Cisco IOS Zone gebaseerde interoperabiliteit met WAAS-implementaties configureren

Inhoud

Inleiding

Dit document beschrijft een nieuw configuratiemodel voor de Cisco IOS® Firewall instelling. Dit nieuwe configuratiemodel biedt intuïtief beleid voor routers met meerdere interfaces, een verhoogde granulariteit van de toepassing van het firewallbeleid en een standaard ontkenningsbeleid dat verkeer tussen firewallbeveiligingszones verbiedt totdat een expliciet beleid wordt toegepast om gewenst verkeer mogelijk te maken.

Voorwaarden

Vereisten

Cisco raadt aan dat u kennis hebt van Cisco IOS® CLI.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 2900 Series routers
- Cisco IOS® softwarerelease 15.2(4)M2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Zone-Based Policy Firewall (ook bekend als Zone-Policy Firewall, ZFW of ZBF) wijzigt de firewallconfiguratie van het oudere op interface gebaseerde model (CBAC) naar een flexibeler, begrijpelijker op zone gebaseerd model. Interfaces worden toegewezen aan zones en het inspectiebeleid wordt toegepast op verkeer dat tussen de zones beweegt. Inter-zone beleid biedt aanzienlijke flexibiliteit en granulariteit, zodat verschillend inspectiebeleid kan worden toegepast op meerdere gastgroepen die met dezelfde routerinterface worden verbonden. Firewallbeleid wordt ingesteld met de Cisco® Policy Language (CPL), die een hiërarchische structuur gebruikt om de inspectie te definiëren voor netwerkprotocollen en de groepen hosts waarop de inspectie wordt toegepast.

WAAS-ondersteuning met Cisco IOS® Firewall

Wide Area Application Services (WAAS) ondersteuning met Cisco IOS® firewall is geïntroduceerd in Cisco IOS® release 12.4(15)T. Het voorziet in een geïntegreerde firewall die veiligheidsconforme WAN's en toepassingsversnellingsoplossingen met deze voordelen optimaliseert:

- Optimaliseert een WAN via volledige stateful inspection mogelijkheden
- Vereenvoudig de PCI-conformiteit (Payment Card Industry)
- Bescherm transparant WAN-versneld verkeer
- Geïntegreerde WAAS-netwerken
- Ondersteunt de netwerkbeheerapparatuur (NME) Wide Area Application Engine (WAE) modules voor standalone WAAS-apparaatimplementatie

WAAS heeft een automatisch zoekmechanisme dat TCP-opties gebruikt tijdens de eerste drie-weg handdruk die wordt gebruikt om WAE-apparaten op transparante wijze te identificeren. Na automatische ontdekking ervaren geoptimaliseerde verkeersstromen (paden) een verandering in het TCP-sequentienummer om de endpoints in staat te stellen onderscheid te maken tussen geoptimaliseerde en niet-geoptimaliseerde verkeersstromen.

De WAAS ondersteuning voor IOS® firewall staat voor het aanpassen van interne TCP status variabelen gebruikt voor Layer 4 inspectie, gebaseerd op de verschuiving in het eerder genoemde sequentienummer. Als de Cisco IOS® firewall opmerkt dat een verkeersstroom met succes WAAS automatische ontdekking heeft voltooid, maakt het de eerste sequentienummer verschuiving voor de verkeersstroom mogelijk en handhaaft de staat Layer 4 op de geoptimaliseerde verkeersstroom.

WAAS Traffic Flow Optimization Advanced Services

De secties beschrijven twee verschillende WAAS verkeersstroomoptimalisatiescenario's voor implementaties van kantoren. WAAS-optimalisatie van de verkeersstroom werkt met de Cisco-

firewallfunctie op een Cisco-geïntegreerde services router (ISR).

Het getal toont een voorbeeld van een end-to-end WAAS verkeersstroom optimalisatie met de Cisco firewall. In deze specifieke implementatie, is een NME-WAE apparaat op het zelfde apparaat zoals de firewall van Cisco. Web Cache Communication Protocol (WCCP) wordt gebruikt om het verkeer voor interceptie opnieuw te richten.

- WAAS Branch-implementatie met een apparaat dat niet op pad is
- WAAS Branch-implementatie met een inline apparaat

WAAS Branch-implementatie met een apparaat dat buiten het pad valt

Een WAE-apparaat kan een standalone Cisco WAN Automation Engine (WAE) apparaat of een Cisco WAAS-netwerkmodule (NME-WAE) zijn die op een ISR als geïntegreerde servicemodule is geïnstalleerd.

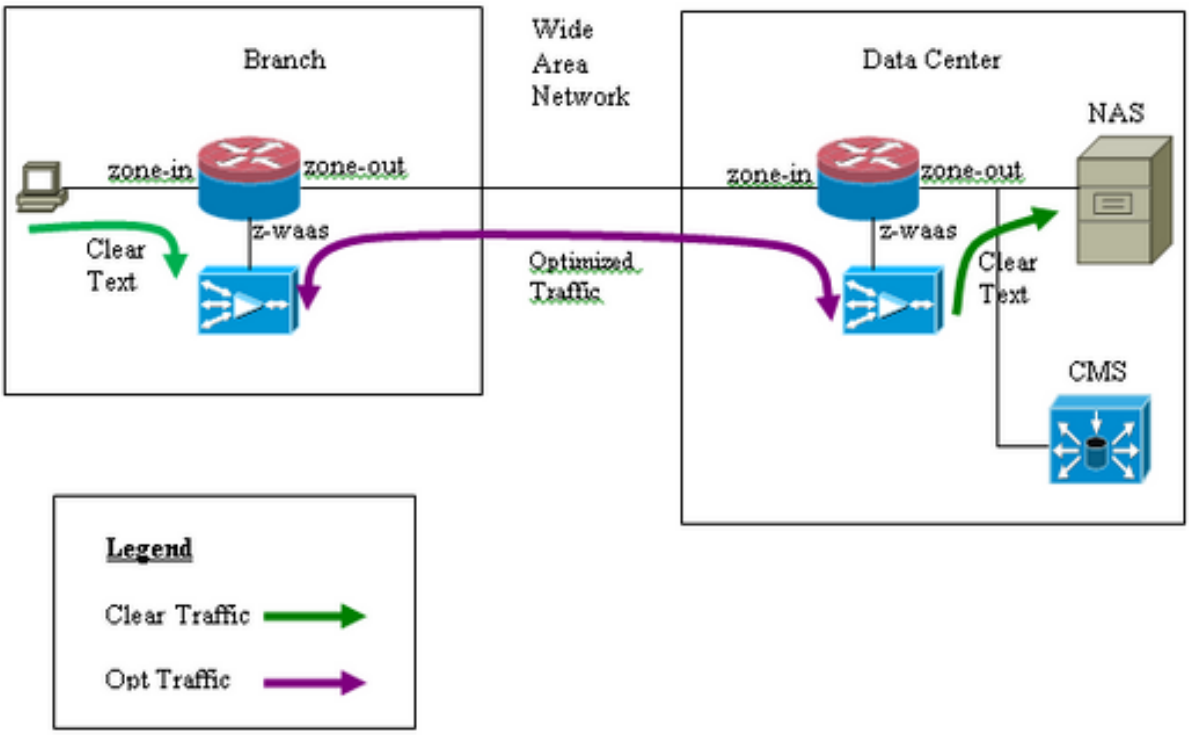
Het getal toont een WAAS-kanaalplaatsing die WCCP gebruikt om het verkeer om te leiden naar een off-path, standalone WAE-apparaat voor verkeersinterceptie. De configuratie voor deze optie is hetzelfde als de WAAS-kanaalplaatsing met een NME-WAE.

Netwerkdiagram

Configuratie en pakketstroom

In dit schema wordt een voorbeeldinstelling weergegeven met WAAS-optimalisatie ingeschakeld

voor end-to-end verkeer en gecentraliseerd beheersysteem (CMS) dat aan het einde van de server aanwezig is. De WAAS-modules die aanwezig zijn aan de Branch-kant en het datacenter-einde (DC) moeten zich voor hun activiteiten bij de CMS registreren. Er wordt op gewezen dat de CMS HTTPS gebruikt voor de communicatie met de WAAS-modules.



End-to-end WAAS-verkeer

Het voorbeeld hier biedt een end-to-end WAAS traffic flow optimization-configuratie voor de Cisco IOS® firewall die WCCP gebruikt om het verkeer om te leiden naar een WAE-apparaat voor verkeersinterceptie.

Sectie 1. IOS-FW WCCP-gerelateerde configuratie:

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

Sectie 2. IOS-FW beleidsconfiguratie:

```
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
```

Sectie 3. IOS-FW Zone en Zone-paarconfiguratie:

```
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
```

Deel 4: Interfaceconfiguratie:

```
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
```

> Opmerking: De nieuwe configuratie in Cisco IOS® release 12.4(20)T en 12.4(22)T plaatst de geïntegreerde service-motor in zijn eigen zone en hoeft geen deel uit te maken van een zonepaar. De zoneparen worden ingesteld tussen zone-in en 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
```

Zonder zone ingesteld op de Integrated—Service—Enginel/0, wordt er verkeer gedropt met dit drop-bericht:

```
*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
```

CMS Traffic Flow (WAAS-apparaat dat zich registreert bij Central Manager)

Het voorbeeld hier geeft de configuratie voor beide scenario's aan:

- End-to-end WAAS traffic flow optimization voor de Cisco IOS® firewall die WCCP gebruikt om het verkeer te richten op een WAE-apparaat voor verkeersinterceptie
- Toewijzing van het CMS-verkeer (WAAS-beheerverkeer dat van/naar WAAS-apparaten stroomt)

Sectie 1. IOS-FW WCCP-gerelateerde configuratie:

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

Sectie 2. IOS-FW beleidsconfiguratie:

```
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
```

Deel 2.1. IOS-FW-beleid met betrekking tot CMS-verkeer:

Opmerking: Er is een klassenkaart nodig om het CMS-verkeer te laten doorlopen:

```
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
```

Sectie 3. IOS-FW Zone en Zone-paarconfiguratie:

```
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
```

Sectie 3.1. IOS-FW CMS-gerelateerde configuratie van zone en zone-paar:

Opmerking: De zoneparen **waren** uitgeput **en** zijn nodig om het eerder voor CMS-verkeer ingevoerde beleid toe te passen.

```
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
```

Deel 4: Interfaceconfiguratie:

```
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
```

Deel 5: Toegangslijst voor CMS-verkeer.

> Opmerking: Toegangslijst die wordt gebruikt voor CMS-verkeer. Er is HTTPS-verkeer in beide richtingen mogelijk, omdat er HTTPS-verkeer is.

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

ZBF-sessieinformatie

Gebruiker op 172.16.11.10 achter Router R1 heeft toegang tot de bestandsserver achter het afstandsbediening met een IP-adres van 172.16.10.10. De ZBF-sessie is gebouwd vanaf een in-out zone-paar en vervolgens stuurt de router het pakket naar een WAAS-motor voor optimalisatie.

```
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]
```

Sessiebeheer ingebouwd in R1-WAAS en R2-WAAS van binnenhost naar externe server.

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%
```

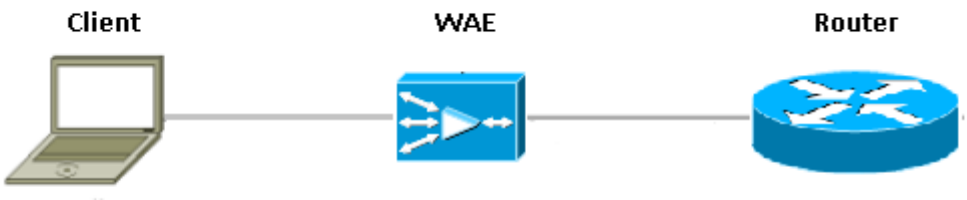
Configuratie van clientrouter (R1) met WAAS en ZBF ingeschakeld

```
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
```

WAAS Branch-implementatie met inline apparaat

Het getal toont een WAAS tak plaatsing die een inline WAE apparaat fysiek voor ISR heeft. Aangezien het WAE-apparaat voor het apparaat staat, wordt de Cisco-firewall geoptimaliseerde pakketten met WAAS ontvangen, en als resultaat hiervan wordt Layer 7-inspectie aan de clientkant niet ondersteund.



De router die de Cisco IOS® Firewall tussen WAAS apparaten in werking stelt, ziet alleen optimaal verkeer. De ZBF functie kijkt voor eerste drie manieren handdruk (TCP optie 33 en de sequentienummer shift) en het past automatisch het verwachte TCP-sequentievenster aan (wijzigt het sequentienummer niet in het pakket zelf). Het past volledige L4 stateful firewallfuncties toe voor de WAAS geoptimaliseerde sessies. WAAS transparante oplossing vergemakkelijkt de handhaving van firewall per sessie van stateful firewall en QoS-beleid.

Details

- Firewall ziet een normaal TCP SYN-pakket met de optie 0x21 en maakt er een sessie voor. Er zijn geen problemen met de input- of uitvoerinterfaces, aangezien WCCP niet bij het proces is betrokken. De terugkeer SYN-ACK is geen omgebogen pakket en de firewall neemt hiervan nota.
- Firewall controleert voor de optie 0x21 in de SYN-ACK en voert indien nodig de sprong in het sequentienummer uit. Ook wordt de L7-inspectie uitgeschakeld als de verbinding wordt geoptimaliseerd.
- Het enige aspect dat dit onderscheidt van het routerscenario is dat het retourverkeer niet wordt omgeleid. Dit vak bevat geen 2 halve aansluitingen.

Configuratie

Standaard ZBF-configuratie zonder specifieke zone voor WAAS-verkeer. Alleen Layer 7 inspectie wordt niet ondersteund.

Beperkingen voor ZBF-interoperabiliteit met WAAS

- WCCP Layer 2 redirect-methode wordt niet ondersteund op Cisco IOS® firewall, maar ondersteunt alleen Generic Routing Encapsulation (GRE)-omleiding.
- Cisco IOS® Firewall ondersteunt alleen WCCP-omleiding. Als WAAS op beleid gebaseerde routing (PBR) gebruikt om de pakketten te hersturen, garandeert deze oplossing NIET

interoperabiliteit en wordt er daarom niet ondersteund.
- Cisco IOS® firewall voert geen L7-inspectie uit op WAAS geoptimaliseerde TCP-sessies.
- Voor Cisco IOS® firewalls is **IP-inspectie** nodig, en **ip wcp stelt** CLI-opdrachten **bij** voor WCCP-omleiding.
- Cisco IOS® firewall met NAT en WAAS-NM interoperabiliteit wordt momenteel niet ondersteund.
- Cisco IOS® WAAS-omleiding is alleen van toepassing op TCP-pakketten.
- Cisco IOS® firewall ondersteunt geen actieve/actieve topologieën.
- Alle pakketten die tot een sessie behoren MOETEN door het vakje Cisco IOS® firewall stromen.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- Security configuratiegids: Zone-Based Policy Firewall, Cisco IOS release 15M&T
- Zone-Based Policy Firewall Design and Application Guide
- Technische ondersteuning en documentatie – Cisco Systems