ASA AnyConnect Secure Mobility-clientverificatie configureren

Inhoud

Inleiding

Dit document beschrijft een configuratie voor ASA AnyConnect Secure Mobility Client-toegang die dubbele verificatie met certificaatvalidatie gebruikt.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van ASA CLI-configuratie (opdrachtregel interface) en SSL-configuratie (Secure Socket Layer)
- Basiskennis van X509-certificaten

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

- Software voor Cisco adaptieve security applicatie (ASA), versie 8.4 en hoger

- Windows 7 met Cisco AnyConnect Secure Mobility Client 3.1

Er wordt aangenomen dat u een externe certificeringsinstantie (CA) hebt gebruikt om het volgende te genereren:

- Een standaard #12 (PKCS #12) op basis van openbare sleutel en cryptografie met 64-codering voor ASA (AnyConnect.pfx)
- Een PKCS-#12 voor AnyConnect

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Dit document beschrijft een configuratievoorbeeld voor adaptieve security applicatie (ASA) voor Cisco AnyConnect Secure Mobility Client-toegang die dubbele verificatie met certificaatvalidatie gebruikt. Als gebruiker van AnyConnect moet u het juiste certificaat en de juiste referenties voor de primaire en secundaire verificatie opgeven om VPN-toegang te krijgen. Dit document biedt ook een voorbeeld van certificaattoewijzing met de voorvulfunctie.

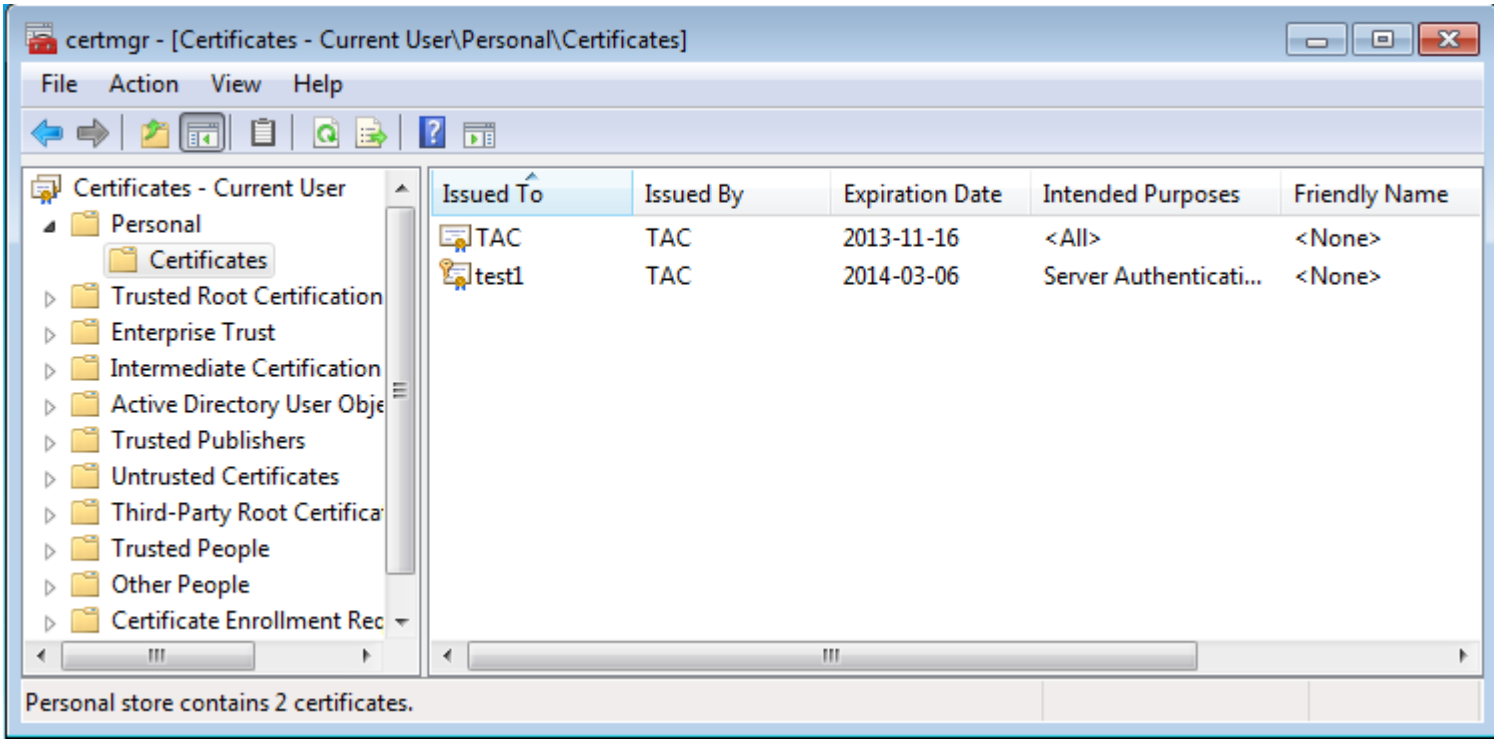
Configureren

> **Opmerking**: gebruik de Opdrachtzoekfunctie om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt. Alleen geregistreerde Cisco-gebruikers kunnen toegang krijgen tot interne Cisco-tools en -informatie.

Certificaat voor AnyConnect

Om een voorbeeldcertificaat te installeren, dubbelklikt u op het AnyConnect.pfx-bestand en installeert u dat certificaat als een persoonlijk certificaat.

Gebruik de certificaatbeheerder (certmgr.msc) om de installatie te controleren:



Standaard probeert AnyConnect een certificaat te vinden in de Microsoft-gebruikerswinkel; het is niet nodig om wijzigingen aan te brengen in het AnyConnect-profiel.

Certificaatinstallatie op ASA

Dit voorbeeld laat zien hoe ASA een base64 PKCS #12-certificaat kan importeren:

<#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:
MIIJAQIBAzCCCMcGCSqGSIb3DQEHAaCCCLgEggi0MIIIsDCCBa8GCSqGSIb3DQEH
...
<output ommitted>
...
83EwMTAhMAkGBSsOAwIaBQAEFCS/WBSkrOIeT1HARHbLF1FFQvSvBAhu0j9bTtZo
3AICCAA=
quit

INFO: Import PKCS12 operation completed successfully
```

Gebruik de opdracht **show crypto ca certificates** om de import te verifiëren:

```
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)
```

```
  Signature Algorithm: SHA1 with RSA Encryption
  Issuer Name:
    cn=TAC
    ou=RAC
    o=TAC
    l=Warsaw
    st=Maz
    c=PL
  Subject Name:
    cn=TAC
    ou=RAC
    o=TAC
    l=Warsaw
    st=Maz
    c=PL
  Validity Date:
    start date: 08:11:26 UTC Nov 16 2012
    end   date: 08:11:26 UTC Nov 16 2013
  Associated Trustpoints: CA

Certificate
  Status: Available
  Certificate Serial Number: 00fe9c3d61e131cda9
  Certificate Usage: General Purpose
  Public Key Type: RSA (1024 bits)
  Signature Algorithm: SHA1 with RSA Encryption
  Issuer Name:
    cn=TAC
    ou=RAC
    o=TAC
    l=Warsaw
    st=Maz
    c=PL
  Subject Name:
    cn=IOS
    ou=UNIT
    o=TAC
    l=Wa
    st=Maz
    c=PL
  Validity Date:
    start date: 12:48:31 UTC Nov 29 2012
    end   date: 12:48:31 UTC Nov 29 2013
  Associated Trustpoints: CA
```

> **Opmerking**: het Uitvoer Tolk Tool ondersteunt bepaalde **show** commando's. Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.** Alleen geregistreerde Cisco-gebruikers kunnen toegang krijgen tot interne Cisco-tools en -informatie.

ASA configuratie voor één verificatie en certificaatvalidatie

ASA maakt gebruik van zowel verificatie-, autorisatie- en accounting (AAA)-verificatie als certificaatverificatie. Certificaatvalidatie is verplicht. AAA-verificatie maakt gebruik van een lokale database.

Dit voorbeeld toont enige authentificatie met certificaatbevestiging.

<#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

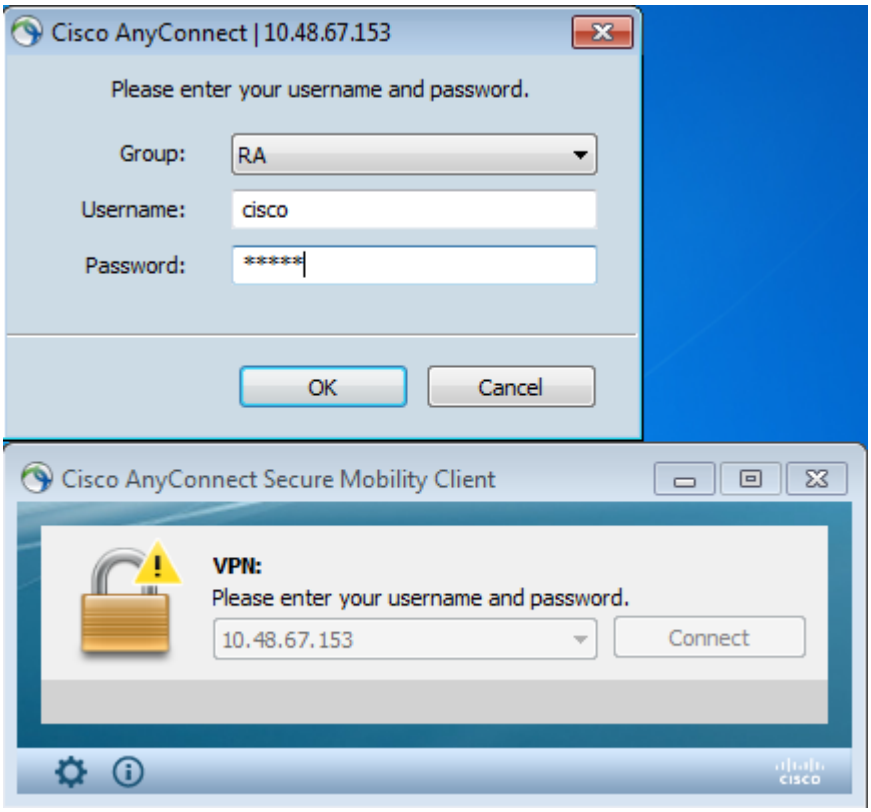
```
 group-alias RA enable
```

Naast deze configuratie, is het mogelijk om Lichtgewicht Directory Access Protocol (LDAP) autorisatie uit te voeren met de gebruikersnaam uit een specifiek certificaatveld, zoals de certificaatnaam (CN). Aanvullende kenmerken kunnen vervolgens worden opgehaald en toegepast op de VPN-sessie. Raadpleeg voor meer informatie over verificatie en certificaatautorisatie "ASA AnyConnect VPN en OpenLDAP-autorisatie met aangepast schema en configuratievoorbeeld van certificaten."

Testen

> **Opmerking**: het Uitvoer Tolk Tool ondersteunt bepaalde **show** commando's. Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.** Alleen geregistreerde Cisco-gebruikers kunnen toegang krijgen tot interne Cisco-tools en -informatie.

Om deze configuratie te testen, moet u de lokale referenties (gebruikersnaam cisco met wachtwoord cisco) opgeven. Het certificaat moet aanwezig zijn:



Voer de opdracht **show vpn-sessiondb details AnyConnect** in op de ASA:

<#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 Rx      : 177
  Pkts Tx Drop : 0                     Pkts Rx Drop : 0

NAC:
  Reval Int (T): 0 Seconds             Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds             EoU Age(T)   : 92 Seconds
  Hold Left (T): 0 Seconds             Posture Token:
  Redirect URL :
```

Debuggen

Opmerking: Raadpleeg Belangrijke informatie over debug commando's voordat u **debug** commando's gebruikt.

In dit voorbeeld is het certificaat niet in de database gecachet, is een corresponderende CA gevonden, is het juiste gebruik van de sleutel gebruikt (client-verificatie) en is het certificaat met succes gevalideerd:

<#root>

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

debug webvpn AnyConnect 255

```
debug crypto ca 255
```

Gedetailleerde debug commando's, zoals de opdracht **debug webvpn 255**, kunnen veel logbestanden genereren in een productieomgeving en een zware belasting plaatsen op een ASA. Sommige WebVPN debugs zijn verwijderd voor meer duidelijkheid:

<#root>

```
CERT_API: Authenticate session 0x0934d687, non-blocking cb=0x00000000012cfc50
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

Dit is de poging om een overeenstemmende tunnelgroep te vinden. Er zijn geen specifieke regels voor certificaattoewijzing en de door u opgegeven tunnelgroep wordt gebruikt:

<#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)

Dit zijn de SSL en algemene sessiedebugs:

<#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.
```

ASA-configuratie voor dubbele verificatie en certificaatvalidatie

Dit is een voorbeeld van dubbele verificatie, waarbij de primaire verificatieserver LOKAAL is en de secundaire verificatieserver LDAP is. Certificaatvalidatie is nog steeds ingeschakeld.

Dit voorbeeld toont de LDAP-configuratie:

```
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
```

Hier is de toevoeging van een secundaire verificatieserver:

<#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

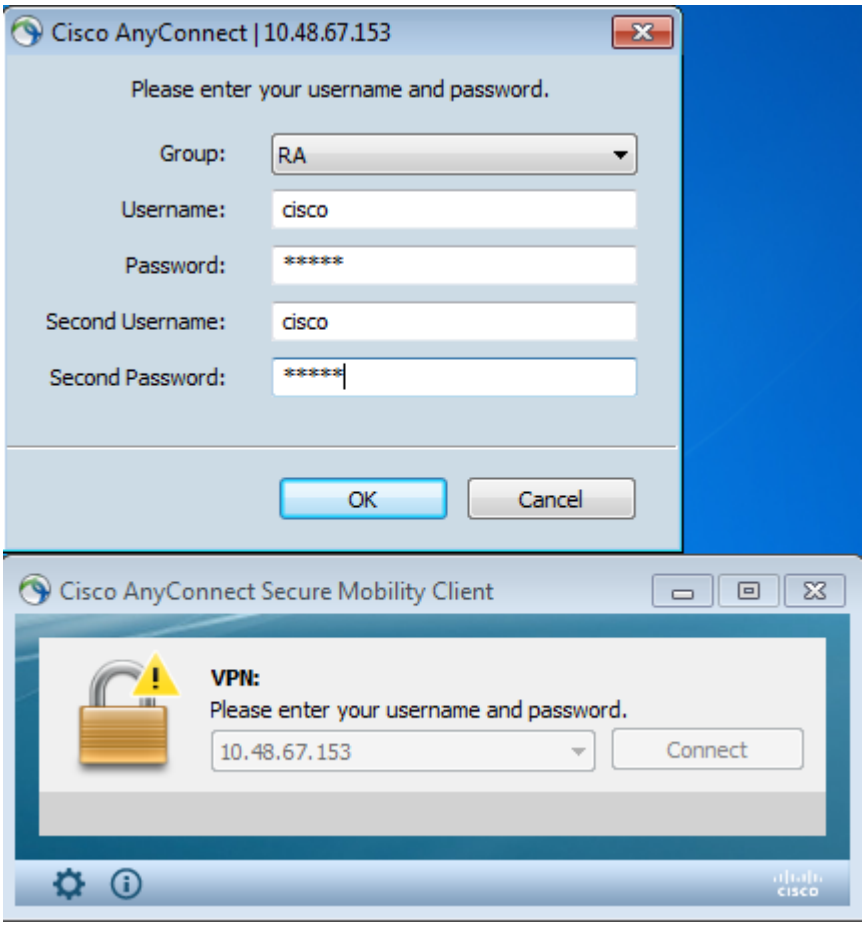
U ziet in de configuratie geen 'verificatieserver-groep LOCAL' omdat dit een standaardinstelling is.

Een andere AAA-server kan gebruikt worden voor 'authenticatie-server-groep'. Voor 'secundair-authenticatie-server-group' is het mogelijk om alle AAA-servers te gebruiken, behalve een Security Dynamics International (SDI) server; in dat geval zou de SDI nog steeds de primaire verificatieserver kunnen zijn.

Testen

> **Opmerking**: het Uitvoer Tolk Tool ondersteunt bepaalde **show** commando's. Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.** Alleen geregistreerde Cisco-gebruikers kunnen toegang krijgen tot interne Cisco-tools en -informatie.

Om deze configuratie te testen, dient u de lokale referenties (gebruikersnaam cisco met wachtwoord) en LDAP-referenties (gebruikersnaam cisco met wachtwoord van LDAP) in te voeren. Het certificaat moet aanwezig zijn:



Voer de opdracht **show vpn-sessiondb details AnyConnect** in op de ASA.

De resultaten zijn vergelijkbaar met de resultaten voor enkelvoudige verificatie. Raadpleeg "ASA Configuration for Single Authentication and Certificate Validation, Test".

Debuggen

Debugs voor WebVPN sessie en verificatie zijn vergelijkbaar. Raadpleeg "ASA Configuration for Single Authentication and Certificate Validation, Debug." Er wordt een extra verificatieproces weergegeven:

<#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
```

Debugs voor LDAP tonen details die kunnen variëren met de LDAP configuratie:

```
[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
[34]    objectClass: value = top
[34]    objectClass: value = posixAccount
[34]    objectClass: value = shadowAccount
[34]    objectClass: value = inetOrgPerson
[34]    objectClass: value = organizationalPerson
[34]    objectClass: value = person
[34]    objectClass: value = CiscoPerson
[34]    loginShell: value = /bin/bash
[34]    userPassword: value = {SSHA}pndf5sfjscTPuyrhL+/QUqhK+i1UCUTy
[34] Fiber exit Tx=315 bytes Rx=911 bytes, status=1
[34] Session End
```

ASA configuratie voor dubbele verificatie en voorvulling

Het is mogelijk om bepaalde certificaatvelden toe te wijzen aan de gebruikersnaam die wordt gebruikt voor primaire en secundaire verificatie:

<#root>

```
username test1 password cisco
```

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

```
 secondary-authentication-server-group LDAP


 default-group-policy Group1
 authorization-required

 username-from-certificate CN


 secondary-username-from-certificate OU


tunnel-group RA webvpn-attributes
 authentication aaa certificate

 pre-fill-username ssl-client


 secondary-pre-fill-username ssl-client


 group-alias RA enable
```

In dit voorbeeld gebruikt de client het certificaat: cn=**test1**,ou=**Security**,o=Cisco,l=Krakau,st=PL,c=PL.

Voor primaire authenticatie, de gebruikersnaam is ontleend aan de CN, dat is de reden waarom lokale gebruiker 'test1' is gemaakt.

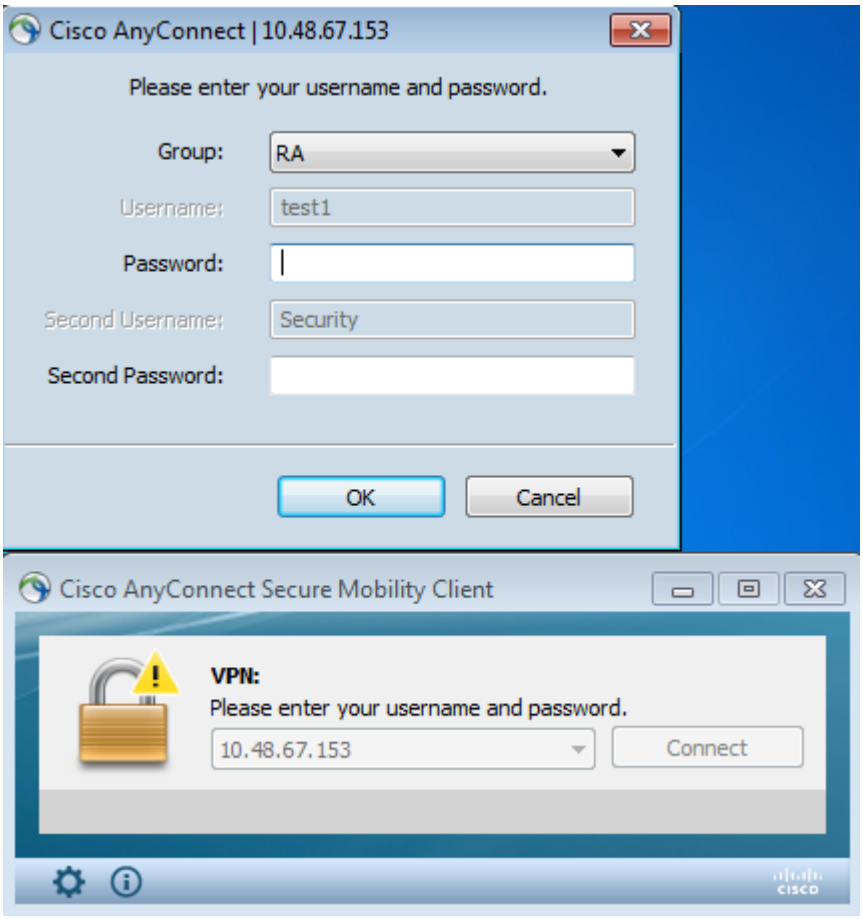
Voor secundaire authenticatie, de gebruikersnaam wordt genomen van de organisatorische eenheid (OU, dat is waarom de gebruiker 'Security' is gemaakt op de LDAP-server.

Het is ook mogelijk om AnyConnect te dwingen om pre-fill opdrachten te gebruiken om de primaire en secundaire gebruikersnaam vooraf in te vullen.

In een real-world scenario is de primaire verificatieserver meestal een AD- of LDAP-server, terwijl de secundaire verificatieserver de Rivest-, Shamir- en Adelman-server (RSA) is die token wachtwoorden gebruikt. In dit scenario moet de gebruiker AD/LDAP-referenties (die de gebruiker kent), een RSA-token-wachtwoord (die de gebruiker heeft) en een certificaat (op de gebruikte machine) opgeven.

Testen

Merk op dat u de primaire of secundaire gebruikersnaam niet kunt wijzigen omdat deze vooraf is ingevuld in de velden certificaat CN en OU:



Debuggen

Dit voorbeeld toont de voorgevulde aanvraag die naar AnyConnect is verzonden:

```
%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]
```

Hier ziet u dat de authentificatie de correcte gebruikersnamen gebruikt:

<#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
```

ASA-configuratie voor dubbele verificatie en certificaattoewijzing

Het is ook mogelijk om specifieke cliëntcertificaten aan specifieke tunnelgroepen in kaart te brengen, zoals in dit voorbeeld wordt getoond:

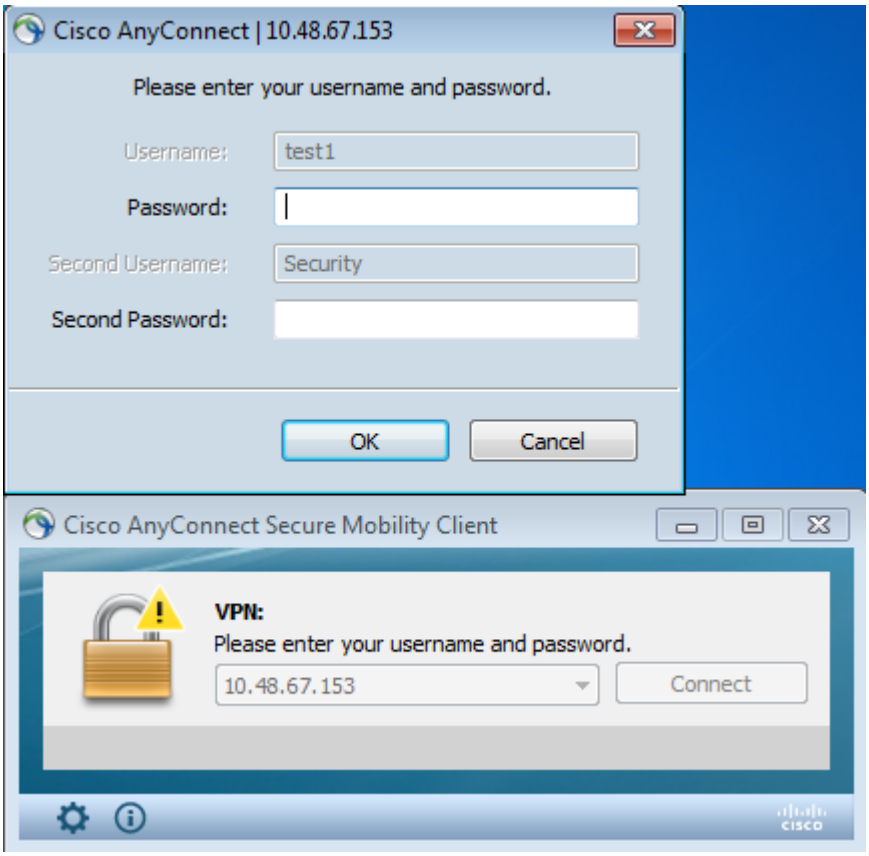
```
crypto ca certificate map CERT-MAP 10
 issuer-name co tac

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

Op deze manier worden alle gebruikerscertificaten die door de Cisco Technical Assistance Center (TAC) zijn ondertekend, toegewezen aan een tunnelgroep met de naam 'RA'.

> **Opmerking**: certificaattoewijzing voor SSL is anders geconfigureerd dan certificaattoewijzing voor IPsec. Voor IPsec, wordt het gevormd met "tunnel-groep-kaart"regels op globale configuratiewijze. Voor SSL is het geconfigureerd met 'certificate-group-map' onder webvpn-configuratiemodus.

Testen

Merk op dat, zodra het in kaart brengen van het certificaat wordt toegelaten, u niet te hoeven om tunnel-groep meer te kiezen:



Debuggen

In dit voorbeeld, staat de regel van de certificaatafbeelding de tunnelgroep toe worden gevonden:

<#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

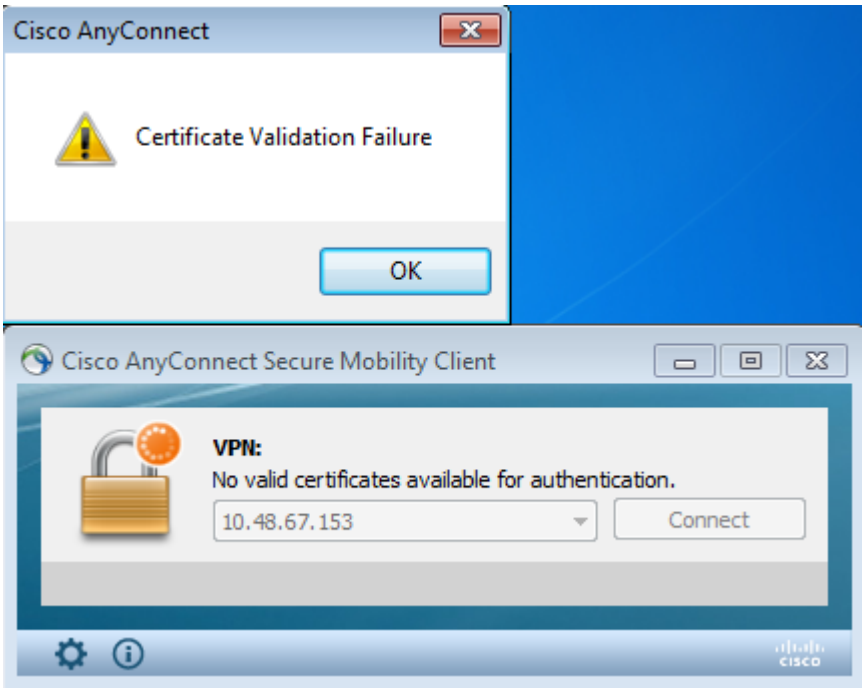
```
, Peer certificate:
serial number: 00FE9C3D61E131CDB1, subject name: cn=test1,ou=Security,o=Cisco,
l=Krakow,st=PL,c=PL, issuer_name: cn=TAC,ou=RAC,o=TAC,l=Warsaw,st=Maz,c=PL.
```

Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

Geldig certificaat niet aanwezig

Nadat u een geldig certificaat uit Windows7 verwijdert, kan AnyConnect geen geldige certificaten vinden:



Op de ASA lijkt het alsof de sessie wordt beëindigd door de client (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

Gerelateerde informatie

- **Tunnelgroepen, groepsbeleid en gebruikers configureren: dubbele verificatie configureren**
- **Gebruikersautorisatie voor een externe server voor security applicatie configureren**
- **Cisco technische ondersteuning en downloads**

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.