Renforcer les périphériques IOS

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Fond
- Opérations sécurisées
  - Surveiller les avis et les réponses de sécurité Cisco
  - Exploitation de l'authentification, de l'autorisation et de la comptabilité
  - Centraliser la collecte des journaux et surveiller le processus
  - Utiliser Des Protocoles Sécurisés Lorsque C'Est Possible
  - Visibilité accrue du trafic avec NetFlow
  - Gestion de la configuration
- Plan de gestion
  - Durcissement Du Plan Général De Gestion
  - Gestion des mots de passe
    - Sécurité de mot de passe améliorée
    - Login Password Retry Lockout
    - Pas de récupération de mot de passe de service
    - Désactivation des services inutilisés
    - Délai EXEC
    - Keepalive pour les sessions TCP
    - Utilisation de l'interface de gestion
    - Notifications de seuil de mémoire
    - Notification de seuil de CPU
    - Réservation de la mémoire pour l'accès à la console
    - Détecteur de fuite de mémoire
    - Buffer Overflow : Détection et correction de la corruption Redzone
    - Collecte de fichiers Crashinfo améliorée
    - Protocole NTP
    - Désactiver Smart Install
    - Clients qui utilisent la fonctionnalité SMI uniquement pour un déploiement sans intervention
    - Clients qui exploitent la fonctionnalité SMI pour un déploiement plus qu'automatique
  - Limiter l'accès au réseau assorti de listes de contrôle d'accès (ACL) d'infrastructure
    - Filtrage des paquets ICMP
    - Filtrer les fragments IP
    - Prise en charge ACL pour filtrer les options IP
    - Soutien ACL pour filtrer la valeur TTL
  - Sessions de gestion interactive sécurisée
    - Protection du plan de gestion
    - Protection du plan de contrôle
    - Chiffrer les sessions de gestion
    - SSHv2
    - Amélioration de SSHv2 pour les clés RSA

- Ports de console et AUX
- Contrôler les lignes vty et tty
- Contrôle du transport pour les lignes vty et tty
- Bannières d'avertissement

- Authentification, autorisation et administration (AAA)
  - Authentification TACACS+
  - Authentification de secours
  - Utilisation de mots de passe de type 7
  - Autorisation de commande TACACS+
  - Comptabilité des commandes TACACS+
  - Serveurs AAA redondants

- Renforcer le protocole SNMP (Simple Network Management Protocol)
  - Chaînes de communauté SNMP
  - Chaînes de communauté SNMP avec ACL
  - ACL d'infrastructure
  - Vues SNMP
  - SNMP version 3
  - Protection du plan de gestion

- Meilleures pratiques de journalisation
  - Envoyer les journaux à un emplacement central
  - Niveau de journalisation
  - Ne pas consigner dans la console ou les sessions de surveillance
  - Utiliser les journaux mis en mémoire tampon
  - Configurer l'interface source de journalisation
  - Configurer les horodatages des journaux

- Gestion de la configuration du logiciel Cisco IOS
  - Remplacement et restauration de la configuration
  - Accès exclusif aux modifications de configuration
  - Configuration résiliente du logiciel Cisco IOS
  - Logiciel Cisco à signature numérique
  - Notification et consignation des modifications de configuration

Plan de contrôle

- Durcissement Général Du Plan De Contrôle
  - Redirections ICMP IP
  - Messages ICMP inaccessibles
  - Proxy ARP

- Limiter l'incidence du trafic du plan de contrôle sur le CPU
  - Comprendre le trafic du plan de contrôle
  - ACL d'infrastructure
  - Recevoir des ACL
  - CoPP
  - Protection du plan de contrôle
  - Limiteurs de débit matériel

- BGP sécurisé
  - Protections de sécurité basées sur TTL
  - Authentification d'homologue BGP avec MD5
  - Configurer le nombre maximal de préfixes
  - Filtrer les préfixes BGP avec les listes de préfixes
  - Filtrer les préfixes BGP avec les listes d'accès au chemin du système autonome

- Protocoles sécurisés de passerelle intérieure
  - Authentification et vérification du protocole de routage avec Message Digest 5
  - Commandes Passive-Interface

- Filtrage de route
- Consommation des ressources du processus de routage
- Protocoles sécurisés de redondance de premier saut

Plan de données

- Durcissement général du plan de données
  - Options IP Abandon sélectif
  - Désactiver le routage de source IP
  - Désactiver les redirections ICMP
  - Désactiver ou limiter les diffusions dirigées IP
- Filtrer le trafic de transit avec les ACL de transit
  - Filtrage des paquets ICMP
  - Filtrer les fragments IP
  - Prise en charge ACL pour filtrer les options IP
- Protections Anti-Usurpation
  - Unicast RPF
  - Protection de la source IP
  - Sécurité du port
  - Inspection ARP dynamique
  - Listes de contrôle d'accès antimystification
- Limiter l'incidence du trafic du plan de données sur le CPU
  - Fonctionnalités et types de trafic ayant un impact sur le processeur
  - Filtrer selon la valeur TTL
  - Filtrer selon la présence des options IP
  - Protection du plan de contrôle
- Identification et retraçage du trafic
  - NetFlow
  - ACL de classification
- Contrôle d'accès avec mappages VLAN et listes de contrôle d'accès aux ports
  - Contrôle d'accès avec VLAN Maps
  - Contrôle d'accès avec PACL
  - Contrôle d'accès avec MAC
- Utilisation d'un VLAN privé
  - VLAN isolés
  - VLAN de communauté
  - Ports de proximité

Conclusion

Remerciements

Annexe : Liste de contrôle du renforcement des périphériques Cisco IOS

- Plan de gestion
- Plan de contrôle
- Plan de données

Introduction

Ce document décrit comment sécuriser vos périphériques système Cisco IOS® et améliorer la sécurité globale de votre réseau.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Fond

Lorsque vous sécurisez vos périphériques système Cisco IOS, la sécurité globale de votre réseau augmente.

La sécurité globale de votre réseau est structurée autour des trois plans dans lesquels les fonctions d’un périphérique réseau peuvent être classées. Les trois plans fonctionnels d’un réseau sont les suivants : du plan de gestion, du plan de contrôle et du plan de données, chaque plan fournit des fonctionnalités différentes qui doivent être protégées. Ce document fournit une vue d'ensemble de chaque fonctionnalité incluse et des références à la documentation associée.

- Plan de gestion - Le plan de gestion gère le trafic envoyé au périphérique Cisco IOS et est composé d'applications et de protocoles, tels que Secure Shell (SSH) et Simple Network Management Protocol (SNMP).
- 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 est constitué d'applications et de protocoles entre des périphériques réseau, tels que le protocole BGP (Border Gateway Protocol), ainsi que les protocoles IGP (Interior Gateway Protocol). Le protocole EIGRP (Enhanced Interior Gateway Routing Protocol) et le protocole OSPF (Open Shortest Path First) sont également inclus.
- Plan de données : Le plan de données achemine les données par un périphérique réseau. Le plan de données n'inclut pas le trafic envoyé au périphérique Cisco IOS local.

Les fonctions de sécurité traitées dans ce document fournissent souvent suffisamment de détails

pour que vous puissiez configurer la fonction décrite. Cependant, lorsque les détails ne sont pas disponibles, la fonction est expliquée de manière à ce que vous puissiez évaluer si une attention supplémentaire à la fonction est requise. Lorsque cela est possible et approprié, ce document contient des recommandations qui, si elles sont mises en oeuvre, aident à sécuriser un réseau.

Opérations sécurisées

La sécurité des opérations réseau est un sujet important. Bien que la majeure partie de ce document soit consacrée à la configuration sécurisée d'un périphérique Cisco IOS, les configurations seules ne sécurisent pas complètement un réseau. Les procédures opérationnelles utilisées sur le réseau contribuent autant à la sécurité qu'à la configuration des périphériques sous-jacents.

Ces rubriques contiennent des recommandations opérationnelles qu'il est conseillé de mettre en oeuvre. Ces rubriques mettent en évidence des domaines critiques spécifiques du fonctionnement du réseau et ne sont pas complètes.

Surveiller les avis et les réponses de sécurité Cisco

L'équipe PSIRT (Product Security Incident Response Team) de Cisco crée et gère des publications, communément appelées avis PSIRT, pour les problèmes de sécurité liés aux produits Cisco. La méthode utilisée pour la communication des problèmes moins graves est la réponse de sécurité Cisco. Les avis et réponses de sécurité sont disponibles sur Cisco Security Advisories.

Des informations supplémentaires sur ces véhicules de communication sont disponibles dans la Politique de vulnérabilité de sécurité de Cisco.

Pour assurer la sécurité d'un réseau, tenez compte des avis et des réponses de sécurité de Cisco qui ont été publiés. Vous devez avoir connaissance d'une vulnérabilité avant de pouvoir évaluer la menace qu'elle peut représenter pour un réseau. Reportez-vous au Triage de risque pour les annonces de vulnérabilité de sécurité pour obtenir de l’aide dans ce processus d’évaluation.

Exploitation de l'authentification, de l'autorisation et de la comptabilité

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 consigner toutes les commandes entrées par tous les utilisateurs. Consultez la section Authentification, autorisation et administration du présent document pour savoir comment tirer

parti du modèle AAA.

Centraliser la collecte des journaux et surveiller le processus

Pour acquérir des connaissances sur les événements actuels, émergents et historiques liés aux incidents de sécurité, votre entreprise doit disposer d'une stratégie unifiée pour les journaux d'événements et la corrélation. Cette stratégie unifiée doit exploiter les journaux de tous les périphériques réseau et utiliser des fonctionnalités de corrélation prépackagées et personnalisables.

Une fois les journaux centralisés mis en oeuvre, vous devez développer une approche structurée pour l'analyse des journaux et le suivi des incidents. En fonction des besoins de votre entreprise, cette approche peut aller d'une simple analyse diligente des données de journal à une analyse avancée basée sur des règles.

Consultez la section Meilleures pratiques de journalisation de ce document pour plus d'informations sur la façon d'implémenter des journaux sur des périphériques réseau Cisco IOS.

Utiliser Des Protocoles Sécurisés Lorsque C'Est Possible

Plusieurs protocoles sont utilisés pour transporter des données de gestion réseau sensibles. Utilisez des protocoles sécurisés chaque fois que 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 sont chiffrées. En outre, utilisez des protocoles de transfert de fichiers sécurisés lorsque vous copiez des données de configuration. L'utilisation du protocole de copie sécurisée (SCP) à la place du protocole FTP ou TFTP en est un exemple.

Consultez la section Sessions de gestion interactive sécurisée du présent document pour en savoir plus sur la gestion sécurisée des périphériques Cisco IOS.

Visibilité accrue du trafic avec NetFlow

NetFlow vous permet de surveiller les flux de trafic sur le réseau. Initialement conçu pour exporter des informations de trafic vers des applications de gestion de réseau, NetFlow peut également être utilisé pour afficher des informations de flux sur un routeur. Cette fonctionnalité vous permet de voir en temps réel le trafic qui traverse le réseau. Que les informations de flux soient exportées ou non vers un collecteur distant, il est conseillé de configurer les périphériques réseau pour NetFlow afin qu'il puisse être utilisé de manière réactive si nécessaire.

Pour plus d'informations sur cette fonctionnalité, consultez la section Identification et retraçage du

trafic de ce document et Cisco IOS NetFlow.

Remarque : Seuls les utilisateurs Cisco inscrits ont accès aux informations et aux outils internes.

Gestion de la configuration

La gestion de la configuration est un processus par lequel les modifications de configuration sont proposées, examinées, 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 : archivage et sécurité de la configuration.

Utilisez les archives de configuration pour annuler les modifications apportées aux périphériques réseau. Dans un contexte de sécurité, les archives de configuration peuvent également être utilisées pour déterminer quelles modifications de sécurité ont été apportées et à quel moment ces modifications se sont produites. Associées aux données du journal AAA, ces informations peuvent faciliter l'audit de sécurité des périphériques réseau.

La configuration d'un périphérique Cisco IOS contient de nombreux détails sensibles. Les noms d'utilisateur, les mots de passe et le contenu des listes de contrôle d'accès sont des exemples de ces informations sensibles. Le référentiel utilisé pour archiver les configurations des périphériques Cisco IOS doit être sécurisé. Un accès non sécurisé à ces informations peut compromettre la sécurité de l'ensemble du réseau.

Plan de gestion

Le plan de gestion est constitué de fonctions qui permettent d'atteindre les objectifs 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. Lorsque vous considérez la sécurité d'un périphérique réseau, il est essentiel que le plan de gestion soit protégé. Si un incident de sécurité est susceptible d'affecter les fonctions du plan de gestion, il peut s'avérer impossible de restaurer ou de stabiliser le réseau.

Les sections suivantes de ce document détaillent les fonctions de sécurité et les configurations disponibles dans la plate-forme logicielle Cisco IOS qui permettent de renforcer le plan de gestion.

Durcissement Du Plan Général De Gestion

Le plan de gestion est utilisé pour accéder à un périphérique, le configurer et le gérer, ainsi que pour surveiller ses opérations et le réseau sur lequel il est déployé. Le plan de gestion reçoit et

envoie du trafic pour les opérations de ces fonctions. Sécurisez le plan de gestion et le plan de contrôle d'un périphérique, car les opérations du plan de contrôle affectent directement les opérations du plan de gestion. Les protocoles utilisés par le plan de gestion sont les suivants :

- Protocole SNMP (Simple Network Management Protocol)
- Telnet
- protocole Secure Shell
- 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 lors des incidents de sécurité. Si l'un de ces plans est exploité avec succès, tous les plans peuvent être compromis.

Gestion des mots de passe

Les mots de passe contrôlent l'accès aux ressources ou aux périphériques. Pour ce faire, il faut utiliser le mot de passe utilisé pour authentifier les demandes. Lorsqu'une demande d'accès à une ressource ou à un périphérique est reçue, la demande est contestée en vue de la vérification du mot de passe et de l'identité, et l'accès peut être accordé, refusé ou limité, en fonction du résultat. Pour des raisons de sécurité, les mots de passe doivent être gérés à l'aide d'un serveur d'authentification TACACS+ ou RADIUS. Cependant, un mot de passe configuré localement pour l'accès privilégié est toujours nécessaire en cas de défaillance des services TACACS+ ou RADIUS. Un périphérique peut également avoir d'autres informations de mot de passe présentes dans sa configuration, telles qu'une clé NTP, une chaîne de communauté SNMP ou une clé de protocole de routage.

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

Si aucun mot de passe n'**enable secret**est défini et qu'un mot de passe est configuré pour la ligne tty

de la console, le mot de passe de la console peut être utilisé pour recevoir un accès privilégié, même à partir d'une session tty virtuelle (vty) distante. Cette action est presque certainement indésirable et est une autre raison d'assurer la configuration d'un secret actif.

La commande de configuration **service password-encryption** globale indique au logiciel Cisco IOS de chiffrer les mots de passe, les secrets CHAP (Challenge Handshake Authentication Protocol) et les données similaires enregistrées dans son fichier de configuration. Ce chiffrement est utile pour empêcher les observateurs occasionnels d'observer les mots de passe, par exemple lorsqu'ils regardent l'écran par-dessus l'épaule d'un administrateur. Cependant, l'algorithme utilisé par la **service password-encryption** commande est un simple chiffrement Vigen re. L'algorithme n'est pas conçu pour protéger les fichiers de configuration contre une analyse sérieuse, même par des pirates un peu plus sophistiqués, et ne doit pas être utilisé à cette fin. Tout fichier de configuration Cisco IOS contenant des mots de passe chiffrés doit être traité avec la même prudence que pour une liste en texte clair de ces mêmes mots de passe.

Bien que cet algorithme de chiffrement faible ne soit pas utilisé par la **enable secret** commande, il est utilisé par la commande de configuration **enable password** globale, ainsi que par la commande de configuration de **password** ligne. Ce type de mots de passe doit être éliminé et la **enable secret** commande ou la fonctionnalité Enhanced Password Security doit être utilisée.

La commande enable secret et la fonction Enhanced Password Security utilisent Message Digest 5 (MD5) pour le hachage de mot de passe. Cet algorithme a fait l'objet d'un examen public considérable et n'est pas réversible. Cependant, l'algorithme est sujet à des attaques par dictionnaire. Lors d'une attaque par dictionnaire, un pirate tente de trouver une correspondance avec chaque mot d'un dictionnaire ou d'une autre liste de mots de passe candidats. Par conséquent, les fichiers de configuration doivent être stockés en toute sécurité et partagés uniquement avec des personnes de confiance.

Sécurité de mot de passe améliorée

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 : Tapez 0, qui est un mot de passe en texte clair, puis 7, qui utilise l'algorithme du chiffre de Vigenère. La fonction Enhanced Password Security ne peut pas être utilisée avec les protocoles qui nécessitent que le mot de passe en texte clair soit récupérable, comme CHAP.

Pour chiffrer un mot de passe utilisateur avec le hachage MD5, exécutez la commande de configuration username secret globale.

!

```
username <name> secret <password>

!
```

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. Lorsqu'un utilisateur est verrouillé, son compte est verrouillé jusqu'à ce que vous le déverrouilliez. Un utilisateur autorisé configuré avec le niveau de privilège 15 ne peut pas être verrouillé avec cette fonctionnalité. Maintenez au minimum le nombre d'utilisateurs disposant d'un niveau de privilège 15.

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

Cet exemple montre comment activer la fonctionnalité de verrouillage de nouvelle tentative de mot de passe de connexion :

```
!

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 CHAP et PAP (Password Authentication Protocol).

Pas de récupération de mot de passe de service

Dans le logiciel Cisco IOS Version 12.3(14)T et ultérieure, la fonctionnalité No Service Password-Recovery ne permet pas à quiconque ayant accès à la console d'accéder de manière non sécurisée à la configuration du périphérique et d'effacer le mot de passe. Il ne permet pas non plus aux utilisateurs malveillants de modifier la valeur du registre de configuration et d'accéder à la

mémoire NVRAM.

```
!
no service password-recovery
!
```

La plate-forme logicielle Cisco IOS fournit une procédure de récupération de mot de passe qui repose sur l'accès au mode moniteur ROM (ROMMON) qui utilise la touche Break au démarrage du système. Dans ROMMON, le logiciel du périphérique peut être rechargé pour demander une nouvelle configuration système incluant un nouveau mot de passe.

La procédure de récupération de mot de passe actuelle permet à toute personne ayant accès à la console d'accéder au périphérique et à 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 d'enregistrer une copie hors connexion de la configuration du périphérique et de mettre en oeuvre une solution d'archivage de la configuration. S'il est nécessaire de récupérer le mot de passe d'un périphérique Cisco IOS une fois cette fonction activée, la configuration entière est supprimée.

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

Désactivation des services inutilisés

Pour des raisons de sécurité, désactivez tout service inutile. Les services inutiles, en particulier ceux qui utilisent le protocole UDP (User Datagram Protocol), sont rarement utilisés à des fins légitimes, mais peuvent être utilisés pour lancer des attaques par déni de service et d'autres attaques qui sont autrement empêchées par le filtrage des paquets.

Désactivez les petits services TCP et UDP. Ces services incluent :

- echo (numéro de port 7)
- discard (numéro de port 9)
- daytime (numéro de port 13)
- chargen (numéro de port 19)

Bien que l'utilisation abusive des petits services puisse être évitée ou rendue moins dangereuse par des listes d'accès anti-mystification, désactivez les services sur tout périphérique accessible au sein du réseau. Par défaut, les petits services sont désactivés dans le logiciel Cisco IOS versions 12.0 et ultérieures. Dans les logiciels antérieurs, **no service tcp-small-servers** les commandes de configuration globale et **no service udp-small-servers** peuvent être exécutées pour les désactiver.

Les services supplémentaires qui doivent être désactivés, s'ils ne sont pas utilisés, incluent :

- Exécutez la commande no ip finger de configuration globale pour désactiver le service Finger. Par défaut, les versions du logiciel Cisco IOS ultérieures à 12.1(5) et 12.1(5)T désactivent ce service.
- no ip bootp serverExécutez la commande de configuration globale pour désactiver le protocole BOOTP (Bootstrap Protocol).
- Dans le logiciel Cisco IOS Version 12.2(8)T et ultérieure, émettez la commande ip dhcp bootp ignore en mode de configuration globale pour désactiver BOOTP. Les services DHCP (Dynamic Host Configuration Protocol) restent donc activés.
- Les services DHCP peuvent être désactivés si les services de relais DHCP ne sont pas requis. Émettez la commande no service dhcp en mode de configuration globale.
- Émettez la commande no mop enabled en mode de configuration d'interface pour désactiver le service MOP (Maintenance Operation Protocol).
- Émettez la commande de configuration globale no ip domain-lookup pour désactiver les services de résolution DNS (Domain Name System).
- Émettez la commande no service pad en mode de configuration globale pour désactiver le service d'assembleur/désassembleur de paquets (PAD), qui est utilisé pour les 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 ne 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 réseau utilisé pour détecter d'autres périphériques compatibles CDP pour la contiguïté de voisinage et la topologie du réseau. Le protocole CDP peut être utilisé par les systèmes de gestion de réseau (NMS) ou pendant l'isolation des problèmes. Le protocole CDP doit être désactivé sur toutes les interfaces connectées à des réseaux non approuvés. Pour ce faire, utilisez la commande no cdp enable interface. Vous pouvez également désactiver le protocole CDP globalement à l'aide de la commande de configuration globale no cdp run. Notez que le protocole CDP peut être utilisé par un utilisateur malveillant à des fins de reconnaissance et pour mapper un réseau.
- Le protocole LLDP (Link Layer Discovery Protocol) est un protocole IEEE défini dans la norme 802.1AB et similaire au protocole CDP. Cependant, ce protocole permet l'interopérabilité entre d'autres périphériques qui ne prennent pas en charge le protocole

CDP. Le protocole LLDP doit être traité de la même manière que le protocole CDP et désactivé sur toutes les interfaces qui se connectent à des réseaux non approuvés. Pour ce faire, émettez les commandes de configuration d'interface no lldp transmit et no lldp receive. Émettez la commande de configuration globale no lldp run pour désactiver LLDP globalement. Le protocole LLDP peut également être utilisé par un utilisateur malveillant à des fins de reconnaissance et pour mapper un réseau.

- Pour les commutateurs qui prennent en charge le démarrage à partir de la mémoire flash, la sécurité peut être améliorée pour démarrer à partir de la mémoire flash et désactiver la mémoire flash avec la commande de configuration « no sdflash ».

Délai EXEC

Pour définir l'intervalle, l'interpréteur de commandes EXEC attend une entrée utilisateur avant de mettre fin à une session, émettez la commande de configuration de ligne exec-timeout. Utilisez la commande exec-timeout pour déconnecter les sessions sur les lignes vty ou tty qui sont laissées 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]
!
```

Keepalive 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. Utilisez cette configuration pour activer les keepalives TCP sur les connexions entrantes au périphérique et les connexions sortantes du périphérique. Cela garantit que le périphérique de l’extrémité distante de la connexion est toujours accessible et que les connexions à moitié ouvertes ou orphelines sont supprimées du périphérique Cisco IOS local.

```
!

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

Utilisation de l’interface de gestion

Le plan de gestion d'un périphérique est accessible en bande ou hors bande sur une interface de gestion physique ou logique. Idéalement, il existe un accès d'administration intrabande et hors bande pour chaque périphérique réseau, de sorte que le plan d'administration est accessible en cas de panne du réseau.

L’une des interfaces les plus couramment utilisées pour l’accès intrabande 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 en tant qu'interface de gestion et de l'utiliser exclusivement pour le plan de gestion. Cela permet à l'administrateur d'appliquer des stratégies sur l'ensemble du réseau pour le plan de gestion. Une fois l'interface de bouclage configurée sur un périphérique, elle peut être utilisée par les protocoles du plan de gestion, tels que SSH, SNMP et syslog, pour envoyer et recevoir du trafic.

```
!
interface Loopback0
 ip address 192.168.1.1 255.255.255.0
!
```

Notifications de seuil de mémoire

La fonctionnalité Memory Threshold Notification, ajoutée dans le logiciel Cisco IOS Version 12.3(4)T, vous permet de limiter les conditions de mémoire insuffisante sur un périphérique. Pour ce faire, cette fonction utilise deux méthodes : Notification de seuil de mémoire et réservation de mémoire.

La notification de seuil de mémoire génère un message de journal pour indiquer que la mémoire libre sur un périphérique est tombée en dessous du seuil configuré. Cet exemple de configuration montre comment activer cette fonctionnalité avec la commande de configuration globale memory free low-watermark. Cela permet à un périphérique de générer une notification lorsque la mémoire libre disponible tombe en dessous du seuil spécifié, et à nouveau lorsque la mémoire libre disponible monte à cinq pour cent au-dessus du seuil spécifié.

```
!

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

La réservation de mémoire est utilisée de sorte que suffisamment de mémoire est disponible pour les notifications critiques. Cet exemple de configuration montre comment activer cette fonctionnalité pour garantir que les processus de gestion continuent à fonctionner lorsque la mémoire du périphérique est épuisée.

```
!

memory reserve critical <value>
!
```

Référez-vous à Notifications de seuil de mémoire pour plus d'informations sur cette fonctionnalité.

Notification de seuil de CPU

Introduite dans le logiciel Cisco IOS Version 12.3(4)T, la fonctionnalité de notification de seuil de CPU vous permet de détecter et de recevoir une notification lorsque la charge de CPU sur un périphérique dépasse un seuil configuré. Lorsque le seuil est dépassé, le périphérique génère et envoie un message de déroutement SNMP. Le logiciel Cisco IOS prend en charge deux méthodes de seuil d'utilisation du processeur : Seuil montant et seuil descendant.

Cet exemple de configuration montre comment activer les seuils montant et descendant pour déclencher un message de notification de seuil de 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 Notification de seuil de CPU pour plus d'informations sur cette fonctionnalité.

Réservation de la mémoire pour l’accès à la console

Dans le logiciel Cisco IOS Version 12.4(15)T et ultérieure, la fonction Reserve Memory for

Console Access peut être utilisée pour réserver suffisamment de mémoire pour garantir l'accès de la console à un périphérique Cisco IOS à des fins d'administration et d'isolation des problèmes. Cette fonctionnalité est particulièrement utile lorsque le périphérique manque de mémoire. Vous pouvez émettre la commande de configuration globale memory reserve console pour activer cette fonctionnalité. Cet exemple configure un périphérique Cisco IOS pour réserver 4 096 kilo-octets à cet effet.

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

Détecteur de fuite de mémoire

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. Le détecteur de fuites de mémoire peut détecter les fuites dans tous les pools de mémoire, les tampons de paquets et les segments. Les fuites de mémoire sont des allocations de mémoire statiques ou dynamiques qui ne remplissent aucune fonction utile. Cette fonction se concentre sur les allocations de mémoire dynamiques. Vous pouvez utiliser la commande EXEC show memory debug leaks pour 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, le Buffer Overflow : La détection et la correction de la fonction Redzone Corruption peut être activée sur un périphérique pour détecter et corriger un débordement de bloc de mémoire et pour poursuivre les opérations.

Les commandes de configuration globale peuvent être utilisées pour activer cette fonctionnalité. Une fois configurée, la commande show memory overflow peut être utilisée pour afficher les statistiques de détection et de correction de débordement de mémoire tampon.

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

Collecte de fichiers Crashinfo améliorée

La fonction de collecte améliorée des fichiers Crashinfo supprime automatiquement les anciens

fichiers Crashinfo. Cette fonctionnalité, ajoutée dans le logiciel Cisco IOS Version 12.3(11)T, permet à un périphérique de récupérer de l'espace pour créer de nouveaux fichiers crashinfo lorsque le périphérique tombe en panne. Cette fonctionnalité permet également de configurer le nombre de fichiers crashinfo à enregistrer.

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

Protocole NTP

Le protocole NTP (Network Time Protocol) n'est pas un service dangereux, mais tout service inutile peut représenter un vecteur d'attaque. Si le protocole NTP est utilisé, il est important de configurer explicitement une source temporelle approuvée et d'utiliser une authentification appropriée. Un temps précis et fiable est nécessaire à des fins syslog, par exemple lors d'enquêtes d'investigation d'attaques potentielles, ainsi que pour une connectivité VPN réussie lorsqu'elle dépend de certificats pour l'authentification de Phase 1.

- Fuseau horaire NTP - Lorsque vous configurez NTP, le fuseau horaire doit être configuré afin que les horodatages puissent être corrélés avec précision. Il existe deux méthodes classiques pour configurer le fuseau horaire des périphériques d'un réseau avec une présence globale. Une méthode consiste à configurer tous les périphériques réseau avec le temps universel coordonné (UTC) (anciennement GMT (Greenwich Mean Time)). L'autre méthode consiste à configurer les périphériques réseau avec le fuseau horaire local. Pour plus d'informations sur cette fonctionnalité, reportez-vous à la section « clock timezone » de la documentation 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.

Voici un exemple de configuration qui utilise 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 meilleures pratiques de sécurité relatives à la fonctionnalité Cisco Smart Install (SMI) dépendent de la manière dont cette fonctionnalité est utilisée dans un environnement utilisateur spécifique. Cisco fait une distinction pour ces cas d'utilisation :

- Utilisateurs qui n'utilisent pas la fonctionnalité SMI.
- Utilisateurs qui utilisent la fonctionnalité SMI uniquement pour un déploiement sans intervention.
- Utilisateurs qui exploitent la fonction Smart InstallSMI pour un déploiement plus simple (configuration et gestion des images).

Ces sections décrivent en détail chaque scénario :

- Utilisateurs qui n'utilisent pas la fonctionnalité SMI.
- Les utilisateurs qui n'utilisent pas la fonctionnalité SMI et qui exécutent une version de Cisco IOS et du logiciel Cisco IOS XE lorsque la commande est disponible, peuvent désactiver la fonctionnalité SMI avec la commande no vstack.

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

Voici un exemple de sortie de la commande show vstack sur un commutateur Cisco Catalyst avec la fonctionnalité de client SMI désactivée :

<#root>

```
switch#

show vstack


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

Clients qui utilisent la fonctionnalité SMI uniquement pour un déploiement sans intervention

Désactivez la fonctionnalité du client SMI une fois l'installation automatique terminée ou utilisez la commande no vstack.

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

- Entrez la commande no vstack sur tous les commutateurs clients, soit manuellement, soit avec un script.
- Ajoutez la commande no vstack dans la configuration Cisco IOS qui est poussée dans chaque client SMI dans le cadre de l'installation sans intervention.
- Dans les versions qui ne prennent pas en charge la commande vstack (Cisco IOS version 12.2(55)SE02 et versions antérieures), appliquez une liste de contrôle d'accès (ACL) sur les commutateurs clients pour bloquer le trafic sur le port TCP 4786.

Pour activer la fonctionnalité client SMI ultérieurement, entrez la commande vstack sur tous les commutateurs clients, manuellement ou avec un script.

Clients qui exploitent la fonctionnalité SMI pour un déploiement plus qu'automatique

Lors de la conception d'une architecture SMI, veillez à ce que l'espace d'adressage IP de l'infrastructure ne soit pas accessible aux parties non approuvées. Dans les versions qui ne prennent pas en charge la commande vstack, assurez-vous que seul le directeur SMI a une connectivité TCP à tous les clients SMI sur le port 4786.

Les administrateurs peuvent utiliser les meilleures pratiques de sécurité suivantes pour les déploiements SMI sur les périphériques concernés :

- 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 montre une liste de contrôle d'accès d'interface avec l'adresse IP du directeur SMI 10.10.10.1 et l'adresse IP du client SMI 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. Il peut également être envoyé par le directeur lors du premier déploiement des commutateurs.

Pour restreindre davantage l'accès à tous les clients de l'infrastructure, les administrateurs peuvent utiliser les meilleures pratiques de sécurité suivantes 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

Conçues pour empêcher les communications directes non autorisées vers les périphériques réseau, les listes de contrôle d'accès IP sont l'un des contrôles de sécurité les plus critiques mis en oeuvre sur les réseaux. Une liste de contrôle d’accès IP repose sur l’idée que presque tout le trafic réseau traverse le réseau et n’est pas destiné au réseau lui-même.

Une liste de contrôle d’accès IP est créée et appliquée pour spécifier les connexions des hôtes ou des réseaux qui doivent être autorisés à accéder aux périphériques réseau. Les exemples courants de ces types de connexion sont eBGP, SSH et SNMP. Une fois que les connexions

requises ont été autorisées, tout autre trafic vers l'infrastructure est explicitement refusé. Tout trafic de transit qui traverse le réseau et n'est pas destiné aux périphériques d'infrastructure est alors explicitement autorisé.

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

Cet exemple de configuration iACL illustre la structure qui doit être utilisée comme point de départ lorsque vous commencez le processus d'implémentation 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 créée, la liste de contrôle d'accès IP doit être appliquée à toutes les interfaces qui font face à des périphériques hors infrastructure. Cela inclut les interfaces qui se connectent à d'autres organisations, les segments d'accès à distance, les segments utilisateur et les segments dans les centres de données.

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

Filtrage des paquets ICMP

Le protocole ICMP (Internet Control Message Protocol) est conçu comme un protocole de contrôle IP. En tant que tels, les messages qu'il transmet peuvent avoir une interaction significative avec les protocoles TCP et IP en général. Alors que les outils réseau, ping et traceroute, pour dépanner l'utilisation d'ICMP, la connectivité ICMP externe est rarement nécessaire pour le bon fonctionnement du réseau.

La plate-forme logicielle Cisco IOS permet de filtrer spécifiquement les messages ICMP par nom, type et code. Cet exemple de liste de contrôle d'accès, qui doit être utilisé avec les entrées de contrôle d'accès (ACE) des exemples précédents, autorise les requêtes ping à partir des stations de gestion approuvées et des serveurs NMS 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 filtrage des paquets IP fragmentés peut représenter un défi pour les périphériques de sécurité. En effet, les informations de couche 4 utilisées pour filtrer les paquets TCP et UDP ne sont présentes que dans le fragment initial. La plate-forme logicielle Cisco IOS utilise une méthode spécifique pour vérifier les fragments non initiaux par rapport aux listes d’accès configurées. La plate-forme logicielle Cisco IOS évalue ces fragments non initiaux par rapport à la liste de contrôle d’accès et ignore les informations filtrées de couche 4. Cela entraîne l'évaluation des fragments non initiaux uniquement sur la partie de couche 3 d'une ACE configurée.

Dans cet exemple de configuration, si un paquet TCP destiné à 192.168.1.1 sur le port 22 est fragmenté en transit, le fragment initial est abandonné comme prévu par la seconde ACE, en fonction des informations de couche 4 dans le paquet. Cependant, tous les fragments (non initiaux) qui restent sont autorisés par le premier ACE, basé entièrement sur les informations de couche 3 dans le paquet et l'ACE. Ce scénario est illustré 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 de la gestion des fragments, les fragments IP sont souvent autorisés par inadvertance par les listes de contrôle d’accès. La fragmentation est souvent utilisée dans les tentatives de contournement de la détection par les systèmes de détection des intrusions. Pour ces raisons, les fragments IP sont souvent utilisés dans les attaques, et pourquoi ils doivent être explicitement filtrés en haut de toutes les iACL configurées. Cet exemple de liste de contrôle d’accès inclut une filtration complète des fragments IP. La fonctionnalité de cet exemple doit être utilisée avec 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.

Prise en charge ACL pour filtrer les options IP

La version 12.3(4)T du logiciel Cisco IOS a ajouté la prise en charge de l'utilisation des listes de contrôle d'accès pour filtrer les paquets IP, en fonction des options IP contenues dans le paquet. Les options IP représentent un défi de sécurité pour les périphériques réseau, car elles doivent être traitées comme des paquets d'exception. Cela nécessite un niveau d'effort processeur qui n'est pas requis pour les paquets typiques qui traversent le réseau. La présence d'options IP dans un paquet peut également indiquer une tentative de subversion des contrôles de sécurité sur le réseau ou de modification des caractéristiques de transit d'un paquet. Pour ces raisons, les paquets avec des options IP doivent être filtrés à la périphérie du réseau.

Cet exemple doit être utilisé avec les ACE des exemples précédents pour 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

La version 12.4(2)T du logiciel Cisco IOS a ajouté un filtre de prise en charge des listes de contrôle d'accès pour les paquets IP, basé sur la valeur TTL (Time to Live). La valeur de durée de vie d'un datagramme IP est décrémentée par chaque périphérique réseau lorsqu'un paquet circule de la source à la destination. Bien que les valeurs initiales varient selon le système d'exploitation, lorsque la durée de vie d'un paquet atteint zéro, le paquet doit être abandonné. Le périphérique qui décrémente la durée de vie à zéro, et abandonne donc le paquet, est requis pour générer et envoyer un message ICMP Time Exceeded (Délai dépassé) à la source du paquet.

La génération et la transmission de ces messages constituent un processus d'exception. Les

routeurs peuvent exécuter cette fonction lorsque le nombre de paquets IP devant expirer est faible, mais si le nombre de paquets devant expirer est élevé, la génération et la transmission de ces messages peuvent consommer toutes les ressources CPU disponibles. Ceci présente un vecteur d'attaque DoS. Pour cette raison, les périphériques doivent être renforcés contre les attaques DoS qui utilisent un taux élevé de paquets IP, qui sont sur le point d'expirer.

Il est recommandé aux entreprises de filtrer les paquets IP avec des valeurs TTL faibles à la périphérie du réseau. La filtration complète des paquets avec des valeurs TTL insuffisantes pour traverser le réseau atténue la menace d'attaques basées sur TTL.

Cet exemple de liste de contrôle d'accès filtre les paquets avec des valeurs TTL inférieures à six. Cela offre une protection contre les attaques d'expiration de durée de vie pour les 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 légitimement appel à des paquets ayant une faible valeur TTL. eBGP est l'un de ces protocoles. Référez-vous à Identification et réduction des attaques TTL Expiry pour plus d'informations pour atténuer les attaques basées sur l'expiration TTL.

Sessions de gestion interactive sécurisée

Les sessions de gestion des périphériques permettent d'afficher et de collecter des informations sur un périphérique et son fonctionnement. Si ces informations sont divulguées à un utilisateur malveillant, le périphérique peut devenir la cible d'une attaque, être compromis et utilisé pour effectuer des attaques supplémentaires. Toute personne disposant d'un accès privilégié à un

périphérique peut contrôler entièrement l'administration de ce périphérique. Il est impératif de sécuriser les sessions de gestion pour empêcher la divulgation d'informations et les accès non autorisés.

Protection du plan de gestion

Dans le logiciel Cisco IOS Version 12.4(6)T et ultérieure, la fonctionnalité Management Plane Protection (MPP) permet à un administrateur d'imposer des restrictions sur le trafic de gestion des différentes interfaces qui est reçu par un périphérique. Cela permet à l'administrateur de contrôler davantage un périphérique et la manière dont il y accède.

Cet exemple montre comment activer le MPP pour autoriser uniquement 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 MPP.

Remarque : MPP ne prend pas en charge IPv6 et est limité au chemin d'entrée IPv4. IPv6 n'étant pas filtré, utilisez CoPP dans les environnements mixtes IPv4/IPv6.

Protection du plan de contrôle

La protection du plan de contrôle (PPCr) s'appuie sur la fonctionnalité de réglementation du plan de contrôle pour restreindre et contrôler le trafic du plan de contrôle qui est destiné au processeur de routage du périphérique Cisco IOS. Ajouté dans le logiciel Cisco IOS Version 12.4(4)T, CPPr divise le plan de contrôle en catégories distinctes, appelées sous-interfaces. Il existe trois sous-interfaces de plan de contrôle : Host, Transit et CEF-Exception. En outre, CPPr inclut les fonctions de protection du plan de contrôle suivantes :

- Fonction de filtrage des ports - Permet à l'administrateur de contrôler ou d'abandonner les paquets qui vont vers les ports TCP et UDP fermés ou sans écoute.
- Queue-threshold policy feature - Limite le nombre de paquets pour un protocole spécifié autorisés dans la file d'attente d'entrée IP du plan de contrôle.

CPPr permet à un administrateur de classer, contrôler et restreindre le trafic envoyé à un périphérique à des fins de gestion avec la sous-interface hôte. Le trafic de gestion, tel que SSH ou Telnet, et les protocoles de routage sont des exemples de paquets classés pour la catégorie de sous-interface hôte.

Remarque : CPPr ne prend pas en charge le protocole IPv6 et est limité au chemin d'entrée IPv4.

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

Chiffrer les sessions de gestion

Étant donné que les informations peuvent être divulguées dans une session de gestion interactive, ce trafic doit être chiffré afin 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 le trafic d'une session de gestion est envoyé sur le réseau en texte clair, un pirate peut obtenir des informations sensibles sur le périphérique et le 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 pas sécurisé et n'est pas normalisé. Il n'est donc pas recommandé de l'utiliser si SSHv2 est une option.

La plate-forme logicielle Cisco IOS prend également en charge le protocole Secure Copy Protocol (SCP), qui permet une connexion chiffrée et sécurisée pour copier des configurations de périphériques ou des images logicielles. La SCP repose 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
!
```

Cet exemple de configuration concerne les services HTTPS :

```
!

crypto key generate rsa modulus 2048
!

ip http secure-server
!
```

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

SSHv2

La fonctionnalité de prise en charge de SSHv2, introduite dans le logiciel Cisco IOS Version 12.3(4)T, permet à un utilisateur de configurer SSHv2. (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. Le seul transport fiable défini pour SSH est TCP. SSH permet d'accéder et d'exécuter en toute sécurité des commandes sur un autre ordinateur ou périphérique sur un réseau. La fonction Secure Copy Protocol (SCP) tunnellisée sur SSH permet le transfert sécurisé des fichiers.

Si la commande ip ssh version 2 n'est pas explicitement configurée, Cisco IOS active SSH version 1.99. SSH version 1.99 autorise les connexions SSHv1 et SSHv2. SSHv1 est considéré comme non sécurisé et peut avoir des effets indésirables sur le système. Si SSH est activé, il est 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 privée/publique sur le client et configurer une clé publique sur le serveur SSH Cisco IOS pour terminer l'authentification.

Un utilisateur SSH qui tente d'établir les informations d'authentification fournit une signature

chiffrée avec la clé privée. La signature chiffrée et la clé publique de l'utilisateur sont envoyées au serveur SSH pour authentification. Le serveur SSH calcule un hachage à l'aide de la clé publique fournie par l'utilisateur. Le hachage est utilisé pour déterminer si le serveur dispose d'une entrée correspondante. 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'indicateur de vérification stricte de la clé hôte est activé sur le client, ce dernier vérifie si l'entrée de clé hôte correspondant 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, alors la session se poursuit; sinon, elle sera interrompue et un message s'affichera, indiquant que l'authentification du serveur a échoué.

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.]

Ports de console et AUX

Dans les périphériques Cisco IOS, les ports de console et auxiliaires (AUX) sont des lignes asynchrones qui peuvent être utilisées pour l'accès local et distant à un périphérique. N'oubliez pas que les ports de console des périphériques Cisco IOS disposent de privilèges spéciaux. En particulier, ces privilèges permettent à un administrateur d'effectuer la procédure de récupération de mot de passe. Pour récupérer un mot de passe, un pirate non authentifié doit avoir accès au port de console et avoir la possibilité d'interrompre l'alimentation du périphérique ou de provoquer sa panne.

Toute méthode utilisée pour accéder au port de console d'un périphérique doit être sécurisée de manière égale à la sécurité appliquée pour l'accès privilégié à un périphérique. Les méthodes utilisées pour sécuriser l'accès doivent inclure l'utilisation des mots de passe AAA, exec-timeout et modem (si un modem est connecté à la console).

Si la récupération de mot de passe n'est pas requise, alors un administrateur peut supprimer la possibilité d'effectuer la procédure de récupération de mot de passe par la commande de configuration globale no service password-recovery ; toutefois, une fois que la commande no service password-recovery a été activée, un administrateur ne peut pas effectuer la récupération de mot de passe sur un périphérique.

Dans la plupart des cas, le port AUX du périphérique doit être désactivé pour 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
!
```

Contrôler les lignes vty et tty

Les sessions de gestion interactives dans le logiciel Cisco IOS utilisent un téléscripteur ou un téléscripteur virtuel (vty). Un téléscripteur est une ligne asynchrone locale à laquelle un terminal peut être connecté pour un accès local au périphérique ou à un modem pour un accès commuté à un périphérique. Notez que les jouets peuvent être utilisés pour les connexions aux ports de console d'autres périphériques. Cette fonction permet à un périphérique doté de lignes tty d'agir comme serveur de console, où des connexions peuvent être établies sur le réseau vers les ports de console des périphériques connectés aux lignes tty. Les lignes tty pour ces connexions inverses sur le réseau doivent également être contrôlées.

Une ligne vty est utilisée pour toutes les autres connexions réseau distantes prises en charge par le périphérique, quel que soit le protocole (SSH, SCP ou Telnet sont des exemples). Pour garantir qu'une session de gestion locale ou distante puisse accéder à un périphérique, des contrôles appropriés doivent être appliqués à la fois sur les lignes vty et tty. Les périphériques Cisco IOS ont un nombre limité de lignes vty ; le nombre de lignes utilisables peut être déterminé grâce à la commande « show line EXEC ». Lorsque toutes les lignes vty sont utilisées, il est impossible d'établir de nouvelles sessions de gestion, ce qui peut créer une condition de déni de service pour l'accès au périphérique.

Le contrôle d'accès le plus simple à un terminal virtuel ou téléscripteur d'un périphérique est l'utilisation de l'authentification sur toutes les lignes, quel que soit l'emplacement du périphérique sur le réseau. Ceci est essentiel pour les lignes vty car elles sont accessibles par le réseau. Une ligne tty connectée à un modem utilisé pour l'accès à distance au périphérique, ou une ligne tty connectée au port de console d'autres périphériques 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 pour déconnecter des sessions sur des lignes vty ou tty qui sont laissées inactives. La commande service tcp-keepalives-in doit également être utilisée pour activer TCP keepalives sur les connexions entrantes au périphérique. Cela garantit que le périphérique de l'extrémité distante de la connexion est toujours accessible et que les connexions à moitié ouvertes ou orphelines sont supprimées du périphérique Cisco IOS local.

Contrôle du transport pour les lignes vty et tty

Configurez un vty et un tty pour n'accepter que les connexions chiffrées et sécurisées de gestion d'accès à distance au périphérique ou via le périphérique s'il est utilisé comme serveur de console. Cette section traite des téléscripteurs, car ces lignes peuvent être connectées à des ports de console sur d'autres périphériques, ce qui permet au téléscripteur d'être accessible sur le réseau. Pour empêcher la divulgation d'informations ou l'accès non autorisé aux données transmises entre l'administrateur et le périphérique, utilisez transport input ssh au lieu de protocoles en texte clair, tels que Telnet et rlogin. La configuration transport input none peut être activée sur un téléscripteur, ce qui désactive l'utilisation de la ligne du téléscripteur pour les connexions de console inverse.

Les lignes vty et tty permettent à un administrateur de se connecter à d'autres périphériques. Pour 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 utilisez transport output none. Cependant, si les connexions sortantes sont autorisées, alors appliquez une méthode d'accès à distance chiffrée et sécurisée pour la connexion par l'utilisation de transport output ssh.

Remarque : IPSec peut être utilisé pour les connexions d'accès à distance chiffrées et sécurisées à un périphérique, si celles-ci sont prises en charge. Si vous utilisez IPSec, il

---

ajoute également une surcharge CPU supplémentaire au périphérique. Cependant, SSH doit toujours être appliqué en tant que transport, même si IPSec est utilisé.

Bannières d'avertissement

Dans certaines juridictions, il peut être impossible de poursuivre et illégal de surveiller les utilisateurs malveillants, à moins qu'ils n'aient été informés qu'ils ne sont pas autorisés à utiliser le système. Une méthode pour fournir cette notification consiste à placer ces informations dans un message de bannière qui est configuré avec la commande banner login du logiciel Cisco IOS.

Les exigences en matière de notification légale sont complexes, varient selon la juridiction et la situation et nécessitent une discussion avec le conseiller juridique. Même au sein des juridictions, les opinions juridiques peuvent différer. En collaboration avec l'avocat, une bannière peut fournir une partie ou la totalité de ces informations :

- Notez que le système doit être connecté ou utilisé uniquement par le personnel spécifiquement autorisé et peut-être des informations sur les personnes autorisées à l'utiliser.
- Notez que toute utilisation non autorisée du système est illégale et peut faire l'objet de sanctions civiles et pénales.
- Notez que toute utilisation du système peut être consignée ou surveillée sans autre préavis et que les journaux résultants peuvent être utilisés comme preuve devant les tribunaux.
- Avis spécifiques requis par les lois locales.

Du point de vue de la sécurité, et non de la légalité, une bannière de connexion ne doit pas contenir d'informations spécifiques sur le nom du routeur, le modèle, le logiciel ou la propriété. Ces informations peuvent être détournées par des utilisateurs malveillants.

Authentification, autorisation et administration (AAA)

Le cadre AAA (Authentication, Authorization, and Accounting) est essentiel pour sécuriser l'accès interactif aux périphériques réseau. Le cadre AAA fournit un environnement hautement configurable qui peut être personnalisé, en fonction des besoins du réseau.

Authentification TACACS+

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

L'authentification TACACS+, ou plus généralement l'authentification AAA, permet d'utiliser des comptes utilisateur 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 semblable à TACACS+; toutefois, il chiffre uniquement 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, utilisez TACACS+ au lieu de RADIUS lorsque TACACS+ est pris en charge par le serveur AAA. Référez-vous à Comparaison 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 l'organisation.

Une liste de méthodes est une liste séquentielle qui décrit les méthodes d'authentification à interroger pour authentifier un utilisateur. Les listes de méthodes vous permettent de désigner un ou plusieurs protocoles de sécurité à utiliser pour l'authentification, et ainsi d'assurer un système de sauvegarde pour l'authentification 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 suivantes ne sont tentées que si les méthodes précédentes échouent en raison d'une indisponibilité du serveur ou d'une configuration incorrecte.

Authentification de secours

Si tous les serveurs TACACS+ configurés deviennent indisponibles, un périphérique Cisco IOS peut alors s'appuyer sur des protocoles d'authentification secondaires. Les configurations typiques incluent l'utilisation de l'authentification locale ou enable si tous les serveurs TACACS+ configurés ne sont pas disponibles.

La liste complète des options d'authentification sur le périphérique inclut les options enable, local et line. Chaque option présente des avantages. L'utilisation du **enable secret** est préférable, car le secret est haché avec un algorithme unidirectionnel qui est intrinsèquement plus sécurisé que l'algorithme de chiffrement utilisé avec les mots de passe de type 7 pour l'authentification de ligne ou locale.

Cependant, sur les versions du logiciel Cisco IOS qui prennent en charge l'utilisation de mots de passe secrets pour les utilisateurs définis localement, le recours à l'authentification locale peut être souhaitable. Cela permet de créer un utilisateur défini localement pour un ou plusieurs administrateurs réseau. Si TACACS+ était totalement indisponible, chaque administrateur peut utiliser son nom d'utilisateur et son mot de passe locaux. 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.

Cet exemple de configuration s'appuie sur l'exemple d'authentification TACACS+ précédent pour inclure l'authentification de secours au mot de passe configuré localement avec la **enable secret** commande :

```
!

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>
!
```

Utilisation de mots de passe de type 7

Conçus à l'origine pour permettre le déchiffrement rapide des mots de passe stockés, les mots de passe de type 7 ne constituent pas une forme sécurisée de stockage de mots de passe. Il existe de nombreux outils permettant de déchiffrer facilement ces mots de passe. Évitez d’utiliser des mots de passe de type 7, sauf si une fonction utilisée sur le périphérique Cisco IOS l’exige.

Dans la mesure du possible, utilisez le type 9 (script) :

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

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

Pour plus d'informations sur la suppression des mots de passe de type 7, consultez la section Durcissement du plan de gestion général.

Autorisation de commande TACACS+

L'autorisation de commande avec TACACS+ et AAA fournit un mécanisme qui autorise ou refuse chaque commande entrée par un utilisateur administratif. Lorsque l'utilisateur entre des commandes EXEC, Cisco IOS envoie chaque commande au serveur AAA configuré. Le serveur AAA utilise ses stratégies configurées pour autoriser ou refuser la commande pour cet utilisateur particulier.

Cette configuration peut être ajoutée à l'exemple d'authentification AAA précédent pour implémenter 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
!
```

Comptabilité des commandes TACACS+

Une fois configurée, la comptabilité des commandes AAA envoie des informations sur chaque commande EXEC entrée aux serveurs TACACS+ configurés. Les informations envoyées au serveur TACACS+ incluent la commande exécutée, la date à laquelle elle a été exécutée et le nom d'utilisateur de la personne qui a entré 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 s'appuie 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
!
```

Serveurs AAA redondants

Les serveurs AAA qui sont exploités dans un environnement peuvent être redondants et déployés de manière insensible aux pannes. Cela permet de s'assurer que l'accès à la gestion interactive, tel que SSH, est possible si un serveur AAA n'est pas disponible.

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

- Disponibilité des serveurs AAA au moment de pannes réseau potentielles
- Emplacement des serveurs AAA dispersé géographiquement
- Charger chaque serveur AAA qui se trouve dans un état stable et en situation de panne
- Latence réseau entre les serveurs d'accès réseau et les serveurs AAA
- serveur AAA synchronisation des bases de données

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

Renforcer le protocole SNMP (Simple Network Management Protocol)

Cette section présente plusieurs méthodes qui peuvent être utilisées pour sécuriser le déploiement SNMP dans les périphériques Cisco IOS. Il est essentiel que le protocole SNMP soit correctement sécurisé pour protéger la confidentialité, l'intégrité et la disponibilité des données réseau et des périphériques réseau par lesquels transitent les données. SNMP fournit une mine d'informations sur l'état des périphériques réseau. Protégez ces informations contre les utilisateurs malveillants qui souhaitent exploiter ces données pour lancer des attaques contre le réseau.

Chaînes de communauté SNMP

Les chaînes de communauté sont des mots de passe appliqués à un périphérique Cisco IOS pour restreindre l'accès, en lecture seule et en lecture-écriture, aux données SNMP du périphérique. Ces chaînes de communauté, comme tous les mots de passe, sont soigneusement choisies pour s'assurer qu'elles ne sont pas triviales. Modifiez les chaînes de communauté à intervalles réguliers et conformément aux politiques de sécurité du réseau. Par exemple, modifiez les chaînes

lorsqu'un administrateur réseau change de rôle ou quitte l'entreprise.

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

```
!

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

Remarque : Les exemples de chaînes de caractères de la communauté précédente ont été choisis pour expliquer clairement l'utilisation de ces chaînes. Pour les environnements de production, choisissez les chaînes de communauté avec précaution et incluez une série de symboles alphabétiques, numériques et non alphanumériques.

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

Chaînes de communauté SNMP avec ACL

Outre la chaîne de communauté, appliquez une liste de contrôle d'accès qui restreint davantage l'accès SNMP à un groupe sélectionné d'adresses IP source. Cette configuration restreint l'accès en lecture seule SNMP aux périphériques hôtes finaux qui résident dans l'espace d'adressage 192.168.100.0/24 et restreint l'accès en lecture-écriture SNMP au seul périphérique hôte final à l'adresse 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.

ACL d'infrastructure

Les listes de contrôle d'accès d'infrastructure (iACL) peuvent être déployées pour garantir que seuls les hôtes finaux possédant des adresses IP approuvées peuvent envoyer du trafic SNMP à un périphérique Cisco IOS. Idéalement, une liste de contrôle d'accès IP contient une stratégie qui refuse les paquets SNMP non autorisés sur le port UDP 161.

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

Vues SNMP

Les vues SNMP sont une fonction de sécurité qui permet ou refuse l'accès à certaines MIB SNMP. Une fois qu'une vue est créée et appliquée à une chaîne de communauté avec les commandes de configuration globale snmp-server community-string view, si vous accédez aux données MIB, vous êtes limité aux autorisations qui sont définies par la vue. Le cas échéant, utilisez des vues pour limiter les utilisateurs de SNMP aux données dont ils ont besoin.

Cet exemple de configuration restreint l'accès SNMP avec la chaîne de communauté LIMITED aux données MIB qui se trouvent dans le groupe système :

```
!

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

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

Référez-vous à Configuration de la prise en charge SNMP pour plus d'informations.

SNMP version 3

SNMP Version 3 (SNMPv3) est défini par les documents RFC3410, RFC3411, RFC3412,

RFC3413, RFC3414 et RFC3415 et est un protocole normalisé interopérable pour l'administration de réseaux. 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, SNMPv3 peut être utilisé pour ajouter une autre couche de sécurité lors du déploiement de SNMP. SNMPv3 se compose de trois options de configuration principales :

- no auth - Ce mode ne nécessite aucune authentification ni 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 pour utiliser les mécanismes de sécurité SNMPv3 (authentification ou authentification et cryptage) pour traiter les paquets SNMP ; par défaut, l'ID de moteur est généré localement. L'ID de moteur peut être affiché avec la **show snmp engineID** commande comme indiqué dans cet exemple :

<#root>

```
router#

show snmp engineID


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

Remarque : Si l'ID du moteur est modifié, tous les comptes utilisateurs SNMP doivent être reconfigurés.

L'étape suivante consiste à 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 un mot de passe de cryptage 3DES de **privpassword**:

```
!

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

Sachez que les commandes de **snmp-server user** configuration ne sont pas affichées dans le résultat de configuration du périphérique, comme requis par la RFC 3414. Par conséquent, le mot de passe utilisateur n'est pas visible dans la configuration. Pour afficher les utilisateurs configurés, entrez la **show snmp user** commande, comme indiqué dans cet exemple :

<#root>

```
router#

show snmp user


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

Référez-vous à Configuration de la prise en charge SNMP pour plus d'informations sur cette fonctionnalité.

Protection du plan de gestion

La fonction MPP (Management Plane Protection) de la plate-forme logicielle Cisco IOS peut être utilisée pour sécuriser le protocole SNMP, car elle restreint les interfaces par lesquelles le trafic SNMP peut se terminer sur le périphérique. La fonctionnalité MPP permet à un administrateur de désigner une ou plusieurs interfaces comme interfaces de gestion. Le trafic de gestion est autorisé à entrer dans un périphérique uniquement via ces interfaces de gestion. Une fois MPP activé, aucune interface, à l'exception des interfaces de gestion désignées, n'accepte le trafic de gestion

du réseau destiné au périphérique.

Le MPP est un sous-ensemble de la fonctionnalité CPPr et nécessite une version de Cisco IOS prenant en charge CPPr. Référez-vous à Comprendre la protection du plan de contrôle pour plus d'informations sur CPPr.

Dans cet exemple, MPP est utilisé pour limiter l'accès SNMP et SSH à l'interface FastEthernet 0/0 uniquement :

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

Référez-vous au Guide des fonctions de protection du plan de gestion pour plus d'informations.

Meilleures pratiques de journalisation

Les journaux d'événements offrent une visibilité sur le fonctionnement d'un périphérique Cisco IOS et sur le réseau sur lequel il est déployé. La plate-forme logicielle Cisco IOS offre plusieurs options de configuration de journal flexibles qui peuvent aider à atteindre les objectifs de gestion et de visibilité du réseau d'une entreprise.

Ces sections fournissent quelques bonnes pratiques de base sur les fonctionnalités de journalisation qui peuvent aider un administrateur à tirer parti des fonctions de journalisation avec succès, avec un impact minimal sur la fonctionnalité de journalisation sur un périphérique Cisco IOS.

Envoyer les journaux à un emplacement central

Il est conseillé d'envoyer les informations de journal 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 non fiable par UDP et en texte clair. Par conséquent, toutes les protections qu'un réseau offre au trafic de gestion (par exemple, le cryptage ou l'accès hors bande) peuvent être étendues pour inclure le trafic syslog.

Cet exemple configure un périphérique Cisco IOS pour envoyer des informations de journal à un

serveur syslog distant :

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

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

Intégrée à la plate-forme logicielle Cisco IOS 12.4(15)T et introduite à l'origine dans la version 12.0(26)S, la fonctionnalité de journalisation sur un disque ATA (Local Nonvolatile Storage) permet d'enregistrer les messages du journal système sur un disque flash ATA (Advanced Technology Attachment). Les messages enregistrés sur un disque ATA persistent après le redémarrage du routeur.

Ces lignes de configuration configurent 134 217 728 octets (128 Mo) de messages de journal dans le répertoire syslog de la mémoire flash ATA (disk0), avec une taille de fichier spécifiée de 16 384 octets :

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

Avant que les messages de journal ne soient écrits dans un fichier sur le disque ATA, le logiciel Cisco IOS vérifie s'il y a suffisamment d'espace disque. Si ce n'est pas le cas, le message du fichier journal le plus ancien (par horodatage) est supprimé et le fichier actuel est 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 la possibilité d'écraser les données stockées.

Cet exemple montre comment copier les messages de journal 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 de journal généré par un périphérique Cisco IOS est affecté à l'une des huit gravités qui vont du niveau 0, Urgences, au niveau 7, Débogage. Sauf indication contraire, il est conseillé d'éviter les journaux de niveau 7. Les journaux de niveau 7 entraînent une charge CPU élevée sur le périphérique, ce qui peut entraîner l'instabilité du périphérique et du réseau.

Le niveau de commande **logging trap** de configuration globale est utilisé pour spécifier quels messages de journal sont envoyés aux serveurs syslog distants. Le niveau spécifié indique le message de gravité la plus faible qui est envoyé. Pour les journaux mis en mémoire tampon, la commande **logging buffered** level est utilisée.

Cet exemple de configuration limite les messages de journal envoyés aux serveurs Syslog distants et au tampon de journal local aux niveaux de gravité 6 (Informationnel) à 0 (Urgences) :

```
!

logging trap 6
logging buffered 6
!
```

Référez-vous à Dépannage, Gestion des pannes et Journalisation pour plus d'informations.

Ne pas consigner dans la console ou les sessions de surveillance

Avec la plate-forme logicielle Cisco IOS, il est possible d'envoyer des messages de journalisation à la console et de surveiller les sessions, qui sont des sessions de gestion interactives dans lesquelles la commande EXEC **terminal monitor** a été exécutée. Cependant, cela peut augmenter la charge CPU d'un périphérique Cisco IOS et n'est donc pas recommandé. Au lieu de cela, envoyez les informations de journal au tampon de journal local qui peut être affiché avec la **show logging** commande.

Utilisez les commandes de configuration globale **no logging console** et **no logging monitor** pour désactiver les journaux sur la console et les sessions de surveillance. Cet exemple de configuration illustre l'utilisation de ces commandes :

```
!
```

```
no logging console
no logging monitor
!
```

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

Utiliser les journaux mis en mémoire tampon

La plate-forme logicielle Cisco IOS prend en charge l'utilisation d'un tampon de journal local pour qu'un administrateur puisse afficher les messages de journal générés localement. L'utilisation de journaux mis en mémoire tampon est fortement recommandée par rapport aux journaux destinés à la console ou aux sessions de surveillance.

Il existe deux options de configuration pertinentes lorsque vous configurez des journaux mis en mémoire tampon : la taille de la mémoire tampon du journal et la gravité des messages stockés dans la mémoire tampon. La taille du **logging buffer** est configurée avec la commande de configuration globale. **logging buffered size**. Le niveau de gravité le plus faible inclus dans la mémoire tampon est configuré avec la commande log buffered severity. Un administrateur peut afficher le contenu de la mémoire tampon du journal à l'aide de la commande **show logging** EXEC.

Cet exemple de configuration inclut la configuration d'un tampon de journal de 16 384 octets, ainsi qu'une gravité de 6, Informationnel, qui indique que les messages de niveaux 0 (Urgences) à 6 (Informationnel) sont stockés :

```
!

logging buffered 16384 6
!
```

Référez-vous à Référence des commandes de gestion de réseau de Cisco IOS pour plus d'informations sur les journaux mis en mémoire tampon.

Configurer l'interface source de journalisation

Pour fournir un niveau de cohérence accru lorsque vous collectez et consultez des messages de journal, il est conseillé de configurer de manière statique une interface source de journalisation. Pour ce faire, utilisez la commande **logging source-interface** interface. Une interface source de journalisation configurée de manière statique garantit que la même adresse IP apparaît dans tous les messages de journalisation envoyés depuis un périphérique Cisco IOS individuel. Pour plus de

stabilité, utilisez une interface de bouclage comme source du journal.

Cet exemple de configuration illustre l'utilisation de la commande de configuration globale **logging source-interface** interface pour spécifier l'adresse IP de l'interface de bouclage 0 à utiliser pour tous les messages de journal :

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

Référez-vous à Référence des commandes Cisco IOS pour plus d'informations.

Configurer les horodatages des journaux

La configuration des horodatages des journaux permet de corréler les événements sur les périphériques réseau. Il est important de mettre en oeuvre une configuration correcte et cohérente de l'horodatage des journaux pour garantir la possibilité de corréler les données des journaux. Configurez les horodatages du journal pour inclure la date et l'heure, avec une précision de millisecondes, et pour inclure le fuseau horaire utilisé sur le périphérique.

Cet exemple inclut la configuration des horodatages de journal, avec une précision de millisecondes, dans la zone Temps universel coordonné (UTC) :

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

Si vous préférez ne pas consigner les heures relatives à UTC, vous pouvez configurer un fuseau horaire local spécifique et configurer la présence de ces informations dans les messages de journal générés. Cet exemple montre la configuration d'un périphérique pour la zone de l'heure normale du Pacifique (PST) :

```
!

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

Gestion de la configuration du logiciel Cisco IOS

La plate-forme logicielle Cisco IOS inclut plusieurs fonctions permettant de gérer la configuration d'un périphérique Cisco IOS. Ces fonctionnalités incluent l'archivage des configurations et la restauration de la configuration vers une version précédente, ainsi que la création d'un journal détaillé des modifications de configuration.

Remplacement et restauration de la configuration

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. Stockées manuellement ou automatiquement, les configurations de cette archive peuvent être utilisées pour remplacer la configuration en cours par la commande **configure replace** filename. Cette commande est différente de la commande **copy** filename **running-config** . La **configure replace** commande filename remplace la configuration en cours, contrairement à la fusion effectuée par la **copy** commande.

Il est conseillé d'activer cette fonction sur tous les périphériques Cisco IOS du réseau. Une fois activée, un administrateur peut ajouter la configuration en cours à l'archive à l'aide de la **archive config EXEC** commande. Les configurations archivées peuvent être affichées à l'aide de la **show archive EXEC** commande.

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

```
!

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

Bien que la fonction d'archivage de configuration puisse stocker jusqu'à 14 configurations de sauvegarde, il est conseillé de prendre en compte l'espace requis avant d'utiliser la **maximum** commande.

Accès exclusif aux modifications de configuration

Ajoutée à la version 12.3(14)T du logiciel Cisco IOS, la fonctionnalité d'accès exclusif aux modifications de configuration garantit qu'un seul administrateur modifie la configuration d'un périphérique Cisco IOS à la fois. Cette fonctionnalité permet d'éliminer l'impact indésirable des modifications simultanées apportées aux composants de configuration associés. Cette fonction est configurée avec le mode de commande de configuration globale, **configuration mode exclusive** et fonctionne dans l'un des deux modes suivants : automatique ou manuelle. En mode automatique, la configuration se verrouille automatiquement lorsqu'un administrateur émet la **configure terminal EXEC** commande. En mode manuel, l'administrateur utilise la **configure terminal lock** commande pour verrouiller la configuration lorsqu'il passe en mode de configuration.

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

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

Configuration résiliente du logiciel Cisco IOS

Ajoutée à la version 12.3(8)T du logiciel Cisco IOS, la fonction Resilient Configuration permet de stocker en toute sécurité une copie de l'image du logiciel Cisco IOS et de la configuration du périphérique actuellement utilisée par un périphérique Cisco IOS. Lorsque cette fonctionnalité est activée, il n'est pas possible de modifier ou de supprimer ces fichiers de sauvegarde. Nous vous conseillons d'activer cette fonctionnalité pour empêcher les tentatives de suppression de ces fichiers, qu'elles soient malveillantes ou non.

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

Une fois cette fonctionnalité activée, il est possible de restaurer une configuration supprimée ou une image du logiciel Cisco IOS. L'état actuel de cette fonctionnalité peut être affiché avec la **show secure boot EXEC** commande.

Logiciel Cisco à signature numérique

Ajoutée à la version 15.0(1)M du logiciel Cisco IOS pour les routeurs des gammes Cisco 1900, 2900 et 3900, la fonctionnalité Logiciel Cisco signé numériquement facilite l'utilisation du logiciel Cisco IOS signé numériquement et donc approuvé, avec l'utilisation d'une cryptographie asymétrique (clé publique) sécurisée.

Une image à signature numérique est assortie d'un hachage chiffré (avec clé privée). Lors de la vérification, le dispositif décrypte le hachage avec la clé publique associée à partir des clés qu'il a dans sa mémoire de clés et calcule également 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. La version de clé associée aux types Production et Special est incrémentée par ordre alphabétique lorsque 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 remplacent et suppriment une clé utilisée pour une vérification du logiciel Cisco signée numériquement du stockage des clés de la plate-forme. 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 incluse dans une image (de production ou de révocation) qui est 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. Lorsque vous révoquez une clé de production, une fois l'image de révocation chargée, la nouvelle

clé qu'elle porte est ajoutée au magasin de clés et l'ancienne clé associée peut être révoquée, tant que l'image ROMMON est mise à niveau et que la nouvelle image de production est 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 au magasin de clés à partir de l'image de production actuelle, copie une nouvelle image ROMMON (C3900_rom-monitor.srec.SSB) dans la zone de stockage (usbflash0:), met à niveau le fichier ROMMON et révoque 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.

Notification et consignation des modifications de configuration

La fonctionnalité Notification et consignation des modifications de configuration, ajoutée au logiciel Cisco IOS Version 12.3(4)T, permet de consigner les modifications de configuration apportées à un périphérique Cisco IOS. Le journal est tenu 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 effectuée. Cette fonctionnalité est activée à l'aide de la commande de mode de configuration du journal des modifications de configuration **logging enable** . Les commandes **hidekeys** et les **logging size** entrées facultatives sont utilisées pour améliorer la configuration par défaut, car elles empêchent les journaux de données de mot

de passe et augmentent la longueur du journal des modifications.

Il est conseillé d'activer cette fonctionnalité afin de mieux comprendre l'historique des modifications de configuration d'un périphérique Cisco IOS. En outre, il est conseillé d'utiliser la commande de **notify syslog** configuration pour activer la génération de messages Syslog lorsqu'une modification de configuration est effectuée.

```
!

archive
 log config
  logging enable
  logging size 200
  hidekeys
  notify syslog
!
```

Une fois que la fonctionnalité Notification et consignation des modifications de configuration a été activée, la commande EXEC privilégiée **show archive log config all** peut être utilisée pour afficher le journal de configuration.

Plan de contrôle

Les fonctions du plan de contrôle comprennent les protocoles et les processus qui communiquent entre les périphériques réseau pour déplacer les données de la source à la destination. Cela inclut les protocoles de routage, tels que le Border Gateway Protocol, ainsi que les protocoles tels que ICMP et RSVP (Resource Reservation Protocol).

Il est important que les événements dans les plans de gestion et de données n'affectent pas le plan de contrôle. Si un événement de plan de données, tel qu'une attaque par déni de service, affecte le plan de contrôle, l'ensemble du réseau peut devenir instable. Ces informations sur les fonctions et les configurations de la plate-forme logicielle Cisco IOS peuvent aider à garantir la résilience du plan de contrôle.

Durcissement Général Du Plan De Contrôle

La protection du plan de contrôle d'un périphérique réseau est essentielle, car le plan de contrôle garantit la maintenance et le fonctionnement des plans de gestion et de données. Si le plan de contrôle devient instable lors d’un incident de sécurité, il peut 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 minimiser la quantité de charge CPU requise pour traiter les paquets inutiles.

Redirections ICMP IP

Un message de redirection ICMP peut être généré par un routeur lorsqu'un paquet est reçu et transmis sur la même interface. Dans cette situation, le routeur transfère le paquet et renvoie un message de redirection ICMP à l'expéditeur du paquet d'origine. Ce comportement permet à l'expéditeur de contourner le routeur et de transférer les paquets futurs directement vers la destination (ou vers un routeur plus proche de la destination). Dans un réseau IP fonctionnant correctement, un routeur envoie des redirections uniquement aux hôtes sur ses propres sous-réseaux locaux. En d'autres termes, les redirections ICMP ne dépassent généralement jamais une limite de couche 3.

Il existe deux types de messages de redirection ICMP : redirection pour une adresse hôte et redirection pour un sous-réseau entier. Un utilisateur malveillant peut exploiter la capacité du routeur à envoyer des redirections ICMP en transmettant continuellement des paquets au routeur, ce qui oblige le routeur à répondre avec des messages de redirection ICMP et a un impact négatif sur le processeur et les performances du routeur. Pour empêcher le routeur de transmettre des redirections ICMP, utilisez la commande de configuration d'**no ip redirects**interface.

Messages ICMP inaccessibles

La filtration avec une liste d'accès d'interface provoque la transmission des messages ICMP inaccessibles à la source du trafic filtré. La génération de ces messages peut augmenter l'utilisation du processeur sur le périphérique. Par défaut, dans le logiciel Cisco IOS, la génération d'ICMP inaccessible est limitée à un paquet toutes les 500 millisecondes. La génération de messages ICMP inaccessibles peut être désactivée à l'aide de la commande de configuration d'interface **no ip unreachables**. La limite de débit ICMP inaccessible peut être modifiée à partir de la valeur par défaut à l'aide de la commande de configuration globale **ip icmp rate-limit unreachable** interval-in-ms.

Proxy ARP

Le proxy ARP est la technique par laquelle un périphérique, généralement un routeur, répond aux requêtes ARP destinées à un autre périphérique. En falsifiant son identité, le routeur accepte la responsabilité d'acheminer les paquets vers la destination réelle. Le proxy ARP peut aider les machines d'un sous-réseau à atteindre des sous-réseaux distants sans configuration de route ou passerelle par défaut. Le proxy ARP est défini dans la RFC 1027 .

L'utilisation du proxy ARP présente des 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 des ressources car chaque requête ARP proxy consomme une petite quantité de mémoire. Un pirate peut épuiser toute la mémoire disponible s'il envoie un grand nombre de requêtes ARP.

Les attaques de type « Man-in-the-Middle » permettent à un hôte du réseau d’usurper l’adresse MAC du routeur, ce qui entraîne la transmission par inadvertance du trafic des hôtes au pirate. Le proxy ARP peut être désactivé avec la commande de configuration d'interface **no ip proxy-arp**.

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

La protection du plan de contrôle est essentielle. Étant donné que les performances des applications et l'expérience de l'utilisateur final peuvent être affectées sans la présence de trafic de données et de gestion, la capacité de survie du plan de contrôle garantit que les deux autres plans sont maintenus et opérationnels.

Comprendre le trafic du plan de contrôle

Pour protéger correctement le plan de contrôle du périphérique Cisco IOS, il est essentiel de comprendre les types de trafic qui sont commutés par processus par le processeur. Le trafic commuté par processus se compose normalement de deux types de trafic différents. Le premier type de trafic est dirigé vers le périphérique Cisco IOS et doit être géré directement par le processeur du périphérique Cisco IOS. Ce trafic consiste en la catégorie visant à recevoir le trafic de contiguïté. Ce trafic contient une entrée dans la table CEF (Cisco Express Forwarding), dans laquelle le saut de routeur suivant est le périphérique lui-même, qui est indiqué par le terme « receive » dans le résultat de l'**show ip cef**interface de ligne de commande. Cette indication est le cas pour toute adresse IP qui nécessite un traitement direct par le processeur du périphérique Cisco IOS, qui inclut les adresses IP d'interface, l'espace d'adressage de multidiffusion et l'espace d'adressage de diffusion.

Le deuxième type de trafic géré par le processeur est le trafic du plan de données, c'est-à-dire le trafic dont la destination se situe au-delà du périphérique Cisco IOS lui-même, ce qui nécessite un traitement spécial par le processeur. Bien qu'il ne s'agisse pas d'une liste exhaustive des impacts du CPU 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 de la liste de contrôle d'accès - Le trafic du journal de liste de contrôle d'accès est constitué de tous les paquets générés en raison d'une correspondance (autorisation ou refus) d'une entrée de contrôle d'accès sur laquelle le mot clé log est utilisé.
- Unicast Reverse Path Forwarding (Unicast RPF) : le protocole Unicast RPF, utilisé avec une liste de contrôle d'accès, 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 processeur pour être traité.
- Expiration TTL (Time-to-live) : les paquets dont la valeur TTL est inférieure ou égale à un nécessitent l'envoi de messages ICMP de type 11 (Internet Control Message Protocol Time Exceeded), ce qui entraîne un traitement par le processeur.
- ICMP Unreachables - Les paquets qui entraînent des messages ICMP inaccessibles en raison de leur route, de leur MTU ou de leur filtrage sont traités par le processeur.
- Trafic nécessitant une requête ARP - Les destinations pour lesquelles aucune entrée ARP n'existe sont traitées par le processeur.
- Trafic non IP : Tout trafic non IP est traité par le CPU.

Cette liste détaille plusieurs méthodes permettant de déterminer les types de trafic à traiter par le processeur du périphérique Cisco IOS :

- La **show ip cef** commande fournit les informations de tronçon suivant pour chaque préfixe IP contenu dans la table 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 processeur.
- Cette **show interface switching** commande fournit des informations sur le nombre de paquets qui sont commutés par un périphérique.
- La **show ip traffic** commande fournit des informations sur le nombre de paquets IP :
    - avec une destination locale (c'est-à-dire, recevoir le trafic de contiguïté)
    - avec options
    - qui nécessitent une fragmentation
    - qui sont envoyées à l'espace d'adressage de diffusion
    - qui sont envoyées à l'espace d'adressage de multidiffusion
- Le trafic de contiguïté de réception peut être identifié à l'aide de la commande show ip cache flow. Tous les flux destinés au périphérique Cisco IOS ont une interface de destination (DstIf) locale.
- La réglementation du plan de contrôle peut être utilisée pour identifier le type et le débit du trafic qui atteint le plan de contrôle du périphérique Cisco IOS. La réglementation du plan de contrôle peut être effectuée à l'aide de listes de contrôle d'accès de classification granulaire, de journaux et de la **show policy-map control-plane** commande.

ACL d'infrastructure

Les listes de contrôle d’accès d’infrastructure (iACL) limitent les communications externes aux périphériques du réseau. Les listes de contrôle d'accès iACL sont traitées en détail dans la section Limiter l'accès au réseau avec des listes de contrôle d'accès d'infrastructure de ce document.

Il est conseillé de mettre en oeuvre des listes de contrôle d'accès IP pour protéger le plan de contrôle de tous les périphériques réseau.

Recevoir des ACL

Pour les plates-formes distribuées, les listes de contrôle d'accès 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. La rACL protège le périphérique du trafic nuisible avant que le trafic n'affecte le processeur de routage. Les rACL sont conçues pour protéger uniquement le périphérique sur lequel elles sont configurées et le trafic de transit n'est pas affecté par une rACL. Par conséquent, l'adresse IP de destination « any » utilisée dans l'exemple d'entrées de liste de contrôle d'accès présenté ne fait référence qu'aux adresses IP physiques ou virtuelles du routeur. Les rACL sont également considérées comme une meilleure pratique en matière de sécurité réseau et peuvent être considérées comme un ajout à long terme à une bonne sécurité réseau.

Il s'agit de la liste de contrôle d'accès du chemin de réception écrite pour autoriser le trafic SSH (port TCP 22) en provenance d'hôtes approuvés 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
!
```

Reportez-vous à GSR : Recevoir des listes de contrôle d'accès pour identifier et autoriser le trafic légitime vers un périphérique et refuser tous les paquets indésirables.

CoPP

La fonction CoPP peut également être utilisée pour restreindre les paquets IP destinés au périphérique d'infrastructure. Dans cet exemple, seul le trafic SSH provenant d'hôtes de confiance est autorisé à atteindre le processeur du périphérique Cisco IOS.

Remarque : Le trafic rejeté à partir d'adresses IP inconnues ou non fiables peut empêcher les hôtes disposant d'adresses IP attribuées dynamiquement d'établir une connexion 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 les versions du logiciel Cisco IOS 12.0S, 12.2SX, 12.2S, 12.3T, 12.4 et 12.4T.

Protection du plan de contrôle

La protection du plan de contrôle (CPPr), introduite dans le logiciel Cisco IOS Version 12.4(4)T, peut être utilisée pour restreindre ou contrôler le trafic du plan de contrôle destiné au processeur du périphérique Cisco IOS. Bien que similaire à CoPP, CPPr peut restreindre le trafic avec une granularité plus fine. Le CPPr divise le plan de contrôle agrégé en trois catégories distinctes de plans de contrôle appelées sous-interfaces. Il existe des sous-interfaces pour les catégories de trafic Hôte, Transit et CEF-Exception. En outre, CPPr inclut les fonctions de protection du plan de contrôle suivantes :

- Fonction de filtrage de port - Cette fonction permet de contrôler et d'abandonner les paquets envoyés à des ports TCP ou UDP fermés ou non en écoute.
- Queue-threshold feature - Cette fonctionnalité limite le nombre de paquets pour un protocole

spécifié autorisés dans la file d'attente d'entrée IP du plan de contrôle.

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

Limiteurs de débit matériel

Les Supervisor Engine 32 et Supervisor Engine 720 de la gamme Cisco Catalyst 6500 prennent en charge des limiteurs de débit (HWRL) matériels spécifiques à la plate-forme pour des scénarios réseau spéciaux. Ces limiteurs de débit matériels sont appelés limiteurs de débit de cas spéciaux car ils couvrent un ensemble prédéfini spécifique de scénarios de déni de service IPv4, IPv6, monodiffusion et multidiffusion. Les HWRL peuvent protéger le périphérique Cisco IOS contre diverses attaques qui nécessitent que les paquets soient traités par le processeur.

Plusieurs HWRL sont activés par défaut. Référez-vous à Paramètres par défaut du limiteur de débit basé sur le matériel PFC3 pour plus d'informations sur les HWRL.

Référez-vous à Limiteurs de débit basés sur le matériel sur la PFC3 pour plus d'informations sur les HWRL.

BGP sécurisé

Le protocole BGP (Border Gateway Protocol) est la base de routage d'Internet. À ce titre, toute entreprise ayant des exigences plus que modestes en matière de connectivité utilise souvent le protocole BGP. Le BGP est souvent ciblé par des attaquants en raison de son omniprésence et de la nature établie et oubliée des configurations BGP dans les petites organisations. Cependant, il existe de nombreuses fonctionnalités de sécurité spécifiques à BGP qui peuvent être utilisées pour augmenter la sécurité d'une configuration BGP.

Ceci fournit une vue d'ensemble des fonctions de sécurité BGP les plus importantes et, le cas échéant, des recommandations de configuration sont faites.

Protections de sécurité basées sur TTL

Chaque paquet IP contient un champ de 1 octet appelé durée de vie (TTL). Chaque périphérique traversé par un paquet IP décrémente cette valeur de un. La valeur de début de durée de vie varie selon le système d’exploitation et se situe généralement entre 64 et 255. Un paquet est abandonné lorsque sa valeur de durée de vie atteint zéro.

Connue sous les noms de Generalized TTL-based Security Mechanism (GTSM) et BGP TTL Security Hack (BTSH), une protection basée sur TTL exploite la valeur TTL des paquets IP pour garantir que les paquets BGP reçus proviennent d'un homologue connecté directement. Cette fonctionnalité nécessite souvent une coordination de la part des routeurs homologues ; cependant, une fois activé, il peut complètement vaincre de nombreuses attaques basées sur TCP contre BGP.

GTSM pour BGP est activé avec l'**ttl-security**option pour la commande de configuration du routeur **neighbor** BGP. 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 des paquets BGP sont reçus, la valeur de durée de vie est vérifiée et doit être supérieure ou égale à 255, moins le nombre de sauts spécifié.

Authentification d'homologue BGP avec MD5

L'authentification de l'homologue avec MD5 entraîne une authentification MD5 pour chaque paquet envoyé lors d'une session BGP. Plus précisément, des parties des en-têtes IP et TCP, des données utiles TCP et une clé secrète sont utilisées pour générer le condensé.

Le condensé créé est ensuite stocké dans l'option TCP Kind 19, qui a été créée spécifiquement à cet effet par RFC 2385 . Le haut-parleur BGP destinataire utilise le même algorithme et la même clé secrète pour régénérer le résumé du message. Si les résumés reçus et calculés ne sont pas identiques, le paquet est rejeté.

L'authentification d'homologue avec MD5 est configurée avec l'**password**option de la commande de configuration du routeur **neighbor** BGP. L'utilisation de cette commande est illustrée ici :

```
!

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

Référez-vous à Authentification de 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 un routeur. Plus un routeur doit contenir de préfixes, plus BGP consomme de mémoire. Dans certaines configurations, un sous-ensemble de tous les préfixes Internet peut être stocké, par exemple dans les configurations qui utilisent uniquement une route par défaut ou des routes pour les réseaux d'utilisateurs du fournisseur.

Pour éviter l'épuisement de la mémoire, configurez le nombre maximal de préfixes acceptés par homologue. Il est recommandé de configurer une limite pour chaque homologue BGP.

Lorsque vous configurez cette fonctionnalité avec la commande de configuration du routeur **neighbor maximum-prefix** BGP, un argument est requis : nombre maximal de préfixes acceptés avant l'arrêt d'un homologue. Vous pouvez également saisir un nombre compris entre 1 et 100. Ce nombre représente le pourcentage de la valeur maximale de préfixes par rapport à l'envoi d'un message de journal.

```
!

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

Référez-vous à Configuration de la fonctionnalité BGP Maximum-Prefix pour plus d'informations sur les préfixes maximum par homologue.

Filtrer les préfixes BGP avec les listes de préfixes

Les listes de préfixes permettent à un administrateur réseau d'autoriser ou de refuser des préfixes spécifiques envoyés ou reçus par BGP. Dans la mesure du possible, utilisez des listes de préfixes pour vous assurer que le trafic réseau est envoyé sur les chemins prévus. Appliquez des listes de préfixes à chaque homologue eBGP dans les directions entrante et sortante.

Les listes de préfixes configurées limitent les préfixes envoyés ou reçus à ceux spécifiquement autorisés par la stratégie de routage d’un réseau. Si cela n'est pas possible en raison du grand nombre de préfixes reçus, configurez une liste de préfixes pour bloquer spécifiquement les préfixes incorrects connus. Ces préfixes incorrects connus incluent l’espace d’adressage IP non

alloué et les réseaux réservés à des fins internes ou de test par la RFC 3330. Configurez les listes de préfixes sortants pour autoriser spécifiquement uniquement les préfixes qu'une organisation a l'intention d'annoncer.

Cet exemple de configuration utilise des listes de préfixes pour limiter les routes apprises et annoncées. Plus précisément, seule une route par défaut est autorisée en entrée par la liste de préfixes BGP-PL-INBOUND, et le préfixe 192.168.2.0/24 est la seule route autorisée à 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 fournisseur de services à l'aide de BGP externe pour la couverture complète des informations de filtre de préfixe BGP.

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

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

Cet exemple de configuration utilise des listes d'accès de chemin AS pour limiter les préfixes entrants à ceux provenant du système autonome distant et les préfixes sortants à ceux provenant du système autonome local. Les préfixes provenant de tous les autres systèmes autonomes sont filtrés et non installés dans la table 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 transférer correctement le trafic et à effectuer une reprise après des modifications ou des défaillances de la topologie dépend d’une vue précise de la topologie. Vous pouvez souvent exécuter un protocole IGP (Interior Gateway Protocol) pour fournir cette vue. Par défaut, les protocoles IGP sont dynamiques et détectent les routeurs supplémentaires qui communiquent avec le protocole IGP utilisé. Les protocoles IGP détectent également les routes qui peuvent être utilisées en cas de défaillance d’une liaison réseau.

Ces sous-sections fournissent une vue d'ensemble des fonctions de sécurité IGP les plus importantes. Le cas échéant, des recommandations et des exemples qui couvrent les protocoles RIPv2 (Routing Information Protocol Version 2), EIGRP (Enhanced Interior Gateway Routing Protocol) et OSPF (Open Shortest Path First) sont fournis.

Authentification et vérification du protocole de routage avec Message Digest 5

L’échec de la sécurisation de l’échange d’informations de routage permet à un pirate d’introduire de fausses informations de routage dans le réseau. Utilisez l’authentification par mot de passe avec les protocoles de routage entre les routeurs pour renforcer la sécurité du réseau. Cependant, comme cette authentification est envoyée en texte clair, il peut être simple pour un pirate de subvertir ce contrôle de sécurité.

Lorsque des fonctionnalités de hachage MD5 sont ajoutées au processus d’authentification, les mises à jour de routage ne contiennent plus de mots de passe en texte clair et l’intégralité du contenu de la mise à jour de routage est plus inviolable. Cependant, l'authentification MD5 est toujours susceptible d'attaques en force et par dictionnaire si des mots de passe faibles sont utilisés. Il est conseillé d'utiliser des mots de passe suffisamment aléatoires. Étant donné que l'authentification MD5 est beaucoup plus sécurisée que l'authentification par mot de passe, ces exemples sont spécifiques à l'authentification MD5. IPSec peut également être utilisé pour valider et sécuriser les protocoles de routage, mais ces exemples ne détaillent pas son utilisation.

Les protocoles EIGRP et RIPv2 utilisent des chaînes de clés dans le cadre de la configuration. Référez-vous à clé pour plus d'informations sur la configuration et l'utilisation des chaînes de clés.

Ceci est un exemple de configuration pour l'authentification de routeur EIGRP qui utilise 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>
!
```

Il s’agit d’un exemple de configuration de l’authentification du 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 avec MD5. OSPF n'utilise pas de chaînes 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'informations, ou l'introduction de fausses informations dans un IGP, peuvent être atténuées par l'utilisation de la **passive-interface** commande qui aide au contrôle de l'annonce d'informations de routage. Nous vous conseillons de ne pas annoncer d'informations aux réseaux qui ne sont pas sous votre contrôle administratif.

Cet exemple illustre l'utilisation de cette fonctionnalité :

```
!

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

Filtrage de route

Pour réduire le risque d'introduction d'informations de route erronées sur le réseau, utilisez le filtrage de route. Contrairement à la commande de configuration du **passive-interface** routeur, le routage se produit sur les interfaces une fois que le filtrage de route est activé, mais les informations qui sont annoncées ou traitées sont limitées.

Pour les protocoles EIGRP et RIP, l'utilisation de la **distribute-list** commande avec le mot-**out**clé limite les informations annoncées, tandis que l'utilisation du mot-**in**clé limite les mises à jour traitées. La **distribute-list** commande est disponible pour OSPF, mais elle n'empêche pas un routeur de propager des routes filtrées. À la place, la **area filter-list** commande peut être utilisée.

Cet exemple EIGRP filtre les annonces sortantes avec la **distribute-list** commande 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 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>
!
```

Cet exemple OSPF utilise une liste de préfixes avec les **area filter-list** command:

```
!

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 du processus de routage

Les préfixes de protocole de routage sont stockés en mémoire par un routeur, et la consommation des ressources augmente avec les préfixes supplémentaires qu'un routeur doit contenir. Pour éviter l'épuisement des ressources, configurez le protocole de routage afin de 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 illustre la configuration de la fonction de protection contre la surcharge de la base de données d'état des liaisons OSPF :

```
!

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

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 une fonctionnalité de passerelle par défaut pour un segment de réseau ou un ensemble de VLAN qui contiennent des serveurs ou des stations de travail.

Le protocole d'équilibrage de charge de passerelle (GLBP), le protocole HSRP (Hot Standby Router Protocol) et le protocole VRRP (Virtual Router Redundancy Protocol) sont tous des protocoles FHRP. Par défaut, ces protocoles utilisent des communications non authentifiées. Ce type de communication peut permettre à un pirate de se faire passer pour un périphérique compatible FHRP et d'assumer le rôle de passerelle par défaut sur le réseau. Cette prise de contrôle permet à un pirate d'exécuter une attaque de type « homme du milieu » et d'intercepter tout le trafic utilisateur qui sort du réseau.

Pour empêcher ce type d'attaque, tous les FHRP pris en charge par le logiciel Cisco IOS incluent une fonctionnalité d'authentification avec des chaînes MD5 ou des chaînes de texte. En raison de la menace posée par les FHRP non authentifiés, il est recommandé que les instances de ces protocoles utilisent l'authentification MD5. Cet exemple de configuration illustre 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 chargé de déplacer les données de la 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 protéger les plans de gestion et de contrôle de préférence au plan de données lorsque vous sécurisez un périphérique réseau .

Cependant, dans le plan de données lui-même, de nombreuses fonctionnalités et options de configuration peuvent contribuer à sécuriser le trafic. Ces sections détaillent les fonctionnalités et les options qui vous permettront de sécuriser plus facilement votre réseau.

Durcissement général du plan de données

La grande majorité du trafic du plan de données circule sur le réseau, comme déterminé par la configuration de routage du réseau. Cependant, la fonctionnalité de réseau IP permet de modifier le chemin des paquets sur le réseau. Des fonctionnalités, telles que les options IP, en particulier l'option de routage source, constituent un défi de sécurité pour les réseaux actuels.

L'utilisation de listes de contrôle d'accès de transit permet également de durcir le plan de données.

Pour plus d'informations, consultez la section Filtrer le trafic de transit avec les ACL de transit.

Options IP Abandon sélectif

Les options IP présentent deux problèmes de sécurité. Le trafic qui contient des options IP doit être commuté par processus par les périphériques Cisco IOS, ce qui peut entraîner une charge CPU élevée. Les options IP incluent également la fonctionnalité permettant de modifier le chemin emprunté par le trafic sur le réseau, ce qui lui permet potentiellement de subvertir les contrôles de sécurité.

En raison de ces préoccupations, la commande de configuration globale **ip options {drop | ignore}** a été ajoutée aux versions 12.3(4)T, 12.0(22)S et 12.2(25)S du logiciel Cisco IOS. Dans la première forme de cette commande, **ip options drop**tous les paquets IP contenant des options IP reçues par le périphérique Cisco IOS sont abandonnés. Cela empêche à la fois la charge élevée du 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 contenues dans les paquets reçus. Bien que cela atténue les menaces liées aux options IP pour le périphérique local, il est possible que les périphériques en aval puissent être affectés par la présence d'options IP. Pour cette raison, la **drop** forme de cette commande est fortement recommandée. Comme le montre cet exemple de configuration :

```
!
ip options drop
!
```

Certains protocoles, par exemple le protocole RSVP, font un usage légitime des options IP. La fonctionnalité de ces protocoles est affectée par cette commande.

Une fois la fonction de suppression sélective des options IP activée, la **show ip traffic EXEC** commande peut être utilisée pour déterminer le nombre de paquets abandonnés en raison de la présence d'options IP. Ces informations sont présentes dans le compteur d'abandon forcé.

Désactiver le routage de source IP

Le routage de la source IP tire parti des options de routage de source libre et de routage d'enregistrement, en tandem ; ou Strict Source Route, ainsi que l'option Record Route pour permettre à la source de datagramme IP de spécifier le chemin réseau emprunté par un paquet. Cette fonctionnalité peut être utilisée pour tenter d'acheminer le trafic autour des contrôles de sécurité sur le réseau.

Si les options IP n'ont pas été complètement désactivées par la fonction d'abandon sélectif des options IP, 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 la commande de configuration **no ip source-route** globale. Cet exemple de configuration illustre l'utilisation de cette commande :

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

Désactiver les redirections ICMP

Les redirections ICMP sont utilisées pour informer un périphérique réseau d'un meilleur chemin vers une destination IP. Par défaut, le logiciel Cisco IOS envoie une redirection s'il reçoit un paquet qui doit être routé via l'interface qui l'a reçu.

Dans certaines situations, il peut être possible pour un pirate de faire en sorte que le périphérique Cisco IOS envoie de nombreux messages de redirection ICMP, ce qui entraîne une charge CPU élevée. Pour cette raison, il est recommandé de désactiver la transmission des redirections ICMP. Les redirections ICMP sont désactivées avec la commande de configuration d'interface, **no ip redirects** comme indiqué dans cet exemple de configuration :

```
!

interface FastEthernet 0
 no ip redirects
!
```

Désactiver ou limiter les diffusions dirigées IP

Les diffusions dirigées IP permettent d’envoyer un paquet de diffusion IP à un sous-réseau IP distant. Une fois que le paquet atteint le réseau distant, le périphérique IP de transfert envoie le paquet sous forme de diffusion de couche 2 à toutes les stations du sous-réseau. Cette fonctionnalité de diffusion dirigée a été exploitée comme aide à l'amplification et à la réflexion dans plusieurs attaques, notamment l'attaque smurf.

Par défaut, cette fonctionnalité est désactivée dans les versions actuelles du logiciel Cisco IOS ; cependant, elle peut être activée par la commande de configuration d'**ip directed-broadcast**interface. Par défaut, cette fonctionnalité est activée dans les versions du logiciel Cisco IOS antérieures à la version 12.0.

Si un réseau nécessite absolument une fonctionnalité de diffusion dirigée, contrôlez son utilisation. Cela est possible avec l’utilisation d’une liste de contrôle d’accès comme option de la **ip directed-broadcast** commande. Cet exemple de configuration limite les diffusions dirigées aux paquets UDP qui proviennent d'un réseau approuvé, 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). Cela contraste avec les iACL qui cherchent à filtrer le trafic destiné au réseau lui-même. Le filtre fourni par les listes de contrôle d’accès de type t est avantageux lorsque l’objectif est de filtrer le trafic vers un groupe particulier de périphériques ou le trafic qui transite par le réseau.

Traditionnellement, les pare-feu exécutent ce type de filtre. Cependant, il existe des cas où il peut être avantageux d'exécuter ce filtre sur un périphérique Cisco IOS sur le réseau. Par exemple, lorsque la filtration doit être effectuée mais qu'aucun pare-feu n'est présent.

Les listes de contrôle d’accès en mode t sont également un endroit approprié pour mettre en oeuvre des protections antimystification statiques.

Pour plus d'informations, consultez la section Protections anti-mystification.

Référez-vous à Listes de contrôle d'accès de transit : Filtrage à votre périphérie pour plus d'informations sur les listes de contrôle d'accès.

Filtrage des paquets ICMP

Le protocole ICMP (Internet Control Message Protocol) a été conçu comme protocole de contrôle pour IP. En tant que tels, les messages qu'il transmet peuvent avoir des ramifications importantes sur les protocoles TCP et IP en général. Le protocole ICMP est utilisé par les outils **ping** et **traceroute**, pour dépanner le réseau, ainsi que par Path MTU Discovery. Cependant, une connectivité ICMP externe est rarement nécessaire pour un fonctionnement correct du réseau.

La plate-forme logicielle Cisco IOS permet de filtrer spécifiquement les messages ICMP par nom, type et code. Cet exemple de liste de contrôle d'accès autorise le protocole ICMP à partir de réseaux approuvés, tout en bloquant tous 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 détaillé précédemment dans la section Limiter l'accès au réseau avec les ACL d'infrastructure de ce document, le filtre de paquets IP fragmentés peut poser un défi aux périphériques de sécurité.

En raison de la nature non intuitive du contrôle des fragments, les fragments IP sont souvent autorisés par inadvertance par les listes de contrôle d’accès. La fragmentation est également souvent utilisée dans les tentatives de contournement de la détection par les systèmes de détection des intrusions. Pour ces raisons, les fragments IP sont souvent utilisés dans les attaques et peuvent être explicitement filtrés en haut de n'importe quelle liste de contrôle d'accès

configurée. L’exemple de liste de contrôle d’accès répertorié inclut un filtre complet de fragments IP. La fonctionnalité illustrée dans cet exemple doit être utilisée avec 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 par l’ACL des paquets IP fragmentés.]

Prise en charge ACL pour filtrer les options IP

Dans le logiciel Cisco IOS Version 12.3(4)T et ultérieure, le logiciel Cisco IOS prend en charge l'utilisation de listes de contrôle d'accès 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 subversion des contrôles de sécurité sur le réseau ou de modification des caractéristiques de transit d’un paquet. Pour ces raisons, il est recommandé de filtrer les paquets avec des options IP à la périphérie du réseau.

Utilisez cet exemple, ainsi que le contenu des exemples précédents, pour inclure un filtre complet pour les paquets IP contenant 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-Usurpation

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. La plate-forme logicielle Cisco IOS fournit Unicast RPF et IP Source Guard (IPSG) pour empêcher les attaques qui reposent sur l'usurpation d'adresse IP source. En outre, les listes de contrôle d'accès et le routage Null sont souvent déployés comme moyen manuel de prévention de l'usurpation.

L'IPSG réduit au minimum l'usurpation pour les réseaux sous contrôle administratif direct en vérifiant le port du commutateur, l'adresse MAC et l'adresse source. Le protocole RPF monodiffusion permet de vérifier le réseau source et peut réduire les attaques par usurpation provenant de réseaux qui ne sont pas sous contrôle administratif direct. La sécurité des ports permet de valider les adresses MAC au niveau de 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

Le protocole RPF de monodiffusion permet à un périphérique de vérifier que l'adresse source d'un paquet transféré peut être atteinte via l'interface qui a reçu le paquet. Ne vous fiez pas à Unicast RPF comme seule protection contre l'usurpation. Les paquets usurpés pourraient entrer dans le réseau via une interface Unicast RPF si une route de retour appropriée vers l'adresse IP 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 : libre ou strict. Dans les cas où il y a un routage asymétrique, le mode lâche est préféré parce que le mode strict est connu pour abandonner des paquets dans ces situations. Lors de la configuration de la commande de configuration d'**ip verify**interface, 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 Présentation de la redirection de chemin inverse de monodiffusion pour plus d'informations sur la configuration et l'utilisation de RPF de monodiffusion.

Protection de la source IP

IP Source Guard est un moyen efficace de prévention de l'usurpation qui peut être utilisé si vous avez le contrôle sur les interfaces de couche 2. IP Source Guard utilise les informations de surveillance DHCP pour configurer dynamiquement une liste de contrôle d'accès de port (PACL) sur l'interface de couche 2, en refusant tout trafic provenant d'adresses IP qui ne sont pas associées dans la table de liaison de source IP.

La protection de source IP peut être appliquée aux interfaces de couche 2 qui appartiennent à des VLAN activés pour la surveillance DHCP. Ces commandes activent la surveillance DHCP :

```
!

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

Une fois la surveillance DHCP activée, ces commandes activent IPSG :

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

La sécurité des ports peut être activée à l'aide de la commande de configuration d'**Tip verify source port security**interface. Cela nécessite la commande de configuration globale. **ip dhcp snooping information option**; De plus, le serveur DHCP doit prendre en charge l'option DHCP 82.

Référez-vous à Configuration des fonctionnalités DHCP et IP Source Guard pour plus d'informations sur cette fonctionnalité.

Sécurité du port

La sécurité des ports est utilisée pour limiter l'usurpation d'adresse MAC au niveau de l'interface d'accès. La sécurité des ports peut utiliser des adresses MAC apprises dynamiquement (rémanentes) 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 les suivants : protéger, restreindre, arrêter et arrêter le VLAN. Dans les cas où un port ne fournit l'accès qu'à une seule station de travail avec l'utilisation de protocoles standard, un nombre maximal d'un peut être suffisant. Les protocoles qui exploitent les adresses MAC virtuelles,

comme HSRP, ne fonctionnent pas lorsque le nombre maximal est défini sur 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 ARP dynamique

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

DAI intercepte et valide la relation d'adresse IP à MAC de tous les paquets ARP sur les ports non approuvés. Dans les environnements DHCP, la DAI se sert des données générées par la fonction d’espionnage DHCP. Les paquets ARP reçus sur les interfaces approuvées ne sont pas validés et les paquets non valides sur les interfaces non approuvées sont rejetés. Dans les environnements non DHCP, l'utilisation de listes de contrôle d'accès ARP est requise.

Ces commandes activent la surveillance DHCP :

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

Une fois la surveillance DHCP activée, ces commandes activent DAI :

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

Dans les environnements non DHCP, les listes de contrôle d'accès ARP sont nécessaires pour activer DAI. Cet exemple illustre 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 ARP dynamique pour plus d'informations sur la façon de configurer DAI.

Listes de contrôle d’accès antimystification

Les ACL configurées manuellement peuvent protéger contre l’usurpation statique si les attaques touchent un espace inutilisé et peu fiable. Généralement, ces listes de contrôle d’accès anti-usurpation sont appliquées au trafic entrant aux limites du réseau en tant que composant d’une liste de contrôle d’accès plus grande. Les listes de contrôle d’accès anti-mystification nécessitent des intervalles de surveillance réguliers 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 montre comment utiliser des listes de contrôle d'accès pour limiter l'usurpation IP. Cette liste de contrôle d’accès est appliquée en entrée sur l’interface souhaitée. Les ACE qui composent cette liste de contrôle d'accès ne sont pas complets. Si vous configurez ces types de liste de contrôle d’accès, recherchez une référence à jour qui soit 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 listes de contrôle d'accès IP couramment utilisées pour plus d'informations sur la façon de configurer des listes de contrôle d'accès.

La liste officielle des adresses Internet non attribuées est tenue à jour par Team Cymru. Des informations supplémentaires sur la façon de filtrer les adresses inutilisées sont disponibles à la page Référence de connexion .

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 les trames à travers le périphérique vers les destinations finales. Ces paquets, qui transitent par les périphériques déployés sur le réseau, peuvent avoir un impact sur le fonctionnement du processeur d'un périphérique. Sécurisez le plan de données, qui est constitué du trafic qui transite par le périphérique réseau, afin de garantir le fonctionnement des plans de gestion et de contrôle. Si le trafic de transit peut amener un périphérique à traiter le trafic du commutateur, le plan de contrôle d'un périphérique peut être affecté, ce qui entraîne une interruption de fonctionnement.

Fonctionnalités et types de trafic ayant un impact sur le processeur

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

- Journalisation ACL - Le trafic du journal ACL est constitué de tous les paquets générés en raison d'une correspondance (permit ou deny) d'une entrée de contrôle d'accès sur laquelle le mot clé log est utilisé.
- Unicast RPF : le protocole Unicast RPF utilisé avec une liste de contrôle d'accès 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.
- ICMP Unreachables - Les paquets qui entraînent des messages ICMP inaccessibles en raison de leur route, de leur MTU ou de leur filtrage sont traités par le processeur.
- Trafic nécessitant une requête ARP - Les destinations pour lesquelles aucune entrée ARP n'existe sont traitées par le processeur.
- Trafic non IP : Tout trafic non IP est traité par le CPU.

Pour plus d'informations sur le durcissement du plan de données, consultez la section Durcissement général du plan de données.

Filtrer selon la valeur TTL

Vous pouvez utiliser la fonctionnalité ACL Support for Filtering on TTL Value, introduite dans le logiciel Cisco IOS Version 12.4(2)T, dans une liste d'accès IP étendue pour filtrer les paquets en fonction de la valeur TTL. Cette fonctionnalité peut protéger un périphérique qui reçoit du trafic de transit lorsque la valeur de durée de vie est égale à zéro ou à un. Un filtre de paquets basé sur des valeurs TTL peut également être utilisé pour garantir que la valeur TTL n'est pas inférieure au diamètre du réseau, ce qui protège le plan de contrôle des périphériques d'infrastructure en aval contre les attaques d'expiration TTL.

Certaines applications et certains outils, tels que, **traceroute** utilisent des paquets d'expiration TTL à des fins de test et de diagnostic. Certains protocoles, tels qu'IGMP, utilisent légitimement une valeur de durée de vie égale à un.

Cet exemple de liste de contrôle d'accès crée une stratégie qui filtre les paquets IP lorsque la valeur 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 des attaques d'expiration de TTL pour plus d'informations sur la façon de filtrer les paquets en fonction de la valeur de TTL.

Référez-vous à Prise en charge ACL pour le filtrage sur la valeur 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 stratégie FPM

abandonne les paquets dont la valeur TTL est inférieure à 6.

```
!

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
!
```

Filtrer selon la présence des options IP

Dans le logiciel Cisco IOS Version 12.3(4)T et ultérieure, vous pouvez utiliser la fonctionnalité de prise en charge des listes de contrôle d'accès pour la fonction Options IP de filtrage dans une liste d'accès IP étendue nommée pour filtrer les paquets IP avec les options IP présentes. Le filtrage des paquets IP basé sur la présence d'options IP peut également être utilisé pour empêcher le plan de contrôle des périphériques d'infrastructure de devoir traiter ces paquets au niveau du processeur.

La fonctionnalité Prise en charge des listes de contrôle d’accès pour le filtrage des options IP ne peut être utilisée qu’avec des listes de contrôle d’accès étendues nommées. RSVP, Multiprotocol Label Switching Traffic Engineering, IGMP Versions 2 et 3 et d'autres protocoles qui utilisent des options IP, les paquets ne peuvent pas fonctionner correctement si les paquets de ces protocoles sont abandonnés. Si ces protocoles sont utilisés sur le réseau, la prise en charge ACL pour le filtrage des options IP peut être utilisée. Cependant, la fonctionnalité de suppression sélective des options IP de la liste de contrôle d'accès peut supprimer ce trafic et ces protocoles ne peuvent 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 de liste de contrôle d'accès crée une stratégie qui filtre les paquets IP contenant 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 de liste de contrôle d'accès illustre une stratégie 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 Record Route (record-route)
- 68 Horodatage (horodatage)
- 131 - Lsr (Loose Source Route)
- 137 - Strict Source Route (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
!
```

Référez-vous à 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 de transit : Filtrage à votre périphérie pour plus d'informations sur la façon de filtrer le transit et le trafic de périphérie.

CoPP est une autre fonctionnalité de la plate-forme logicielle Cisco IOS qui peut être utilisée pour filtrer les paquets avec des options IP. 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 ACL Support for Filtering IP Options, introduit dans le logiciel Cisco IOS Version 12.3(4)T, peut utiliser une politique de liste d'accès pour filtrer les paquets qui contiennent des options IP.

Cette stratégie CoPP supprime les paquets de transit reçus par un périphérique lorsque 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 stratégie CoPP supprime les paquets de transit reçus par un périphérique lorsque ces options IP sont présentes :

- 0 Fin de la liste d'options (eool)
- 7 Record Route (record-route)
- 68 Horodatage (horodatage)
- 131 Route de source libre (LSR)
- 137 Strict Source Route (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 stratégies CoPP précédentes, les entrées de liste de contrôle d'accès (ACE) qui correspondent aux paquets avec l'action d'autorisation entraînent l'abandon de ces paquets par la fonction policy-map drop, tandis que les paquets qui correspondent à l'action deny (non affichée) ne sont pas affectés par la fonction policy-map drop.

Protection du plan de contrôle

Dans le logiciel Cisco IOS Version 12.4(4)T et ultérieure, la protection du plan de contrôle (CPPr) peut être utilisée pour restreindre ou contrôler le trafic du plan de contrôle par le processeur d'un périphérique Cisco IOS. Bien que similaire à CoPP, CPPr peut restreindre ou contrôler le trafic avec une granularité plus fine que CoPP. CPPr divise le plan de contrôle agrégé en trois catégories distinctes appelées sous-interfaces : Il existe des sous-interfaces d'hôte, de transit et CEF-Exception.

Cette politique CPPr abandonne les paquets de transit reçus par un périphérique dont la valeur TTL est inférieure à 6 et les paquets de transit ou non reçus par un périphérique dont la valeur TTL est égale à zéro ou un. La stratégie CPPr abandonne également les paquets avec des 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 stratégie CPPr précédente, les entrées de la liste de contrôle d'accès qui correspondent aux paquets avec le résultat de l'action d'autorisation étaient que ces paquets ont été rejetés par la fonction policy-map drop, tandis que les paquets qui correspondent à l'action deny (non montré) n'étaient pas affectés par la fonction policy-map drop.

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

Identification et retraçage du trafic

Parfois, vous pouvez avoir besoin d'identifier et de retracer rapidement le trafic réseau, en particulier lors d'une réponse à un incident ou lors de performances réseau médiocres. Les listes de contrôle d’accès NetFlow et Classification sont deux méthodes principales pour y parvenir avec le logiciel Cisco IOS. NetFlow peut fournir une visibilité sur tout le trafic sur le réseau. En outre, NetFlow peut être mis en oeuvre avec des collecteurs qui peuvent fournir des tendances à long terme et une analyse automatisée. Les listes de contrôle d’accès de classification sont un composant des listes de contrôle d’accès et nécessitent une planification préalable pour identifier le trafic spécifique et une intervention manuelle lors de l’analyse. Ces sections fournissent un bref aperçu de chaque fonctionnalité.

NetFlow

NetFlow identifie les activités réseau anormales et liées à la sécurité par suivi des flux réseau. Les données NetFlow peuvent être visualisées et analysées par l'interface de ligne de commande, ou exportées vers un collecteur NetFlow commercial ou logiciel gratuit à des fins d'agrégation et d'analyse. Grâce aux tendances à long terme, les collecteurs NetFlow peuvent fournir un comportement réseau et une analyse de l'utilisation. NetFlow analyse des attributs spécifiques des paquets IP et crée des flux. La version 5 est la version la plus utilisée de NetFlow ; cependant, la 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 un prérequis pour activer NetFlow. NetFlow peut être configuré sur les routeurs et les commutateurs.

Cet exemple illustre la configuration de base de NetFlow. Dans les versions précédentes de la plate-forme logicielle Cisco IOS, la commande permettant d'activer NetFlow sur une interface est **ip route-cache flow** à la place de **ip flow {ingress | egress}**.

```
!

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

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

Voici un exemple de la sortie NetFlow de l'interface de ligne de commande. L'attribut SrcIf peut faciliter la remontée.

```
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 Cisco IOS NetFlow pour plus d'informations sur les capacités de NetFlow.

Référez-vous à Introduction à Cisco IOS NetFlow - A Technical Overview pour une présentation technique de NetFlow.

ACL de classification

Les listes de contrôle d’accès de classification offrent une visibilité sur le trafic traversant une interface. Les listes de contrôle d’accès de classification ne modifient pas la stratégie de sécurité d’un réseau et sont généralement conçues pour classer des protocoles, des adresses source ou des destinations individuels. Par exemple, une ACE qui autorise tout le trafic peut être séparée en protocoles ou ports spécifiques. Cette classification plus granulaire du trafic dans des ACE spécifiques peut aider à fournir une visibilité du trafic réseau, car chaque catégorie de trafic a son propre compteur d'accès. Un administrateur peut également séparer le refus implicite à la fin d'une liste de contrôle d'accès en ACE granulaires pour aider à identifier les types de trafic refusés.

Un administrateur peut accélérer une réponse à un incident en utilisant des listes de contrôle d’accès de classification avec les commandes **show access-list** et **clear ip access-list counters** EXEC.

Cet exemple montre la configuration d'une liste de contrôle d'accès 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
!
```

Pour identifier le trafic qui utilise une liste de contrôle d'accès de classification, utilisez la **show access-list EXEC** commande . La **clear ip access-list counters EXEC** commande permet de supprimer les compteurs de la liste de contrôle d'accès.

```
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 Présentation de la journalisation des listes de contrôle d'accès pour plus d'informations sur la façon d'activer les fonctionnalités de journalisation dans les ACL.

Contrôle d'accès avec mappages VLAN et listes de contrôle d'accès aux ports

Les listes de contrôle d'accès VLAN (VACL), ou les cartes VLAN et les listes de contrôle d'accès de port (PACL), permettent d'appliquer le contrôle d'accès au trafic non routé qui est plus proche des périphériques d'extrémité que les listes de contrôle d'accès appliquées aux interfaces routées.

Ces sections présentent les fonctionnalités, les avantages et les scénarios d'utilisation potentiels des VACL et des PACL.

Contrôle d'accès avec VLAN Maps

Les VACL, ou mappages de VLAN qui s'appliquent à tous les paquets qui entrent dans le VLAN, permettent d'appliquer le contrôle d'accès au trafic intra-VLAN. C'est toutefois impossible avec les ACL des interfaces routées. Par exemple, un mappage de VLAN peut être utilisé pour empêcher les hôtes du même VLAN de communiquer entre eux, ce qui réduit les possibilités pour les pirates locaux ou les vers d'exploiter un hôte sur le même segment de réseau. Pour empêcher les paquets d'utiliser une carte VLAN, créez une liste de contrôle d'accès (ACL) qui corresponde au trafic et, dans la carte VLAN, définissez l'action à abandonner. Une fois qu'un VLAN map est configuré, tous les paquets qui entrent dans le LAN sont évalués séquentiellement par rapport au

VLAN map configuré. Les cartes d'accès VLAN prennent en charge les listes d'accès IPv4 et MAC ; toutefois, ils ne prennent pas en charge les journaux ou 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 d'un VLAN map pour 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 cartes VLAN.

Contrôle d'accès avec PACL

Les listes de contrôle d'accès peuvent uniquement être appliquées à la direction entrante sur les interfaces physiques de couche 2 d'un commutateur. Tout comme les mappages VLAN, les listes de contrôle d'accès fournissent un contrôle d'accès sur le 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 une liste de contrôle d'accès est appliquée à une interface de couche 2, elle est appelée 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 nommée étendue pour illustrer la configuration de cette fonctionnalité :

```
!

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 à l'aide de cette commande en mode de configuration d'interface :

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

Remarque : Les listes de contrôle d'accès MAC permettent 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 dans le logiciel Cisco IOS Version 12.2(33)SRA ou ultérieure.

Cette commande d'interface doit être appliquée à l'interface d'entrée et indique au moteur de transfert de ne pas inspecter l'en-tête IP. Vous pouvez donc 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 couche 2 qui limite la connectivité entre les stations de travail ou les serveurs sur un VLAN. Sans PVLAN, tous les périphériques d’un VLAN de couche 2 peuvent communiquer librement. Il existe des situations de réseau où la sécurité peut être renforcée par la limitation de la communication entre les périphériques sur un VLAN unique. Par exemple, les PVLAN sont souvent utilisés pour interdire la communication entre les serveurs sur un sous-réseau accessible publiquement. Si un seul serveur est compromis, le manque de connectivité aux autres serveurs en raison de l'application de PVLAN peut aider à limiter la compromission à un seul serveur.

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

VLAN isolés

La configuration d'un VLAN secondaire en tant que VLAN isolé empêche complètement la communication entre les périphériques sur le VLAN secondaire. Il ne peut y avoir qu'un seul VLAN isolé par VLAN principal et seuls les ports proches peuvent communiquer avec les ports d'un VLAN isolé. Les VLAN isolés peuvent être utilisés sur des réseaux non fiables, tels que les réseaux qui prennent en charge les invités.

Cet exemple de configuration configure le VLAN 11 en tant que VLAN isolé et l’associe au VLAN principal, le VLAN 20. Cet exemple configure également l’interface FastEthernet 1/1 en tant que port isolé sur 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 configuré en tant que VLAN de communauté permet la communication entre les membres du VLAN et avec tous les ports proches du VLAN principal. Cependant, aucune communication n'est possible entre deux VLAN de communauté ou entre un VLAN de communauté et un VLAN isolé. Les VLAN de communauté doivent être utilisés pour regrouper les serveurs qui ont besoin d'une connectivité entre eux, mais où la connectivité à tous les autres périphériques sur le VLAN n'est pas requise. Ce scénario est courant sur un réseau accessible publiquement ou partout où les serveurs fournissent du contenu à des clients non approuvés.

Cet exemple configure un VLAN de communauté unique et configure le port de commutateur FastEthernet 1/2 en tant que membre de ce VLAN. Le VLAN de communauté, VLAN 12, est un VLAN secondaire par rapport au 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 de proximité

Les ports de commutateur placés dans le VLAN principal sont appelés ports proches. Les ports

proches peuvent communiquer avec tous les autres ports des VLAN principal et secondaire. Les interfaces de routeur ou de pare-feu sont les périphériques les plus courants sur ces VLAN.

Cet exemple de configuration combine les exemples de VLAN isolés et de communauté précédents et ajoute la configuration de l'interface FastEthernet 1/12 en tant que 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
!
```

Lorsque vous implémentez des PVLAN, il est important de s'assurer que la configuration de couche 3 en place prend en charge les restrictions imposées par les PVLAN et ne permet pas à la configuration PVLAN d'être subvertie. Un filtre de couche 3 avec une ACL de routeur ou un pare-feu peut empêcher la subversion de la configuration PVLAN.

Référez-vous à VLAN privés (PVLANs) - Promiscuous, Isolated, Community, situé sur la page d'accueil de LAN Security, pour plus d'informations sur l'utilisation et la configuration des VLAN privés.

Conclusion

Ce document vous donne une large vue d'ensemble des méthodes qui peuvent être utilisées pour sécuriser un périphérique système Cisco IOS. Si vous sécurisez les périphériques, cela augmente la sécurité globale des réseaux que vous gérez. Dans cette présentation, la protection des plans de gestion, de contrôle et de données est abordée, et des recommandations de configuration sont fournies. Dans la mesure du possible, des détails suffisants sont fournis 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 plus approfondie.

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 toutes les étapes de durcissement des périphériques présentées dans ce 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
    - Configurer le filtrage des 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)
    - Avertir à l'aide 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
    - Utiliser AAA à des fins de compte
    - Utilisation des serveurs AAA redondants
- SNMP
    - Configuration des communautés SNMPv2 et application des ACL
    - Configuration de SNMPv3
- Journalisation
    - Configurer les journaux centralisés
    - Définition des niveaux de journalisation pour tous les composants concernés
    - Set log source-interface
    - Configurer la granularité des horodatages du journal
- Gestion de la configuration
    - Remplacer et restaurer
    - Accès exclusif aux modifications de configuration
    - Configuration de la résilience logicielle
    - Configuration des notifications de changement

Plan de contrôle

- Désactiver (tenir compte des risques)
    - Redirections ICMP
    - Messages ICMP inaccessibles
    - Proxy ARP
- Configurez l'authentification NTP si NTP doit être utilisé
- Configurer la protection/la réglementation du plan de contrôle (filtres de port, seuils de 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, filtres de route, consommation de 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)
    - Routes 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 ARP dynamique
    - 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.