

AnyConnect لوح ةل وادتمل ةلئس أال ىل ع درلا - طاشنللا مدع تقومو DPDs ةزهجأو قافنأال

تايوتحمللا

[ةمدقملا](#)

[ةيساسأ تامولعم](#)

[قافنأال عاونأ](#)

[ASA نم تاجرخم لبل جذومت](#)

[طاشنللا مدع تقوت ةزهجأو DPD تادجو](#)

[ةطشن ريغ لمع ةسلج ربتعت ىتم](#)

[SSL ؤفن ASA طقس ىتم](#)

[لعل فلاب ةنكمم DPDs تناك اذا لىصتاللا طيشنت لئاسر نيكم بت بجى اذامل](#)

[لىصتاللا ةداعا ةلاحي ف AnyConnect لىمع كولىس](#)

[ةيلعل فلابا ةيلعمللا](#)

[مياظنللا قىلعت ةلاحي ف AnyConnect لىمع كولىس](#)

[قررتك تملا ةلئس أاللا](#)

[- ةل واعم ةداعا تايلمع دجوت ال نكلو ةيتمز ةرتف ىلعل DPD AnyConnect ىوتجى لولأا عبرلا - دىعبلا فرطاللا ىلعل "تىم" ةمالع عضو موقى نأ لبق اهتوقت نأ بجى ىتاللا مرخلا ددع مك](#)

[IKEv2 مادختسا اب AnyConnect ل ةفلت تخم DPD ةجلا عم له ىتاللا عبرلا](#)

[قوفنللا لىصتاللا AnyConnect ل رخأ ضرغ كانه له ىتاللا عبرلا](#)

[اهنم جورخللا لىجست و طقف ةطشنللا ريغ لمعللا تاسلج ةيفصت كنكم ى له ىبارللا عبرلا](#)

[DTLS و TLS Idle- قافنأا ةيحللص اهتتنا دنع لىصتاللا قوفنللا شجى اذامل ىس ماخلا عبرلا Timeout؟](#)

[ع طقف DPD تقوت تادجو موقت نأ درجيب ةسلج لىصتاللا اذامل ىس داسلا عبرلا IPS ناوتع رادصا اب ASA موقى ال اذاملو ةسلج لىصتاللا](#)

[داعوتسا لىصتاللا عضو لىصتاللا نم ASA لىصتاللا اذا كولىسلا وه اعىب لىصتاللا عبرلا](#)

[انك اذا لىصتاللا عطق لىصتاللا لومخللا ةلهم ىتاللا فل تخم نا تلهم دجوت اذامل ىتاللا عبرلا ةمى قولا ىس فن امهالك](#)

[اقتوم لىصتاللا زاهج فا قىلعتى اذامل ىس داسلا عبرلا](#)

[له مأ AnyConnect ىر هاظلا ىر هامللا ةفر فر شجى له لىصتاللا ةداعا ةيلمع شوج دنع Q10](#)

[قوال طاللا ىلعل هىجوتلا لودج ريغتى](#)

[قوال طاللا ىلعل هىجوتلا لودج ريغتى](#)

[قوال طاللا ىلعل هىجوتلا لودج ريغتى](#)

[قوال طاللا ىلعل هىجوتلا لودج ريغتى](#)

[قوال طاللا ىلعل هىجوتلا لودج ريغتى](#)

[قوال طاللا ىلعل هىجوتلا لودج ريغتى](#)

[قوال طاللا ىلعل هىجوتلا لودج ريغتى](#)

[قلىصتاللا تامولعم](#)

ةمدقملا

لاصتالا ةداعإ كولسو Cisco AnyConnect Secure Mobility Client قافنأ دننسملا اذه فصوي طاشنلا مدع تقومو، (DPD) تيملا ريظنلا فاشتكوا

ةيساسأ تامولعم

قافنألا عاونأ

AnyConnect لمع ةسلج ليصوت لجأ نم نامدختست ناتقيرط كانه

- ءالمع نود) ةباوبلا ربع
- لقتسملا قيبطتلا لالخ نم

نامأل زاغ يلع ةفلتخم (تاسلج) قافنأ ةثالث ءاشنإ كنكمي، كلاصتإ ةقيرط يلإ ادانتسا نيعم ضرغ اهنم لكل، Cisco نم (ASA) فيكتلل لباقلا

1. ClientLess وأ Parent-Tunnel: ههه ةيسسيئرلا ةسلجلا يه ههه بلسب لاصتالا ةداعإ يلإ ةجالحا ةلاح يف مزاللا ةسلجلا زيمملا زمزلا دادعإل ضوافتلا جارداپ ASA موقوي، لاصتالا ةيلأ يلإ ادانتسا. تابسإلا وأ ةكبشلا لاصتالا لكاشم (لقتسملا AnyConnect) لصلأ وأ (ةباوبلا ربع WebLaunch) ليعم نودبك ةسلجلا



لصتم ريغ ليعملا نوكي ام دنع لمعلا ةسلج AnyConnect-parent لثمي: ةطالحالم ةدعاق لاخدا ههه ثيح نم، طابترا فيرعت فلمك لمعي، لاعف لكشب. طشن لكشب عضو/ليعملا مان اذا. نيعم ليعم نم لاصتالا نييعتب موقوي ASA يلع تانايب لقنلا ةقبط نامأ تالوكوتورب) قافنألا ليطعت ممي، تابسإلا (DTLS)/DataRam لقنلا ةقبط نامأ (IPsec/Internet Key Exchange (IKE) (DTLS) Transport Layer Security (DTLS)، تقوملا نايرس أدبي ىتح لصلألا لطي نكلو، نود لاصتالا ةداعإ مدختسملل حمسي اذهو. لاصتالا تقول ىصقألا دحلأ وأ لمخال ةقداصملا ةداعإ

2. ريرمت مميو، الوأ SSL لاصتالا ءاشنإ ممي: (SSL)-Tunnel ةنمألا ليصوتلا ذخأم ةقبط لاصتالا ءاشنإ درجمبو. DTLS لاصتالا ءاشنإ ةلواحم ءانثأ لاصتالا اذه ربع تانايبلا، ىرخأ ههه نمو. SSL لاصتالا ربع نم ال دب DTLS لاصتالا ربع مزحلا ليعملا لسري، DTLS لاصتالا ربع امئاد مكحتلا مزح لقتنت
3. DTLS-Tunnel: قفن يلإ تانايبلا عيمج لقتنت، لمك لكشب DTLS-Tunnel ءاشنإ دنع ءيش شح اذا. ةيضرعلا مكحتلا ءانق رورم ةكرحل طقف SSL قفن مادختسا مميو، DTLS رمتسو DTLS قفن ميسقت ممي سف، (UDP) مدختسملا تانايب ططخم لوكوتوربلا ام ىرخأ ةرم SSL-Tunnel ربع تانايبلا عيمج

ASA نم تاجرخم لل جذومن

ل.اصتالاي تقي رط نم تاجر خم لل ج ذومن انه

ب يوالا قال ط ا ربع AnyConnect ل اصتا

```
ASA5520-C(config)# show vpn-sessiondb detail anyconnect
```

Session Type: AnyConnect Detailed

```
Username      : walter                      Index       : 1435
Assigned IP   : 192.168.1.4                Public IP   : 172.16.250.17
Protocol      : Clientless SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : Clientless: (1)RC4  SSL-Tunnel: (1)RC4  DTLS-Tunnel: (1)AES128
Hashing       : Clientless: (1)SHA1  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
Bytes Tx      : 335765                    Bytes Rx    : 31508
Pkts Tx       : 214                      Pkts Rx     : 18
Pkts Tx Drop  : 0                        Pkts Rx Drop : 0
Group Policy  : My-Network                 Tunnel Group : My-Network
Login Time    : 22:13:37 UTC Fri Nov 30 2012
Duration      : 0h:00m:34s
Inactivity    : 0h:00m:00s
NAC Result    : Unknown
VLAN Mapping  : N/A                       VLAN        : none
```

```
Clientless Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
```

Clientless:

```
Tunnel ID      : 1435.1
Public IP      : 172.16.250.17
Encryption     : RC4                      Hashing       : SHA1
Encapsulation  : TLSv1.0                  TCP Dst Port  : 443
Auth Mode      : userPassword
Idle Time Out  : 2 Minutes                 Idle TO Left  : 1 Minutes
Client Type    : Web Browser
Client Ver     : Mozilla/5.0 (Windows NT 5.1; rv:16.0) Gecko/20100101 Firefox/16.0
Bytes Tx       : 329671                    Bytes Rx      : 31508
```

SSL-Tunnel:

```
Tunnel ID      : 1435.2
Assigned IP    : 192.168.1.4                Public IP     : 172.16.250.17
Encryption     : RC4                      Hashing       : SHA1
Encapsulation  : TLSv1.0                  TCP Src Port  : 1241
TCP Dst Port   : 443                      Auth Mode     : userPassword
Idle Time Out  : 2 Minutes                 Idle TO Left  : 1 Minutes
Client Type    : SSL VPN Client
Client Ver     : Cisco AnyConnect VPN Agent for Windows 3.1.01065
Bytes Tx       : 6094                      Bytes Rx      : 0
Pkts Tx        : 4                        Pkts Rx       : 0
Pkts Tx Drop   : 0                        Pkts Rx Drop  : 0
```

DTLS-Tunnel:

```
Tunnel ID      : 1435.3
Assigned IP    : 192.168.1.4                Public IP     : 172.16.250.17
Encryption     : AES128                   Hashing       : SHA1
Encapsulation  : DTLSv1.0                Compression   : LZS
UDP Src Port   : 1250                     UDP Dst Port  : 443
Auth Mode      : userPassword
```

Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : DTLS VPN Client
Client Ver : Mozilla/5.0 (Windows NT 5.1; rv:16.0) Gecko/20100101 Firefox/16.0
Bytes Tx : 0 Bytes Rx : 0
Pkts Tx : 0 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

لوقت سمل قيبطت ل ربع AnyConnect لاصتا

<#root>

ASA5520-C(config)# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : walter Index : 1436
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 12244 Bytes Rx : 777
Pkts Tx : 8 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : My-Network Tunnel Group : My-Network
Login Time : 22:15:24 UTC Fri Nov 30 2012
Duration : 0h:00m:11s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none

AnyConnect-Parent Tunnels: 1

SSL-Tunnel Tunnels: 1

DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 1436.1
Public IP : 172.16.250.17
Encryption : none Hashing : none
TCP Src Port : 1269 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : AnyConnect
Client Ver : 3.1.01065
Bytes Tx : 6122 Bytes Rx : 777
Pkts Tx : 4 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel

:

Tunnel ID : 1436.2
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Encryption : RC4 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 1272
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : SSL VPN Client

Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.01065
Bytes Tx : 6122 Bytes Rx : 0
Pkts Tx : 4 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel

:
Tunnel ID : 1436.3
Assigned IP : 192.168.1.4 Public IP : 172.16.250.17
Encryption : AES128 Hashing : SHA1
Encapsulation: DTLSv1.0 Compression : LZS
UDP Src Port : 1280 UDP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 2 Minutes Idle TO Left : 1 Minutes
Client Type : DTLS VPN Client
Client Ver : 3.1.01065
Bytes Tx : 0 Bytes Rx : 0
Pkts Tx : 0 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

طاشننلا مدع تي قوت ةزهجأو DPD تادحو

ةطاشن ريغ لمع ةسلج ربتعت ىتم

SSL قفن نوكي ال امدن ع طقف (ةداي زلا يف تقوؤملا أدبيو) ةطاشن ريغ لمع ال ةسلج دع
SSL-طاقسإ تقوعم تقوولاب ةسلج لك متخ متي، كذلك. لمع ال ةسلج يف ك لذ دعب ادوجوم
Tunnel.

ASA5520-C# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed


Username : walter Index : 1336
Public IP : 172.16.250.17
Protocol : AnyConnect-Parent <- Here just the AnyConnect-Parent is active
but not SSL-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none
Hashing : AnyConnect-Parent: (1)none
Bytes Tx : 12917 Bytes Rx : 1187
Pkts Tx : 14 Pkts Rx : 7
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : My-Network Tunnel Group : My-Network
Login Time : 17:42:56 UTC Sat Nov 17 2012
Duration : 0h:09m:14s
Inactivity : 0h:01m:06s <- So the session is considered Inactive
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none

SSL قفن ASA طاقسي ىتم

SSL: قفن لاصتا عطق امه ب نكمي ناتقيرط كانه

1. DPD - ليمع نيبتالاصتالاي ف لشف فاشتكال ليمعلا لبق نم DPD مادختسا متي - AnyConnect لعل دراوملا فيظنتل اضيا DPDs مادختسا متي. ASA ليسيئرلا فرطلالو ASD. اذا تانايبالادعاقي فتالاصتالاب ظفتحتي اليسيئرلا فرطلال نأ نمضي اذهو ASD. عطقن لىل DPD لاسررب ASD اذ. DPD تاودال عبيجتسم ريغ عياهنلا عطقن تناك، عبيجتسم ريغ عياهنلا عطقن تناك اذ. عاجا يا ذاختا متي نلف، عاجالاب ماقو عياهنلا موقوي (IKEv1 و IKEv2) مادختسا مت اذ لىل عدمتعي) لاسررال ادعاي ددعل لىل صقأل دحلل ادع عضو لىل لمعلا عسلج لقنيو، لمعلا عسلج تانايب ادعاقي قفنلا قيومتب ASD سأللا عطقن نأو، ادب دق سأللا عطقن نم DPD نأ وه اذه هينعي ام. فانئتسالل راطنتا لىل عأل يسيئرلا قفنلا ASD لمحي، تالاحل هذه لثم يف. ليمعلا عم لىل صتت دعت مل دادرتساو، نوكتسالا عضو لىل باهذالو، تاكبشلا يف لوجتلاب مدختسملل حامسلل لىل عسلا ممتي و طاشنب لىل صتسالا لىل عسلا لىل باقم تاسلجلا هذه باسح متي. عسلجلا طورشلا هذه بجومب:
 - مدختسملل لومخالا عضو قلهم
 - جيحص لكشب جورخالا ليجستو عياصلالا لمعلا عسلج فانئتساب لىل عسلا موقوي.

جهن تادادعاي في WebVPN تامس نمض anyconnect dpd-interval رمال مدختسا، DPDs نيوكتل نم لكل عياهنلا 30 لىل عهنييغت متي و DPD نيكمت متي، يضا رتفا لكشب. عومجمل ASD. لىل عسلاو (عابوال) ASD.

 DPD لشف في - [CSCts66926](#) Cisco نم عاطخال جيحصت فرعمب ملع لىل عك: ريذحت لىل عسلا لاصتا دق دب DTLS قفن عاهنلا يف.

2. Idle-timeout - ام دنع يه SSL-Tunnel لاصتا عطق اهيف متي يتلا عياهنلا عطقيرطال - Idle-timeout يف لومخالا عضو بجي ال هنا ركذت، كلذعمو. قفنلا اذهل Idle-Timeout عياهنلا صيهتنت DTLS، SSL-، عسلج تقو عاقبتسا متي مل ام. اضيا DTLS قفن يف لب، طوق SSL قفن تانايبالادعاقي في Tunnel.

لعللاب عكمم DPDs تناك اذ لىل صتالا طيشنت لىل اسر نيكمت بجي اذامل

طوق لتقوي هنلا. اهسفن AnyConnect لمعلا عسلج لىل DPD ييضقوي ال، اقبسم حضورم وه امك لىل عسلا لىل عرذعت اذ. قفنلا عاشنلا ادعاي نم لىل عسلا نيكمتي يتحت عسلجلا كلت يف قفنلا ASD. لىل عسلا لىل عسلا صيهتنت يتحت عسلجلا نلف، قفنلا عاشنلا ادعاي تاقفدتلل ببسب ابلاغ مهلصف متي نأ نكمي عالسلا نلف، يضا رتفا عكمم DPDs نأ امب نلا. ليكولا زهجاو عياهنلا رادجو (NAT) عكبشلا ناو نع عمجرت عم دحاو حاجتا يف قلغت يتلا لىل عسلا، عياهنلا 20 لثم، عضفخنم عياهنلا لىل عسلا لىل صتالا طيشنت لىل اسر نيكمت اذه عنم.

مادختسا ب نيعم عومجملههنب عصال WebVPN تامس نمض Keepalives لىل اسر نيكمت متي عياهنلا 20 لىل عسلا تادحو نييغت متي، يضا رتفا لكشب. anyconnect ssl keepalive رمال

لصاصتالا ادعاي علاحي في AnyConnect ليمع كولس

،نيوكتلل لباق ريغ اذه .لاصتالا ليطعت ةلاح يف لاصتالا ةداع| AnyConnect لواجي
عيطتسي AnyConnect ناك اذوا ةحلاص لارت ال ASA لىل ع VPN ةسلج نأ املاط .ايئقلت
تفنؤتسأ ةسلج VPN لىل ،يلعفا لاصتالا عاشن ةداع|

،لاصتالا عطق ةلهم ءاهتنا وأ لمعلا ةسلج ةلهم ءاهتنا ىتح "لاصتالا ةداع|" ةزيم رمتست
تارتف نيوكت متي مل اذوا ةقيد 30 (وأ) اهتيحالص يهتنتو ،لومخال ةلهم عقاولا يف يهو
دق هنأ ةعباتملا ليمعلا نكمي ال ،تاكبشلا هذه ةيحالص ءاهتنا درجمبو .(ةلهملا ءاهتنا
للمعلا رمتسي .ASA لىل ع (VPN) ةيرهظلا ةصاخلا ةكبشلا لمع تاسلج طاقس| لعفلاب مت
VPN ةسلج هيذل لازي ال ASA نأ دقتعي هنأ املاط

اذام مهى ال .ةكبشلا ةهجاو ريغيغ ةيفيكي نع رظنلا ضغب AnyConnect لاصتا ةداع| مت
عقابط نم لاصتالا تالوحم تناك اذام وأ ،(NIC) ةكبشلا ةهجاو عقابطب صاخلا IP ناووع ريغت
(سكعل وأ يكللس لىل يكلسال) ىرخأ ةكبش ةهجاو عقابط لىل (NIC) ةكبش ةهجاو

نم تايوتسم ةثالث كانه ،رابتعالا يف AnyConnect ل لاصتالا ةداع| ةيلمع عضت امدنع
نم ةسلج لكل لاصتالا ةداع| كولس نإف ،كلذ لىل ةفاضلإابو .اهركدت كيلىل بجي تاسللجلا
لىل دامتعالا نود اهنم يأ عاشن ةداع| نكمي ثيحب ،عساو لكشب انرتقم نوكي تاسللجلا هذه
:ةقباسلا ةقبطلال نم ةسلجلا رصانع

1. [3 OSI ةقبطل] UDP وأ TCP لاصتا ةداع| .
2. موعدم ريغ TLS فانئتس| - [4 OSI ةقبطل] IPsec(IKE+ESP) وأ DTLS وأ TLS .
3. ةقداصم زمرك VPN ةكبش ةسلج ل زيمملا زمرلا مادختسا متي - [7 OSI ةقبطل] VPN
وه .عاطقنا كانه نوكي امدنع ةنمأ ةانق ربع VPN ةكبش لمع ةسلج عاشن ةداع| زيمم
وأ زيمملا Kerberos زمرمادختسا ةيفيكي ،ةيرظنلا ةيخانلا نم ،ادج لثامت ةصاخ ةيلأ
فرطالا ةطساوب هؤاشن| مت رفشمو ديرف زيمملا زمرلا .ةقداصملا ليمعلا ةداهش
اهؤاشن| مت ةيئوشع ةلومح لىل ةفاضلإاب ةسلجلا فرعم لىل ع يوتحي يذلاو ،يسئيرلا
ةيرهظلا ةصاخلا ةكبشلا عاشن| نم عزجك ليمعلا لىل اهريرمت متي .ريفت لكشب
احلاص لظي وه .يسئيرلا فرطالا لىل لوصولل ةنمأ ةانق عاشن| دعب ةيلوالا (VPN)
يهو ،ليمعلا ةركاذي ف هنيخت متي .يسئيرلا فرطالا لىل لمعلا ةسلج ةدم لاوط
زايتم تاذ ةيلمع

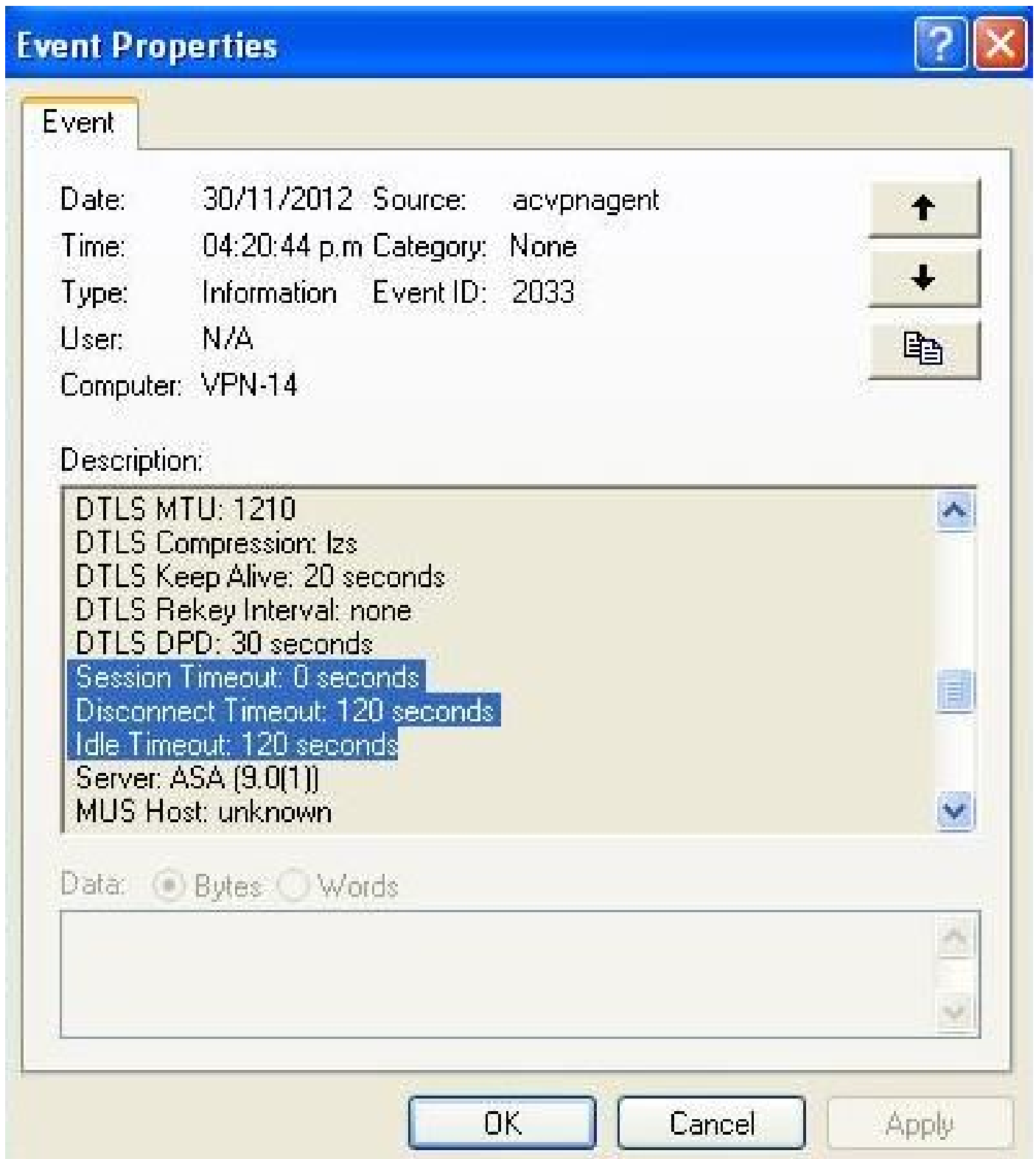


ريفت لمع ةسلج ل زيمم زمريلىل دعب اميفوه هذه ASA تارادص| يوتحت :حيملت
8.4(7.1) و 9.1(3) :ىوقأ

ةيلعفا لىل ةيلمعلا


للمع رمتسي .ةكبشلا لاصتا ليطعت درجمب "لاصتالا عطق ةلهم" تقؤم ليغشت ادب متي
ةلهم نييعت مت .تقؤملا اذه ةيحالص هتنت مل املاط لاصتالا ةداع| ةلواحم يف AnyConnect
لاصتالا تقول ىصقألا دحلا وأ Idle-Timeout ةعومجملا جهنل ىندألا دادعإلا لىل لاصتالا عطق

:ضوافتلا يف AnyConnect لمع ةسلج ل اذحألا ضراع يف تقؤملا اذه ةميق رهظت




اهم ققحتال نكم يو، (ةيناث 120) نيتقي قد دع بةسلجال لاصتا عطق متي، لاثملا اذه يف AnyConnect بةصاخلا "لئاسرلا تاظوفحم" يف


```
[30/11/2012 04:30:02 p.m.] Checking for product updates...
[30/11/2012 04:30:02 p.m.] Checking for customization updates...
[30/11/2012 04:30:02 p.m.] Performing any required updates...
[30/11/2012 04:30:02 p.m.] Establishing VPN session...
[30/11/2012 04:30:02 p.m.] Establishing VPN - Initiating connection...
[30/11/2012 04:30:02 p.m.] Establishing VPN - Examining system...
[30/11/2012 04:30:02 p.m.] Establishing VPN - Activating VPN adapter...
[30/11/2012 04:30:05 p.m.] Establishing VPN - Configuring system...
[30/11/2012 04:30:05 p.m.] Establishing VPN...
[30/11/2012 04:30:05 p.m.] Connected to 10.198.16.140.
[30/11/2012 04:30:06 p.m.] Connected to 10.198.16.140.
[30/11/2012 04:33:28 p.m.] Reconnecting to 10.198.16.140...
[30/11/2012 04:33:28 p.m.] Reconnecting, waiting for network connectivity...
[30/11/2012 04:35:28 p.m.] Reconnecting to 10.198.16.140...
[30/11/2012 04:35:28 p.m.] Disconnect in progress, please wait...
[30/11/2012 04:35:28 p.m.] Disconnect in progress, please wait...
[30/11/2012 04:35:34 p.m.] Verify your network connection.
```

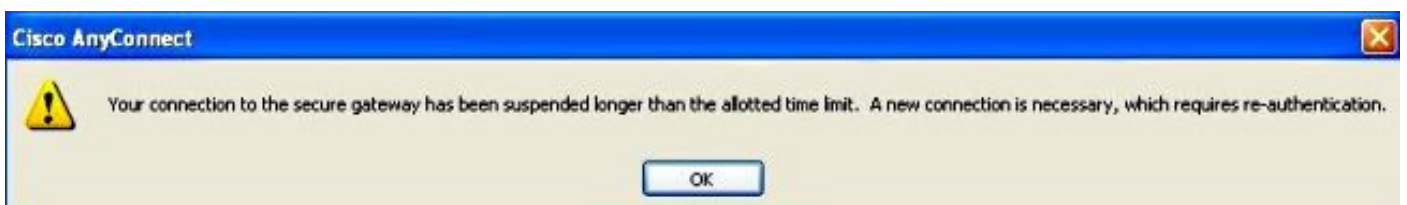
 لمع ةس لظت نأ بجي ،لاصتالا ةداع| لواحي ليمع ل ASA بيحتسي ي كل :حيملت اضيأ مزلي ،لش فال زواجت ةلاح ي في ASA تانايب ةدعاق ي ف ةدوجوم Parent-Tunnel لاصتالا ةداع| كولس لمعي يتحت DPDs ني كمت

ةداع| ةي لمع تناك اذا ،كلذ عمو .لاصتالا ةداع| تلشف ،ةقبا سلال لئاسرلا نم يئر مه امك ثدحي ام يلي امي فف ،ةحجان لاصتالا

1. ظفحتحي قفنلا اذه نأل عارجال اذهب ضوافتلا ةداع| مت مل .وه امك لصلال قفنلا يقبي .لاصتالا ةداع| لمع ل ةس لجل بولطم ل ةس لجل زيمم ل زمرباب
2. reconnect ل ي ف تلمعتسا فلتخم رصم ذفانمو ،ةس لجل DTLS وديج SSL تقلخ .
3. Idle-Timeout ميق عيمج ةداعتسا متي .
4. طاشنلا مدع ةلهم ةداعتسا مت .

 ةدعاق موقت ال Cisco [CSCtg33110](#) نم ءاطخال حيحصت فرع مبلع يلع نك :ريذحت ةداع| دنع ASA لمع ةس لجل تانايب ةدعاق ي ف ماع ل IP ناو نع ثيذحت ب VPN ةس لجل تانايب لاصتالا AnyConnect.

ةلاسرلا هذه هجاوت ،لاصتالا ةداع| تالواحم اهي ف تلشف يتلا ةلاح ل هذه ي في



✎ عاڤخأل احي حصت فرعم :ةقد رثكأ رمألا اذه لعجل اذه نيسحتل بلط مي دقت مت :ةظالم ل نيوكتلل ةلباق ةلصتم ريغ ةلهم يلع ASA يوتحي ال - [CSCsl52873](#) Cisco نم AnyConnect.

ماظنللا قيلعت ةلاح في AnyConnect ليمع كولس

رمتسي .رتوي بمكلا نوكس دعب لاصتالا ةداعإ AnyConnect ل حمست ل اوجت ةزيم كانه مدهب ليمعلا موقيا الو لمعلا ةسلج وأ لومخلا عضو ةلهم اءاتنا ىتحت ةلواحلما في ليمعلا ال نيلذلا ني مدختسم لل .دادعتسالا/اتابساإل عضو في ماظنلا لوخذ دنع روفلا يلع قفنلا لاصتالا ةداعإ عنمل ةضفخنم ةميق يلع ةسلجلا ةلهم نيسي عتب مق ،ةزيملا هذه نوديري فانئسالا/انوكسلا .

✎ نم عاڤخأل احي حصت فرعم حالصإ دعب :ةظالم Cisco [CSCso17627](#) (2.3(111)+ رادصإلا) ، فانئسالا ةزيم يلع هذه لاصتالا ةداعإ ةزيم ليطعتل مكحت ضبقم لاخذإ مت .

فيرعت فلم لالخنم AnyConnect ل ئاقلا لتلا لاصتالا ةداعإ كولس في مكحتلا نكمي دادعإلا اذه مادختساب XML AnyConnect

```
<AutoReconnect UserControllable="true">true
  <AutoReconnectBehavior>ReconnectAfterResume</AutoReconnectBehavior>
</AutoReconnect>
```

عضو نم رتوي بمكلا عاجرتسا متي ام دنع لاصتالا ةداعإ AnyConnect لواحي ،ريغيغلا اذه عم DisconnectOnSuspend ب ايضار تافا AutoReconnectBehavior ليضفت موقيا .نوكسلا دعب لاصتالا ةداعإ 2.2 رادصإلا AnyConnect ليمع كولس نع كولسلا اذه فل تخي فلم في ReconnectAfterResume نيسي عت ام ةكبشلا لوؤسم يلع بجي ،فانئسالا مدختسملا مكحت ةحاتم AutoReconnectBehavior و AutoReconnect تال يضفت لعج وأ في رعنتلا اهنيسي عتب ني مدختسم لل حامس لل في رعنتلا فلم في اهيف .

ةرركتملا ةلئسالا

تايللمع دجوت ال نكلو ةي نمز ةرتف يلع DPD AnyConnect يوتحي .لوالا عبرلا ةمالع عضو موقيا نأ لبق اهتوفت نأ بجي يتلا مزحللا ددع مك - ةلواحلما ةداعإ ؟ديعبلا فرطلا يلع "تيم"

ءاشنإ ةلحرم لالخنم مدهب ال مالعلا نوؤش ةرادإ مقت مل ،ءالمعلا روظنم نمو - فلأ ملو قفنلا ءاشنإ ةلحرم ءانثأ (مزع برأ لسري) تالواحلما ثالث ليمعلا هجاوا إذا .قفنلا إذا يطايتحال خسنلا مداوخ دحأ مادختساإل دوعي في ،يساسالا VPN مداخنم ةباجتساإل يقلت في أهلمشت مل يتلا ذفاونلل نوكي ال ،قفنلا ءاشنإ درجم ،كلذ عمو .ةدحاو نيوكت مت وه امك لدان VPN لال يلع DPDs ل يقي قحلا ريثأتلل .ليمعلا روظنم نم قفنلا يلع ريثأت مسقلا في حضوم [DPDs و Inactivity Timers](#).

AnyConnect لة فلتخ م DPD ة جلاع له . ينال ع برلا

ة داع ا تايلمع تس - ة لواجم ا داع ا تايلمع نم تباث ددع ل ع IKEv2 يوتحي ،معن .
م.زح ع بس/ة لواجم

ق فنل-لصلال AnyConnect ل رخآ ضرغ كانه له . ثلال ع برلا

ا. تايقرت ع فد ل جأ نم يسيئرلا ق فنل ا مادختسا م تي ،ASA ل ع ة طرخ هنا ل ة فاضال اب .
ة يل مع اناثأ طشن لكشب لصتم ريغ ليمعلا نأل ،ليمعلا ل ASA نم AnyConnect ة روص
ة يقرتلا .

ل ج س ت و ط ق ف ة طشن ل ريغ لمعلا تاسلج ة يفصت كنكمي له . ع بارل ع برلا
ل اهنم جورخل

a. show vpn-sessionDB AnyConnect رمأل ا مادختسا اب ة طشن ل ريغ تاسلج ل ة يفصت كنكمي .
ل ج ا تحت ،كلذ نم ال دب . طشن ريغ ة سلج ط ق ف نوذي نأ رمأ نم ام كانه ،امم .
filter inactive .
م دختسم لكل لمع ة سلج لك نم جورخل ل ج س ت و ا ة ني عم لمع تاسلج نم جورخل ل ج س ت
ء ا ط خ ال ا حي حصت فرعم ،زيعت بلط في نصت م . ق ف ن ة ع و م ج م و ا ،لوكوتورب ،(م سا - ة سرهف)
ة طشن ل ريغ لمعلا تاسلج نم جورخل ل ج س ت ل راخ ل ة فاضا ل جأ نم ، Cisco [CSCuh55707](#) نم
ط ق ف .

و DTLS ق افنا ة يحيالص اءاتنا دنع لصلال ق فنل ل ثدحي اذام . س ماخ ل ع برلا
TLS Idle-Timeout?

a. AnyConnect- لمع ة سلج صاخال "راسيلا ل لومخال عضو نم" تقوؤم ل ني عت ة داع ا متت .
parent له م ك لمعلا اب ة لمخال ا له ملل حمسي اذهو . DTLS-Tunnel و SSL ق فن ع ط ق م تي نأ دعب
مل اذا . ل اع ف لكشب لاصلتال ة داع ا ل ليمعلا ه ب حومس م ل تقولا اذه حبصي و . ة لصتم ريغ
ي . سيئرلا ق فنل اءاهن ا م تي سف ، تقوؤم ل نمض لاصلتال ة داع ا ل ليمعلا مق ي .

ت ي ق و ت ا د ح و م و ق ت ن ا درجم ة سلج ل اب ظا فتحال م تي اذامل . س داس ل ع برلا
IP؟ ناو نع رادصا اب ASA موق ي ال اذامل و ، ة سلج ل لاصلتال ع ط ق ب DPD

ل ع ل ليمعلا لاصلتال ة داع ا ASA رظت ني ، ة ل حال هذه ي ف . ل ليمعلا ة ل حال س ا ر ل ا فرط فرعي ال - فلأ
لمع ة سلج DPD لتقت ال . لمخال تقوؤم ل ل ع لمعلا ة سلج يهتنت ل تحت كلذ م تي نأ لمأ
ءاشن ا ة داع ا نم ل ليمعلا نكم تي ل تحت (ة سلج ل هذه ي ف) ط ق ف ق فنل ل لتقت ل ب ،
AnyConnect ،
ة يحيالص اءاتنا ل تحت ل ق ب ت لمعلا ة سلج ل ن ا ف ، ق فن ءاشن ا ة داع ا ل ليمعلا مق ي مل اذا . ق فنل ل
لمخال تقوؤم ل .


ل ج س ت ا تايلمع ني ع ت ب مق ف ، ا م ا د خ ت س ا م تي ي ت ل ل لمعلا تاسلج ل و ح ق ل ق ل ن ا ك اذا
لمعلا ة سلج ف ذ م تي ، د ا د ع ا ل ا ذ ه م ا د خ ت س ا ب . د ح و ل ث م ة ض ف خ ن م ة م ي ق ل ا ة ن م ا ز ت م ل ل و خ د ل
ا م د ن ع لمعلا ة سلج ل ت ا ن ا ي ب ة د ع ا ق ي ف لمع ة سلج ل م ه ي د ل ن ي ذ ل ن ي م د خ ت س م ل ا ب ة ص ا خ ل
ي . رخآ ة ر م ل و خ د ل ل ج س ت ب ن و م و ق ي .

د ا د ع ت س ا ل ا ع ض و ل ا ط ش ن ن م ASA ل ش ف اذا ك و ل س ل ا و ه ا م . ع ب ا س ل ع برلا

و SSL و لصلال) ة ثلال ق افنأل خسن م تي ، ة سلج ل اءاشن ا م تي ا م د ن ع ، ة ي ا د ب ل ا ي ف - فلأ

TLS و DTLS لمع تاسلج عاشنإ ةداعإ متت، ASA لشف درجمب .ةيطايتحال ةدحولإ ىلإ (DTLS نأ بجي قافنألأ ربع قفدتت تانايب يأ نكلو ،ةيطايتحال ةدحولإ ىلإ اهتنامزم متت ال اهأنل AnyConnect لمع ةسلج عاشنإ ةداعإ دعب عاطقنا نود لمعت

مقرلإو SSL ةلحاب ظافتحال متي ال كذل ،ةلحال نع ةربعم ريغ SSL/DTLS لمع تاسلج نوكي نأ ةسلج كلت جاتحت ،كذل .ام دح ىلإ ةبيريضلل ةعضاخ نوكت نأ نكمي وي لسلستل ةسلج زمر ةسلج لصلأل عم تزجنأ نوكي يأ ،رفصل نم reestablished

 زاهجلا ىلإ SSL VPN ليمع لمع تاسلج لقن متي ال ،لشفال زواجت ةلح يفي :حيملت لاصتالاطيشنت لئاسر ليطعت مت اذإ يطايتحال

عطق ليطعت ولومخال ةلهم ،ناتفلتخم ناتلهم دجوت اذامل .نمائل عبرلا ةميقيال سفن امهالك انك اذإ ،لاصتال

نيتفلتخم نيتترتف ىلع صنلال مت ،تالوكوتوربال تعضو امندنعو - فلأ

- لاصتال ربع تانايب يأ ريرمت متي ال امندنع يه لومخال ةلهم - لومخال ةلهم
- نع ىلختت امندنع ةصاخ اهب لاصتال عطق مت يتل ةلهملا نوكت - لاصتال عطق ةلهم هئاشنإ ةداعإ نكمي الو لاصتال نادقف مت دق هنأل VPN لمع ةسلج

ASA لسري ،كلذ نم ال دبو .ASA ىلع اهب لاصتال عطق مت يتل ةلهملا ذيفنت متي مل ليمعلل ةلصتمل ريغو ةلمخال ةلهملا اهتتا تارتف نم لكل لومخال ةلهم ةميقي

ةميقي ليمعلل مدختسي .ةلمخال ةلهملا جلاعي ASA نأل ،ةلمخال ةلهملا ليمعلل مدختسي ال ةفرعمل ،لومخال ةلهم ةميقي اهسفن يه يتلوا ،اهب لاصتال عطق مت يتل ةلهملا اهتتا ةسلجال طاقساب ASA ماق نأل ذنم لاصتال ةداعإ تالواحم نع يلختل متي ىتم

ةدحولال ةرمل يفي ةسلجال لاسرلا ىلع ASA لمعي ،ليمعلل طشن لكشب لصتم ريغ هنأ عم اهب لاصتال عطق مت يتل ةلهملا ذيفنت مدعل يسيئرل ببسل ناك .لومخال ةلهم ربع ةمعال تاقفنل ةدايزو VPN ةكبشل لمع ةسلج لكل رخآ تقؤم ةفاضل بنجت وه ASA ىلع ميق عم طقف ،نيتلحال الك يفي تقؤملا سفن مادختسا نكمي هنأ نم مغلل ىلع ASA ىلع (نيتلدابت م ريغو نيتلحال نأل ارظن ،ةفلتخم ةلهم

حامسلا يه اهب لاصتال عطق مت يتل ةلهملا اهتتا عم اهتفاضل تمت يتل ةدحولال ةميقيال .لمل لباقم طشن لكشب لصتم ريغو ليمعلل نوكي امندنع ةفلتخم ةلهم ديدحتب لوؤسملل اذهل [Cisco CSCsl52873](#) نم عاطخال حيحصت فرعم فينصت مت ،اقبسم ةراشال تمت امك ضرغل

اتقؤم ليمعلل زاهج فاقبي متي امندنع ثدحي اذام .عساتل عبرلا

ال .لاصتال دقفت امندنع VPN لاصتال عاشنإ ةداعإ AnyConnect لواحي ،يضارتفا لكشب A. [كوليس](#) ىلإ عجرا .يضارتفا لكشب ماظنل فانئتسا دعب VPN لاصتال عاشنإ ةداعإ لواحي لىصافت ىلع لوصحلل [ماظنللا قيلعت ةلح يفي AnyConnect ليمع](#)

يرهاظلا لوحملا ةفرفر ثدحي له ،لاصتال ةداعإ ةي لمع ثودح دنع .Q10 زارطلأ قاطال ىلع هيحوتل لودج ريغت ي له م ،AnyConnect

DTLS و SSL يلع لاصتا ةداع| هذه .اضيأ كلذ لعلفت ال قفنللا يوتسم يلع لاصتالا ةداع| A. طقف هطاقس| متي ،DTLS لش ف اذا .م لستست نأ لبق ةيناث 30 يلاوح قرغتست هذه .طقف لاصتالا ةداع| موقت .ةسلجللا يوتسم يلع لاصتالا ةداع| يف ببستي هنإف ،SSL لش ف اذا ليمعللا ناونع ريغتت ي مل اذا .لمكلا ب هيچوتلا ذيفنت ةداع| لمعللا ةسلج يوتسم يلع الف ،(VA) يره اظلالا لوجملا يلع رثوت يرخأ نيوكت تاملعم ةيأ وأ لاصتالا ةداع| يف نيوملا لاصتالا ةمدختسملا ةيداملا ةهجاو لا يف ريغتتلا يديوي نأ نكمملا نم ،ASA نم ةم لتسملا (WiFi) لىل يكلسللا لاصتالا نم تلقت ناو عاسرالا اغلاب تمق اذا ،لثملا لىبس يلع (VPN) دحلا ةدحو ةميقي رثوت .VPN لاصتالا (MTU) يوصقلا لاسرالا ةدحول ةفلتخم ةميقي لىل .هنكمت ةداع| مث VA لىطعت يف اهيف ريغتتلا ببستي و ،VA يلع (MTU) لقنلل يصرقألا

ناك اذا ؟ةسلجللا ةيرارمتس| يئاقلل لاصتالا ةداع| رفوت له .Q11 زارطلا AnyConnect ليمع يف اهتفاضل| تمت ةيفاضل فئاطو ةيأ دجوت له ،كلذك رمالا

a. تاقىب بطلل لمعللا ةسلج ةيرارمتس| باعيتسالا يفاضل رحس ي AnyConnect رفوي ال . ةكبشلا لاصتالا فانئتس| نم ةزيجو ةرتف دعب ،ايئاقلل VPN لاصتالا ةداعيتس| متي نكلو لمعللا ةسلجو لومخللا ةيخالص اهت نا تارتف ةيخالص اهت نا مدع ةطيرش ،نمألا ربملا ب يئاقلل لاصتالا ةداع| نع جتني ،IPsec ليمع س كع يلعو .ASA يلع اهنيوكت مت يتلا لظي ،لاصتالا ةداع| AnyConnect ةلواحم نم مغرلا يلع .للمعلا ب صاخلا IP ناونع سفن ادوجوم ليمعلل IP ناونع لظي كلذل ،لاصتالا ةلواحم يفو انكمم AnyConnect يره اظلالا ئيهاهملالا ،كلذ عمو .ليمعلل IP ناونع ةمواقم رفوي امم ،تقولا لاوط ليمعللا رتوي بمك يلع انكمم و ةكبش يلع اهب ةصاخلا مداوخلاب لاصتالا نادقف كرتد ليمعللا رتوي بمكلا تاقىب بطت لازت ةيره اظلالا ةصاخلا ةكبشلا لاصتالا ةداعيتسالا ةيغالل ال يوط اتقو رمالا قرغتسالا اذا ةسسؤملا (VPN).

ليغش تلا ماظن تاريغتت م عيمج يلع ةزيملا هذه لمعت .رشع يثلاثلا عبرلا لمع يله ؟شوتنكاملال نع اذا م .(XP و تب-64 و تب-32 Vista) Microsoft Windows OS X 10.4؟ يلع

ءارج| مت نكلو ،سكن يلو كام عم لكاشم كانه تناك .Linux و Mac يلع ةزيملا هذه لمعت أ . يفاضلالمعدلا ضع ب لطي Linux لازي ال .كام يلى ةبسنلاب اميس ال ،ارخؤم تاني سحت .اضيأ ةدوجوم ةيساسالا ةفيظولا نكل ،(CSCsm69213 id قب cisco ، CSCsr16670 id قب Cisco) فانئتس| تقوم فاقى| ثودح AnyConnect كردي ال ،Linux ليغش تلا ماظن ب قلعتت اميف :ناربتات هل يساسا لكش ب اذه .(هينبتل/نوكسالا عضو)

- ماظن يلع اموعدم AutoReconnectBehavior ليضفت/في رعت فلم دادع| نوكي نأ نكمي ال ةداع| ةي لمع شحت كلذل ،فانئتسالا/تقؤملا فاقى|إلا معد نودب Linux ليغش تلا فانئتسالا/تقؤملا فاقى|إلا دعب امئاد لاصتالا .
- يلع روفلا يلع لاصتالا ةداع| تاي لمع ءارج| متي ،Macintosh و Microsoft Windows ةيدام ةهجاو يلى عرسأ لوجم ب حمسي امم ،فانئتسالا دعب لمعللا ةسلج يوتسم ةداع| متت ،فانئتسالا/اقىل لعللل امامت كرديم ريغ AnyConnect نأل ،Linux يلع .ةفلتخم لاصتالا ةداع| ةي لمع نأ ينعي دق اذه و (DTLS و SSL) الاو قفنللا يوتسم يلع لاصتالا ليغش تلا ماظن يلع شحت لاصتالا ةداع| تاي لمع لازت ال نكلو .ال يلق لوطأ ةرتف ذخت Linux.

،(ةيكلسللا) لاصتالا شيح نم ةزيملا يلع دويقي يأ كانه له .رشع ثلاثلا عبرلا

Wi-Fi (نم) رخآ ىلإ عضو نم لاقنتال معددي له؟ (كلذ ىلإ امو 3G و Wi-Fi ةكبشو
ىلإ 3G، 3G ىلإ امو، ىكللس ىلإ 3G، ىلإ 3G)؟

a. اذإ VPN لاصتال ىضارتفال رمعل ل او ط ةنعم ةي دام ةهجاوب AnyConnect طبر متي ال
دح هقوف لاصتال ةداع ل الواحم تزواجت اذإ و VPN لاصتال ةمدختسم ل ةي دام ل ةهجاول تدقف
ةباوب ل ىل لوصول ل و احي و ةهجاول كلت مدختسي دعي مل AnyConnect نإف، نعيم لشف
ةسلج و لومخ ل عضو تيقوت تادحو ةي حالص يهتنت ىتح رفوتت تاهجاو ي مادختساب ةنم آل
امم، VA ل ةفلتخم MTU ةميق ىلإ يدؤي دق ةيلع ل ةهجاول ي ف ريغت ياً نأ ظحال . لمعل
ل ىمعلاب صاخ ل IP ناو نع دوجو رارمتسا عم نكلو، هنم ةداع و VA ل ىطعت ىلإ يدؤي
هسفن.

تاهجاول، اهرىغت متي تالكبش ل، ةلطم ةهجاول) ةكبش ل ي ف عاطقنا ياً كانه ناك اذإ
ةقداصم ل ةداع ل ةجاج دجوت ال ثيح، لاصتال ةداع ل AnyConnect ل و احي، (اهرىغت متي تال
ةي دام ل تاهجاول نم ل وحم ىلع اضيأ اذو قبطني . لاصتال ةداع ل ىلع

لالم:

1. wireless off, wired on: AC connection established
2. disconnect wired physically, turn wired on: AC re-established connection in 30 seconds
3. connect wired, turn off wireless: AC re-established connection in 30 secs

فانئتسال ةي لمع ةقداصم متت فيك . رشع عبارل ع برل

a. ةرتفل ىقبي يذال هيلع قداصم ل زيمم ل زمرل ل اسرا ةداع ل كنكمي، ةيتاذل ةرسل ي ف
ةسلجل عاشن ةداع ل م، لمعل ةسلج عاقب

و لاصتال ةداع ل دنع اضيأ LDAP ضيوفت عارج متي له . رشع س ماخ ل ع برل
طقف ةقداصم ل

ي لوال ل ىصوتل ي ف طقف اذو متي أ.

صخفل و أو لوخدل ل ىجست ل بق ام ةزيم ل ىغشت متي له . رشع سداس ل ع برل
فانئتسال دنع ىئاق ل ل

مىيقت ةزيم ل لمام عضو دىدحت متي فوسو . طقف لوال ل ىصوتل ىلع لمعت هذه، ال أ.
ل بقستسم ل ي ف ىرودل عضولا

ةيره اظلال ةصاخ ل ةكبش ل لمح ةنزاوم ب قلعتي امي ف . رشع عباس ل ع برل
وضع ب ةرشابم ىرخأ ةرم ل ىمعل ل لصتي له، لاصتال فانئتساو (LB) (VPN)
ل بق نم هب هلىصوت متي يذال ةعومجم ل ماظن

ةسلجل عاشن ةداع ل DNS ربع فيضم ل مسا ل ةداع ل موقت ال كنأل حىحص اذو، م عن A:
ةل لال

ةلص تاذا تامولعم

- ام دنع DPD لاسرا م تي ال - Cisco [CSCsr63074](#) نم ءاطخألا حيصت فرعم ASA DPD عجرم 7.2.4 عم S2s ىلع لم اخ ريغ ق فنل او ال طعم ريظنلا نوكي
- [Cisco Systems - تادنتس مل او ينقتلا معدلا](#)

ةمچرتل هذه لوح

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاء انء مچي ف ني مدختسمل معد ىوتحم مي دقتل ةيرشبل او
امك ةقيد نوك ت نل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاأل مه تلبل
Cisco ي لخت. فرتحم مچرت مامدقي يتل ةي فارتحال ةمچرتل عم لالحل وه
ىل إأمئاد ةوچرلاب ي صؤت و تامچرتل هذه ةقد نع اهتيل وئسم Cisco
Systems (رفوتم طبارل) ي لصلأل يزي لچن إل دن تسمل