Configurer l'interopérabilité du pare-feu basé sur la zone Cisco IOS avec le déploiement WAAS

Contenu

Introduction
Conditions préalables
Conditions requises
Components Used
Informations générales
Prise en charge WAAS avec Cisco IOS® Firewall
Scénarios de déploiement d'optimisation du flux de trafic WAAS
Déploiement de filiales WAAS avec périphérique hors chemin
Diagramme du réseau
Configuration et flux de paquets
Flux de trafic WAAS de bout en bout
Flux de trafic CMS (enregistrement du périphérique WAAS auprès du gestionnaire central)
Informations de session ZBF
Configuration de travail du routeur côté client (R1) avec WAAS et ZBF activés
Déploiement de succursales WAAS avec périphérique en ligne
Détails
Configuration
Restrictions relatives à l'interopérabilité ZBF avec WAAS
Vérification
Dépannage
Informations connexes

Introduction

Ce document décrit un nouveau modèle de configuration pour l'ensemble de fonctionnalités du pare-feu Cisco IOS®. Ce nouveau modèle de configuration propose des politiques intuitives pour les routeurs à interfaces multiples, une plus grande granularité de l'application de la politique de pare-feu et une politique de déni par défaut qui empêche le trafic entre les zones de sécurité du pare-feu jusqu'à ce qu'une politique explicite soit appliquée pour permettre un trafic souhaitable.

Conditions préalables

Conditions requises

Cisco vous recommande de connaître l'interface de ligne de commande Cisco IOS®.

Components Used

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

logiciel suivantes :

- Routeurs de la gamme Cisco 2900
- Logiciel Cisco IOS® version 15.2(4) M2

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

Informations générales

Le pare-feu Zone-Based Policy Firewall (également appelé Zone-Policy Firewall, ZFW ou ZBF) transforme la configuration du pare-feu de l'ancien modèle basé sur les interfaces (CBAC) en un modèle basé sur les zones plus flexible et plus facile à comprendre. Les interfaces sont affectées aux zones et la politique d'inspection est appliquée au trafic qui se déplace entre les zones. Les politiques interzonales offrent une flexibilité et une granularité considérables, afin que différentes politiques d'inspection puissent être appliquées aux multiples groupes hôtes connectés à la même interface du routeur . Les stratégies de pare-feu sont configurées avec le langage de stratégie Cisco® (CPL), qui utilise une structure hiérarchique afin de définir l'inspection pour les protocoles réseau et les groupes d'hôtes auxquels l'inspection est appliquée.

Prise en charge WAAS avec Cisco IOS® Firewall

La prise en charge des services WAAS (Wide Area Application Services) avec le pare-feu Cisco IOS® a été introduite dans Cisco IOS® version 12.4(15)T. Il fournit un pare-feu intégré qui optimise les WAN et les solutions d'accélération des applications conformes à la sécurité avec les avantages suivants :

- Optimise un WAN grâce à des fonctionnalités complètes d'inspection dynamique
- Simplifie la conformité PCI (Payment Card Industry)
- Protège le trafic WAN accéléré transparent
- Intégration transparente des réseaux WAAS
- Prend en charge les modules WAE (Wide Area Application Engine) NME (Network Management Equipment) ou le déploiement de périphériques WAAS autonomes

WAAS dispose d'un mécanisme de détection automatique qui utilise les options TCP lors de la connexion initiale en trois étapes utilisée afin d'identifier les périphériques WAE de manière transparente. Après la détection automatique, les flux de trafic optimisés (chemins) subissent un changement dans le numéro de séquence TCP afin de permettre aux points d'extrémité de distinguer les flux de trafic optimisés des flux de trafic non optimisés.

La prise en charge WAAS du pare-feu IOS® permet de régler les variables d'état TCP internes utilisées pour l'inspection de couche 4, en fonction du changement de numéro de séquence mentionné précédemment. Si le pare-feu Cisco IOS® constate qu'un flux de trafic a réussi la détection automatique WAAS, il autorise le déplacement du numéro de séquence initial pour le flux de trafic et maintient l'état de couche 4 sur le flux de trafic optimisé.

Scénarios de déploiement d'optimisation du flux de trafic WAAS

Les sections décrivent deux scénarios d'optimisation du flux de trafic WAAS différents pour les déploiements de filiales. L'optimisation du flux de trafic WAAS fonctionne avec la fonctionnalité de

pare-feu Cisco sur un routeur à services intégrés (ISR) Cisco.

La figure présente un exemple d'optimisation du flux de trafic WAAS de bout en bout avec le pare-feu Cisco. Dans ce déploiement particulier, un périphérique NME-WAE se trouve sur le même périphérique que le pare-feu Cisco. Le protocole WCCP (Web Cache Communication Protocol) est utilisé afin de rediriger le trafic pour l'interception.

- Déploiement de filiales WAAS avec un périphérique hors chemin
- Déploiement d'une filiale WAAS avec un périphérique en ligne

Déploiement de filiales WAAS avec périphérique hors chemin

Un périphérique WAE peut être soit un périphérique autonome Cisco WAN Automation Engine (WAE), soit un module de réseau Cisco WAAS (NME-WAE) installé sur un routeur de service intégré.

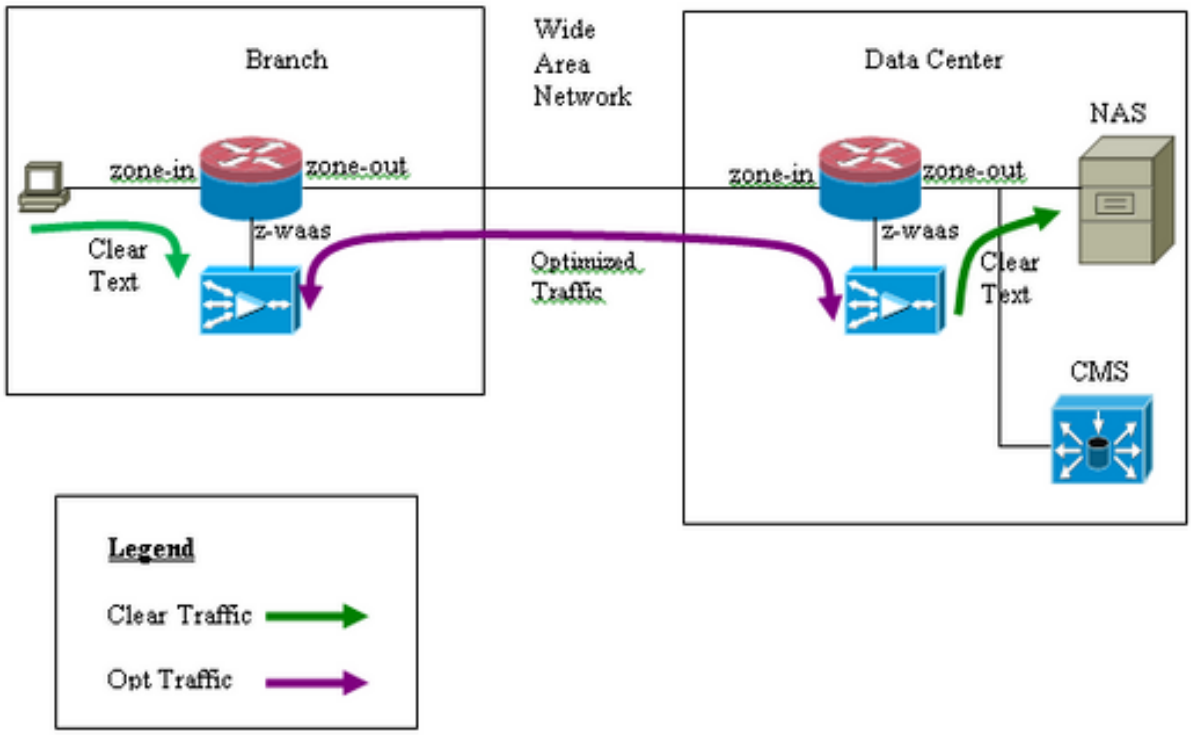
La figure illustre un déploiement de filiale WAAS qui utilise WCCP afin de rediriger le trafic vers un périphérique WAE autonome et hors chemin pour l'interception du trafic. La configuration de cette option est identique au déploiement de la filiale WAAS avec un NME-WAE.

Diagramme du réseau

Configuration et flux de paquets

Ce diagramme illustre un exemple de configuration avec l'optimisation WAAS activée pour le trafic de bout en bout et le système de gestion centralisée (CMS) qui est présent à l'extrémité du serveur. Les modules WAAS présents à l'extrémité de la filiale et du centre de données doivent

s'enregistrer auprès du CMS pour leurs opérations. Il est observé que le CMS utilise HTTPS pour sa communication avec les modules WAAS.



Flux de trafic WAAS de bout en bout

L'exemple ci-dessous fournit une configuration d'optimisation du flux de trafic WAAS de bout en bout pour le pare-feu Cisco IOS® qui utilise WCCP afin de rediriger le trafic vers un périphérique WAE pour l'interception du trafic.

Section 1. Configuration associée à IOS-FW WCCP :

```
ip wccp 61
ip wccp 62
ip inspect waas enable
```

Section 2. Configuration de la stratégie IOS-FW :

```
class-map type inspect most-traffic
 match protocol icmp
 match protocol ftp
 match protocol tcp
 match protocol udp
!
policy–map type inspect p1
 class type inspect most–traffic
  inspect
 class class–default
  drop
```

Section 3. Configuration des zones et des zones IOS-FW :

```
zone security zone-in
zone security zone-out
zone security z-waas

zone—pair security in—out source zone-in destination zone-out
service—policy type inspect p1

zone—pair security out-in source zone-out destination zone-in
service—policy type inspect p1
```

Section 4. Configuration de l’interface :

```
interface GigabitEthernet0/0
 description Trusted interface
 ip address 172.16.11.1 255.255.255.0
 ip wccp 61 redirect in
 zone—member security zone-in

! interface GigabitEthernet0/1 description Untrusted interface ip address 203.0.113.1
255.255.255.0 ip wccp 62 redirect in zone—member security zone-out
```

> **Note**: La nouvelle configuration de Cisco IOS® versions 12.4(20)T et 12.4(22)T place le moteur de service intégré dans sa propre zone et ne doit faire partie d'aucune paire de zones. Les zones-paires sont configurées entre zone-in et zone-out.

```
interface Integrated—Service—Enginel/0
 ip address 192.168.10.1 255.255.255.0
 ip wccp redirect exclude in
 zone—member security z-waas
```

Avec aucune zone configurée sur Integrated—Service—Enginel/0, le trafic est abandonné avec ce message d'abandon :

```
*Mar 9 11:52:30.647: %FW-6-DROP_PKT: Dropping tcp session 172.16.11.59:44191 172.16.10.10:80 due
to One of the interfaces not being cfged for zoning with ip ident 0
```

Flux de trafic CMS (enregistrement du périphérique WAAS auprès du gestionnaire central)

L'exemple ci-dessous fournit la configuration des deux scénarios répertoriés :

- Configuration d'optimisation du flux de trafic WAAS de bout en bout pour le pare-feu Cisco IOS® qui utilise WCCP afin de rediriger le trafic vers un périphérique WAE pour l'interception du trafic
- Autorisation du trafic CMS (trafic de gestion WAAS qui circule vers/depuis CMS depuis/vers des périphériques WAAS)

Section 1. Configuration associée à IOS-FW WCCP :

```
ip wccp 61
ip wccp 62
ip inspect waas enable
```

Section 2. Configuration de la stratégie IOS-FW :

```
class-map type inspect most-traffic
 match protocol icmp
 match protocol ftp
 match protocol tcp
 match protocol udp

policy—map type inspect p1
 class type inspect most—traffic
  inspect
 class class—default
  drop
```

Section 2.1. Stratégie IOS-FW liée au trafic CMS :

Note: La carte de classe ici est nécessaire pour permettre au trafic CMS de passer par :

```
class-map type inspect waas-special
 match access-group 123

policy-map type inspect p-waas-man
 class type inspect waas-special
  pass
 class class-default
  drop
```

Section 3. Configuration des zones et des zones IOS-FW :

```
zone security zone-in
zone security zone-out
zone security z-waas

zone—pair security in—out source zone-in destination zone-out
service—policy type inspect p1

zone—pair security out—in source zone-out destination zone-in
service—policy type inspect p1
```

Section 3.1. Configuration de zone et de zone associée à IOS-FW CMS :

Note: Les zones-paires **waas-out** et **out-waas** sont nécessaires pour appliquer la stratégie créée précédemment pour le trafic CMS.

```
zone-pair security waas-out source z-waas destination zone-out
service-policy type inspect p-waas-man

zone-pair security out-waas source zone-out destination z-waas
service-policy type inspect p-waas-man
```

Section 4. Configuration de l'interface :

```
interface GigabitEthernet0/0
description Trusted interface
ipaddress 172.16.11.1 255.255.255.0
ip wccp 61 redirect in
zone—member security zone-in
!
```

```
interface GigabitEthernet0/1
description Untrusted interface
ip address 203.0.113.1 255.255.255.0
ip wccp 62 redirect in
zone—member security zone-out ! interface Integrated—Service—Enginel/0
ip address 192.168.10.1 255.255.255.0
ip wccp redirect exclude in
zone—member security z-waas
```

Section 5. Liste d'accès pour le trafic CMS.

> **Note**: Liste d'accès utilisée pour le trafic CMS. Il autorise le trafic HTTPS dans les deux directions car le trafic CMS est HTTPS.

```
access-list 123 permit tcp any eq 443 any
access-list 123 permit tcp any any eq 443
```

Informations de session ZBF

L'utilisateur 172.16.11.10 derrière le routeur R1 accède au serveur de fichiers hébergé derrière l'extrémité distante avec l'adresse IP 172.16.10.10, la session ZBF est créée à partir de la paire de zones entrantes et ensuite le routeur redirige le paquet vers le moteur WAAS pour l'optimisation.

```
R1#sh policy-map type inspect zone-pair in-out sess

policy exists on zp in-out
  Zone-pair: in-out

  Service-policy inspect : p1

    Class-map: most-traffic (match-any)
      Match: protocol icmp
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol ftp
        0 packets, 0 bytes
        30 second rate 0 bps
      Match: protocol tcp
        2 packets, 64 bytes
        30 second rate 0 bps
      Match: protocol udp
        0 packets, 0 bytes
        30 second rate 0 bps

   Inspect

      Number of Established Sessions = 1
      Established Sessions
        Session 3D4A32A0 (172.16.11.10:49300)=>(172.16.10.10:445) tcp SIS_OPEN/TCP_ESTAB
          Created 00:00:40, Last heard 00:00:10
          Bytes sent (initiator:responder) [0:0]
```

Session intégrée dans R1-WAAS et R2-WAAS de l'hôte interne au serveur distant.

R1-WAAS :

```
R1-WAAS#show statistics connection

Current Active Optimized Flows:                       1
   Current Active Optimized TCP Plus Flows:           1
   Current Active Optimized TCP Only Flows:           0
   Current Active Optimized Single Sided Flows:       0
   Current Active Optimized TCP Preposition Flows:    0
Current Active Auto-Discovery Flows:                  1
Current Reserved Flows:                               10
Current Active Pass-Through Flows:                    0
Historical Flows:                                     13


D:DRE,L:LZ,T:TCP Optimization RR:Total Reduction Ratio
A:AOIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,I:ICA,M:MAPI,N:NFS,S:SSL,W:WAN SECURE,V:VID
EO, X: SMB Signed Connection

ConnID        Source IP:Port          Dest IP:Port            PeerID Accel RR
    14    172.16.11.10:49185   172.16.10.10:445 c8:9c:1d:6a:10:61 TCDL  00.0%
```

R2-WAAS :

```
R2-WAAS#show statistics connection

Current Active Optimized Flows:                       1
   Current Active Optimized TCP Plus Flows:           1
   Current Active Optimized TCP Only Flows:           0
   Current Active Optimized TCP Preposition Flows:    0
Current Active Auto-Discovery Flows:                  0
Current Reserved Flows:                               10
Current Active Pass-Through Flows:                    0
Historical Flows:                                     9


D:DRE,L:LZ,T:TCP Optimization RR:Total Reduction Ratio
A:AOIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,M:MAPI,N:NFS,S:SSL,V:VIDEO

ConnID        Source IP:Port          Dest IP:Port            PeerID Accel RR
    10    172.16.11.10:49185   172.16.10.10:445 c8:9c:1d:6a:10:81 TCDL  00.0%
```

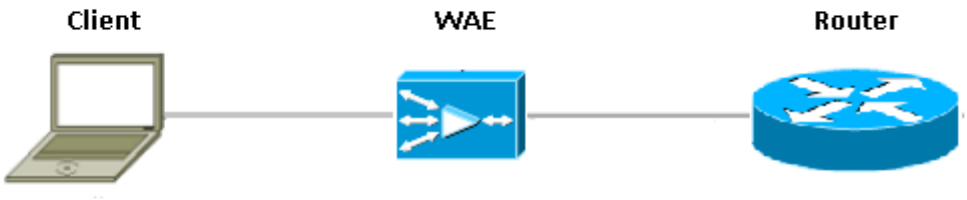
Configuration de travail du routeur côté client (R1) avec WAAS et ZBF activés

```
R1#sh run
Building configuration...
Current configuration : 3373 bytes
!
hostname R1
!
boot-start-marker
boot bootstrap tftp c2900-universalk9-mz.SPA.153-3.M4.bin 255.255.255.255
boot system flash c2900-universalk9-mz.SPA.153-3.M4.bin
boot-end-marker
!
ip wccp 61
ip wccp 62
no ipv6 cef
!
parameter-map type inspect global
```

```
 WAAS enable
 log dropped-packets enable
 max-incomplete low 18000
 max-incomplete high 20000
multilink bundle-name authenticated
!
license udi pid CISCO2911/K9 sn FGL171410K8
license boot module c2900 technology-package securityk9
license boot module c2900 technology-package uck9
license boot module c2900 technology-package datak9
hw-module pvdm 0/1
!
hw-module sm 1
!
class-map type inspect match-any most-traffic
 match protocol icmp
 match protocol ftp
 match protocol tcp
 match protocol udp
!
policy-map type inspect p1
 class type inspect most-traffic
  inspect
 class class-default
  drop
!
zone security in-zone
zone security out-zone
zone security waas-zone
zone-pair security in-out source in-zone destination out-zone
 service-policy type inspect p1
zone-pair security out-in source out-zone destination in-zone
 service-policy type inspect p1
!
interface GigabitEthernet0/0
 description Connection to IPMAN FNN N6006654R
 bandwidth 6000
 ip address 203.0.113.1 255.255.255.0
 ip wccp 62 redirect in
 ip flow ingress
 ip flow egress
 zone-member security out-zone
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 ip address 172.16.11.1 255.255.255.0
 no ip redirects
 no ip proxy-arp
 ip wccp 61 redirect in
 zone-member security in-zone
 duplex auto
 speed auto
!
interface SM1/0
 description WAAS Network Module Device Name dciacbra01c07
 ip address 192.168.10.1 255.255.255.0
 ip wccp redirect exclude in
 service-module ip address 192.168.183.46 255.255.255.252
 !Application: Restarted at Sat Jan  5 04:47:14 2008
 service-module ip default-gateway 192.168.183.45
 hold-queue 60 out
!
end
```

Déploiement de succursales WAAS avec périphérique en ligne

La figure illustre un déploiement de filiale WAAS qui a un périphérique WAE en ligne physiquement devant le routeur de service intégré. Puisque le périphérique WAE se trouve devant le périphérique, le pare-feu Cisco reçoit des paquets optimisés WAAS et, par conséquent, l'inspection de couche 7 côté client n'est pas prise en charge.



Le routeur qui exécute le pare-feu Cisco IOS® entre des périphériques WAAS ne voit que le trafic optimisé. La fonction ZBF surveille la connexion initiale en trois étapes (option TCP 33 et décalage du numéro de séquence) et ajuste automatiquement la fenêtre de séquence TCP attendue (ne modifie pas le numéro de séquence dans le paquet lui-même). Il applique des fonctionnalités complètes de pare-feu dynamique de couche 4 pour les sessions optimisées WAAS. La solution transparente WAAS facilite l'application du pare-feu par session avec pare-feu avec état et stratégies QoS.

Détails

- Le pare-feu voit un paquet SYN TCP normal avec l'option 0x21 et crée une session pour lui. Il n'y a aucun problème avec les interfaces d'entrée ou de sortie, car WCCP n'est pas impliqué. Le SYN-ACK de retour n'est pas un paquet redirigé et le pare-feu en prend note.
- Le pare-feu recherche l'option 0x21 dans SYN-ACK et effectue le saut du numéro de séquence, si nécessaire. Il désactive également l'inspection L7 si la connexion est optimisée.
- Il est à noter que le seul aspect qui distingue cette opération du scénario Router-1 est que le trafic de retour n'est pas redirigé. Il n'y a pas 2 demi-connexions sur cette boîte.

Configuration

Configuration ZBF standard sans zone spécifique pour le trafic WAAS. Seule l'inspection de couche 7 n'est pas prise en charge.

Restrictions relatives à l'interopérabilité ZBF avec WAAS

- La méthode de redirection de couche 2 WCCP n'est pas prise en charge sur le pare-feu Cisco IOS®, elle prend uniquement en charge la redirection GRE (Generic Routing Encapsulation).
- Le pare-feu Cisco IOS® prend uniquement en charge la redirection WCCP. Si WAAS utilise le routage basé sur des politiques (PBR) pour obtenir la redirection des paquets, cette solution

ne garantit PAS l'interopérabilité et donc pas la prise en charge.
- Le pare-feu Cisco IOS® n'effectue pas d'inspection L7 sur les sessions TCP optimisées WAAS.
- Le pare-feu Cisco IOS® nécessite les commandes CLI **ip inspect waas enable** et **ip wccp notify** pour la redirection WCCP.
- Le pare-feu Cisco IOS® avec interopérabilité NAT et WAAS-NM n'est pas pris en charge pour le moment.
- La redirection WAAS du pare-feu Cisco IOS® est appliquée uniquement aux paquets TCP.
- Le pare-feu Cisco IOS® ne prend pas en charge les topologies actives/actives.
- Tous les paquets qui appartiennent à une session DOIVENT traverser la zone de pare-feu Cisco IOS®.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Guide de configuration de la sécurité : Pare-feu de stratégie basé sur les zones, Cisco IOS version 15M&T
- Guide de conception et d'application du pare-feu de stratégie basé sur la zone
- Support et documentation techniques - Cisco Systems