

FTD ىل ع ةددعتمل تاداهشل ةقداصم نيوكت RAPN ل

تايوتحمل

[ةمدقملا](#)

[ةيساسالاب لطلتلا](#)

[تاب لطلتلا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسا تامولعم](#)

[تان نيوكتلا](#)

[FTD ىل ع نيوكتلا](#)

[مدختسملا زاهج ىل ع ةدوجوملا تاداهشلا](#)

[ةحصلاب نم ققحتلا](#)

[اهجالصا وءاطخالا فاشكتسا](#)

ةمدقملا

نع عافدلا" ي ف نم آ لي عمل ةددعتمل تاداهشل ةقداصم مادختسا عارجا دننتملا اذه فص ي FMC ةطساوب هترادإ متت يذلا " (FTD) FirePOWER ديدهت

ةيساسالاب لطلتلا

تاب لطلتلا

ةيلاتلا عيضاوملاب ةفرعم كي دل نوكت ناب Cisco ي صوت:

- (RAVPN) دع ب نع لوصول VPN ةكبشل يساسالاب مهفلا
- FirePOWER (FMC) ةرادا زكرم ةبرجت
- X509 تاداهشب ةيساسا ةفرعم

ةمدختسملا تانوكملا

ةيلاتلا ةيدامل تانوكملا وجوماربل تارادصا ىل دننتملا اذه ي ف ةدراول تامولعمل دننست:

- Cisco FTD - 7.6
- Cisco FMC - 7.6
- Cisco Secure Client 5.1.4.74 عم Windows 11

ةصاخ ةيلمعم ةئي ب ي ف ةدوجوملا ةزهجالا نم دننتملا اذه ي ف ةدراول تامولعمل عاشنإ مت تناك اذا. (يضا رتفا) حوسمم نيوكتب دننتملا اذه ي ف ةمدختسملا ةزهجالا عيمج تأدب رمأ يال لم تحمل ريثأتلل كمهف نم دكأتف ،ليغشتلا دي قكتكبش

ةيساسأ تامولعم

هنا ينعى امم ،ةداهشلا ىلإ ةدنتسملا ةيداحألا ةقداصملا FTD معدي ،7.0 جم انربلا رادصإ لبقي دحاو لاصتا ةلواحمل ،امهيلك سيل نكلو زاهجل وأ مدختسملا ةقداصم نكمي

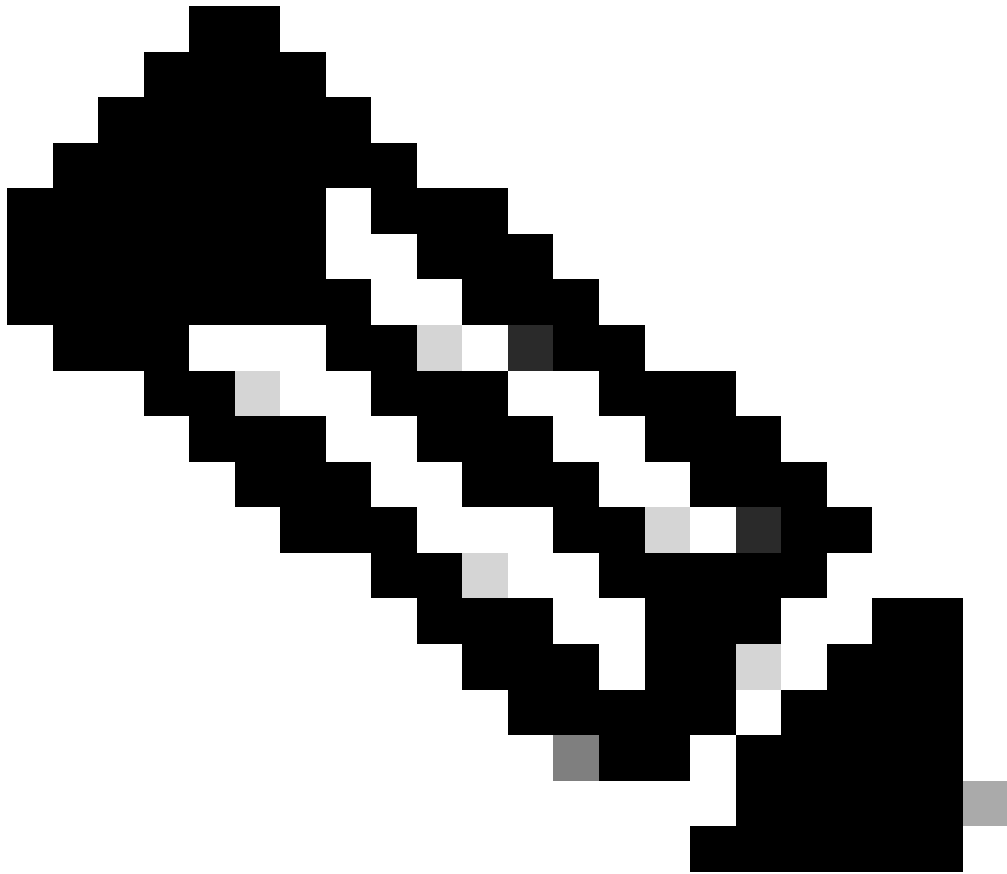
ةداهش ءحص نم ققحتلا ةيناكلما تاداهشلا ىلإ ةدنتسملا ةددعتملا ةقداصملا حيتت ىلإ ةفاضلإاب ،ةكرشلا نع رداص زاهج وه زاهجل نأ نامضل ،زاهجل وأ زاهجل ىلع ديهتلا Secure ةلحرم مادختساب VPN لوصوب حامسلل نيمدختسملا ةي وه ةداهش ةقداصم ClientDuring SSL أو IKEv2 EAP.

Secure ريشي نأ بجي .نيتنثإ ىلإ تاداهشلا ددع ايلاح ةددعتملا تاداهشلا ةقداصم ددحت ةباوبلا مدختست ذئدنعف ،لاحلا وه اذه نكي مل اذا .ةددعتم تاداهش ةقداصم معد ىلإ Client أو Secure ClientVersion 4.4.04030 معدي .لاصتالا يف لشفت وأ ةميدقلا ةقداصملا قرط يدحإ .تاداهش ةدع ىلإ ةدنتسملا ةقداصملا ثدحأ رادصإ

تانويكتلا

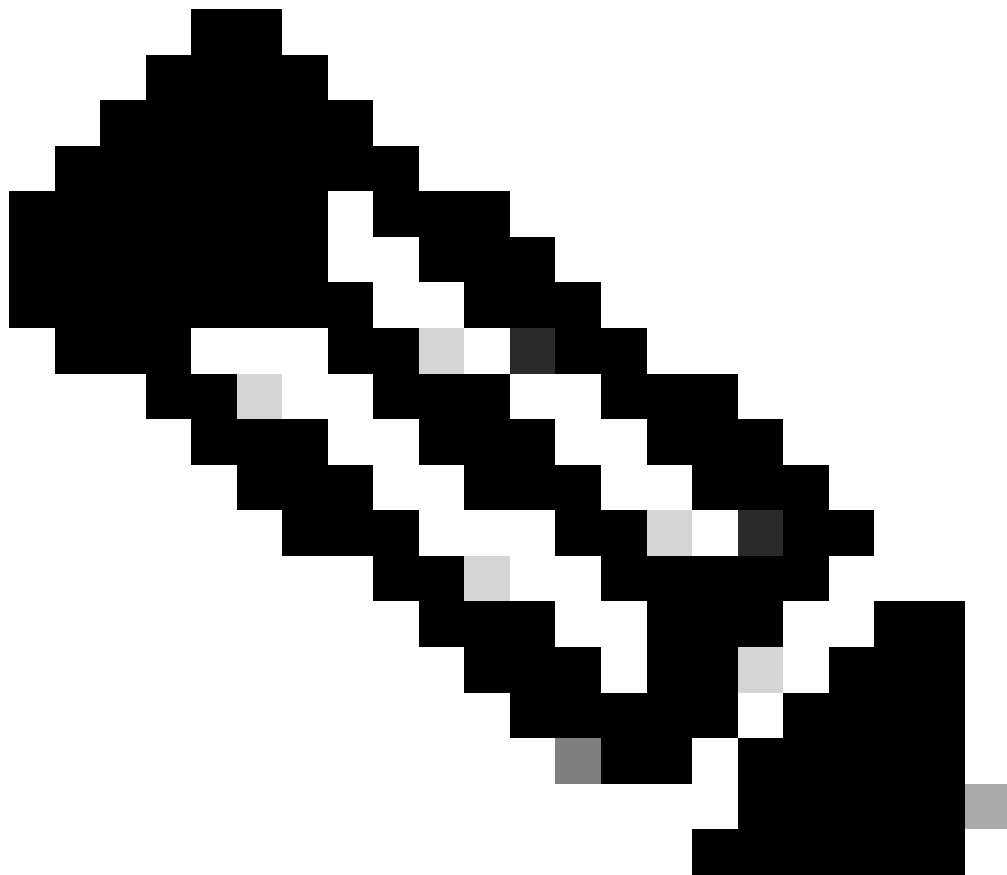
FTD ىلع نيوكتلا

1. دعب نع لوصول > VPN > ةزهجألا ىلإ لقتنا .
2. ريحت قوف رقتاو دعب نع لوصول VPN جهن ددح .



ةفاضا قوف رقنا ف ،دع ب نع لوصولل VPN ةكبش نيوكتب مقت مل اذا :ةطحالم
ديج دع ب نع لوصولل VPN ةكبش جهن ءاشنإل

-
3. ةددعتم تاداهش ةقداصم نيوكتل اذه ررحوليصوت فيصوت ددح.
 4. & ليمع ةداهش وأ طقف ليمع ةداهشك ةقداصم لا بولسأ رتخاو AAA تادادعإ ىلع رقنا AAA.



ليعمل الةءاهش ةقءاصم ةقيرط ءءء ءنك اءا ةقءاصم ال مءاخ ءء: ةظءالم
AAA. ةقءاصم و

5. ةءءءم ال ءاءاهش ال ةقءاصم نئك مء راءءءال ال ةءاخ ءء.

6. لئعمل ال ةءاهش نم مءءءسم ال مسا نئئئءل ءاءاهش ال ءءء رءءا:

- زاهء ال ةءاهش نم مءءءسم ال مسا نئئئءل راءءل ال ءء ءء — ءل وائل ةءاهش ال
VPN. لئعمل نم ةلسرم ال
- مءءءسم ال ةءاهش نم مءءءسم ال مسا نئئئءل راءءل ال ءء ءء — ةئءائل ةءاهش ال
لئعمل ال نم ةلسرم ال.

لمع ةسلء مءءءسم مساك لئعمل ال نم هل اسرل مء ءءل مءءءسم ال مسا مءءءسم ال مءئ
ضئ وءءل ال ةقءاصم ال نئك مءئ مءئ امءع. طقق ةءاهش ال ةقءاصم نئك مءئ ءن VPN
راءءل ال VPN ةكبش ةسلء مءءءسم ال مسا مءءئ، ةءاهش ال ةقءاصم و (AAA) ةبسءم ال و
ةقءاصم ال ةئءل.

7. ةءاهش نم مءءءسم ال مسا نمضئئ ءءل و، ءءم نئئئءل لقق راءء ءئءءب ءمق اءا.
مسال: ةئضارءال ال مئق ال ناضرئئ وئءائل وئسأس ال نئل لقق ال نإف، لئعمل

يلاوتلا ىلع (OU) ةيمىظنتلا ةدحولو (CN) عئاشلا

Connection Profile:*	RA-VPN-Multi-Cert
Group Policy:*	RAVPN-Multi-Cert-GP +
Edit Group Policy	
Client Address Assignment	AAA Aliases

Authentication

Authentication Method: Client Certificate Only

☒ Enable multiple certificate authentication

▼ Map username from client certificate

☒ Map specific field

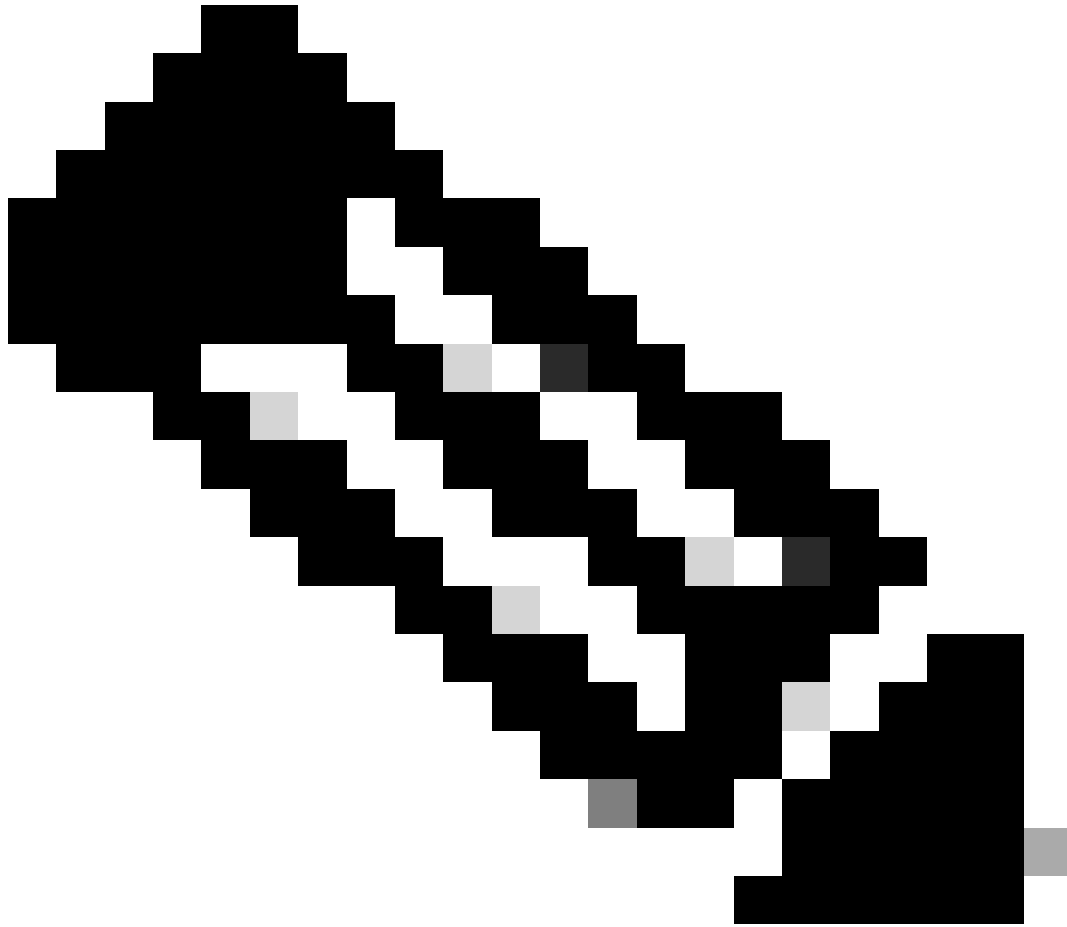
Primary Field:	Secondary Field:
CN (Common Name)	OU (Organisational Unit)

☐ Use entire DN (Distinguished Name) as username

Certificate to choose: Second Certificate

ليصوتلا فيصوتل AAA تادادع

ماظنلا نإف ،مدختسم مساك (DN) لماكلا ب زيمملا مسالا مادختسا راىخ ديدحتب تمق اذا 8. ةدرفنم لوقح نم نوكم ،ديرف فيرعت وه زيمملا مسالا .ايئاقلت مدختسملا ةي وه عجرتسي مادختسا متي .لاصتا فيرعت فلمل ني مدختسملا ةقباطم دنع فرعمك اهمادختسا نكمي .ةنحرملا ةداهشلا ةقداصلم DN دعاوق



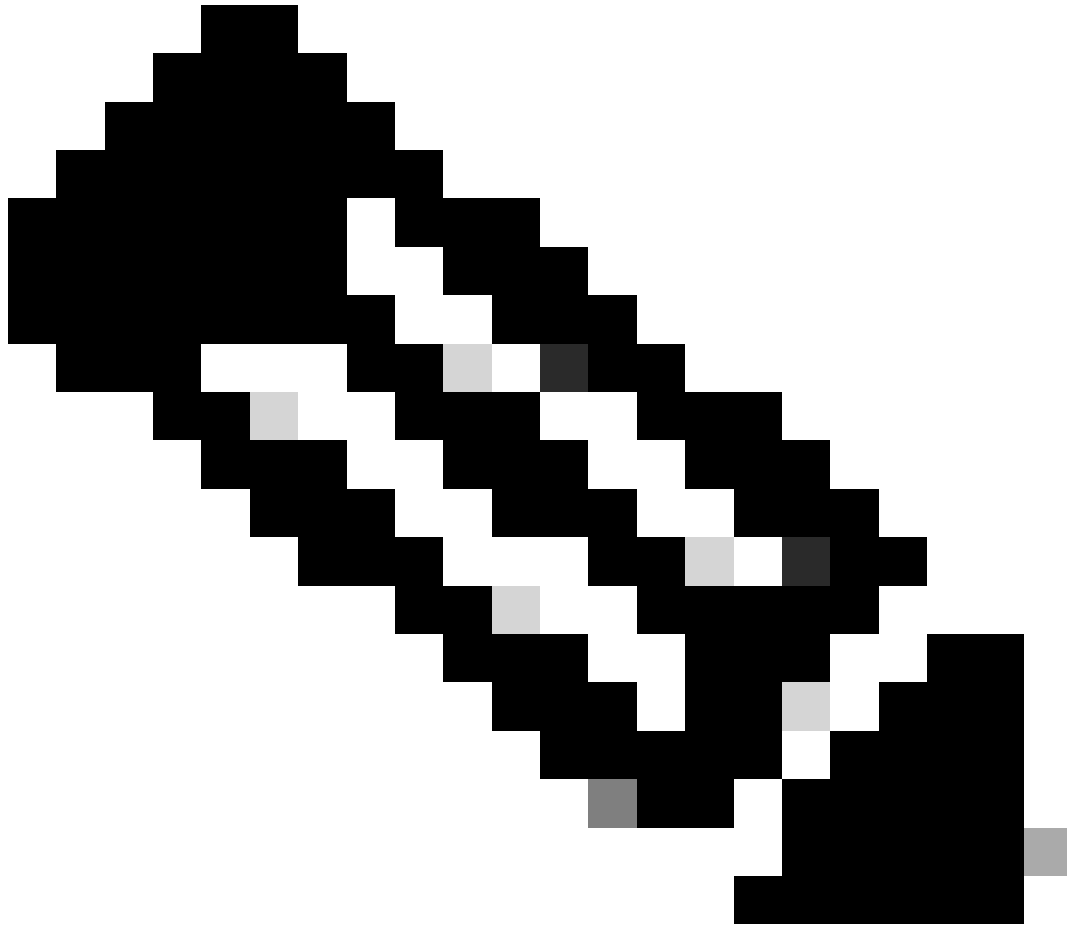
مسا راڤيخ ددح ف AAA، ةقداصم و ليمعلا ةداهش ةقداصم ديدحتب تمق اذا :ةظحال م
مسا علمل مدختسمال لوخد ليجست ةذفان في ةدوجومال ةداهشال نم ةئدابل مدختسم
VPN ةدحو ربع مدختسمال لصتي امدنع ليمعلا ةداهش نم اقبس م يوناتال مدختسمال
Cisco Secure Client نم نمآال ليمعلا ةصاخال

أبع م يوناتال مدختسمال مسا :لوخدال ليجست ةذفان في مدختسمال مسا ءافخ
مدختسمال موقاي ال ثيح مدختسمال فيفخم هنكلو ،ليمعلا ةداهش نم اقبس م
اقبس م أبعمال مدختسمال مسا ليدعتب

9. [دعب نع لوصولل VPN ةكبش نيوكت](#) ىلا عجرا ،رخآ يلي صفت نيوكت ىلع لوصحلل
[FTD ىلع \(AnyConnect\) نمآال ليمعلا](#)

10. FTD ىلا زاهجال نزخم ةداهش و مدختسمال نزخم ةداهشب ةصاخال CA تاداهش ليمحتب مق
مدختسمال نزخم ةداهش عيقوت متي ،ويرانيسال اذه في هنأ امب .حاجنب ةحصلال نم ققحتلل
دحاولا قدصمال عجرمال نأ تبثي امم ،هسفن قدصمال عجرمال ةطساوب زاهجال نزخم ةداهش و
فلتخم قدصم عجرم نم ةعقوم زاهجال نيزخت ةداهش و مدختسمال نيزخت ةداهش تناك اذا .فاك
FTD ىلا قدصمال عجرمال يتداهش نم لك ليمحتب جي في

- Issued By :
 - CN : IdenTrust Commercial Root CA 1
 - O : IdenTrust
 - C : US
- Issued To :
 - CN : HydrantID Server CA O1
 - OU : HydrantID Trusted Certificate Service
 - O : IdenTrust
 - C : US
- Public Key Type : RSA (2048 bits)
- Signature Algorithm : RSA-SHA256
- Associated Trustpoints : ftdha HydrantID-Server-CA-O1
- Valid From : 16:56:15 UTC December 12 2019
- Valid To : 16:56:15 UTC December 12 2029



نعم CertificateStore إلى AnyConnect ليمع فيرعت فلم يوتحي نأ بجي:ةظحالم
يدل نكي مل اذا true إلى CertificateStoreOverride نيعت متي نأولكل إلى
لوؤسمال قوقح مدختسمال.

مدختسمال زاهج إلى ةدوجومال تاداهشال

إلى اذه لاصلتال فيرعت فلمب هليصوت ضررتفي يذال مدختسمال زاهج يوتحي نأ بجي
زاهجال نزخمو مدختسمال نزخم في ةتبثم ةحلاص تاداهش.

مدختسمال نزخم نم ةداهش:

General

Details

Certification Path

**Certificate Information****This certificate is intended for the following purpose(s):**

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.23.140.1.2.2
- 2.16.840.1.113839.0.6.3

Issued to: client.cisco.com**Issued by:** HydrantID Server CA O1**Valid from** 18/03/2025 **to** 18/03/2026

You have a private key that corresponds to this certificate.

Issuer Statement

OK

مدخستسمال نزخم ةداهش

ةزهجال نزخم نم ةداهشال



Certificate



General

Details

Certification Path



Certificate Information

This certificate is intended for the following purpose(s):

- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- 2.23.140.1.2.2
- 2.16.840.1.113839.0.6.3

Issued to: machine.cisco.com

Issued by: HydrantID Server CA O1

Valid from 18/03/2025 **to** 18/03/2026



You have a private key that corresponds to this certificate.

Issuer Statement

OK

زاهجلا نيزخت ةداهش

ةحصللا نم ققحتلا

FTD: بة صااا (CLI) رماوااا رطسا ةهجاو نم لاصتااا فبرعا فلما نفاوكت نم ققحاااا 1.

<#root>

```
firepower# show run tunnel-group
tunnel-group RA-VPN-Multi-Cert type remote-access
tunnel-group RA-VPN-Multi-Cert general-attributes
  address-pool RAVPN-MultiCert-Pool
  default-group-policy RAVPN-Multi-Cert-GP
tunnel-group RA-VPN-Multi-Cert webvpn-attributes
```

authentication multiple-certificate

group-alias RAVPN-MultiCert enable

لصاصااا نم ققحاااا رماوااا ااا ااا ففنااا مق 2:

<#root>

```
firepower# show vpn-sessiondb detail anyconnect
```

Session Type: AnyConnect Detailed

Username : client.cisco.com

```
      Index      : 28
Assigned IP   : 192.168.13.1      Public IP   : 10.106.56.89
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256
Hashing      : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384
Bytes Tx     : 19324              Bytes Rx    : 134555
Pkts Tx     : 2                  Pkts Rx    : 1379
Pkts Tx Drop : 0                 Pkts Rx Drop : 0
Group Policy : RAVPN-Multi-Cert-GP Tunnel Group : RA-VPN-Multi-Cert
Login Time   : 07:18:53 UTC Wed Mar 19 2025
Duration     : 0h:21m:00s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A              VLAN        : none
Audt Sess ID : 0a6a43590001c00067da6fdd
Security Grp : none              Tunnel Zone  : 0
```

AnyConnect-Parent Tunnels: 1

SSL-Tunnel Tunnels: 1

DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 28.1

Public IP : 10.106.56.89

Encryption : none

TCP Src Port : 53927

Hashing : none

TCP Dst Port : 443

Auth Mode : Multiple-certificate

Idle Time Out: 30 Minutes Idle TO Left : 9 Minutes
Client OS : win
Client OS Ver: 10.0.22000
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74
Bytes Tx : 11581 Bytes Rx : 224
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 28.2
Assigned IP : 192.168.13.1 Public IP : 10.106.56.89
Encryption : AES-GCM-128 Hashing : SHA256
Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 53937
TCP Dst Port : 443

Auth Mode : Multiple-certificate

Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74
Bytes Tx : 7743 Bytes Rx : 240
Pkts Tx : 1 Pkts Rx : 3
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:

Tunnel ID : 28.3
Assigned IP : 192.168.13.1 Public IP : 10.106.56.89
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 62975
UDP Dst Port : 443

Auth Mode : Multiple-certificate

Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74
Bytes Tx : 0 Bytes Rx : 134091
Pkts Tx : 0 Pkts Rx : 1376
Pkts Tx Drop : 0 Pkts Rx Drop : 0

مدختسمال نزخم ةداهش نم هدادرتسا مت يذل client.cisco.comيسا مدختسمال مسا ديدحت متي ةداهشال" ديدحت ةلاح في AAA مسق في ةيناثال ةداهشال نم ةطي رخلل مدختسم مساك machine.cisco.com. هو "زاهجال نزخم" ةداهش نم مدختسمال مسا دادرتسا متي ،"ىلوال

اهجال صا وءاطخال فاشكتسا

1. زاهجال تاداهش نزخم و مدختسمال تاداهش نزخم في ةحالص تاداهش دوجو نم دكأت .
2. ةحص نم ققحتلاب ةقلعتمال تالچسمل صحتل FTD لىل ءاطخال حيحصت عي مجتب مق .
14. debug crypto ca مءدختساب ةداهشال

3. مَدْخُتْ سَمَلَا زَاهَجْ نَمِ DART عَجْجَارِمِ.

لَمْعَلَا وَيِرَانِيَسْ نَمِ DART تَالْحَسْ:

<#root>

Date : 03/19/2025
Time : 00:18:50
Type : Information
Source : csc_vpnapi

Description : Function: ConnectMgr::processResponseStringFromSG
File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\Api\ConnectMgr.cpp
Line: 12100

[MCA] Multiple client cert auth requested by peer (via AggAuth)

Date : 03/19/2025
Time : 00:18:50
Type : Information
Source : csc_vpnapi

Description : Function: ConnectMgr::nextClientCert
File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\Api\ConnectMgr.cpp
Line: 6774
Subject Name: C=US, ST=California, L=San Jose, O=Cisco Systems Inc.,

CN=machine.cisco.com

Issuer Name : C=US, O=IdenTrust, OU=HydrantID Trusted Certificate Service, CN=HydrantID Server CA 01
Store : Microsoft Machine

Date : 03/19/2025
Time : 00:18:50
Type : Information
Source : csc_vpnapi

Description : Function: CTransportCurlStatic::ClientCertRequestCB
File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\Api\CTransportCurlStatic.cpp
Line: 1358

Using client cert: /C=US/ST=California/L=San Jose/O=Cisco Systems Inc./CN=machine.cisco.com

Date : 03/19/2025
Time : 00:18:51
Type : Information

Source : csc_vpnapi

Description : Function: ConnectMgr::processResponseStringFromSG

File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\Api\ConnectMgr.cpp

Line: 12105

[MCA] Client certificate accepted at protocol level

Date : 03/19/2025

Time : 00:18:51

Type : Information

Source : csc_vpnapi

Description : Function: ConnectMgr::processResponseStringFromSG

File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\Api\ConnectMgr.cpp

Line: 12124

[MCA] Received and successfully parsed Multiple Certificate Authentication request from secure gateway.

Date : 03/19/2025

Time : 00:18:51

Type : Information

Source : csc_vpnapi

Description : Function: ConnectMgr::nextClientCert

File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\Api\ConnectMgr.cpp

Line: 6774

Subject Name: C=US, ST=California, L=San Jose, O=Cisco Systems Inc.,

CN=client.cisco.com

Issuer Name : C=US, O=IdenTrust, OU=HydrantID Trusted Certificate Service, CN=HydrantID Server CA 01

Store : Microsoft User

Date : 03/19/2025

Time : 00:18:51

Type : Information

Source : csc_vpnapi

Description : Function: ConnectMgr::processIfcData

File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\Api\ConnectMgr.cpp

Line: 4129

[MCA] Second certificate for Multiple Certificate Authentication found - now sending 2nd certificate to

Date : 03/19/2025

Time : 00:18:51

Type : Information

Source : csc_vpnapi

Description : Function: ConnectMgr::userResponse

File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\Api\ConnectMgr.cpp

Line: 1690
Processing user response.

Date : 03/19/2025
Time : 00:18:52
Type : Information
Source : csc_vpnapi

Description : Function: ConnectMgr::createMultiCertAuthReplyXML
File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\Api\ConnectMgr.cpp
Line: 17127

[MCA] Successfully signed Multiple Certificate Authentication data with 2nd certificate

Date : 03/19/2025
Time : 00:18:52
Type : Information
Source : csc_vpnapi

Description : Function: ConnectMgr::sendResponse
File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\Api\ConnectMgr.cpp
Line: 6522

[MCA] Multiple Certificate Authentication response ready to send to secure gateway

Date : 03/19/2025
Time : 00:18:52
Type : Information
Source : csc_vpnapi

Description : Message type prompt sent to the user:
Your client certificate will be used for authentication

Date : 03/19/2025
Time : 00:18:53
Type : Information
Source : csc_vpnapi

Description : Function: CVpnApiShim::SaveUserPrompt
File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\ApiShim\ApiShim.cpp
Line: 3538

User submitted response for host ftdha.cisco.com and tunnel group: RAVPN-MultiCert

Date : 03/19/2025
Time : 00:18:53
Type : Information
Source : csc_vpnapi

Description : Function: ConnectMgr::userResponse
File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\Api\ConnectMgr.cpp
Line: 1690
Processing user response.

Date : 03/19/2025
Time : 00:18:53
Type : Information
Source : csc_vpnapi

Description : Function: ConnectMgr::processIfcData
File: C:\temp\build\thehoff\Raccoon_MR40.765445939442\Raccoon_MR4\vpn\Api\ConnectMgr.cpp
Line: 3815

Authentication succeeded

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م 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 د ن ت س م ل ا