配置與思科統一邊界元素(CUBE)企業版共存的基於區域的防火牆(ZBFW)

目錄

簡介

本檔案介紹如何設定與思科整合邊界元件(CUBE)企業版共存的區型防火牆(ZBFW)。

必要條件

需求

本文件沒有特定需求。

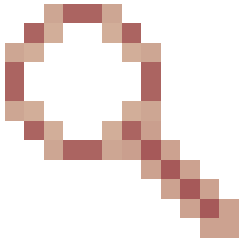
採用元件

— 運行Cisco IOS® XE 17.10.1a的Cisco路由器

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

- Cisco IOS XE 16.7.1+之前的版本不支持CUBE Enterprise和ZBFW共置



- CUBE Enterprise僅支援CUBE + ZBFW RTP-RTP媒體流。請參閱:CSCwe66293

— 本文檔不適用於CUBE媒體代理、CUBE服務提供商、MGCP或SCCP網關、Cisco SRST或ESRST網關、H323網關或其他模擬/TDM語音網關。

— 對於TDM/模擬語音網關和ZBFW，請參閱以下文檔：https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/213550-troubleshoot-one-way-audio-problems-in-f.html

網路圖表

示例配置將說明兩個名為INSIDE和OUTSIDE的邏輯網路分段。

INSIDE包含一個IP網路，OUTSIDE包含兩個IP網路。

第3層網路拓撲

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

第7層呼叫流

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

第7層媒體流

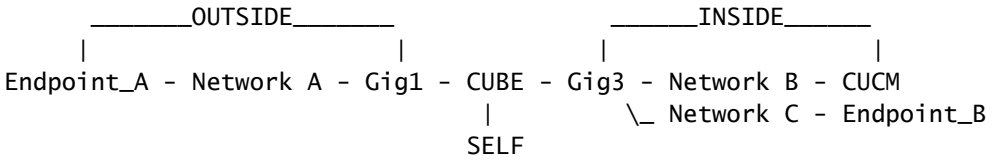
```
Endpoint_A <> RTP <> CUBE <> RTP <> Endpoint_B
```

ZBFW速成課程概念

- 在配置ZBFW時，可以配置安全區域名稱，然後在介面上定義該名稱。此後，所有進出該介面的流量都會與該區域名稱相關聯。
  - 始終允許進出同一區域的流量。
  - 除非管理員配置允許，否則不同區域之間的流量將被丟棄。
- 要定義允許的通訊流，您必須通過單向區域對配置建立區域對映，該配置定義了源區域名稱和目標區域名稱。
  - 然後，此區域對對映會繫結到服務策略，該策略用於對檢查、允許和禁止的流量型別提供精細控制。
- CUBE Enterprise在特殊的SELF區域中運行。SELF區域包括進出路由器的其它流量，例如ICMP、SSH、NTP、DNS等。
  - 與CUBE LTI一起使用的硬體PVDM在自身區域中不存在，必須對映到管理性配置的區域。
- ZBFW不會自動允許返回流量，因此管理員必須配置區域對以定義返回流量。

記住以下3個要點，可在我們的第3層網路拓撲上疊加以下區域，其中：

- 網路A、Gig1是OUTSIDE區域
- 網路B、網路C和Gig3位於INSIDE區域
- CUBE是SELF區域的一部分



接下來，我們可以從邏輯上建立通過CUBE+ZBFW的流量所需的四個單向區域對對映：

來源	目的地	使用率
OUTSIDE	SELF	來自終端A的入站SIP和RTP媒體
SELF	INSIDE	從CUBE到CUCM和終端B的出站SIP和RTP介質。
INSIDE	SELF	來自CUCM和終端B的入站SIP和RTP介質。

SELF	OUTSIDE	從CUBE到終端A的出站SIP和RTP介質。

記住這些概念後，我們便可以在充當CUBE的Cisco IOS XE路由器上配置ZBFW。

組態

定義安全區域

回想一下，我們需要配置兩個安全區域：INSIDE和OUTSIDE。不需要定義自身，因為它是預設自身。

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

為受信任流量建立訪問清單、類對映和策略對映

為了控制哪些流量，我們必須配置路由器要匹配和允許的方法。

為此，我們將建立擴展訪問清單、類對映和策略對映來檢查流量。

為簡單起見，我們將為每個區域建立一個對映入站和出站流量的策略。

請注意，可以使用match protocol sip和match protocol sip-tls等配置，但為了說明目的，已配置IP/埠

OUTSIDE Extended Access List、Class Map、Policy Map

<#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 Extended Access List， Class Map， Policy Map

```
!
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
!
```

建立區域對對映

接下來，我們必須建立表中前面討論的四個區域對對映。

這些區域對將引用我們之前建立的策略對映的服務策略。

```
! 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
!
```

為介面分配區域

<#root>

```
! Assign Zones to interfaces


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

驗證

資料包流示例 — 呼叫

此時，從端點B到CUBE且目的地為CUCM的呼叫將呼叫以下順序：

1. 到5060上的CUBE的入站TCP SIP資料包將輸入GIG 1並對映到OUTSIDE源區域
2. CUBE在SELF區域中運行，因此將使用OUTSIDE to SELF區域對(OUT-SELF)
3. service-policy/policy-map TRUSTED-POLICY-OUT將用於根據TRUSTED-CLASS-OUT class-map和TRUSTED-ACL-OUT access-list檢查流量
4. 然後，CUBE將使用本地呼叫路由邏輯來確定將呼叫傳送到何處以及要使用哪個輸出介面。在本示例中，CUCM的出口介面將是GIG 3。
    1. 有關CUBE呼叫路由概述，請參閱以下文檔：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將建立新的TCP套接字和SIP INVITE，所有源自GIG 3(INSIDE)。CUBE在SELF區域中運行，因此它將使用SELF-OUT區域對
6. service-policy/policy-map TRUSTED-POLICY-IN 將用於根據TRUSTED-CLASS-IN class-

map和TRUSTED-ACL-IN access-list檢查流量

7. 對於此流IN-SELF和SELF-OUT區域中的返回流量，以傳送呼叫的響應。

顯示命令

show zone-pair security

- 此命令將顯示所有區域對對映和應用的服務策略。
- source、destination關鍵字可用於定義特定區域對對映以檢查是否存在多個區域對。

<#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

- 此命令將從CUBE>的角度顯示遠端介質連線

<#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
```

show voip rtp connections

- 此命令從CUBE的角度顯示遠端和本地媒體連線資訊

<#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

- 此命令與通過語音服務voip配置的media bulk-stats命令一起將顯示呼叫段的傳送(TX)和接收(RX)統計資訊。
- 如果介質流經CUBE和ZBFW，則TX應與對等呼叫支路上的RX匹配，例如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

- 此命令通過CUBE顯示活動的SIP TCP連線詳細資訊
- show sip-ua connections udp detail或show sip-ua connections tcp tls detail等命令可用於顯示UDP SIP和TCP-TLS SIP的相同詳細資訊

<#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

- 此命令將從ZBFW的角度顯示呼叫。
- 將會有RTP和RTCP的SIP會話和子流。
- 以後調試ZBFW時，可以使用此輸出的會話ID。
- show policy-firewall sessions platform detail可用於檢視更多資料。

<#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/
Session ID:0x000000A8 192.168.2.58 51875 192.168.3.52 5060 proto 6 (-global-:0:-global-:0) (0x16:sip) [
 +-Session ID:0x000000AA 192.168.2.58 0 192.168.3.52 5060 proto 6 (-global-:0:-global-:0) (0x16:sip)  [
 +-Session ID:0x000000A9 192.168.3.52 0 192.168.2.58 5060 proto 6 (-global-:0:-global-:0) (0x16:sip)  [
Session ID:0x000000AC 192.168.3.59 16386 192.168.2.58 8122 proto 17 (-global-:0:-global-:0) (0x2:udp) [
Session ID:0x000000AD 192.168.1.48 16384 192.168.1.12 8120 proto 17 (-global-:0:-global-:0) (0x3a:sip r
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:si
 +-Session ID:0x000000AD 192.168.1.48 16384 192.168.1.12 8120 proto 17 (-global-:0:-global-:0) (0x3a:si
 +-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

- 此命令顯示的資料與show policy-firewall sessions platform類似，但是輸出中還包含區域對對映，方便調試。

```
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
```

疑難排解

Cisco IOS XE區域型防火牆的故障排除可在本文檔中找到：

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

CUBE本地轉碼介面(LTI)+ ZBFW

- 當CUBE配置了主機板上的硬體PVDM資源或網路介面模組(NIM)時，這些資源可用於CUBE LTI。
- PVDM的背板介面將有一個靜態服務引擎x/y/z，該引擎與PVDM的位置相對應。例如，服務引擎0/4是主機板PVDM/DSP插槽。
- 此服務引擎必須配置有區域，且不存在於自帶區域中。

以下配置將用於ZBFW的CUBE LTI使用的服務引擎對映到INSIDE區域。

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

服務引擎區域對對映的類似邏輯可用於基於硬體PVDM/DSP的SCCP媒體資源和SCCP繫結介面，但本主題不在本檔案的範圍之內。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。