Cisco guident pour durcir le Pare-feu de Cisco ASA

Contenu

Introduction

Ce document contient les informations pour vous aider à sécuriser des périphériques de Cisco ASA, qui augmente la Sécurité globale de votre réseau. Ce document est structuré dans 4 sections

Durcissement d'avion de Gestion - Ceci applique à tout le Management/To associé par ASA le trafic de case comme SNMP, SSH etc.
Sécurisant le config - Commandes par lesquelles nous pouvons nous arrêter remplir mots de passe etc. pour la configuration en cours etc.
Se connecter et surveiller - Ceci s'applique à n'importe quel paramètre relatif à ouvrir une session l'ASA.
Par le trafic - Ceci s'applique au trafic qui passe par l'ASA.

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

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de

logiciel suivantes :

- Cisco ASA5500-X 9.4(1) et plus tard.

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

Produits connexes

Cette configuration peut également être utilisée avec la version de logiciel 9.x d'appareils de Sécurité de gamme 5500-X de Cisco ASA.

Conventions

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

Opérations sécurisées

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

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

Surveiller les avis et les réponses de la sécurité Cisco

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

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

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

Exploiter Authentication, Authorization, and Accounting (AAA)

Le cadre d'Authentification, autorisation et comptabilité (AAA) est essentiel aux périphériques de réseau sécurisé. Le cadre AAA fournit l'authentification des sessions de gestion et peut également

limiter les utilisateurs à des commandes spécifiques définies par l´administrateur et enregistrer toutes les commandes saisies par tous les utilisateurs. Voyez la section d'authentification, d'autorisation, et de comptabilité de ce document pour plus d'informations sur la façon accroître l'AAA.

Centraliser la collection et la surveillance du journal

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

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

Utiliser les protocoles sécurisés quand c'est possible

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

Obtenir la visibilité du trafic avec Netflow

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

Gestion de la configuration

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

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

La configuration d'un périphérique de Cisco ASA contient beaucoup de détails sensibles. Les noms d'utilisateur, les mots de passe et le contenu des listes de contrôle d'accès sont des

exemples de ce type d'information. Le référentiel que vous utilisez afin d'archiver des configurations de périphérique de Cisco ASA doit être sécurisé. Un accès non sécurisé à ces informations peut nuire à la sécurité de tout le réseau.

Plan de gestion

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

Durcissement de l'avion de Gestion

Le plan de gestion est utilisé afin d'accéder, configurer et gérer un périphérique, ainsi que pour surveiller ses opérations et le réseau sur lequel il est déployé. Le plan de gestion est le plan qui reçoit et envoie le trafic pour les opérations de ces fonctions. Cette liste des protocoles est utilisée par le plan de gestion :

- Protocole SNMP
- Secure Shell Protocol
- Protocole de transfert de fichiers
- Trivial File Transfer Protocol
- Secure Copy Protocol
- TACACS+
- RAYON
- NetFlow
- Network Time Protocol
- Syslog
- ICMP
- PME

Remarque: Activant TELNET n'est pas recommandé car c'est texte brut.

Gestion des mots de passe

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

L'ASA utilise le Message Digest 5 (MD5) pour le hachage de mot de passe. Cet algorithme a eu une revue publique considérable et n'est pas connu pour être réversible. Cependant, l'algorithme

est sujet à des attaques de dictionnaire. Dans une attaque de dictionnaire, un attaquant essaye chaque mot d´un dictionnaire ou autre liste de mots de passe candidats afin de rechercher une correspondance. Par conséquent, les fichiers de configuration doivent être stockés de manière sécurisée et seulement partagés avec des personnes de confiance.

Service HTTP d'enable

Pour utiliser l'ASDM, vous devez activer le serveur HTTPS, et permettez des connexions HTTPS à l'ASA. Les dispositifs de sécurité permettent un maximum de 5 exemples simultanés ASDM par contexte, si disponibles, avec un maximum de 32 exemples ASDM entre tous les contextes. Pour configurer l'utilisation d'accès ASDM :

```
http server enable <port>
```

Permettez seulement l'IP qui sont nécessaires dans la liste d'ACL. Permettre un accès large est un erroné pratiquent.

```
http 0.0.0.0 0.0.0.0 <interface>
```

Configurez le contrôle d'accès ASDM :

```
http <remote_ip_address> <remote_subnet_mask> <interface_name>
```

Commençant par la version logicielle ASA 9.1(2),8.4(4.1), L'ASA prend en charge maintenant les suites éphémères suivantes de chiffrement SSL de Diffie-Hellman (DHE).

DHE-AES128-SHA1
DHE-AES256-SHA1

Ces suites de chiffrement sont spécifiées dans **RFC 3268**, Norme AES (Advanced Encryption Standard) Ciphersuites pour le Transport Layer Security (TLS).

Une fois pris en charge par le client, DHE est le chiffrement préféré parce qu'il fournit le perfect forward secrecy. Voyez les limites suivantes :

DHE n'est pas pris en charge sur des connexions SSL 3.0, ainsi veillez à activer également le TLS 1.0 pour le serveur SSL.

```
// Set server version ASA(config)# ssl server-version tlsv1 sslv3
// Set client version ASA(config) # ssl client-version any
```

Quelques applications populaires ne prennent en charge pas DHE, ainsi incluez au moins une autre méthode de ssl encryption pour s'assurer qu'une suite de chiffrement commune à chacun des deux le client et serveur SSL peut être utilisée. Quelques clients peuvent ne pas prendre en charge DHE, y compris AnyConnect 2.5 et 3.0, Cisco Secure Desktop, et Internet Explorer 9.0.

L'ASA a au-dessous des chiffrements activés dans la commande en tant que ci-dessous par défaut.

```
ASA(config)#ssl encryption rc4-sha1 dhe-aes128-sha1 dhe-aes256-sha1 aes128-sha1 aes256-sha1
3des-sha1
```

version serveur SSL (par défaut)

L'ASA par défaut utilise un certificat Auto-signé provisoire qui change sur chaque réinitialisation. Si vous recherchez un certificat simple, vous pouvez suivre le lien ci-dessous pour générer un certificat Auto-signé par constante.

Maintenant le startig de version 1.2 de TLS de supports ASA de la version de logiciel 9.3.1for sécurisent la transmission de message pour l'ASDM, le SSVPN sans client, et l'AnyConnect VPN. Des commandes suivantes ont été introduites ou ont modifié des commandes : **version du client SSL**, **version serveur SSL**, **chiffrement SSL**, **SSL confiance point**, CAD-**groupe SSL**, **show ssl**, **chiffrement de show ssl**, **exposition VPN-sessiondb**

```
ASA-1/act(config)# ssl server-version ?

configure mode commands/options:
  tlsv1    Enter this keyword to accept SSLv2 ClientHellos and negotiate TLSv1
           (or greater)
  tlsv1.1  Enter this keyword to accept SSLv2 ClientHellos and negotiate
           TLSv1.1 (or greater)
  tlsv1.2  Enter this keyword to accept SSLv2 ClientHellos and negotiate
           TLSv1.2 (or greater)
ASA-1/act(config)# ssl cipher ?

configure mode commands/options:
  default  Specify the set of ciphers for outbound connections
  dtlsv1   Specify the ciphers for DTLSv1 inbound connections
  tlsv1    Specify the ciphers for TLSv1 inbound connections
  tlsv1.1  Specify the ciphers for TLSv1.1 inbound connections
  tlsv1.2  Specify the ciphers for TLSv1.2 inbound connections
```

SSH d'enable

L'ASA permet des connexions SSH à l'ASA pour la Gestion. L'ASA permet un maximum de 5 connexions SSH simultanées par contexte, si disponible, avec un maximum de 100 connexions divisées entre tous les contextes.

```
hostname <device_hostname>
domain-name <domain-name>
crypto key generate rsa modulus 2048
```

Le type par défaut de paire de clés est clé générale. La taille par défaut de module est 1024. La quantité de l'espace NVRAM pour enregistrer des paires de clés varie selon la plate-forme ASA. Vous pouvez atteindre une limite si vous générez plus de 30 paires de clés. Les clés RSA 4096-bit sont seulement prises en charge sur l'ASA5580, les 5585, ou les Plateformes postérieures.

Pour enlever les paires de clés du type indiqué (la RSA ou DSA)

```
crypto key zeroize { rsa | dsa } [ label key-pair-label ] [ default ] [ noconfirm ]
```

Configurez le SSH pour le périphérique distant Access :

```
ssh <remote_ip_address> <remote_subnet_mask> <interface_name>
```

Pour limiter la version du SSH reçue par l'ASA, utilisez la commande de version de ssh en mode de configuration globale. Pour limiter l'ASA pour utiliser seulement la version 2 peut être mettent wusing au-dessous de la commande.

```
ASA(config)#ssh version 2
```

Pour permuter des clés suivre la méthode d'échange de clés du groupe 1 de Protocole DH (Diffie-Hellman) ou du groupe 14 CAD, utilisez la commande de clé-échange de ssh en mode de

configuration globale. à partir 9.1(2) de l'ASA prend en charge dh-group14-sha1 pour le SSH

```
ASA(config)#ssh key-exchange dh-group14-sha1
```

Configurez le délai d'attente pour des sessions d'ouverture de connexion

```
// Configure Console timeout
ASA(config)#console timeout 10

// Configure Console timeout
ASA(config)#ssh timeout 10
```

Gestion des mots de passe

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

Configurez l'utilisateur local et le mot de passe chiffré

```
username <local_username> password <local_password> encrypted
```

Configurez le mot de passe d'enable

```
enable password <enable_password> encrypted
```

Configurez l'authentification d'AAA pour le mode enable

```
ASA(config)#aaa authentication enable console LOCAL
```

Authentification, autorisation, et comptabilité

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

Authentification TACACS+

TACACS+ est un protocole d'authentification que l'ASA peut utiliser pour l'authentification des utilisateurs de Gestion contre un serveur distant d'AAA. Ces utilisateurs de Gestion peuvent accéder au périphérique ASA par l'intermédiaire du SSH, du HTTPS, du telnet, ou du HTTP.

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

Le RAYON est un protocole semblable dans le but à TACACS+ ; cependant, il chiffre seulement le mot de passe envoyé à travers le réseau. En revanche, TACACS+ chiffre la charge utile entière

de TCP, qui inclut chacun des deux le nom d'utilisateur et mot de passe. Pour cette raison, TACACS+ devrait être utilisé de préférence à RADIUS quand TACACS+ est supporté par le serveur AAA. Référez-vous à Comparaison de TACACS+ et RADIUS pour une comparaison plus détaillée de ces deux protocoles.

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

```
aaa authentication serial console Tacacs
aaa authentication ssh console Tacacs
aaa authentication http console Tacacs
aaa authentication telnet console Tacacs
```

Signature et vérification d'image ASA

Àpartir de la version de logiciel 9.3.1 ASA des images sont maintenant signées utilisant une signature numérique. La signature numérique est vérifiée après que l'ASA soit amorcée.

```
ASA-1/act(config)# verify flash:/asa941-smp-k8.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Done! Embedded Hash SHA-512:
0e707a0e45b1c7c5afa9ef4e802a273677a5e46f7e1d186292abe1154
c948a63c625463b74119194da029655487659490c2873506974cab78b66d6d9742ed73e Computed Hash SHA-512:
0e707a0e45b1c7c5afa9ef4e802a273677a5e46f7e1d186292abe1154
c948a63c625463b74119194da029655487659490c2873506974cab78b66d6d9742ed73e CCO Hash SHA-512:
1b6d41e893868aab9e06e78a9902b925227c82d8e31978ff2c412c18a
c99f49f70354715441385e0b96e4bd3e861d18fb30433d52e12b15b501fa790f36d0ea0 Signature Verified
ASA(config)# verify /signature running Requesting verify signature of the running image...
Starting image verification Hash Computation: 100% Done! Computed Hash SHA2:
2fbb0f62b5fbc61b081acfca76bddbb2 26ce7a5fb4b424e5e21636c6c8a7d665
1e688834203dfb7ffa6eaefc7fdf9d3d 1d0a063a20539baba72c2526ca37771c Get key records from key
storage: PrimaryASA, key_store_type: 6 Embedded Hash SHA2: 2fbb0f62b5fbc61b081acfca76bddbb2
26ce7a5fb4b424e5e21636c6c8a7d665 1e688834203dfb7ffa6eaefc7fdf9d3d
1d0a063a20539baba72c2526ca37771c Returned. rc: 0, status: 1 The digital signature of the running
image verified successfully

ASA-1/act(config)# show software authenticity running
Image type : Release
Signer Information
Common Name : abraxas
Organization Unit : ASAv
Organization Name : CiscoSystems
Certificate Serial Number : 550DBBD5
Hash Algorithm : SHA2 512
Signature Algorithm : 2048-bit RSA
Key Version : A
```

Configurez le fuseau horaire d'horloge

```
clock timezone GMT <hours offset>
```

Configurez le NTP

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

- **Fuseau horaire de NTP** - Quand vous configurez le NTP, le fuseau horaire doit être configuré de sorte que des horodateurs puissent être exactement corrélés. Il y a habituellement deux approches pour configurer le fuseau horaire pour des périphériques dans un réseau avec une présence globale. Une méthode est de configurer tous les périphériques réseau avec l´UTC (Coordinated Universal Time) (précédemment heure GMT (Greenwich Mean Time)). L'autre approche est de configurer les périphériques réseau avec le fuseau horaire local.

```
ntp server ip_address [ key key_id ] [ source interface_name ] [ prefer ]
```

- **Authentification de NTP** - Si vous configurez l'authentification de NTP, elle fournit l'assurance que des messages de NTP sont permutés entre les pairs de confiance de NTP. Activez l'authentification utilisant la commande de ntp authenticate, placez l'ID de clé de confiance pour ce serveur. Si vous activez l'authentification, l'ASA communique seulement avec un serveur de NTP si elle utilise la clé de confiance correcte dans les paquets. Pour activer l'authentification avec un serveur de NTP, utilisez la commande de ntp authenticate en mode de configuration globale.

```
ASA(config)#ntp authenticate
```

Service de serveur DHCP (sinon étant utilisé)

```
clear configure dhcpd
no dhcpd enable <interface_name>
```

Remarque: L'ASA ne prend en charge pas le CDP.

Liste d'accès de Contrôle-avion

Les règles de contrôle d'accès pour le trafic d'administration d'à-le-case (défini par des commandes telles que le HTTP, le ssh, ou le telnet) ont une priorité plus élevée qu'une liste d'accès appliquée avec l'option de contrôle-avion. Par conséquent, on permettra à l'un tel trafic d'administration permis pour entrer même si explicitement refusé par la liste d'accès d'à-le-case.

```
access-list <name> in interface <Interface_name> control-plane
```

De l'ASA

Voici les protocoles qui peuvent être utilisés pour copier/fichiers de transfert sur l'ASA.

Texte clair :

- FTP
- HTTP
- TFTP
- PME

Sécurisé :

- HTTPS
- SCP (client sécurisé de copie) à partir de 9.1(5), ASA prend en charge le client SCP pour transférer des fichiers à et d'un serveur SCP.

Pour le trafic traversant

Randomisation de numéro de séquence de TCP

Chaque connexion TCP a deux ISNs : un généré par le client et un généré par le serveur. L'ASA sélectionne de façon aléatoire l'ISN de la synchronisation de TCP passant dans le d'arrivée et des directions sortantes.

Sélectionner de façon aléatoire l'ISN de l'hôte protégé empêche un attaquant de predecting le prochain ISN pour une nouvelle connexion et de détourner potentiellement la nouvelle session.

La randomisation de nombre de séquence initiale de TCP peut être désactivée s'il y a lieu. Exemple :

- Si un autre Pare-feu intégré sélectionne de façon aléatoire également les nombres de séquence initiale, il n'y a aucun besoin des deux Pare-feu d'exécuter cette action, quoique cette action n'affecte pas le trafic.
- Si vous utilisez la connexion multiple entre deux noeuds d'eBGP par l'ASA, et les pairs d'eBGP utilisent le MD5. La randomisation casse la somme de contrôle de MD5.
- Si nous utilisons un périphérique WAAS qui exige de l'ASA de ne pas sélectionner de façon aléatoire les numéros de séquence de connexions.

Décrément TTL

Par défaut, ne décrémente pas le TTL dans l'en-tête IP due à quelle ASA n'apparaît pas comme saut de routeur en faire la traceroute.

dnsguard

Impose une réponse de DN par requête. Il peut être activé utilisant la commande en mode de configuration globale.

```
ASA(config)#dns-guard
```

Configurez les contrôles de fragmentation de fragment chain

Pour fournir la Gestion supplémentaire de la fragmentation de paquets et améliorer la compatibilité avec le NFS, utilisez la commande de fragment en mode de configuration globale.

```
fragment reassembly { full | virtual } { size | chain | timeout limit } [ interface ]
```

Configurez l'inspection de Protocol

Des engines d'inspection sont exigées pour des services qui incluent les informations d'adressage IP dans le paquet de données d'utilisateur ou qui les canaux auxiliaires ouverts sur les ports dynamiquement assignés. Ces protocoles exigent de l'ASA de faire une inspection profonde de paquet au lieu de passer le paquet par le chemin rapide. En conséquence, les engines d'inspection peuvent affecter le débit global. Veuillez se référer le guide de config ASA 9.4 pour les informations détaillées sur l'inspection de protocole de la couche applicative.

L'inspection sur l'ASA peut être utilisation activée au-dessous de commande

```
policy-map <Policy-map_name>
 class inspection_default
  inspect <Protocol>

service-policy <Policy-map_name> interface <Interface_name> (Per Interface)
service-policy <Policy-map_name> global (Globally)
```

Par défaut l'ASA a le **« global_policy »** activé globalement.

Configurez l'Unicast Reverse Path Forwarding

```
ip verify reverse-path interface <interface_name>
```

Quand le trafic obtient en raison abandonné du contrôle RPF, « la baisse d'asp d'exposition » ci-dessous contre- sur l'ASA incrémente.

```
ASA(config)# show asp drop

Frame drop:
 Invalid TCP Length (invalid-tcp-hdr-length)                 21
   Reverse-path verify failed (rpf-violated)                   90

// Check Reverse path statistics

ASA(config)# sh ip verify statistics
 interface inside: 11 unicast rpf drops
interface outside: 79 unicast rpf drops
```

Détection de menace

La détection de menace fournit à des administrateurs de Pare-feu les outils nécessaires pour identifier, comprendre, et arrêter des attaques avant qu'elles atteignent l'infrastructure de réseau interne. Afin de faire ainsi, la caractéristique se fonde sur un certain nombre de déclencheurs et de statistiques différents, qui sont décrites dans davantage de détail dans ces sections.

Veuillez se référer la fonctionnalité et la configuration de détection de menace ASA pour l'explication détaillée sur la détection de menace sur l'ASA.

Filtre de Botnet

Les demandes et les réponses de Domain Name Server de moniteurs de filtre du trafic de BotNet (DN) entre les clients DNS internes et les serveurs DNS externes. Quand une réponse de DN est traitée, le domaine associé avec la réponse est vérifié contre la base de données des domaines malveillants connus. S'il y a une correspondance, promouvez le trafic à l'adresse IP actuelle dans les DN que la réponse est bloquée.

Le malware est un logiciel malveillant qui est installé sur un hôte inconscient. Le malware qui tente l'activité réseau telle que l'envoi des données privées (mots de passe, numéros de carte de crédit, rappes principales, ou données de propriété industrielle) peut être détecté par le filtre du trafic de Botnet quand le malware commence une connexion à une mauvaise adresse IP connue. Le filtre du trafic de Botnet vérifie les connexions entrantes et sortantes contre une base de données dynamique de mauvais noms de domaine et adresses IP connus (la *liste noire*), et puis les logs ou bloque n'importe quelle activité suspecte.

Vous pouvez également compléter la base de données dynamique de Cisco avec des adresses mises sur la liste noire de votre choisir en les ajoutant à une liste noire statique ; si la base de données dynamique inclut les adresses mises sur la liste noire que vous pensez si est mise sur la liste noire, vous pouvez manuellement les écrire dans un *whitelist* statique. Les adresses de Whitelisted génèrent toujours des messages de Syslog, mais parce que vous visez seulement des messages de Syslog de liste noire, ils sont informationnels. Référez-vous s'il vous plaît en configurant le filtre du trafic de Botnet pour information les informations détaillées.

Ajouts de cache d'ARP pour des sous-réseaux non-connectés

Par défaut l'ASA ne répond pas à l'ARP pour les adresses IP non-directly connectées de sous-réseau. Si vous avez un IP NAT sur l'ASA qui n'appartient pas au même IP de sous-réseau de l'interface ASA, nous devrons activer la « autorisation-nonconnected d'ARP » sur l'ASA au proxy-arp pour l'IP de NATted.

```
arp permit-nonconnected
```

Il est toujours recommandé pour avoir le routage correct sur en amont et en aval des périphériques pour que NAT fonctionne sans activer la commande ci-dessus.

Se connecter et surveiller

Configurer le SNMP

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

Chaînes de caractères de la communauté SNMP

Les chaînes de la Communauté sont des mots de passe qui sont appliqués à un périphérique ASA pour limiter l'accès, en lecture seule et l'accès en lecture-écriture, aux données SNMP sur le périphérique. Ces chaînes de caractères de la communauté, comme avec tous les mots de passe, devraient être soigneusement choisies pour assurer qu'elles ne sont pas insignifiantes. Les chaînes de caractères de la communauté devraient être changées à intervalles réguliers et conformément aux stratégies de sécurité du réseau. Par exemple, les chaînes de caractères devraient être changées quand un administrateur réseau change des rôles ou quitte la société.

Accès en lecture SNMP d'enable :

```
snmp-server host <interface_name> <remote_ip_address>
```

Déroutements SNMP d'enable

```
snmp-server enable traps all
```

Configurer le Syslog

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

- ASDM
- Mémoire tampon
- Éclair
- Email
- Ftp server
- Serveur SNMP comme déroutements
- Serveur de Syslog

Configurez le niveau d'importance de journalisation console

```
logging console critical
```
Le Syslog basé par TCP est également disponible. Tous les Syslog peuvent être envoyés au serveur de Syslog dans le plaintext ou être dedans chiffrés en cas de TCP.

Plaintext

syslog_ip d'interface_name d'hôte de journalisation [port tcp/

Chiffré

*syslog_ip d'interface_name d'*hôte de journalisation [*port* tcp/ / [sécurisez]

Si une connexion TCP ne peut pas être établie avec les Syslog serveur, toutes les nouvelles connexions seront refusées. Vous pouvez changer ce comportement par défaut en écrivant la commande « **se connectant autorisation-hostdown »**.

Configurez les horodateurs dans des messages de log

La configuration des horodatages des journalisations vous aide à corréler des événements à travers les périphériques réseau. Il est important de mettre en application une configuration d´horodatage correct et cohérent des journalisations pour assurer que vous pouvez corréler les données de journalisation.

```
logging timestamp
```
Pour relatif à l'information supplémentaire au Syslog référez-vous s'il vous plaît l'exemple de configuration de Syslog ASA.

Configurer le NetFlow

Parfois, vous pouvez devoir identifier rapidement le trafic sur le réseau et revenir en arrière, particulièrement pendant une réponse d'incident ou des mauvaises performances du réseau. Le Netflow peut fournir la visibilité dans tout le trafic du réseau. En outre, le Netflow peut être mis en application avec des collecteurs qui peuvent fournir les tendances à long terme et une analyse automatisée.

Cisco ASA prend en charge des services de version 9 de NetFlow. Les réalisations ASA et ASASM de NSEL fournissent un avec état, ip flow dépistant la méthode qui exporte seulement ces enregistrements qui indiquent des événements significatifs dans un écoulement. Dans l'écoulement d'avec état dépistant, les écoulements dépistés passent par une gamme de modifications d'état. Des événements NSEL sont utilisés pour exporter des données au sujet d'état d'écoulement et sont déclenchés par l'événement qui a entraîné la modification d'état.

Veuillez se référer le pour en savoir plus de guide d'implémentation de NetFlow de Cisco ASA du NetFlow sur l'ASA :

Sécuriser le config

Vérification d'image sur l'ASA

Àpartir de 9.1(2) et de 8.4(4.1), le soutien de vérifier d'intégrité de l'image SHA-512 a été ajouté. Pour vérifier la somme de contrôle d'un fichier, utilisez la commande de vérifier dans le mode d'exécution privilégié.

Calcule et affiche la valeur de MD5 pour l'image logicielle spécifiée. Comparez cette valeur à la valeur disponible sur Cisco.com pour cette image.

```
verify [ /md5 path ] [ md5-value ]
```

Mots de passe dans le config

Tous les mots de passe et clés sont chiffrés ou assombris. Le « show running-config » n'indique pas les mots de passe réels.

Une telle sauvegarde ne peut pas être utilisée pour la sauvegarde/restauration sur l'ASA. La sauvegarde qui est prise pour le whould de buts de restauration soit exécutée utilisant la commande « plus de système : running-config ». Les mots de passe de config ASA peuvent être chiffrés utilisant un mot de passe principal. Veuillez se référer le cryptage de mot de passe pour information les informations détaillées.

Entretenez la reprise de mot de passe

Désactivant ceci désactivera le mécanisme de reprise de mot de passe et désactivera l'accès à ROMMON. Les seuls moyens de récupérer des mots de passe perdus ou oubliés seront pour que ROMMON efface tous les systèmes de fichiers comprenant des fichiers de configuration et des images. Vous devriez faire une sauvegarde de votre configuration et avoir un mécanisme pour restaurer des images de la ligne de commande ROMMON.

Dépannez

Il n'y a aucune section dépannage pour ce document.