

ISE في IP لوصول دي يوقت ني وكت

تا يوت حمل

[قم دق م ل](#)

[ة ي س اس أ ل ا ت ا ب ل ط ت م ل ا](#)

[ت ا ب ل ط ت م ل ا](#)

[ة م د خ ت س م ل ا ت ا ن و ك م ل ا](#)

[ة ي س اس أ ت ا م و ل ع م](#)

[ل ق أ و ISE 3.1 في ك و ل س ل ا](#)

[ن ي و ك ت ل ا](#)

[ISE 3.2 في ك و ل س ل ا](#)

[ن ي و ك ت ل ا](#)

[ر ب ك أ و ISE 3.2 P4 في ك و ل س ل ا](#)

[ن ي و ك ت ل ا](#)

[ISE \(CLI\) ر م ا و أ ل ا ر ط س ة ه ج ا و \(GUI\) ة ي م و س ر ل ا م د خ ت س م ل ا ة ه ج ا و ت د ر ت س ا](#)

[ا ه ج ا ل ص ا و ا ط ا خ أ ل ا ف ا ش ك ت س ا](#)

[ISE ة ي م ح ر ا د ج د ع ا و ق ص ح ف](#)

[ح ي ح ص ت ل ا ت ا ل ج س ص ح ف](#)

[ة ل ص ت ا ذ ت ا م و ل ع م](#)

ة م د ق م ل ا

3.3 و 3.2 و ISE 3.1 في IP لوصول دي يوقت ني وكت ل ة ح ا ت م ل ا ت ا ر ا ي خ ل ا د ن ت س م ل ا ا ذ ه ف ص ي

ة ي س اس أ ل ا ت ا ب ل ط ت م ل ا

ت ا ب ل ط ت م ل ا

ة ي ل ل ا ت ل ا ع ي ض ا و م ل ا ب ة ف ر ع م ك ي د ل ن و ك ت ن أ ب Cisco ي ص و ت

- Cisco Identity Service Engine ل ة ي س اس أ ل ا ة ف ر ع م ل ا

ة م د خ ت س م ل ا ت ا ن و ك م ل ا

ة ن ي ع م ة ي د ا م ت ا ن و ك م و ج م ا ر ب ت ا ر ا د ص ا ل ع د ن ت س م ل ا ا ذ ه ر ص ت ق ي ا ل

ة ص ا خ ة ي ل م ع م ة ئ ي ب ي ف ة د و ج و م ل ا ة ز ه ج أ ل ا ن م د ن ت س م ل ا ا ذ ه ي ف ة د ر ا و ل ا ت ا م و ل ع م ل ا ع ا ش ن ا م ت ت ن ا ك ا ذ ا (ي ض ا ر ت ف ا). ح و س م م ن ي و ك ت ب د ن ت س م ل ا ا ذ ه ي ف ة م د خ ت س م ل ا ة ز ه ج أ ل ا ع ي م ج ت ا د ب ر م ا ي أ ل ل م ت ح م ل ا ر ي ث ا ت ل ل ك م ه ف ن م د ك ا ت ف ، ل ي غ ش ت ل ا د ي ق ك ت ك ب ش

ة ي س اس أ ت ا م و ل ع م

وأ IP نيوانع يف مكحتلا ةيناكم | ني لوؤسم لل "IP" لى لوصول ديقت " ةزيم حيتت اهتامدخو ISE ةراد لخدم لى لوصول اه نكمي يتل تاقاطنلل

كلذ يف امب ، اهتامدخو ISE تاهجاو فل تخم لىع ةزيملا هذه قبطنت

- (رم أوأل رطس ةهجاو) CLI و لوؤسملا لخدم لى لوصول
- ERS API لوصول
- ةاعرلاو فويضلا ةبواب لى لوصول
- ب ةصاخلا ةزهجالا ةبواب لى لوصول

م تي . طقف ةدحمل تاقاطنلا وأ IP نيوانع نم تالاصتالاب ISE حمسي ، رايل اذه ني كمت دنع ةدحمل ريغ IP تالوكوتورب نم ISE لوؤسم تاهجاو لى لوصول تالواحم يا رطح

هنكمي يذلا "نمأل اءصولا" ليغشت ءدب رايل ISE ماظن رفوي ، يضرعلا ني مأتلا ةلاح يف يا حيصتو لوصول ةداعتساب ني لوؤسم لل حمسي اذهو . IP لى لوصول دويق زواجت ةئطاخ تانيوكت

لقاؤ 3.1 ISE يف كولسللا

هذه كي دل . Access > (لوصول تادادع) Administration > Admin Access > Settings لى لقتنا تارايل:

- ةسلج
- IP لى لوصول
- MNt لى لوصول

نيوكتلا

- "ليصوتلاب طقف ةجر دمل IP نيوانع ل اءصولا" ددح
- "فيضي" ةق طقط

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](#)



IP



MASK

No data available

IP لى لوصول نى وكت

- عنم لى لى دوى امم، "User" و "Admin" تامدخ نى ب دى دحت راى خ كى دل سى ل، ISE 3.1 ي ف
ب: IP لوصول و دوى ق تالاصت
◦ مېوسر لى مدخت سمل اة جاو
◦ CLI
◦ SNMP
◦ (SSH) نم آلا لقن لى لوك و تورب
- CIDR قى س ن ت ي ف، IPv4 و IPv6، ناو نعل ل خ دت ت ن ا شى ح راو ح ب ر م ح ت ف ي
- نى ب ل د اب ت م ل ا ه ي ج و ت ل ل) CIDR قى س ن ت ب ع ا ن ق ل ل نى ي ع ت ب م ق، IP نى و ك ت در ج م ب
(تائى ف ن و د ب تال ا ج م ل).

restriction

in
d



Edit IP CIDR

IP Address/Subnet in CIDR format

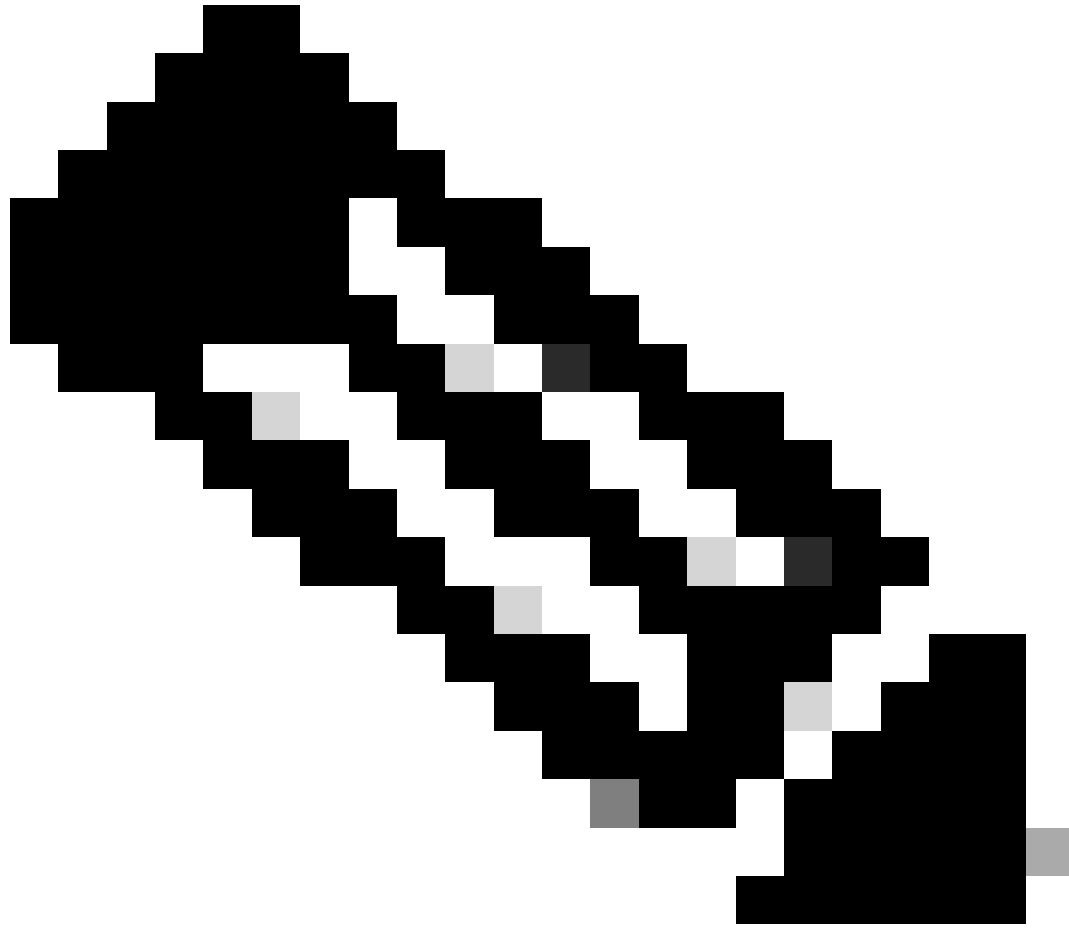
IP Address 

Netmask in CIDR format

Cancel

OK

رېځت IP CIDR

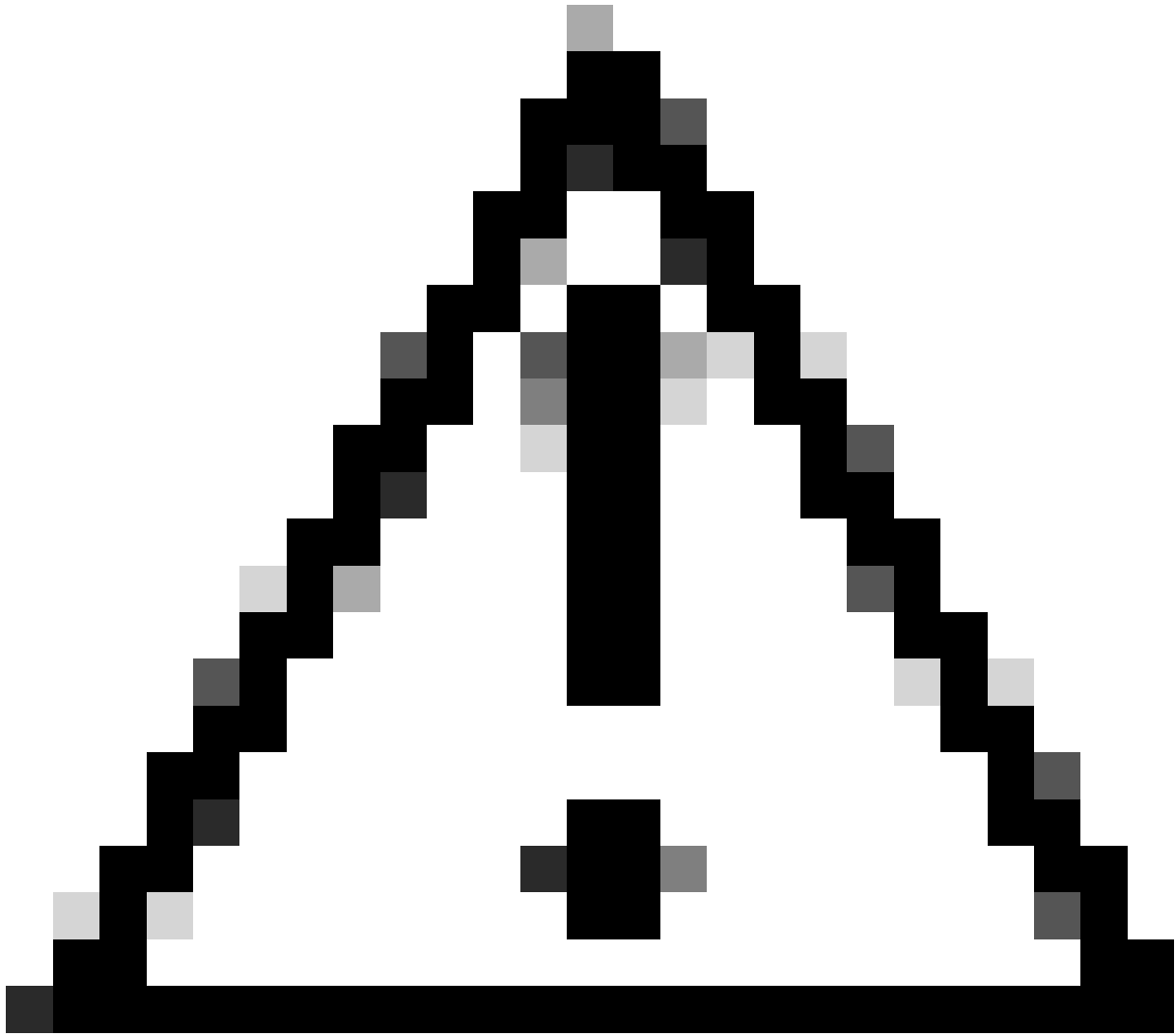


ليتم تل قيرط وه (تائف نود تالاجملا نيپ هيچوتلا) IP CIDR قيسنت :ةظحالم
اهب ةطبترملا هيچوتلا تائدابو IP نيوانع

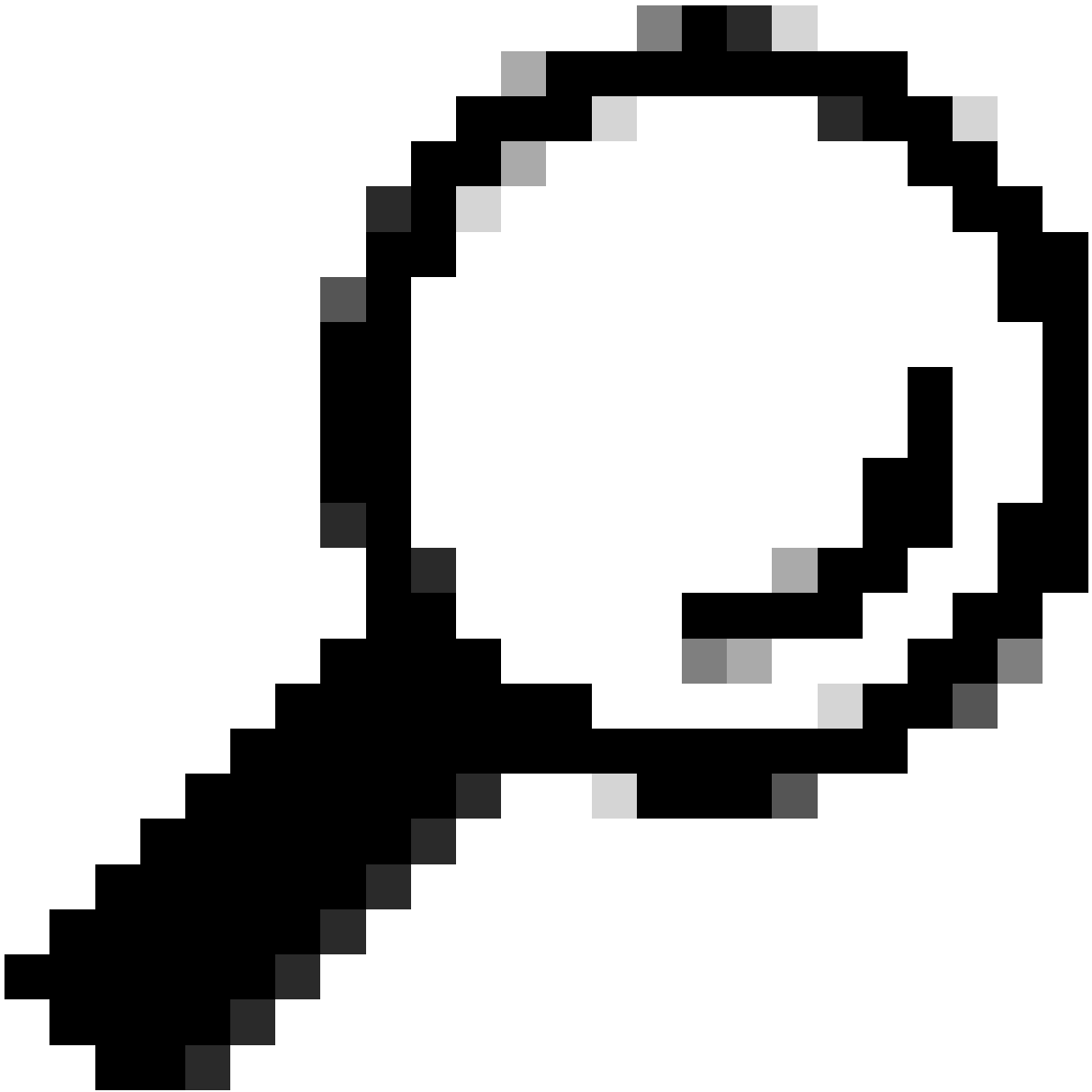
لائم:

IP: 10.8.16.32

عانقلا /32



عورشملا لوصولا لفق بئجتل IP دووق نيوكت دنع رذحلا يڤوت بڤي: ريذحت
لبق IP دئقئتل نيوكت يأل لماش رابتخا ءارڤاب Cisco يڤوت. دصق نود لوؤسملل
لماكلاب هذئفنت.



IPv4 نېوانع ل: حېملت

- ةدحمل IP نېوانع ل /32 مدختسأ
- لاثم: 10.26.192.0/18 رخآ راځي أمدختسأ ةيعرفلا تاكبشلل

ISE 3.2 ي كولسلا

كلت كي دل. Access. (لوصول ا تاداع) Administration>Admin Access>Settings ل لقتنا ةرفوتلا تاراځلا:

- ةسلج
- IP لوصول
- MNT لوصول

نيوكتلا

- "ليصوتلاب طقف ةجردملا IP نيوان عمل حامسلا" ددح
- "فيضي" ةقطق

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

<input type="checkbox"/>	IP	MASK	Admin Services	User Services
<input type="checkbox"/>	10.10.10.0/21	21	on	off
<input type="checkbox"/>	10.10.10.0/25	25	on	off

IP لى لوصول نيوكت

- CIDR قيسنت في IPv4 او IPv6، ناو نعل لخدت تنأ شيح راوح ع برم حت في
- ني ب لدابت مل هي جوتلا CIDR قيسنتب عانقل ني ني عت ب مق، IP نيوكت درجم ب (تائف نودب تالاجملا).
- IP لى لوصول ديقتل تاراخيلا هذه رفوتت
 - ةرادإلا تامدخ: GUI، CLI (SSH)، SNMP، ERS، OpenAPI، UDN، ةرابع API، PxGrid (لمطعم)
 - MnT تاليلحت (2) ححصتلا في
 - طيمننو، ةيعضو، BYOD، فيضي: ني مدختس مل تامدخ
 - ني مدختس مل او ةرادإلا تامدخ

✕

Edit IP CIDR

IP Address/Subnet in CIDR format

IP Address

Netmask in CIDR format

Services and portals that receives incoming connection :

Admin Services ⓘ

User Services ⓘ

Admin and User Services

رېرھت IP CIDR

- "ظفح" رزىل ع رقنا
- مءءء س م ل ا م ءء ل ى ط ع ت ى ن ع ى "OFF" و ؁ ء ر ا ء ل ا م ءء ن ى ك م ت ى ن ع ى "ON"

∨ Configure IP List for Access Restriction

IP List

+ Add Edit Delete

<input type="checkbox"/>	IP	MASK	Admin Services	User Services
<input checked="" type="checkbox"/>	10.10.10.10	21	on	off
<input type="checkbox"/>	10.10.10.10	25	on	off

3.2 ى ف IP لى ل ل و ص و ل ا ن ى و ك ت

ر ب ك ا و ISE 3.2 P4 ى ف ك و ل س ل ا

ك ل ت ك ى ء ل Access. (ل و ص و ل ا ء ا ء ء ع) Administration > Admin Access > Settings لى ل ل ق ت ن ا ء ر و ت م ل ا ء ا ر ا ى خ ل ا

- ةس ل ج
- مدختس م ل ة ه ج ا و : ل و و س م ل ل (CLI) ر م ا و ا ل ر ط س ة ه ج ا و و (GUI) ة م و س ر ل ا م د خ ت س م ل ا ة ه ج ا و ل و ك و ت و ر ب و (ISE) CLI (SSH TCP22) ر م ا و ا ل ر ط س ة ه ج ا و و (ISE) GUI (TCP 443) ة م و س ر ل ا (SNMP) ط ي س ب ل ل ا ص ت ا ل ا ة ك ب ش ة ر ا د ا
- DataConnect و pxGrid و Open API و ERS API : ة ر ا د ا ل ا ت ا م د خ .
- Posture و BYOD و فيض : م د خ ت س م ل ا ت ا م د خ .
- MNT Access: م ن م ة ل س ر م ل a syslog لئ س ر ر ا ي خ ل ا ا ذ ب ISE ك ل ه ت س ي ا ل

ن ي و ك ت ل ا

- " ل ي ص و ت ل ا ب ط ق ف ة ج ر د م ل ا IP ن ي و ا ن ع ل ح ا م س ل ا " د د ح
- " ف ي ض ي " ة ق ط ق ط

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

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

No data available

3.3 في IP لى ل و ص و ل ا ن ي و ك ت

- CIDR ق ي س ن ت ي ف ، IPv4 و IPv6 ، ن ا و ن ع ل ا ل خ د ت ت ن ا ش ي ح ر ا و ح ع ب ر م ح ت ف ي .
- ن ي ب ل د ا ب ت م ل ا ه ي ج و ت ل ا) CIDR ق ي س ن ت ب ع ا ن ق ل ا ن ي ي ع ت ب م ق ، IP ن ي و ك ت د ر ج م ب (ت ا ئ ف ن و د ب ت ا ل ا ج م ل ا .
- " ف ي ض ي " ة ق ط ق ط

ر م ا و ا ل ر ط س ة ه ج ا و / (GUI) ة م و س ر ل ا م د خ ت س م ل ا ة ه ج ا و ت د ر ت س ا (CLI) ISE

- م ك ح ت ل ا ة د ح و م ا د خ ت س ا ب ل و خ د ل ا ل ي ج س ت
- ق ي ب ط ت ل ا ف ا ق ي ا ل ISE م ا د خ ت س ا ب ISE ت ا م د خ ف ا ق ي ا
- ن م آ ق ي ب ط ت ل ا ل ي غ ش ت ع د ب م ا د خ ت س ا ب ISE ت ا م د خ ل ي غ ش ت ع د ب
- (GUI) ة م و س ر ل ا م د خ ت س م ل ا ة ه ج ا و ن م IP لى ل و ص و ل ا د ي ي ق ت ة ل ا ز ا ب م ق

ا ه ح ا ل ص ا و ا ط خ ا ل ا ف ا ش ك ت س ا

ر و ر م ل ا ة ك ر ح ط ا ق س ا ب م و ق ي ه ن ا و ا ب ي ج ت س ي ا ل ISE ن ا ك ا ذ ا م ق ق ح ت ل ل ة م ز ح ط ا ق ت ل ا ب م ق

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 يامح راج دعاوق صحف

- ينقنل ضرعل ي طرف اذه نم ققحتل كنكمي لقأو 3.1 ل
 - "show tech-support file <filename>" مادختساب يلحمل صرقل ي ف اهنيزختو ضرع ةينقت ذخأ كنكمي
 - <filename>/صرقل خسن مادختساب عدوتسم يل فلمل لقن كنكمي مث عون يلع ءانب عدوتسم لاب صاخل URL ناوع تاريغيغت "ftp://<ip_address>/path"
 - مدختست يذلا عدوتسملا "Running iptables -nvL" نع شحبل او هتءارق نم نكمتت يتح كزاهج يل فلمل ليزنت كنكمي
 - انه كنكمي ،رخآ ينعمب .هانأ ضرعل ةينقت ي في ةيلوأل دعاوقل ني مضت متي ال "tech by IP Access Restriction" ضرع" ةزيمب ققحمل ةريخأل دعاوقل يلع روثلع

<#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

- ةيامحل راج دعاوق نم ققحتل "show firewall" رمأل مادختسا كنكمي ،يلعأو 3.2 ل

- ديقت ةطساوب اهرظح م تي يتلا تامدخلال ي ف مكحتلال نم ديزملا رفوي ىلعأ وه امو 3.2
الى لوصولال IP.

<#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
```

```
irewall 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
```

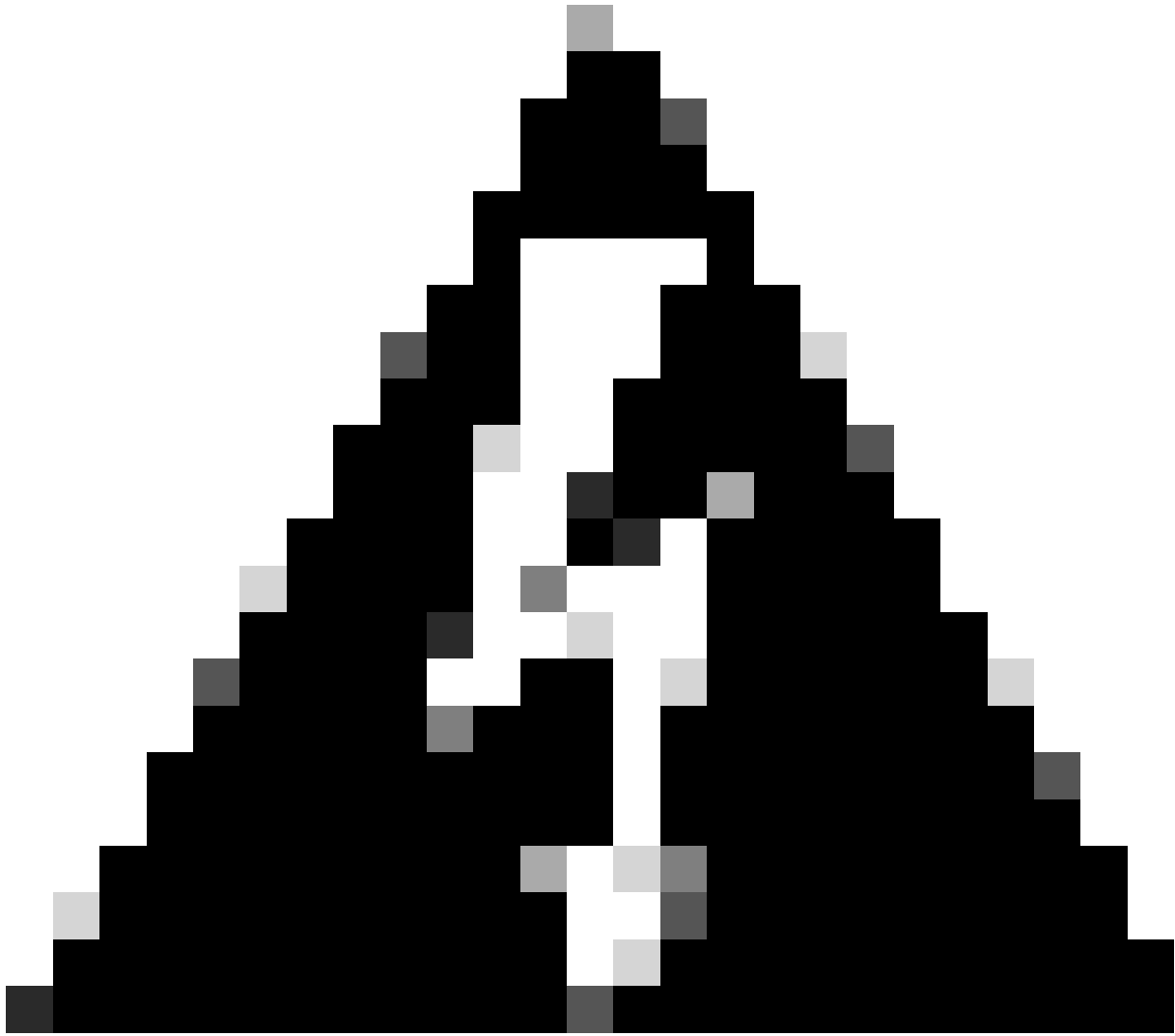
```
Chain ACCEPT_8445_tcp_ipv4 (1 references)
pkts bytes target prot opt in out source destination
0 0 ACCEPT tcp -- * * x.x.x.x/x 0.0.0.0/0
```

```
tcp dpt:8445 F
```

```
irewall 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
```

حيحصتالالتالجس صحف



دېيقت ي دؤي نأ نكمي .تالجس عاشنإب موقت رورملا تاكرح عي مج تسيل :ريذحت
ةيامح رادج مادختساب قي بطتلا يوتسم يلع رورملا ةكرح رطح يلإ IP يلإ لوصول
ةيامح رادج يوتسم يلع SSH و CLI و SNMP تالوكوتورب رطح متي .يلخادلا Linux
تالجس يأ عاشنإ متي ال يتح

- مدختسملا ةهجاو نم عاخالأ حيحصت ي ف "ةيساسألا ةينبلا" نوكملا نيكم تب مق
ةيموسرلا
- مدختسأ show logging application ise-psc.log tail

IP. يلإ لوصول ديقتل عارح اذختا دنع ةيلتلا تالجسلا يلع عالطالا نكمي

```
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
```

ةلص تاذا تامولعم

- [Cisco نيم تاليزنت لاولا وينفلا م عدلا](#)
- [ISE 3.1 لوؤسم ليلد](#)
- [ISE 3.2 لوؤسم ليلد](#)
- [ISE 3.3 لوؤسم ليلد](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخل مهتبل ب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إأمئاد ةوچرلاب ي صؤت وتامچرتل هذه ةقدنع اهتيل وئسم Cisco
Systems (رفوتم طبارل) ي لصلأل يزي لچن إل دن تسمل