使用 CSD、DAP 和 AnyConnect 4.0 配置 ASA VPN 安全评估

目录

简介

本文档介绍如何对自适应安全设备 (ASA) 上终止的远程 VPN 会话执行安全评估。 安全评估由ASA使用带HostScan模块的思科安全桌面(CSD)本地执行。在建立VPN会话后，允许合规站点进行完全网络访问，而不合规站点的网络访问有限。

此外，还显示CSD和AnyConnect 4.0调配流。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco ASA VPN配置
- Cisco AnyConnect 安全移动客户端

使用的组件

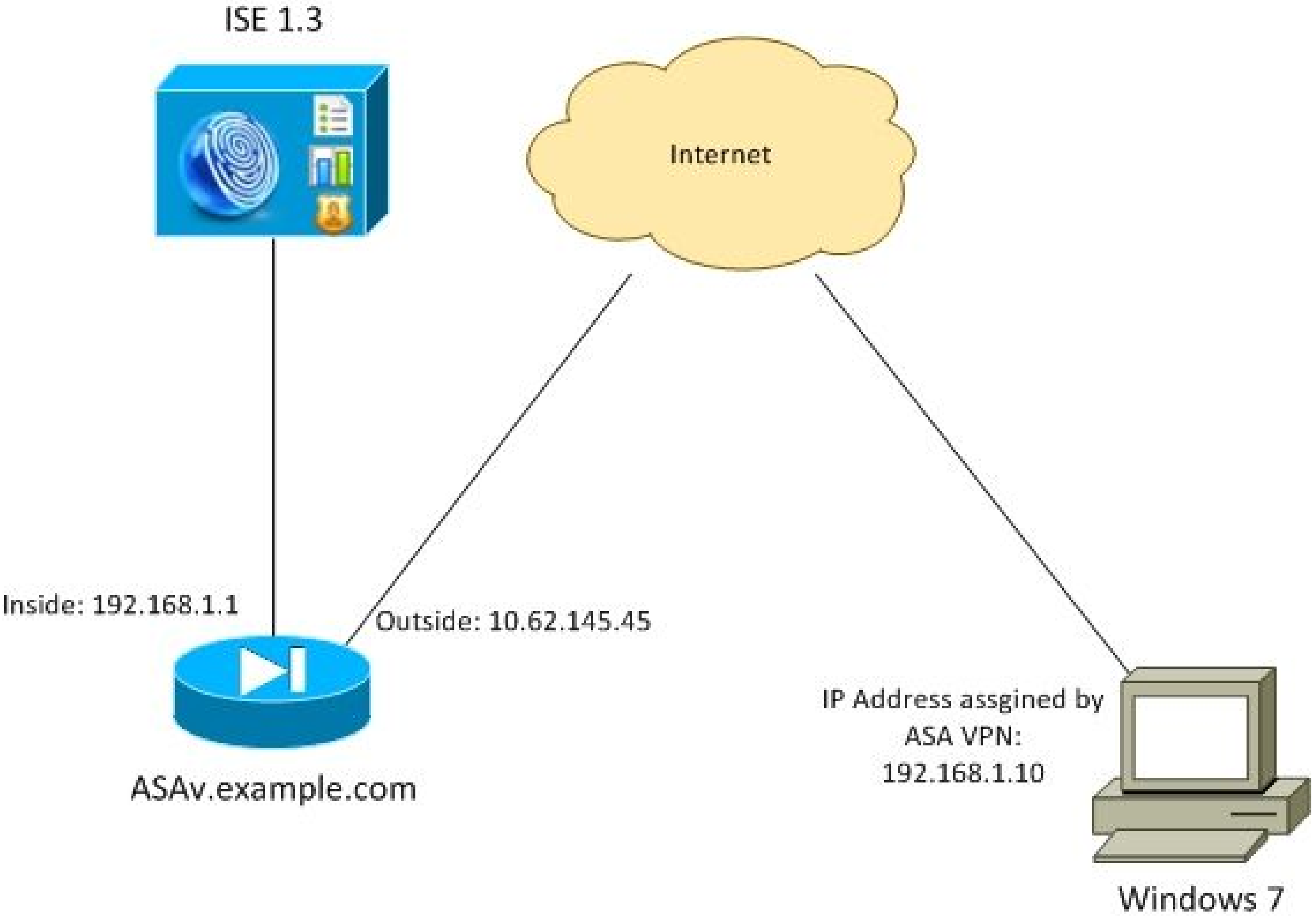
本文档中的信息基于以下软件和硬件版本：

- Microsoft Windows 7
- Cisco ASA 9.3版或更高版本
- 思科身份服务引擎(ISE)软件，版本1.3及更高版本
- Cisco AnyConnect安全移动客户端4.0版及更高版本
- CSD 3.6版或更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图



公司政策如下：

- 具有文件c:\test.txt（兼容）的远程VPN用**户必**须具有对公司内部资源的完全网络访问权限
- 没有文件**c:\test.txt**（不合规）的远程VPN用户必须对公司内部资源进行有限的网络访问：仅提供对补救服务器1.1.1.1的访问。

文件存在是最简单的例子。可以使用任何其他条件（防病毒、反间谍软件、进程、应用、注册表）。

流程如下：

- 远程用户未安装AnyConnect。他们访问CSD和AnyConnect调配的ASA网页（以及VPN配置文件）

- 通过AnyConnect连接后，不合规用户便可进行有限的网络访问。匹配名为FileNotExists的动态访**问策**略(DAP)。
- 用户执行补救(手动安装文**件c:\test.txt**)并再次与AnyConnect连接。此时，提供完全网络访问(匹配名为**FileExists**的**DAP策**略)。

HostScan模块可手动安装在终端上。示例文件(hostscan-win-4.0.00051-pre-deploy-k9.msi)在思科在线连接(CCO)上共享。 但是，它也可能从ASA推送。HostScan是CSD的一部分，可从ASA进行调配。本例中使用第二种方法。

对于AnyConnect（3.1及更低版本）的较旧版本，CCO上有单独的软件包(例如：hostscan_3.1.06073-k9.pkg)，可以单独在ASA上配置和调配(使用**csd hostscan image**命令) — 但该选项对于AnyConnect版本4.0已不存在。

ASA

步骤1.基本SSL VPN配置

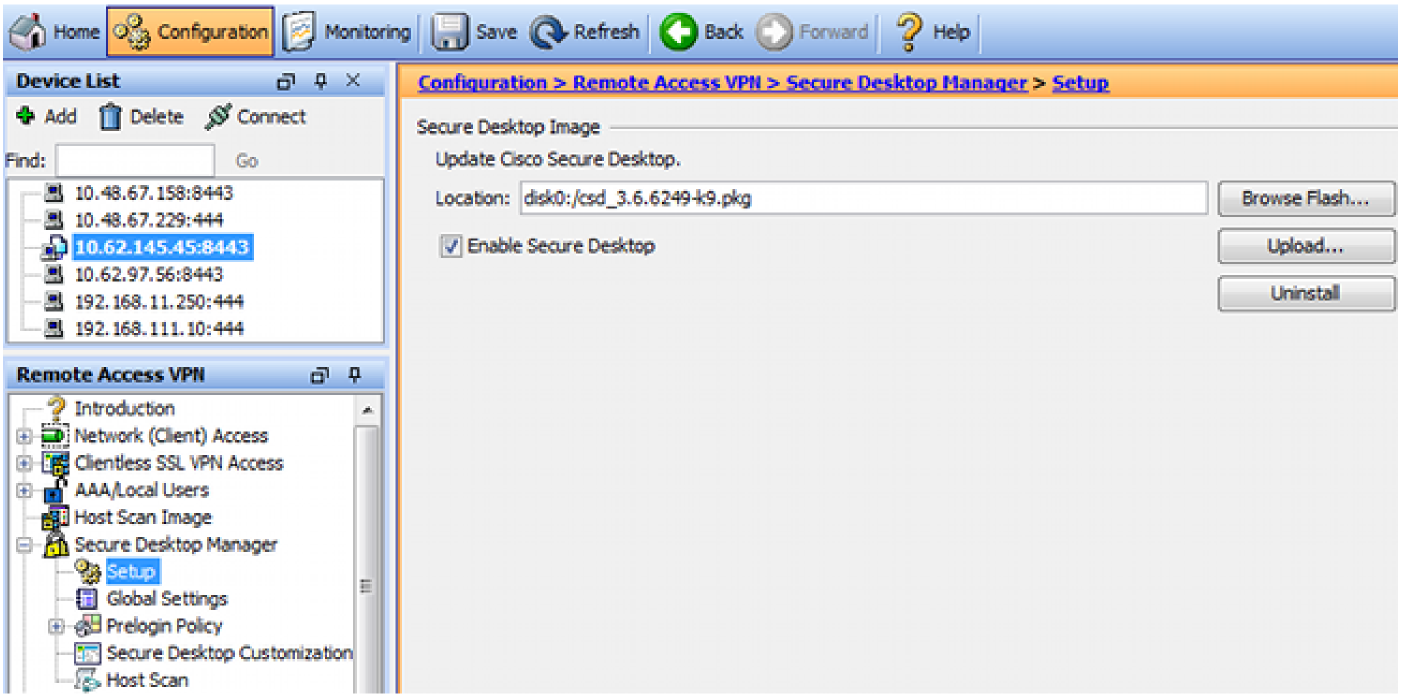
ASA预配置了基本远程VPN访问(安全套接字层(SSL)):

```
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软件包已下载并使用。

步骤2. CSD安装

随后的配置使用自适应安全设备管理器(ASDM)执行。需要下载CSD软件包，以便闪存并从配置中获取参考，如图所示。



Configuration > Remote Access VPN > Secure Desktop Manager > Setup

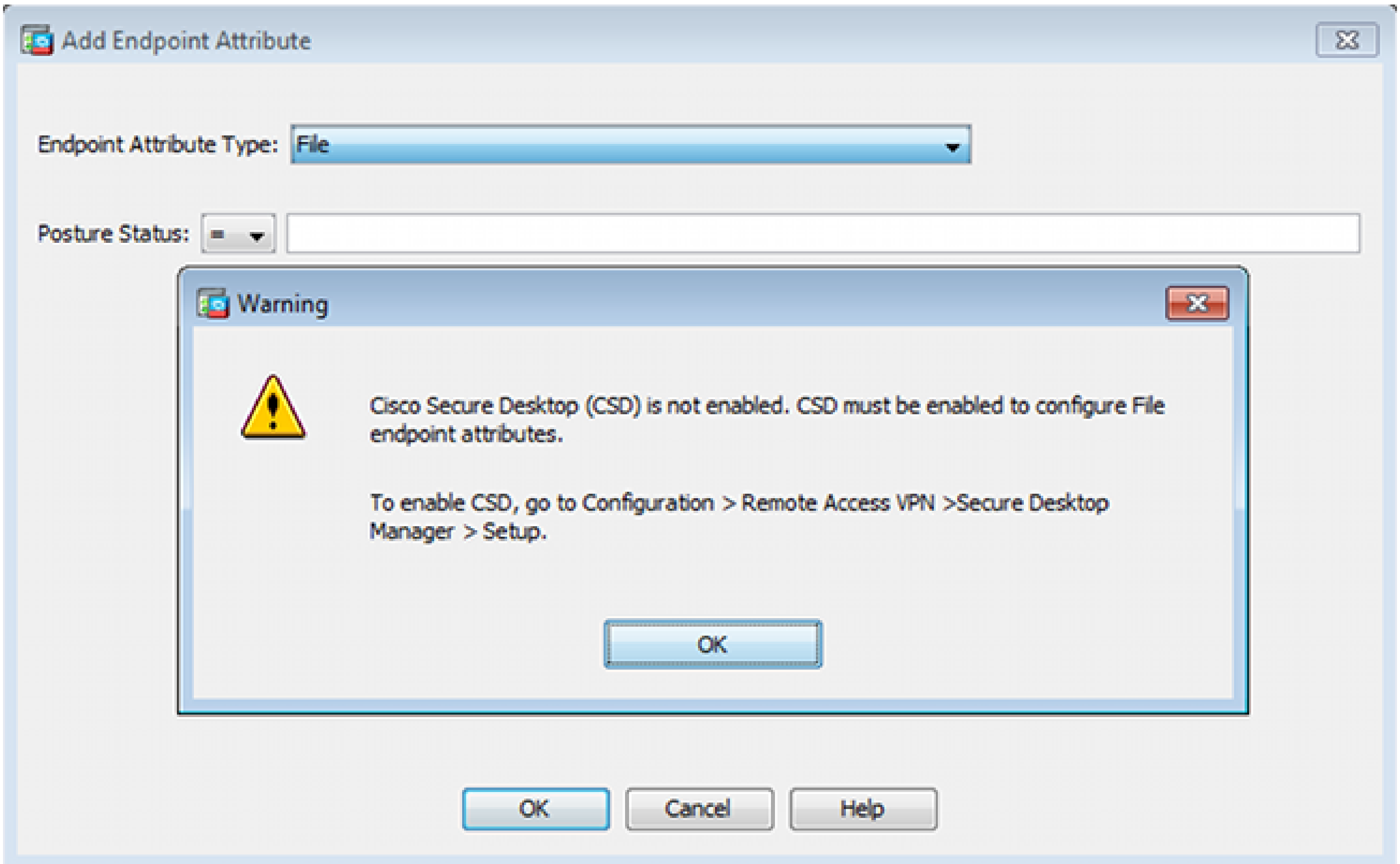
Secure Desktop Image

Update Cisco Secure Desktop.

Location: disk0:/csd_3.6.6249-k9.pkg

☑ Enable Secure Desktop

如图所示，如果不启用Secure Desktop，则无法在DAP策略中使用CSD属性。



Endpoint Attribute Type: File

Posture Status: =

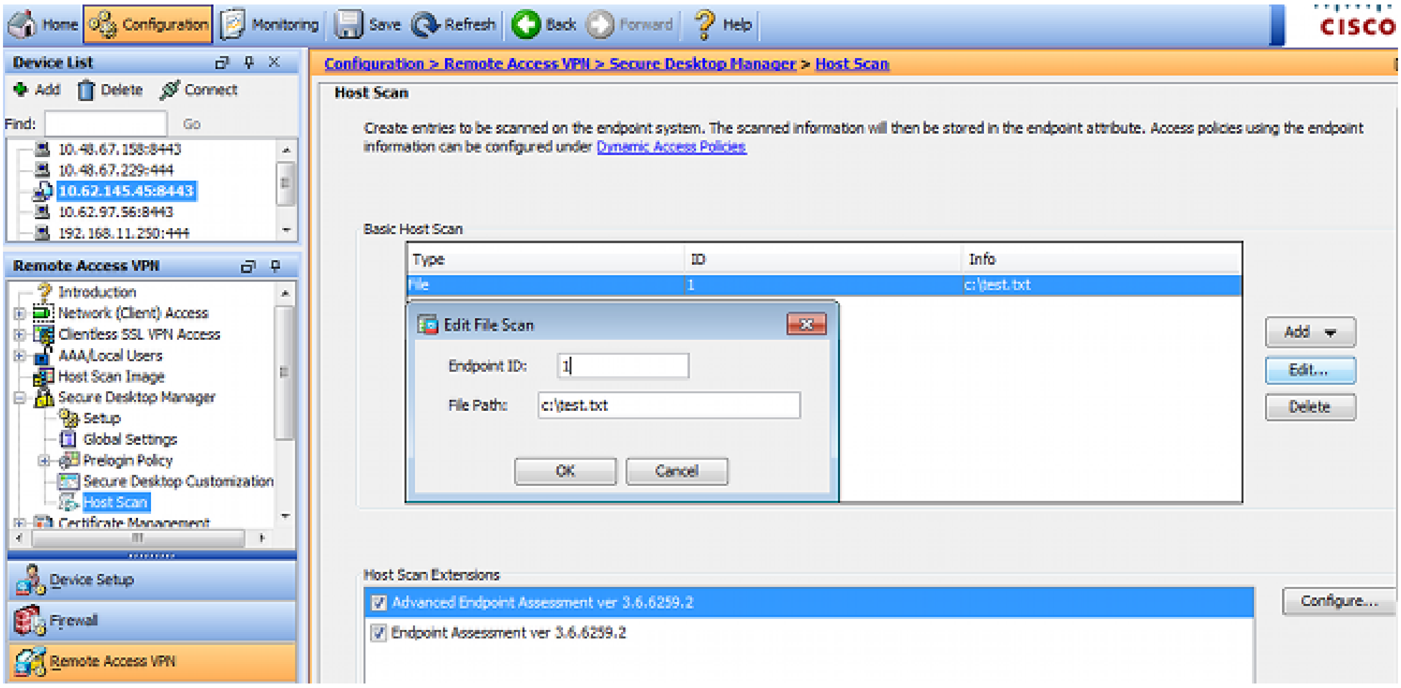
Cisco Secure Desktop (CSD) is not enabled. CSD must be enabled to configure File endpoint attributes.

To enable CSD, go to Configuration > Remote Access VPN >Secure Desktop Manager > Setup.

启用CSD后，Secure Desktop Manager下会显示多个选项。

> **注意：**请注意，其中一些已弃用。有关已弃用功能的详细信息，请参阅：安全桌面(Vault)、缓存清理器、按键记录器检测和主机仿真检测的功能弃用通知

HostScan仍完全受支持，新的基本HostScan规则已添加。如图所示，已验证c:\test.txt的存在。



Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan

Host Scan

Create entries to be scanned on the endpoint system. The scanned information will then be stored in the endpoint attribute. Access policies using the endpoint information can be configured under Dynamic Access Policies

Basic Host Scan

Type	ID	Info
File	1	c:\test.txt

Edit File Scan

Endpoint ID: 1

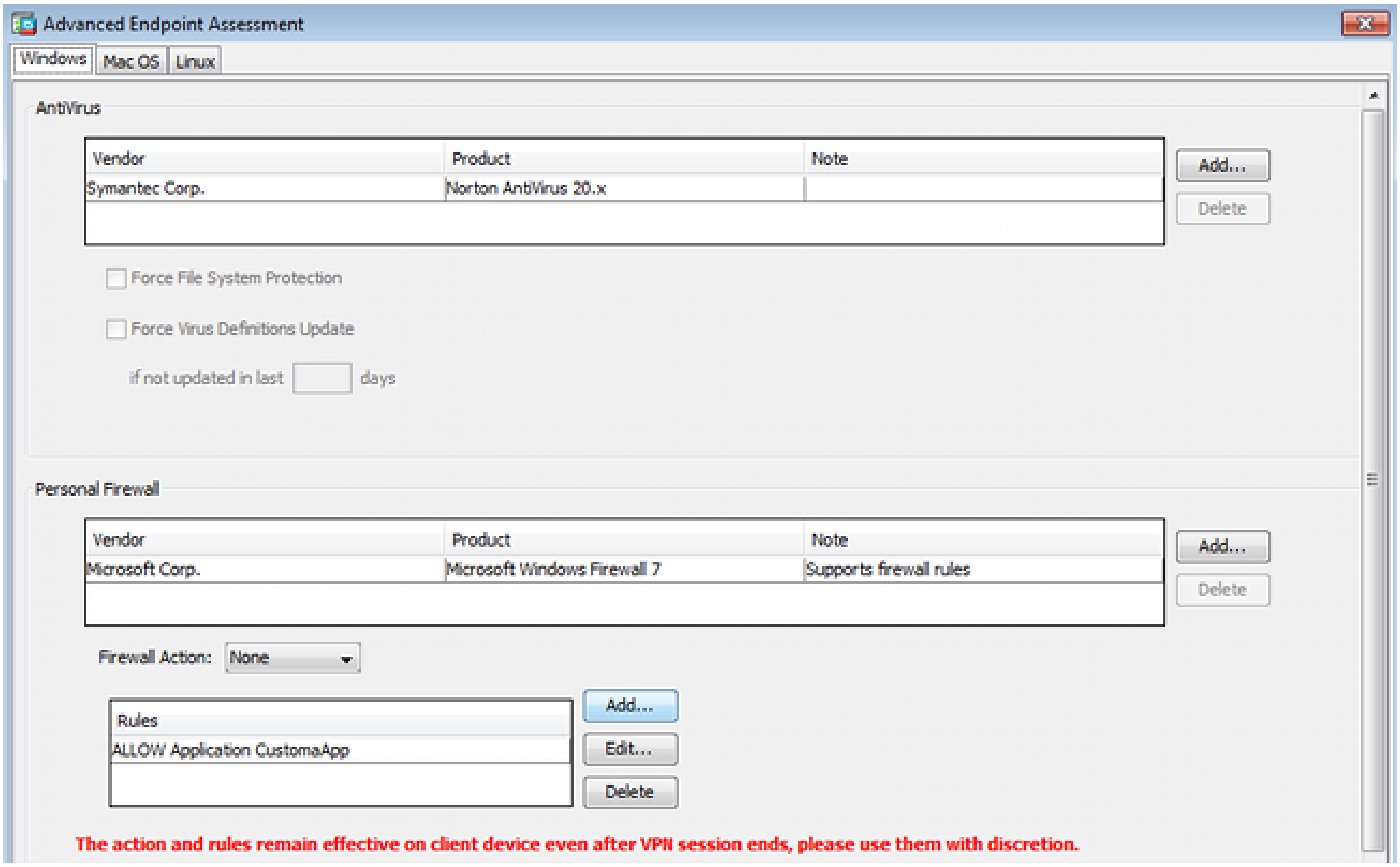
File Path: c:\test.txt

Host Scan Extensions

☑ Advanced Endpoint Assessment ver 3.6.6259.2

☑ Endpoint Assessment ver 3.6.6259.2

此外，还会添加其他高级终端评估规则，如图所示。



Advanced Endpoint Assessment

AntiVirus

Vendor	Product	Note
Symantec Corp.	Norton AntiVirus 20.x	

□ Force File System Protection

□ Force Virus Definitions Update

if not updated in last days

Personal Firewall

Vendor	Product	Note
Microsoft Corp.	Microsoft Windows Firewall 7	Supports firewall rules

Firewall Action: None

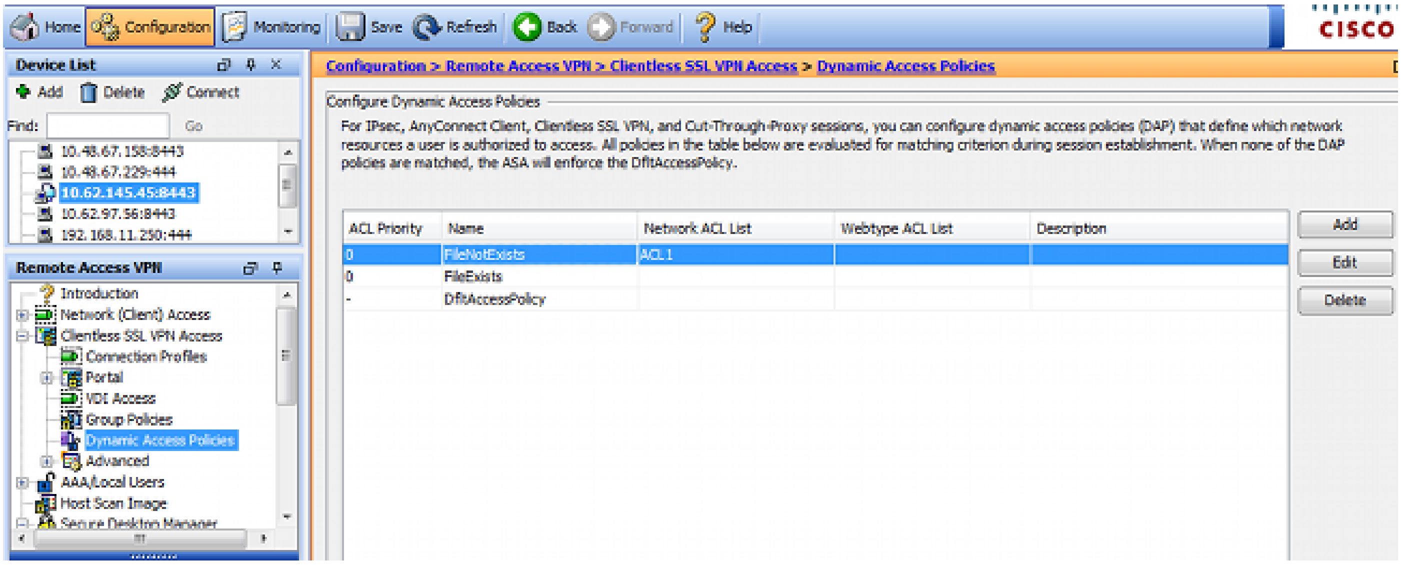
Rules
ALLOW Application CustomaApp

The action and rules remain effective on client device even after VPN session ends, please use them with discretion.

该模块检查是否存在Symantec Norton AntiVirus 20.x和Microsoft Windows Firewall 7。状态模块(HostScan)检查这些值，但不会实施（DAP策略不验证是否）。

步骤3. DAP策略

DAP策略负责将HostScan收集的数据用作条件，并因此将特定属性应用到VPN会话。要从ASDM创建DAP策略，请导航到**Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies**，如图所示。



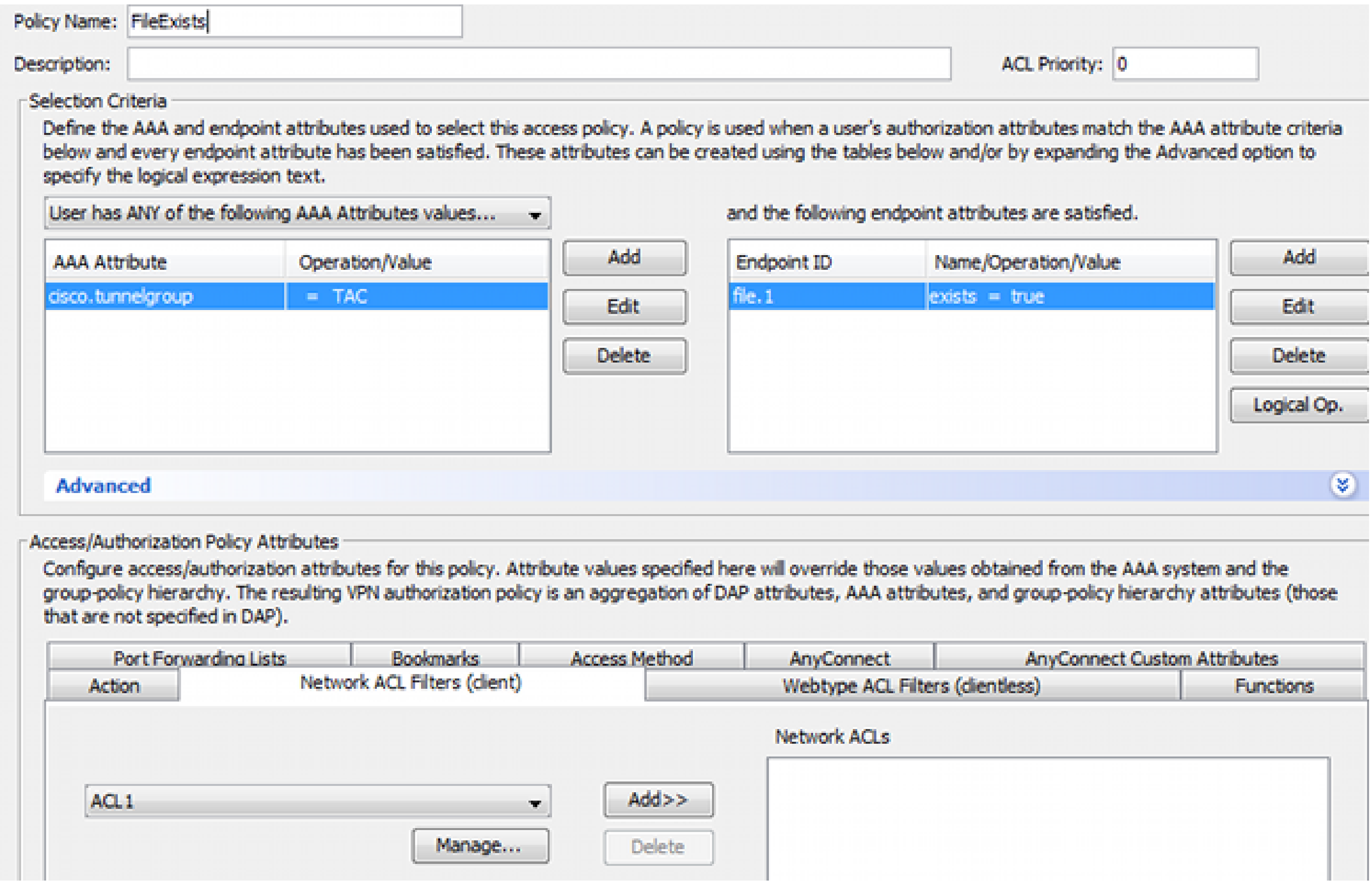
Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies

Configure Dynamic Access Policies

For IPsec, AnyConnect Client, Clientless SSL VPN, and Cut-Through-Proxy sessions, you can configure dynamic access policies (DAP) that define which network resources a user is authorized to access. All policies in the table below are evaluated for matching criterion during session establishment. When none of the DAP policies are matched, the ASA will enforce the DfltAccessPolicy.

ACL Priority	Name	Network ACL List	Webtype ACL List	Description
0	FileNotExists	ACL1		
0	FileExists			
-	DfltAccessPolicy			

第一个策略(FileExists)检查已配置的VPN配置文件使用的隧道组名称（为清楚起见，已省略VPN配置文件配置）。 然后，如图所示，对文**件c:\test.txt**执行其他检查。



Policy Name: FileExists

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

Access/Authorization Policy Attributes

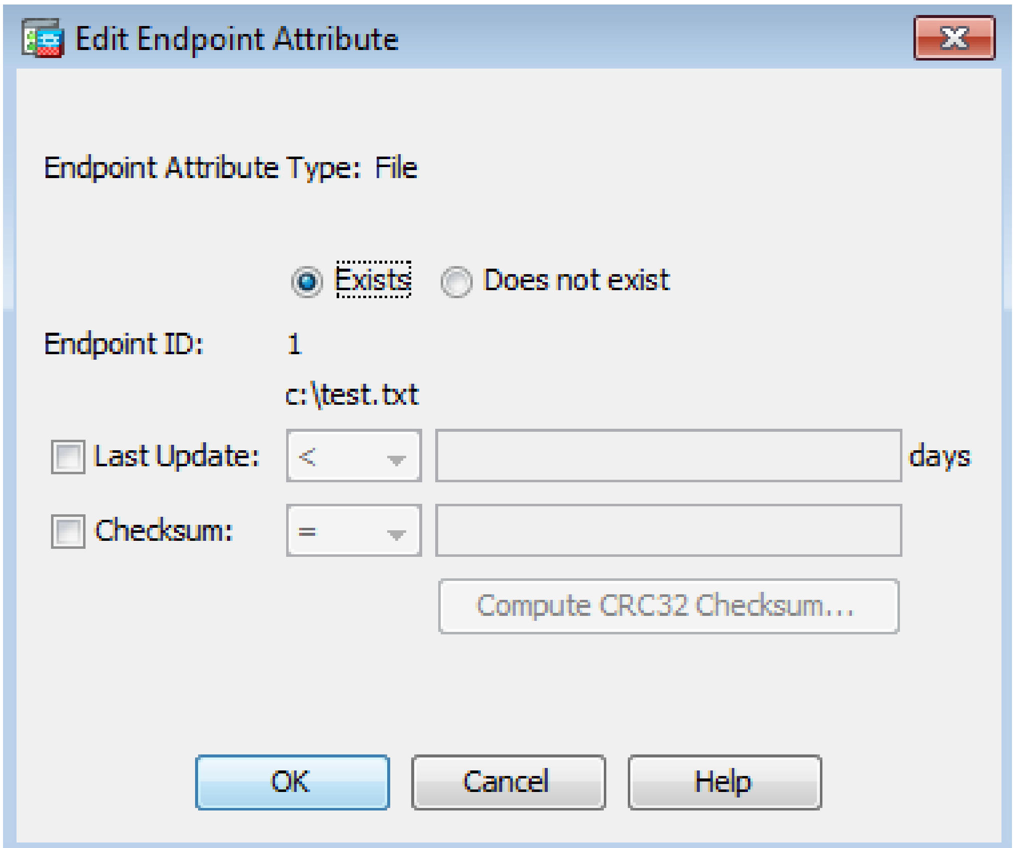
Configure access/authorization attributes for this policy. Attribute values specified here will override those values obtained from the AAA system and the group-policy hierarchy. The resulting VPN authorization policy is an aggregation of DAP attributes, AAA attributes, and group-policy hierarchy attributes (those that are not specified in DAP).

ACL1

Network ACLs

因此，不使用默认设置执行任何操作以允许连接。不使用ACL — 提供完全网络访问。

文件检查的详细信息如图所示。



Edit Endpoint Attribute

Endpoint Attribute Type: File

● Exists ○ Does not exist

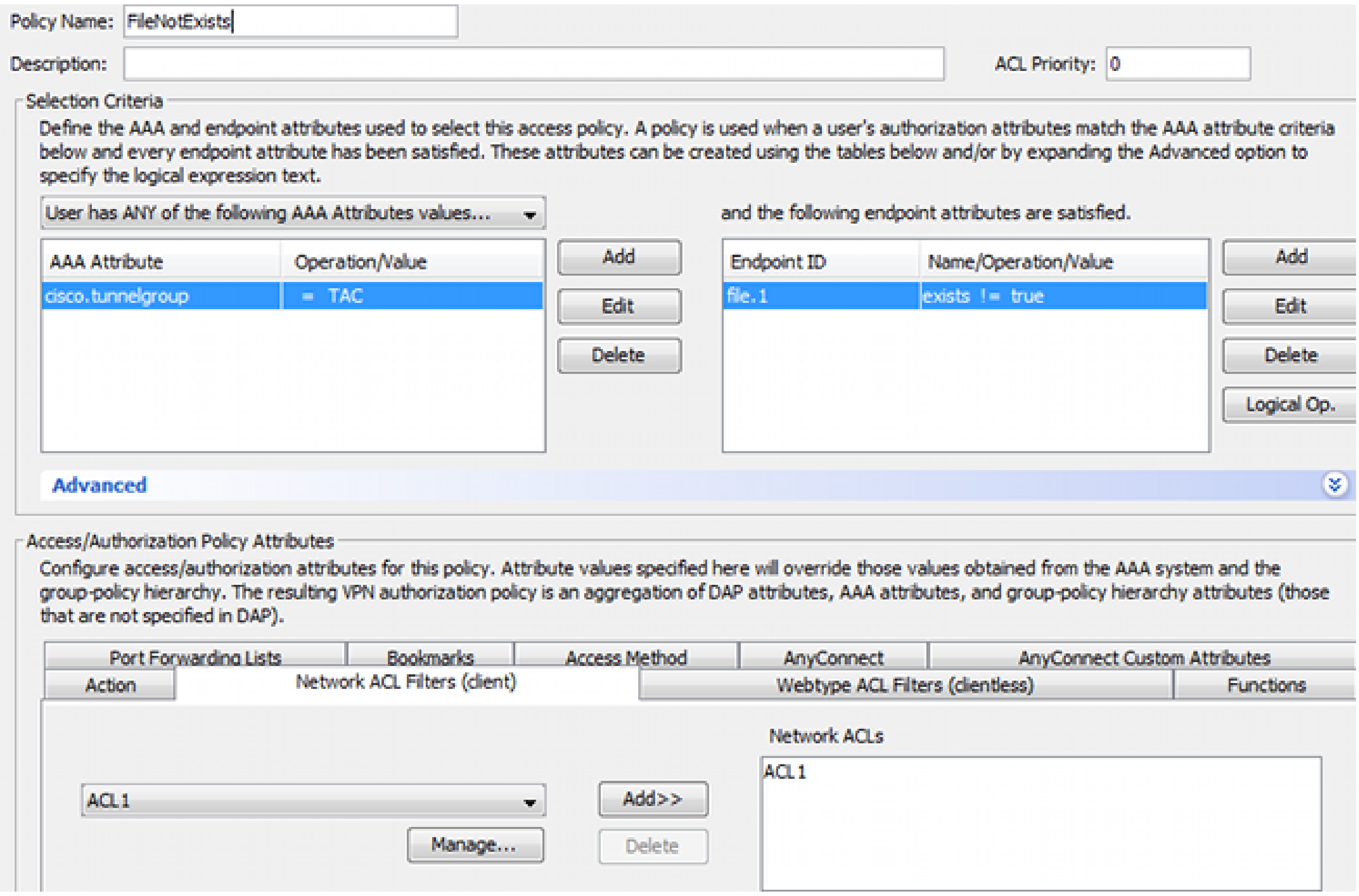
Endpoint ID: 1

c:\test.txt

□ Last Update: < days

□ Checksum: =

第二个策略(FileNotExists)类似 — 但此时间条件是**如果文件不存在**，如图所示。



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

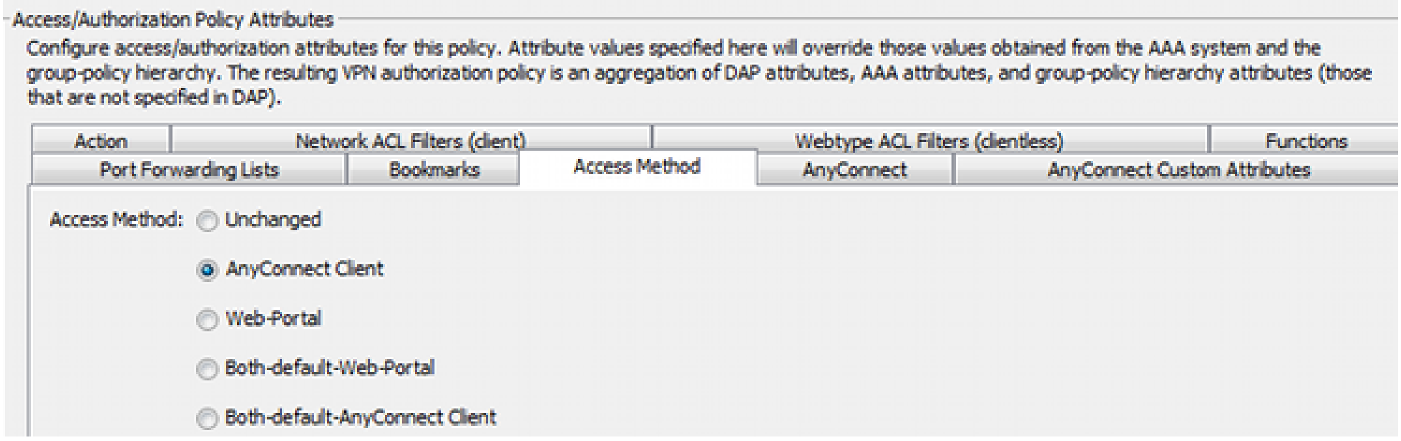
Access/Authorization Policy Attributes

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).

Network ACLs: ACL1

结果配置了访问列表ACL1。这适用于不合规的VPN用户，并提供有限的网络访问。

两个DAP策略都推送**AnyConnect**客户端访问，如图所示。



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

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).

Access Method:
○ Unchanged
● AnyConnect Client
○ Web-Portal
○ Both-default-Web-Portal
○ Both-default-AnyConnect Client

ISE

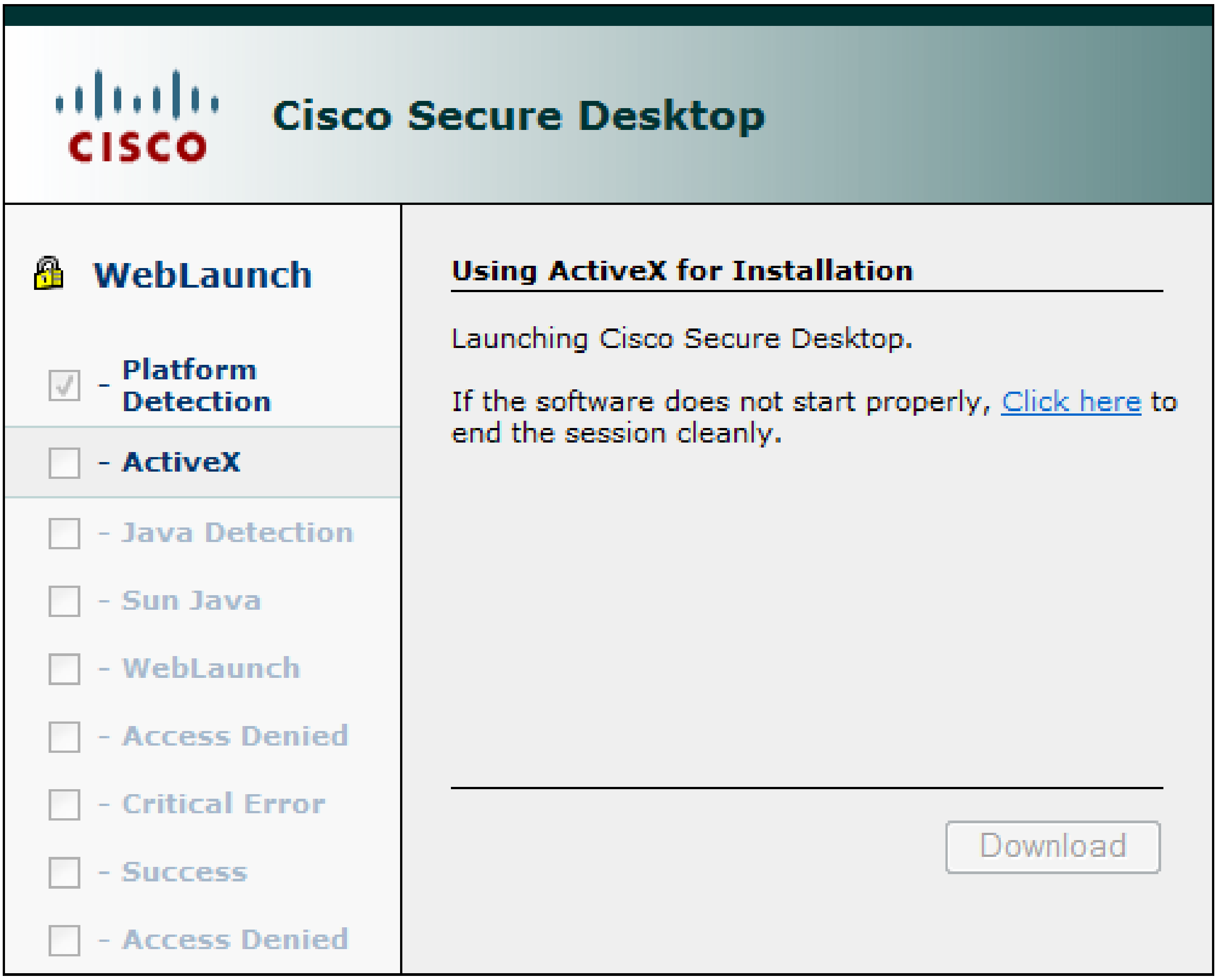
ISE用于用户身份验证。只能配置网络设备(ASA)和正确的用户名(cisco)。本文未涵盖该部分。

验证

使用本部分可确认配置能否正常运行。

CSD和AnyConnect调配

最初，用户未调配AnyConnect客户端。用户也不符合策略(文**件c:\test.txt**不存在)。 输入 https://10.62.145.45，然后立即重定向用户进行CSD安装，如图所示。



Cisco Secure Desktop

WebLaunch

☑ - Platform Detection

□ - ActiveX

□ - Java Detection

□ - Sun Java

□ - WebLaunch

□ - Access Denied

□ - Critical Error

□ - Success

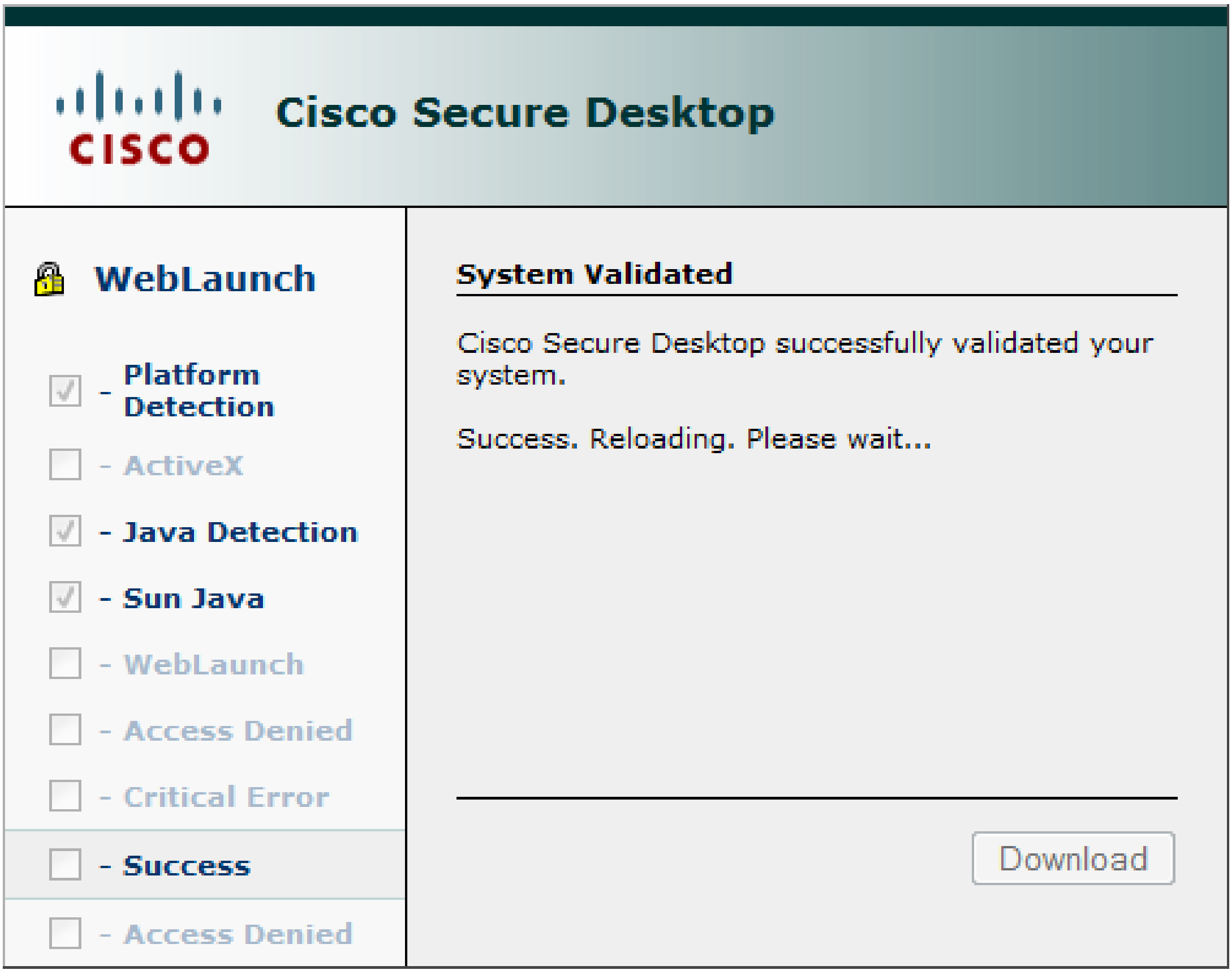
□ - Access Denied

Using ActiveX for Installation

Launching Cisco Secure Desktop.

If the software does not start properly, Click here to end the session cleanly.

这可以通过Java或ActiveX实现。安装CSD后，将报告如图所示。



Cisco Secure Desktop

WebLaunch

☑ - Platform Detection

□ - ActiveX

☑ - Java Detection

☑ - Sun Java

□ - WebLaunch

□ - Access Denied

□ - Critical Error

□ - Success

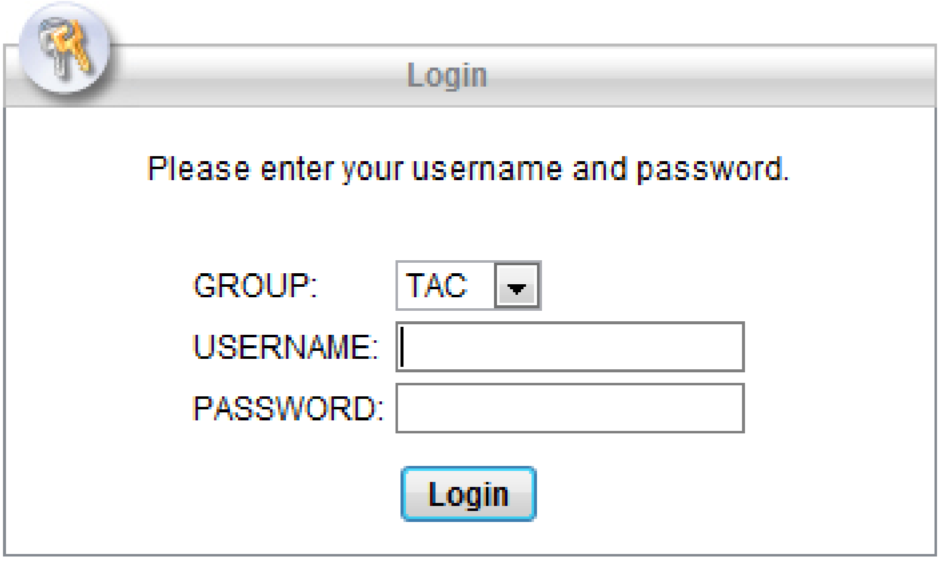
□ - Access Denied

System Validated

Cisco Secure Desktop successfully validated your system.

Success. Reloading. Please wait...

然后，如图所示，用户被重定向以进行身份验证。



Login

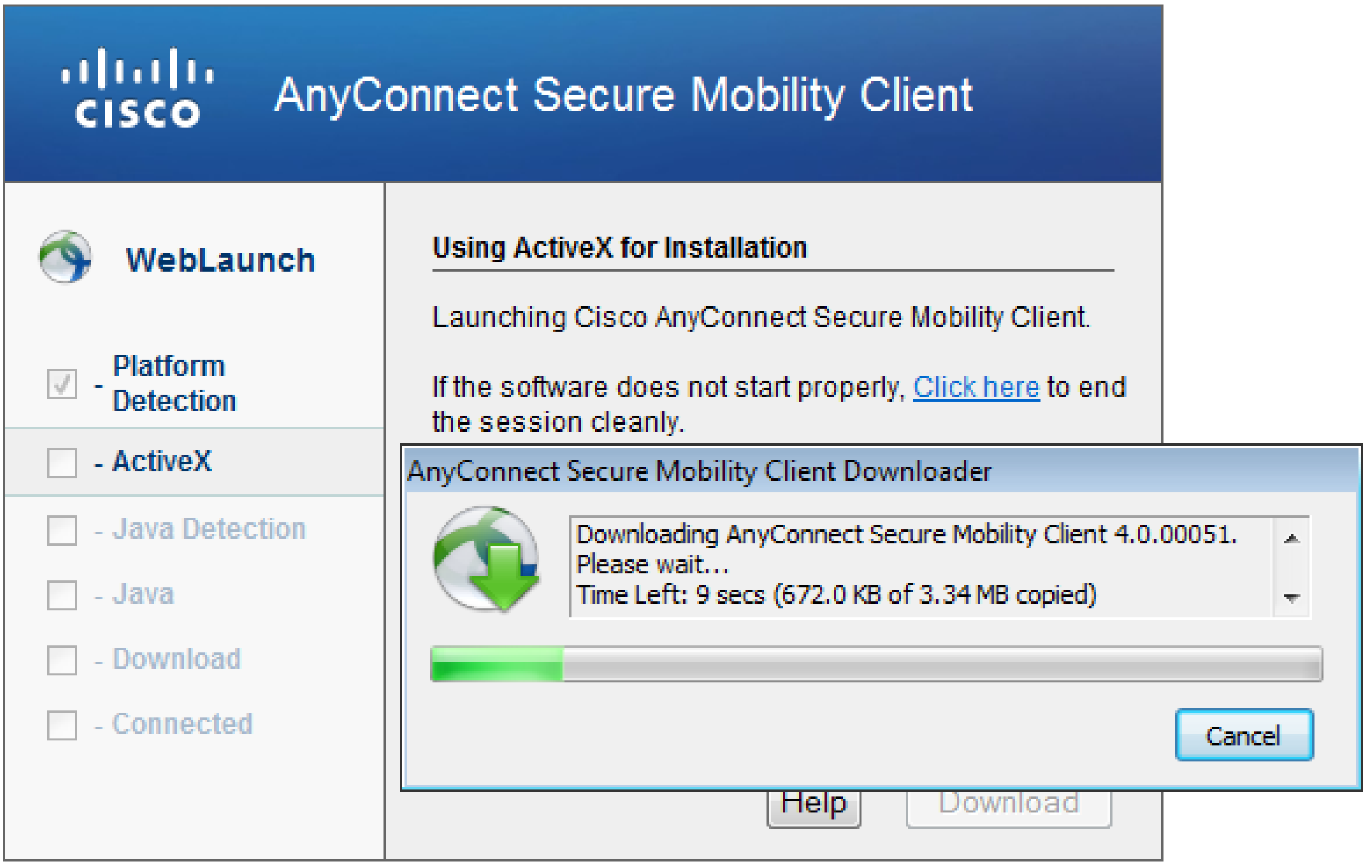
Please enter your username and password.

GROUP: TAC

USERNAME:

PASSWORD:

如果成功，则部署AnyConnect和已配置的配置文件 — 同样，也可使用ActiveX或Java，如图所示。



Using ActiveX for Installation

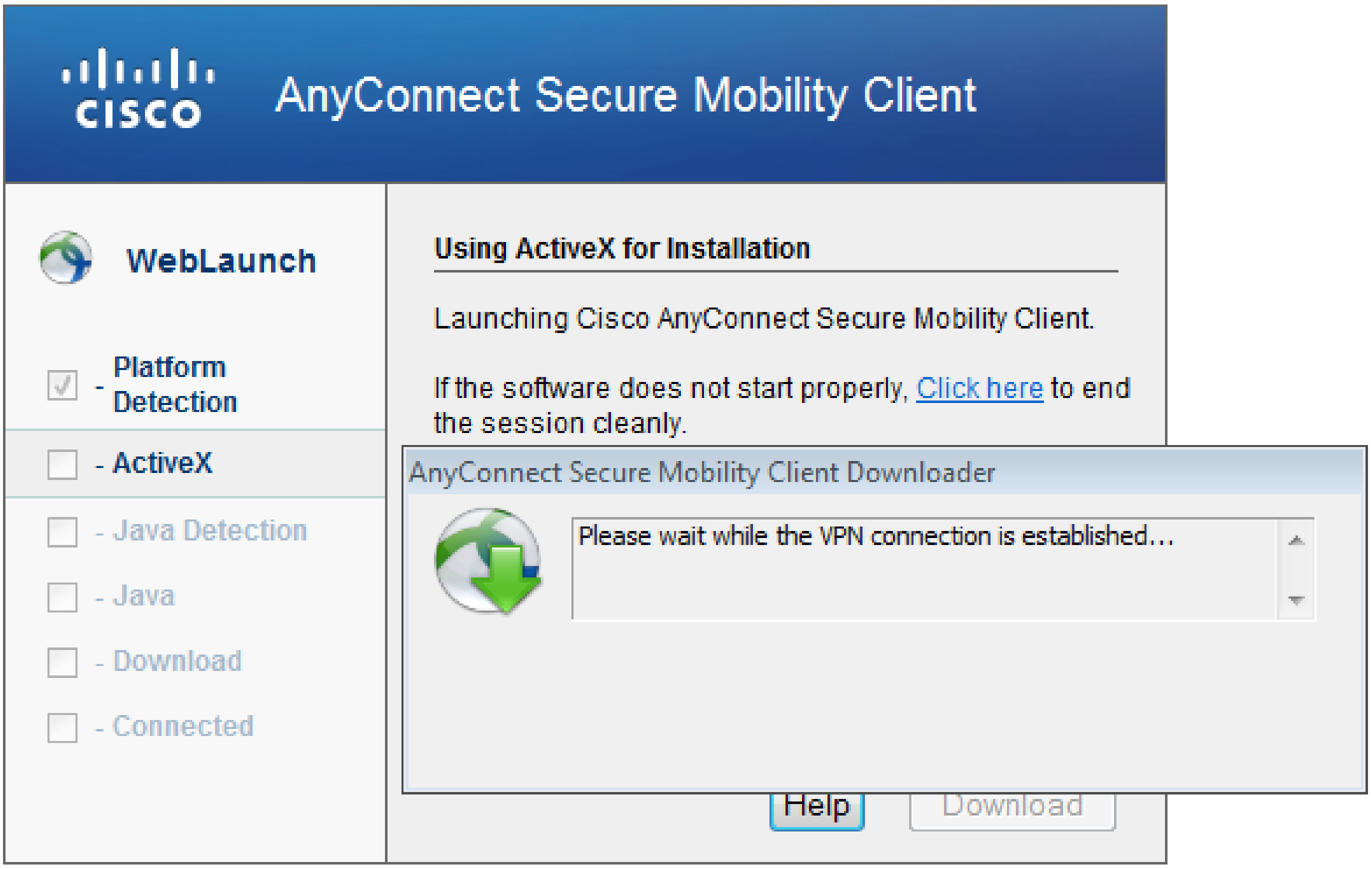
Launching Cisco AnyConnect Secure Mobility Client.

If the software does not start properly, Click here to end the session cleanly.

AnyConnect Secure Mobility Client Downloader

Downloading AnyConnect Secure Mobility Client 4.0.00051.
Please wait...
Time Left: 9 secs (672.0 KB of 3.34 MB copied)

而且，VPN连接已建立，如图所示。



Using ActiveX for Installation

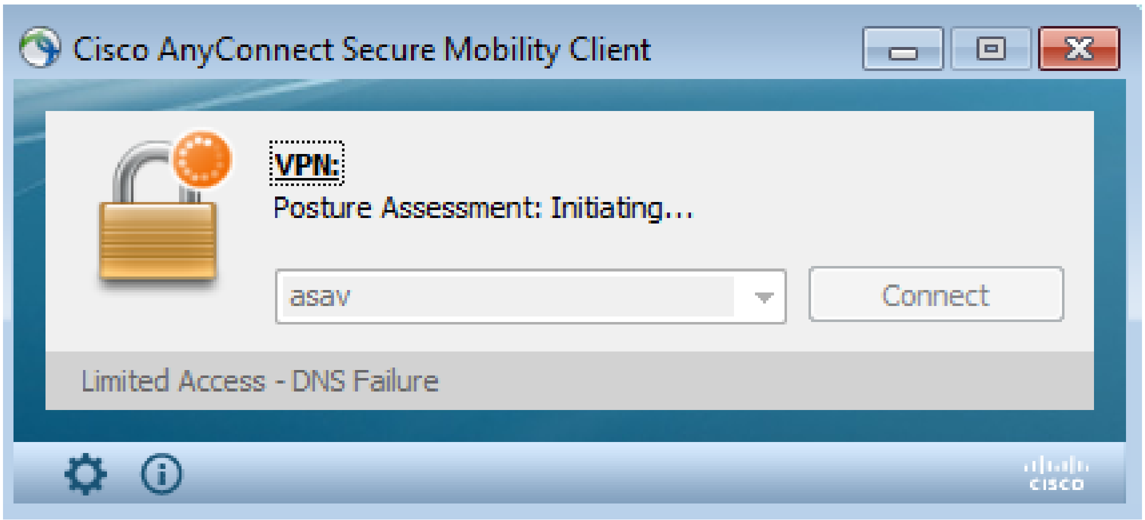
Launching Cisco AnyConnect Secure Mobility Client.

If the software does not start properly, Click here to end the session cleanly.

AnyConnect Secure Mobility Client Downloader

Please wait while the VPN connection is established...

AnyConnect的第一步是执行状态检查(HostScan)并将报告发送到ASA，如图所示。



Cisco AnyConnect Secure Mobility Client

VPN:
Posture Assessment: Initiating...

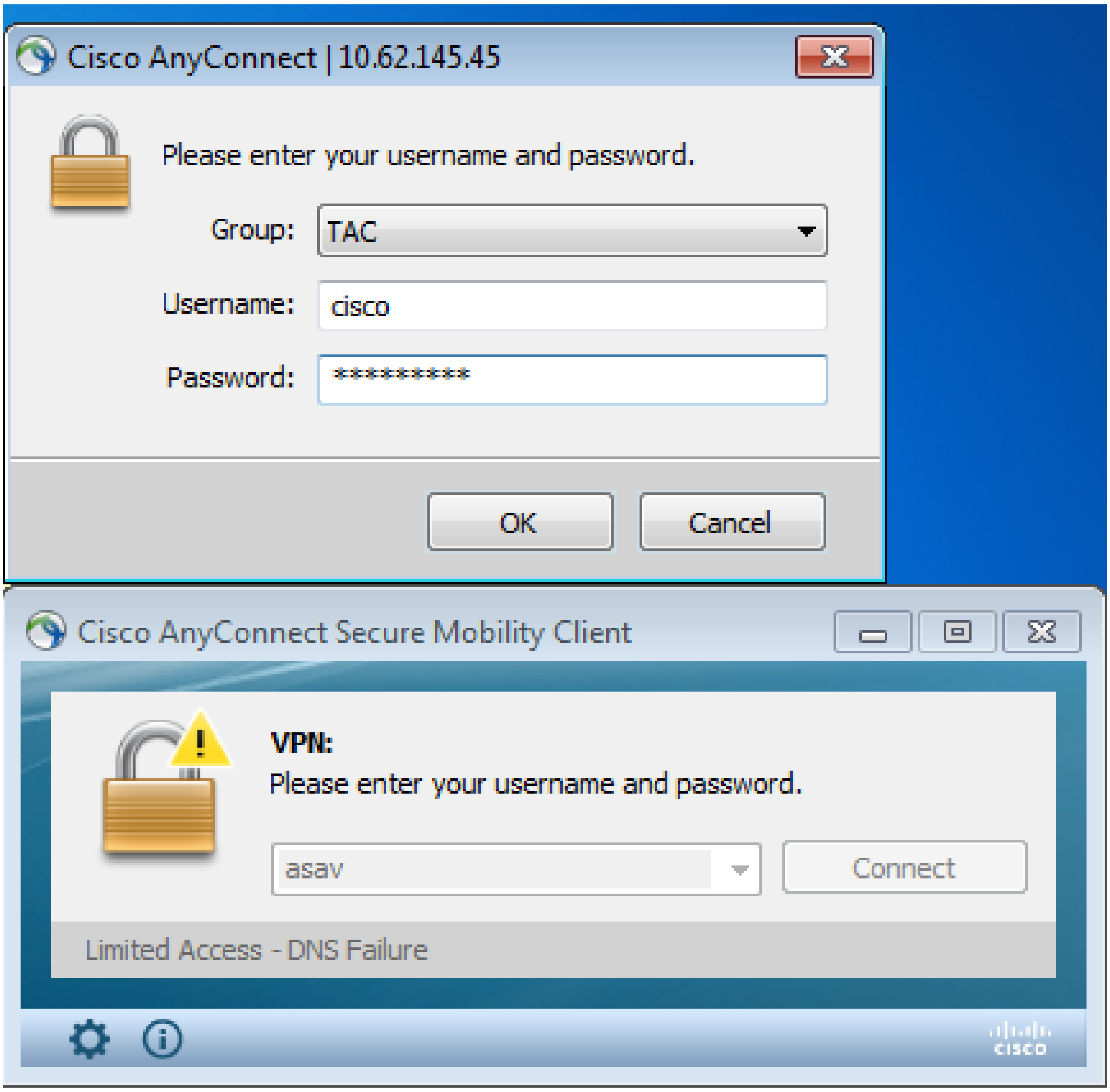
asav

Limited Access - DNS Failure

然后，AnyConnect对VPN会话进行身份验证并完成。

AnyConnect VPN会话与状态 — 不合规

当您与AnyConnect建立新的VPN会话时，第一步是如前面屏幕截图所示的状态(HostScan)。然后，进行身份验证并建立VPN会话，如图所示。



Cisco AnyConnect | 10.62.145.45

Please enter your username and password.

Group: TAC

Username: cisco

Password: **********

Cisco AnyConnect Secure Mobility Client

VPN:
Please enter your username and password.

asav

Limited Access - DNS Failure

ASA报告HostScan报告已收到：

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

然后执行用户身份验证：

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

并启动该VPN会话的授权。启用“debug dap trace 255”后，将返回有关c:\test.txt文件存**在的**信息：

```
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，有关Microsoft Windows防火墙的信息：

```
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（根据之前配置的HostScan高级终端评估规则）。

因此，DAP策略匹配：

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

该策略强制使用AnyConnect，并应用访问列表ACL1，该ACL1为用户提供受限的网络访问（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
```

日志还显示ACIDEX扩展，DAP策略可使用（甚至在Radius-Requests中传递到ISE，在授权规则中作为条件使用）：

```
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会话处于启用状态，但网络访问受限：

```
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历史记录显示安全评估流程的详细步骤：

```
     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会话与状态 — 兼容

创建c:\test.txt文件后，流程类似。启动新的AnyConnect会话后，日志将指示文件是否存在：

```
%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，使用了另一个DAP策略：

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

策略不强制任何ACL作为网络流量的限制。

会话处于Up状态，没有任何ACL（完全网络访问）：

```
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报告HostScan空闲并等待下一个扫描请求：

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

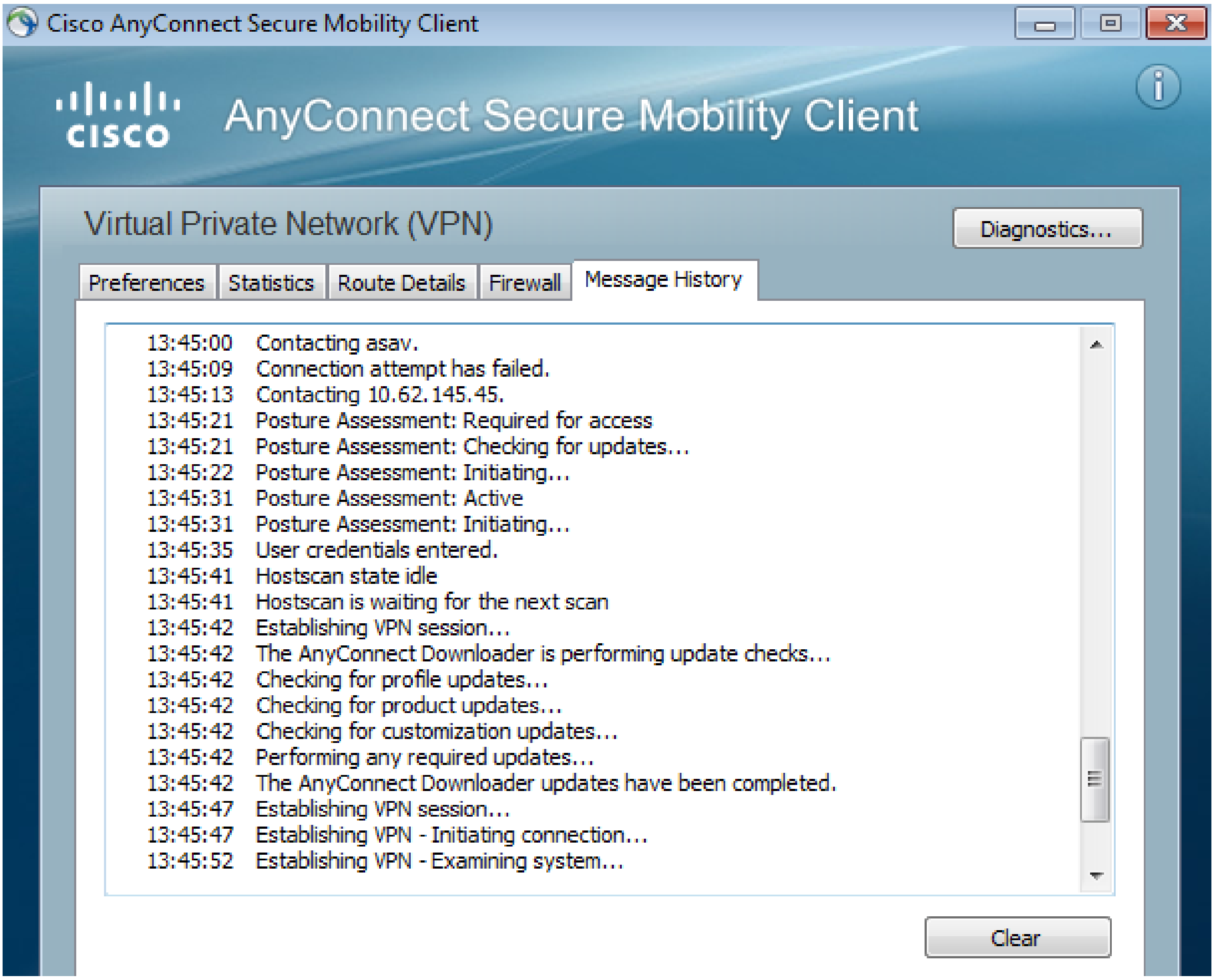
注意：要进行重新评估，建议使用与ISE集成的状态模块。

故障排除

本部分提供了可用于对配置进行故障排除的信息。

AnyConnect DART

AnyConnect提供诊断，如图所示。


Cisco AnyConnect Secure Mobility Client
AnyConnect Secure Mobility Client
Virtual Private Network (VPN)
Diagnostics...
Preferences
Statistics
Route Details
Firewall
Message History
Clear

```
13:45:00   Contacting asav.
13:45:09   Connection attempt has failed.
13:45:13   Contacting 10.62.145.45.
13:45:21   Posture Assessment: Required for access
13:45:21   Posture Assessment: Checking for updates...
13:45:22   Posture Assessment: Initiating...
13:45:31   Posture Assessment: Active
13:45:31   Posture Assessment: Initiating...
13:45:35   User credentials entered.
13:45:41   Hostscan state idle
13:45:41   Hostscan is waiting for the next scan
13:45:42   Establishing VPN session...
13:45:42   The AnyConnect Downloader is performing update checks...
13:45:42   Checking for profile updates...
13:45:42   Checking for product updates...
13:45:42   Checking for customization updates...
13:45:42   Performing any required updates...
13:45:42   The AnyConnect Downloader updates have been completed.
13:45:47   Establishing VPN session...
13:45:47   Establishing VPN - Initiating connection...
13:45:52   Establishing VPN - Examining system...
```

收集所有AnyConnect日志并将其保存到桌面上的压缩文件。该zip文件包含Cisco AnyConnect安全移动Client/Anyconnect.txt中的日志。

这提供了有关ASA的信息，并请求HostScan收集数据：

```
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.
```

然后，多个其他日志显示CSD已安装。以下是CSD调配和后续AnyConnect连接以及状态的示例：

```
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之间的通信已优化，ASA请求仅执行特定检查 — AnyConnect下载其他数据以便能够执行此操作（例如特定防病毒验证）。

当您使用TAC打开案例时，请附加Dart日志，以及来自ASA的“show tech”和“debug dap trace 255”。

相关信息

- 配置主机扫描和状态模块 — Cisco AnyConnect安全移动客户端管理员指南
- 思科ISE配置指南上的状态服务
- 思科ISE 1.3管理员指南
- 技术支持和文档 - Cisco Systems