配置与思科统一边界元素(CUBE)企业版共存的基于区域的防火墙(ZBFW)

目录

简介

本文档介绍如何配置与思科统一边界要素(CUBE)企业共存的基于区域的防火墙(ZBFW)。

先决条件

要求

本文档没有任何特定的要求。

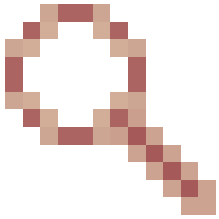
使用的组件

— 运行Cisco IOS® XE 17.10.1a的Cisco路由器

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

- Cisco IOS XE在16.7.1+之前不支持CUBE企业版和ZBFW同置功能



- CUBE Enterprise仅支持CUBE + ZBFW RTP-RTP媒体流。请参阅：CSCwe66293

— 本文档不适用于CUBE媒体代理、CUBE服务提供商、MGCP或SCCP网关、Cisco SRST或ESRST网关、H323网关或其他模拟/TDM语音网关。

— 对于TDM/模拟语音网关和ZBFW，请参阅以下文档：https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/213550-troubleshoot-one-way-audio-problems-in-f.html

网络图

示例配置将说明两个名为INSIDE和OUTSIDE的逻辑网络分段。

INSIDE包含一个IP网络，OUTSIDE包含两个IP网络。

第3层网络拓扑

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

第7层呼叫流

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

第7层介质流

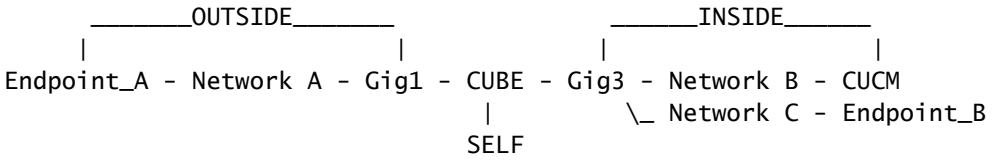
```
Endpoint_A <> RTP <> CUBE <> RTP <> Endpoint_B
```

ZBFW崩溃课程概念

- 配置ZBFW时，需要配置安全区域名称，然后在接口上定义该名称。之后，所有流入/流出该接口的流量都会与该区域名称关联。
  - 始终允许进出同一区域的流量。
  - 除非管理员配置允许，否则不同区域之间的流量将被丢弃。
- 要定义允许的流量，必须通过单向区域对配置创建区域映射，该配置定义了源和目标区域名称。
  - 然后，此区域对映射会绑定到服务策略，该策略用于对已检查、已允许和已禁止的流量类型提供精细控制。
- CUBE Enterprise在特殊的SELF区域中运行。SELF区域包括往返路由器的其他流量，例如ICMP、SSH、NTP、DNS等。
  - 与CUBE LTI一起使用的硬件PVDM在自身区域中不存在，必须映射到管理配置区域。
- ZBFW不会自动允许返回流量，因此管理员必须配置区域对以定义返回流量。

在记住以下3个要点后，可以在我们的第3层网络拓扑上叠加以下区域，其中：

- 网络A，Gig1是外部区域
- 网络B、网络C和Gig3位于内部区域
- CUBE是SELF区域的一部分



接下来，我们可以从逻辑上创建流经CUBE+ZBFW所需的四个单向区域对映射：

来源	目的地	使用率
外部	SELF	来自终端A的入站SIP和RTP媒体
SELF	内部	从CUBE到CUCM和终端B的出站SIP和RTP媒体。
内部	SELF	来自CUCM和终端B的入站SIP和RTP媒体。
SELF	外部	从CUBE到终端A的出站SIP和RTP媒体。

有了这些概念，我们就可以开始在Cisco IOS XE路由器上配置ZBFW作为CUBE。

配置

定义安全区域

回想一下，我们需要配置两个安全区域：INSIDE和OUTSIDE。不需要定义自身，因为它是默认自身。

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

为受信任流量创建访问列表、类映射和策略映射

为了控制哪些流量，我们必须配置路由器匹配和允许的方法。

为此，我们将创建扩展访问列表、类映射和策略映射来检查流量。

为简单起见，我们将为每个区域创建一个映射入站和出站流量的策略。

请注意，可以使用match protocol sip和match protocol sip-tls等配置，但为了说明目的，已配置IP/端口

外部扩展访问列表、类映射、策略映射

<#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
!
```

内部扩展访问列表、类映射、策略映射

```
!
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
!
```

创建区域对映射

接下来，我们必须创建表中前面讨论的四个区域对映射。

这些区域对将引用我们之前创建的策略映射的服务策略。

<#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
!
```

为接口分配区域

<#root>

```
! Assign Zones to interfaces


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

验证

数据包流示例 — 呼叫

此时，从终端B到发往CUCM的CUBE的呼叫将调用以下顺序：

1. 到5060上的CUBE的入站TCP SIP数据包将进入GIG 1并映射到OUTSIDE源区域
2. CUBE在SELF区域中运行，因此将使用OUTSIDE到SELF区域对(OUT-SELF)
3. service-policy/policy-map TRUSTED-POLICY-OUT 将用于根据TRUSTED-CLASS-OUT class-map和TRUSTED-ACL-OUT access-list检查流量
4. 然后，CUBE将使用本地呼叫路由逻辑来确定将呼叫发送到何处以及要使用哪个出口接口。在本示例中，CUCM的出口接口将为GIG 3。
    1. 有关CUBE呼叫路由概述，请参阅本文档：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将创建新的TCP套接字和SIP INVITE，所有源自GIG 3（内部）。CUBE在SELF区域中运行，因此它将使用SELF-OUT区域对
6. service-policy/policy-map TRUSTED-POLICY-IN 将用于根据TRUSTED-CLASS-IN 类映射和TRUSTED-ACL-IN access-list检查流量
7. 对于此流中的返回流量IN-SELF和SELF-OUT，以发送呼叫响应。

显示命令

show zone-pair security

- 此命令将显示所有区域对映射和应用的服务策略。
- source、destination关键字可用于定义特定区域对映射，以检查是否存在多个区域对。

<#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
```

显示呼叫活动语音压缩

- 此命令将从CUBE>的角度显示远程媒体连接

<#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

- 此命令从CUBE的角度显示远程和本地媒体连接信息

<#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

- 此命令与通过语音服务voip配置的media bulk-stats命令相结合，将显示呼叫段的send(TX)和received(RX)统计信息。
- 如果媒体流经CUBE和ZBFW，则TX应与对等呼叫段上的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

- 此命令通过CUBE显示活动的SIP TCP连接详细信息
- show sip-ua connections udp detail或show sip-ua connections tcp tls detail等命令可用于显示UDP SIP和TCP-TLS SIP的相同详细信息

<#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

- 此命令将从ZBFW的角度显示呼叫。
- RTP和RTCP将有SIP会话和子流。
- 以后调试ZBFW时，可以使用此输出的会话ID。
- show policy-firewall sessions platform detail可用于查看更多数据。

<#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

- 此命令显示的数据与show policy-firewall sessions platform类似，但输出中还包含区域对映射，便于调试。

```
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
```

故障排除

本文档中提供了Cisco IOS XE区域防火墙的故障排除信息：

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

CUBE本地转码接口(LTI)+ ZBFW

- 当CUBE配置有主板上的硬件PVDM资源或网络接口模块(NIM)时，这些资源可用于CUBE LTI目的。
- PVDM的背板接口将有一个静态服务引擎x/y/z，它与PVDM的位置相对应。例如，service-engine 0/4是主板PVDM/DSP插槽。
- 此service-engine必须配置一个区域，且自身区域中不存在。

以下配置将CUBE LTI使用的服务引擎映射到INSIDE区域，以用于ZBFW。

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

服务引擎区域对映射的类似逻辑可用于基于PVDM/DSP的硬件SCCP媒体资源和SCCP绑定接口，但本主题不属于本文档的范围。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。