

CUBE(Cisco Unified Border Element) Enterprise와 함께 배치된 ZBFW(Zone-Based Firewall) 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[네트워크 다이어그램](#)

[ZBFW 크래시 교육 과정 개념](#)

[설정](#)

[보안 영역 정의](#)

[신뢰할 수 있는 트래픽에 대한 access-list, class-map 및 policy-map 생성](#)

[영역 쌍 매핑 생성](#)

[인터페이스에 영역 할당](#)

[다음을 확인합니다.](#)

[샘플 패킷 흐름 - 통화](#)

[명령 표시](#)

[영역 쌍 보안 표시](#)

[통화 활성화 음성 압축 표시](#)

[show voip rtp connections](#)

[통화 활성화 음성 요약 표시](#)

[show sip-ua connections tcp detail](#)

[show policy-firewall sessions 플랫폼](#)

[show policy-map type inspect zone-pair 세션](#)

[문제 해결](#)

[CUBE LTI\(Local Transcoding Interface\) + ZBFW](#)

소개

이 문서에서는 CUBE(Cisco Unified Border Element) Enterprise와 함께 ZBFW(Zone-Based Firewall)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

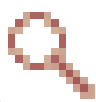
사용되는 구성 요소

- Cisco IOS® XE 17.10.1a를 실행하는 Cisco 라우터

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

- CUBE Enterprise 및 ZBFW 공동 배치는 16.7.1이 경과할 때까지 Cisco IOS XE에서 지원되지 않았습니다.

- CUBE Enterprise는 CUBE + ZBFW RTP 미디어 플로우만 지원합니다. 참조: [CSCwe66293](https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/213550-troubleshoot-one-way-audio-problems-in-f.html) 

- 이 문서는 CUBE Media Proxy, CUBE Service Provider, MGCP 또는 SCCP 게이트웨이, Cisco SRST 또는 ESRST 게이트웨이, H323 게이트웨이 또는 기타 아날로그/TDM 음성 게이트웨이에 적용할 수 없습니다.

- TDM/아날로그 음성 게이트웨이 및 ZBFW의 경우 다음 문서를 참조하십시오.

<https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/213550-troubleshoot-one-way-audio-problems-in-f.html>

네트워크 다이어그램

샘플 컨피그레이션에서는 INSIDE와 OUTSIDE라는 두 개의 논리적 네트워크 세그먼트를 보여줍니다.

INSIDE에는 단일 IP 네트워크가 포함되어 있으며 OUTSIDE에는 두 개의 IP 네트워크가 포함되어 있습니다.

레이어 3 네트워크 토폴로지

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

레이어 7 통화 흐름

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

레이어 7 미디어 흐름

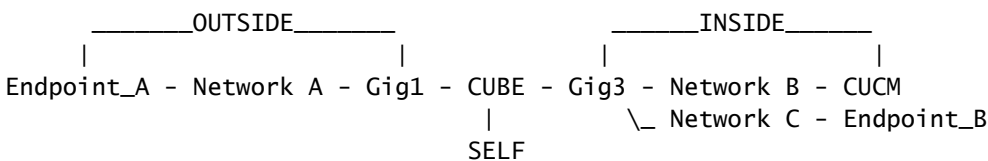
Endpoint_A <> RTP <> CUBE <> RTP <> Endpoint_B

ZBFW 크래시 교육 과정 개념

- ZBFW를 구성할 때 보안 영역 이름을 구성합니다. 그러면 인터페이스에서 정의됩니다. 이렇게 하면 해당 인터페이스로 드나드는 모든 트래픽이 해당 영역 이름과 연결됩니다.
 - 동일한 영역을 오가는 트래픽은 항상 허용됩니다.
 - 다른 영역으로 드나드는 트래픽은 관리자 컨피그레이션에서 허용하지 않는 한 삭제됩니다.
- 허용되는 트래픽 흐름을 정의하려면 소스 및 대상 영역 이름을 정의하는 단방향 영역 쌍 컨피그레이션을 통해 영역 매핑을 생성해야 합니다.
 - 그런 다음 이 영역 쌍 매핑은 검사, 허용 및 허용되지 않는 트래픽 유형을 세부적으로 제어하는 데 사용되는 서비스 정책과 연결됩니다.
- CUBE Enterprise는 특별 자체 영역에서 운영됩니다. SELF 영역은 ICMP, SSH, NTP, DNS 등과 같이 라우터에서 주고받는 다른 트래픽을 포함합니다.
 - CUBE LTI와 함께 사용할 하드웨어 PVDM이 자체 영역에 없으며 관리자가 구성한 영역에 매핑되어야 합니다.
- ZBFW는 반환 트래픽을 자동으로 허용하지 않으므로 관리자가 반환 트래픽을 정의하기 위해 영역 쌍을 구성해야 합니다.

다음 3개의 글머리 기호를 옆두에 두고 다음 영역을 L3 네트워크 토폴로지에 오버레이하여 추가할 수 있습니다.

- 네트워크 A, Gig1은 외부 영역
- 네트워크 B, 네트워크 C 및 Gig3는 내부 영역입니다.
- CUBE는 자체 영역의 일부입니다.



다음으로 CUBE+ZBFW를 통한 트래픽 흐름에 필요한 네 가지 단방향 영역 쌍 매핑을 논리적으로 생성할 수 있습니다.

소스	대상	사용
외부	셀프	엔드포인트 A의 인바운드 SIP 및 RTP 미디어
셀프	내부	CUBE에서 CUCM 및 엔드포인트

		트 B로의 아웃바운드 SIP 및 RTP 미디어
내부	셀프	CUCM 및 엔드포인트 B의 인바운드 SIP 및 RTP 미디어.
셀프	외부	CUBE에서 엔드포인트 A로의 아웃바운드 SIP 및 RTP 미디어.

이러한 개념을 염두에 두고 CUBE의 역할을 하는 Cisco IOS XE 라우터에서 ZBFW 구성을 시작할 수 있습니다.

설정

보안 영역 정의

INSIDE와 OUTSIDE의 두 가지 보안 영역을 구성해야 합니다. Self는 기본값이므로 정의할 필요가 없습니다.

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

신뢰할 수 있는 트래픽에 대한 access-list, class-map 및 policy-map 생성

어떤 트래픽을 제어하려면 라우터가 매칭하고 허용할 방법을 구성해야 합니다.

이를 위해 트래픽을 검사하는 확장 access-list, class-map 및 정책 맵을 만듭니다.

간소화를 위해 인바운드 트래픽과 아웃바운드 트래픽을 모두 매핑하는 각 영역에 대한 정책을 생성합니다.

match protocol sip 및 match protocol sip-tls와 같은 컨피그레이션이 사용될 수 있지만, 이해를 돕기 위해 IP/Ports가 구성되었습니다

OUTSIDE Extended Access List, 클래스 맵, 정책 맵

```
<#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, 클래스 맵, 정책 맵

```

!
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
 !

```

영역 쌍 매핑 생성

그 다음에는 앞에서 설명한 4개의 영역 쌍 매핑을 생성해야 합니다.

이러한 영역 쌍은 이전에 생성한 정책 맵에서 서비스 정책을 참조합니다.

```
<#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
!
```

인터페이스에 영역 할당

```
<#root>
```

```
! Assign Zones to interfaces
```

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

다음을 확인합니다.

샘플 패킷 흐름 - 통화

이때 엔드포인트 B에서 CUCM으로 향하는 CUBE로의 호출은 다음 시퀀스를 호출합니다.

1. 5060의 CUBE에 대한 인바운드 TCP SIP 패킷은 GIG 1을 인그레스(ingress)하고 외부 소스 영역에 매핑됩니다.

2. CUBE는 자체 영역에서 작동하므로 외부 대 자체 영역 쌍이 사용됩니다(OUT-SELF)
3. service-policy/policy-map TRUSTED-POLICY-OUT은 TRUSTED-CLASS-OUT 클래스 맵 및 TRUSTED-ACL-OUT 액세스 목록을 기반으로 트래픽을 검사하는 데 사용됩니다
4. 그러면 CUBE는 로컬 통화 라우팅 논리를 사용하여 통화를 전송할 위치와 사용할 이그레스 인터페이스를 결정합니다. 이 예에서는 이그레스 인터페이스가 CUCM에 대해 GIG 3이 됩니다.
 1. CUBE 통화 라우팅 개요는 다음 문서를 참조하십시오.
<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. CUBE는 GIG 3(내부)에서 소싱된 새 TCP 소켓 및 SIP INVITE를 생성합니다. CUBE는 자체 영역에서 작동하므로 자체 발신 영역 쌍을 사용합니다.
6. service-policy/policy-map TRUSTED-POLICY-IN은 TRUSTED-CLASS-IN 클래스 맵 및 TRUSTED-ACL-IN 액세스 목록을 기반으로 트래픽을 검사하는 데 사용됩니다
7. 이 흐름의 반환 트래픽은 IN-SELF 및 SELF-OUT 영역에서 통화에 대한 응답을 전송합니다.

명령 표시

영역 쌍 보안 표시

- 이 명령은 모든 영역 쌍 매핑 및 적용된 서비스 정책을 표시합니다.
- source, destination 키워드를 사용하여 특정 영역 쌍 매핑을 정의하여 여러 개의 영역 쌍 매핑을 확인할 수 있습니다.

<#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
```

통화 활성 음성 압축 표시

- 이 명령은 CUBE>의 관점에서 원격 미디어 연결을 표시합니다.

<#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	g711u1aw	VOIP	Psipp	192.168.1.48:16384
468	ORG	T2	g711u1aw	VOIP	P8675309	192.168.3.59:16386

```
show voip rtp connections
```

- 이 명령은 CUBE의 관점에서 원격 및 로컬 미디어 연결 정보를 표시합니다

<#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

통화 활성 음성 요약 표시

- 이 명령은 음성 서비스 voip를 통해 구성된 media bulk-stats 명령과 함께 통화 레그에 대한 TX(Send) 및 RX(Received) 통계를 표시합니다.
- 미디어가 CUBE 및 ZBFW를 통해 이동하는 경우 TX는 피어 통화 레그의 RX와 일치해야 합니다(예: 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
```


- 이 명령은 CUBE를 통한 활성 SIP TCP 연결 세부 정보를 표시합니다
- show sip-ua connections udp detail 또는 show sip-ua connections tcp tls detail과 같은 명령을 사용하여 UDP SIP 및 TCP-TLS SIP에 대한 동일한 세부사항을 표시할 수 있습니다

<#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 플랫폼

- 이 명령은 ZBFW 관점에서 통화를 표시합니다.
- RTP 및 RTCP에 대한 SIP 세션 및 하위 플로우가 있습니다.
- 이 출력의 세션 ID는 나중에 ZBFW를 디버깅할 때 사용할 수 있습니다.
- show policy-firewall sessions platform detail을 사용하면 더 많은 데이터를 볼 수 있습니다.

<#root>

Router#

show policy-firewall sessions platform

```
--show platform hardware qfp active feature firewall datapath scb 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 세션

- 이 명령은 show policy-firewall sessions 플랫폼과 유사한 데이터를 표시하지만 영역 쌍 매핑도 출력에 포함되어 디버깅에 유용합니다.

```
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
```

문제 해결

Cisco IOS XE 영역 기반 방화벽 트러블슈팅은 다음 문서에서 확인할 수 있습니다.

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

CUBE LTI(Local Transcoding Interface) + ZBFW

- 마더보드의 하드웨어 PVDM 리소스 또는 NIM(Network Interface Module)을 사용하여 CUBE를 구성하는 경우 CUBE LTI 용도로 사용할 수 있습니다.
- PVDM용 백플레인 인터페이스에는 PVDM의 배치에 해당하는 고정 서비스 엔진 x/y/z가 있습니다. 예를 들어, 서비스 엔진 0/4는 마더보드 PVDM/DSP 슬롯입니다.
- 이 서비스 엔진은 영역으로 구성되어야 하며 자체 영역에 없습니다.

다음 컨피그레이션에서는 ZBFW 용도로 CUBE LTI에서 사용하는 서비스 엔진을 INSIDE 영역에 매핑합니다.

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

하드웨어 PVDM/DSP 기반 SCCP 미디어 리소스 및 SCCP 바인딩 인터페이스에는 서비스 엔진 영역 쌍 매핑에 대해 유사한 논리를 사용할 수 있지만 이 항목은 이 문서의 범위를 벗어납니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.