Configurar a interoperabilidade do firewall com base na zona do Cisco IOS com a implantação do WAAS

Contents

Introduction

Este documento descreve um novo modelo de configuração para o conjunto de recursos do Cisco IOS® Firewall. Esse novo modelo de configuração oferece políticas intuitivas para roteadores de várias interfaces, maior granularidade de aplicação de política de firewall e uma política padrão de negação total que proíbe tráfego entre zonas de segurança de firewall até uma política explícita aplicada para permitir o tráfego desejável.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento da CLI do Cisco IOS®.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 2900 Series Routers
- Software Cisco IOS® versão 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.

Informações de Apoio

O Zone-Based Policy Firewall (também conhecido como Zone-Policy Firewall, ZFW ou ZBF) altera a configuração do firewall do modelo baseado em interface (CBAC) mais antigo para um modelo baseado em zona mais flexível e facilmente compreensível. As interfaces são atribuídas a zonas e a política de inspeção é aplicada ao tráfego que se move entre as zonas. As políticas entre as zonas oferecem flexibilidade e granularidade consideráveis; portanto, políticas de inspeção diferentes podem ser aplicadas a vários grupos de hosts conectados à mesma interface do roteador. As políticas de firewall são configuradas com o Cisco® Policy Language (CPL), que emprega uma estrutura hierárquica para definir a inspeção para protocolos de rede e os grupos de hosts aos quais a inspeção é aplicada.

Suporte a WAAS com Cisco IOS® Firewall

O suporte do Wide Area Application Services (WAAS) com o firewall Cisco IOS® foi introduzido no Cisco IOS® versão 12.4(15)T. Ele oferece um firewall integrado que otimiza WANs compatíveis com segurança e soluções de aceleração de aplicativos com estes benefícios:

- Otimiza uma WAN por meio de recursos completos de inspeção stateful
- Simplifica a conformidade com o setor de cartões de pagamento (PCI)
- Protege o tráfego acelerado de WAN transparente
- Integra redes WAAS de forma transparente
- Suporta os módulos do Network Management Equipment (NME) Wide Area Application Engine (WAE) ou a implantação de dispositivo WAAS autônomo

O WAAS tem um mecanismo de descoberta automática que usa opções de TCP durante o handshake triplo inicial usado para identificar dispositivos WAE de forma transparente. Após a descoberta automática, os fluxos de tráfego otimizados (caminhos) sofrem uma alteração no número de sequência TCP para permitir que os endpoints diferenciem entre fluxos de tráfego otimizados e não otimizados.

O suporte WAAS para o firewall IOS® permite o ajuste de variáveis de estado TCP internas usadas para inspeção da camada 4, com base na mudança no número de sequência mencionado anteriormente. Se o firewall do Cisco IOS® perceber que um fluxo de tráfego concluiu com êxito a detecção automática do WAAS, ele permite o turno do número de sequência inicial para o fluxo de tráfego e mantém o estado da Camada 4 no fluxo de tráfego otimizado.

Cenários de implantação da otimização do fluxo de tráfego WAAS

As seções descrevem dois cenários diferentes de otimização do fluxo de tráfego WAAS para

implantações em filiais. A otimização do fluxo de tráfego WAAS funciona com o recurso de firewall da Cisco em um Cisco Integrated Services Router (ISR).

A figura mostra um exemplo de otimização de fluxo de tráfego do WAAS de ponta a ponta com o firewall da Cisco. Nesta implantação específica, um dispositivo NME-WAE está no mesmo dispositivo que o firewall da Cisco. O Web Cache Communication Protocol (WCCP) é usado para redirecionar o tráfego para interceptação.

- Implantação de filial WAAS com um dispositivo fora de caminho
- Implantação da filial WAAS com um dispositivo em linha

Implantação da filial WAAS com dispositivo externo

Um dispositivo WAE pode ser um dispositivo autônomo do Cisco WAN Automation Engine (WAE) ou um Cisco WAAS Network Module (NME-WAE) instalado em um ISR como um mecanismo de serviço integrado.

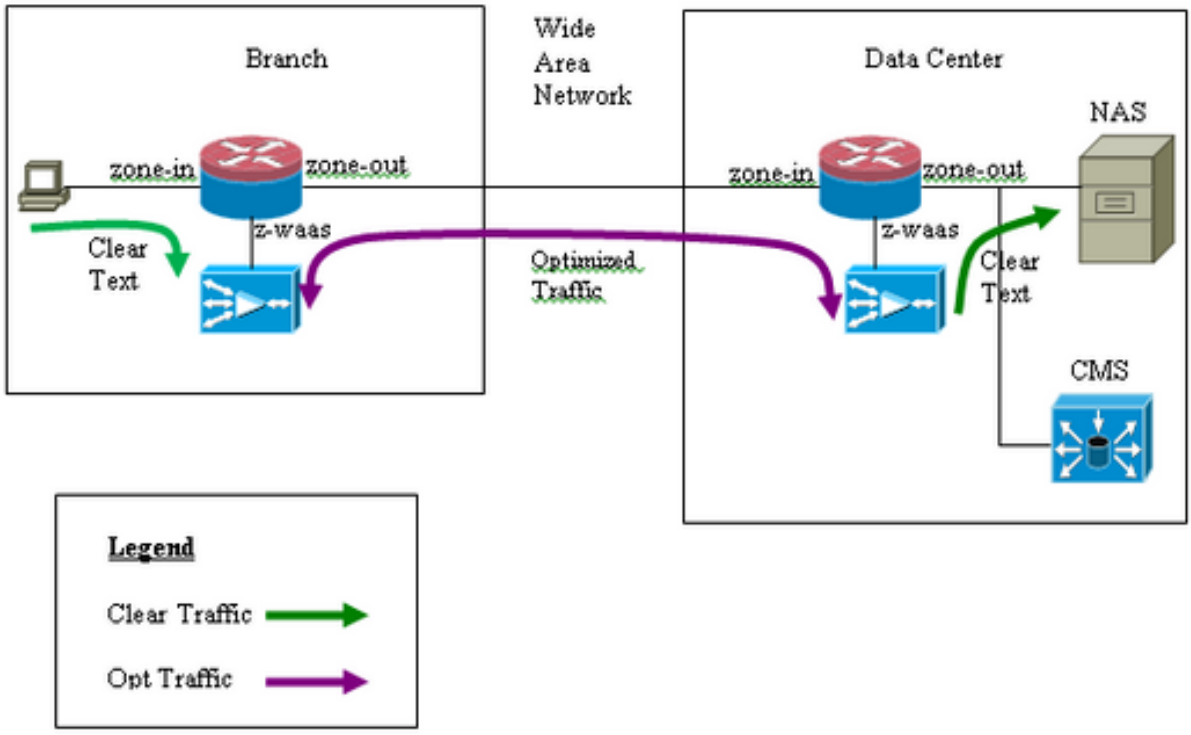
A figura mostra uma implantação de filial do WAAS que usa o WCCP para redirecionar o tráfego para um dispositivo WAE independente e fora do caminho para interceptação de tráfego. A configuração para essa opção é a mesma da implantação da filial WAAS com um NME-WAE.

Diagrama de Rede

Configuração e fluxo de pacote

Este diagrama descreve um exemplo de configuração com a otimização WAAS ativada para tráfego de ponta a ponta e o CMS (Centralized Management System) presente na extremidade do

servidor. Os módulos WAAS presentes na filial e a extremidade do data center (DC) precisam se registrar no CMS para suas operações. Observe que o CMS usa HTTPS para sua comunicação com os módulos WAAS.



Fluxo de tráfego de WAAS de ponta a ponta

O exemplo aqui fornece uma configuração de otimização de fluxo de tráfego do WAAS de ponta a ponta para o firewall Cisco IOS® que usa o WCCP para redirecionar o tráfego para um dispositivo WAE para interceptação de tráfego.

Seção 1. Configuração relacionada ao IOS-FW WCCP:

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

Seção 2. Configuração da 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
```

Seção 3. Configuração do IOS-FW Zone e Zone-pair:

```
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
```

Seção 4. Configuração da 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**: A nova configuração no Cisco IOS® versão 12.4(20)T e 12.4(22)T coloca o mecanismo de serviço integrado em sua própria zona e não precisa fazer parte de nenhum par de zonas. Os pares de zona são configurados entre 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
```

Sem zona configurada no Integrated—Service—Enginel/0, o tráfego é descartado com esta mensagem 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
```

Fluxo de tráfego do CMS (registro de dispositivo WAAS com Central Manager)

O exemplo aqui fornece a configuração para ambos os cenários listados:

- Configuração de otimização de fluxo de tráfego de WAAS de ponta a ponta para o firewall Cisco IOS® que usa WCCP para redirecionar o tráfego para um dispositivo WAE para interceptação de tráfego
- Permitindo o tráfego CMS (tráfego de gerenciamento WAAS que flui para/de CMS de/para dispositivos WAAS)

Seção 1. Configuração relacionada ao IOS-FW WCCP:

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

Seção 2. Configuração da 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
```

Seção 2.1. Política IOS-FW relacionada ao tráfego CMS:

Note: O mapa de classes aqui é necessário para permitir que o tráfego CMS passe por:

```
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
```

Seção 3. Configuração do IOS-FW Zone e Zone-pair:

```
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
```

Seção 3.1. Configuração de zona e par de zona relacionada ao CMS IOS-FW:

Note: Os pares de zona **waas-out** e **out-waas** são necessários para aplicar a política criada anteriormente para o tráfego 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
```

Seção 4. Configuração da 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
```

Seção 5. Lista de acesso para tráfego CMS.

> **Note**: Lista de acesso usada para tráfego CMS. Permite o tráfego HTTPS em ambas as direções, pois o tráfego CMS é HTTPS.

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

Informações da sessão ZBF

O usuário em 172.16.11.10 atrás do Roteador R1 acessa o servidor de arquivos hospedado atrás da extremidade remota com um endereço IP de 172.16.10.10, a sessão ZBF é construída do par de zona de entrada e, em seguida, o roteador redireciona o pacote para o mecanismo WAAS para otimização.

```
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]
```

Sessão integrada de R1-WAAS e R2-WAAS de host interno para 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%
```

Configuração funcional do roteador do lado do cliente (R1) com WAAS e ZBF ativados

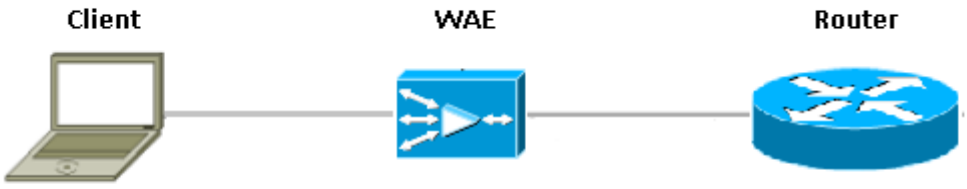
```
R1#sh run
Building configuration...
Current configuration : 3373 bytes
!
hostname R1
!
boot-start-marker
boot bootstrap tftp c2900-universalk9-mz.SPA.153-3.M4.bin 255.255.255.255
boot system flash c2900-universalk9-mz.SPA.153-3.M4.bin
boot-end-marker
!
ip wccp 61
ip wccp 62
no ipv6 cef
```

```
!
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
```

Implantação da filial WAAS com dispositivo em linha

A figura mostra uma implantação de filial WAAS que tem um dispositivo WAE em linha fisicamente na frente do ISR. Como o dispositivo WAE está na frente do dispositivo, o firewall da Cisco recebe pacotes otimizados de WAAS e, como resultado, a inspeção de Camada 7 no lado do cliente não é suportada.



O roteador que executa o Cisco IOS® Firewall entre dispositivos WAAS vê apenas tráfego otimizado. O recurso ZBF observa o handshake triplo inicial (opção TCP 33 e o turno do número de sequência) e ajusta automaticamente a janela de sequência TCP esperada (não altera o número de sequência no próprio pacote). Ele aplica todos os recursos de firewall stateful L4 para as sessões otimizadas do WAAS. A solução transparente WAAS facilita a aplicação do Firewall por firewall stateful por sessão e políticas de QoS.

Detalhes

- O firewall vê um pacote TCP SYN normal com a opção 0x21 e cria uma sessão para ele. Não há problemas com as interfaces de entrada ou saída, pois o WCCP não está envolvido. O SYN-ACK devolvido não é um pacote redirecionado e o firewall toma nota dele.
- O firewall verifica a opção 0x21 no SYN-ACK e executa o salto do número de sequência, se necessário. Ele também desliga a inspeção L7 se a conexão for otimizada.
- Observe-se que o único aspecto que distingue isso do cenário do Roteador 1 é que o tráfego de retorno não é redirecionado. Não há 2 meia conexão nesta caixa.

Configuração

Configuração ZBF padrão sem nenhuma zona específica para o tráfego WAAS. Somente a inspeção de Camada 7 não é suportada.

Restrições para interoperabilidade de ZBF com WAAS

- O método de redirecionamento de Camada 2 do WCCP não é suportado no firewall Cisco IOS®, ele suporta apenas o redirecionamento GRE (Generic Routing Encapsulation).
- O Cisco IOS® Firewall suporta apenas redirecionamento WCCP. Se o WAAS usar o Roteamento Baseado em Políticas (PBR - Policy Based Routing) para redirecionar os

pacotes, essa solução NÃO garante a interoperabilidade e, portanto, não é suportada.
- O firewall do Cisco IOS® não realiza inspeção L7 em sessões de TCP otimizadas para WAAS.
- O firewall do Cisco IOS® requer **ip inspect waas enable** e comandos CLI **ip wccp notify** para redirecionamento WCCP.
- O firewall Cisco IOS® com interoperabilidade de NAT e WAAS-NM não é suportado atualmente.
- O redirecionamento WAAS do firewall do Cisco IOS® é aplicado somente para pacotes TCP.
- O firewall do Cisco IOS® não suporta topologias ativas/ativas.
- Todos os pacotes que pertencem a uma sessão DEVEM fluir pela caixa de firewall do Cisco IOS®.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Guia de configuração de segurança: Firewall de política baseado em zona, Cisco IOS versão 15M&T
- Guia de aplicativos e design de firewall de política baseada em zona
- Suporte Técnico e Documentação - Cisco Systems