Configurazione dell'interoperabilità del firewall basato su zone Cisco IOS con l'implementazione WAAS

Sommario

Introduzione

In questo documento viene descritto un nuovo modello di configurazione per il set di funzionalità di Cisco IOS® Firewall. Questo nuovo modello di configurazione offre criteri intuitivi per router con più interfacce, una maggiore granularità dell'applicazione dei criteri firewall e un criterio di negazione totale predefinito che impedisce il traffico tra le aree di sicurezza del firewall fino a quando non viene applicato un criterio esplicito per consentire il traffico desiderato.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza della CLI di Cisco IOS®.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco serie 2900 Router
- Software Cisco IOS® versione 15.2(4) M2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Zone-Based Policy Firewall (noto anche come Zone-Policy Firewall, ZFW o ZBF) modifica la configurazione del firewall dal precedente modello basato su interfaccia (CBAC) a un modello basato su zona più flessibile e più facilmente comprensibile. Le interfacce vengono assegnate alle zone e i criteri di ispezione vengono applicati al traffico che si sposta tra le zone. Le policy interzona offrono notevole flessibilità e granularità, pertanto è possibile applicare policy di ispezione diverse a più gruppi host collegati alla stessa interfaccia router. I criteri firewall vengono configurati con Cisco® Policy Language (CPL), che utilizza una struttura gerarchica per definire l'ispezione per i protocolli di rete e i gruppi di host a cui viene applicata l'ispezione.

Supporto WAAS con Cisco IOS® Firewall

Il supporto WAAS (Wide Area Application Services) con firewall Cisco IOS® è stato introdotto in Cisco IOS® versione 12.4(15)T. Fornisce un firewall integrato che ottimizza le WAN conformi alla sicurezza e le soluzioni di accelerazione delle applicazioni con i seguenti vantaggi:

- Ottimizza una WAN grazie alle funzionalità complete di ispezione stateful
- Semplifica la conformità PCI (Payment Card Industry)
- Protezione del traffico accelerato trasparente sulla WAN
- Integrazione trasparente delle reti WAAS
- Supporta i moduli WAE (Wide Area Application Engine) NME (Network Management Equipment) o l'installazione di dispositivi WAAS autonomi

WAAS dispone di un meccanismo di rilevamento automatico che utilizza le opzioni TCP durante l'handshake iniziale a tre vie utilizzato per identificare i dispositivi WAE in modo trasparente. Dopo il rilevamento automatico, i flussi di traffico (percorsi) ottimizzati subiscono una modifica nel numero di sequenza TCP in modo da consentire agli endpoint di distinguere tra flussi di traffico ottimizzati e non ottimizzati.

Il supporto WAAS per il firewall IOS® consente la regolazione delle variabili di stato TCP interne utilizzate per l'ispezione sul layer 4, in base allo spostamento del numero di sequenza menzionato in precedenza. Se il firewall Cisco IOS® rileva che un flusso del traffico ha completato correttamente il rilevamento automatico WAAS, consente lo spostamento del numero di sequenza iniziale per il flusso del traffico e mantiene lo stato di layer 4 sul flusso del traffico ottimizzato.

Scenari di distribuzione di WAAS Traffic Flow Optimization

Nelle sezioni vengono descritti due diversi scenari di ottimizzazione del flusso del traffico WAAS per le installazioni nelle filiali. L'ottimizzazione del flusso del traffico WAAS funziona con la

funzionalità Cisco Firewall su un Cisco Integrated Services Router (ISR).

Nella figura viene mostrato un esempio di ottimizzazione completa del flusso del traffico WAAS con il firewall Cisco. In questa particolare implementazione, un dispositivo NAME-WAE si trova sullo stesso dispositivo del firewall Cisco. Il protocollo WCCP (Web Cache Communication Protocol) viene usato per reindirizzare il traffico per l'intercettazione.

- Installazione di filiali WAAS con un dispositivo off-path
- Distribuzione di branch WAAS con un dispositivo inline

Installazione di filiali WAAS con dispositivo off-path

Un dispositivo WAE può essere un dispositivo Cisco WAN Automation Engine (WAE) standalone o un Cisco WAAS Network Module (NME-WAE) installato su un ISR come motore di servizio integrato.

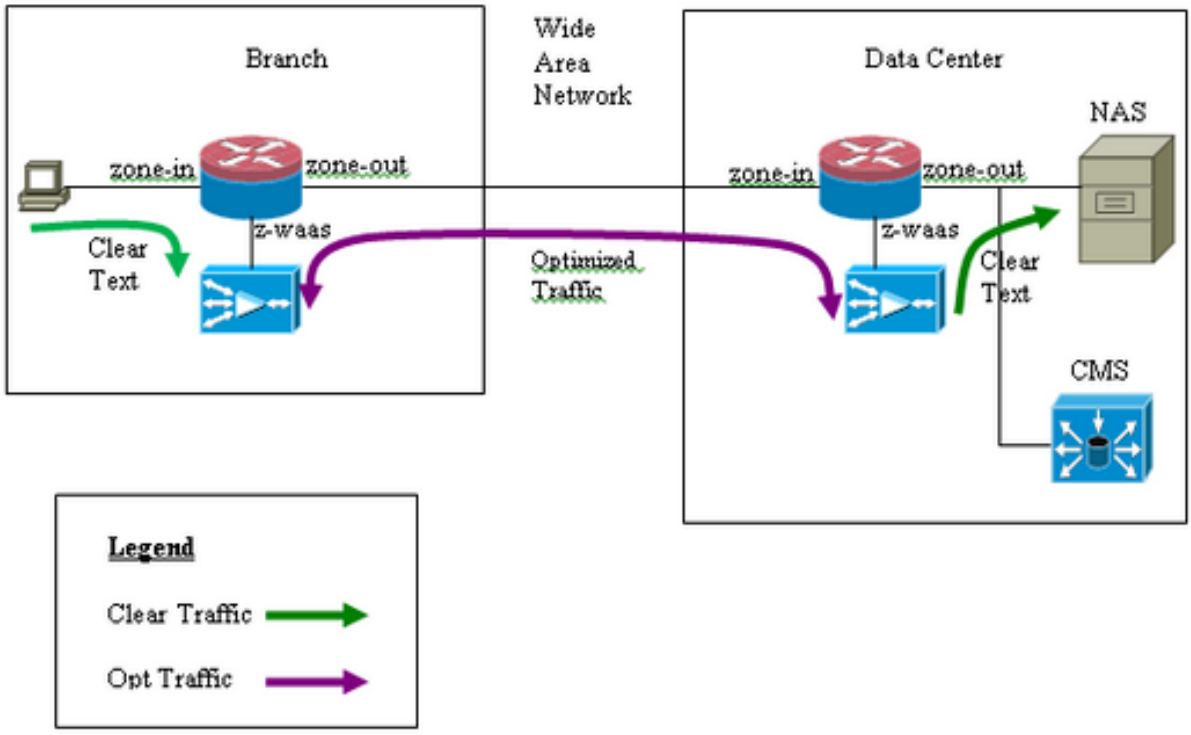
Nella figura viene illustrata un'implementazione di un branch WAAS che utilizza WCCP per reindirizzare il traffico a un dispositivo WAE standalone fuori percorso per l'intercettazione del traffico. La configurazione di questa opzione è la stessa della distribuzione del ramo WAAS con un nome WAE.

Esempio di rete

Configurazione e flusso del pacchetto

In questo diagramma viene illustrato un esempio di configurazione con l'ottimizzazione WAAS attivata per il traffico end-to-end e il sistema di gestione centralizzata (CMS, Centralized

Management System) presente all'estremità del server. I moduli WAAS presenti all'estremità della filiale e all'estremità del centro dati devono registrarsi presso il CMS per le operazioni. Si osserva che il CMS utilizza HTTPS per la comunicazione con i moduli WAAS.



Flusso di traffico WAAS end-to-end

Nell'esempio viene fornita una configurazione end-to-end dell'ottimizzazione del flusso del traffico WAAS per il firewall Cisco IOS® che utilizza WCCP per reindirizzare il traffico a un dispositivo WAE per intercettarlo.

Sezione 1. Configurazione relativa a IOS-FW WCCP:

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

Sezione 2. Configurazione della policy 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
```

Sezione 3. Configurazione della zona e della coppia di zone 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
```

Sezione 4. Configurazione dell'interfaccia:

```
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
```

> **Nota:** La nuova configurazione di Cisco IOS® versione 12.4(20)T e 12.4(22)T colloca il motore di servizio integrato nella propria zona e non deve necessariamente far parte di una coppia di zone. Le coppie di zone sono configurate tra zona-in e zona-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
```

Senza una zona configurata sul servizio integrato Enginel/0, il traffico viene interrotto con questo messaggio:

```
*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
```

Flusso del traffico CMS (registrazione del dispositivo WAAS con Central Manager)

L'esempio seguente fornisce la configurazione per entrambi gli scenari elencati:

- Configurazione completa dell'ottimizzazione del flusso del traffico WAAS per il firewall Cisco IOS® che utilizza WCCP per reindirizzare il traffico a un dispositivo WAE per l'intercettazione
- Autorizzazione del traffico CMS (traffico di gestione WAAS da/verso dispositivi WAAS)

Sezione 1. Configurazione relativa a IOS-FW WCCP:

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

Sezione 2. Configurazione della policy 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
```

Sezione 2.1. Politica IOS-FW relativa al traffico CMS:

Nota: La mappa delle classi è necessaria per consentire il passaggio del traffico CMS:

```
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
```

Sezione 3. Configurazione della zona e della coppia di zone 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
```

Sezione 3.1. Configurazione della zona e della coppia di zone relativa al sistema CMS IOS-FW:

Nota: Le coppie di zone **waas-out** e **waas-out** sono necessarie per applicare i criteri creati in precedenza per il traffico 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
```

Sezione 4. Configurazione dell'interfaccia:

```
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
```

Sezione 5. Elenco degli accessi al traffico CMS.

> **Nota:** Access-list utilizzato per il traffico CMS. Consente il traffico HTTPS in entrambe le direzioni poiché il traffico CMS è HTTPS.

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

Informazioni sulla sessione ZBF

L'utente che accede alla versione 172.16.11.10 dietro il router R1 accede al file server ospitato dietro un'estremità remota con indirizzo IP 172.16.10.10. La sessione ZBF è creata da una coppia di zone in-out e successivamente il router reindirizza il pacchetto al motore WAAS per l'ottimizzazione.

```
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]
```

Sessione incorporata in R1-WAAS e R2-WAAS dall'host interno al server remoto.

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%
```

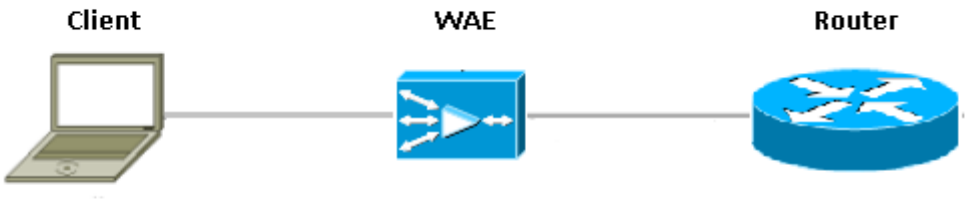
Configurazione operativa del router lato client (R1) con WAAS e ZBF abilitati

```
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
```

Distribuzione branch WAAS con dispositivo inline

Nella figura viene illustrata una distribuzione di un ramo WAAS con un dispositivo WAE in linea fisicamente davanti all'ISR. Poiché il dispositivo WAE si trova davanti al dispositivo, il firewall Cisco riceve pacchetti ottimizzati WAAS e, di conseguenza, l'ispezione di layer 7 sul lato client non è supportata.



Il router che esegue il firewall Cisco IOS® tra i dispositivi WAAS rileva solo il traffico ottimizzato. La funzione ZBF monitora l'handshake iniziale a tre vie (opzione TCP 3 e spostamento del numero di sequenza) e regola automaticamente la finestra di sequenza TCP prevista (non modifica il numero di sequenza nel pacchetto stesso). Applica funzionalità firewall complete con stato L4 per le sessioni ottimizzate WAAS. La soluzione WAAS trasparente facilita l'applicazione di firewall per sessione con conservazione dello stato e criteri QoS.

Dettagli

- Il firewall rileva un normale pacchetto TCP SYN con l'opzione 0x21 e crea una sessione per tale pacchetto. Non ci sono problemi con le interfacce di input o output perché WCCP non è coinvolto. Il SYN-ACK restituito non è un pacchetto reindirizzato e il firewall ne prende nota.
- Il firewall controlla l'opzione 0x21 nel SYN-ACK ed esegue il salto del numero di sequenza, se necessario. Disattiva inoltre l'ispezione L7 se la connessione è ottimizzata.
- Si deve osservare che l'unico aspetto che distingue questo dallo scenario del router-1 è che il traffico di ritorno non viene reindirizzato. Non ci sono 2 connessioni half in questa scatola.

Configurazione

Configurazione ZBF standard senza una zona specifica per il traffico WAAS. Non è supportata solo l'ispezione di livello 7.

Restrizioni per l'interoperabilità ZBF con WAAS

- Il metodo di reindirizzamento WCCP Layer 2 non è supportato sul firewall Cisco IOS®. Supporta solo il reindirizzamento GRE (Generic Routing Encapsulation).
- Cisco IOS® Firewall supporta solo il reindirizzamento WCCP. Se WAAS utilizza Policy Based Routing (PBR) per ottenere il reindirizzamento dei pacchetti, questa soluzione NON garantisce l'interoperabilità e quindi non è supportata.
- Il firewall Cisco IOS® non esegue l'ispezione L7 sulle sessioni TCP ottimizzate per WAAS.
- Il firewall Cisco IOS® richiede l'**abilitazione di ip inspect waas** e i comandi **ip wccp notification** CLI per il reindirizzamento WCCP.

- Al momento non è supportato il firewall Cisco IOS® con interoperabilità NAT e WAAS-NM.
- Il reindirizzamento WAAS del firewall Cisco IOS® viene applicato solo ai pacchetti TCP.
- Il firewall Cisco IOS® non supporta topologie attive/attive.
- Tutti i pacchetti che appartengono a una sessione DEVONO passare attraverso il firewall di Cisco IOS®.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Guida alla configurazione della protezione: Policy Firewall basato su zone, Cisco IOS release 15M&T
- Guida alla progettazione e all'applicazione di firewall per i criteri basati su zone
- Documentazione e supporto tecnico – Cisco Systems