IOS : La zone a basé l'Interopérabilité de Pare-feu avec le déploiement WAAS

Contenu

La version de logiciel 12.4(6)T de Cisco IOS® a introduit le Pare-feu basé sur zone de stratégie (ZBPFW), 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.

Le Pare-feu basé sur zone de stratégie (également connu sous le nom de Pare-feu de Zone-stratégie, ou ZFW) change la configuration de Pare-feu du modèle basé sur interface plus ancien (CBAC) à un modèle basé sur zone plus flexible et plus facilement compréhensible. Des 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 .

Des politiques de pare-feu sont configurées avec la politique linguistique de Cisco® (CPL), qui utilise une structure hiérarchisée pour définir l'inspection pour des protocoles de réseau et les groupes d'hôtes auxquels l'inspection sera appliquée.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez une compréhension de base du Cisco IOS® CLI.

Composants utilisés

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

- Routeurs de la gamme Cisco 2900
- Version de logiciel d'IOS Software 15.2(4) m2

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.

Support WAAS avec le Pare-feu Cisco IOS

Le support WAAS (Services d'applications de réseau étendu Cisco) avec le Pare-feu Cisco IOS a été introduit dans la Cisco IOS version 12.4(15)T. Il fournit un pare-feu intégré qui optimise des WAN conformes à la sécurité et des solutions d'accélération des applications avec les avantages suivants :

- Optimise un WAN par de pleines capacités d'inspection avec état.
- Simplifie la conformité du secteur de carte de paiement (PCI).
- Protège le trafic accéléré par WAN transparent.
- Intègre des réseaux WAAS d'une manière transparente.
- Prend en charge les modules du matériel de Gestion de réseau (NME) WAE (engine d'application d'étendu) ou le déploiement autonome de périphérique WAAS.

WAAS a un mécanisme automatique de détection qui utilise des options de TCP pendant la connexion en trois étapes initiale utilisée pour identifier des périphériques WAE d'une manière transparente. Après détection automatique, la circulation optimisée (chemins) éprouve un changement du numéro de séquence de TCP pour permettre à des points finaux pour distinguer la circulation optimisée et nonoptimized.

Le soutien WAAS du pare-feu d'IOS tient compte du réglage des variables d'état internes de TCP utilisées pour l'inspection de la couche 4, basé sur la variation dans le numéro de séquence mentionné ci-dessus. Si le Pare-feu Cisco IOS note qu'une circulation s'est avec succès terminée la détection automatique WAAS, elle permet le shift de nombre de séquence initiale pour la circulation et met à jour l'état de la couche 4 sur la circulation optimisée.

Scénarios de déploiement d'optimisation de la circulation WAAS

Les sections suivantes décrivent deux scénarios différents d'optimisation de la circulation WAAS pour des déploiements de succursale. L'optimisation de la circulation WAAS fonctionne avec la fonctionnalité de pare-feu de Cisco sur un Integrated Services Router de Cisco (ISR).

La figure ci-dessous affiche un exemple d'une optimisation de la circulation de bout en bout WAAS avec le Pare-feu de Cisco. Dans ce déploiement particulier, un matériel de Gestion de réseau (NME) - périphérique WAE est sur le même périphérique que le Pare-feu de Cisco. Le Web Cache Communication Protocol (WCCP) est utilisé pour réorienter le trafic pour l'interception.

- **Déploiement de branchement WAAS avec un périphérique de Hors fonction-chemin**
- **Déploiement de branchement WAAS avec un périphérique intégré**

Déploiement de branchement WAAS avec un périphérique de Hors fonction-chemin

Un périphérique de l'engine d'application d'étendu (WAE) peut être un périphérique autonome de l'engine d'automatisation de WAN Cisco (WAE) ou un module réseau de Cisco WAAS (NME-WAE) qui est installé sur un Integrated Services Router (ISR) comme une engine de service intégré (suivant les indications du déploiement de branchement de service d'application d'étendu de figure [WAAS]).

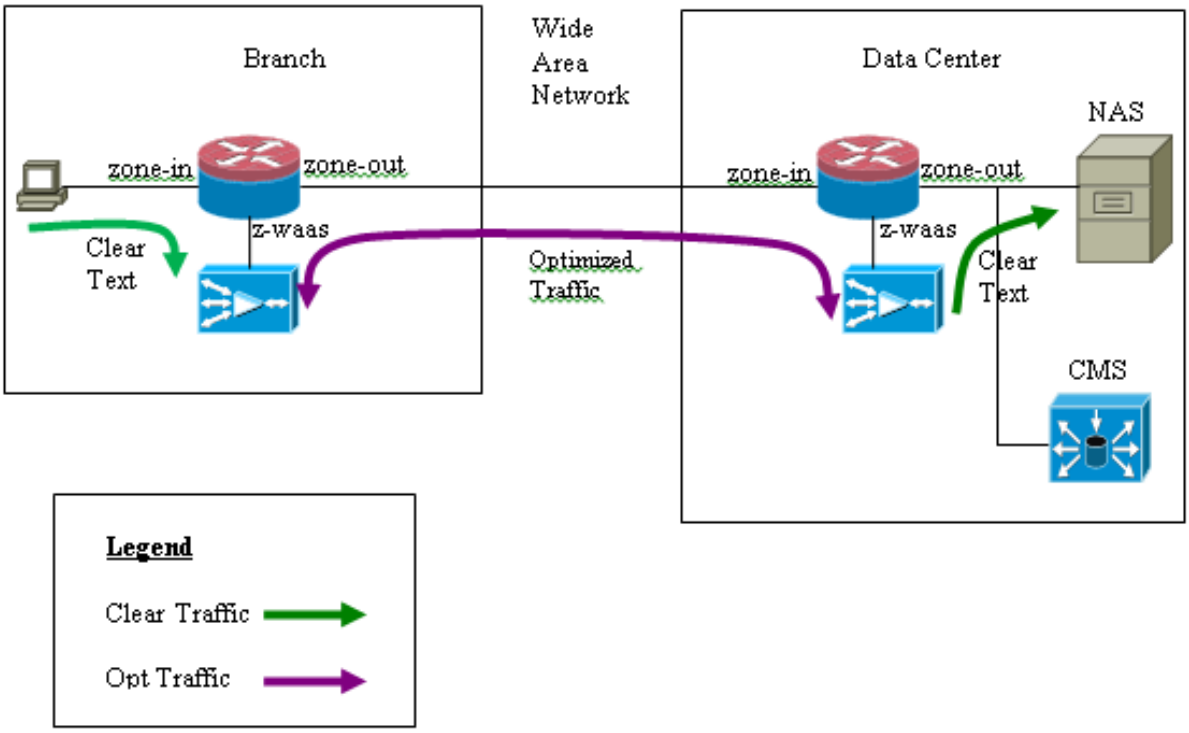
La figure ci-dessous affiche un déploiement de branchement WAAS qui emploie le Web Cache Communication Protocol (WCCP) pour réorienter le trafic à un hors fonction-chemin, périphérique autonome WAE pour l'interception du trafic. La configuration pour cette option est identique comme le déploiement de branchement WAAS avec un NME-WAE.

Exemple de schéma de réseau

Configuration et écoulement de paquet

Ce qui suit est un diagramme dépeignant une installation d'exemple avec l'optimisation WAAS activée pour le trafic et le CMS de bout en bout

(Système de gestion centralisé) étant présent à l'extrémité de serveur. Les modules de waas actuels à l'extrémité de branchement et à l'extrémité de Data Center doivent s'inscrire au CMS pour leurs exécutions. On l'observe que les utilisations HTTPS CMS pour lui est transmission avec les modules WAAS.



La circulation de bout en bout WAAS

L'exemple suivant fournit une configuration de bout en bout d'optimisation de la circulation WAAS pour le Pare-feu Cisco IOS qui emploie le WCCP pour réorienter le trafic à un périphérique WAE pour l'interception du trafic

Section 1 : Config relatif IOS-FW WCCP

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

Section 2 : Config de 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 : Config de zone et de zone-paire 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 d'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
```

Notez la nouvelle configuration dans les Cisco IOS versions 12.4(20)T et 12.4(22)T place l'intégrer-service-engine dans sa propre zone et n'a pas besoin de faire partie de n'importe quel zone-paire. Les zone-paire sont configurés entre zone-dans et zone-.

```
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
```

Sans la zone configurée sur le service intégré — Le trafic Enginel/0 obtient relâché avec le message de baisse suivant :

```
*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
```

La circulation CMS (périphérique WAAS s'inscrivant au gestionnaire central)

L'exemple suivant fournit le config pour les les deux les scénarios répertoriés ci-dessous :

- configuration de bout en bout d'optimisation de la circulation WAAS pour le Pare-feu Cisco IOS qui emploie le WCCP pour réorienter le trafic à un périphérique WAE pour l'interception du trafic
- Permettre le trafic CMS (le trafic d'administration WAAS circulant à/de le CMS de/à des périphériques WAAS).

Section 1 : Config relatif IOS-FW WCCP

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

Section 2 : Config de 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

Notez le class map ci-dessous est nécessaire pour permettre au trafic CMS pour intervenir.

```
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 : Config de zone et de zone-paire 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 : Config relatif de zone et de zone-paire CMS IOS-FW

Notez le *waas-out de* zone-paire et des ***out-waas*** sont exigés pour appliquer la stratégie créée ci-dessus 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 d'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

Notez la liste d'accès qui est utilisée pour le trafic CMS. Il permet le trafic HTTPS dans les les deux les 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
```

Les informations de session ZBF

L'utilisateur chez 172.16.11.10 derrière le routeur R1 accède au serveur de fichiers hébergé derrière l'extrémité distante avec une adresse IP de 172.16.10.10, la session ZBF est établie de dans- le zone-paire et ensuite le routeur réoriente le paquet à l'engine 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 établie dans R1-WAAS et R2-WAAS de l'intérieur de l'hôte 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%
```

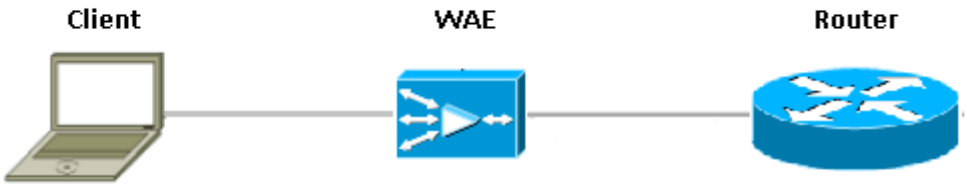
Configuration en cours du routeur de côté client (R1) avec WAAS et ZBF activés.

```
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 branchement WAAS avec un périphérique intégré

La figure ci-dessous affiche un déploiement de branchement du service d'application d'étendu (WAAS) qui a un périphérique intégré de l'engine d'application d'étendu (WAE) qui est physiquement devant l'Integrated Services Router (ISR). Puisque le périphérique WAE est devant le périphérique, le Pare-feu de Cisco reçoit les paquets optimisés par WAAS, et en conséquence, posez 7 que l'inspection sur le côté client n'est pas prise en charge.



Le routeur exécutant le pare-feu d'IOS entre les périphériques WAAS, voit seulement le trafic optimisé. Les montres de caractéristique ZBF pour la prise de contact à trois voies initiale (option 33 de TCP et le shift de numéro de séquence) et elle ajuste automatiquement la fenêtre prévue d'ordre de TCP (ne modifie pas le numéro de séquence dans le paquet lui-même). Il applique de pleines caractéristiques du pare-feu dynamique L4 pour les sessions optimisées par WAAS. La solution transparente WAAS facilite le Pare-feu imposent par pare-feu dynamique et stratégies QoS de session.

Détails

- Le Pare-feu voit un paquet normal de synchronisation de TCP avec l'option 0x21 et crée une session pour elle. Il n'y a aucune question avec les interfaces d'entrée ou de sortie puisque le WCCP n'est pas impliqué. Le retour SYN-ACK n'est pas un paquet réorienté et le Pare-feu note lui.
- Le Pare-feu vérifie l'option 0x21 dans le SYN-ACK et exécute l'accès de numéro de séquence s'il y a lieu. Il arrête également l'inspection L7 si la connexion est optimisée.
- Il doit être observé que le seul aspect qui distingue ceci du scénario Router-1 soit que le trafic de retour n'est pas réorienté. Il n'y a aucun 2" de demi » connexions sur cette case.

Configuration

Configuration standard ZBF sans toute zone spécifique pour le trafic WAAS. Seulement l'inspection de la couche 7 ne sera pas prise en charge.

Restrictions pour l'Interopérabilité ZBF avec WAAS

- La couche 2 WCCP réorientent la méthode n'est pas prise en charge sur le pare-feu d'IOS qu'elle prend en charge seulement la redirection d'Encapsulation de routage générique (GRE).
- Le pare-feu d'IOS prend en charge seulement la redirection WCCP. Si WAAS emploie le Routage à base de règles (PBR) pour obtenir des paquets réorientés, cette solution n'assurera pas l'Interopérabilité et par conséquent sans support.
- Le pare-feu d'IOS n'exécutera pas l'inspection L7 sur les sessions TCP optimisées par WAAS.
- Le pare-feu d'IOS exige **« l'enable de waas d'ip inspect »** et le **« ip wccp informent » des** commandes CLI pour la redirection WCCP**.**
- Le pare-feu d'IOS avec l'Interopérabilité NAT et WAAS-NM n'est pas pris en charge actuellement.
- La redirection du pare-feu d'IOS WAAS est seulement appliquée pour des paquets TCP.
- Le pare-feu d'IOS ne prend en charge pas topologies actives/actives. Tous les paquets appartenant à une session DOIVENT traverser la case du pare-feu d'IOS.

Informations connexes

Guide de configuration de sécurité : Pare-feu basé sur zone de stratégie, version de Cisco IOS 15M&T

Guide de conception et d'application du pare-feu de stratégie basé sur la zone