

使用CSD、DAP和AnyConnect 4.0配置ASA VPN安全狀態

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[ASA](#)

[步驟1. 基本SSL VPN配置](#)

[步驟2. CSD安裝](#)

[步驟3. DAP策略](#)

[ISE](#)

[驗證](#)

[CSD和AnyConnect調配](#)

[安全狀態的AnyConnect VPN會話 — 不相容](#)

[安全狀態的AnyConnect VPN會話 — 相容](#)

[疑難排解](#)

[AnyConnect DART](#)

[相關資訊](#)

簡介

本文檔介紹如何執行在自適應安全裝置(ASA)上終止的遠端VPN會話的狀態。ASA使用帶有HostScan模組的Cisco Secure Desktop(CSD)在本地執行安全狀態。建立VPN會話後，允許符合的站點進行完全網路訪問，而不符合的站點進行有限的網路訪問。

此外，還介紹了CSD和AnyConnect 4.0調配流程。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco ASA VPN配置
- Cisco AnyConnect Security Mobility Solution — 遠端存取

採用元件

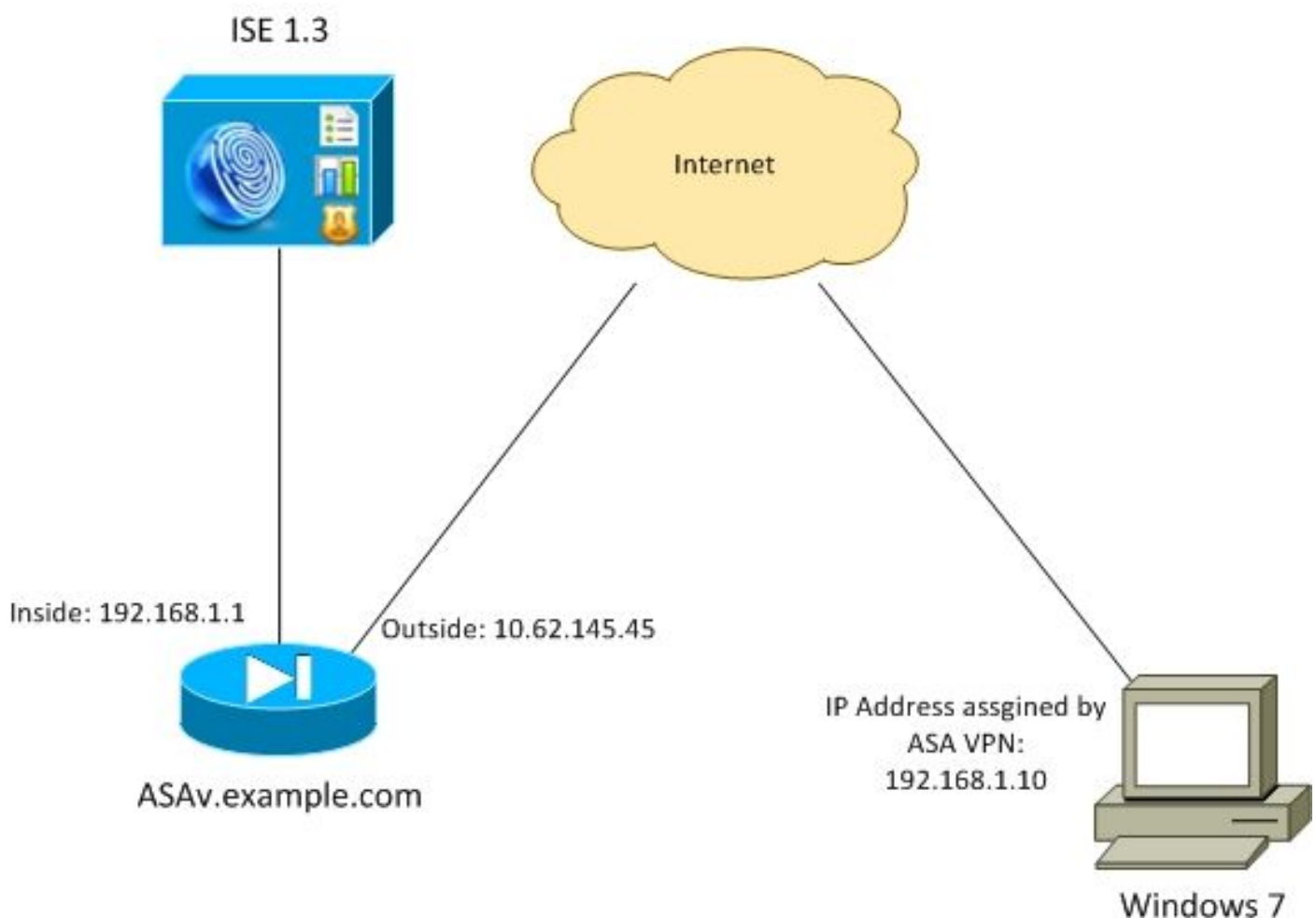
本文中的資訊係根據以下軟體和硬體版本：

- Microsoft Windows 7
- Cisco ASA 9.3版或更高版本
- Cisco Identity Services Engine(ISE)軟體1.3版及更新版本
- Cisco AnyConnect Security Mobility Solution 4.0及更新版本
- CSD 3.6版或更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

網路圖表



公司政策如下：

- 具有檔案c:\test.txt (相容) 的遠端VPN使用者必須擁有對公司內部資源的完全網路訪問許可權
- 沒有檔案c:\test.txt (不符合) 的遠端VPN使用者必須對公司內部資源具有有限的網路訪問許可權：僅提供對補救伺服器1.1.1.1的訪問。

檔案存在是最簡單的示例。可以使用任何其他條件 (防病毒、反間諜軟體、進程、應用程式、登錄檔)。

流程如下：

- 遠端使用者未安裝AnyConnect。他們訪問CSD和AnyConnect調配的ASA網頁 (以及VPN配置檔案)

- 通過AnyConnect進行連線後，允許不合規使用者訪問有限網路。已匹配名為FileNotExists的動態訪問策略(DAP)。
- 使用者執行修復(手動安裝檔案c:\test.txt)，然後再次與AnyConnect連線。這一次，將提供完整的網路訪問(匹配名為FileExists的DAP策略)。

可以在終端上手動安裝HostScan模組。示例檔案(hostscan-win-4.0.00051-pre-deploy-k9.msi)在Cisco Connection Online(CCO)上共用。但是，也可以從ASA推送它。HostScan是可以從ASA調配的CSD的一部分。第二個方法在本示例中使用。

對於舊版AnyConnect (3.1及更低版本)，CCO上有一個單獨的軟體包(例如 : hostscan_3.1.06073-k9.pkg)，可以單獨在ASA上配置和調配(使用csd hostscan image命令) — 但是對於AnyConnect版本4.0，該選項不再存在。

ASA

步驟1.基本SSL VPN配置

ASA預配置了基本遠端VPN訪問(安全套接字層(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

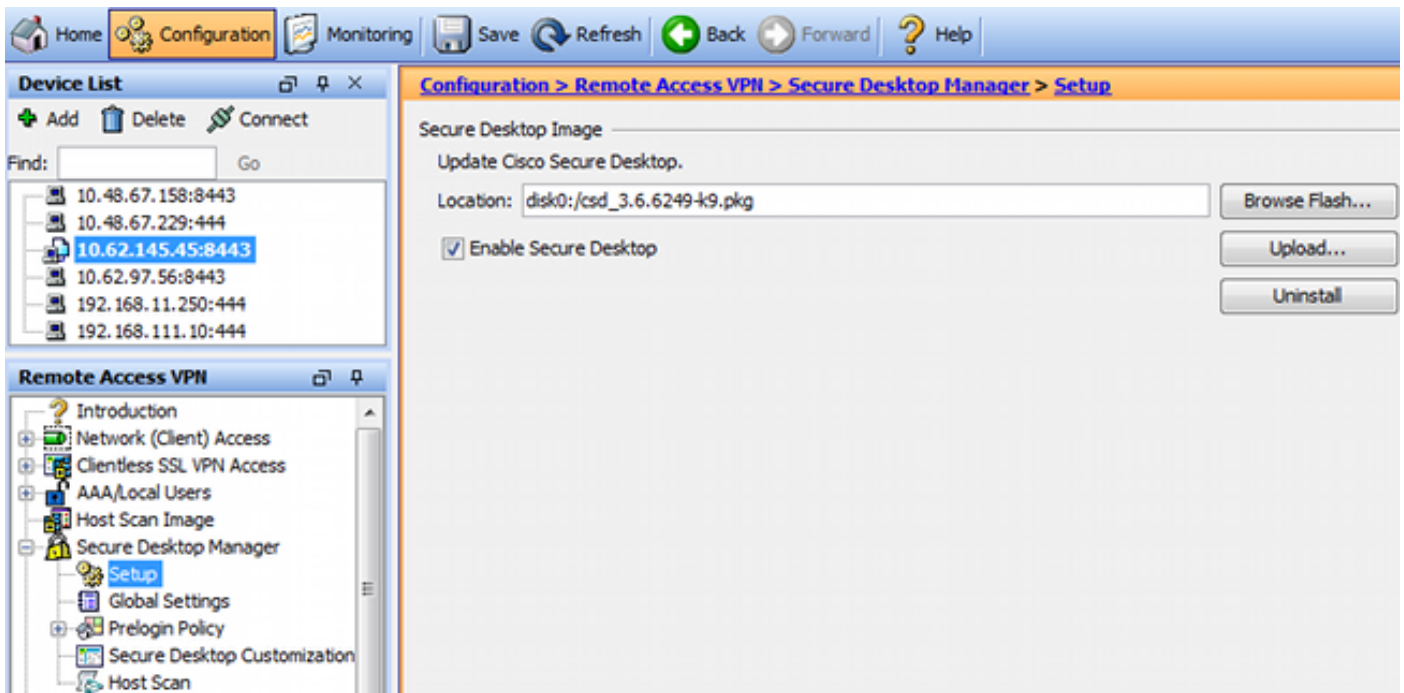
ip local pool POOL 192.168.1.10-192.168.1.20 mask 255.255.255.0

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

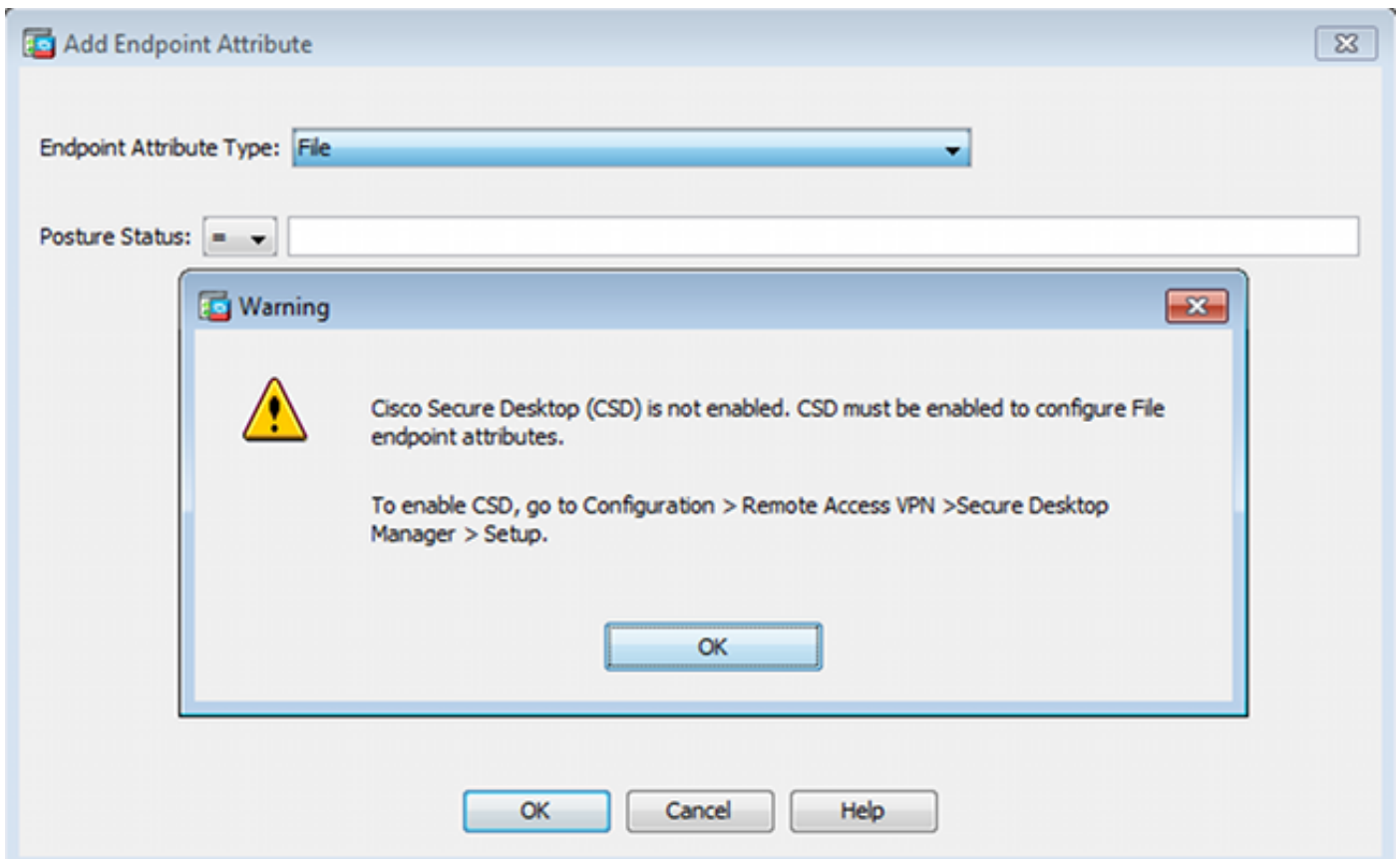
已下載並使用AnyConnect軟體包。

步驟2. CSD安裝

後續配置使用自適應安全裝置管理器(ASDM)執行。CSD軟體包需要下載以快閃記憶體，並從配置中獲得參考，如圖所示。



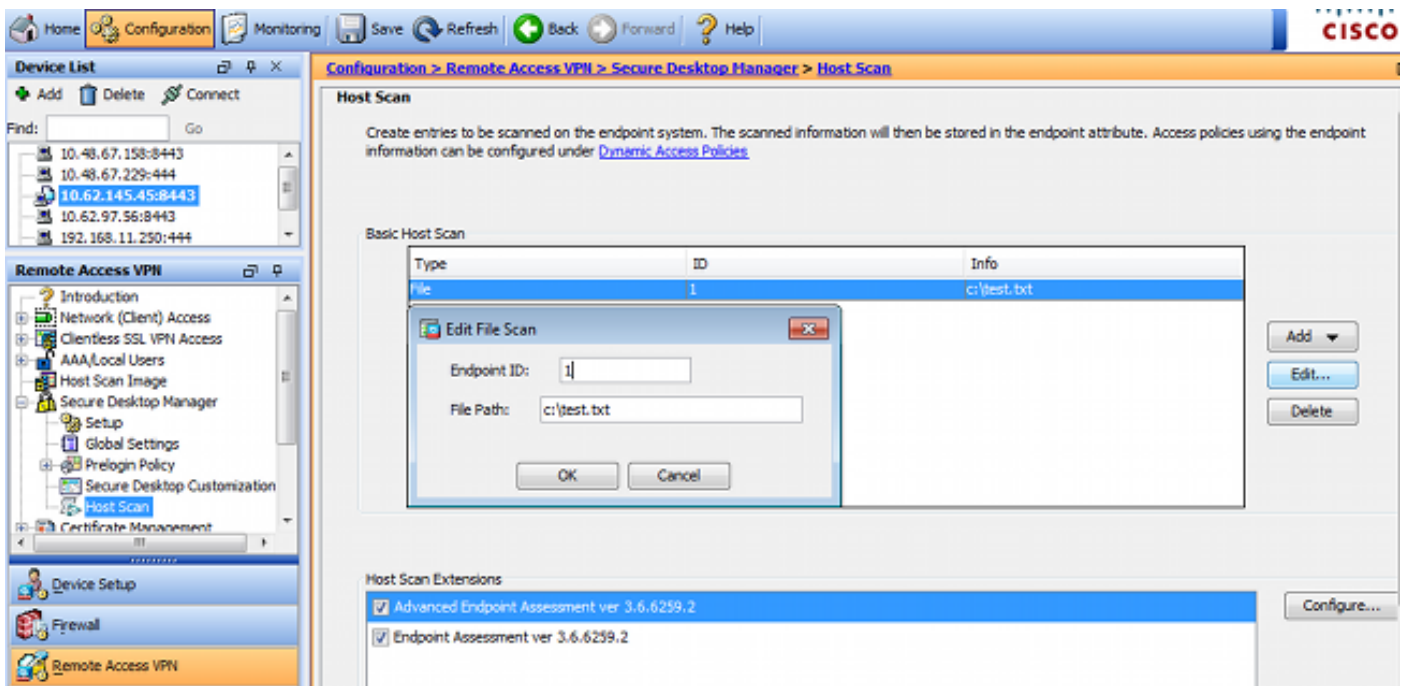
如果不啟用Secure Desktop，則無法在DAP策略中使用CSD屬性，如圖所示。



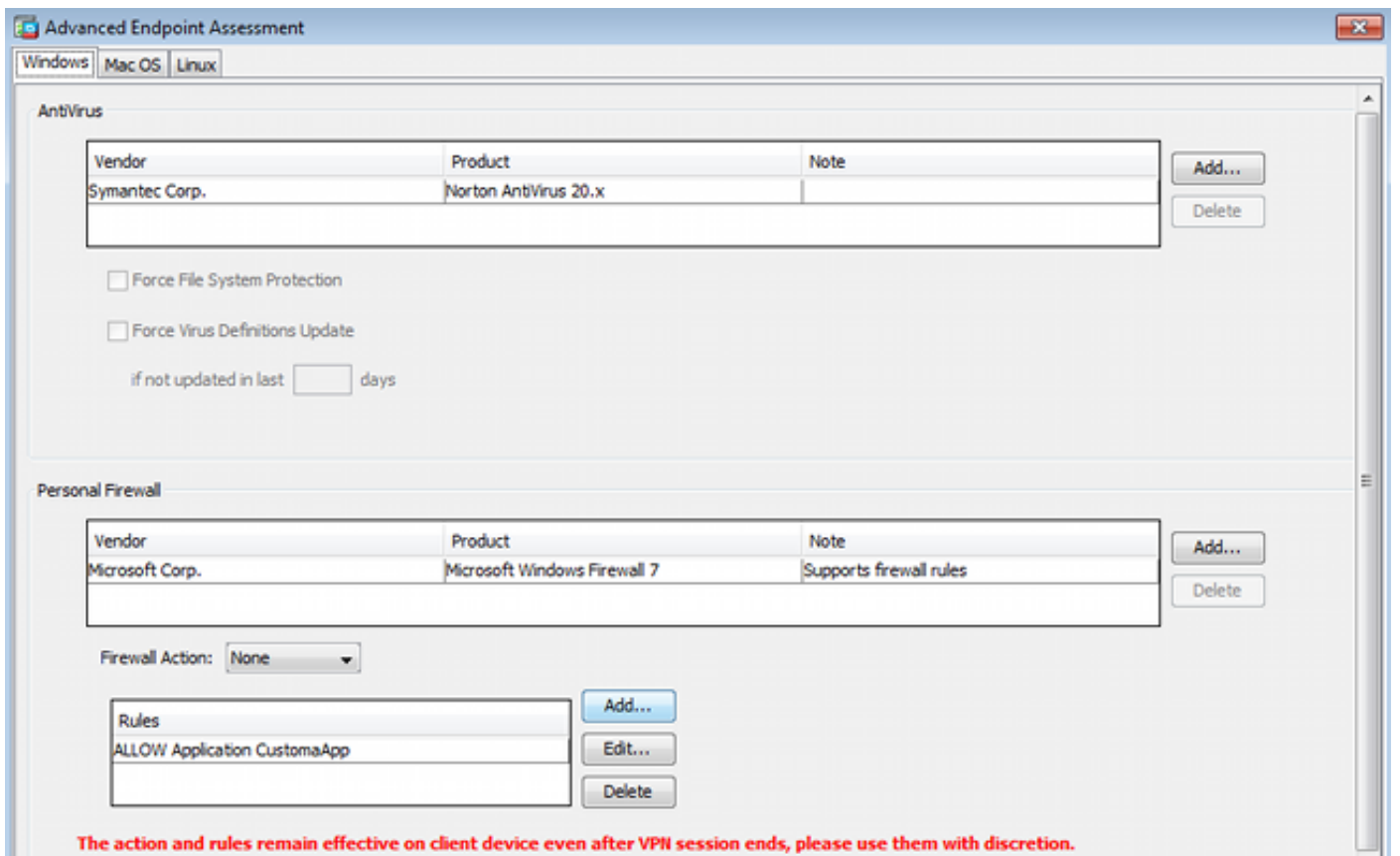
啟用CSD後，安全案頭管理器下會顯示多個選項。

附註：請注意，其中有些已棄用。有關不推薦使用的功能的更多資訊，請參閱：[安全案頭 \(Vault\)、快取清理器、按鍵記錄器檢測和主機模擬檢測的功能棄用通知](#)

仍完全支援HostScan，新增新的基本HostScan規則。如圖所示，c:\test.txt的存在已得到驗證。



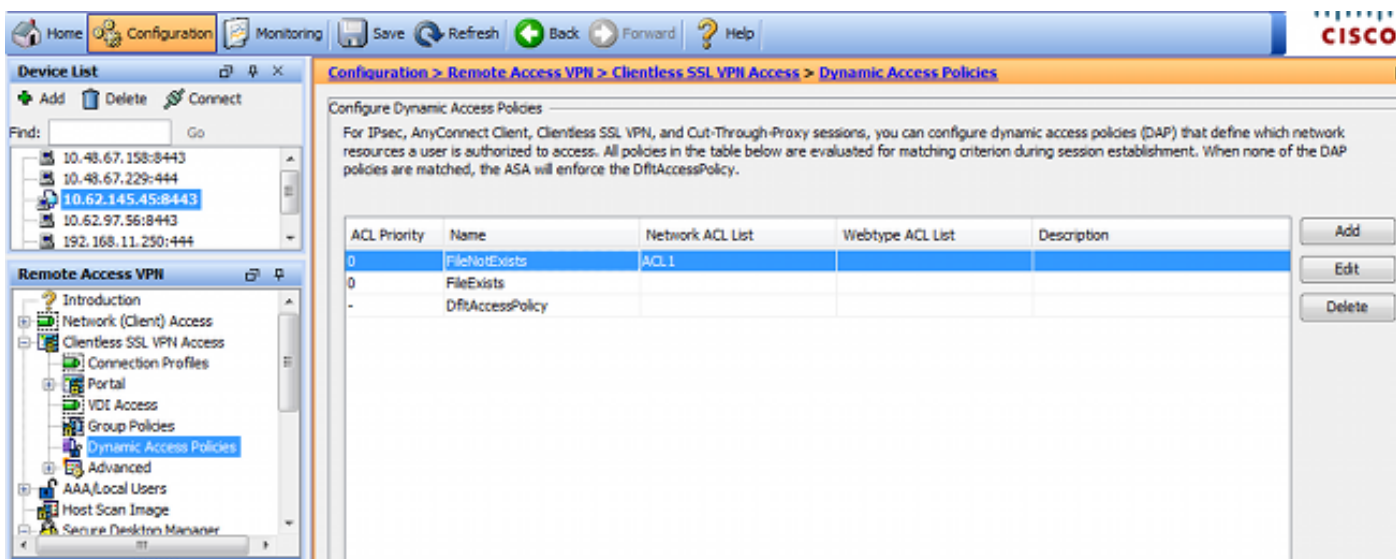
此外，還會新增其他高級終端評估規則，如下圖所示。



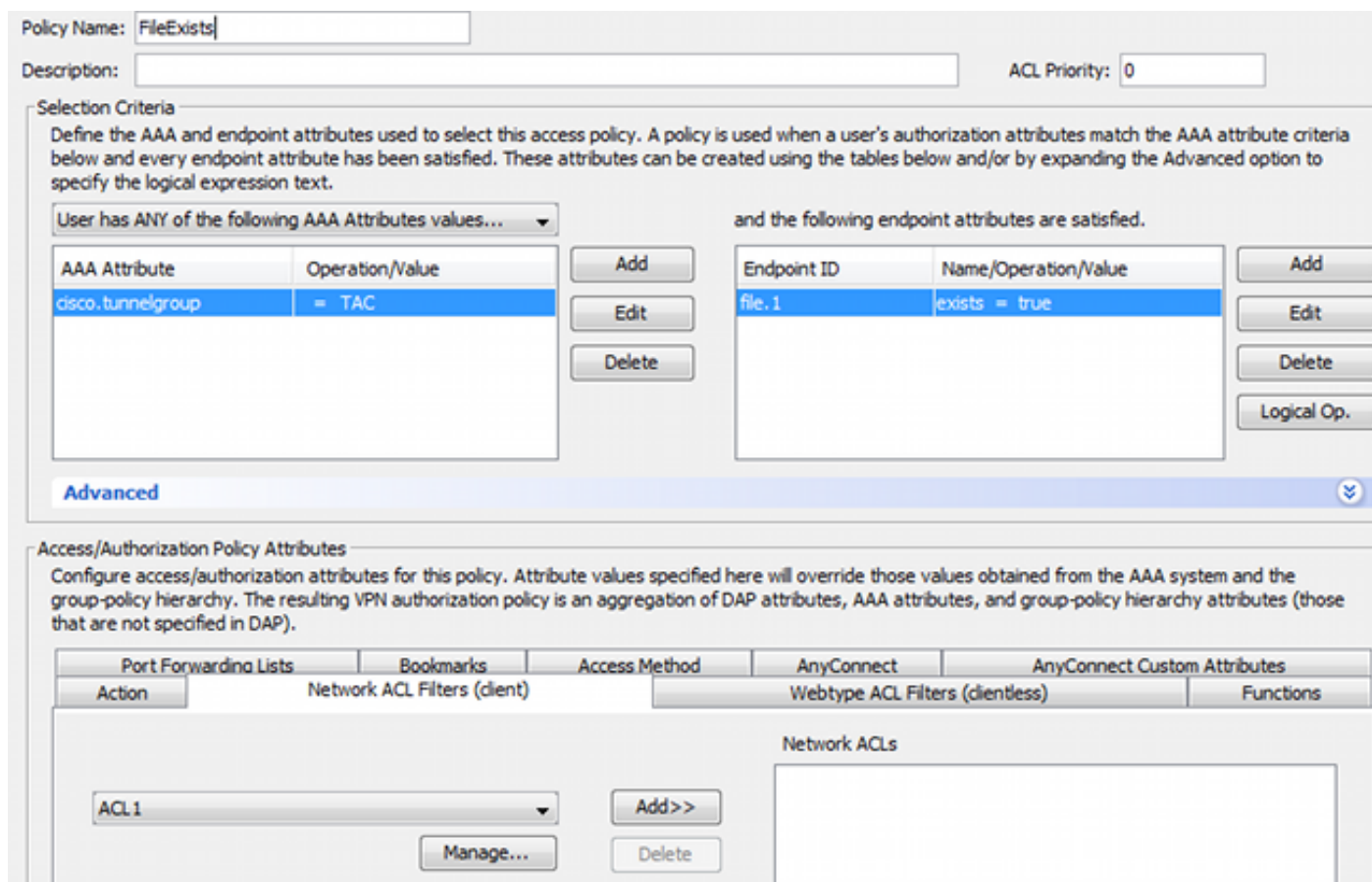
該策略檢查是否存在Symantec Norton AntiVirus 20.x和Microsoft Windows Firewall 7。狀態模組 (HostScan)檢查這些值，但不會強制執行 (DAP策略不會驗證這一點)。

步驟3. DAP策略

DAP策略負責使用HostScan收集的資料作為條件，並將特定屬性應用到VPN會話。若要從ASDM建立DAP策略，請導覽至**Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies**，如下圖所示。

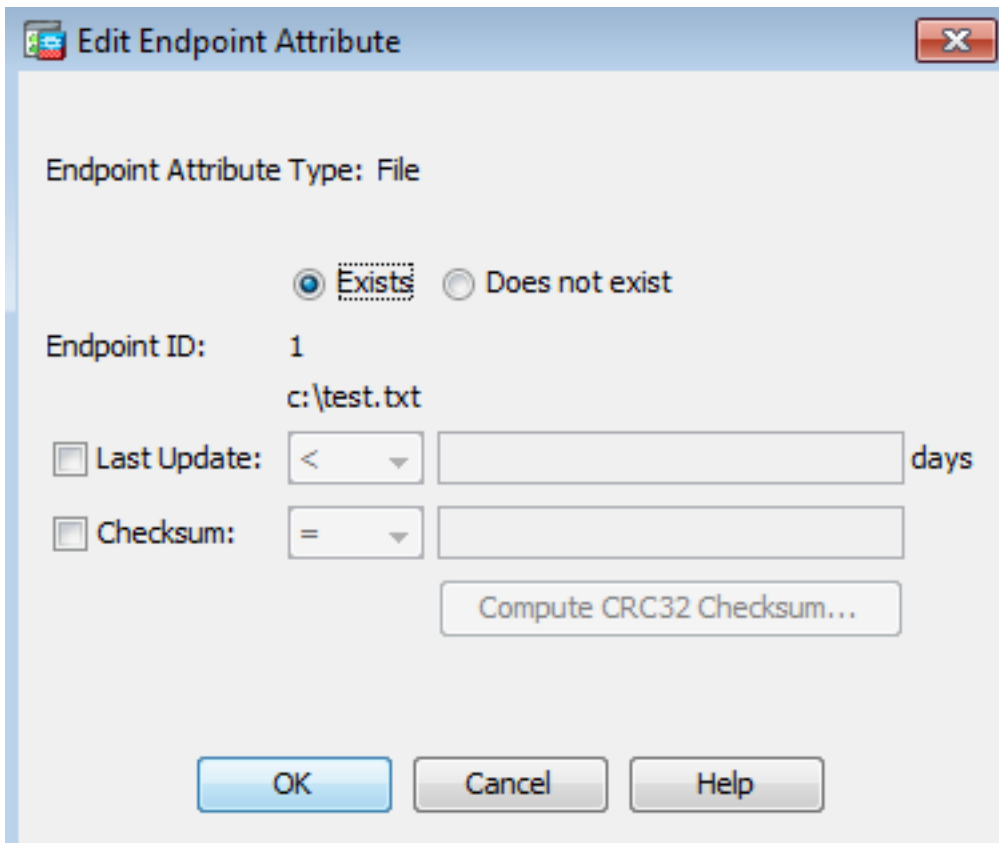


第一個策略(FileExists)檢查已配置的VPN配置檔案使用的隧道組名稱 (為清楚起見，已省略VPN配置檔案配置)。然後會執行其他檢查，檢查檔案c:\test.txt，如下圖所示。

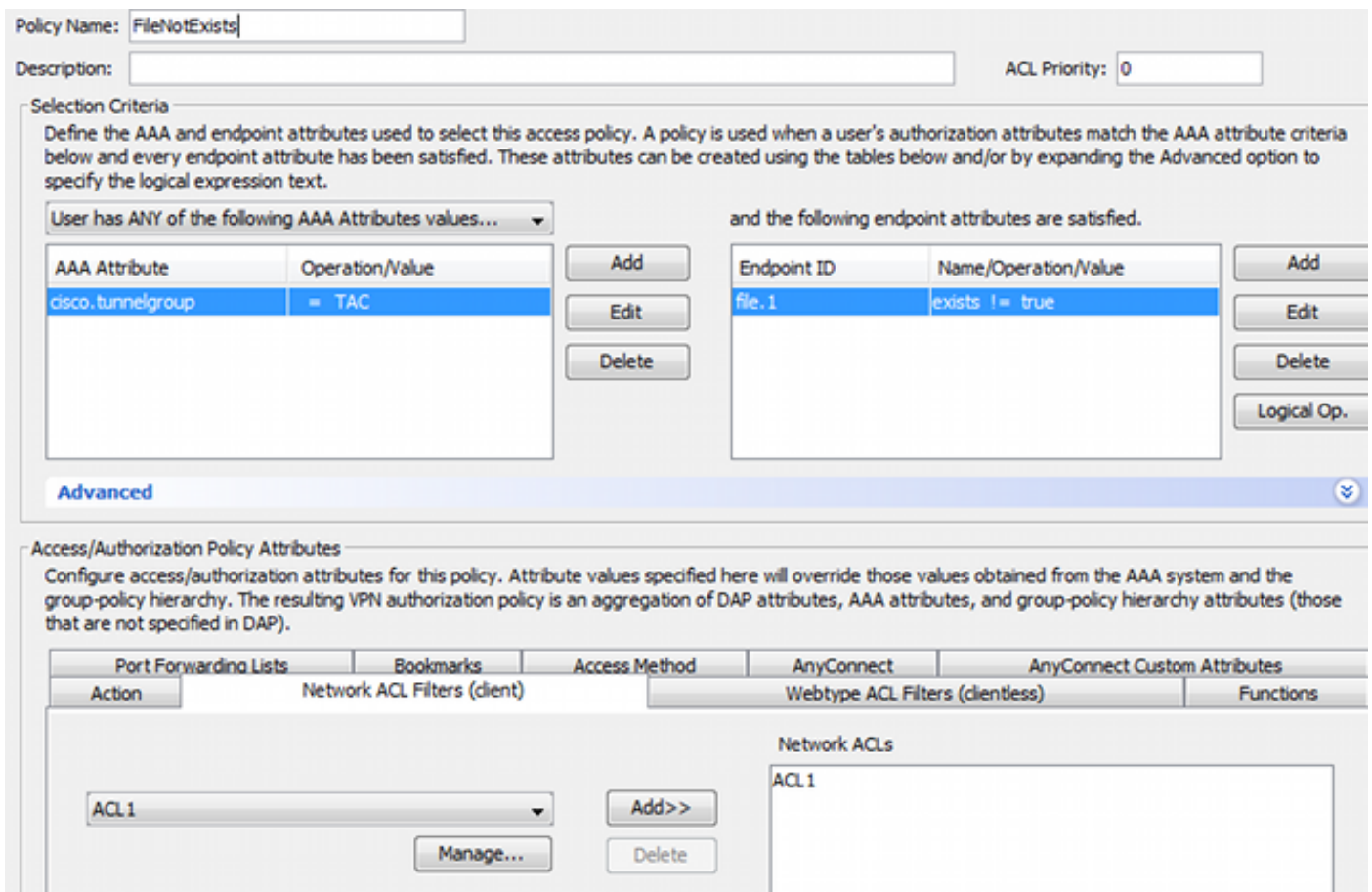


因此，不會使用預設設定執行任何操作來允許連線。未使用ACL — 提供完全網路訪問。

檔案檢查的詳情載於圖中。

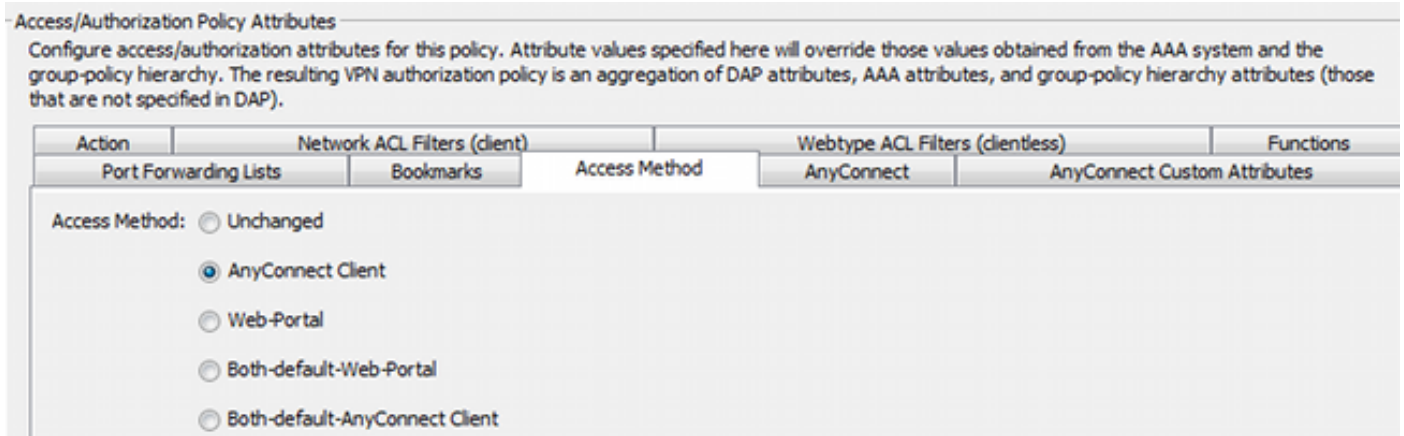


第二個策略(FileNotExists)類似 — 但此時間條件是**如果檔案不存在**，如下圖所示。



結果配置了access-list ACL1。適用於提供有限網路訪問的非合規VPN使用者。

兩個DAP策略都推送了AnyConnect客戶端訪問，如下圖所示。



ISE

ISE用於使用者身份驗證。必須僅配置網路裝置(ASA)和正確的使用者名稱(cisco)。本文未涉及該部分。

驗證

使用本節內容，確認您的組態是否正常運作。

CSD和AnyConnect調配

最初，使用者沒有使用AnyConnect客戶端進行調配。使用者也不符合策略(檔案c:\test.txt不存在)。輸入<https://10.62.145.45>，系統會立即將使用者重新導向以安裝CSD，如下圖所示。



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

這可以通過Java或ActiveX來實現。安裝CSD後，如圖所示進行報告。



Cisco Secure Desktop



WebLaunch

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

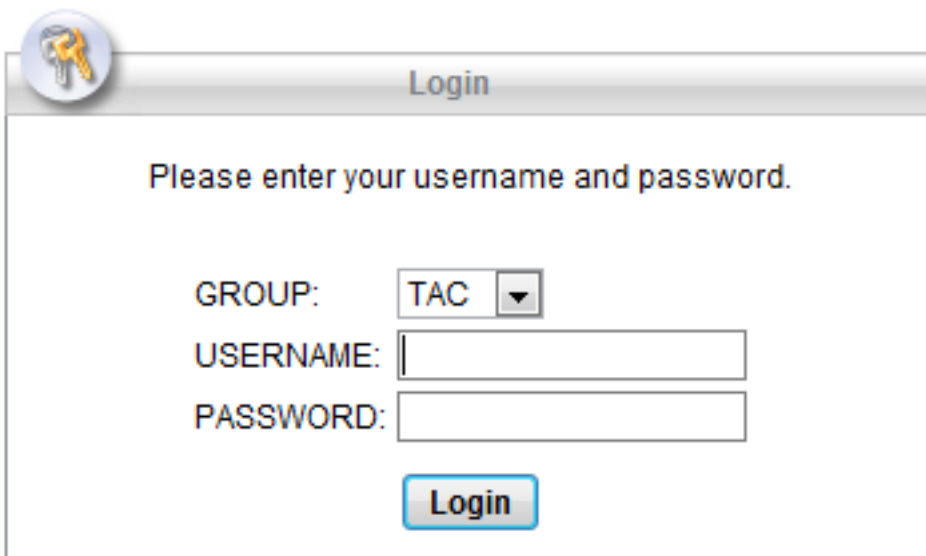
System Validated

Cisco Secure Desktop successfully validated your system.

Success. Reloading. Please wait...

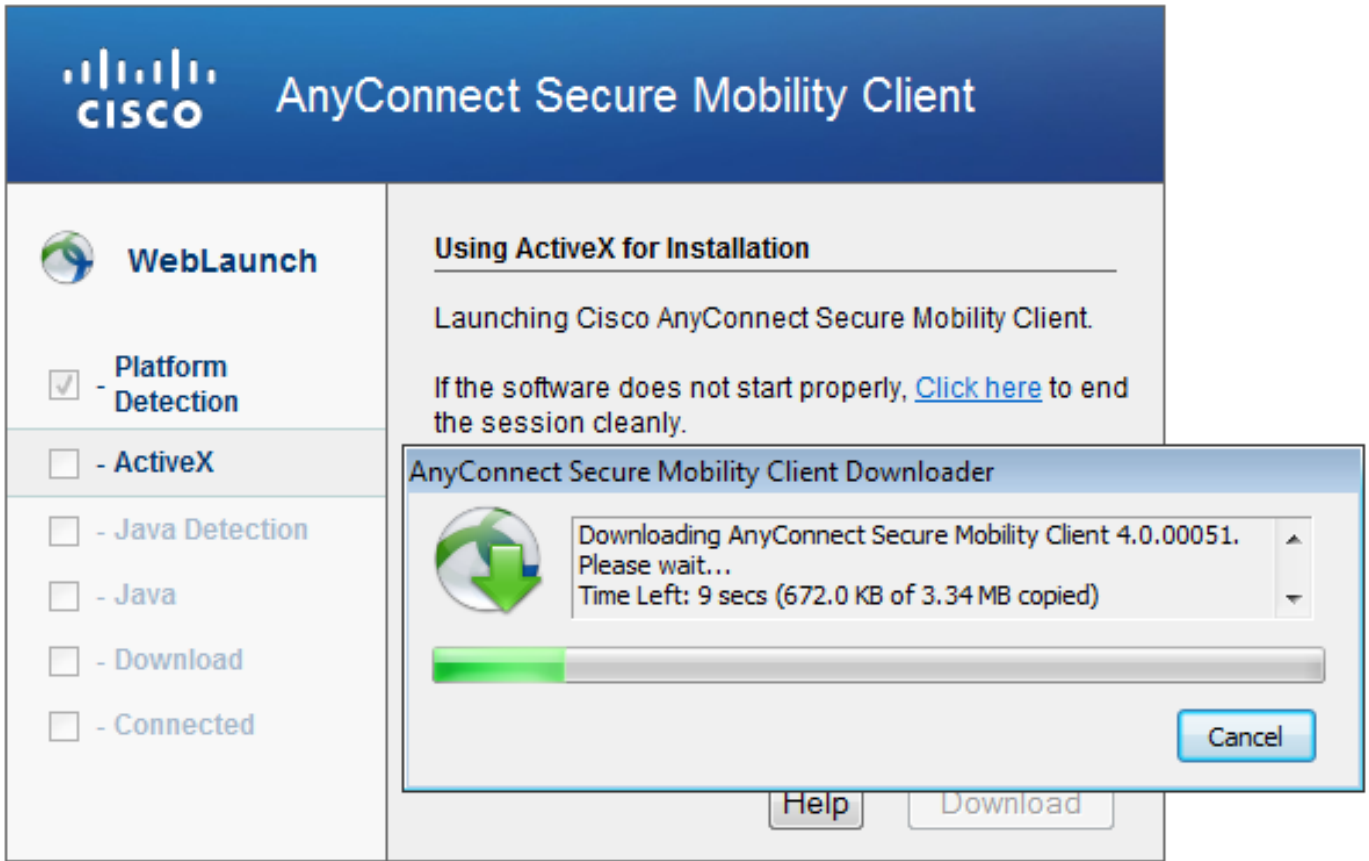
Download

然後使用者重新導向以進行驗證，如下圖所示。

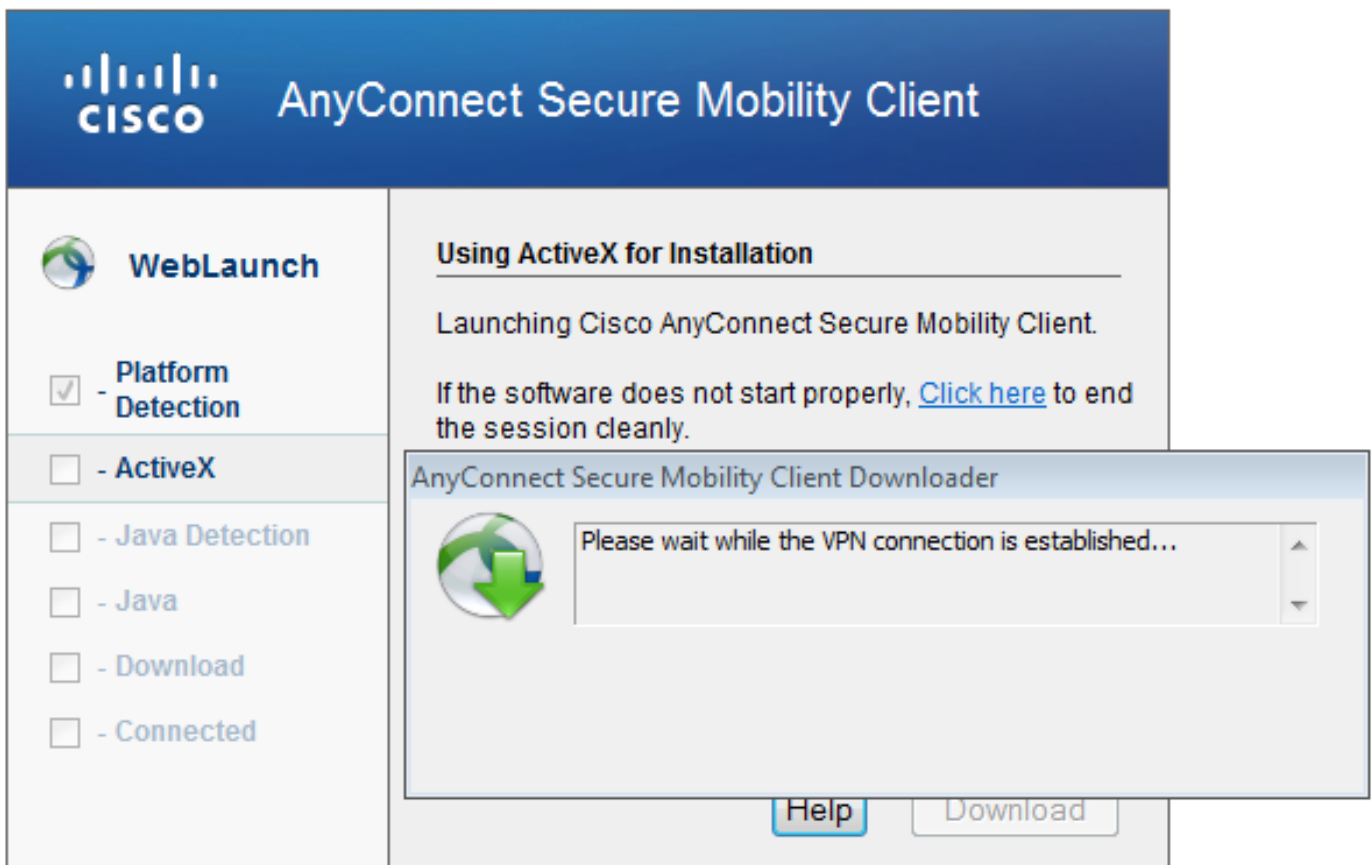


The image shows a 'Login' dialog box with a key icon in the top-left corner. The title bar reads 'Login'. The main text says 'Please enter your username and password.' Below this, there are three input fields: 'GROUP:' with a dropdown menu showing 'TAC', 'USERNAME:' with a text box, and 'PASSWORD:' with a text box. At the bottom center is a blue 'Login' button.

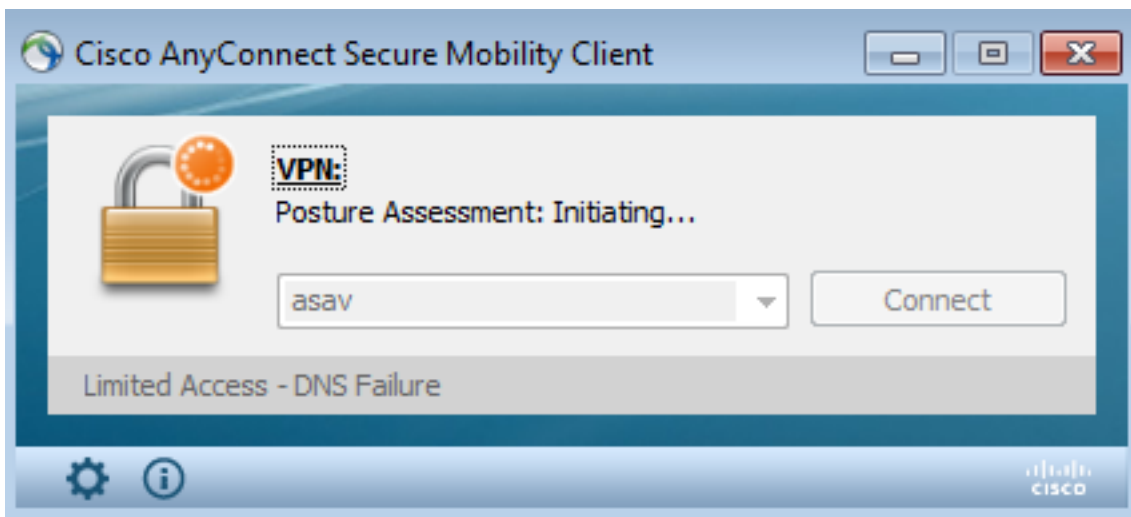
如果成功，將部署AnyConnect以及配置的配置檔案 — 同樣可以使用ActiveX或Java，如下圖所示。



並且，VPN連線已建立，如下圖所示。



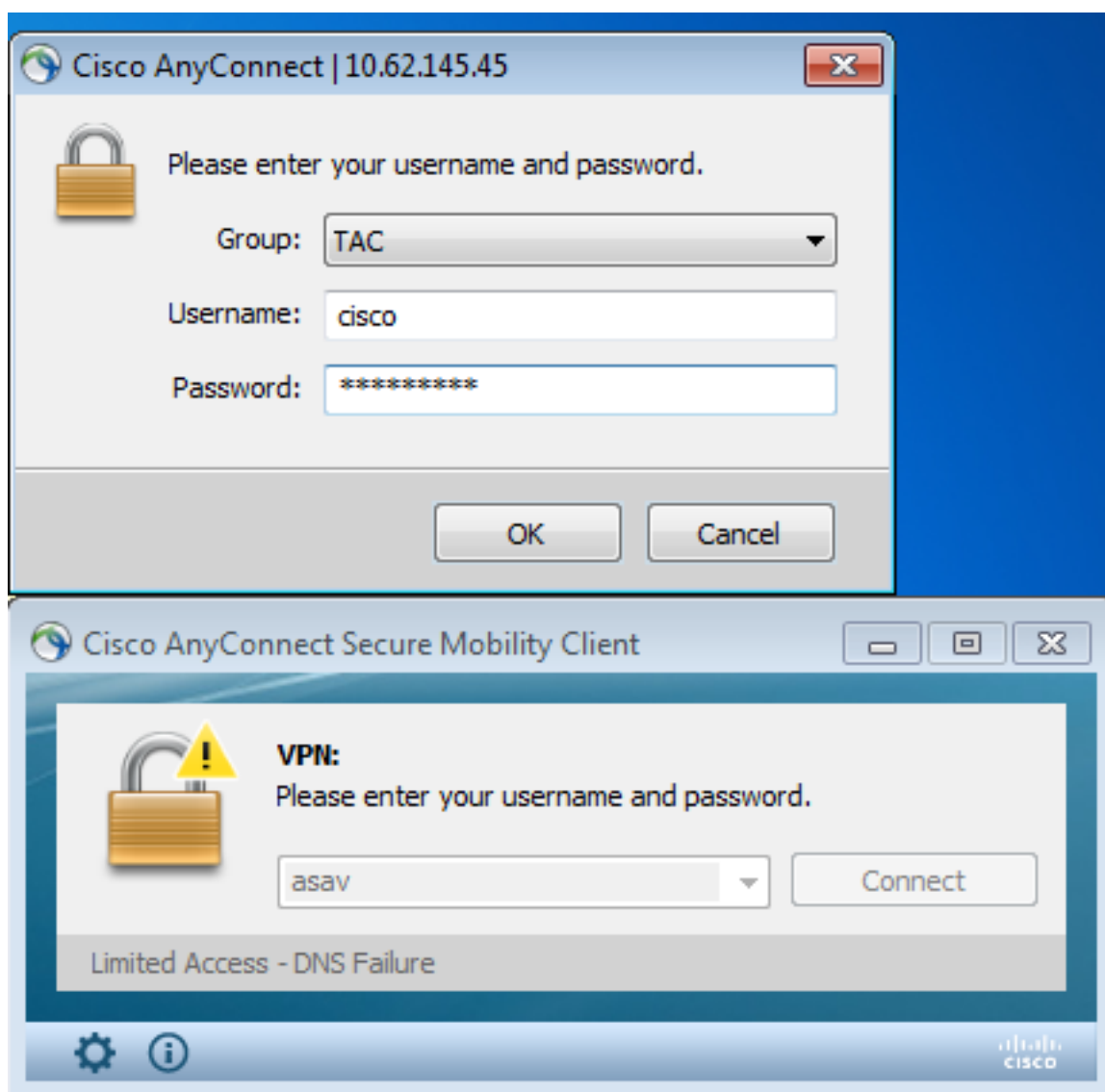
AnyConnect的第一步是執行狀態檢查(HostScan)並將報告傳送到ASA，如下圖所示。



然後，AnyConnect驗證並完成VPN會話。

安全狀態的AnyConnect VPN會話 — 不相容

當您使用AnyConnect建立新的VPN會話時，第一步是如螢幕截圖所示的終端安全評估狀態 (HostScan)。然後，進行身份驗證，並建立VPN會話，如圖所示。



ASA報告已收到HostScan報告：

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

然後執行使用者身份驗證：

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

並啟動該VPN會話的授權。啟用「debug dap trace 255」後，會返回有關c:\test.txt檔案存在的資訊：

```
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"
```

此外，有關Microsoft Windows防火牆的資訊：

```
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"
```

和Symantec AntiVirus (根據之前配置的HostScan Advanced Endpoint Assessment規則)。

因此，DAP策略匹配：

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

該策略強制使用AnyConnect並應用訪問清單ACL1，該清單為使用者提供受限的網路訪問 (不符合公司策略)：

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
```

日誌還顯示ACIDEX擴展，該擴展可由DAP策略使用 (或者甚至在Radius-Requests中傳遞到ISE，並在授權規則中用作條件)：

```
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";
```

因此，VPN會話為Up，但網路訪問受到限制：

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歷史記錄顯示了狀態進程的詳細步驟：

```
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.
```

安全狀態的AnyConnect VPN會話 — 相容

建立c:\test.txt檔案後，流程相似。啟動新的AnyConnect會話後，日誌將指示檔案的存在：

```
%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"
```

因此使用另一個DAP策略：

```
DAP_TRACE: Username: cisco, Selected DAPs: ,FileExists
該策略不會將任何ACL強制用作網路流量的限制。
```

且作業階段在沒有任何ACL的情況下為Up (完全網路存取)：

```
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

此外，Anyconnect報告HostScan處於空閒狀態並等待下一個掃描請求：

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

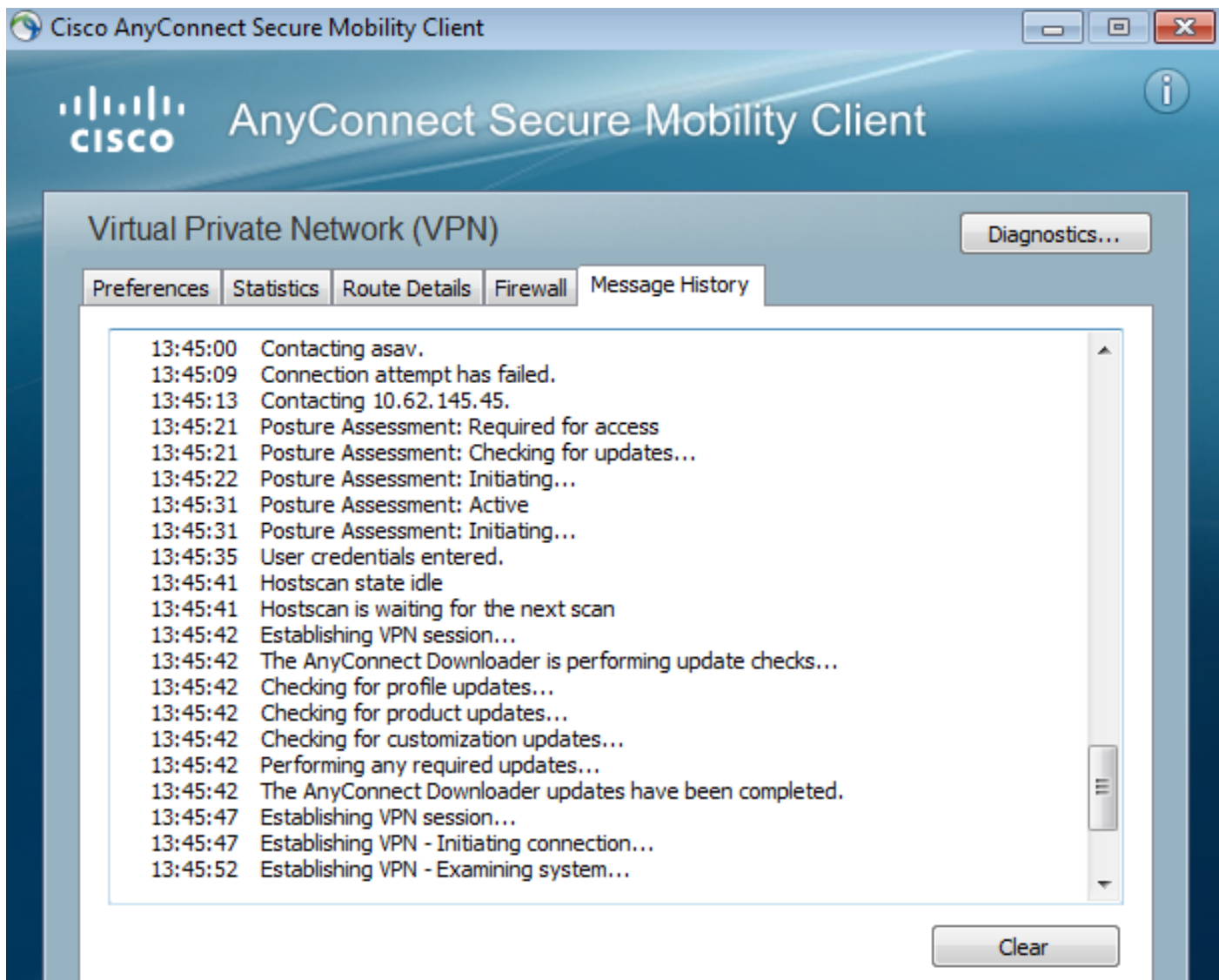
附註：對於重新評估，建議使用與ISE整合的狀態模組。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

AnyConnect DART

AnyConnect提供診斷，如下圖所示。



收集所有AnyConnect日誌並將其儲存到案頭上的zip檔案。該zip檔案包括Cisco AnyConnect Secure Mobility Client/Anyconnect.txt中的日誌。

它提供有關ASA的資訊，並請求HostScan收集資料：

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.

然後，多個其他日誌顯示CSD已安裝。以下是CSD調配和後續的AnyConnect連線以及安全狀態的示例：

```
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...
```

ASA和AnyConnect之間的通訊已最佳化，ASA請求僅執行特定檢查 — AnyConnect將下載其他資料以便執行該檢查（例如特定防病毒驗證）。

當您使用TAC開啟案例時，請附上Dart日誌以及ASA中的「show tech」和「debug dap trace 255」。

相關資訊

- [配置主機掃描和狀態模組 — Cisco AnyConnect安全移動客戶端管理員指南](#)
- [思科ISE上的終端安全評估服務配置指南](#)
- [思科ISE 1.3管理員指南](#)
- [技術支援與文件 - Cisco Systems](#)