

ىلإ لوصولا يف مكحتلا تاسايس نيوكت رادج ديدهت نع نمآلا عافدلل مكحتلا يوتسم ASA و ةيامحلا

تايوتحملا

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[نيوكتلا](#)

[تاننيوكتلا](#)

[FMC](#) ةطساوب ةرادملا FTD ل مكحتلا يوتسم ىلإ لوصولا يف مكحتلا ةمئاق نيوكت

[FDM](#) ةطساوب ةرادملا FTD ل مكحتلا يوتسم ىلإ لوصولا يف مكحتلا ةمئاق نيوكت

[CL](#) مادختساب ASA ل مكحتلا يوتسم ىلإ لوصولا يف مكحتلا ةمئاق نيوكت

[shun](#) رمألا مادختساب نمآلا ةيامحلا رادجلا تامجهل رطخل ليدب نيوكت

[ةحصلا نم ققحتلا](#)

[ةلصللا تاذءاطخألا](#)

ةمدقملا

نع نمآلا عافدلل مكحتلا يوتسم ىلإ لوصولا دعاوق نيوكت ةيلمع دنتسملا اذه فصبي (ASA) ةلدعمل نامآلا ةزهجأو ةيامحلا رادج ديدهت

ةيساسألا تابلطتملا

تابلطتملا

ةيلالتا عيضاوملاب ةفرعم كيديل نوكت ناب Cisco يوصوت

- (FTD) ةيامحلا رادج ديدهت نع نمآلا عافدللا
- (FDM) نمآلا ةيامحلا رادج ةزهجأ ريديم
- (FMC) نمآلا ةيامحلا رادج ةرادا زكرم
- Secure Firewall ASA
- (ACL) لوصولا يف مكحتلا ةمئاق
- FlexConfig

ةمدختسملا تانوكملا

ةيلالتا ةيداملا تانوكملا و اجماربلا تارادصا ىلإ دنتسملا اذه يف ةدراولا تامولعمل دنتست

- 7.2.5 رادصلإا ،نمآلا ةياملال رادج ديدت دض عافدلا
- Secure Firewall Manager Center، رادصلإا 7.2.5
- Secure Firewall Device Manager، رادصلإا 7.2.5
- Secure Firewall ASA، رادصلإا 9.18.3

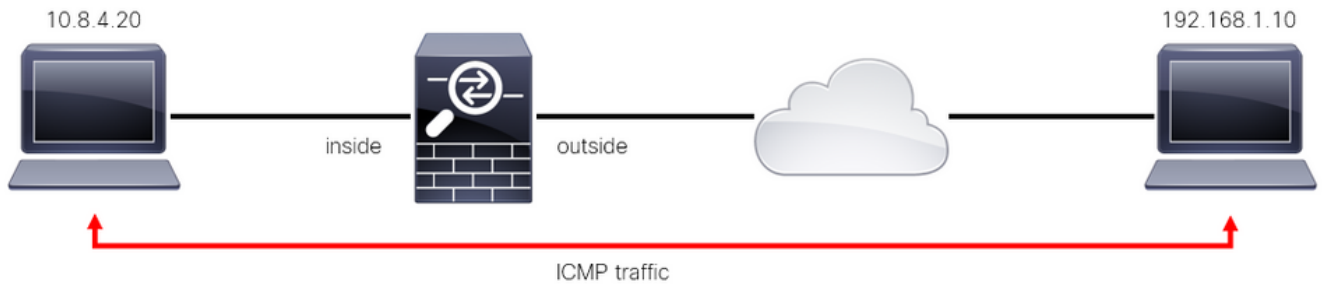
ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجال نم دنتسمل اذه يف ةدراول تامولعمل عاشنإ مت تناك اذا .(يضارتفا) حوسمم نيوكتب دنتسمل اذه يف ةمدختسمل ةزهجال عيمج تادب رما يال لمحتمل ريثاتلل كمهف نم دكاتف ،ليغشتلا ديق كتكبش

ةيساسا تامولعم

نم ،فورظلا ضعب يف ؛تانايبلا تاهجاو نيب اههيجوت متيو ةياملال رادج ةداع رورملا ةكرح ربعت ةياملال رادج مدختسي نأ نكمي . "نمآلا ةياملال رادج" لىلا ةهجوملا رورملا ةكرح ضفر ديفملا رورملا ةكرح ديفيقتل (ACL) مكحتلا يوتسم لىلا لوصولا يف مكحتلا ةمئاق Cisco نم نمآلا يف مكحتلا ةمئاق هيف نوكت نأ نكمي يذلا تقولا لىلع ةلثمألا دحأ نوكي دق . "عبرملا لىلا" (نم) VPN قفن عاشنإ مهنكمي عارظنلا يآ يف مكحتلا وه اديفم مكحتلا يوتسم لىلا لوصولا نمآلا ةياملال رادج (دعب نع لوصولل VPN وأ عقوم لىلا عقوم

"عبرملا لالخنم" ةياملال رادج رورم ةكرح نيأت

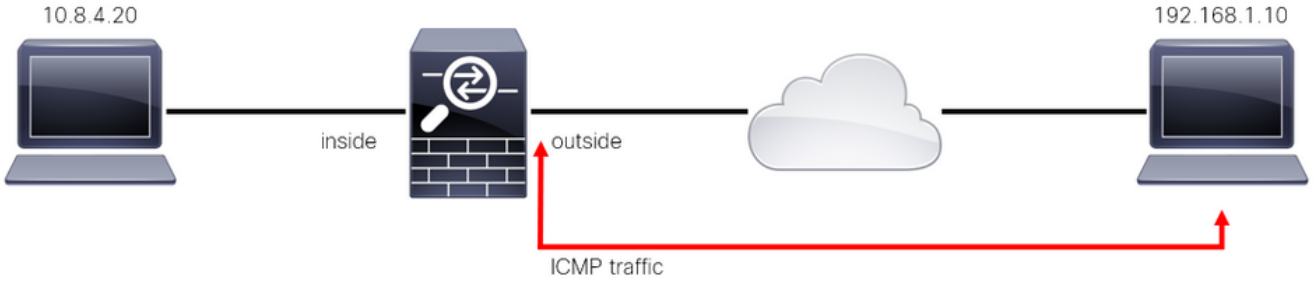
فرعي اذهو ،(ةرداص) ىرخأ ةهجاو لىلا (ةدراو) ةدحاو ةهجاو نم ةياملال نارديج ةداع رورملا ةكرح ربعت لوصولا يف مكحتلا جهن نم لك ةطساوب اهترادا متتو "عبرملا لالخنم" رورم ةكرح مساب ةقبسمل ةيفصتلا دعاوقو (ACP)



عبرملا لالخنم تانايبلا رورم ةكرح لاثم 1. ةروصل

"عبرملا لىلا" ةياملال رادج رورم ةكرح نيأت

وأ عقوم لىلا عقوم نم) FTD ةهجاو لىلا ةرشابم رورملا ةكرح هيجوت اهيف متي ىرخأ تالاح كانه ةطساوب اهترادا متتو "عبرملا لىلا" رورم ةكرح مساب فرعي اذهو ،(دعب نع لوصولل VPN ةكبش ةددحمل ةهجاو لىلا كلتل مكحتلا يوتسم



تانايبال رورم ةكرح ىلع لاثم 2. ةروصولا

مكحتللا ىوتسم ىلإ (ACL) لوصولا يف مكحتللا مئاوقب قلعتي اميف ةمهم تارابتعا

- ىلإ (ACL) لوصولا يف مكحتللا ةمئاق نيوكت بجي، FMC/FTD نم 7.0 رادصلإا نم ارابتعا ىلع ةمدختسمال رمألا ةغايص سفن مادختساب، FlexConfig مادختساب مكحتللا ىوتسم ASA.
- ىذلاو، لوصولا ةومجم نيوكتب ةيساسألا ةملكلاب مكحتللا ىوتسم قاحلإا متي ىوتسم ةملك نودب. ةنمألا ةيامحل رادج ةهجاو "ىلإ" تانايبال رورم ةكرح ضرغب موقيس ةكرح ديقت ىلع (ACL) لوصولا يف مكحتللا ةمئاق لمعتس، رمألاب ةقحلمل مكحتللا نمألا ةيامحل رادج "لالخ نم" رورملا.
- SSH أو ICMP أو Telnet مكحتللا ىوتسم (ACL) لوصولا يف مكحتللا ةمئاق ديقت نل تاسايسل اقبط (ضفرل/حامسل) هذه ةجلاعم متت. ةنمألا ةيامحل رادج ةهجاو ىلإ ةدراول ىلع ةيقبسا أهلو ىساسألا ماظنلا تاداعلإ.
- رورملا ةكرح ديقت ىلع مكحتللا ىوتسم (ACL) لوصولا يف مكحتللا ةمئاق لمعت أو FTD لوصولا يف مكحتللا ةسايس مكحتت نيح يف، هسفن نمألا ةيامحل رادج "ىلإ" نمألا ةيامحل رادج "لالخ نم" رورملا ةكرح يف، ASA ل ةيداعل لوصولا يف مكحتللا مئاوقب.
- ةياهن يف ىنمض "ضفر" دجوي ال، ةيداعل (ACL) لوصولا يف مكحتللا ةمئاق فالخب (ACL) لوصولا يف مكحتللا ةمئاق.
- "FTD ل يفارغلل عقوملا ديدحت" ةزيم مادختسا نكمي ال، دنتسمل اذه ءاشن تقوي يف "FTD" ىلإ لوصولا ديقتل.

نيوكتلا

ةفينعل VPN ةوق مادختسا ةنيعم ةلود نم IP نيوانع نم ةومجم لواحت، ىلاتلا لاثملا يف دض FTD ةيامحل راىخ لصفأ. FTD ةهجاو ىلإ لوخدلا ليجست ةلواحم لالخن نم ةكبشللا يف (ACL) لوصولا يف مكحتللا ةمئاق نيوكت وه هذه VPN ةكبشل ةيشحولا ةوقلا تامحه ةيخرال FTD ةهجاوب تالاصتالا هذه رطلل مكحتللا ىوتسم.

تانايبال

FMC ةطساوب ةرادملا FTD ل مكحتللا ىوتسم ىلإ لوصولا يف مكحتللا ةمئاق نيوكت

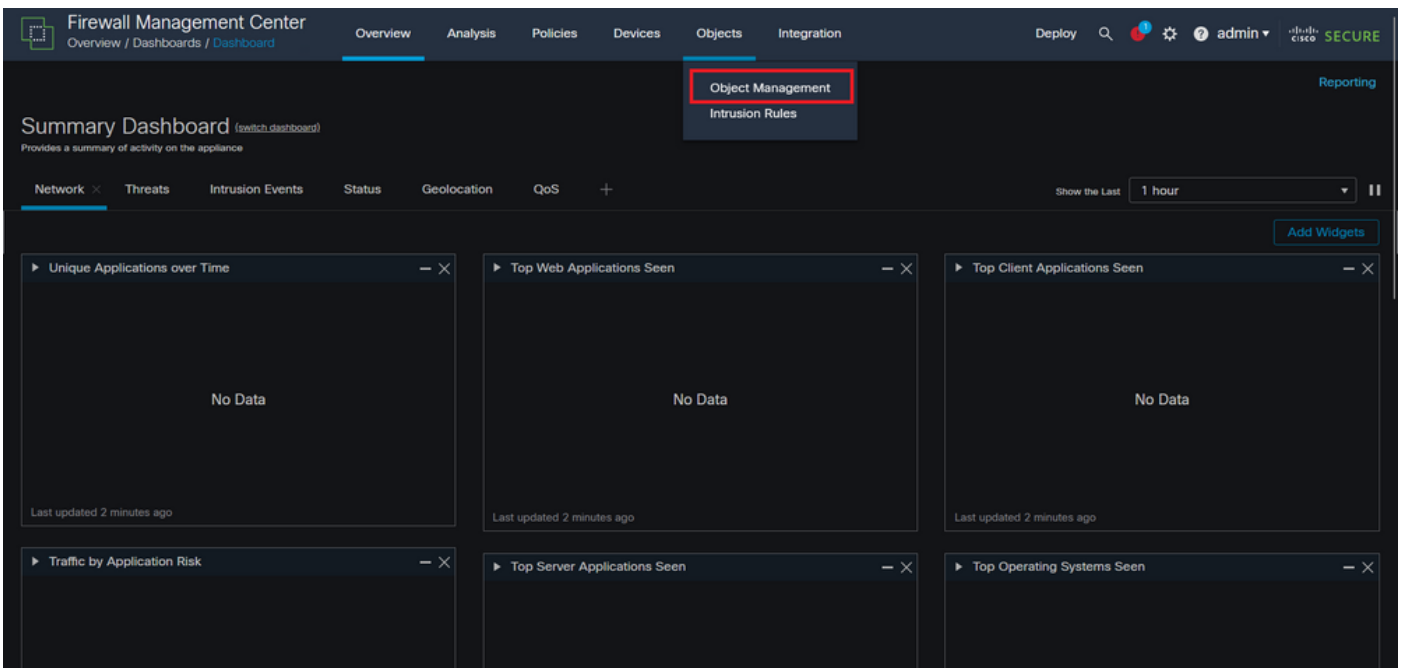
نيوكتل (FMC) دع ب نع لوصولو ي ف مكحتلا ةدحو ي ف هتعباتم يلى جاتحت يذلا ءارجإلا وه اذه ةكبشل ةمشاغلا ةوقلا تامجه رظحل مكحتلا يوتسمل (ACL) لوصولو ي ف مكحتلا ةمئاق ةجراخلا FTD ةهجاو يلى ةدراولا VPN:

ر ب ع HTTPS ف م ك ح ت ل ا ة د ح و ب ة ص ا خ ل ا (GUI) ة م و س ر ل ا م د خ ت س م ل ا ة ه ج ا و ح ت ف ا . 1 ة و ط خ ل ا . ك ب ة ص ا خ ل ا د ا م ت ع ا ل ا ت ا ن ا ي ب م ا د خ ت س ا ب ل و خ د ل ا ل ج س و .



FMC يلى لوخدلا ليحست ةحفص 3. ةروصل

يلى لقتنا، اذهل. ةعسوم (ACL) لوصولو ي ف مكحت ةمئاق ءاشنإ يلى جاتحت تنأ. 2. ةوطخل تانئالك ةراد > تانئالك.



تانئالك ةراد 4. ةروصل

ي ف مكحت ةمئاق ءاشنإل عسوم > لوصولو ةمئاق يلى لقتنا، يرسيل ءحوللا نم. 2.1. ةوطخل

ةةسوم (ACL) لوصول

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** Integration Deploy

AAA Server
Access List
Extended
Standard
Address Pools
Application Filters
AS Path
Cipher Suite List
Community List
Distinguished Name
DNS Server Group
External Attributes
File List
FlexConfig
Geolocation
Interface
Key Chain
Network
PKI
Policy List
Port
Prefix List

Network

Add Network Filter Show Unused Objects

A network object represents one or more IP addresses. Network objects are used in various places, including access control policies, network variables, intrusion rules, identity rules, network discovery rules, event searches, reports, and so on.

Name	Value	Type	Override
any	0.0.0.0/0 ::/0	Group	
any-ipv4	0.0.0.0/0	Network	
any-ipv6	::/0	Host	
IPv4-Benchmark-Tests	198.18.0.0/15	Network	
IPv4-Link-Local	169.254.0.0/16	Network	
IPv4-Multicast	224.0.0.0/4	Network	
IPv4-Private-10.0.0.0-8	10.0.0.0/8	Network	
IPv4-Private-172.16.0.0-12	172.16.0.0/12	Network	
IPv4-Private-192.168.0.0-16	192.168.0.0/16	Network	
IPv4-Private-All-RFC1918	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	Group	

Displaying 1 - 14 of 14 rows Page 1 of 1

ةةسوم ل (ACL) لوصول في مكحتل ةمئاق ةمئاق 5 ةروصل

ةةسوم ل لوصول ةمئاق ةفاضل ددح م 2.2 ةوطخل

Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** Integration Deploy

AAA Server
Access List
Extended
Standard
Address Pools
Application Filters
AS Path
Cipher Suite List
Community List
Distinguished Name
DNS Server Group
External Attributes
File List
FlexConfig
Geolocation
Interface
Key Chain
Network
PKI
Policy List
Port
Prefix List

Extended

Add Extended Access List Filter

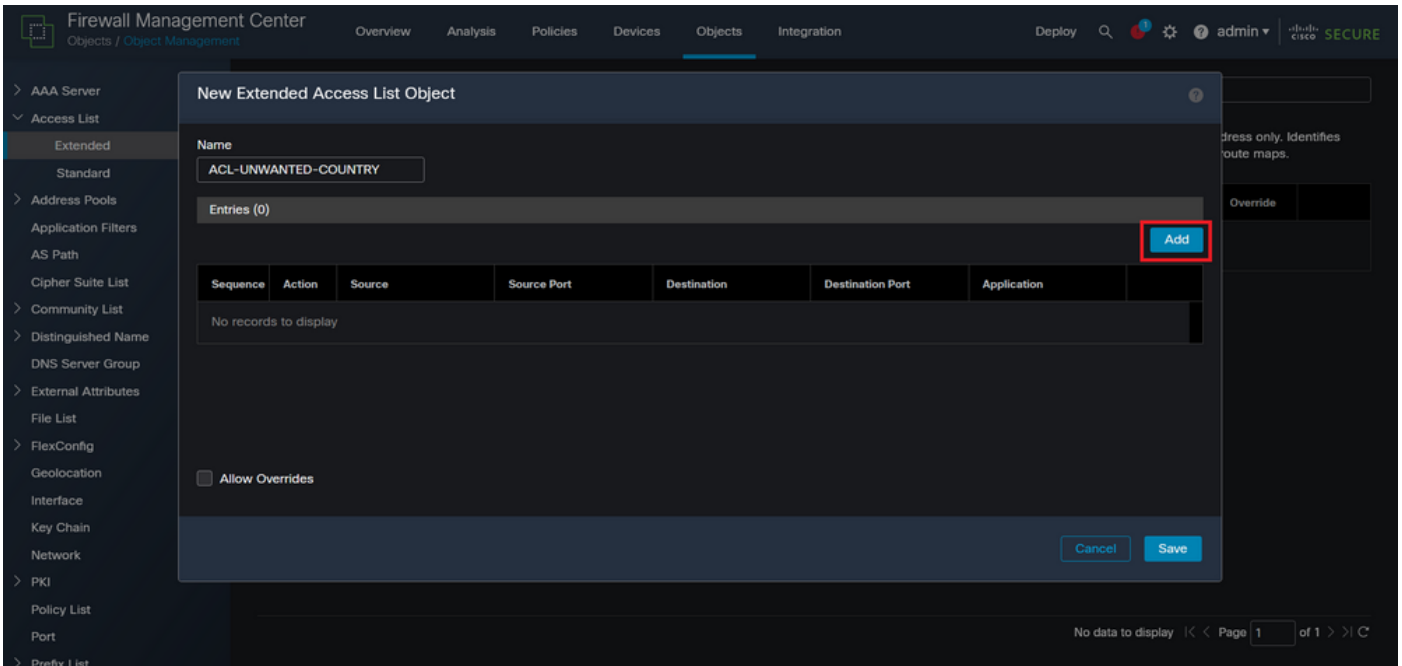
An access list object, also known as an access control list (ACL), selects the traffic to which a service will apply. Standard - Identifies traffic based on destination address only. Identifies traffic based on source and destination address and ports. Supports IPv4 and IPv6 addresses. You use these objects when configuring particular features, such as route maps.

Name	Value	Override
No records to display		

No data to display Page 1 of 1

ةةسوم ل (ACL) لوصول في مكحتل ةمئاق ةفاضل 6 ةروصل

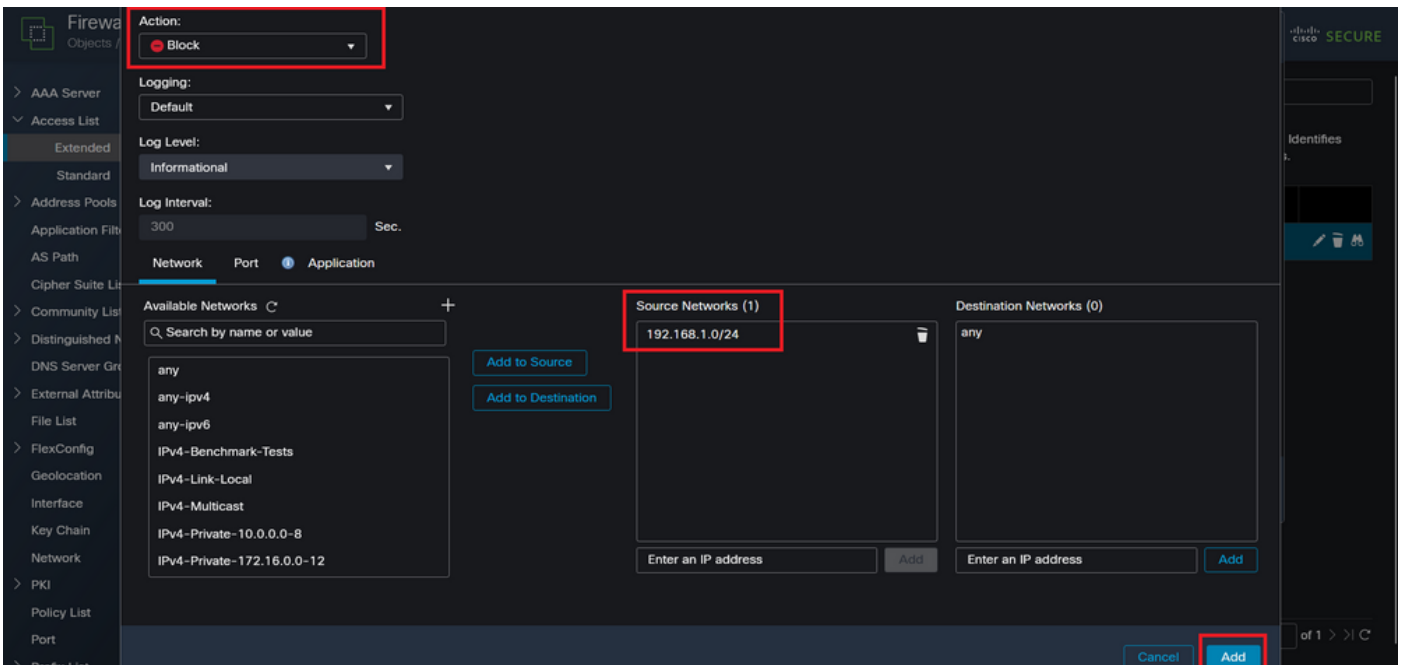
ةفاضل رزل قوف رقنا م ،ةةسوم ل (ACL) لوصول اب مكحتل ةمئاق ل مسا بتك 2.3 ةوطخل
(ACE): لوصول في مكحتل ل اءاشنل



ة عسوملا (ACL) لوصول يف مكحتلا مئاقق تالخدإ. 7 ةروصل

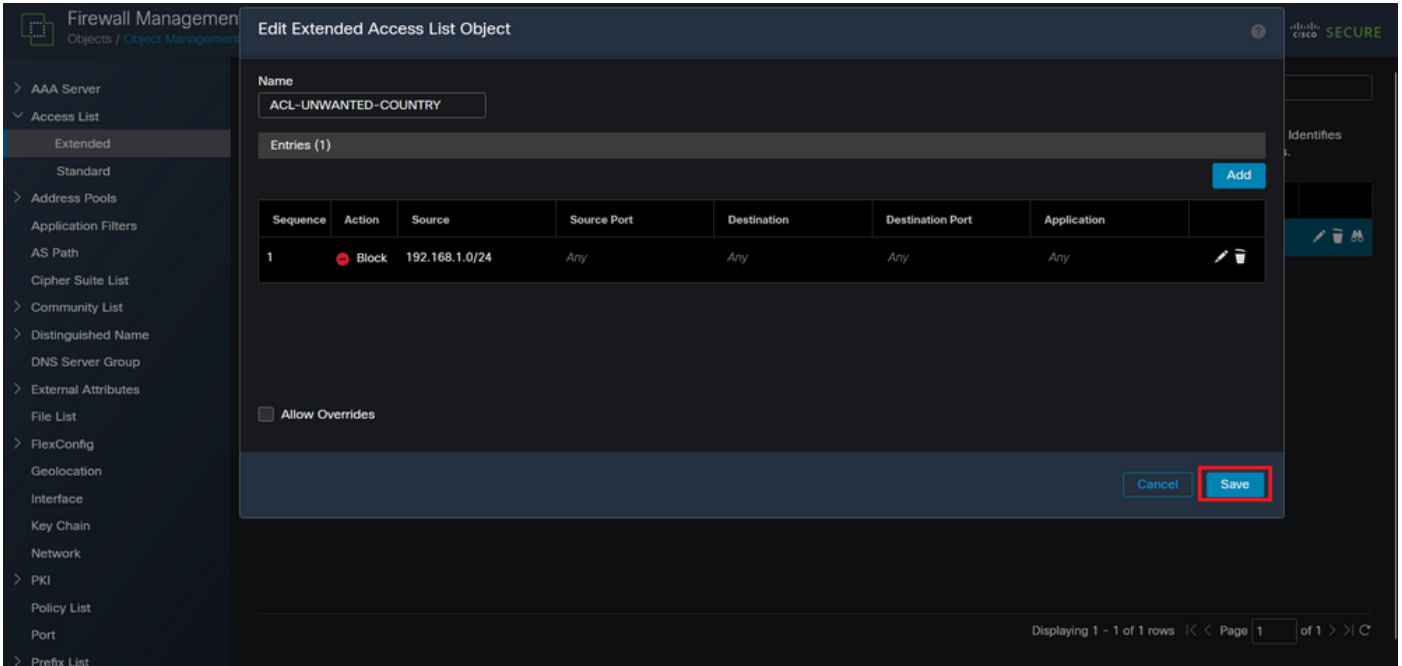
ةقباطم ل ردصملا ةكبشلا ةفاضاب مق مث ، "رطح" ل ACE ءارجإ ريغت ب مق 2.4 ةوطخل رزلا قوف رقناو ، ياك ةهجولا ةكبشلا يقبأو ، FTD ل اهضفر مزلي يتلا رورملا ةكرح ACE لخدإ لامكإل "ةفاضإ":

ةكبشلا ةمشاغللا ةوقلا تامجه رطح هنيوكت مت يذلا ACE لخدإ موقيس ، لاثملا اذه يف - 192.168.1.0/24 ةيعرفلا ةكبشلا نم ةمداكل VPN.



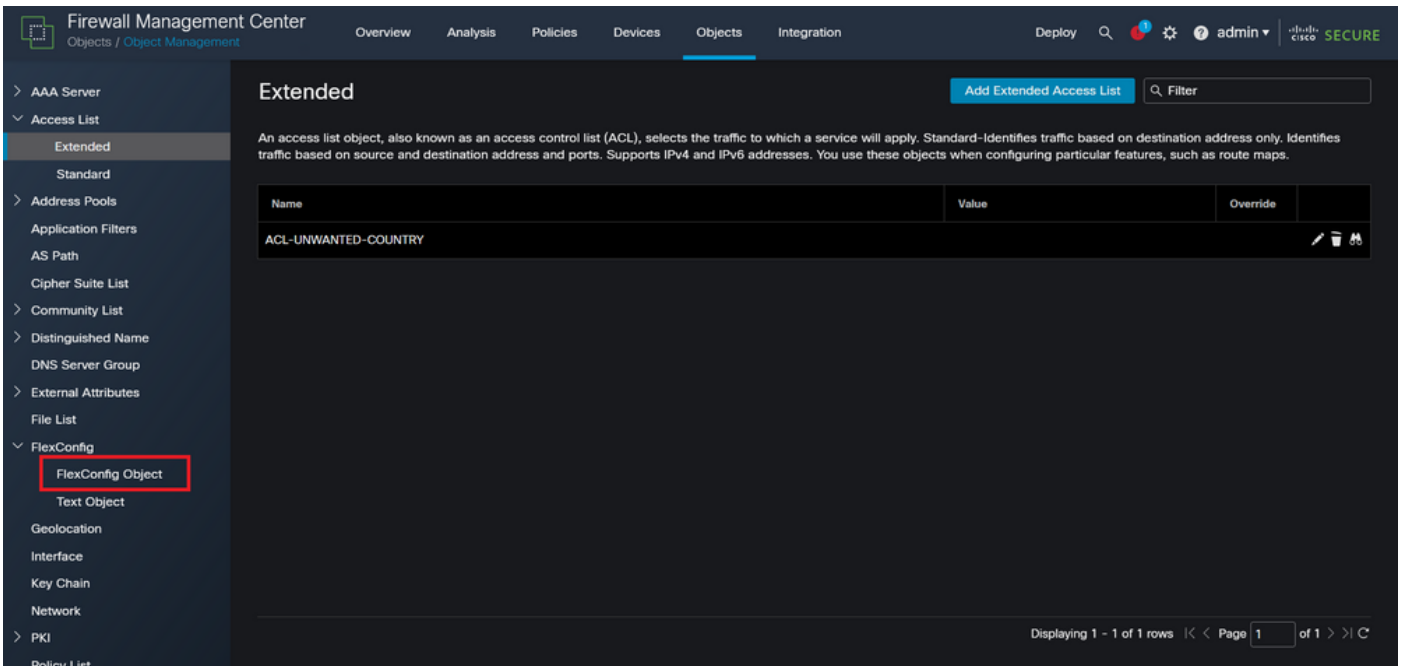
ةضوفرمل تالكبشلا. 8 ةروصل

يرخأ ةرم ةفاضإ رزلا قوف رقنا ، ACE تالخدإ نم ديزملا ةفاضإ ل ةجالحلا ةلاح يف 2.5 ةوطخل يف مكحتلا مئاقق نيوكت لامكتسال ظفح رزلا قوف رقنا ، كلذ دع ب 2.4 ةوطخل ررك مث (ACL) لوصول.



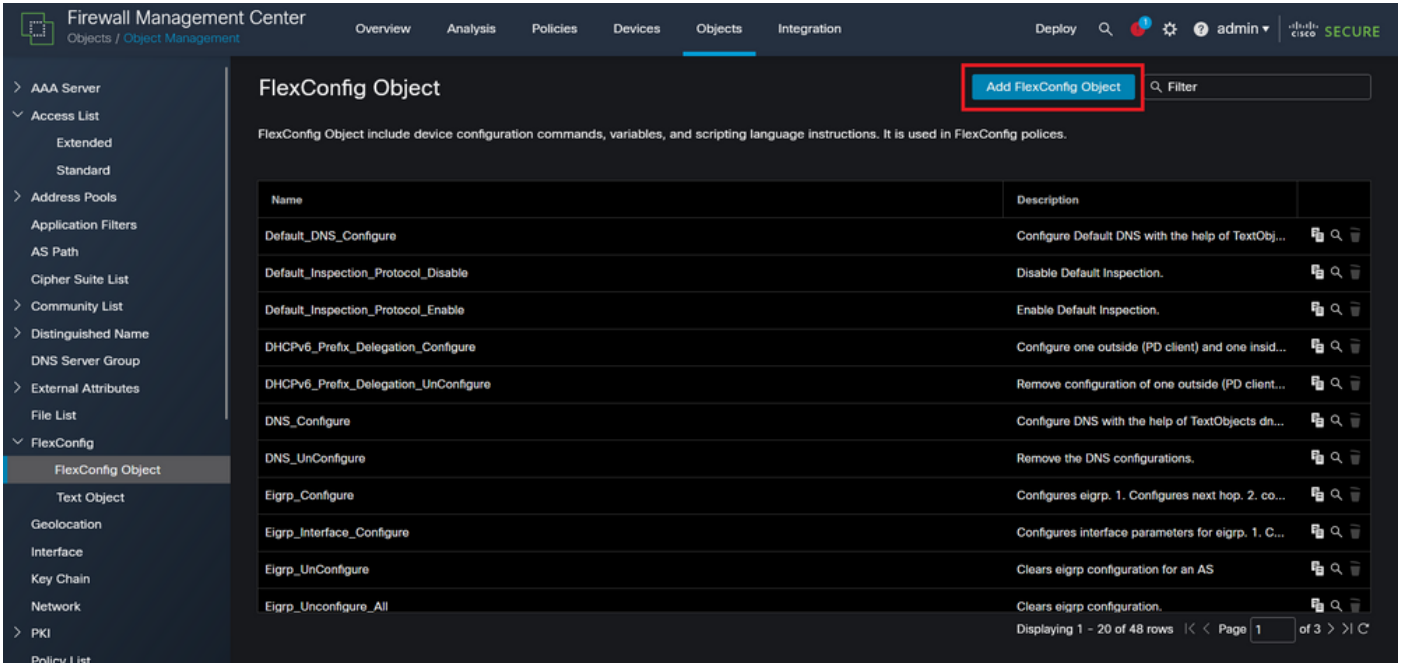
ةلمتكم لة عسوم ل (ACL) لوصول ي ف مكحتل مئوق تال اءءء. ةروصول

ل لوصول ي ف مكحتل ةمئاق ق ي بطل Flex-Config نئ اء نئ وءء ك مزل ي ، مء 3 ةوطلء راءل ءءءو ، ىرس ل ءءول ل ل ل ل قءءنا ، اءءل . ةءءءءل ءءء ةءءء ل ل ءءءءم FlexConfig > FlexConfig Object.



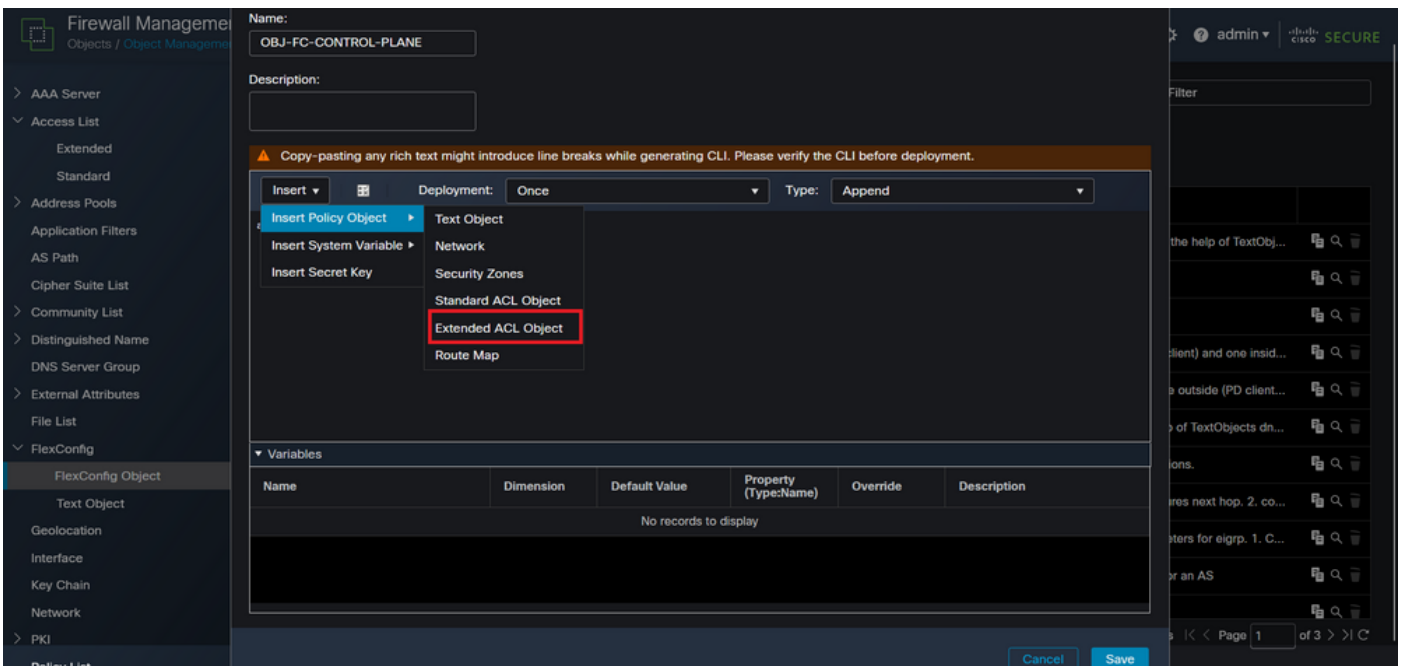
ل ءءءءء FlexConfig ةمئاق 10. ةروصول

FlexConfig نئ اء ةءاض ل قوف رءنا 3.1 ةوطلءل.



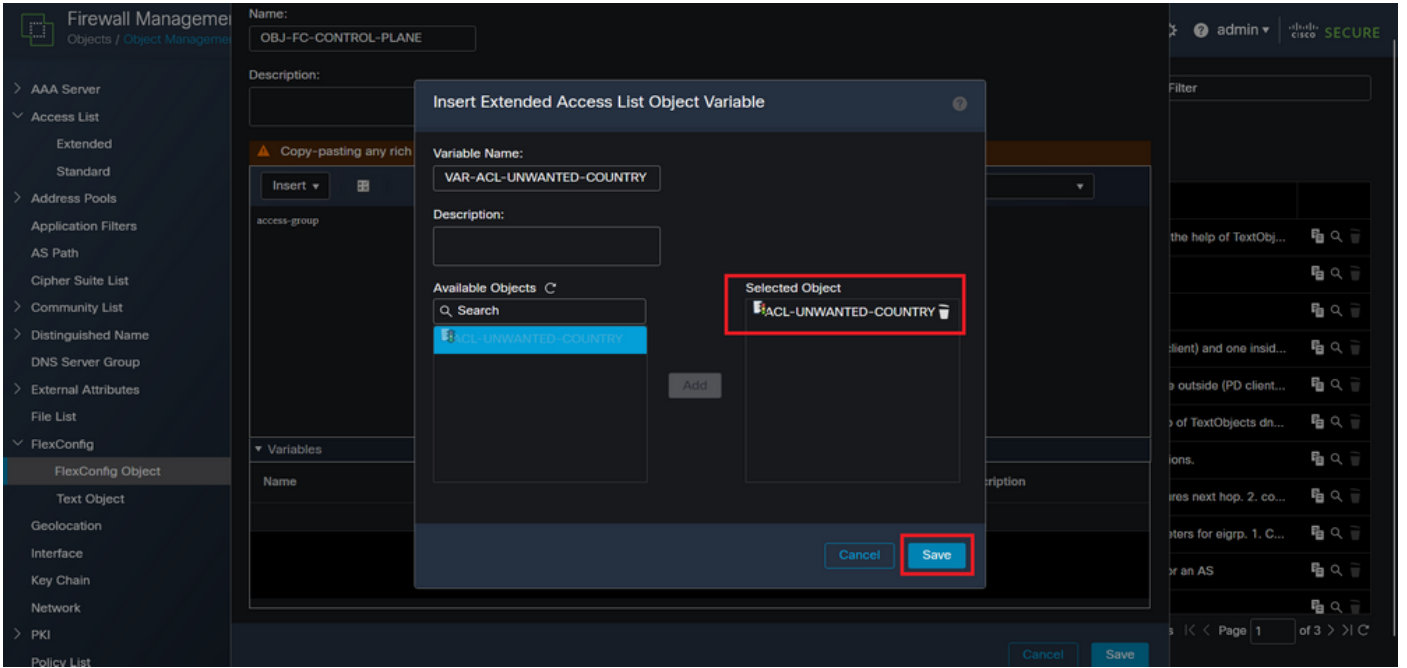
Flexconfig نئىك ةفاضلا 11. ةروصولا

ف م كحتلا ةمئاق جهن نئىك چارداب مق مث FlexConfig نئىك ل مسا ةفاضاب مق 3.2 ةوطخلال ةعسوملا لوصولال ف م كحتلا ةمئاق نئىك > جهن نئىك چارداب > چارداب ددح، اذهل (ACL) لوصولال



FlexConfig نئىك ريغتم 12. ةروصولال

ةمئاق ددح مث (ACL) لوصولال م كحتلا ةمئاق نئىك ريغتم ل مسا ةفاضاب مق 3.3 ةوطخلال رزلا قوف رقنلا، كلذ دعب، 2.3 ةوطخلال ف اهؤاشن م ت لوصولال (ACL) لوصولال م كحتلا لوظفح



FlexConfig نئال (ACL) لوصولي في مكحتال ةمئاق ةلإح. 13 ةروصل

ةهجاولل ةدراوك مكحتال يوتسم إلى لوصولي في مكحتال ةمئاق نيوكتب مق، م. 3.4 ةوطخلال
يللي امك ةيجراخلال

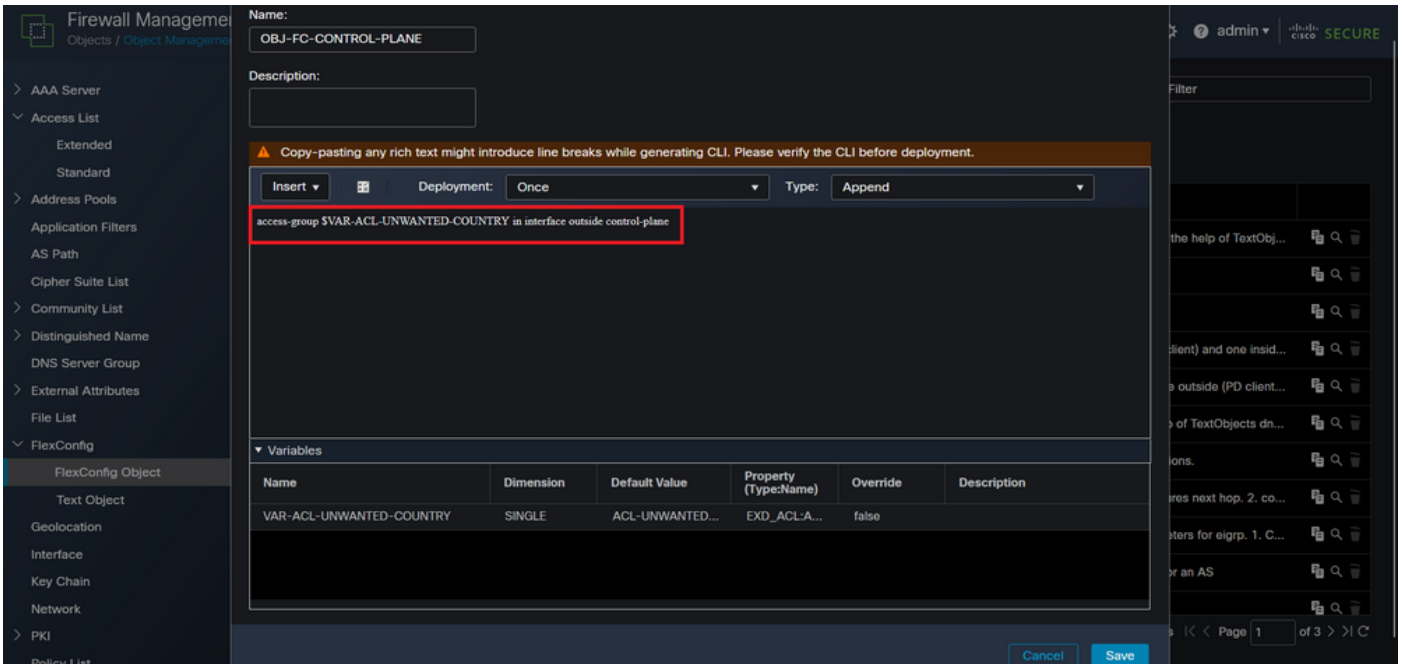
رمأوالا رطس ةغايص:

access-group "variable name starting with \$ symbol" in interface "interface-name" control-plane

(ACL) لوصولي في مكحتال ةمئاق ريغت ممدختسي يذلا، يلاتال رمأال لاثم إلى اذه مجرتي
يللي امك 'var-ACL-UNWANTED-Country' ةال ع 2.3 ةوطخلال في هؤاشن م يذلا:

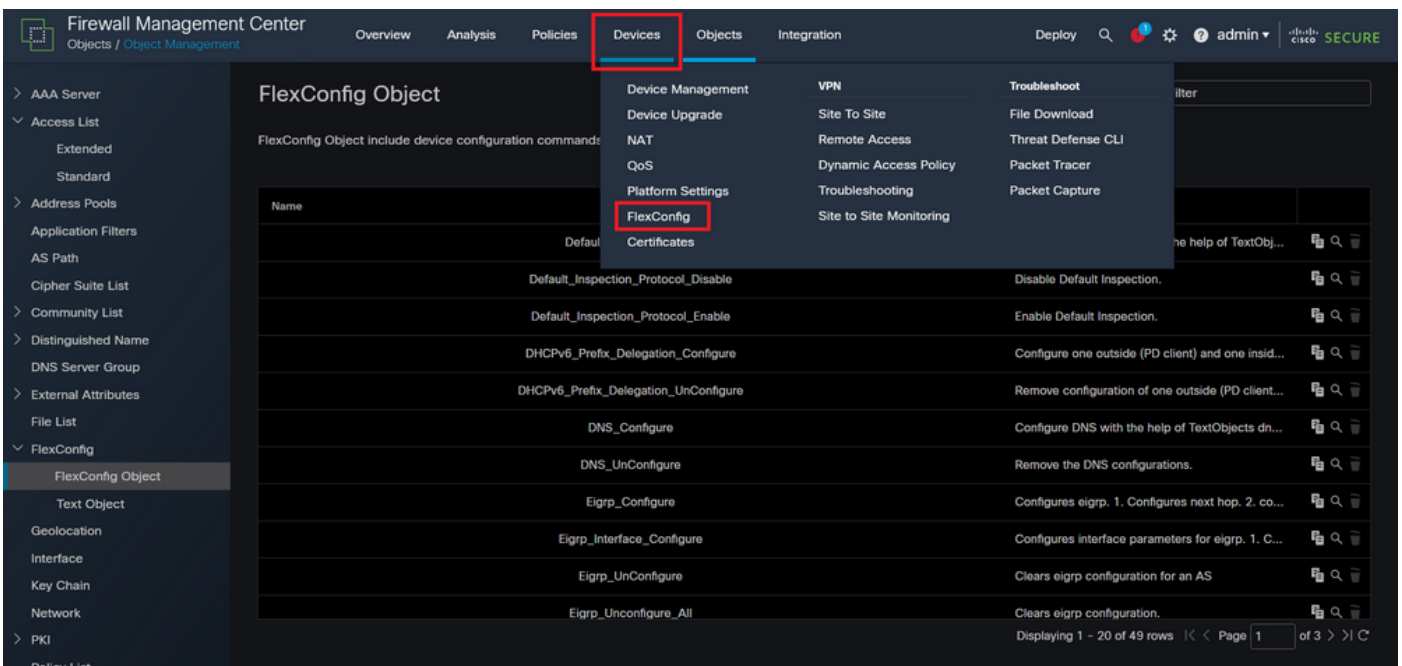
access-group \$VAR-ACL-UNWANTED-COUNTRY in interface outside control-plane

"ظفح" رزلا دح، كلذ دعب، FlexConfig نئال ةذفان في اهب اهنيوكتب بچي يتيلا ةقيرطال يه هذه
FlexConfig نئال لامك إلى



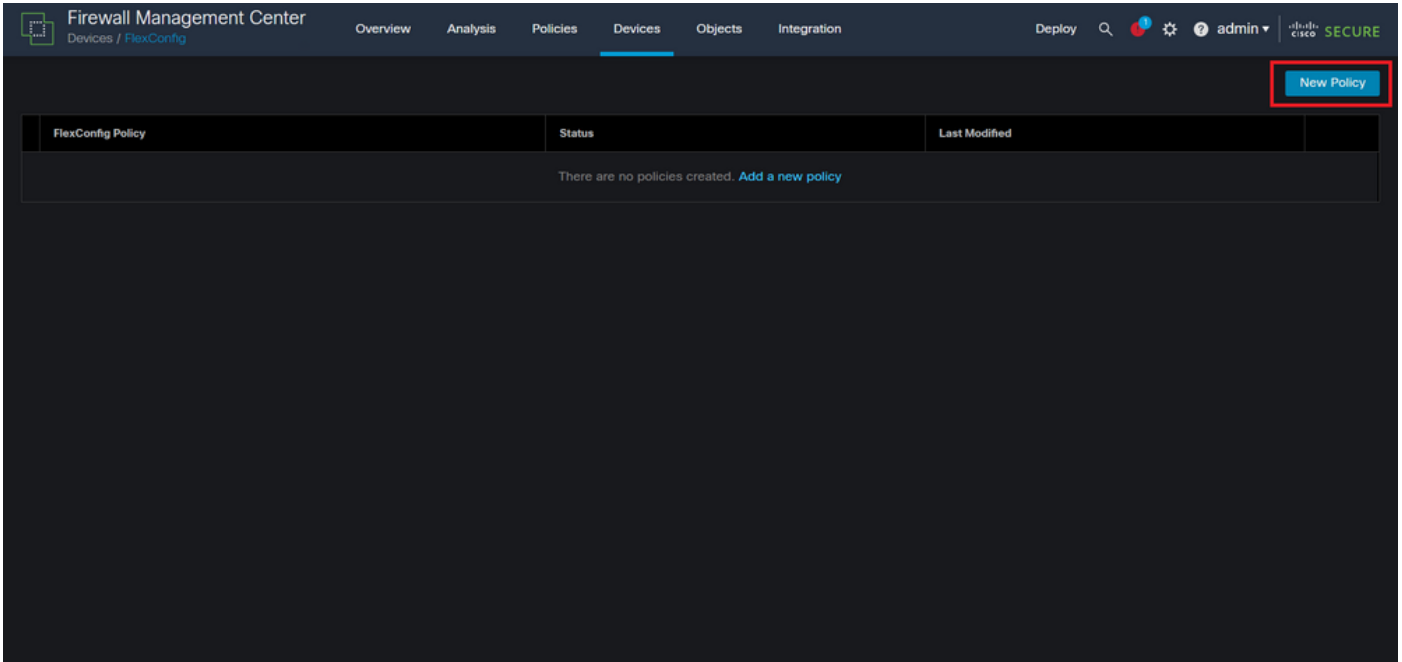
Flexconfig نئىكل لمكلا رماوالا رطس. 14. ةروصل

> ةزهجالا لىل لوقت نا ، اذهلو ، FTD لىل FlexConfig نئىك نىوكت قىب طت لىل جاتحت 4. ةوطخل FlexConfig.



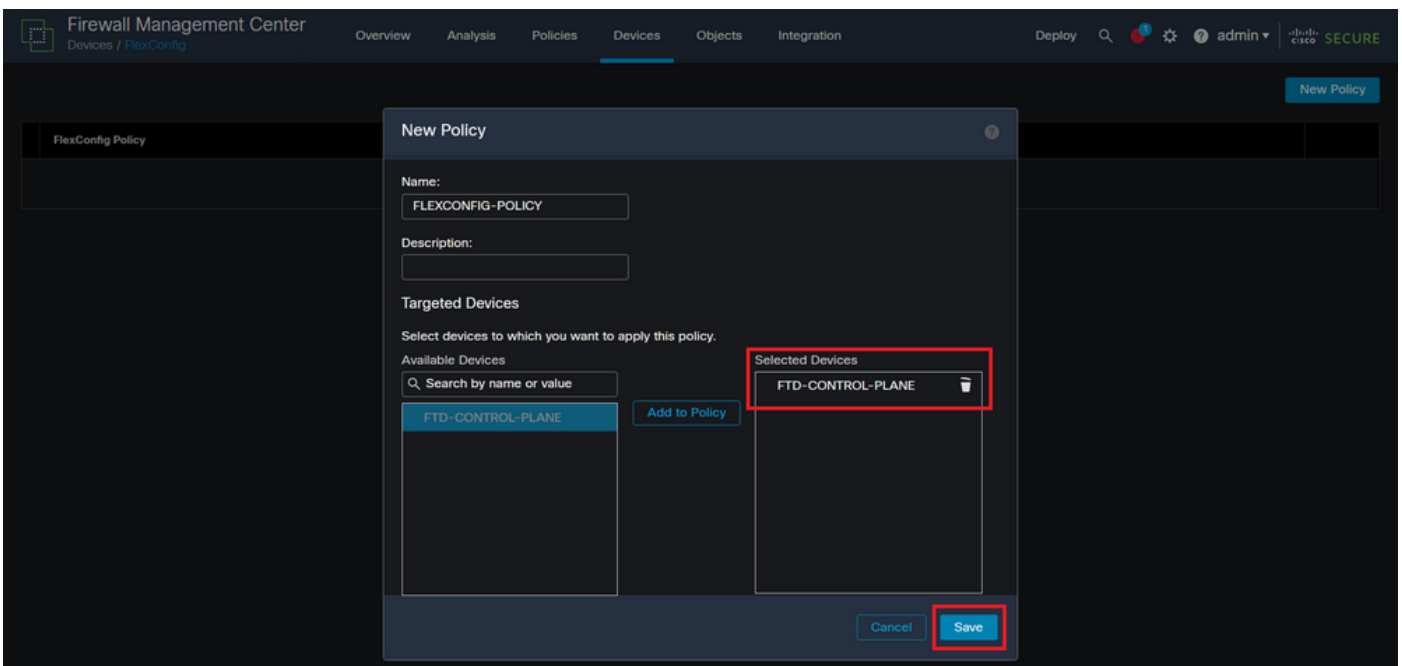
FlexConfig ةسايس ةمئاق. 15. ةروصل

كب صاخلا FTD ل هؤاشن مت FlexConfig كانه نكي مل اذا "ديج جهن" قوف رقنا م. 4.1. ةوطخل ، دوجوملا FlexConfig جهن ريرحتب مق وأ.



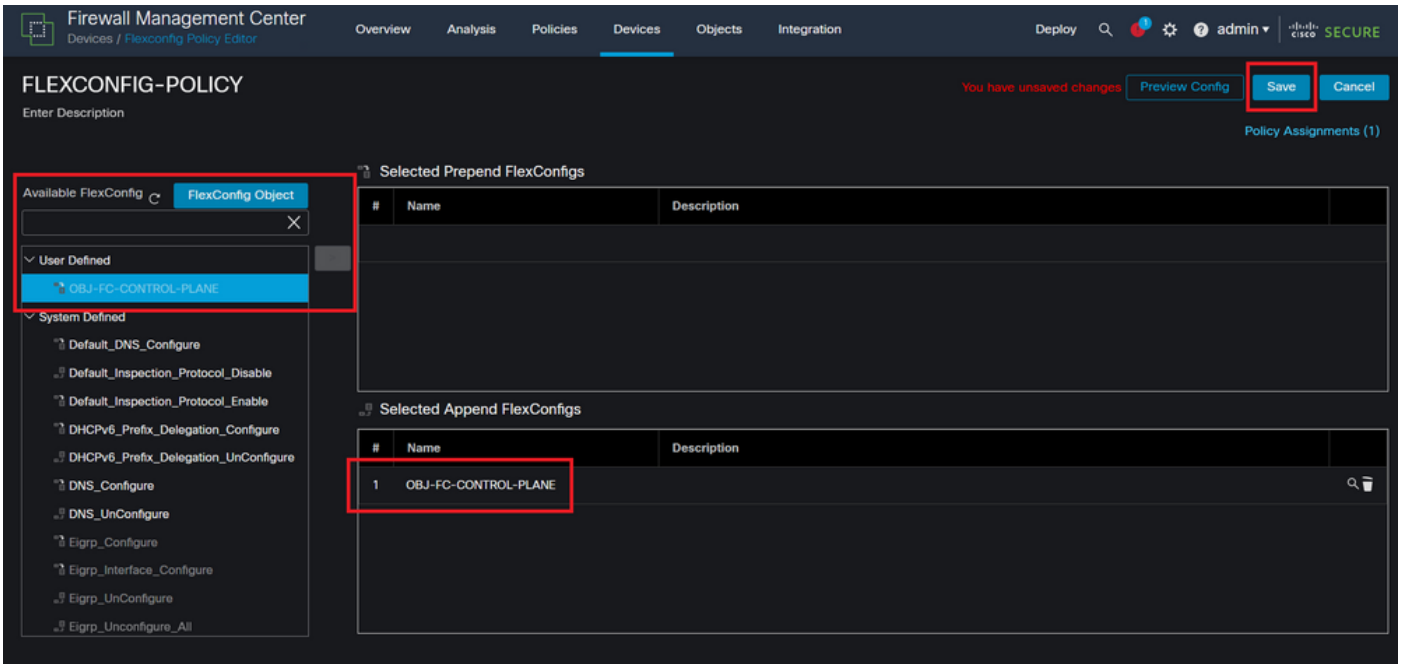
FlexConfig ةسايس ءاشنإ 16. ةروصلإ

ةمئاق قيبطت ديرت يذلا FTD ددحو ديدجلإ FlexConfig جهنل مساة فاضاب مق 4.2 ةوطخلإ
مكحتلإ يوتسمل اهؤاشنإ مت يتلإ (ACL) لوصولإ يف مكحتلإ



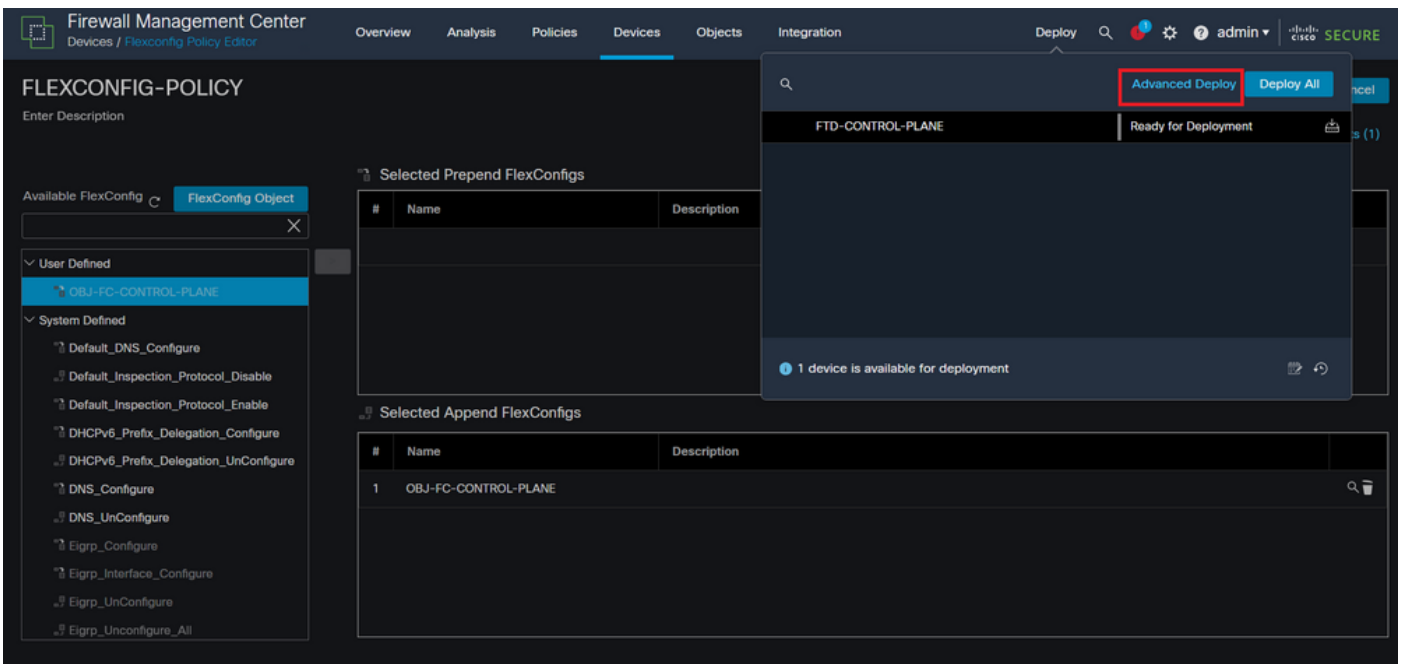
FlexConfig ةسايس زاھج نييعت 17. ةروصلإ

3.2 ةوطخلإ يف هؤاشنإ مت يذلا FlexConfig نئاك نع شحبا، یرسيلإ ةحوللإ نم 4.3 ةوطخلإ
فصتنم يف دوجوملإ نميالإ مهسللا قوف رقنلاب FlexConfig جهنلإ هتفاضاب مق م، هالعأ
ظفح رزللا قوف رقنا، كلذ دعب، ةذفانلإ



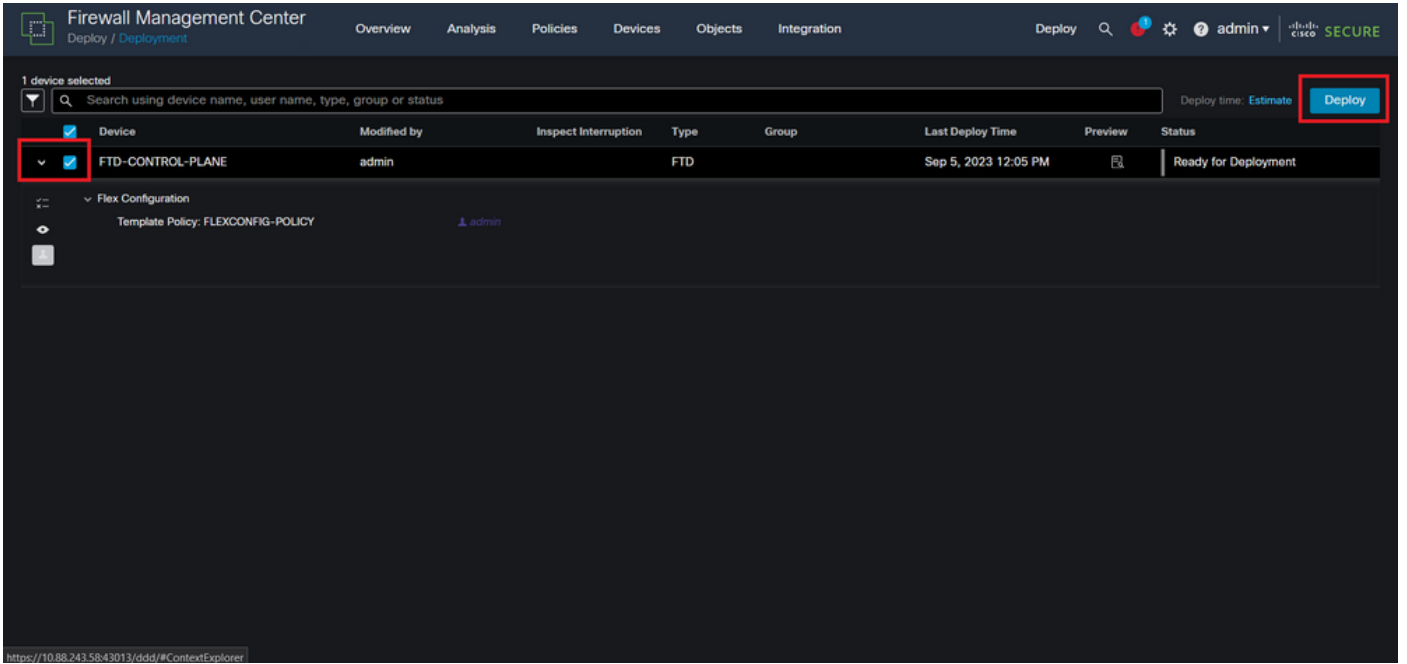
18. FlexConfig ةسايس نئاك نيغت ةروصل

رشن" > "رشن" ىل لقتنا ،كذل ،FTD في نيوكتلا ريغت رشنل ةعبات ملاب مق 5 ةوطخلال "مدمتق م".



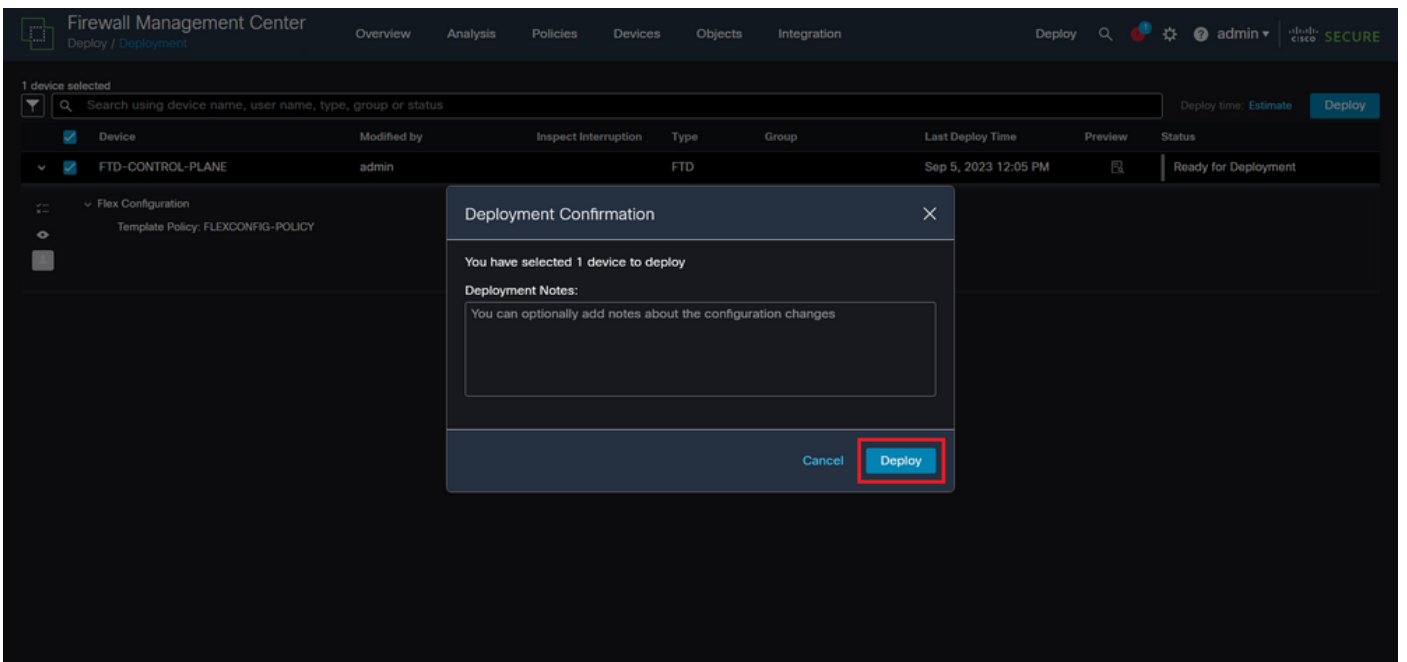
19. FTD جم انرب في مدمتق م رشنلا ةروصل

،اىحص عيش لك ناك اذا .هيلي مع FlexConfig جهن قي ببط ديتر يذلا FTD ددح م 5.1 ةوطخلال "رشن" قوف رقناف .



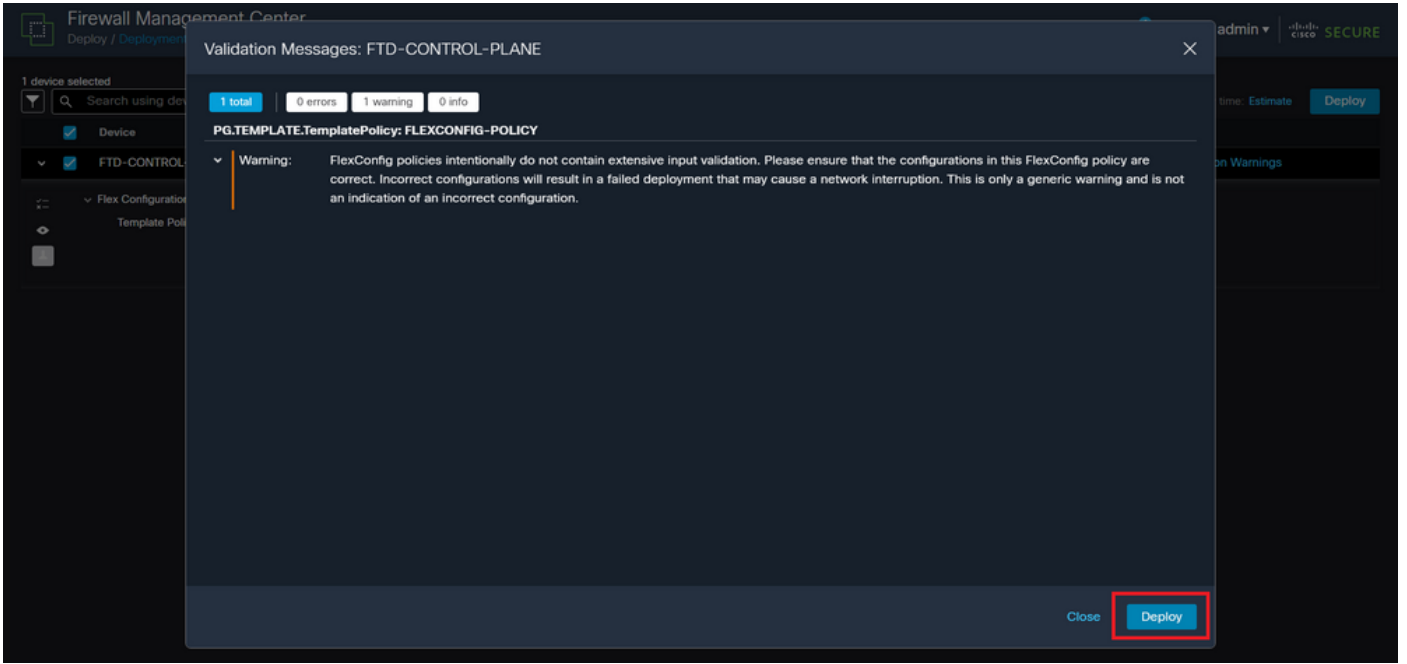
FTD رشن ةحص نم ققحتلا 20 ةروصل

ةعباتم و رشنلا بقعتل اقلعت فضا م ث ، "رشنلا ديكات" راطا رهظيس ، كلذ دع 5.2 ةوطخل رشنلا.



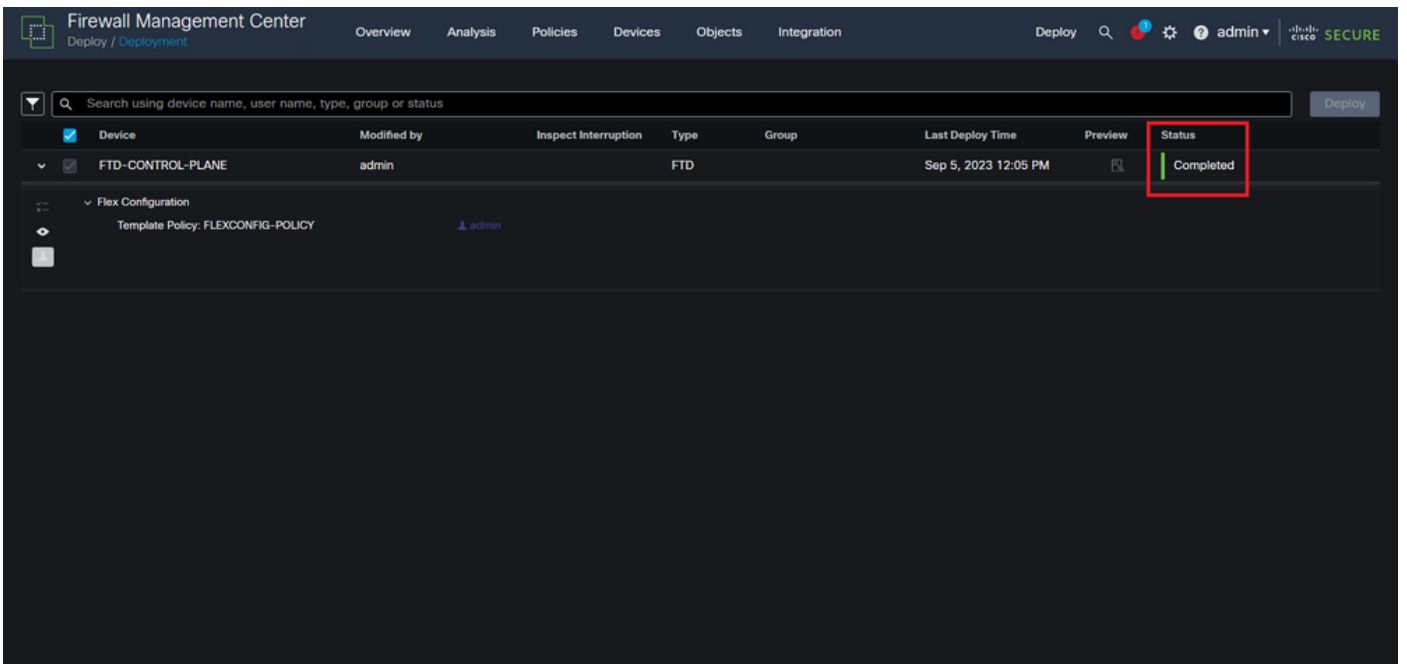
(FTD) ةرسللا قئاف لاسرالا جم انرب رشن تاقيلعت 21 ةروصل

اذا طقف "رشن" قوف رونا FlexConfig تاريغت رشن دنع ريذحت ةلاسر رهظت دق 5.3 ةوطخل جهنلا نيوكت ةحص نم امامت ادكاتم تنك.



FTD رشن ب صاخال FlexConfig ريذحت. 22 ةروصل

FTD ل جهنلا رشن حاجن نم دكأت. 5.4 ةوطخال



FTD جامانرب رشن حجج. 23 ةروصل

تمق اذإ وأ ك ب صاخال FTD ل ةديج (ACL) لوصولا يف مكحت ةمئاق عاشناب تمق اذإ. 6 ةوطخال تاريغت نأ زاربإ مهمل نمف ،طشن لكش ب مادختسالال ديقي ةدوجوم مكحت ةمئاق ريرحتب FTD، ب لعفلاب اهؤاشنإ مت يتللا تالاصتالال لعل قبطنت ال اهؤارج مت يتللا نيوكتلال مق ،كلذ لعل لوصولل .ايودي FTD ل ةطشنللا لاصتالال تالواحم حسم لىل جاتحت ،يللاتلابو .يللي امك ةطشنللا تالاصتالال حسمو FTD ب ةصاخال (CLI) رماوالا رطس ةهجاوب لاصتالال

نعم فيضم ل IP ناوعل طشنللا لاصتالال حسم ل:


```
> clear conn address 192.168.1.10 all
```

اهل مكأب ةي عرف ةكبشل ةطشنل تالاصتال احسمل:

```
> clear conn address 192.168.1.0 netmask 255.255.255.0 all
```

IP نيوانع نم قاطنل ةطشنل تالاصتال احسمل:

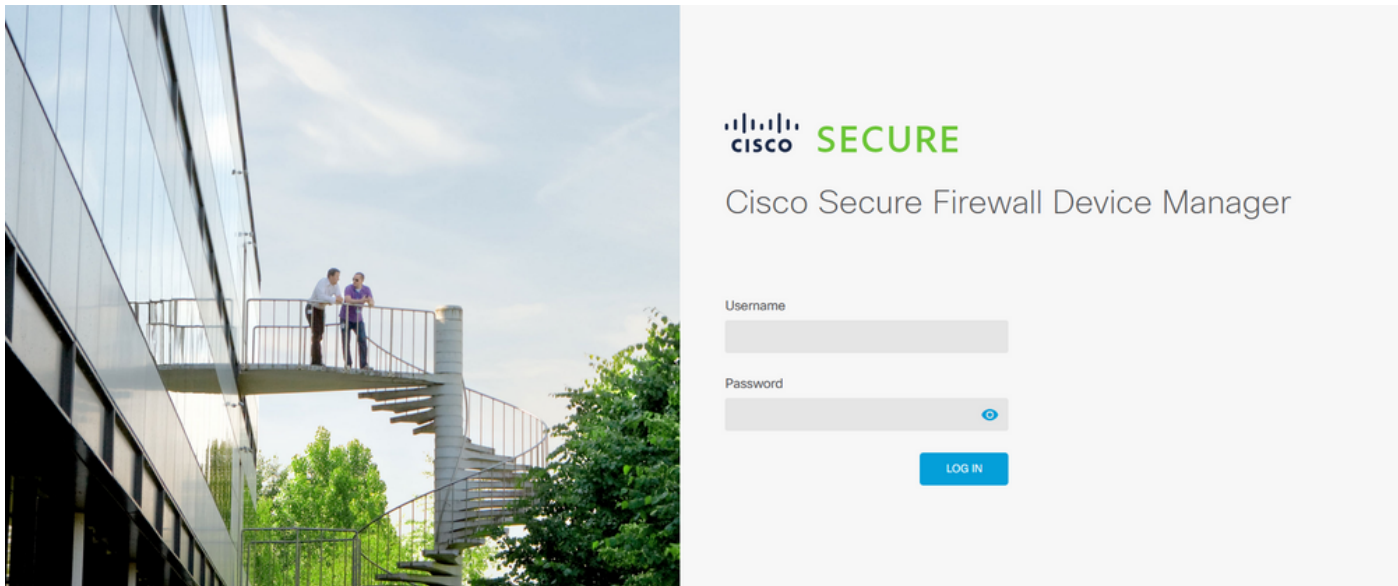
```
> clear conn address 192.168.1.1-192.168.1.10 all
```

 يوتحمل ناو نع رمأ ةياهن في "all" ةيساسأل ةم لكلا مادختسا ةدشب ي صوي: ةظالم راج يلى ةطشنل VPN ةكبشل ةمشاغل ةوقل لاصتال واحم ةلازا ضرفل حضاولا قاطب ةمشاغل VPN ةوق موجه ةعيبط موقت ام دنع يسيئر لكشب، نم آل ةي امحل ةتباثل لاصتال واحمل راجفنا.

FDM ةطساوب ةرادم ال FTD ل مكحتل يوتسم يلى لوصولا في مكحتل ةمئاق نيوكت

ةمئاق نيوكتل (FDM) لوحمل تانايب ةدعاق ةرادا في هتعباتم يلى جاتحت يذلا ءارجإل وه اذه VPN ةكبشل ةفينعل ةوقل تامجه رطل مكحتل يوتسم يلى (ACL) لوصولا في مكحتل ةي جراخل FTD ةهجاو يلى ةدراول:

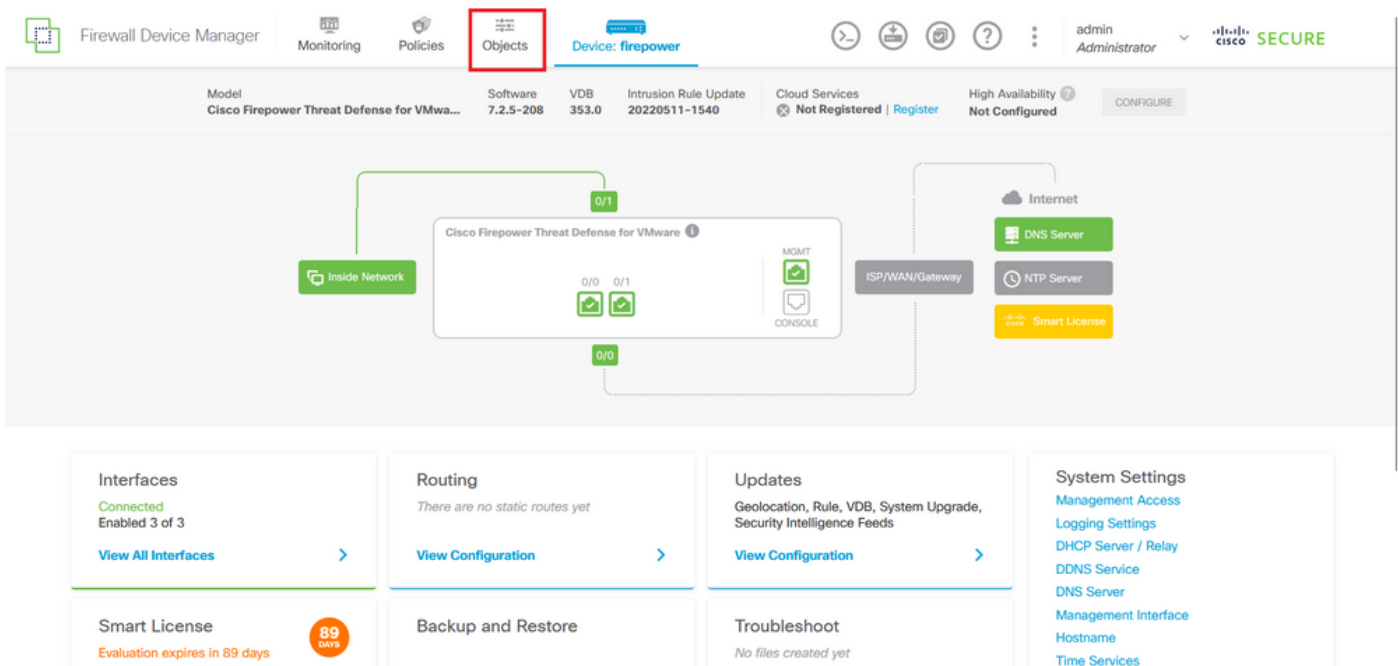
ل وخذل ل جسو و HTTPS ربع FDM ب ةصاخلا (GUI) ةي موسرلا مدختسملا ةهجاوحت فا 1. ةوطخل ك ب ةصاخلا دامتعال تانايب مادختساب



© 2015-2023 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc. This product contains some software licensed under the "GNU Lesser General Public License, versions: 2, 2.1 and 3" provided with ABSOLUTELY NO WARRANTY under the terms of "GNU Lesser General Public License, version 2 version 2.1 and version 3".

FDM إى لى لودل لى لى جى سى ت ة ح ف ص . 24 ة ر و ص ل ل

ت ا ن ئ ا ك ل ل إ ل ل ل ق ت ن ا ، ا ذ ه ل . ن ئ ا ك ة ك ب ش ء ا ش ن ل إ ل ل ج ا ت ح ت . 2 ة و ط خ ل ل



FDM ل ة س ي س ل ل ا ت ا م و ل ع م ل ا ة ح و ل . 25 ة ر و ص ل ل

د ي د ج ة ك ب ش ن ئ ا ك ء ا ش ن ل '+' ر ز ل ل ع ر ق ن ا م ت ت ا ك ب ش د ح ، ل ر س ل ل ة ح و ل ل ل ن م . 2.1 ة و ط خ ل ل

Object Types

Networks

Ports

Security Zones

Application Filters

URLs

Geolocations

Syslog Servers

IKE Policies

IPSec Proposals

Secure Client Profiles

Identity Sources

Users

Certificates

Secret Keys

Monitoring

Policies

Objects

Device: firepower

admin Administrator

SECURE

Network Objects and Groups

6 objects

Filter

Preset filters: System defined, User defined

#	NAME	TYPE	VALUE	ACTIONS
1	IPv4-Private-10.0.0.0-8	NETWORK	10.0.0.0/8	
2	IPv4-Private-172.16.0.0-12	NETWORK	172.16.0.0/12	
3	IPv4-Private-192.168.0.0-16	NETWORK	192.168.0.0/16	
4	any-ipv4	NETWORK	0.0.0.0/0	
5	any-ipv6	NETWORK	::/0	
6	IPv4-Private-All-RFC1918	Group	IPv4-Private-10.0.0.0-8, IPv4-Private-172.16.0.0-12, IPv4-Private-192.168.0.0-16	

نئالكلا ءاشن | 26 ةروصل

ةافاضاب مقو، نئالكلا ةكبشلا عون ددحو، ةكبشلا نئالكلا مسا ةافاضاب مق 2.2 ةوطخلل
 لى اهضفر مزلي يتلا رورملا ةكرح ةقباطم ل IP نىوانع قاطن و ةكبشلا ناووع و IP ناووع
 نئالكلا ةكبش لامكلا قفاوم رزلا قوف رقنا م. FTD.

ةمشاغللا ةوقلا تامجه رطح لى اهنيوكت مت يتلا نئالكلا ةكبش فدهت، لاثملا اذه يف -
 ةيعرفلا ةكبشلا نم ةدراوللا VPN ةكبشلا 192.168.1.0/24.

Firewall Device Manager

Monitoring

Policies

Objects

Device: firepower

admin Administrator

SECURE

Object Types

Networks

Ports

Security Zones

Application Filters

URLs

Geolocations

Syslog Servers

IKE Policies

IPSec Proposals

Secure Client Profiles

Identity Sources

Users

Certificates

Secret Keys

Network Objects and Groups

6 objects

Filter

Preset filters: System defined, User defined

Actions

Add Network Object

Name

OBJ-NET-UNWANTED-COUNTRY

Description

Type

Network Host FQDN Range

Network

192.168.1.0/24

e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL

OK

ةكبش نئالكلا ةافاضا | 27 ةروصل

ضرغلا اذهل، ةعسوم (ACL) لوصللا يف مكحت ةمئاق ءاشن لى جاتحت، كلذ دعب 3 ةوطخلل
 ايلعللا ةمئاقلا يف "ءادا" بيوبتلا ةمالع لى لقتنا.

Firewall Device Manager | Monitoring | Policies | **Objects** | Device: firepower | admin Administrator | cisco SECURE

Object Types

- Networks
- Ports
- Security Zones
- Application Filters
- URLs
- Geolocations
- Syslog Servers
- IKE Policies
- IPSec Proposals
- Secure Client Profiles
- Identity Sources
- Users
- Certificates
- Secret Keys

Network Objects and Groups

7 objects

Filter

Preset filters: System defined, User defined

#	NAME	TYPE	VALUE	ACTIONS
1	IPv4-Private-All-RFC1918	Group	IPv4-Private-10.0.0.0-8, IPv4-Private-172.16.0.0-12, IPv4-Private-192.168.0.0-16	
2	IPv4-Private-10.0.0.0-8	NETWORK	10.0.0.0/8	
3	IPv4-Private-172.16.0.0-12	NETWORK	172.16.0.0/12	
4	IPv4-Private-192.168.0.0-16	NETWORK	192.168.0.0/16	
5	any-ipv4	NETWORK	0.0.0.0/0	
6	any-ipv6	NETWORK	::/0	
7	OBJ-NET-UNWANTED-COUNTRY	NETWORK	192.168.1.0/24	

زاهجلا تادادع | ةحفص 28 ةروصل

يلي امك مدقتملا نيوكتلا عبرم نم نيوكتلا ضرع ددحو لفسأل ريرمتلاب مق 3.1 ةوطخل

Firewall Device Manager | Monitoring | Policies | Objects | **Device: firepower** | admin Administrator | cisco SECURE

0/0

Interfaces

Connected
Enabled 3 of 3

[View All Interfaces](#)

Routing

There are no static routes yet

[View Configuration](#)

Updates

Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds

[View Configuration](#)

System Settings

[Management Access](#)
[Logging Settings](#)
[DHCP Server / Relay](#)
[DDNS Service](#)
[DNS Server](#)
[Management Interface](#)
[Hostname](#)
[Time Services](#)

[See more](#)

Smart License

Evaluation expires in 89 days

Tier: Not selected (Threat Defense Virtual - Variable)

[View Configuration](#)

Backup and Restore

[View Configuration](#)

Troubleshoot

No files created yet

REQUEST FILE TO BE CREATED

Site-to-Site VPN

There are no connections yet

[View Configuration](#)

Remote Access VPN

Requires RA VPN license
No connections | 1 Group Policy

[Configure](#)

Advanced Configuration

Includes: FlexConfig, Smart CLI

[View Configuration](#)

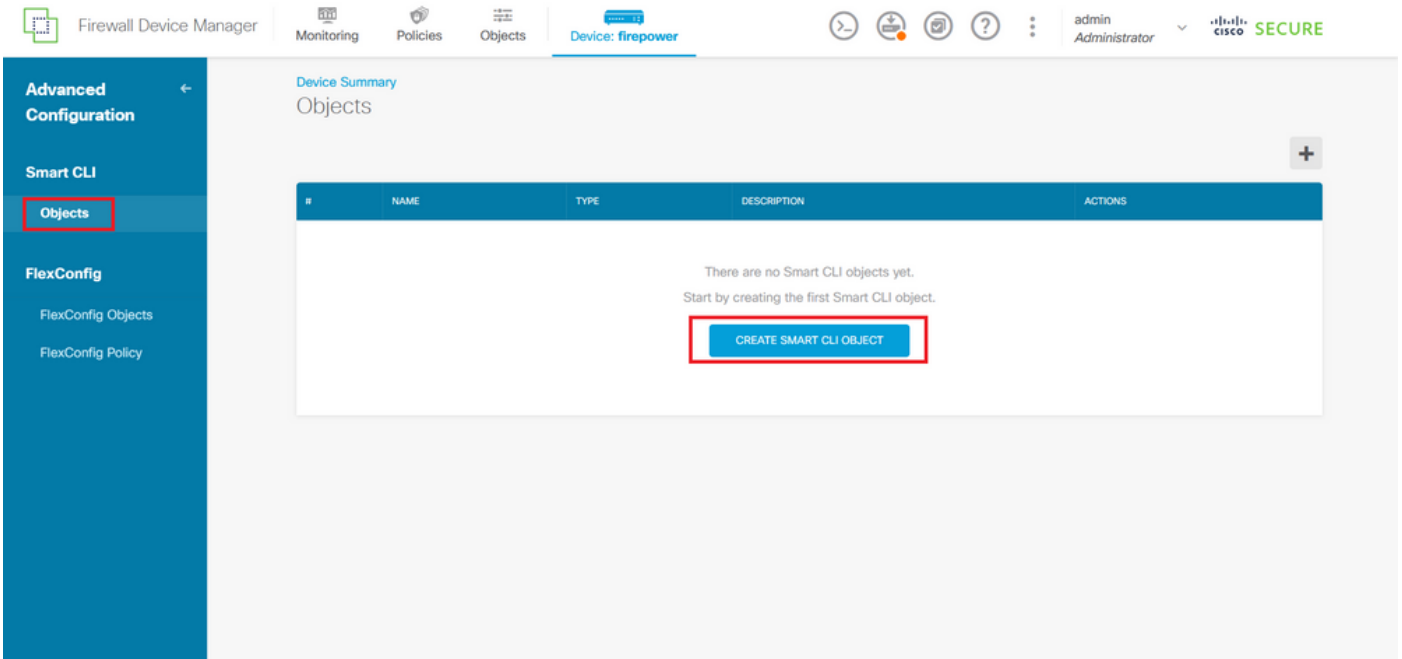
Device Administration

[Audit Events, Deployment History, Download Configuration](#)

[View Configuration](#)

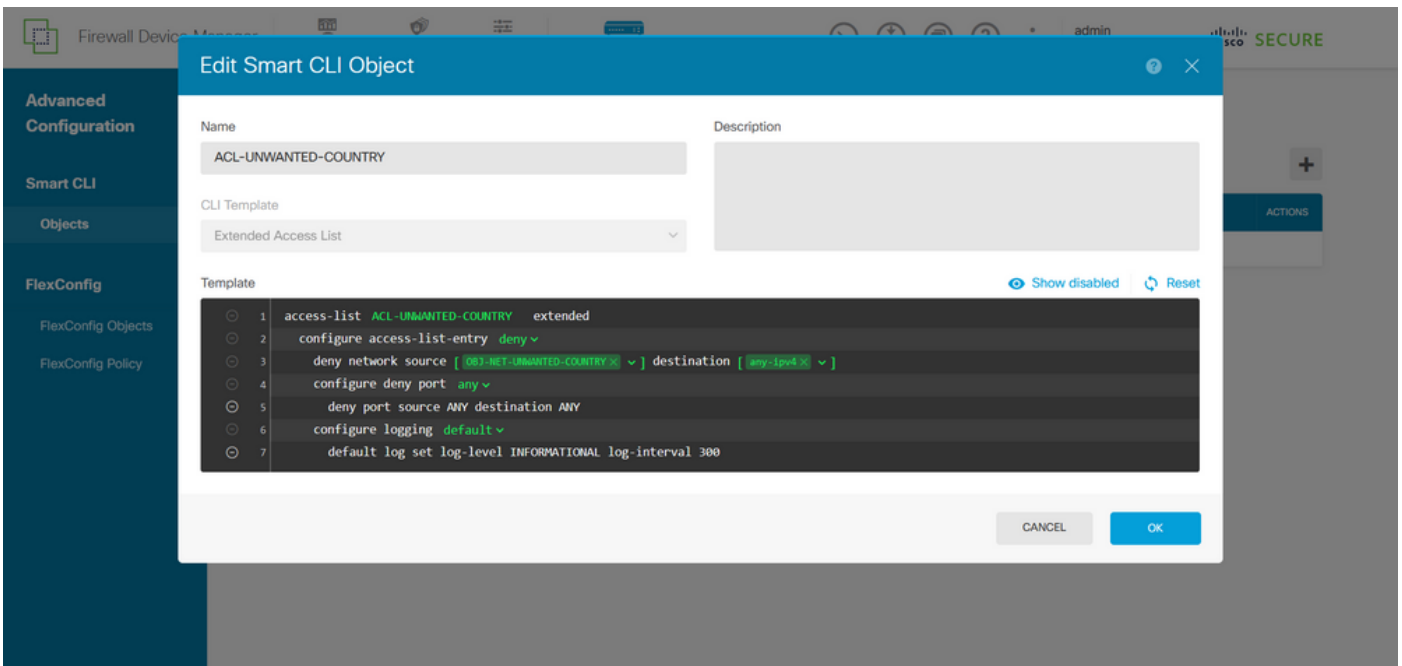
FDM مدقتملا نيوكتلا 29 ةروصل

CLI نئاك عاشن | رقن او تانئاك > كذا CLI ىل ءحفصت ، ىرسىلا ءحوللل نم ، م 3.2 ةوطخل
كذا



ةيكدلأ (CLI) رمأوألأ رطس ةهأو تانئاك 30. ةروصلأ

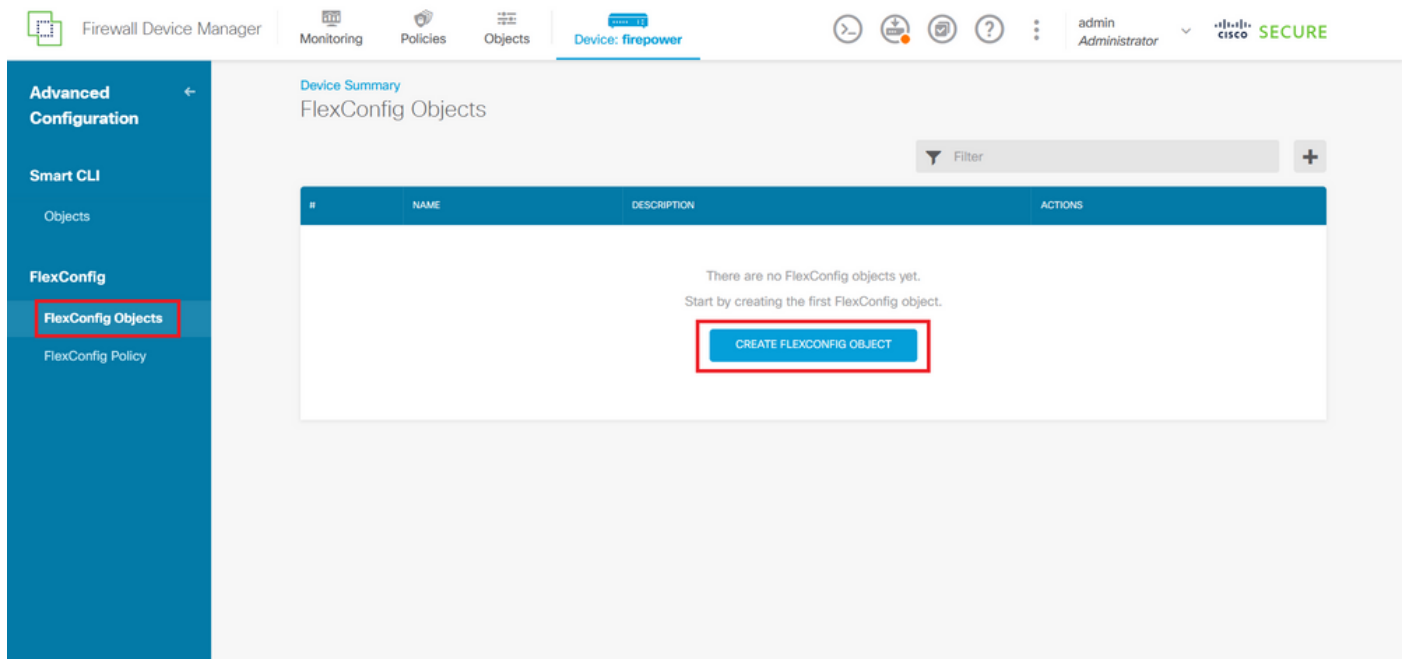
ةمئاق ءاشنإل ةعسوملأ (ACL) لوصولأ يف مكحتلأ ةمئاقل مسأ ةفاضاب مق 3.3 ةوطخلأ نيوكتب مق مئ، (CLI) رمأوألأ رطس ةهأو بلاقل ةلدسنملا ةمئاقلا نم ةعسوملا لوصولأ يف هؤاشنإ مئ ذلأ ةكبشلا نئاك مادختساب ةبولطملا (ACEs) لوصولأ يف مكحتلأ مئاق (ACL) لوصولأ يف مكحتلأ ةمئاق لامكإل قفاوم رزلأ قوف رقنأ مئ، ءالءأ 2.2 ةوطخلأ



ةعسوملأ (ACL) لوصولأ يف مكحتلأ ةمئاق ءاشنإ 31. ةروصلأ

✍ لوصولأب مكحتلأ ةمئاقل ACE تادحو نم ديزملا ةفاضإ إلأ ةءاحب تنك إذا: ةظءالم مئ، لءالءل ACE راسي قوف سواملا كي رءءل لءالءل نم كلذب مءاقلا كنكمي ف، (ACL) نم ديزملا ةفاضإل ةفءاضم دء مئ مهيلء رقنأ. رقنلل ةلباق طاقن ءالء رهظءس (ACE) لوصولأ يف مكحتلأ ءالءالءل.

ددحو یرسیلا ةحوللا ىلى لىقتنا ، اذهل ، FlexConfig نئىك ءاشنلىلى جاتحت ، كلذ دعب 4. ةوطخلال FlexConfig > Flexconfig نئىك ءاشنلىلى قوف رقن او ، FlexConfig تانىك



FlexConfig تانىك 32. ةروصلال

ىلى (ACL) لوصولال ىف مكحتللا ةمئىق ءاشنلىلى FlexConfig نئىك ل مسا ةفاضا ب مق 4.1. ةوطخلال ىلى امك ةجراخلال ةهجاو للى ةدراوك اهنىوكتو مكحتللا ىوتسم

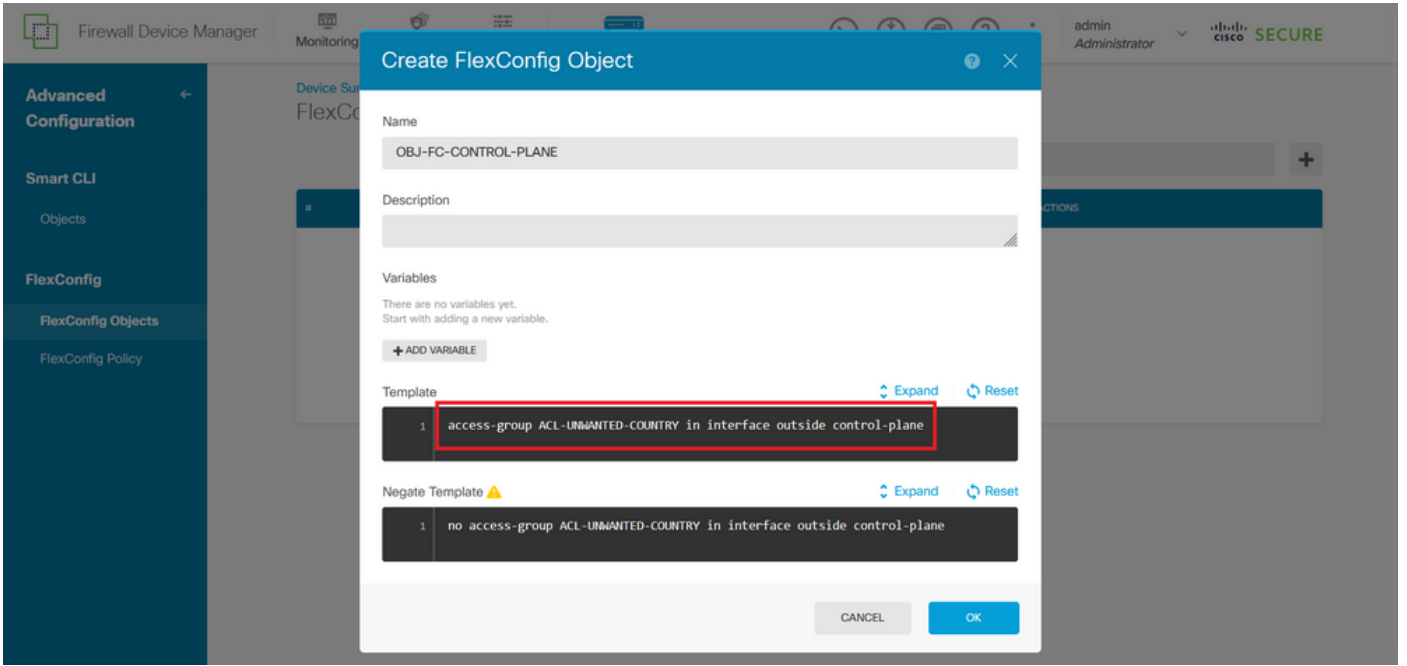
رم اوألا رطس ةغاىص:

```
access-group "ACL-name" in interface "interface-name" control-plane
```

ةعسوملا (ACL) لوصولال ىف مكحتللا ةمئىق مدختسى ىذلا ، ىلالتال رمالا لاثم ىلى اذه مچرتى ىلى امك 'ACL-UNWANTED-COUNTRY' هالعا 3.3 ةوطخلال ىف اوؤاشنلىلى مت ىتلا

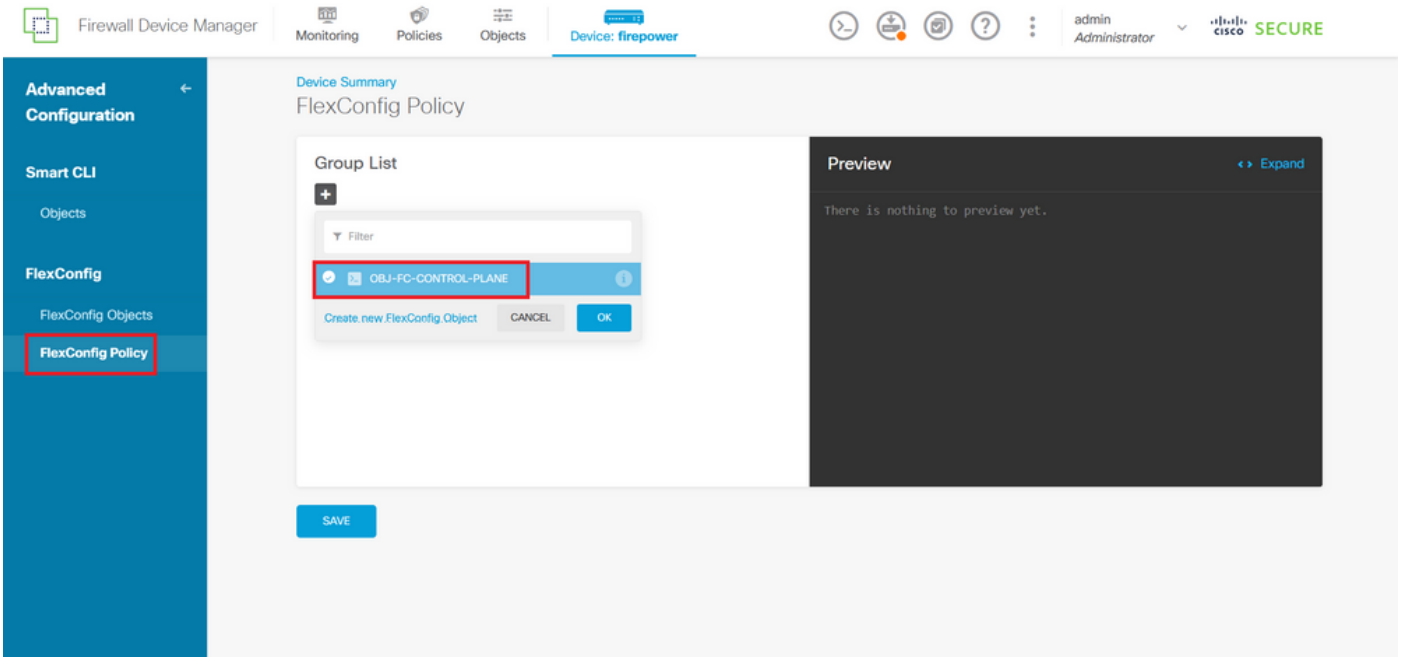
```
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

رزلا ددح ، كلذ دعب ، FlexConfig نئىك ةذفان ىف اهب اهنىوكت بچى ىتلا ةقىرطلال ىه هذو FlexConfig نئىك لامكلىلى "قف اوام"



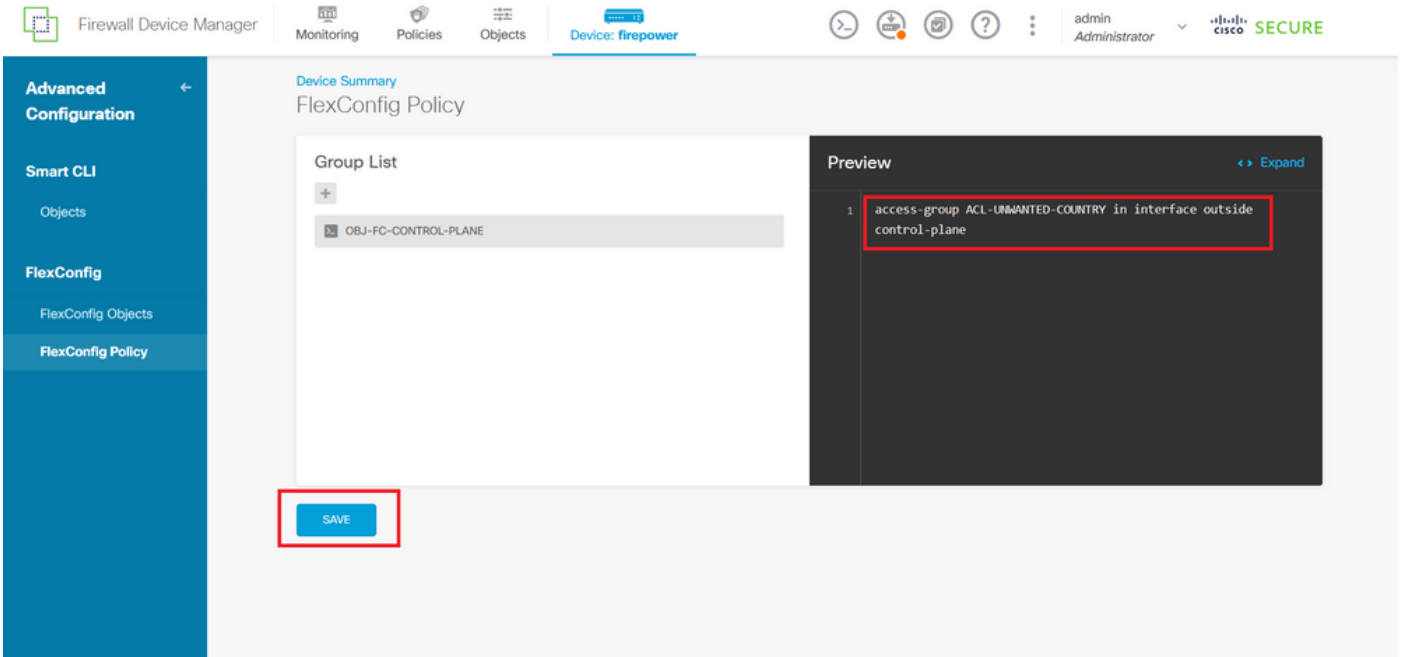
FlexConfig نئىك ءاشن | 33 ةروصل

FlexConfig > FlexConfig جەن ىل لىق تىنا، ضرغلا اذەل، FlexConfig جەن ىل لىق تىنا. 5 ةوطخال
 4.1 ةوطخال ي ف هؤاشن م ت يذال FlexConfig نئىك ددحو، '+' رزلا قوف رقن او.



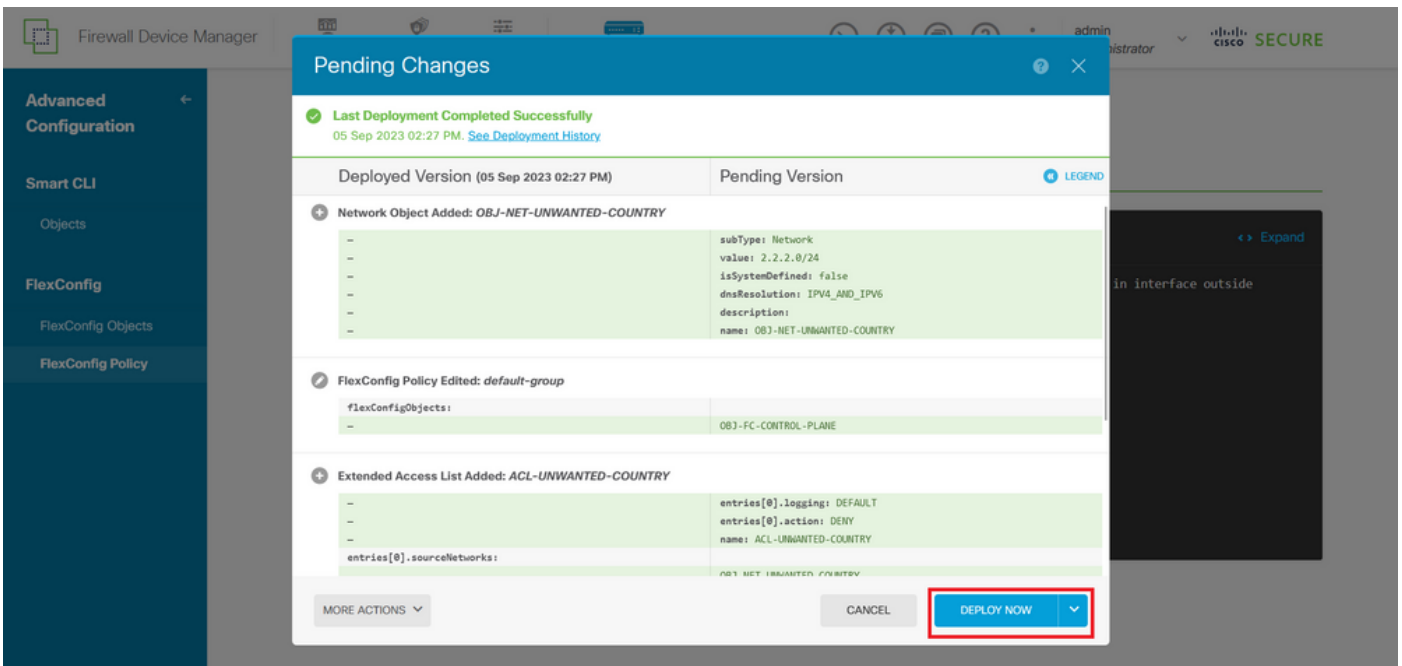
FlexConfig ةسايس | 34 ةروصل

ي ف مكحتال ةمئاق ل حيحصال نيوكتال ضرعت FlexConfig ةنياع م نأ م ققحت. 5.1 ةوطخال
 ظفحل رز ىل ع رقن او هؤاشن م ت يذال (ACL) لوصول.



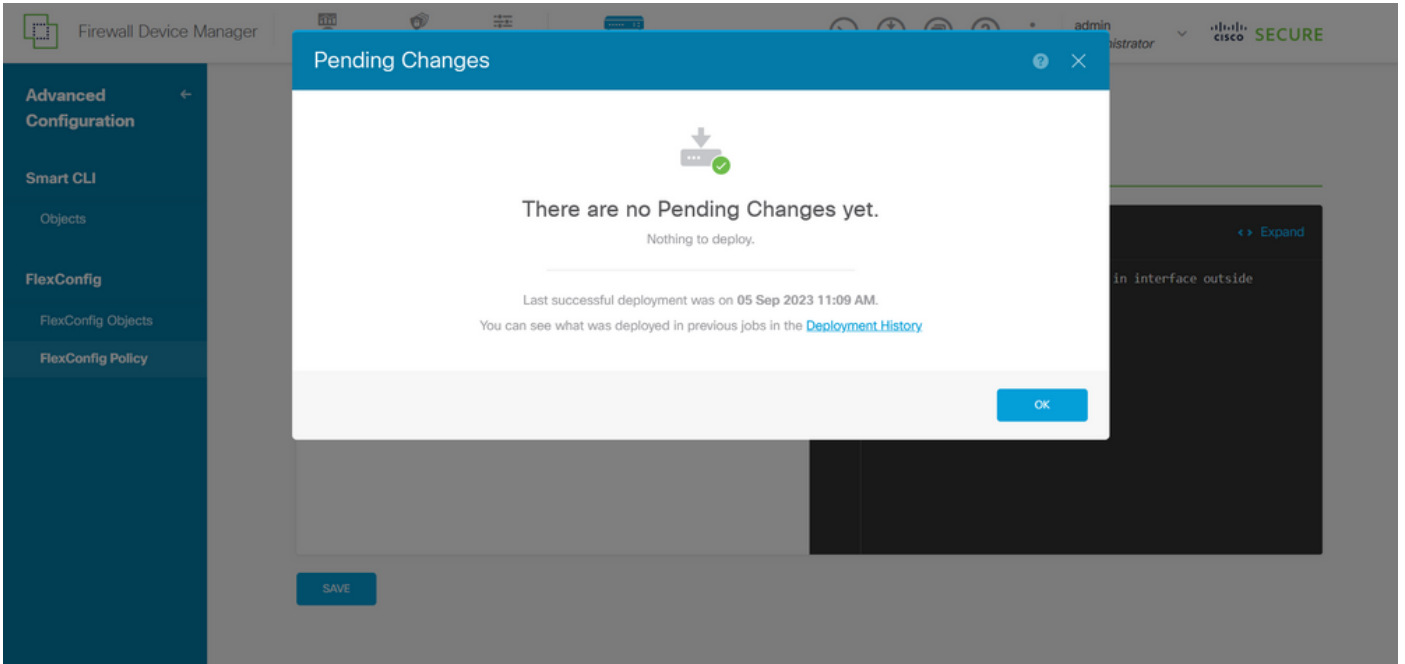
FlexConfig ةسايس ةنياعم 35. ةروصل

ةوقلا تامجه دض هتياح ديرت يذلا FTD لىل نيوكتلا تاريغي رشن ب مق 6. ةوطخلا نم ققحتو، ايلعلا ةمئاقلا يف رشنلا رز قوف رقنا، بسبب اذهل و، VPN ةكبشلة شحولوا "نال رشن" قوف رقنا م، اه رشن متيس يتلا نيوكتلا تاريغي ةحص



قلعلا رشنلا 36. ةروصل

جهنلا رشن حاجن نم ققحت 6.1. ةوطخلا



حاجت رشنال مت 37. ةروصلال

تمق اذوا كبا صاخلا FTD ل ةديج (ACL) لوصولال يف مكحت ةمئاق عاشناب تمق اذوا 7. ةوطخلال تاريغت نا زاربإ مهمال نمف، طشن لكشب مادختسالال ديقت ةدوجوم مكحت ةمئاق ريرحتب FTD، ب لعفلاب اهؤاشنإ مت يتللالاصتالال لعل قبطنت ال اهؤارجإ مت يتللالنيوكتلال مق، كلذ لعل لوصولل. ايودي FTD ل ةطشنلال لاصتالال الواحم حسم لال جاتحت، يلاتلابو يلي امك ةطشنلال لاصتالال حسمو FTD ب صاخلا (CLI) رماوالا رطس ةهجاوب لاصتالاب

ننيم فيضم ل IP ناو نعل طشنلال لاصتالال حسم ل:

```
> clear conn address 192.168.1.10 a11
```

اهل مكأب ةيعرف ةكبشل ةطشنلال لاصتالال حسم ل:

```
> clear conn address 192.168.1.0 netmask 255.255.255.0 a11
```

IP ننيوانع نم قاطنل ةطشنلال لاصتالال حسم ل:

```
> clear conn address 192.168.1.1-192.168.1.10 a11
```

يوتحمل ناو نعل رمأ ةياهن يف "all" ةيساسالال ةمكللال مادختسا ةدشب يصوي: ةطخال م رادج لال ةطشنلال VPN ةكبشل ةمشاغلا ةوقلا لاصتالال الواحم ةلازا ضرفل حضاو لال قاطناب ةمشاغلا VPN ةوق موجه ةعيبط موقت ام دنع يسيئر لكشب، نمالال ةيامحل



```
asa# clear conn address 192.168.1.10 all
```

اهل مكأب ةي عرف ةكبشل ةطشنل تالاصتال احسمل:

```
asa# clear conn address 192.168.1.0 netmask 255.255.255.0 all
```

IP نيوانع نم قاطنل ةطشنل تالاصتال احسمل:

```
asa# clear conn address 192.168.1.1-192.168.1.10 all
```

 يوتحمل ناو نع رمأ ةياهن في "all" ةي اساسأل ةم لكلا مادختسا ةدشب ي صوي: ةظحال م راجل ةطشنل VPN ةكبشل ةمشاغل ةوقل لاصتال واحم ةلازا ضرفل حضاو ل قالطاب ةمشاغل VPN ةوق موجه ةعيبط موقت ام دنع يسيئر لكشب ، نمأل ةي امحل ةتباثل لاصتال واحم ل راجفنا.

'shun' رمأل مادختساب نمأل ةي امحل راجل تامجهل رطل ل لي دب نيوكت

"بنجت" رمأل مادختسا كنكمي ، نمأل ةي امحل راجل تامجهل رطل يروف راخي دوجو ةلاح في مجاهم فيضم نم تالاصتال رطل رمأل اذه كل حيتي

IP ناو نع نم ةيلبقتسم ل تالاصتال عي مج طاقسا كلذ دعب متي ، IP ناو نع بنجت درجم - ايودي رطل ةفيظو ةلازا متت يتح اهل يجستو ردصم ل

دحمل فيضم ل ناو نع لاصتال ناك ءاوس رمأل اذهب ةصاخل رطل ةفيظو قيبت متي - ال ما ايلاح اطشن

طاقسا ب موقت تنأف ، لوكوتوربل او ةهجو ل او ردصم ل ذفانمو ةهجو ل ناو نع دي دجتب تمق اذ - IP نم ةيلبقتسم ل تالاصتال عي مج يلع ةراش عضو ل ةفاضل اب ةقباطم ل لاصتال ردصم ل

قباطت يتل كلت طقف سيلو ، ةيلبقتسم ل تالاصتال عي مج بنجت متي ، ناو نع ل هذه ةدحمل لاصتال تامل عم

ردصم ل ل IP ناو نع كل طقف OneConnectCommand يلع لوصحل كنكمي -

نيوكت في هضرع متي ال هنإف ، يكي مانيد لكشب تامجهل رطل هم ادختسا متي رمأل نأل - عافدل زاوجل ديدهتال

ةهجو ل كلتب ةلصتال تارايلخا عي مج ةلازا اضيأ متت ، ةهجو نيوكت ةلازا دنع -

بنج ت رم أة غاي ص -

```
shun source_ip [ dest_ip source_port dest_port [ protocol]] [ vlan vlan_id]
```

رم أا اذه نم no أة غاي ص ل م دخت س أ ، ام أة لاس ر ل ي طعت ل -

```
no shun source_ip [ vlan vlan_id]
```

لا ث م ل اذه ي ف . نم أا أة م ح ل ر ا د ج ل ي ل ا ت ل و ح ن ل ا ي ل ع ر م ت س ا م ث ، ف ي ص م IP ن ا و ن ع ب ن ج ت ل ، IP ن ا و ن ع ن م أة د ر ا و ل VPN أة ك ب ش ل أة م ش ا غ ل ا أة و ق ل ا ت ا م ج ه ر ط ح ل 'shun' رم أا م ا د خ ت س ا م ت ي 192.168.1.10 ر د ص م ل ا

FTD ل ن ي و ك ت ل ل ا ث م

رم أا ق ي ب ط ت ب م ق و (CLI) رم ا و ا ل ر ط س أة ه ج ا و ر ب ع FTD ل ل ا و خ د ل ا ل ي ج س ت ب م ق 1. أة و ط خ ل ا ي ل ا م ك ل ه ا ج ت ل ا

```
<#root>
```

```
>
```

```
shun 192.168.1.10
```

```
Shun 192.168.1.10 added in context: single_vf
```

```
Shun 192.168.1.10 successful
```

FTD ي ف أة م د خ ت س م ل ا ر ي غ IP ن ي و ا ن ع د ي ك أ ت ل أة ي ل ا ت ل ا ض ر ع ل ا ر م ا و ا م ا د خ ت س ا ك ن ك م ي 2. أة و ط خ ل ا IP ن ا و ن ع ل ك ل أة م د خ ت س م ل ا ر ي غ ل و ص و ل ا ت ا ر م د د ع ب ق ا ر م و

```
<#root>
```

```
>
```

```
show shun
```

```
shun (outside) 192.168.1.10 0.0.0.0 0 0 0
```

```
>
```

```
show shun statistics
```

```
diagnostic=OFF, cnt=0
```

```
outside=ON, cnt=0
```

```
Shun 192.168.1.10 cnt=0, time=(0:00:28)
```

ASA لنيوكتال لاثم

يولي امك ةنع للا رمأ قبطو CLI ربع ASA ىل لوخدلا ل جس 1. ةوطخلال

```
<#root>
```

```
asa#
```

```
shun 192.168.1.10
```

```
Shun 192.168.1.10 added in context: single_vf
```

```
Shun 192.168.1.10 successful
```

ASA ف ةمدختسم لا ريغ IP نيوانع ديكتل ةيلال ل ضرعلا رمأ اوام ادختس كنكمي 2. ةوطخلال
IP ناونع لكل ةمدختسم لا ريغ لوصول تارم ددع ةبقارمو

```
<#root>
```

```
asa#
```

```
show shun
```

```
shun (outside) 192.168.1.10 0.0.0.0 0 0 0
```

```
asa#
```

```
show shun statistics
```

```
outside=ON, cnt=0
```

```
inside=OFF, cnt=0
```

```
dmz=OFF, cnt=0
```

```
outside1=OFF, cnt=0
```

```
mgmt=OFF, cnt=0
```

```
Shun 192.168.1.10 cnt=0, time=(0:01:39)
```

 [عجم عجار](#)، "نمآل ةياملال رادج ب نجت" رمأل ل وحتامول عملال نم ديزم ىلع لوصحلل :ةظحالم
[Cisco نم نمآل ةياملال رادج ديدهت نع عافدلارمأ](#)

ةحصلال نم ققحتلال

بسانملا عضو لا يف مكحتلا وتسم إلى (ACL) لوصولا يف مكحتلا ةمئاق نيوكت ديكأتلا
يلتلا وحنلا لىل عةباتم لاب مق م ث ، نمألا ةيامحلا رادجلا

ليغشتب مقو (CLI) رماوأل رطس ةهجاو ربع نمألا ةيامحلا رادج لىل لوخدلا لجس 1. ةوطخل
وتسم إلى (ACL) لوصولا يف مكحتلا ةمئاق نيوكت قيبتت ديكأتلا ةيلتلا رماوأل
مكحتلا.

FMC: ةطساوب هترادإ متت FTD ل جارخإ لاثم

```
<#root>
```

```
>
```

```
show running-config access-list ACL-UNWANTED-COUNTRY
```

```
access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any
```

```
>
```

```
show running-config access-group
```

```
***OUTPUT OMITTED FOR BREVITY***
```

```
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

FDM: ةطساوب هترادإ متت يذلا FTD ل جارخإ لاثم

```
<#root>
```

```
> show running-config object id OBJ-NET-UNWANTED-COUNTRY
```

```
object network OBJ-NET-UNWANTED-COUNTRY
```

```
subnet 192.168.1.0 255.255.255.0
```

```
>
```

```
show running-config access-list ACL-UNWANTED-COUNTRY
```

```
access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any4 log default
```

```
> show running-config access-group
```

```
***OUTPUT OMITTED FOR BREVITY***
```

```
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

ASA: ل جارخإ لاثم

```
<#root>
```

```
asa#
```

```
show running-config access-list ACL-UNWANTED-COUNTRY
```

```
access-list ACL-UNWANTED-COUNTRY extended deny ip 192.168.1.0 255.255.255.0 any
```

```
asa#
```

```
show running-config access-group
```

```
***OUTPUT OMITTED FOR BREVITY***
```

```
access-group ACL-UNWANTED-COUNTRY in interface outside control-plane
```

رظح ب موقت يتي التل مكحتل لى وتسم لى لى ع (ACL) لوصول لى ف مكحتل لى ةمئاق ديكأتل 2. ةوطخل لى ةهجالول لى لى دراول TCP 443 لاصت لى ةكاحم لى packet-tracer رمل لى مدختس لى ، ةبولطم لى رورم لى ةكح دد ةدايز بچي ، `show access-list <acl-name>` رمل لى مادختس لى مئ ، نمل لى ةيامحل لى رادل لى ةيچارخل لى VPN ةوق لى لاصت لى رظح لى ف مئ لى ةم لى ف (ACL) لوصول لى ف مكحتل لى ةمئاق لى لوصول لى تارم لى (ACL) لوصول لى ف مكحتل لى ةمئاق لى ةطساوب نمل لى ةيامحل لى رادل لى ةيئاوش لى ع

نم هيل لى لوصول لى مئ مئاق TCP 443 لى لى لى ةكاحم لى packet-tracer رمل لى موقبي ، لى لى لى اذى ف لى - انب صاخ لى نمل لى ةيامحل لى رادل لى ةيچارخل لى IP ناونع لى لى ههيجوت مئ لى و 192.168.1.10 فى لى ضم لى تادايىز 'show access-list' ةيچارخل لى ضرعي و لى ةطاق لى مئ لى يتي لى رورم لى ةكح 'packet-tracer' ةيچارخل لى دكؤي ةدوچوم لى مكحتل لى وتسم لى (ACL) لوصول لى ف مكحتل لى ةمئاق لى لوصول لى تارم دد

FTD لى ةيچارخل لى لى مئ

```
<#root>
```

```
>
```

```
packet-tracer input outside tcp 192.168.1.10 1234 10.3.3.251 443
```

```
Phase: 1
```

```
Type:
```

```
ACCESS-LIST
```

```
Subtype: log
```

```
Result: DROP
```

```
Elapsed time: 21700 ns
```

```
Config:
```

```
Additional Information:
```

```
Result:
```

```
input-interface: outside(vrfid:0)
```

```
input-status: up
```

```
input-line-status: up
```

```
Action: drop
```

```
Time Taken: 21700 ns
```

Drop-reason: (acl-drop) Flow is denied by configured rule

, Drop-location: frame 0x00005623c7f324e7 flow (NA)/NA

>

show access-list ACL-UNWANTED-COUNTRY

access-list ACL-UNWANTED-COUNTRY; 1 elements; name hash: 0x42732b1f

access-list ACL-UNWANTED-COUNTRY line 1 extended deny ip 192.168.1.0 255.255.255.0 any (

hitcnt=1

) 0x142f69bf

ASA جارجا للاثم

<#root>

asa#

packet-tracer input outside tcp 192.168.1.10 1234 10.3.3.5 443

Phase: 1

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Elapsed time: 19688 ns

Config:

Implicit Rule

Additional Information:

MAC Access list

Phase: 2

Type:

ACCESS-LIST

Subtype: log

Result: DROP

Elapsed time: 17833 ns

Config:

Additional Information:

Result:

input-interface: outside

input-status: up

input-line-status: up

Action: drop

Time Taken: 37521 ns


Drop-reason: (acl-drop) Flow is denied by configured rule

, Drop-location: frame 0x0000556e6808cac8 flow (NA)/NA

asa#

```
show access-list ACL-UNWANTED-COUNTRY
```

```
access-list ACL-UNWANTED-COUNTRY; 1 elements; name hash: 0x42732b1f
access-list ACL-UNWANTED-COUNTRY line 1 extended deny ip 192.168.1.0 255.255.255.0 any
(hitcnt=1)
0x9b4d26ac
```

 في Cisco نم نم آل ليمع ل باب ة صاخ ل VPN ة كبش ل ثم RAPN ل ح ذيفنت مت اذا: ة ظالم نم آل ة امحل راج ة قيققح ل اصتا ة لواحم ءارح ذئنيح نكميف، نم آل ة امحل راج ة كرح رطال عقوتم وه امك مكحت ل يوتسمل لوصول ي ف مكحت ل ة مئاق لمع ديكأتل ة بولطم ل رورم ل.

ة لصل تا ذ ءاطخال

- حيحصت فرعم: يفارغل عقوم ل ل ة دنتم ل AnyConnect ليمع تالاصت | هن | [Cisco CSCvs65322](#) نم ءاطخال

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت
م ل ا ل ا ل ا ن ا ع مچ م ف ن م دخت س م ل م عد و ت م م م دقت ل ة يرش ب ل و
م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت م م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا م ل ا ح ل ا و ه
ل ا ل ا م ا د ا د و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا