Zone-Based Firewall (ZBFW) configureren samen met Cisco Unified Border Element (CUBE) Enterprise

Inhoud

Inleiding

Dit document beschrijft hoe u Zone-Based Firewall (ZBFW) kunt configureren in combinatie met Cisco Unified Border Element (CUBE) Enterprise.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

- Cisco router met Cisco IOS® XE 17.10.1a

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als

uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

- CUBE Enterprise- en ZBFW-colocatie werden niet ondersteund op Cisco IOS XE tot 16.7.1+

- CUBE Enterprise ondersteunt alleen CUBE + ZBFW RTP-RTP-mediastromen. Zie: CSCwe66293

- Dit document is niet van toepassing op CUBE Media Proxy, CUBE Service Provider, MGCP of SCCP-gateways, Cisco SRST of ESR-gateways, H323-gateways of andere analoge/TDM-spraakgateways.

- Zie voor TDM/Analog Voice Gateways en ZBFW het volgende document: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/213550-troubleshoot-one-way-audio-problems-in-f.html

Netwerkdiagram

De voorbeeldconfiguratie illustreert twee logische netwerksegmentaties die binnen en buiten worden genoemd.

BINNENKANT bevat één IP-netwerk en BUITENZIJDE bevat twee IP-netwerken.

Layer 3-netwerktopologie

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

Layer 7 Call Flow

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

Layer 7 Media Flow

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

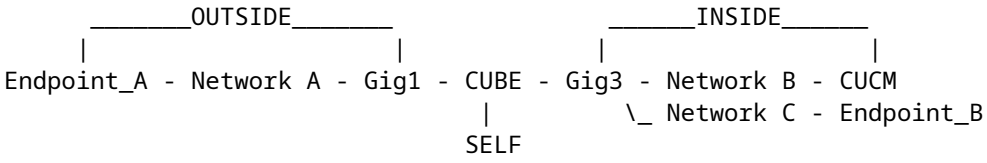
ZBFW-concepten voor crashprogrammaâ€™s

- Wanneer u ZBFW configureert, configureert u een naam van de beveiligingszone die vervolgens op een interface wordt gedefinieerd. Daarna wordt al het verkeer naar/van die interface gekoppeld aan die zonenaam.
  - Verkeer van/naar dezelfde zone is altijd toegestaan.
  - Het verkeer naar/van verschillende zones wordt verbroken, tenzij dit is toegestaan door de beheerderconfiguratie.
- Om toegestane verkeersstromen te definiëren moet u een zone-mapping maken via een unidirectionele

zone-paarconfiguratie die de namen van de bron- en doelzone definieert.
    - Deze zone-paar-afbeelding bindt vervolgens aan een service-policy dat wordt gebruikt om granulaire controle te bieden over de geïnspecteerde, toegestane en verboden verkeerstypen.
- CUBE Enterprise werkt in de speciale Self-zone. De ZELF-zone bevat ander verkeer naar/van de router, zoals ICMP, SSH, NTP, DNS, enzovoort.
    - Hardware PVDM voor gebruik met CUBE LTI bestaat niet in de zelfzone en moet worden toegewezen aan een administratief ingestelde zone.
- ZBFW staat automatisch retourverkeer niet toe, zodat een beheerder zoneparen moet configureren om retourverkeer te definiëren.

Met de volgende 3 kogels in gedachten kunnen de volgende zones worden toegevoegd overlayed op onze L3-netwerktopologie waar:

- Netwerk A, Gig1 zijn de BUITENzone
- Network B, Network C en Gig3 zijn INSIDE-zone
- CUBE maakt deel uit van de ZELF-zone



Daarna kunnen we logisch de vier unidirectionele zone-paartoewijzingen maken die we nodig hebben voor verkeersstromen door CUBE+ZBFW:

Bron	**Bestemming**	**Gebruik**
BUITEN	ZELF	Inkomende SIP- en RTP-media van Endpoint A
ZELF	BINNENKANT	Uitgaande SIP- en RTP-media van CUBE naar CUCM en Endpoint B.
BINNENKANT	ZELF	Inkomende SIP- en RTP-media van CUCM en Endpoint B.
ZELF	BUITEN	Uitgaande SIP- en RTP-media van CUBE naar Endpoint A.

Met deze concepten in gedachten kunnen we ZBFW op de Cisco IOS XE-router configureren als CUBE.

Configuraties

Beveiligingszones definiëren

We moeten twee veiligheidszones instellen: BINNEN en BUITEN. Zelf hoeft niet te worden gedefinieerd, omdat het standaard is.

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

Maak een toegangslijst, een klasse-kaart en een beleidskaart voor vertrouwd verkeer

Om te controleren welk verkeer we moeten configureren methodes voor de router om aan te passen en toe te laten.

Om dit te doen zullen we een uitgebreide toegangslijst, class-map en beleidskaart maken die ons verkeer inspecteren.

Voor eenvoud zullen we een beleid maken voor elke zone die zowel inkomend als uitgaand verkeer in kaart brengt.

Merk op dat configuraties zoals **match protocol sip** en **match protocol sip-tls** kunnen worden gebruikt, maar voor illustratieve doeleinden zijn de IP/poorten geconfigureerd

BUITEN UITGEBREIDE TOEGANGSLIJST, KLASSENKAART, BELEIDSKAART

<#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
```

```
!
```

Binnen Uitgebreide Toegangslijst, Klasse Kaart, Beleidskaart

```
!
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
!
```

Zone-paar toewijzingen maken

Daarna moeten we de vier zone-paar toewijzingen eerder in de tabel besproken.

Deze zone-paren verwijzen naar een dienstenbeleid dat de beleidsplannen die we eerder hebben gemaakt.


```
! 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
!
```

Zones toewijzen aan interfaces

<#root>

```
! Assign Zones to interfaces


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

Verifiëren

Steekproef Packet Flow - Call

Op dit punt zal een vraag van Endpoint B aan CUBE die voor CUCM wordt bestemd de volgende opeenvolging aanhalen:

1. Inkomend TCP SIP-pakket naar CUBE op 5060 gaat GIG 1 binnen en wordt toegewezen aan externe bronzone
2. CUBE werkt in Self-zone zodat de buitenkant naar ZELF zone-paar wordt gebruikt (**OUT-ZELF**)
3. De service-policy/policy-map **TRUSTED-POLICY-OUT** zal worden gebruikt om verkeer te inspecteren op basis van **TRUSTED-CLASS-OUT** class-map en **TRUSTED-ACL-OUT** toegangslijst
4. CUBE zal dan lokale vraag gebruiken die logica om te bepalen waar te om de vraag te verzenden en welke uitgaande interface aan gebruik. In dit voorbeeld zal uitgaande interface GIG 3 voor CUCM zijn.
    1. Verwijs naar dit document voor de vraag van CUBE het routeren overzicht: 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. CUBE maakt een nieuwe TCP Socket en SIP INVITE all sourced van GIG 3 (INSIDE). CUBE werkt in Self Zone, dus dit gebruikt het ZELF-OUT zone-paar
6. De service-policy/policy-map **TRUSTED-POLICY-IN** zal worden gebruikt om verkeer te inspecteren op basis van **TRUSTED-CLASS-IN** class-map en **TRUSTED-ACL-IN** toegangslijst
7. Voor terugkeerverkeer in deze stroom **IN-ZELF** en **ZELF-UIT** streken om reacties voor de vraag te verzenden.

Opdrachten weergeven

toon streek-paar veiligheid

- Deze opdracht toont alle zone-paartoewijzingen en het toegepaste servicebeleid.
- De bron, de bestemmingssleutelwoorden kunnen worden gebruikt om een specifieke streek-paar

afbeelding te bepalen om te controleren als velen bestaan.

```
<#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
```

toon vraag actieve stem compact

- Deze opdracht toont externe mediaverbindingen vanuit het perspectief van 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>              V
       467      ANS       T2      g711ulaw    VOIP        Psipp          192.168.1.48:16384
       468      ORG       T2      g711ulaw    VOIP        P8675309       192.168.3.59:16386           NA
```

voip rtp-verbindingen tonen

- Deze opdracht toont zowel externe als lokale media-verbindingsinformatie vanuit het perspectief van 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
```

toon vraag actieve stemsamenvatting

- Dit commando, gekoppeld aan de media bulk-stats commando geconfigureerd via Voice Service VoIP zal verzenden (TX) en ontvangen (RX) statistieken tonen voor de call benen.
- Als media door CUBE en ZBFW stromen, moet de TX overeenkomen met de RX op een peer call leg. bijv. 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
```

toon sip-ua verbindingen tcp detail

- Deze opdracht toont actieve SIP TCP-verbindingsdetails via CUBE
- Opdrachten zoals **tonen sip-ua verbindingen udp detail** of **tonen sip-ua verbindingen tcp tls** detail kan worden gebruikt om dezelfde details voor UDP SIP en TCP-TLS SIP te tonen

<#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 beleid-firewall sessieplatform

- Deze opdracht toont de aanroep vanuit het ZBFW-perspectief.
- Er zullen SIP-sessies en substromen zijn voor RTP en RTCP.
- De sessie-ID van deze uitvoer kan later worden gebruikt bij het debuggen van ZBFW.
- **tonen beleid-firewall sessies platform detail** kan worden gebruikt om nog meer gegevens te

bekijken.

<#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)
```

toon beleid-kaart type inspecteren zone-paar sessies

- Deze opdracht toont vergelijkbare gegevens zoals **tonen beleid-firewall sessieplatform** maar de zone-paar afbeelding is ook opgenomen in de uitvoer die handig is voor het debuggen.

```
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
```

Problemen oplossen

In dit document vindt u problemen met de op Cisco IOS XE-zone gebaseerde firewall:

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

CUBE lokale transcoderingsinterface (LTI) + ZBFW

- Wanneer CUBE is geconfigureerd met hardware-PVDM-bronnen op het moederbord of een netwerkinterfacemodule (NIM), kunnen deze worden gebruikt voor CUBE LTI-doeleinden.

- De backplane interface voor de PVDM zal een statische servicemotor x/y/z hebben die overeenkomt met de plaatsing van de PVDM. bijvoorbeeld is servicemotor 0/4 de PVDM/DSP-sleuf op het moederbord.
- Deze servicemotor MOET worden geconfigureerd met een zone en bestaat niet in de zelfzone.

De volgende configuratie zal de servicemotor die door CUBE LTI wordt gebruikt in kaart brengen aan de BINNENzone voor ZBFW-doeleinden.

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

Gelijkaardige logica voor service-engine zone-pair mapping kan worden gebruikt voor op hardware PVDM/DSP gebaseerde SCCP Media Resources en de SCCP Bind Interface, maar dit onderwerp valt buiten het bereik van dit document.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.