

ي ق فن ل ل ا ص ت ا ن ي و ك ت ي ك ي م ا ن ي د ل ا م ي س ق ت ل ل

ت ا ي و ت ح م ل ا

[ة م د ق م ل ا](#)

[ة ي س ا س ا 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 ا س ا ت ا م و ل ع م](#)

[ن ي و ك ت ل ا](#)

[ة ك ب ش ل ل ي ط ي ط خ ت ل ا م س ر ل ا](#)

[ة ص ص خ م ل ا A n y C o n n e c t ت ا م س ا ع ا ش ن ا . 1 ة و ط خ ل ا](#)

[م ي ق ل ا ن ي و ك ت و ص ص خ م ل ا A n y C o n n e c t م س ا ع ا ش ن ا . 2 ة و ط خ ل ا](#)

[ة ع و م ح م ل ا ح م ت ي ل ا م س ا ل ا و ع و ن ل ا ة ف ا ض ا . 3 ة و ط خ ل ا](#)

[ل ا ث م ل ي ك ش ت C L I](#)

[د و ي ق ل ا](#)

[ة ح ص ل ا ن م ق ق ح ت ل ا](#)

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

[م ي ق ل ا ل ق ح ي ف ل د ل ا ف ر ح م ا د خ ت س ا ة ل ا ح ي ف](#)

[ا س م ل ا ل ي ص ا ف ت ب ي و ب ت ل ا ة م ا ل ع ي ف ة ن م ا ل ا ر ي غ ت ا ر ا س م ل ا ة ي ف ر م د ع ة ل ا ح ي ف](#)

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

[ة ل ص ت ا ذ ت ا م و ل ع م](#)

ة م د ق م ل ا

ي ق فن ل ل ا ص ت ا ل ل A n y C o n n e c t S e c u r e M o b i l i t y C l i e n t ن ي و ك ت ة ي ف ي ك د ن ت س م ل ا ا ذ ه ح ض و ي
A S D M . ر ب ع ي ك ي م ا ن ي د ل ا م ي س ق ت ل ا د ا ع ب ت س ا ب

ة ي س ا س ا 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 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 ا ب C i s c o ي ص و ت:

- A S A ب ة ي س ا س ا ة ف ر ع م
- C i s c o A n y C o n n e c t S e c u r i t y M o b i l i t y C l i e n t ب ة ي س ا س ا ة ف ر ع م

ة م د خ ت س م ل ا ت ا ن و ك م ل ا

ة ي ل ل ا ل ا ح م ا ر ب ل ا ت ا ر ا د ص ا ي ل ا 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 د ن ت س ت

- ASA 9.12(3)9
- Adaptive Security Device Manager (ASDM) 7.13(1)
- AnyConnect 4.7.0

ةصاخ ةي لمعم ةئي ب ي ف ةدوجوم ل ةزهجأ ل نم دنتس م ل اذ ه ي ف ةدراول تامول عم ل ءاشن إ م ت ت ن ا ك ا ذ ا . (يضا رت ف ا) حوس م م نيوك ت ب دنتس م ل اذ ه ي ف ةمدختس م ل ةزهجأ ل ءي م ج ت ا د ب رم أ ي أ ل م ت ح م ل ر ي ث ا ت ل ل ك م ه ف ن م د ك ا ت ف ، ل ي غ ش ت ل د ي ق ك ت ك ب ش

ةي س ا س ا تامول عم

Cisco AnyConnect Secure Mobility Client ل مسقن م ل ي ق ف ن ل AnyConnect ل اص ت ا ح ي ت ي (SSL) ةن م أ ل ل ي ص و ت ل ا ذ خ أ م ة ق ب ط و أ IKEV2 ر ب ع ة ك ر ش ل ا دراوم ي ل ا ن م أ ل ل و ص و ل ا

ن ا م أ ل ز ا ه ج ي ل ع ا ه ن ي و ك ت م ت ي ت ل ا ة س ا ي س ل ا ي ل ا ا د ا ن ت س ا و ، AnyConnect 4.5 ر ا د ص ا ل ب ق و أ Tunnel All ق ف ن د ي د ح ت و أ م ي س ق ت ل ا ق ف ن ك و ل س د ي د ح ت ن ك م ي ، (ASA) ف ي ك ت ل ل ل ب ا ق ل ل Exclude Specified د ا ع ب ت س ا ل ا

IP ن ا و ن ع ي ل ا ت ا م د خ ل ل ح ا ن ا ي ح أ م ت ي ، ة ب ا ح س ل ا ي ل ع ة ف ا ض ت س م ل ر ت و ي ب م ك ل ا دراوم ر و ه ظ ع م ي ل ع ة ف ا ض ت س م ل ا دراوم ل م ح ي ل ا ا د ا ن ت س ا و أ م د خ ت س م ل ا ع ق و م ي ل ا ا د ا ن ت س ا ف ل ت خ م ة ب ا ح س ل ا .

ة ك ب ش ل ا ق ا ط ن ي ل ا ة م س ق م ت ا و ن ق ء ا ش ن إ ر ف و ي AnyConnect Secure Mobility Client ن أ ل ا ر ط ن ة ك ب ش ل ا ي ل و و س م ل ب ع ص ل ا ن م ح ب ص ي ، IPv6 و أ IPv4 ع م ج ت و أ ف ي ض م و أ ة ت ب ا ث ل ا ء ي ع ر ف ل ا AnyConnect ن ي و ك ت ء ا ن ث ا FQDNs / ت ا ل ا ج م ل ا د ا ع ب ت س ا ل ا

م ي س ق ت ق ف ن ن ي و ك ت ن م Cisco.com ل ا ج م د ا ع ب ت س ا ل ة ك ب ش ل و و س م د ي ر ي ، ل ا ث م ل ا ل ي ب س ي ل ع ة ب ا ح س ل ا ة ط س ا و ب ف ا ض ت س م ه ن أ ل Cisco.com ل DNS ن ي ي ع ت ر ي غ ت ي ن ك و ل و

AnyConnect م و ق ي ، ي ك ي م ا ن ي د ل ا م ي س ق ت ل ا د ا ع ب ت س ا ب ص ا خ ل ا ي ق ف ن ل ل ا ص ت ا ل ا م ا د خ ت س ا ب ا ر ج ا ب م و ق ي و ف ا ض ت س م ل ا ق ي ب ط ت ل ا ب ص ا خ ل ا IPv4/IPv6 ن ا و ن ع ل ي ك ي م ا ن ي د ل ا ل ح ل ا ب ج ر ا خ ل ا ص ت ا ل ا ء ا ر ج ا ب ح ا م س ل ل ء ي ف ص ت ل ا ل م ا و ع و ه ي ج و ت ل ل ل و د ج ي ف ء ي ر و ر و ض ل ا ت ا ر ي ي غ ت ل ا ق ف ن ل ا .

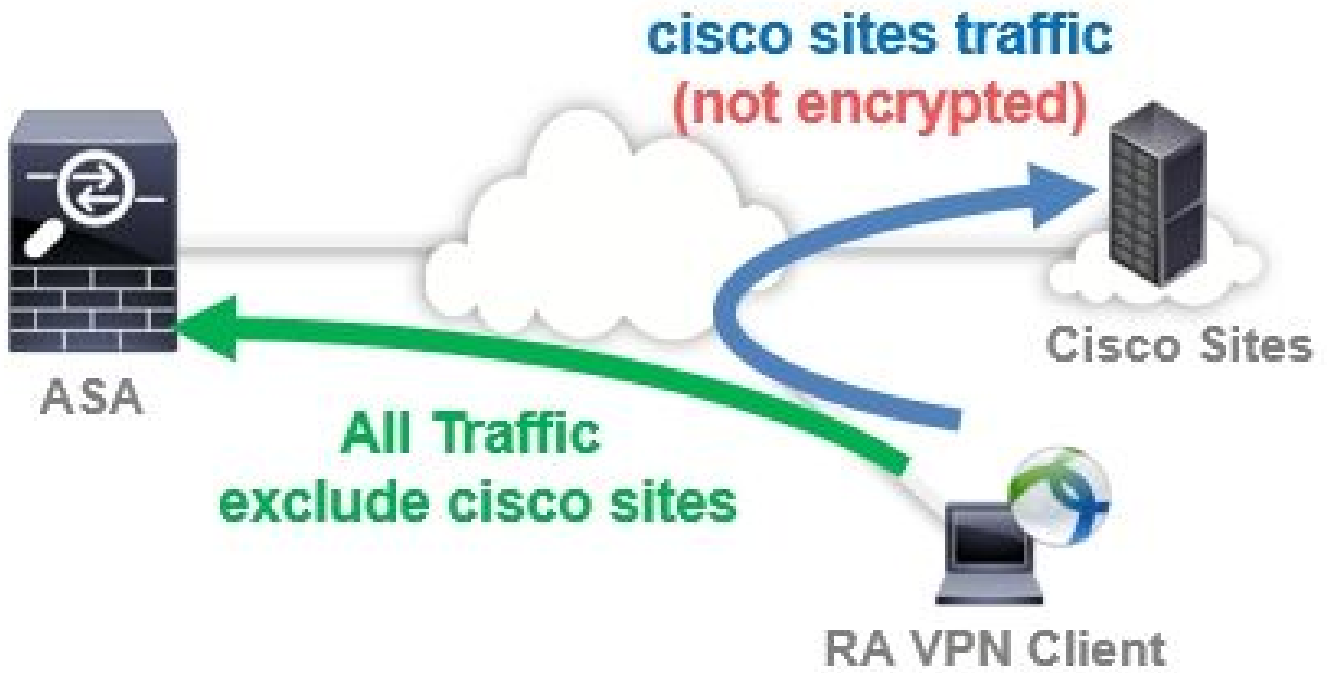
م و ق ي ث ي ح ي ك ي م ا ن ي د ل ا ي ق ف ن ل ا AnyConnect ل ا ص ت ا م ا د خ ت س ا ل ن ك م ي ، AnyConnect 4.5 ن م ا د ب م و ق ي و ف ا ض ت س م ل ا ق ي ب ط ت ل ا ب ص ا خ ل ا IPv4/IPv6 ن ا و ن ع ل ي ك ي م ا ن ي د ل ا ل ح ل ا ب AnyConnect ل ا ص ت ا ل ا ء ا ر ج ا ب ح ا م س ل ل ء ي ف ص ت ل ا ل م ا و ع و ه ي ج و ت ل ل ل و د ج ي ف ء ي ر و ر و ض ل ا ت ا ر ي ي غ ت ل ا ء ا ر ج ا ب ق ف ن ل ا ج ر ا خ

ن ي و ك ت ل ا

ASA ي ل ع Cisco AnyConnect Secure Mobility Client ن ي و ك ت ء ي ف ي ك م س ق ل ا اذ ه ف ص ي

ة ك ب ش ل ل ي ط ي ط خ ت ل ا م س ر ل ا

د ن ت س م ل ا اذ ه ء ل ث م أ ل ه م ا د خ ت س ا م ت ي ي ذ ل ا ط ا ط خ م ل ا ء ر و ص ل ا ه ذ ه ض ر ع ت



ةصصخملا AnyConnect تامس عاشنإ. 1 ةوطخل

يل لقتنا [Configuration > Remote Access VPN > Network \(Client\) Access > Advanced > AnyConnect Custom Attributes](#). يف حضوم وه امك، يرايتخالال فصولاو ةمسلا `dynamic-split-exclude-domains` طبضو، رز Add رقنا ةروصل:

The screenshot shows the Cisco configuration interface. The breadcrumb trail is [Configuration > Remote Access VPN > Network \(Client\) Access > Advanced > AnyConnect Custom Attributes](#). The main content area shows a table with one entry:

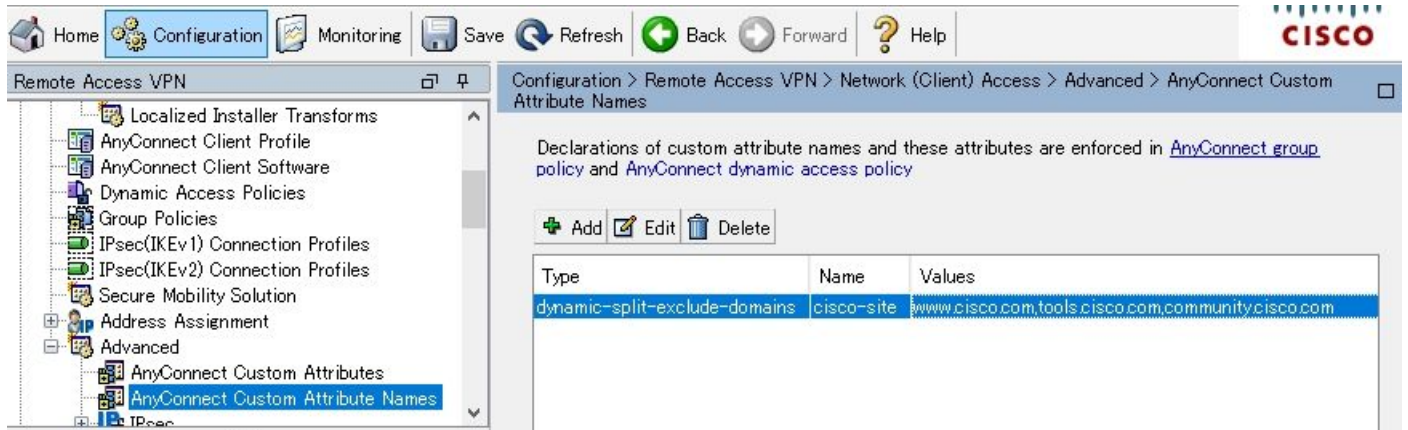
Type	Description
<code>dynamic-split-exclude-domains</code>	Dynamic Split Tunneling

ميقلل نيوكت و صصخملا AnyConnect مس عاشنإ. 2 ةوطخل

يل لقتنا [Configuration > Remote Access VPN > Network \(Client\) Access > Advanced > AnyConnect Custom Attribute Names](#).

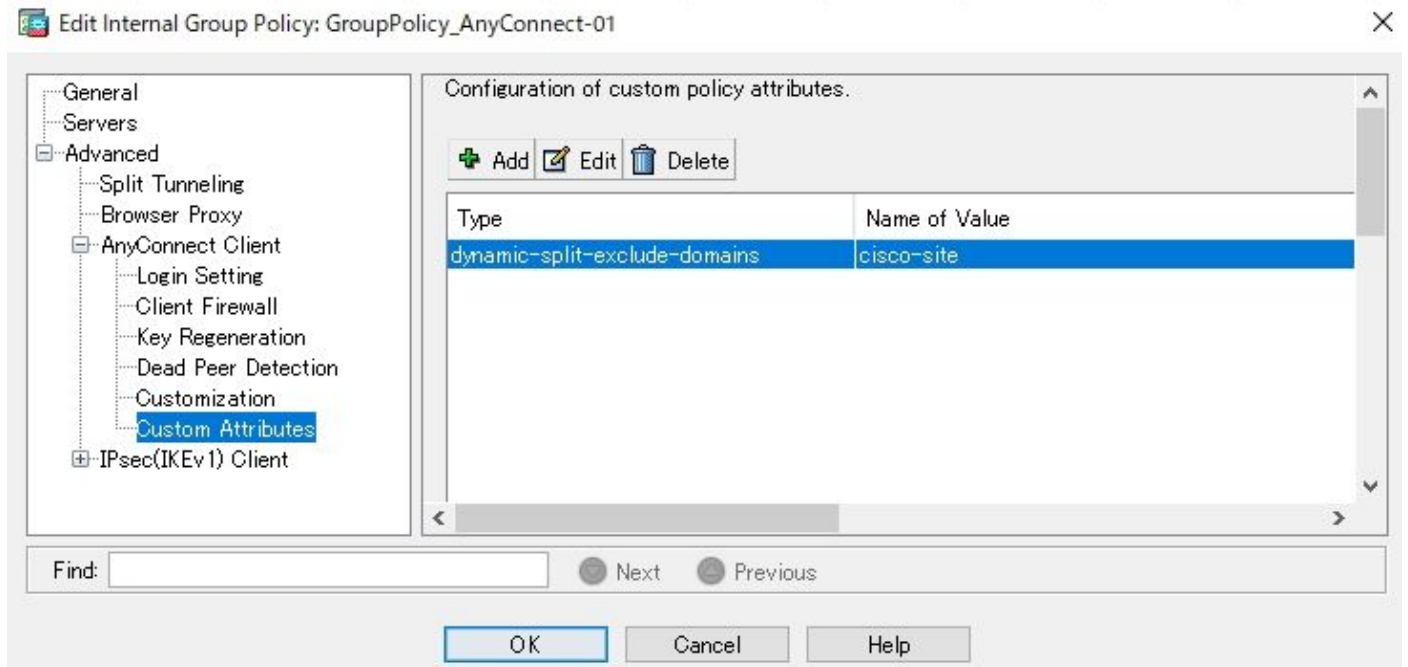
يهو "عونلا" نم كلذ لبق ةمسلال عاشن| م مت dynamic-split-exclude-domains رزلا طبض م Add رقنا ةروصلال يف حضوم وه امك ، ةححص ريغ مي قوسا

عقوم ، لم تحملا Cisco عقوم : لاثملا لئبس يلعل . مسالا يف ةفاسم لاخدا مدع يلعل صرحا اهلاص فب مق ، مي قلا يف FQDNs وأ ةددعتم تالاجم لئجست متي ام دنع (لئجست مسالا Cisco) ، ةلصافب .



ةومجملا جهن لئ مسالا و عونلا ةفاضلا 3 ةوطخلال

كلذ دعب . ةومجملا جهن ددحو Configuration > Remote Access VPN > Network (Client) Access > Group Policies لئ لقتنا ، يف حضوم وه امك ، Type و Name نئوك تالاضا أو Advanced > AnyConnect Client > Custom Attributes لئ لقتنا ةروصلال :



لاثم لئكشت CLI

عجرم دصاقم tunneling يف كرح ماسقنا نم لئكشت CLI لئ مسق اذه دوزي .

<#root>

```

ASAv10# show run
--- snip ---

webvpn

enable outside

AnyConnect-custom-attr dynamic-split-exclude-domains description Dynamic Split Tunneling

hsts
enable
max-age 31536000
include-sub-domains
no preload
AnyConnect image disk0:/AnyConnect-win-4.7.04056-webdeploy-k9.pkg 1
AnyConnect enable
tunnel-group-list enable
cache
disable
error-recovery disable

AnyConnect-custom-data dynamic-split-exclude-domains cisco-site www.cisco.com,tools.cisco.com,community.

group-policy GroupPolicy_AnyConnect-01 internal
group-policy GroupPolicy_AnyConnect-01 attributes

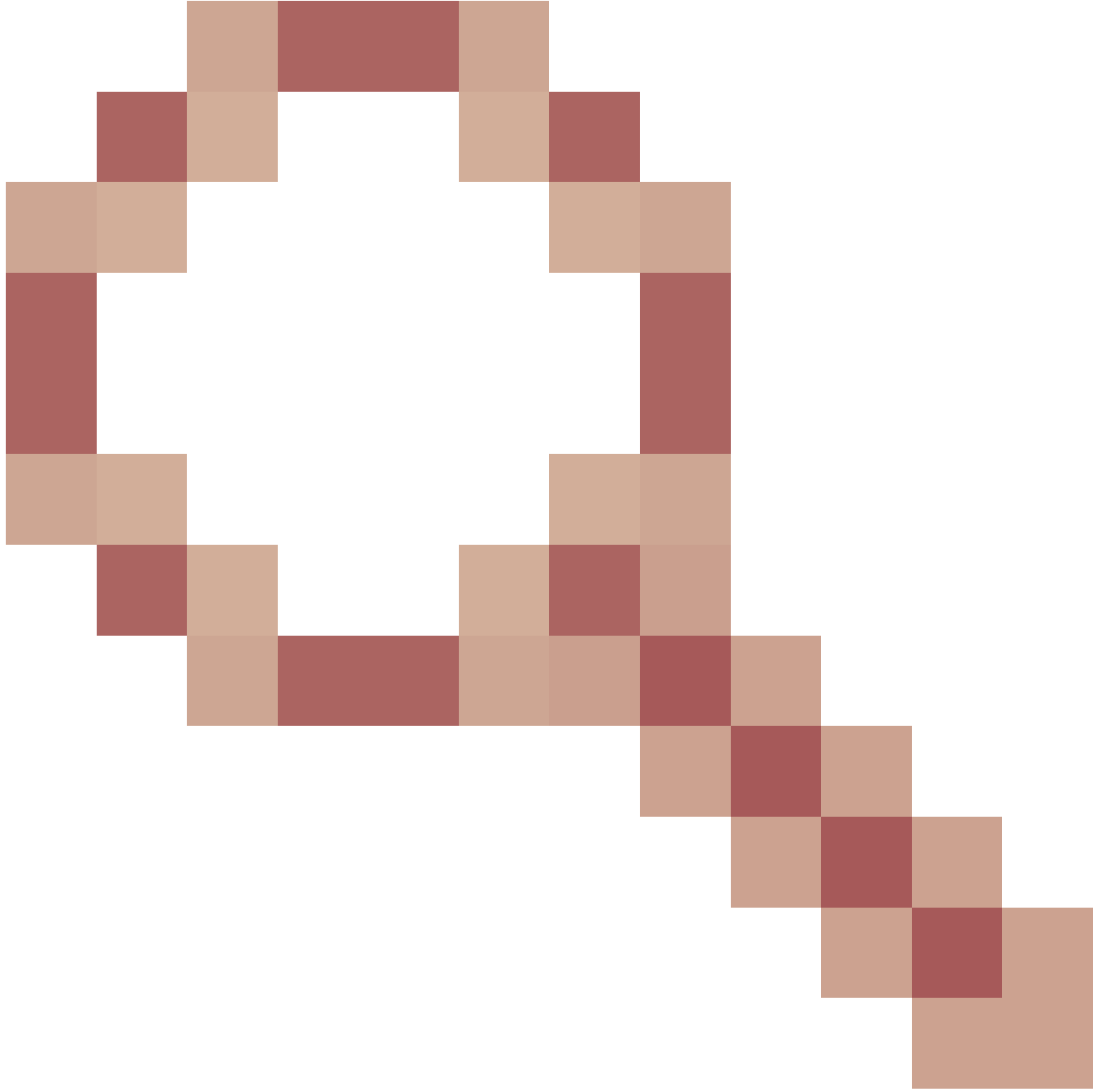
wins-server none
dns-server value 10.0.0.0
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelall
split-tunnel-network-list value SplitACL
default-domain value cisco.com

AnyConnect-custom dynamic-split-exclude-domains value cisco-site

```

دويقلا

- لاصتاللا ميسقتل ةصصخملا تامسلا مادختسال ثدحاً رادصاً وأ ASA 9.0 رادصاً مزلي
- يكيما نيدلا يقفنلا
- موعدم ريغ ميقلال قح يف لدبلا فرح
- نيسحتلا بلط) iOS (Apple) ةزهجأ ىلع موعدم ريغ يقفنلا يكيما نيدلا ميسقتلا:
نم عاخالأ ححصت فرعم Cisco [CSCvr54798](#)



).

ةحصلا نم ققحتلا

Advanced قوف رقنا ، ليمعلا ىلع AnyConnect قالطإ ، Dynamic Tunnel Exclusions، نيوكتلا نم ققحتلل
ةروصلا رهظت امك ، Window>Statistics.



Virtual Private Network (VPN)

Preferences Statistics **Route Details** Firewall Message History

Connection Information	
State:	Connected
Tunnel Mode (IPv4):	Tunnel All Traffic
Tunnel Mode (IPv6):	Drop All Traffic
Dynamic Tunnel Exclusion:	www.cisco.com tools.cisco.com community.cisco.com
Dynamic Tunnel Inclusion:	None
Duration:	00:00:43
Session Disconnect:	None
Management Connection State:	Disconnected (user tunnel active)
Address Information	
Client (IPv4):	1.176.100.101
Client (IPv6):	Not Available
Server:	100.0.0.254
Bytes	

Reset Export Stats...

نم ققحتللا كنكمي شيح بيوبتلا ةمالع Advanced Window>Route Details إلى لاقنتالاضيا كنكمي ةروصلاليف حضورم وه امك، Non-Secured Routes تحت ةجردم Dynamic Tunnel Exclusions أن



Virtual Private Network (VPN)

Preferences | Statistics | Route Details | Firewall | Message History

Non-Secured Routes (IPv4)

72.163.4.38/32 (tools.cisco.com)
 173.37.145.84/32 (www.cisco.com)
 208.74.205.244/32 (community.cisco.com)

Secured Routes (IPv4)

0.0.0.0/0

طاقات الة دكؤي امك Dynamic Tunnel Exclusion list لفسأ www.cisco.com نيوكتب تمق ،لاثملا اذه يف
 الة تانايبلا رورم ةكرح نأ AnyConnect لي عمل ةيداملا ةهجالا الة عومج مت يذلا Wireshark
 DTLS ةطساوب ةرفشم ريغ ،(198.51.100.0) www.cisco.com

Capturing from □-カル エリア接続 [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	S.Port	Destination	D.Port	Length	Info
17	2.991100000	100.0.0.1	56319	100.0.0.254	443	569	CID: 254, Seq: 0
18	3.092024000	100.0.0.1	2095	173.37.145.84	443	66	2095→443 [SYN] Seq=0
19	3.128694000	173.37.145.84	443	100.0.0.1	2093	60	443→2093 [SYN, ACK] Seq=1
20	3.128697000	173.37.145.84	443	100.0.0.1	2094	60	443→2094 [SYN, ACK] Seq=1
21	3.128848000	100.0.0.1	2093	173.37.145.84	443	54	2093→443 [ACK] Seq=1
22	3.128886000	100.0.0.1	2094	173.37.145.84	443	54	2094→443 [ACK] Seq=1
23	3.129667000	100.0.0.1	2093	173.37.145.84	443	296	Client Hello
24	3.130049000	100.0.0.1	2094	173.37.145.84	443	296	Client Hello

اهحال صاوا عا طخال افاشك ت سا

ميقلا لقا ي ف لدبلا فرح مادختسا ةلا ح ي ف

ي ف `*.cisco.com` نيوكت متي، لاثملا لابس ىلع، "ميقلا" لقا ي ف لدب فرح نيوكت مت اذا
تالجال ي ف حضوم وه امك، AnyConnect لمع ةسلج لاصتا عطق متي و، "ميق"

```
Apr 02 2020 10:01:09: %ASA-4-722041: TunnelGroup <AnyConnect-01> GroupPolicy <GroupPolicy_AnyConnect-01>  
Apr 02 2020 10:01:09: %ASA-5-722033: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> Fir  
Apr 02 2020 10:01:09: %ASA-6-722022: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> TCP  
Apr 02 2020 10:01:09: %ASA-6-722055: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> Cli  
Apr 02 2020 10:01:09: %ASA-4-722051: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> IPv  
Apr 02 2020 10:01:09: %ASA-6-302013: Built inbound TCP connection 8570 for outside:172.16.0.0/44868 (17  
Apr 02 2020 10:01:09: %ASA-4-722037: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> SVC  
Apr 02 2020 10:01:09: %ASA-5-722010: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> SVC  
Apr 02 2020 10:01:09: %ASA-6-716002: Group <GroupPolicy_AnyConnect-01> User <cisco> IP <172.16.0.0> Web  
Apr 02 2020 10:01:09: %ASA-4-113019: Group = AnyConnect-01, Username = cisco, IP = 172.16.0.0, Session
```

 FQDN تالكبش ب حامس لل "ميقلا" ي ف Cisco.com لاجم مادختسا كنكمي، ليدبك: ةظالم
www.cisco.com و tools.cisco.com لثم

راسملا ليصافات بيوبتلا ةمالع ي ف ةنمآلا ريغ تاراسملا ةيؤر مدع ةلا ح ي ف

ليصافات بيوبتلا ةمالع ي ف FQDN و IP ناوع فيضي و ايئاقلت AnyConnect ليمع ملعي
ةدعبتسملا تاهجولل تانايبلا رورم ةكرح ادبب ليمعلا موقوي امدنع، راسملا

كنكمي، حيحصلا AnyConnect ةومجم جهنل AnyConnect يمدختسم نييغت نم ققحتلل
show vpn-sessiondb anyconnect filter name رمالا ليغشت

<#root>

```
ASAv10# show vpn-sessiondb anyconnect filter name cisco
```

Session Type: AnyConnect

```
Username      : cisco                      Index : 7  
Assigned IP   : 172.16.0.0                Public IP : 10.0.0.0  
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel  
License       : AnyConnect Premium  
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256 DTLS-Tunnel: (1)AES-GCM-256  
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384 DTLS-Tunnel: (1)SHA384  
Bytes Tx      : 7795373                    Bytes Rx : 390956
```

Group Policy : GroupPolicy_AnyConnect-01

```
Tunnel Group : AnyConnect-01  
Login Time   : 13:20:48 UTC Tue Mar 31 2020  
Duration     : 20h:19m:47s
```


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 اء ان ا ع مچ ي ف ن ي م دخت س م ل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و
امك ة ق ي ق د ن و ك ت ن ل ة ي ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال 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 مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م اء ا د ع 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