

Configure la evaluación de estado de seguridad de VPN en ASA con CSD, DAP y AnyConnect 4.0

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[ASA](#)

[Paso 1. Configuración básica de SSL VPN](#)

[Paso 2. Instalación de CSD](#)

[Paso 3. Políticas DAP](#)

[ISE](#)

[Verificación](#)

[Aprovisionamiento de CSD y AnyConnect](#)

[Sesión VPN de AnyConnect con estado: no conforme](#)

[Sesión VPN de AnyConnect con estado: compatible](#)

[Troubleshoot](#)

[DART de AnyConnect](#)

[Información Relacionada](#)

Introducción

En este documento se describe cómo realizar la evaluación del estado de seguridad de las sesiones de VPN remotas terminadas en Adaptive Security Appliance (ASA). El estado lo realiza localmente ASA con el uso de Cisco Secure Desktop (CSD) con el módulo HostScan. Una vez establecida la sesión VPN, se permite el acceso completo a la red a la estación compatible, mientras que la estación no compatible tiene acceso limitado a la red.

Además, se presentan los flujos de aprovisionamiento de CSD y AnyConnect 4.0.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de Cisco ASA VPN
- Cisco AnyConnect Secure Mobility Client

Componentes Utilizados

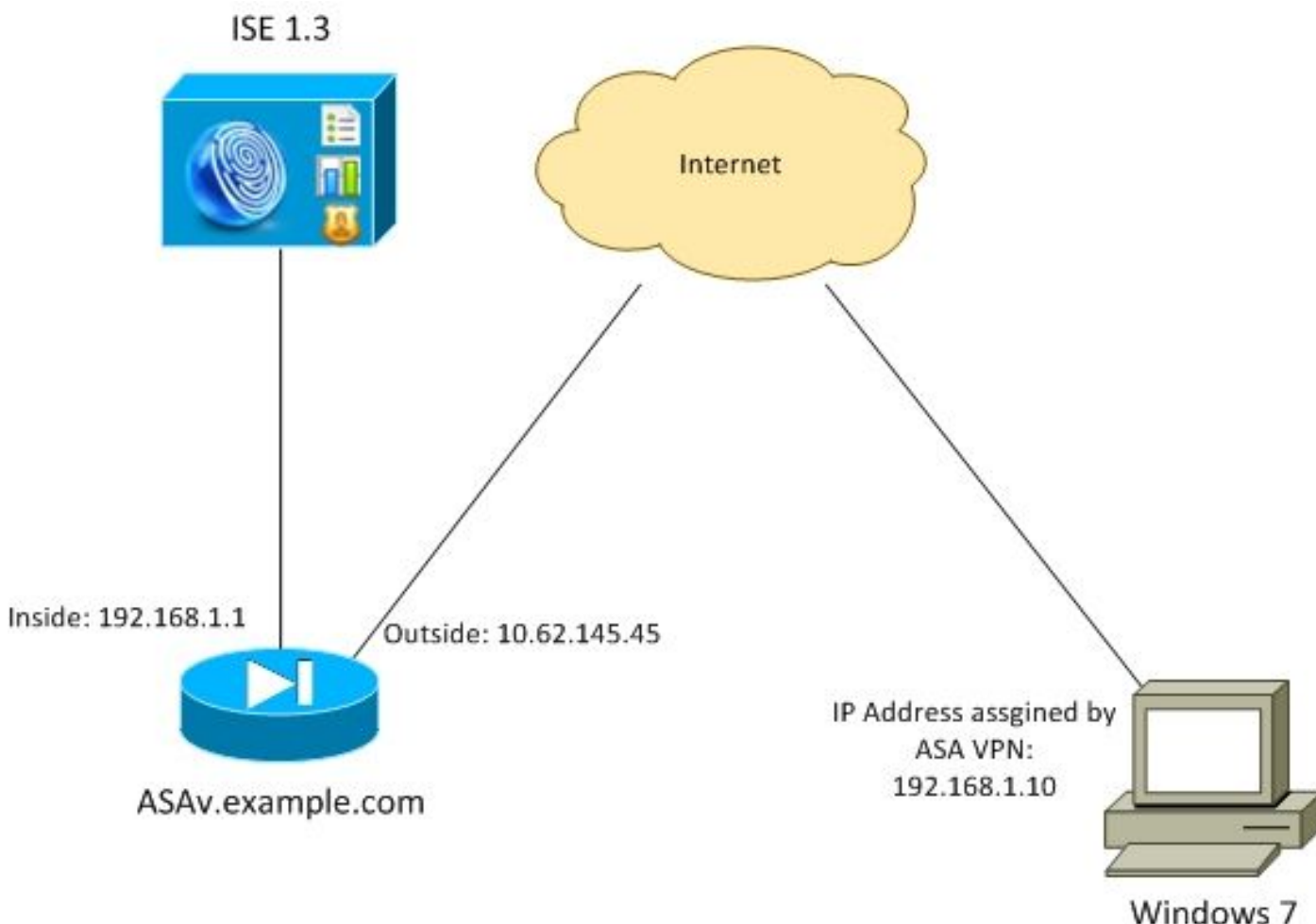
La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Microsoft Windows 7
- Cisco ASA, versión 9.3 o posterior
- Software Cisco Identity Services Engine (ISE), versiones 1.3 y posteriores
- Cisco AnyConnect Secure Mobility Client, versión 4.0 y posterior
- CSD, versión 3.6 o 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama de la red



La política corporativa es la siguiente:

- Los usuarios de VPN remotos que tienen el archivo `c:\test.txt` (conforme) deben tener acceso completo a la red para los recursos internos de la empresa
- Los usuarios de VPN remotos que no tienen el archivo `c:\test.txt` (no compatible) deben tener

un acceso de red limitado a los recursos internos de la empresa: sólo se proporciona acceso al servidor de corrección 1.1.1.1.

La existencia de archivos es el ejemplo más simple. Se puede utilizar cualquier otra condición (antivirus, antispyware, proceso, aplicación, registro).

El flujo es el siguiente:

- Los usuarios remotos no tienen instalado AnyConnect. Acceden a la página web de ASA para el aprovisionamiento de CSD y AnyConnect (junto con el perfil de VPN)
- Una vez que la conexión se realiza a través de AnyConnect, los usuarios que no cumplen las normas tienen acceso limitado a la red. La política de acceso dinámico (DAP) denominada **FileNotExists** coincide.
- El usuario realiza la remediación (instalar manualmente el archivo **c:\test.txt**) y se conecta de nuevo con AnyConnect. Esta vez, se proporciona acceso completo a la red (la política DAP llamada **FileExists** coincide).

El módulo HostScan se puede instalar manualmente en el terminal. Los archivos de ejemplo (hostscan-win-4.0.00051-pre-Deploy-k9.msi) se comparten en Cisco Connection Online (CCO). Sin embargo, también se podría sacar de ASA. HostScan es una parte de CSD que se puede aprovisionar desde ASA. Ese segundo enfoque se utiliza en este ejemplo.

Para las versiones anteriores de AnyConnect (3.1 y anteriores), había un paquete separado disponible en CCO (ejemplo: hostscan_3.1.06073-k9.pkg) que podría haberse configurado y aprovisionado en ASA por separado (con el comando **csd hostscan image**) - pero esa opción ya no existe para AnyConnect versión 4.0.

ASA

Paso 1. Configuración básica de SSL VPN

ASA está preconfigurado con acceso 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

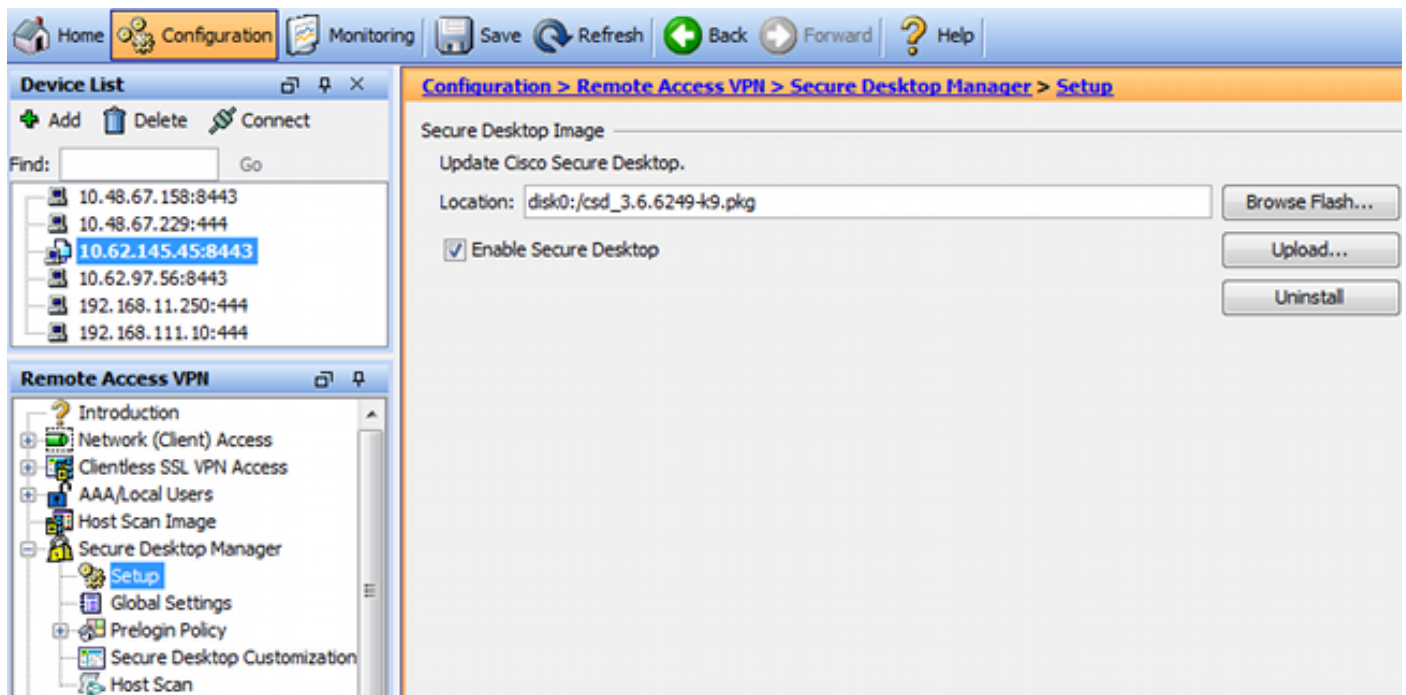
ip local pool POOL 192.168.1.10-192.168.1.20 mask 255.255.255.0
```

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

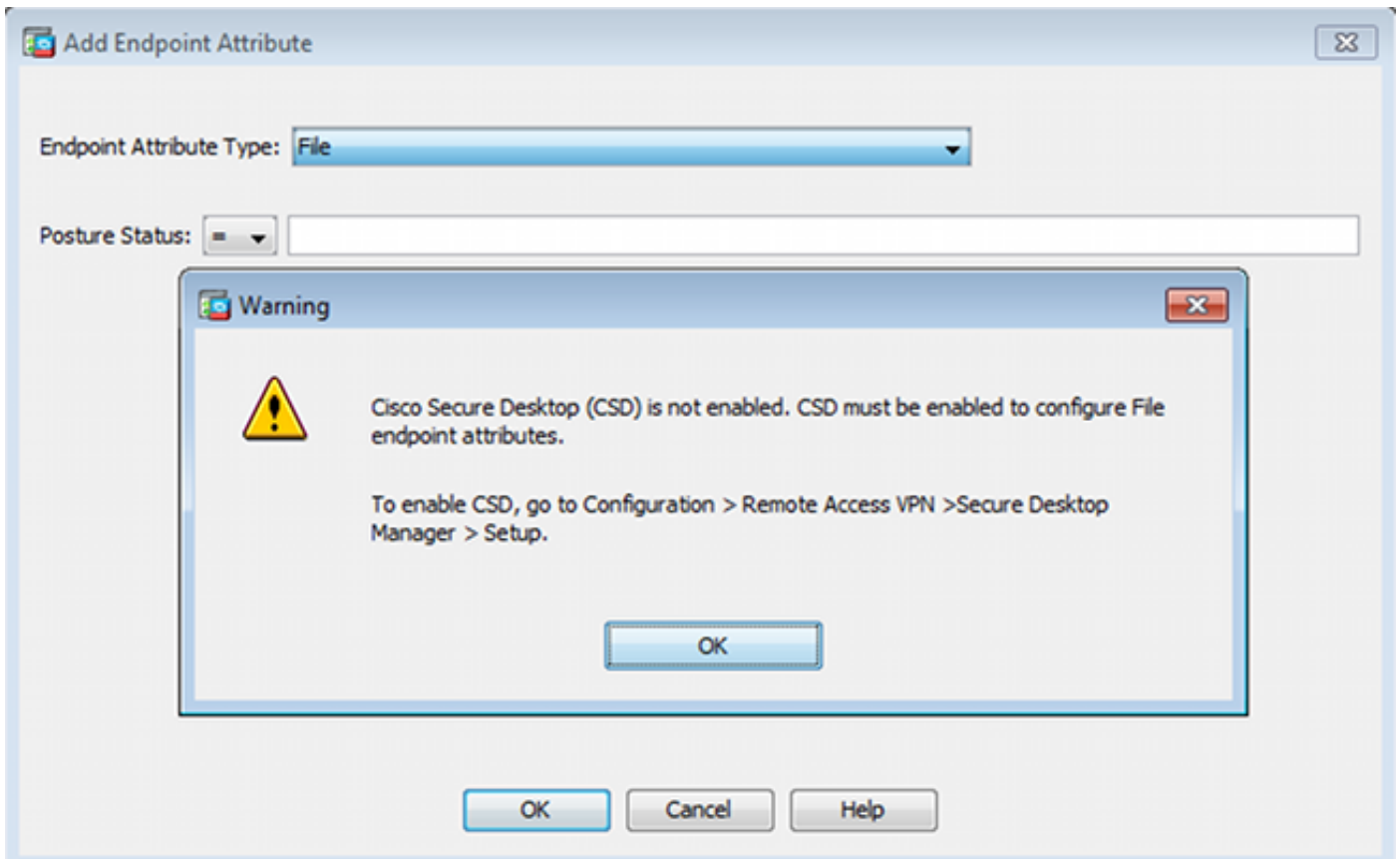
El paquete de AnyConnect se ha descargado y utilizado.

Paso 2. Instalación de CSD

La configuración posterior se realiza con Adaptive Security Device Manager (ASDM). El paquete CSD debe descargarse para parpadear y tomar referencia de la configuración como se muestra en la imagen.



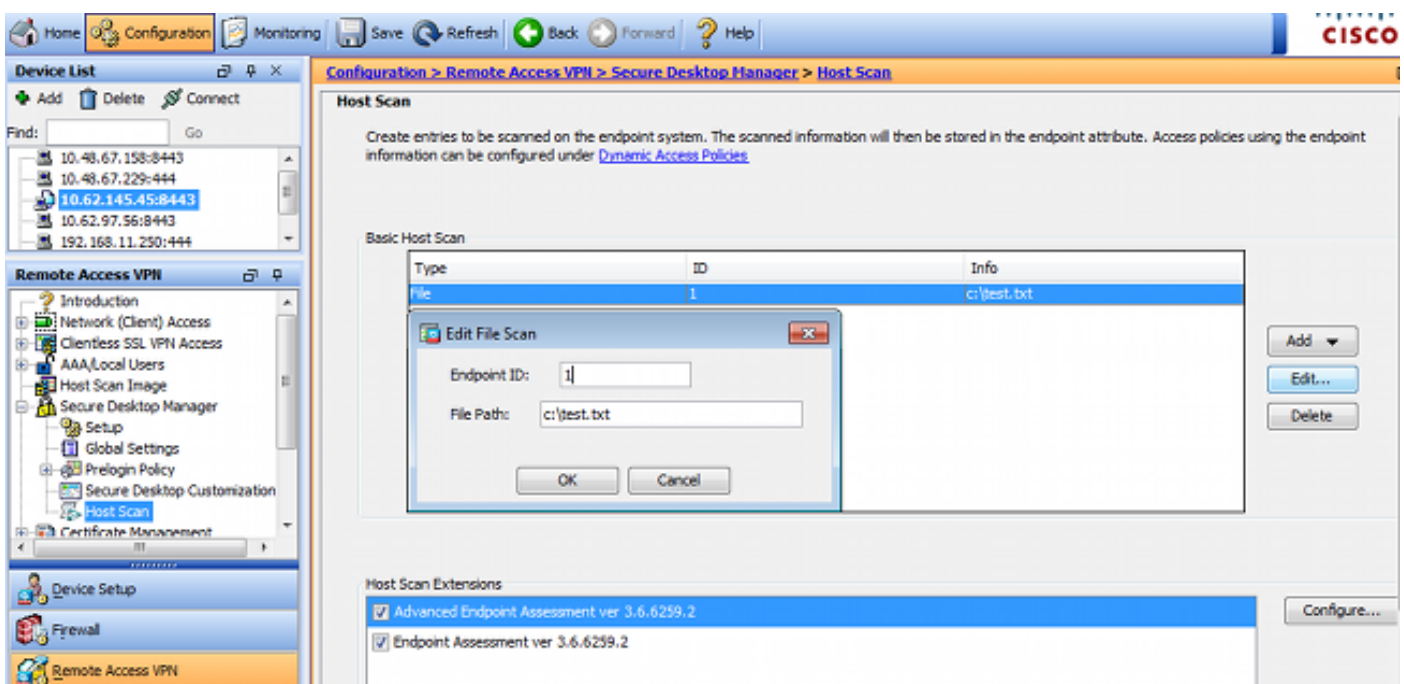
Sin activar Secure Desktop no sería posible utilizar atributos CSD en las políticas DAP como se muestra en la imagen.



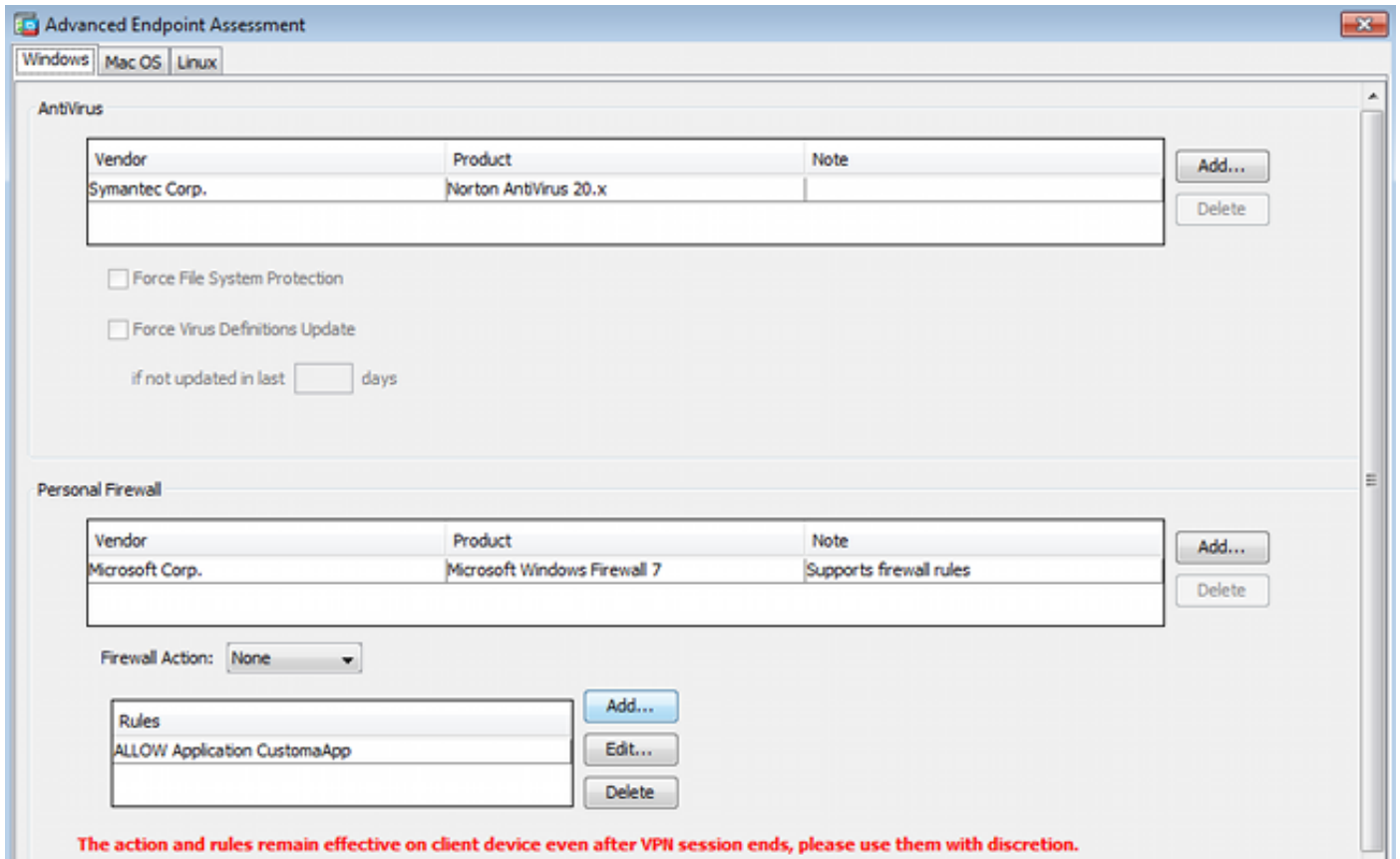
Después de activar CSD, aparecen varias opciones en Secure Desktop Manager.

Nota: Tenga en cuenta que algunos de ellos ya están obsoletos. Puede encontrar más información sobre las funciones obsoletas: [Aviso de desaprobarción de funciones para Secure Desktop \(Vault\), limpiador de caché, detección de registrador de pulsaciones de teclas y detección de emulación de host](#)

HostScan todavía está totalmente soportado, se agrega una nueva regla de HostScan básica. La existencia de `c:\test.txt` se verifica como se muestra en la imagen.



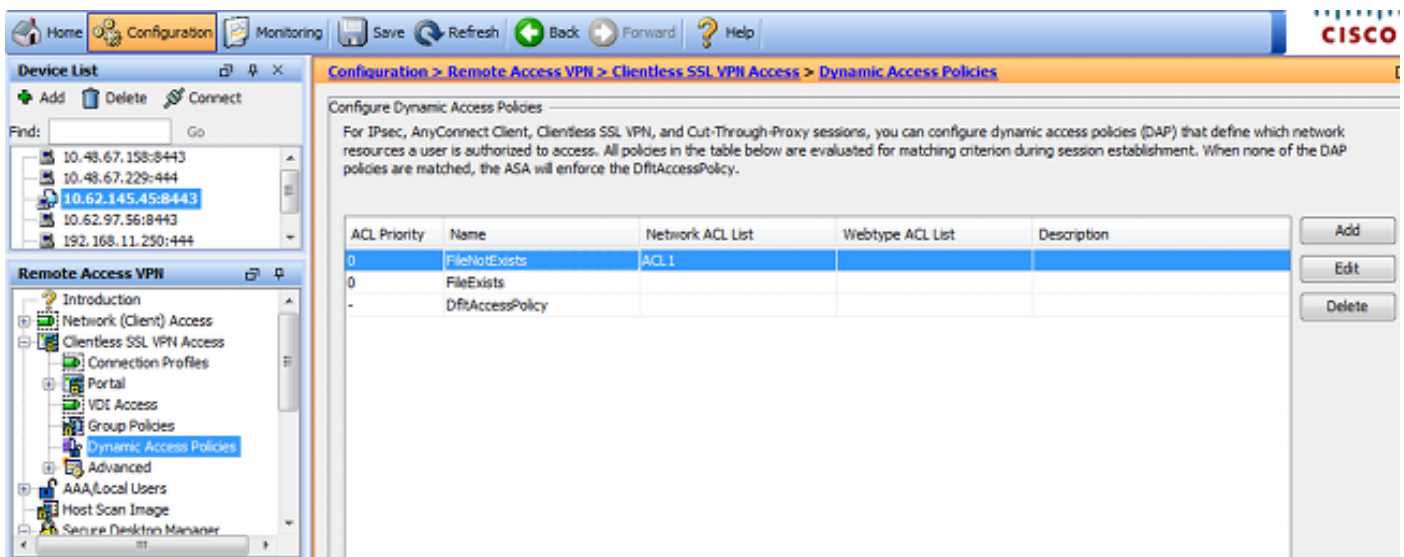
Además, se agrega una regla de evaluación de terminal avanzada adicional, como se muestra en la imagen.



Este verifica la existencia de Symantec Norton AntiVirus 20.x y Microsoft Windows Firewall 7. El módulo de estado (HostScan) verifica estos valores, pero no habrá aplicación (la política DAP no lo verifica).

Paso 3. Políticas DAP

Las políticas DAP son responsables de utilizar los datos recopilados por HostScan como condiciones y aplicar atributos específicos a la sesión VPN como resultado. Para crear la política DAP desde ASDM, navegue hasta **Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies** como se muestra en la imagen.



La primera política (FileExists) verifica el nombre del grupo de túnel que utiliza el perfil VPN configurado (la configuración del perfil VPN se ha omitido para mayor claridad). A continuación, se realiza una comprobación adicional del archivo `c:\test.txt` como se muestra en la imagen.

The screenshot shows a configuration window for a policy named "FileExists". The "Policy Name" field contains "FileExists" and the "ACL Priority" is set to "0". The "Description" field is empty.

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
cisco.tunnelgroup	= TAC

Buttons: Add, Edit, Delete

Endpoint ID	Name/Operation/Value
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

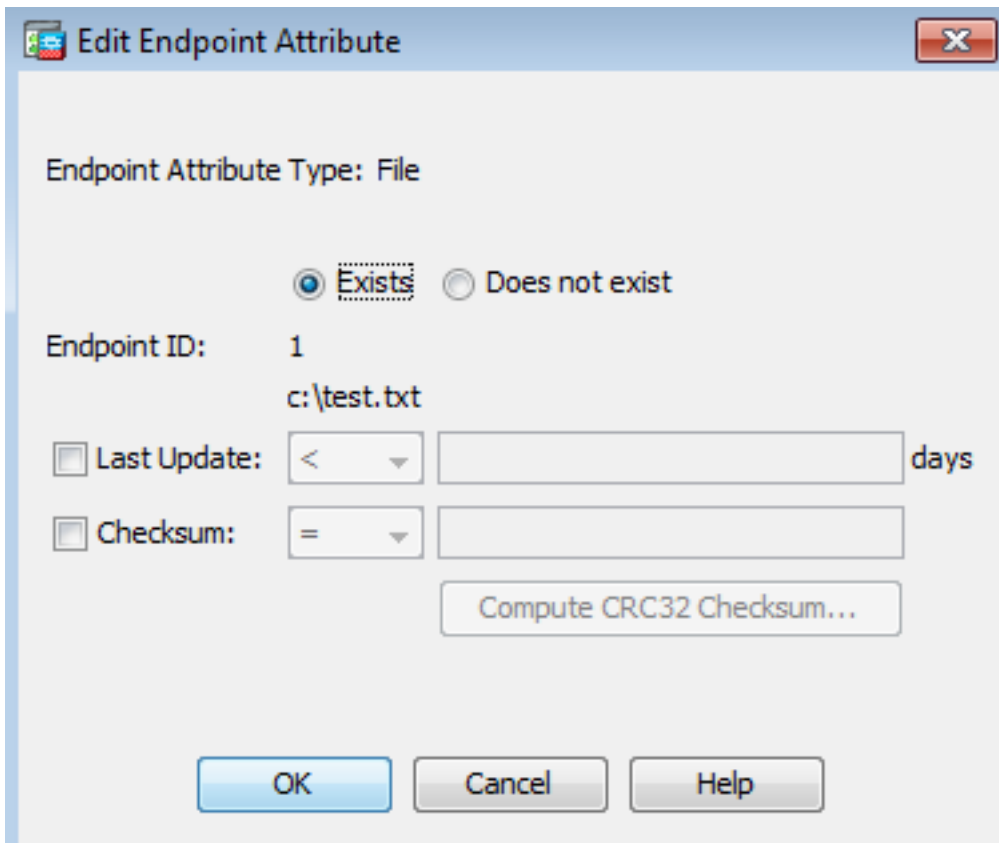
Action | Network ACL Filters (client) | Webtype ACL Filters (clientless) | Functions

Network ACLs

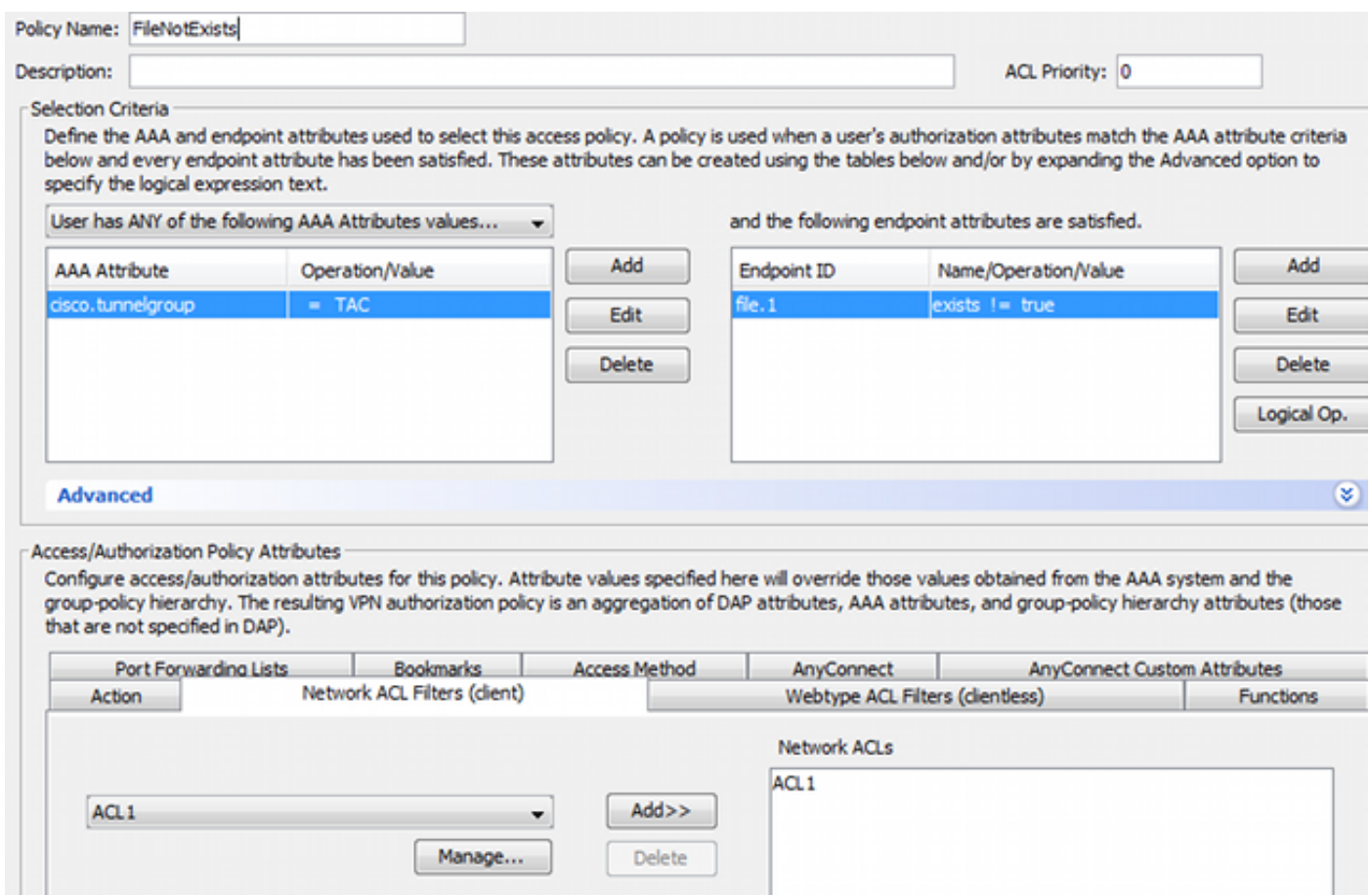
ACL1 | Add >> | Manage... | Delete

Como resultado, no se realiza ninguna acción con la configuración predeterminada para permitir la conectividad. No se utiliza ACL; se proporciona acceso completo a la red.

Los detalles de la comprobación de archivo son los que se muestran en la imagen.

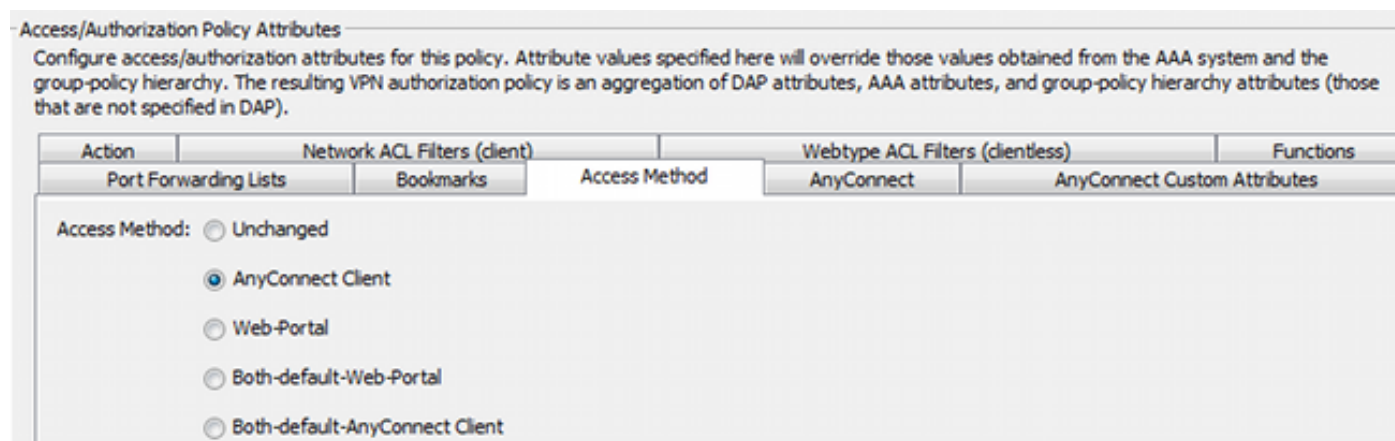


La segunda política (FileNotExists) es similar, pero esta condición temporal es **si el archivo no existe** como se muestra en la imagen.



El resultado tiene la lista de acceso ACL1 configurada. Esto se aplica a los usuarios de VPN que no cumplen con la normativa con el suministro de acceso limitado a la red.

Ambas políticas DAP impulsan el acceso **AnyConnect Client** como se muestra en la imagen.



ISE

ISE se utiliza para la autenticación de usuarios. Solo se deben configurar el dispositivo de red (ASA) y el nombre de usuario (cisco) correcto. Esta parte no se trata en este artículo.

Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

Aprovisionamiento de CSD y AnyConnect

Inicialmente, el usuario no se aprovisiona con el cliente AnyConnect. El usuario tampoco cumple con la política (el archivo `c:\test.txt` no existe). Ingrese <https://10.62.145.45> y el usuario se redirigirá inmediatamente para la instalación de CSD como se muestra en la imagen.



Cisco Secure Desktop



WebLaunch

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

Using ActiveX for Installation

Launching Cisco Secure Desktop.

If the software does not start properly, [Click here](#) to end the session cleanly.

Download

Esto se puede hacer con Java o ActiveX. Una vez instalado CSD, se informa como se muestra en la imagen.



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

A continuación, se redirige al usuario para la autenticación, como se muestra en la imagen.



Login

Please enter your username and password.

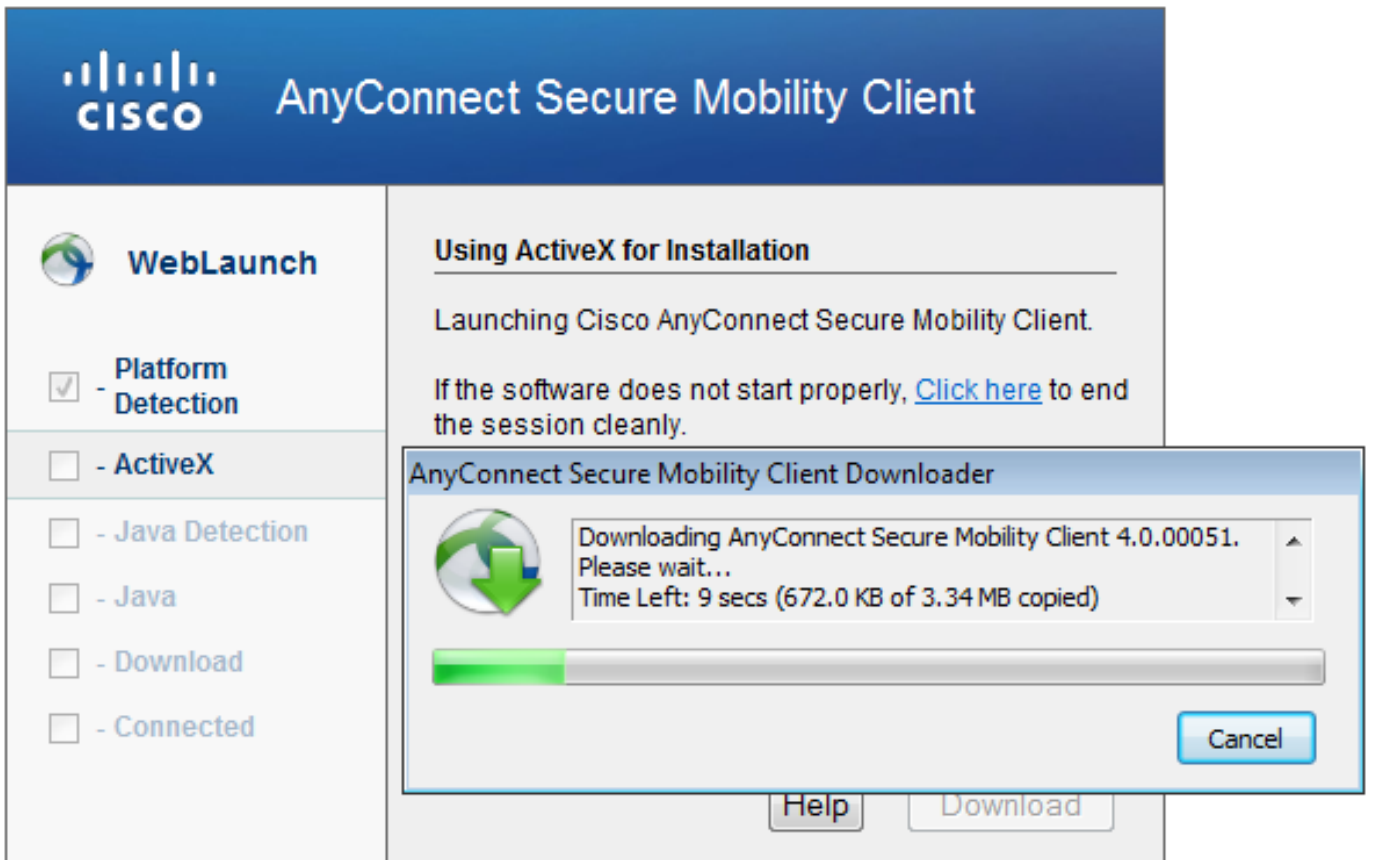
GROUP: TAC ▼

USERNAME:

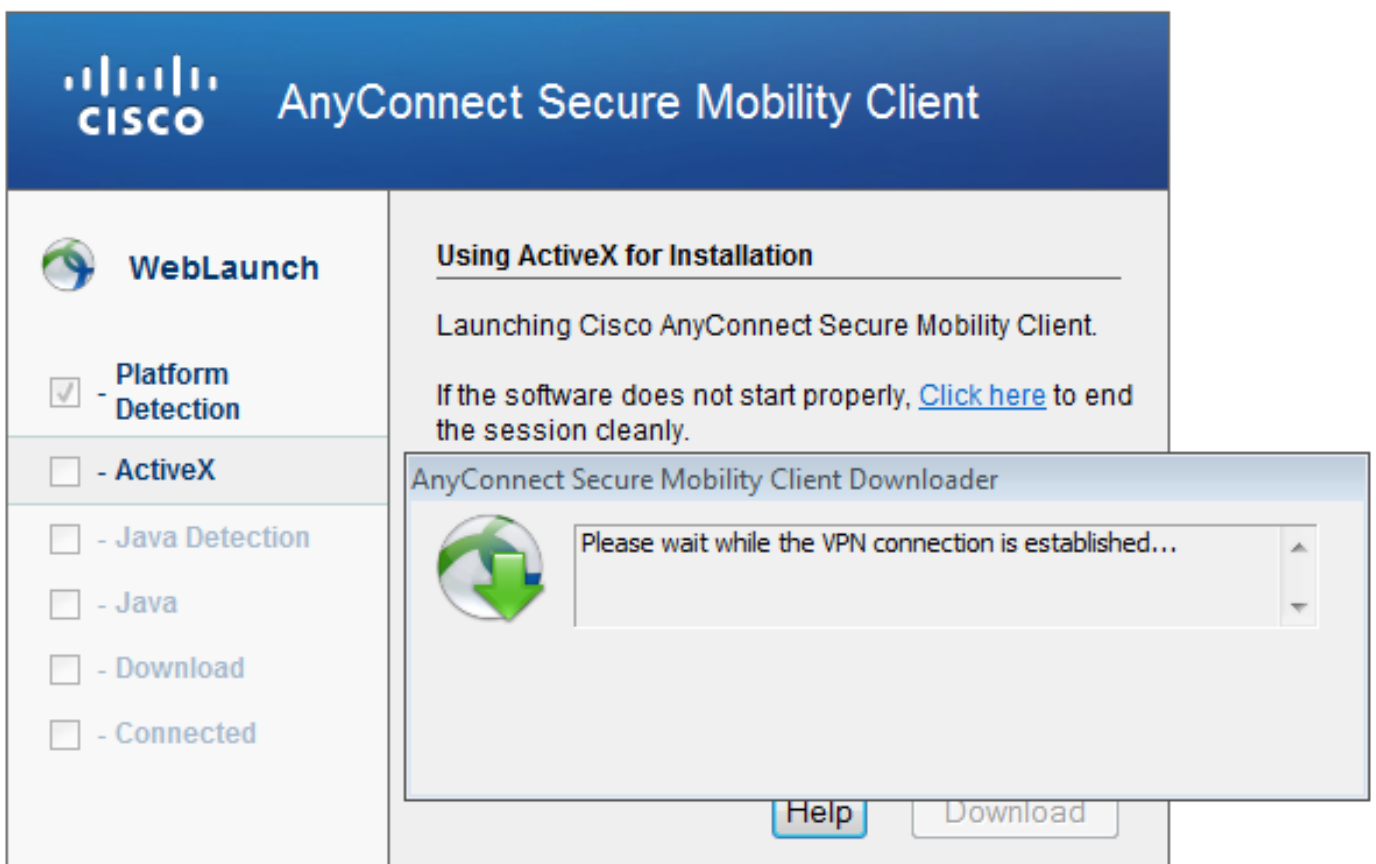
PASSWORD:

Login

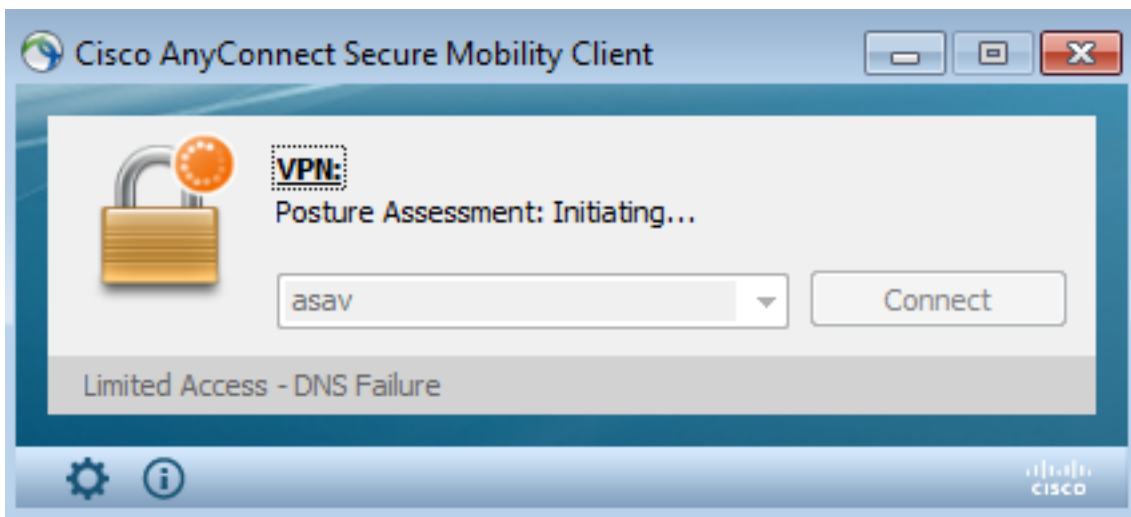
Si se realiza correctamente, se implementa AnyConnect junto con el perfil configurado; de nuevo, se puede utilizar ActiveX o Java, como se muestra en la imagen.



Además, la conexión VPN se establece como se muestra en la imagen.



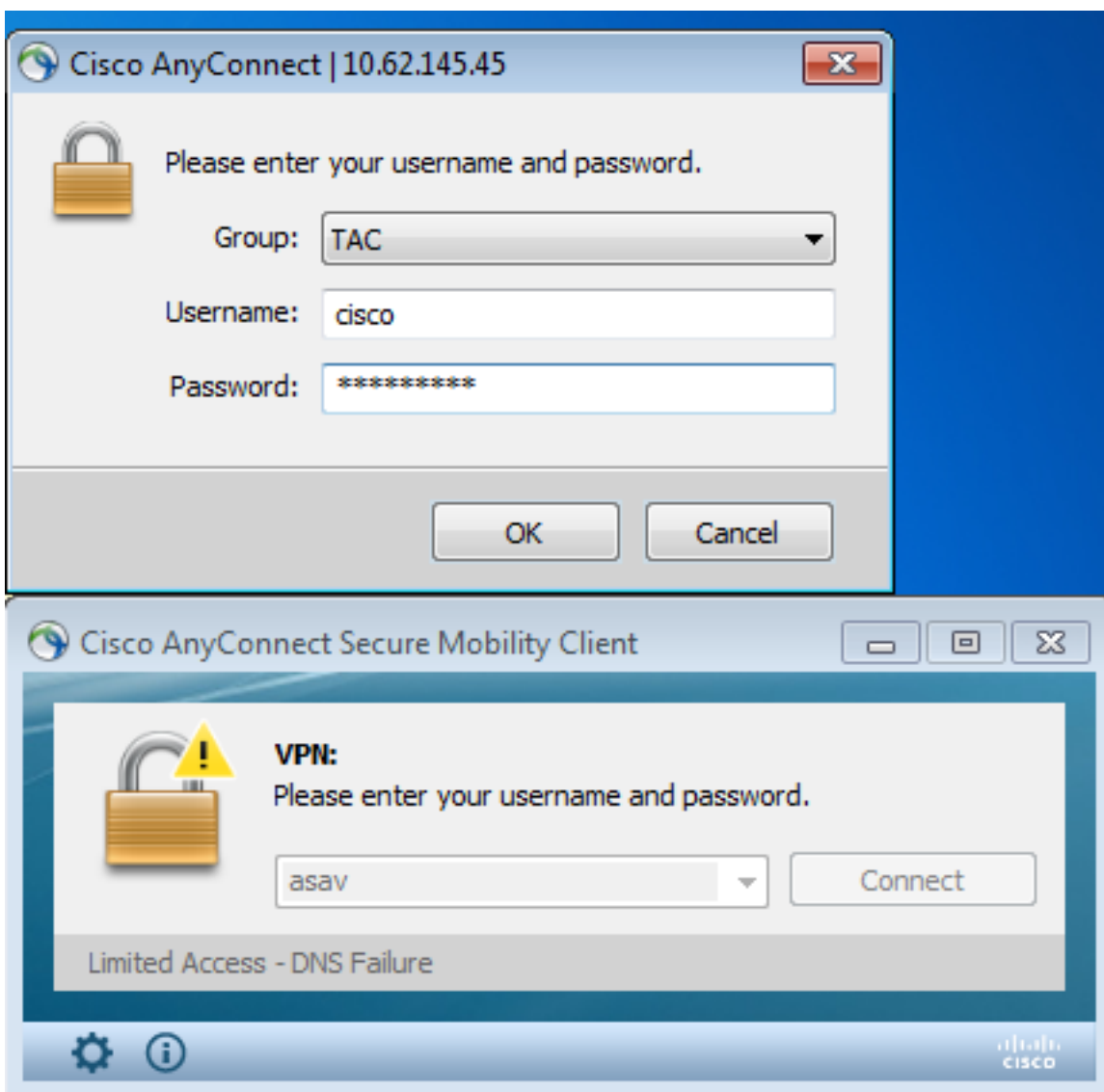
El primer paso para AnyConnect es realizar comprobaciones de estado (HostScan) y enviar los informes a ASA como se muestra en la imagen.



A continuación, AnyConnect autentica y finaliza la sesión VPN.

Sesión VPN de AnyConnect con estado: no conforme

Cuando establece una nueva sesión VPN con AnyConnect, el primer paso es el estado (HostScan) tal y como se presentó en la captura de pantalla anterior. Luego, se produce la autenticación y se establece la sesión VPN como se muestra en las imágenes.



ASA informa que se recibe el informe de HostScan:

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

A continuación, realiza la autenticación de usuario:

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

Y comienza la autorización para esa sesión VPN. Cuando tiene "debug dap trace 255" habilitado, la información con respecto a la existencia del archivo `c:\test.txt` se devuelve:

```
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"
```

Además, información con respecto a Microsoft Windows Firewall:

```
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"
```

Y Symantec AntiVirus (según las reglas de evaluación avanzada de punto final de HostScan configuradas anteriormente).

Como resultado, se compara la política DAP:

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

Esa política obliga a utilizar AnyConnect y también aplica la lista de acceso ACL1, que proporciona acceso restringido a la red para el usuario (que no cumple con la 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
```

Los registros también presentan extensiones ACIDEX que pueden ser utilizadas por la política DAP (o incluso pasadas en Solicitudes Radius a ISE y se utilizan en Reglas de Autorización como condiciones):

```
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, la sesión VPN está activa pero con acceso restringido a la red:

```
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
```

El historial de AnyConnect muestra los pasos detallados para el proceso de estado:

```
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.
```

Sesión VPN de AnyConnect con estado: compatible

Después de crear el archivo `c:\test.txt`, el flujo es similar. Una vez iniciada la nueva sesión de AnyConnect, los registros indican la existencia del archivo:

```
%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"
```

Y como resultado se utiliza otra política DAP:

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

La política no impone ninguna ACL como restricción para el tráfico de red.

Y la sesión está activa sin ninguna ACL (acceso completo a la red):

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

Además, Anyconnect informa que HostScan está inactivo y esperando la siguiente solicitud de escaneo:

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

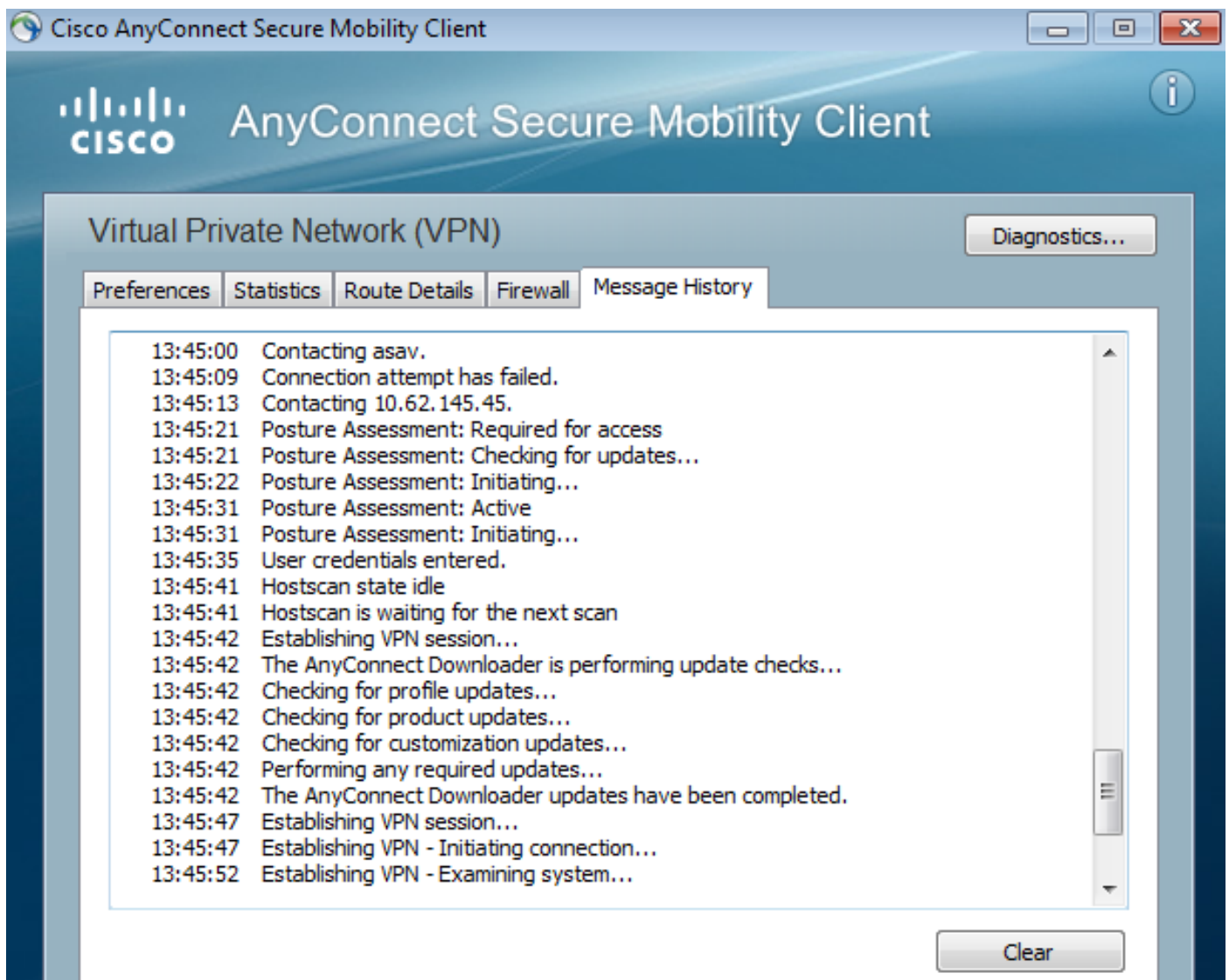
Nota: Para la reevaluación, se recomienda utilizar el módulo de estado integrado con ISE.

Troubleshoot

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

DART de AnyConnect

AnyConnect proporciona diagnósticos como se muestra en la imagen.



Que recopila y guarda todos los registros de AnyConnect en un archivo zip del escritorio. Ese archivo zip incluye los registros de Cisco AnyConnect Secure Mobility Client/Anyconnect.txt.

Esto proporciona información sobre ASA y solicita a HostScan que recopile datos:

```
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.

Luego, varios otros registros revelan que el CSD está instalado. Este es el ejemplo de un aprovisionamiento de CSD y de una conexión AnyConnect posterior junto con el estado:

```
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...
```

La comunicación entre ASA y AnyConnect está optimizada, ASA solicita para realizar solamente verificaciones específicas. AnyConnect descarga datos adicionales para poder realizar esto (por ejemplo, verificación AntiVirus específica).

Cuando abra el caso con el TAC, adjunte los registros Dart junto con "show tech" y "debug dap trace 255" desde ASA.

Información Relacionada

- [Configuración del análisis de host y del módulo de estado: Guía del administrador de Cisco AnyConnect Secure Mobility Client](#)
- [Servicios de estado en la guía de configuración de Cisco ISE](#)
- [Guía del administrador de Cisco ISE 1.3](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)