Configuración de la Interoperabilidad del Firewall Basado en Zona de Cisco IOS con la Implementación de WAAS

Contenido

Introducción

Este documento describe un nuevo modelo de configuración para el conjunto de funciones de Cisco IOS® Firewall. Este nuevo modelo de configuración ofrece políticas intuitivas para routers de varias interfaces, mayor granularidad de la aplicación de políticas de firewall y una política predeterminada de deny-all que prohíbe el tráfico entre zonas de seguridad del firewall hasta que se aplica una política explícita para permitir el tráfico deseado.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento de Cisco IOS® CLI.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco 2900 series routers
- Versión 15.2(4) M2 del software del IOS® de Cisco

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.

Antecedentes

El firewall de políticas basado en zonas (también conocido como firewall de políticas de zona, ZFW o ZBF) cambia la configuración del firewall del modelo basado en interfaces antiguo (CBAC) a un modelo basado en zonas más flexible y fácil de entender. Las interfaces se asignan a zonas y la política de inspección se aplica al tráfico que se mueve entre las zonas. Las políticas entre zonas ofrecen considerable flexibilidad y granularity (especificidad), de modo que se pueden aplicar distintas políticas de inspección a varios grupos de hosts conectados a la misma interfaz del router. Las políticas de firewall se configuran con Cisco® Policy Language (CPL), que emplea una estructura jerárquica para definir la inspección de los protocolos de red y los grupos de hosts a los que se aplica la inspección.

Soporte WAAS con Cisco IOS® Firewall

La compatibilidad con los servicios Wide Area Application Services (WAAS) con el firewall Cisco IOS® se introdujo en la versión 12.4(15)T de Cisco IOS®. Proporciona un firewall integrado que optimiza las soluciones de aceleración de aplicaciones y WAN compatibles con la seguridad con estas ventajas:

- Optimiza una WAN mediante funciones de inspección exhaustiva
- Simplifica la conformidad con la industria de tarjetas de pago (PCI)
- Protege el tráfico acelerado de WAN transparente
- Integra las redes WAAS de forma transparente
- Admite los módulos de motor de aplicaciones de área extensa (WAE) del equipo de gestión de red (NME) o la implementación de dispositivos WAAS independientes

WAAS tiene un mecanismo de detección automática que utiliza las opciones TCP durante el intercambio de señales tridireccional inicial utilizado para identificar los dispositivos WAE de forma transparente. Después de la detección automática, los flujos de tráfico optimizados (trayectos) experimentan un cambio en el número de secuencia TCP para permitir que los terminales distingan entre flujos de tráfico optimizados y no optimizados.

El soporte WAAS para el firewall IOS® permite el ajuste de las variables de estado TCP internas utilizadas para la inspección de capa 4, en función del cambio en el número de secuencia mencionado anteriormente. Si el firewall Cisco IOS® detecta que un flujo de tráfico ha completado con éxito la detección automática WAAS, permite el cambio de número de secuencia inicial para el flujo de tráfico y mantiene el estado de Capa 4 en el flujo de tráfico optimizado.

Escenarios de implementación de optimización del flujo de tráfico WAAS

En las secciones se describen dos escenarios diferentes de optimización del flujo de tráfico WAAS para implementaciones en sucursales. La optimización del flujo de tráfico WAAS funciona con la función de firewall de Cisco en un router de servicios integrados (ISR) de Cisco.

La figura muestra un ejemplo de optimización del flujo de tráfico WAAS de extremo a extremo con el firewall de Cisco. En esta implementación en particular, un dispositivo NME-WAE se encuentra en el mismo dispositivo que el firewall de Cisco. El protocolo de comunicación de caché web (WCCP) se utiliza para redirigir el tráfico para interceptarlo.

- Implementación de sucursales WAAS con un dispositivo fuera de ruta
- Implementación de sucursales WAAS con un dispositivo en línea

Implementación de sucursales WAAS con dispositivos fuera de ruta

Un dispositivo WAE puede ser un dispositivo Cisco WAN Automation Engine (WAE) independiente o un módulo de red Cisco WAAS (NME-WAE) instalado en un ISR como motor de servicio integrado.

La figura muestra una implementación de sucursal WAAS que utiliza WCCP para redirigir el tráfico a un dispositivo WAE independiente y fuera de ruta para la intercepción del tráfico. La configuración para esta opción es la misma que la implementación de sucursales WAAS con un NME-WAE.

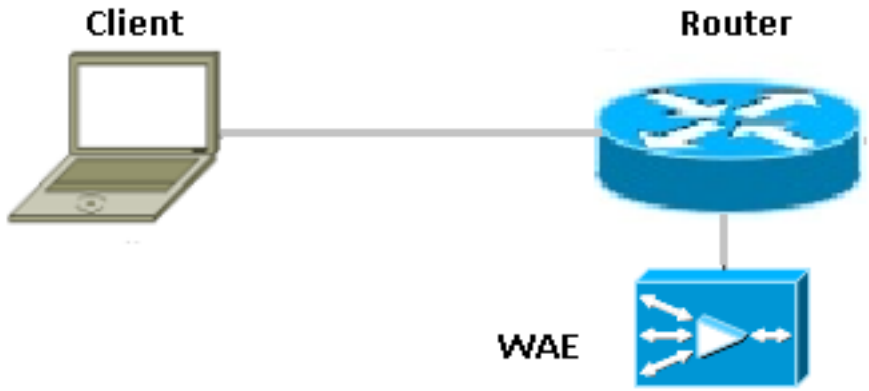
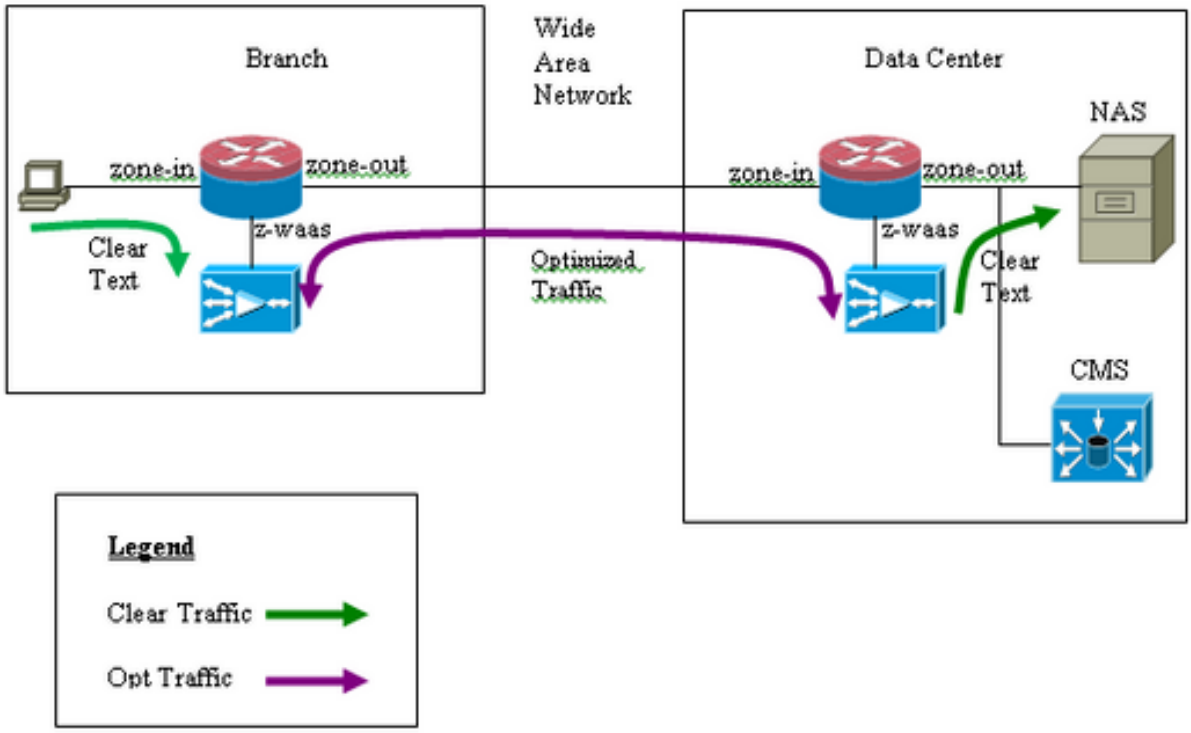


Diagrama de la red

Flujo de paquetes y configuración

Este diagrama muestra una configuración de ejemplo con la optimización de WAAS activada para el tráfico de extremo a extremo y el sistema de gestión centralizada (CMS) que está presente en el extremo del servidor. Los módulos WAAS presentes en el extremo de la sucursal y el extremo del Data Center (DC) deben registrarse en el CMS para sus operaciones. Se observa que el CMS utiliza HTTPS para su comunicación con los módulos WAAS.



Flujo de tráfico WAAS de extremo a extremo

El ejemplo aquí proporciona una configuración de optimización de flujo de tráfico WAAS de extremo a extremo para el firewall Cisco IOS® que utiliza WCCP para redirigir el tráfico a un dispositivo WAE para la intercepción del tráfico.

Sección 1. Configuración relacionada con WCCP de IOS-FW:

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

Sección 2. Configuración de la política 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
```

Sección 3. Configuración de zona y par de zonas de 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
```

Sección 4. Configuración de la interfaz:

```
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 nueva configuración en Cisco IOS® Release 12.4(20)T y 12.4(22)T coloca el motor de servicio integrado en su propia zona y no necesita ser parte de ningún par de zonas. Los pares de zonas se configuran entre zone-in y 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
```

Sin ninguna zona configurada en el servicio integrado: Enginel/0, el tráfico se descarta con este mensaje de descarte:

```
*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
```

Flujo de tráfico de CMS (dispositivo WAAS que se registra con Central Manager)

El ejemplo aquí proporciona la configuración para ambos escenarios enumerados:

- Configuración de optimización de flujo de tráfico WAAS de extremo a extremo para el firewall Cisco IOS® que utiliza WCCP para redirigir el tráfico a un dispositivo WAE para la intercepción del tráfico
- Permiso del tráfico de CMS (tráfico de administración de WAAS que fluye hacia/desde CMS desde/hacia dispositivos WAAS)

Sección 1. Configuración relacionada con WCCP de IOS-FW:

```
ip wccp 61
```

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

Sección 2. Configuración de la política 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
```

Sección 2.1. Política IOS-FW relacionada con el tráfico CMS:

> **Nota:** El mapa de clase aquí es necesario para permitir que pase el tráfico de 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
```

Sección 3. Configuración de zona y par de zonas de 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
```

Sección 3.1. Configuración de zona y par de zonas relacionada con CMS de IOS-FW:

> **Nota:** Los pares de zonas **waas-out** y **out-waas** son necesarios para aplicar la política creada anteriormente para el tráfico 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
```

Sección 4. Configuración de la interfaz:

```
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
```

Sección 5. Lista de acceso para el tráfico de CMS.

> **Nota:** Lista de acceso que se utiliza para el tráfico de CMS. Permite el tráfico HTTPS en ambas direcciones ya que el tráfico CMS es HTTPS.

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

Información de sesión ZBF

El usuario 172.16.11.10 que se encuentra detrás del router R1 accede al servidor de archivos alojado detrás de un extremo remoto con una dirección IP de 172.16.10.10. La sesión ZBF se genera a partir de un par de zonas de salida y, a continuación, el router redirige el paquete al motor WAAS para su optimización.

```
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]
```

Sesión integrada en R1-WAAS y R2-WAAS desde host interno a servidor 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%
```

Configuración en funcionamiento del router del lado del cliente (R1) con WAAS y ZBF habilitados

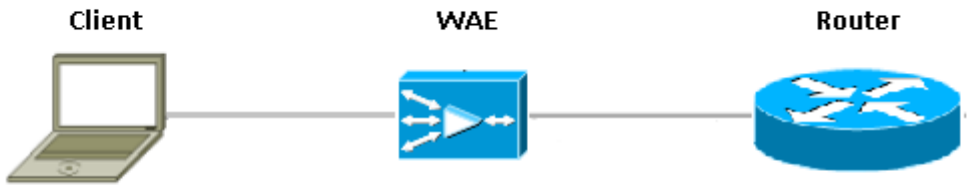
```
R1#sh run
Building configuration...
Current configuration : 3373 bytes
!
hostname R1
!
boot-start-marker
boot bootstrap tftp c2900-universalk9-mz.SPA.153-3.M4.bin 255.255.255.255
boot system flash c2900-universalk9-mz.SPA.153-3.M4.bin
boot-end-marker
!
ip wccp 61
```

```
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
```

Implementación de sucursales WAAS con dispositivo en línea

La figura muestra una implementación de sucursal WAAS que tiene un dispositivo WAE en línea físicamente delante del ISR. Dado que el dispositivo WAE está delante del dispositivo, el firewall de Cisco recibe paquetes optimizados WAAS y, como resultado, no se admite la inspección de capa 7 en el lado del cliente.



El router que ejecuta el Cisco IOS® Firewall entre dispositivos WAAS solo ve tráfico optimizado. La función ZBF vigila la entrada en contacto inicial de tres direcciones (opción TCP 33 y el cambio de número de secuencia) y ajusta automáticamente la ventana de secuencia TCP esperada (no modifica el número de secuencia en el paquete mismo). Aplica funciones completas de firewall con estado L4 para las sesiones optimizadas de WAAS. La solución transparente WAAS facilita el cumplimiento por parte del firewall de las políticas de QoS y de estado por sesión.

Detalles

- El firewall ve un paquete SYN TCP normal con la opción 0x21 y crea una sesión para él. No hay problemas con las interfaces de entrada o salida ya que WCCP no está involucrado. El SYN-ACK de retorno no es un paquete redirigido y el firewall toma nota de él.
- El firewall verifica la opción 0x21 en SYN-ACK y realiza el salto de número de secuencia, si es necesario. También desactiva la inspección L7 si la conexión está optimizada.
- Hay que observar que el único aspecto que lo distingue del escenario Router-1 es que el tráfico de retorno no se redirige. No hay 2 conexiones medias en esta caja.

Configuración

Configuración estándar ZBF sin ninguna zona específica para el tráfico WAAS. No se admite solo la inspección de capa 7.

Restricciones de la Interoperabilidad ZBF con WAAS

- El firewall Cisco IOS® no admite el método de redirección de capa 2 de WCCP, solo admite la redirección de encapsulación de routing genérico (GRE).

- Cisco IOS® Firewall sólo admite la redirección WCCP. Si WAAS utiliza el routing basado en políticas (PBR) para que los paquetes se redirijan, esta solución NO garantiza la interoperabilidad y, por lo tanto, no es compatible.
- El firewall Cisco IOS® no realiza la inspección L7 en las sesiones TCP optimizadas de WAAS.
- El firewall Cisco IOS® requiere los comandos **ip inspect waas enable** e **ip wccp notify** CLI para la redirección WCCP.
- El firewall Cisco IOS® con interoperabilidad NAT y WAAS-NM no es compatible actualmente.
- La redirección WAAS del firewall Cisco IOS® sólo se aplica a los paquetes TCP.
- El firewall Cisco IOS® no admite topologías activas/activas.
- Todos los paquetes que pertenecen a una sesión DEBEN fluir a través del cuadro de firewall Cisco IOS®.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Guía de configuración de seguridad: Firewall de políticas basado en zonas, Cisco IOS Release 15M&T
- Guía de Aplicación y Diseño de Zone-Based Policy Firewall
- Soporte Técnico y Documentación - Cisco Systems