CSD, DAP 및 AnyConnect 4.0으로 ASA VPN 상태 구성

목차

소개

이 문서에서는 ASA(Adaptive Security Appliance)에서 종료된 원격 VPN 세션에 대한 포스처를 수행하는 방법에 대해 설명합니다. 포스처는 HostScan 모듈과 함께 Cisco CSD(Secure Desktop)를 사용하여 ASA에서 로컬로 수행됩니다.VPN 세션이 설정되면 규정 준수 스테이션은 전체 네트워크 액세스가 허용되지만 규정을 준수하지 않는 스테이션은 네트워크 액세스가 제한됩니다.

또한 CSD 및 AnyConnect 4.0 프로비저닝 플로우가 표시됩니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco ASA VPN 컨피그레이션
- Cisco AnyConnect Secure Mobility Client

사용되는 구성 요소

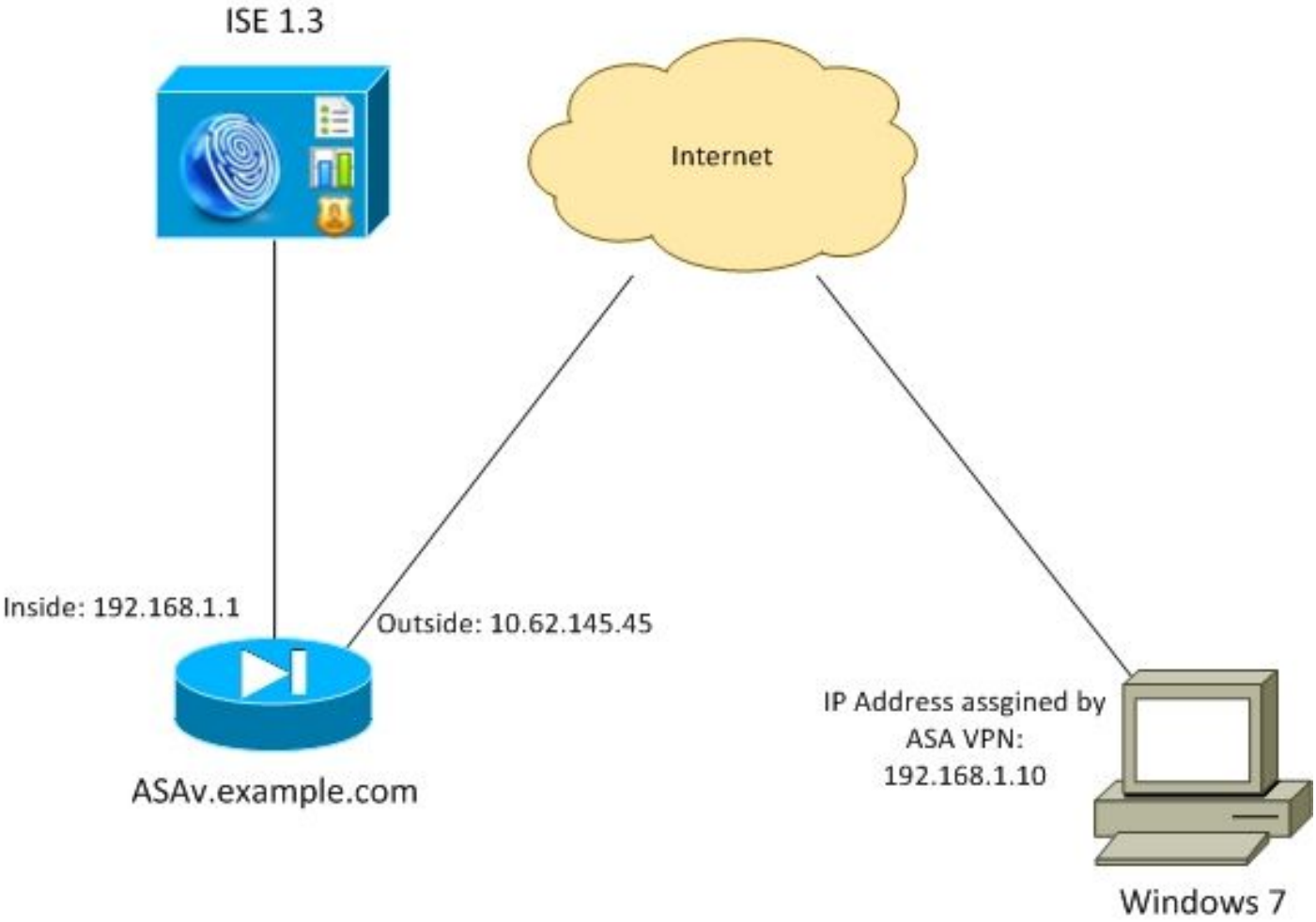
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Microsoft Windows 7
- Cisco ASA, 버전 9.3 이상
- Cisco ISE(Identity Services Engine) 소프트웨어, 버전 1.3 이상
- Cisco AnyConnect Secure Mobility Client, 버전 4.0 이상
- CSD, 버전 3.6 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

구성

네트워크 다이어그램



기업 정책은 다음과 같습니다.

- c:\test.txt 파일(규정 준수)이 있는 원격 VPN 사용자는 내부 회사 리소스에 대한 전체 네트워크 액세스 권한이 있어야 합니다.
- c:\test.txt 파일이 없는 원격 VPN 사용자는 내부 회사 리소스에 대한 네트워크 액세스가 제한되어야 합니다.리미디에이션 서버 1.1.1.1에 대한 액세스만 제공됩니다.

파일 존재 자체가 가장 간단한 예입니다.다른 모든 조건(안티바이러스, 안티스파이웨어, 프로세스, 애플리케이션, 레지스트리)을 사용할 수 있습니다.

플로우는 다음과 같습니다.

- 원격 사용자에게 AnyConnect가 설치되어 있지 않습니다.CSD 및 AnyConnect 프로비저닝을 위한 ASA 웹 페이지(VPN 프로필과 함께)에 액세스합니다.
- AnyConnect를 통한 연결이 이루어지면 네트워크 액세스가 제한되어 규정을 준수하지 않는 사용자가 허용됩니다.FileNotExists라는 DAP(Dynamic Access **Policy)가** 일치합니다.
- 사용자가 리미디에이션(수동으로 파일 설치 **c:\test.txt**)을 수행하고 AnyConnect에 다시 연결합니다.이번에는 전체 네트워크 액세스가 제공됩니다(FileExists라는 DAP 정책**이** 일치함).

HostScan 모듈은 엔드포인트에 수동으로 설치할 수 있습니다.예제 파일(hostscan-win-4.0.00051-pre-deploy-k9.msi)은 CCO(Cisco Connection Online)에서 공유됩니다. 하지만 ASA에서 푸시될 수도 있습니다.HostScan은 ASA에서 프로비저닝할 수 있는 CSD의 일부입니다.이 예제에서는 두 번째 방법을 사용합니다.

이전 버전의 AnyConnect(3.1 이하)에서는 CCO에서 사용할 수 있는 별도의 패키지가 있습니다(예:ASA에서 별도로 구성 및 프로비저닝될 수 있는 hostscan_3.1.06073-k9.pkg(csd hostscan **image** 명령 사용) - 그러나 AnyConnect 버전 4.0에는 이 옵션이 더 이상 존재하지 않습니다.

ASA

1단계. 기본 SSL VPN 컨피그레이션

ASA는 기본 원격 VPN 액세스(SSL(Secure Sockets Layer))로 미리 구성됩니다.

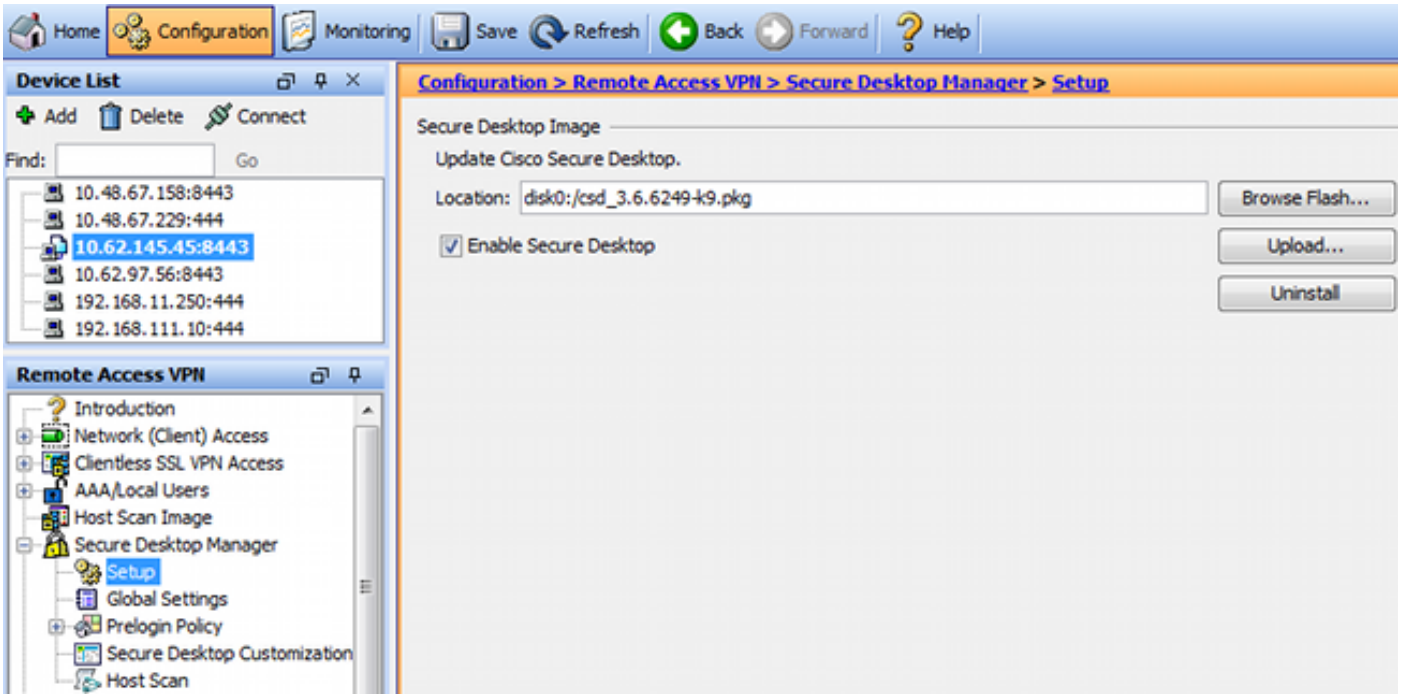
```
webvpn
 enable outside
 no anyconnect-essentials
 anyconnect image disk0:/anyconnect-win-4.0.00051-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable

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 패키지가 다운로드되어 사용되었습니다.

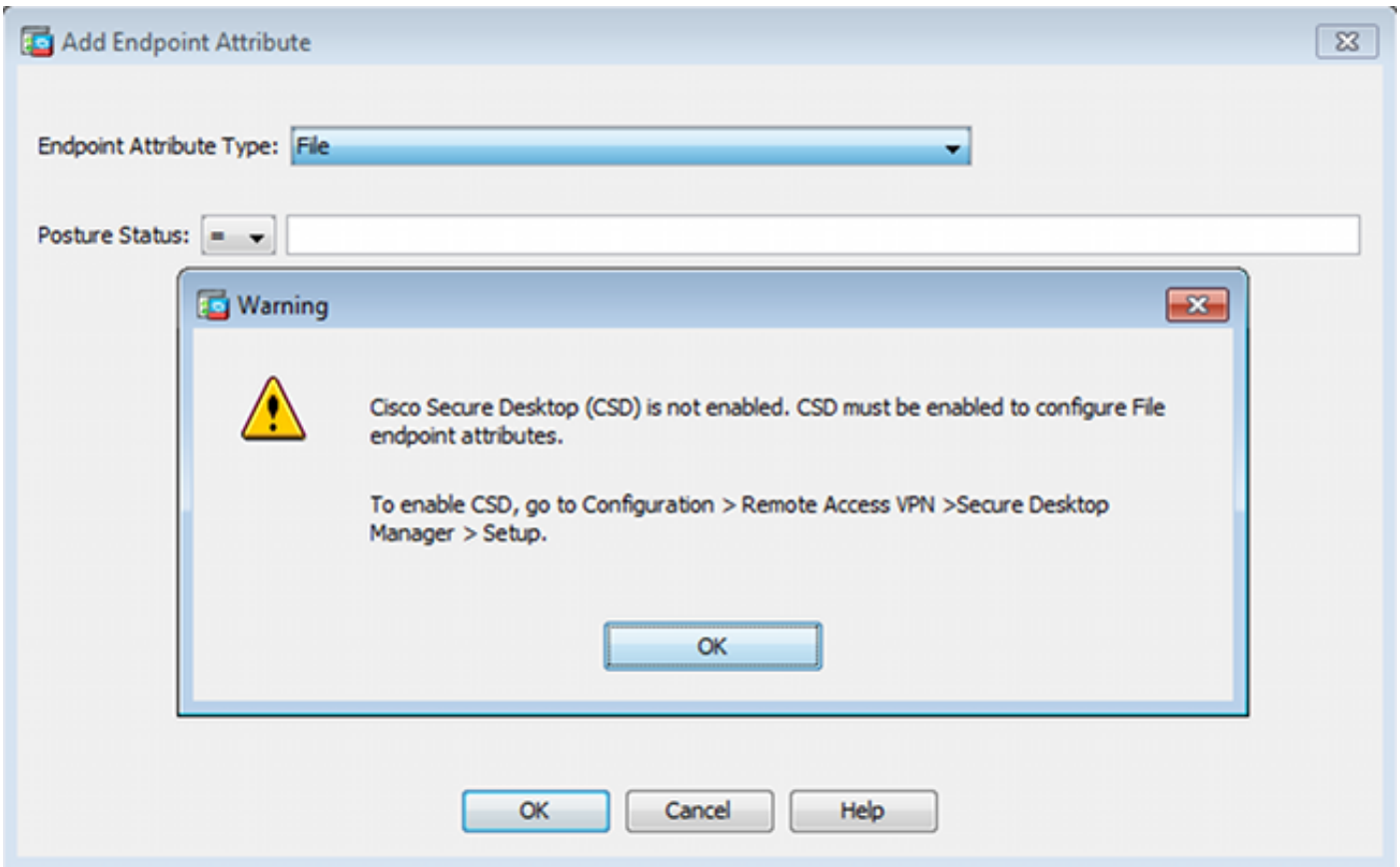
2단계. CSD 설치

후속 컨피그레이션은 ASDM(Adaptive Security Device Manager)을 사용하여 수행됩니다.이미지에

표시된 대로 컨피그레이션에서 참조를 가져오려면 CSD 패키지를 다운로드해야 합니다.



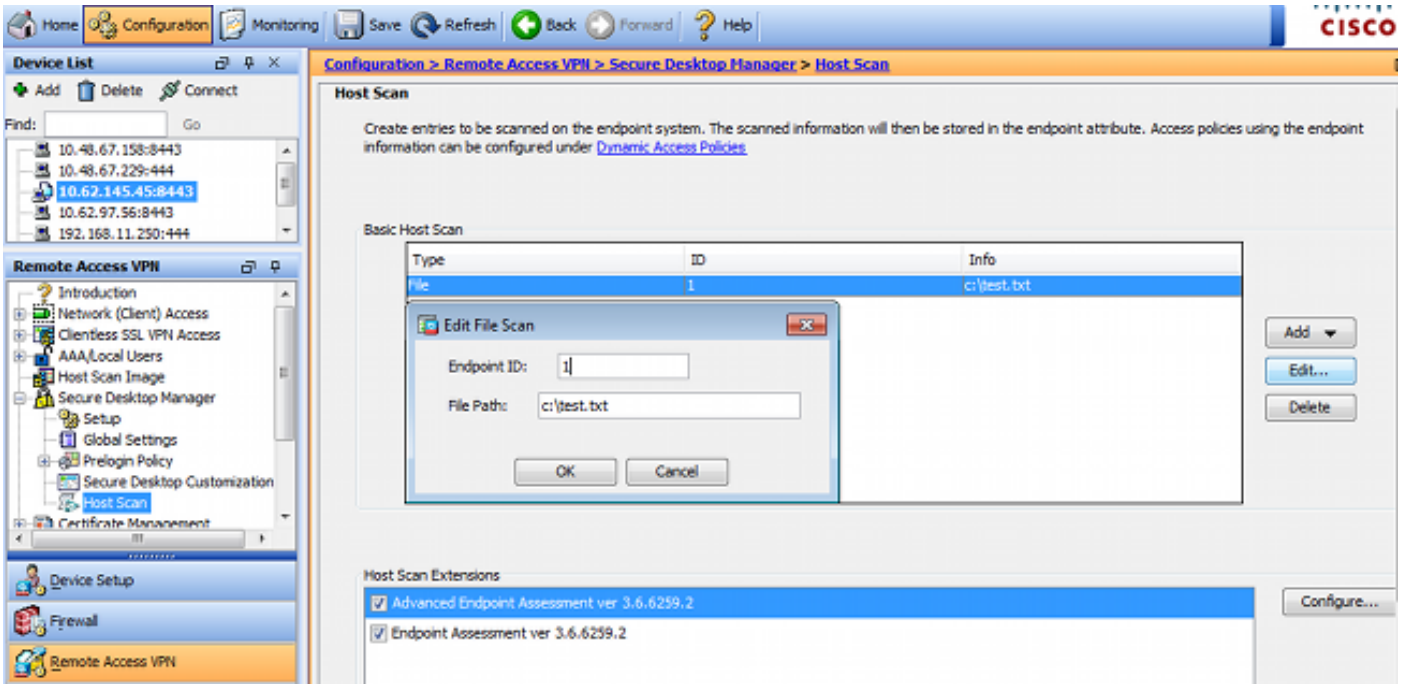
Secure Desktop을 활성화하지 않으면 이미지에 표시된 대로 DAP 정책에서 CSD 특성을 사용할 수 없습니다.



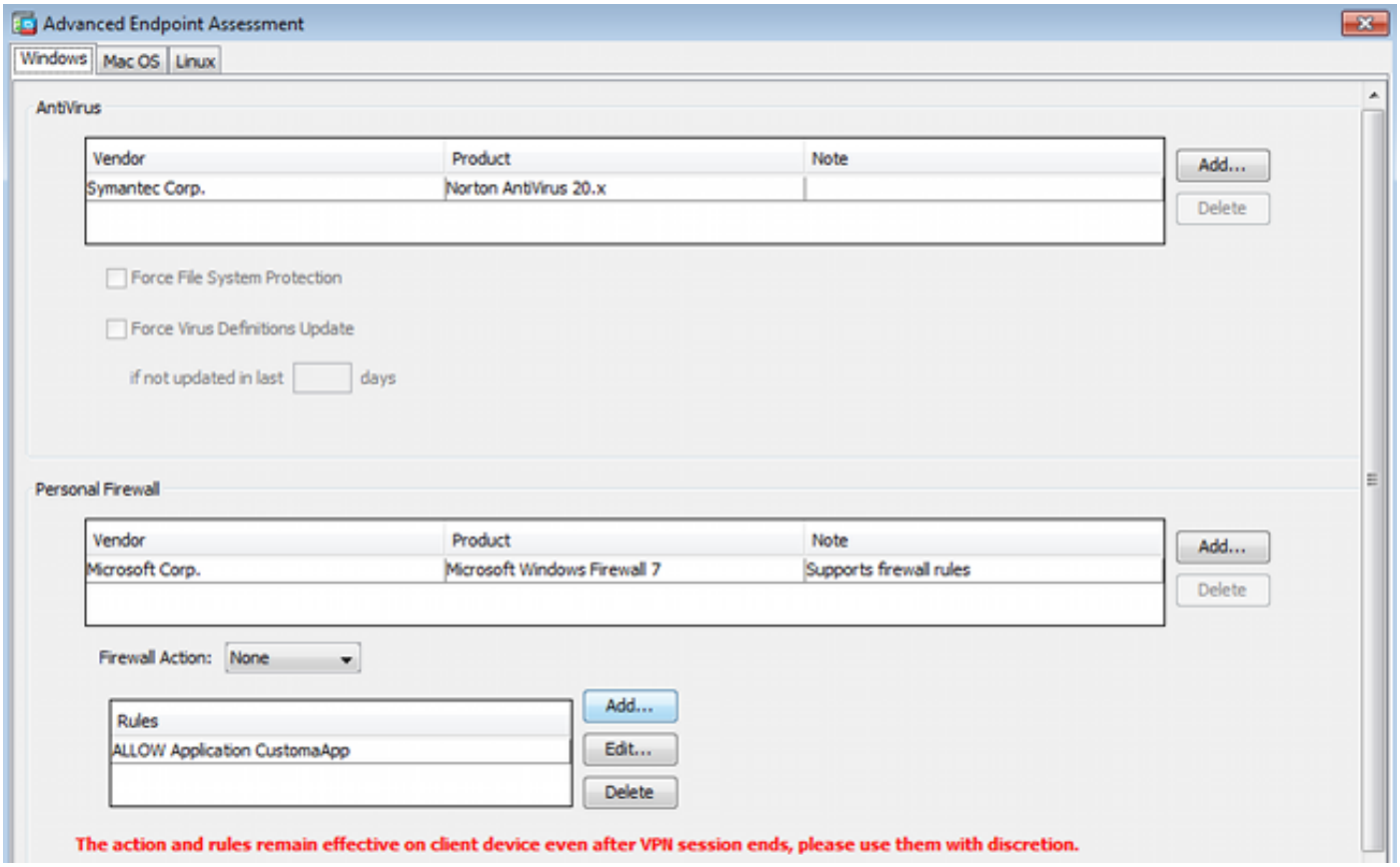
CSD를 활성화하면 Secure Desktop Manager 아래에 여러 옵션이 나타납니다.

> **참고:**이들 중 일부는 이미 사용되지 않음을 알려주십시오.사용되지 않는 기능에 대한 자세한 내용은 다음을 참조하십시오.Secure Desktop(Vault), Cache Cleaner, Keystroke Logger Detection 및 Host Emulation Detection에 대한 기능 사용 중단 알림

HostScan은 여전히 완벽하게 지원되며 새로운 Basic HostScan 규칙이 추가됩니다.이미지에 표시된 대로 **c:\test.txt**의 존재 여부를 확인합니다.



또한 이미지에 표시된 대로 추가 고급 엔드포인트 평가 규칙이 추가됩니다.

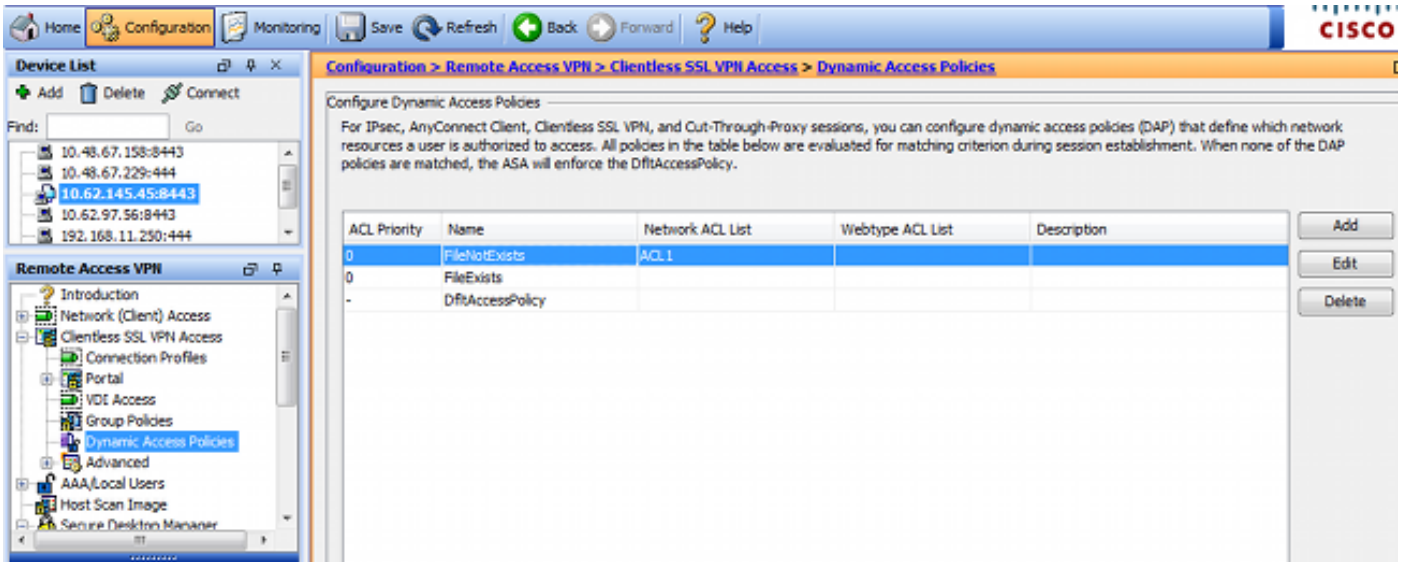


Symantec Norton AntiVirus 20.x 및 Microsoft Windows Firewall 7이 있는지 확인합니다. Posture 모듈(HostScan)은 이러한 값을 확인하지만 시행은 수행되지 않습니다(DAP 정책은 확인하지 않음).

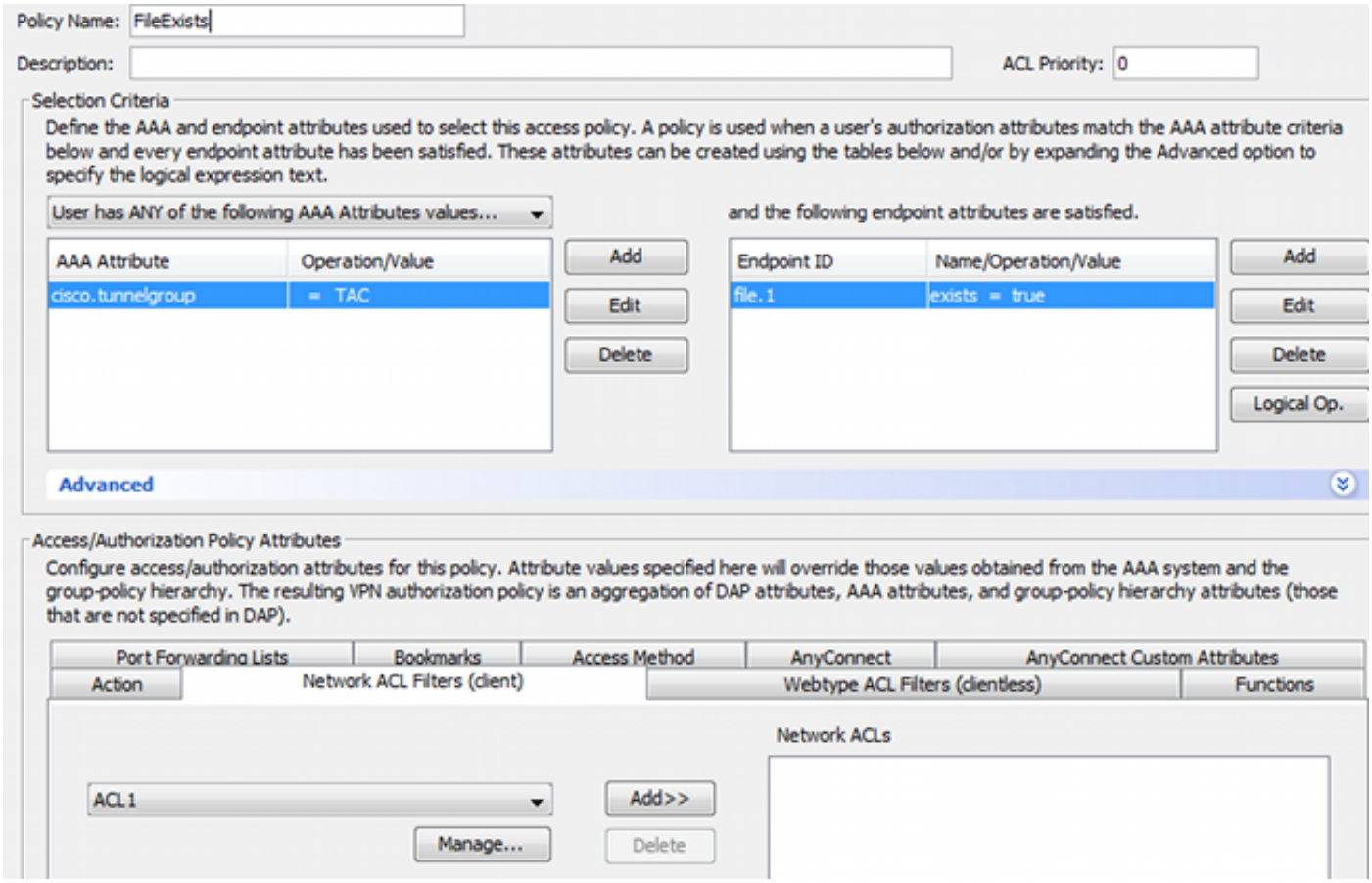
3단계. DAP 정책

DAP 정책은 HostScan에서 수집한 데이터를 조건으로 사용하고 그 결과 특정 특성을 VPN 세션에

적용해야 합니다.ASDM에서 DAP 정책을 생성하려면 이미지에 표시된 대로 **Configuration(구성) > Remote Access VPN(원격 액세스 VPN) > Clientless SSL VPN Access(클라이언트리스 SSL VPN 액세스) > Dynamic Access Policies(동적 액세스 정책)로** 이동합니다.

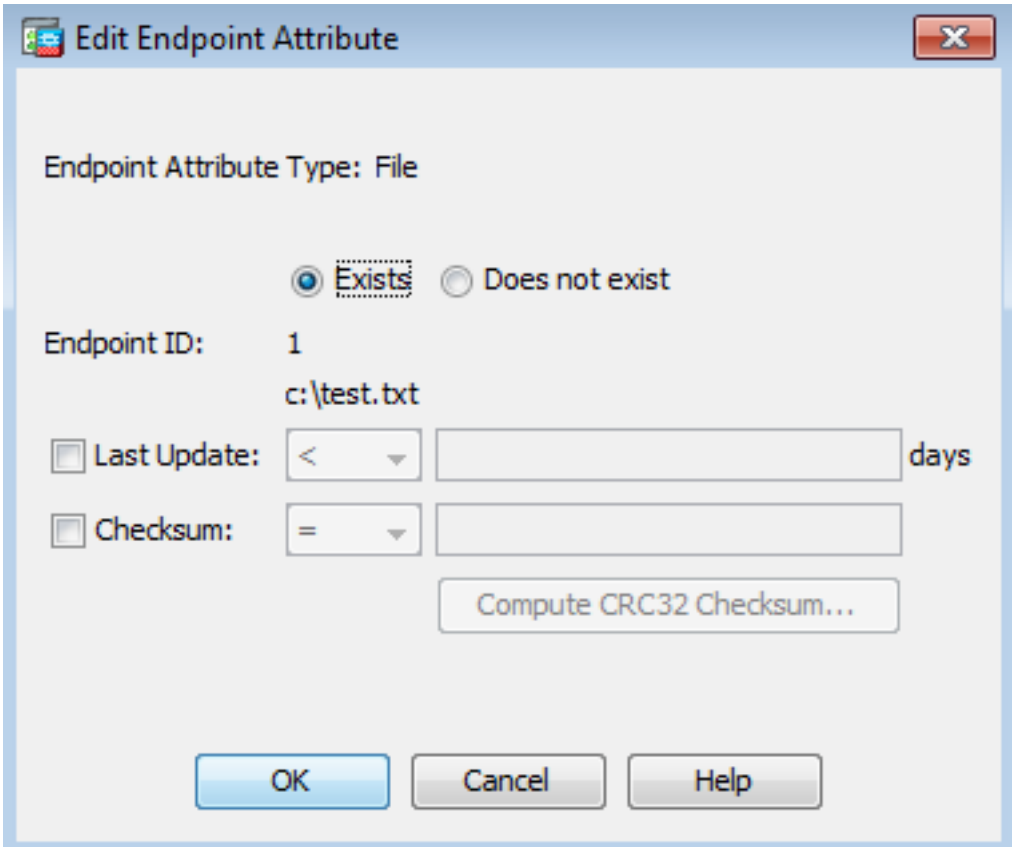


첫 번째 정책(FileExists)은 구성된 VPN 프로필에 사용되는 터널 그룹 이름을 확인합니다(VPN 프로필 컨피그레이션은 명확성을 위해 생략됨). 그런 다음 이미지에 표시된 대로 **c:\test.txt** 파일에 대한 추가 검사가 수행됩니다.

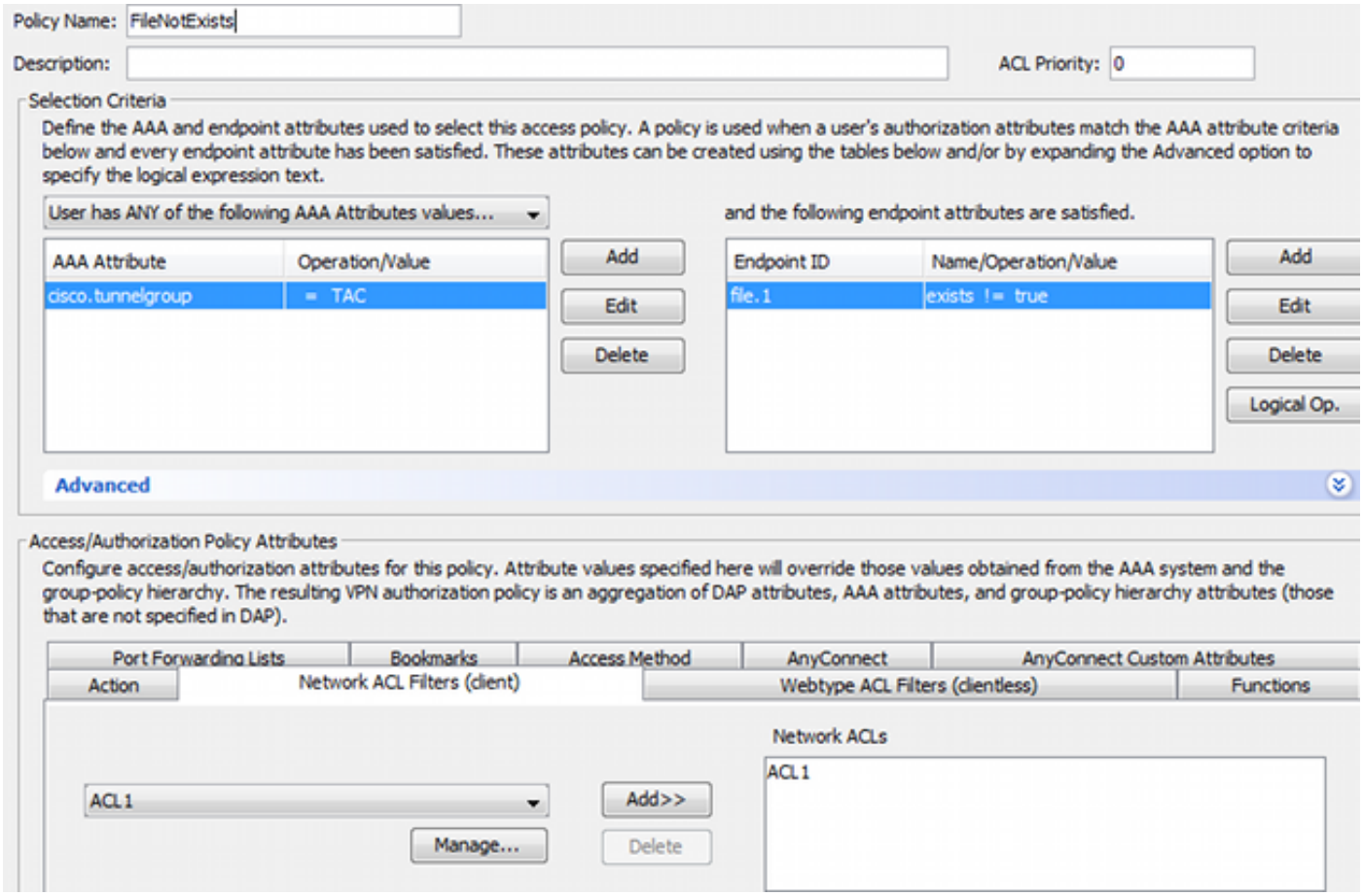


따라서 연결을 허용하기 위해 기본 설정으로 어떤 작업도 수행되지 않습니다.ACL이 사용되지 않습니다. 전체 네트워크 액세스가 제공됩니다.

파일 확인에 대한 자세한 내용은 이미지에 나와 있습니다.

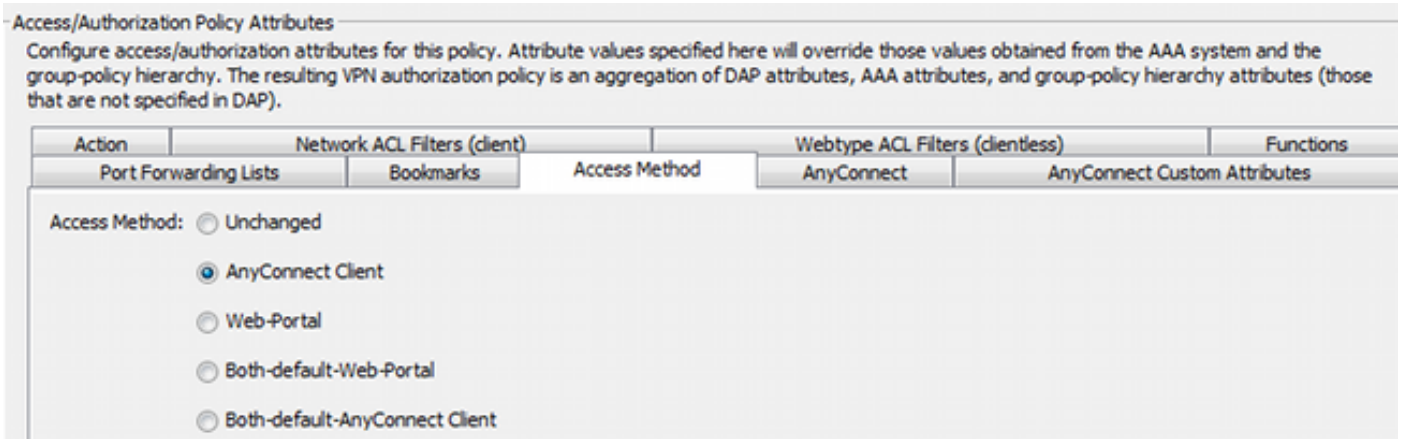


두 번째 정책(FileNotExists)은 비슷하지만 이 시간 조건은 이미지에 표시된 것처럼 **파일이 존재하지 않는 경우입니다**.



그 결과 access-list ACL1이 구성되었습니다.이는 제한된 네트워크 액세스 프로비저닝을 통해 규정을 준수하지 않는 VPN 사용자에게 적용됩니다.

두 DAP 정책 모두 이미지에 표시된 대로 AnyConnect 클라이언트 액세스를 푸시합니다.



ISE

ISE는 사용자 인증에 사용됩니다.네트워크 장치(ASA) 및 올바른 사용자 이름(cisco)만 구성해야 합니다.그 부분은 이 기사에서 다루지 않는다.

다음을 확인합니다.

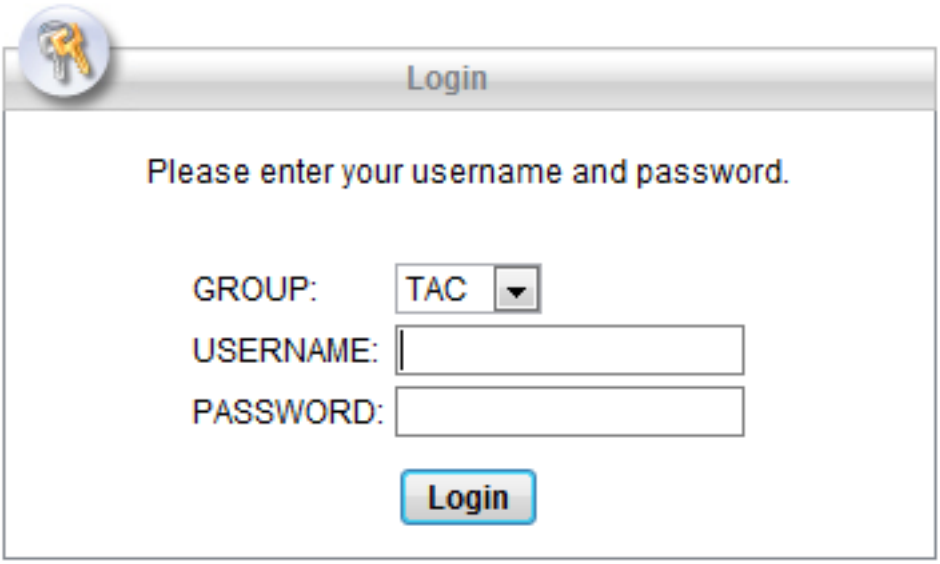
이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

CSD 및 AnyConnect 프로비저닝

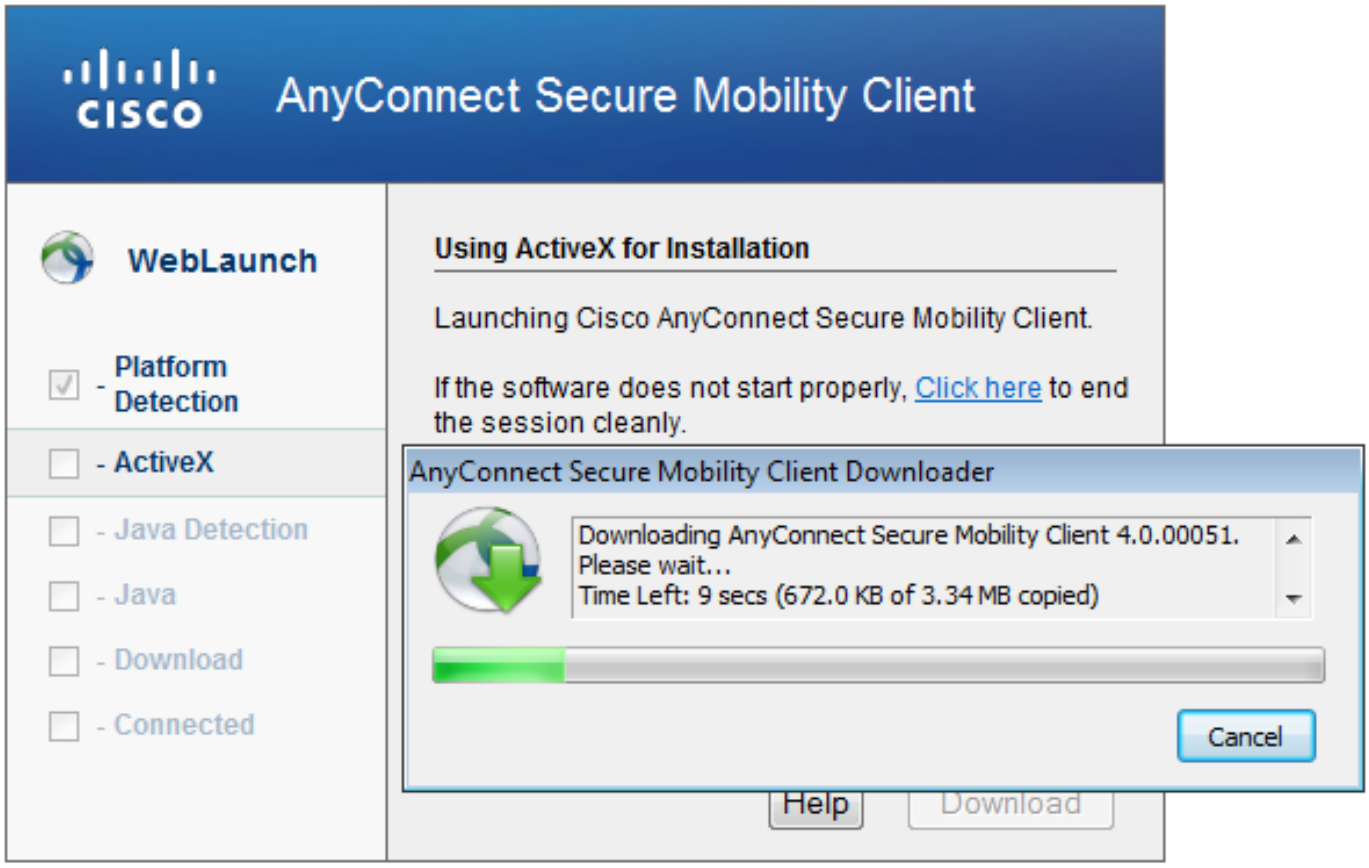
처음에는 사용자가 AnyConnect 클라이언트로 프로비저닝되지 않습니다.또한 사용자가 정책을 준수하지 않습니다(c:\test.txt 파일이 존재하지 않음). https://10.62.145.45를 입력하면 이미지에 표시된 대로 CSD 설치를 위해 사용자가 즉시 리디렉션됩니다.

이는 Java 또는 ActiveX를 사용하여 수행할 수 있습니다.CSD가 설치되면 이미지에 표시된 대로 보고됩니다.

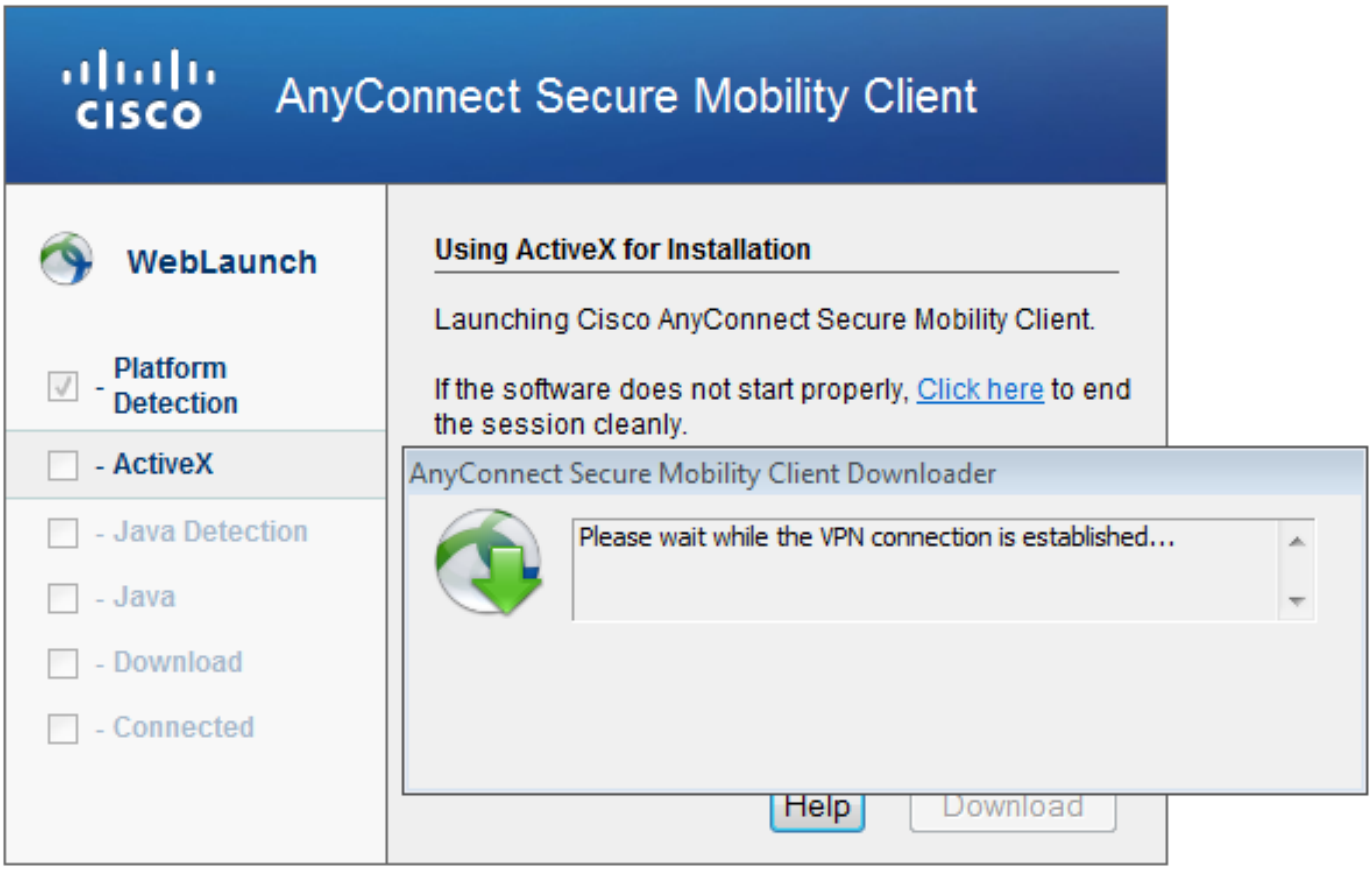
그러면 이미지에 표시된 대로 인증을 위해 사용자가 리디렉션됩니다.



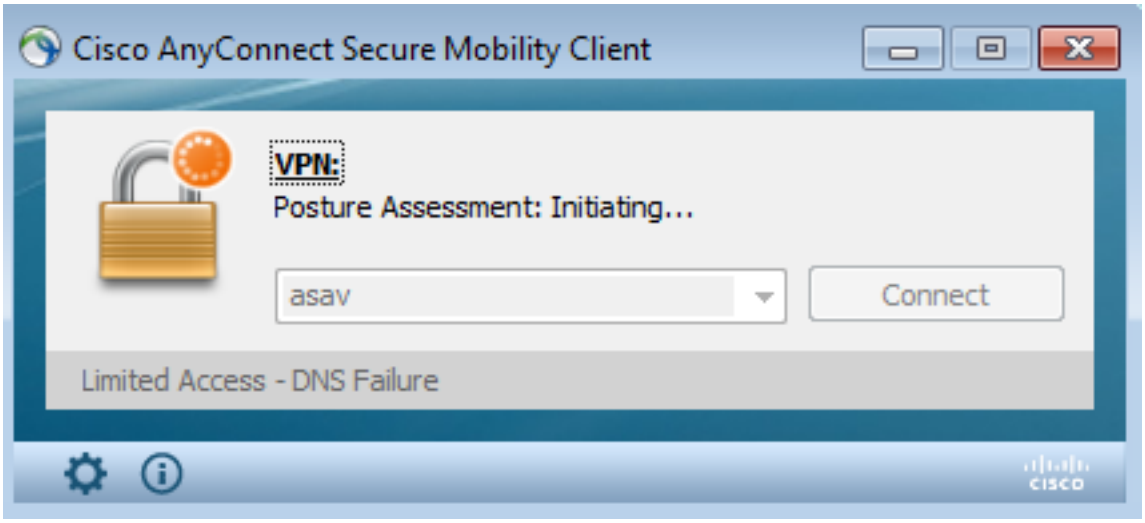
성공한 경우 구성된 프로파일과 함께 AnyConnect가 구축됩니다. 이미지에 표시된 대로 ActiveX 또는 Java를 다시 사용할 수 있습니다.



VPN 연결은 이미지에 표시된 대로 설정됩니다.



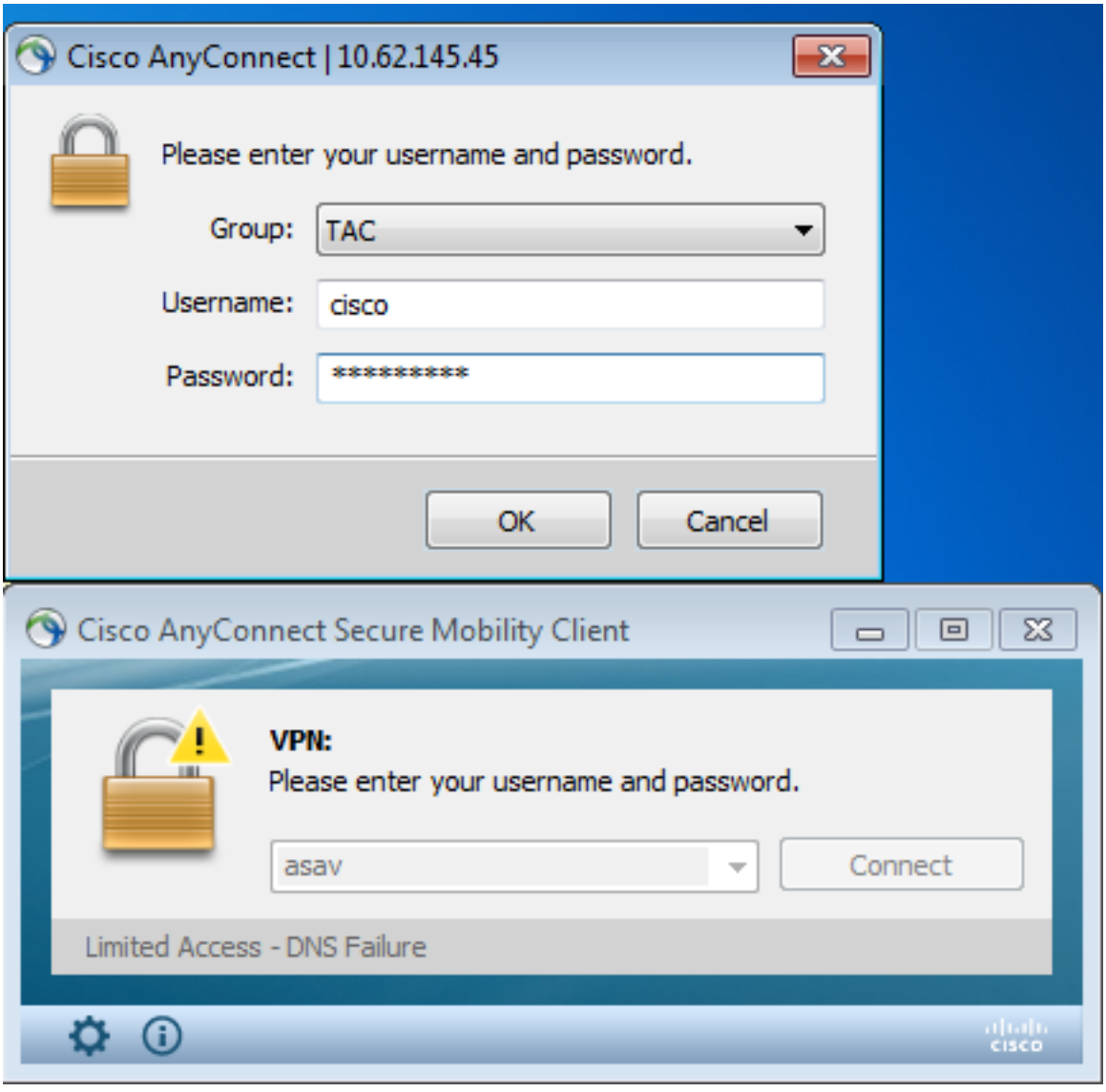
AnyConnect의 첫 번째 단계는 상태 확인(HostScan)을 수행하고 이미지에 표시된 대로 보고서를 ASA로 전송하는 것입니다.



그런 다음 AnyConnect가 VPN 세션을 인증하고 완료합니다.

AnyConnect VPN 세션(상태 - 비준수)

AnyConnect를 사용하여 새 VPN 세션을 설정할 때 첫 번째 단계는 이전 스크린샷에 표시된 상태(HostScan)입니다.그런 다음 인증이 발생하고 이미지에 표시된 대로 VPN 세션이 설정됩니다.



ASA에서 HostScan 보고서를 수신한다고 보고합니다.

```
%ASA-7-716603:  Received 4 KB Hostscan data from IP <10.61.87.251>
```
그런 다음 사용자 인증을 수행합니다.

```
%ASA-6-113004: AAA user authentication Successful : server =  10.62.145.42 : user = cisco
```
그리고 해당 VPN 세션에 대한 권한 부여를 시작합니다."debug dap trace 255"를 활성화하면 c:\test.txt 파일의 존재와 관련된 정보가 반환됩니다.

```
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"
```
또한 Microsoft Windows 방화벽과 관련된 정보:

```
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"
```
Symantec AntiVirus(앞에서 구성한 HostScan 고급 엔드포인트 평가 규칙에 따라)

따라서 DAP 정책이 일치합니다.

```
DAP_TRACE: Username: cisco, Selected DAPs: ,FileNotExists
```
이 정책은 AnyConnect를 사용해야 하며, 사용자에 대한 제한된 네트워크 액세스를 제공하는 액세스 목록 ACL1도 적용합니다(기업 정책을 준수하지 않음).

```
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
```
로그는 DAP 정책에서 사용할 수 있는 ACIDEX 확장 기능(또는 ISE에 Radius-Requests에서 전달되어 권한 부여 규칙에서 조건으로 사용)도 제공합니다.

```
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";
```
따라서 VPN 세션이 작동하지만 제한된 네트워크 액세스가 있는 경우

```
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 기록은 상태 프로세스에 대한 자세한 단계를 보여줍니다.

```
     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.
```

Posture를 사용하는 AnyConnect VPN 세션 - 규정 준수

c:\test.txt 파일을 만든 후에는 플로우가 유사합니다.새 AnyConnect 세션이 시작되면 로그는 파일이 있음을 나타냅니다.

```
%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"
```

그 결과 또 다른 DAP 정책이 사용됩니다.

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

정책은 네트워크 트래픽에 대한 제한으로서 어떤 ACL도 부과하지 않습니다.

그리고 세션이 ACL 없이 작동(전체 네트워크 액세스):

```
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
```

또한 AnyConnect는 HostScan이 유휴 상태이며 다음 스캔 요청을 기다리고 있음을 보고합니다.

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

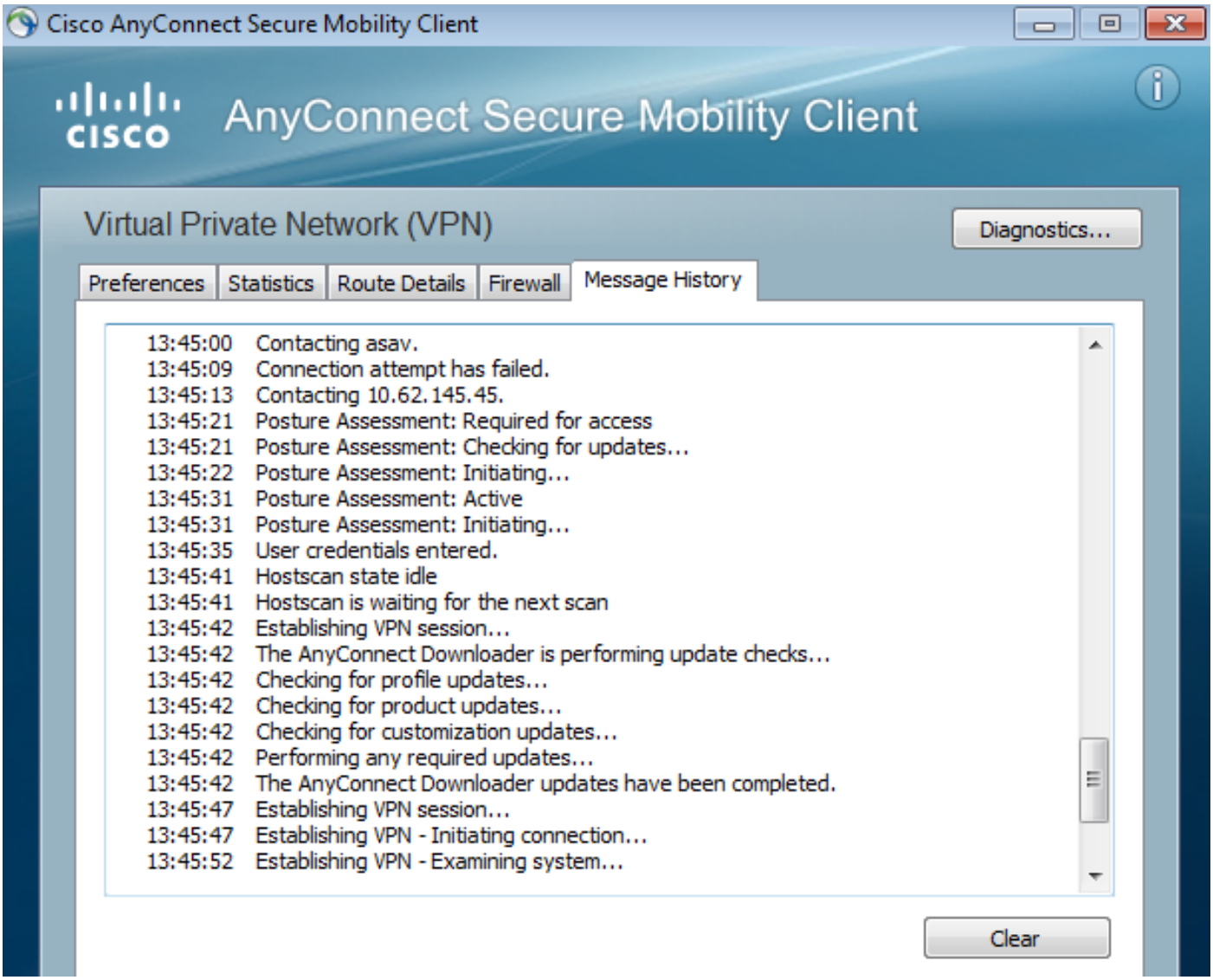
참고:재평가를 위해 ISE와 통합된 상태 모듈을 사용하는 것이 좋습니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

AnyConnect DART

AnyConnect는 이미지에 표시된 대로 진단을 제공합니다.



모든 AnyConnect 로그를 수집하여 데스크톱의 zip 파일에 저장합니다.이 zip 파일에는 Cisco AnyConnect Secure Mobility Client/Anyconnect.txt의 로그가 포함되어 있습니다.

ASA에 대한 정보를 제공하고 HostScan에 데이터 수집을 요청합니다.

```
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.
```

그런 다음 다른 여러 로그를 통해 CSD가 설치되어 있음을 알 수 있습니다.다음은 CSD 프로비저닝 및 포스처와 함께 후속 AnyConnect 연결의 예입니다.

```
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...
```

ASA와 AnyConnect 간의 통신이 최적화되어 특정 확인만 수행하기 위한 ASA 요청 - AnyConnect는 추가 데이터를 다운로드하여 이를 수행할 수 있습니다(예: 특정 안티바이러스 확인).

TAC에서 케이스를 열면 ASA에서 "show tech" 및 "debug dap trace 255"와 함께 Dart 로그를 첨부합니다.

관련 정보

- Host Scan 및 Posture 모듈 구성 - Cisco AnyConnect Secure Mobility Client 관리자 설명서
- Cisco ISE 컨피그레이션 가이드의 포스처 서비스
- Cisco ISE 1.3 관리자 가이드
- 기술 지원 및 문서 – Cisco Systems