Configurer un pare-feu basé sur les zones (ZBFW) situé au même endroit que Cisco Unified Border Element (CUBE) Enterprise

Table des matières

Introduction

Ce document décrit comment configurer un pare-feu basé sur les zones (ZBFW) colocalisé avec Cisco Unified Border Element (CUBE) Enterprise.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

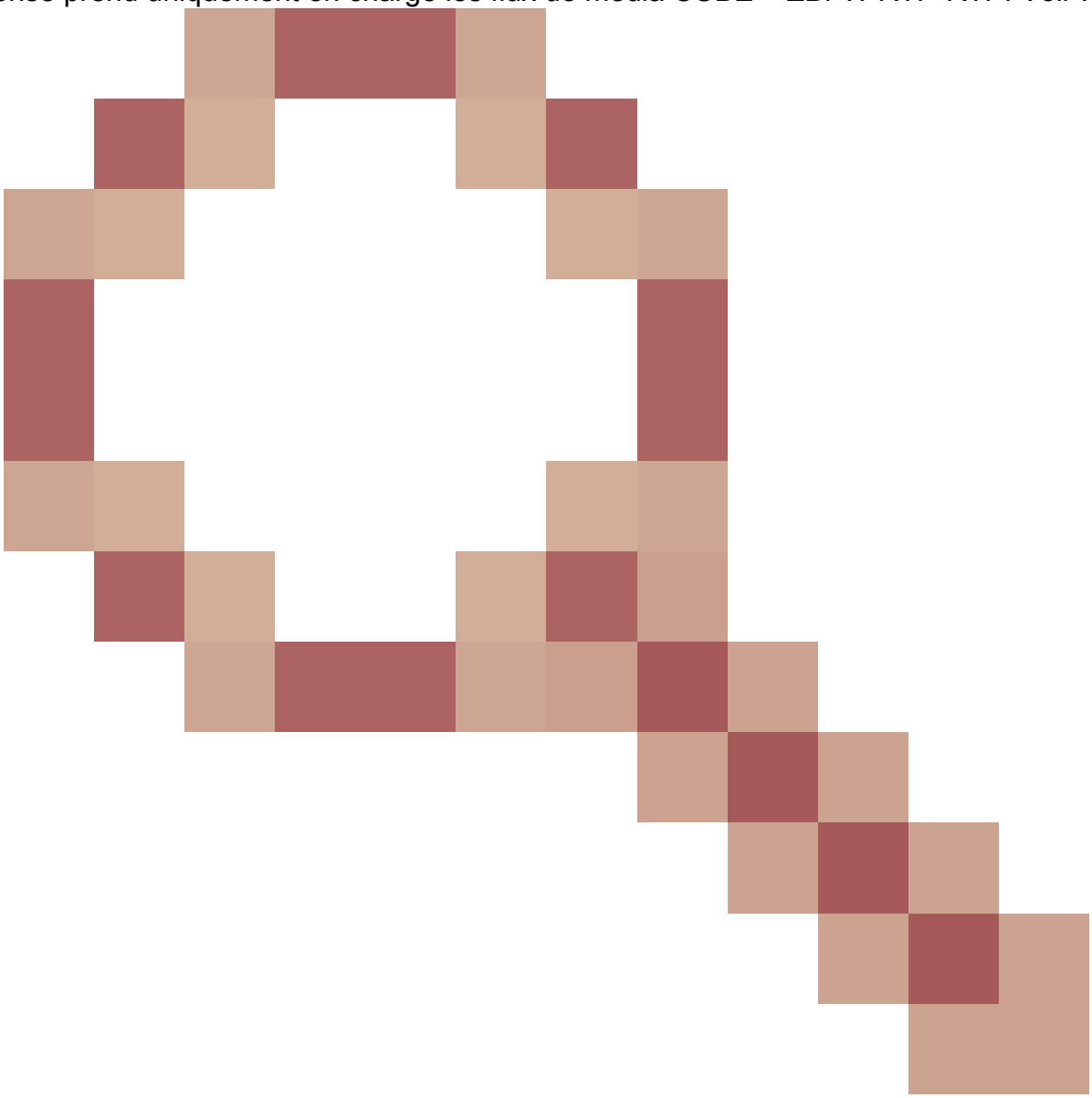
- Routeur Cisco exécutant Cisco IOS® XE 17.10.1a

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

- La colocalisation CUBE Enterprise et ZBFW n'était pas prise en charge sur Cisco IOS XE avant la version 16.7.1+

- CUBE Enterprise prend uniquement en charge les flux de média CUBE + ZBFW RTP-RTP. Voir :



CSCwe66293

- Ce document ne s'applique pas aux passerelles CUBE Media Proxy, CUBE Service Provider, MGCP ou SCCP, aux passerelles Cisco SRST ou ESRST, aux passerelles H323 ou aux autres passerelles vocales analogiques/TDM.

- Pour les passerelles vocales TDM/analogiques et ZBFW, consultez le document suivant : https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/213550-troubleshoot-one-way-audio-problems-in-f.html

Diagramme du réseau

L'exemple de configuration illustre deux segmentations de réseau logiques nommées INSIDE et OUTSIDE.

INSIDE contient un réseau IP unique et OUTSIDE contient deux réseaux IP.

Topologie réseau de couche 3

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

Flux d'appels de couche 7

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

Flux multimédia de couche 7

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

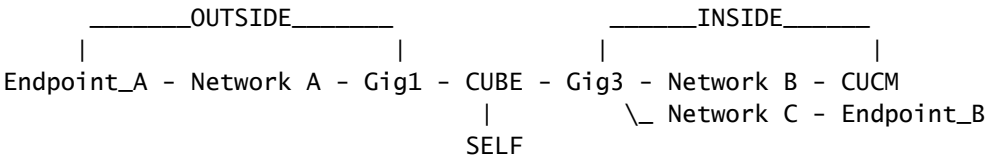
Concepts du cours ZBFW Crash

- Lors de la configuration de ZBFW, vous configurez un nom de zone de sécurité qui est ensuite défini sur une interface. Après cela, tout le trafic vers/depuis cette interface est associé à ce nom de zone.
  - Le trafic vers/depuis la même zone est toujours autorisé.
  - Le trafic en provenance/à destination de différentes zones est abandonné sauf autorisation de la configuration administrateur.
- Pour définir les flux de trafic autorisés, vous devez créer un mappage de zone via une configuration de paire de zones unidirectionnelle qui définit les noms des zones source et de destination.
  - Ce mappage de zone-paire est ensuite lié à une politique de service utilisée pour fournir un contrôle granulaire sur les types de trafic inspectés, autorisés et non autorisés.
- CUBE Enterprise fonctionne dans la zone spéciale SELF. La zone SELF inclut d'autres

trafics en provenance/à destination du routeur, tels que ICMP, SSH, NTP, DNS, etc.
    - Le PVDM matériel à utiliser avec CUBE LTI n'existe pas dans la zone self et doit être mappé à une zone configurée par l'administrateur.
- ZBFW n'autorisant pas automatiquement le trafic de retour, un administrateur doit configurer des paires de zones pour définir le trafic de retour.

Avec les 3 puces suivantes à l'esprit, les zones suivantes peuvent être ajoutées en superposition sur notre topologie de réseau L3 où :

- Réseau A, Gig1 sont la zone EXTERNE
- Les réseaux B, C et Gig3 sont des zones INSIDE
- CUBE fait partie de la zone SELF



Ensuite, nous pouvons créer logiquement les quatre mappages de paires de zones unidirectionnels dont nous avons besoin pour les flux de trafic via CUBE+ZBFW :

Source	Destination	Utilisation
EXTÉRIEUR	SOI-MÊME	Support SIP et RTP entrant du point d'extrémité A
SOI-MÊME	INTÉRIEUR	Supports SIP et RTP sortants de CUBE vers CUCM et le point d'extrémité B.
INTÉRIEUR	SOI-MÊME	Supports SIP et RTP entrants de CUCM et du point d'extrémité B.
SOI-MÊME	EXTÉRIEUR	Supports SIP et RTP sortants de CUBE vers le point d'extrémité A.

En gardant ces concepts à l'esprit, nous pouvons commencer à configurer ZBFW sur le routeur Cisco IOS XE agissant comme CUBE.

Configurations

Définir les zones de sécurité

Rappelez-vous que nous devons configurer deux zones de sécurité : INSIDE et OUTSIDE. Self n'a pas besoin d'être défini car il est défini par défaut.

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

Créer une liste d'accès, une carte de classe et une carte de stratégie pour le trafic sécurisé

Afin de contrôler le trafic, nous devons configurer des méthodes pour que le routeur corresponde et autorise.

Pour ce faire, nous allons créer une liste d'accès étendue, une carte de classe et une carte de stratégie qui inspecteront notre trafic.

Pour plus de simplicité, nous allons créer une politique pour chaque zone qui mappe le trafic entrant et sortant.

Notez que des configurations telles que match protocol sip et match protocol sip-tls peuvent être utilisées, mais à des fins d'illustration, les ports IP/IP ont été configurés

Liste d'accès étendue EXTERNE, mappage de classe, mappage de stratégie

<#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
!
```

Liste d'accès étendue INSIDE, mappage de classe, mappage de stratégie

```
!
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
!
```

Créer des mappages zone-paire

Ensuite, nous devons créer les quatre mappages de paires de zones décrits précédemment dans le tableau.

Ces zones-paires référenceront une politique de service que la carte-politique que nous avons créée précédemment.

<#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
!
```

Affectation de zones aux interfaces

<#root>

```
! Assign Zones to interfaces


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

Vérifier

Exemple de flux de paquets - Appel

À ce stade, un appel du point de terminaison B vers CUBE destiné à CUCM appelle la séquence suivante :

1. Le paquet SIP TCP entrant vers CUBE sur 5060 entrera dans GIG 1 et sera mappé à la zone source EXTERNE
2. CUBE fonctionne dans la zone SELF de sorte que la paire de zones OUTSIDE à SELF sera utilisée (OUT-SELF)
3. Le service-policy/policy-map TRUSTED-POLICY-OUT sera utilisé pour inspecter le trafic basé sur TRUSTED-CLASS-OUT class-map et TRUSTED-ACL-OUT access-list
4. CUBE utilise ensuite la logique de routage des appels locaux pour déterminer où envoyer l'appel et quelle interface de sortie utiliser. Dans cet exemple, l'interface de sortie sera GIG 3 pour CUCM.
    1. Reportez-vous à ce document pour une présentation du routage des appels 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 va créer un nouveau socket TCP et SIP INVITE, tous provenant de GIG 3 (INSIDE). CUBE fonctionne dans la zone SELF et utilise donc la paire de zones SELF-OUT
6. Le service-policy/policy-map TRUSTED-POLICY-IN sera utilisé pour inspecter le trafic basé sur TRUSTED-CLASS-IN class-map et TRUSTED-ACL-IN access-list
7. Pour le trafic de retour dans ces zones IN-SELF et SELF-OUT de flux pour envoyer des réponses pour l'appel.

Commandes show

show zone-pair security

- Cette commande affiche tous les mappages de paires de zones et la stratégie de service appliquée.
- Les mots-clés source et de destination peuvent être utilisés pour définir un mappage de zone-paire spécifique afin de vérifier s'il en existe plusieurs.

<#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

- Cette commande affiche les connexions de support à distance du point de vue 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           N
```

show voip rtp connections

- Cette commande affiche les informations de connexion au support local et distant du point de vue 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

- Cette commande, associée à la commande media bulk-stats configurée via le service vocal voip, affiche les statistiques d'envoi (TX) et de réception (RX) pour les tronçons d'appel.
- Si le média circule dans CUBE et ZBFW, le TX doit correspondre au RX sur une branche d'appel homologue. Par exemple, 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

- Cette commande affiche les détails de la connexion TCP SIP active via CUBE
- Des commandes telles que show sip-ua connections udp detail ou show sip-ua connections tcp tls detail peuvent être utilisées pour afficher les mêmes détails pour UDP SIP et 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

- Cette commande affiche l'appel du point de vue ZBFW.
- Il y aura des sessions et des sous-flux SIP pour RTP et RTCP.
- L'ID de session de ce résultat peut être utilisé lors du débogage ultérieur de ZBFW.
- show policy-firewall sessions platform detail peut être utilisé pour afficher encore plus de données.

<#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

- Cette commande montre des données similaires à show policy-firewall sessions platform cependant le mappage de zone-pair est également inclus dans le résultat qui est pratique pour le débogage.

```
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
```

Dépannage

Dépannage du pare-feu de zone Cisco IOS XE dans ce document :

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

Interface de transcodage local (LTI) CUBE + ZBFW

- Lorsque CUBE est configuré avec des ressources PVDM matérielles sur la carte mère ou un module d'interface réseau (NIM), ces ressources peuvent être utilisées pour CUBE LTI.
- L'interface de fond de panier du module PVDM aura un moteur de service statique x/y/z qui correspond à l'emplacement du module PVDM. Par exemple, le moteur de service 0/4 est le logement PVDM/DSP de la carte mère.
- Ce service-engine DOIT être configuré avec une zone et n'existe pas dans la zone self.

La configuration suivante mappe le service-engine utilisé par CUBE LTI à la zone INSIDE pour ZBFW.

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

Une logique similaire pour le mappage de paire de zones de moteur de service peut être utilisée pour les ressources matérielles SCCP Media Resources basées sur PVDM/DSP et l'interface de liaison SCCP. Toutefois, cette rubrique n'est pas traitée dans ce document.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.