Configurar a autenticação do ASA AnyConnect Secure Mobility Client

Contents

Introduction

Este documento descreve uma configuração para acesso do ASA AnyConnect Secure Mobility Client que usa autenticação dupla com validação de certificado.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento básico da configuração da interface de linha de comando (CLI) do ASA e da configuração da VPN Secure Socket Layer (SSL)
- Conhecimento básico dos certificados X509

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

- Software Cisco Adaptive Security Appliance (ASA), versão 8.4 e posterior

- Windows 7 com Cisco AnyConnect Secure Mobility Client 3.1

Presume-se que você usou uma Autoridade de Certificação (CA) externa para gerar:

- Um certificado codificado na base64 de #12 padrão de criptografia de chave pública (PKCS #12) para ASA (AnyConnect.pfx)
- Um certificado PKCS #12 para AnyConnect

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este documento descreve um exemplo de configuração para o acesso do Cisco AnyConnect Secure Mobility Client do Adaptive Security Appliance (ASA) que usa autenticação dupla com validação de certificado. Como usuário do AnyConnect, você deve fornecer o certificado e as credenciais corretos para a autenticação primária e secundária para obter acesso à VPN. Este documento também fornece um exemplo de mapeamento de certificado com o recurso de pré-preenchimento.

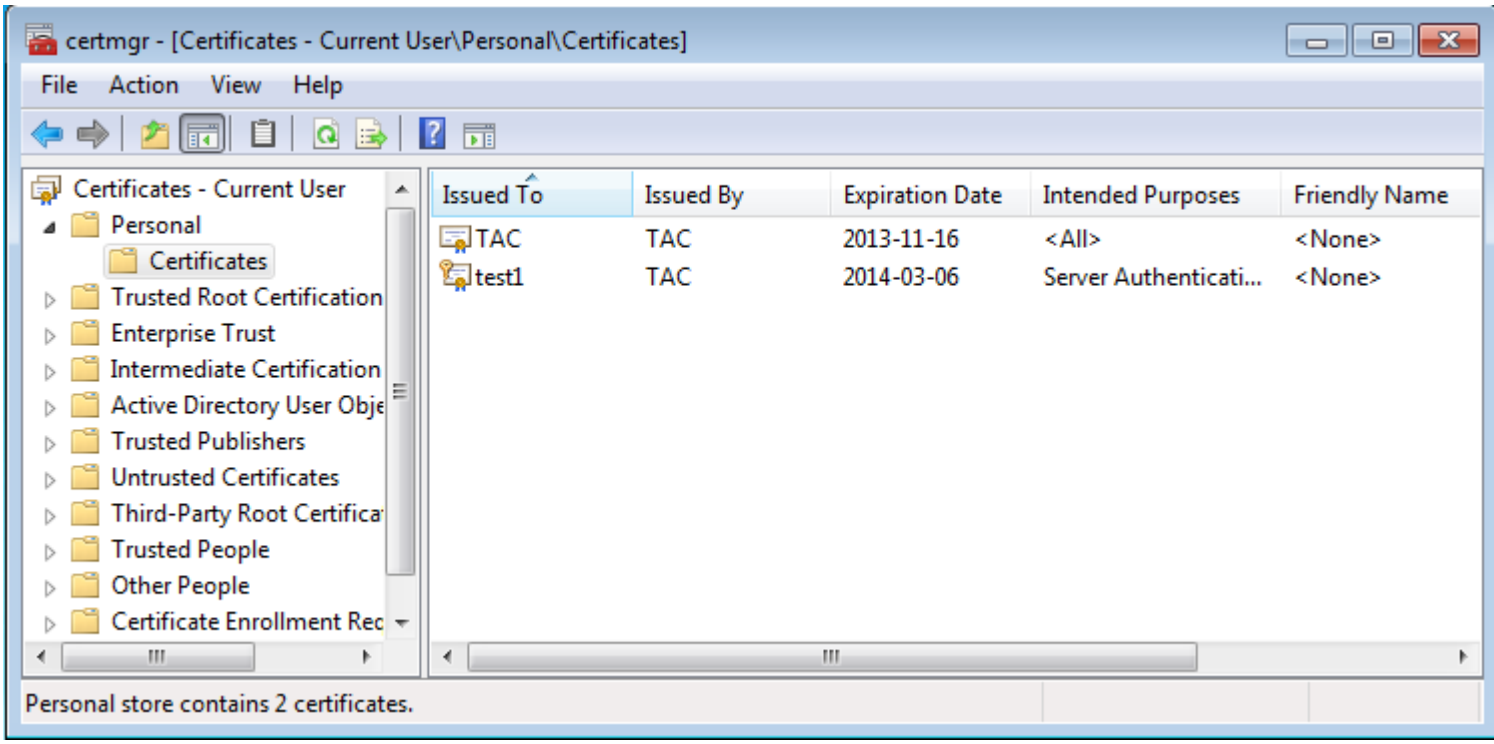
Configurar

> **Observação**: use a Command Lookup Tool para obter mais informações sobre os comandos usados nesta seção. Somente usuários registrados da Cisco podem acessar ferramentas e informações internas da Cisco.

Certificado para AnyConnect

Para instalar um certificado de exemplo, clique duas vezes no arquivo AnyConnect.pfx e instale esse certificado como um certificado pessoal.

Use o Gerenciador de Certificados (certmgr.msc) para verificar a instalação:



Por padrão, o AnyConnect tenta encontrar um certificado no armazenamento de usuários da Microsoft; não há necessidade de fazer alterações no perfil do AnyConnect.

Instalação de certificado no ASA

Este exemplo mostra como o ASA pode importar um certificado de #12 PKCS 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
```

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

```
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
```

> **Observação**: a Output Interpreter Tool oferece suporte a determinados comandos show. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show.. Somente usuários registrados da Cisco podem acessar ferramentas e informações internas da Cisco.

Configuração do ASA para autenticação única e validação de certificado

O ASA usa autenticação AAA (authentication, authorization, and accounting) e autenticação de certificado. A validação do certificado é obrigatória. A autenticação AAA usa um banco de dados local.

Este exemplo mostra a autenticação única com validação de certificado.

<#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

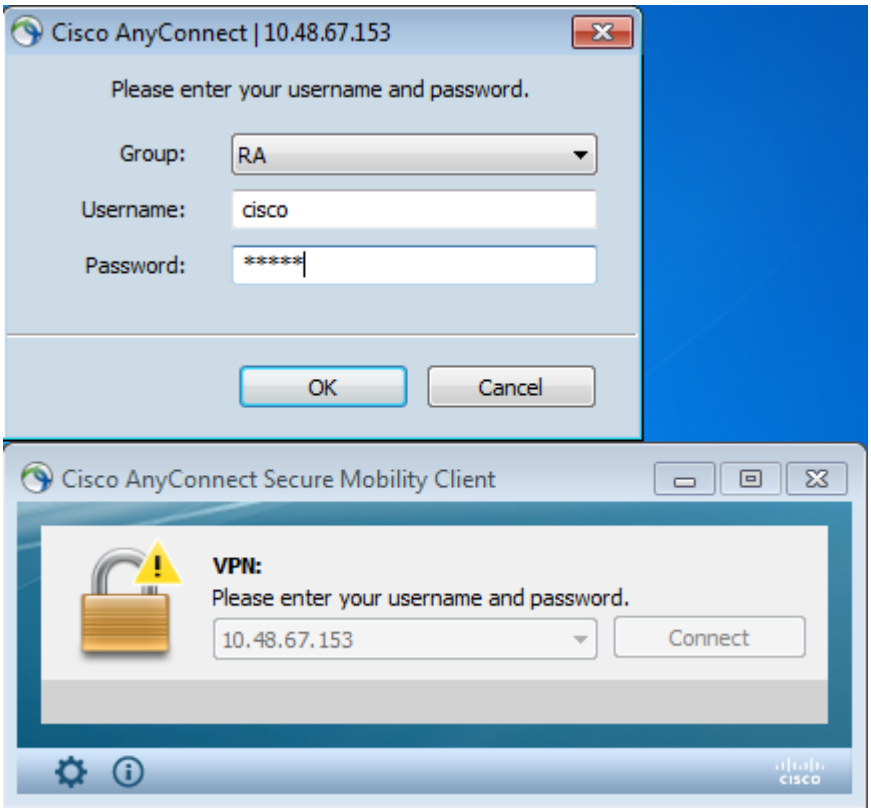
```
 group-alias RA enable
```

Além dessa configuração, é possível executar a autorização do Lightweight Diretory Access Protocol (LDAP) com o nome de usuário de um campo de certificado específico, como o nome do certificado (CN). Atributos adicionais podem ser recuperados e aplicados à sessão VPN. Para obter mais informações sobre autenticação e autorização de certificado, consulte "Exemplo de Configuração de ASA AnyConnect VPN e Autorização do OpenLDAP com Esquema Personalizado e Certificados".

Teste

> **Observação**: a Output Interpreter Tool oferece suporte a determinados comandos show. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show.. Somente usuários registrados da Cisco podem acessar ferramentas e informações internas da Cisco.

Para testar essa configuração, forneça as credenciais locais (nome de usuário cisco com senha cisco). O certificado deve estar presente:



Insira o comando **show vpn-sessiondb detail AnyConnect** no 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 :
```

Debug

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

Neste exemplo, o certificado não foi armazenado em cache no banco de dados, uma CA correspondente foi encontrada, o uso de chave correto foi usado (ClientAuthentication) e o certificado foi validado com êxito:

<#root>

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

debug webvpn AnyConnect 255

```
debug crypto ca 255
```

Comandos de depuração detalhados, como o comando **debug webvpn 255**, podem gerar muitos logs em um ambiente de produção e colocar uma carga pesada em um ASA. Algumas depurações do WebVPN foram removidas para esclarecer:

<#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

Esta é a tentativa de encontrar um grupo de túneis correspondente. Não há regras específicas de mapeamento de certificados e o grupo de túneis fornecido é usado:

<#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)

Estas são as depurações de sessão geral e SSL:

<#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.
```

Configuração do ASA para autenticação dupla e validação de certificado

Este é um exemplo de autenticação dupla, em que o servidor de autenticação principal é LOCAL e o servidor de autenticação secundário é LDAP. A validação de certificado ainda está habilitada.

Este exemplo mostra a configuração 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
```

Aqui está a adição de um servidor de autenticação secundário:

<#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

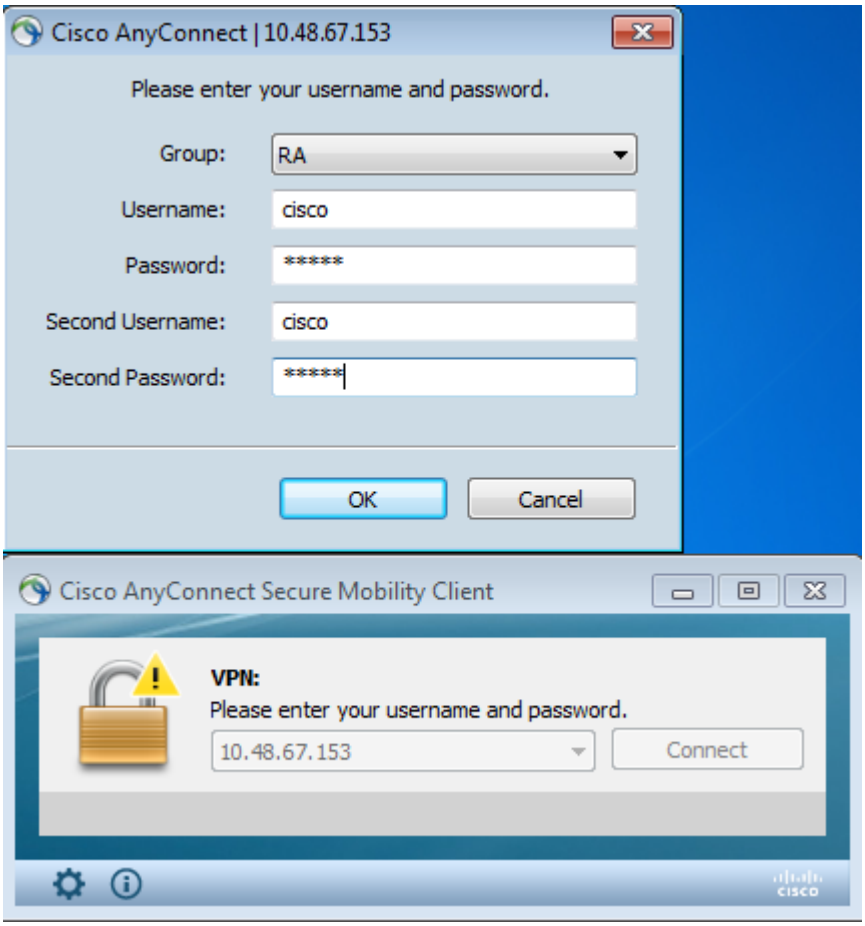
Você não vê 'authentication-server-group LOCAL' na configuração porque ela é uma configuração padrão.

Qualquer outro servidor AAA pode ser usado para 'authentication-server-group'. Para 'secondary-authentication-server-group,' é possível usar todos os servidores AAA exceto um servidor Security Dynamics International (SDI); nesse caso, o SDI ainda poderia ser o servidor de autenticação primário.

Teste

> **Observação**: a Output Interpreter Tool oferece suporte a determinados comandos show. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show.. Somente usuários registrados da Cisco podem acessar ferramentas e informações internas da Cisco.

Para testar essa configuração, forneça as credenciais locais (nome de usuário cisco com senha cisco) e as credenciais LDAP (nome de usuário cisco com senha LDAP). O certificado deve estar presente:



Insira o comando **show vpn-sessiondb detail AnyConnect** no ASA.

Os resultados são semelhantes aos da autenticação única. Consulte "Configuração do ASA para Autenticação Única e Validação de Certificado, Teste".

Debug

As depurações para a sessão WebVPN e a autenticação são semelhantes. Consulte "Configuração do ASA para Autenticação Única e Validação de Certificado, Depuração". Um processo de autenticação adicional é exibido:

```
<#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
```

As depurações para LDAP mostram detalhes que podem variar com a configuração 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
```

Configuração do ASA para autenticação dupla e pré-preenchimento

É possível mapear certos campos de certificado para o nome de usuário usado para a autenticação primária e secundária:

<#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
```

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

Para a autenticação primária, o nome de usuário é obtido do CN, razão pela qual o usuário local 'test1' foi criado.

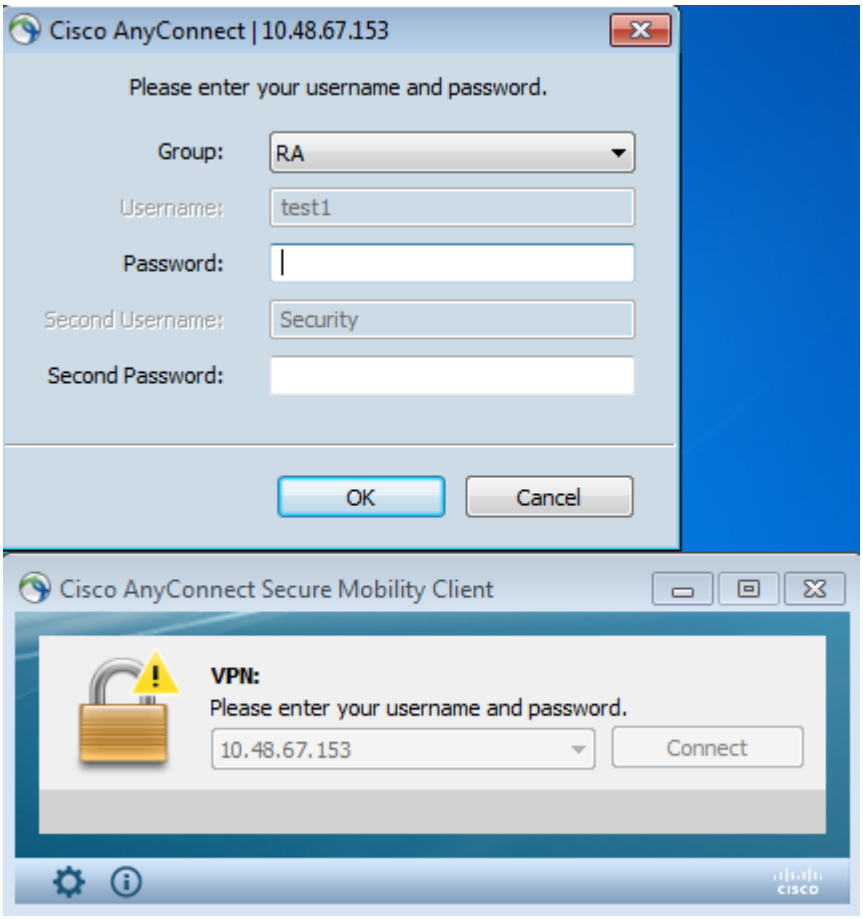
Para autenticação secundária, o nome de usuário é obtido da unidade organizacional (OU), que é o motivo pelo qual o usuário 'Security' foi criado no servidor LDAP.

Também é possível forçar o AnyConnect a usar comandos de pré-preenchimento para pré-preencher o nome de usuário primário e secundário.

Em um cenário real, o servidor de autenticação principal é geralmente um servidor AD ou LDAP, enquanto o servidor de autenticação secundário é o servidor Rivest, Shamir e Adelman (RSA) que usa senhas de token. Neste cenário, o usuário deve fornecer credenciais AD/LDAP (que o usuário conhece), uma senha de token RSA (que o usuário tem) e um certificado (na máquina que é usada).

Teste

Observe que você não pode alterar o nome de usuário principal ou secundário porque ele é pré-preenchido a partir dos campos CN e OU do certificado:



Debug

Este exemplo mostra a solicitação de pré-preenchimento enviada ao 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]
```

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

<#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
```

Configuração do ASA para autenticação dupla e mapeamento de certificado

Também é possível mapear certificados de clientes específicos para grupos de túneis específicos, como mostrado neste exemplo:

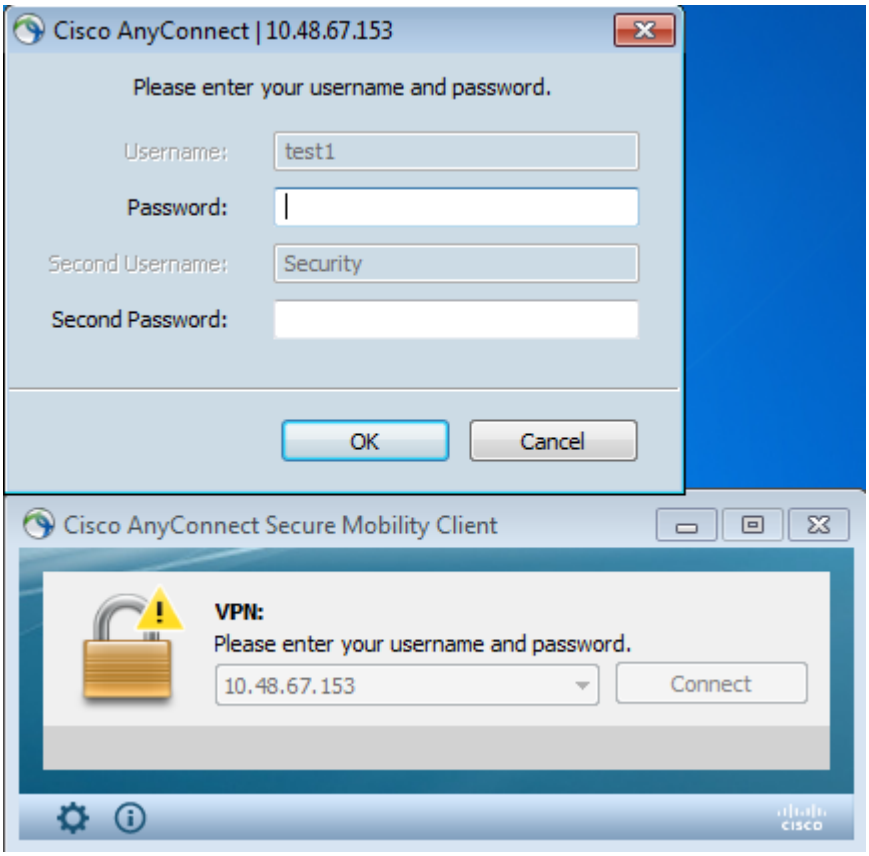
```
crypto ca certificate map CERT-MAP 10
 issuer-name co tac

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

Dessa forma, todos os certificados de usuário assinados pela CA do Cisco Technical Assistance Center (TAC) são mapeados para um grupo de túneis chamado 'RA'.

> **Observação**: o mapeamento de certificado para SSL é configurado de forma diferente do mapeamento de certificado para IPsec. Para IPsec, ele é configurado com regras 'tunnel-group-map' no modo de configuração global. Para SSL, ele é configurado com 'certificate-group-map' no modo de configuração webvpn.

Teste

Observe que, uma vez que o mapeamento do certificado esteja ativado, você não precisa mais escolher tunnel-group:



Debug

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

<#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.
```

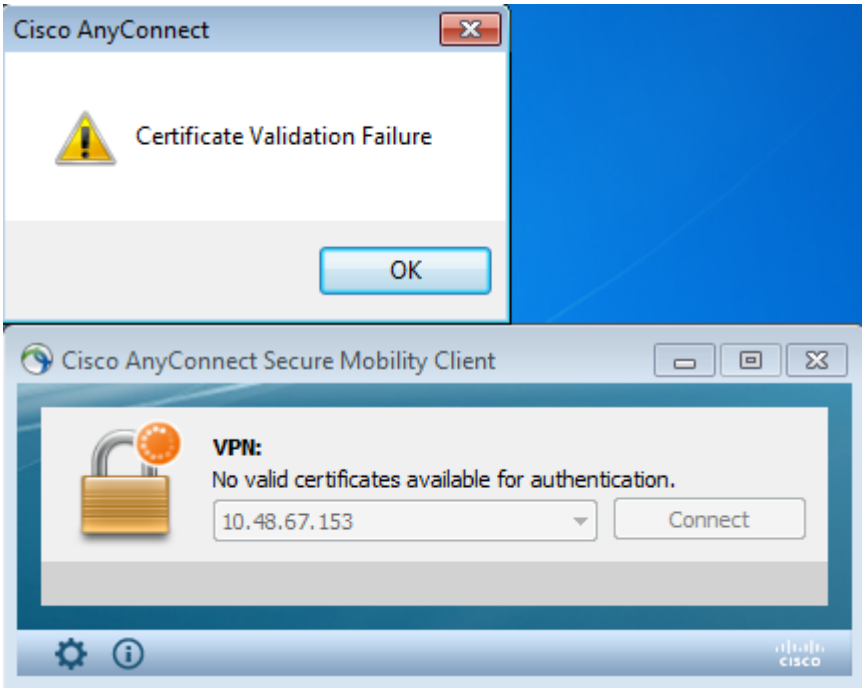
Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

Certificado Válido Ausente

Depois de remover um certificado válido do Windows7, o AnyConnect não consegue encontrar nenhum

certificado válido:



No ASA, parece que a sessão foi terminada pelo 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

Informações Relacionadas

- **Configurar grupos de túnel, políticas de grupo e usuários: configurar autenticação dupla**

- **Configurar um servidor externo para a autorização do usuário do dispositivo de segurança**
- **Suporte técnico e downloads da Cisco**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.