Configurazione di ZBFW (Zone-Based Firewall) con Cisco Unified Border Element (CUBE) Enterprise

Sommario

Introduzione

In questo documento viene descritto come configurare Zone-Based Firewall (ZBFW) insieme a Cisco Unified Border Element (CUBE) Enterprise.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

- Router Cisco con Cisco IOS® XE 17.10.1a

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata

ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

- La co-locazione di CUBE Enterprise e ZBFW non è supportata in Cisco IOS XE fino alle versioni 16.7.1+

- CUBE Enterprise supporta solo i flussi di supporti CUBE + ZBFW RTP-RTP. Vedere: CSCwe6293

- Il presente documento non è applicabile a CUBE Media Proxy, CUBE Service Provider, Gateways MGCP o SCCP, Cisco SRST o ESRST, H323 Gateways o altri gateway voce analogici/TDM.

- Per TDM/Analog Voice Gateway e ZBFW, consultare il seguente documento: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/213550-troubleshoot-one-way-audio-problems-in-f.html

Esempio di rete

Nella configurazione di esempio verranno illustrate due segmentazioni logiche di rete denominate INSIDE ed OUTSIDE.

L'interno contiene una singola rete IP, l'esterno contiene due reti IP.

Topologia di rete di livello 3

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

Flusso di chiamate di livello 7

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

Flusso dei supporti Layer 7

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

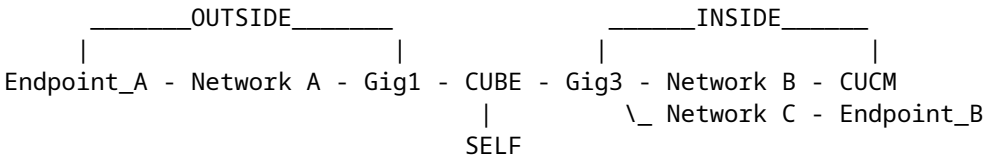
Concetti del corso di arresto anomalo ZBFW

- Durante la configurazione di ZBFW, è necessario configurare un nome per l'area di sicurezza che venga quindi definito su un'interfaccia. Dopodiché tutto il traffico da/verso l'interfaccia viene associato al nome della zona.
  - Il traffico da/verso la stessa zona è sempre consentito.
  - Il traffico da/verso zone diverse viene interrotto a meno che non sia consentito dalla configurazione dell'amministratore.

- Per definire i flussi di traffico consentiti, è necessario creare un mapping di zona tramite una configurazione di coppia di zone unidirezionale che definisce i nomi delle zone di origine e di destinazione.
    - Questo mapping di coppia di zone si associa quindi a un criterio di servizio utilizzato per fornire un controllo granulare sui tipi di traffico ispezionato, consentito e non consentito.
- L'organizzazione CUBE opera nella zona SELF speciale. La zona SELF include altro traffico da/verso il router, ad esempio ICMP, SSH, NTP, DNS e così via.
    - Il PVDM hardware da utilizzare con l'LTI CUBO non esiste nella zona autonoma e deve essere mappato a una zona configurata amministrativamente.
- Il protocollo ZBFW non consente automaticamente il traffico di ritorno, pertanto un amministratore deve configurare le coppie di zone per definire il traffico di ritorno.

Con i seguenti 3 punti elenco in mente, le seguenti zone possono essere aggiunte sovrapposte sulla topologia di rete L3 in cui:

- Rete A, Gig1 sono la zona ESTERNA
- La rete B, la rete C e Gig3 sono nella zona INSIDE
- CUBE fa parte della zona SELF



Successivamente è possibile creare in modo logico le quattro associazioni unidirezionali di coppia di zone necessarie per i flussi di traffico che passano attraverso CUBE+ZBFW:

Origine	**Destinazione**	**Utilizzo**
ESTERNO	SELF	Supporti SIP e RTP in entrata dall'endpoint A
SELF	INTERNO	Supporti SIP e RTP in uscita da CUBE a CUCM e all'endpoint B.
INTERNO	SELF	Supporti SIP e RTP in entrata da CUCM e dall'endpoint B.
SELF	ESTERNO	Supporti SIP e RTP in uscita da CUBE all'endpoint A.

Tenendo presenti questi concetti, è possibile iniziare a configurare lo ZBFW sul router Cisco IOS XE che agisce come CUBE.

Configurazioni

Definizione delle aree di sicurezza

Richiamo è necessario configurare due aree di sicurezza: INTERNA ed ESTERNA. Non è necessario definire se stesso come predefinito.

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

Creazione di elenchi degli accessi, mappe delle classi e mappe dei criteri per il traffico attendibile

Per controllare il traffico, è necessario configurare i metodi affinché il router corrisponda e autorizzi.

A tale scopo, verrà creato un elenco degli accessi esteso, una mappa delle classi e una mappa delle policy per il controllo del traffico.

Per semplicità, verrà creato un criterio per ogni zona che esegue il mapping del traffico in entrata e in uscita.

Si noti che possono essere utilizzate configurazioni quali **match protocol sip** e **match protocol sip-tls**, ma che a scopo illustrativo le porte IP/tls sono state configurate

EXTERNAL Extended Access List, mappa classi, mappa criteri

<#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
!
```

INSIDE Elenco accessi esteso, Mappa classi, Mappa criteri

```
!
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
!
```

Crea mapping di coppie di zone

È quindi necessario creare le quattro mappature di coppie di zone descritte in precedenza nella tabella.

Queste coppie di zone faranno riferimento a un criterio del servizio creato in precedenza dalla mappa dei criteri.

<#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
!
```

Assegna zone alle interfacce

<#root>

```
! Assign Zones to interfaces


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

Verifica

Flusso pacchetto di esempio - Chiamata

A questo punto una chiamata dall'endpoint B al CUBE destinato a CUCM richiamerà la sequenza seguente:

1. Il pacchetto SIP TCP in entrata verso CUBE su 5060 entrerà nel GIG 1 e verrà mappato alla zona di origine esterna
2. CUBE opera nella zona SELF in modo da utilizzare la coppia DA ESTERNO a ZONA SELF (**OUT-SELF**)
3. Il servizio-policy/policy-map **TRUSTED-POLICY-OUT** verrà utilizzato per ispezionare il traffico in base alla class-map **TRUSTED-CLASS-OUT** e all'elenco degli accessi **TRUSTED-ACL-OUT**
4. CUBE utilizzerà quindi la logica di routing delle chiamate locali per determinare dove inviare la chiamata e quale interfaccia di uscita utilizzare. In questo esempio l'interfaccia in uscita sarà GIG 3 per CUCM.
    1. Per una panoramica del routing delle chiamate CUBE, consultare il documento 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 creerà un nuovo socket TCP e SIP INVITE tutti originati da GIG 3 (INSIDE). Il CUBE opera nella zona SELF in modo da utilizzare la coppia di zone SELF-OUT
6. Il servizio-policy/policy-map **TRUSTED-POLICY-IN** verrà utilizzato per ispezionare il traffico in base alla mappa delle classi **TRUSTED-CLASS-IN** e all'elenco degli accessi **TRUSTED-ACL-IN**
7. Per il traffico di ritorno in questo flusso nelle zone **IN-SELF** e **SELF-OUT** per l'invio di risposte per la chiamata.

Comandi show

show zone-pair security

- Questo comando visualizza tutti i mapping di coppia di zone e i criteri del servizio applicati.

- Le parole chiave di origine e destinazione possono essere utilizzate per definire una specifica mappatura della coppia di zone per verificare se ne esistono molte.

<#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 active voice compact

- Questo comando visualizza le connessioni multimediali remote dal punto di vista di 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
```

mostra connessioni voip rtp

- Con questo comando vengono visualizzate le informazioni sulla connessione multimediale locale e remota dal punto di vista di 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 active voice brief

- Questo comando, insieme al comando media bulk-stats configurato tramite il voip del servizio vocale, visualizza le statistiche di invio (TX) e ricezione (RX) per le parti della chiamata.
- Se il supporto passa attraverso CUBE e ZBFW, il TX deve corrispondere al RX su un segmento di chiamata peer. Ad esempio, 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
```

mostra dettagli tcp connessioni sip-ua

- Questo comando visualizza i dettagli della connessione TCP SIP attiva tramite CUBE
- Comandi quali **show sip-ua connections udp detail** o **show sip-ua connections tcp tls** detail possono essere utilizzati per visualizzare gli stessi dettagli per 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 session platform

- Questo comando visualizza la chiamata dalla prospettiva ZBFW.
- Saranno disponibili sessioni SIP e flussi secondari per RTP e RTCP.
- L'ID di sessione di questo output può essere utilizzato durante il debug di ZBFW in seguito.

- **show policy-firewall session: è** possibile utilizzare i **dettagli della piattaforma** per visualizzare una quantità ancora maggiore di dati.

<#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

- Questo comando mostra dati simili a quelli della **piattaforma show policy-firewall session**, ma il mapping della coppia di zone è incluso nell'output ed è utile per il debug.

```
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
```

Risoluzione dei problemi

Per la risoluzione dei problemi del firewall basato su zone Cisco IOS XE, consultare questo 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 CUBE è configurato con risorse PVDM hardware sulla scheda madre o su un modulo di

interfaccia di rete (NIM), queste risorse possono essere utilizzate per CUBE LTI.

- L'interfaccia backplane per il PVDM avrà un motore di servizio statico x/y/z che corrisponde al posizionamento del PVDM. ad esempio, il motore di servizio 0/4 è lo slot PVDM/DSP della scheda madre.
- Questo service-engine DEVE essere configurato con una zona e non esiste nella zona autonoma.

La seguente configurazione consente di mappare il motore di servizio utilizzato da CUBE LTI alla zona INSIDE per gli scopi ZBFW.

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

Una logica simile per la mappatura delle coppie di zone del motore dei servizi può essere utilizzata per le risorse multimediali SCCP basate su PVDM/DSP e per l'interfaccia di binding SCCP. Tuttavia, questo argomento esula dall'ambito di questo documento.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).