

ISE에서 IP 액세스 제한 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[ISE 3.1 이하의 동작](#)

[구성](#)

[ISE 3.2의 동작](#)

[구성](#)

[ISE 3.2 P4 이상의 동작](#)

[구성](#)

[ISE GUI/CLI 복구](#)

[문제 해결](#)

[ISE 방화벽 규칙 확인](#)

[디버그 로그 확인](#)

[관련 정보](#)

소개

이 문서에서는 ISE 3.1, 3.2 및 3.3에서 IP 액세스 제한을 구성하는 데 사용할 수 있는 옵션에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Identity Service Engine에 대한 기본 지식

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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

IP 액세스 제한 기능을 사용하면 관리자가 ISE 관리 포털 및 서비스에 액세스할 수 있는 IP 주소 또는 범위를 제어할 수 있습니다.

이 기능은 다음을 비롯한 다양한 ISE 인터페이스 및 서비스에 적용됩니다.

- 관리 포털 액세스 및 CLI
- ERS API 액세스
- 게스트 및 스폰서 포털 액세스
- 내 디바이스 포털 액세스

활성화된 경우 ISE는 지정된 IP 주소 또는 범위의 연결만 허용합니다. 지정되지 않은 IP에서 ISE 관리 인터페이스에 액세스하려는 모든 시도는 차단됩니다.

우발적인 잠금의 경우, ISE는 IP 액세스 제한을 우회할 수 있는 '안전 모드' 시작 옵션을 제공합니다. 이를 통해 관리자는 액세스 권한을 다시 얻고 잘못된 컨피그레이션을 수정할 수 있습니다.

ISE 3.1 이하의 동작

Administration(관리)>Admin Access(관리 액세스)>Settings(설정)>Access(액세스)로 이동합니다. 다음과 같은 옵션이 있습니다.

- 세션
- IP 액세스
- MnT 액세스

구성

- "Allow only listed IP addresses to connect(나열된 IP 주소만 연결 허용)"를 선택합니다.
- "Add(추가)"를 클릭합니다.

∨ Access Restriction

- Allow all IP addresses to connect
- Allow only listed IP addresses to connect

∨ Configure IP List for Access Restriction

IP List

+ Add Edit Delete

<input type="checkbox"/>	IP	▼	MASK
--------------------------	----	---	------

No data available

IP 액세스 컨피그레이션

- ISE 3.1에서는 "Admin"과 "User" 서비스 중에서 선택할 수 있는 옵션이 없으므로 IP Access Restriction을 활성화하면 다음에 대한 연결이 차단됩니다.
 - GUI
 - CLI
 - SNMP
 - SSH
- IP 주소 IPv4 또는 IPv6를 CIDR 형식으로 입력하는 대화 상자가 열립니다.
- IP가 구성되면 마스크를 CIDR 형식으로 설정합니다.

restriction

in
d



Edit IP CIDR

IP Address/Subnet in CIDR format

IP Address



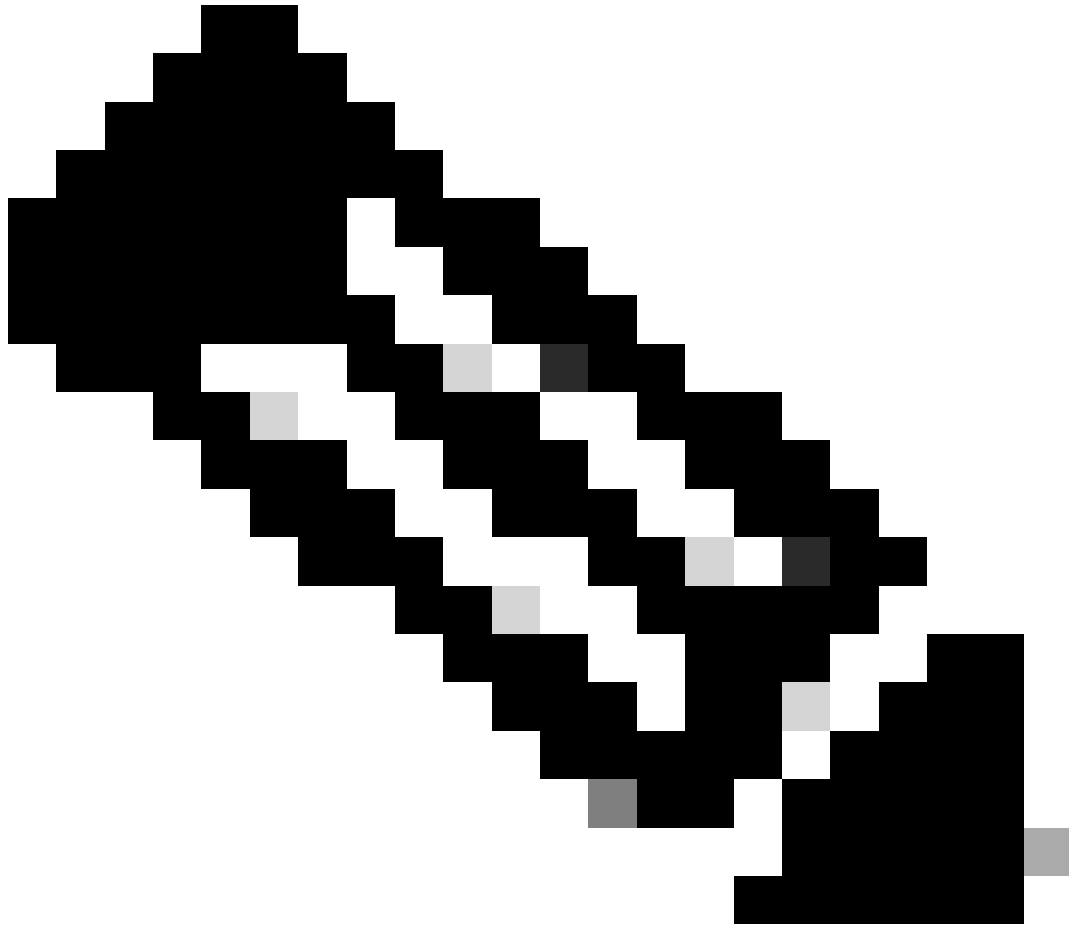
Netmask in CIDR format

32

Cancel

OK

IP CIDR 편집

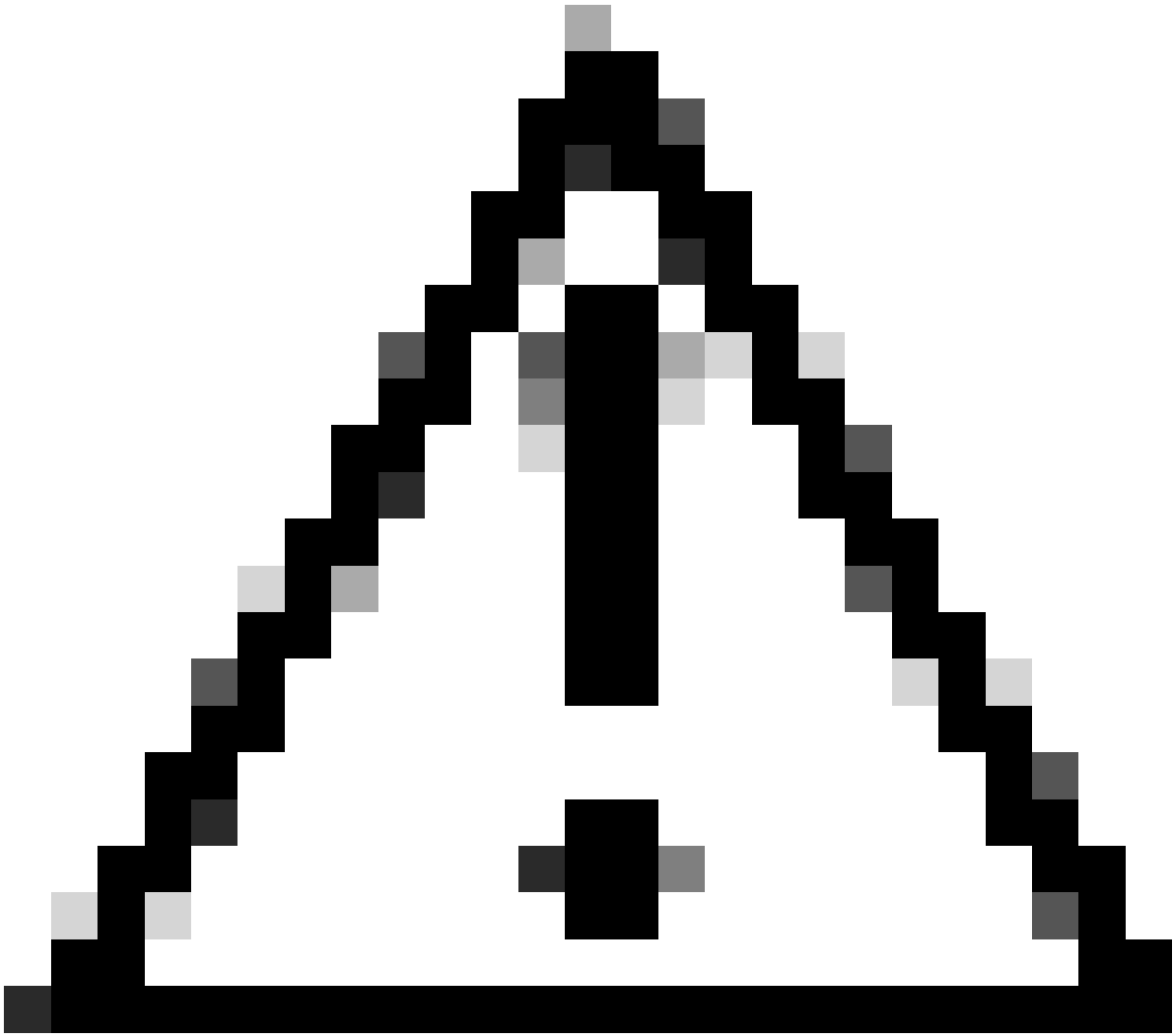


참고: IP CIDR(Classless Inter-Domain Routing) 형식은 IP 주소와 해당 라우팅 접두사를 나타내는 방법입니다.

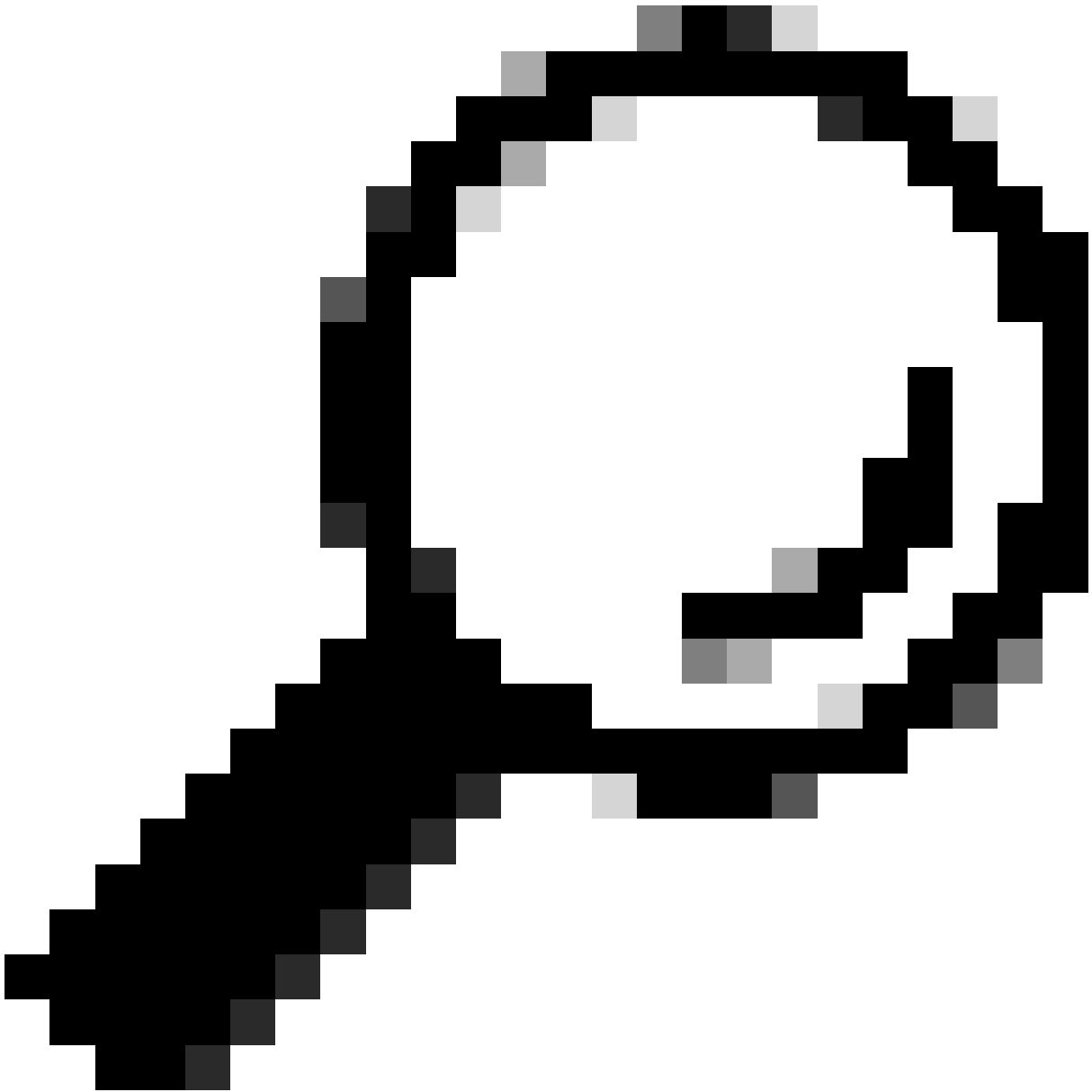
예:

IP: 10.8.16.32

마스크: /32



주의: IP 제한을 구성할 때 주의해야 합법적인 관리자 액세스 권한을 실수로 잠글 수 있습니다. Cisco에서는 IP 제한 컨피그레이션을 완전히 구현하기 전에 철저하게 테스트하는 것을 권장합니다.



팁: IPv4 주소의 경우:

- 특정 IP 주소에 /32를 사용합니다.
- 서브넷의 경우 다른 옵션을 사용합니다. 예: 10.26.192.0/18

ISE 3.2의 동작

Administration(관리)>Admin Access(관리 액세스)>Settings(설정)>Access(액세스)로 이동합니다.
다음 옵션을 사용할 수 있습니다.

- 세션
- IP 액세스
- MnT 액세스

구성

- "Allow only listed IP addresses to connect(나열된 IP 주소만 연결 허용)"를 선택합니다.
- "Add(추가)"를 클릭합니다.

Session **IP Access** MnT Access



∨ Access Restriction

Allow all IP addresses to connect

Allow only listed IP addresses to connect

∨ Configure IP List for Access Restriction

IP List

+ Add  Edit  Delete

<input type="checkbox"/>	IP	MASK	Admin Services	User Services
<input type="checkbox"/>	192.168.1.0/21	21	on	off
<input type="checkbox"/>	192.168.1.0/25	25	on	off

IP 액세스 컨피그레이션

- IP 주소 IPv4 또는 IPv6를 CIDR 형식으로 입력하는 대화 상자가 열립니다.
- IP가 구성되면 마스크를 CIDR 형식으로 설정합니다.
- 이러한 옵션은 IP 액세스 제한에 사용할 수 있습니다
 - 관리 서비스: GUI, CLI(SSH), SNMP, ERS, OpenAPI, UDN, API Gateway, PxGrid(패치 2에서 비활성화됨), MnT Analytics
 - 사용자 서비스: 게스트, BYOD, 포스터, 프로파일링
 - 관리자 및 사용자 서비스

IP CIDR 편집

- "Save(저장)" 버튼을 클릭합니다.
- "ON"은 관리자 서비스가 활성화되었음을, "OFF"는 사용자 서비스가 비활성화되었음을 의미합니다.

Configure IP List for Access Restriction

IP List

+ Add Edit Delete

<input type="checkbox"/>	IP	MASK	Admin Services	User Services
<input checked="" type="checkbox"/>	[Color-coded IP]	21	on	off
<input type="checkbox"/>	[Color-coded IP]	25	on	off

3.2의 IP 액세스 컨피그레이션

ISE 3.2 P4 이상의 동작

Administration(관리)>Admin Access(관리 액세스)>Settings(설정)>Access(액세스)로 이동합니다.

다음 옵션을 사용할 수 있습니다.

- 세션
- 관리 GUI&CLI: ISE GUI(TCP 443), ISE CLI(SSH TCP22) 및 SNMP.
- 관리 서비스: ERS API, Open API, pxGrid, DataConnect.
- 사용자 서비스: 게스트, BYOD, 상태
- MNT 액세스: 이 옵션을 사용하면 ISE는 외부 소스에서 전송된 Syslog 메시지를 사용하지 않습니다.

구성

- "Allow only listed IP addresses to connect(나열된 IP 주소만 연결 허용)"를 선택합니다.
- "Add(추가)"를 클릭합니다.

Session **Admin GUI & CLI** Admin Services User Services MnT Access

Access Restriction for Admin GUI & CLI

Allow all IP addresses to connect

Allow only listed IP addresses to connect

Configure IP List for Access Permission

+ Add Edit Delete

IP	MASK
----	------

No data available

3.3의 IP 액세스 컨피그레이션

- IP 주소 IPv4 또는 IPv6를 CIDR 형식으로 입력하는 대화 상자가 열립니다.
- IP가 구성되면 마스크를 CIDR 형식으로 설정합니다.
- "Add(추가)"를 클릭합니다.

ISE GUI/CLI 복구

- 콘솔을 사용하여 로그인
- 애플리케이션 중지 ise를 사용하여 ISE 서비스 중지
- 애플리케이션을 사용하여 ISE 서비스 시작 ise safe 시작
- GUI에서 IP 액세스 제한을 제거합니다.

문제 해결

패킷 캡처를 수행하여 ISE가 응답하지 않거나 트래픽을 삭제하고 있는지 확인합니다.

No.	Time	Source	Destination	Protocol	Length	Info	Acct-Session-id
181	2024-07-04 20:52:39.828119	10.0.193.197	10.4.17.115	TCP		59162 → 22 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1119 WS=64 TS...	
189	2024-07-04 20:52:39.985504	10.0.193.197	10.4.17.115	TCP		[TCP Retransmission] 59162 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=11...	
196	2024-07-04 20:52:39.998112	10.0.193.197	10.4.17.115	TCP		[TCP Retransmission] 59162 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=11...	
197	2024-07-04 20:52:40.059885	10.0.193.197	10.4.17.115	TCP		[TCP Retransmission] 59162 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=11...	
198	2024-07-04 20:52:40.148891	10.0.193.197	10.4.17.115	TCP		[TCP Retransmission] 59162 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=11...	
202	2024-07-04 20:52:40.215029	10.0.193.197	10.4.17.115	TCP		[TCP Retransmission] 59162 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=11...	
208	2024-07-04 20:52:40.347076	10.0.193.197	10.4.17.115	TCP		[TCP Retransmission] 59162 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=11...	
212	2024-07-04 20:52:40.598114	10.0.193.197	10.4.17.115	TCP		[TCP Retransmission] 59162 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=11...	
229	2024-07-04 20:52:41.096856	10.0.193.197	10.4.17.115	TCP		[TCP Retransmission] 59162 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=11...	
289	2024-07-04 20:52:42.076448	10.0.193.197	10.4.17.115	TCP		[TCP Retransmission] 59162 → 22 [SYN] Seq=0 Win=65535 Len=0 MSS=11...	

ISE 방화벽 규칙 확인

- 3.1 이하라면 쇼테크에서만 확인할 수 있습니다.
 - show tech를 가져와 "show tech-support file <filename>"을 사용하여 로컬 디스크에 저장할 수 있습니다.
 - 그런 다음 "copy disk:/<filename> ftp://<ip_address>/path"를 사용하여 저장소에 파일을 전송할 수 있습니다. 저장소 URL은 사용 중인 저장소 유형에 따라 변경됩니다
 - 파일을 컴퓨터에 다운로드하여 읽고 "Running iptables -nvL"을 찾을 수 있습니다.
 - 쇼테크의 초기 규칙은 아래에 포함되어 있지 않습니다. 즉, 여기서는 IP 액세스 제한 기능별 show tech에 추가된 마지막 규칙을 찾을 수 있습니다.

<#root>

Running iptables -nvL...

.

.

Chain ACCEPT_22_tcp_ipv4 (1 references)

pkts bytes target prot opt in out source destination

0 0 ACCEPT tcp -- eth0 * x.x.x.x/x 0.0.0.0/0

tcp dpt:22

Firewall rule permitting the SSH traffic from segment x.x.x.x/x

461 32052 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED

65 4048 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain ACCEPT_161_udp_ipv4 (1 references)

pkts bytes target prot opt in out source destination

0 0 ACCEPT udp -- * * x.x.x.x/x 0.0.0.0/0

udp dpt:161

Firewall rule permitting the SNMP traffic from segment x.x.x.x/x

0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED

0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

- 3.2 이상의 경우 "show firewall" 명령을 사용하여 방화벽 규칙을 확인할 수 있습니다.
- 3.2 이상 버전에서는 IP 액세스 제한으로 차단되는 서비스에 대한 제어력을 강화합니다.

<#root>

gjuarez-311/admin#show firewall

.
.

Chain ACCEPT_22_tcp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
170 13492 ACCEPT tcp -- eth0 * x.x.x.x/x 0.0.0.0/0

tcp dpt:22

Firewall rule permitting the SSH traffic from segment x.x.x.x/x

0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
13 784 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain ACCEPT_161_udp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT udp -- * * x.x.x.x/x 0.0.0.0/0

udp dpt:161

Firewall rule permitting the SNMP traffic from segment x.x.x.x/x

0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain ACCEPT_8910_tcp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp -- * * x.x.x.x/x 0.0.0.0/0

tcp dpt:8910

Firewall rule permitting the PxGrid traffic from segment x.x.x.x/x

0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
90 5400 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain ACCEPT_8443_tcp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp -- * * x.x.x.x/x 0.0.0.0/0

tcp dpt:8443 F

irewall rule permitting the HTTPS traffic from segment x.x.x.x/x

0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0

Chain ACCEPT_8444_tcp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp -- * * x.x.x.x/x 0.0.0.0/0

tcp dpt:8444 F

iptables rule permitting the Block List Portal traffic from segment x.x.x.x/x

```
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0
```

```
Chain ACCEPT_8445_tcp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp -- * * x.x.x.x/x 0.0.0.0/0
```

tcp dpt:8445 F

iptables rule permitting the Sponsor Portal traffic from segment x.x.x.x/x

```
0 0 ACCEPT all -- * * 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
0 0 DROP all -- * * 0.0.0.0/0 0.0.0.0/0
```

디버그 로그 확인



경고: 일부 트래픽에서는 로그를 생성하지 않습니다. IP 액세스 제한은 애플리케이션 수준에서 그리고 Linux 내부 방화벽을 사용하여 트래픽을 차단할 수 있습니다. SNMP, CLI 및 SSH는 로그가 생성되지 않도록 방화벽 레벨에서 차단됩니다.

- GUI에서 DEBUG에서 "Infrastructure" 구성 요소를 활성화합니다.
- show logging application ise-psc.log tail 사용

다음 로그는 IP 액세스 제한에서 조치를 취하는 시점을 확인할 수 있습니다.

```
2024-07-04 18:19:11,339 DEBUG [admin-http-pool31] [] cisco.cpm.infrastructure.systemconfig.CpmIpFilterCa
2024-07-04 18:19:11,339 DEBUG [admin-http-pool31] [] cisco.cpm.infrastructure.systemconfig.CpmIpFilterCa
2024-07-04 18:19:11,339 DEBUG [admin-http-pool31] [] cisco.cpm.infrastructure.systemconfig.CpmIpFilterCa
2024-07-04 18:19:11,339 DEBUG [admin-http-pool31] [] cisco.cpm.infrastructure.systemconfig.CpmIpFilterCa
2024-07-04 18:19:11,339 DEBUG [admin-http-pool31] [] cisco.cpm.infrastructure.systemconfig.CpmIpFilterCa
```

관련 정보

- [Cisco 기술 지원 및 다운로드](#)
- [ISE 3.1 관리 가이드](#)
- [ISE 3.2 관리 설명서](#)
- [ISE 3.3 관리 설명서](#)

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.