

Configurar a postura de VPN ASA com CSD, DAP e AnyConnect 4.0

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[ASA](#)

[Etapa 1. Configuração básica de VPN SSL](#)

[Etapa 2. Instalação do CSD](#)

[Etapa 3. Políticas de DAP](#)

[ISE](#)

[Verificar](#)

[Provisionamento de CSD e AnyConnect](#)

[Sessão AnyConnect VPN com postura - Não compatível](#)

[Sessão AnyConnect VPN com postura - Compatível](#)

[Troubleshoot](#)

[DART do AnyConnect](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve como executar a postura para sessões de VPN remotas encerradas no Adaptive Security Appliance (ASA). A postura é executada localmente pelo ASA com o uso do Cisco Secure Desktop (CSD) com o módulo HostScan. Depois que a sessão VPN é estabelecida, a estação compatível tem acesso total à rede, enquanto a estação não compatível tem acesso limitado à rede.

Além disso, os fluxos de provisionamento do CSD e do AnyConnect 4.0 são apresentados.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração do Cisco ASA VPN
- Cisco AnyConnect Secure Mobility Client

Componentes Utilizados

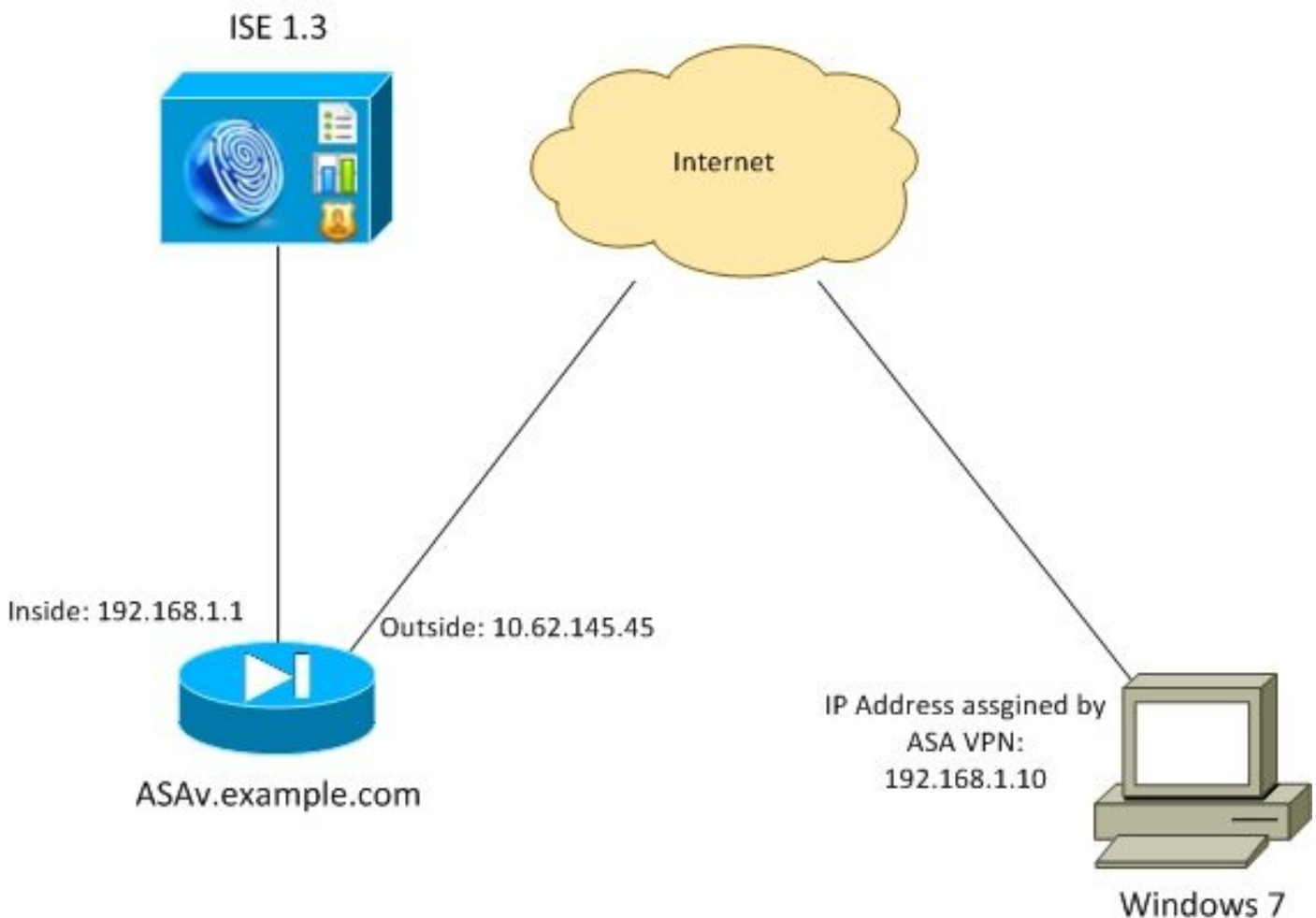
As informações neste documento são baseadas nestas versões de software e hardware:

- Microsoft Windows 7
- Cisco ASA, versão 9.3 ou posterior
- Software Cisco Identity Services Engine (ISE), versões 1.3 e posteriores
- Cisco AnyConnect Secure Mobility Client, versão 4.0 e posterior
- CSD, versão 3.6 ou posterior

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.

Configurar

Diagrama de Rede



A política corporativa é a seguinte:

- Os usuários remotos de VPN com arquivo **c:\test.txt** (compatível) devem ter acesso total à rede para os recursos internos da empresa
- Os usuários remotos de VPN que não têm o arquivo **c:\test.txt** (não compatível) devem ter acesso limitado à rede aos recursos internos da empresa: somente o acesso ao servidor de correção 1.1.1.1 é fornecido.

A existência de arquivo é o exemplo mais simples. Qualquer outra condição (antivírus, antispysware, processo, aplicativo, registro) pode ser usada.

O fluxo é o seguinte:

- Os usuários remotos não têm o AnyConnect instalado. Eles acessam a página da Web do ASA para provisionamento de CSD e AnyConnect (junto com o perfil de VPN)
- Após a conexão via AnyConnect, usuários não compatíveis são permitidos com acesso limitado à rede. A DAP (Dynamic Access Policy, Política de acesso dinâmico) chamada **FileNotExists** é combinada.
- O usuário executa a correção (instale manualmente o arquivo `c:\test.txt`) e se conecta novamente com o AnyConnect. Desta vez, é fornecido acesso total à rede (a política DAP chamada **FileExists** é combinada).

O módulo HostScan pode ser instalado manualmente no endpoint. Arquivos de exemplo (hostscan-win-4.0.00051-pre-Deployment-k9.msi) são compartilhados no Cisco Connection Online (CCO). Mas também pode ser empurrado da ASA. O HostScan faz parte do CSD que pode ser provisionado do ASA. Esta segunda abordagem é utilizada neste exemplo.

Para versões mais antigas do AnyConnect (3.1 e anteriores), havia um pacote separado disponível no CCO (por exemplo: hostscan_3.1.06073-k9.pkg) que poderia ter sido configurado e provisionado no ASA separadamente (com o comando `csd hostscan image`) - mas essa opção não existe mais para o AnyConnect versão 4.0.

ASA

Etapa 1. Configuração básica de VPN SSL

O ASA é pré-configurado com acesso VPN remoto básico (Secure Sockets Layer (SSL)):

```
webvpn
  enable outside
  no anyconnect-essentials
  anyconnect image disk0:/anyconnect-win-4.0.00051-k9.pkg 1
  anyconnect enable
  tunnel-group-list enable

group-policy AllProtocols internal
group-policy AllProtocols attributes
  vpn-tunnel-protocol ikev1 ikev2 ssl-client ssl-clientless

tunnel-group TAC type remote-access
tunnel-group TAC general-attributes
  address-pool POOL
  authentication-server-group ISE3
  default-group-policy AllProtocols
tunnel-group TAC webvpn-attributes
  group-alias TAC enable

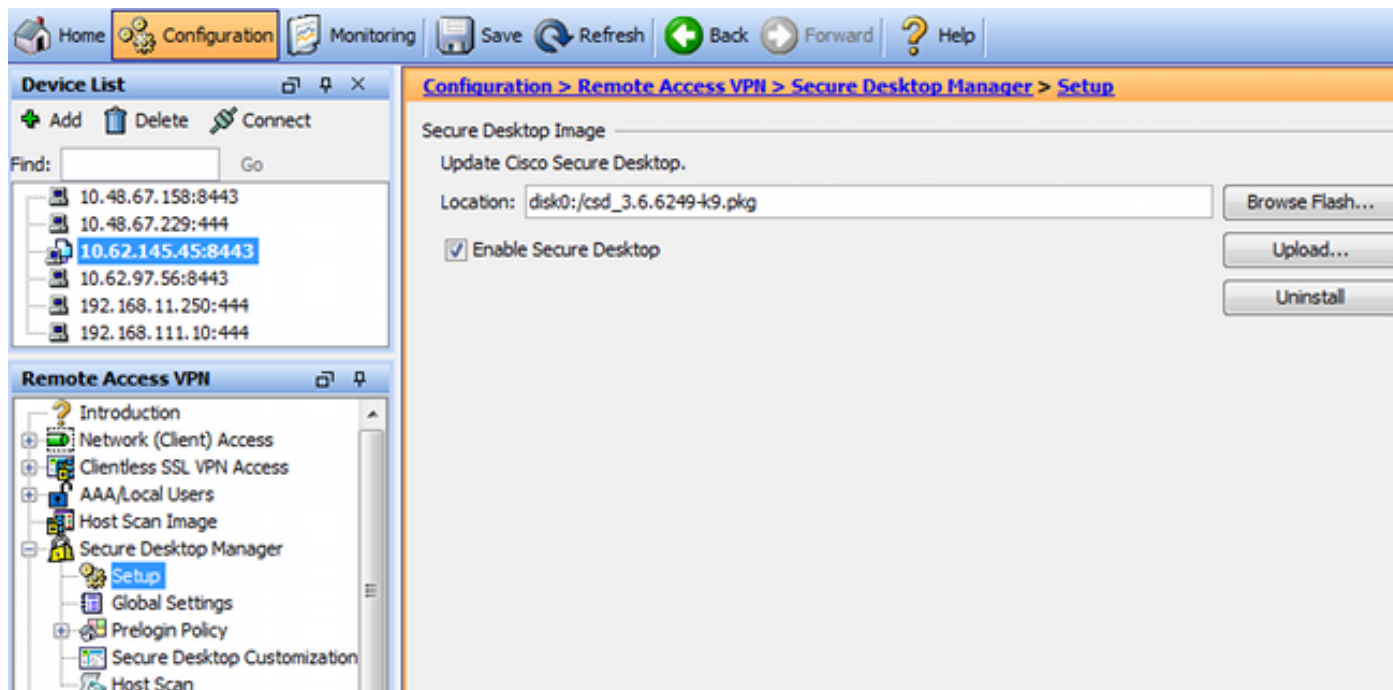
ip local pool POOL 192.168.1.10-192.168.1.20 mask 255.255.255.0

aaa-server ISE3 protocol radius
aaa-server ISE3 (inside) host 10.1.1.100
  key *****
```

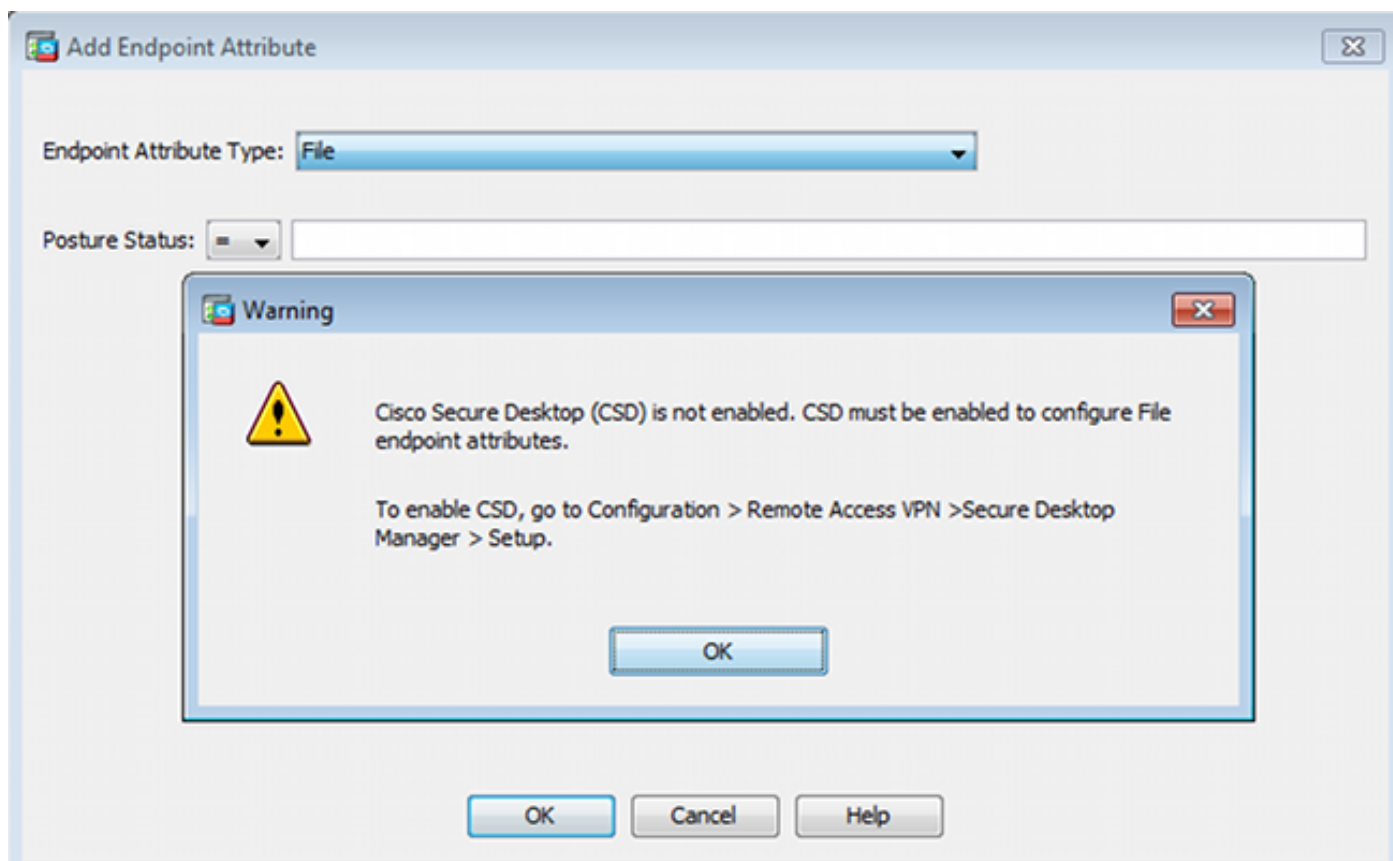
O pacote do AnyConnect foi baixado e usado.

Etapa 2. Instalação do CSD

A configuração subsequente é executada com o Adaptive Security Device Manager (ASDM). O pacote CSD precisa ser baixado para que o flash e a referência da configuração sejam mostrados na imagem.



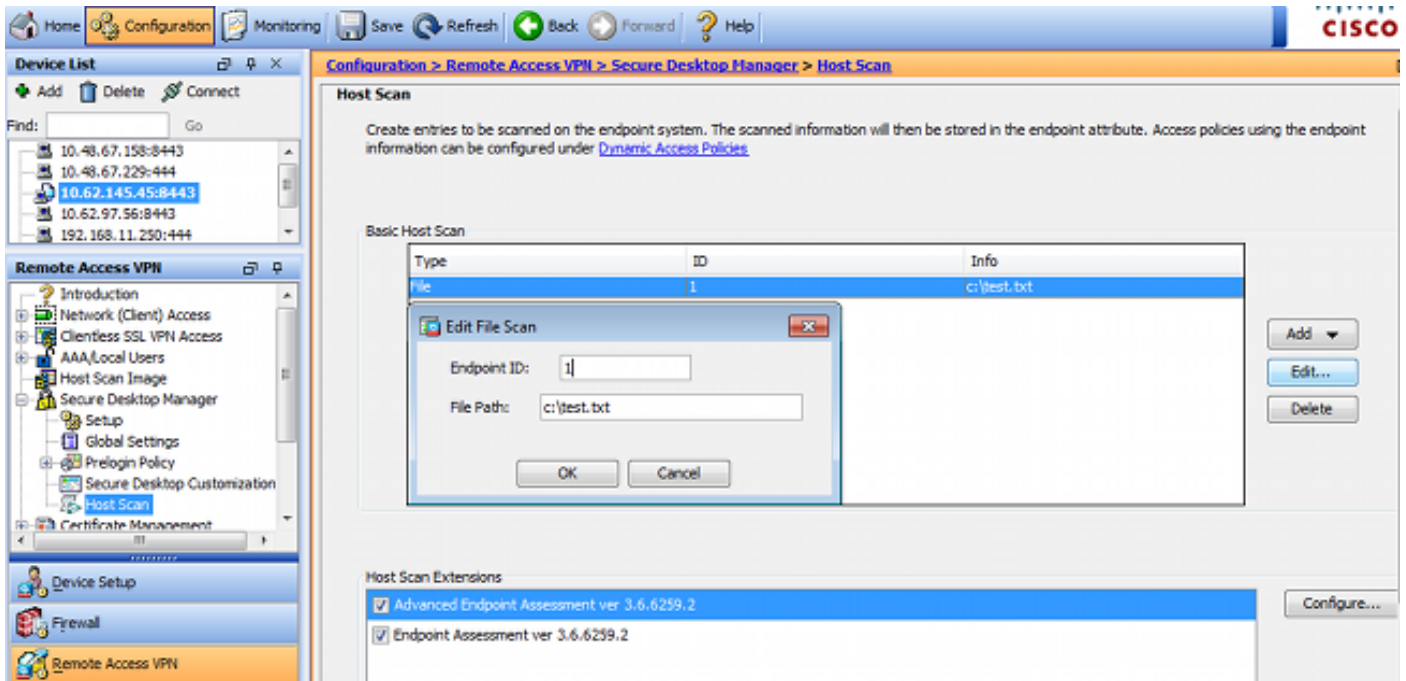
Sem habilitar o Secure Desktop, não seria possível usar atributos de CSD nas políticas de DAP como mostrado na imagem.



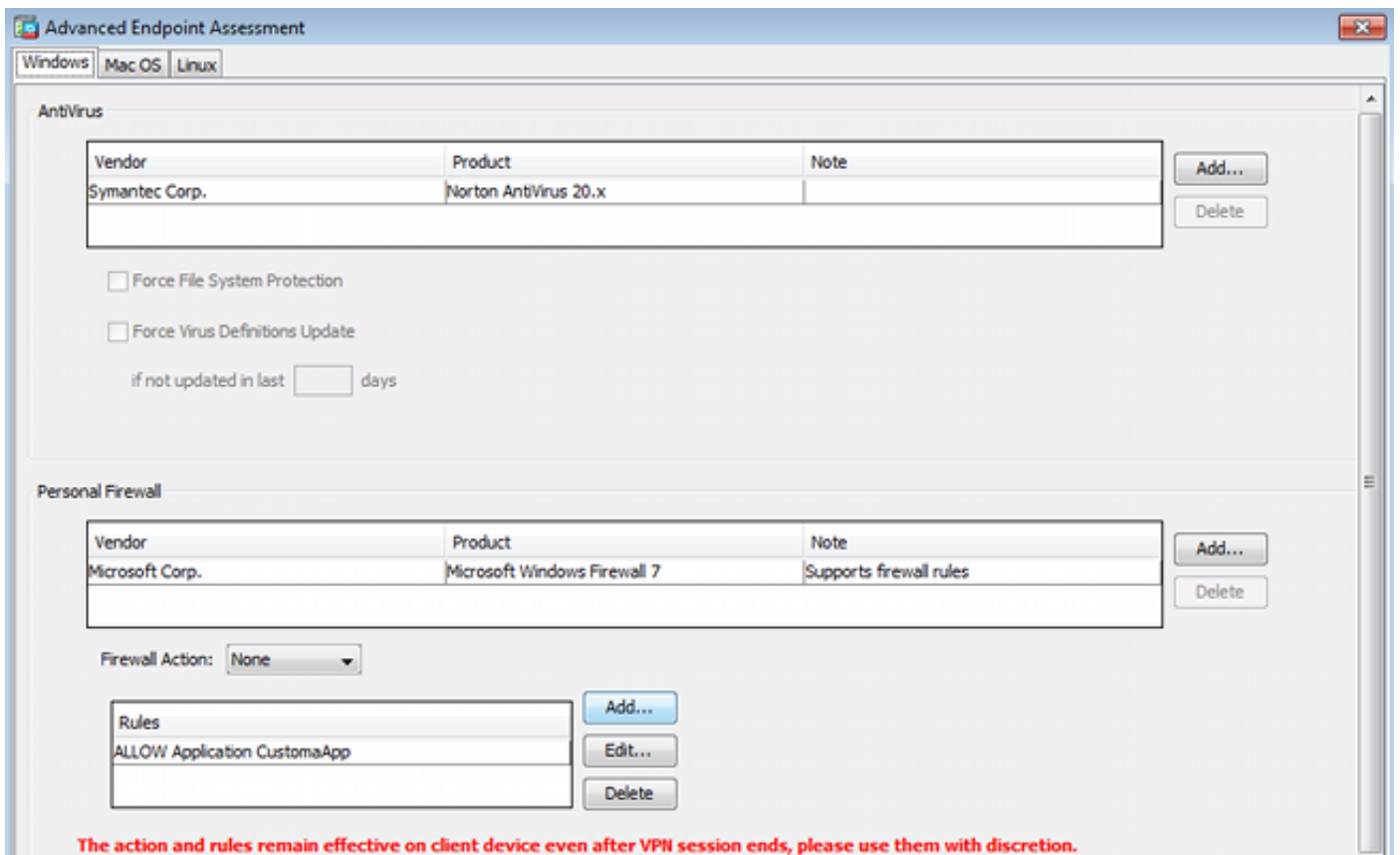
Depois de habilitar o CSD, várias opções em Secure Desktop Manager são exibidas.

Note: Esteja informado de que alguns deles já estão em decadência. Mais informações sobre recursos obsoletos podem ser encontradas: [Aviso de Deterioração de Funcionalidade para Ambiente de Trabalho Seguro \(Cofre\), Limpeza de Cache, Detecção de Bloqueador de Teclas e Detecção de Emulação de Host](#)

O HostScan ainda é totalmente suportado, uma nova regra básica do HostScan é adicionada. A existência de `c:\test.txt` é verificada como mostrado na imagem.



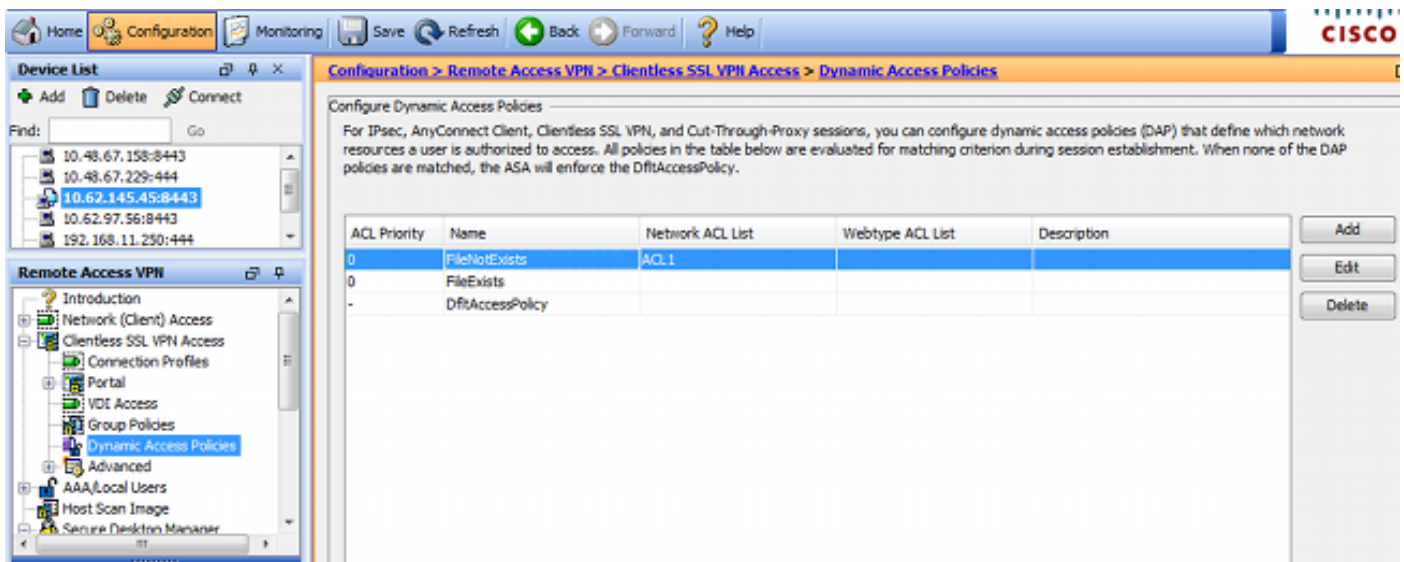
Além disso, uma regra adicional de avaliação de endpoint avançado é adicionada conforme mostrado na imagem.



Essa opção verifica a existência do Symantec Norton AntiVirus 20.x e do Microsoft Windows Firewall 7. O módulo de postura (HostScan) verifica esses valores, mas não haverá aplicação (a política de DAP não verifica isso).

Etapa 3. Políticas de DAP

As políticas de DAP são responsáveis por usar os dados coletados pelo HostScan como condições e aplicar atributos específicos à sessão VPN como resultado. Para criar uma política de DAP a partir do ASDM, navegue para **Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies** como mostrado na imagem.



A primeira política (FileExists) verifica o nome do grupo de túneis que é usado pelo perfil VPN configurado (a configuração do perfil VPN foi omitida para maior clareza). Em seguida, a verificação adicional do arquivo `c:\test.txt` é executada como mostrado na imagem.

Policy Name: ACL Priority:

Description:

Selection Criteria
 Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AAA attribute criteria below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advanced option to specify the logical expression text.

User has ANY of the following AAA Attributes values... and the following endpoint attributes are satisfied.

AAA Attribute	Operation/Value	Endpoint ID	Name/Operation/Value
isco.tunnelgroup	= TAC	file.1	exists = true

Buttons: Add, Edit, Delete, Logical Op.

Advanced

Access/Authorization Policy Attributes
 Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarchy attributes (those that are not specified in DAP).

Port Forwarding Lists | Bookmarks | Access Method | AnyConnect | AnyConnect Custom Attributes

Action | Network ACL Filters (client) | Webtype ACL Filters (clientless) | Functions

Network ACLs

ACL1 | Add >> | Manage... | Delete

Como resultado, nenhuma ação é executada com a configuração padrão para permitir a conectividade. Nenhuma ACL é usada - é fornecido acesso total à rede.

Os detalhes da verificação do arquivo são como mostrado na imagem.

Edit Endpoint Attribute

Endpoint Attribute Type: File

Exists Does not exist

Endpoint ID: 1
 c:\test.txt

Last Update: < days

Checksum: =

Compute CRC32 Checksum...

OK Cancel Help

A segunda política (FileNotExists) é semelhante - mas esta condição de tempo é se o arquivo não

existir como mostrado na imagem.

The screenshot shows the configuration page for a policy named "FileNotExists". The "Selection Criteria" section is expanded, showing two tables. The first table, "AAA Attribute", has one entry: "cisco.tunnelgroup" with the operation "=" and value "TAC". The second table, "Endpoint attributes", has one entry: "file.1" with the operation "exists != true". Below these tables are "Add", "Edit", and "Delete" buttons. The "Advanced" section is also visible, showing "Access/Authorization Policy Attributes" with a tabbed interface. The "Access Method" tab is selected, showing "AnyConnect Client" as the chosen option.

AAA Attribute	Operation/Value
cisco.tunnelgroup	= TAC

Endpoint ID	Name/Operation/Value
file.1	exists != true

Access Method: AnyConnect Client

O resultado tem a ACL1 da lista de acesso configurada. Isso é aplicado a usuários VPN não compatíveis com o fornecimento de acesso limitado à rede.

As duas políticas de DAP enviam o acesso do **AnyConnect Client**, conforme mostrado na imagem.

The screenshot shows the "Access Method" configuration section. It features a list of radio buttons for selecting the access method: "Unchanged", "AnyConnect Client" (which is selected), "Web-Portal", "Both-default-Web-Portal", and "Both-default-AnyConnect Client".

Access Method: AnyConnect Client

ISE

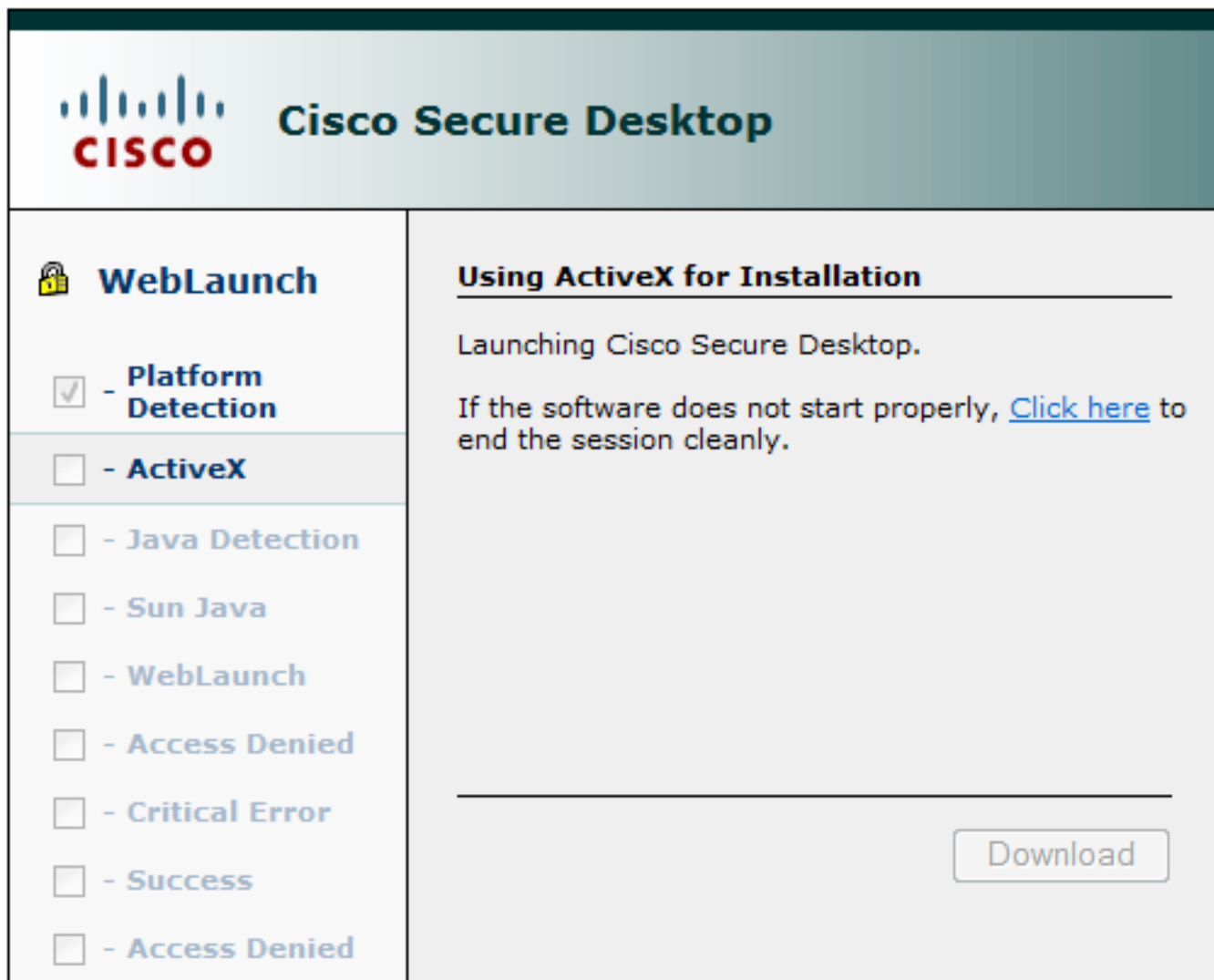
O ISE é usado para autenticação de usuário. Somente o dispositivo de rede (ASA) e o nome de usuário correto (cisco) devem ser configurados. Esta parte não é abrangida por este artigo.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Provisionamento de CSD e AnyConnect

Inicialmente, o usuário não é provisionado com o cliente AnyConnect. O usuário também não está em conformidade com a política (o arquivo `c:\test.txt` não existe). Digite <https://10.62.145.45> e o usuário será imediatamente redirecionado para a instalação do CSD, como mostrado na imagem.



Isso pode ser feito com Java ou ActiveX. Quando o CSD é instalado, ele é relatado como mostrado na imagem.



Cisco Secure Desktop



WebLaunch

- Platform Detection
- ActiveX
- Java Detection
- Sun Java
- WebLaunch
- Access Denied
- Critical Error
- Success
- Access Denied


System Validated

Cisco Secure Desktop successfully validated your system.

Success. Reloading. Please wait...

Download

Em seguida, o usuário é redirecionado para autenticação, conforme mostrado na imagem.



Login

Please enter your username and password.

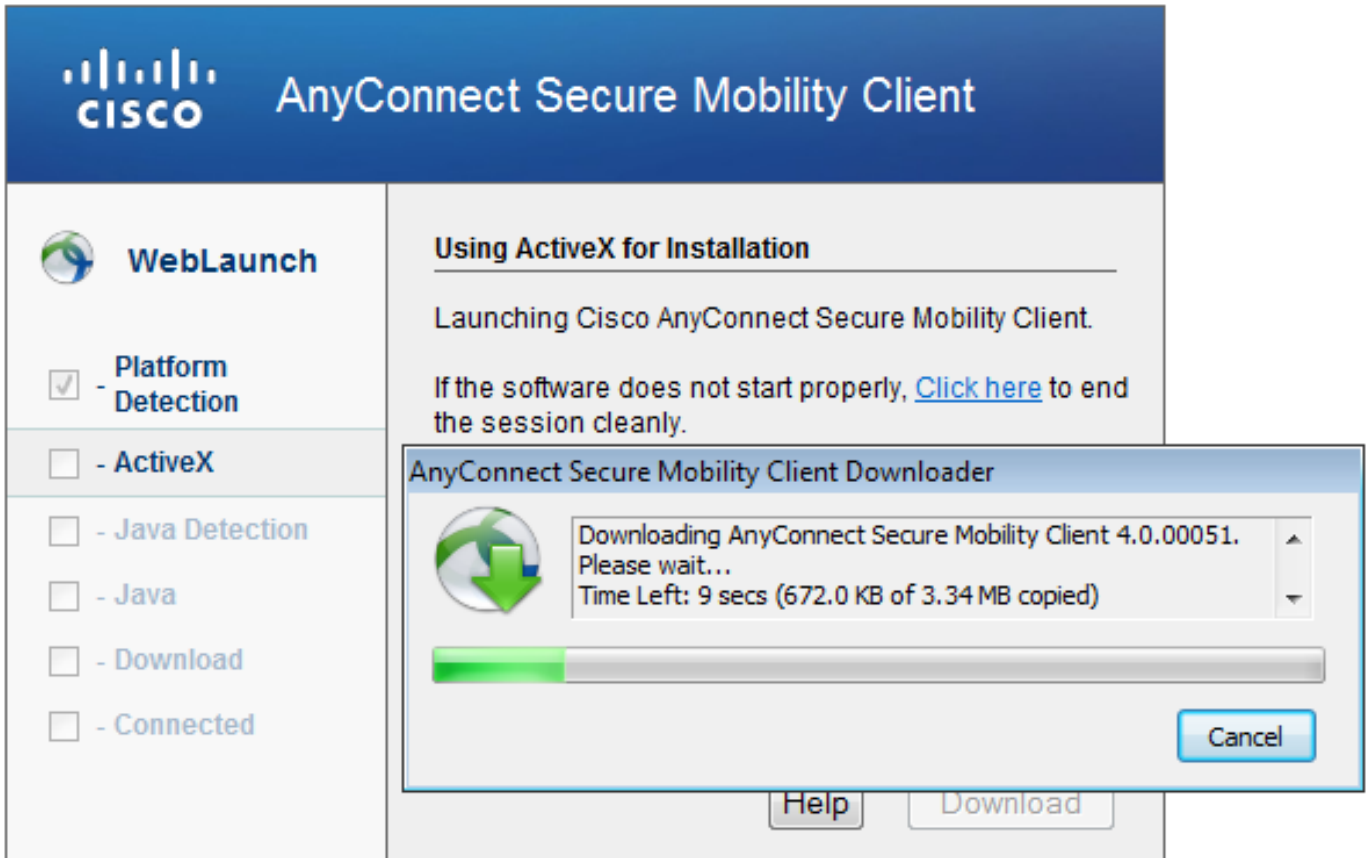
GROUP: TAC ▼

USERNAME:

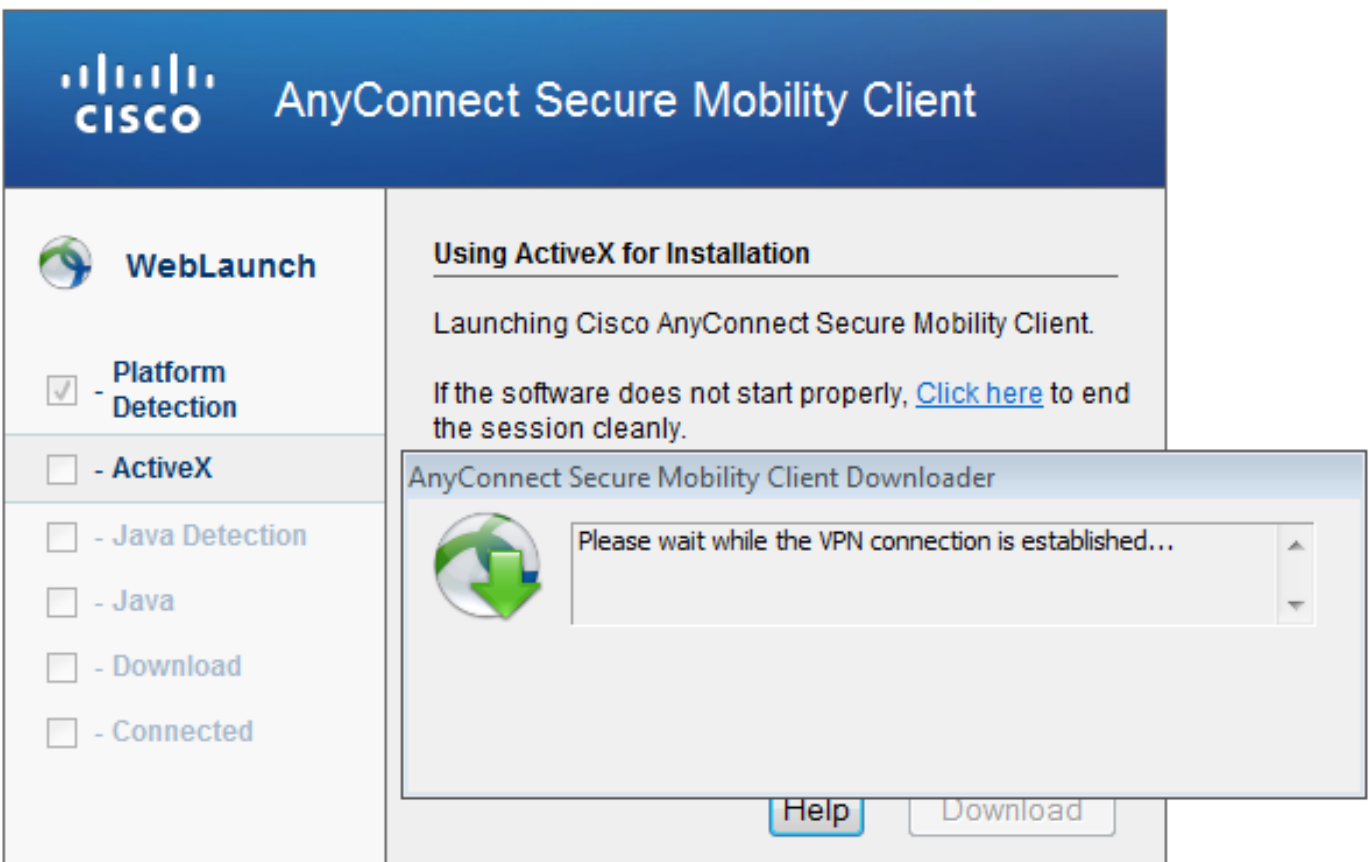
PASSWORD:

Login

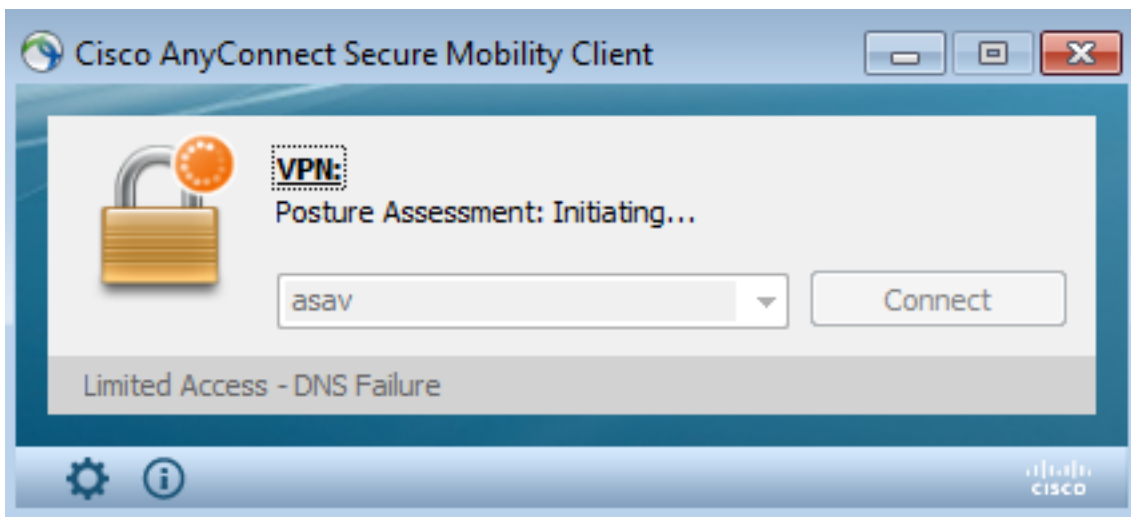
Se bem-sucedido, o AnyConnect e o perfil configurado são implantados - novamente, o ActiveX ou o Java podem ser usados como mostrado na imagem.



E a conexão VPN é estabelecida conforme mostrado na imagem.



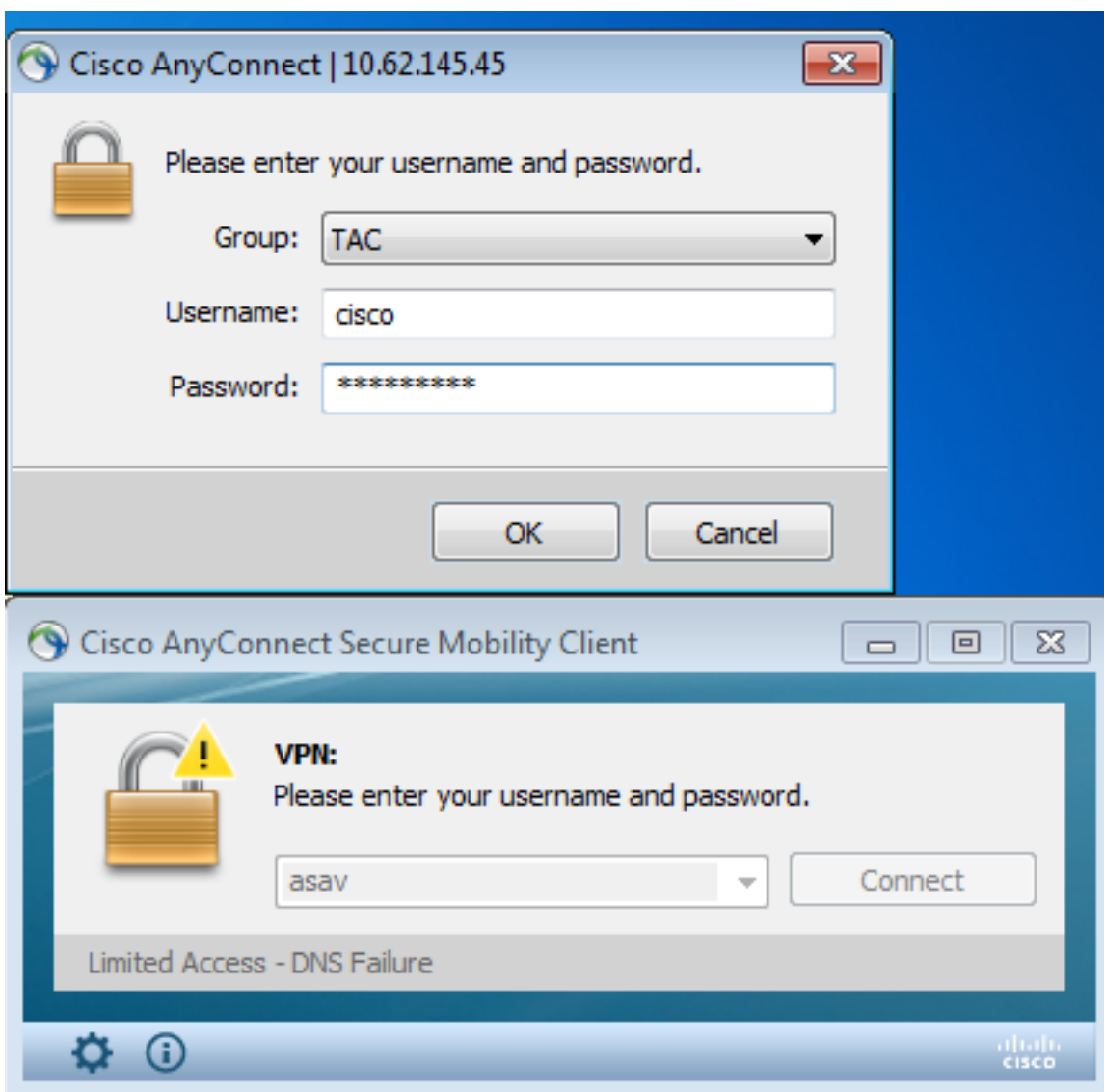
A primeira etapa do AnyConnect é executar verificações de postura (HostScan) e enviar os relatórios ao ASA, como mostrado na imagem.



Em seguida, o AnyConnect autentica e conclui a sessão de VPN.

Sessão AnyConnect VPN com postura - Não compatível

Quando você estabelece uma nova sessão de VPN com o AnyConnect, o primeiro passo é a postura (HostScan), conforme apresentada na captura de tela anterior. Em seguida, a autenticação ocorre e a sessão VPN é estabelecida conforme mostrado nas imagens.



O ASA relata que o relatório do HostScan é recebido:

```
%ASA-7-716603: Received 4 KB Hostscan data from IP <10.61.87.251>
```

Em seguida, executa a autenticação do usuário:

```
%ASA-6-113004: AAA user authentication Successful : server = 10.62.145.42 : user = cisco
```

E inicia a autorização para essa sessão VPN. Quando você tem "debug dap trace 255" habilitado, as informações sobre a existência do arquivo **c:\test.txt** são retornadas:

```
DAP_TRACE[128]: dap_install_endpoint_data_to_lua:endpoint.file["1"].exists="false"
DAP_TRACE: endpoint.file["1"].exists = "false"
DAP_TRACE[128]: dap_install_endpoint_data_to_lua:endpoint.file["1"].path="c:\test.txt"
DAP_TRACE: endpoint.file["1"].path = "c:\\test.txt"
```

Além disso, informações sobre o Firewall do Microsoft Windows:

```
DAP_TRACE[128]: dap_install_endpoint_data_to_lua:endpoint.fw["MSWindowsFW"].exists="false"
DAP_TRACE: endpoint.fw["MSWindowsFW"].exists = "false"
DAP_TRACE[128]:
dap_install_endpoint_data_to_lua:endpoint.fw["MSWindowsFW"].description="Microsoft Windows Firewall"
DAP_TRACE: endpoint.fw["MSWindowsFW"].description = "Microsoft Windows Firewall"
DAP_TRACE[128]: dap_install_endpoint_data_to_lua:endpoint.fw["MSWindowsFW"].version="7"
DAP_TRACE: endpoint.fw["MSWindowsFW"].version = "7"
DAP_TRACE[128]: dap_install_endpoint_data_to_lua:endpoint.fw["MSWindowsFW"].enabled="failed"
DAP_TRACE: endpoint.fw["MSWindowsFW"].enabled = "failed"
```

E o Symantec AntiVirus (de acordo com as regras de avaliação de endpoint avançado do HostScan configuradas anteriormente).

Como resultado, a política de DAP é combinada:

```
DAP_TRACE: Username: cisco, Selected DAPs: ,FileNotExists
```

Essa política força o uso do AnyConnect e também aplica a ACL1 da lista de acesso que fornece acesso restrito à rede para o usuário (não compatível com a política corporativa):

```
DAP_TRACE:The DAP policy contains the following attributes for user: cisco
```

```
DAP_TRACE:-----
```

```
DAP_TRACE:1: tunnel-protocol = svc
DAP_TRACE:2: svc ask = ask: no, dflt: svc
DAP_TRACE:3: action = continue
DAP_TRACE:4: network-acl = ACL1
```

Os registros também apresentam extensões ACIDEX que podem ser usadas pela política de DAP (ou mesmo transmitidas em Solicitações de RADIUS ao ISE e são usadas em Regras de Autorização como condições):

```
endpoint.anyconnect.clientversion = "4.0.00051";
endpoint.anyconnect.platform = "win";
endpoint.anyconnect.devicetype = "innotek GmbH VirtualBox";
endpoint.anyconnect.platformversion = "6.1.7600 ";
endpoint.anyconnect.deviceuniqueid =
"A1EDD2F14F17803779EB42C281C98DD892F7D34239AECDBB3FEA69D6567B2591";
```

```
endpoint.anyconnect.macaddress["0"] = "08-00-27-7f-5f-64";
endpoint.anyconnect.useragent = "AnyConnect Windows 4.0.00051";
```

Como resultado, a sessão VPN está ativa, mas com acesso restrito à rede:

```
ASAv2# show vpn-sessiondb detail anyconnect
```

Session Type: AnyConnect Detailed

```
Username      : cisco                Index      : 4
Assigned IP   : 192.168.1.10         Public IP  : 10.61.87.251
Protocol      : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License       : AnyConnect Premium
Encryption    : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing       : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx      : 11432                Bytes Rx   : 14709
Pkts Tx       : 8                   Pkts Rx   : 146
Pkts Tx Drop  : 0                   Pkts Rx Drop : 0
Group Policy  : AllProtocols         Tunnel Group : TAC
Login Time    : 11:58:54 UTC Fri Dec 26 2014
Duration      : 0h:07m:54s
Inactivity    : 0h:00m:00s
VLAN Mapping  : N/A                  VLAN       : none
Audt Sess ID  : 0add006400004000549d4d7e
Security Grp  : none
```

```
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
```

AnyConnect-Parent:

```
Tunnel ID    : 4.1
Public IP    : 10.61.87.251
Encryption   : none                Hashing      : none
TCP Src Port : 49514                TCP Dst Port : 443
Auth Mode    : userPassword
Idle Time Out: 30 Minutes           Idle TO Left : 22 Minutes
Client OS    : win
Client OS Ver: 6.1.7600
Client Type  : AnyConnect
Client Ver   : Cisco AnyConnect VPN Agent for Windows 4.0.00051
Bytes Tx     : 5716                 Bytes Rx    : 764
Pkts Tx     : 4                    Pkts Rx    : 1
Pkts Tx Drop : 0                   Pkts Rx Drop : 0
```

SSL-Tunnel:

```
Tunnel ID    : 4.2
Assigned IP   : 192.168.1.10         Public IP    : 10.61.87.251
Encryption    : RC4                 Hashing      : SHA1
Encapsulation: TLSv1.0              TCP Src Port : 49517
TCP Dst Port  : 443                 Auth Mode    : userPassword
Idle Time Out: 30 Minutes           Idle TO Left : 22 Minutes
Client OS     : Windows
Client Type   : SSL VPN Client
Client Ver    : Cisco AnyConnect VPN Agent for Windows 4.0.00051
Bytes Tx      : 5716                 Bytes Rx    : 2760
Pkts Tx       : 4                   Pkts Rx    : 12
Pkts Tx Drop  : 0                   Pkts Rx Drop : 0
Filter Name   : ACL1
```

DTLS-Tunnel:

```
Tunnel ID    : 4.3
Assigned IP   : 192.168.1.10         Public IP    : 10.61.87.251
```



```
Encryption      : AES128                Hashing          : SHA1
Encapsulation:  DTL SV1.0                UDP Src Port    : 52749
UDP Dst Port    : 443                    Auth Mode       : userPassword
Idle Time Out:  30 Minutes                Idle TO Left    : 24 Minutes
Client OS       : Windows
Client Type     : DTLS VPN Client
Client Ver      : Cisco AnyConnect VPN Agent for Windows 4.0.00051
Bytes Tx        : 0                       Bytes Rx        : 11185
Pkts Tx         : 0                       Pkts Rx        : 133
Pkts Tx Drop    : 0                       Pkts Rx Drop   : 0
Filter Name    : ACL1
```

```
ASAv2# show access-list ACL1
```

```
access-list ACL1; 1 elements; name hash: 0xe535f5fe
```

```
access-list ACL1 line 1 extended permit ip any host 1.1.1.1 (hitcnt=0) 0xe6492cbf
```

O histórico do AnyConnect mostra as etapas detalhadas do processo de postura:

```
12:57:47    Contacting 10.62.145.45.
12:58:01    Posture Assessment: Required for access
12:58:01    Posture Assessment: Checking for updates...
12:58:02    Posture Assessment: Updating...
12:58:03    Posture Assessment: Initiating...
12:58:13    Posture Assessment: Active
12:58:13    Posture Assessment: Initiating...
12:58:37    User credentials entered.
12:58:43    Establishing VPN session...
12:58:43    The AnyConnect Downloader is performing update checks...
12:58:43    Checking for profile updates...
12:58:43    Checking for product updates...
12:58:43    Checking for customization updates...
12:58:43    Performing any required updates...
12:58:43    The AnyConnect Downloader updates have been completed.
12:58:43    Establishing VPN session...
12:58:43    Establishing VPN - Initiating connection...
12:58:48    Establishing VPN - Examining system...
12:58:48    Establishing VPN - Activating VPN adapter...
12:58:52    Establishing VPN - Configuring system...
12:58:52    Establishing VPN...
12:58:52    Connected to 10.62.145.45.
```

Sessão AnyConnect VPN com postura - Compatível

Depois de criar o arquivo `c:\test.txt`, o fluxo é semelhante. Quando uma nova sessão do AnyConnect é iniciada, os registros indicam a existência do arquivo:

```
%ASA-7-734003: DAP: User cisco, Addr 10.61.87.251: Session Attribute
endpoint.file["1"].exists="true"
%ASA-7-734003: DAP: User cisco, Addr 10.61.87.251: Session Attribute
endpoint.file["1"].path="c:\test.txt"
```

Como resultado, outra política de DAP é usada:

```
DAP_TRACE: Username: cisco, Selected DAPs: ,FileExists
```

A política não impõe nenhuma ACL como a restrição para o tráfego de rede.

E a sessão está ativa sem qualquer ACL (acesso total à rede):

ASAv2# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : cisco Index : 5
Assigned IP : 192.168.1.10 Public IP : 10.61.87.251
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)RC4 DTLS-Tunnel: (1)AES128
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 11432 Bytes Rx : 6298
Pkts Tx : 8 Pkts Rx : 38
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : AllProtocols Tunnel Group : TAC
Login Time : 12:10:28 UTC Fri Dec 26 2014
Duration : 0h:00m:17s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0add006400005000549d5034
Security Grp : none

AnyConnect-Parent Tunnels: 1

SSL-Tunnel Tunnels: 1

DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 5.1
Public IP : 10.61.87.251
Encryption : none Hashing : none
TCP Src Port : 49549 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : win
Client OS Ver: 6.1.7600
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.0.00051
Bytes Tx : 5716 Bytes Rx : 764
Pkts Tx : 4 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 5.2
Assigned IP : 192.168.1.10 Public IP : 10.61.87.251
Encryption : RC4 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 49552
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.0.00051
Bytes Tx : 5716 Bytes Rx : 1345
Pkts Tx : 4 Pkts Rx : 6
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:

Tunnel ID : 5.3
Assigned IP : 192.168.1.10 Public IP : 10.61.87.251
Encryption : AES128 Hashing : SHA1
Encapsulation: DTLSv1.0 UDP Src Port : 54417
UDP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes
Client OS : Windows

```
Client Type   : DTLS VPN Client
Client Ver    : Cisco AnyConnect VPN Agent for Windows 4.0.00051
Bytes Tx      : 0                               Bytes Rx     : 4189
Pkts Tx       : 0                               Pkts Rx      : 31
Pkts Tx Drop  : 0                               Pkts Rx Drop : 0
```

Além disso, o Anyconnect relata que o HostScan está ocioso e aguardando a próxima solicitação de verificação:

```
13:10:15    Hostscan state idle
13:10:15    Hostscan is waiting for the next scan
```

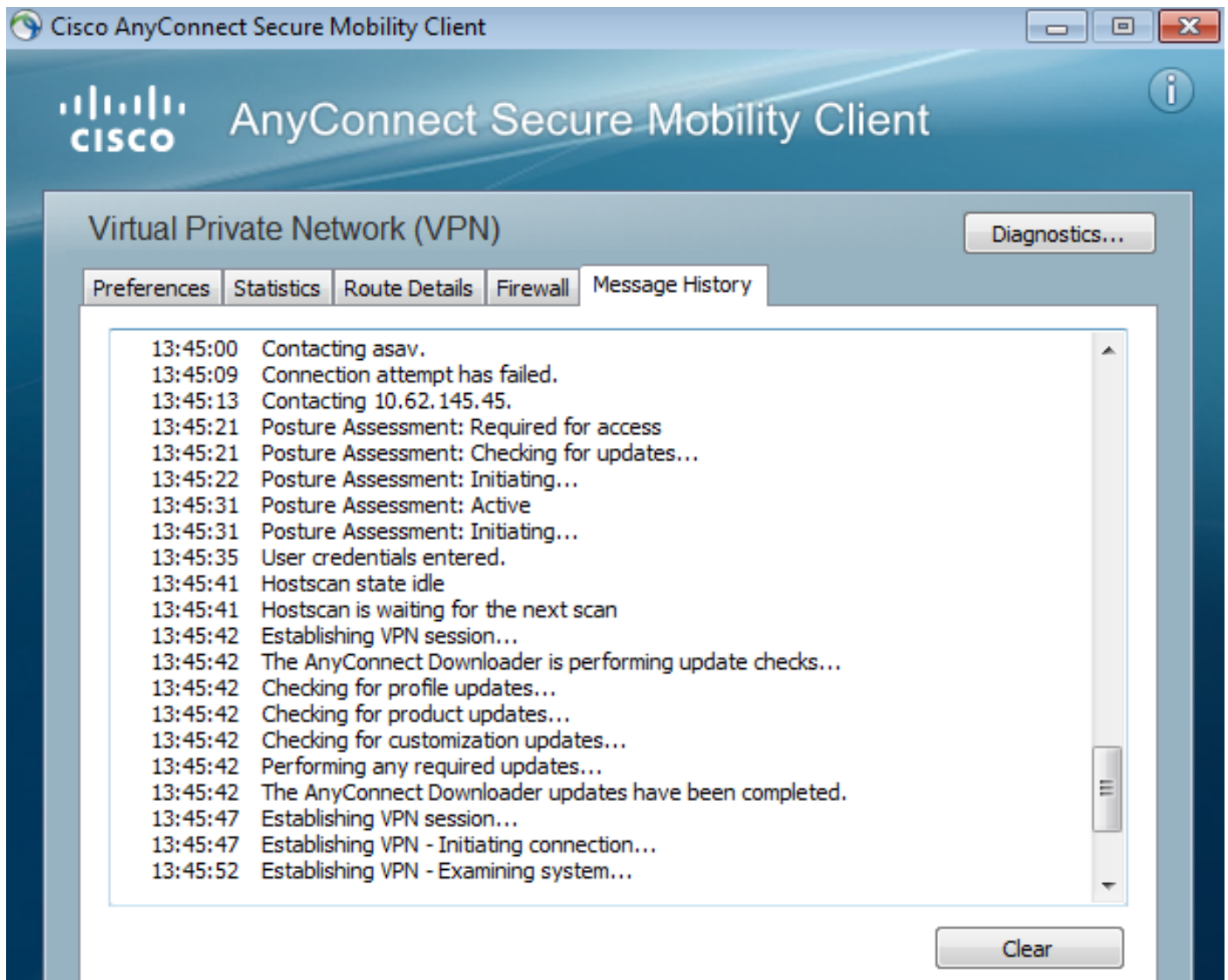
Note: Para reavaliação, é aconselhável usar um módulo de postura integrado ao ISE.

Troubleshoot

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

DART do AnyConnect

O AnyConnect fornece diagnósticos conforme mostrado na imagem.



Que reúne e salva todos os logs do AnyConnect em um arquivo zip na área de trabalho. Esse arquivo zip inclui os registros no Cisco AnyConnect Secure Mobility Client/Anyconnect.txt.

Isso fornece informações sobre o ASA e solicita que o HostScan reúna dados:

```
Date       : 12/26/2014
Time       : 12:58:01
Type      : Information
Source    : acvpnui
```

```
Description : Function: ConnectMgr::processResponseString
File: .\ConnectMgr.cpp
Line: 10286
Invoked Function: ConnectMgr::processResponseString
Return Code: 0 (0x00000000)
```

Description: HostScan request detected.

Em seguida, vários outros registros revelam que o CSD está instalado. Este é o exemplo de um provisionamento de CSD e conexão subsequente do AnyConnect junto com a postura:

```
CSD detected, launching CSD
Posture Assessment: Required for access
Gathering CSD version information.
Posture Assessment: Checking for updates...
CSD version file located
Downloading and launching CSD
Posture Assessment: Updating...
Downloading CSD update
CSD Stub located
Posture Assessment: Initiating...
Launching CSD
Initializing CSD
Performing CSD prelogin verification.
CSD prelogin verification finished with return code 0
Starting CSD system scan.
CSD successfully launched
Posture Assessment: Active
CSD launched, continuing until token is validated.
Posture Assessment: Initiating...

Checking CSD token for validity
Waiting for CSD token validity result
CSD token validity check completed
CSD Token is now valid
CSD Token validated successfully
Authentication succeeded
Establishing VPN session...
```

A comunicação entre o ASA e o AnyConnect é otimizada, as solicitações do ASA para executar apenas verificações específicas - o AnyConnect faz o download de dados adicionais para poder realizar isso (por exemplo, verificação específica de antivírus).

Ao abrir o caso com o TAC, anexe os logs do Dart junto com "show tech" e "debug dap trace 255" do ASA.

Informações Relacionadas

- [Configurando a verificação de host e o módulo de postura - Guia do administrador do Cisco AnyConnect Secure Mobility Client](#)
- [Serviços de postura no Guia de configuração do Cisco ISE](#)
- [Guia do administrador do Cisco ISE 1.3](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)