

ASA VPN-post configureren met CSD, DAP en AnyConnect 4.0

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[ASA](#)

[Stap 1. De configuratie van basis-SSL VPN](#)

[Stap 2: Installatie van CSD](#)

[Stap 3. Het DAP-beleid](#)

[ISE](#)

[Verifiëren](#)

[CSD en AnyConnect-provisioning](#)

[AnyConnect VPN-sessie met vertraging - niet conform](#)

[AnyConnect VPN-sessie met poster - conform](#)

[Problemen oplossen](#)

[AnyConnect DART](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe de positie van externe VPN-sessies die worden beëindigd op adaptieve security applicatie (ASA) moet worden uitgevoerd. De taak wordt lokaal uitgevoerd door ASA met het gebruik van Cisco Secure Desktop (CSD) met HostScan-module. Nadat een VPN-sessie is ingesteld, wordt een volgzzaam station volledige toegang tot het netwerk verleend terwijl het niet-conforme station beperkte toegang tot het netwerk heeft.

Daarnaast worden CSD- en AnyConnect 4.0-voorzieningsstromen gepresenteerd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco ASA VPN-configuratie
- Cisco AnyConnect beveiligde mobiliteit-client

Gebruikte componenten

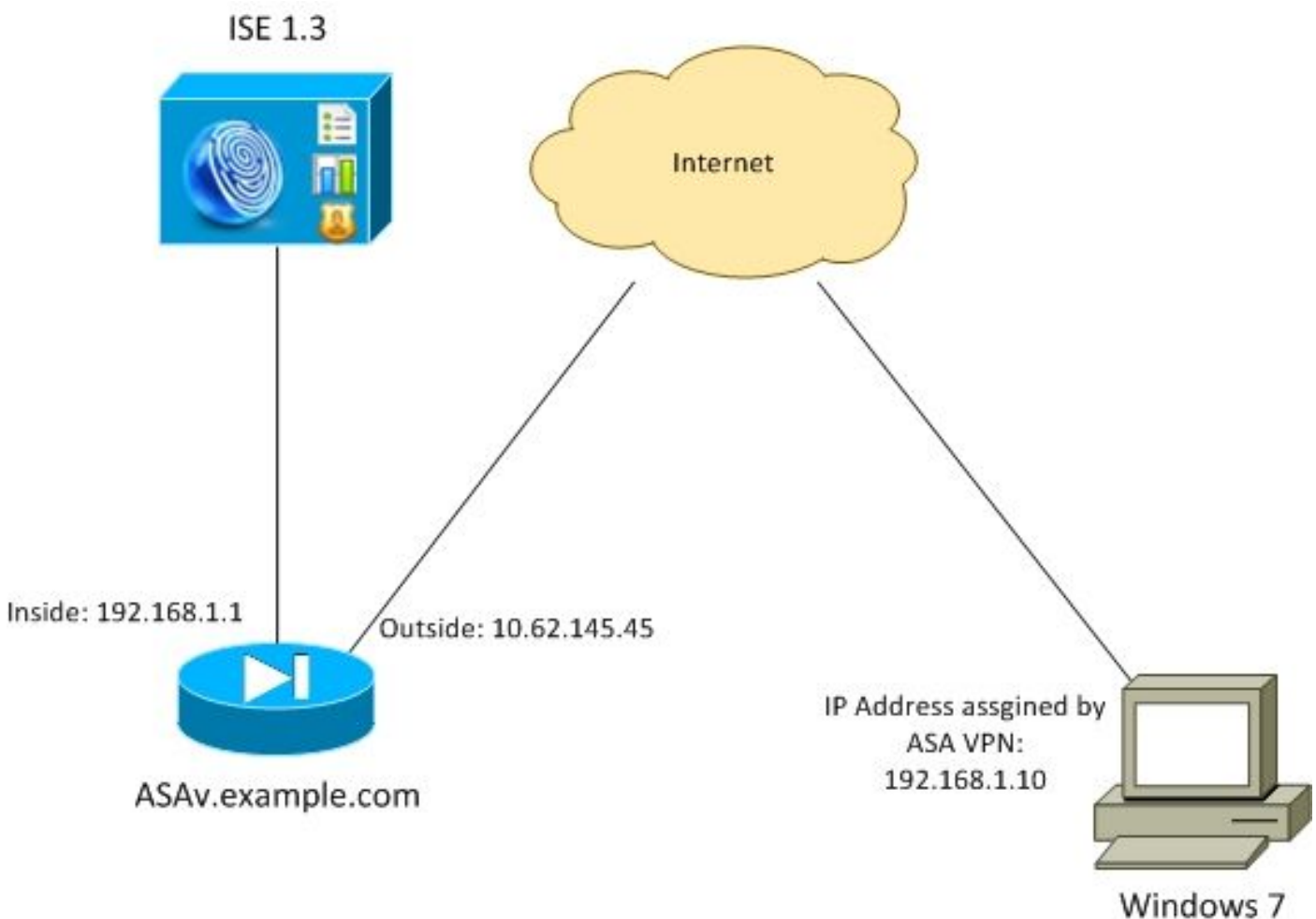
De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Microsoft Windows 7
- Cisco ASA, versie 9.3 of hoger
- Software voor Cisco Identity Services Engine (ISE), versies 1.3 en hoger
- Cisco AnyConnect Secure Mobility Client, versie 4.0 en hoger
- CSD, versie 3.6 of hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Configureren

Netwerkdigram



Ondernemingsbeleid is als volgt:

- Remote VPN-gebruikers die bestand **c:\test.txt** hebben (compatibel) moeten volledige netwerktoegang hebben tot interne bedrijfsmiddelen
- AfstandsVPN-gebruikers die geen bestand hebben **c:\test.txt** (niet-conform) moeten beperkte netwerktoegang hebben tot interne bedrijfsmiddelen: alleen toegang tot de herstelservers 1.1.1.1 wordt verleend.

Bestandsbestaan is het eenvoudigste voorbeeld. Elke andere aandoening (antivirus, antispysware,

proces, toepassing, registratie) kan worden gebruikt.

De stroom is als volgt:

- Remote-gebruikers hebben geen AnyConnect geïnstalleerd. Zij hebben toegang tot ASA-webpagina voor CSD en AnyConnect-provisioning (samen met het VPN-profiel)
- Zodra de verbinding via AnyConnect is voltooid, mogen niet-conforme gebruikers een beperkte netwerktoegang hebben. Dynamic Access Policy (DAP) **FileNotExists** worden genoemd.
- Gebruiker voert corrigerende maatregelen (handmatig installeren bestand **c:\test.txt**) uit en sluit deze opnieuw aan op AnyConnect. In dit geval wordt de volledige netwerktoegang geboden (het DAP-beleid dat **FileExists** wordt genoemd, wordt ook uitgevoerd).

U kunt de HostScan-module handmatig op het eindpunt installeren. Voorbeelden van bestanden (hostscan-win-4.0.0051-pre-implementatie-k9.msi) worden gedeeld op Cisco Connection Online (CCO). Maar het kan ook van ASA worden gedownload. HostScan is een onderdeel van CSD dat van ASA kan worden voorzien. Deze tweede benadering wordt in dit voorbeeld gebruikt.

Voor oudere versies van AnyConnect (3.1 en eerder) was er een afzonderlijk pakket beschikbaar op CCO (bijvoorbeeld: hostscan_3.1.06073-k9.pkg), die afzonderlijk op ASA hadden kunnen worden ingesteld en ingesteld (met opdracht **csd hostscan-afbeelding**), maar die optie bestaat niet meer voor AnyConnect versie 4.0.

ASA

Stap 1. De configuratie van basis-SSL VPN

ASA is ingesteld met Secure Remote VPN-toegang (Secure Socket 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

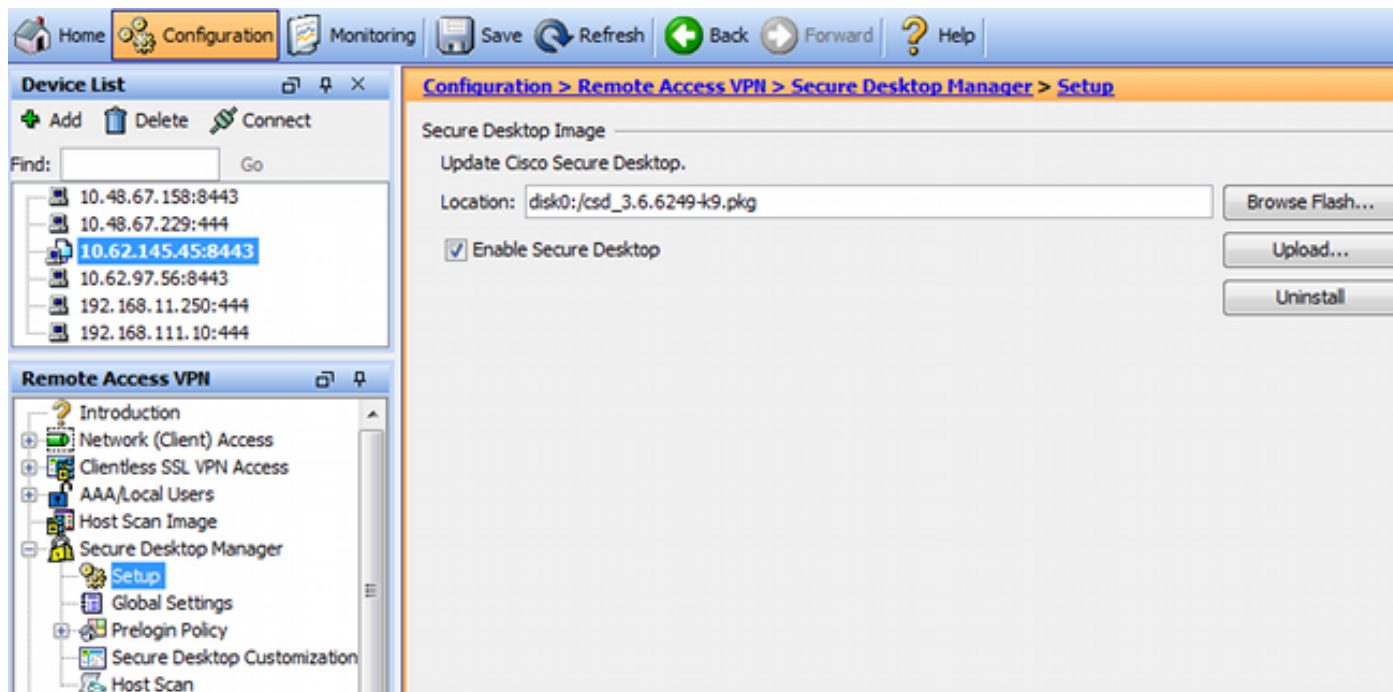
ip local pool POOL 192.168.1.10-192.168.1.20 mask 255.255.255.0

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

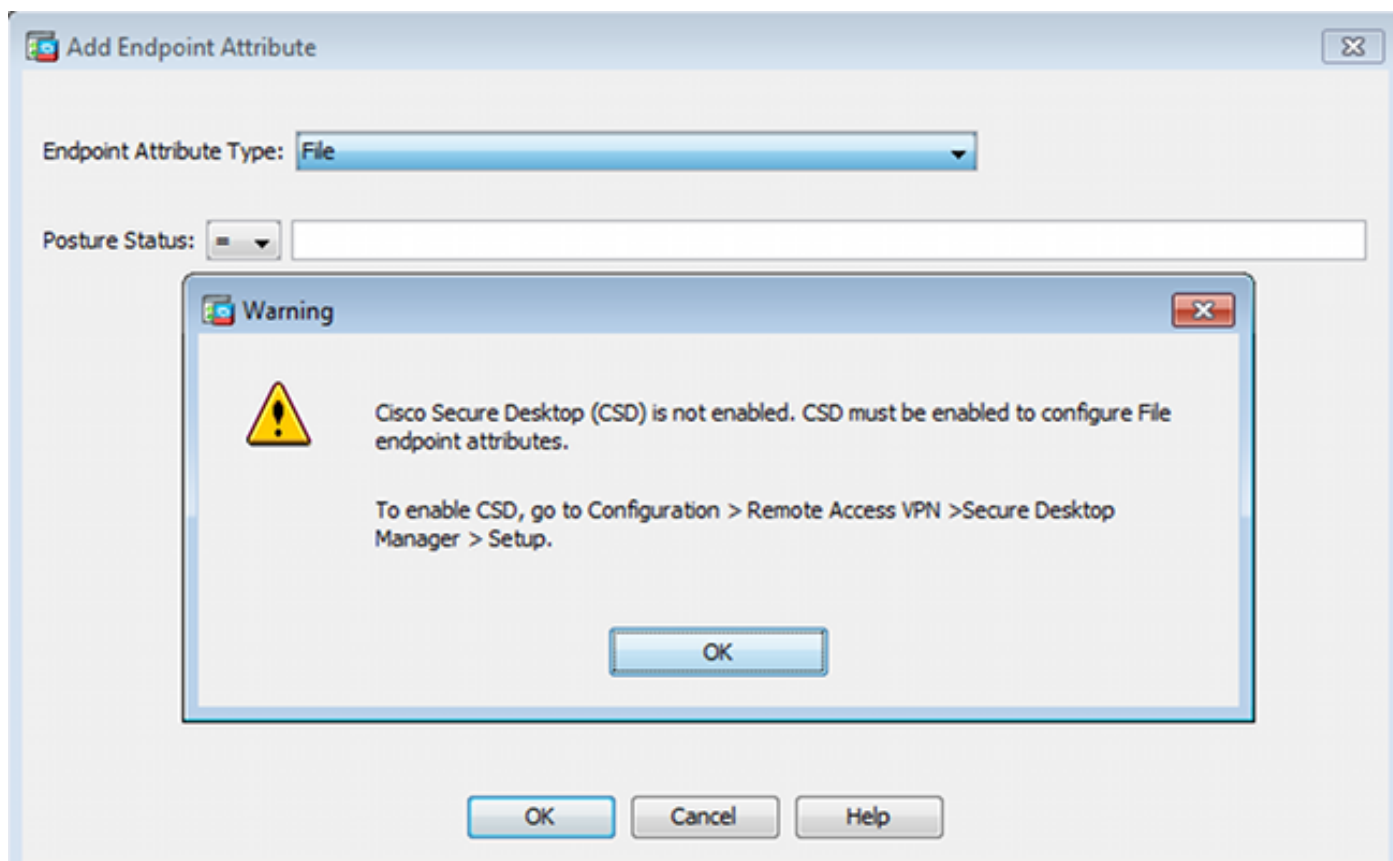
AnyConnect-pakket is gedownload en gebruikt.

Stap 2: Installatie van CSD

De volgende configuratie wordt uitgevoerd met Adaptieve Security Devices Manager (ASDM). Het CSD-pakket moet worden gedownload om te knippen en rekening te houden met de configuratie zoals weergegeven in de afbeelding.



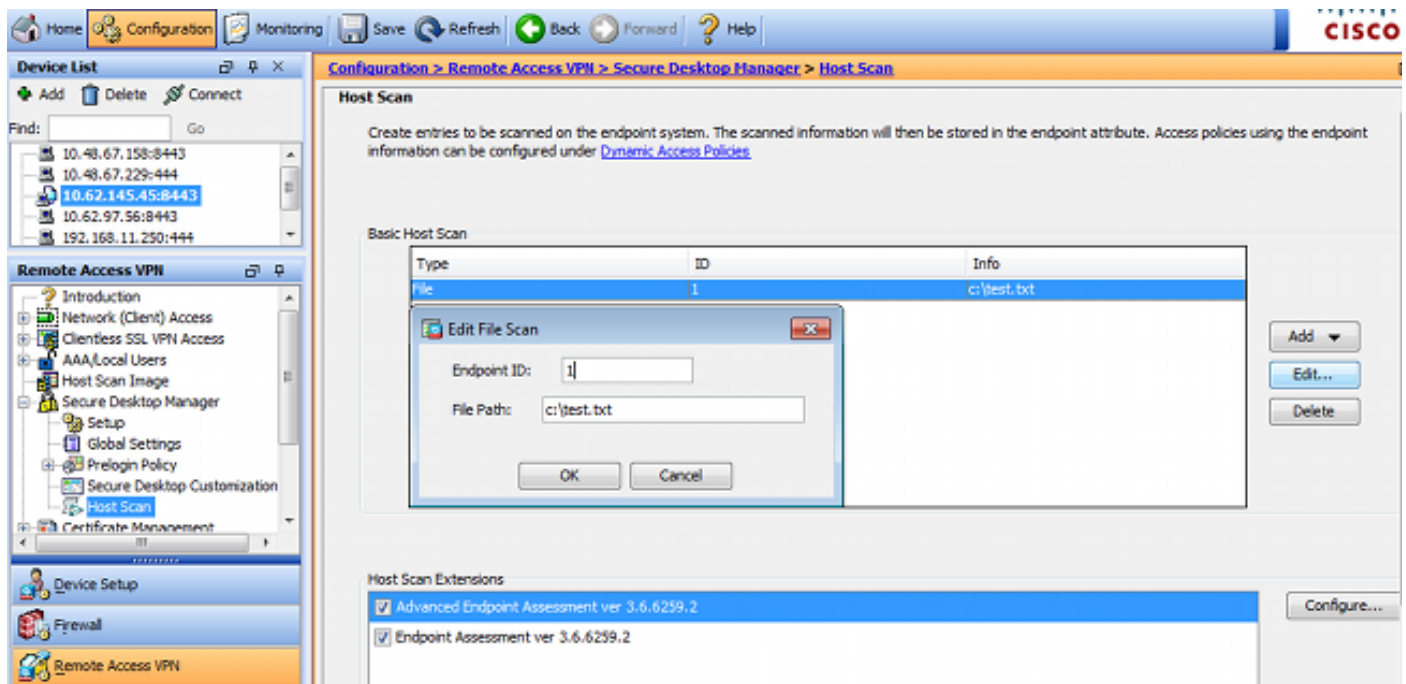
Zonder beveiligde desktop in staat te stellen, zou het niet mogelijk zijn om CSD-eigenschappen te gebruiken in DAP-beleid zoals in de afbeelding wordt getoond.



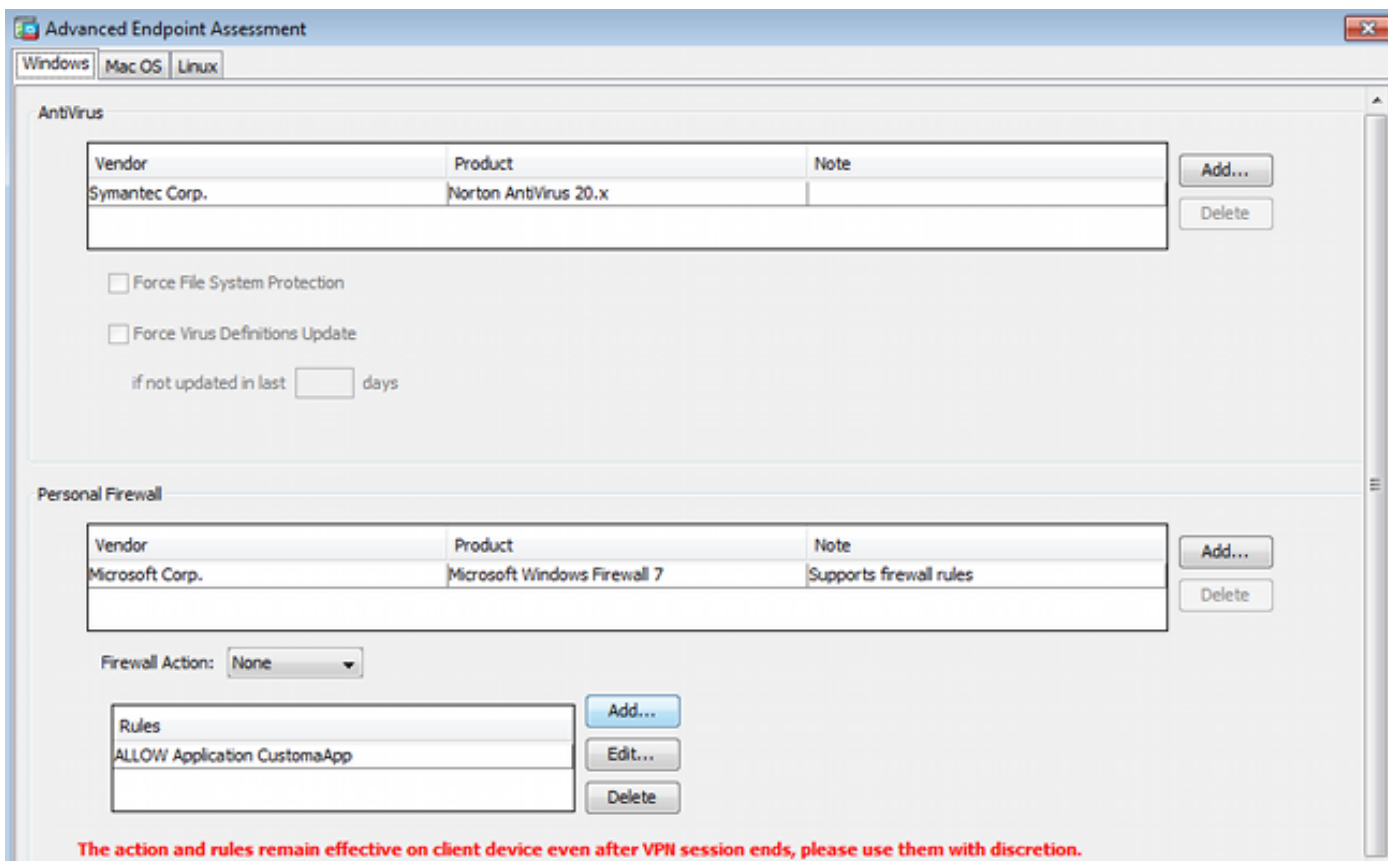
Nadat u CSD hebt ingeschakeld, verschijnen er meerdere opties onder Secure Desktop Manager.

Opmerking: Informeer dat sommige van deze al zijn afgekeurd. Meer informatie over de afgekeurde kenmerken is te vinden op: [Kennissegeving van functievermindering voor beveiligde desktop \(Vault\), cache-reiniger, trapezium-herkenning en host-Emulation-detectie](#)

HostScan wordt nog steeds volledig ondersteund, er wordt een nieuwe Basic HostScan-regel toegevoegd. Het bestaan van `c:\test.txt` wordt geverifieerd zoals in de afbeelding wordt getoond.



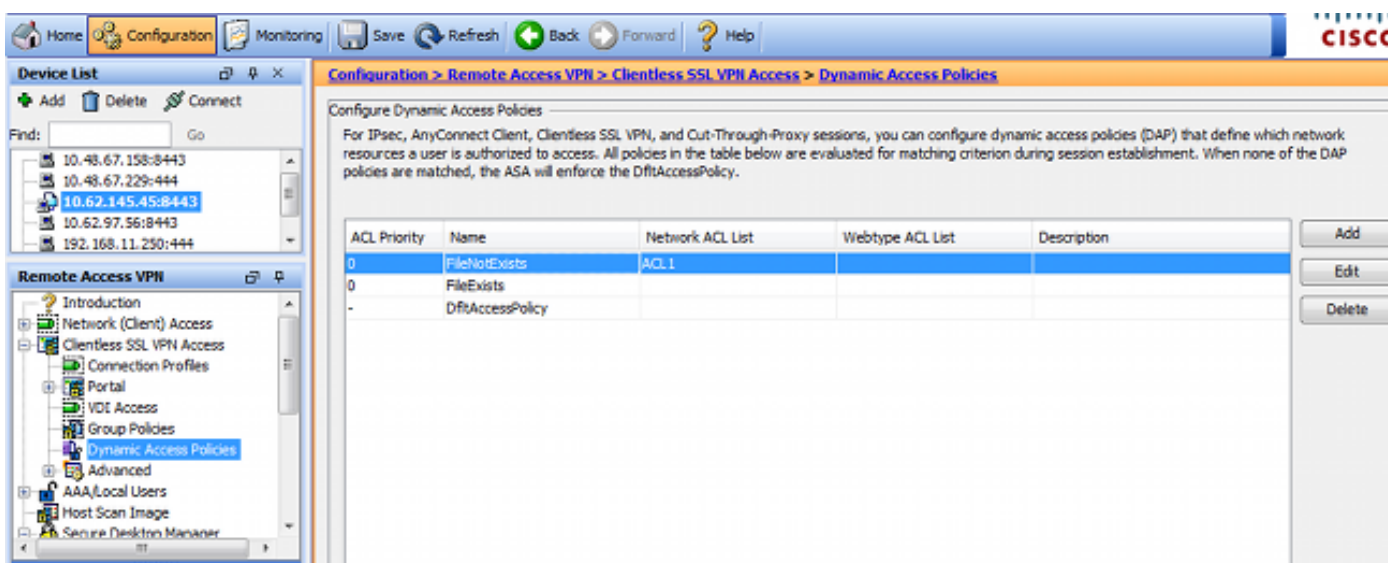
Bovendien wordt er een extra regel voor Advanced Endpoint Assessment toegevoegd zoals in de afbeelding.



Dat je controleert of er Symantec Norton AntiVirus 20.x en Microsoft Windows Firewall 7 bestaat. Postmodule (HostScan) controleert deze waarden, maar er wordt geen controle uitgevoerd (dat wordt niet geverifieerd door het DAP-beleid).

Stap 3. Het DAP-beleid

Het DAP-beleid is verantwoordelijk voor het gebruik van de gegevens die door HostScan worden verzameld, als voorwaarden, en voor het toepassen van specifieke eigenschappen op de VPN-sessie. Om het DAP-beleid van ASDM te maken, navigeer dan naar **Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policy** zoals in de afbeelding.



Eerste beleid (FileExists) controleert tunnelgroepnaam die door het geconfigureerde VPN-profiel wordt gebruikt (VPN-profielconfiguratie is voor helderheid weggelaten). Vervolgens wordt extra controle voor het bestand c:\test.txt uitgevoerd zoals in de afbeelding.

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

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

ACL 1

Als resultaat hiervan worden er geen acties uitgevoerd met de standaardinstelling om connectiviteit toe te staan. Geen ACL wordt gebruikt - volledige netwerktoegang wordt geboden.

Details voor de bestandscontrole zijn weergegeven in de afbeelding.

Edit Endpoint Attribute

Endpoint Attribute Type: File

Exists Does not exist

Endpoint ID: 1
 c:\test.txt

Last Update: < days

Checksum: =

Het tweede beleid (FileNotExists) is hetzelfde - maar deze tijdvoorwaarde is **gelijk als het bestand**

niet bestaat zoals in de afbeelding.

The screenshot shows the configuration 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 !=' and value 'true'. Below these tables are 'Add', 'Edit', and 'Delete' buttons. The 'Advanced' section is also visible, showing 'Access/Authorization Policy Attributes' with a dropdown menu set to 'ACL 1' and an 'Add >>' button.

Het resultaat is ingesteld op toegangslijst ACL1. Dat wordt toegepast voor niet-conforme VPN-gebruikers met beperkte netwerktoegang.

In beide DAP-beleidslijnen wordt naar **AnyConnect Client** toegang gevraagd zoals in de afbeelding wordt getoond.

The screenshot shows the 'Access/Authorization Policy Attributes' section. The 'Access Method' is set to 'AnyConnect Client' via radio buttons. Other options include 'Unchanged', 'Web-Portal', 'Both-default-Web-Portal', and 'Both-default-AnyConnect Client'. The 'Network ACL Filters (client)' tab is selected, and 'ACL 1' is visible in the dropdown menu.

ISE

ISE wordt gebruikt voor gebruikersverificatie. Alleen een netwerkapparaat (ASA) en de juiste gebruikersnaam (cisco) moeten worden ingesteld. Dit deel is niet in dit artikel opgenomen.

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

CSD en AnyConnect-provisioning

Aanvankelijk is de gebruiker niet voorzien van een AnyConnect-client. Gebruiker is ook niet compatibel met het beleid (het bestand `c:\test.txt` bestaat niet). Voer <https://10.62.145.45> in en de gebruiker wordt onmiddellijk opnieuw gericht voor CSD-installatie zoals in de afbeelding wordt getoond.



CISCO 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

Dat kan met Java of ActiveX worden gedaan. Zodra CSD is geïnstalleerd, wordt het gerapporteerd zoals in de afbeelding wordt weergegeven.



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

Vervolgens wordt de gebruiker opnieuw gericht op verificatie zoals in de afbeelding weergegeven.



Login

Please enter your username and password.

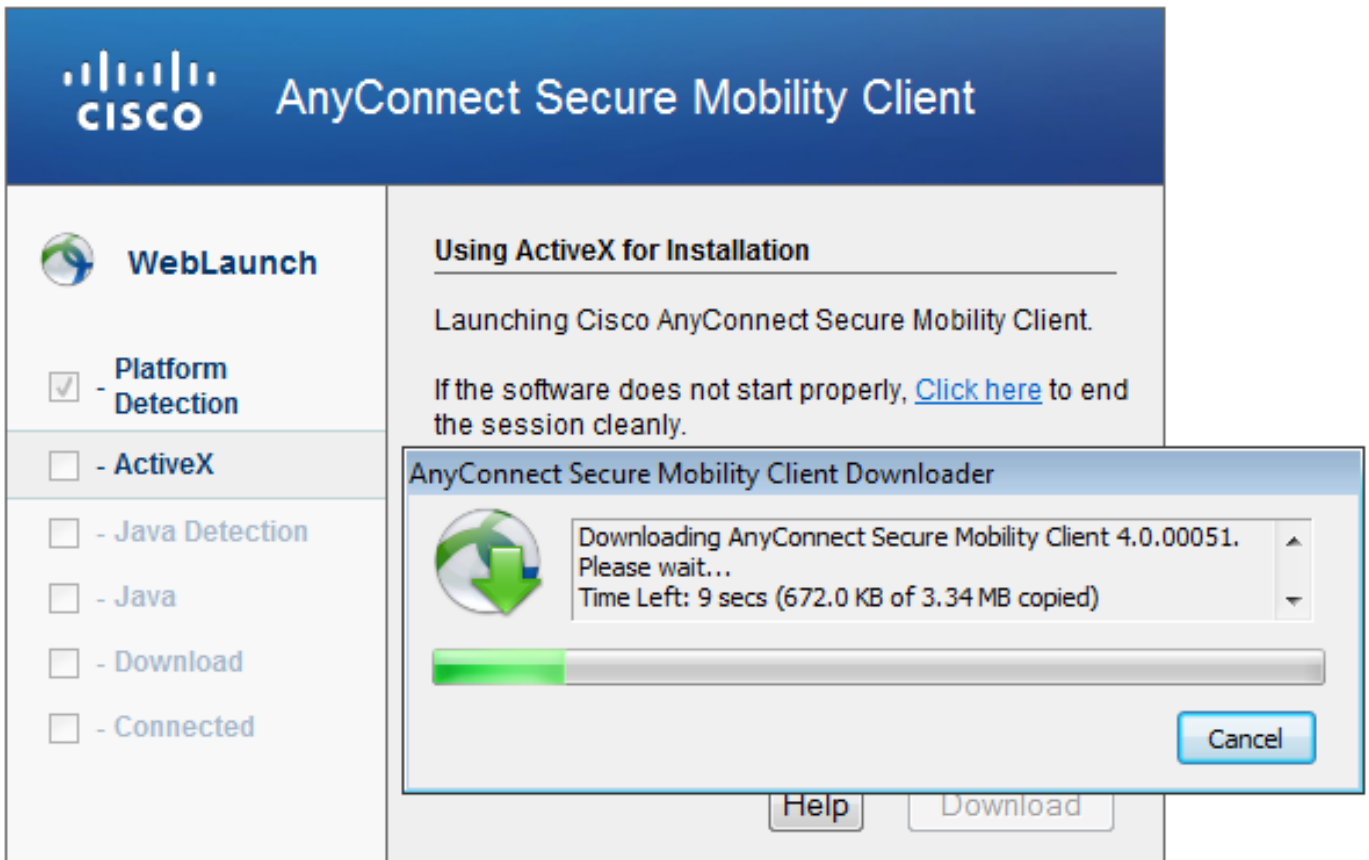
GROUP: TAC ▼

USERNAME:

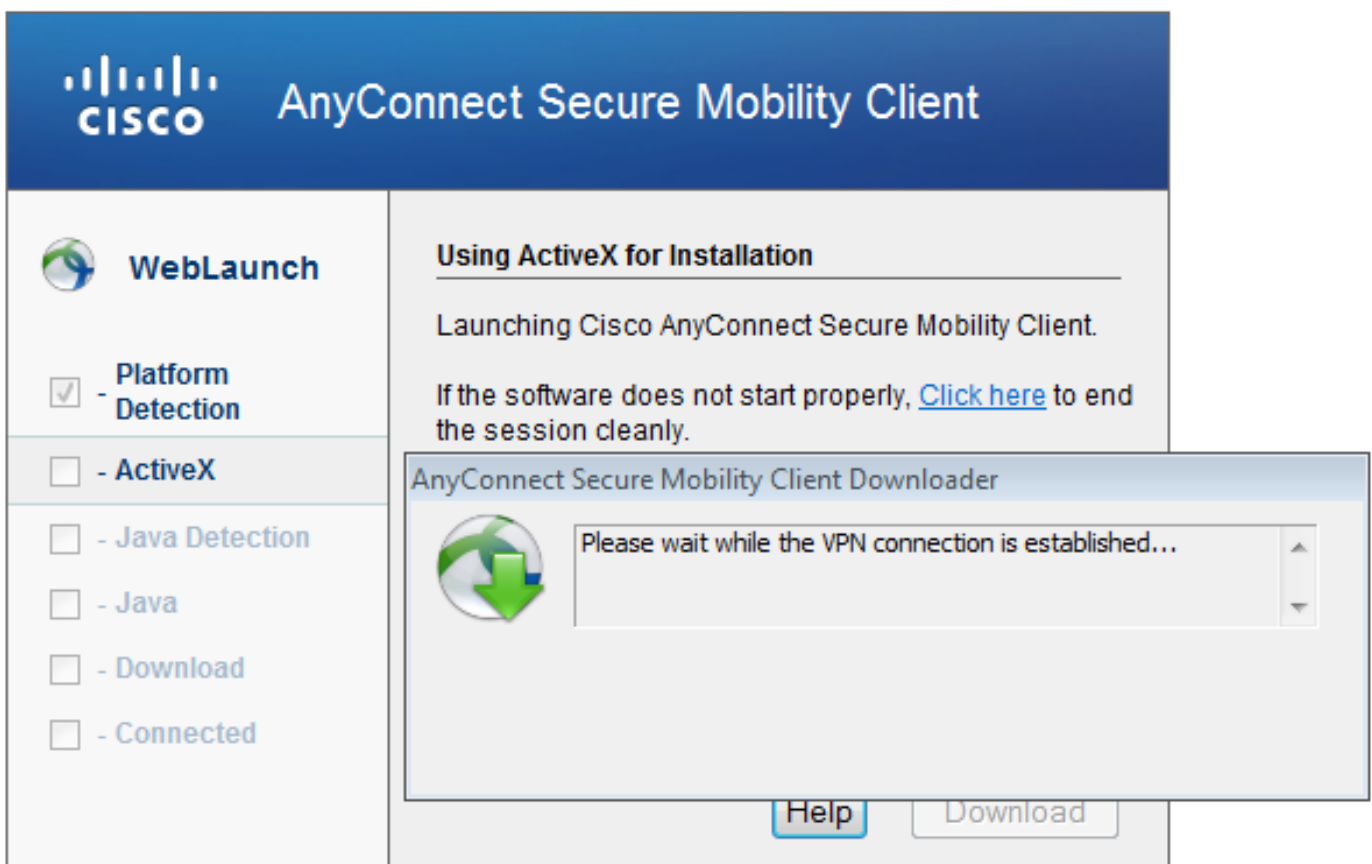
PASSWORD:

Login

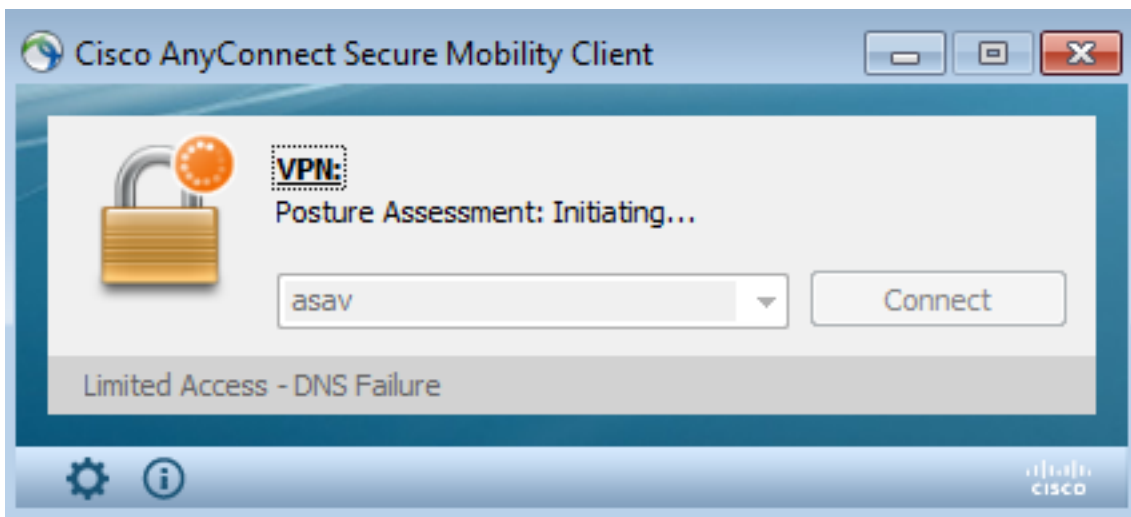
Indien geslaagd, wordt AnyConnect met het geconfigureerde profiel uitgevoerd - opnieuw ActiveX of Java kan worden gebruikt zoals in de afbeelding.



En de VPN verbinding wordt gevestigd zoals in de afbeelding.



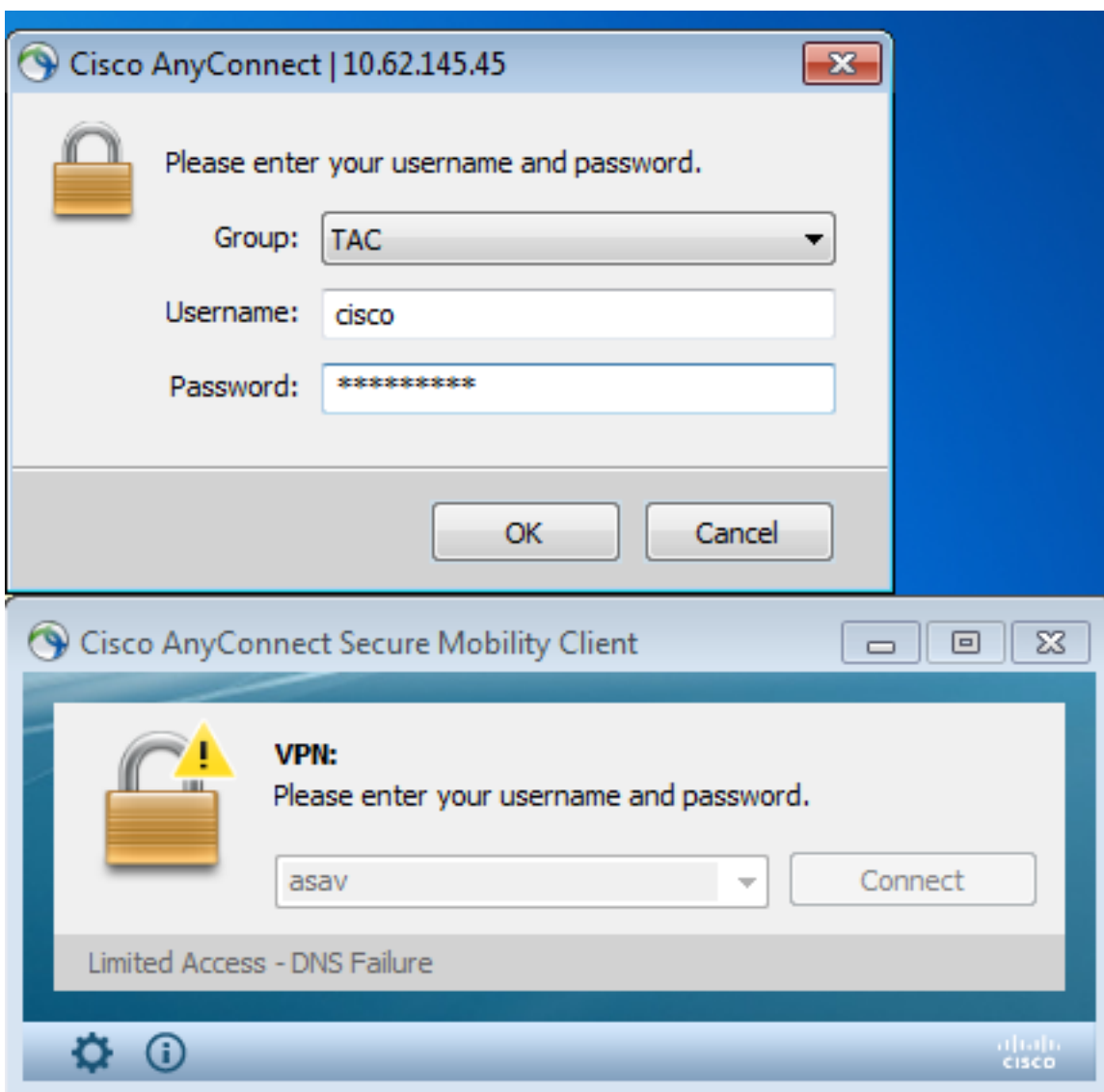
De eerste stap voor AnyConnect is het uitvoeren van postelcontroles (HostScan) en het doorsturen van de rapporten naar ASA zoals in de afbeelding.



Daarna maakt AnyConnect VPN-sessie echt en voltooid.

AnyConnect VPN-sessie met vertraging - niet conform

Wanneer u een nieuwe VPN-sessie maakt met AnyConnect, is de eerste stap de houding (HostScan) zoals deze eerder op het scherm wordt weergegeven. Vervolgens wordt verificatie uitgevoerd en wordt de VPN-sessie ingesteld zoals in de afbeeldingen wordt weergegeven.



ASA meldt dat HostScan rapport wordt ontvangen:

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

Daarna voert u gebruikersverificatie uit:

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

En start autorisatie voor die VPN sessie. Wanneer u "debug dap trace 255" hebt ingeschakeld, geeft u de informatie met betrekking tot het bestaan van `c:\test.txt`-bestand op:

```
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"
```

Raadpleeg ook informatie over 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"
```

En Symantec AntiVirus (volgens de HostScan Advanced Endpoint Assessment regels die eerder zijn ingesteld).

Het DAP-beleid is dus gelijk:

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

Dat beleid dwingt om AnyConnect te gebruiken en past ook ACL1 (toegangslijst) toe die beperkte netwerktoegang voor de gebruiker biedt (niet compatibel met het bedrijfsbeleid):

```
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, dflt: svc  
DAP_TRACE:3: action = continue  
DAP_TRACE:4: network-acl = ACL1
```

Logs presenteren ook ACIDEX-uitbreidingen die door het DAP-beleid kunnen worden gebruikt (of zelfs worden doorgegeven in Radius-aanvragen aan ISE en die als voorwaarden worden gebruikt in de machtigingsregels):

```
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";
```

Als resultaat hiervan is VPN sessie Up maar met de beperkte netwerktoegang:

```
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:  DTLSSv1.0              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
```

AnyConnect-historie toont gedetailleerde stappen voor het postuur:

```
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.
```

AnyConnect VPN-sessie met poster - conform

Nadat u `c:\test.txt`-bestand hebt gemaakt, is de stroom gelijk. Nadat de nieuwe AnyConnect-sessie is gestart, geven de logbestanden aan dat het bestand bestaat:

```
%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"
```

Als gevolg daarvan wordt een ander DAP-beleid gebruikt:

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

Het beleid legt geen ACL op als beperking voor het netwerkverkeer.

En de sessie is omhoog zonder enige ACL (volledige netwerktoegang):

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

Ook maakt AnyConnect melding dat HostScan niets doet en wacht op de volgende scanaanvraag:

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

Opmerking: Voor een herbeoordeling wordt aanbevolen een posteringsmodule te gebruiken die geïntegreerd is met ISE.

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

AnyConnect DART

AnyConnect biedt diagnostiek zoals in de afbeelding.



Hiermee verzamelt en slaat u alle AnyConnect-logbestanden op een zip-bestand op het bureaublad. Dat zip-bestand bevat de bestanden in Cisco AnyConnect Secure Mobility Client/Anyconnect.txt.

Dat geeft de informatie over ASA en vraagt HostScan om gegevens te verzamelen:

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.

Uit meerdere andere logbestanden blijkt dat CSD is geïnstalleerd. Dit is het voorbeeld voor een CSD-provisioning en volgende AnyConnect-verbinding samen met houding:

```
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...
```

De communicatie tussen ASA en AnyConnect wordt geoptimaliseerd, ASA verzoekt om alleen specifieke controles uit te voeren - AnyConnect downloads met aanvullende gegevens om dat te kunnen uitvoeren (bijvoorbeeld specifieke verificatie van het antivirus).

Wanneer u de case opent met TAC, sluit u Dart-logbestanden samen met "show tech" aan en "debug dap trace 255" uit ASA.

Gerelateerde informatie

- [Host Scan en de Postmodule configureren - Cisco AnyConnect Secure Mobility Client Administrator-gids](#)
- [Postservices op Cisco ISE Configuration Guide](#)
- [Cisco ISE 1.3 beheerdershandleiding](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)