

AnyConnect Secure Mobility Client نيوكت ةدحاو ل ةرمل رورم ةم لك مادخت ساب

تاوت حمل

[ةمدقم](#)

[ةيساس الابل طت مل](#)

[تابل طت مل](#)

[ةمدخت سمل تانوكت مل](#)

[ةيساس ا تامول عم](#)

[ةمزحل قفدت](#)

[نيوكت مل](#)

[ةكبش ل ل يطيطخت مل مسرل](#)

[ةحصل مل نم ققحت مل](#)

[مدخت سمل ةبرجت](#)

[اهال ص او ااطخ ال فاشكت سا](#)

[حاض ال اة لسو](#)

[قلص تاذا تامول عم](#)

ةمدقم

فيكتل لباق ل نام ال زاهج نيوكتل الاثم دن تسمل اذه فصوي (ASA) Cisco AnyConnect Secure Mobility Client Access.

ةيساس الابل طت مل

تابل طت مل

Cisco Adaptive ل حامس ل هنيوكت متو لم الك ل ل يغشتل دي ق ASA نأ دن تسمل اذه ضررت في نيوكتل تاريخت ارجاب (CLI) رم او ال رطس ةهجاو و (ASDM) Security Device Manager.

ةيلاتل عيضاوم ل ابة فرعم كي دل نوكت نأ Cisco ي صوت:

- ASDM و ASA CLI بةيساس اة فرعم
- Cisco ASA Head End ل ل ع ل ل كشت SSLVPN
- نيل معل اة قداصم بةيساس اة فرعم

ةمدخت سمل تانوكت مل

ةيدامل تانوكت مل او جم اربال اارادص ل ل دن تسمل اذه في ةدراول تامول عم ل اذه دن تسمل

ةةللالت:

- Cisco نم ASA5506 فةكئلل لباقلل نامأل زاآ
- Cisco نم فةكئلل لباقلل نامأل زاآ ءم انرب (1)9.6 راءصإل
- Adaptive Security Device Manager، راءصإل (2)7.8
- AnyConnect، راءصإل 4.5.02033

[ءم ارب لةزنن](#) نم (AnyConnect-win*.pkg) AnyConnect VPN لةم عم ءم زء لةزنن: ءظءالم
Cisco ASA flash ءركا ذىل AnyConnect VPN لةم عم ءسنا. (طقق نةل ءسم ل [ءالم ءلل](#))
SSL VPN لاصنا ءاشنإل ءءىءب الل مءءءسم الل رءوئبمك ءزهءأىل إله لةزنن مءى ءئل او
ءىزم ءل ءل وءصءلل ASA نىوكت لةلء نم [AnyConnect لةم عم ءبءء](#) مءسقق ءءار. ASA عم
ءامول ءم ل نم.

ءصاء ءىلم عم ءىءب ءى ءءوءومل ءزهءأل نم ءنءسم الل اءه ءى ءءراول ءامول ءم ل ءاشنإل مء
ءنءك اءل. (ءىضارءفا) ءوسمم نىوكتب ءنءسم الل اءه ءى ءمءءءسم الل ءزهءأل ءىمء ءءب
رمل ءىل لمءءم الل رىءءءلل كمءهف نم ءكأءف، لىءشءءل ءىق كءءبش

ءىسأسأ ءامول عم

ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم
ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم
ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم

ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم
ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم

- هءرءء ءىش
- كءءل ءىش
- هءلء ءنأ ءىش

ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم
ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم
ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم
ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم
ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم

ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم
ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم
ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم
ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم ءىسأسأ ءامول عم

ءه نم ققءءلل كنكمى. ءنءسم الل اءه قاطن ءءارء هنأل انه OpenOTP نىوكت ءىطءء مءء الل
ءءارقل نم ءىزم لءاطابءالل

إداع OpenOTP

https://www.rcdevs.com/docs/howtos/openotp_quick_start/openotp_quick_start/

OpenOTP ةقداصم ل ASA نيوكت

https://www.rcdevs.com/docs/howtos/asa_ssl_vpn/asa/

ةمزل ق فدت

10.106.50.20 لىل AAA مداخل ةلصت م ل ASA ل ةيخرال ةهجال لىل ةه ةمزل طاق ت م

1. نيوكت لىل فقوطي و ASA وحن لىمعال لاصتا ةئيهت ب AnyConnect م دختسم موقى لىل لاصتا ل طبه و ةومج م ل اب صاخ ل راعت س م ل مسالا و ةومج م ل اب صاخ ل URL ناونع نم بلطي ةطقن ل هذه دنع (لصاصتا ل فيرعت فلم) ةني عم ق فن ةومج لىل دامتعال تانا ب ل ا خ دا م دختسم ل
2. بلط ةمزل (ةقداصم ل بلط هي جوت ةداع م مت ةامتعال تانا ب ل م دختسم ل ل ا خ دا درج م ب ASA نم AAA مداخل لىل (لوصول)

Time	Source	Destination	Protocol	Length	Port	Port	Details
923	2017-10-21 08:20:07.184621	10.106.48.191	10.106.50.20	RADIUS	222	UDP	Access-Request(1) (id=9, l=180)
924	2017-10-21 08:20:07.264100	10.106.50.20	10.106.48.191	RADIUS	122	UDP	Access-Challenge(11) (id=9, l=80)
947	2017-10-21 08:20:13.996393	10.106.48.191	10.106.50.20	RADIUS	240	UDP	Access-Request(1) (id=10, l=198)
948	2017-10-21 08:20:14.065258	10.106.50.20	10.106.48.191	RADIUS	86	UDP	Access-Accept(2) (id=10, l=44)


```
Frame 923: 222 bytes on wire (1776 bits), 222 bytes captured (1776 bits) on interface 0
Ethernet II, Src: CiscoInc_f0:3e:e2 (54:75:d0:f0:3e:e2), Dst: CiscoInc_3c:96:7f (00:23:5e:3c:96:7f)
Internet Protocol Version 4, Src: 10.106.48.191, Dst: 10.106.50.20
User Datagram Protocol, Src Port: 13512 (13512), Dst Port: 1645 (1645)
RADIUS Protocol
  Code: Access-Request (1)
  Packet identifier: 0x9 (9)
  Length: 180
  Authenticator: 8be6bdba618e4fe0be854cdc65d1522c
  [The response to this request is in frame 924]
  Attribute Value Pairs
    AVP: 1=7 t=User-Name(1): cisco
      User-Name: cisco
    AVP: 1=18 t=User-Password(2): Encrypted
      User-Password (encrypted): 6e315c38e33f3832226b3f37944127a0
```

3. ت ناك اذا ةامتعال تانا ب ةحص نم ق قحتي ةامتعال لىل ةقداصم ل بلط لوصول دعب ةرم رورم ةمزل ل ا خ دا م دختسم ل نم بلطي شي لوصول ي دختب AAA مداخل دري ةحص لىل ASA ةمزل ل Access-Reject ةمزل لاسرا م تي ةحص ل رىغ ةامتعال تانا ب ل ا خ ي ةدحاو

Time	Source IP	Destination IP	Protocol	Source Port	Destination Port	Details
923 2017-10-21 08:20:07.184621	10.106.48.191	10.106.50.20	RADIUS	222	UDP	Access-Request(1) (id=9, l=180)
924 2017-10-21 08:20:07.264100	10.106.50.20	10.106.48.191	RADIUS	122	UDP	Access-Challenge(11) (id=9, l=80)
947 2017-10-21 08:20:13.996393	10.106.48.191	10.106.50.20	RADIUS	240	UDP	Access-Request(1) (id=10, l=198)
948 2017-10-21 08:20:14.065258	10.106.50.20	10.106.48.191	RADIUS	86	UDP	Access-Accept(2) (id=10, l=44)

```

Frame 924: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
Ethernet II, Src: CiscoInc_3c:96:7f (00:23:5e:3c:96:7f), Dst: CiscoInc_f0:3e:e2 (54:75:d0:f0:3e:e2)
Internet Protocol Version 4, Src: 10.106.50.20, Dst: 10.106.48.191
User Datagram Protocol, Src Port: 1645 (1645), Dst Port: 13512 (13512)
RADIUS Protocol
Code: Access-Challenge (11)
Packet identifier: 0x9 (9)
Length: 80
Authenticator: 291ef37118c398ae35187b27252dcc74
[This is a response to a request in frame 923]
[Time from request: 0.079479000 seconds]
Attribute Value Pairs
AVP: l=18 t=State(24): 6a6557357a6d625a6749326531664134
AVP: l=36 t=Reply-Message(18): Enter your TOKEN one-time password
Reply-Message: Enter your TOKEN one-time password
AVP: l=6 t=Session-Timeout(27): 90

```

4. لكش ي ف ة ق داصم ل بلط لاسرا متي ، ة دح اول ا ة رمل ا رورم ة م لك مدخت سمل ل خ دي امن ي ب

AAA مداخ لى ل ASA نم لوصول ا بلط ة مزح

Time	Source IP	Destination IP	Protocol	Source Port	Destination Port	Details
923 2017-10-21 08:20:07.184621	10.106.48.191	10.106.50.20	RADIUS	222	UDP	Access-Request(1) (id=9, l=180)
924 2017-10-21 08:20:07.264100	10.106.50.20	10.106.48.191	RADIUS	122	UDP	Access-Challenge(11) (id=9, l=80)
947 2017-10-21 08:20:13.996393	10.106.48.191	10.106.50.20	RADIUS	240	UDP	Access-Request(1) (id=10, l=198)
948 2017-10-21 08:20:14.065258	10.106.50.20	10.106.48.191	RADIUS	86	UDP	Access-Accept(2) (id=10, l=44)

```

Frame 947: 240 bytes on wire (1920 bits), 240 bytes captured (1920 bits)
Ethernet II, Src: CiscoInc_f0:3e:e2 (54:75:d0:f0:3e:e2), Dst: CiscoInc_3c:96:7f (00:23:5e:3c:96:7f)
Internet Protocol Version 4, Src: 10.106.48.191, Dst: 10.106.50.20
User Datagram Protocol, Src Port: 13512 (13512), Dst Port: 1645 (1645)
RADIUS Protocol
Code: Access-Request (1)
Packet identifier: 0xa (10)
Length: 198
Authenticator: 8be6bdba618e4fe0be854cdc65d1522c
[The response to this request is in frame 948]
Attribute Value Pairs
AVP: l=7 t=User-Name(1): cisco
User-Name: cisco
AVP: l=18 t=User-Password(2): Encrypted
User-Password (encrypted): 3b6f1e69bd063832226b3f37944127a0

```

5. ة مزح لاسرا متي ، AAA مداخ لى ل ة حاجن ب ة دح اول ا ة رمل ا رورم ة م لك ة حص نم ق قحت ل ا درجم ب و

لامتكا لى ل ا دي ة وى امم حاجن ب مدخت سمل ا ة ق داصم متي و ، لى ل ا مدخال نم لوصول ل و ب ق

نيل ل م ا ل ا تاذ ة ق داصم ل ا ة ل م ع .

Time	Source IP	Destination IP	Protocol	Source Port	Destination Port	Details
923 2017-10-21 08:20:07.184621	10.106.48.191	10.106.50.20	RADIUS	222	UDP	Access-Request(1) (id=9, l=180)
924 2017-10-21 08:20:07.264100	10.106.50.20	10.106.48.191	RADIUS	122	UDP	Access-Challenge(11) (id=9, l=80)
947 2017-10-21 08:20:13.996393	10.106.48.191	10.106.50.20	RADIUS	240	UDP	Access-Request(1) (id=10, l=198)
948 2017-10-21 08:20:14.065258	10.106.50.20	10.106.48.191	RADIUS	86	UDP	Access-Accept(2) (id=10, l=44)

```

Frame 948: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
Ethernet II, Src: CiscoInc_3c:96:7f (00:23:5e:3c:96:7f), Dst: CiscoInc_f0:3e:e2 (54:75:d0:f0:3e:e2)
Internet Protocol Version 4, Src: 10.106.50.20, Dst: 10.106.48.191
User Datagram Protocol, Src Port: 1645 (1645), Dst Port: 13512 (13512)
RADIUS Protocol
Code: Access-Accept (2)
Packet identifier: 0xa (10)
Length: 44
Authenticator: d86b54ccaf531e9efc116cfb11d91d75
[This is a response to a request in frame 947]
[Time from request: 0.068865000 seconds]
Attribute Value Pairs
AVP: l=24 t=Reply-Message(18): Authentication success
Reply-Message: Authentication success

```

AnyConnect صيخرت تامولعم

Cisco AnyConnect Secure Mobility Client صيخارت لوح ة دي فم تامولعم لى ل ا طاب ترال ا ضعب لى ل ا مي ف

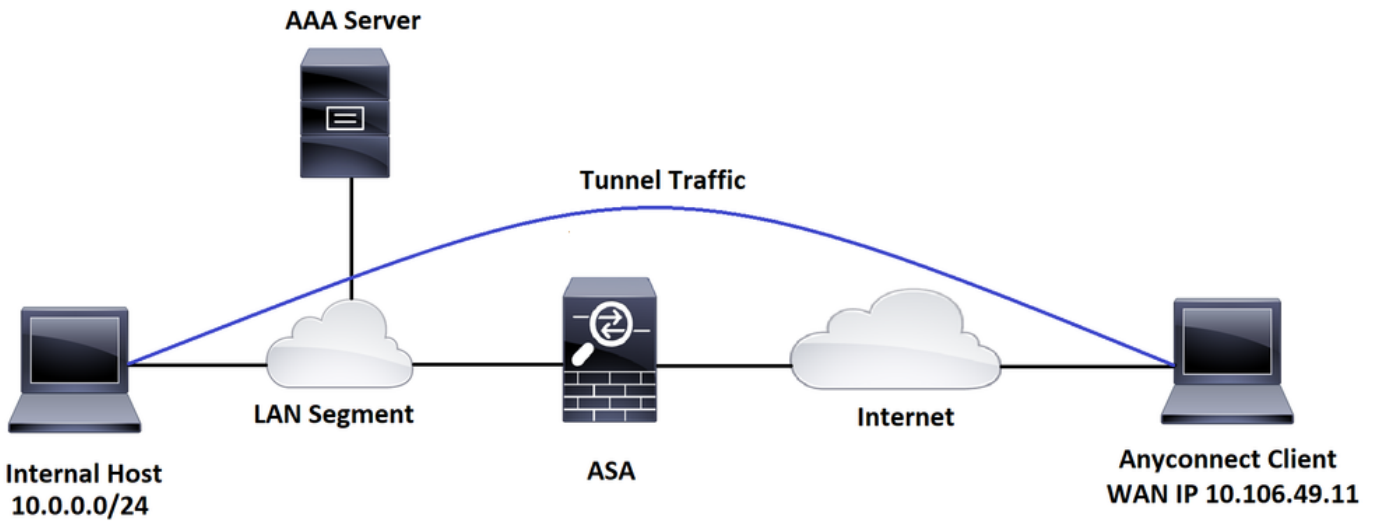
- ةرركتم ال AnyConnect صيخرت ةلئسأ ىلع لوصحلل [دنتسملا اذه](#) عجار
- صيخارت لوح تامولعم ىلع لوصحلل Cisco [نم AnyConnect ب ل ط ل ي ل د](#) ىلا عجار AnyConnect Top و Plus.

نيوكتلا

ASA ىلع Cisco AnyConnect Secure Mobility Client نيوكت ةي فيك مسقلا اذه فصي

نم ديزم ىلع لوصحلل (طقف [ني ل ج س م ل ا](#) ءالمعلل) [رم اوألا ث ح ب ة ا د ا](#) مدختسأ :ةظحالم مسقلا اذه في ةمدختسملا رم اوألا لوح تامولعملا

ةكبش ل ل ي ط ي ط خ ت ل ا م س ر ل ا



ASDM AnyConnect نيوكت جلاعم

دكأت AnyConnect Secure Mobility Client نيوكتل AnyConnect نيوكت جلاعم مادختسإ نكمي ةعباتملا لبق ASA ةي امح رادجل Flash/disk ةركاذ ىلا AnyConnect ليمع ةمزح ليمحت نم

نيوكتل جلاعم لال خ نم AnyConnect Secure Mobility Client نيوكتل تاوطلخال هذه لمكأ

يجري، هتي بثتو AnyConnect لي زنتل ASDM ربع قفنلا ماسقنا نيوكت ىلع لوصحلل دنتسملا اذه ىلا عوجرلا


```
no arp permit-nonconnected
```

```
route outside 0.0.0.0 0.0.0.0 10.106.56.1 1
```

```
!-----Configure AAA server -----
```

```
aaa-server RADIUS_OTP protocol radius
```

```
aaa-server RADIUS_OTP (outside) host 10.106.50.20
```

```
key *****
```

```
!-----Configure Trustpoint containing ASA Identity Certificate -----
```

```
crypto ca trustpoint ASDM_Trustpoint 0
```

```
enrollment self
```

```
subject-name CN=bg1anyconnect.cisco.com
```

```
keypair self
```

```
!-----Apply trustpoint on outside interface-----
```

```
ssl trust-point ASDM_Trustpoint0 outside
```

```
!-----Enable AnyConnect and configuring AnyConnect Image-----
```

```
webvpn
```

```
enable outside
```

```
anyconnect image disk0:/anyconnect-win-4.5.02033-webdeploy-k9.pkg 1
```

```
anyconnect enable
```

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

```
!-----Group Policy configuration-----
```

```

group-policy GroupPolicy_ANYCONNECT-PROFILE interna1
group-policy GroupPolicy_ANYCONNECT-PROFILE attributes
  dns-server value 10.10.10.99
  vpn-tunnel-protocol ssl-client
  split-tunnel-policy tunnelspecified
  split-tunnel-network-list value SPLIT-TUNNEL
  default-domain value cisco.com

!-----Tunnel-Group (Connection Profile) Configuration-----

tunnel-group ANYCONNECT_PROFILE type remote-access
tunnel-group ANYCONNECT_PROFILE general-attributes
  address-pool ANYCONNECT-POOL
  authentication-server-group RADIUS_OTP
  default-group-policy GroupPolicy_ANYCONNECT-PROFILE
tunnel-group ANYCONNECT_PROFILE webvpn-attributes
  group-alias ANYCONNECT-PROFILE enable

: end

```

اذه ىلإ عجرا AnyConnect، لىم مع تالاصتال ASA ىل ع اهتېبثتو ةيچراخ ةه ج ةداهش نيوكتل دنن سملال.

[ASA SSL ةي مقربلا ةداهش لال نيوكتل](#)

ةحصلال نم ققحتلال

جحص لكشب نيوكتل لىم ع ديكأتل مسقلا اذه مدختسا

مدختسا show رماو اضعب (طقف نولج سملال عالمعلال) جارخالال مجرتم ةادأ معدت: عظالم show رمالال جارخالال لىلحت ضرعل "جارخالال مجرتم ةادأ"

هتاءاصحو AnyConnect لىم ع قلا ح ديكأتل هذه ضرعل رمالال ذيفنت نكمي


```
ASA(config)# show vpn-sessiondb anyconnect
```

Session Type: AnyConnect

```
Username      : cisco                Index      : 1
Assigned IP   : 192.168.100.1        Public IP  : 10.106.49.111
Protocol      : AnyConnect-Parent DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none DTLS-Tunnel: (1)AES256
Hashing       : AnyConnect-Parent: (1)none DTLS-Tunnel: (1)SHA1
Bytes Tx      : 15122                Bytes Rx   : 5897
Group Policy  : GroupPolicy_ANYCONNECT-PROFILE
Tunnel Group  : ANYCONNECT_PROFILE
Login Time    : 14:47:09 UTC Wed Nov 1 2017
Duration      : 1h:04m:52s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                  VLAN       : none
Audt Sess ID  : 000000000000100059f9de6d
Security Grp  : none
```

```
ASA(config)# show vpn-sessiondb detail anyconnect filter name cisco
```

Session Type: AnyConnect Detailed

```
Username      : cisco                Index      : 1
Assigned IP   : 192.168.100.1        Public IP  : 10.106.49.111
Protocol      : AnyConnect-Parent DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none DTLS-Tunnel: (1)AES256
Hashing       : AnyConnect-Parent: (1)none DTLS-Tunnel: (1)SHA1
Bytes Tx      : 15122                Bytes Rx   : 5897
```

Pkts Tx : 10 Pkts Rx : 90
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : GroupPolicy_ANYCONNECT-PROFILE
Tunnel Group : ANYCONNECT_PROFILE
Login Time : 14:47:09 UTC Wed Nov 1 2017
Duration : 1h:04m:55s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 000000000000100059f9de6d
Security Grp : none

AnyConnect-Parent Tunnels: 1

DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 1.1
Public IP : 10.106.49.111
Encryption : none Hashing : none
TCP Src Port : 53113 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 1 Minutes
Client OS : win
Client OS Ver: 6.1.7601 Service Pack 1
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.5.02033
Bytes Tx : 7561 Bytes Rx : 0
Pkts Tx : 5 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:

Tunnel ID : 1.3

Assigned IP : 192.168.100.1 Public IP : 10.106.49.111
Encryption : AES256 Hashing : SHA1
Ciphersuite : AES256-SHA
Encapsulation: DTLSv1.0 UDP Src Port : 63257
UDP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 0 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.5.02033
Bytes Tx : 0 Bytes Rx : 5801
Pkts Tx : 0 Pkts Rx : 88
Pkts Tx Drop : 0 Pkts Rx Drop : 0

مدخست سمللة برجت

لوالا يوتسملا مادختسا متي؛ ةفلتخم ءاطخأ حيحصت تايوتسم نييعت كنكمي في باهسإلا ديزي نأ نكمي، ءاطخألا حيحصت يوتسم ريغتب تمق اذا. أيضارتفا جاتنإلا تاييبي فةصاخو، رذحب كلذب مق. ءاطخألا حيحصت.

ءاحالصإو دراوال AnyConnect ليعم لاصتال ةلمالكلا ةقداصملا ةيلمع ءاطخأ فاشكتسال ةيلائلا ءاطخألا حيحصت تايلمع مادختسا كنكمي:

- debug radius all
- (ةبساوملاو ضيوفتلاو ةقداصملا) aaa ةقداصم ءاطخأ حيحصت
- debug wrbvpn AnyConnect

ءاحتص مدع وأ مدختسملا دامتعا تانايب ةحص رماوالا هذء دكؤت.

رورملا ةملك <user> مدختسملا مسا [<host_ip>] <aaa_server_group> AAA مءاخ ةقداصم رابتخا <password>

رورملا ةملك و مدختسملا مسا حيحصت ةلاح في

```
ASA(config)# test aaa authentication RADIUS_OTP host 10.106.50.20
```

```
Username: cisco
```

```
Password: *****
```

```
INFO: Attempting Authentication test to IP address <10.106.50.20> (timeout: 12 seconds)
```

```
ERROR: Authentication Challenged: No error
```

رورم ةملك لاخدا مدختسملا نم عقوتي AAA مءاخ نأل ارظن هنا ةقبيقحب ريخألا أطلخا قلعتي لوخد رابتخالا اءه نمضتي الو، رورملا ةملك و مدختسملا مسال ججانلا رشنلا لىل ةءحاو ةرم هلاسرا متي ذل Access-Challenge ىرت تنأف، طشن لكشب OTP لوكوتوربل مدختسملا لىل ASA. ءاطخ رهظي ال كلذل ةباجتسا لىل AAA مءاخ ةطساوب

رورملا ةملك و/و مدختسملا مسا ةحص مدع ةلاح في

```
ASA(config)# test aaa authentication RADIUS_OTP host 10.106.50.20
```

```
Username: cisco
```

```
Password: ***
```

```
INFO: Attempting Authentication test to IP address <10.106.50.20> (timeout: 12 seconds)
```

```
ERROR: Authentication Rejected: AAA failure
```

اذه هبشي ام لمع دادعإ نم ءاطخألا حيحصت

حاضري الة لى سو

AnyConnect Client Real IP: 10.106.49.111

ASA IP: 10.106.48.191

```
ASA(config)# debug radius all
ASA(config)# debug aaa authentication
debug aaa authentication enabled at level 1
radius mkreq: 0x8
alloc_rip 0x74251058
    new request 0x8 --> 7 (0x74251058)
got user 'cisco'
got password
add_req 0x74251058 session 0x8 id 7
RADIUS_REQUEST
radius.c: rad_mkpkt
rad_mkpkt: ip:source-ip=10.106.49.111
```

RADIUS packet decode (authentication request)

```
-----
Raw packet data (length = 180).....
01 07 00 b4 b6 c2 bf 25 cf 80 53 a9 a2 3d c8 ca | .....%..S..=..
74 05 27 5c 01 07 63 69 73 63 6f 02 12 d7 99 45 | t.'\..cisco....E
6e 0f 46 71 bc 52 47 b0 81 b4 18 ae 34 05 06 00 | n.Fq.RG.....4...
00 40 00 1e 0f 31 30 2e 31 30 36 2e 34 38 2e 31 | .@...10.106.48.1
39 31 1f 0f 31 30 2e 31 30 36 2e 34 39 2e 31 31 | 91..10.106.49.11
31 3d 06 00 00 00 05 42 0f 31 30 2e 31 30 36 2e | 1=.....B.10.106.
34 39 2e 31 31 31 04 06 0a 6a 30 bf 1a 22 00 00 | 49.111...j0..."..
00 09 01 1c 69 70 3a 73 6f 75 72 63 65 2d 69 70 | ....ip:source-ip
3d 31 30 2e 31 30 36 2e 34 39 2e 31 31 31 1a 1a | =10.106.49.111..
```

```
00 00 0c 04 92 14 41 4e 59 43 4f 4e 4e 45 43 54 | .....ANYCONNECT
2d 50 52 4f 46 49 4c 45 1a 0c 00 00 0c 04 96 06 | -PROFILE.....
00 00 00 02 | ....
```

Parsed packet data.....

Radius: Code = 1 (0x01)

Radius: Identifier = 7 (0x07)

Radius: Length = 180 (0x00B4)

Radius: Vector: B6C2BF25CF8053A9A23DC8CA7405275C

Radius: Type = 1 (0x01) User-Name

Radius: Length = 7 (0x07)

Radius: Value (String) =

```
63 69 73 63 6f | cisco
```

Radius: Type = 2 (0x02) User-Password

Radius: Length = 18 (0x12)

Radius: Value (String) =

```
d7 99 45 6e 0f 46 71 bc 52 47 b0 81 b4 18 ae 34 | ..En.Fq.RG.....4
```

Radius: Type = 5 (0x05) NAS-Port

Radius: Length = 6 (0x06)

Radius: Value (Hex) = 0x4000

Radius: Type = 30 (0x1E) Called-Station-Id

Radius: Length = 15 (0x0F)

Radius: Value (String) =

```
31 30 2e 31 30 36 2e 34 38 2e 31 39 31 | 10.106.48.191
```

Radius: Type = 31 (0x1F) Calling-Station-Id

Radius: Length = 15 (0x0F)

Radius: Value (String) =

```
31 30 2e 31 30 36 2e 34 39 2e 31 31 31 | 10.106.49.111
```

Radius: Type = 61 (0x3D) NAS-Port-Type

Radius: Length = 6 (0x06)

Radius: Value (Hex) = 0x5

Radius: Type = 66 (0x42) Tunnel-Client-Endpoint

Radius: Length = 15 (0x0F)

Radius: Value (String) =

31 30 2e 31 30 36 2e 34 39 2e 31 31 31 | 10.106.49.111

Radius: Type = 4 (0x04) NAS-IP-Address

Radius: Length = 6 (0x06)

Radius: Value (IP Address) = 10.106.48.191 (0x0A6A30BF)

Radius: Type = 26 (0x1A) Vendor-Specific

Radius: Length = 34 (0x22)

Radius: Vendor ID = 9 (0x00000009)

Radius: Type = 1 (0x01) Cisco-AV-pair

Radius: Length = 28 (0x1C)

Radius: Value (String) =

69 70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e | ip:source-ip=10.

31 30 36 2e 34 39 2e 31 31 31 | 106.49.111

Radius: Type = 26 (0x1A) Vendor-Specific

Radius: Length = 26 (0x1A)

Radius: Vendor ID = 3076 (0x00000C04)

Radius: Type = 146 (0x92) Tunnel-Group-Name

Radius: Length = 20 (0x14)

Radius: Value (String) =

41 4e 59 43 4f 4e 4e 45 43 54 2d 50 52 4f 46 49 | ANYCONNECT-PROFI

4c 45 | LE

Radius: Type = 26 (0x1A) Vendor-Specific

Radius: Length = 12 (0x0C)

Radius: Vendor ID = 3076 (0x00000C04)

Radius: Type = 150 (0x96) Client-Type

Radius: Length = 6 (0x06)

Radius: Value (Integer) = 2 (0x0002)

send pkt 10.106.50.20/1645

rip 0x74251058 state 7 id 7

rad_vrfy() : response message verified

rip 0x74251058

: chall_state ''

: state 0x7

: reqauth:

b6 c2 bf 25 cf 80 53 a9 a2 3d c8 ca 74 05 27 5c

: info 0x74251190

session_id 0x8

request_id 0x7

user 'cisco'

response '***'

app 0

reason 0

skey 'testing123'

sip 10.106.50.20

type 1

RADIUS packet decode (response)

Raw packet data (length = 80).....

0b 07 00 50 ed 7a 06 92 f7 18 16 6b 97 d4 83 5f		...P.z.....k..._
be 9b d7 29 18 12 75 6b 35 36 58 49 4f 6e 35 31		...)..uk56XI0n51
58 36 4b 75 4c 74 12 24 45 6e 74 65 72 20 79 6f		X6KuLt.\$Enter yo
75 72 20 54 4f 4b 45 4e 20 6f 6e 65 2d 74 69 6d		ur TOKEN one-tim
65 20 70 61 73 73 77 6f 72 64 1b 06 00 00 00 5a		e password.....Z

Parsed packet data.....

Radius: Code = 11 (0x0B)

Radius: Identifier = 7 (0x07)

Radius: Length = 80 (0x0050)

Radius: Vector: ED7A0692F718166B97D4835FBE9BD729

Radius: Type = 24 (0x18) State

Radius: Length = 18 (0x12)

Radius: Value (String) =

75 6b 35 36 58 49 4f 6e 35 31 58 36 4b 75 4c 74 | uk56XIO n51X6KuLt

Radius: Type = 18 (0x12) Reply-Message

Radius: Length = 36 (0x24)

Radius: Value (String) =

45 6e 74 65 72 20 79 6f 75 72 20 54 4f 4b 45 4e | Enter your TOKEN

20 6f 6e 65 2d 74 69 6d 65 20 70 61 73 73 77 6f | one-time passwo

72 64 | rd

Radius: Type = 27 (0x1B) Session-Timeout

Radius: Length = 6 (0x06)

Radius: Value (Hex) = 0x5A

rad_procpkt: CHALLENGE

radius mkreq: 0x8

old request 0x8 --> 8 (0x74251058), state 3

wait pass - pass '***'. make request

RADIUS_REQUEST

radius.c: rad_mkpkt

rad_mkpkt: ip:source-ip=10.106.49.111

RADIUS packet decode (authentication request)

Raw packet data (length = 198).....

01 08 00 c6 b6 c2 bf 25 cf 80 53 a9 a2 3d c8 ca |%.S.=..

74 05 27 5c 01 07 63 69 73 63 6f 02 12 83 c4 00 | t.'\..cisco.....

3e 56 73 71 bc 52 47 b0 81 b4 18 ae 34 05 06 00 | >Vsq.RG.....4...

00 40 00 1e 0f 31 30 2e 31 30 36 2e 34 38 2e 31 | .@...10.106.48.1

39 31 1f 0f 31 30 2e 31 30 36 2e 34 39 2e 31 31 | 91..10.106.49.11

```

31 3d 06 00 00 00 05 42 0f 31 30 2e 31 30 36 2e | 1=.....B.10.106.
34 39 2e 31 31 31 04 06 0a 6a 30 bf 18 12 75 6b | 49.111...j0...uk
35 36 58 49 4f 6e 35 31 58 36 4b 75 4c 74 1a 22 | 56XIOn51X6KuLt."
00 00 00 09 01 1c 69 70 3a 73 6f 75 72 63 65 2d | .....ip:source-
69 70 3d 31 30 2e 31 30 36 2e 34 39 2e 31 31 31 | ip=10.106.49.111
1a 1a 00 00 0c 04 92 14 41 4e 59 43 4f 4e 4e 45 | .....ANYCONNE
43 54 2d 50 52 4f 46 49 4c 45 1a 0c 00 00 0c 04 | CT-PROFILE.....
96 06 00 00 00 02 | .....

```

Parsed packet data.....

Radius: Code = 1 (0x01)

Radius: Identifier = 8 (0x08)

Radius: Length = 198 (0x00C6)

Radius: Vector: B6C2BF25CF8053A9A23DC8CA7405275C

Radius: Type = 1 (0x01) User-Name

Radius: Length = 7 (0x07)

Radius: Value (String) =

```
63 69 73 63 6f | cisco
```

Radius: Type = 2 (0x02) User-Password

Radius: Length = 18 (0x12)

Radius: Value (String) =

```
83 c4 00 3e 56 73 71 bc 52 47 b0 81 b4 18 ae 34 | ...>Vsq.RG.....4
```

Radius: Type = 5 (0x05) NAS-Port

Radius: Length = 6 (0x06)

Radius: Value (Hex) = 0x4000

Radius: Type = 30 (0x1E) Called-Station-Id

Radius: Length = 15 (0x0F)

Radius: Value (String) =

```
31 30 2e 31 30 36 2e 34 38 2e 31 39 31 | 10.106.48.191
```

Radius: Type = 31 (0x1F) Calling-Station-Id

Radius: Length = 15 (0x0F)

Radius: Value (String) =

31 30 2e 31 30 36 2e 34 39 2e 31 31 31 | 10.106.49.111

Radius: Type = 61 (0x3D) NAS-Port-Type

Radius: Length = 6 (0x06)

Radius: Value (Hex) = 0x5

Radius: Type = 66 (0x42) Tunnel-Client-Endpoint

Radius: Length = 15 (0x0F)

Radius: Value (String) =

31 30 2e 31 30 36 2e 34 39 2e 31 31 31 | 10.106.49.111

Radius: Type = 4 (0x04) NAS-IP-Address

Radius: Length = 6 (0x06)

Radius: Value (IP Address) = 10.106.48.191 (0x0A6A30BF)

Radius: Type = 24 (0x18) State

Radius: Length = 18 (0x12)

Radius: Value (String) =

75 6b 35 36 58 49 4f 6e 35 31 58 36 4b 75 4c 74 | uk56XI0n51X6KuLt

Radius: Type = 26 (0x1A) Vendor-Specific

Radius: Length = 34 (0x22)

Radius: Vendor ID = 9 (0x00000009)

Radius: Type = 1 (0x01) Cisco-AV-pair

Radius: Length = 28 (0x1C)

Radius: Value (String) =

69 70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e | ip:source-ip=10.

31 30 36 2e 34 39 2e 31 31 31 | 106.49.111

Radius: Type = 26 (0x1A) Vendor-Specific

Radius: Length = 26 (0x1A)

Radius: Vendor ID = 3076 (0x00000C04)

Radius: Type = 146 (0x92) Tunnel-Group-Name

Radius: Length = 20 (0x14)

Radius: Value (String) =

41 4e 59 43 4f 4e 4e 45 43 54 2d 50 52 4f 46 49 | ANYCONNECT-PROFI

Radius: Type = 26 (0x1A) Vendor-Specific

Radius: Length = 12 (0x0C)

Radius: Vendor ID = 3076 (0x00000C04)

Radius: Type = 150 (0x96) Client-Type

Radius: Length = 6 (0x06)

Radius: Value (Integer) = 2 (0x0002)

send pkt 10.106.50.20/1645

rip 0x74251058 state 7 id 8

rad_vrfy() : response message verified

rip 0x74251058

: chall_state 'uk56XI0n51X6KuLt'

: state 0x7

: reqauth:

b6 c2 bf 25 cf 80 53 a9 a2 3d c8 ca 74 05 27 5c

: info 0x74251190

session_id 0x8

request_id 0x8

user 'cisco'

response '***'

app 0

reason 0

skey 'testing123'

sip 10.106.50.20

type 1

RADIUS packet decode (response)

Raw packet data (length = 44).....

02 08 00 2c c0 80 63 1c 3e 43 a4 bd 46 78 bd 68 | ...,..c.>C..Fx.h

```
49 29 23 bd 12 18 41 75 74 68 65 6e 74 69 63 61 | I)#...Authentica
74 69 6f 6e 20 73 75 63 63 65 73 73 | tion success
```

Parsed packet data.....

Radius: Code = 2 (0x02)

Radius: Identifier = 8 (0x08)

Radius: Length = 44 (0x002C)

Radius: Vector: C080631C3E43A4BD4678BD68492923BD

Radius: Type = 18 (0x12) Reply-Message

Radius: Length = 24 (0x18)

Radius: Value (String) =

```
41 75 74 68 65 6e 74 69 63 61 74 69 6f 6e 20 73 | Authentication s
75 63 63 65 73 73 | uccess
```

rad_procpkt: ACCEPT

RADIUS_ACCESS_ACCEPT: normal termination

RADIUS_DELETE

remove_req 0x74251058 session 0x8 id 8

free_rip 0x74251058

radius: send queue empty

قلم تاذ تامول عم

- [يلع مّس قملا يقف نللا لاصتالا مادختساب AnyConnect Secure Mobility Client نيوكت ASA](#)
- [نم ثبل او لابقتسال اة دحو نيوكت يلع AnyConnect عالم عمل RSA SecureID اة قداصم Cisco IOS](#)
- [ACS و ASA ل SDI لوكوت وربو زي ممللا RSA ماداخ مادختسا](#)
- [ليلدو طي طختلا او اة داهشلا اة حص نم ققحتلا عم اة قود زملا ASA AnyConnect اة قداصم](#)

[قۇبۇل قىلىنغان نىيەتلەر](#)

- [Cisco Systems - تادىت سىستېمىسىنىڭ نىيەتلىرى](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئ. ةصاغل مه تلبل
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتهال ةمچرتل عم لاعل وه
ىل إامءاد ةوچرلاب يصوت و تامچرتل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارل) يلصلأل يزىلچنل دن تسمل