Amélioration de la sécurité sur les gammes CSS 11000 et CSS 11500

Contenu

Introduction
Conditions préalables
Conditions requises
Composants utilisés
Conventions
Gestion des mots de passe
Profils d'utilisateur local
Contrôle d'accès interactif
Ports de console
Accès interactif général
Contrôle de console Access
Contrôle de VTYs
Prise en charge de la fonctionnalité SSH
RAYON
TACACS+
Messages d'avertissement
Services de supervision généralement configurés
SNMP
HTTP
HTTPS
Gestion et accès interactif au-dessus de l'Internet (et d'autres réseaux non approuvés)
Analyseurs de paquets
D'autres dangers d'accès à l'Internet
Se connecter
Sauvegardez les informations de log
Enregistrez les violations de liste d'accès
Sécurisez le Routage IP
Antispoofing
Antispoofing avec ACLs
Contrôle des diffusions dirigées
Intégrité du chemin
Acheminement de source IP
Redirections ICMP
Filtrage et authentification de protocole de routage
Gestion d'inondation
Inondations de transit

Services probablement inutiles
SNTP
Cisco Discovery Protocol
Séjour à jour
Informations connexes

Introduction

Ce document fournit des informations au sujet des paramètres de configuration de Cisco qui peuvent améliorer la Sécurité sur le Commutateur de services de contenu (CSS) 11000 de Cisco ou CSS 11500. Ce document décrit les configurations de configuration de base qui s'appliquent presque universellement dans les réseaux IP et couvre quelques éléments inattendus dont vous devez se rendre compte.

Ce document ne présente pas une liste exhaustive de ces éléments, ni peuvent les informations dans le document être substituées à la connaissance de la part de l'administrateur réseau. Le document sert de rappel des éléments qui sont parfois oubliés.

Ce document mentionne seulement les commandes qui sont importantes dans les réseaux IP. Beaucoup des services que vous pouvez activer sur le CSS exigent la configuration soigneuse de la sécurité. Cependant, ce document se concentre sur les informations pour des services qui sont activés par défaut ou qui sont presque toujours activés par des utilisateurs et qui peut exiger la désactivation ou la reconfiguration.

Certaines des valeurs par défaut en logiciel de Cisco WebNS existent pour des raisons historiques. Ces configurations s'appliquaient quand elles ont été choisies, mais seraient probablement différentes si de nouveaux par défaut étaient choisis aujourd'hui. D'autres par défaut s'appliquent pour la plupart des systèmes, mais peuvent créer des risques contre la sécurité si ces par défaut sont utilisés dans des périphériques ces forment la défense de périmètre de partie du réseau. Encore d'autres par défaut sont exigés réellement par des normes, mais ne sont pas toujours desirables d'un point de vue de la sécurité.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Gestion des mots de passe

Les mots de passe et l'information propriétaire semblable, telle que des chaînes de la communauté de Protocole SNMP (Simple Network Management Protocol), sont la défense principale contre l'accès non autorisé à votre CSS. La meilleure manière de manipuler la plupart des mots de passe est de les mettre à jour sur un TACACS+ ou un serveur d'authentification RADIUS. Cependant, presque chaque CSS a toujours un mot de passe localement configuré pour l'accès privilégié. Le CSS peut également inclure d'autres informations de mot de passe dans le fichier de configuration. N'importe quel mot de passe qui est configuré en texte clair apparaît dans la configuration chiffrée avec le Norme de chiffrement de données (DES).

Profils d'utilisateur local

Cette liste décrit les profils d'utilisateur local :

- *Administrateur* — Le profil Administrateur inclut ces privilèges :Access au menu hors ligne de moniteur de diagnosticsAccès complet à la ligne de commandePlein accès de répertoireCes configurations peuvent être configurées de la ligne de commande ou du menu hors ligne de moniteur de diagnostics.
- *Technicien* — Le profil de technicien inclut ces privilèges :Accès complet à la ligne de commandePlein accès de répertoireCes configurations peuvent être configurées avec l'utilisation de la ligne de commande. N'utilisez pas le profil de technicien pour le CSS administratif.
- *Super utilisateur* — Le profil de super utilisateur inclut ces privilèges :Accès complet à la ligne de commandeLa capacité de sauvegarder des restrictions d'accès de répertoireCes configurations peuvent être configurées avec l'utilisation de la ligne de commande.
- *Utilisateur* — Le profil utilisateur ne peut pas apporter des modifications de configuration et inclut des restrictions d'accès de répertoire. Ces configurations peuvent être configurées avec l'utilisation de la ligne de commande.

Quand vous émettez la commande impliquant l'accès à la base de données de **limiter**, vous imposez des restrictions d'accès de répertoire sur chaque utilisateur. Les niveaux utilisateurs seulement d'administrateur et de technicien peuvent exécuter ces actions :

- Retirez la commande impliquant l'accès à la base de données de **limiter**.
- Changez la commande de **base de données locale des utilisateurs**.
- Émettez la commande **claire de running-config**.

Contrôle d'accès interactif

N'importe quel utilisateur qui peut ouvrir une session à un CSS peut afficher les informations que le grand public n'a pas besoin nécessairement de visualiser. Dans certains cas, un utilisateur qui peut ouvrir une session au CSS peut utiliser le CSS comme relais pour des futures attaques du réseau. Un utilisateur qui gagne l'accès privilégié au CSS peut modifier le CSS. Afin d'empêcher l'accès inapproprié, vous devez contrôler des procédures de connexion interactive au CSS.

Bien que la plupart d'accès interactif soit désactivé par défaut, il y a des exceptions. Les exceptions les plus évidentes sont des sessions interactives des terminaux asynchrones directement connectés, tels que la console, et accès au port de gestion Ethernet.

Référez-vous à configurer des méthodes d'Accès à distance CSS pour plus d'informations sur la façon contrôler l'accès interactif au CSS.

Ports de console

Un important élément à se souvenir est que le port de console d'un périphérique de Cisco a des privilèges spéciaux. En particulier, supposez que quelqu'un envoie un caractère d'ESC (évasion) au port de console quand le passage de diagnostics de POST. Après qu'une réinitialisation, cette personne puisse facilement employer la procédure de récupération de mot de passe afin de prendre le contrôle du système. Les attaquants qui peuvent interrompre l'alimentation ou induisent un blocage système, et qui ont accès au port de console par un terminal câblé, un modem, un serveur de terminaux, ou un autre périphérique de réseau, peuvent prendre le contrôle du système. Ces attaquants peuvent prendre le contrôle même si ils n'ont pas accès physique au système ou à la capacité d'ouvrir une session au système normalement.

Par conséquent, n'importe quel modem ou périphérique de réseau qui donnent l'accès au port de console Cisco doit être sécurisé à une norme qui est comparable à la Sécurité qui est utilisée pour l'accès privilégié au CSS. Au minimum, n'importe quel modem de console doit être d'un type qui peut exiger de l'utilisateur de connexion téléphonique de fournir un mot de passe pour l'accès, et le mot de passe du modem doit être soigneusement géré.

Accès interactif général

Il y a plus de manières d'obtenir les connexions interactives à un CSS que des utilisateurs peut réaliser. Vous pouvez employer ces méthodes afin de gérer le CSS :

- Telnet
- Hôte sécurisé de shell (SSH)
- SNMP
- Console
- FTP
- XML
- Gestion de Web

Émettez la commande de **limiter** afin d'activer ou désactiver. Le CSS écoute toujours sur le port particulier, mais ferme la connexion. De sorte que les paquets ne frappent pas ces ports, configurez les clauses de liste de contrôle d'accès (ACL) pour refuser les paquets.

Il est difficile d'être certain que tous les modes possibles de l'accès aient été bloqués. Dans la plupart des cas, les administrateurs doivent employer un certain tri de mécanisme d'authentification afin de s'assurer que les procédures de connexion sur toutes les lignes sont commandées. Les administrateurs doivent s'assurer que les procédures de connexion sont contrôlées même sur les ordinateurs qui sont censés être inaccessibles des réseaux non approuvés.

Contrôle de console Access

Par défaut, la console authentifie contre des profils utilisateurs localement configurés. Afin de lancer l'authentification TACACS+ ou de RAYON, émettez la commande globale d'**authentification de console** et les options associées.

Contrôle de VTYs

Par défaut, les vtys authentifient contre des profils utilisateurs localement configurés. Afin de

lancer l'authentification TACACS+ ou de RAYON, émettez la commande globale **virtuelle d'authentification** et les options associées.

Prise en charge de la fonctionnalité SSH

Si vos supports logiciels un protocole d'accès chiffré tel que le SSH, Cisco recommande que vous activiez seulement ce protocole et désactivez l'accès de telnet quand vous voulez utiliser le serveur de SSH. Afin d'activer le démon de SSH (SSHD), vous avez besoin d'un permis de serveur SSHD, qui active la fonctionnalité SSHD sur le niveau et des versions améliorées de logiciel CSS. Émettez les commandes de **sshd**. Référez-vous à configurer le pour en savoir plus de protocoles réseau CSS.

Remarque: Support de la version SSH 1 commencé en 4.01. Support de la version SSH 2 commencé en 5.20.

RAYON

En date de la version 5.00 et ultérieures, vous pouvez configurer le CSS pour utiliser le RAYON pour l'authentification d'utilisateur. Afin de configurer le CSS pour l'authentification de RAYON, référez-vous à configurer des profils utilisateurs et des paramètres CSS.

Remarque: Un profil d'utilisateur/groupe exige seulement des attributs RADIUS de l'Internet Engineering Task Force (IETF), type de service [006] = administratif.

Cette liste identifie les codes de message de débogage :

```
PW_ACCESS_REQUEST       1
PW_ACCESS_ACCEPT        2
PW_ACCESS_REJECT        3
PW_ACCOUNTING_REQUEST   4
PW_ACCOUNTING_RESPONSE  5
PW_ACCOUNTING_STATUS    6
PW_ACCESS_CHALLENGE     11
```

Afin de visualiser met au point qui sont associés avec des procédures de connexion de RAYON, émettent ces commandes :

```
logging subsystem radius level debug-7
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

C'est un exemple d'une authentification réussie mettent au point :

```
logging subsystem radius level debug-7
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

C'est un exemple d'une authentification qui a manqué en raison d'un nom d'utilisateur ou d'un mot de passe incorrect :

```
logging subsystem radius level debug-7
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

C'est un exemple d'une authentification qui a manqué parce que le type de service de l'attribut RADIUS 006 de profil d'utilisateur n'est pas configuré :

```
logging subsystem radius level debug-7
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

TACACS+

Dans la version 5.03 et ultérieures, vous pouvez configurer le CSS pour utiliser TACACS+ pour l'authentification d'utilisateur. Afin de configurer le CSS pour l'authentification TACACS+, référez-vous aux notes en version pour la gamme 11000 CSS.

Afin de visualiser met au point qui sont associés avec des procédures de connexion TACACS+, émettent ces commandes :

```
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

C'est un exemple d'une authentification réussie mettent au point :

```
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

C'est un exemple d'une authentification défaillante en raison d'un nom d'utilisateur ou d'un mot de passe incorrect :

```
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

Messages d'avertissement

Dans quelques juridictions, vous pouvez considérablement soulager le processus de civil et/ou la poursuite pénale des casseurs qui divisent en vos systèmes si vous fournissez une bannière qui informe des utilisateurs non autorisés que leur utilisation est non autorisée. D'autres juridictions interdisent le moniteur des activités même des utilisateurs non autorisés à moins que vous ayez pris des mesures pour informer des utilisateurs de votre intention de faire ainsi. Une manière de donner cette notification est de la mettre dans un message de bannière. Vous pouvez configurer un message de bannière avec la commande **réglée de bannière** CSS. Cette commande a été introduite en 5.03.

Les exigences de notification légale sont complexes et varient dans chaque juridiction et situation. Même dans des juridictions, les avis juridiques varient. Discutez cette question avec votre conseiller juridique. En coopération avec l'avocat-conseil, considérez qui de ces notices de mettre dans votre bannière :

- Un avis que spécifiquement le personnel autorisé d'états seulement doivent ouvrir une session à ou utiliser le système et peut-être les informations sur qui peut autoriser l'utilisation.
- Un avis que n'importe quelle utilisation non autorisée du système est illégale et peut être sujette à des pénalités civiles et/ou criminelles.
- Un avis que n'importe quelle utilisation du système peut sont enregistré ou ont surveillé sans préavis et que les logs en résultant peuvent être utilisés comme preuves devant le tribunal.
- Notices spécifiques qui sont exigées par des lois locales.

Pour des raisons de Sécurité (plutôt que juridique), n'incluez pas dans votre bannière de procédure de connexion ces informations sur votre CSS :

- Nom
- Modèle
- Logiciel qui fonctionne
- Propriétaire

Services de supervision généralement configurés

Beaucoup d'utilisateurs gèrent leurs réseaux avec l'utilisation des protocoles autres que la procédure de connexion à distance interactive. Les protocoles les plus communs sont à cet effet SNMP et HTTP. Les la plupart option sécurisée ne sont pas d'activer ces protocoles du tout. Cependant, si vous avez activé un des protocoles, sécurisez-le comme cette section décrit.

SNMP

Le SNMP est très très utilisé pour le périphérique de réseau surveillant et, fréquemment, pour des modifications de configuration. Le SNMP a deux révisions standard importantes, SNMPv1 et SNMPv2. Votre CSS prend en charge la version 2C SNMP (SNMPv2C), qui est connue en tant que SNMP à caractère communautaire. Le CSS génère des déroutements dans le format SNMPv1.

Afin de contrôler l'accès SNMP au CSS, émettez l'**aucun limitent la** commande **SNMP** et la commande **SNMP de limiter**. Access par le SNMP est activé par défaut. Si vous désactivez l'accès par le SNMP, le CSS écoute toujours sur le port particulier 1, mais ferme la connexion. Configurez les clauses d'ACL pour refuser les paquets de sorte que les paquets ne frappent pas le port SNMP.

Malheureusement, SNMPv1 et SNMPv2C utilisent un schéma d'authentification très faible qui est basé sur une chaîne de la communauté. L'authentification s'élève à un mot de passe fixe qui est transmis au-dessus du réseau sans cryptage. Si vous devez utiliser le SNMPv2C, faites attention à choisir les chaînes obscures de la communauté (et n'utilisez pas, par exemple, public ou privé). Si à tout le possible, évitez l'utilisation des mêmes chaînes de la communauté pour tous les périphériques de réseau. Utilisez une différente chaîne ou chaînes pour chaque périphérique, ou au moins pour chaque zone du réseau. Ne faites pas à une chaîne en lecture seule les mêmes qu'une chaîne en lecture/écriture. Si possible, faites le SNMPv2C périodique votant avec une chaîne de caractères de la communauté en lecture seule. Les chaînes en lecture/écriture d'utilisation seulement pour l'effectif écrivent des exécutions.

Il n'est pas approprié l'utiliser SNMPv2C à travers l'Internet public pour ces raisons :

- Chaînes d'authentification en texte en clair d'utilisations de SNMPv2C.
- Le SNMPv2C est un protocole de transaction basé sur des datagrammes qui est facilement charrié.
- La plupart des réalisations SNMP envoient ces chaînes à plusieurs reprises en tant qu'élément de l'interrogation périodique.

Considérez soigneusement les implications avant que vous utilisiez le SNMPv2C à travers l'Internet public.

Dans la plupart des réseaux, les messages SNMP légitimes proviennent seulement des certaine station de gestion. Si les messages SNMP légitimes proviennent seulement les certaine station de gestion dans votre réseau, considérez l'utilisation d'ACLs qui sont appliqués aux VLAN de circuit

afin de refuser les messages SNMP non désirés.

Les stations de gestion SNMP ont souvent de grandes bases de données des informations d'authentification, telles que des chaînes de la communauté. Ces informations peuvent permettre d'accéder à beaucoup de CSS et à d'autres périphériques de réseau. Cette concentration des informations incite la gestion SNMP à poster une cible naturelle pour l'attaque. Sécurisez la station de gestion SNMP en conséquence.

HTTP

Le CSS prend en charge la configuration distante par l'intermédiaire du protocole HTTP avec l'utilisation des documents de langage extensible de balisage (XML). Dans la version 4.10 ou antérieures de WebNS, vous pouvez atteindre l'accès aux interfaces utilisateur de Gestion de périphériques de WebNS en texte clair si vous parcourez au port 8081 de TCP. Généralement l'accès HTTP est équivalent à l'accès interactif au CSS. Le protocole d'authentification qui est utilisé pour le HTTP est équivalent à l'envoi d'un mot de passe de libellé à travers le réseau. Malheureusement, il n'y a aucune disposition efficace dans le HTTP pour des mots de passe basés sur défi ou une fois. Par conséquent, le HTTP est un choix relativement risqué pour l'usage à travers l'Internet public.

Si vous choisissez d'utiliser le HTTP pour la Gestion, limitez l'accès aux adresses IP appropriées avec l'utilisation d'ACLs qui sont appliquées aux VLAN de circuit. Afin de contrôler l'accès du HTTP XML au CSS, émettez l'**aucun limitent la** commande de **xml** et la commande de **xml de limiter**. Dans les versions ultérieures de WebNS, la commande a changé à l'**état de Web-mgt** *[débronchement | enable]*. Accédez à par le HTTP XML est désactivé par défaut. Afin de contrôler l'accès client de Gestion de périphériques de WebNS de HTTP, émettez l'**aucun limitent la** commande de **Web-gestion** et la commande de **Web-gestion de limiter**. L'interface utilisateur de Gestion de périphériques de WebNS est désactivée par défaut. Vous devez configurer l'**aucun limitez la** commande de **xml** et l'**aucun limite la** commande de **Web-gestion** afin de parcourir au CSS sur le port 8081.

Dans la version 5.00 et ultérieures, si vous HTTP-parcourez à l'adresse de circuit sur le port 8081, le programme de lecture est réorienté pour utiliser HTTPS et pour se connecter à la même adresse de circuit.

HTTPS

La configuration distante de supports CSS par le protocole sécurisé de HTTP (HTTPS). Ce Protocole SSL (Secure Socket Layer) protège les transferts des données (qui peuvent inclure des mots de passe) entre l'interface utilisateur de Gestion de périphériques de WebNS et votre navigateur Web.

Afin de contrôler l'accès client de Gestion de périphériques HTTPS WebNS, émettez l'**aucun limitent la** commande de **Web-gestion** et la commande de **Web-gestion de limiter**. L'interface utilisateur de Gestion de périphériques de WebNS est désactivée par défaut. S'il est désactivé, le CSS continue à écouter sur le port particulier mais ferme la connexion. De sorte que les paquets ne frappent pas le port TCP 443 SSL, configurez les clauses d'ACL pour refuser les paquets.

Gestion et accès interactif au-dessus de l'Internet (et d'autres réseaux non approuvés)

Beaucoup d'utilisateurs gèrent leurs CSS à distance, et parfois ce fait au-dessus de l'Internet. N'importe quel accès à distance non chiffré comporte un certain risque, mais l'accès au-dessus d'un réseau public tel que l'Internet est particulièrement dangereux. Tous les modèles de gestion à distance, qui incluent l'accès interactif, le HTTP, et le SNMP, sont vulnérables.

Les attaques que cette section discute sont relativement les sophistiquées, mais elles sont nullement hors d'atteinte des casseurs d'aujourd'hui. Les fournisseurs de services réseau publics qui prennent les mesures de sécurité appropriées peuvent souvent contrecarrer ces attaquants. Évaluez votre niveau de confiance dans les mesures de sécurité qui tous les fournisseurs qui portent votre utilisation du trafic d'administration. Même si vous faites confiance à vos fournisseurs, prise au moins quelques étapes pour se protéger contre les résultats de toutes erreurs que ces fournisseurs pourraient faire.

Toutes les attentions dans cette section appliquent autant aux hôtes quant au CSS. Tandis que ce document discute comment se protéger les sessions d'ouverture de connexion CSS, examinent également l'utilisation des mécanismes analogues afin de protéger vos hôtes si vous gérez ces hôtes à distance. L'administration à distance par Internet est utile, mais il exige une attention particulière à la Sécurité.

Analyseurs de paquets

Les casseurs divisent fréquemment en ordinateurs que les fournisseurs d'accès Internet possèdent, ou en ordinateurs sur d'autres grands réseaux. Les casseurs installent les programmes d'analyseur de paquets, qui surveillent le trafic qui traverse le réseau. Ces programmes d'analyseur de paquets dérobent des données, telles que des mots de passe et des chaînes de caractères de la communauté SNMP. Les opérateurs réseau ont commencé à améliorer leur Sécurité, qui rend ce vol plus difficile. Cependant, ce vol est toujours relativement commun. En plus du risque des pirates de l'extérieur, le personnel d'un ISP peu scrupuleux peut également installer des renifleurs. N'importe quel mot de passe qui est envoyé au-dessus d'un canal non chiffré est en danger, qui inclut les mots de passe de procédure de connexion et d'enable pour vos CSS.

Si vous pouvez, éviter de se connecter dans votre CSS avec l'utilisation de tout protocole non chiffré au-dessus de tout réseau non approuvé. Si votre logiciel CSS le prend en charge, utilisez un protocole chiffré de procédure de connexion tel que le SSH.

Si vous n'avez pas accès à un protocole d'Accès à distance chiffré, une autre possibilité est d'utiliser un système de mot de passe à usage unique tel que S/KEY ou OPIE, ainsi qu'un serveur TACACS+ ou de RAYON, afin de contrôler des procédures de connexion interactive et l'accès privilégié à votre CSS. L'avantage est qu'un mot de passe dérobé est inutile. Un mot de passe dérobé est rendu non valide par la session même dans laquelle il est dérobé. Des données qui sont transmises en session et non associé aux mots de passe restez disponible aux oreilles indiscrètes, mais beaucoup de programmes de renifleur sont installés pour se concentrer sur des mots de passe.

Si vous devez envoyer des mots de passe au-dessus des sessions de telnet de libellé, changez vos mots de passe fréquemment. et grande attention de paiement au chemin que vos sessions traversent.

D'autres dangers d'accès à l'Internet

En plus des analyseurs de paquets, la gestion d'Internet distante d'un CSS présente ces risques

de sécurité :

- Afin de gérer un CSS au-dessus de l'Internet, vous devez permettre au moins à quelques hôtes d'Internet pour avoir accès au CSS. Ces hôtes peuvent être compromis, ou leurs adresses peuvent être charriées. Quand vous permettez l'accès interactif de l'Internet, vous faites votre personne à charge de Sécurité, non seulement sur vos propres mesures antispoofing, mais sur les mesures antispoofing des fournisseurs de services qui sont impliqués.Vous pouvez réduire ces dangers si vous exécutez ces actions :Assurez-vous que tous les hôtes qui sont permis pour ouvrir une session à votre CSS sont sous votre propre contrôle.Protocoles de procédure de connexion chiffrés par utilisation avec l'authentification poussée.
- Parfois, l'accès à une connexion TCP décryptée (telle qu'une session de telnet) est possible pour obtenir. Quelqu'un qui obtient l'accès à ce type de session peut réellement prendre le contrôle à partir d'un utilisateur qui est ouvert une session. De telles attaques ne sont pas presque aussi communes que le paquet simple reniflant et peuvent être complexes pour monter. Cependant, de telles attaques sont possibles, et un attaquant qui a votre réseau spécifiquement à l'esprit pendant qu'une cible peut les utiliser. La seule véritable solution au problème du vol de session est d'utiliser un protocole de gestion fortement authentifié et chiffré.
- Les attaques du déni de service (DOS) sont relativement communes sur l'Internet. Si votre réseau est soumis à une attaque DoS, vous pouvez ne pouvoir pas atteindre votre CSS afin de collecter des informations ou prendre une mesure défensive. Même une attaque sur le réseau de quelqu'un d'autre peut altérer l'accès de Gestion à votre propre réseau. Bien que vous puissiez prendre des mesures pour rendre votre réseau plus résistant aux attaques DoS, la seule véritable défense contre ce risque est d'avoir un distinct, canal de gestion hors bande (tel qu'un modem commuté) pour l'usage dans les urgences.

Se connecter

Les Cisco CSS peuvent des informations sur les enregistrements au sujet d'un grand choix d'événements, beaucoup dont ayez la signification en matière de sécurité. Les logs peuvent être inestimables pour la caractérisation et la réponse aux incidents de sécurité. Vous pouvez émettre la commande de **sous-système se connectante** afin d'activer ouvre une session le CSS. Le niveau se connectant par défaut est warning-4 pour tous les sous-systèmes.

Émettez ces commandes pour que la commande logging on de sous-système collecte ces informations :

- Ouvertures de session utilisateur
- Déconnexions
- Authentification RADIUS
- Authentification TACACS+

```
logging subsystem radius level debug-7
logging subsystem security level debug-7
logging subsystem netman level debug-7
```

Remarque: Les couvertures TACACS+ de commande de **sous-système de netman** met au point.

D'un point de vue de la sécurité, les événements les plus importants que la journalisation système

enregistre habituellement incluent ces événements :

- Changements d'état d'interface
- Modifications à la configuration de système
- Correspondances d'ACL

```
logging subsystem netman level info-6
!--- Note that the default logging level is warning-4, which does !--- not appear in the
configuration. logging commands enable
logging subsystem acl level debug-7
```

Le Surveillance à distance (RMON) vous permet à distance surveillent et analysent l'activité des paquets sur des ports Ethernet CSS. Le RMON également permet la configuration d'alarme pour le moniteur des objets MIB et permet à la configuration d'événement pour vous informer de ces conditions d'alarme. Un événement de RMON est l'action qui se produit quand une alarme associée de RMON est déclenchée. Vous pouvez configurer un événement d'alarme tels que, quand un événement d'alarme se produit, il génère un ou chacun des deux éléments :

- Un événement de log
- Un déroutement à une station de Gestion de réseau SNMP

Sauvegardez les informations de log

Par défaut, le CSS enregistre des messages de journal d'événements de démarrage et de sous-système aux fichiers journal sur le dur ou le disque Flash. Le contenu de ces fichiers est enregistré en texte ASCII. Vous pouvez également configurer le CSS pour envoyer des messages de log à une session active CSS, à une adresse e-mail, ou à un système hôte différent.

La taille maximale d'un fichier journal local est 50 Mo pour les systèmes à disques durs et 10 Mo pour les systèmes à disques instantanés.

Les messages de log de sous-système sont des événements de sous-système qui se produisent pendant l'exécution du CSS. Le CSS enregistre ces messages dans le fichier de sys.log. Le CSS crée ce fichier quand le premier événement de sous-système se produit qui doit sont enregistré. Le CSS détermine quels messages de sous-système à se connecter par son se connecter configuré de niveau.

La plupart des installations plus grandes ont des serveurs de Syslog. Vous pouvez émettre la commande d'**hôte de journalisation** afin d'envoyer les informations de journalisation à un démon de Syslog sur le système hôte. Même si vous avez un serveur de Syslog, vous devriez encore activer des gens du pays se connectant au disque.

Tous les logs sont horodatés avec le mois, jour, et chronomètrent au deuxième. Si vous configurez une source temporelle commune telle que le protocole de diffusion du temps en réseau (SNTP) (SNTP) pour vos logs, vous pouvez plus facilement dépister l'ordre des événements loggés. Afin de configurer le sntp server sur le CSS, émettez la commande de **sntp**. SNTP a été introduit en code 5.00.

Enregistrez les violations de liste d'accès

Si vous employez ACLs pour filtrer le trafic qui accède à des adresses de circuit ou des adresses virtuelles IP de règle de contenu (VIP), vous pouvez choisir de se connecter les paquets qui

violent vos critères de filtre. Afin d'activer ouvrir une session la clause d'ACL, émettez la **clause # la** commande d'**enable de log**. En outre, émettez la commande **se connectante du niveau debug-7 d'acl de sous-système**. Le CSS se connecte ces informations :

- Protocol
- Port de source
- Destination port
- adresse IP source
- adresse IP de destination

Essayez d'éviter la configuration de se connecter pour les rubriques de liste ACL qui apparient très un grand nombre de paquets. Cette configuration fait développer des fichiers journal excessivement grands et peut couper en performance du système.

Vous pouvez également utiliser l'ACL se connectant pour caractériser le trafic qui est associé avec des attaques réseau. Dans ce cas, vous configurez l'ACL se connectant pour se connecter le trafic suspect. Vous pouvez caractériser sur le routeur de Cisco du côté d'Internet du CSS afin d'ouvrer un ACL. Référez-vous à la caractérisation et aux inondations de paquets de découverte utilisant le pour en savoir plus de Routeurs de Cisco.

Remarque: CSS ACLs sont seulement appliqués sur des paquets entrant. L'ACL ne vérifie pas les paquets qui sont sortants d'une interface.

Sécurisez le Routage IP

Cette section discute quelques mesures de sécurité de base qui associent à la manière dans laquelle de routeur les paquets IP en avant. Référez-vous au Cisco ISP Essentials - L'IOS essentiel comporte chaque ISP devrait considérer pour plus d'informations sur ces questions.

Par défaut, une configuration du CSS :

- Limite le nombre de paquets de synchronisation qui vont à un VIP avant que le CSS se connecte les comme attaque DoS**Remarque:** Ce comportement ne peut pas être désactivé.
- Refuse des diffusions dirigées
- Refuse des paquets avec la mêmes source et adresse IP de destination
- Refuse des adresses IP de source multicast
- Refuse la source ou la destination port 0 paquets

Antispoofing

Beaucoup d'attaques réseau se fondent sur un attaquant qui le falsifie, ou charrie, les adresses sources des datagrammes IP. Quelques attaques se fondent sur la mystification pour que l'attaque fonctionne. Il est beaucoup plus difficile de tracer d'autres attaques si les attaquants peuvent utiliser l'adresse de quelqu'un d'autre au lieu de leur propre adresse. Par conséquent, empêcher charrier partout où il est faisable est valeur pour des administrateurs réseau.

Antispoofing devrait être fait à chaque point dans le réseau où il est pratique. Mais il est habituellement le plus facile faire antispoofing et le plus efficace aux cadres entre de grands blocs d'adresses ou entre les domaines de l'administration réseau. Antispoofing sur chaque routeur dans un réseau est habituellement irréaliste parce que la détermination dont les adresses sources peuvent légitimement apparaître sur n'importe quelle interface donnée est difficile.

Si vous êtes un fournisseur de services Internet (ISP), vous pouvez constater qu'efficace antispoofing, ainsi que d'autres mesures de sécurité efficaces, des causes chères, des abonnés de problème de prendre leur entreprise à d'autres fournisseurs. Si vous êtes un ISP, faites attention particulièrement à appliquer des contrôles antispoofing aux groupes commutés et à d'autres points de connexion d'utilisateur.

Remarque: Référez-vous à RFC 2267 .

Les administrateurs de pare-feu d'entreprise ou les Routeurs de périmètre installent parfois des mesures antispoofing de sorte que les hôtes sur l'Internet ne puissent pas assumer les adresses des hôtes internes. Cependant, les hôtes internes peuvent encore assumer les adresses du hôte sur l'Internet. Essayez d'empêcher charrier dans les deux directions. Il y a au moins trois bonnes raisons d'installer antispoofing dans les deux directions à un pare-feu d'organisation :

- Des utilisateurs internes moins sont tentés pour essayer de lancer des attaques réseau et moins probable pour réussir s'ils essayent.
- Les hôtes internes qui misconfigured accidentellement sont moins pour entraîner le problème pour des sites distants. Par conséquent, ils sont moins pour générer le mécontentement de client.
- Les pirates de l'extérieur divisent souvent en réseaux en tant que lancer des protections pour des futures attaques. Ces casseurs peuvent être moins intéressés par un réseau avec la protection contre l'usurpation du trafic sortant.

Antispoofing avec ACLs

Malheureusement, pour répertorier simplement les commandes qui fournissent la protection appropriée contre l'usurpation n'est pas pratique. La configuration d'ACL dépend trop du réseau individuel. L'objectif de base est de jeter les paquets qui arrivent sur les interfaces qui ne sont pas les chemins viables des adresses sources supposées de ces paquets. Par exemple, sur un deux-circuit CSS qui connecte une batterie de serveur à l'Internet, vous voulez jeter n'importe quel datagramme qui arrive sur le circuit d'Internet, mais avez une zone adresse d'adresse source qui réclame qu'elle est provenue un ordinateur sur la batterie de serveur.

De même, vous voulez jeter n'importe quel datagramme qui arrive sur l'interface qui est connectée à la batterie de serveur, mais qui a une zone adresse d'adresse source qui réclame qu'elle est provenue un ordinateur en dehors de la batterie de serveur. Si les ressources CPU laissent, appliquez antispoofing sur n'importe quel circuit où une détermination quel trafic peut légitimement arriver est faisable.

Les ISP qui portent le trafic de transit peuvent avoir limité des occasions de configurer ACLs antispoofing, mais de tels ISP peuvent habituellement filtrer le trafic extérieur ce des prétendre de commencer dans l'espace d'adressage de cet ISP.

Des filtres antispoofing généralement doivent être construits avec des ACLs en entrée. Des paquets doivent être filtrés aux circuits par lesquels les paquets arrivent. Le CSS peut seulement appliquer ACLs aux paquets entrant.

Antispoofing ACLs existez, ils devraient toujours rejeter des datagrammes avec l'émission ou les adresses sources multicasts. Par défaut, le CSS refuse ces datagrammes. Antispoofing ACLs devrait également rejeter les datagrammes qui ont l'adresse de bouclage réservée comme adresse source. En outre, vous devriez habituellement avoir un filtre d'ACL antispoofing que tout le Protocole ICMP (Internet Control Message Protocol) réoriente, indépendamment de l'adresse

source ou de destination. L'ACL CSS ne te permet pas pour spécifier le type ICMP pour refuser. Au lieu de cela, émettez l'**aucun réoriente la** commande afin de configurer toutes les adresses IP de circuit pour ne pas recevoir l'ICMP réoriente. Ce sont les commandes :

```
clause # deny any 127.0.0.0 255.0.0.0 destination any
clause # deny any 0.0.0.0 0.0.0.0 destination any
```

Remarque: La clause # refusent n'importe quelle destination de 0.0.0.0 0.0.0.0 que n'importe quelle commande filtre des paquets de beaucoup de clients de protocole bootstrap (Protocole BOOTP) /DHCP. Par conséquent, la commande n'est pas appropriée dans tous les environnements.

Contrôle des diffusions dirigées

Attaques DoS extrêmement communes et populaires de smurf, et quelques attaques relatives, diffusions dirigées IP d'utilisation. Par défaut, le CSS est configuré avec l'**aucune** commande de **diffusion de sous-réseau d'IP**, qui refuse des diffusions dirigées.

Une diffusion dirigée IP est un datagramme qui est envoyé à l'adresse d'émission d'un sous-réseau auquel l'ordinateur expéditeur n'est pas directement relié. La diffusion dirigée est conduite par le réseau comme paquet monodiffusion jusqu'à ce que la diffusion dirigée arrive au sous-réseau cible. Au sous-réseau, la diffusion dirigée est convertie en émission de couche de liaison. En raison de la nature de l'architecture d'adressage IP, seulement le dernier routeur ou périphérique réseau de la couche 3 dans la chaîne peut d'une manière concluante identifier une diffusion dirigée. Ce périphérique est celui qui est connecté directement au sous-réseau cible. Les diffusions dirigées sont parfois utilisées pour des raisons légitimes, mais une telle utilisation n'est pas courante en dehors du secteur des services financiers.

Dans une attaque par rebond (« smurf »), l'attaquant envoie des demandes d'écho ICMP à partir d'une adresse source falsifiée à une adresse de diffusion dirigée. En conséquence, tous les hôtes sur le sous-réseau cible envoient des réponses à la source falsifiée. Quand un attaquant envoie un flux continu de telles demandes, l'attaquant peut créer un flot beaucoup plus grand des réponses, qui peuvent complètement inonder l'hôte dont l'adresse est falsifiée.

Référez-vous au plus en retard dans les attaques par déni de service : Description et informations de « Smurfing » pour réduire des effets pour qu'une stratégie bloque des attaques smurf sur quelques Routeurs de Pare-feu (qui dépend de la conception de réseaux). Le document fournit également les informations générales sur l'attaque smurf.

Intégrité du chemin

Beaucoup d'attaques dépendent de la capacité d'influencer les chemins que les datagrammes prennent par le réseau. Si les casseurs contrôlent le routage, il y a une occasion qu'ils peuvent charrier l'adresse de l'ordinateur d'un autre utilisateur et avoir le trafic de retour envoyé à eux. Dans certains cas, les casseurs peuvent intercepter et lire les données qui sont destinées pour quelqu'un d'autre. Le routage peut également être perturbé purement pour le DOS.

Acheminement de source IP

Le protocole IP prend en charge les options de routage de source qui permettent à l'expéditeur d'un datagramme IP pour contrôler l'artère que le datagramme prend vers la destination finale, et généralement, l'artère que n'importe quelle réponse prend. Ces options sont rarement utilisées

pour des raisons légitimes dans les réseaux réels. Quelques réalisations plus anciennes IP ne traitent pas des paquets d'origine acheminés correctement. Quelqu'un peut envoyer des datagrammes avec des options de routage de source et, probablement, pour tomber en panne les ordinateurs qui exécutent ces réalisations.

Le CSS est configuré par défaut avec l'**aucune commande set d'ip source-route**. Le CSS jamais en avant un paquet IP qui porte une option de routage de source. Laissez la commande par défaut configurée à moins que vous sachiez que votre réseau a besoin du routage de source.

Redirections ICMP

Un ICMP réorientent le message demande à un noeud d'extrémité d'utiliser un routeur spécifique comme chemin à une destination particulière. Dans un réseau IP qui fonctionne correctement, un routeur envoie réoriente seulement aux hôtes sur les sous-réseaux locaux du routeur. Le noeud d'extrémité n'envoient jamais une réorientation, et la réorientent ne traverse jamais plus d'un saut de réseau. Cependant, un attaquant peut violer ces règles, et quelques attaques sont basées sur ces règles. Filtrez l'ICMP entrant réoriente aux interfaces d'entrée de n'importe quel routeur qui se trouve à un cadre entre les domaines administratifs. En outre, vous pouvez avoir tout ACL qui est appliqué du côté entrée d'une interface de routeur de Cisco filtrent tout l'ICMP réoriente. Ceci qui filtre n'entraîne aucune incidence opérationnelle dans un réseau qui est configuré correctement.

Ce type de filtrage empêche réorientent seulement les attaques que les attaquants distants lancent. En outre, les attaquants peuvent utiliser le problème significatif de cause de redirect to si l'hôte d'attaquant est directement connecté au même segment comme hôte qui est soumis aux attaques.

Par défaut, le CSS est configuré pour recevoir réoriente sur chaque adresse IP de circuit qui est configurée. Émettez l'**aucun réorientent la** commande sous l'adresse IP de circuit afin d'arrêter cette fonction.

Filtrage et authentification de protocole de routage

Si vous utilisez un protocole de routage dynamique qui prend en charge l'authentification, activez cette authentification. L'authentification empêche quelques attaques malveillantes sur l'infrastructure de routage et peut également aider à empêcher les dommages qui misconfigured les périphériques escrocs sur le réseau peuvent entraîner.

Pour les mêmes raisons, les fournisseurs de services et d'autres opérateurs de grands réseaux peuvent considérer l'utilisation du filtrage d'artère. Avec l'artère filtrant, les Routeurs de réseau ne reçoivent pas les informations de routage clairement incorrectes. Pour l'artère filtrant, utilisez le paramètre de **distribute-list** dans la commande. L'utilisation excessive du filtrage de route peut détruire les avantages du routage dynamique. Mais l'utilisation sélective aide souvent à empêcher de mauvais résultats. Par exemple, si vous employez un protocole de routage dynamique afin de communiquer avec un réseau client de stub, ne recevez aucune artère de ce client autre que des artères à l'espace d'adressage que vous avez délégué réellement au client.

Le CSS ne peut pas filtrer des artères. Au lieu de cela, configurez les pairs de routage du CSS avec cette fonction.

Ce document ne fournit pas l'instruction détaillée sur la configuration de l'authentification de routage et conduit le filtrage. Une telle documentation est disponible sur Cisco.com et ailleurs. Vous pouvez se référer au Cisco ISP Essentials de document - L'IOS essentiel comporte chaque

ISP devrait considérer. En raison de la complexité, demandez l'avis expérimenté si vous êtes un novice avant que vous configuriez ces caractéristiques sur des réseaux importants.

Gestion d'inondation

Beaucoup d'attaques DoS se fondent sur des inondations de paquets inutiles. Ces inondations congestionnent des liaisons réseau, des hôtes de ralentissement, et peuvent surcharger des Routeurs aussi bien. La configuration soigneuse du routeur peut réduire l'impact de ce type d'inondation.

Une partie importante de la gestion d'inondation est connaissance d'où les étranglements de représentation peuvent se produire. Si une inondation surcharge une ligne de t1, filtrez l'inondation sur le routeur à l'extrémité source de la ligne. Il y a peu ou pas d'effet si vous filtrez à l'extrémité de destination dans ce cas. Si le routeur lui-même est la partie du réseau la plus surchargée, vous pouvez rendre des sujets plus mauvais si vous filtrez les protections qui placent les fortes demandes sur le routeur. Maintenez ceci dans l'esprit quand vous considérez une implémentation des suggestions dans cette section.

Inondations de transit

Vous pouvez employer des caractéristiques de Cisco QoS sur les Routeurs en amont de Cisco IOS® afin de protéger le CSS, les hôtes, et les liens contre quelques genres d'inondations. Malheureusement, ce document ne fournit pas un traitement général de ce tri de gestion d'inondation. En outre, la protection dépend largement de l'attaque. Le seul conseil simple et généralement applicable est d'utiliser le Mise en file d'attente pondérée (WFQ) partout où les ressources CPU peuvent prendre en charge WFQ. WFQ est le par défaut pour les lignes série à vitesse réduite dans les versions ultérieures du logiciel de Cisco IOS. D'autres caractéristiques d'intérêt possible incluent :

- Fonction Committed Access Rate (CAR)
- Formatage du trafic générique (GTS)
- Mise en file d'attente faite sur commande

Parfois, vous pouvez configurer ces caractéristiques quand sous une attaque active.

Le CSS peut réduire l'incidence des attaques par inondation SYN sur le VIP et les vrais serveurs. Par défaut, le CSS limite le nombre de synchronisations et de connexions en trois étapes inachevées et se connecte les comme attaques DoS.

Référez-vous au pour en savoir plus de l'information de référence de Sécurité.

Services probablement inutiles

En règle générale, désactivez n'importe quel service inutile dans n'importe quel routeur qui est accessible potentiellement d'un réseau hostile. Les services que cette section répertorie sont parfois utiles. Mais désactivez ces services s'ils ne sont pas dans l'utilisation active.

SNTP

SNTP n'est pas particulièrement dangereux, mais n'importe quel service inutile peut présenter un

chemin pour la traversée. Si vous utilisez réellement SNTP, soyez sûr de configurer explicitement la source temporelle de confiance. SNTP n'utilise pas l'authentification. Une corruption de la base de temps est une bonne manière de renverser certains protocoles de Sécurité. La meilleure méthode est d'utiliser une source qui est interne et moins pour être charriée.

Cisco Discovery Protocol

Le Protocole CDP (Cisco Discovery Protocol), qui a été introduit dans WebNS 5.10, est utilisé pour quelques fonctions de Gestion de réseau. Le CDP est dangereux parce que n'importe quel système sur un segment directement connecté peut exécuter ces actions :

- Apprenez que le routeur est un périphérique de Cisco
- Déterminez le numéro de version et la version de logiciel qui des passages

Un attaquant peut employer ces informations afin de concevoir des attaques contre le CSS. Les informations de CDP sont accessibles seulement directement aux systèmes connectés. Le CSS annonce seulement les informations de CDP. Le CSS n'écoute pas. Vous ne pouvez émettre l'**aucune** commande de configuration globale de **cdp run** afin de désactiver le protocole CDP. Vous ne pouvez pas désactiver le CDP sur le CSS par interface.

Séjour à jour

Comme tout le logiciel, le logiciel de Cisco WebNS a des bogues. Certaines de ces bogues ont des implications en matière de sécurité. En outre, de nouvelles attaques continuent à être inventées. Et le comportement qui a été considéré correct quand un composant logiciel a été écrit peut avoir des effets néfastes quand le comportement est délibérément exploité.

Quand une nouvelle grave vulnérabilité de sécurité est trouvée dans un produit de Cisco, Cisco délivre généralement un avis consultatif au sujet de la vulnérabilité. Référez-vous à la stratégie de faille de la sécurité pour des informations sur le processus par lequel ces notices sont sorties. Référez-vous aux bulletins de renseignements de Sécurité pour les notices.

Presque n'importe quel comportement inhabituel de n'importe quel composant logiciel peut créer un risque contre la sécurité quelque part. Bogues de mention de bulletins de renseignements seulement qui ont des implications directes pour la sécurité des systèmes. Vous pouvez améliorer votre Sécurité si vous maintenez votre logiciel à jour, même faute de n'importe quel bulletin de renseignements de Sécurité.

Quelques problèmes de Sécurité ne sont pas le résultat des erreurs de programmation, et les administrateurs réseau doivent rester avertis des tendances dans les attaques. Il y a un certain nombre de sites Web, de listes de diffusion d'Internet, et de groupes de discussion Usenet qui sont concernés par ces tendances.

Informations connexes

- RFC 2267
- Bulletins de renseignements de Sécurité
- Stratégie de faille de la sécurité
- Informations de référence de sécurité
- Configurer des protocoles réseau CSS

- Configurer des méthodes d'Accès à distance CSS
- Configurer des profils utilisateurs et des paramètres CSS
- Notes de mise à jour
- Caractérisation et suivi des inondations de paquets à l'aide de routeurs Cisco
- Cisco ISP Essentials - L'IOS essentiel comporte chaque ISP devrait considérer
- Le plus en retard dans les attaques par déni de service : Description et informations de « Smurfing » pour réduire des effets
- Support et documentation techniques - Cisco Systems