

ممت فTD لى RAPN ل صصخم ذفنم نيوكت FMC ةطساوب هترادإ

تايوتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[تانويوتلا](#)

[AnyConnect ل SSL/DTLS ذفنم ريغت](#)

[AnyConnect ل IKEv2 ذفنم ريغت](#)

[ةحصلا نمققحتلا](#)

[اهجالصاواطخألا فاشكتسا](#)

ةمدقملا

لىل AnyConnect IKEv2 و SSL ل صصخملا ذفنملا نيوكت ءارجإ دننتملا اذه فصوي
FMC ةطساوب هترادإ ممت يذلا (FTD) FirePOWER Threat Defense.

ةيساسألا تابلطتملا

تابلطتملا

ةيلال عيضاوملاب ةفرعم كيذل نوكت ناب Cisco ي صوت:

- (RAVPN) دعب نع لوصولل VPN ةكبشل يساسألا مهفلا
- FirePOWER (FMC) ةرادإ زكرم ةبجرت

ةمدختسملا تانوكملا

ةيلال ةيداملا تانوكملا و اجماربلا تارادصإ لىل دننتملا اذه يف ةدراولا تامولعمل دننست:

- Cisco FTD - 7.6
- Cisco FMC - 7.6
- Windows 10 ليغشتلا ماظن

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ءزهجال نم دننتملا اذه يف ةدراولا تامولعمل ءاشنإ مت
تناك اذإ. (يضاوتفا) حوسمم نيوكتب دننتملا اذه يف ةمدختسملا ءزهجال عيمج تادب
رمأ يال لمتمحمل ريثأتلل كمهف نم دكأتف، ليغشتلا ديقتك تبش.

تانويوتلا

SSL/DTLS ل AnyConnect ذفنم ريغت

1. ةيلال دعب نع لوصول ةسايس ريغتو دعب نع لوصول > VPN > ةزهجالا لىل لقتنا.
2. مقرر DTLS و بول لىل لوصول ذفنم مقرر ريغت ب مقرر لوصول تاهجاو مسق لىل لقتنا. كرايتخ نم ذفنم لىل SSL تاداع لفسا ذفنم ل.

SSL Settings

Web Access Port Number:*	<input type="text" value="444"/>
DTLS Port Number:*	<input type="text" value="444"/>

ذفنم ريغت SSL و DTLS ل AnyConnect

3. نيوكتال ظفح.

IKEv2 ل AnyConnect ذفنم ريغت

1. ةيلال دعب نع لوصول ةسايس ريغتو دعب نع لوصول > VPN > ةزهجالا لىل لقتنا.
2. ريغت ب مقرر. ريغتال طئارخ > IPsec لىل لقتنا م مدمقت تارايتخ مسق لىل لقتنا. هديرت يذال ذفنم لىل ذفنم ل ريغتو جهنل.

The screenshot displays the 'Edit Crypto Map' configuration page for the 'FTD-HA-OUTSIDE' interface group. The 'Advanced' tab is active, showing the 'Crypto Maps' section. The 'IKEv2 IPsec Proposals' list contains 'AES-GCM'. The 'Enable Reverse Route Injection' and 'Enable Client Services' options are checked. The 'Port' is set to 444. The 'Modulus Group' is set to 14. The 'Lifetime Duration' is set to 28800 seconds. The 'Lifetime Size' is set to 4608000 Kbytes. The 'Enable Perfect Forward Secrecy' option is unchecked. The 'RRI' checkbox is checked.

ذفنم ريغت IKEv2 ل AnyConnect

3. رشنل او نيوكتال ظفح مقرر.

ظحال AnyConnect Client فيرعت تافل م عم صصخملا ذفنملا مادختسا دنع :ةظحالم
X.X.X.X:Port ذفنم يلع يوتحي نأ بجي مداوخللا ةمئاق ي فيضملا ناو نع ل قح نأ
ل.الصتال (192.168.50.5:444)

ةحصلا نم ققحتلا

1. show run webVPN و show run crypto ikev2 رم اوأ مادختساب نيوكتل نم ققحتلا نكمي ،رشنلا دع ب .

```
<#root>
```

```
>
```

```
show run webvpn
```

```
webvpn
```

```
port 444 <----- Custom Port that has been configured for SSL
```

```
enable outside
```

```
dtls port 444 <----- Custom Port that has been configured for DTLS
```

```
http-headers
```

```
  hsts-server  
  enable
```

```
  max-age 31536000  
  include-sub-domains  
  no preload
```

```
hsts-client  
  enable
```

```
x-content-type-options
```

```
x-xss-protection
```

```
content-security-policy
```

```
anyconnect image disk0:/csm/cisco-secure-client-win-X.X.X.X-webdeploy-k9.pkg 1 regex "Windows"
```

```
anyconnect enable
```

```
tunnel-group-list enable
```

```
cache
```

```
  disable
```

```
error-recovery disable
```

```
<#root>
```

```
>
```

```
show run crypto ikev2
```

```
crypto ikev2 policy 10
```

```
  encryption aes-gcm-256 aes-gcm-192 aes-gcm
```

```
  integrity null
```

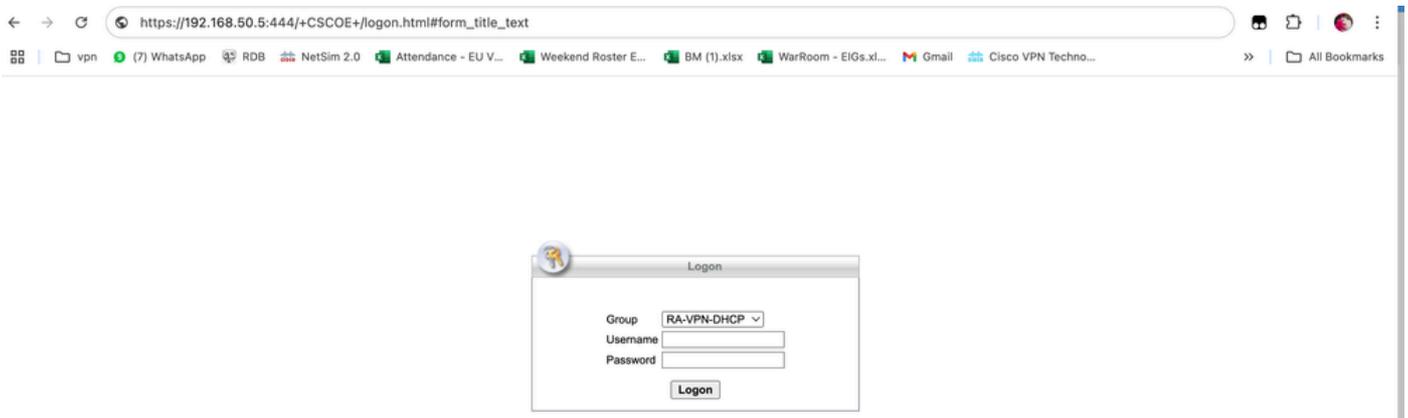
```
  group 21 20 19 16 15 14
```

```
  prf sha512 sha384 sha256 sha
```

```
  lifetime seconds 86400
```

```
crypto ikev2 enable outside client-services port 444 <----- Custom Port configured for IKEv2 Client Serv
```

2. دوزم ال AnyConnect قی ب ط ت / ضرعت س م ال نم دعب نع لوصول ال ال لوصول ال لال خ نم ققحت .
ص ص خ م ذ ف نم ب :



ص ص خ م ال ذ ف نم ال م اد خ ت س اب AnyConnect ال لوصول ال لال خ نم ققحت ال

اهحال صإو ءاطخأل ا فاشك تس ا

- تامدخال ا ف دع ب نع لوصول ا ن ا وكت ا ف مدخت س م ل ا ذفن م ل ا مادخت س ا مدع ن م دك أ ت ا
ا ا ا ا ا ا ا a
- طس و تم ءا ا ا ا و ا isp ب ا ن ا م ل ا ع ن م ا ا ن ا ن ا م ض .
- ت ن ا ك ا ا م و ء ا م ا ل ا ر ا ا ا ا ل ا ل ص ت م ز ا ل ا ت ن ا ك ا ا ا م ق ق ا ل ل FTD ا ل ع ط ا ق ت ل ا ن ك م ا ا
ا ل م ا ل ا س ر ا ل ا ا ا ا ا ا ا ا ا ا a

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إل دن تسمل