Autenticação dupla ASA AnyConnect com validação certificada, mapeamento, e manual de configuração do Pre-Fill

Índice

Introdução

Este documento descreve um exemplo de configuração para o acesso de Cliente de mobilidade Cisco AnyConnect Secure adaptável da ferramenta de segurança (ASA) que usa a Autenticação dupla com validação certificada. Como um usuário de AnyConnect, você deve fornecer o certificado e as credenciais corretos para o preliminar e a autenticação secundária a fim obter o acesso VPN. Este documento igualmente fornece um exemplo do mapeamento do certificado a característica do pre-fill.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico da configuração do comando line interface(cli) ASA e da configuração de VPN do Secure Socket Layer (SSL)
- Conhecimento básico dos Certificados X509

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Software adaptável da ferramenta de segurança de Cisco (ASA), versão 8.4 e mais recente
- Windows 7 com Cliente de mobilidade Cisco AnyConnect Secure 3.1

Supõe-se que você usou um Certificate Authority (CA) externo a fim gerar:

- Um certificado do padrão #12 da criptografia de chave pública (PKCS-12) base64-encoded para ASA (anyconnect.pfx)
- Um certificado do PKCS-12 para AnyConnect

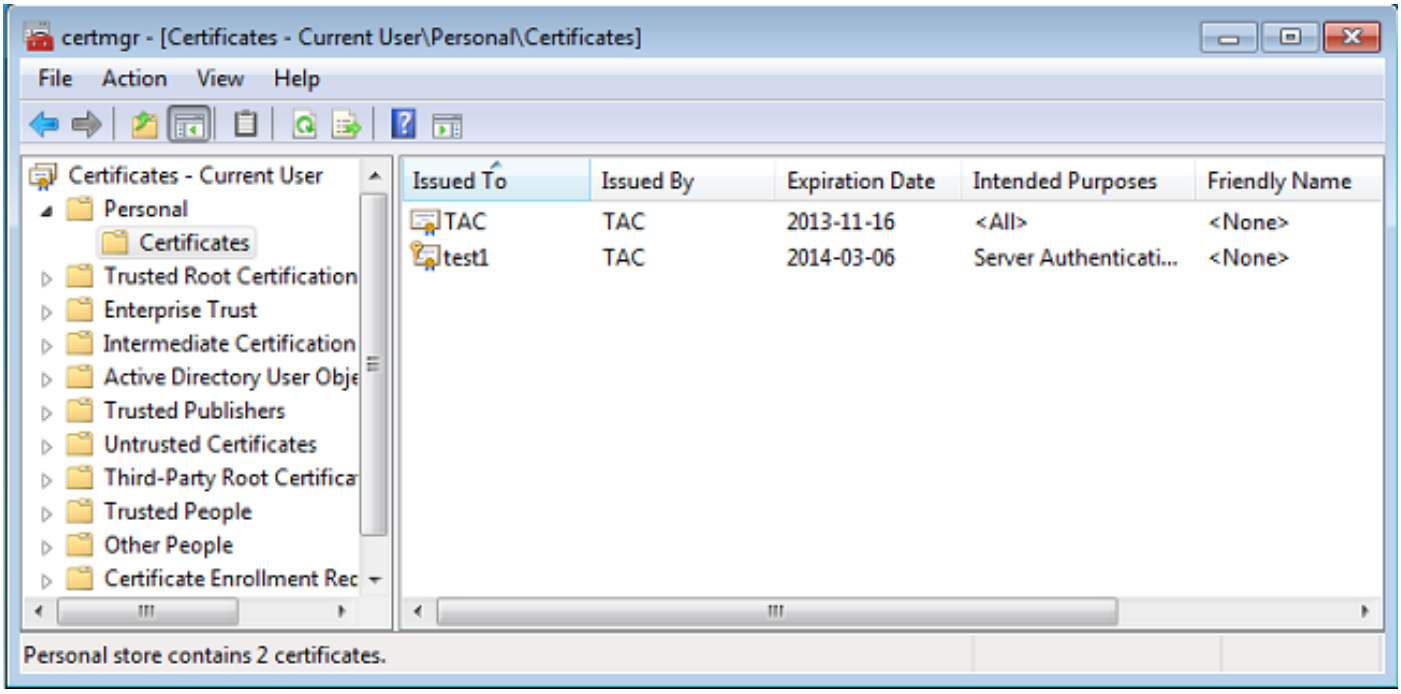
Configurar

> Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Certificado para AnyConnect

A fim instalar um certificado do exemplo, fazer duplo clique o arquivo anyconnect.pfx, e instale esse certificado como um certificado pessoal.

Use o gerenciador certificado (certmgr.msc) a fim verificar a instalação:



Àrevelia, tentativas de AnyConnect para encontrar um certificado na loja do usuário de Microsoft; não há nenhuma necessidade de fazer nenhumas mudanças no perfil de AnyConnect.

Instalação certificada no ASA

Este exemplo mostra como o ASA pode importar um certificado do PKCS-12 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
```

Use o **comando show crypto ca certificates** a fim verificar a importação:

```
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: Os determinados comandos de exibição dos apoios da ferramenta Output Interpreter (clientes registrados somente). Use a ferramenta Output Interpreter a fim ver uma

análise do emissor de comando de execução.

Configuração ASA para a únicas autenticação e validação certificada

O ASA usa a autenticação e o certificado de autenticação do Authentication, Authorization, and Accounting (AAA). A validação certificada é imperativa. A autenticação de AAA usa um base de dados local.

Este exemplo mostra a única autenticação com validação certificada.

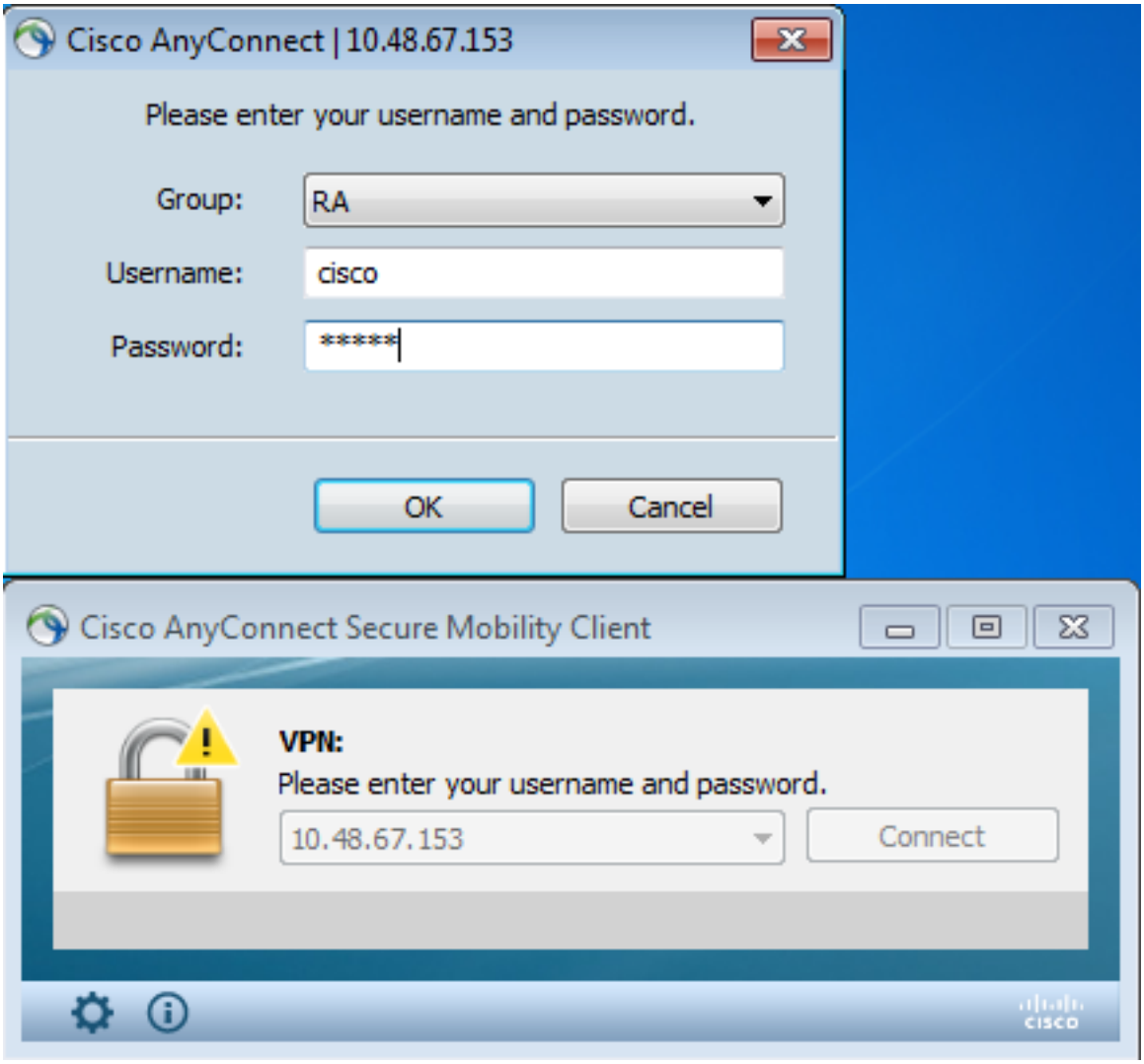
```
ip local pool POOL 10.1.1.10-10.1.1.20
username cisco password cisco

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
```

Além do que esta configuração, é possível executar a autorização do Lightweight Directory Access Protocol (LDAP) com o username de um campo específico do certificado, tal como o nome do certificado (CN). Os atributos adicionais podem então ser recuperados e aplicado à sessão de VPN. Para obter mais informações sobre da autenticação e da autorização do certificado, refira "ASA Anyconnect VPN e autorização de OpenLDAP com exemplo de configuração feito sob encomenda do esquema e dos Certificados."

Teste

> Nota: A ferramenta Output Interpreter (clientes registrados somente) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

A fim testar esta configuração, forneça as credenciais locais (username Cisco com senha Cisco). A obrigação do certificado esta presente:



Incorpore o comando do **anyconnect do detalhe da mostra VPN-sessiondb no** 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 :
```

Debug

> Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

Neste exemplo, o certificado não foi posto em esconderijo no base de dados, CA correspondente foi encontrado, o uso chave correto foi usado (ClientAuthentication), e o certificado foi validado com sucesso:

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

Os comandos debug detalhados, tais como o **comando debug webvpn 255**, podem gerar muitos entram um ambiente de produção e colocam uma carga pesada em um ASA. Algum WebVPN debuga foi removido para maior 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
```

Esta é a tentativa de encontrar um grupo de túneis de harmonização. Não há nenhuma regra do mapeamento do certificado do específico, e o grupo de túneis que você fornece é usado:

```
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)
```

Estes são o SSL e a sessão geral debuga:

```
%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.
```

Configuração ASA para a Autenticação dupla e a validação certificada

Este é um exemplo da Autenticação dupla, onde o server da autenticação principal é LOCAL, e o server da autenticação secundária é LDAP. A validação certificada é permitida ainda.

Este exemplo mostra a configuração 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.
```

Está aqui a adição de um server da autenticação secundária:

```
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
```

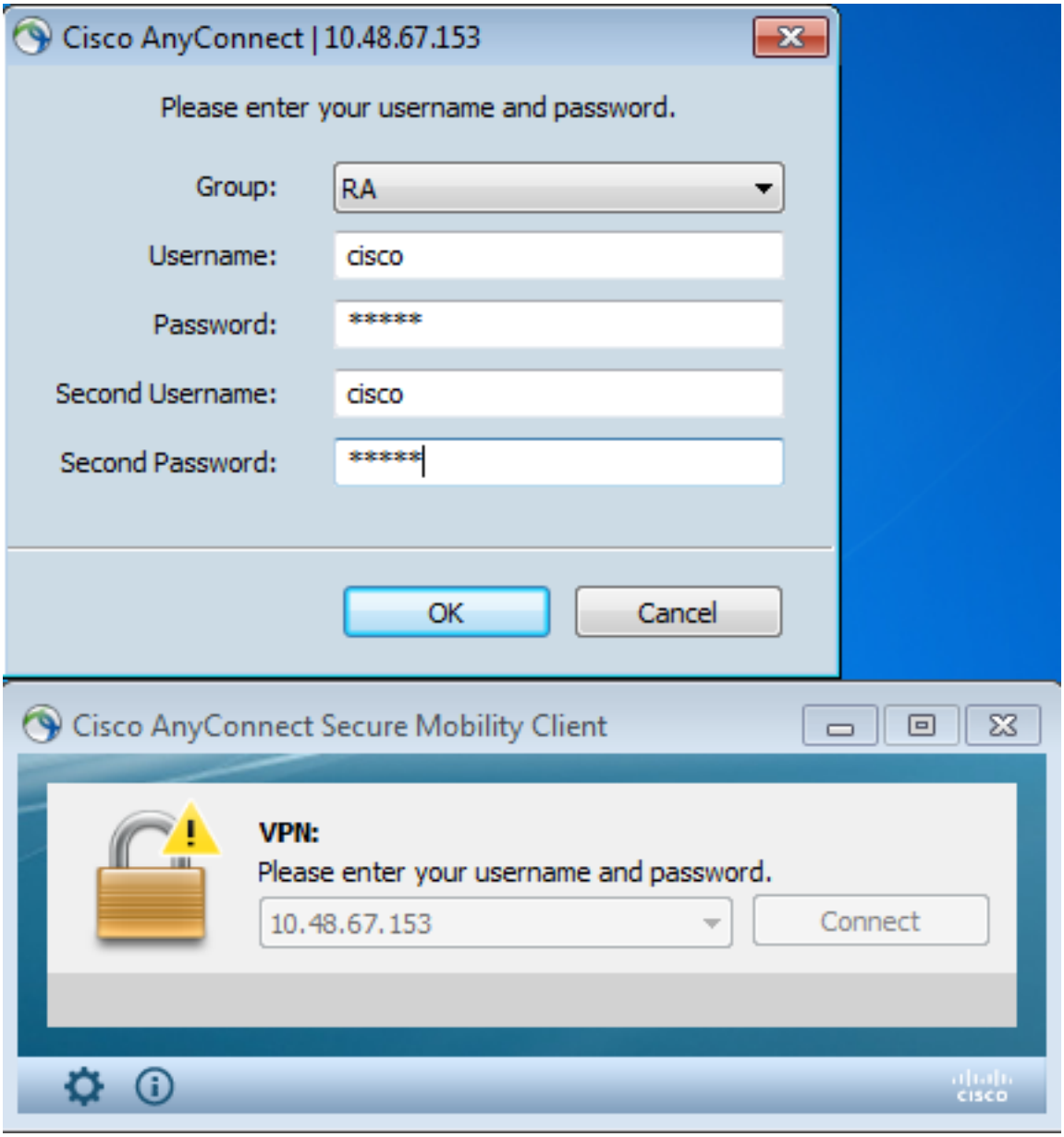
Você não vê o “autenticação-server-grupo LOCAL” na configuração porque é uma configuração padrão.

Todo o outro servidor AAA pode ser usado para o “autenticação-server-grupo.” Para o “secundário-autenticação-server-grupo,” é possível usar todos os servidores AAA à exceção de um server do Security Dynamics International (SDI); nesse caso, o SDI podia ainda ser o server da autenticação principal.

Teste

> Nota: A ferramenta Output Interpreter (clientes registrados somente) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

A fim testar esta configuração, forneça as credenciais locais (username Cisco com senha Cisco) e as credenciais LDAP (username Cisco com senha do LDAP). A obrigação do certificado esta presente:



Incorpore o comando do **anyconnect do detalhe da mostra VPN-sessiondb no** ASA.

Os resultados são similares àqueles para a única autenticação. Refira [“a configuração ASA para a única autenticação e a validação certificada, testa](#).”

Debug

Debuga para a sessão de VPN da Web e a autenticação é similar. Refira “a [configuração ASA para a única autenticação e a validação certificada, debuga](#).” Um processo de autenticação 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
```

Debuga para os detalhes da mostra LDAP que puderam variar com a configuração 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
```

Configuração ASA para a Autenticação dupla e o Pre-Fill

Épossível traçar determinados campos do certificado ao username que é usado para preliminar e a autenticação secundária:

```
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
```

Neste exemplo, o cliente está usando o certificado: **cn=test1,ou=Security**, o=Cisco, l=Krakow, st=PL, c=PL.

Para a autenticação principal, o username é tomado do CN, que é porque o usuário local 'test1 foi criado.

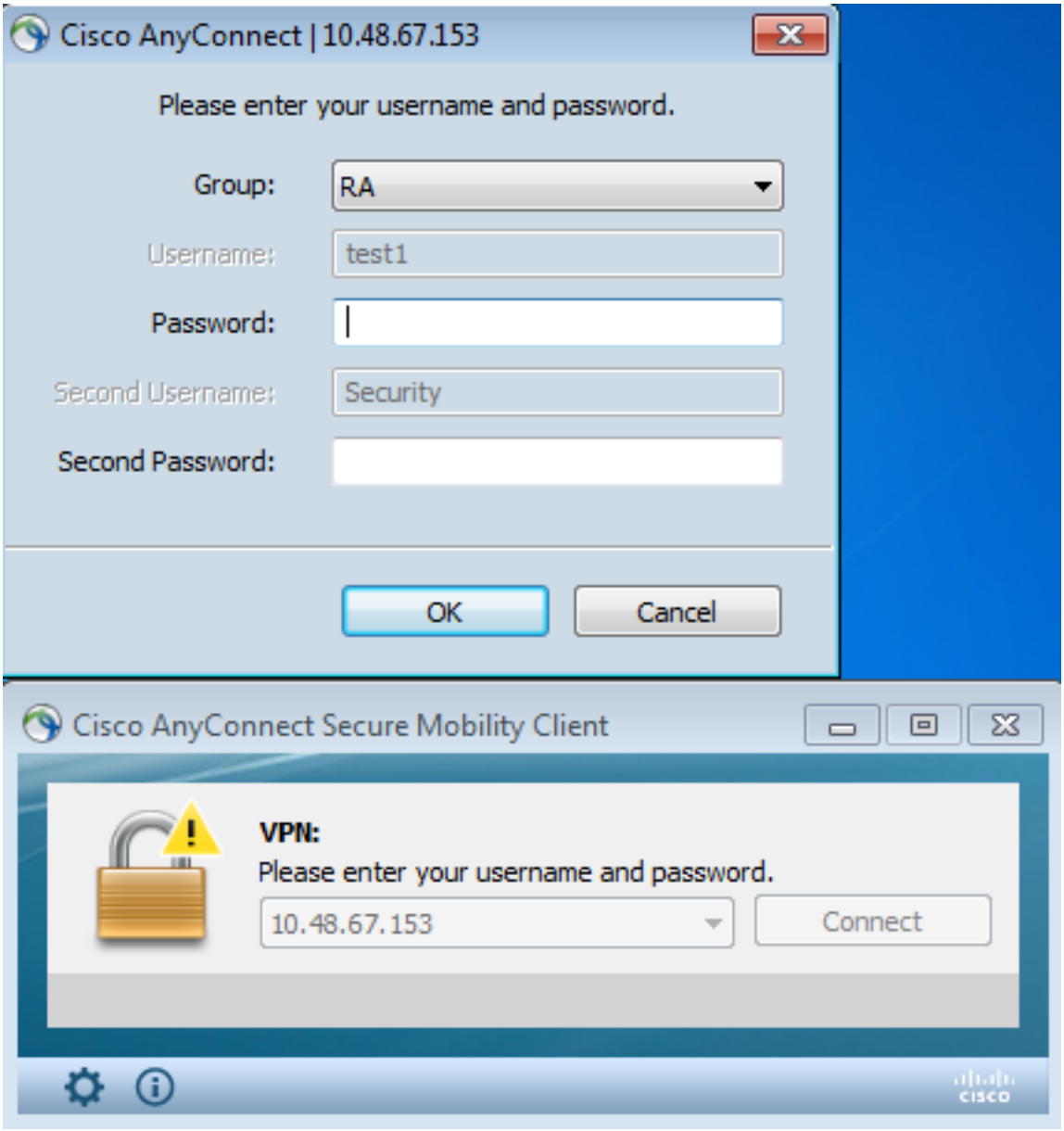
Para a autenticação secundária, o username é tomado da unidade organizacional (o OU, que é porque o usuário “Segurança” foi criado no servidor ldap.

Éigualmente possível forçar AnyConnect para usar comandos do pre-fill a fim preencher o username preliminar e secundário.

Em uma encenação do mundo real, o server da autenticação principal é geralmente um AD ou um servidor ldap, quando o server da autenticação secundária for o server de Rivest, de Shamir, e de Adelman (RSA) que usa as senhas simbólicas. Nesta encenação, o usuário deve fornecer as credenciais AD/LDAP (que o usuário conhece), uma senha simbólica RSA (que o usuário tem) e um certificado (na máquina que é usada).

Teste

Observe que você não pode mudar o username preliminar ou secundário porque é preenchido dos campos do CN e OU do certificado:



Debug

Este exemplo mostra o pedido do pre-fill enviado 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
```

Aqui você vê que a autenticação está usando os nomes de usuário corretos:

```
%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
```

Configuração ASA para a Autenticação dupla e o mapeamento do certificado

Éigualmente possível traçar certificados de cliente específicos aos grupos de túneis específicos, segundo as indicações deste exemplo:

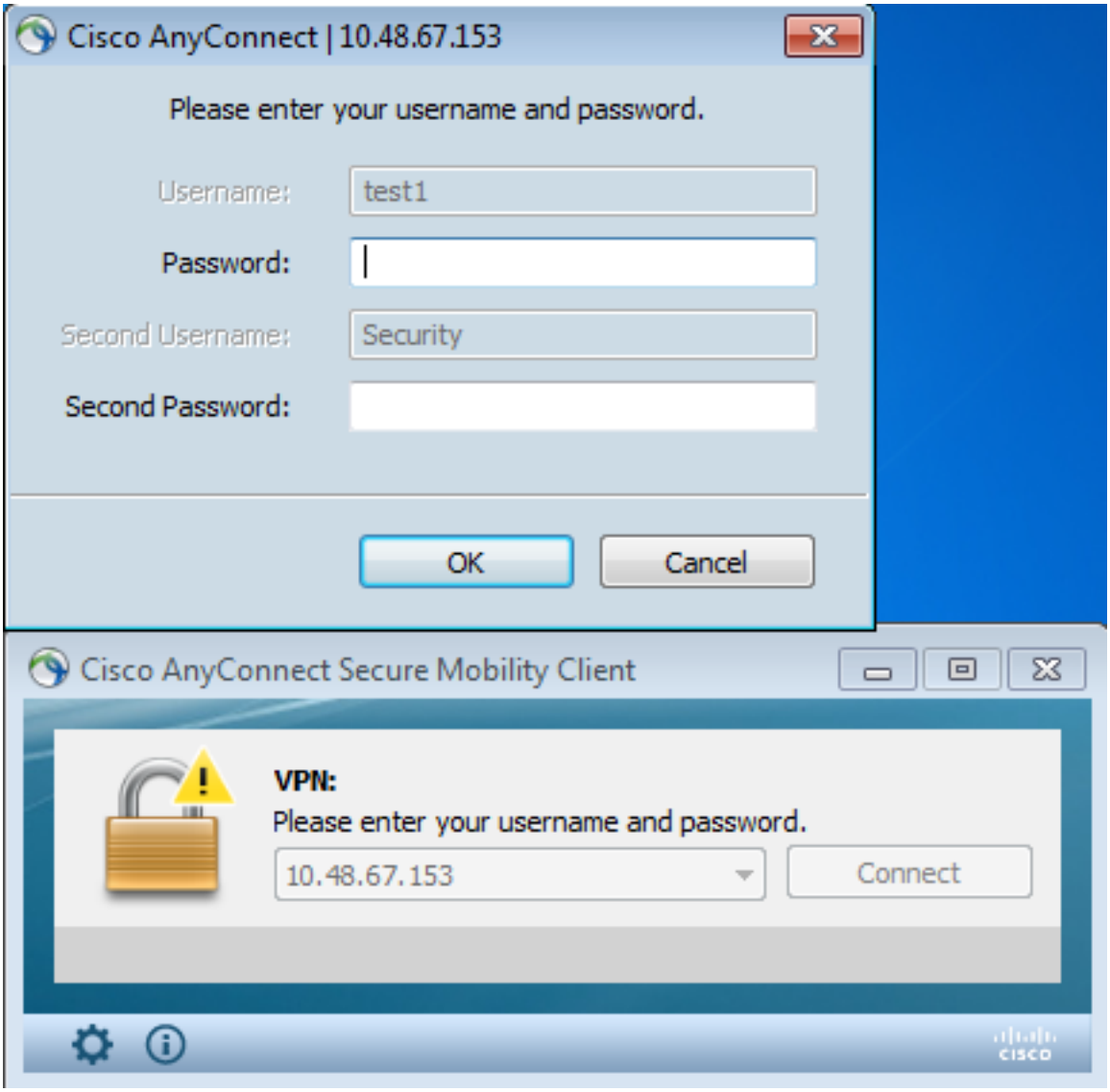
```
%ASA-6-113012: AAA user authentication Successful : local database : user = test1
%ASA-6-302013: Built outbound TCP connection 2137 for outside:10.147.24.60/389
(10.147.24.60/389) to identity:10.48.67.153/46606 (10.48.67.153/46606)
%ASA-6-113004: AAA user authentication Successful : server =  10.147.24.60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

Esta maneira, todos os certificados de usuário assinados pelo centro de assistência técnica da Cisco (TAC) CA é traçada a um grupo de túneis nomeado o “RA.”

> Nota: O mapeamento do certificado para o SSL é configurado diferentemente do que o mapeamento do certificado para o IPsec. Para o IPsec, é configurado usando regras do “túnel-grupo-mapa” no modo de config global. Para o SSL, é configurado usando o “certificado-grupo-mapa” sob o modo de configuração do webvpn.

Teste

Observe que, uma vez que o mapeamento do certificado é permitido, você não precisa de escolher anymore o grupo de túneis:



Debug

Neste exemplo, a regra do mapeamento do certificado permite que o grupo de túneis seja encontrado:

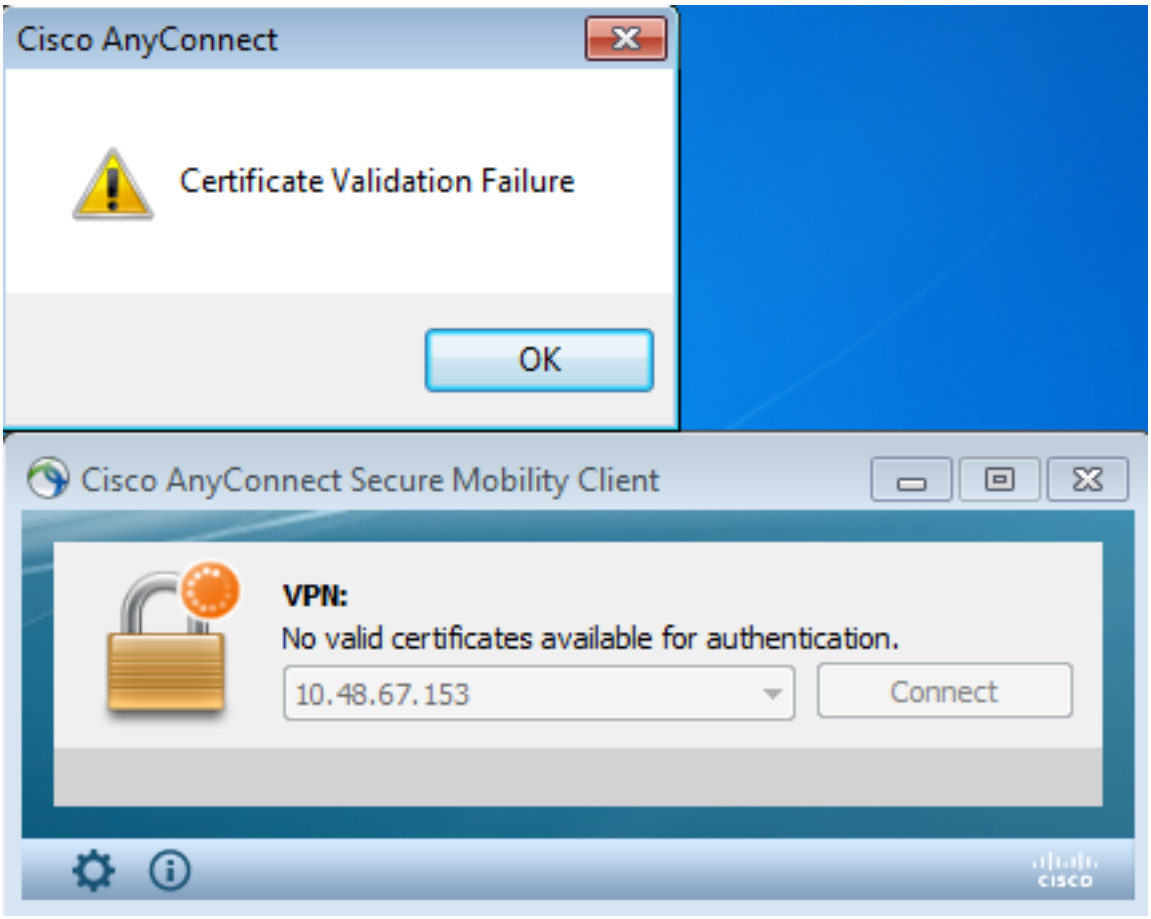
```
%ASA-7-717036: Looking for a tunnel group match based on certificate maps for
peer certificate with serial number: 00FE9C3D61E131CDB1, subject name: cn=test1,
ou=Security,o=Cisco,l=Krakow,st=PL,c=PL, issuer_name: cn=TAC,ou=RAC,o=TAC,
l=Warsaw,st=Maz,c=PL.
%ASA-7-717038: Tunnel group match found. 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 seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

Certificado válido não atual

Depois que você remove um certificado válido de Windows7, AnyConnect não pode encontrar nenhuns certificados válidos:



No ASA, olha como a sessão é terminado pelo cliente (restauração-Eu):

```
%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
```

Informações Relacionadas

- Configurando o túnel Grouips, as políticas do grupo, e os usuários: Configurando a Autenticação dupla
- Configurando um servidor interno para a autorização de usuário da ferramenta de segurança
- Suporte Técnico e Documentação - Cisco Systems