seq 10 permit <prefix>
!
```

```
router ospf <process-id>
 area <area-id> filter-list prefix <list-name> in
!
```

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. Cela est possible avec le protocole OSPF si vous utilisez la fonction de protection contre une surcharge de la base de données d'états de liaison.

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

```
!

router ospf <process-id>
 max-lsa <maximum-number>
!
```

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.

## Protocoles sécurisés de redondance de premier saut

Les protocoles FHRP (First Hop Redundancy Protocols) assurent la résilience et la redondance des périphériques qui jouent le rôle de 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 utilisent des communications non authentifiées. 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.

Pour éviter ce type d'attaques, les protocoles FHRP pris en charge par le logiciel Cisco IOS intègrent une fonction d'authentification avec soit des chaînes de texte, soit MD5. 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 :

```
!

interface FastEthernet 1
 description *** GLBP Authentication ***
 glbp 1 authentication md5 key-string <glbp-secret>
 glbp 1 ip 10.1.1.1
!

interface FastEthernet 2
 description *** HSRP Authentication ***
 standby 1 authentication md5 key-string <hsrp-secret>
 standby 1 ip 10.2.2.1
!

interface FastEthernet 3
 description *** VRRP Authentication ***
 vrrp 1 authentication md5 key-string <vrrp-secret>
 vrrp 1 ip 10.3.3.1
!
```

# 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. Pour cette raison, il est important de privilégier la protection des plans de gestion et de contrôle plutôt que le plan de données lorsque vous sécurisez un périphérique 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.

Consultez la section sur le filtre du trafic de transit avec les ACL de transit du présent document pour en savoir plus.

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 permettent également de modifier le chemin qu'emprunte le trafic sur le réseau, et ainsi contourner possiblement les 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. Dans le premier formulaire de la commande ip options drop, tous les paquets IP qui contiennent des options IP reçues par le périphérique Cisco IOS 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 :

```
!
ip options drop
!
```

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 :

```
!
no ip source-route
!
```

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 certains cas, il est possible qu'un agresseur parvienne à faire envoyer de nombreux messages de redirection ICMP par le périphérique Cisco IOS, ce qui se solde par une charge élevée du CPU. Pour cette raison, il est recommandé que la transmission des redirections d'ICMP soit désactivée. Les redirections ICMP sont désactivées à l'aide de la commande de configuration d'interface no ip redirections, comme l'illustre l'exemple suivant :

```
!

interface FastEthernet 0
 no ip redirects
!
```

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.

Cette fonctionnalité est désactivée par défaut dans les versions actuelles de la plate-forme logicielle Cisco IOS ; toutefois, elle peut être activée via 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. Cela est possible grâce à l'utilisation d'une liste de contrôle d'accès en option avec la commande ip directed-broadcast. La configuration donnée en exemple ici limite les diffusions dirigées vers les paquets UDP qui proviennent d'un réseau fiable, 192.168.1.0/24 :

```
!

access-list 100 permit udp 192.168.1.0 0.0.0.255 any
!
```

```
interface FastEthernet 0
 ip directed-broadcast 100
!
```

## Filtrer le trafic de transit avec les ACL de transit

Il est possible de contrôler le trafic qui transite par le réseau à l'aide des ACL de transit (tACL). Ceci contraste avec les ACL d'infrastructure qui recherchent à filtrer le trafic qui est destiné au réseau lui-même. Le filtre que fournissent les tACL est avantageux pour le trafic devant idéalement être filtré pour un groupe particulier de périphériques ou pour le trafic qui transite par 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.

Pour en savoir plus, consultez, dans le présent document, la section portant sur les protections contre l'usurpation de contenu.

Référez-vous à Listes de contrôle d'accès de transit : Filtrage à 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. Le protocole ICMP est utilisé par les outils de dépannage réseau ping et traceroute, ainsi que par la détection de MTU de chemin ; cependant, la connectivité ICMP externe est rarement nécessaire pour le bon fonctionnement d'un réseau.

Le logiciel Cisco IOS fournit la fonctionnalité pour filtrer spécifiquement des messages ICMP par nom ou type et code. Ici, l'ACL donné en exemple permet l'utilisation du protocole ICMP à partir de réseaux fiables, tout en bloquant les paquets ICMP provenant d'autres sources :

```
!

ip access-list extended ACL-TRANSIT-IN
!
!--- Permit ICMP packets from trusted networks only
!

 permit icmp host <trusted-networks> any
!
!--- Deny all other IP traffic to any network device
!
```

```
 deny icmp any any
!
```

Filtrer les fragments IP

Comme indiqué précédemment dans la section Limiter l’accès au réseau assorti de listes de contrôle d’accès (ACL) d’infrastructure du présent document, le filtre des paquets IP fragmentés peut poser problème lorsqu’il est question des 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 :

```
!

ip access-list extended ACL-TRANSIT-IN
!
!--- Deny IP fragments using protocol-specific ACEs to aid in
!--- classification of attack traffic
!

 deny tcp any any fragments
 deny udp any any fragments
 deny icmp any any fragments
 deny ip any any fragments
!
```

Consultez les listes de contrôle d’accès et les fragments IP pour en savoir plus sur le traitement des paquets IP fragmentés par l’ACL.

Support d'ACL pour le filtrage des options IP

Dans les versions 12.3(4)T et ultérieures, le logiciel Cisco IOS prend en charge l’utilisation des ACL pour filtrer les paquets IP en fonction des options IP contenues dans le paquet. La présence d’options IP dans un paquet peut indiquer une tentative de contournement des contrôles de sécurité dans le réseau ou une altération des 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 :

```
!
```

```
ip access-list extended ACL-TRANSIT-IN
!
!--- Deny IP packets containing IP options
!

 deny ip any any option any-options
!
```

## Protections anti-spoofing

Bien des attaques consistent à usurper une adresse IP source pour être efficaces ou pour dissimuler la véritable source de l'attaque et ainsi empêcher d'être retracé. Cisco IOS offre le transfert RPF en monodiffusion et le service IPSG (IP Source Guard) afin de dissuader les agresseurs de lancer des attaques basées sur l'usurpation d'adresse IP source. En outre, les ACL et le routage null sont souvent déployés en tant que moyens manuels de prévention du spoofing.

IP Source Guard permet de réduire au minimum l'usurpation pour les réseaux sous contrôle administratif direct en vérifiant le port de commutation, l'adresse MAC et l'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 ARP (Address Resolution Protocol) dynamique (DAI) atténue les vecteurs d'attaque qui utilisent l'empoisonnement des caches ARP sur les 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. Le transfert RPF en monodiffusion, configuré pour chaque interface, compte sur votre capacité à activer Cisco Express Forwarding sur chaque périphérique.

Le protocole RPF monodiffusion peut être configuré dans l'un des deux modes suivants : 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 :

```
!

ip cef
!

interface <interface>
```

```
  ip verify unicast source reachable-via <mode>
!
```

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 :

```
!

ip dhcp snooping
ip dhcp snooping vlan <vlan-range>
!
```

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

```
!
interface <interface-id>
   ip verify source
!
```

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

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 des ports a repéré une violation MAC, un des quatre modes de violation peut alors être utilisé. Ces modes sont protect, restrict, shutdown et

shutdown VLAN. Dans les cas où un port donne accès seulement à un ordinateur à l'aide de protocoles standard, un seul peut suffire. Les protocoles qui exploitent les adresses virtuelles MAC, tel que HSRP, ne fonctionnent pas quand le nombre maximal est égal à un.

```
!

interface <interface>
  switchport
  switchport mode access
  switchport port-security
  switchport port-security mac-address sticky
  switchport port-security maximum <number>
  switchport port-security violation <violation-mode>
!
```

Pour en savoir plus sur la [configuration de la sécurité des ports, consultez le document à cet effet.]

Inspection dynamique d'ARP

La DAI peut être utilisée pour limiter les attaques par empoisonnement ARP sur les 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 pour corrompre le cache ARP des 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 les environnements DHCP, la DAI se sert des données générées par la fonction d'espionnage 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 :

```
!
ip dhcp snooping
ip dhcp snooping vlan <vlan-range>
!
```

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

```
!
ip arp inspection vlan <vlan-range>
!
```

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 :

```
!

arp access-list <acl-name>
 permit ip host <sender-ip> mac host <sender-mac>
!

ip arp inspection filter <arp-acl-name> vlan <vlan-range>
!
```

La DAI peut également être activée par interface, si elle est prise en charge.

```
ip arp inspection limit rate <rate_value> burst interval <interval_value>
```

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

ACL anti-spoofing

Les ACL configurées manuellement peuvent protéger contre l'usurpation statique si les attaques touchent un espace inutilisé et peu fiable. Généralement, ces ACL anti-spoofing sont appliquées au trafic entrant aux frontières du réseau comme composants d'une plus grande ACL. Les ACL anti-usurpation nécessitent une surveillance régulière, car elles peuvent changer fréquemment. L'usurpation peut être réduite au minimum dans le trafic provenant du réseau local si vous appliquez des ACL sortantes qui limitent le trafic à des 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.

```
!

ip access-list extended ACL-ANTISPOOF-IN
 deny    ip 10.0.0.0 0.255.255.255 any
 deny    ip 192.168.0.0 0.0.255.255 any
!

interface <interface>
 ip access-group ACL-ANTISPOOF-IN in
!
```

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.

## Limiter l’incidence du trafic du plan de données sur le CPU

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 comprend un trafic qui transite par le périphérique réseau, doit être sécurisé pour garantir le bon fonctionnement des plans 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 :

- Journalisation des listes de contrôle d’accès : Le trafic de journalisation des listes de contrôle d’accès (ACL) est constitué de tout paquet généré à la suite d’une correspondance (« permit » ou « deny ») d’ACE où est utilisé le mot clé « log ».
- Transfert RPF en monodiffusion : L’utilisation du RPF en monodiffusion, conjointement avec une ACL, pourrait entraîner la commutation de certains paquets.
- Options IP : Tout paquet IP ayant des options intégrées doit être traité par le CPU.
- Fragmentation : Tout paquet IP nécessitant une fragmentation doit être transmis au CPU aux fins de traitement.
- Expiration de la durée de vie (TTL) : Les paquets dont la valeur TTL est inférieure ou égale à 1 nécessitent l’envoi de messages ICMP « time-exceeded » [délai expiré] (type 11, code 0), entraînant ainsi le traitement du CPU.
- Messages ICMP inaccessibles : Les paquets qui génèrent des messages ICMP inaccessibles en raison du routage, de la MTU ou du filtre sont traités par le CPU.
- Trafic nécessitant une requête ARP : Les destinations n’ayant aucune entrée ARP n’ont pas besoin d’être traitées par le CPU.
- Trafic non IP : Tout trafic non IP est traité par le CPU.

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

sur le durcissement du plan de données.

Filtrer selon la valeur 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.

```
!
!--- Create ACL policy that filters IP packets with a TTL value
!--- less than 6
!

ip access-list extended ACL-TRANSIT-IN
 deny ip any any ttl lt 6
 permit ip any any
!
!--- Apply access-list to interface in the ingress direction
!

interface GigabitEthernet 0/0
 ip access-group ACL-TRANSIT-IN in
!
```

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 les versions 12.4(4)T et ultérieures de Cisco IOS, FPM (Flexible Packet Matching) permet à un administrateur de faire correspondre les bits arbitraires d’un paquet. Cette politique de FPM rejette les paquets avec une valeur de TTL inférieure à six.

```
!

load protocol flash:ip.phdf
```

```
!

class-map type access-control match-all FPM-TTL-LT-6-CLASS
 match field IP ttl lt 6
!

policy-map type access-control FPM-TTL-LT-6-DROP-POLICY
 class  FPM-TTL-LT-6-CLASS
  drop
!

interface FastEthernet0
 service-policy type access-control input FPM-TTL-LT-6-DROP-POLICY
!
```

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

Filtrer selon la présence des options IP

Dans les versions 12.3(4)T et ultérieures de Cisco IOS, vous pouvez prendre en charge les ACL pour les options de filtre IP dans une liste d'accès IP étendue donnée afin de filtrer les paquets IP disposant d'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. Soulignons également que les protocoles RSVP, l'ingénierie de trafic MPLS (Multiprotocol Label Switching), les protocoles IGMP de versions 2 et 3, et les autres protocoles utilisant les paquets d'options IP risquent de fonctionner incorrectement si les paquets de ces protocoles sont supprimés. Si ces protocoles sont utilisés sur le réseau, la prise en charge ACL pour le filtrage des options IP peut être utilisée. Toutefois, la fonction de suppression sélective des options IP ACL peut supprimer ce trafic et ces protocoles risquent de ne pas fonctionner correctement. Si aucun protocole nécessitant les options IP n'est utilisé, la suppression sélective des options IP des ACL sera la méthode privilégiée pour la suppression des paquets.

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

```
!

ip access-list extended ACL-TRANSIT-IN
 deny ip any any option any-options
 permit ip any any
!

interface GigabitEthernet 0/0
 ip access-group ACL-TRANSIT-IN in
!
```

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)

```
!

ip access-list extended ACL-TRANSIT-IN
 deny ip any any option eool
 deny ip any any option record-route
 deny ip any any option timestamp
 deny ip any any option lsr
 deny ip any any option ssr
 permit ip any any
!

interface GigabitEthernet 0/0
 ip access-group ACL-TRANSIT-IN in
!
```

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

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

Une autre fonctionnalité du logiciel Cisco IOS qui peut être utilisée afin de filtrer les paquets avec options IP est CoPP. Dans les versions 12.3(4)T et ultérieures de Cisco IOS, CoPP permet à un administrateur de filtrer le débit du trafic pour les paquets du plan de contrôle. 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 :

```
!

ip access-list extended ACL-IP-OPTIONS-ANY
 permit ip any any option any-options
```

```
!

class-map ACL-IP-OPTIONS-CLASS
 match access-group name ACL-IP-OPTIONS-ANY
!

policy-map COPP-POLICY
 class ACL-IP-OPTIONS-CLASS
  drop
!

control-plane
 service-policy input COPP-POLICY
!
```

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)

```
!

ip access-list extended ACL-IP-OPTIONS
 permit ip any any option eool
 permit ip any any option record-route
 permit ip any any option timestamp
 permit ip any any option lsr
 permit ip any any option ssr
!

class-map ACL-IP-OPTIONS-CLASS
 match access-group name ACL-IP-OPTIONS
!

policy-map COPP-POLICY
 class ACL-IP-OPTIONS-CLASS
  drop
!

control-plane
 service-policy input COPP-POLICY
!
```

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.

Consultez la section portant sur le déploiement des politiques du plan de contrôle pour obtenir de plus amples renseignements sur la fonction CoPP.

Protection du plan de contrôle

Dans les versions 12.4(4)T et ultérieures de Cisco IOS, la fonction CPPr (Control Plane Protection) peut être utilisée pour limiter ou contrôler le plan de contrôle au moyen du CPU du périphérique 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 agrégé en trois catégories distinctes de plans de contrôle appelées sous-interfaces : les sous-interfaces Host, Transit et 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.

```
!

ip access-list extended ACL-IP-TTL-0/1
 permit ip any any ttl eq 0 1
!

class-map ACL-IP-TTL-0/1-CLASS
 match access-group name ACL-IP-TTL-0/1
!

ip access-list extended ACL-IP-TTL-LOW
 permit ip any any ttl lt 6
!

class-map ACL-IP-TTL-LOW-CLASS
 match access-group name ACL-IP-TTL-LOW
!

ip access-list extended ACL-IP-OPTIONS
 permit ip any any option eool
 permit ip any any option record-route
 permit ip any any option timestamp
 permit ip any any option lsr
 permit ip any any option ssr
!

class-map ACL-IP-OPTIONS-CLASS
 match access-group name ACL-IP-OPTIONS
!

policy-map CPPR-CEF-EXCEPTION-POLICY
 class ACL-IP-TTL-0/1-CLASS
  drop
```

```
 class ACL-IP-OPTIONS-CLASS
  drop
!

!-- Apply CPPr CEF-Exception policy CPPR-CEF-EXCEPTION-POLICY to
!-- the CEF-Exception CPPr sub-interface of the device

!

control-plane cef-exception
 service-policy input CPPR-CEF-EXCEPTION-POLICY
!

policy-map CPPR-TRANSIT-POLICY
 class ACL-IP-TTL-LOW-CLASS
  drop
!

control-plane transit
 service-policy input CPPR-TRANSIT-POLICY
!
```

Dans la politique de CPPr précédente, les entrées ACL qui correspondent aux paquets ayant l'action « permit » causent l'abandon de ces paquets par la suppression de la liste des politiques, tandis que les paquets dont l'action est « deny » (non illustré) ne sont pas touchés par une telle suppression.

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. Les deux principales méthodes qu'utilise le logiciel Cisco IOS à cet effet sont NetFlow et les ACL de classification. 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. Les données NetFlow peuvent être consultées et analysées par l'interface CLI, ou exportées vers un collecteur NetFlow commercial ou gratuit à des fins d'agrégation et d'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. Les flux de NetFlow peuvent être créés grâce à des

données de trafic échantillonnées dans des environnements à haut volume.

CEF, ou CEF distribué, est une condition préalable à l'activation de 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 | sortie}.

```
!

ip flow-export destination <ip-address> <udp-port>
ip flow-export version <version>
!

interface <interface>
 ip flow <ingess|egress>
!
```

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 aussi séparer un refus implicite à la fin d'une ACL en entrées ACE granulaires pour cibler les types de trafic refusés.

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 :

```
!

ip access-list extended ACL-SMB-CLASSIFY
 remark Existing contents of ACL
 remark Classification of SMB specific TCP traffic
 deny    tcp any any eq 139
 deny    tcp any any eq 445
 deny    ip any any
!
```

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

```
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. C'est toutefois impossible avec les ACL des interfaces routées. Par exemple, le mappage du réseau local virtuel (VLAN) peut être utilisé pour empêcher les hôtes d'un même VLAN de communiquer entre eux, et réduire ainsi les occasions des agresseurs locaux ou les vers d'exploiter 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 cartes d'accès VLAN prennent en charge les listes d'accès IPv4 et MAC ; toutefois, elles ne prennent pas en charge la journalisation ni les listes de contrôle d'accès IPv6.

Dans cet exemple, on emploie une ACL étendue nommée pour illustrer la configuration de cette fonction :

```
!

ip access-list extended <acl-name>
 permit <protocol> <source-address> <source-port> <destination-address>
     <destination-port>
!

vlan access-map <name> <number>
 match ip address <acl-name>
 action <drop|forward>
!
```

Cet exemple illustre l'utilisation du mappage du VLAN en vue de refuser les ports TCP 139 et 445 ainsi que le protocole vines-ip :

```
!

ip access-list extended VACL-MATCH-ANY
 permit ip any any
!

ip access-list extended VACL-MATCH-PORTS
 permit tcp 192.168.1.0 0.0.0.255 192.168.1.0 0.0.0.255 eq 445
 permit tcp 192.168.1.0 0.0.0.255 192.168.1.0 0.0.0.255 eq 139
!

mac access-list extended VACL-MATCH-VINES
 permit any any vines-ip
!

vlan access-map VACL 10
 match ip address VACL-MATCH-VINES
 action drop
!

vlan access-map VACL 20
 match ip address VACL-MATCH-PORTS
 action drop
!

vlan access-map VACL 30
 match ip address VACL-MATCH-ANY
 action forward
!

vlan filter VACL vlan 100
!
```

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 employée pour la création PACL, qui a préséance sur le mappage du VLAN et les ACL du routeur, est identique à celle des ACL du routeur. Si un ACL est appliqué à une interface de couche 2, il est alors désigné sous le nom de PACL. La configuration implique la création d'une ACL IPv4, IPv6 ou MAC ainsi que son application à l'interface de couche 2.

Cet exemple utilise une liste d'accès étendue nommée pour illustrer la configuration de cette fonction :

```
!

ip access-list extended <acl-name>
 permit <protocol> <source-address> <source-port> <destination-address>
     <destination-port>
!

interface <type> <slot/port>
 switchport mode access
 switchport access vlan <vlan_number>
 ip access-group <acl-name> in
!
```

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
```

---

Remarque : il est nécessaire de classer les paquets de couche 3 en 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. Par la suite, vous pourrez utiliser une liste d’accès MAC dans l’environnement IP.

## Utilisation d’un 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 PVLAN, tous les périphériques d’un VLAN de couche 2 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 seul serveur est compromis, l’absence de connectivité vers d’autres serveurs découlant de l’application des PVLAN pourrait contribuer à limiter ce compromis.

Il existe trois types de VLAN privés : les VLAN isolés, les VLAN de communauté et les 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 n'y avoir qu'un seul VLAN isolé par VLAN principal, et seuls les ports de proximité peuvent communiquer avec les ports d'un VLAN isolé. 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 :

```
!

vlan 11
 private-vlan isolated
!

vlan 20
 private-vlan primary
 private-vlan association 11
!

interface FastEthernet 1/1
 description *** Port in Isolated VLAN ***
 switchport mode private-vlan host
 switchport private-vlan host-association 20 11
!
```

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.

```
!
```

```
vlan 12
 private-vlan community
!

vlan 20
 private-vlan primary
 private-vlan association 12
!

interface FastEthernet 1/2
 description *** Port in Community VLAN ***
 switchport mode private-vlan host
 switchport private-vlan host-association 20 12
!
```

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 :

```
!

vlan 11
 private-vlan isolated
!

vlan 12
 private-vlan community
!

vlan 20
 private-vlan primary
 private-vlan association 11-12
!

interface FastEthernet 1/1
 description *** Port in Isolated VLAN ***
 switchport mode private-vlan host
 switchport private-vlan host-association 20 11
!

interface FastEthernet 1/2
 description *** Port in Community VLAN ***
 switchport mode private-vlan host
 switchport private-vlan host-association 20 12
!

interface FastEthernet 1/12
 description *** Promiscuous Port ***
```

```
 switchport mode private-vlan promiscuous
 switchport private-vlan mapping 20 add 11-12
!
```

Si vous mettez en place des PVLAN, il faut vous assurer que la configuration de couche 3 existante prend en charge les restrictions imposées par les PVLAN et n'autorise pas le contournement de la configuration du PVLAN. Le filtre de couche 3 ayant une ACL ou un pare-feu de routeur peut empêcher le contournement de la configuration du 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

Les descriptions de certaines fonctions figurant dans ce document ont été rédigées par les équipes d'élaboration de l'information de Cisco.

# Annexe : Liste de contrôle du renforcement des périphériques Cisco IOS

Cette liste de contrôle regroupe les étapes de renforcement présentées dans le présent guide. Les administrateurs peuvent s'en servir comme référence pour les fonctions de renforcement utilisées et prises en considération pour un périphérique Cisco IOS, même si la fonction n'a pas été mise en œuvre étant donné qu'elle ne s'appliquait pas. Idéalement, les administrateurs devraient évaluer chaque option en fonction de son risque potentiel avant de la mettre en œuvre.

## Plan de gestion

- Mots de passe
    - Activation du hachage MD5 (option secrète) pour les mots de passe des utilisateurs locaux
    - Configuration du verrouillage des nouvelles tentatives pour la saisie du mot de passe

    - Désactivation de la récupération du mot de passe (tenir compte des risques)

- Désactivation des services inutilisés
- Configuration des messages keepalive TCP pour les sessions de gestion
- Réglage des notifications concernant le seuil de la mémoire et du CPU
- Configurer
    - Notifications concernant le seuil de la mémoire et du CPU
    - Réservation de la mémoire pour l'accès à la console
    - Détecteur de fuite de mémoire
    - Détection des débordements de mémoire tampon
    - Fonction Enhanced crashinfo collection
- Utilisation des iACL pour restreindre l'accès à la gestion
- Filtrer (tenir compte des risques)
    - Paquets ICMP
    - Fragments IP
    - Options IP
    - Valeur de durée de vie dans les paquets
- Protection du plan de contrôle
    - Configuration du filtre pour les ports
    - Configuration des seuils de la file d'attente
- Accès de gestion
    - Utilisation de la protection du plan de gestion pour restreindre les interfaces de gestion
    - Réglage du délai d'expiration de la commande EXEC
    - Utilisation d'un protocole de transport chiffré (comme SSH) pour l'accès à l'interface CLI
    - Contrôle du transport pour les lignes VTY et TTY (option de classe d'accès)
    - Avertissement au moyen de bannières
- AAA
    - Utilisation du cadre AAA pour les options d'authentification et de rechange
    - Utilisation du cadre AAA (TACACS+) pour l'autorisation des commandes
    - Utilisation du cadre AAA pour l'administration
    - Utilisation des serveurs AAA redondants

- SNMP
    - Configuration des communautés SNMPv2 et application des ACL
    - Configuration de SNMPv3
- Journalisation
    - Configuration de la journalisation centralisée
    - Réglage des niveaux de journalisation pour les composants pertinents
    - Réglage de l'interface source de la journalisation
    - Configuration de la granularité de l'horodatage de journalisation
- Gestion de la configuration
    - Remplacer et restaurer
    - Exclusive Configuration Change Access
    - Configuration de la résilience logicielle
    - Configuration des notifications de changement

## Plan de contrôle

- Désactiver (tenir compte des risques)
    - Redirections ICMP
    - Messages ICMP inaccessibles
    - ARP Proxy
- Configurez l'authentification NTP si le protocole NTP est utilisé.
- Configurez la protection ou les règles du plan de contrôle (filtre des ports, seuils de la file d'attente)
- Protocoles de routage sécurisés
    - BGP (TTL, MD5, nombre maximal de préfixes, listes de préfixes, ACL du chemin du système)
    - IGP (MD5, interface passive, filtre de routage, consommation des ressources)
- Configurez les limiteurs de débit matériels
- Protocoles de redondance de premier saut sécurisés (GLBP, HSRP, VRRP)

## Plan de données

- Configurez la suppression sélective des options IP

- Désactiver (tenir compte des risques)
    - Routage source IP
    - Diffusions IP dirigées
    - Redirections ICMP
- Limitez les diffusions dirigées IP
- Configurez les tACL (tenir compte des risques)
    - Filtrez le protocole ICMP
    - Filtrer les fragments IP
    - Filtrez les options IP
    - Filtrez les valeurs TTL
- Configurez les protections anti-usurpation requises
    - ACL
    - Protection de la source IP
    - Inspection dynamique d'ARP
    - Unicast RPF
    - Sécurité du port
- Protection du plan de contrôle (plan de contrôle; exception CEF)
- Configurez NetFlow et les ACL de classification pour l’identification du trafic
- Configurez les ACL requises (mappage du VLAN, PACL, MAC)
- Configurez les VLAN privés

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.