Configuración de firewall basado en zonas (ZBFW) ubicado junto con Cisco Unified Border Element (CUBE) Enterprise

Contenido

Introducción

En este documento se describe cómo configurar el firewall basado en zonas (ZBFW) ubicado junto con Cisco Unified Border Element (CUBE) Enterprise.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

- Router de Cisco con Cisco IOS® XE 17.10.1a

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

- La coubicación de CUBE Enterprise y ZBFW no se admitió en Cisco IOS XE hasta 16.7.1+

- CUBE Enterprise sólo admite flujos de medios RTP-RTP CUBE + ZBFW. Consulte: CSCwe66293

- Este documento no es aplicable a CUBE Media Proxy, CUBE Service Provider, Gateways MGCP o SCCP, Gateways Cisco SRST o ESRST, Gateways H323 u otras Gateways de voz analógicas/TDM.

- Para TDM/Analog Voice Gateways y ZBFW, consulte el siguiente documento: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/213550-troubleshoot-one-way-audio-problems-in-f.html

Diagrama de la red

La configuración de ejemplo ilustrará dos segmentaciones de red lógica denominadas INSIDE y OUTSIDE.

INSIDE contiene una única red IP y OUTSIDE contiene dos redes IP.

Topología de red de capa 3

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

Flujo de llamadas de capa 7

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

Flujo de medios de capa 7

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

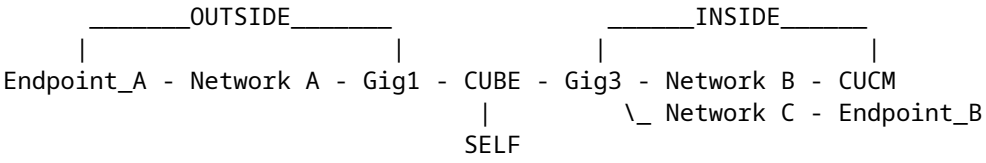
Conceptos del curso de ZBFW Crash

- Al configurar ZBFW, se configura un nombre de zona de seguridad que se define en una interfaz. Después de esto, todo el tráfico hacia/desde esa interfaz se asocia con ese nombre de zona.
  - Siempre se permite el tráfico hacia/desde la misma zona.
  - El tráfico hacia/desde diferentes zonas se descarta a menos que lo permita la configuración del administrador.
- Para definir los flujos de tráfico permitidos, debe crear una asignación de zona a través de una configuración de par de zonas unidireccional que defina los nombres de zona de origen y de destino.

    - Esta asignación de par de zonas se vincula a continuación a una política de servicio utilizada para proporcionar un control granular sobre los tipos de tráfico inspeccionados, permitidos y no permitidos.
- CUBE Enterprise opera en la zona especial SELF. La zona SELF incluye otro tráfico hacia/desde el router como ICMP, SSH, NTP, DNS, etc.
    - El PVDM de hardware para su uso con CUBE LTI no existe en la zona automática y debe asignarse a una zona configurada administrativamente.
- ZBFW no permite automáticamente el tráfico de retorno, por lo que un administrador debe configurar pares de zonas para definir el tráfico de retorno.

Con las siguientes 3 viñetas en mente, se pueden agregar las siguientes zonas superpuestas en nuestra topología de red L3 donde:

- Red A, Gig1 son la zona OUTSIDE
- La red B, la red C y Gig3 se encuentran dentro de la zona
- CUBE forma parte de la zona SELF



A continuación, podemos crear lógicamente las cuatro asignaciones de pares de zonas unidireccionales que necesitamos para los flujos de tráfico a través de CUBE+ZBFW:

Fuente	**Destino**	**Uso**
FUERA	UNO MISMO	Medios SIP y RTP entrantes desde el terminal A
UNO MISMO	DENTRO	Medios SIP y RTP salientes de CUBE a CUCM y al terminal B.
DENTRO	UNO MISMO	Medios SIP y RTP entrantes desde CUCM y el terminal B.
UNO MISMO	FUERA	Medios SIP y RTP salientes de CUBE al terminal A.

Con estos conceptos en mente, podemos comenzar a configurar ZBFW en el router Cisco IOS XE que actúa como CUBE.

Configuraciones

Definir zonas de seguridad

Recuerde que tenemos que configurar dos zonas de seguridad: INTERIOR y EXTERIOR. No es necesario definir Self, ya que es el valor predeterminado.

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

Crear una lista de acceso, mapa de clase y mapa de políticas para el tráfico de confianza

Para controlar qué tráfico debemos configurar los métodos para que el router coincida y lo permita.

Para ello, crearemos una lista de acceso ampliada, un mapa de clase y un mapa de políticas que inspeccionarán nuestro tráfico.

Para simplificar, crearemos una política para cada zona que asigne tanto el tráfico entrante como el saliente.

Tenga en cuenta que las configuraciones tales como **match protocol sip** y **match protocol sip-tls** pueden ser utilizadas pero para fines ilustrativos se han configurado los puertos/IP

Lista de acceso ampliada EXTERNA, mapa de clase, 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
!
```

Lista de acceso ampliada interna, mapa de clase, 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
!
```

Crear asignaciones de pares de zonas

A continuación, debemos crear los cuatro mapeos de pares de zonas que se discutieron anteriormente en la tabla.

Estos pares de zonas harán referencia a una política de servicio que el policy-map que creamos 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
!
```

Asignar zonas a interfaces

<#root>

```
! Assign Zones to interfaces


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

Verificación

Flujo de paquetes de ejemplo: llamada

En este momento, una llamada del terminal B a CUBE con destino a CUCM invocará la siguiente secuencia:

1. El paquete SIP TCP entrante a CUBE en 5060 ingresará a GIG 1 y se asignará a la zona de origen EXTERNA
2. CUBE funciona en la zona SELF, por lo que se utilizará el par de zonas OUTSIDE a SELF (**OUT-SELF**)
3. El service-policy/policy-map **TRUSTED-POLICY-OUT** se utilizará para inspeccionar el tráfico basado en el **TRUSTED-CLASS-OUT** class-map y la lista de acceso **TRUSTED-ACL-OUT**
4. A continuación, CUBE utilizará la lógica de enrutamiento de llamadas locales para determinar a dónde enviar la llamada y qué interfaz de salida utilizar. En este ejemplo, la interfaz de salida será GIG 3 para CUCM.
    1. Consulte este documento para obtener información general sobre el enrutamiento de llamadas 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. CUBE creará un nuevo socket TCP y SIP INVITE, todos ellos obtenidos de GIG 3 (INSIDE). CUBE funciona en la zona SELF, por lo que usará el par de zonas SELF-OUT
6. El service-policy/policy-map **TRUSTED-POLICY-IN** se utilizará para inspeccionar el tráfico basado en la lista de acceso **TRUSTED-CLASS-IN** class-map y **TRUSTED-ACL-IN**
7. Para el tráfico de retorno en este flujo **IN-SELF** y **SELF-OUT** zonas para enviar respuestas para la llamada.

Comandos show

show zone-pair security

- Este comando mostrará todas las asignaciones de pares de zonas y la política de servicio aplicada.
- Las palabras clave source, destination se pueden utilizar para definir una asignación específica de par de zonas para comprobar si existen muchas.

<#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
```

<#root>

```
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

- Este comando mostrará las conexiones de medios remotos desde la perspectiva de 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

- Este comando muestra la información de conexión de medios local y remota desde la perspectiva de 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

- Este comando, junto con el comando media bulk-stats configurado a través del servicio de voz voip, mostrará las estadísticas de envío (TX) y recepción (RX) para los tramos de llamada.
- Si el medio fluye a través de CUBE y ZBFW, el TX debe coincidir con el RX en un tramo de llamada de peer. Por ejemplo, 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

- Este comando muestra los detalles de la conexión TCP SIP activa a través de CUBE
- Los comandos como **show sip-ua connections udp detail** o **show sip-ua connections tcp tls** detail se pueden utilizar para mostrar los mismos detalles para UDP SIP y 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

- Este comando mostrará la llamada desde la perspectiva de ZBFW.
- Habrá sesiones SIP y subflujos para RTP y RTCP.
- El ID de sesión de esta salida se puede utilizar cuando se depure ZBFW más adelante.
- **show policy-firewall sessions platform detail** se puede utilizar para ver aún más datos.

<#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

- Este comando muestra datos similares como **show policy-firewall sessions platform** sin embargo, la asignación de par de zonas también se incluye en el resultado, lo cual es útil para la depuración.

```
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

En este documento se puede encontrar la solución de problemas del firewall basado en zonas Cisco IOS XE:

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

Interfaz de transcodificación local (LTI) de CUBE + ZBFW

- Cuando CUBE se configura con recursos PVDM de hardware en la placa base o un módulo de interfaz de red (NIM), estos se pueden utilizar para CUBE LTI.
- La interfaz de placa base para el PVDM tendrá un motor de servicio estático x/y/z que corresponde a la ubicación del PVDM. Por ejemplo, el motor de servicio 0/4 es la ranura PVDM/DSP de la placa base.
- Este motor de servicio DEBE configurarse con una zona y no existe en la zona automática.

La siguiente configuración asignará el motor de servicio utilizado por CUBE LTI a la zona INSIDE para fines de ZBFW.

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

Se puede utilizar una lógica similar para la asignación de pares de zonas de motores de servicio para los recursos de medios SCCP basados en PVDM/DSP de hardware y la interfaz de enlace SCCP; sin embargo, este tema no se trata en este documento.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).