Configurar o Zone-Based Firewall (ZBFW) co-localizado com o Cisco Unified Border Element (CUBE) Enterprise

Contents

Introduction
Prerequisites
Requirements
Componentes Utilizados
Informações de Apoio
Diagrama de Rede
Conceitos do curso de travamento ZBFW
Configurações
Definir Zonas de Segurança
Crie listas de acesso, mapas de classes e mapas de políticas para tráfego confiável
Criar mapeamentos de pares de zonas
Atribuir zonas a interfaces
Verificar
Exemplo de fluxo de pacote - Chamada
comandos show
show zone-pair security
show call ative voice compact
show voip rtp connections
show call ative voice brief
show sip-ua connections tcp detail
show policy-firewall sessions platform
show policy-map type inspect zone-pair sessions
Troubleshoot
CUBE Local Transcoding Interface (LTI) + ZBFW

Introduction

Este documento descreve como configurar o Zone-Based Firewall (ZBFW) co-localizado com o Cisco Unified Border Element (CUBE) Enterprise.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

- Roteador Cisco executando Cisco IOS® XE 17.10.1a

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. Se a rede estiver ativa,

certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

- A co-localização do CUBE Enterprise e ZBFW não era suportada no Cisco IOS XE até 16.7.1+

- O CUBE Enterprise suporta apenas fluxos de mídia CUBE + ZBFW RTP-RTP. Consulte: CSCwe66293

- Este documento não se aplica ao CUBE Media Proxy, ao CUBE Service Provider, aos gateways MGCP ou SCCP, aos gateways Cisco SRST ou ESRST, aos gateways H323 ou a outros gateways de voz analógicos/TDM.

- Para Gateways de Voz TDM/Analógica e ZBFW, consulte o seguinte documento: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/213550-troubleshoot-one-way-audio-problems-in-f.html

Diagrama de Rede

O exemplo de configuração ilustrará duas segmentações de rede lógica denominadas INSIDE e OUTSIDE.

INSIDE contém uma única rede IP e OUTSIDE contém duas redes IP.

Topologia de rede da camada 3

```
Endpoint_A - Network A - Gig1 - CUBE - Gig3 - Network B - CUCM
                                          \_ Network C - Endpoint_B
```

Fluxo de chamada da camada 7

```
Call Direction ========================================>
Endpoint_A > SIP > CUBE > SIP > CUCM > SIP > Endpoint_B
```

Fluxo de mídia da camada 7

```
Endpoint_A <> RTP <> CUBE <> RTP <> Endpoint_B
```

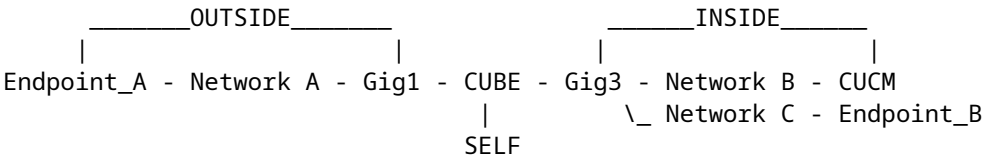
Conceitos do curso de travamento ZBFW

- Ao configurar o ZBFW, você configura um nome de zona de segurança que é então definido em uma interface. Depois disso, todo o tráfego de/para essa interface é associado a esse nome de região.
  - O tráfego de/para a mesma zona é sempre permitido.
  - O tráfego de/para diferentes regiões é descartado, a menos que seja permitido pela configuração do administrador.
- Para definir fluxos de tráfego permitidos, você deve criar um mapeamento de zona por meio de uma configuração unidirecional de par de zonas que defina os nomes de zona de origem e de destino.

    - Esse mapeamento de par de zonas é vinculado a uma política de serviço usada para fornecer controle granular sobre os tipos de tráfego inspecionados, permitidos e não permitidos.
- O CUBE Enterprise opera na zona especial SELF. A zona SELF inclui outro tráfego de/para o roteador, como ICMP, SSH, NTP, DNS, etc.
    - O PVDM de hardware para uso com o CUBE LTI não existe na autoregião e deve ser mapeado para uma região configurada administrativamente.
- O ZBFW não permite automaticamente o tráfego de retorno; portanto, um administrador deve configurar pares de zonas para definir o tráfego de retorno.

Com os 3 marcadores a seguir em mente, as seguintes zonas podem ser adicionadas sobrepostas em nossa topologia de rede L3, onde:

- Rede A, Gig1 são a zona EXTERNA
- A Rede B, a Rede C e o Gig3 são DENTRO da zona
- O CUBE faz parte da zona SELF



Em seguida, podemos criar logicamente os quatro mapeamentos unidirecionais de par de zonas de que precisamos para fluxos de tráfego através do CUBE+ZBFW:

Fonte	**Destino**	**Uso**
EXTERNA	PRÓPRIO	Mídia SIP e RTP de Entrada do Ponto de Extremidade A
PRÓPRIO	INTERNA	Mídia SIP e RTP de saída do CUBE para o CUCM e o endpoint B.
INTERNA	PRÓPRIO	Mídia SIP e RTP de entrada do CUCM e do endpoint B.
PRÓPRIO	EXTERNA	Mídia SIP e RTP de saída do CUBE para o endpoint A.

Com esses conceitos em mente, podemos começar a configurar o ZBFW no roteador Cisco IOS XE que atua como CUBE.

Configurações

Definir Zonas de Segurança

Lembre-se de que precisamos configurar duas zonas de segurança: INTERNA e EXTERNA. Não é necessário definir o valor próprio, pois ele é padrão.

```
!
zone security INSIDE
zone security OUTSIDE
!
```

Crie listas de acesso, mapas de classes e mapas de políticas para tráfego confiável

Para controlar qual tráfego devemos configurar métodos para que o Roteador corresponda e permita.

Para fazer isso, criaremos uma lista de acesso estendida, um mapa de classe e um mapa de políticas que inspecionam nosso tráfego.

Para simplificar, criaremos uma política para cada zona que mapeie o tráfego de entrada e saída.

Observe que configurações como **match protocol sip** e **match protocol sip-tls** podem ser usadas, mas para fins ilustrativos, o IP/Portas foram configurados

EXTERNA Lista de Acesso Estendida, Mapa de Classe, Mapa de Política

<#root>

```
! Define Access List with ACLs for OUTSIDE interface


ip access-list extended TRUSTED-ACL-OUT
 10 remark Match SIP TCP/UDP 5060 and TCP TLS 5061
 11 permit tcp 192.168.1.0 0.0.0.255 any range 5060 5061
 12 permit tcp any 192.168.1.0 0.0.0.255 range 5060 5061
 13 permit udp 192.168.1.0 0.0.0.255 any eq 5060
 14 permit udp any 192.168.1.0 0.0.0.255 eq 5060
 !
 20 remark Match RTP Port Range, IOS-XE and Remote Endpoints
 21 permit udp 192.168.1.0 0.0.0.255 any range 8000 48198
 22 permit udp any 192.168.1.0 0.0.0.255 range 8000 48198
!

! Tie ACL with Class Map


class-map type inspect match-any TRUSTED-CLASS-OUT
 match access-group name TRUSTED-ACL-OUT
!

! Tie Class Map with Policy and inspect


policy-map type inspect TRUSTED-POLICY-OUT
 class type inspect TRUSTED-CLASS-OUT
  inspect
 class class-default
  drop log
!
```

DENTRO da lista de acesso estendida, mapa de classe, mapa de política

```
!
ip access-list extended TRUSTED-ACL-IN
 1 remark SSH, NTP, DNS
 2 permit tcp any any eq 22
 3 permit udp any any eq 123
 4 permit udp any any eq 53
 !
 10 remark Match SIP TCP/UDP 5060 and TCP TLS 5061
 11 permit tcp 192.168.2.0 0.0.0.255 any range 5060 5061
 12 permit tcp any 192.168.2.0 0.0.0.255 range 5060 5061
 13 permit udp 192.168.2.0 0.0.0.255 any eq 5060
 14 permit udp any 192.168.2.0 0.0.0.255 eq 5060
 !
 20 remark Match RTP Port Range, IOS-XE and Remote Endpoints
 21 permit udp 192.168.2.0 0.0.0.255 any range 8000 48198
 22 permit udp any 192.168.2.0 0.0.0.255 range 8000 48198
 23 permit udp 192.168.3.0 0.0.0.31 any range 8000 48198
 24 permit udp any 192.168.3.0 0.0.0.31 range 8000 48198
!
class-map type inspect match-any TRUSTED-CLASS-IN
 match access-group name TRUSTED-ACL-IN
!
policy-map type inspect TRUSTED-POLICY-IN
 class type inspect TRUSTED-CLASS-IN
  inspect
 class class-default
  drop log
!
```

Criar mapeamentos de pares de zonas

Em seguida, devemos criar os mapeamentos de quatro pares de zonas discutidos anteriormente na tabela.

Esses pares de zonas farão referência a uma política de serviço que corresponde ao mapa de políticas criado anteriormente.

<#root>

```
! INSIDE <> SELF


zone-pair security IN-SELF source INSIDE destination self
 service-policy type inspect TRUSTED-POLICY-IN
zone-pair security SELF-IN source self destination INSIDE
 service-policy type inspect TRUSTED-POLICY-IN
!

! OUTSIDE <> SELF


zone-pair security OUT-SELF source OUTSIDE destination self
 service-policy type inspect TRUSTED-POLICY-OUT
zone-pair security SELF-OUT source self destination OUTSIDE
 service-policy type inspect TRUSTED-POLICY-OUT
!
```

Atribuir zonas a interfaces

<#root>

```
! Assign Zones to interfaces


int gig1
 zone-member security INSIDE
!
int gig3
 zone-member security OUTSIDE
!
```

Verificar

Exemplo de fluxo de pacote - Chamada

Neste ponto, uma chamada do ponto de extremidade B para o CUBE destinada ao CUCM chamará a seguinte sequência:

1. O pacote SIP TCP de entrada para o CUBE no 5060 ingressará no GIG 1 e será mapeado para a zona de origem EXTERNA
2. O CUBE opera na zona SELF, portanto, o par de zona EXTERNO a SELF será usado (**OUT-SELF**)
3. O mapa de política/serviço **TRUSTED-POLICY-OUT** será usado para inspecionar o tráfego baseado em **TRUSTED-CLASS-OUT** class-map e **TRUSTED-ACL-OUT** access-list
4. O CUBE usará a lógica de roteamento de chamada local para determinar para onde enviar a chamada e qual interface de saída usar. Neste exemplo, a interface de saída será GIG 3 para CUCM.
    1. Consulte este documento para obter uma visão geral do roteamento de chamadas do CUBE: https://www.cisco.com/c/en/us/support/docs/voice/ip-telephony-voice-over-ip-voip/211306-In-Depth-Explanation-of-Cisco-IOS-and-IO.html
5. O CUBE criará um novo soquete TCP e um CONVITE SIP, todos originados do GIG 3 (INTERNO). O CUBE opera na zona SELF, portanto, ele usará o par de zonas SELF-OUT
6. O mapa de políticas/políticas de serviços **TRUSTED-POLICY-IN** será usado para inspecionar o tráfego baseado no mapa de classes **TRUSTED-CLASS-IN** e na lista de acessos **TRUSTED-ACL-IN**
7. Para tráfego de retorno nesse fluxo **IN-SELF** e **SELF-OUT** zonas para enviar respostas para a chamada.

comandos show

show zone-pair security

- Esse comando mostrará todos os mapeamentos de par de zonas e a política de serviço aplicada.
- As palavras-chave source e destination podem ser usadas para definir um mapeamento de par de zonas específico para verificar se existem muitas.

<#root>

```
Router#
```

show zone-pair security

```
Zone-pair name IN-SELF 2
    Source-Zone INSIDE Destination-Zone self
    service-policy TRUSTED-POLICY-IN
Zone-pair name OUT-SELF 4
    Source-Zone OUTSIDE Destination-Zone self
    service-policy TRUSTED-POLICY-OUT
Zone-pair name SELF-IN 5
    Source-Zone self Destination-Zone INSIDE
    service-policy TRUSTED-POLICY-IN
Zone-pair name SELF-OUT 6
    Source-Zone self Destination-Zone OUTSIDE
    service-policy TRUSTED-POLICY-OUT

Router#
```

show zone-pair security source INSIDE destination self

```
Zone-pair name IN-SELF 2
    Source-Zone INSIDE Destination-Zone self
    service-policy TRUSTED-POLICY-IN
```

show call ative voice compact

- Esse comando mostrará as conexões de mídia remotas da perspectiva do CUBE>

<#root>

```
Router#
```

show call active voice com | i NA|VRF

```
       <callID> A/O FAX   T<sec>  Codec       type        Peer Address   IP R:<ip>:<udp>              \
       467      ANS       T2      g711ulaw    VOIP        Psipp          192.168.1.48:16384
       468      ORG       T2      g711ulaw    VOIP        P8675309       192.168.3.59:16386           NA
```

show voip rtp connections

- Esse comando mostra informações de conexão de mídia remota e local da perspectiva do CUBE

<#root>

```
Router#
```

show voip rtp con | i NA|VRF

```
No. CallId     dstCallId  LocalRTP RmtRTP   LocalIP                                  RemoteIP
1     467        468        8120     16384    192.168.1.12                              192.168.1.48
2     468        467        8122     16386    192.168.2.58                             192.168.3.59
```

show call ative voice brief

- Esse comando, juntamente com o comando media bulk-stats configurado via serviço de voz voip, exibirá estatísticas de envio (TX) e de recebimento (RX) para os segmentos de chamada.
- Se a mídia estiver fluindo pelo CUBE e ZBFW, o TX deve corresponder ao RX em um trecho de chamada de peer. Por exemplo, 109 RX, 109 TX

<#root>

```
Router#
```

```
show call active voice br | i dur
```

```
 dur 00:00:03 tx:107/24156 rx:109/24592 dscp:0 media:0 audio tos:0xB8 video tos:0x0
 dur 00:00:03 tx:109/24592 rx:107/24156 dscp:0 media:0 audio tos:0xB8 video tos:0x0
```

show sip-ua connections tcp detail

- Esse comando mostra detalhes da conexão TCP SIP ativa através do CUBE
- Comandos como **show sip-ua connections udp detail** ou **show sip-ua connections tcp tls** detail podem ser usados para mostrar os mesmos detalhes para UDP SIP e TCP-TLS SIP

<#root>

```
Router#
```

```
show sip-ua connections tcp detail
```

```
Total active connections      : 2
[..truncated..]
Remote-Agent:192.168.3.52, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size            Local-Address               Tenant
  =========== ======= =========== =========== ======================================= ======
         5060      51 Established           0 192.168.2.58:51875                        0

Remote-Agent:192.168.1.48, Connections-Count:1
  Remote-Port Conn-Id Conn-State  WriteQ-Size            Local-Address               Tenant
  =========== ======= =========== =========== ======================================= ======
        33821      50 Established           0 192.168.1.12:5060                         0
[..truncated..]
```

show policy-firewall sessions platform

- Esse comando mostrará a chamada da perspectiva ZBFW.
- Haverá sessões e subfluxos SIP para RTP e RTCP.
- A ID de sessão desta saída pode ser usada ao depurar o ZBFW posteriormente.
- **o show policy-firewall sessions platform detail** pode ser usado para exibir ainda mais dados.

<#root>

```
Router#
```

show policy-firewall sessions platform

```
--show platform hardware qfp active feature firewall datapath scb any any any any any all any --
[s=session  i=imprecise channel c=control channel  d=data channel u=utd inspect A/D=appfw action allow/d
Session ID:0x000000A8 192.168.2.58 51875 192.168.3.52 5060 proto 6 (-global-:0:-global-:0) (0x16:sip) [s
 +-Session ID:0x000000AA 192.168.2.58 0 192.168.3.52 5060 proto 6 (-global-:0:-global-:0) (0x16:sip)  [i
 +-Session ID:0x000000A9 192.168.3.52 0 192.168.2.58 5060 proto 6 (-global-:0:-global-:0) (0x16:sip)  [i
Session ID:0x000000AC 192.168.3.59 16386 192.168.2.58 8122 proto 17 (-global-:0:-global-:0) (0x2:udp) [s
Session ID:0x000000AD 192.168.1.48 16384 192.168.1.12 8120 proto 17 (-global-:0:-global-:0) (0x3a:sip rt
Session ID:0x000000A6 192.168.1.48 33821 192.168.1.12 5060 proto 6 (-global-:0:-global-:0) (0x16:sip)
 +-Session ID:0x000000AE 192.168.1.48 16385 192.168.1.12 8121 proto 17 (-global-:0:-global-:0) (0x3a:sip
 +-Session ID:0x000000AD 192.168.1.48 16384 192.168.1.12 8120 proto 17 (-global-:0:-global-:0) (0x3a:sip
 +-Session ID:0x000000AB 192.168.1.48 0 192.168.1.12 5060 proto 6 (-global-:0:-global-:0) (0x16:sip)
 +-Session ID:0x000000A7 192.168.1.12 0 192.168.1.48 5060 proto 6 (-global-:0:-global-:0) (0x16:sip)
```

show policy-map type inspect zone-pair sessions

- Esse comando mostra dados semelhantes como **show policy-firewall sessions platform** no entanto, o mapeamento de par de zonas também é incluído na saída que é útil para a depuração.

```
Router# show policy-map type inspect zone-pair sessions | i Zone-pair|Session ID
  Zone-pair: IN-SELF
         Session ID 0x000000AD (192.168.1.48:16384)=>(192.168.1.12:8120) sip-RTP-data SIS_OPEN
         Session ID 0x000000A6 (192.168.1.48:33821)=>(192.168.1.12:5060) sip SIS_OPEN
         Session ID 0x000000A7 (192.168.1.12:0)=>(192.168.1.48:5060) sip SIS_PREGEN
         Session ID 0x000000AE (192.168.1.48:16385)=>(192.168.1.12:8121) sip-RTP-data SIS_PREGEN
         Session ID 0x000000AB (192.168.1.48:0)=>(192.168.1.12:5060) sip SIS_PREGEN
  Zone-pair: OUT-SELF
         Session ID 0x000000AC (192.168.3.59:16386)=>(192.168.2.58:8122) udp SIS_OPEN
  Zone-pair: SELF-IN
  Zone-pair: SELF-OUT
         Session ID 0x000000A8 (192.168.2.58:51875)=>(192.168.3.52:5060) sip SIS_OPEN
         Session ID 0x000000AA (192.168.2.58:0)=>(192.168.3.52:5060) sip SIS_PREGEN
         Session ID 0x000000A9 (192.168.3.52:0)=>(192.168.2.58:5060) sip SIS_PREGEN
```

Troubleshoot

O Troubleshooting do Cisco IOS XE firewall baseado em zona pode ser encontrado neste documento:

https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/117721-technote-iosfirewall-00.html

CUBE Local Transcoding Interface (LTI) + ZBFW

- Quando o CUBE é configurado com recursos PVDM de hardware na placa-mãe ou em um módulo de interface de rede (NIM), eles podem ser usados para fins de CUBE LTI.
- A interface do painel traseiro para o PVDM terá um mecanismo de serviço estático x/y/z que corresponde ao posicionamento do PVDM. Por exemplo, o mecanismo de serviço 0/4 é o slot PVDM/DSP da placa-mãe.
- Este mecanismo de serviço DEVE ser configurado com uma região e não existe na autoregião.

A configuração a seguir mapeará o mecanismo de serviço usado pelo CUBE LTI para a zona INTERNA

para fins de ZBFW.

```
!
interface Service-Engine0/4/0
 zone-member security INSIDE
!
```

Uma lógica semelhante para o mapeamento de par de zonas do mecanismo de serviço pode ser usada para Recursos de mídia SCCP baseados em PVDM/DSP de hardware e para a Interface de vinculação SCCP, no entanto, este tópico está fora do escopo deste documento.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.