ASA AnyConnect Secure Mobility Client-Authentifizierung konfigurieren

Inhalt

Einleitung

In diesem Dokument wird eine Konfiguration für den Zugriff durch den ASA AnyConnect Secure Mobility Client beschrieben, die eine doppelte Authentifizierung mit Zertifikatsvalidierung verwendet.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundkenntnisse der Konfiguration der ASA-Kommandozeile (CLI) und der SSL-VPN-Konfiguration (Secure Socket Layer)
- Grundkenntnisse der X509-Zertifikate

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

- Cisco Adaptive Security Appliance (ASA)-Software, Version 8.4 und höher

- Windows 7 mit Cisco AnyConnect Secure Mobility Client 3.1

Es wird davon ausgegangen, dass Sie eine externe Zertifizierungsstelle (Certificate Authority, CA) verwendet haben, um Folgendes zu generieren:

- Ein Public-Key-Verschlüsselungsstandard #12 (PKCS #12) mit Base64-Kodierung für ASA (AnyConnect.pfx)
- Ein PKCS #12 Zertifikat für AnyConnect

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

In diesem Dokument wird ein Konfigurationsbeispiel für den Zugriff durch die Adaptive Security Appliance (ASA) Cisco AnyConnect Secure Mobility Client beschrieben, der eine doppelte Authentifizierung mit Zertifikatsvalidierung verwendet. Als AnyConnect-Benutzer müssen Sie das richtige Zertifikat und die richtigen Anmeldeinformationen für die primäre und sekundäre Authentifizierung bereitstellen, um VPN-Zugriff zu erhalten. Dieses Dokument enthält auch ein Beispiel für die Zertifikatszuordnung mit der Pre-Fill-Funktion.

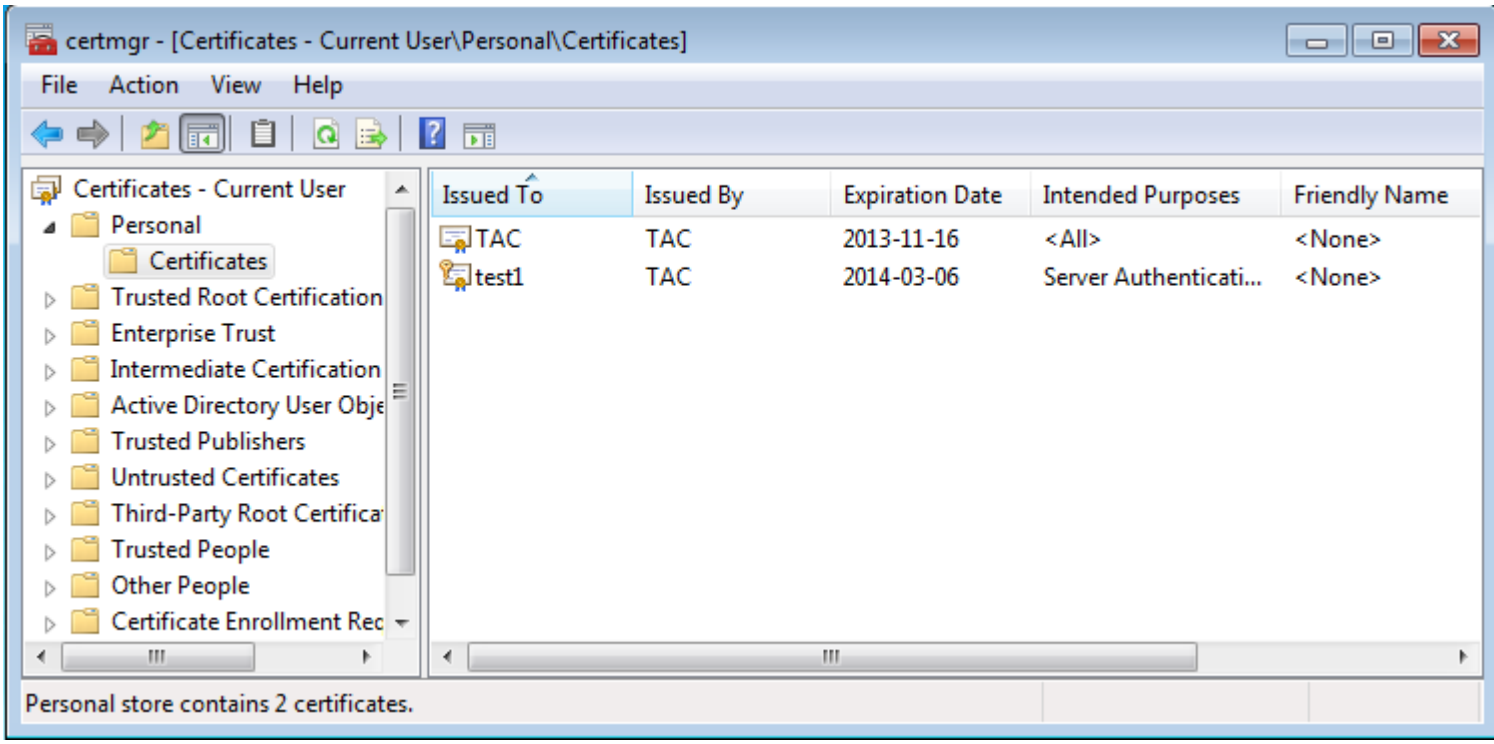
Konfigurieren

> **Hinweis**: Verwenden Sie das Tool zur Befehlssuche, um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten. Nur registrierte Cisco Benutzer können auf interne Tools und Informationen von Cisco zugreifen.

Zertifikat für AnyConnect

Um ein Beispielzertifikat zu installieren, doppelklicken Sie auf die Datei AnyConnect.pfx, und installieren Sie das Zertifikat als persönliches Zertifikat.

Verwenden Sie den Zertifikats-Manager (certmgr.msc), um die Installation zu überprüfen:



Standardmäßig versucht AnyConnect, ein Zertifikat im Microsoft-Benutzerspeicher zu finden. Änderungen am AnyConnect-Profil sind nicht erforderlich.

Installation des Zertifikats auf der ASA

Dieses Beispiel zeigt, wie ASA ein Base64 PKCS #12-Zertifikat importieren kann:

<#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
```

Verwenden Sie den Befehl **show crypto ca Certificates**, um den Import zu überprüfen:

```
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
```

> **Hinweis**: Das Output Interpreter Tool unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter-Tool, um eine Analyse der **show**-Befehlsausgabe anzuzeigen. Nur registrierte Cisco Benutzer können auf interne Tools und Informationen von Cisco zugreifen.

ASA-Konfiguration für Einzelauthentifizierung und Zertifikatsvalidierung

ASA verwendet sowohl Authentifizierung, Autorisierung und Abrechnung (Authentication, Authorization, Accounting - AAA) als auch Zertifikatsauthentifizierung. Die Zertifikatsvalidierung ist obligatorisch. Bei der AAA-Authentifizierung wird eine lokale Datenbank verwendet.

Dieses Beispiel zeigt eine einzelne Authentifizierung mit Zertifikatvalidierung.

<#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

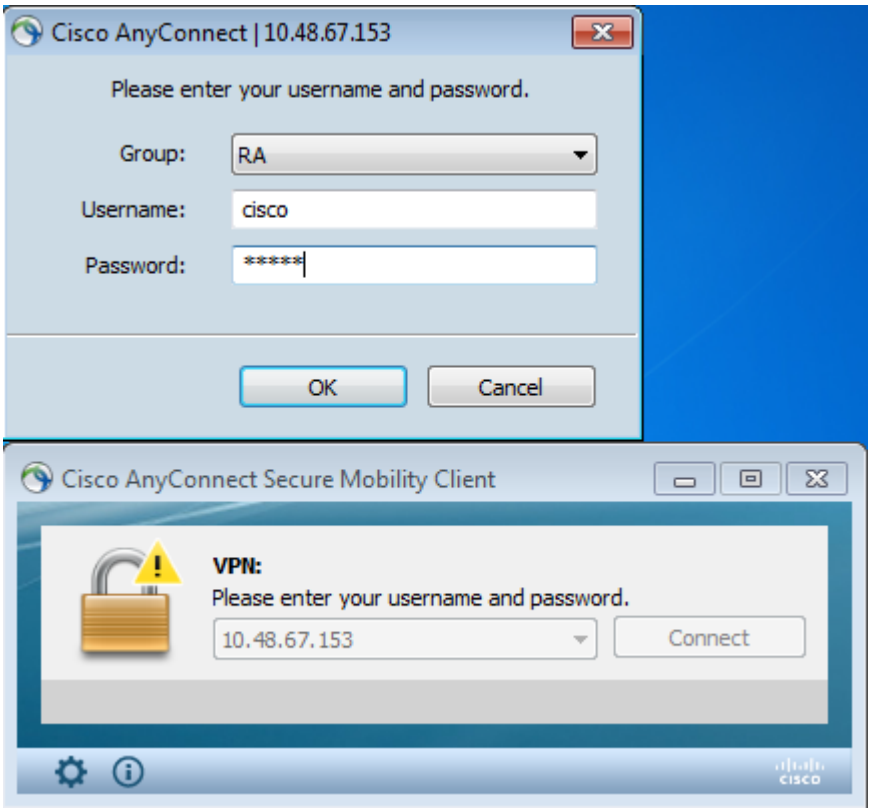
```
 group-alias RA enable
```

Zusätzlich zu dieser Konfiguration ist es möglich, eine LDAP-Autorisierung (Lightweight Directory Access Protocol) mit dem Benutzernamen eines bestimmten Zertifikatfelds, z. B. des Zertifikatsnamens (Certificate Name, CN), durchzuführen. Zusätzliche Attribute können abgerufen und auf die VPN-Sitzung angewendet werden. Weitere Informationen zur Authentifizierung und Zertifikatsautorisierung finden Sie unter "ASA AnyConnect VPN and OpenLDAP Authorization with Custom Schema and Certificates Configuration Example".

Test

> **Hinweis**: Das Output Interpreter Tool unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter-Tool, um eine Analyse der **show**-Befehlsausgabe anzuzeigen. Nur registrierte Cisco Benutzer können auf interne Tools und Informationen von Cisco zugreifen.

Um diese Konfiguration zu testen, geben Sie die lokalen Anmeldeinformationen an (Benutzername cisco mit Kennwort cisco). Das Zertifikat muss vorhanden sein:



Geben Sie den Befehl **show vpn-sessiondb detail AnyConnect** auf der ASA ein:

<#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 :
```

Fehlersuche

> **Hinweis**: Lesen Sie Wichtige Informationen zu Debug-Befehlen, bevor Sie **Debug**-Befehle verwenden.

In diesem Beispiel wurde das Zertifikat nicht in der Datenbank zwischengespeichert, eine entsprechende Zertifizierungsstelle wurde gefunden, die korrekte Schlüsselverwendung wurde verwendet (ClientAuthentication), und das Zertifikat wurde erfolgreich validiert:

<#root>

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

debug webvpn AnyConnect 255

```
debug crypto ca 255
```

Detaillierte Debug-Befehle, wie der Befehl **debug webvpn 255**, können viele Protokolle in einer Produktionsumgebung generieren und die ASA stark belasten. Einige WebVPN-Debugging-Programme wurden der Übersichtlichkeit halber entfernt:

<#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

Dies ist der Versuch, eine passende Tunnelgruppe zu finden. Es gibt keine spezifischen Zertifikatzuordnungsregeln, und die von Ihnen angegebene Tunnelgruppe wird verwendet:

<#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)

Dies sind die SSL- und allgemeinen Sitzungsdebugs:

<#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-Konfiguration für doppelte Authentifizierung und Zertifikatsvalidierung

Dies ist ein Beispiel für die doppelte Authentifizierung, bei der der primäre Authentifizierungsserver LOKAL und der sekundäre Authentifizierungsserver LDAP ist. Die Zertifikatsvalidierung ist weiterhin aktiviert.

Dieses Beispiel zeigt die LDAP-Konfiguration:

```
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 sehen Sie die Erweiterung eines sekundären Authentifizierungsservers:

```
<#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
```

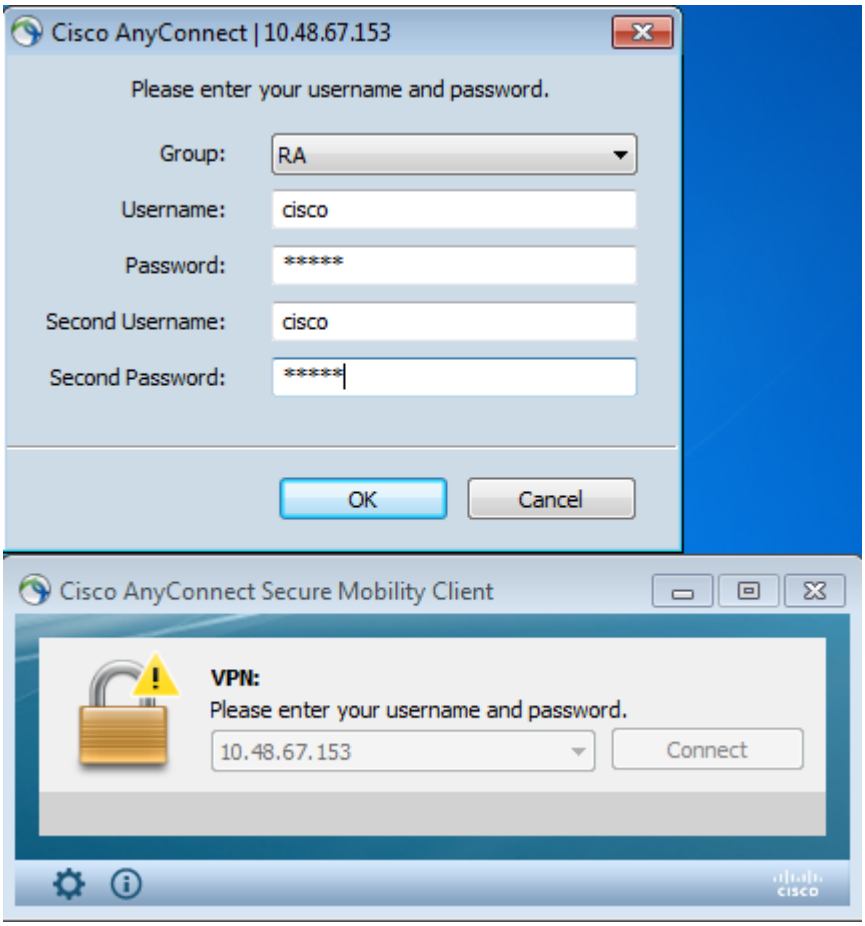
'authentication-server-group LOCAL' wird in der Konfiguration nicht angezeigt, da es sich um eine Standardeinstellung handelt.

Für 'authentication-server-group' kann jeder andere AAA-Server verwendet werden. Für "second-authentication-server-group" können alle AAA-Server mit Ausnahme eines SDI-Servers (Security Dynamics International) verwendet werden. In diesem Fall kann das SDI weiterhin der primäre Authentifizierungsserver sein.

Test

> **Hinweis**: Das Output Interpreter Tool unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter-Tool, um eine Analyse der **show**-Befehlsausgabe anzuzeigen. Nur registrierte Cisco Benutzer können auf interne Tools und Informationen von Cisco zugreifen.

Geben Sie zum Testen dieser Konfiguration die lokalen Anmeldeinformationen (Benutzername cisco mit Kennwort cisco) und LDAP-Anmeldeinformationen (Benutzername cisco mit Kennwort vom LDAP) an. Das Zertifikat muss vorhanden sein:



Geben Sie den Befehl **show vpn-sessiondb detail AnyConnect** auf der ASA ein.

Die Ergebnisse ähneln denen für die Einzelauthentifizierung. Weitere Informationen finden Sie unter "ASA Configuration for Single Authentication and Certificate Validation, Test".

Fehlersuche

Die Debugging-Optionen für WebVPN-Sitzungen und -Authentifizierung sind ähnlich. Weitere Informationen finden Sie unter "ASA Configuration for Single Authentication and Certificate Validation, Debug". Ein weiterer Authentifizierungsprozess wird angezeigt:

<#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
```

Die Debugger für LDAP zeigen Details an, die von der LDAP-Konfiguration abweichen können:

```
[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-Konfiguration für Doppelauthentifizierung und Vorabfüllung

Bestimmte Zertifikatfelder können dem Benutzernamen zugeordnet werden, der für die primäre und sekundäre Authentifizierung verwendet wird:

<#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 diesem Beispiel verwendet der Client das Zertifikat: cn=**test1**,ou=**Security,**o=Cisco,l=Krakow,st=PL,c=PL.

Für die primäre Authentifizierung wird der Benutzername aus der CN übernommen, weshalb der lokale Benutzer 'test1' erstellt wurde.

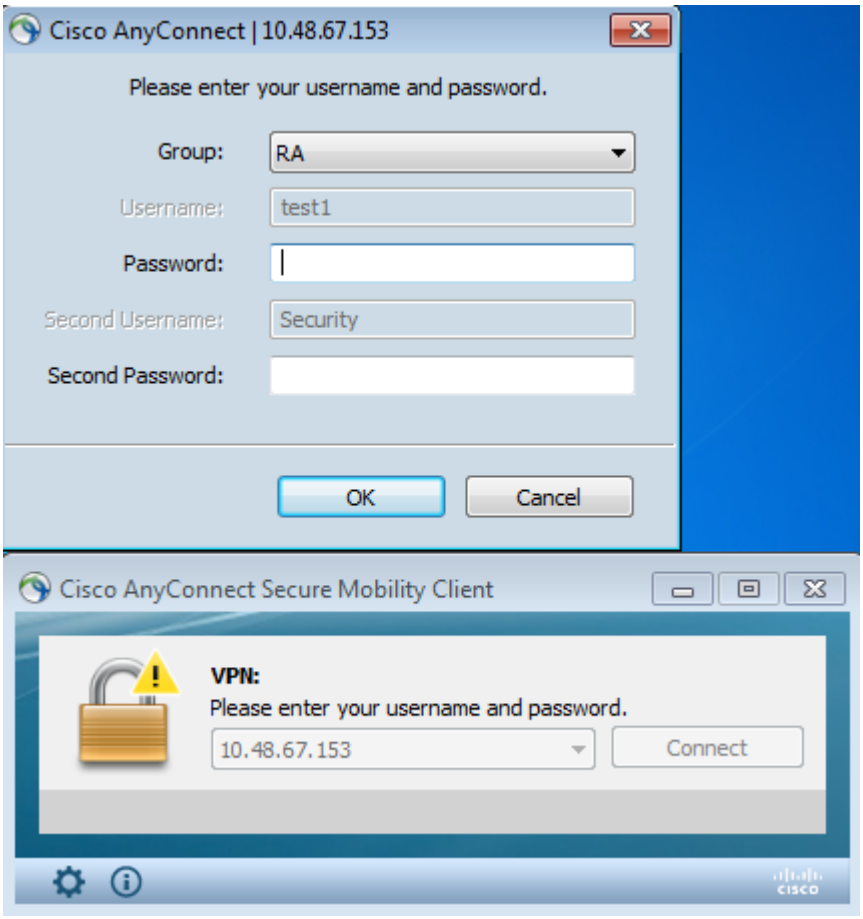
Für die sekundäre Authentifizierung wird der Benutzername von der Organisationseinheit (OU) übernommen, weshalb der Benutzer 'Sicherheit' auf dem LDAP-Server erstellt wurde.

Es ist auch möglich, AnyConnect zu zwingen, Pre-Fill-Befehle zu verwenden, um den primären und sekundären Benutzernamen vorab zu füllen.

In der Praxis ist der primäre Authentifizierungsserver in der Regel ein AD- oder LDAP-Server, während der sekundäre Authentifizierungsserver der Rivest-, Shamir- und Adelman (RSA)-Server ist, der Tokenpasswörter verwendet. In diesem Szenario muss der Benutzer AD/LDAP-Anmeldeinformationen (die der Benutzer kennt), ein RSA-Token-Kennwort (das der Benutzer besitzt) und ein Zertifikat (auf dem verwendeten Computer) angeben.

Test

Beachten Sie, dass Sie den primären oder sekundären Benutzernamen nicht ändern können, da er aus den Zertifikats-CN- und -OU-Feldern bereits ausgefüllt ist:



Fehlersuche

Dieses Beispiel zeigt die an AnyConnect gesendete Pre-Fill-Anforderung:

```
%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 sehen Sie, dass bei der Authentifizierung die richtigen Benutzernamen verwendet werden:

<#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-Konfiguration für Doppelauthentifizierung und Zertifikatszuordnung

Es ist auch möglich, bestimmte Clientzertifikate bestimmten Tunnelgruppen zuzuordnen, wie in diesem Beispiel gezeigt:

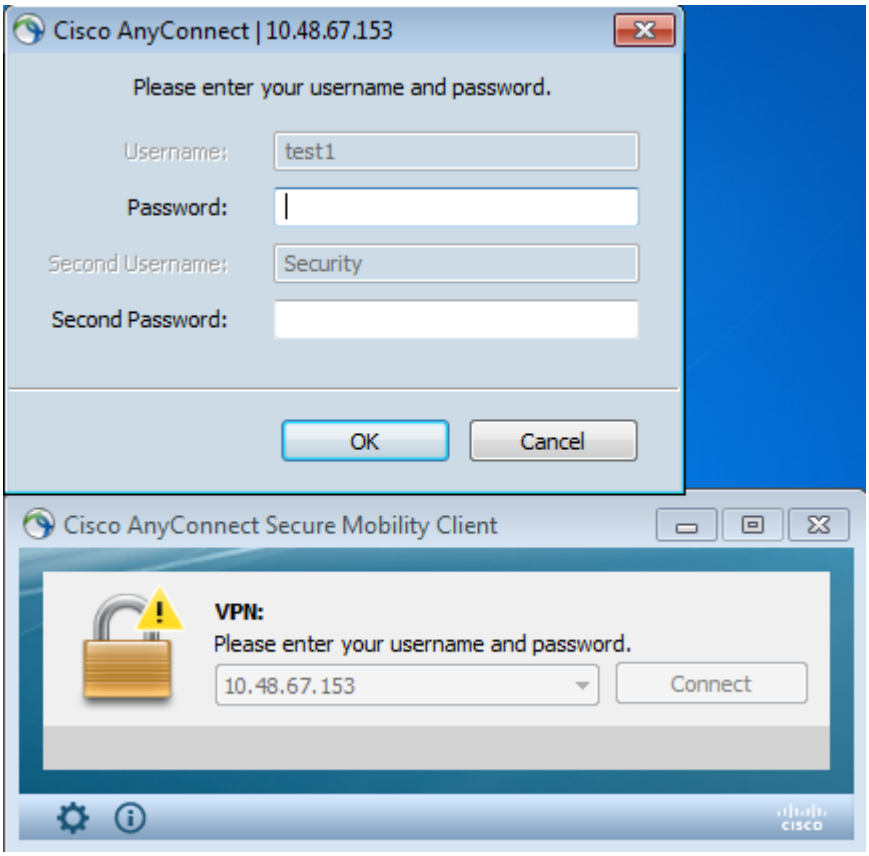
```
crypto ca certificate map CERT-MAP 10
 issuer-name co tac

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

Auf diese Weise werden alle Benutzerzertifikate, die von der CA des Cisco Technical Assistance Center (TAC) signiert wurden, einer Tunnelgruppe mit der Bezeichnung "RA" zugeordnet.

> **Hinweis**: Die Zertifikatzuordnung für SSL wird anders konfiguriert als die Zertifikatzuordnung für IPsec. Für IPsec wird es mit 'tunnel-group-map'-Regeln im globalen Konfigurationsmodus konfiguriert. Für SSL wird sie im WebVPN-Konfigurationsmodus mit "certificate-group-map" konfiguriert.

Test

Beachten Sie, dass Sie nach dem Aktivieren der Zertifikatszuordnung nicht mehr "tunnel-group" auswählen müssen:



Fehlersuche

In diesem Beispiel ermöglicht die Zertifikatzuordnungsregel das Auffinden der Tunnelgruppe:

<#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

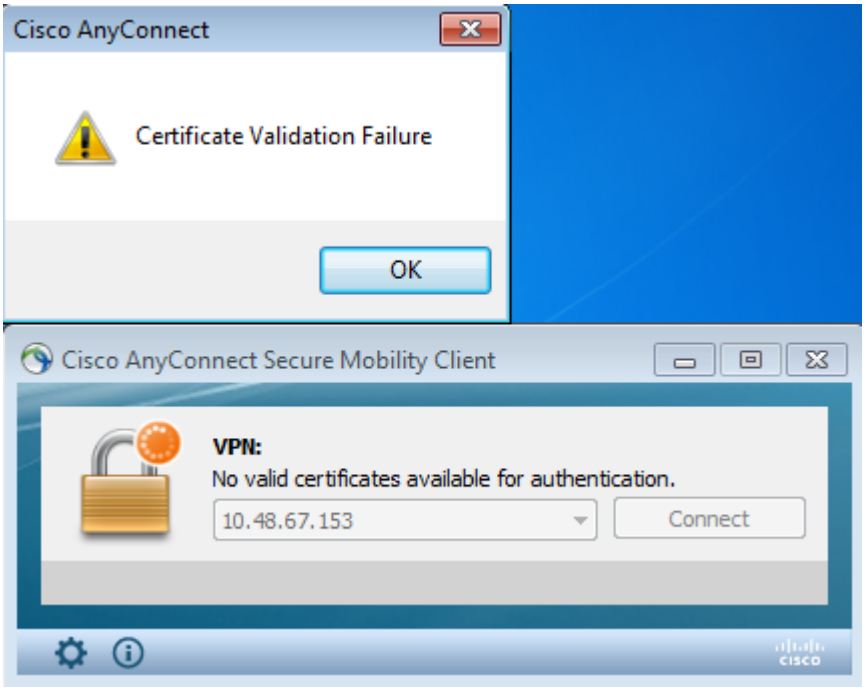
```
, Peer certificate:
serial number: 00FE9C3D61E131CDB1, subject name: cn=test1,ou=Security,o=Cisco,
l=Krakow,st=PL,c=PL, issuer_name: cn=TAC,ou=RAC,o=TAC,l=Warsaw,st=Maz,c=PL.
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Gültiges Zertifikat nicht vorhanden

Nachdem Sie ein gültiges Zertifikat aus Windows7 entfernt haben, kann AnyConnect keine gültigen Zertifikate finden:



Auf der ASA sieht es so aus, als ob die Sitzung vom Client beendet wird (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

Zugehörige Informationen

- **Konfigurieren von Tunnelgruppen, Gruppenrichtlinien und Benutzern: Konfigurieren der doppelten Authentifizierung**
- **Konfigurieren eines externen Servers für die Benutzerautorisierung der Sicherheitsappliance**
- **Technischer Support und Downloads von Cisco**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.