IO: A zona baseou a Interoperabilidade do Firewall com desenvolvimento WAAS

Índice

O Software Release 12.4(6)T de Cisco IOS® introduzido Zona-baseou o Firewall da política (ZBPFW), um modelo novo da configuração para o Cisco IOS Firewall Feature Set. Este modelo novo da configuração oferece políticas intuitivas para o Roteadores da interface múltipla, a granularidade aumentada do aplicativo da política de firewall, e um padrão negar-toda política que proibe o tráfego entre zonas de Segurança do Firewall até que uma política explícita esteja aplicada para permitir o tráfego desejável.

O Firewall Zona-baseado da política (igualmente conhecido como o Firewall da Zona-política, ou o ZFW) muda a configuração de firewall do modelo relação-baseado mais velho (CBAC) a um modelo zona-baseado mais flexível, mais de fácil compreensão. As relações são atribuídas às zonas, e a política da inspeção é aplicada para traficar mover-se entre as zonas. as políticas da Inter-zona oferecem a flexibilidade e a granularidade consideráveis, assim que as políticas diferentes da inspeção podem ser aplicadas aos grupos do host múltiplo conectados à relação do mesmo roteador.

As políticas de firewall são configuradas com a língua da política de Cisco® (COMPLETA), que emprega uma estrutura hierárquica para definir a inspeção para protocolos de rede e os grupos de anfitriões a que a inspeção será aplicada.

Pré-requisitos

Requisitos

Cisco recomenda que você tem uma compreensão básica do ® CLI do Cisco IOS.

Componentes Utilizados

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

- Cisco 2900 Series Routers
- IOS Software release 15.2(4) M2

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Apoio WAAS com Cisco IOS Firewall

O apoio WAAS (Wide Area Application Services) com Cisco IOS Firewall foi introduzido no Cisco IOS Release 12.4(15)T. Fornece um firewall integrada que aperfeiçoe WAN conformes a segurança e soluções da aceleração do aplicativo com os seguintes benefícios:

- Aperfeiçoa WAN com as capacidades completas da inspeção stateful.
- Simplifica a conformidade da indústria do cartão do pagamento (PCI).
- Protege o tráfego acelerado WAN transparente.
- Integra redes WAAS transparentemente.
- Apoia os módulos do equipamento do Gerenciamento de redes (NME) WAE (application engine da área ampla) ou o desenvolvimento autônomo do dispositivo WAAS.

WAAS tem um mecanismo de descoberta automático que use opções de TCP durante o cumprimento de três vias inicial usado para identificar transparentemente dispositivos WAE. Após a descoberta automática, os fluxos de tráfego aperfeiçoados (trajetos) experimentam uma mudança no número de sequência TCP para permitir que os valores-limite distingam entre fluxos de tráfego aperfeiçoados e nonoptimized.

O apoio WAAS para o firewall de IOS permite o ajuste dos variáveis de estado internos TCP usados para a inspeção da camada 4, com base na SHIFT no número de sequência mencionado acima. Se o Cisco IOS Firewall observa que um fluxo de tráfego terminou com sucesso a descoberta automática WAAS, permite a SHIFT do número de sequência inicial para o fluxo de tráfego e mantém o estado da camada 4 no fluxo de tráfego aperfeiçoado.

Cenários de distribuição da otimização do fluxo de tráfego WAAS

As seguintes seções descrevem duas encenações diferentes da otimização do fluxo de tráfego WAAS para disposições do escritório filial. A otimização do fluxo de tráfego WAAS trabalha com os recursos de firewall de Cisco em um roteador dos Serviços integrados de Cisco (ISR).

A figura abaixo mostra um exemplo de uma otimização fim-a-fim do fluxo de tráfego WAAS com o Firewall de Cisco. Neste desenvolvimento particular, um equipamento do Gerenciamento de redes (NME) - dispositivo WAE está no mesmo dispositivo que o Firewall de Cisco. O Protocolo de Comunicação de Cache da Web (WCCP) é usado para reorientar o tráfego para a intercepção.

- **Desenvolvimento do ramo WAAS com um dispositivo Fora-PATH**
- **Desenvolvimento do ramo WAAS com um dispositivo Inline**

Desenvolvimento do ramo WAAS com um dispositivo Fora-PATH

Um dispositivo do application engine da área ampla (WAE) pode ser um dispositivo MACILENTO autônomo do motor da automatização de Cisco (WAE) ou um módulo de rede de Cisco WAAS (NME-WAE) que seja instalado em um roteador dos Serviços integrados (ISR) como um motor do serviço integrado (segundo as indicações da figura desenvolvimento do ramo do [WAAS] dos serviços de aplicativo da área ampla).

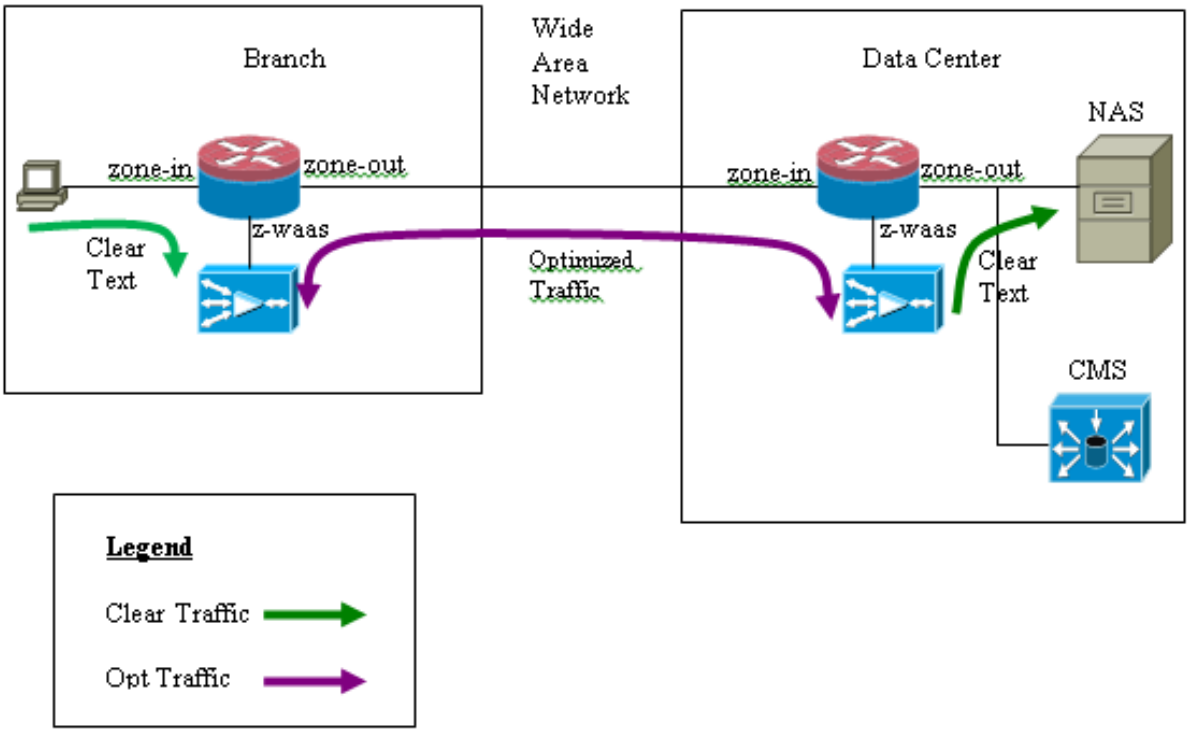
A figura abaixo mostra um desenvolvimento do ramo WAAS que use o Protocolo de Comunicação de Cache da Web (WCCP) para reorientar o tráfego a um fora-PATH, dispositivo autônomo WAE para a intercepção do tráfego. A configuração para esta opção é a mesma como o desenvolvimento do ramo WAAS com um NME-WAE.

Exemplo de diagrama de rede

Configuração e fluxo de pacote de informação

O seguinte é um diagrama que descreve uma instalação do exemplo com a otimização WAAS girada sobre para o tráfego de ponta a ponta e o CMS

(Sistema de gerenciamento centralizado) estando presente na extremidade do server. Os módulos dos waas atuais na extremidade do ramo e na extremidade do centro de dados precisam de registrar-se com o CMS para suas operações. Observa-se que os usos HTTPS CMS para ele são uma comunicação com os módulos WAAS.



Fluxo de tráfego fim-a-fim WAAS

O exemplo seguinte fornece uma configuração fim-a-fim da otimização do fluxo de tráfego WAAS para o Cisco IOS Firewall que usa o WCCP para reorientar o tráfego a um dispositivo WAE para a intercepção do tráfego

Seção 1: Configuração relacionada 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: Zona IOS-FW e configuração dos Zona-pares

```
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 relação

```
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 configuração nova no Cisco IOS Release 12.4(20)T e 12.4(22)T coloca o integrar-serviço-motor em sua própria zona e não o precisa de ser parte de qualquer zona-par. Os zona-pares são configurados no meio zona-em e zona-para fora.

```
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 a zona configurada no serviço integrado — O tráfego Enginel/0 obtém deixado cair com a seguinte mensagem de gota:

```
*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 CMS (dispositivo WAAS que se registra com gerente central)

O exemplo seguinte fornece a configuração para ambas as encenações alistadas abaixo:

- configuração fim-a-fim da otimização do fluxo de tráfego WAAS para o Cisco IOS Firewall que usa o WCCP para reorientar o tráfego a um dispositivo WAE para a intercepção do tráfego
- Permitindo o tráfego CMS (fluxo de tráfego de gerenciamento WAAS para/desde o CMS desde/até dispositivos WAAS).

Seção 1: Configuração relacionada 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
```

2.1 da seção: Política IOS-FW relativa ao tráfego CMS

Note a classe que o mapa abaixo é precisado de permitir que o tráfego CMS vá completamente.

```
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: Zona IOS-FW e configuração dos Zona-pares

```
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: Zona IOS-FW CMS e configuração relacionadas dos Zona-pares

Note o *waas-out dos zona*-pares e os ***out-waas*** são exigidos para aplicar a política criada acima 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 relação

```
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 o tráfego CMS

Note a lista de acesso que é usada para o tráfego CMS. Está permitindo o tráfego HTTPS em

ambos os sentidos porque o tráfego CMS é HTTPS.

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

Informação de sessão ZBF

O usuário em 172.16.11.10 atrás do r1 do roteador está alcançando o servidor de arquivo hospedado atrás da extremidade remota com um endereço IP de Um ou Mais Servidores Cisco ICM NT de 172.16.10.10, a sessão ZBF é construída -para fora nos zona-pares e depois disso o roteador reorienta o pacote ao motor WAAS para a 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 construída em R1-WAAS e em R2-WAAS do interior do host ao 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%
```

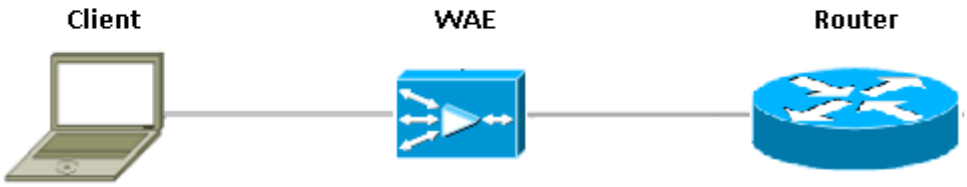
Configuração em funcionamento do roteador do lado do cliente (r1) com o WAAS e o ZBF permitidos.

```
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
```

Desenvolvimento do ramo WAAS com um dispositivo Inline

A figura abaixo mostra um desenvolvimento do ramo dos serviços de aplicativo da área ampla (WAAS) que tenha um dispositivo inline do application engine da área ampla (WAE) que seja fisicamente na frente do roteador dos Serviços integrados (ISR). Porque o dispositivo WAE é na frente do dispositivo, o Firewall de Cisco recebe pacotes aperfeiçoados WAAS, e em consequência, a inspeção da camada 7 no lado do cliente não é apoiada.



O roteador que executa o firewall de IOS entre dispositivos WAAS, vê somente o tráfego aperfeiçoado. Os relógios da característica ZBF para o reconhecimento de sentido da inicial três (opção de TCP 33 e a SHIFT do número de sequência) e ele ajustam automaticamente esperaram o indicador da sequência TCP (não altera o número de sequência no pacote próprio). Aplica características completas do firewall stateful L4 para as sessões aperfeiçoadas WAAS. A solução transparente WAAS facilita o Firewall reforça pelo firewall stateful e as políticas de QoS da sessão.

Detalhes

- O Firewall vê um pacote SYN de TCP normal com a opção 0x21 e cria uma sessão para ela. Não há nenhuma edição com a interface de entrada ou de saída desde que o WCCP não é involvido. O retorno SYN-ACK não é um pacote reorientado e o Firewall toma a nota dele.
- O Firewall verifica para ver se há a opção 0x21 no SYN-ACK e executa o salto do número de sequência caso necessário. Igualmente desliga a inspeção L7 se a conexão é aperfeiçoada.
- Deve ser observada que o único aspecto que distingue este da encenação Router-1 é que o tráfego de retorno não está reorientado. Não há nenhum 2" meias" conexões nesta caixa.

Configuração

Configuração padrão ZBF sem alguma zona específica para o tráfego WAAS. Somente a inspeção da camada 7 não será apoiada.

Limitações para a Interoperabilidade ZBF com WAAS

- A camada 2 WCCP reorienta o método não é apoiada no firewall de IOS que apoia somente a reorientação do Generic Routing Encapsulation (GRE).
- O firewall de IOS apoia somente o redirecionamento de WCCP. Se WAAS usa o Policy Based Routing (PBR) para obter pacotes reorientados, esta solução não assegurará a Interoperabilidade e daqui unsupported.
- O firewall de IOS não executará a inspeção L7 em sessões de TCP aperfeiçoadas WAAS.
- O firewall de IOS exige o **"IP inspeciona waas permite"** e **"o wccp IP notifica"** comandos CLI para o redirecionamento de WCCP.
- O firewall de IOS com Interoperabilidade NAT e WAAS-NM não é apoiado presentemente.
- A reorientação do firewall de IOS WAAS é somente aplicada para pacotes de TCP.
- O firewall de IOS não apoia o active/topologias ativa. Todos os pacotes que pertencem a uma sessão DEVEM correr através da caixa do firewall de IOS.

Informações Relacionadas

Guia de configuração de segurança: Firewall Zona-baseado da política, Cisco IOS Release

15M&T

Projeto do Firewall da política e guia Zona-baseados do aplicativo