

# ل ةكبشلا ةيؤر ةدحو ةبنت ءاطخأ فاشكتسأ ةنمآلا ةكبشلا تاليلحت يف AnyConnect اهحالصإو

## تايوتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[نيوكتلا ةلدأ](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[اهحالصإو ءاطخألا فاشكتسأ ةيلمع](#)

[SNA نيوكت](#)

[صيخرتلا نم ققحتلا](#)

[NVM تانايب ةبنت قيبطت نم ققحتلا](#)

[NVM ةبنت تانايب لىلا عامتسالا قفدتلا عمجم نيوكت نم ققحتلا](#)

[ةياهنلا ةطقن نيوكت](#)

[NVM فيرعت فلم نم ققحتلا](#)

[\(TND\) هب قوئوملا ةكبشلا فاشكتسأ تاداعا نم ققحتلا](#)

[VPN فيرعت فلم يف TND نيوكت](#)

[NVM فيرعت فلم يف TND نيوكت](#)

[مزحلا طاقتلا عيمجت](#)

[ةلص تاذ بويع](#)

[ةلص تاذ تامولعم](#)

## ةمدقملا

اهحالصإو (NVM) ةكبشلا ةيؤر ةدحو تانايب ةبنت ءاطخأ فاشكتسأ ءارجا دننتملا اذه فصبي (SNA) ةنمآلا ةكبشلا تاليلحت يف

## ةيساسألا تابلطتملا

- ةفرعم Cisco SNA
- ةفرعم Cisco AnyConnect

## نيوكتلا ةلدأ

- [\(NVM\) ةكبشلا ةيؤر ةدحو ةنمآلا ةكبشلا تاليلحت ةياهن ةطقن صيخرت نيوكت ليلد](#)
- [Cisco AnyConnect Administrator Visibility Module، رادصالا 4.10](#)

## تابلطتملا

- تحديث أو 7.3.2 رادصإلإ يف قفدتللا عمجم و SNA ري دم
- SNA ةياهن ةطقن صيخرت
- Cisco AnyConnect ةكبشلال ةيؤر ةدحو عم

## ةمدختسملل تانوكملا

- ةياهنلال ةطقن صيخرت و 7.4.0 رادصإلإ Flow Collection و SNA ري دم
- ةكبشلال ةيؤر ةيناكم او VPN عم 4.10.03104 Cisco AnyConnect ةيطمنللا ةدحو لا
- Windows 10 ليغشلال ماطنل يرهاظلال زاهجلا
- كراشري و تايجمرب

ةصاخ ةيلعم ةئيبي يف ةدوجوملا ةزهجال نم دنتسمللا اذو يف ةدراوللا تامولعملا عاشنإ مت تناك اذا (يضا رتفا). حوسمم نيوكتب دنتسمللا اذو يف ةمدختسمللا ةزهجاللا عيمج تادب رما يال لمحتحمللا ريثاتلل كمهف نم دكأتف، ليغشلال ديقتك تكبش

## اهحالص او عاطخال فاشكتسا ةيلعم

### SNA نيوكت

#### صيخرتللا نم ققحتللا

هيدل، هيلع SNA ةرادا ليحست مت يذال يذال صيخرتلل يرهاظلال باسحللا نأ نم دكأت ةياهنلال طاقن صيخارت

#### NVM تانايب عبتت قيبطت نم ققحتللا

ةياهنلال طاقن نم اهجردي و NVM عبتت تانايب ملتسي SNA قفدت عمجم ناك اذا ام ديكأتل يلي امك ةعباتمللا متي:

1. رذجل دامتعا تانايب مادختساب مكحتللا ةدحو او SSH ربع قفدتللا عمجم يلا لوخدلا لجلس.
2. رما /lancope/var/sw/today/logs/sw.log :ةرتفلا هذه لجلسي GREP 'NVM' لغش.
3. يف اهجردي و NVM تالجلس لاخداب موقوي قفدتللا عمجم ناك اذا ام دكأت، عجت رمللا جارخاللا نم. تانايبلا ةدعاق.

```
ao-fc01-cds:~# grep 'NVM records this period:' /lancope/var/sw/today/logs/sw.log
04:00:01 I-pro-t: NVM records this period: received 0 at 0 rps, inserted 0 at 0 rps, discarded 0
04:05:00 I-pro-t: NVM records this period: received 0 at 0 rps, inserted 0 at 0 rps, discarded 0
04:10:00 I-pro-t: NVM records this period: received 0 at 0 rps, inserted 0 at 0 rps, discarded 0
04:15:00 I-pro-t: NVM records this period: received 0 at 0 rps, inserted 0 at 0 rps, discarded 0
```

بحي كلذ عمو، قال طلاللا لعل NVM تالجلس ي ملتسي مل قفدتللا عمجم نأ ودبي جارخاللا اذو نم NVM عبتت تانايب يلا عامتسالل هنيوكت مت اذا ام ديكأت كي لعل

#### NVM عبتت تانايب يلا عامتسالل قفدتللا عمجم نيوكت نم ققحتللا

1. (UI) قفدتللا عمجم لوؤسم مدختسم ةهجاو يلا لوخدلا لجلس.

2. ةمدقتم تادادع | > معدلا ىل ل لقتنا .

3. حيص لكشب ةبولطملا تامسلا نيوكت نم دكأت :

7.4.0 وأ 7.3.2 رادصإلا SNA

=====

- قباطتي نأ بجي .اهنيوكت مت يتيلا ةميقلل نم ققحتو `nvm_netflow_port` ةمس عقوم دح AnyConnect NVM فيرعت فلم ي ف هنيوكت مت يذلا ذفنملا عم اذه



وأ 514 وأ 2055 سيولو زوجم ريغ ذفنم وه هنيوكت مت يذلا ذفنملا نأ نم دكأت :ةظحالم 8514. ةزيملا ليطعت متي ،"0" يه اهنيوكت مت يتيلا ةميقلل تناك اذا .

لقح قوف رقنا .ةحفصلال لفسأ ىل ريرمتلاب مق ،لقح ضرع متي مل اذا :ةظحالم عجار ،قفتللا عمجم ي ف ةمدقتملا تادادعإلا لوح تامولعملل نم ديزمل .ديج راىخ ةفاضا ةمدقتملا تادادعإلا تنرتنإلا ىلع تاميلعتللا عوضوم .

7.4.1 رادصإلا ،SNA

=====

- قباطتي نأ بجي .اهنيوكت مت يتيلا ةميقلل نم ققحتو `nvm_netflow_port` ةمس عقوم دح AnyConnect NVM فيرعت فلم ي ف هنيوكت مت يذلا ذفنملا عم اذه
- ليطعت متي سف ال او ،1 ىلع ةميقلل نييعت نم دكأتو `enable_nvm` ةمس عقوم دح .ةزيملا



Option Label	Option Value	Delete
enable_nvm	1	<input type="checkbox"/>
nvm_netflow_port	2030	<input type="checkbox"/>

وأ 514 وأ 2055 سيولو زوجم ريغ ذفنم وه هنيوكت مت يذلا ذفنملا نأ نم دكأت :ةظحالم 8514.

لقح قوف رقنا. ةحفصلا لفسأ لىل ريرم تلاب مق، لقح ضرع متي مل اذا: ةظحالم عجار، قفدتلا عمجم يف ةمدقتملا تادادعلا لوح تامولعمل نم ديزمل. ديدج رايخ ةفاضلا ةمدقتملا تادادعلا لتنرتنلا لىل تاميلعتلا عوضوم.

4. ناك اذا امم ققحت، ححص لكشب قفدتلا عمجم لىل ةمدقتملا تادادعلا نيوكت درجم ب. مسق يف حضورم وه امك عارجلا سفن مادختساب، نالاه مادختسلا مت دق دعب نع سايقلا NVM. عبتت نم ققحتلا

5. قفدتلا عمجم لىل ةدوجوملا تادادعلا او AnyConnect NVM عم ةياهنلا ةطقن نيوكت ناك اذا. sw.log فلم هسكعي نأ بجي يف، اححص

```
ao-fc01-cds:~# grep 'NVM records this period:' /lancope/var/sw/today/logs/sw.log
04:35:00 I-pro-t: NVM records this period: received 78 at 0 rps, inserted 78 at 0 rps, discarded 0
04:40:00 I-pro-t: NVM records this period: received 66 at 0 rps, inserted 66 at 0 rps, discarded 0
04:45:00 I-pro-t: NVM records this period: received 91 at 0 rps, inserted 91 at 0 rps, discarded 0
04:50:00 I-pro-t: NVM records this period: received 80 at 0 rps, inserted 80 at 0 rps, discarded 0
```

6. تانايبلا عمجم ناك اذا امم ققحت، NVM تالجس لخدي ال لازي ال قفدتلا عمجم ناك اذا. ححص ةياهنلا طاقن نيوكت نأ نم دكات، لاجي لىل وعو، ةهجالول لىل مزحلا ملتسي

## ةياهنلا ةطقن نيوكت

يدج ب AnyConnect ب ةصاخلا (NVM) ةيرهاظلا ةصاخلا ةكبشلا ةدحو رشن كنكمي بكتملا حطس لىل) ةلقستسملا NVM ةمزح عمم (ب) وأ AnyConnect ةمزح عم (أ): نيتقيرطلا (طاقف AnyConnect).

نيوكت يف قرفلا نمكي شيح، رشنلا تايلمع نم لك هسفن وه بولطملا نيوكتلا "اهب قووثوملا ةكبشلا فاشتكا".

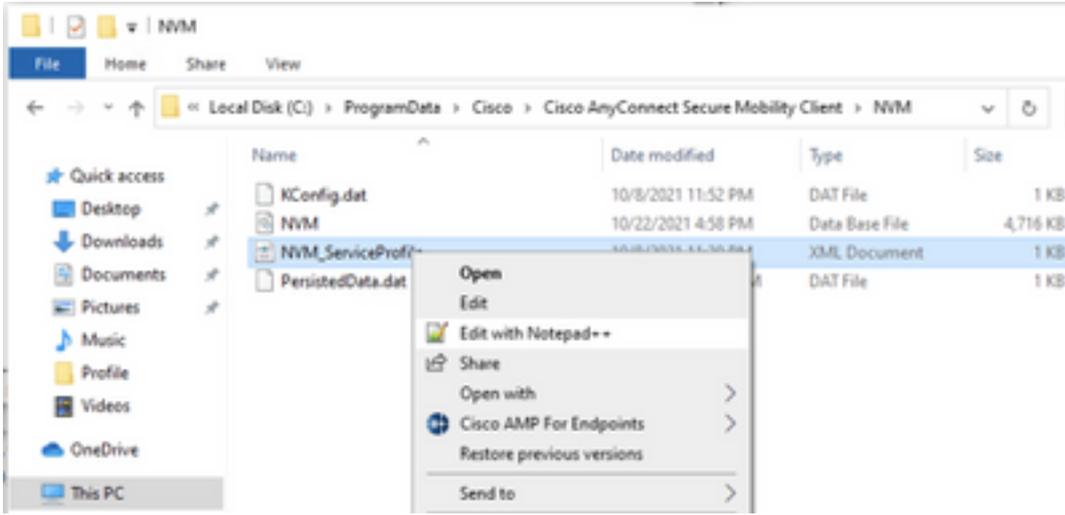
## NVM فيرعت فلم نم ققحتلا

عمجم نيوكت تادادعلا نم دكات و ةياهنلا ةطقن لبق نم مدختسملا NVM فيرعت فلم عقوم ددح

NVM فيرعت فلم عقوم:

- Windows: %ProgramData%\Cisco\AnyConnect Secure Mobility Client\NVM نم Cisco
- MAC: /opt/cisco/anyconnect/nvm

ةدحو" تالشف ال او، NVM\_ServiceProfile وه NVM فيرعت فلم مسانوكي نأ بجي: ةظحالم اهالساوا تانايبلا عيمجت يف "ةكبشلا ةيؤر



فلم رصانع إنف كلذ عمو، كب صاخلا نيوكتلا لىل نVM فيرعت فلم يوتحم دمتعي  
دعب تاطحالملل عجارم نم دكأت. قم اغلال طخالل اهميلعت متي SNA بة لصللا تا ذ فيرعتلا  
نVM: فيرعت فلم لاثم

أو 514 أو 2055 سيلو زوجحم ريغ ذفنم وه هنيوكت متي ذللا ذفنملا نأ نم دكأت: **عظالم**  
ذفنملا هسفن وه اذ فيرعتلا فلم يه هنيوكت متي ذللا ذفنملا نوكتي نأ بجي. 8514  
قفدتلا عمجم يه هنيوكت متي ذللا

متيسف، **نمأل** XML رصنع لىل يوتحي نVM فيرعت فلم ناك اذ هأن نم دكأت: **عظالم**  
عمجمل نكمي الو DTLS مادختساب تاقفدتلا ريفشت متيسف الو، **false** لىل هنييعت  
اهتجال عم قفدتلا.

### (TND) هب قووثوملا ةكبشلا فاشتك تاداعل نم ققحتلا

لىل نوكت ام دنع طقف قفدتلا تامولعم ةكبشلا ةيؤر ةينكامل ةيظمنلا ةدحول لسرت  
تانايبلل عيمجت متي. تانايبلل ةيؤر عيمجت متي ال، يضارتفا لكشبو. اهب قووثوملا ةكبشلا  
دنع تانايبلل عيمجت رمتسيو، فيرعتلا فلم يه وحنلا اذ لىل هنيوكت دنع طقف  
اتقؤم هنيخت متي، اهب قووثوم ريغ ةكبش لىل عيمجتلا مت اذ. ةياهنلا ةطقن لىل صوت  
قفدت عمجم جاتحي. اهب قووثوم ةكبش لىل ةياهنلا ةطقن نوكت ام دنع عمجملا لىل اهلاسراو  
اتقؤم ةنخملل تاقفدتلا ةجال عم موقوي كل يفاضل نيوكت لىل ةنمأل ةكبشلا تاليلحت

(ببولطم لال نيوكتلل [ةكبشلل جراخ اتقوم ةنزم لال افاقفدتلل قفدتلل عمجم نيوكتل](#) عجان).

(TND) ضيرعلل يددرتلل قاطنللا ةزيم لال لال خ نم اهب قووثوم لال ةكبشلللا ةلاح دي دحت نكم ي قاطنللا نيوكتل لال لال خ نم وأ (VPN ةكبشلل فيرعت فلم ي في اهن نيوكتل مت يتللا) VPN ةكبشلل NVM: فيرعت فلم ي في (TND) ضيرعلل يددرتلل

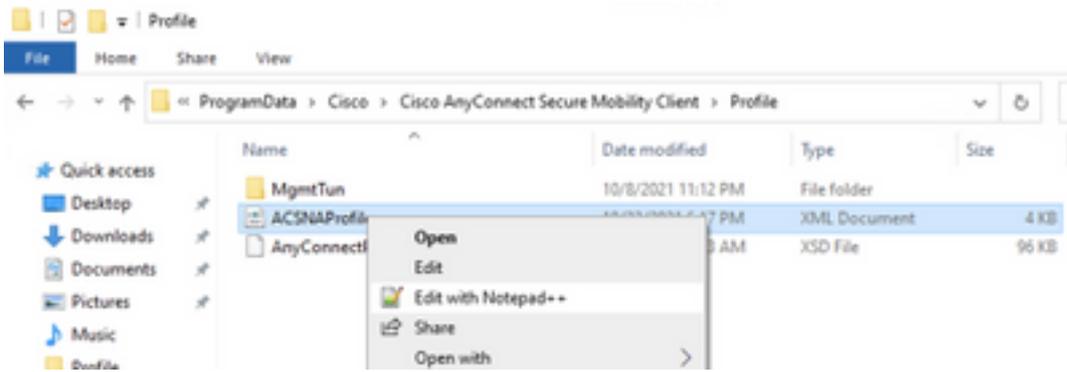
## VPN فيرعت فلم ي في TND نيوكتل

ةلقوتسملل NVM رشن تاي لمعل ارايخ اذه دع ي ال :ةظحال م.

VPN جهن تادادع نم دكأتو ةياهنللا ةطقن لبق نم مدختسملل VPN فيرعت فلم ي عقوم دح 1. اهن نيوكتل مت يتللا يئاقلتللا

VPN فيرعت فلم ي عقوم:

- Windows: %ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
  - MAC: /opt/cisco/anyconnect/profile
- VPN ACSNAPProfile صيصخت فلم ي مسي، لال م ل اذه ي في



2. AutoVPNPolicy رصنعلل ناكم دحو صوصن ررحم مادختساب صيصختللا فلم ي ريرحتب مق. هذه ي في. اهب قووثوم لال ةكبشلللا عجانللا فشك لال هنيوكتل مت يتللا جهنللا ةحص نم دكأت ةلاحللا:

...

هب قووثوم لال ةكبشلللا جهن نم لك نييعت ةلاح ي في: NVM لال صتال ةبسنلاب :ةظحال م

فاشتك ليطعت متي، عيش ي أب مايقلا مدع ىلع هب قووثوملا ريغ ةكبشلا جهنو  
VPN. فيرعت فلم نم اهب قووثوملا ةكبشلا

## NVM فيرعت فلم ي في TND نيوكت

ةمئاق تادادع! ةحص نم دكأتو ةيانهنلا ةطقن لبق نم مدختسملا NVM فيرعت فلم عقوم ددح  
اهنيوكت مت ي تال اهب قووثوملا مداوخلال

NVM فيرعت فلم عقوم:

- Windows: %ProgramData%\Cisco\AnyConnect Secure Mobility Client\NVM نم Cisco
- MAC: /opt/cisco/anyconnect/nvm

...

</NVMProfile>

مت ي تال ةقووثوملا ثبلاو لابق تسالا ةدحو ىل SSL قي قحت لاسرا متي: **ةظالم**  
متي كلذ دعب. انك مم اه ي ل لوصولناك اذا، ةداهش عم بيحتست ي تال او، اهنيوكت  
فلم ررحم ي في ةئزجتال ةومجم عم اهتقباطم و (SHA-256 ةئزجت) ماهبإل ةمصب جارختسإ  
، كلذ عم و، اهب قووثوم ةكبش ي في ةيانهنلا ةطقن نأ ىلع حج انال قباطتال لدي. فيرعتال  
، ةداهشال ةئزجت قباطت مل اذا و؛ لوصول لابق ريغ ثبلاو لابق تسالا ةدحو ناك اذا  
اهب قووثوم ريغ ةكبش ي في ةيانهنلا ةطقن ربتعت ذئنع

ةم و ع دم ريغ ءالكولال فلخ اهب قووثوملا مداوخلال: **ةظالم**

## مزحلا طاقتال عي مجت

تاقفدتال لاسرا نم ققحتلل ةيانهنلا ةطقن ةكبش لوحم ىلع ةمزح طاقتال عي مجت كنك مي  
ققفدتال عمجم ىلإ

بجي في VPN، ةكبش بةلصت م ريغ اهنكلو اهب قووثوم ةكبش ىلع ةيانهنلا ةطقن تناك اذا. أ.  
ي لعل ءال ةكبشال لوحم ىلع طاقتالال نيكمت

امم، اهب قووثوم ةكبش ىلع ةيانهنلا ةطقن نأ ىل AnyConnect ليمع ريشي، ءالجال هذه ي  
مت ي ذللا ذفنملا ربع هنيوكت مت ي ذللا قفدتال عمجم ىلإ اه لاسرا متي تاقفدتال نأ ينع ي  
ةذفان ي في ىرن نأ انك مي امك، ةيانهنلا ةطقن ل ءي داملا ةكبشال لوحم لال خ نم هنيوكت  
كلذ دعب ءضورعمل Wireshark ءذفان و AnyConnect

The screenshot shows a Wireshark capture of network traffic on the interface \*Ethernet0. The filter is set to 'ip.addr == 10.64.0.32'. The packet list shows several UDP packets from source 10.64.0.100 to destination 10.64.0.32 on port 2030. The packet details for frame 131 show the protocol stack: Ethernet II, Internet Protocol Version 4, and User Datagram Protocol (Src Port: 25001, Dst Port: 2030). The packet bytes are shown in hexadecimal and ASCII at the bottom. Overlaid on the Wireshark window is the Cisco AnyConnect Secure Mobility Client window, which displays a green checkmark and the text 'VPN: On a trusted network.' with a 'Connect' button.

ب. دوجوم ايئاقلت ربتت اهناف، AnyConnect VPN ةكبش ب ةلصت م ةياهنلا ةطقن تناك اذا ب. ةيرهظالا ةكبشلا لوحم يلع طاقتلالا نيكم ت بجي كلذل، اه ب قوئوملا ةكبشلا يلع

ةيؤر ةدحو فيرعت فلم في TND نيوكتو ةيظمنلا VPN ةدحو تيبتت ةلاح في: **ةظحالم** ةكبش فاشتكا ذي فننتب ةكبشلا ةيؤر ةينكامل ةيظمنلا ةدحو لا موقت، ةكبشلا ةكبش لخاد يتح هب قوئوم

نأ ينعى امم، VPN ةكبش ب ةلصت م ةياهنلا ةطقن نأ يلى AnyConnect ليمع ريشي نم هنيوكت مت يذلا ذفنملا ربع هنيوكت مت يذلا قفدتلا عمجم يلى اهلا سرام تي تاقفدتلا ةذفان في رن نأ اننكمي امك، (VPN قفن) ةياهنلا ةطقن ل ةيرهظالا ةكبشلا لوحم لالخ كلذ دعب ةضورعملا Wireshark ةذفانو AnyConnect.

متي يذلا VPN فيرعت فلمل "مسقمل قفنلا" نيوكت نمضتت نأ بجي: **ةظحالم** لاسرام تي نلف الاو، قفدتلا عمجم ب صاخلا IP ناو نع هب ةياهنلا ةطقن ليصوت VPN قفن ربع تاقفدتلا

\*Ethernet 3

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.64.0.32

No.	Time	Source	Destination	Protocol	Length	Info
1	18:21:21.444614	192.168.100.4	10.64.0.32	UDP	655	25001 → 2030 Len=613
4	18:21:26.259175	192.168.100.4	10.64.0.32	UDP	384	25001 → 2030 Len=342
5	18:21:26.312552	192.168.100.4	10.64.0.32	UDP	1035	25001 → 2030 Len=993
6	18:21:36.652493	192.168.100.4	10.64.0.32	UDP	989	25001 → 2030 Len=947
7	18:21:47.934603	192.168.100.4	10.64.0.32	UDP	1035	25001 → 2030 Len=993
8	18:22:22.975969	192.168.100.4	10.64.0.32	UDP	648	25001 → 2030 Len=606
11	18:23:03.411742	192.168.100.4	10.64.0.32	UDP	437	25001 → 2030 Len=395
14	18:23:08.507612	192.168.100.4	10.64.0.32	UDP	1035	25001 → 2030 Len=993
15	18:23:23.539073	192.168.100.4	10.64.0.32	UDP		
16	18:24:28.117600	192.168.100.4	10.64.0.32	UDP		
19	18:24:38.007397	192.168.100.4	10.64.0.32	UDP		
20	18:25:28.663613	192.168.100.4	10.64.0.32	UDP		
23	18:25:38.695000	192.168.100.4	10.64.0.32	UDP		
24	18:26:03.586302	192.168.100.4	10.64.0.32	UDP		
27	18:26:33.226458	192.168.100.4	10.64.0.32	UDP		

Cisco AnyConnect Secure Mobility Client

**VPN:** Connected to VPN headend for SNA.

VPN headend for SNA

Disconnect

00:07:05 IPv4

> Frame 1: 655 bytes on wire (5240 bits), 655 bytes captured (5240 bits) on interface \Device\NPF\_{3A925E5D-6F49-4710-8B90-...}

> Ethernet II, Src: Cisco\_3c:7a:00 (00:05:9a:3c:7a:00), Dst: CIMSYS\_33:44:55 (00:11:22:33:44:55)

> Internet Protocol Version 4, Src: 192.168.100.4, Dst: 10.64.0.32

> User Datagram Protocol, Src Port: 25001, Dst Port: 2030

> Data (613 bytes)

0000 00 11 22 33 44 55 00 05 9a 3c 7a 00 08 00 45 00 .."3DU...<z...E-

0010 02 81 8d 5f 00 00 80 11 7c 00 c0 a8 64 04 0a 40 ... ..|...d..@

wireshark\_Ethernet 3B2JUB1.pcapng | Packets: 27 · Displayed: 15 (55.6%) | Profile: Default

c. معجم ىلا تاقفدتلا لاسرا متي نلف ، اهب قوثوم ةكبش ىلع ةياهنلا ةطقن نكت مل اذإ قفدتلا

\*Ethernet0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 10.64.0.32

No.	Time	Source	Destination	Protocol	Length	Info
-----	------	--------	-------------	----------	--------	------

Cisco AnyConnect Secure Mobility Client

**VPN:** Ready to connect.

VPN headend for SNA

Connect

## ةلص تاذ بويع

عبتت تانايب عبتت ةيلمع ىلع رثؤت نأ نكمي يتللة فورعملل بويعلل نم ناناثلل ايللح كانه  
ةنمآلال ةكبشلل تاليلحت ىلع NVM مادختسا

- قب cisco تيار. ETH1 ىلع NVM عبتت تانايب للاخدا FC كرحم ىلع رذعتي [CSCwb84013](#) id
- ارادصا وا 4.10.04071 رادصاإل AnyConnect نم NVM تالچس جارداپ Flow Collector موقبي ال  
Cisco [CSCwb91824](#) نم ءاطألل احيصت فرعم عجار. ىلعأ

## ةلص تاذ تامولعم

- مزلي. (TAC) ةينقتلا ةدعاسملا زكرمب لاصتالا ىجري، ةيفاضا ةدعاسم ىلع لوصحلل  
[ملاعلل ءاخنأ عيمج ي في Cisco معد لاصتلا تاهج](#): حلص معد دقع
- [إنه](#) Cisco نم نامألل تاليلحت عم تجم ةرايز اضيا ك نكمي.
- [Cisco Systems - تادنتس ملاو ينقتلا معدلا](#)

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 ةلخت. فرتمة مچرت مء مء دقء ةل ةل ةفارتحال ةمچرتل عم لاعل او  
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةلصلأل ةزءل ءنل دن تسمل