Autenticación doble ASA AnyConnect con la validación de certificado, la asignación, y la guía de configuración del Pre-Fill

Contenido

Introducción

Este documento describe un ejemplo de configuración para el acceso de Cliente de movilidad Cisco AnyConnect Secure adaptante del dispositivo de seguridad (ASA) que utiliza la Autenticación doble con la validación de certificado. Como usuario de AnyConnect, usted debe proporcionar el certificado y las credenciales correctos para el primario y la autenticación secundaria para conseguir el acceso VPN. Este documento también proporciona un ejemplo de la asignación del certificado con la característica del pre-fill.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento básico de la configuración del comando line interface(cli) ASA y de la configuración VPN del Secure Socket Layer (SSL)
- Conocimiento básico de los Certificados X509

Componentes Utilizados

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

- Software adaptante del dispositivo de seguridad de Cisco (ASA), versión 8.4 y posterior
- Windows 7 con el Cliente de movilidad Cisco AnyConnect Secure 3.1

Se asume que usted utilizó un Certificate Authority (CA) externo para generar:

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

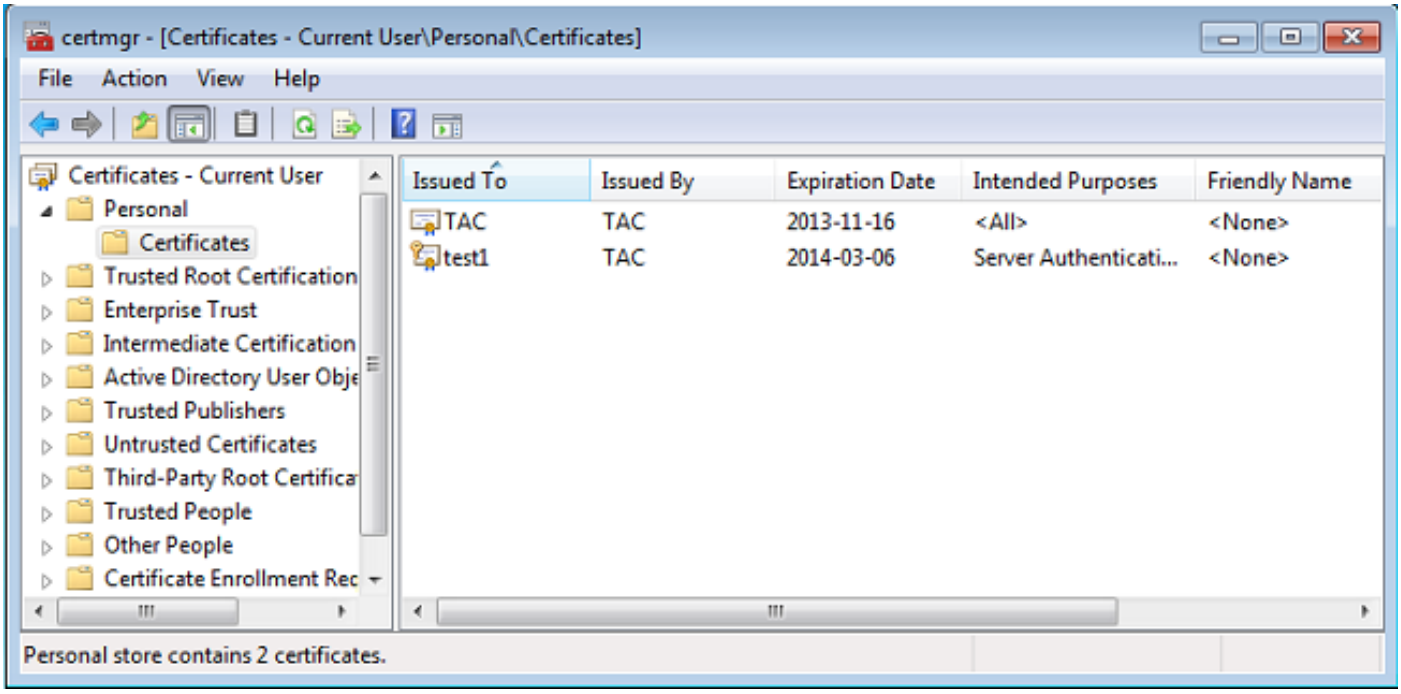
Configurar

> Nota: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Certificado para AnyConnect

Para instalar un certificado del ejemplo, haga doble clic el archivo anyconnect.pfx, y instale ese certificado como certificado personal.

Utilice al Certificate Manager (certmgr.msc) para verificar la instalación:



Por abandono, intentos de AnyConnect para encontrar un certificado en el almacén del usuario de Microsoft; no hay necesidad de realizar ningunos cambios en el perfil de AnyConnect.

Instalación del certificado en el ASA

Este ejemplo muestra cómo el ASA puede importar un certificado del PKCS-12 del base64:

```
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)# 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
```

> Nota: Los ciertos comandos show de los soportes de la herramienta del Output Interpreter (clientes registrados solamente). Utilice la herramienta del Output Interpreter para

ver una análisis de la salida del comando show.

Configuración ASA para la solas autenticación y validación de certificado

El ASA utiliza la autenticación y la autenticación certificada del Authentication, Authorization, and Accounting (AAA). La validación de certificado es obligatoria. La autenticación AAA utiliza una base de datos local.

Este ejemplo muestra la sola autenticación con la validación de certificado.

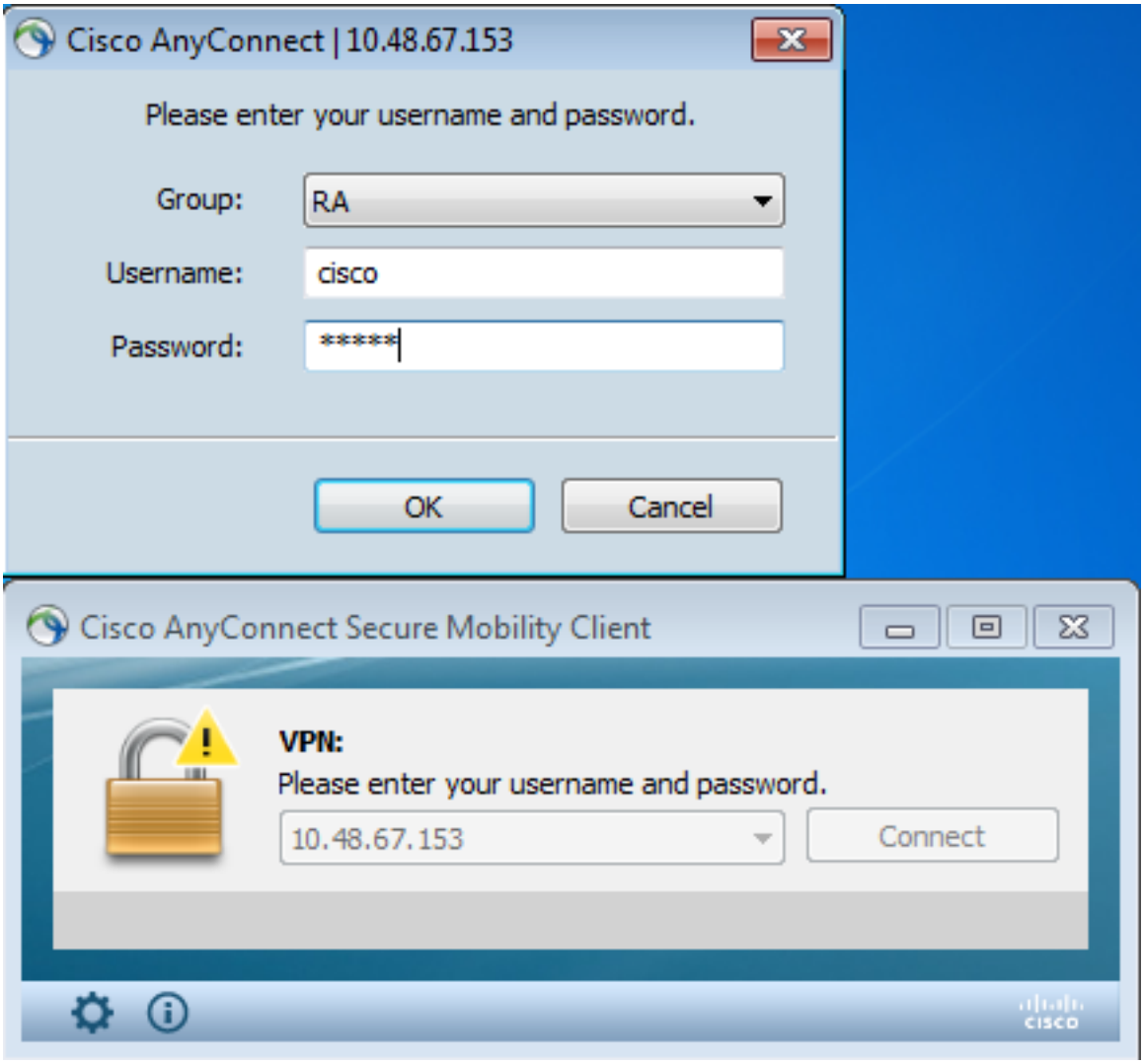
```
ip local pool POOL 10.1.1.10-10.1.1.20
username cisco password cisco

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 la autorización del Lightweight Directory Access Protocol (LDAP) con el nombre de usuario de un campo específico del certificado, tal como el nombre del certificado (CN). Los atributos adicionales se pueden después extraer y aplicar a la sesión de VPN. Para más información sobre la autenticación y la autorización del certificado, refiera a “ASA Anyconnect VPN y a la autorización de OpenLDAP con el esquema de encargo y certifica el ejemplo de configuración.”

Prueba

> Nota: La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

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



Ingrese el comando del **anyconnect del detalle de VPN-sessiondb de la demostración** en el ASA:

```
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 de Debug antes de usar un **comando debug**.

En este ejemplo, el certificado no fue ocultado en la base de datos, se ha encontrado CA correspondiente, el uso dominante correcto fue utilizado (ClientAuthentication), y el certificado se ha validado con éxito:

```
debug aaa authentication
debug aaa authorization
debug webvpn  255
debug webvpn anyconnect 255
debug crypto ca 255
```

Los comandos debug detallados, tales como el **comando debug webvpn 255**, pueden generar muchos abren una sesión un entorno de producción y ponen una carga pesada en un ASA. Algunos debugs del WebVPN se han quitado para mayor clareza:

```
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
```

Ésta es la tentativa de encontrar a un grupo de túnel que corresponde con. No hay reglas de la asignación del certificado del específico, y utilizan al grupo de túnel que usted proporciona:

```
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)
```

Éstos son SSL y los debugs de la sesión general:

```
%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 la Autenticación doble y la validación de certificado

Éste es un ejemplo de la Autenticación doble, donde está LOCAL el servidor de la autenticación primaria, y el servidor de la autenticación secundaria es LDAP. La validación de certificado todavía se habilita.

Este ejemplo muestra la Configuración LDAP:

```
%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.
```

Aquí está la adición de un servidor de la autenticación secundaria:

```
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
```

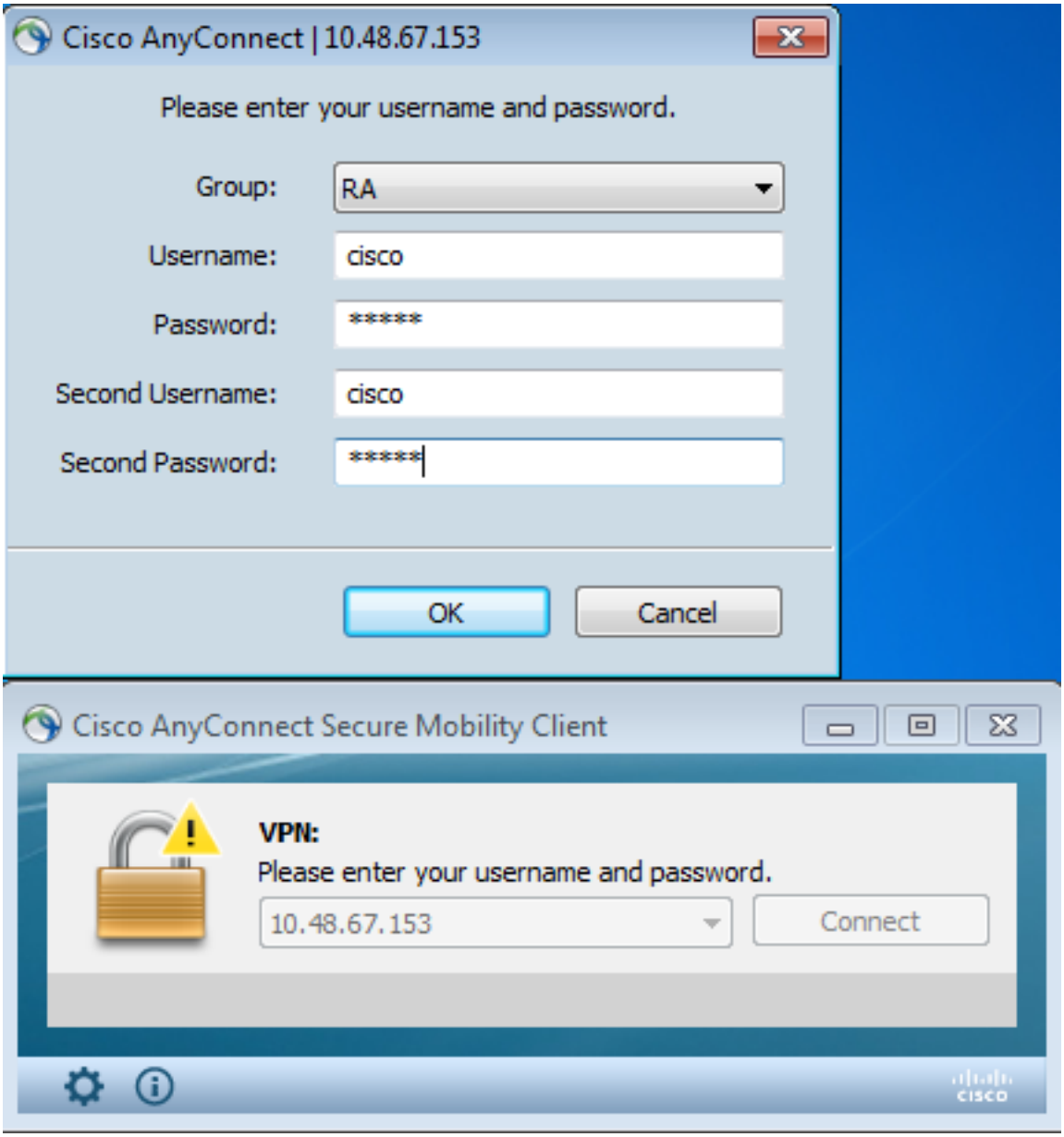
Usted no ve al “autenticación-servidor-grupo LOCAL” en la configuración porque es una configuración predeterminada.

Cualquier otro servidor de AAA puede ser utilizado para el “autenticación-servidor-grupo.” Para el “secundario-autenticación-servidor-grupo,” es posible utilizar a todos los servidores de AAA a excepción de un servidor del Security Dynamics International (SDI); en ese caso, el SDI podía todavía ser el servidor de la autenticación primaria.

Prueba

> Nota: La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

Para probar esta configuración, proporcione las credenciales locales (nombre de usuario cisco con la palabra clave Cisco) y las credenciales LDAP (nombre de usuario cisco con la contraseña del LDAP). El certificado debe estar presente:



Ingrese el comando del **anyconnect del detalle de VPN-sessiondb de la demostración** en el ASA.

Los resultados son similares a ésos para la sola autenticación. Refiera a la [“configuración ASA para la sola autenticación y la validación de certificado, prueba](#).”

Depurar

Los debugs para la sesión WebVPN y la autenticación son similares. Refiera a la “[configuración ASA para la solas autenticación y validación de certificado, debug](#).” Un proceso de autenticación adicional aparece:

```
%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 el LDAP muestran los detalles que pudieron variar con la Configuración LDAP:

```
%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
```

Configuración ASA para la Autenticación doble y el Pre-Fill

Es posible asociar ciertos campos del certificado al nombre de usuario que se utiliza para primario y la autenticación secundaria:

```
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 está utilizando el certificado: **cn=test1,ou=Security**, o=Cisco, l=Krakow, st=PL, c=PL.

Para la autenticación primaria, el nombre de usuario se toma del CN, que es porqué crearon al usuario local 'test1.

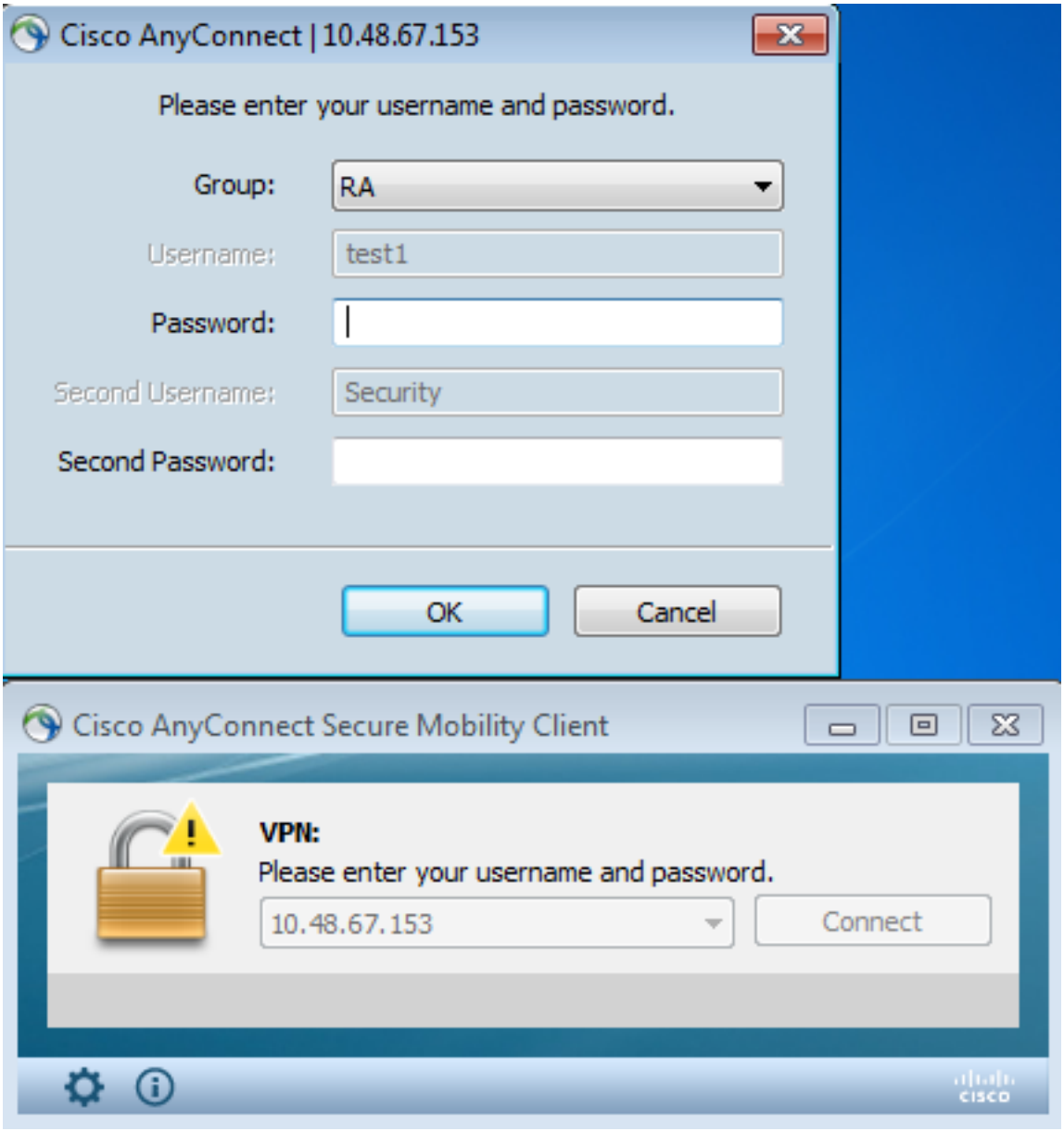
Para la autenticación secundaria, el nombre de usuario se toma de la unidad organizativa (el OU, que es porqué crearon al usuario “Seguridad” en el servidor LDAP.

Es también posible forzar AnyConnect para utilizar los comandos del pre-fill para prellenar el nombre de usuario primario y secundario.

En un escenario del mundo real, el servidor de la autenticación primaria es generalmente un AD o servidor LDAP, mientras que el servidor de la autenticación secundaria es el servidor del Rivest, del Shamir, y del Adelman (RSA) que utiliza las contraseñas simbólicas. En este escenario, el usuario debe proporcionar las credenciales AD/LDAP (que el usuario conoce), una contraseña simbólica RSA (que el usuario tenga) y un certificado (en la máquina se utiliza que).

Prueba

Observe que usted no puede cambiar el nombre de usuario primario o secundario porque se prellena del certificado CN y de los campos OU:



Depurar

Este ejemplo muestra la petición del pre-fill enviada a AnyConnect:

```
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
```

Aquí usted ve que la autenticación está utilizando los nombres de usuario correctos:

```
%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 la Autenticación doble y la asignación del certificado

Es también posible asociar los certificados del cliente específicos a los grupos de túnel específicos, tal y como se muestra en de este ejemplo:

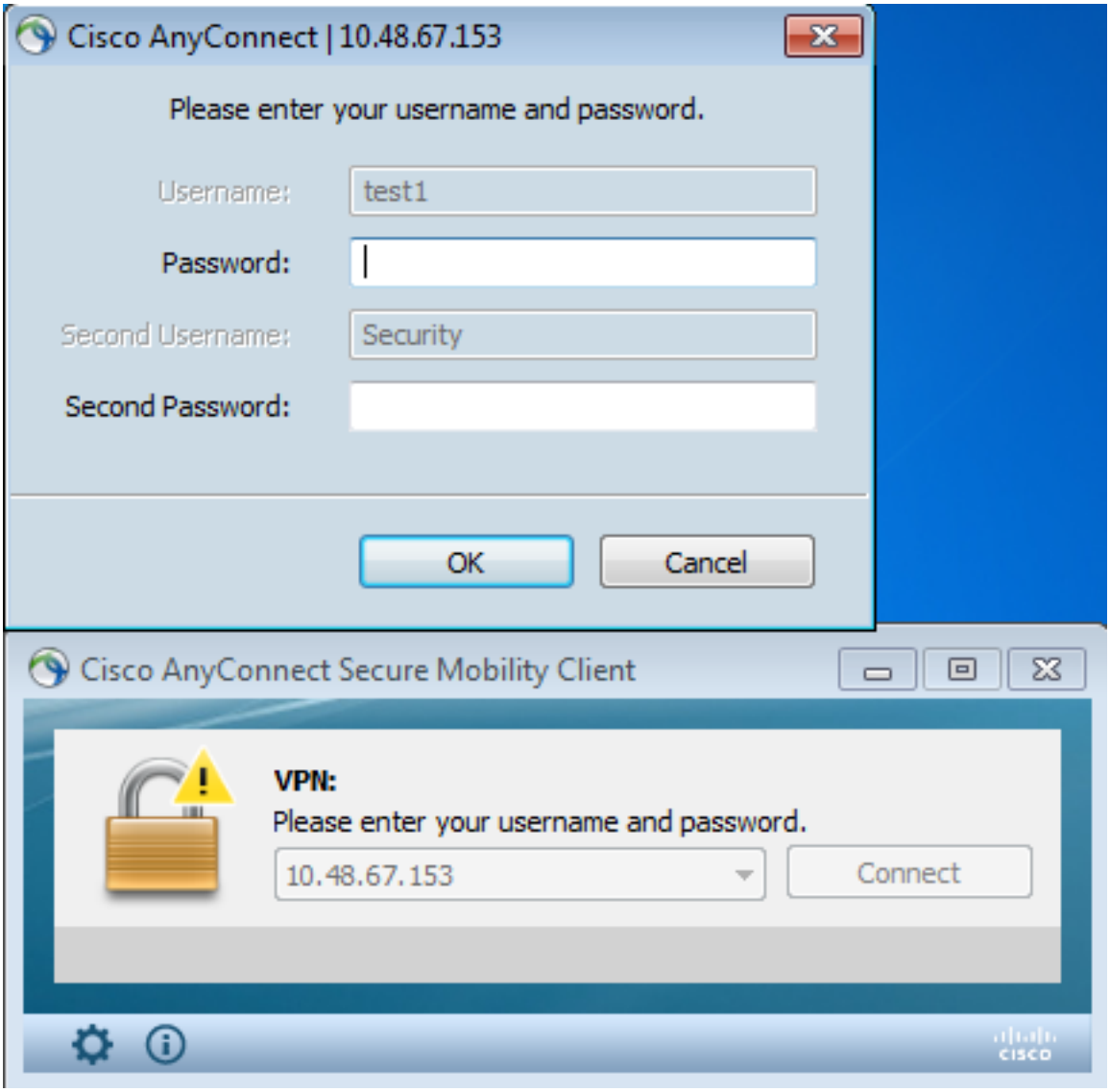
```
%ASA-6-113012: AAA user authentication Successful : local database : user = test1
%ASA-6-302013: Built outbound TCP connection 2137 for outside:10.147.24.60/389
(10.147.24.60/389) to identity:10.48.67.153/46606 (10.48.67.153/46606)
%ASA-6-113004: AAA user authentication Successful : server =  10.147.24.60 :
user = Security
```

Esta manera, todos los Certificados de usuario firmados por el Centro de Asistencia Técnica de Cisco (TAC) CA se asocia a un grupo de túnel nombrado el “RA.”

> Nota: La asignación del certificado para el SSL se configura diferentemente que la asignación del certificado para el IPSec. Para el IPSec, se configura usando las reglas del “túnel-grupo-mapa” en el modo de configuración global. Para el SSL, se configura usando el “certificado-grupo-mapa” bajo modo de configuración del webvpn.

Prueba

Observe que, una vez que se habilita la asignación del certificado, usted no necesita elegir al grupo de túnel más:



Depurar

En este ejemplo, la regla de la asignación del certificado permite que encuentren al grupo de túnel:

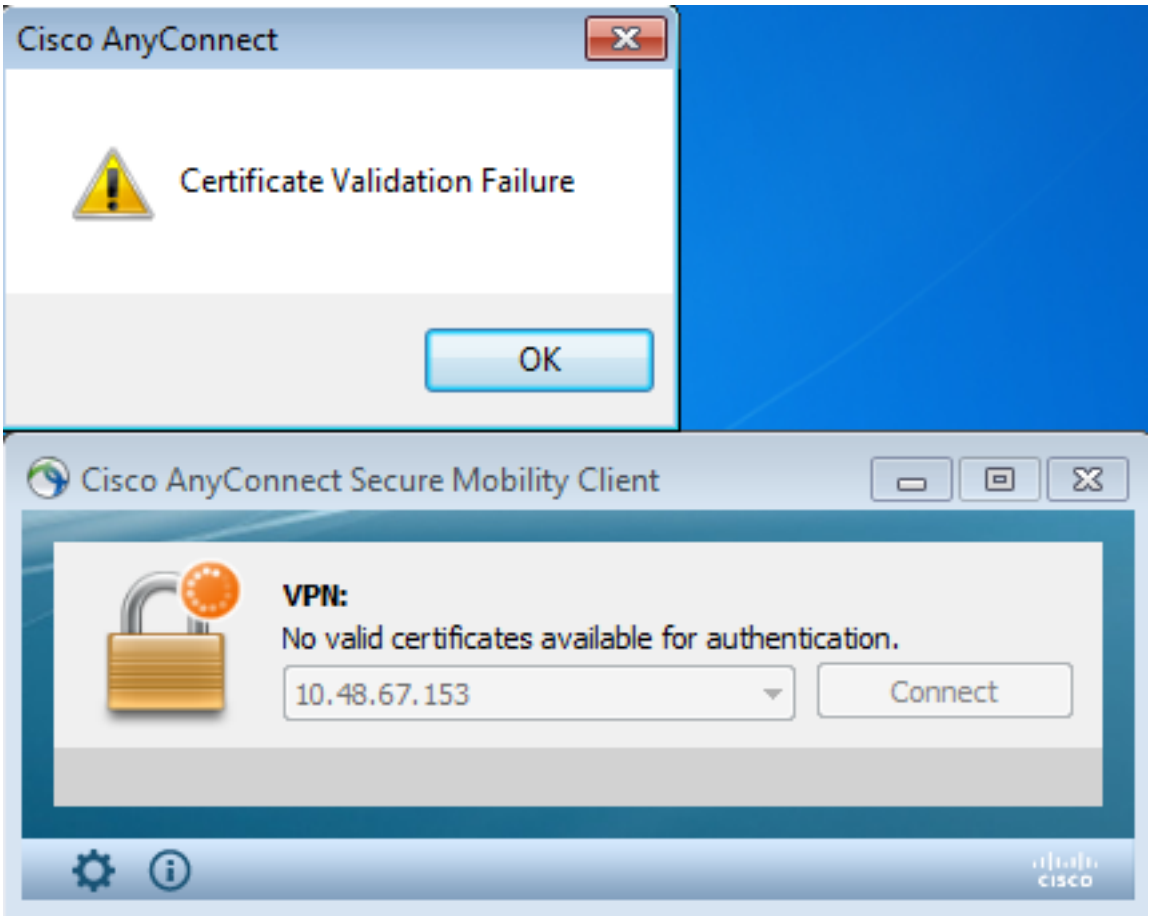
```
%ASA-7-717036: Looking for a tunnel group match based on certificate maps for
peer certificate with serial number: 00FE9C3D61E131CDB1, subject name: cn=test1,
ou=Security,o=Cisco,l=Krakow,st=PL,c=PL, issuer_name: cn=TAC,ou=RAC,o=TAC,
l=Warsaw,st=Maz,c=PL.
%ASA-7-717038: Tunnel group match found. 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.
```

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

Certificado válido no presente

Después de que usted quite un certificado válido de Windows7, AnyConnect no puede encontrar ninguna certificados válidos:



En el ASA, parece la sesión es terminado por el cliente (restauración-Yo):

```
%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

- Configurar el túnel Grouips, las directivas del grupo, y a los usuarios: Configuración de la Autenticación Doble
- Configurar a un servidor externo para la autorización de usuario del dispositivo de seguridad
- Soporte Técnico y Documentación - Cisco Systems