

Configure ASA VPN Posture with CSD, DAP and AnyConnect 4.0

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Network Diagram](#)

[ASA](#)

[Step 1. Basic SSL VPN Configuration](#)

[Step 2. CSD Installation](#)

[Step 3. DAP Policies](#)

[ISE](#)

[Verify](#)

[CSD and AnyConnect Provisioning](#)

[AnyConnect VPN Session with Posture - Non Compliant](#)

[AnyConnect VPN Session with Posture - Compliant](#)

[Troubleshoot](#)

[AnyConnect DART](#)

[Related Information](#)

Introduction

This document describes how to perform the posture for remote VPN sessions terminated on Adaptive Security Appliance (ASA). The posture is performed locally by ASA with the use of Cisco Secure Desktop (CSD) with HostScan module. After VPN session is established, compliant station are allowed full network access whereas non-compliant station has limited network access.

Also, CSD and AnyConnect 4.0 provisioning flows are presented.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco ASA VPN configuration
- Cisco AnyConnect Secure Mobility Client

Components Used

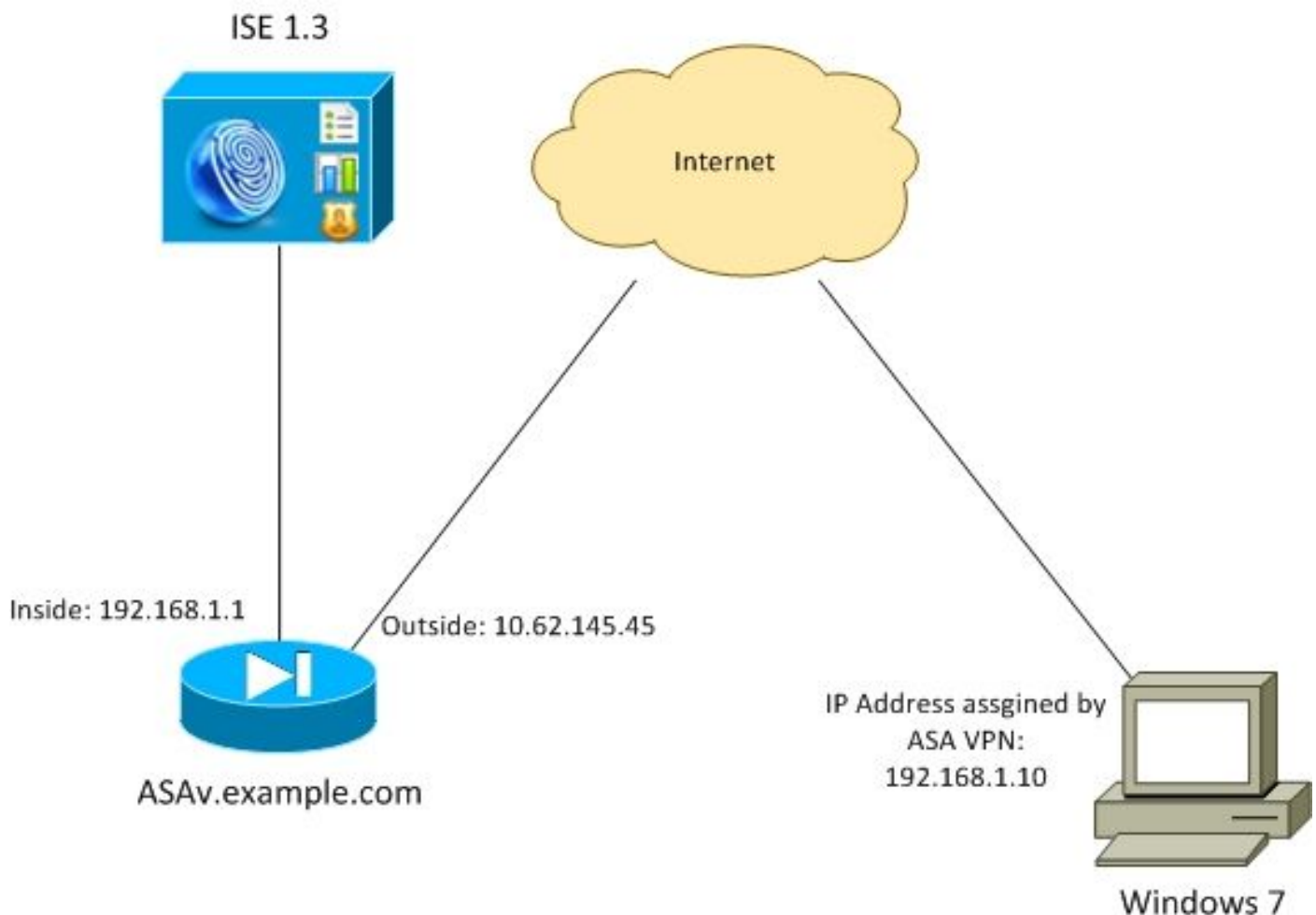
The information in this document is based on these software and hardware versions:

- Microsoft Windows 7
- Cisco ASA, Version 9.3 or Later
- Cisco Identity Services Engine (ISE) Software, Versions 1.3 and Later
- Cisco AnyConnect Secure Mobility Client, Version 4.0 and Later
- CSD, Version 3.6 or Later

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. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram



Corporate policy is as follows:

- Remote VPN users which has file **c:\test.txt** (compliant) must have full network access to inside company resources
- Remote VPN users which do not have file **c:\test.txt** (non-compliant) must have limited network access to inside company resources: only access to remediation server 1.1.1.1 is provided.

File existence is the simplest example. Any other condition (antivirus, antispyware, process, application, registry) can be used.

The flow is as follows:

- Remote users does not have AnyConnect installed. They access ASA web page for CSD and AnyConnect provisioning (along with the VPN profile)
- Once the connection via AnyConnect, non-compliant users are allowed with limited network access. Dynamic Access Policy (DAP) called **FileNotExists** are matched.
- User performs remediation (manually install file **c:\test.txt**) and connects again with AnyConnect. This time, full network access is provided (DAP policy called **FileExists** are matched).

HostScan module can be installed manually on the endpoint. Example files (hostscan-win-4.0.00051-pre-deploy-k9.msi) are shared on Cisco Connection Online (CCO). But, it could be also pushed from ASA. HostScan is a part of CSD which could be provisioned from ASA. That second approach is used in this example.

For older versions of AnyConnect (3.1 and earlier), there was a separate package available on CCO (example: hostscan_3.1.06073-k9.pkg) which could have been configured and provisioned on ASA separately (with **csd hostscan image** command) - but that option do not exists anymore for AnyConnect version 4.0.

ASA

Step 1. Basic SSL VPN Configuration

ASA is preconfigured with basic remote VPN access (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

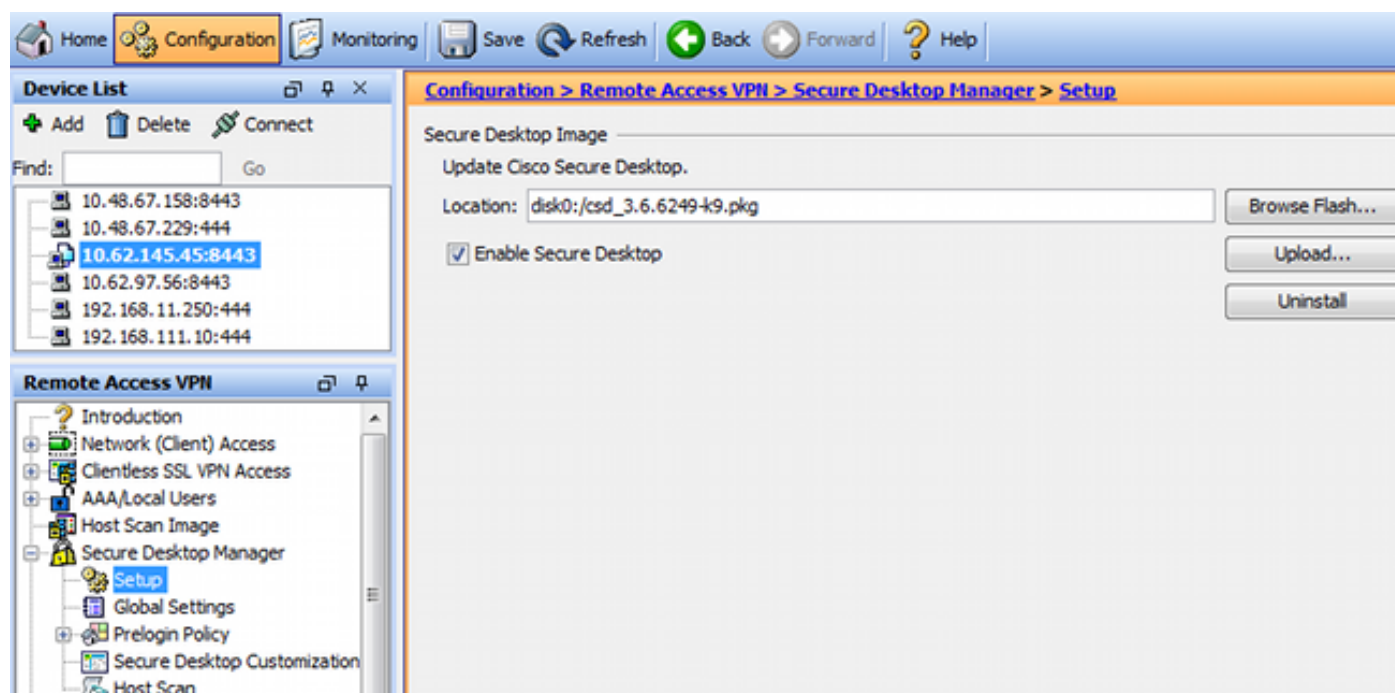
ip local pool POOL 192.168.1.10-192.168.1.20 mask 255.255.255.0

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

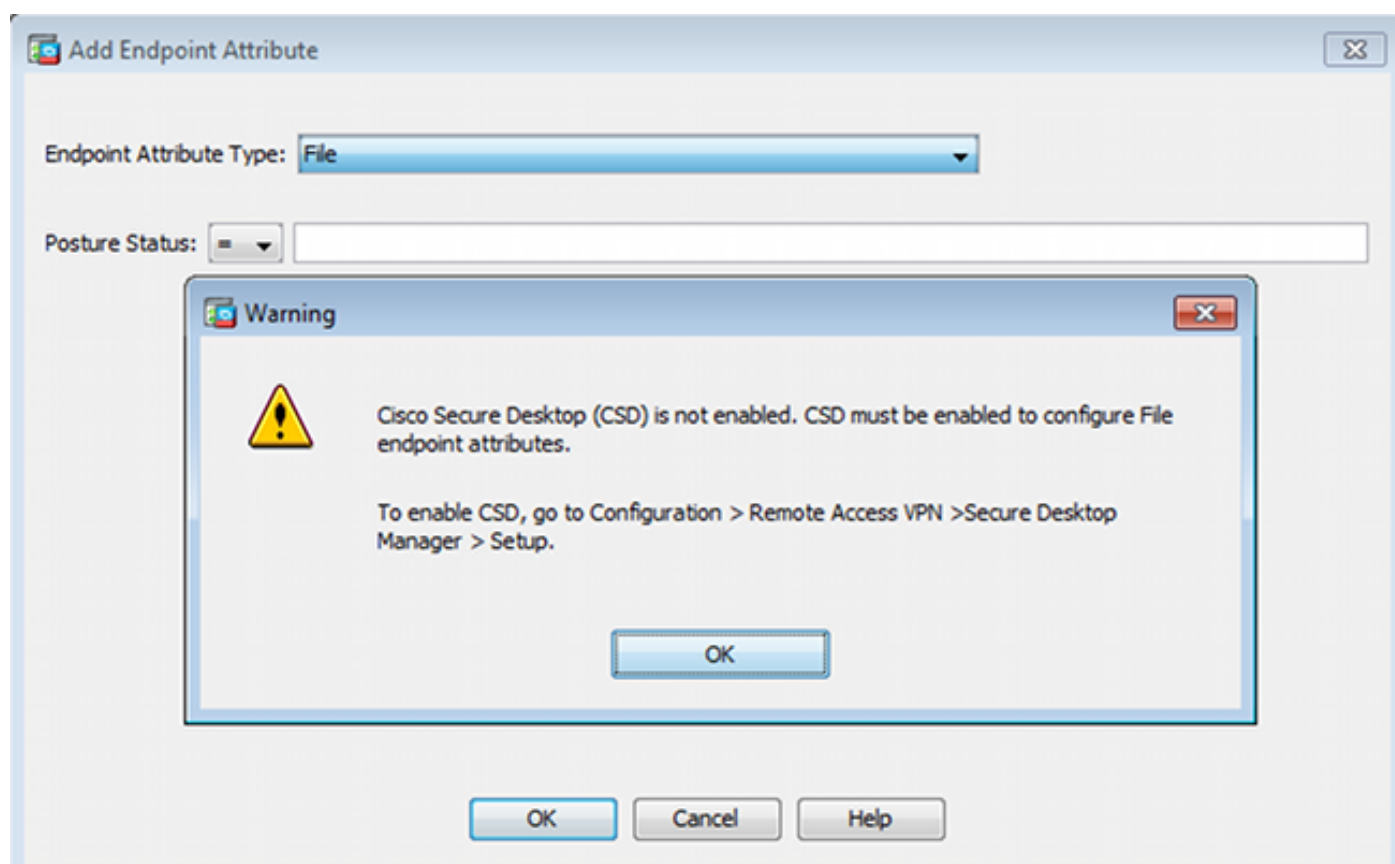
AnyConnect package has been downloaded and used.

Step 2. CSD Installation

Subsequent configuration is performed with Adaptive Security Device Manager (ASDM). CSD package needs to be downloaded in order to flash and take reference from configuration as shown in the image.



Without enabling Secure Desktop it would not be possible to use CSD attributes in DAP policies as shown in the image.

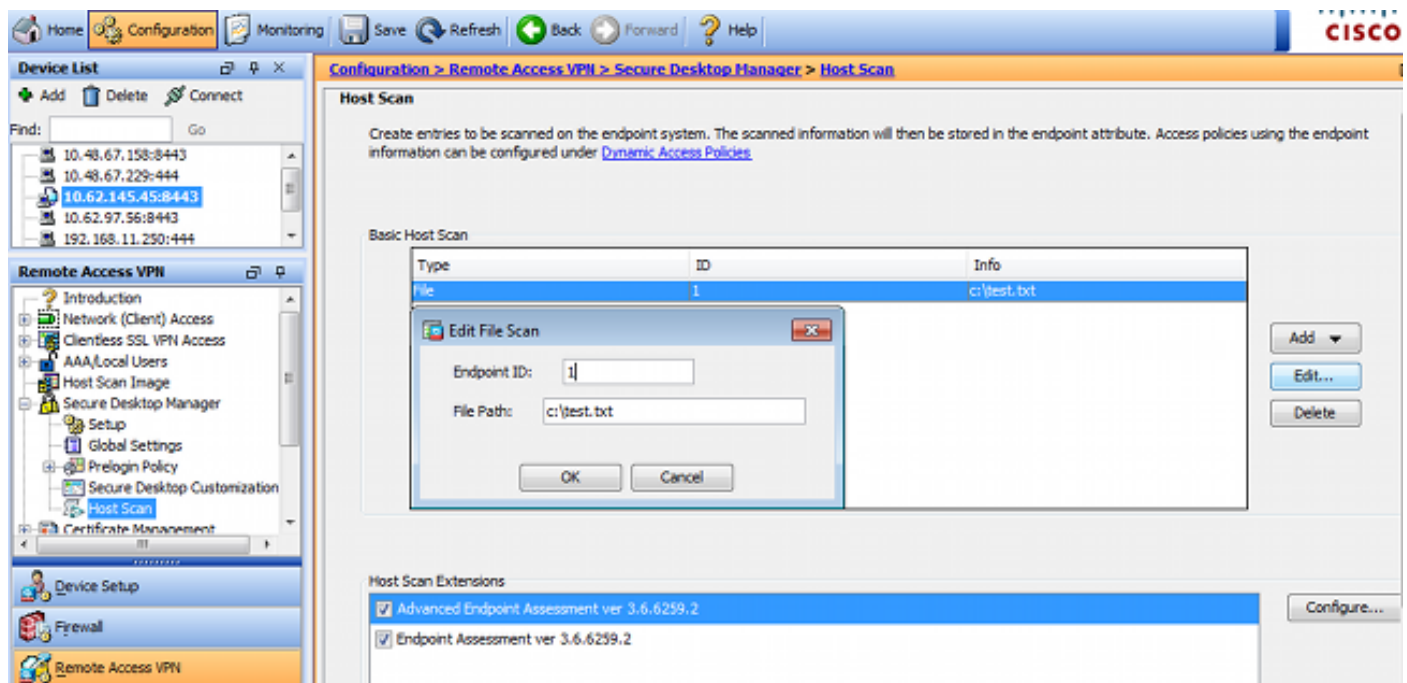


After you enable CSD, multiple options under Secure Desktop Manager appears.

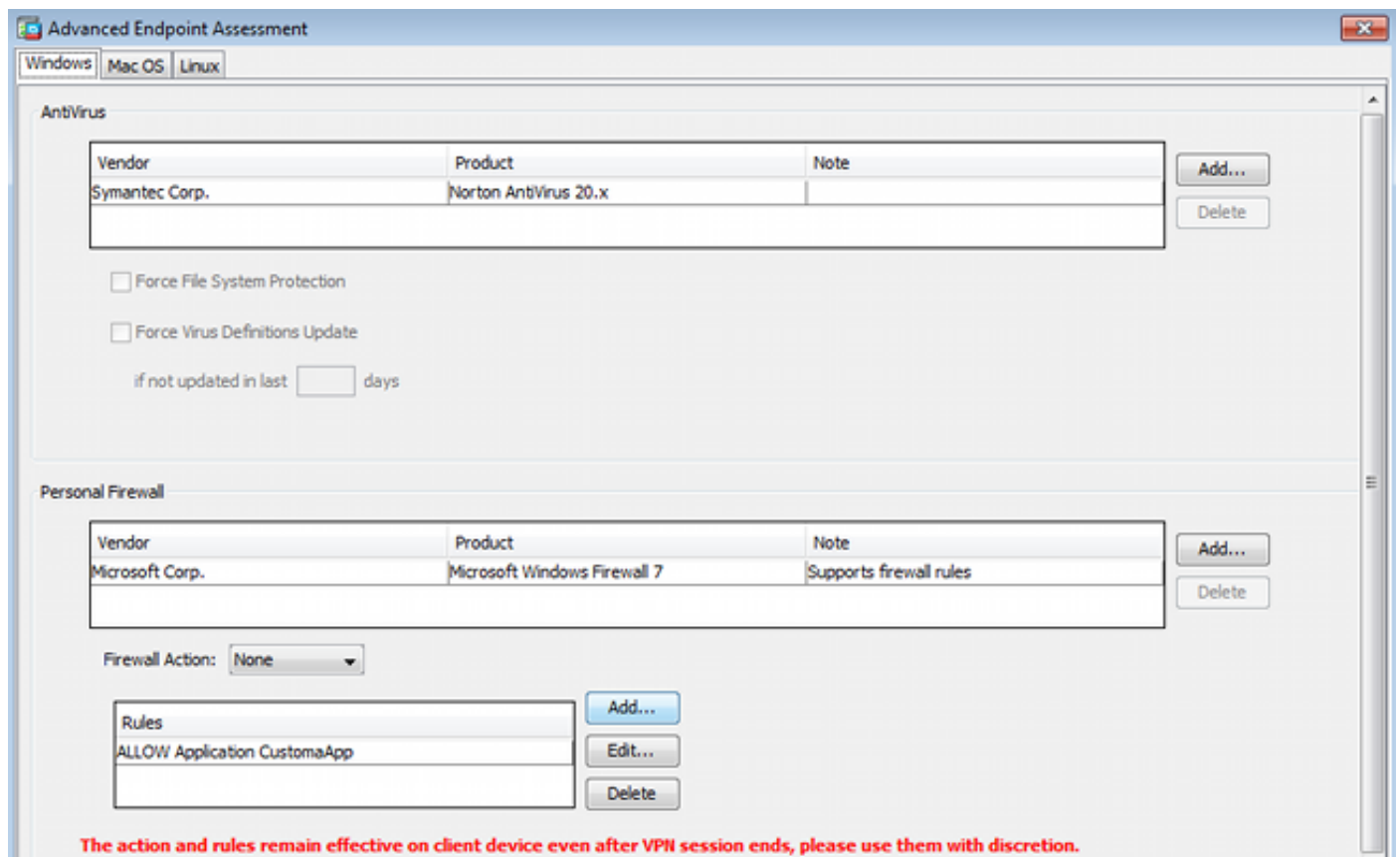
Note: Be informed that some of them are already deprecated. More information with regards

to deprecated features can be found: [Feature Deprecation Notice for Secure Desktop \(Vault\), Cache Cleaner, Keystroke Logger Detection, and Host Emulation Detection](#)

HostScan is still fully supported, new Basic HostScan rule is added. Existence of `c:\test.txt` is verified as shown in the image.



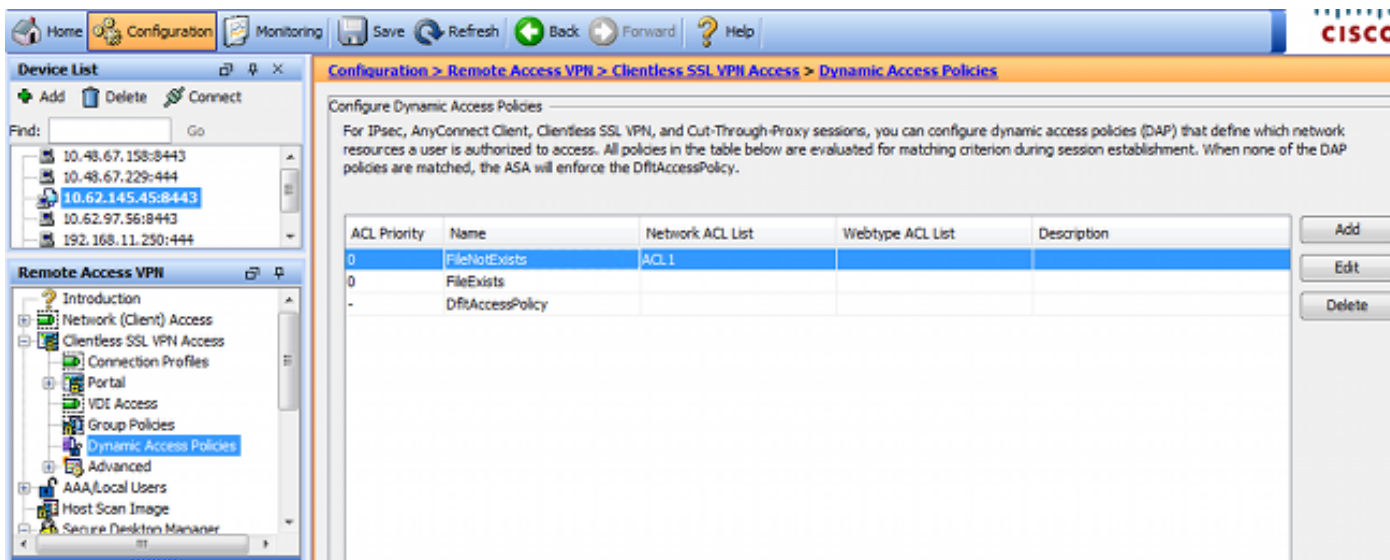
Also, additional Advanced Endpoint Assessment rule is added as shown in the image.



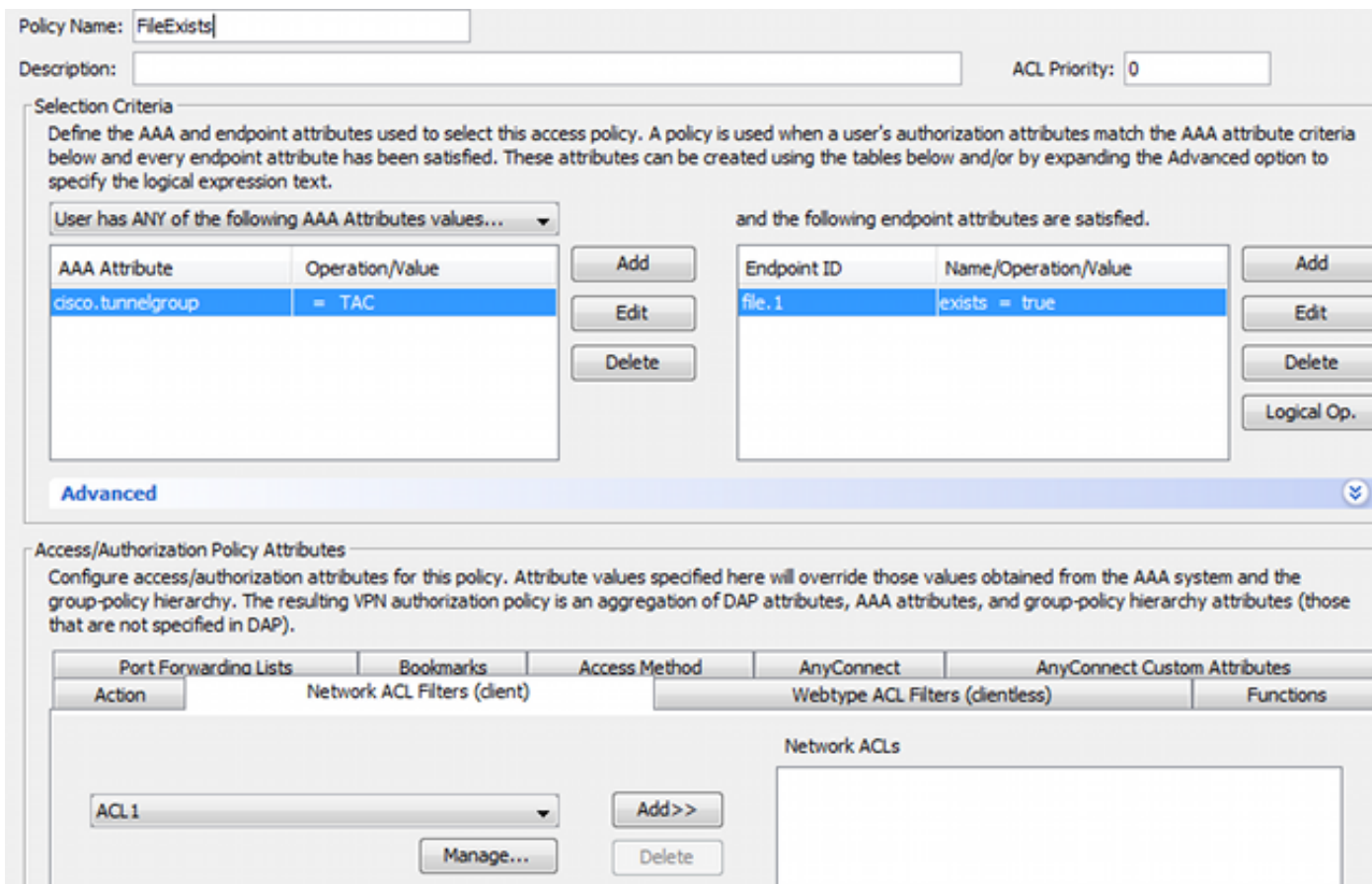
That one checks for the existence of Symantec Norton AntiVirus 20.x and Microsoft Windows Firewall 7. Posture module (HostScan) checks these values but there will be no enforcement (DAP policy does not verify that).

Step 3. DAP Policies

DAP policies are responsible to use the data gathered by HostScan as conditions and apply specific attributes to the VPN session as a result. In order to create DAP policy from ASDM, navigate to **Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies** as shown in the image.



First policy (FileExists) checks tunnel-group name which is used by configured VPN profile (VPN profile configuration has been omitted for clarity). Then, additional check for the file **c:\test.txt** is performed as shown in the image.



As a result, no actions are performed with the default setting in order to permit connectivity. No ACL is used - full network access is provided.

Details for the file check are as shown in the image.

Endpoint Attribute Type: File

☒ Exists ☐ Does not exist

Endpoint ID: 1
c:\test.txt

☐ Last Update: < days

☐ Checksum: =

Compute CRC32 Checksum...

OK Cancel Help

Second policy (FileNotExists) is similar - but this time condition is **if file is not existing** as shown in the image.

Policy Name: FileNotExists

Description: ACL Priority: 0

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...

AAA Attribute	Operation/Value
cisco.tunnelgroup	= TAC

and the following endpoint attributes are satisfied.

Endpoint ID	Name/Operation/Value
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

Add>> Manage... Delete

The result has access-list ACL1 configured. That is applied for non-compliant VPN users with the

provision of limited network access.

Both DAP policies push for **AnyConnect Client** access as shown in the image.

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).

Action	Network ACL Filters (client)	Webtype ACL Filters (clientless)	Functions
Port Forwarding Lists	Bookmarks	Access Method	AnyConnect AnyConnect Custom Attributes

Access Method: ☐ Unchanged
☒ AnyConnect Client
☐ Web-Portal
☐ Both-default-Web-Portal
☐ Both-default-AnyConnect Client

ISE

ISE is used for user authentication. Only network device (ASA) and correct username (cisco) must be configured. That part is not covered in this article.

Verify

Use this section in order to confirm that your configuration works properly.

CSD and AnyConnect Provisioning

Initially, user is not provisioned with AnyConnect client. User is also not compliant with the policy (the file **c:\test.txt** does not exist). Enter <https://10.62.145.45> and the user is immediately redirected for CSD installation as shown in the image.



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

That can be done with Java or ActiveX. Once CSD is installed, it is reported as shown in the image.



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

Then user is redirected for authentication as shown in the image.



Login

Please enter your username and password.

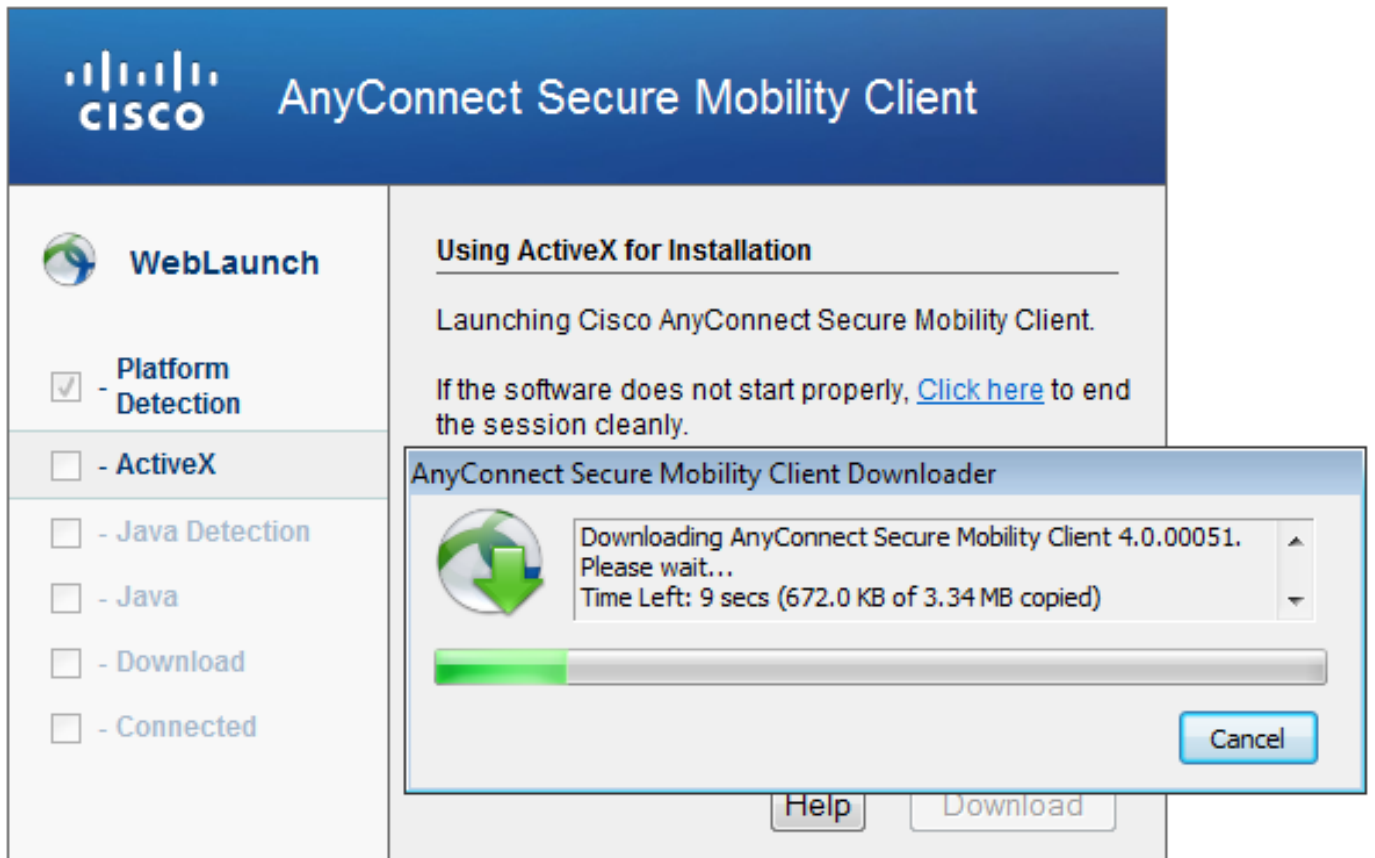
GROUP: TAC ▼

USERNAME:

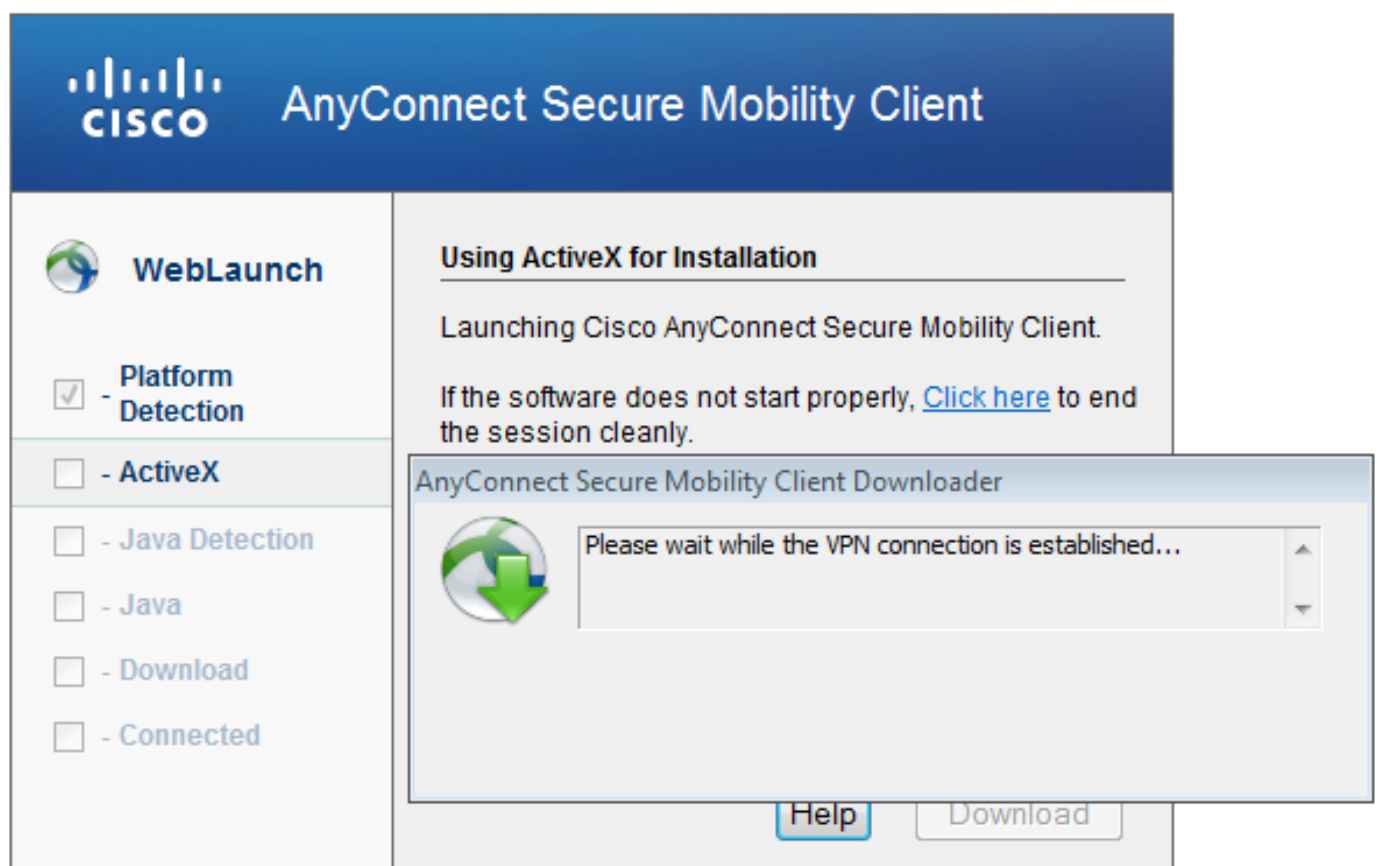
PASSWORD:

Login

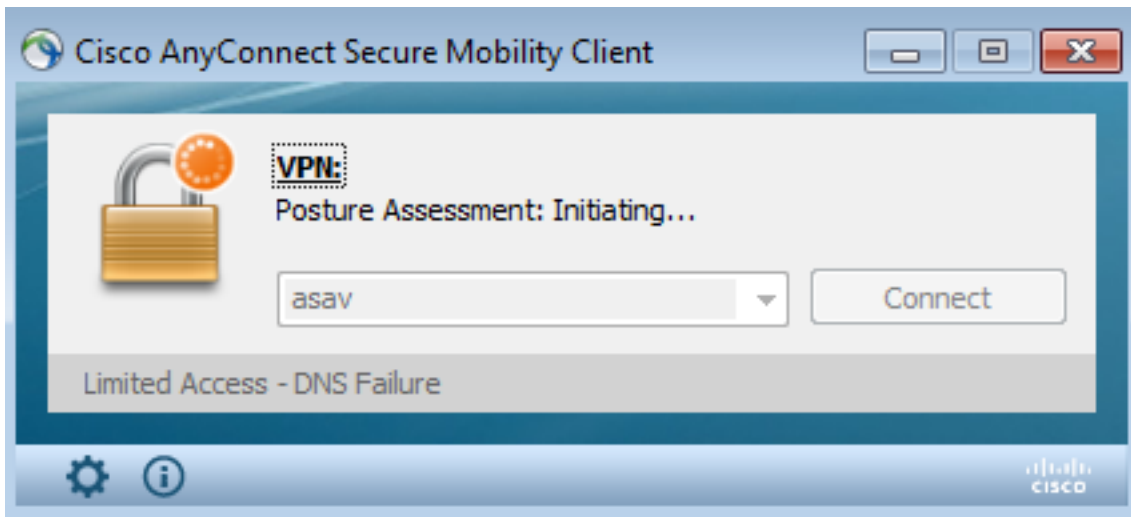
If successful, AnyConnect along with configured profile is deployed - again ActiveX or Java can be used as shown in the image.



And, the VPN connection is established as shown in the image.



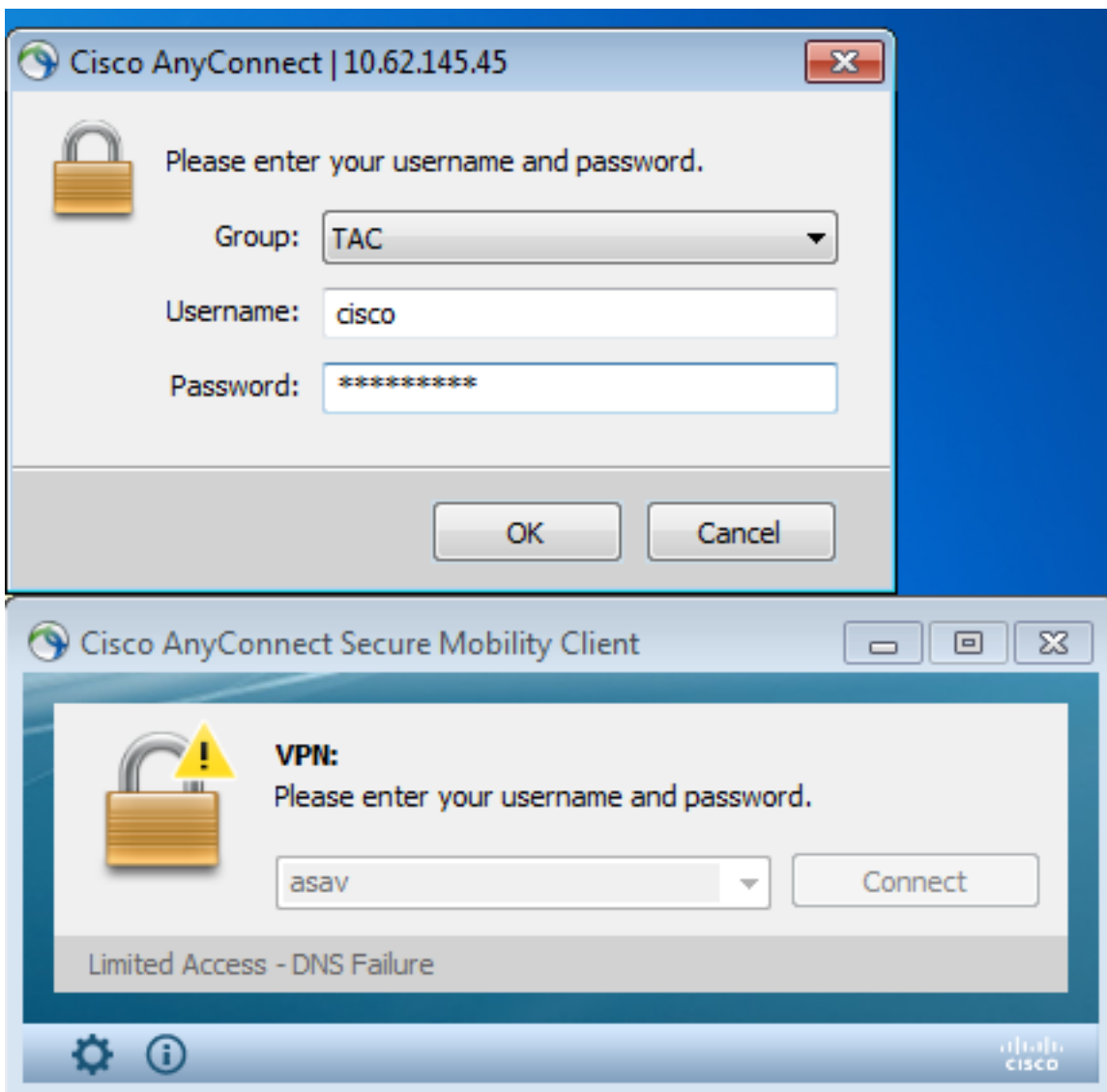
The first step for AnyConnect is to perform posture checks (HostScan) and send the reports to ASA as shown in the image.



Then, AnyConnect authenticates and finishes VPN session.

AnyConnect VPN Session with Posture - Non Compliant

When you establish a new VPN session with AnyConnect, the first step is the posture (HostScan) as presented on the screenshot earlier. Then, authentication occurs and the VPN session is established as shown in the images.



ASA reports that HostScan report is received:

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

Then performs user authentication:

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

And starts authorization for that VPN session. When you have "debug dap trace 255" enabled, the information with regards to the existence of **c:\test.txt** file is returned:

```
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"
```

Also, information with regards to 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"
```

And Symantec AntiVirus (as per HostScan Advanced Endpoint Assessment rules configured earlier).

As a result, the DAP policy is matched:

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

That policy forces to use AnyConnect and also applies access-list ACL1 which provides restricted network access for the user (not compliant with the corporate policy):

```
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
```

Logs also present ACIDEX extensions which can be used by DAP policy (or even passed in Radius-Requests to ISE and is used in Authorization Rules as conditions):

```
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";
```

As a result, VPN session is Up but with the restricted network access:

```
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
```

AnyConnect history shows detailed steps for the posture process:

```
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 Session with Posture - Compliant

After you create **c:\test.txt** file, the flow is similar. Once new AnyConnect session is initiated, the logs indicate the existence of the file:

```
%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"
```

And as a result another DAP policy is used:

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

The policy does not impose any ACL as the restriction for the network traffic.

And the session is Up without any ACL (full network access):

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
```

Also, Anyconnect reports that HostScan is idle and waiting for the next scan request:

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

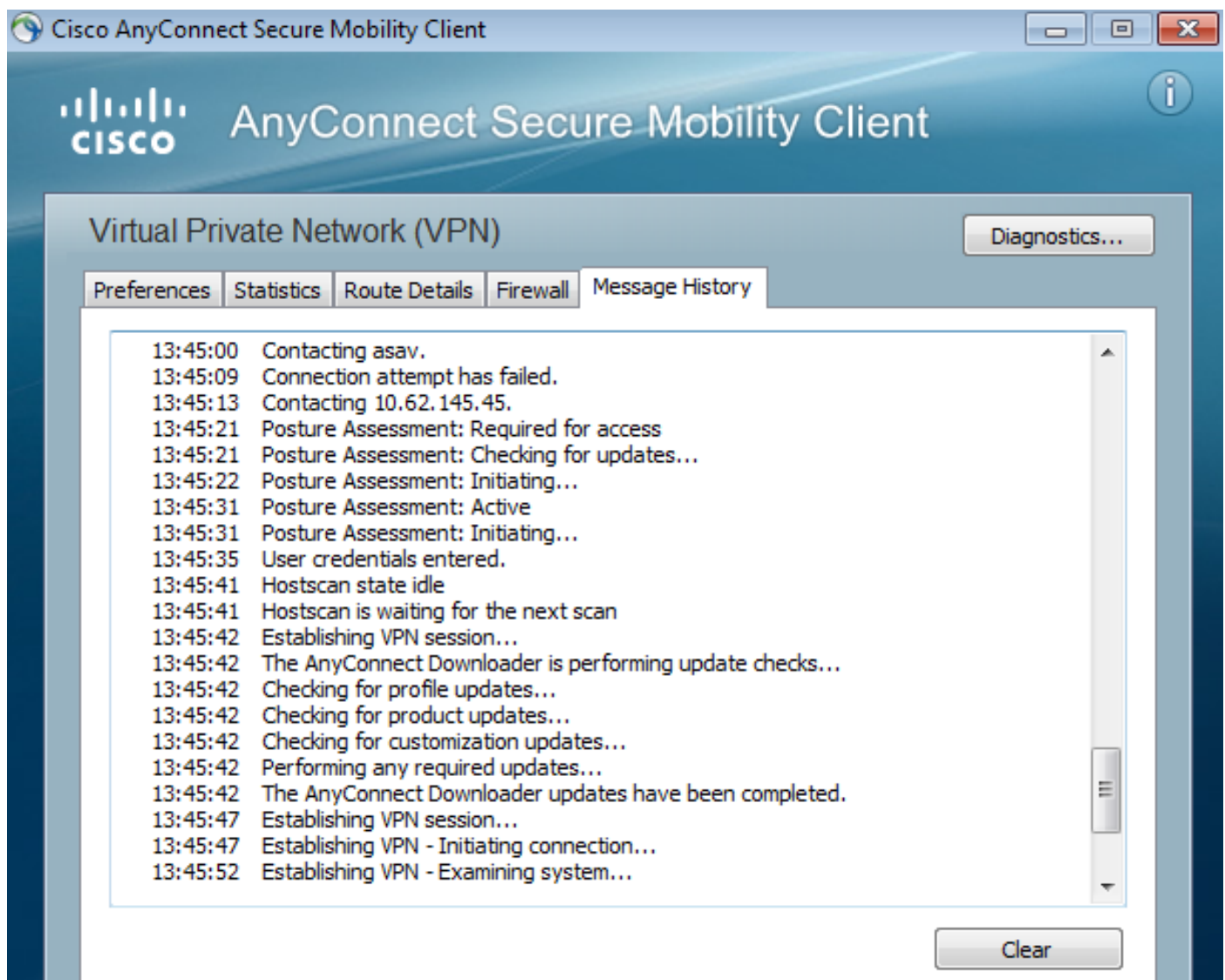
Note: For reassessment, it is advised to use posture module integrated with ISE.

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

AnyConnect DART

AnyConnect provides Diagnostics as shown in the image.



Which gathers and saves all the AnyConnect logs to a zip file on the desktop. That zip file includes the logs in Cisco AnyConnect Secure Mobility Client/Anyconnect.txt.

That provides the information about ASA and requests HostScan to gather data:

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.

Then, multiple other logs reveal that CSD is installed. This is the example for a CSD provisioning and subsequent AnyConnect connection along with posture:

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...

Communication between ASA and AnyConnect is optimized, ASA requests in order to perform only specific checks - AnyConnect downloads additional data in order to be able to perform that (for example specific AntiVirus verification).

When you open the case with TAC, attach Dart logs along with "show tech" and "debug dap trace 255" from ASA.

Related Information

- [Configuring Host Scan and the Posture Module - Cisco AnyConnect Secure Mobility Client Administrator Guide](#)
- [Posture services on Cisco ISE Configuration Guide](#)

- [Cisco ISE 1.3 Administrators Guide](#)
- [Technical Support & Documentation - Cisco Systems](#)