# ليمع نيمأتل زيزعتلا ريبادت ذيفنت AnyConnect VPN

# تايوتحملا

<u>قمدق م ال</u>
<u>قي، س اس أل ا ت ابل طت مل ا</u>
<u>تابل طتمل ا</u>
<u>ةمدختسمل اتانوكمل ا</u>
<u>ةي،س.اس.أ تـامول.عم</u>
مي افعل ا
<u>Cisco: نم نمآلاً قيامحلاً رادج يالع قنمآلاً ليومعاناً قووقت تباسرامم</u>
<u>syslog و ل،يچسټل،ا ټافرعم مادختساب تامچەل،ا دي.دخت</u>
<u>ال تحرقرة من الموجعة معاملة من الموجعة الموجعة الموجعة الموجعة الموجعة الموجعة الموجعة الموجعة الموجعة الموجعة</u>
<u>FMC نيوكت ةل، ثمأ</u>
DefaultRagGroup و DefaultWebVPNGgroup ل.ي.ص.وت ټاف.ي.ص.وت ي.ف AAA ةق.داص.م ل.ي.ط.عت
<u>ل مطعت Hostscan / و DefaultRAGgroup مل ع نمآل اقوامحل ارادج عض ال DefaultWEBvpngGroup ل و DefaultRAGgroup (مراع تمآل)</u>
<u>قعومجمل اب قص إخل ا URL نيوانع نيكمتو قراعتسمل اقعومجمل اعامساً ليوطعت</u>
<u>قداەش ل ا نېيىعت</u>
IPsec-IKEv2
ASA ن <u>يوكت ةل.ثمأ</u>
DefaultRagGroup و DefaultWebVPNGgroup ل.يصروت ټاف.يصروت ي.ف AAA قوّ.داصم ل.يطعت
<u>ليطعت Hostscan / و Default WEBvpngGroup دلع نمآلا قيامحلا رادج عضو DefaultRAGgroup ليطعت</u> ( <u>درايټخا)</u>
<u>قعومچمل اب قص اخل ا URL نيوان ع نيكمتو قراعتسمل ا قعومچمل ا عامس أ ليوطعت</u>
<u>قداەش ل.ا نېيعت</u>
IPsec-IKEv2
بارقاليا
<u>ةل ص تاذ تامول عم</u>

# ةمدقملا

.كيدل دعب نع لوصولل VPN ةكبش ذيفنت نامأ نيسحت ةيفيك دنتسملا اذه حضوي

# ةيساسألا تابلطتملا

### تابلطتملا

:ةيلاتلا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

• Cisco Secure Client AnyConnect VPN.

• دعب نع لوصولا نيوكت

ةمدختسملا تانوكملا

ةيلاتا جماربلاو ةزهجألا تارادصإ ىلإ تاسرامملا لضفأ ليلد دنتسي:

- Cisco ASA 9.x
- Firepower 7.x / FMC 7.x ديدهت دض عافدلا جمانرب •

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألاا نم دنتسملا اذه يف ةدراولا تامولعملا عاشنإ مت. تناك اذإ .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجألا عيمج تأدب رمأ يأل لمتحملا ريثأتلل كمهف نم دكأتف ،ليغشتلا ديق كتكبش.



تريذحت FDM معدي .(FDM اذه يوتحي ال :ريذحت DefaultWEBVPNGgroup مئاوق مادختسإ ءاجرلا. طقف DefaultWEBVPNGgroup يلع ققداصملا اقيرط رييغت ل "ةماعلا تادادعإلاا" مسق يف صصخم ذفنم وأ مكحتلا يوتسمل لوصولا يف مكحتلا تدعاسملا زكرمب لاصتالا يجري .FDM مدختسم ةهجاو لخاد دعب نع لوصولل VPN .رمألا مزل اذإ ةدعاسملا نم ديزم يلع لوصحلل Cisco نم (TAC) قينقتلا

# ةيساسأ تامولعم

نم نمآلا ليمعلاب صاخلا AnyConnect VPN نيوكت مازتلا نامض وه دنتسملا اذه نم ضرغلا .ةعئاش ينورتكلإلا نامألا تامجه نوكت ثيح ثيدح ملاع يف نامألا تاسرامم لضفأب Cisco

- دنع ةصاخ) نمآلا Cisco ةيامح رادجل لماكلاب ةلەؤملا تالاجملا ءامسأ فشك .1 (لاصتالا فيرعت فلم يف ةيعامج ةراعتسم ءامسأ مادختسإ:
  - دعب مەيدل نوكيسف ،كب صاخلا VPN ةيامح رادجل FQDN مجاەملا فشتكا اذإ يذلا ةعومجملل راعتسملا مسالا مادختساب قفنلا ةعومجم ديدحت رايخ كلذ .ەيف ةمشاغلا ةوقلا موجە ءدب نوديري
- تانايبلا ةدعاق وأ AAA مادختساب يضارتفالا لاصتالا فيرعت فلم نيوكت مت .2 :ةيلحملا
  - AAA مداخ ةمجاهم ةلواحم هنكميف ،VPN ةيامح رادجل FQDN ىلع مجاهملا رثع اذا يف FQDN دودحب لاصتالا نأل اذه ثدحي .ةوقلاب ةيلحملا تانايبلا ةدعاق وأ قراعتسم ءامسأ ديدحت مدع ةلاح يف يتح ،يضارتفالا لاصتالا فيرعت فلم .تاعومجملل.
- :AAA مداوخ ىلع وأ ةيامحلا رادج ىلع دراوملا كالەتسإ .3
  - َ لااسرا لالخ نم ةيامحلا رادج دراوم وأ AAA مداوخ ىلع بلغتلا نيمجاهملل نكمي . قمدخلا عطق ةلاح ءاشنإو ةقداصملا تابلط نم ةريبك تايمك .

### ميەافملا

:ةراعتسملا تاعومجملا ءامسأ

• المحب دعب المحتال فيرعت فلم ىلإ عوجرلا هلالخ نم ةيامحلا رادجل نكمي ليدب مسا ليمعلا مدختسم ةهجاو يف ةلدسنم ةمئاق يف ءامسألا هذه رهظت ،ةيامحلا رادجب لاصتا ةراعتسملا ءامسألا ةلازا يدؤت .مهديدحت متيس نيذلا نيمدختسملل ةنمآلا نمآلا ليمعلا مدختسم ةهجاو يف ةلدسنملا ةفيظولا ةلازا يلإ تاعومجملل.

:ةعومجملاب ةصاخلا URL نيوانع

ةدراولا تالاصتالا نييعت متي ثيحب لاصتا فيرعت فلمب هطبر نكمي URL ناونع • نكمي ثيح ،ةلدسنم ةفيظو دجوت ال .بوغرم لاصتا فيرعت فلم ىلإ ةرشابم جمد نكمي وأ ،نمآلا ليمعلا مدختسم ةهجاو يف لماكلا URL ناونع لاخدا نيمدختسملل مدختسملا نم URL ناونع ءافخإل XML فيرعت فلم يف 'ضرعلا مسا' عم URL ناونع.

مدختسملا رشابي ثيح ،ةيعامج ةراعتسم ءامسأ قيبطت ةلاح يف انه فالتخالا نمكي فلم ىلإ مەعفد ديدحتل ةراعتسم ءامسأ عم مدقيو to vpn\_gateway.example.com لاصتالا ب لاصتالا مدختسملا أدبي ،ةعومجملاب ةصاخلا URL نيوانع مادختساب .لاصتا فيرعت vpn\_gateway.example.com/example\_group نودب لاصتالا فيرعت فلم يارة قرشابم مەدوقيو vpn\_gateway.example.com/example\_group نودب لاصتال فيرعت فلم ىلإ ةرشابم مەدوقيو الله.

### نم نمآلا ةيامحلا رادج ىلع ةنمآلا ليمعلا ةيوقت تاسرامم Cisco:

تاعومجم/لاصتالا فيرعت تافلمل نييعرشلا نيمدختسملا نييعت ىلع قرطلا هذه دمتعت قفن ةعومجم ىلإ نيلمتحملا نيراضلا نيمدختسملا لاسرا متي امنيب ةبسانملا قفنلا مغرلا ىلعو .رورملا ةملكو مدختسملا مسا تابيكرتب حامسلا مدعل اهنيوكتب موقن ةمئالم رييغتو ةراعتسملا تاعومجملا ءامسأ ليطعت نأ الإ ،تاعيمجتلا ةفاك ذيفنت بجي ال هنأ نم ذيفنتل نابولطم DefaultRAGgroup و DefaultWEBvpngGroup ب ةصاخلا ةقداصملا ةقيرط ليصوتل

- طقف ةعومجملاب صاخلا URL ناونع مدختساو ةراعتسملا تاعومجملا ءامسأ ليطعتب مق
   نم نوكي نل ددجم FQDN كالتماب كل حمسي اذهو ،لاصتالا فيرعت فلم نيوكت يف مه بسانملا FQDN مهيدل نيذلا ءالمعلا نأل ارظن هديدحتو هفاشتكا مجاهملل لهسلا ،لاثملا ليبس ىلع للاصتالا عدب ىلع نورداقلا طقف
   vpn\_gateway.example.com/example\_group عقوم نع فشكل نم مجاهمل مل قبو مي vpn\_gateway.example.com/example\_group
- نيوكتو DefaultRAGgroup و DefaultWEBvpngGroup يف AAA ةقداصم ليطعتب مق تانايبلا ةدعاق ىلع ساق لكشب رمألا ضرف ةيناكمإ انبنجي امم ،ةداهشلا ةقداصم قلواحم دنع ةيروف ءاطخأ ويرانيسلا اذه يف مجاهملا مجاويسو .AAA مداخ وأ ةيلحملا ىلإ دنتست ةقداصملا نأل ارظن رورم ةملك وأ مدختسم مسا لقح دجوي ال .لاصتالا نودب AAA مداخ ءاشنإ وه رخآ رايخ .ةمشاغلا ةوقلا تالواحم فاقيا متي يلاتلابو ،تاداهش نودب AAA مداخ عاشن إلا مرغا رايخ .قمشاغلا اوقل الالواحم فاقي متي ما متي يل
- تالاصتالا نييعتب حمسي اذهو .لاصتالا فيرعت فلمل ةداهشلا نييعت مادختسا تاداهشلا نم ةملتسملا تامسلا ىلإ ادانتسا ةددم ليصوت تافيصوت ىلع قدراولا قبسانملا تاداهشلا مهيدل نيذلا نيمدختسملا نييعت متي .ليمعلا زامج ىلع قدوجوملا ىلإ نييعتلا ريياعم يف نوقفخي نيذلا نيمجاهملا لاسرا متي امنيب ،حيحص لكشب DefaultWEBVPNGgroup.
- نييعت ىلع قفنلا تاعومجم دامتعا يف SSL نم الدب IKEv2-IPSec مادختسإ ببستي مدختسملا زامج ىلع XML نودب .XML فيرعت فلم يف نيمدختسملا ةعومجمل ددحم .ةيضارتفالا قفنلا ةعومجم ىلإ ايئاقلت نيمدختسملا لاسرإ متي ،يئاهنلا



،ةعومجملل راعتسملا مسالا ةفيظو لوح تامولعملا نم ديزم ىلع لوصحلل :ةظحالم <u>نيوكت ليلد</u> عجار A<u>SA VPN</u> ن<u>يوكت ليلد</u> عجار SSL VPN'.

## syslog و ليجستلا تافرعم مادختساب تامجهلا ديدحت

لوصولاب ةصاخلا VPN تاكبشب ةيحضتلل ةدئاسلا ةقيرطلا ةمشاغلا ةوقلا تامجه لثمت مهملا نم .هب حرصملا ريغ لوخدلا ىلع لوصحلل ةفيعضلا رورملا تاملك لالغتساو ،دعب نع ليجست مادختسإ نم ةدافتسالا لالخ نم موجهلا تامالع ىلع فرعتلا ةيفيك ةفرعم ةياغلل تمت اذا موجه ىلإ ريشت نأ نكمي يتلا ةعئاشلا syslogs تافرعم . يه ةيداع ريغ نيزخت ةدحوب اهتهجاوم

%ASA-6-113015

<#root>

%ASA-6-113015

: AAA user authentication Rejected : reason = User was not found : local database : user = admin : user

#### %ASA-6-113005

#### <#root>

#### %ASA-6-113005

: AAA user authentication Rejected : reason = Unspecified : server = x.x.x.x : user = \*\*\*\*\* : user IP =

#### %ASA-6-716039

#### <#root>

#### %ASA-6-716039

: Group <DfltGrpPolicy> User <admin> IP <x.x.x.> Authentication: rejected, Session Type: WebVPN

.ASA ىلع no logging hide username رمألا نيوكت متي ىتح امئاد يفخم مدختسملا مسا



نم مەتڧرعم وأ نيحلاص نيمدختسم ءاشنإ مت اذإ ام لوح تامولعم اذه رفوي :ةظحالم يف نيمدختسملا ءامسأ روەظل ارظن رذحلا يخوت ىجري ،ةئيسملا IP نيوانع لالخ تالجسلا.

نم ASA لوخد ليجست Cisco:

<u>نمآلا ASA ةيامح رادجل مدختسملا ليل د</u>

ن العام العالي المعالي المعالي المعالي المعالي الماف المافي المعالي المعالي المعالي المعالي المعالي المعالي الم Firewall ASA Series General Operations CLI

Cisco: نم (FTD) ةعرسلا قئاف لاسرإلا جمانرب ىلإ لوخدلا ليجست

<u>FMC ربع FTD دلع ليجستاا نيوكت</u>

رادج ةرادإ زكرم زاهج نيوكت ليلد نم يساسألا ماظنلا تادادعإ لصف يف <u>syslog م</u>سق <u>نيوكت</u> نم نمآلا ةيامحلا <u>د جنجص نم ققحتلاو syslog نيوكت FirePOWER Device Manager</u> نع عافدلا نيوكت ليلد نم ماظنلا تادادعا لصف يف <u>ماظنلا ليچست تادادعا</u> مسق <u>نيوكت</u> ل FirePOWER ديدهت FirePOWER

موجەلا نم ققحتلا

ليغشتب مق مث ،FTD وأ CLI) ASA (CLI) رماوألا رطس ةمجاو ىلإ لوخدلا ليجستب مق ،ققحتلل اميلع ةلواحملا مت يتلا ةقداصملا تابلط نم يداع ريغ ددع نم ققحتو ،show aaa-server رمألا امنيوكت مت يتلا AAA مداوخ نم يأ ىلإ امضفر وأ:

<#root>

ciscoasa#

show aaa-server

Server Group: LOCAL - - - - - >>>> Sprays against the LOCAL database
Server Protocol: Local database
Server Address: None
Server port: None
Server status: ACTIVE, Last transaction at 16:46:01 UTC Fri Mar 22 2024
Number of pending requests 0
Average round trip time Oms
Number of authentication requests 8473575 - - - - - >>>> Unusual increments
Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions 0
Number of accepts 0
Number of rejects 8473574 - - - - >>>> Unusual increments

<#root>

ciscoasa#

show aaa-server

Server Group: LDAP-SERVER - - - - - >>>> Sprays against the LDAP server Server Protocol: ldap Server Hostname: ldap-server.example.com Server Address: 10.10.10.10 Server port: 636 Server status: ACTIVE, Last transaction at unknown Number of pending requests 0 Average round trip time Oms Number of authentication requests 2228536 - - - - - >>>> Unusual increments Number of authorization requests 0 Number of accounting requests 0 Number of retransmissions 0 Number of accepts 1312 Number of rejects 2225363 - - - - - >>>> Unusual increments Number of challenges 0 Number of malformed responses 0

Number of bad authenticators 0 Number of timeouts 1 Number of unrecognized responses 0

# FMC نيوكت ةلثمأ

### و DefaultWebVPNGgroup ليصوت تافيصوت يف AAA ةقداصم ليطعت DefaultRagGroup

دعب نع لوصولا < ةزهجألا ىلإ لقتنا.

	Firewa Overview	II Manage / Dashboards	ement Center	Overview	Analysis	Policies	Devices	Objects	Integration			
Sum Provides Netw	Summary Dashboard (switch dashboard) Provides a summary of activity on the appliance Network Threats Intrusion Events Statu:				Geolocation	QoS	Device M NAT QoS Platform FlexCon Certifica	Aanagement Settings fig tes	VPN Site To Site Remote Access Dynamic Access Troubleshooting	Policy	Troubleshoot File Download Threat Defense CLI Packet Tracer Packet Capture	
► To	ıp Zero Tr	ust Application	ns			- ×					Upgrade Threat Defense Upgrade Chassis Upgrade	

.دعب نع لوصولل VPN جەن نيوكت ىلإ لوصولل FMC ل (GUI) ةيموسرلا مدختسملا قەجاو يف لقنتلا ضرعي

### مساب لاصتا فيرعت فلم ءاشناٍو دعب نع لوصولل دوجوملا VPN جەن ريرحت 'DefaultRAGgroup'

Firewall Management Center Devices / VPN / Remote Access	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹١	0 ¢ (	admin ~	the SECURE
												Add
Name				Status			Last Modified					
RAVPN				Targeting 1 o	devices on all targeted		2024-03-07 10:58:20 Modified by "admin"				9 / i	

FMC. مدختسم ةەجاو لخاد دعب نع لوصولل VPN جەن ريرحت ةيفيك ضرع

#### 'DefaultRAGroup' و 'DefaultWEBVPNGroup' ةامسملا لاصتال فيرعت تافلم ريرحت

Firewall Management Center Devices / VPN / Edit Connection Profile	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹	0	° 0	admin v 🔤 🖞	see secure
RAVPN													Cancel
Enter Description Connection Profile Access Interfaces Adva	inced							Local Realm: LOCAL-I	EALM			Policy Ass Dynamic Access	ignments (1) Policy: None
Namo			AAA				Group Policy						
DefaultWEBVPNGroup				None None			DfttGrpPolicy						

FMC. مدختسم ةەجاو نمض DefaultWEBVPNGgroup ريرحت ةيفيك ضرع

### ةداەش' ددح .ةقداصملا بولسأ ةلدسنملا ةمئاقلا ددحو AAA بيوبتلا ةمالع ىلإ لقتنا ظفح ددحو 'طقف ليمعلا.

Edit Connection Profile		
Connection Profile:*	DefaultWEBVPNGroup	
Group Policy:*	DfltGrpPolicy +	
Client Address Assignment	AAA Aliases	
Authentication		
Authentication Method:	Client Certificate Only -	
٩	Enable multiple certificate authentication	
Map username from clier	nt certificate	
Authorization		
Authorization Server:	▼	
	Allow connection only if user exists in authorization database	
Accounting		
Accounting Server:	▼	
	Cancel	е

.FMC مدختسم ةمجاو لخاد DefaultWEBVPNGgroup ل طقف ليمعلا ةداهش ىلا ةقداصملا ققيرط رييغت

قلدسنملا ةمئاقلا ددجو AAA بيوبتلا ةمالع ىلإ لقتناو DefaultRAGgroup ريرحتب مق ظفح ددجو 'طقف ليمعلا ةداهش' ددح .ققداصملا بولسأ.

Edit Connection Profile		
Connection Profile:*	DefaultRAGroup	
Group Policy:*	DfltGrpPolicy +	
Client Address Assignment	AAA Aliases	
Authentication		
Authentication Method:	Client Certificate Only -	
	Enable multiple certificate authentication	
► Map username from clie	nt certificate	
Authorization		
Authorization Server:	<b></b>	
	Allow connection only if user exists in authorization database	
Accounting		
Accounting Server:		
	Cancel	ve 🛛

.FMC مدختسم ةمجاو لـخاد DefaultRAGgroup لـ طقف لـيمعلاا ةدامش ىلاٍ ةقداصملاً ققيرط رييغت



مت اذإ .ةريخألاا ةحتفلل AAA مداخ اضيأ ةقداصملا بولسأ نوكي نأ نكمي :ةظحالم تابلط يأ جلاعي الو افيزم نوكي AAA مداخ نيوكت نإف ،ةقيرطلا هذه مادختسإ ليمعلا ناونع نييعت" بيوبتلا ةمالع يف VPN عمجت فيرعت اضيأ بجي .لعفلاب تارييغتلا ظفحل.

و DefaultWEBvpngGroup ىلع نمآلا ةيامحلا رادج عضو / Hostscan ليطعت (يرايتخإ) DefaultRAGgroup

ةيامحلا رادج ةيعضو) Hostscan / Secure Firewall Posture كيدل ناك اذإ الإ ايرورض اذه نوكي ال ةيامحلا رادج ىلع دراوملا مادختسإ قدايز نم نيمجاهملا قوطخلا هذه عنمت .كتىئيب يف (قنمآلا ءاشنإ لالخ نم كلذ قيقحت متي ،FMC يف .قياهنلا قطقنل يىئوضلا حسملا قيلمع ببسب قطقنل يىئوضلا حسملا قفيظو ليطعتل without-csd رمألا مادختساب FlexConfig نىئاك .قاهنلا

. FlexConfig نئاك ةفاضإ < FlexConfig نئاك < نئاكلا ةرادإ < تانئاكلا ىل لقتنا

Firewall Manageme Objects / Object Manageme	nt Center Overview Analysis Policies Devices Objects Integration	Deploy Q 🧬 🌣 😡 admin 🗸	disce SECURE
AAA Server     Access List     Address Pools     Application Filters	FlexConfig Object FlexConfig Object include device configuration commands, variables, and scripting language instructions. It is used in FlexConfig polices.	Add FisicConfig Object	
AS Path	Name	Description	
BFD Template Cipher Suite List	Anyconnect_route_filtering		<u>م</u> ا
> Community List	Default_DNS_Configure	Configure Default DNS with the help of TextObjects defaultDNS	¶a Q ⊕
DHCP IPv6 Pool	Default_Inspection_Protocol_Disable	Disable Default Inspection.	¶_ ⊂, ⊕
> Distinguished Name DNS Server Group	Default_Inspection_Protocol_Enable	Enable Default Inspection.	£ <u>a</u> α
> External Attributes	DHCPv6_Pretx_Delegation_Configure	Configure one outside (PD client) and one inside interface (recip	¶a ⊂, ≣
File List	DHCPv6_Prefx_Delegation_UnConfigure	Remove configuration of one outside (PD client) and one inside i	¶aq. ⊕
FlexConfig     FlexConfig Object	DNS_Configure	Configure DNS with the help of TextObjects dnsParameters and	¶a ⊂ ≣
Text Object	DNS_UnConfigure	Remove the DNS configurations.	¶a Q, ⊕
Geolocation	Eigrp_Configure	Configures eigrp. 1. Configures next hop. 2. configures auto-su	¶a ⊜
Key Chain	Eigrp_interface_Configure	Configures interface parameters for eigrp. 1. Configures authent	¶∎ Q ≣
Network	Eigrp_UnConfigure	Clears eigrp configuration for an AS	¶a q ≣

.FlexConfig نئاك ءاشنإل FMC مدختسم ةەجاو يف لقنتلا

عونلا مادختساب تقو لك ىلع رشنلا نييعتب مق مث ،FlexConfig نئاكلا ةيمستب مق .نئاكلا ظفحا مث امامت حضوم وه امك ةغايصلا لخدأ مث

Edit FlexConfig Object						Ø
Name: Wtihout-CSD Description: Copy-pasting any rich text might int	roduce line breaks wf	nile generating CLI. Please	e verify the	CLI before deployr	nent.	
Insert 🔻 🖽 Deployment	Everytime	•	Туре:	Append	•	
tunnel-group DefaultWEBVPNGroup w without-csd tunnel-group DefaultRAGroup webvp without-csd	ebvpn-attributes					
▼ Variables		Dros	anti-			
Name	Dimension D	efault Value (Typ	e:Name)	Override	Description	
		No records to display				
					Cancel	Save

'without-csd' مادختساب FlexConfig نﺉاك ءاشטן

.FlexConfig ةسايس ريرحتل Cil قوف رقنا مث FlexConfig < ةزهجألا ىلإ لقتنا

	Firewall Management Center Devices / FlexConfig	Overview	Analysis	Policies	Devices	Objects	Integration		Deploy	۹ (	<b>°</b> 0	0	admin $\lor$	tiste SECURE
														New Policy
F	lexConfig Policy					Status		Last Modified						
	Flox-Test					Targeting 1 Out-of-date	devices on 1 targeted devices	2024-04-10 21:54:19 Modified by "admin"						9 Z ¥

.FMC لخاد FlexConfig ةسايس ريرحت

مەسلا ددح مث .مدختسملا لبق نم فرعملا مسقلا نم ەئاشناب تمق يذلا نئاكلا عقوم ددح جەن ظفحل ظفح ددح ،اريخأ .ددحملا Append FlexConfigs ىلإ ەتڧاضإل FlexConfigs

Firewall Management Center         Owney         Analysis         Paties         Objects         Devices         Objects         Paties         Devices         Objects         Paties         Devices         Objects         Paties         Devices         Objects         Paties         Devices         Objects         Devices         Devices <thdevices< th="" th<=""><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></thdevices<>								
FlexConfig   Enter Description     Available ForsConfig © ResConfig Object <ul> <li>Selected Propond FlexConfigs</li> <li>Anyconnect_route_Mannage</li> <li>Keepout</li> <li>Ne_Keepout</li> <li>Ne_Keepout</li> <li>Defaud_Inspection_Protocol_Enable</li> <li>Defaud_Inspection_Protocol_Enable</li> <li>Defaud_Inspection_Protocol_Enable</li> <li>Defaud_Inspection_Configure</li> <li>Defaud_Inspection_Configure</li> <li>Defaud_Inspection_Protocol_Enable</li> <li>Manne</li> <li>Description</li> </ul>	Firewall Management Center Devices / Flexconfig Policy Editor	Overview	v Analysis	Policies	Devices	Objects	Integration	Deploy Q 🥩 🔅 🕑 admin - 🖓 store secure
Available FlexConfig or FlexConfigs         V User Defined         1 Anyconnect _route_Ittering         2 Keepoot         1 Anyconnect _route_Ittering         2 Keepoot         3 Nume         0 Ministrated         1 Default_Inspection_Protocol_Disable         1 Default_Inspection_Protocol_Disable         1 Default_Inspection_Protocol_Disable         1 Default_Inspection_Protocol_Disable         1 Default_Inspection_Protocol_Disable         1 Default_Inspection_Protocol_Disable         1 Dischol_Arrektz_Delayation_Configure         1 Dischol_Arrektz_Delayation_Configure         1 Without-CSO	FlexConfig Enter Description							You have unsaved changes Migrate Control Preview Control Save Cancel
Image: Field Config 2       Image: Field Config 2         V User Defined       Image: Field Config 2         1 Mane       Description         V User Defined       Image: Field Config 2         1 Mane       Description         V User Defined       Image: Field Config 2         1 Mane       Description         2 Default_Inspection_Protocol_Disable       Image: Field Config 2         1 Default_Inspection_Protocol_Disable       Image: Field Config 2         1 Default_Inspection_Protocol_Enable       Image: Field Config 2         1 Default_Inspection_Config 2       Image: Field Config 2         2 Name       Description         1 Without-CSO       Image: Field Config 2         1 Without-CSO       Image: Field Config 2	Available FlaxConfin	°] Sek	acted Prepend F	lexConfigs				
V User Defined       Image: Configure         1 Kepport       Image: Configure         1 Defined       Image: Configure         1 Defined_Inspection_Protocol_Enable       Image: Configure         1 Defined_Inspection_Configure       Image: Configure         1 Without-CSO       Image: Configure	FlexConing Object		Name			Description		
DHCPv6_Prefx_Delegation_Configure     II     Name     Description       DHCPv6_Prefx_Delegation_Lik/Configure     II     Name     Description       ID ND_Configure     I     Without-CSD     Q m	V User Defined ? Anyconnect, routin_titlering ? Koepout ? No_Koepout ? No_Koepout ? Definut_CSD > System Defined ? Definut_Inspection_Protocol_Disable ? Definut_Inspection_Protocol_Finable							
I         Name         Description           1         Wthout-CSD         Q	DHAM_INDECLOT_PRODUCT_CHADE     DHCPv6_Prefix_Delegation_Configure	Sek	cted Append Fl	exConfigs				
T DNS_Configure 1 Without-CSD Q	. DHCPv6_Prefix_Delegation_UnConfigure		Name			Description		
	" DNS_Configure		Wtihout-CSD					٩.
.∬ DNS_Uk-Contgure	_ DNS_UnConfigure							
Eigrp_Configure     Some Interface Configure	*2 Eigrp_Configure							

.FlexConfig ةسايسب FlexConfig نئاكلا قافراب مق

ددح .قفاوم ددح مث ،هيلع اذه FlexConfig جهن قيبطت ديرت يذلا FTD رتخاو جهنلا تانييعت ددح نم ققحتلا .تارييغتلا رشنب مقو ديدج FlexConfig نييعت وه اذه ناك اذإ ىرخأ ةرم ظفح رشنلا درجمب ةحصلا

Firewall Management Center Devices / Flexcorify Policy Editor	Overview Anal	ysis Policies	Devices Objec	ts Integration			Deploy Q 🧬 🌣 🔞	admin ~ atom SECURE
FlexConfig Enter Description								Ing Sive Cancel
Available RiexConfig C FlexConfig Object	Selected Prep	end FlexConfigs Targeted Devic		Policy Assignments (1)				
V User Defined      Anyconnect_route_filtering      Anyconnect_route_filtering      Keepout      No_Keepout      Without-CSD      System Defined      Default_INS_Configure     _/ Default_Inspection_Protocol_Disable		Targeted Devices Select devices to v Available Devices Q. Search by nam FTD1	which you want to app te or value	<b>ly this policy</b> . Add to Policy				
1 Default_Inspection_Protocol_Enable 1 DHCPv6_Protoc_Delegation_Configure 1 DHCPv6_Protoc_Delegation_UncConfigure 2 DNS_Configure 1 DNS_UnConfigure 2 Egrp_Configure 2 Egrp_Configure 3 Egrp_UncConfigure 1 Egrp_UncConfigure	Selected Apr Name 1 Without-Ct					Cancel		Q.∰

.FirePOWER زاهجل FlexConfig ةسايس صيصختب مق

ل DefaultWEBvpngGroup رمألا ردصأو FTD يف (CLI) رماوأ رطس ةەجاو لخدأ و Csd نود نأ تققد csd ليف رضاح نآلا ايف رضاح نا ال

#### <#root>

FTD72#

show run tunnel-group DefaultRAGroup

tunnel-group DefaultRAGroup general-attributes
address-pool TEST-POOL
tunnel-group DefaultRAGroup webvpn-attributes
authentication certificate

without-csd

FTD72#

show run tunnel-group DefaultWEBVPNGroup

tunnel-group DefaultWEBVPNGroup general-attributes
address-pool TEST-POOL
tunnel-group DefaultWEBVPNGroup webvpn-attributes
authentication certificate

without-csd

ةعومجملاب ةصاخلا URL نيوانع نيكمتو ةراعتسملا ةعومجملا ءامسأ ليطعت

فذح وأ ليطعتب مق ."ةراعتسم ءامسأ بيوبتلا ةمالع ددحو لاصتا فيرعت فلم ىلإ لقتنا

URL. ل راعتسم مسا ةفاضإل دئاز ةنوقيأ رقناو ،ةعومجملل راعتسملا مسالا

Edit Connection Profile		
Connection Profile:* LDAP-TG		
Group Policy:* DfltGrpPolicy Edit Group Policy	• +	
Client Address Assignment AAA Aliases		
Alias Names:		
Incoming users can choose an alias name upon first login. Alia on this device can be turned on or off for display.	ses from all connections	configured
Name	Status	
LDAP	Disabled	1
URL Alias:		
Configure the list of URL alias which your endpoints can select following URLs, system will automatically log them in via this c	on web access. If users	choose the
	onnection prome.	+
URL	Status	

.FMC مدختسم ةەجاو لخاد قڧنلا ةعومجملل راعتسملا مسالا رايخ ليطعت

IP ناونع وأ/و FQDN ةئبعتب مقو ،URL ناونعل راعتسملا مسالل نئاك مسا نيوكتب مق اذه يف .هب لاصتالا فيرعت فلم نارقإ ديرت يذلا مسالاب اعوبتم ،URL ناونعل ةيامحلا رادجل لمتحملا ريغ نم نوكي ثيح ،انامأ رثكأ ناك املك ،رثكأ امهبم ناك املك .'aaldap' انرتخا ،لاثملا درجمب .كب صاخلا FQDN ىلع اولصح دق اوناك اذإ ىتح لماكلا URL ناونع نيمخت نيمجاهملل ظفح ددح ،ءاهتنالا



.FMC مدختسم ةهجاو لخاد URL-Alias نﺉاك ءاشטן

.قفاوم ددجو نكمم عبرملا ددجو ،ةلدسنملا ةمئاقلا نم URL ناونعل راعتسملا مسالا ددج



.FMC مدختسم ةهجاو لخاد URL ناونعل راعتسملا مسالا نيكمت نم دكأت

راعتسملا مسالا نيكمت نم ققحتو هليطعت وأ ةعومجملل راعتسملا مسالا فذح نم دكأت ظفح ددح مث نآلا URL ناونعل.

Edit Connection Profile		0
Connection Profile:* LDAP-TG		
Group Policy:* DfltGrpPolicy Edit Group Policy	• +	
Client Address Assignment AAA Aliases		
Incoming users can choose an alias name upon first login. Alia on this device can be turned on or off for display.	ases from all connections	configured
Name	Status	
LDAP	Disabled	/1
URL Alias:		
Configure the list of URL alias which your endpoints can select following URLs, system will automatically log them in via this of the second s	t on web access. If users connection profile.	choose the +
URL	Status	
LDAP-ALIAS (https://ftd1 com/aaaldap)	Enabled	/1
		·
	Cance	Save

.FMC مدختسم ةهجاو نمض قفنلا ةعومجمل URL ناونعل راعتسملا مسالا رايخ نيكمت

ل الخ نم كلذ قيقحت متيو .XML نم ءزجك ةراعتسملا URL ءامساً عفد اضياً نكمي ،تبغر اذا ،كلذب مايقلل .ASA فيرعت فلم ررحم وأ VPN فيرعت فلم ررحم مادختساب XML ريرحت عم "نيمدختسملا ةعومجم" لقح قباطت نم دكأتو "مداوخلا ةمئاق" بيوبتلا ةمالع ىلإ لقتنا ل ةبسنلاب .SSL مادختسا دنع لاصتالا فيرعت فلمب صاخلا URL ناونعل راعتسملا مسالا IKEv2، لاصتالا فيرعت فلمل ددحمل مسالا عم نيمدختسملا ةعومجم لقح قباطت نم دكأت

Server List Entry	×
Server Load Balancing Servers SCEP Mo	obile Certificate Pinning
Primary Server	Connection Information
Display Name (required) FTD1-SS	L Primary Protocol SSL V
FQDN or IP A User (	Group ASA gateway
ftd1com / asald	ap Auth Method During IKE Negotiation EAP-AnyConnect ~
Group URL	IKE Identity (IOS gateway only)
ftd1com/aaaldap	
Backup Servers	
Host Address	s Add
	Move Up
	Move D
	Delete
	OK Cancel

.SSL تالاصتال URL ل راعتسم مسا يلع لوصحلل XML فيرعت فلم ريرجت

### ةداەشلا نييعت

دادعا رايخ رتخأ .دعب نع لوصولل VPN جەن نمض ةمدقتم تارايخ بيوبتلا ةمالع ىلإ لقتنا طيطخت ةفاضاٍ ددح ،ەديدحت درجمب .ليضفتلا ىلع ءانب ماع.

RAVPN			You have unsave	d changes Save Cancel
Enter Description Connection Profile Access Inter	faces Advanced		Local Realm: None	Policy Assignments (1) Dynamic Access Policy: None
Secure Client Images Secure Client Customization GUI Text and Messages Icons and Images Scripts Binaries Custom Installer Transforms	General Settings for Connection Profile Mapping The device processes the polices in the order lawed below until it finds a match Use group URL if group URL and Certificate Map match different Connection Profiles Use the configured rules to match a certificate to a Connection Profile Certificate to Connection Profile Mapping Client request is checked against each Certificate Map, associated Connection Profile will be used when rules are matc Please provide at least one Certificate Mapping.	hed. If none of the Certificate Map is matched, default connection profile w	Il be chosen.	Add Mapping
Localized Installer Transforms	Certificate Map	Connection Profile		
Address Assignment Policy Certificate Maps		No Records Found		
Group Policies				
LDAP Attribute Mapping				
Load Balancing				
V IPsec				
Crypto Maps IKE Policy IPsec/IKEv2 Parameters	Default Connection Profile: This Connection Profile will be applied when none of the Continues Map's rade is matched.			•

مدختسم ةمجاو لخاد صيخرت ةطيرخ نﺉاك ءاشטָןل FMC مدختسم ةمجاو نمض ةمدقتم تارايخ بيوبتاا ةمالع ىلٍا لاقتنالا FMC.

صئاصخ ديدحتب مق ،ةدعاقلا هذه يف .ةدعاق ةفاضإ ددحو ةداهشلا ةطيرخ نئاك ةيمستب مق درجمب .نيعم لاصتا فيرعت فلم ىلإ مدختسملا نييعتل اهفيرعت يف بغرت يتلا ةداهشلا ظفح ددح مث قفاوم ددح ،ءاهتنالا.

Add (	Certificate Map				0
Map I Cer Mapp Config	Name*: tificate-Map-CN ing Rule gure the certificate	matching rule			Add Rule
#	Field	Component	Operator	Value	
1	Subject	CN (Common Nam	Equals -	customval	ue
	OK Cancel				
				Cance	Save

.FMC مدختسم ةەجاو لخاد ةطيرخلل ريياعم ةفاضإو ةداەش ةطيرخ ءاشنإب مق

نرتقي نأ ديرت يذلا ليصوتلا فيصوتو ،ةداەشلا ةطيرخ نﺉاك ددح ،ةلدسنملا ةمﺉاقلا نم قڧاوم ددح مث .ةداەشلا ةطيرخ ەب.

Add Connection Profile to Certificate Map	
Choose a Certificate Map and associate Connection Profiles to selected Certficate Map.	
Certificate Map Name*:	
Certificate-Map-CN +	
Connection Profile*:	
LDAP-TG 🔻	
Cancel	

.FMC مدختسم ةەجاو لخاد ةبولطملا قفنلا ةعومجمب ةداەشلا ةطيرخ نىئاك طبرب مق

لشف اذإ ىتح DefaultWEBVPNGgroup ك يضارتفالا لاصتالا فيرعت فلم نيوكت نم دكأت ظفح ددح ،ءاەتنالا درجمب .DefaultWEBVPNGgroup ىلإ ەلاسرا متي نييعتلا يف مدختسملا تارييغتلا رشنو.

RAVPN Enter Description	faces Advanced	Yeu h Local Realm: None	ee unaaved changer Save Cancel Policy Assignments (1) Dynamic Access Policy: None
Secure Client Images Secure Client Customization GUI Text and Messages Icons and Images Scripts Binaries Custom Installer Transforms	General Settings for Connection Profile Mapping The device processes the policies in the order listed below until it finds a match Use group URL if group URL and Certificate Map match different Connection Profiles Votes the configured rules to match a certificate to connection Profile Certificate to Connection Profile Mapping Client request is checked against each Certificate Map, associated Connection Profile will be used when rules are match	ched. If none of the Certificate Map is matched, default connection profile will be chosen.	Add Mapping
Localized Installer Transforms	Certificate Map	Connection Profile	
Address Assignment Policy	Certificate-Map-CN	LDAP-TG	/1
Ceromicate Mapps Group Policies LDAP Attribute Mapping Load Balancing > IPacc Crypto Maps IKE Policy			
IPsec/IKEv2 Parameters	Default Connection Profile: This Connection Profile will be applied when none of the Cortificate May's rule is matched.		DefaultWEBVPNGroup •

.FMC مدختسم ةمجاو نمض DefaultWEBVPNGgroup ىل قدامشلا نييعتل يضارتفالا لاصتالا فيرعت فلم رييغتب مق

### IPsec-IKEv2

.ةعومجملا جەن ريرحت ىلإ لقتناو ،بولطملا IPsec-IKEv2 لاصتا فيرعت فلم ددح

Edit Connection Profile	e	
Connection Profile:*	IKEV2	
Group Policy:*	IKEV2-IPSEC  +	
Client Address Assignmen	t AAA Aliases	

IP Address for the remote clients can be assigned from local IP Address pools/DHCP Servers/AAA Servers. Configure the 'Client Address Assignment Policy' in the Advanced tab to define the assignment criteria.

Address Pools:

Name	IP Address Range	
AnyConnect_Pool	10.50.50.1-10.50.50.6	1

#### DHCP Servers:

Name	DHCP Server IP Address		
		Cancel	Save

.FMC مدختسم ةەجاو لخاد ةعومجم جەن ريرحت

عبرم ديدحت نم دكأتو VPN تالوكوتورب مسق ىلإ لقتنا ،ماع بيوبتلا ةمالع يف IKEv2.

Edit Group Policy	
Name:* IKEV2-IPSEC	
Description: General Secure	Client Advanced
VPN Protocols IP Address Pools Banner DNS/WINS Split Tunneling	VPN Tunnel Protocol: Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel. ☐ SSL ✔ IPsec-IKEv2

.FMC مدختسم ةەجاو يف ةعومجملا جەن لخاد IPsec-IKEv2 نيكمتب مق

ةمئاق بيوبتلا ةمالع ىلإ لقتنا ،ASA فيرعت فلم ررحم وأ ،VPN فيرعت فلم ررحم يف لاصتالا فيرعت فلم مسال امامت اقباطم نيمدختسملا ةعومجم مسا نوكي نأ بجي .مداوخلا ةعومجم مسا / لاصتالا فيرعت فلم وه IKEV2 ناك ،لاثملا اذه يف .ةيامحلا رادج ىلع دوجوملا ةهجاو يف "ضرعلا مسا" ضرع متي .IPsec كيساسألاا لوكوتوربلا نيوكت مت .نيمدختسملا اذه لاصتالا فيرعت فلم من عن يعتال فيرعت فلمب ل

Server List Entry	×
Server Load Balancing Servers SCEP Mobile Certifica	ate Pinning
Primary Server Display Name (required) FTD1-IPSEC FQDN or IP A Itter Group ftd1 Com Itter Group URL Itter Group	Connection Information Primary Protocol IPsec  ASA gateway Auth Method During IKE Negotiation EAP-AnyConnect KE Identity (IOS gateway only)
Backup Servers Host Address	Add Move Up Move D Delete
OK	Cancel

فيرعت فلم مسا نيمدختسملا ةعومجم قباطتو ،IPsec يساسألا لوكوتوربلا نوكي ىتح XML فيرعت فلم ريرحتب مق لااصتالا



دنع .ةيامحلا رادج نم ليمعلا ىلإ XML تافيصوت عفدل SSL لاصتا مزلي :ريذحت جراخ ةقيرطب ءالمعلا ىلإ XML تافيصوت عفد بجي ،طقف IKEV2-IPsec مادختسإ قاطنلا

نم نيمدختسملاً ةعومجم Secure Client مدختسي ،ليمعلاً ىلإ XML فيرعت فلم عفد درجمب الالاي اللالاي المتا فيرعت فلم المت المتال الك XML فيرعت فلم

🕲 Cisco Secure	Client			×
	AnyConnect VPN: Contacting FTD1-IPSEC. FTD1-IPSEC	×	Connect	
Cisco Sec	ure Client   FTD1-IPSEC		×	dialia cisco
Use Pas	rname: nroche sword:			
	ОК	Cancel		

# ASA نيوكت ةلثمأ

### و DefaultWebVPNGgroup ليصوت تافيصوت يف AAA ةقداصم ليطعت DefaultRagGroup

اەنأ ىلع ةقداصملا ددجو DefaultWEBvpngGroup قەنلا ةعومجمل WebVPN تامس مسق لخدأ نوطحي نيذلا نومدختسملا ربجي DefaultRAGgroup ل ةيلمعلا ەذە ررك .ةداەش ىلإ ةدنتسم مەل حاتت الو ةقداصملل ةداەش ميدقت ىلع ەذە ةيضارتڧالا ليصوتلا تاڧيصوت ىلع رورملا ةملكو مدختسملا مسا تاغوسم لاخدإ ةصرف

ASA# configure terminal ASA(config)# tunnel-group DefaultWEBVPNGroup webvpn-attributes ASA(config-tunnel-webvpn)# authentication certificate

ASA# configure terminal

### و DefaultWEBvpngGroup ىلع نمآلا ةيامحلا رادج عضو / Hostscan ليطعت DefaultRAGgroup (يرايتخإ)

قيامحلا رادج ةيعضو) Hostscan / Secure Firewall Posture كيدل ناك اذإ الإ ايرورض اذه نوكي ال قيامحلا رادج ىلع دراوملا مادختسإ قدايز نم نيمجاهملا قوطخلا هذه عنمت .كتىئيب يف (قنمآلا ل webVPN تامس مسق لخدأ .قياهنلا قطقنل يىئوضلا حسملا قيلمع ببسب DefaultRAGgroup تامال فيرعت تافلمو DefaultRAGgroup و DefaultWEBvpngGroup د عتال

ASA# configure terminal ASA(config)# tunnel-group DefaultWEBVPNGroup webvpn-attributes ASA(config-tunnel-webvpn)# without-csd

ASA# configure terminal ASA(config)# tunnel-group DefaultRAGroup webvpn-attributes ASA(config-tunnel-webvpn)# without-csd

### ةعومجملاب ةصاخلا URL نيوانع نيكمتو ةراعتسملا ةعومجملا ءامسأ ليطعت

راعتسم مسا دوجو ةلاح يف .اەب نيلصتملا قفنلا (تاعومجم) ةعومجم يمدختسم لخدا ناونع ءاشناب مق ،كلذ لامتكا درجمب .لطعم وه لاثم اذه يف .هتلازا وأ هليطعتب مق ،ةعومجمل مسالا نوكي نأ بجي .RAPN ءاهنا ةهجاوب صاخلا IP ناونع وأ FQDN مادختساب ةعومجمل URL و ،VPN لثم ةكرتشملا ميقلا بنجت .اضماغ ةعومجملا تامولعم عقوم ددحم ةياهن يف دوجوملا AAA و اذإ لماكلا URL ناونع نيمخت نيمجاهملا ىلع لهست هذه نأ ثيح DAP و ،SADIUS و . قاوم مي مي اولصح قومجم ديدت على كدعاست قيلخاد قيمها تاذ عامسا مدختسا ،كلذ نم الدب .FQDN و . قافنالا

ASA# configure terminal ASA(config)# tunnel-group NAME webvpn-attributes ASA(config-tunnel-webvpn)# group-alias NAME disable ASA(config-tunnel-webvpn)# group-url https://FQDN/name enable

ةداەشلا نييعت

اەل يلسلست مقرو مسا نييعتب مقو تاداەش ةطيرخ ءاشنإب مق ،ماعلا نيوكتلا عضو نم. بجي ،لاثملا اذه يف .نييعتلا مادختسال اەتقباطم نيمدختسملا ىلع بجي ةدعاق ددح مث دعب ."customValue" يواست يتلا ةكرتشملا مسالا ةميق ريياعم ةقباطم نيمدختسملا ىلع ،متي نإ ام .ةبولطملا قفنلا ةعومجم ىلع ةداەشلا ةطيرخ قبطو WebVPN نيوكت لخدأ ،كلذ لخدي DefaultWEBVPNGgroup نيذلاا نيمدختسملل يضارتفالا او group قفنلا اذه لعجيو DefaultWEBVPNGgroup لخدي مههيجوت متي ،نييعتلا يف نيمدختسملا لشف ةلاح يف .قداهشلا نييعت يف نوقفخي ال ،ةداهشلا ةقداصمب DefaultWEBvpngGroup نيوكت متي امنيب .DefaultWEBVPNGgroup يلإ .رورملا ةملك وأ مدختسملا مسا دامتعا تانايب ريرمت رايخ نيمدختسملل رفوتي

ASA(config)# crypto ca certificate map NAME 1 ASA(config-ca-cert-map)# subject-name attr cn eq customvalue

ASA(config)# webvpn ASA(config-webvpn)# certificate-group-map NAME 1 TG-NAME

ASA(config)# tunnel-group DefaultWEBVPNGroup webvpn-attributes ASA(config-tunnel-webvpn)# tunnel-group-map default-group

IPsec-IKEv2

لاخداو ديدج ةعومجم جەن ءاشنا وأ دوجوم ةعومجم جەن ريرحت كنكمي ،ماعلا نيوكتلا عضو نم اللاحيان اللاحي اللاحي IKEv2 نيكمتب مق ،تامسلا مسق يف نوكت نأ درجمب .اذه ةعومجملا جەنب قصاخلا تامسلا متيس قافنأ ةعومجمب اذه ةعومجملا جەن طبر نم دكأت .ديحولا VPN قفن لوكوتوربك بجي ،FMC تاوطخ رارغ ىلع .IPsec-IKEV2 ىلإ دعب نع لوصولل VPN تالاصتال اەمادختسا رييغتو ASA فيرعت فلم ررحم وأ VPN فيرعت فلم ررحم ربع XML فيرعت فلم ريرحت كيلع ىلإ لوكوتوربلا رييغتو ،ASA يلع قفنلا ةعومجم مسا قباطيل نيمدختسملا ةعومجم لقح

ASA# configure terminal ASA(config)# group-policy GP-NAME internal ASA(config)# group-policy GP-NAME attributes ASA(config-group-policy)# vpn-tunnel-protocol ikev2

ASA(config)# tunnel-group TG-NAME general-attributes ASA(config-tunnel-general)# default-group-policy GP-NAME

قمئاق بيوبتلا ةمالع ىلإ لقتنا ،ASA فيرعت فلم ررحم وأ ،VPN فيرعت فلم ررحم يف لاصتالا فيرعت فلم مسال امامت اقباطم نيمدختسملا ةعومجم مسا نوكي نأ بجي .مداوخلا ضرعلا مسا رهظي .IPsec كيساسألا لوكوتوربلا نيوكت مت .ةيامحلا رادج ىلع دوجوملا .اذه لاصتالا فيرعت فلمب لاصتا ءاشنإ دنع نمآلا ليمعلا مدختسم ةهجاو يف مدختسمل

Server List Entry	×
Server Load Balancing Servers SCEP Mobile Certific	ate Pinning
Primary Server Display Name (required) ASA-IPsec FQDN or IP A User Group FQDN Group URL FQDN/TG-NAME	Connection Information Primary Protocol IPsec  ASA gateway Auth Method During IKE Negotiation EAP-AnyConnect  IKE Identity (IOS gateway only)
Backup Servers Host Address	Add Move Up Move D Delete
OK Cancel	

مسا نيمدختسملا ةعومجم مسا قباطيو IPsec وه يساسألا لوكوتوربلا مسا نوكي ىتح XML فيرعت فلم ريرحتب مق تالاصتال ASA ب صاخلا قفنلا ةعومجم IPsec-IKEv2 RAPN.



دنع .ةيامحلا رادج نم ليمعلا ىلإ XML تافيصوت عفدل SSL لاصتا مزلي :ريذحت جراخ ةقيرطب ءالمعلا ىلإ XML تافيصوت عفد بجي ،طقف IKEV2-IPsec مادختسإ قاطنلا.

# رارقلا

نييعت يف دنتسملا اذه يف ةدراولا زيزعتلا تاسرامم نم ضرغلا لثمتي ،ةصالخلا يف نيمجاهملا رابجإ متي امنيب ةصصخم لاصتا فيرعت تافلم ىلإ نييعرشلا نيمدختسملا فيرعت فلم يوتحي ال ،نسحم نيوكت يف DefaultRAGgroup و DefaultWEBvpngGroup ىلع قفاضإلاب .ينوناقلا كيرشلل صصخم ممداخ نيوكت يأ ىلع نايضارتفالا ليصوتلا فيرعت تافلم ىلع ةلوهسب فرعتلا نم نيمجاهملا تاعومجملا عامسأ قلازا عنمت ،كلذ ىلإ وأ RQDN ىلإ لقنتلا دنع قلدسنملا ةيؤرلا ةيناكما قلازا قيرط نع قصصخملا اليصوتلا اونع

# ةلص تاذ تامولعم

<u>Cisco نم تاليزنتلاو ينفلا معدلا</u>

<u>رورملا ةملك ذاذر تامجه</u>

<u>2023 ربمتبس ەب حرصملاا ريغ لوصول لە قېنمألاا تارغثا ا</u>

<u>ASA نيوكت ةلدأ</u>

<u>FMC / FDM نيوكت ةلدأ</u>

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما