

ASA AnyConnect Secure Mobility Client ةقداصم نيوكت

تايوتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[نيوكتلا](#)

[AnyConnect ةداهش](#)

[ASA ةلغ ةداهشلا تيبثت](#)

[ةداهشلا نم ققحتلا او ةداخال ةقداصملا ل ASA نيوكت](#)

[رابتخا](#)

[ءاطخألا ءيحصت](#)

[ةداهشلا نم ققحتلا او ةجودزم ةقداصملا ل ASA نيوكت](#)

[رابتخا](#)

[ءاطخألا ءيحصت](#)

[ةقبسم ةئبعتو ةجودزم ةقداصملا ل ASA نيوكت](#)

[رابتخا](#)

[ءاطخألا ءيحصت](#)

[تاداهش طيختو ةجودزم ةقداصملا ل ASA نيوكت](#)

[رابتخا](#)

[ءاطخألا ءيحصت](#)

[ءءالصل او ءاطخألا فاشكتسا](#)

[ةدوجوم ريغ ءءالصل ةداهشلا](#)

[ةلصل تاذا تامولعم](#)

ةمدقملا

ةقداصم مدختسي ASA AnyConnect Secure Mobility Client لوصول نيوكت دنتسملا اذه فصبي ةداهشلا ءحص نم ققحتلا عم ةجودزم.

ةيساسألا تابلطتملا

تابلطتملا

ةيلالل عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوصت:

- لوصوللا ذءأم ةقبط نيوكتو ASA (CLI) رم او رطس ةءءاو نيوكتب ةيساسأ ةفرعم
- VPN (SSL) ةنمألا
- X509 تاداهشب ةيساسأ ةفرعم

ةمدختسمل تانوكملا

ةيلالتل جماربل تارادصلإل دننتسمل اذه يف ةدراول تامولعمل دننتست:

- 8.4 رادصلإل، Cisco Adaptive Security Appliance (ASA) ةلدعمل نامأل ةزهجأ جم انرب شذأل تارادصلإل او
- 3.1 رادصلإل، Cisco AnyConnect Secure Mobility Client عم Windows 7

ءاشنإل (CA) يجرأخ تاداهش عجرم تم دختسأ كنأ ضررتفملا نم:


- 64 ل ASA ساسألأب زمرم ةداهش (PKCS #12) 12 مقرر ماع حاتفمب يسايق ريفشت (AnyConnect.pfx)
- AnyConnect ل PKCS #12 ةداهش

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجال نم دننتسمل اذه يف ةدراول تامولعمل ءاشنإم تناك اذا. (يضا رتفا) حوسمم نيوكتب دننتسمل اذه يف ةمدختسمل ةزهجال عيمج تادب رملأل لمحتمل ريثأتلل كمهف نم دكأتف، ليغشتل ديقتك تبش

ةيساسأ تامولعمل

Cisco AnyConnect (ASA) فيكتلل لباقل نامأل زاهج نيوكتل الاثم دننتسمل اذه فصبي ةداهشلا ةحص نم ققحتلا عم ةجودزمل ةقداصلملا مدختسي يذلا Secure Mobility Client access ةححصلا دامتعالا تانايبو ةداهشلا ريفوت كيلع بجي، AnyConnect مدختسم كتفصب الاثم دننتسمل اذه مدقي امك. VPN لوصو لعل لوصحلل ةيوناثلاو ةيساسأل ةقداصلل ةقبسمل ةئبعتلا ةزيم مادختساب ةداهشلا نييعتل

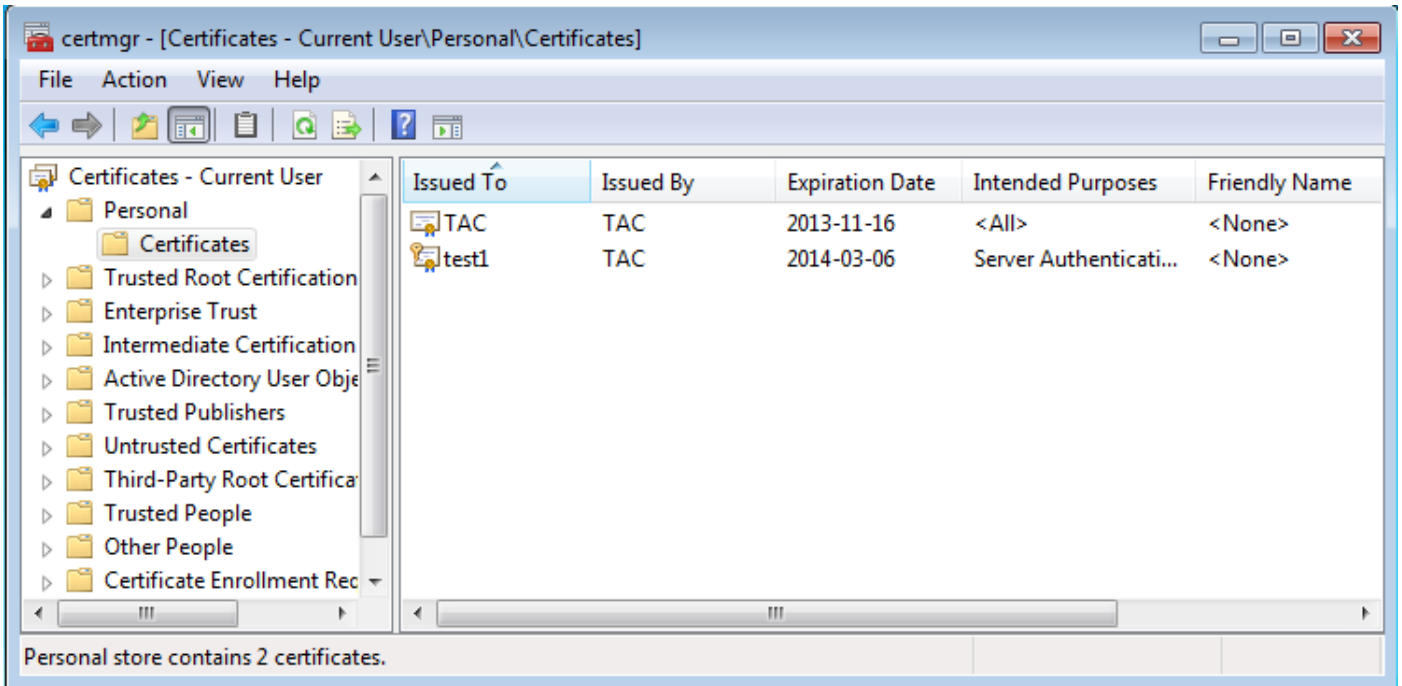
نيوكتل

 رماوأل لوح تامولعمل نم ديزم لعل لوصحلل [رماوأل شحب ةادا](#) مدختسأ: ةظالم لىل لوصولا نيلجسمل Cisco يمدختسمل لطقف نكمي. مسقلا اذه يف ةمدختسمل ةيلخاد تامولعمل Cisco تاودأ

AnyConnect ةداهش

كلت تيبتب مقو، AnyConnect.pfx فلم لعل اجدوزم ارقن رقنا، الاثم ةداهش تيبتتل ةيصخش ةداهشك ةداهشلا

تيبتتل نم ققحتلل (certmgr.msc) تاداهشلا ريديم مدختسأ:



الف Microsoft، یمدخستسم نزخم ینف ةداهش یلع روثعل AnyConnect لواحی، ینضارتفا لكش ب
 AnyConnect فی رعت فلم ینف تاریغیت یا عارجل ةجاح.

ASA یلع ةداهش ل تیبتت

PKCS #12 base64: ةداهش داریتسا ل ASA ل نكمی فیک لاثملا اذه حضوی

<#root>

```
BSNS-ASA5580-40-1(config)# crypto ca import CA pkcs12 123456
```

Enter the base 64 encoded pkcs12.

End with the word "quit" on a line by itself:

```
MIIJAQIBAzCCCMcGCSqGSIb3DQEHAaCCCLgEggiOMIII sDCCBa8GCSqGSIb3DQEH
```

...

<output ommitted>

...

```
83EwMTAhMAkGBSsOAwIaBQAeFCS/WBSkrOIeT1HARHbLF1FFQvSvBAhu0j9bTtZo
```

```
3AICCAA=
```

```
quit
```

```
INFO: Import PKCS12 operation completed successfully
```

داریتسالال نم ققحتلل show crypto ca certificates رمال مدختسا:

```
BSNS-ASA5580-40-1(config)# show crypto ca certificates
```

```
CA Certificate
```

```
Status: Available
```

```
Certificate Serial Number: 00cf946de20d0ce6d9
```

```
Certificate Usage: General Purpose
```

```
Public Key Type: RSA (1024 bits)
```


<#root>

```
ip local pool POOL 10.1.1.10-10.1.1.20
username cisco password cisco
```

```
webvpn
  enable outside
  AnyConnect image disk0:/AnyConnect-win-3.1.01065-k9.pkg 1
  AnyConnect enable
  tunnel-group-list enable
```

```
group-policy Group1 internal
group-policy Group1 attributes
  vpn-tunnel-protocol ssl-client ssl-clientless
  address-pools value POOL
```

```
tunnel-group RA type remote-access
tunnel-group RA general-attributes
```

```
  authentication-server-group LOCAL
```

```
  default-group-policy Group1
```

```
  authorization-required
```


```
tunnel-group RA webvpn-attributes
```

```
  authentication aaa certificate
```

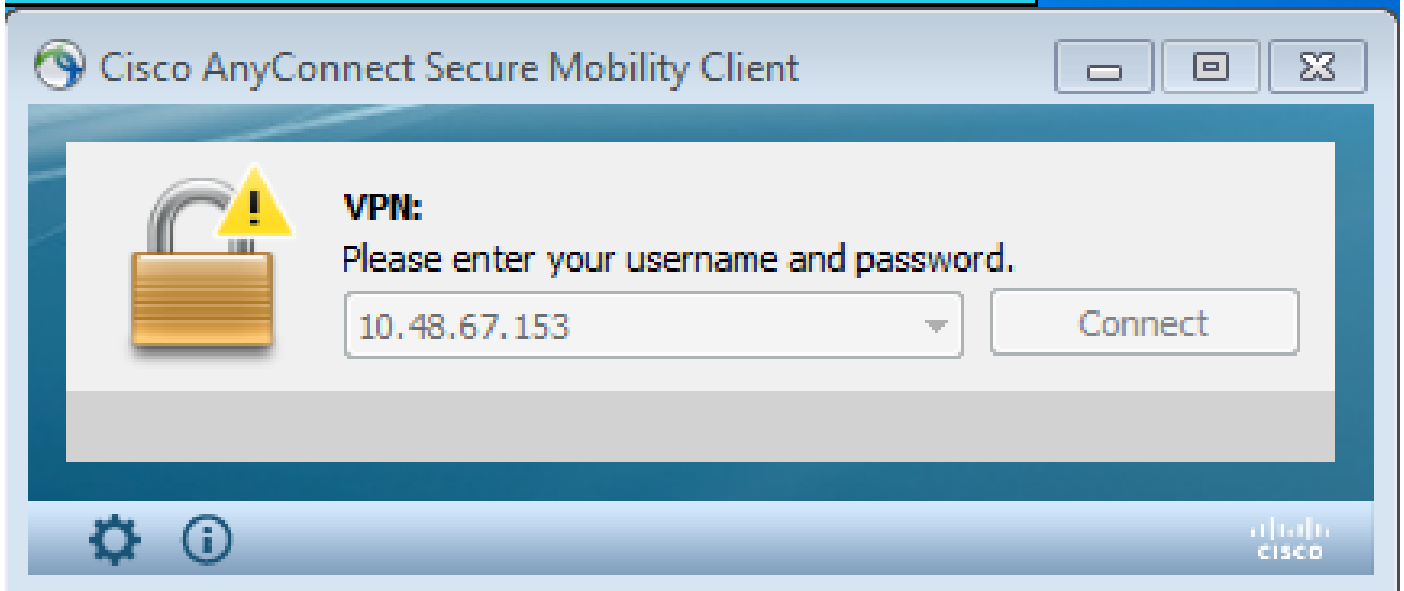
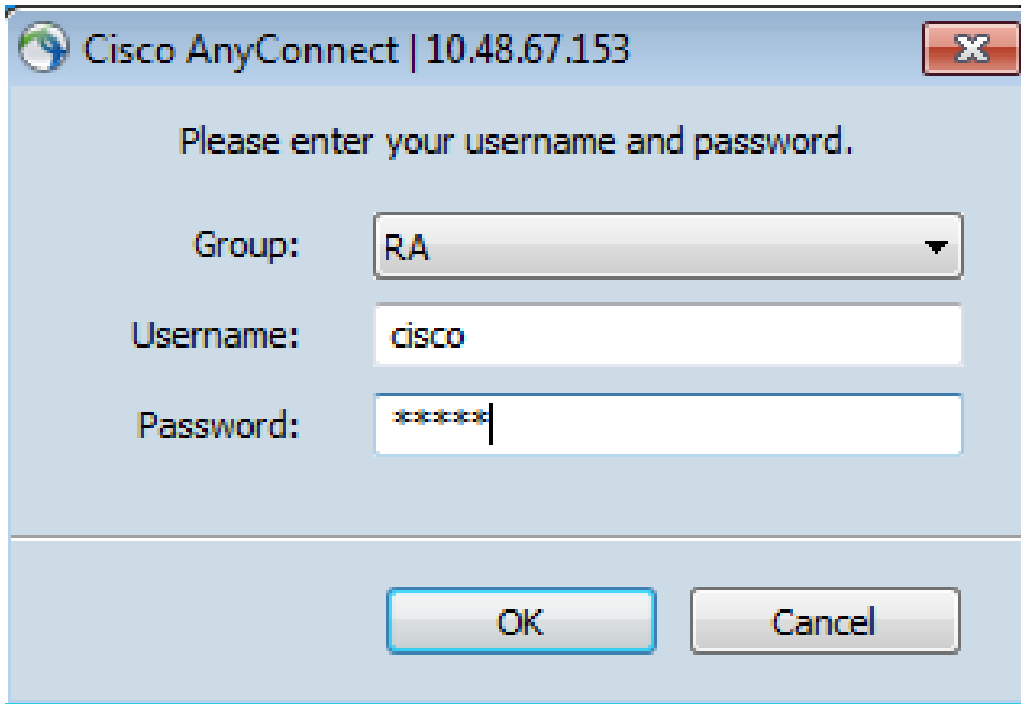
```
  group-alias RA enable
```

لېلدل ىل لوصول لوكوتورب ضيوفت ذيفنت نكمملا نم، نېوكتلا اذه ىل ةفاضل اب دع ب (CN) ةداهشل مسال لم، ددحم ةداهش ل قح نم مدختسمل مسال مادختساب (LDAP) في فخلل ةيره اظلال ةصاخلا ةكبشلا لمع ةسلج ىلع اهق يبطتو ةفاضل تامس دادرست نكمي كلذ [ASA AnyConnect VPN](#) ىل عجرا، ةداهشل ضيوفتو ةقداصل لوج تامولعمل نم ديزمل (VPN). [OpenLDAP Authorization with Custom Schema and Certificates Configuration Example](#) و

رابتخا

 ضرعل "جارخالل مچرتم ةادأ" مدختسا. show رماو اضعب [جارخالل مچرتم ةادأ معدت](#): ةظحالم تاودأ ىل لوصول نيلجسمل Cisco يمدختسمل طقف نكمي. show رمال جارخمل ليلحت ةلخاد تامولعمل Cisco.

نأ ب جي. (cisco ةم لك عم cisco) يلم تاغوسم لا، ليلكشت اذه تربتخا in order to تدوز ةدوجوم ةداهشل نوكت:



ASA: لى لى رما AnyConnect لى صفت vpn-sessionDB ضرع لى تلخدا

<#root>

```
BSNS-ASA5580-40-1(config-tunnel-general)# show vpn-sessiondb detail AnyConnect  
Session Type: AnyConnect Detailed
```

```
Username      :
```

```
cisco
```

```
Index        : 10
```

```
Assigned IP  :
```

```
10.1.1.10
```

```
Public IP    : 10.147.24.60
```

```
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
```

```
License      : AnyConnect Premium
```

```
Encryption   : RC4 AES128          Hashing      : none SHA1
```

Bytes Tx : 20150 Bytes Rx : 25199
Pkts Tx : 16 Pkts Rx : 192
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : Group1 Tunnel Group : RA
Login Time : 10:16:35 UTC Sat Apr 13 2013
Duration : 0h:01m:30s
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 : 10.1
Public IP : 10.147.24.60
Encryption : none TCP Src Port : 62531
TCP Dst Port : 443 Auth Mode :

Certificate

and userPassword

Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client Type : AnyConnect
Client Ver : 3.1.01065
Bytes Tx : 10075 Bytes Rx : 1696
Pkts Tx : 8 Pkts Rx : 4
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 10.2
Assigned IP : 10.1.1.10 Public IP : 10.147.24.60
Encryption : RC4 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 62535
TCP Dst Port : 443 Auth Mode :

Certificate

and userPassword

Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.01065
Bytes Tx : 5037 Bytes Rx : 2235
Pkts Tx : 4 Pkts Rx : 11
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:

Tunnel ID : 10.3
Assigned IP : 10.1.1.10 Public IP : 10.147.24.60
Encryption : AES128 Hashing : SHA1
Encapsulation: DTLSv1.0 UDP Src Port : 52818
UDP Dst Port : 443 Auth Mode :

Certificate

and userPassword

Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client Type : DTLS VPN Client
Client Ver : 3.1.01065
Bytes Tx : 0 Bytes Rx : 21268

Pkts Tx : 0
Pkts Tx Drop : 0

Pkts Rx : 177
Pkts Rx Drop : 0

NAC:

Reval Int (T): 0 Seconds
SQ Int (T) : 0 Seconds
Hold Left (T): 0 Seconds
Redirect URL :

Reval Left(T): 0 Seconds
EoU Age(T) : 92 Seconds
Posture Token:

ءاطخأل حىحصت

 debug رماوأ مادختس إلبق [حىحصت لارمأوا لوح ةمهم تامولعم](#) ىلإ عجرا :ةظحالم

عجرم ىلع روثلعل متو ، تاناىب لال ءءاق ىف اتقؤم ءءاهشلل نىزخت متى مل ، لاثم ل اءه ىف نم ققحتل متو ، (ClientAuthentication) حىحصت لال حاتفم لال مادختس إلبق ، قباطم قءصم :ءاجنب ءءاهشلل ءحص

<#root>

```
debug aaa authentication
debug aaa authorization
debug webvpn 255
```

```
debug webvpn AnyConnect 255
```

```
debug crypto ca 255
```

ءاشن إلب ، debug webVPN 255 رمال لثم ، ءىل ىف ءاطخأل حىحصت رماوأ موقت نأ نكمى حىحصت ضعب ءلازا تمت . ASA ىلع رىبك لمح ءضوو ءاتنإ ءئىب ىف تالءسلل نم ءىءعل ءاطخأل WebVPN لولل ءضولل

<#root>

```
CERT_API: Authenticate session 0x0934d687, non-blocking cb=0x0000000012cfc50
CERT API thread wakes up!
CERT_API: process msg cmd=0, session=0x0934d687
CERT_API: Async locked for session 0x0934d687
CRYPTO_PKI:
```

```
Checking to see if an identical cert is
```

```
already in the database
```

```
...
```

```
CRYPTO_PKI: looking for cert in handle=0x00007ffd8b80ee90, digest=
ad 3d a2 da 83 19 e0 ee d9 b5 2a 83 5c dd e0 70 | .=.....*.\..p
CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
CRYPTO_PKI:
```


Cert not found in database

.
CRYPTO_PKI:

Looking for suitable trustpoints

...
CRYPTO_PKI: Storage context locked by thread CERT API
CRYPTO_PKI:

Found a suitable authenticated trustpoint CA

.
CRYPTO_PKI(make trustedCerts list)CRYPTO_PKI:check_key_usage: ExtendedKeyUsage
OID = 1.3.6.1.5.5.7.3.1
CRYPTO_PKI:

check_key_usage:Key Usage check OK

CRYPTO_PKI:

Certificate validation: Successful, status: 0

. Attempting to
retrieve revocation status if necessary
CRYPTO_PKI:Certificate validated. serial number: 00FE9C3D61E131CDB1, subject name:
cn=test1,ou=Security,o=Cisco,l=Krakow,st=PL,c=PL.
CRYPTO_PKI: Storage context released by thread CERT API
CRYPTO_PKI: Certificate validated without revocation check

م ت ي و ، ة د د ح م ت ا د ا ه ش ن ي ي ع ت د ع ا و ق د ج و ت ال . ة ق ب ا ط م ق ف ن ة ع و م ج م ي ل ع ر و ث ع ل ا ة ل و ا ح م ي ه ه ذ ه
ا ه ر ف و ت ي ت ل ا ق ف ن ل ا ة ع و م ج م ا د خ ت س ا :

<#root>

CRYPTO_PKI: Attempting to find tunnel group for cert with serial number:
00FE9C3D61E131CDB1, subject name: cn=test1,ou=Security,o=Cisco,l=Krakow,st=PL,
c=PL, issuer_name: cn=TAC,ou=RAC,o=TAC,l=Warsaw,st=Maz,c=PL.
CRYPTO_PKI:

No Tunnel Group Match for peer certificate

.
CERT_API: Unable to find tunnel group for cert using rules (SSL)

ة م ا ع ل ا ة س ل ج ل ا ء ا ط خ ا ح ي ح ص ت و SSL ي ه ه ذ ه :

<#root>

%ASA-7-725012: Device chooses cipher : RC4-SHA for the SSL session with client
outside:10.147.24.60/64435
%ASA-7-717025:

Validating certificate chain containing 1 certificate(s).

%ASA-7-717029:

Identified client certificate

within certificate chain. serial
number: 00FE9C3D61E131CDB1, subject name:

cn=test1,ou=Security,o=Cisco,l=Krakow,
st=PL,c=PL

%ASA-7-717030:

Found a suitable trustpoint CA to validate certificate

%ASA-6-717022:

Certificate was successfully validated

. serial number:

00FE9C3D61E131CDB1, subject name: cn=test1,ou=Security,o=Cisco,l=Krakow,st=PL,
c=PL.

%ASA-6-717028: Certificate chain was successfully validated with warning,
revocation status was not checked.

%ASA-6-725002: Device completed SSL handshake with client outside:

10.147.24.60/64435

%ASA-7-717036:

Looking for a tunnel group match based on certificate maps

for

peer certificate with serial number: 00FE9C3D61E131CDB1, subject name: cn=test1,
ou=Security,o=Cisco,l=Krakow,st=PL,c=PL, issuer_name: cn=TAC,ou=RAC,o=TAC,
l=Warsaw,st=Maz,c=PL.

%ASA-4-717037:

Tunnel group search using certificate maps failed for peer
certificate

: serial number: 00FE9C3D61E131CDB1, subject name: cn=test1,
ou=Security,o=Cisco,l=Krakow,st=PL,c=PL, issuer_name: cn=TAC,ou=RAC,o=TAC,
l=Warsaw,st=Maz,c=PL.

%ASA-6-113012:

AAA user authentication Successful : local database : user = cisco

%ASA-6-113009:

AAA retrieved default group policy (Group1) for user = cisco

%ASA-6-113008: AAA transaction status ACCEPT : user = cisco

%ASA-7-734003: DAP: User cisco, Addr 10.147.24.60:

Session Attribute aaa.cisco.grouppolicy = Group1

%ASA-7-734003: DAP: User cisco, Addr 10.147.24.60:

Session Attribute aaa.cisco.username = cisco

%ASA-7-734003: DAP: User cisco, Addr 10.147.24.60:

Session Attribute aaa.cisco.username1 = cisco

%ASA-7-734003: DAP: User cisco, Addr 10.147.24.60:

Session Attribute aaa.cisco.username2 =

%ASA-7-734003: DAP: User cisco, Addr 10.147.24.60:

Session Attribute aaa.cisco.tunnelgroup = RA

%ASA-6-734001: DAP: User cisco, Addr 10.147.24.60, Connection AnyConnect: The

following DAP records were selected for this connection: DfltAccessPolicy
%ASA-6-113039: Group <Group1> User <cisco> IP <10.147.24.60> AnyConnect parent
session started.

ةداهشللا نم ققحتلالاو ةجودزم ةقداصلملا ASA نيوكت

ةقداصلملا مءاخو، ايلحم ياساسألا ةقداصلملا مءاخ نيوكي شيح، ةجودزملا ةقداصلملا لىل ءلاثم اءه
انكمم ةداهشللا ءحص نم ققحتلالا لازلل ال LDAP. وه يونائل

LDAP: نيوكت لائلملا اءه ءضوي

```
aaa-server LDAP protocol ldap
aaa-server LDAP (outside) host 10.147.24.60
  ldap-base-dn DC=test-cisco,DC=com
  ldap-scope subtree
  ldap-naming-attribute uid
  ldap-login-password *****
  ldap-login-dn CN=Manager,DC=test-cisco,DC=com
server-type openldap
```

يونائل ةقداصلم مءاخ ةفاضل يلى امي

<#root>

```
tunnel-group RA general-attributes
  authentication-server-group LOCAL
  secondary-authentication-server-group LDAP

default-group-policy Group1
authorization-required

tunnel-group RA webvpn-attributes
authentication aaa certificate
```

يضا رءفا ءاءع! هائل نيوكتلالا يى 'authentication-server-group local' لى رءال

مءاوخ ةءومءم "ل ءبس نللاب 'authentication-server-group.' ل رءال AAA مءاخ يى مءاخءءس ل نكمي
Security Dynamics مءاخ ءانءءس اب AAA مءاوخ ءيمء مءاخءءس ل نكمملا نم، "ءيوناائل ةقداصلملا
International (SDI): سىيئرلا ةقداصلملا مءاخ وه SDI لظى ءق، ءلالا هءه يى فو: (SDI)

رابلء

✎ ضررل "جارخال مجرتم ةادا" مدختسا show رماوا ضعب [جارخال مجرتم ةادا معدت](#): ةظالم تاودأ لىل لوصول نىلجسمل Cisco يمدختسمل طقف نكمي. show رمالا جرخم لىلحت ةىلخاد تامولعمو Cisco.

و (cisco ةم لك عم username cisco) دامتعا ةقرو يلحم لىل، لىكشت اذه تربتخا in order to تردصأ LDAP نم ةم لك عم username cisco) دامتعا ةقرو (LDAP): ةدوجوم ةداهش لىل نوكت نأ بجي.

The image shows two screenshots of the Cisco AnyConnect interface. The top screenshot is a login dialog box titled "Cisco AnyConnect | 10.48.67.153". It contains the text "Please enter your username and password." and several input fields: "Group:" with a dropdown menu showing "RA", "Username:" with "cisco", "Password:" with "*****", "Second Username:" with "cisco", and "Second Password:" with "*****". There are "OK" and "Cancel" buttons at the bottom. The bottom screenshot is the "Cisco AnyConnect Secure Mobility Client" window. It features a yellow warning icon with an exclamation mark and a padlock icon. The text "VPN: Please enter your username and password." is displayed above a dropdown menu showing "10.48.67.153" and a "Connect" button. The Cisco logo is visible in the bottom right corner.

ASA لىل رما AnyConnect لىل صفت vpn-sessionDB ضررل تلخد

ةقداصم لىل ASA نىوكت" لىل عجرا. ةىدخال ةقداصم لىل ةصخال كلىل ةلثامم جئاتن لىل

["رابط الخال، عداهشل، نم ققحتل او عي داخالا"](#)

ءاطخألا حيحصت

[ASA نيوكت](#) لى عجرا. ةقداصم ل او WebVPN ةسلجل ءاطخألا حيحصت تاي لمع ل ثامتت ةيفاضل ةقداصم ةي لمع رهظت. ["ءاطخألا حيحصت و عداهشل، نم ققحتل او عي داخالا ةقداصم ل"](#) ةدحاو:

```
<#root>
```

```
%ASA-6-113012:
```

```
AAA user authentication Successful : local database : user = cisco
```

```
%ASA-6-302013: Built outbound TCP connection 1936 for outside:10.147.24.60/389  
(10.147.24.60/389) to identity:10.48.67.153/54437 (10.48.67.153/54437)
```

```
%ASA-6-113004:
```

```
AAA user authentication Successful : server = 10.147.24.60 :  
user = cisco
```

```
%ASA-6-113009: AAA retrieved default group policy (Group1) for user = cisco
```

```
%ASA-6-113008: AAA transaction status ACCEPT : user = cisco
```

LDAP نيوكت عم فل تخت نأ نكمي لى صافات LDAP ءاطخألا حيحصت يدبى:

```
[34] Session Start  
[34] New request Session, context 0x00007ffd8d7dd828, reqType = Authentication  
[34] Fiber started  
[34] Creating LDAP context with uri=ldap://10.147.24.60:389  
[34] Connect to LDAP server: ldap://10.147.24.60:389, status = Successful  
[34] supportedLDAPVersion: value = 3  
[34] Binding as Manager  
[34] Performing Simple authentication for Manager to 10.147.24.60  
[34] LDAP Search:  
      Base DN = [DC=test-cisco,DC=com]  
      Filter  = [uid=cisco]  
      Scope   = [SUBTREE]  
[34] User DN = [uid=cisco,ou=People,dc=test-cisco,dc=com]  
[34] Server type for 10.147.24.60 unknown - no password policy  
[34] Binding as cisco  
[34] Performing Simple authentication for cisco to 10.147.24.60  
[34] Processing LDAP response for user cisco  
[34] Authentication successful for cisco to 10.147.24.60  
[34] Retrieved User Attributes:  
[34]   cn: value = John Smith  
[34]   givenName: value = John  
[34]   sn: value = cisco  
[34]   uid: value = cisco  
[34]   uidNumber: value = 10000  
[34]   gidNumber: value = 10000  
[34]   homeDirectory: value = /home/cisco  
[34]   mail: value = name@dev.local
```


اذهلو، OU) ةيمظنتلا ةدحو لا نم مدختسملا مسا ذخأ متي، ةيوناثلا ةقداصملا ةبسنلاب
LDAP. مداخ ىلع مدختسملا "نامأ" عاشنإ مت ببسلا

مسا علمل AnyConnect ىلع ةقبسملا ةئبعتلا رماو مادختسا صرف اضيأ نكمملا نم
اقبسم يوناثلا ويسياسلا مدختسملا.

امنيب، LDAP و AD مداخ ةداعيسياسلا ةقداصملا مداخ نوكي، يعقاولا ملال ويرانيسي في
تاملك مدختسي يذلا (RSA) Adelman و Shamir و Rivest مداخ وه يوناثلا ةقداصملا مداخ نوكي
AD/LDAP دامتعانايب ريفوت مدختسملا ىلع بجي، ويرانيسيلا اذه في. زي ممل زمرلا رورم
ىلع) ةداهشو (مدختسملا اهكلمتي يذلا) RSA زمر رورم ةملاكو (اهب مدختسملا ملعي يذلا)
(همادختسا متي يذلا زاهجلا).

رابتخا

يلقح نم اقبسم ابعم هنأل يوناثلا ويسياسلا مدختسملا مسا ريغت كنكمي ال هنأ طحال
:ةداهشلل OU و CN

Cisco AnyConnect | 10.48.67.153

Please enter your username and password.

Group: RA

Username: test1


Password: |

Second Username: Security

Second Password:

OK Cancel

Cisco AnyConnect Secure Mobility Client

 **VPN:**
Please enter your username and password.

10.48.67.153

Connect

Settings Information Cisco

ءاطخأل احي حصت

AnyConnect: إل هل اسرامت يذلا ةقوبس ملاء ةبعتل بلط لاثملا اذه حضوي

```
%ASA-7-113028: Extraction of username from VPN client certificate has been requested. [Request 5]
%ASA-7-113028: Extraction of username from VPN client certificate has started. [Request 5]
%ASA-7-113028: Extraction of username from VPN client certificate has finished successfully. [Request 5]
%ASA-7-113028: Extraction of username from VPN client certificate has completed.
```



```
[Request 5]
%ASA-7-113028: Extraction of username from VPN client certificate has been
requested. [Request 6]
%ASA-7-113028: Extraction of username from VPN client certificate has started.
[Request 6]
%ASA-7-113028: Extraction of username from VPN client certificate has finished
successfully. [Request 6]
%ASA-7-113028: Extraction of username from VPN client certificate has completed.
[Request 6]
```

ة:ح ي ص ل ل ن ي م د خ ت س م ل ا ء م س أ م د خ ت س ت ة ق د ا ص م ل ا ن أ ي ر ت ا ن ه

<#root>

%ASA-6-113012:

AAA user authentication Successful : local database : user = test1

%ASA-6-302013: Built outbound TCP connection 2137 for outside:10.147.24.60/389
(10.147.24.60/389) to identity:10.48.67.153/46606 (10.48.67.153/46606)

%ASA-6-113004:

AAA user authentication Successful : server = 10.147.24.60 :
user = Security


ت ا د ا ه ش ط ي ط خ ت و ة ج و د ز م ة ق د ا ص م ل ا S A ن ي و ك ت

ا ذ ه ي ف ح ض و م و ه ا م ك ، ة ن ي ع م ق ا ف ن ا ت ا ع و م ج م ل ا ة د د ح م ل ي م ع ت ا د ا ه ش ن ي ي ع ت ا ض ي ا ن ك م م ل ا ن م
ل ا ث م ل :

```
crypto ca certificate map CERT-MAP 10  
issuer-name co tac
```

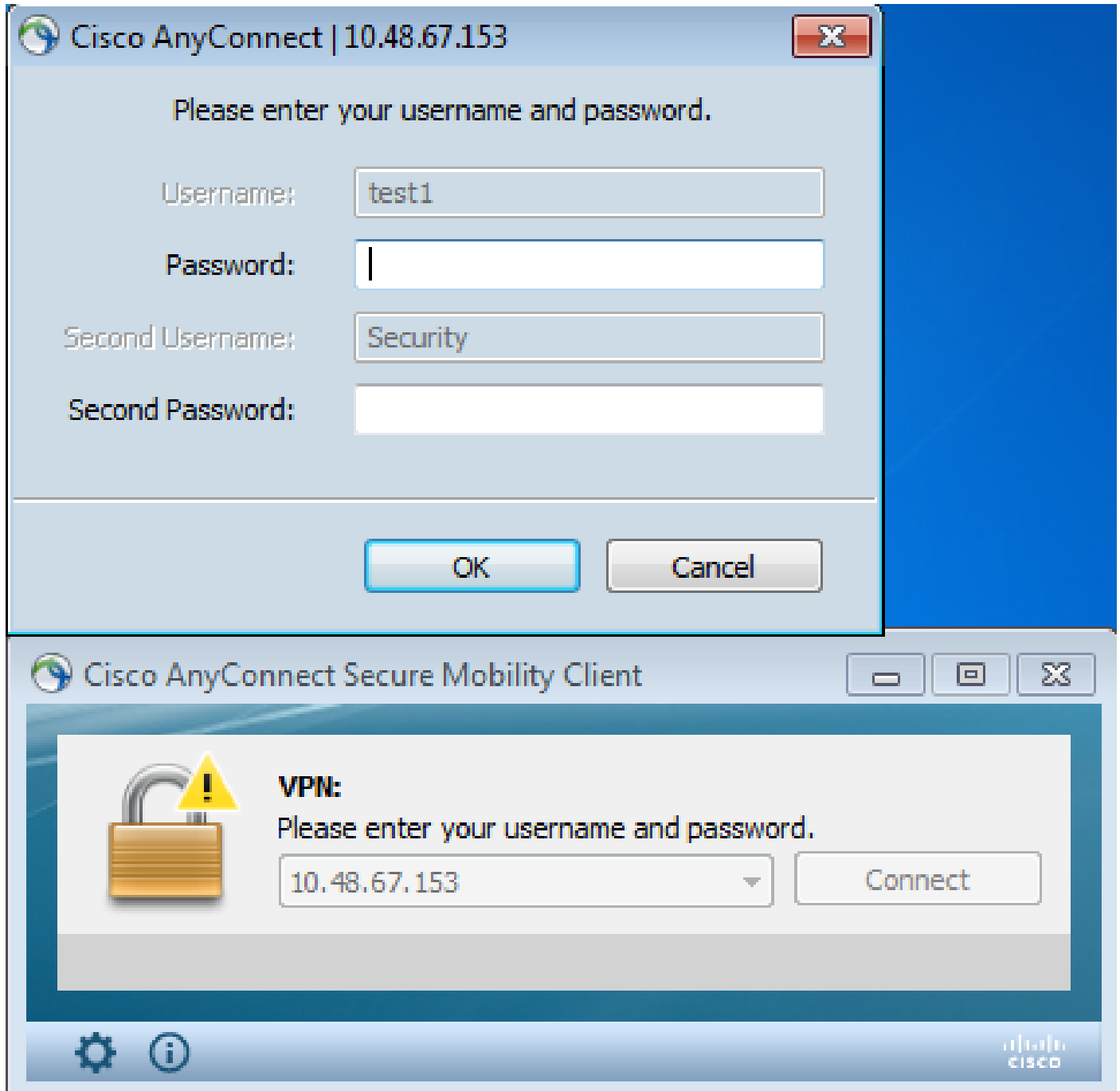
```
webvpn  
certificate-group-map CERT-MAP 10 RA
```

ة د ع ا س م ل ا ز ك ر م) T A C ل ب ق ن م ة ق و م ل ا م د خ ت س م ل ا ت ا د ا ه ش ع ي م ج ن ي ي ع ت م ت ي ، ة ق ي ر ط ل ا ه ذ ه ب
' R A . ' م س ا ب ق ف ن ة ع و م ج م ل ا C i s c o ن م C A (T A C) ة ن ق ت ل ا

 IPsec ل ة د ا ه ش ل ل ن ي ي ع ت ن ع ف ل ت خ م ل ك ش ب S S L ل ة د ا ه ش ل ل ن ي ي ع ت ن ي و ك ت م ت : ة ط ح ا ل م
ن ي و ك ت ل ا ع ض و ي ف ' t u n n e l - g r o u p - m a p ' د ع ا و ق م ا د خ ت س ا ب ه ن ي و ك ت م ت ي ، IPsec ل ة ب س ن ل ا ب
ع ض و ن م ض ' c e r t i f i c a t e - g r o u p - m a p ' م ا د خ ت س ا ب ه ن ي و ك ت م ت ي ، S S L ل ة ب س ن ل ا ب . م ا ع ل ل
ن ي و ك ت W e b V P N .

ر ا ب ت خ ا

نآل دعب ق فنل ة و م جم را ي ت خ ال ج ا ت ح ت ن ل ، ة د ا ه ش ل ا ن ي ي ع ت ن ي ك م ت د ر ج م ب ه ن ا ظ ح ال



ء ا ط خ ال ا ح ي ح ص ت

ق فنل ة و م جم ي ل ع ر و ث ع ل ا ب ة د ا ه ش ل ا ن ي ي ع ت ة د ع ا ق ح م س ت ، ل ا ث م ل ا ا ذ ه ي ف

<#root>

%ASA-7-717036:

Looking for a tunnel group match based on certificate maps

for
peer certificate with serial number: 00FE9C3D61E131CDB1, subject name: cn=test1,
ou=Security,o=Cisco,l=Krakow,st=PL,c=PL, issuer_name: cn=TAC,ou=RAC,o=TAC,

l=Warsaw,st=Maz,c=PL.
%ASA-7-717038:

Tunnel group match found. Tunnel Group: RA

, Peer certificate:

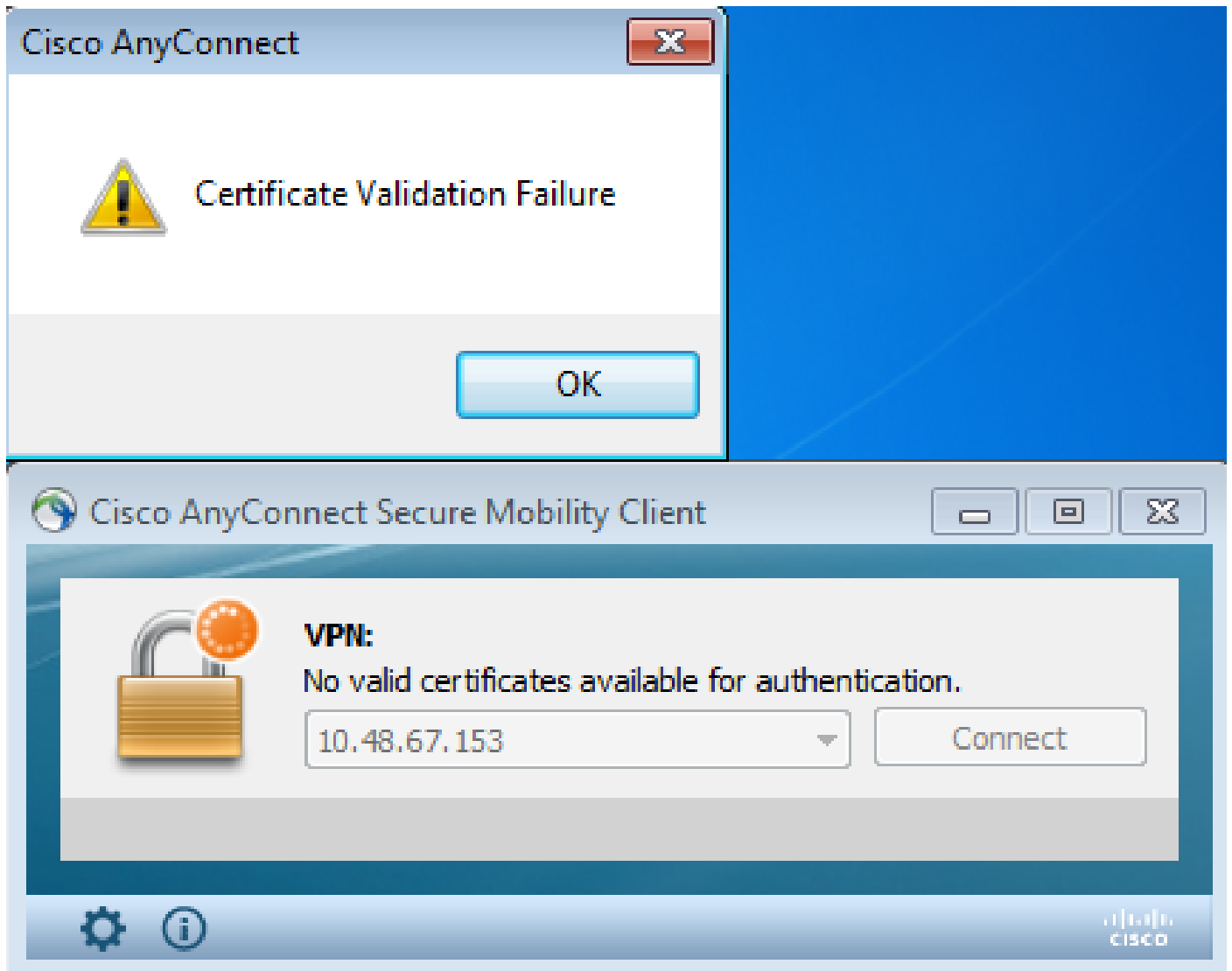
serial number: 00FE9C3D61E131CDB1, subject name: cn=test1,ou=Security,o=Cisco,
l=Krakow,st=PL,c=PL, issuer_name: cn=TAC,ou=RAC,o=TAC,l=Warsaw,st=Maz,c=PL.

اهحال صإو ءاطخأل فاشك تسإ

اهحال صإو نيوكتل ءاطخأ فاشك تسإل اهم ادختسإ كنكمي تام ولعم مسقلا اذه رفوي

ةدوجوم ريغ ءحل اصلل ءداهشلل

ةحل اصلل ءداهش يأل عل روثلعل AnyConnect لعل رذعتي، Windows7 نم ءحل اصلل ءداهش ءلازا دعب



للمعمل لبق نم تيهنأ ءسلجل نأ ودبي، ASA لعل (reset-i):

<#root>

```
%ASA-6-302013: Built inbound TCP connection 2489 for outside:10.147.24.60/52838
(10.147.24.60/52838) to identity:10.48.67.153/443 (10.48.67.153/443)
%ASA-6-725001: Starting SSL handshake with client outside:10.147.24.60/52838 for
TLSv1 session.
%ASA-7-725010: Device supports the following 4 cipher(s).
%ASA-7-725011: Cipher[1] : RC4-SHA
%ASA-7-725011: Cipher[2] : AES128-SHA
%ASA-7-725011: Cipher[3] : AES256-SHA
%ASA-7-725011: Cipher[4] : DES-CBC3-SHA
%ASA-7-725008: SSL client outside:10.147.24.60/52838 proposes the following 8
cipher(s).
%ASA-7-725011: Cipher[1] : AES128-SHA
%ASA-7-725011: Cipher[2] : AES256-SHA
%ASA-7-725011: Cipher[3] : RC4-SHA
%ASA-7-725011: Cipher[4] : DES-CBC3-SHA
%ASA-7-725011: Cipher[5] : DHE-DSS-AES128-SHA
%ASA-7-725011: Cipher[6] : DHE-DSS-AES256-SHA
%ASA-7-725011: Cipher[7] : EDH-DSS-DES-CBC3-SHA
%ASA-7-725011: Cipher[8] : RC4-MD5
%ASA-7-725012: Device chooses cipher : RC4-SHA for the SSL session with client
outside:10.147.24.60/52838
%ASA-6-302014:

Teardown TCP connection 2489 for outside:10.147.24.60/52838 to
identity:10.48.67.153/443 duration 0:00:00 bytes 1448 TCP Reset-I
```

ةلص تاذا مومول عم

- [ةجود زملا ةقدا صملا نيوك ت : ني مدخت سملا او ةومج ملاء هنو قف نلا تا عومج م نيوك ت](#)
- [نامألا زا هج مدخت سم ضي وف تل ي چراخ مداخ نيوك ت](#)
- [Cisco نم تال يزن ت لا وي ن ف لا م عد لا](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخل مهتبل ب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إأمئاد ةوچرلاب ي صؤت وتامچرتل هذه ةقدنع اهتيل وئسم Cisco
Systems (رفوتم طبارل) ي لصلأل يزي لچن إل دن تسمل