Configuración de la autenticación de ASA AnyConnect Secure Mobility Client

Contenido

Introducción

Este documento describe una configuración para el acceso de ASA AnyConnect Secure Mobility Client que utiliza doble autenticación con validación de certificados.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimientos básicos de la configuración de la interfaz de línea de comandos (CLI) de ASA y de la configuración VPN de capa de conexión segura (SSL)
- Conocimientos básicos de los certificados X509

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Software Cisco Adaptive Security Appliance (ASA), versión 8.4 y posteriores

- Windows 7 con Cisco AnyConnect Secure Mobility Client 3.1

Se supone que ha utilizado una autoridad de certificación (CA) externa para generar:

- Certificado codificado en base64 del estándar de criptografía de clave pública #12 (PKCS #12) para ASA (AnyConnect.pfx)
- Un certificado PKCS #12 para AnyConnect

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Este documento describe un ejemplo de configuración para el acceso de Cisco AnyConnect Secure Mobility Client del dispositivo de seguridad adaptable (ASA) que utiliza doble autenticación con validación de certificados. Como usuario de AnyConnect, debe proporcionar el certificado y las credenciales correctas para la autenticación primaria y secundaria para obtener acceso VPN. Este documento también proporciona un ejemplo de asignación de certificados con la función de relleno previo.

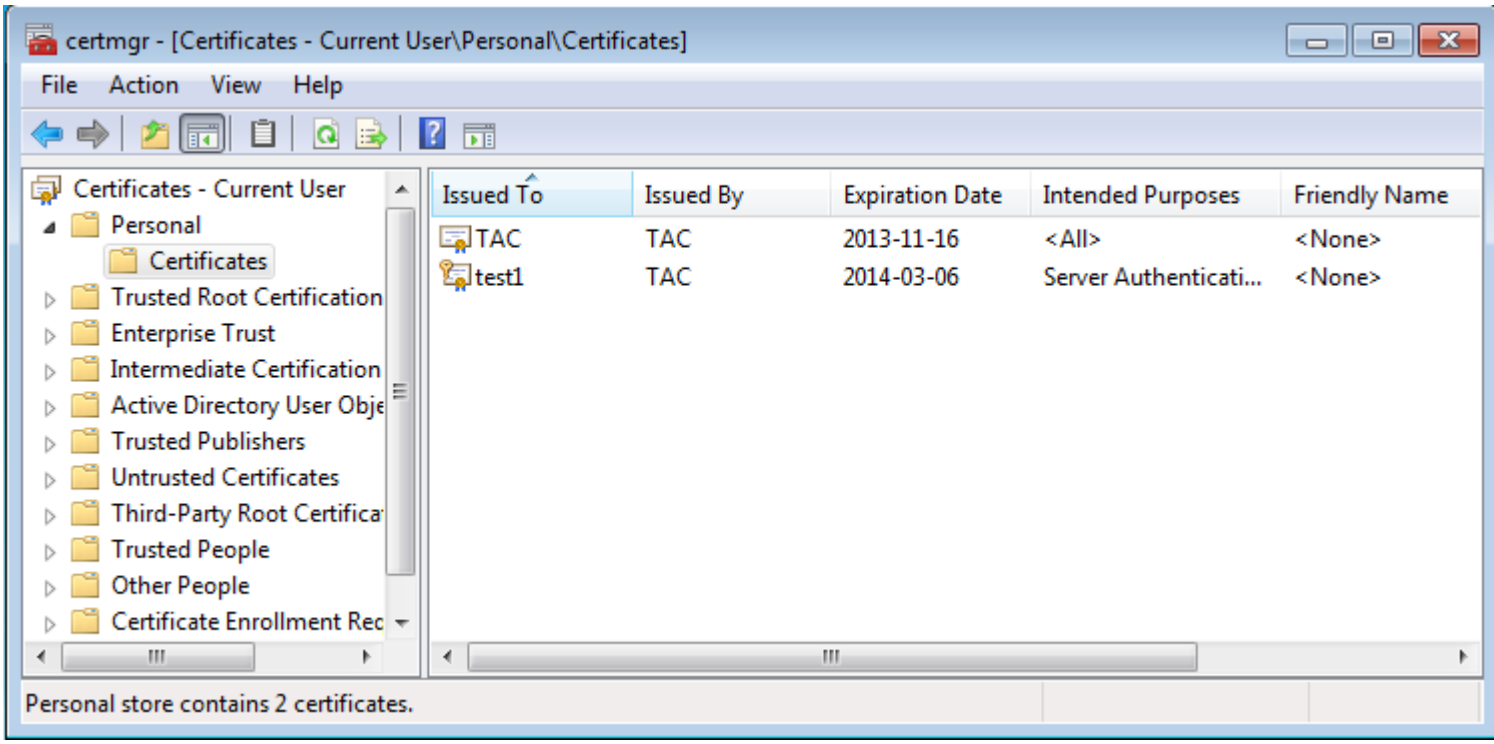
Configurar

> **Nota**: Utilice la Command Lookup Tool para obtener más información sobre los comandos utilizados en esta sección. Solo los usuarios registrados de Cisco pueden acceder a la información y las herramientas internas de Cisco.

Certificado para AnyConnect

Para instalar un certificado de ejemplo, haga doble clic en el archivo AnyConnect.pfx e instale ese certificado como certificado personal.

Utilice el Administrador de certificados (certmgr.msc) para verificar la instalación:



De forma predeterminada, AnyConnect intenta encontrar un certificado en el almacén de usuarios de Microsoft; no es necesario realizar ningún cambio en el perfil de AnyConnect.

Instalación del certificado en ASA

Este ejemplo muestra cómo ASA puede importar un certificado PKCS #12 base64:

<#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
```

Utilice el comando **show crypto ca certificates** para verificar la importación:

```
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
```

Nota: La herramienta Output Interpreter Tool soporta ciertos comandos **show**. Utilice la herramienta para ver una análisis de información de salida del comando show. Solo los usuarios registrados de Cisco pueden acceder a la información y las herramientas internas de Cisco.

Configuración de ASA para autenticación única y validación de certificados

ASA utiliza autenticación de autenticación, autorización y contabilidad (AAA) y autenticación de certificados. La validación del certificado es obligatoria. La autenticación AAA utiliza una base de datos local.

Este ejemplo muestra la autenticación única con validación de certificados.

<#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

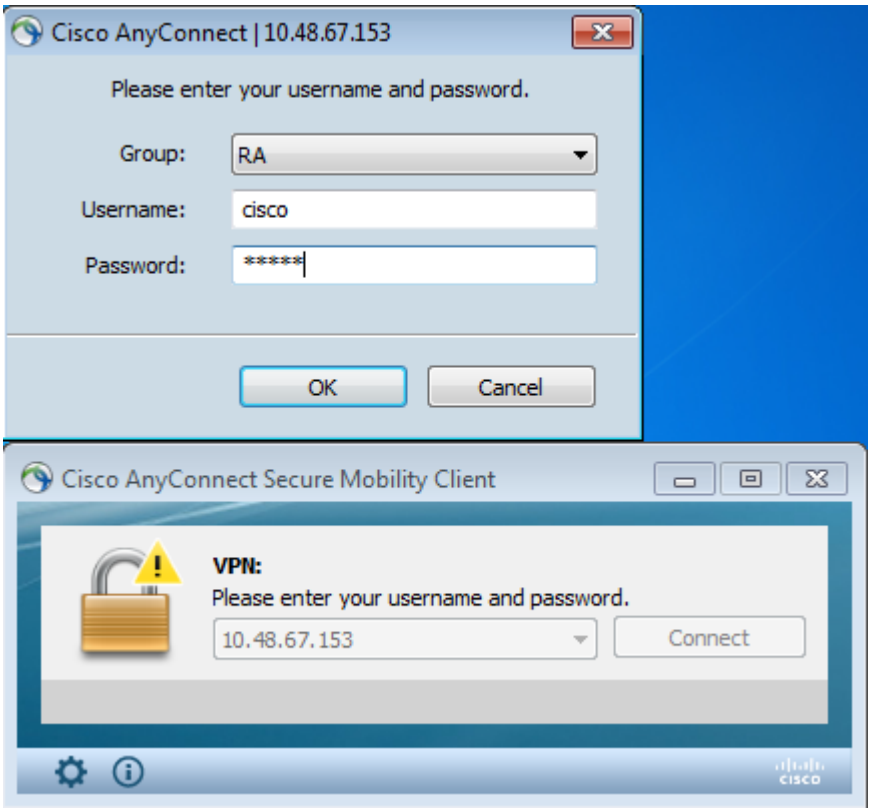
```
 group-alias RA enable
```

Además de esta configuración, es posible realizar una autorización LDAP (protocolo ligero de acceso a directorios) con el nombre de usuario de un campo de certificado específico, como el nombre de certificado (CN). Los atributos adicionales se pueden recuperar y aplicar a la sesión VPN. Para obtener más información sobre la autenticación y la autorización de certificados, consulte el "Ejemplo de Configuración de ASA AnyConnect VPN y OpenLDAP Authorization con Esquema y Certificados Personalizados".

Prueba

> **Nota**: La herramienta Output Interpreter Tool soporta ciertos comandos **show**. Utilice la herramienta para ver una análisis de información de salida del comando show. Solo los usuarios registrados de Cisco pueden acceder a la información y las herramientas internas de Cisco.

Para probar esta configuración, proporcione las credenciales locales (nombre de usuario cisco con contraseña cisco). El certificado debe estar presente:



Ingrese el comando **show vpn-sessiondb detail AnyConnect** en 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 :
```

Depurar

Nota: Consulte Información Importante sobre Comandos Debug antes de utilizar los comandos debug.

En este ejemplo, el certificado no se almacenó en caché en la base de datos, se encontró una CA correspondiente, se utilizó el uso de clave correcto (ClientAuthentication) y el certificado se validó correctamente:

<#root>

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

debug webvpn AnyConnect 255

```
debug crypto ca 255
```

Los comandos de depuración detallados, como el comando **debug webvpn 255**, pueden generar muchos registros en un entorno de producción y colocar una carga pesada en un ASA. Algunas depuraciones de WebVPN se han eliminado para mayor claridad:

<#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

Este es el intento de encontrar un grupo de túnel coincidente. No hay reglas de asignación de certificados específicas y se utiliza el grupo de túnel que proporcione:

<#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)

Éstas son las depuraciones SSL y de sesión general:

<#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.
```

Configuración ASA para Autenticación Doble y Validación de Certificados

Este es un ejemplo de doble autenticación, donde el servidor de autenticación primario es LOCAL, y el servidor de autenticación secundario es LDAP. La validación de certificados sigue habilitada.

Este ejemplo muestra la configuración de LDAP:

```
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
```

Aquí está la adición de un servidor de autenticación secundario:

<#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

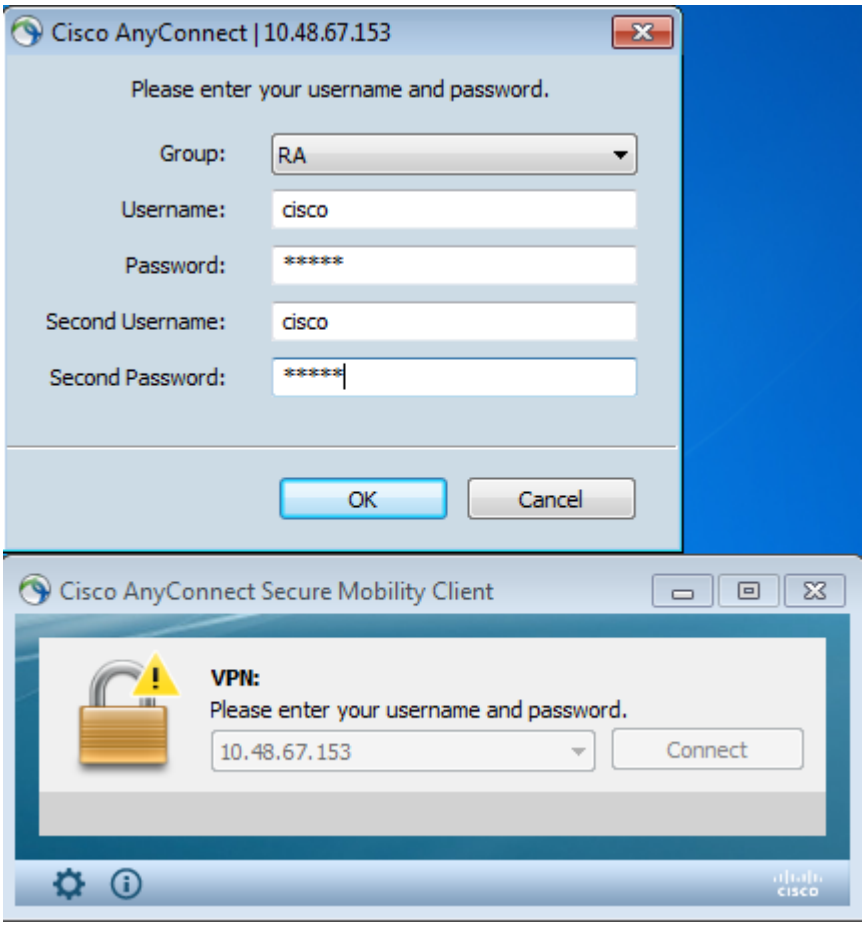
No ve 'authentication-server-group LOCAL' en la configuración porque es una configuración predeterminada.

Cualquier otro servidor AAA se puede utilizar para 'authentication-server-group'. Para 'secondary-authentication-server-group', es posible utilizar todos los servidores AAA excepto un servidor de Security Dynamics International (SDI); en ese caso, el SDI podría seguir siendo el servidor de autenticación principal.

Prueba

> **Nota**: La herramienta Output Interpreter Tool soporta ciertos comandos **show**. Utilice la herramienta para ver una análisis de información de salida del comando show. Solo los usuarios registrados de Cisco pueden acceder a la información y las herramientas internas de Cisco.

Para probar esta configuración, proporcione las credenciales locales (username cisco with password cisco) y las credenciales LDAP (username cisco with password from LDAP). El certificado debe estar presente:



Ingrese el comando **show vpn-sessiondb detail AnyConnect** en ASA.

Los resultados son similares a los de la autenticación única. Consulte "Configuración de ASA para Autenticación Única y Validación de Certificados, Prueba".

Depurar

Las depuraciones para la sesión y la autenticación WebVPN son similares. Consulte "Configuración ASA para Autenticación Única y Validación de Certificados, Debug". Aparece un proceso de autenticación adicional:

<#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
```

Los debugs para LDAP muestran detalles que pueden variar con la configuración de LDAP:

```
[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
```

Configuración ASA para Autenticación Doble y Pre-Llenado

Es posible asignar ciertos campos de certificado al nombre de usuario que se utiliza para la autenticación primaria y secundaria:

<#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
```

En este ejemplo, el cliente utiliza el certificado: cn=**test1**,ou=**Security**,o=Cisco,l=Cracovia,st=PL,c=PL.

Para la autenticación primaria, el nombre de usuario se toma del CN, razón por la cual se creó el usuario local 'test1'.

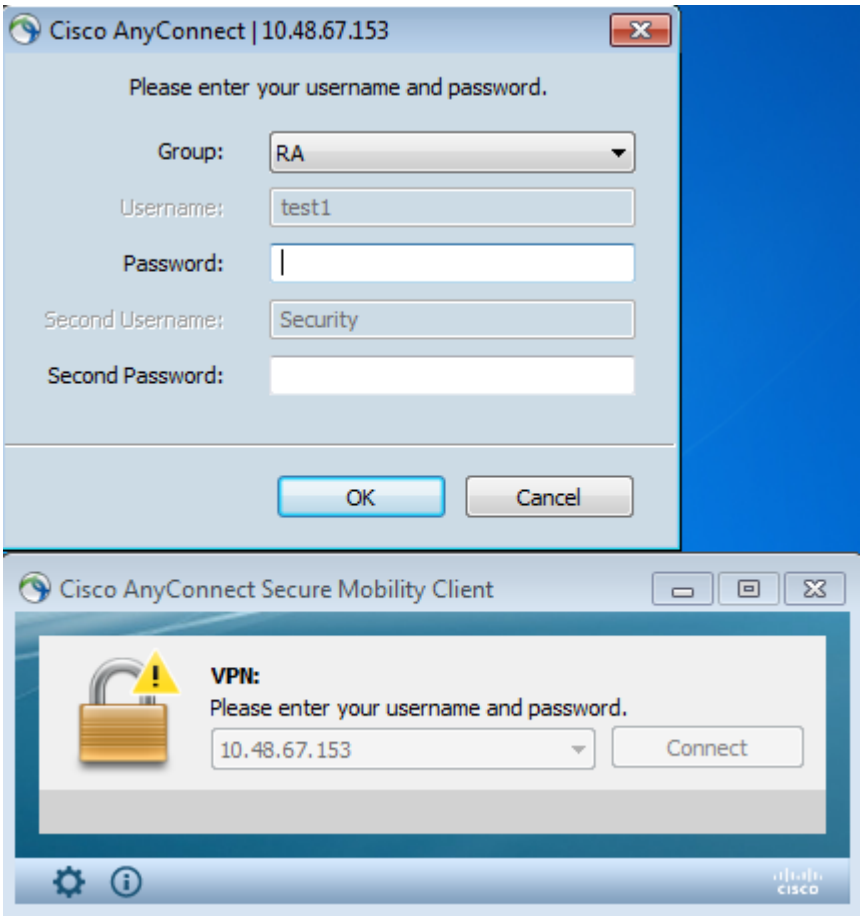
Para la autenticación secundaria, el nombre de usuario se toma de la unidad organizativa (OU), razón por la cual se creó el usuario 'Security' en el servidor LDAP.

También es posible forzar a AnyConnect a utilizar comandos pre-fill para pre-llenar el nombre de usuario primario y secundario.

En una situación real, el servidor de autenticación principal suele ser un servidor AD o LDAP, mientras que el servidor de autenticación secundario es el servidor Rivest, Shamir y Adelman (RSA) que utiliza contraseñas de token. En esta situación, el usuario debe proporcionar credenciales de AD/LDAP (que el usuario conoce), una contraseña de token RSA (que el usuario tiene) y un certificado (en el equipo que se utiliza).

Prueba

Tenga en cuenta que no puede cambiar el nombre de usuario principal o secundario porque ya está rellenado desde los campos CN y OU del certificado:



Depurar

En este ejemplo se muestra la solicitud de relleno enviada a AnyConnect:

```
%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]
```

Aquí puede ver que la autenticación utiliza los nombres de usuario correctos:

<#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
```

Configuración ASA para Autenticación Doble y Asignación de Certificados

También es posible asignar certificados de cliente específicos a grupos de túnel específicos, como se muestra en este ejemplo:

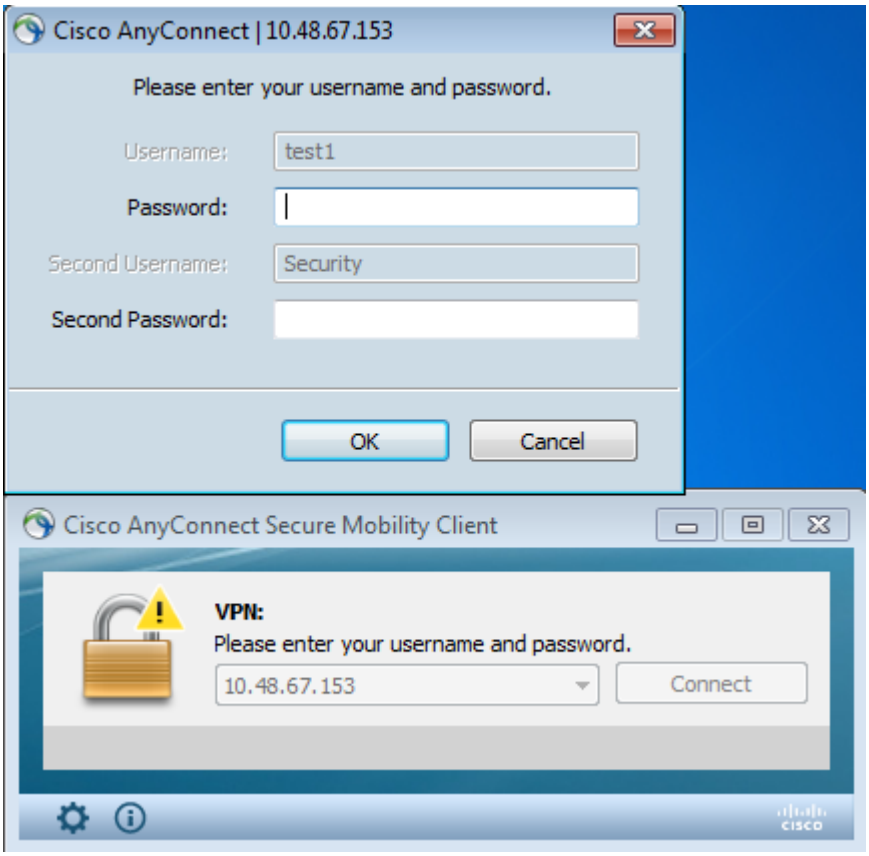
```
crypto ca certificate map CERT-MAP 10
 issuer-name co tac

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

De este modo, todos los certificados de usuario firmados por la CA del centro de asistencia técnica Cisco Technical Assistance Center (TAC) se asignan a un grupo de túnel denominado 'RA'.

> **Nota**: La asignación de certificados para SSL se configura de manera diferente que la asignación de certificados para IPSec. Para IPSec, se configura con las reglas 'tunnel-group-map' en el modo de configuración global. Para SSL, se configura con 'certificate-group-map' en el modo de configuración webvpn.

Prueba

Observe que, una vez habilitada la asignación de certificados, ya no necesita elegir el grupo de túnel:



Depurar

En este ejemplo, la regla de asignación de certificados permite encontrar el grupo de túnel:

<#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.
```

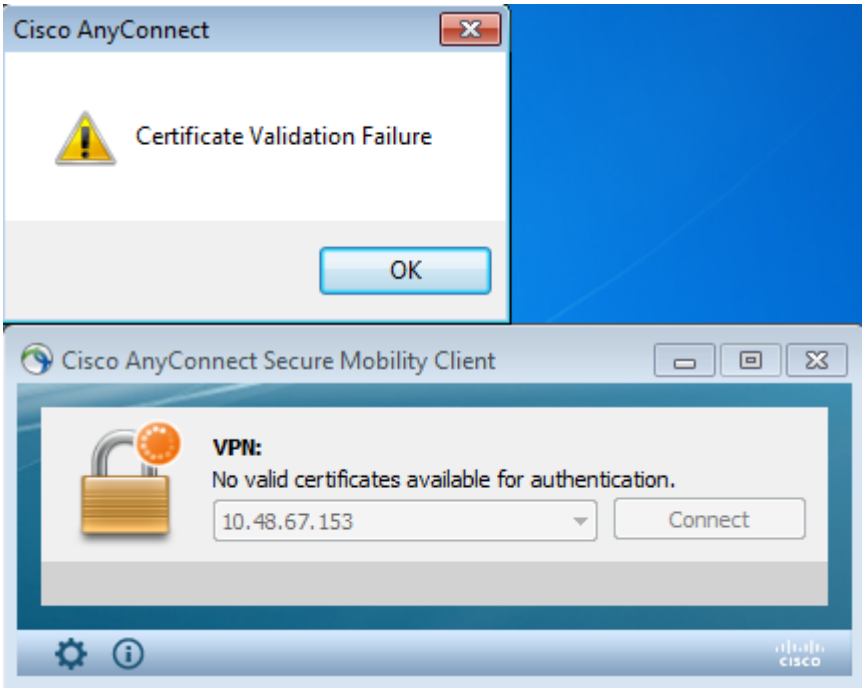
Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

No hay certificado válido

Después de quitar un certificado válido de Windows7, AnyConnect no puede encontrar ningún certificado

válido:



En el ASA, parece que la sesión es terminada por el cliente (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

Información Relacionada

- **Configuración de Grupos de Túnel, Políticas de Grupo y Usuarios: Configuración de**

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).