Konfigurieren einer zonenbasierten Firewall (ZBFW) in Verbindung mit Cisco Unified Border Element (CUBE) Enterprise

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration einer zonenbasierten Firewall (ZBFW) in Verbindung mit dem Cisco Unified Border Element (CUBE) Enterprise beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

- Cisco Router mit Cisco IOS® XE 17.10.1a

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

- CUBE Enterprise und ZBFW Co-Location wurden auf Cisco IOS XE erst ab 16.7.1 unterstützt.

- CUBE Enterprise unterstützt nur CUBE- und ZBFW-RTP-RTP-Medien-Flows. Siehe: CSCwe66293

- Dieses Dokument gilt nicht für CUBE Media Proxy, CUBE Service Provider, MGCP- oder SCCP-Gateways, Cisco SRST- oder ESRST-Gateways, H323-Gateways oder andere Analog-/TDM-Voice-Gateways.

- Informationen zu TDM/Analog Voice Gateways und ZBFW finden Sie im folgenden Dokument: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/213550-troubleshoot-one-way-audio-problems-in-f.html

Netzwerkdiagramm

Die Beispielkonfiguration veranschaulicht zwei logische Netzwerksegmentierungen mit den Namen INSIDE und OUTSIDE.

INSIDE enthält ein einzelnes IP-Netzwerk und OUTSIDE enthält zwei IP-Netzwerke.

Layer-3-Netzwerktopologie

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

Anruffluss auf Layer 7

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

Medienfluss auf Schicht 7

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

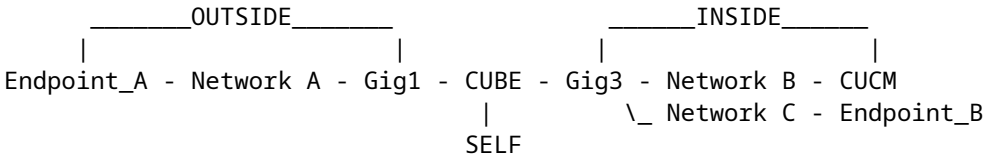
ZBFW Crash Course Konzepte

- Bei der Konfiguration von ZBFW konfigurieren Sie einen Sicherheitszonennamen, der dann auf einer Schnittstelle definiert wird. Danach wird der gesamte Datenverkehr zu/von dieser Schnittstelle mit dem Zonennamen verknüpft.
    - Datenverkehr von und zu derselben Zone ist immer zulässig.

    - Der Datenverkehr zu/von verschiedenen Zonen wird verworfen, es sei denn, die Administratorkonfiguration erlaubt dies.
- Um zulässige Datenverkehrsflüsse zu definieren, müssen Sie eine Zonenzuordnung über eine unidirektionale Zonenpaarkonfiguration erstellen, die die Namen der Quell- und Zielzone definiert.
    - Diese Zonenpaar-Zuordnung wird dann in eine Dienstrichtlinie eingebunden, die eine präzise Kontrolle der inspizierten, zulässigen und nicht zulässigen Datenverkehrstypen ermöglicht.
- CUBE Enterprise arbeitet in der speziellen SELF-Zone. Die SELF-Zone umfasst anderen Datenverkehr zum/vom Router, wie ICMP, SSH, NTP, DNS usw.
    - Hardware-PVDM zur Verwendung mit CUBE LTI ist in der Kernzone nicht vorhanden und muss einer administrativ konfigurierten Zone zugeordnet werden.
- ZBFW lässt Rückverkehr nicht automatisch zu. Daher muss der Administrator Zonenpaare konfigurieren, um Rückverkehr zu definieren.

Unter Berücksichtigung der folgenden drei Punkte können die folgenden Zonen in unserer L3-Netzwerktopologie überlagert hinzugefügt werden:

- Netzwerk A, Gig1 sind die Außenzone.
- Netzwerk B, Netzwerk C und Gig3 sind innerhalb der Zone
- CUBE ist Teil der SELF-Zone



Als Nächstes können die vier unidirektionalen Zonenpaar-Zuordnungen erstellt werden, die für den Datenverkehr über CUBE+ZBFW erforderlich sind:

Quelle	**Ziel**	**Nutzung**
AUSSEN	Selbst	Eingehende SIP- und RTP-Medien von Endpunkt A
Selbst	INNEN	Ausgehende SIP- und RTP-Medien von CUBE zu CUCM und Endpunkt B.
INNEN	Selbst	Eingehende SIP- und RTP-Medien vom CUCM und Endpunkt B.
Selbst	AUSSEN	Ausgehende SIP- und RTP-Medien von CUBE an Endpunkt A.

Vor dem Hintergrund dieser Konzepte können wir mit der Konfiguration von ZBFW auf dem Cisco IOS XE-Router beginnen, der als CUBE fungiert.

Konfigurationen

Sicherheitszonen definieren

Denken Sie daran, dass wir zwei Sicherheitszonen konfigurieren müssen: INNEN und AUSSEN. Self muss nicht definiert werden, da es sich um eine Standardeinstellung handelt.

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

Erstellung von Zugriffslisten, Klassenzuordnungen und Richtlinienzuordnungen für vertrauenswürdigen Datenverkehr

Um zu kontrollieren, welcher Datenverkehr verarbeitet werden soll, müssen Methoden konfiguriert werden, die vom Router zugelassen werden.

Zu diesem Zweck erstellen wir eine erweiterte Zugriffsliste, Klassenzuordnung und Richtlinienzuordnung, die unseren Datenverkehr überprüfen.

Der Einfachheit halber erstellen wir für jede Zone eine Richtlinie, die eingehenden und ausgehenden Datenverkehr zuordnet.

Es ist zu beachten, dass Konfigurationen wie **match protocol sip** und **match protocol sip-tls** verwendet werden können. Zur Veranschaulichung wurden die IP/Ports jedoch konfiguriert.

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
!
```

Zonenpaar-Zuordnungen erstellen

Als Nächstes müssen die vier Zonenpaar-Zuordnungen erstellt werden, die weiter oben in der Tabelle besprochen wurden.

Diese Zonenpaare verweisen auf eine Dienstrichtlinie, die von der zuvor erstellten Richtlinienzuordnung erstellt wurde.

<#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
!
```

Schnittstellen Zonen zuweisen

<#root>

```
! Assign Zones to interfaces


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

Überprüfung

Beispielpaketfluss - Anruf

An diesem Punkt wird bei einem für CUCM bestimmten Anruf von Endpunkt B an CUBE die folgende Sequenz aufgerufen:

1. Eingehendes TCP-SIP-Paket an CUBE auf 5060 geht in GIG 1 ein und wird der EXTERNEN Quellzone zugeordnet
2. CUBE wird in der SELF-Zone betrieben, sodass das OUTSIDE-to-SELF-Zonenpaar verwendet wird **(OUT-SELF**)
3. Die Funktion "service-policy/policy-map-**TRUSTED-POLICY-OUT"** wird verwendet, um Datenverkehr auf der Grundlage von "**TRUSTED-CLASS-OUT** class-map" und "**TRUSTED-ACL-OUT** access-list" zu prüfen.
4. CUBE verwendet dann eine lokale Anrufweiterleitungslogik, um zu bestimmen, wohin der Anruf gesendet werden soll und welche Ausgangsschnittstelle verwendet werden soll. In diesem Beispiel lautet die Ausgangsschnittstelle GIG 3 für CUCM.
    1. Informationen zur CUBE-Anrufweiterleitung finden Sie in diesem Dokument: 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 erstellt einen neuen TCP-Socket und eine SIP-INVITE-Nachricht, die alle von GIG 3 (INSIDE) stammen. CUBE wird in der SELF-Zone betrieben, daher wird das SELF-OUT-Zonenpaar verwendet.
6. Die Funktion "service-policy/policy-map-**TRUSTED-POLICY-IN"** wird verwendet, um Datenverkehr basierend auf "**TRUSTED-CLASS-IN** class-map" und "**TRUSTED-ACL-IN** access-

list" zu prüfen.
7. Für den Rückverkehr in dieser Fluss-**IN-SELF-** und **SELF-OUT-**Zone, um Antworten für den Anruf zu senden.

Befehle anzeigen

Zonenpaar-Sicherheit anzeigen

- Mit diesem Befehl werden alle Zonenpaar-Zuordnungen und die angewendete Servicerichtlinie angezeigt.
- Die Quell- und Zielschlüsselwörter können verwendet werden, um eine bestimmte Zonenpaarzuordnung zu definieren, um zu überprüfen, ob viele vorhanden sind.

<#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

- Dieser Befehl zeigt Remote-Medienverbindungen aus der Perspektive von CUBE an>

<#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
```

Zeigt VoIP-RTP-Verbindungen an

- Dieser Befehl zeigt Informationen zur Remote- und lokalen Medienverbindung aus Sicht von CUBE an.

<#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
```

Anzeige der aktiven Sprachnachrichten

- Dieser Befehl zeigt in Verbindung mit dem über Voice Service Voip konfigurierten Befehl media bulk-stats Statistiken zum Senden (TX) und Empfangen (RX) für die Anrufabschnitte an.
- Wenn Medien über CUBE und ZBFW übertragen werden, muss der TX mit dem RX auf einem Peer-Call-Abschnitt übereinstimmen, z. B. 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

- Dieser Befehl zeigt Details der aktiven SIP-TCP-Verbindung über CUBE an.
- Befehle wie **show sip-ua connections udp detail** oder **show sip-ua connections tcp tls** detail können verwendet werden, um die gleichen Details für UDP SIP und TCP-TLS SIP anzuzeigen

<#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..]
```

Plattform für Firewall-Sitzungen anzeigen

- Dieser Befehl zeigt den Anruf aus der ZBFW-Perspektive an.
- Es gibt SIP-Sitzungen und Sub-Flows für RTP und RTCP.
- Die Session-ID aus dieser Ausgabe kann beim späteren Debuggen von ZBFW verwendet werden.
- **show policy-firewall sessions Plattformdetails** können verwendet werden, um noch mehr Daten anzuzeigen.

<#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

- Dieser Befehl zeigt ähnliche Daten wie **show policy-firewall sessions platform,** die Zonenpaarzuordnung ist jedoch ebenfalls in der Ausgabe enthalten, was praktisch für Debugging ist.

```
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
```

Fehlerbehebung

Die Fehlerbehebung für die zonenbasierte Firewall Cisco IOS XE finden Sie in diesem Dokument:

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

CUBE Local Transcoding Interface (LTI) + ZBFW

- Wenn CUBE mit Hardware-PVDM-Ressourcen auf dem Motherboard oder einem Netzwerkschnittstellenmodul (Network Interface Module, NIM) konfiguriert ist, können diese für CUBE LTI-Zwecke verwendet werden.
- Die Backplane-Schnittstelle für das PVDM verfügt über eine statische Service-Engine x/y/z, die der Platzierung des PVDM entspricht. Service-Engine 0/4 ist beispielsweise der PVDM/DSP-Steckplatz auf dem Motherboard.
- Diese Service-Engine MUSS mit einer Zone konfiguriert werden und ist in der Kernzone nicht vorhanden.

Mit der folgenden Konfiguration wird die von CUBE LTI verwendete Service-Engine der INSIDE-Zone für ZBFW-Zwecke zugeordnet.

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

Eine ähnliche Logik für die Zuordnung von Service Engine-Zonenpaaren kann für Hardware-PVDM/DSP-basierte SCCP-Medienressourcen und die SCCP-Bindungsschnittstelle verwendet werden. Dieses Thema wird in diesem Dokument jedoch nicht behandelt.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.