

Konfigurieren des ASA VPN-Status mit CSD, DAP und AnyConnect 4.0

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[ASA](#)

[Schritt 1: Grundlegende SSL VPN-Konfiguration](#)

[Schritt 2: CSD-Installation](#)

[Schritt 3: DAP-Richtlinien](#)

[ISE](#)

[Überprüfen](#)

[CSD- und AnyConnect-Bereitstellung](#)

[AnyConnect VPN-Sitzung mit Status - nicht konform](#)

[AnyConnect VPN-Sitzung mit Status - konform](#)

[Fehlerbehebung](#)

[AnyConnect DART](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird beschrieben, wie Sie den Status für Remote-VPN-Sitzungen ausführen, die auf der Adaptive Security Appliance (ASA) terminiert werden. Die Statusüberprüfung wird lokal durch ASA mit Cisco Secure Desktop (CSD) mit HostScan-Modul durchgeführt. Nach Einrichtung einer VPN-Sitzung wird kompatiblen Station der vollständige Netzwerkzugriff gewährt, während nicht konforme Station nur eingeschränkten Netzwerkzugriff hat.

Außerdem werden CSD- und AnyConnect 4.0-Bereitstellungsabläufe dargestellt.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco ASA VPN-Konfiguration
- Cisco AnyConnect Secure Mobility Client

Verwendete Komponenten

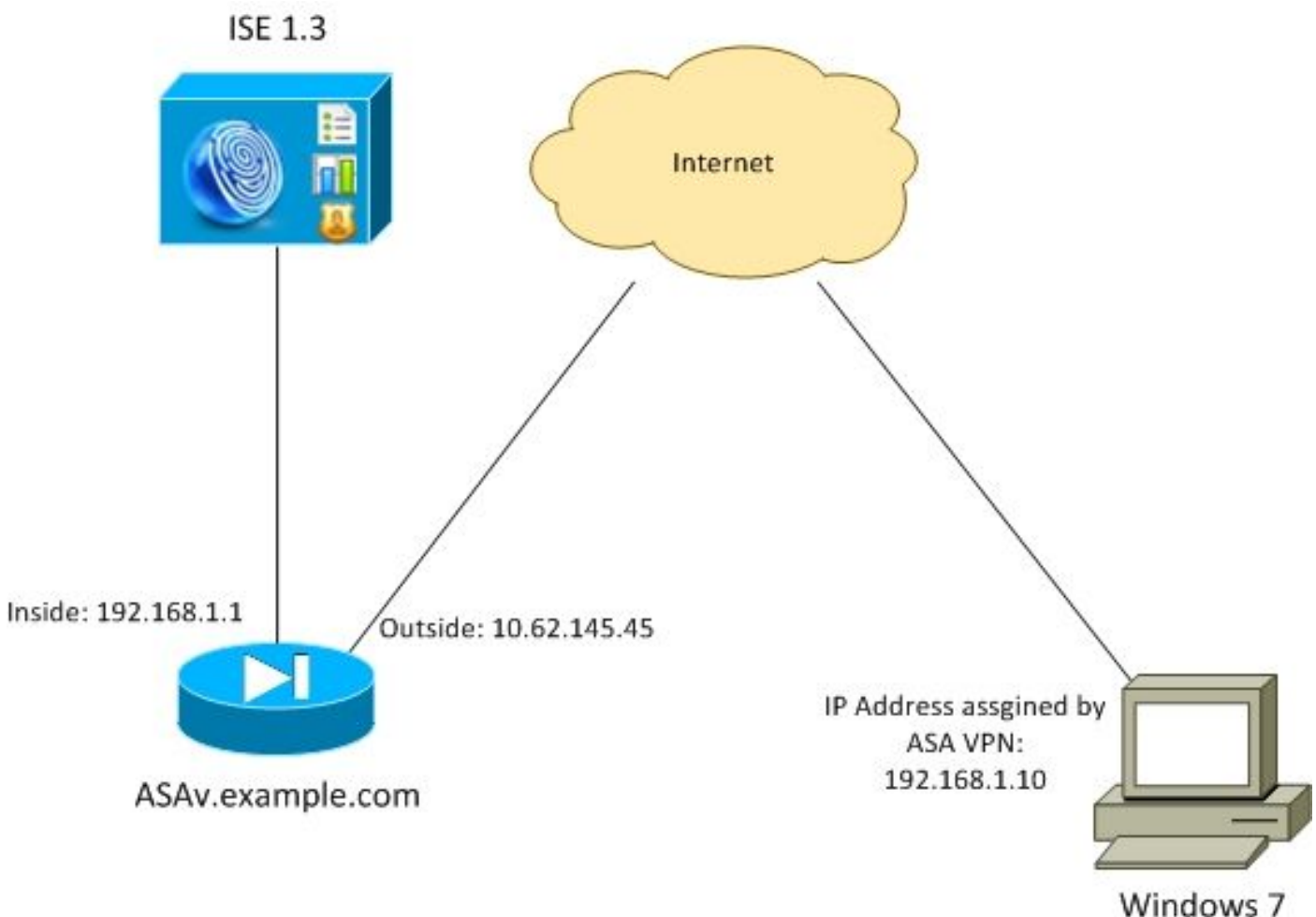
Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Microsoft Windows 7
- Cisco ASA, Version 9.3 oder höher
- Cisco Identity Services Engine (ISE)-Software, Versionen 1.3 und höher
- Cisco AnyConnect Secure Mobility Client, Version 4.0 und höher
- CSD, Version 3.6 oder höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Netzwerkdiagramm



Unternehmenspolitik:

- Remote-VPN-Benutzer mit Datei **c:\test.txt** (kompatibel) müssen vollständigen Netzwerkzugriff auf unternehmensinterne Ressourcen haben.
- Remote-VPN-Benutzer ohne Datei **c:\test.txt** (nicht konform) müssen eingeschränkten Netzwerkzugriff auf interne Unternehmensressourcen haben: Es wird nur Zugriff auf den Wiederherstellungsserver 1.1.1.1 gewährt.

Das einfachste Beispiel ist das Vorhandensein einer Datei. Alle anderen Bedingungen (Antivirus, Antispyware, Prozess, Anwendung, Registrierung) können verwendet werden.

Der Ablauf ist wie folgt:

- Remote-Benutzer haben AnyConnect nicht installiert. Sie greifen auf die ASA-Webseite für die CSD- und AnyConnect-Bereitstellung zu (zusammen mit dem VPN-Profil).
- Nach der Verbindung über AnyConnect sind nicht konforme Benutzer mit eingeschränktem Netzwerkzugriff zulässig. Dynamische Zugriffsrichtlinie (DAP) mit dem Namen **FileNotExists** wird zugeordnet.
- Der Benutzer führt die Problembehebung durch (manuelle Installation der Datei **c:\test.txt**) und stellt erneut eine Verbindung mit AnyConnect her. Diesmal wird ein vollständiger Netzwerkzugriff bereitgestellt (die DAP-Richtlinie **FileExists** heißt zugeordnet).

HostScan-Modul kann manuell auf dem Endgerät installiert werden. Beispieldateien (hostscan-win-4.0.00051-pre-deploy-k9.msi) werden auf Cisco Connection Online (CCO) freigegeben. Sie kann aber auch von der ASA übernommen werden. HostScan ist ein Teil des CSD, der von ASA bereitgestellt werden kann. Dieser zweite Ansatz wird in diesem Beispiel verwendet.

Für ältere Versionen von AnyConnect (3.1 und früher) war auf CCO ein separates Paket verfügbar (Beispiel: hostscan_3.1.06073-k9.pkg), die auf ASA separat konfiguriert und bereitgestellt werden konnte (mit dem Befehl **csd hostscan image**) - diese Option existiert jedoch nicht mehr für AnyConnect Version 4.0.

ASA

Schritt 1: Grundlegende SSL VPN-Konfiguration

ASA ist mit einfachem Remote-VPN-Zugriff (Secure Sockets Layer (SSL)) vorkonfiguriert:

```
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

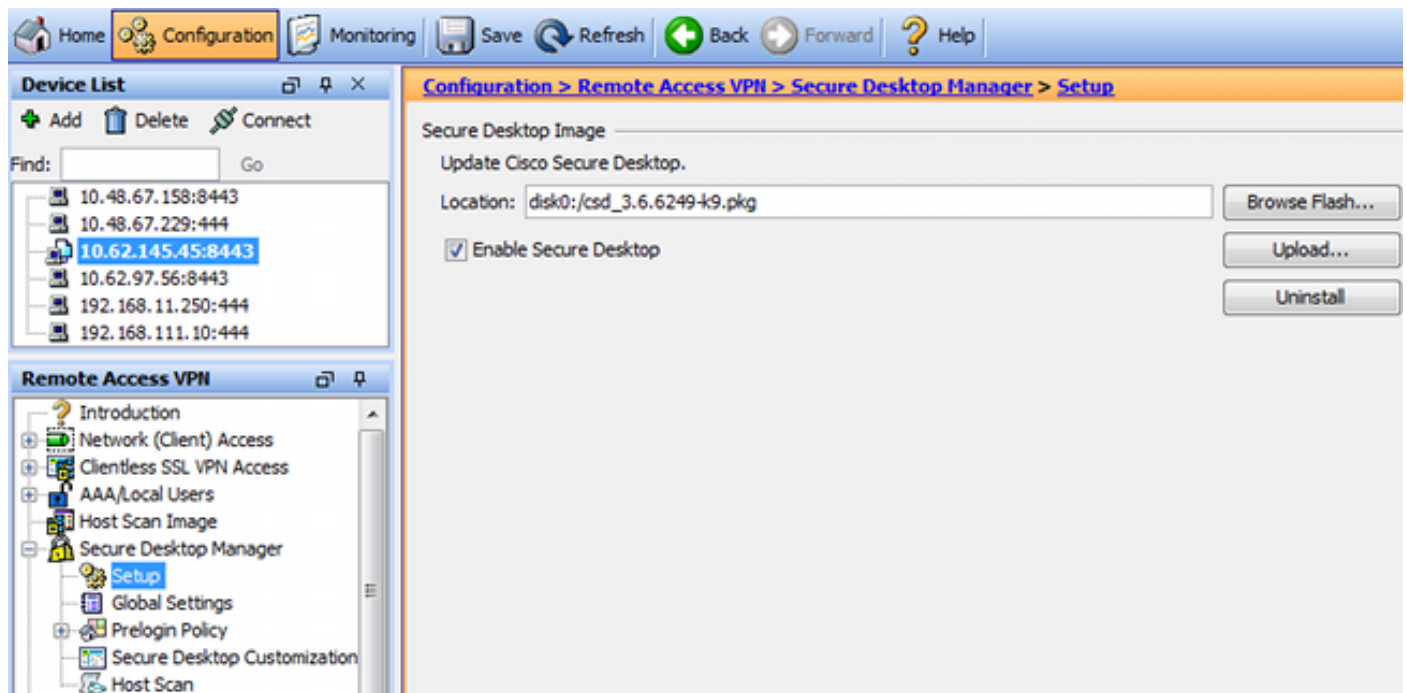
aaa-server ISE3 protocol radius
aaa-server ISE3 (inside) host 10.1.1.100
```

key *****

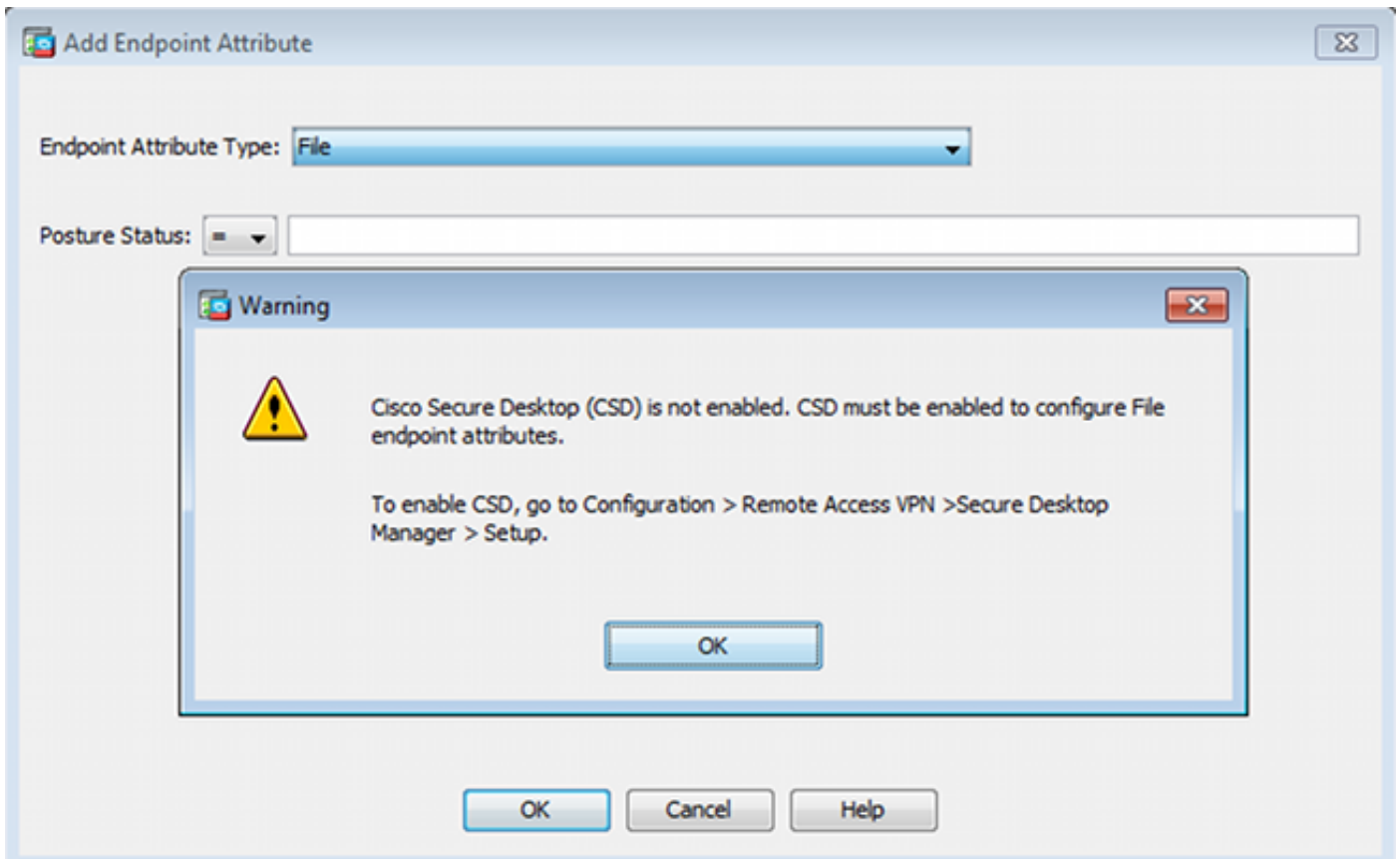
Das AnyConnect-Paket wurde heruntergeladen und verwendet.

Schritt 2: CSD-Installation

Die nachfolgende Konfiguration wird mit dem Adaptive Security Device Manager (ASDM) durchgeführt. Das CSD-Paket muss heruntergeladen werden, um zu flashen und auf die Konfiguration zu verweisen, wie im Bild gezeigt.



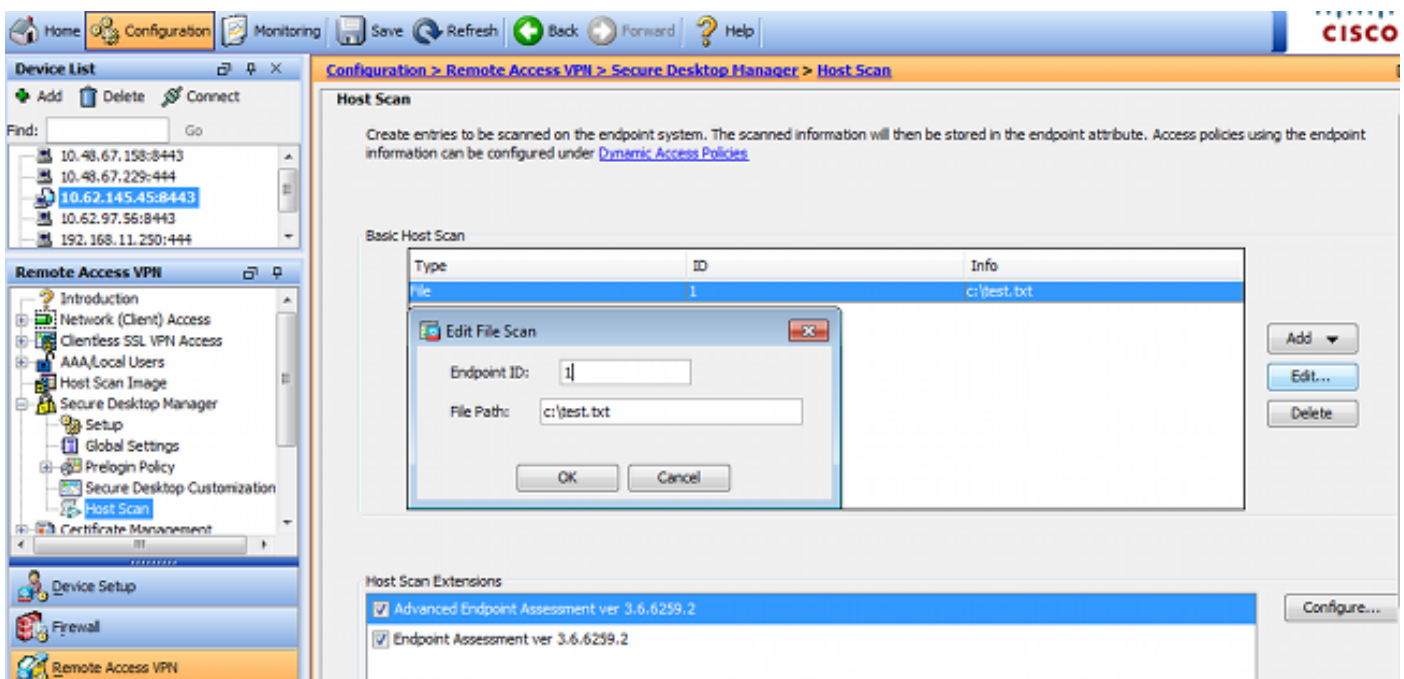
Ohne die Aktivierung von Secure Desktop wäre es nicht möglich, CSD-Attribute in DAP-Richtlinien zu verwenden, wie im Bild gezeigt.



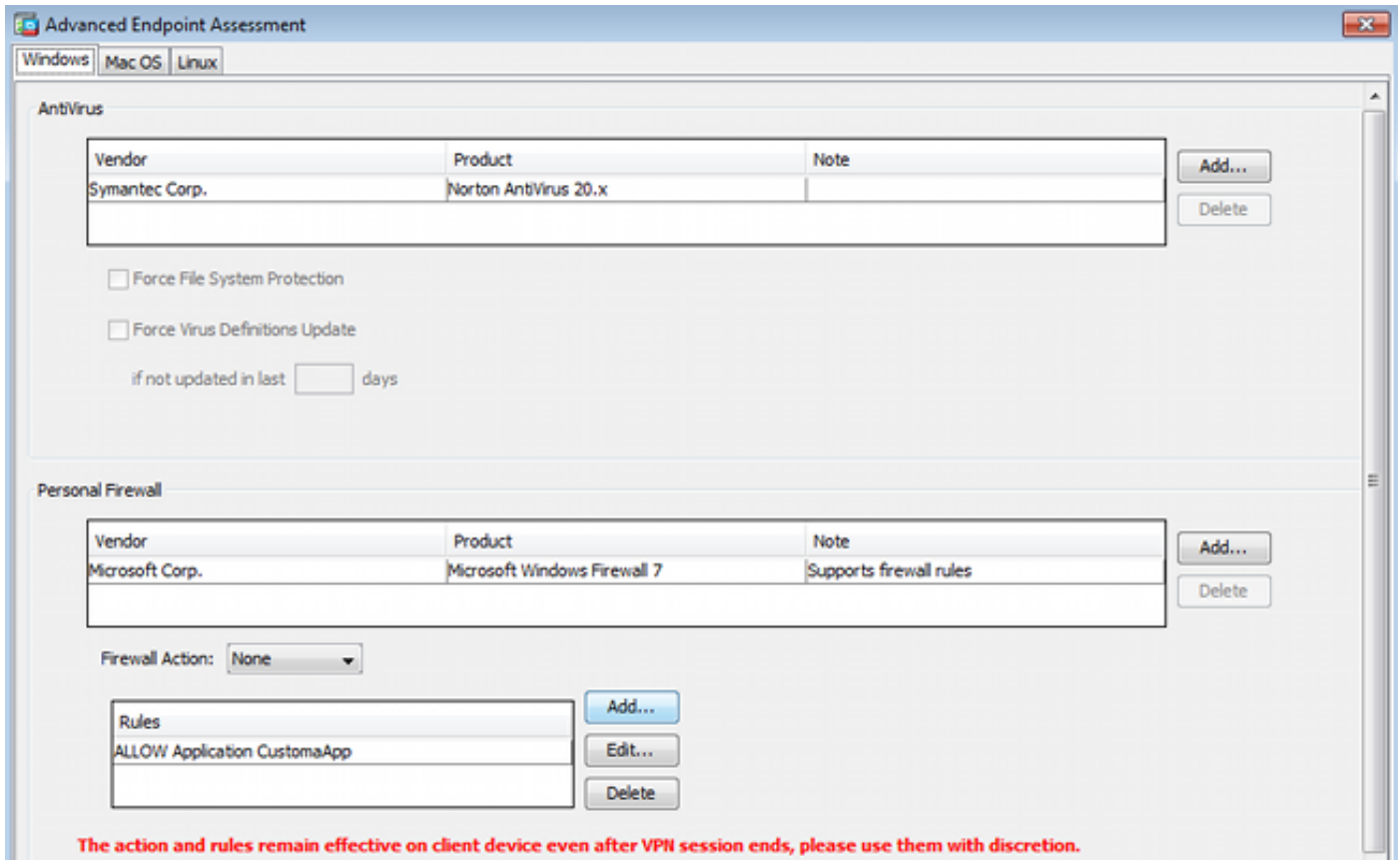
Nachdem Sie CSD aktiviert haben, werden unter Secure Desktop Manager mehrere Optionen angezeigt.

Hinweis: Seien Sie darüber informiert, dass einige von ihnen bereits veraltet sind. Weitere Informationen zu veralteten Funktionen finden Sie unter: [Hinweis zur Funktionsumwandlung für Secure Desktop \(Vault\), Cache Cleaner, Keystroke Logger Detection und Host Emulation Detection](#)

HostScan wird weiterhin vollständig unterstützt, die neue Standard HostScan-Regel wird hinzugefügt. Das Vorhandensein von `c:\test.txt` wird wie im Bild gezeigt überprüft.



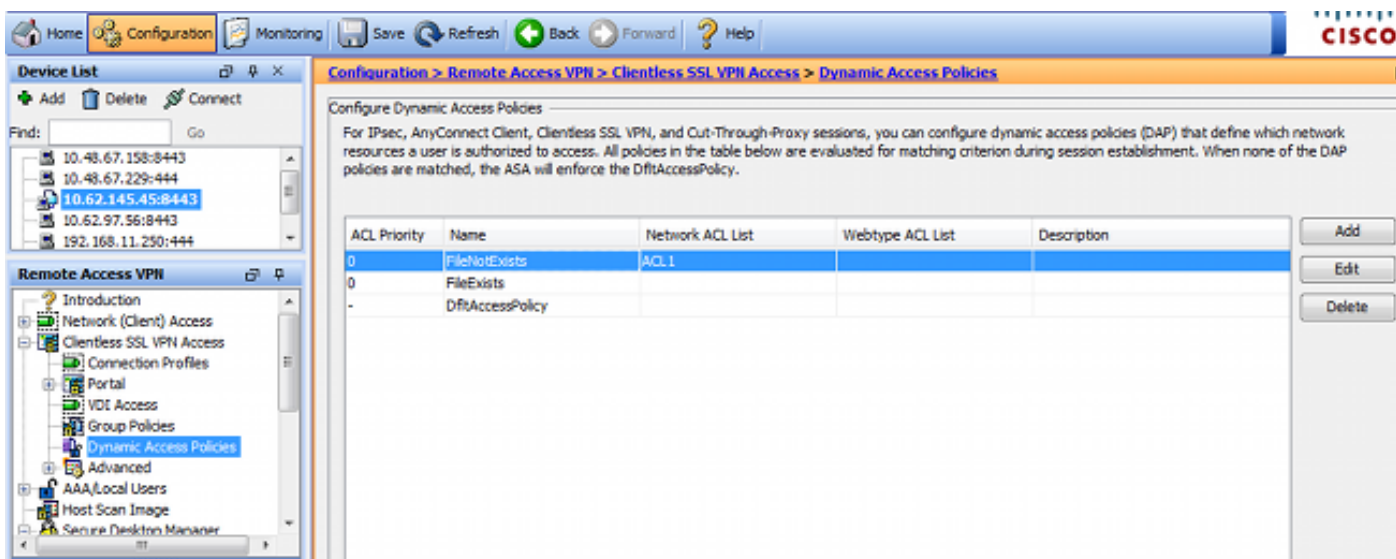
Darüber hinaus wird eine weitere Advanced Endpoint Assessment-Regel hinzugefügt, wie im Bild gezeigt.



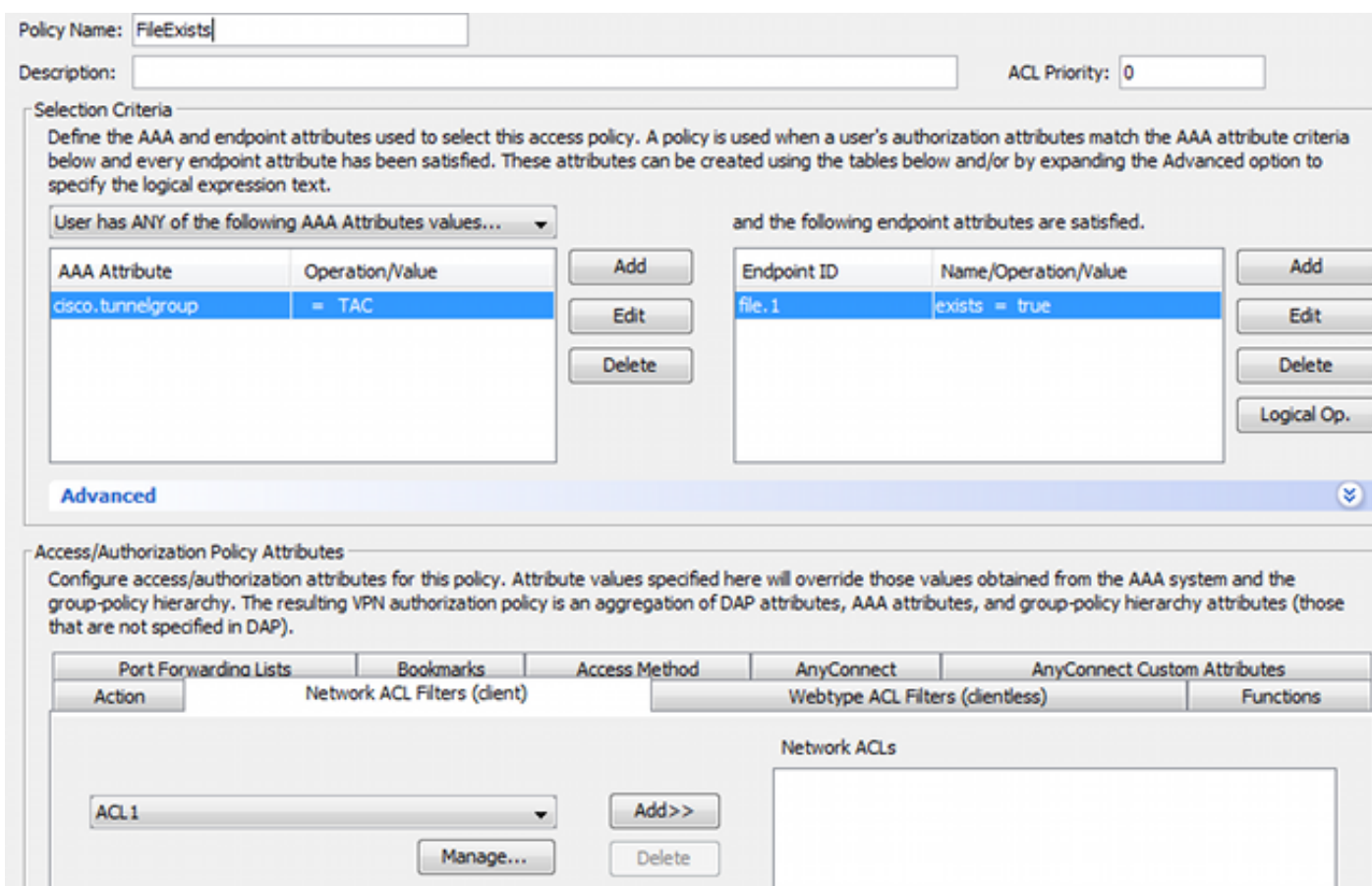
Diese prüft, ob Symantec Norton AntiVirus 20.x und Microsoft Windows Firewall 7 vorhanden sind. Das Posture Module (HostScan) überprüft diese Werte, aber es wird keine Durchsetzung gegeben (die DAP-Richtlinie überprüft dies nicht).

Schritt 3: DAP-Richtlinien

Die DAP-Richtlinien sind dafür verantwortlich, die von HostScan gesammelten Daten als Bedingungen zu verwenden und infolgedessen spezifische Attribute auf die VPN-Sitzung anzuwenden. Um eine DAP-Richtlinie von ASDM zu erstellen, navigieren Sie zu **Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies (Konfiguration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies (Dynamische Zugriffsrichtlinien)**, wie im Bild gezeigt.

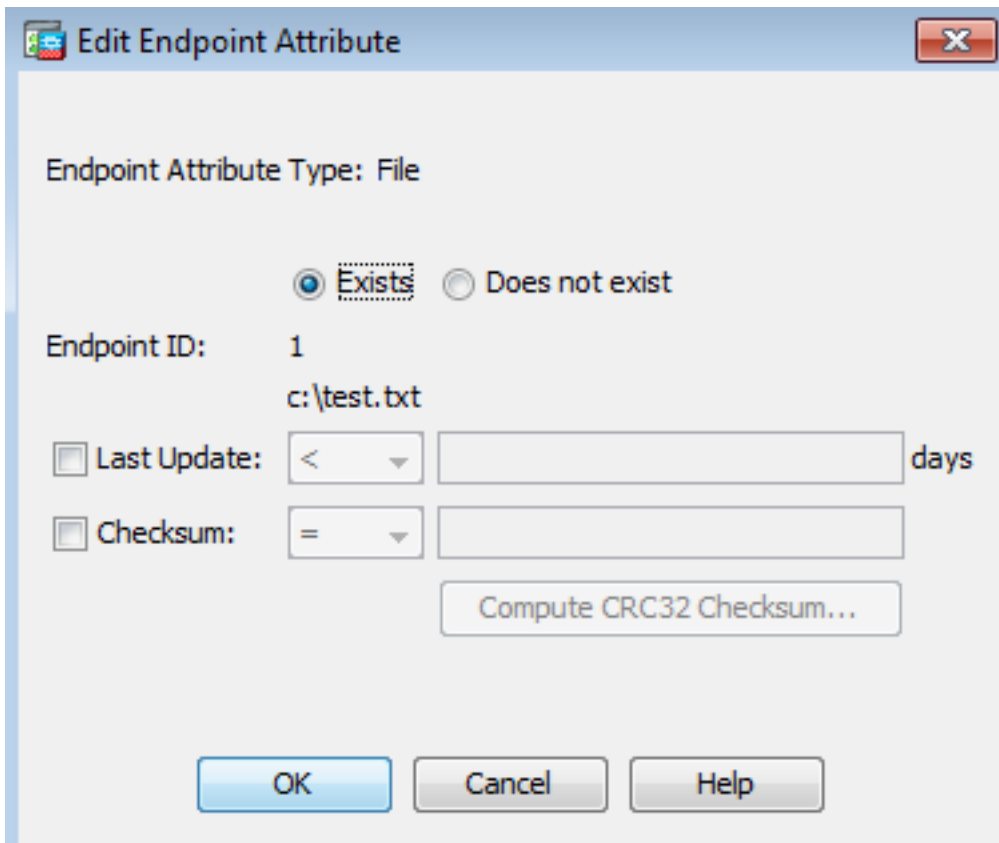


Die erste Richtlinie (FileExists) überprüft den Tunnelgruppennamen, der vom konfigurierten VPN-Profil verwendet wird (aus Gründen der Klarheit wurde die VPN-Profilkonfiguration weggelassen). Anschließend wird die Datei `c:\test.txt` wie im Bild gezeigt zusätzlich überprüft.

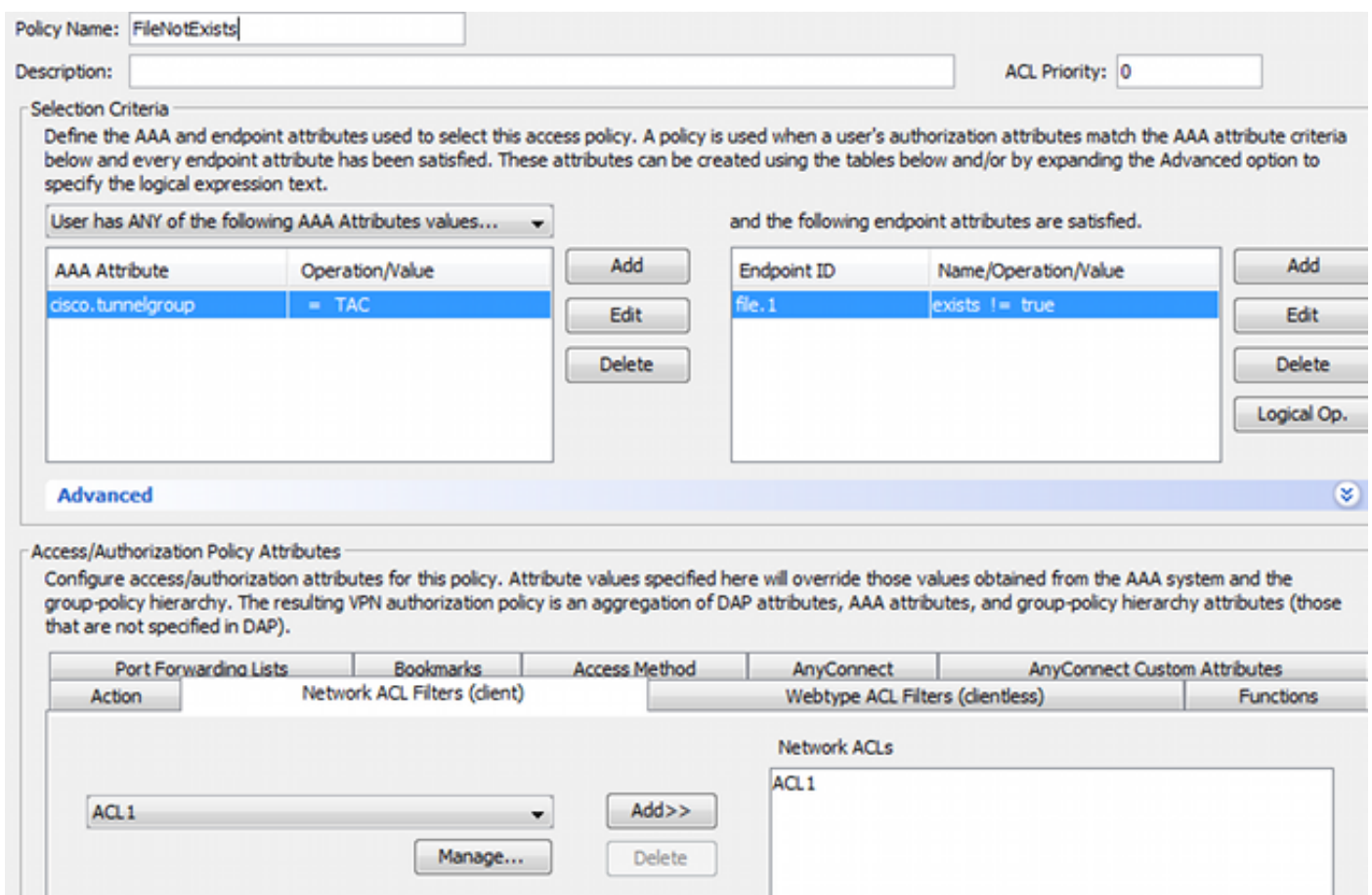


Daher werden mit der Standardeinstellung keine Aktionen ausgeführt, um die Verbindung zuzulassen. Es wird keine ACL verwendet - der gesamte Netzwerkzugriff wird bereitgestellt.

Details zur Dateiprüfung sind im Bild dargestellt.

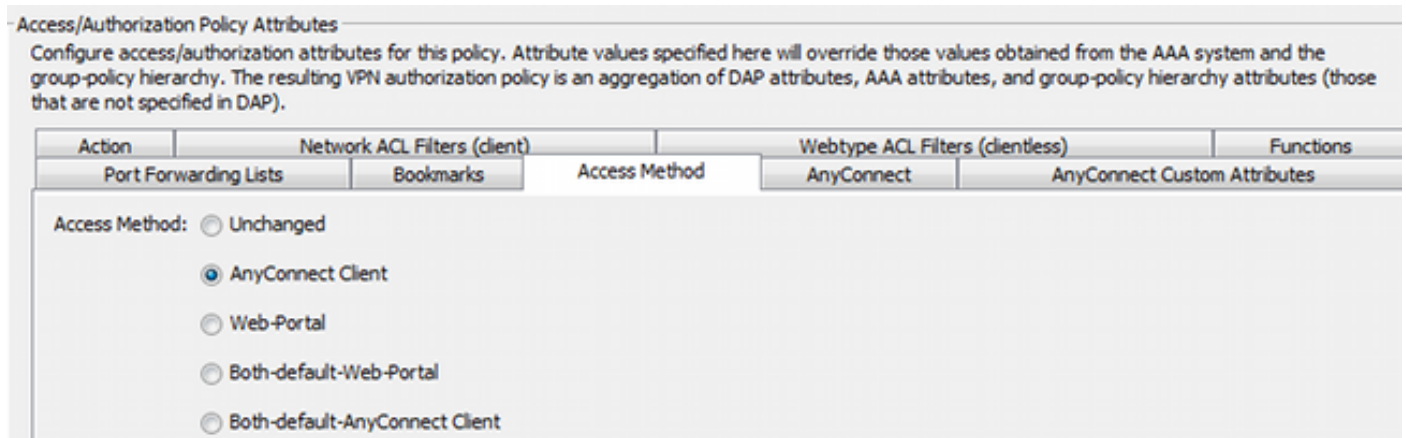


Die zweite Richtlinie (FileNotExists) ist ähnlich, aber diese Bedingung ist, **wenn die Datei nicht wie im Bild gezeigt vorhanden ist**.



Im Ergebnis wurde die Zugriffskontrollliste ACL1 konfiguriert. Dies gilt für nicht konforme VPN-Benutzer mit eingeschränktem Netzwerkzugriff.

Beide DAP-Richtlinien drängen auf **AnyConnect Client**-Zugriff, wie im Bild gezeigt.



ISE

Die ISE wird für die Benutzerauthentifizierung verwendet. Es müssen nur das Netzwerkgerät (ASA) und der richtige Benutzername (cisco) konfiguriert werden. Dieser Teil wird in diesem Artikel nicht behandelt.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

CSD- und AnyConnect-Bereitstellung

Zunächst wird der Benutzer nicht mit dem AnyConnect-Client bereitgestellt. Der Benutzer ist ebenfalls nicht mit der Richtlinie konform (die Datei `c:\test.txt` existiert nicht). Geben Sie <https://10.62.145.45> ein, und der Benutzer wird sofort zur CSD-Installation umgeleitet, wie im Bild gezeigt.



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

Dies kann über Java oder ActiveX erfolgen. Nach der Installation des CSD wird dieser wie im Bild gezeigt angezeigt.



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

Dann wird der Benutzer zur Authentifizierung umgeleitet, wie im Bild gezeigt.



Login

Please enter your username and password.

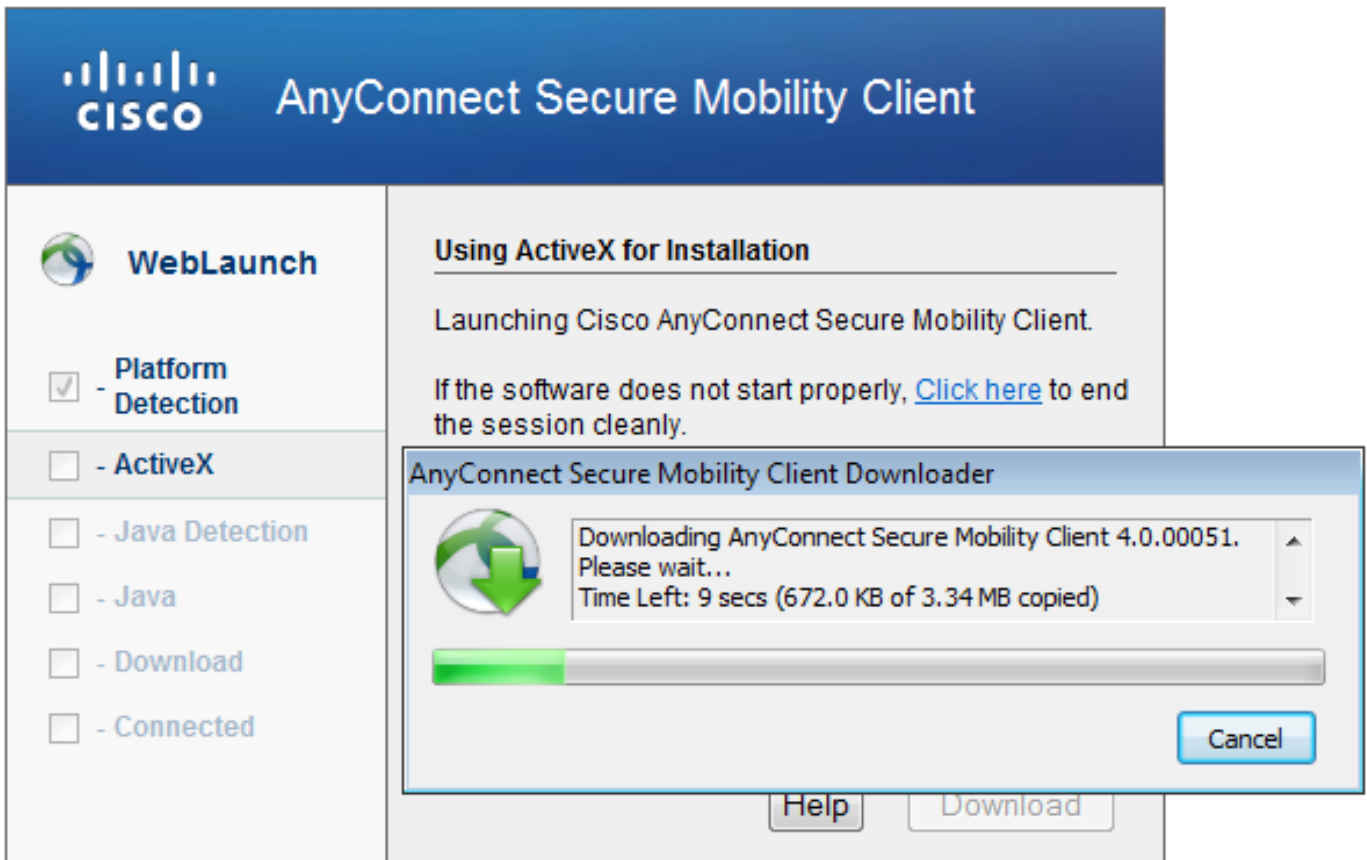
GROUP: TAC ▼

USERNAME:

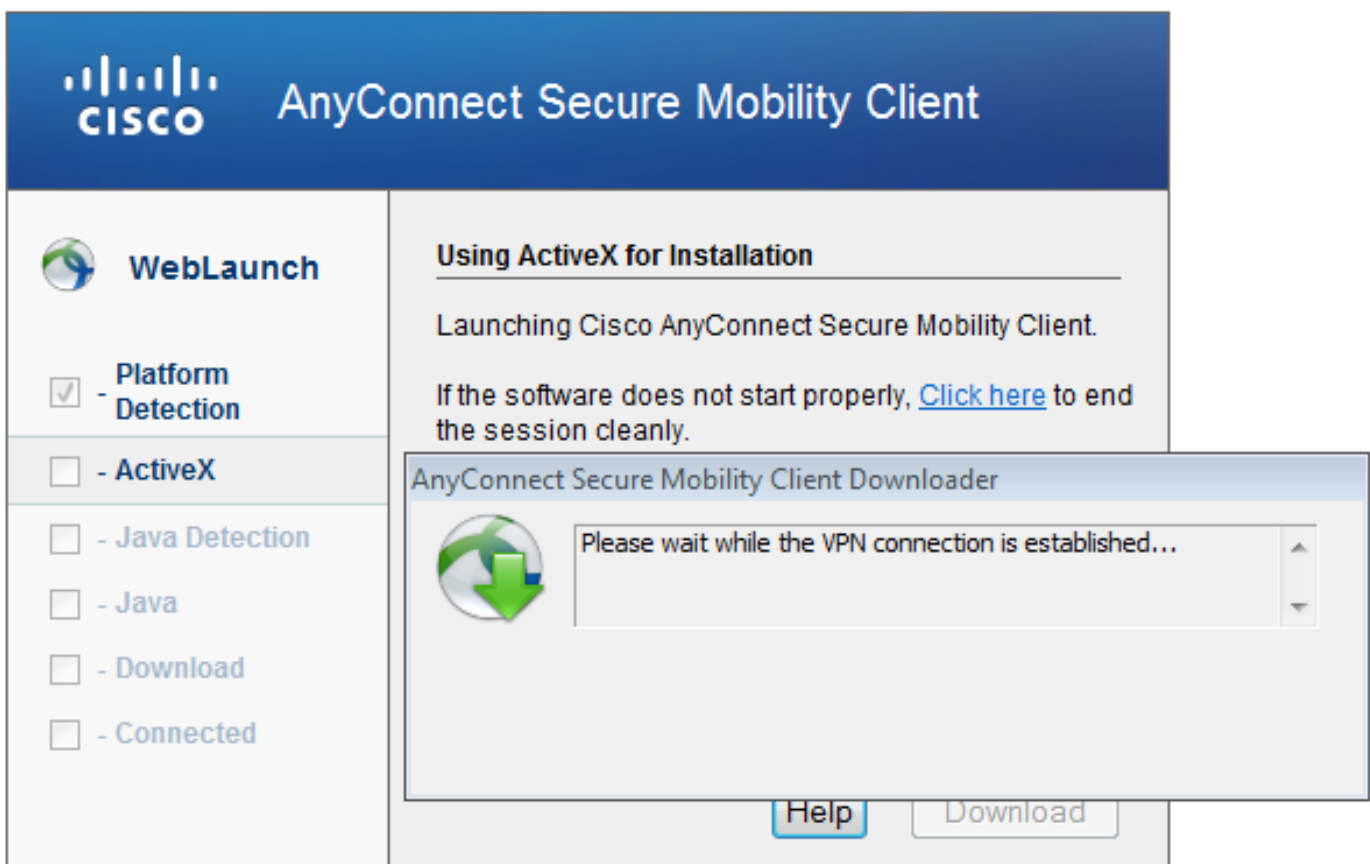
PASSWORD:

Login

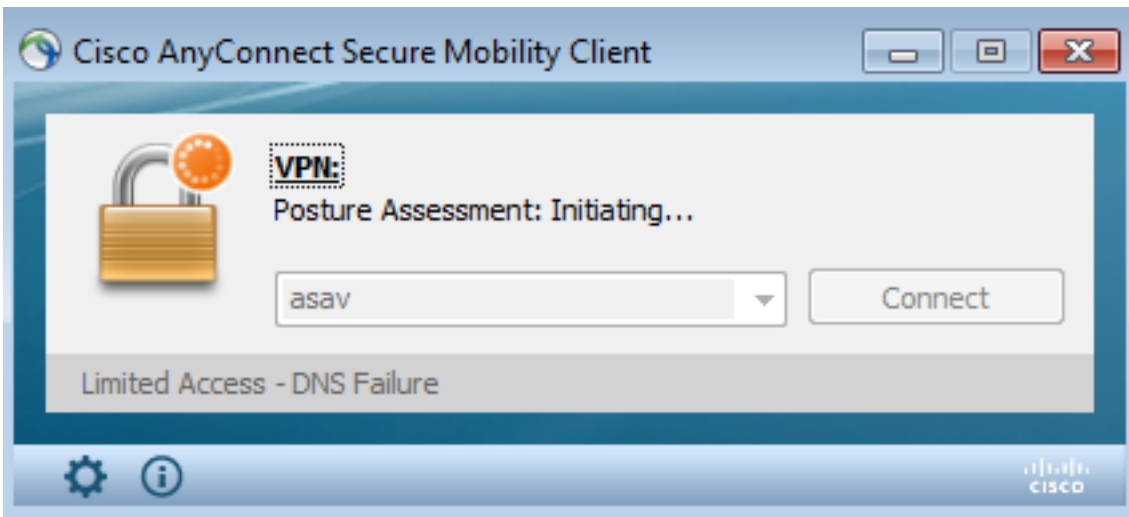
Wenn der Test erfolgreich war, wird AnyConnect zusammen mit dem konfigurierten Profil bereitgestellt - wiederum können ActiveX oder Java wie im Bild gezeigt verwendet werden.



Die VPN-Verbindung wird wie im Bild gezeigt hergestellt.



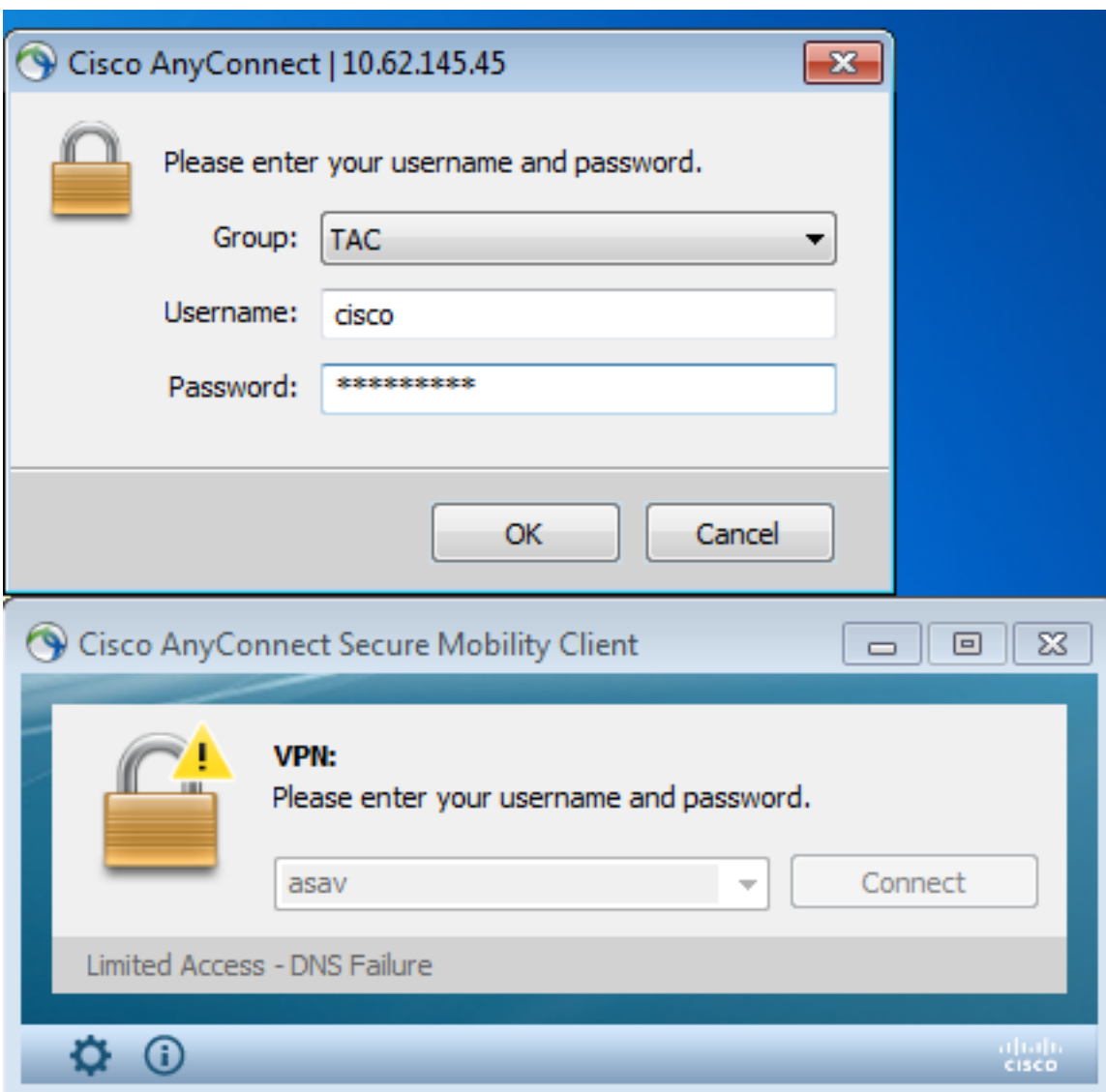
Der erste Schritt für AnyConnect besteht in der Durchführung von Statusprüfungen (HostScan) und dem Senden der Berichte an die ASA, wie im Bild gezeigt.



Anschließend authentifiziert und beendet AnyConnect die VPN-Sitzung.

AnyConnect VPN-Sitzung mit Status - nicht konform

Wenn Sie eine neue VPN-Sitzung mit AnyConnect einrichten, ist der erste Schritt die Statusüberprüfung (HostScan), wie im Screenshot weiter oben beschrieben. Anschließend wird eine Authentifizierung durchgeführt, und die VPN-Sitzung wird wie in den Bildern gezeigt eingerichtet.



ASA berichtet, dass der HostScan-Bericht empfangen wird:

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

Anschließend wird die Benutzerauthentifizierung durchgeführt:

```
%ASA-6-113004: AAA user authentication Successful : server = 10.62.145.42 : user = cisco  
und startet die Autorisierung für diese VPN-Sitzung. Wenn "debug dap trace 255" aktiviert ist,  
werden die Informationen zum Vorhandensein der c:\test.txt-Datei zurückgegeben:
```

```
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"
```

Informationen zur 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"
```

und Symantec AntiVirus (gemäß den zuvor konfigurierten HostScan Advanced Endpoint Assessment-Regeln).

Als Ergebnis wird die DAP-Richtlinie zugeordnet:

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

Diese Richtlinie erfordert die Verwendung von AnyConnect und wendet außerdem die Zugriffsliste-ACL1 an, die den Benutzern eingeschränkten Netzwerkzugriff ermöglicht (nicht mit der Unternehmensrichtlinie konform):

```
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
```

Die Protokolle stellen außerdem ACIDEX-Erweiterungen bereit, die von der DAP-Richtlinie verwendet werden können (oder sogar in Radius-Requests an die ISE übergeben werden können und in den Autorisierungsregeln als Bedingungen verwendet werden):

```
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 Ergebnis ist die VPN-Sitzung beendet, jedoch mit eingeschränktem Netzwerkzugriff:

```
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: DTLSv1.0              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
```

Der AnyConnect-Verlauf zeigt detaillierte Schritte für den Status-Prozess:

```
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-Sitzung mit Status - konform

Nachdem Sie die `c:\test.txt`-Datei erstellt haben, ist der Fluss ähnlich. Sobald eine neue AnyConnect-Sitzung initiiert wurde, weisen die Protokolle auf das Vorhandensein der Datei hin:

```
%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"
```

Daher wird eine andere DAP-Richtlinie verwendet:

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

Die Richtlinie schreibt keine ACL als Einschränkung für den Netzwerkverkehr vor.

Die Sitzung ist ohne Zugriffskontrollliste (vollständiger Netzwerkzugriff) beendet:

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
```

Darüber hinaus meldet Anyconnect, dass HostScan inaktiv ist und auf die nächste Scan-Anfrage wartet:

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

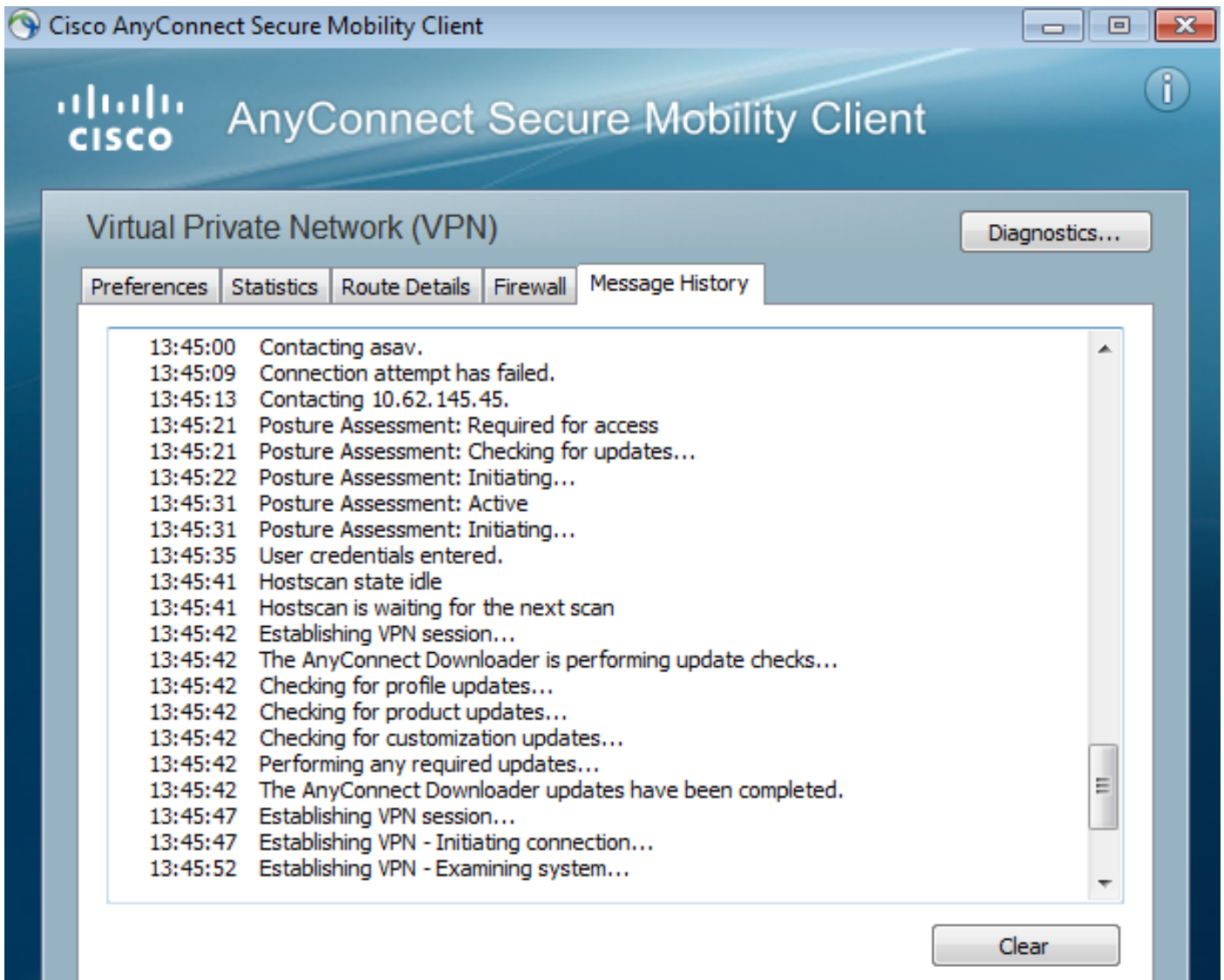
Hinweis: Es wird empfohlen, zur Neubewertung das in die ISE integrierte Statusmodul zu verwenden.

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

AnyConnect DART

AnyConnect stellt Diagnosen bereit, wie im Bild gezeigt.



Dabei werden alle AnyConnect-Protokolle in einer Zip-Datei auf dem Desktop erfasst und gespeichert. Diese Zip-Datei enthält die Protokolle in Cisco AnyConnect Secure Mobility Client/Anyconnect.txt.

Diese stellt Informationen über ASA bereit und fordert HostScan auf, Daten zu sammeln:

```

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.

```

Dann zeigen mehrere andere Protokolle, dass CSD installiert ist. Dies ist das Beispiel für eine CSD-Bereitstellung und eine nachfolgende AnyConnect-Verbindung mit Status:

```

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...

Die Kommunikation zwischen ASA und AnyConnect ist optimiert, und ASA-Anfragen werden nur zur Durchführung bestimmter Prüfungen durchgeführt - AnyConnect lädt zusätzliche Daten herunter, um diese durchführen zu können (z. B. spezielle AntiVirus-Verifizierung).

Wenn Sie das Ticket mit TAC öffnen, fügen Sie die Dart-Protokolle zusammen mit "show tech" und "debug dap trace 255" von ASA an.

Zugehörige Informationen

- [Host Scan und das Statusmodul konfigurieren - Administratoranleitung für den Cisco AnyConnect Secure Mobility Client](#)
- [Statusservices im Cisco ISE-Konfigurationsleitfaden](#)
- [Cisco ISE 1.3 Administratorhandbuch](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)