

Configurazione della postura della VPN ASA con CSD, DAP e AnyConnect 4.0

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[ASA](#)

[Passaggio 1. Configurazione VPN SSL di base](#)

[Passaggio 2. Installazione CSD](#)

[Passaggio 3. Criteri DAP](#)

[ISE](#)

[Verifica](#)

[CSD e provisioning di AnyConnect](#)

[Sessione VPN AnyConnect con postura - Non conforme](#)

[Sessione VPN con postura di AnyConnect - Conforme](#)

[Risoluzione dei problemi](#)

[AnyConnect DART](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come eseguire la postura per le sessioni VPN remote terminate su ASA (Adaptive Security Appliance). La postura viene eseguita localmente dall'ASA con l'uso di Cisco Secure Desktop (CSD) con il modulo HostScan. Una volta stabilita la sessione VPN, alle stazioni conformi è consentito l'accesso completo alla rete, mentre alle stazioni non conformi è consentito un accesso limitato alla rete.

Inoltre, vengono presentati i flussi di provisioning di CSD e AnyConnect 4.0.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione VPN Cisco ASA
- Cisco AnyConnect Secure Mobility Client

Componenti usati

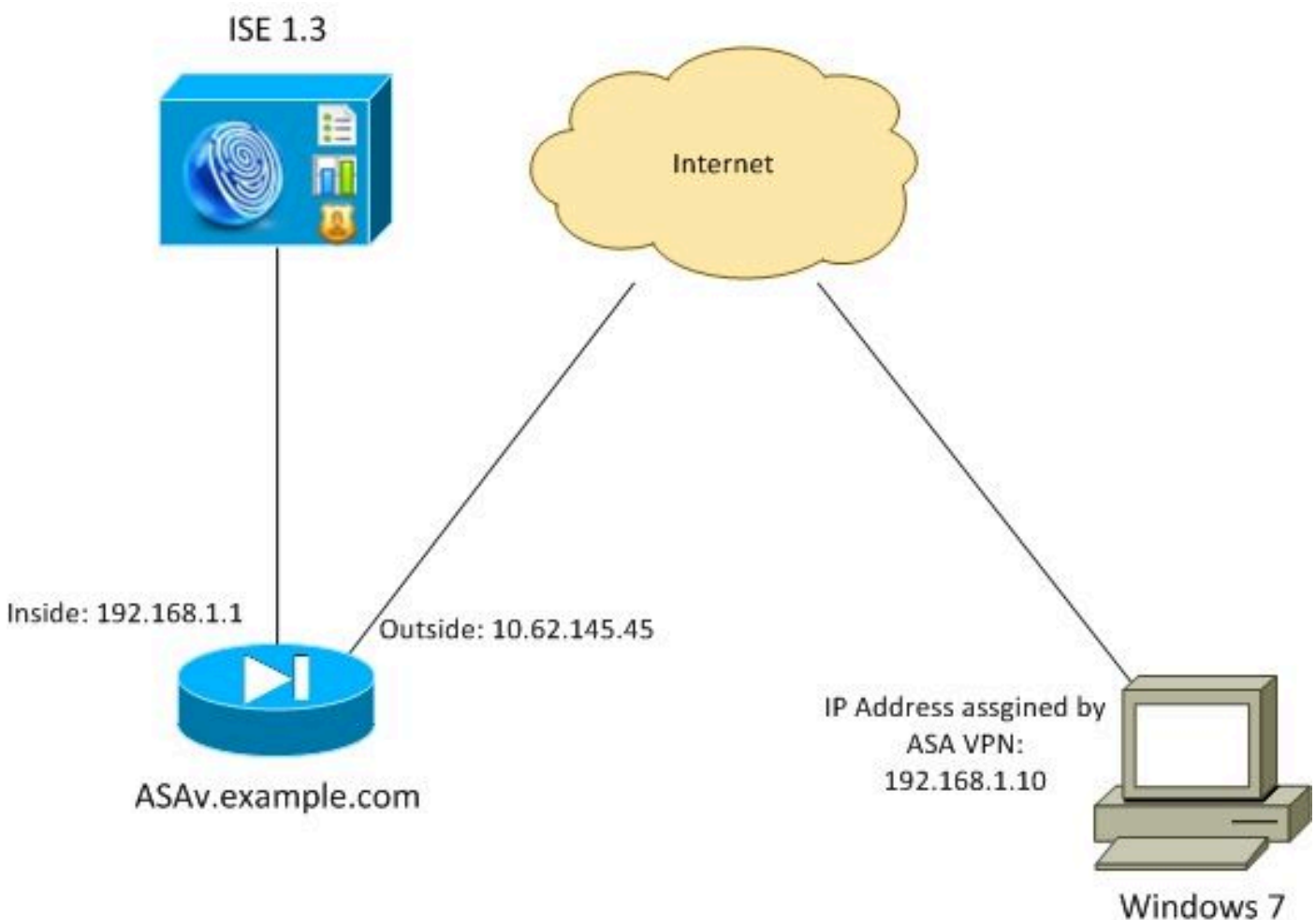
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Microsoft Windows 7
- Cisco ASA versione 9.3 o successive
- Software Cisco Identity Services Engine (ISE), versione 1.3 e successive
- Cisco AnyConnect Secure Mobility Client, versione 4.0 e successive
- CSD, versione 3.6 o successiva

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete



La politica aziendale è la seguente:

- Gli utenti VPN remoti che dispongono del file c:\test.txt (conforme) devono disporre dell'accesso completo alla rete per le risorse interne della società
- Gli utenti VPN remoti che non dispongono del file c:\test.txt (non conforme) devono disporre di accesso limitato alla rete per le risorse interne della società. È fornito solo l'accesso a Remediation Server 1.1.1.1.

L'esempio più semplice è l'esistenza dei file. È possibile utilizzare qualsiasi altra condizione (antivirus, antispyware, processo, applicazione, registro).

Il flusso è il seguente:

- AnyConnect non è installato sugli utenti remoti. Accedono alla pagina Web ASA per il provisioning di CSD e AnyConnect (insieme al profilo VPN)
- Dopo la connessione tramite AnyConnect, gli utenti non conformi possono accedere alla rete con accesso limitato. I criteri di accesso dinamico (DAP) denominati FileNotExists vengono associati.
- L'utente esegue il monitoraggio e l'aggiornamento (installa manualmente il file c:\test.txt) e si connette di nuovo con AnyConnect. Questa volta viene fornito l'accesso completo alla rete (il criterio DAP denominato FileExists corrisponde).

Il modulo HostScan può essere installato manualmente sull'endpoint. I file di esempio (hostscan-win-4.0.00051-pre-deploy-k9.msi) sono condivisi su Cisco Connection Online (CCO). Ma potrebbe anche essere spinto dall'ASA. HostScan fa parte di un CSD a cui è possibile eseguire il provisioning dall'ASA. In questo esempio viene utilizzato il secondo approccio.

Nelle versioni precedenti di AnyConnect (3.1 e precedenti), era disponibile un pacchetto separato su CCO (ad esempio: hostscan_3.1.06073-k9.pkg) che avrebbe potuto essere configurato e configurato sull'appliance ASA separatamente (con il comando `csd hostscan image`). Tuttavia, questa opzione non è più disponibile per AnyConnect versione 4.0.

ASA

Passaggio 1. Configurazione VPN SSL di base

L'ASA è preconfigurata con l'accesso VPN remoto di base (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

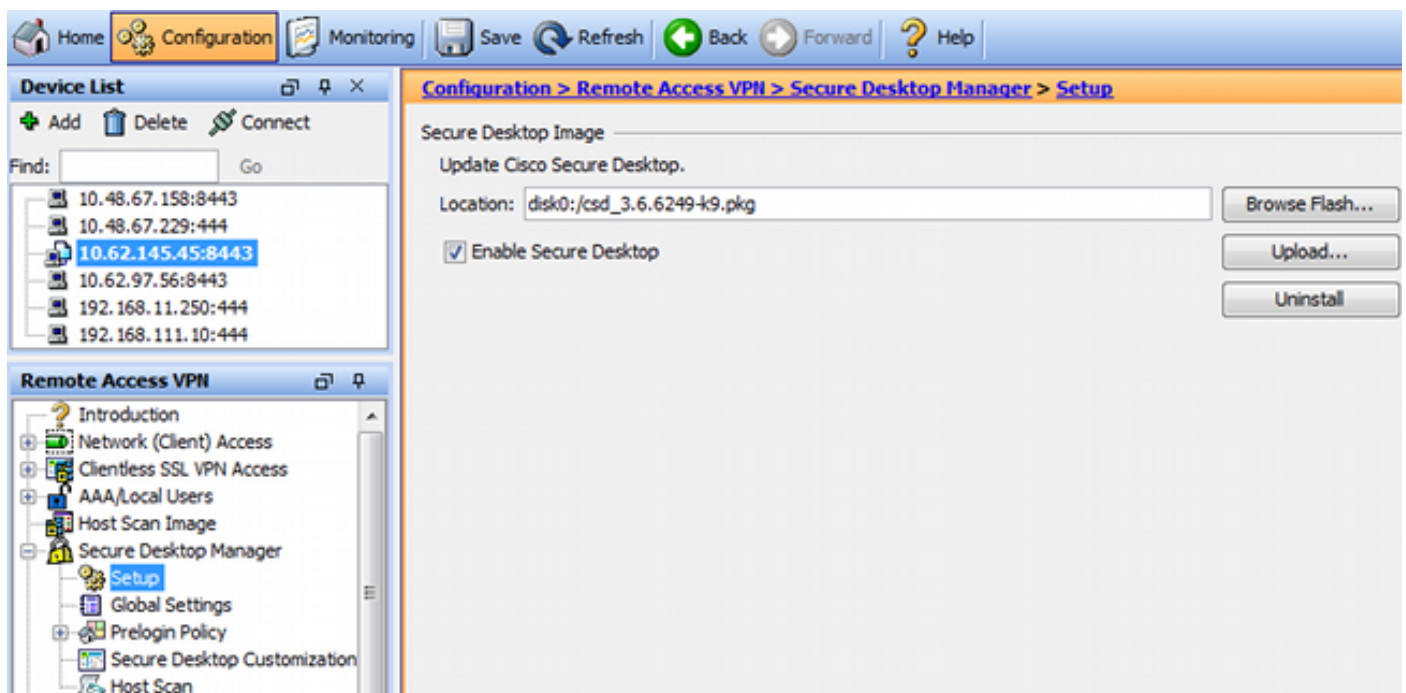
aaa-server ISE3 protocol radius
aaa-server ISE3 (inside) host 10.1.1.100
key *****

```

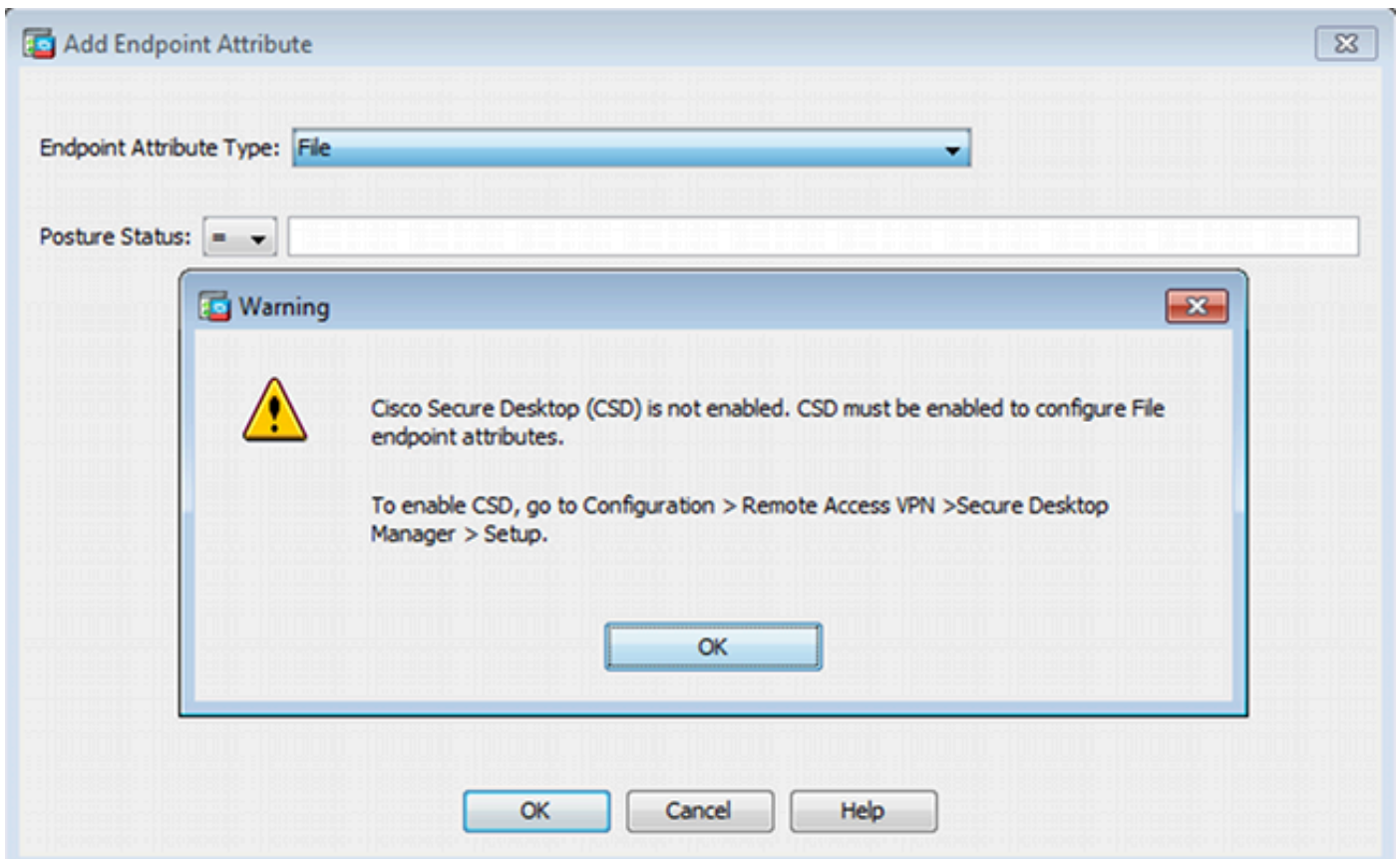
Il pacchetto AnyConnect è stato scaricato e utilizzato.

Passaggio 2. Installazione CSD

La configurazione successiva viene eseguita con Adaptive Security Device Manager (ASDM). Il pacchetto CSD deve essere scaricato per poter lampeggiare e prendere riferimento dalla configurazione come mostrato nell'immagine.



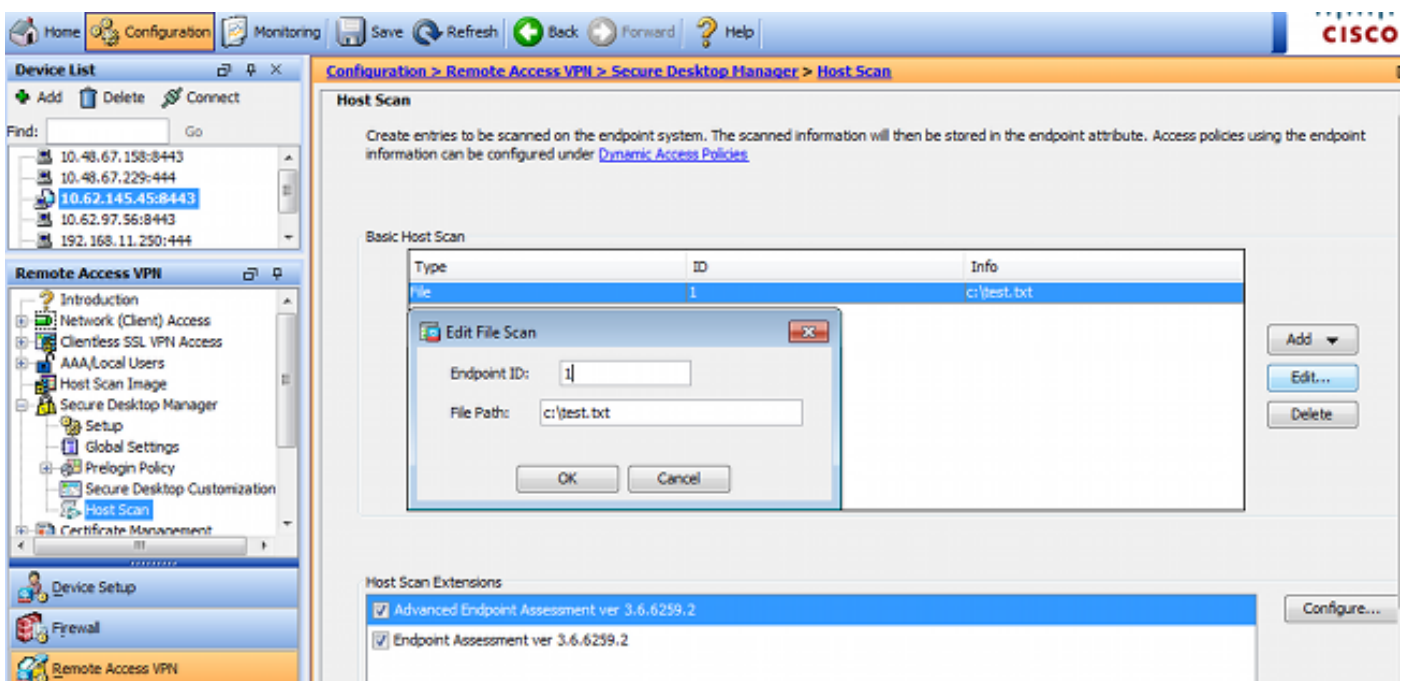
Senza l'attivazione di Secure Desktop non sarebbe possibile utilizzare gli attributi CSD nei criteri DAP, come mostrato nell'immagine.



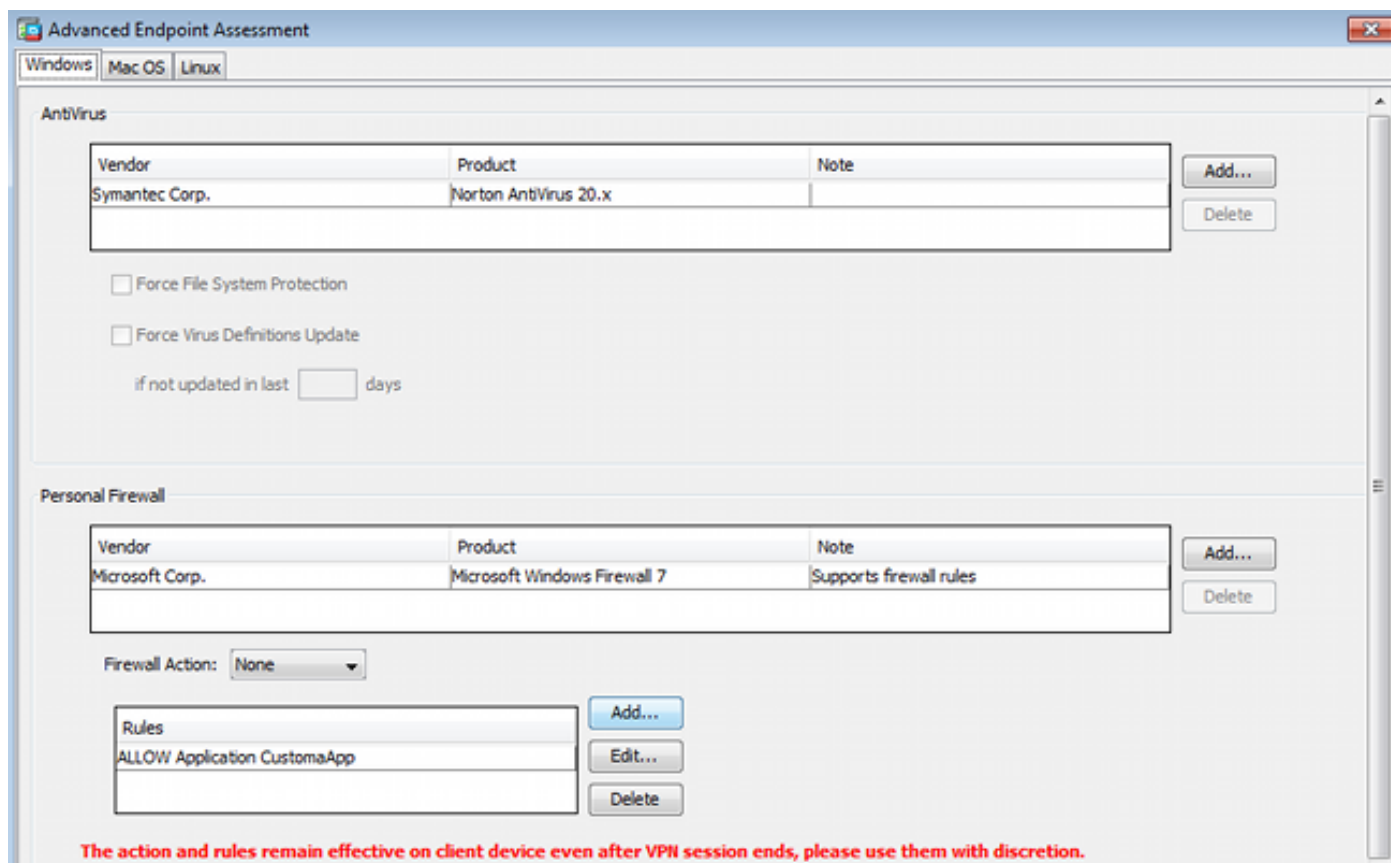
Dopo aver abilitato CSD, vengono visualizzate più opzioni in Secure Desktop Manager.

✍ Nota: si tenga presente che alcuni di essi sono già obsoleti. Per ulteriori informazioni sulle funzionalità deprecate, vedere: [avviso di deprecazione delle funzionalità per il desktop sicuro \(vaulting\), pulitura cache, rilevamento logger tasti e rilevamento emulazione host](#)

HostScan è ancora completamente supportato. Verrà aggiunta una nuova regola di base di HostScan. L'esistenza di c:\test.txt viene verificata come mostrato nell'immagine.



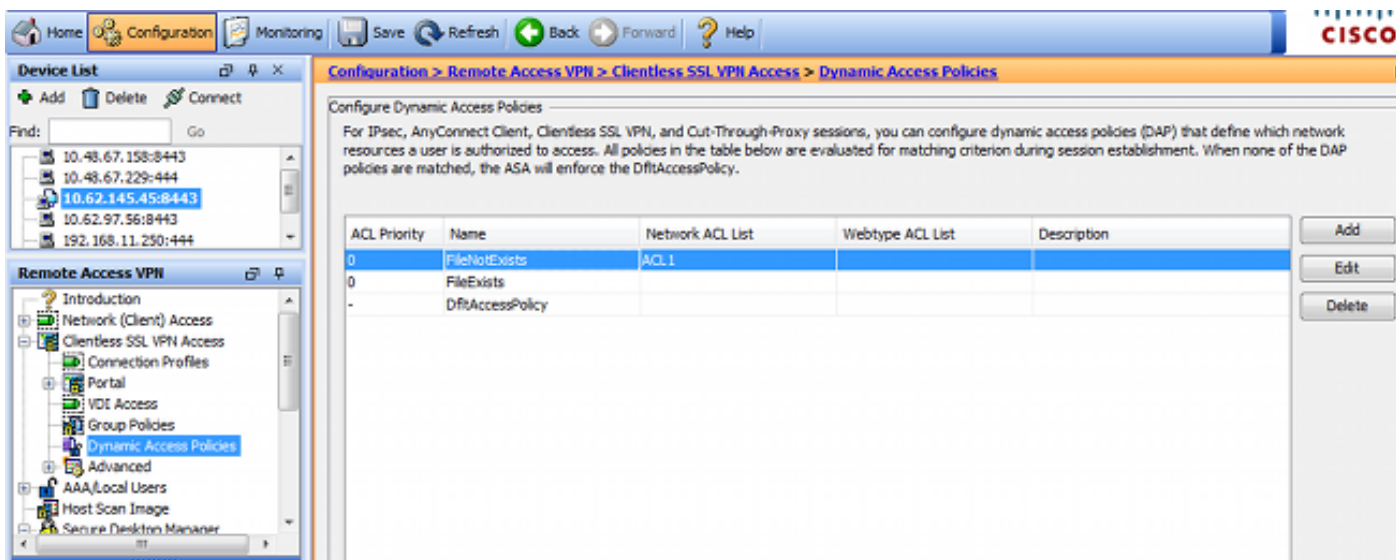
Inoltre, viene aggiunta una regola di Advanced Endpoint Assessment, come mostrato nell'immagine.



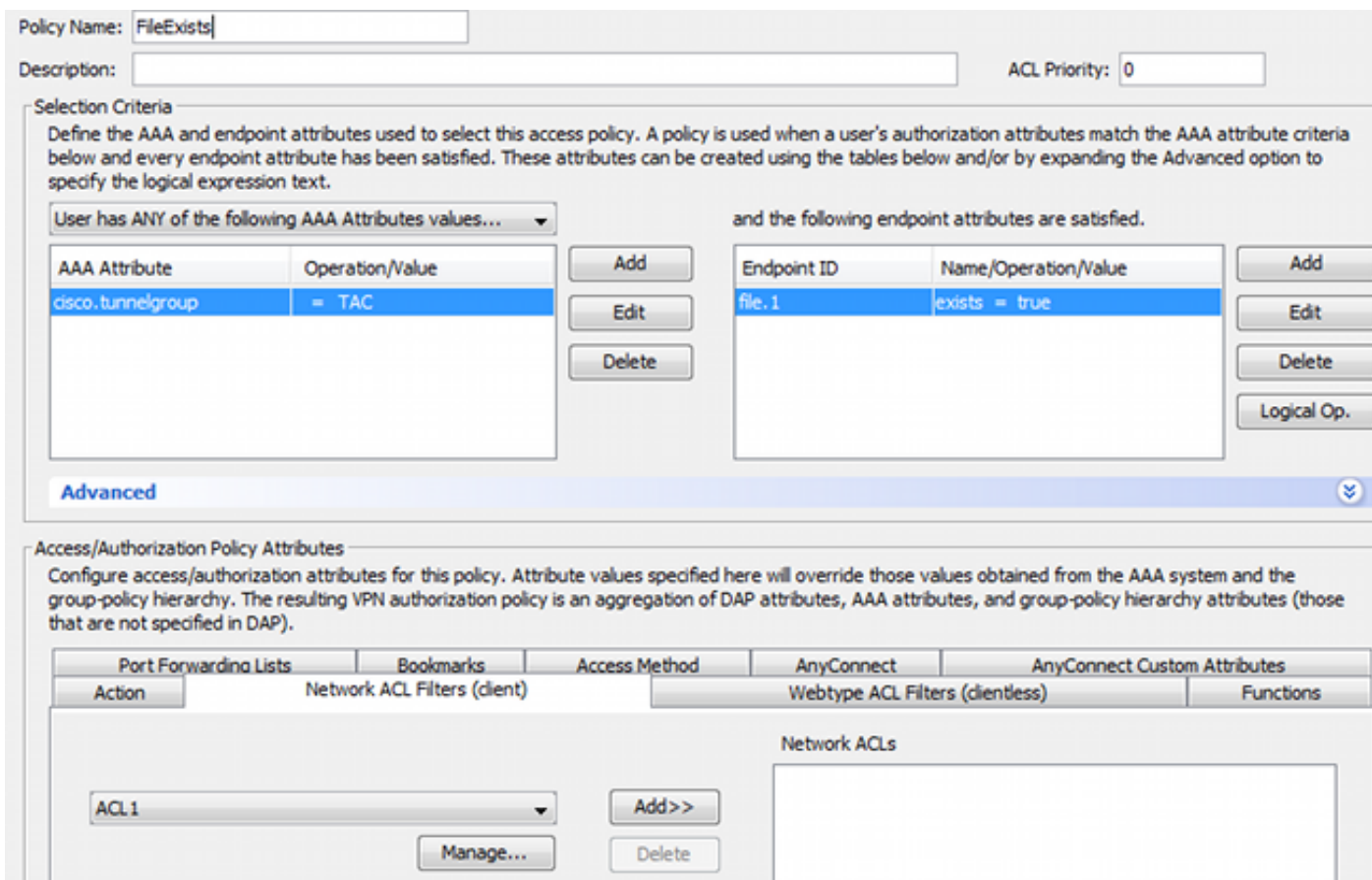
Questo controlla l'esistenza di Symantec Norton AntiVirus 20.x e Microsoft Windows Firewall 7. Il modulo di postura (HostScan) controlla questi valori, ma non vi sarà alcuna imposizione (il criterio DAP non lo verifica).

Passaggio 3. Criteri DAP

I criteri DAP sono responsabili dell'utilizzo dei dati raccolti da HostScan come condizioni e, di conseguenza, dell'applicazione di attributi specifici alla sessione VPN. Per creare la policy DAP da ASDM, selezionare Configurazione > VPN ad accesso remoto > Accesso VPN SSL senza client > Policy di accesso dinamico, come mostrato nell'immagine.

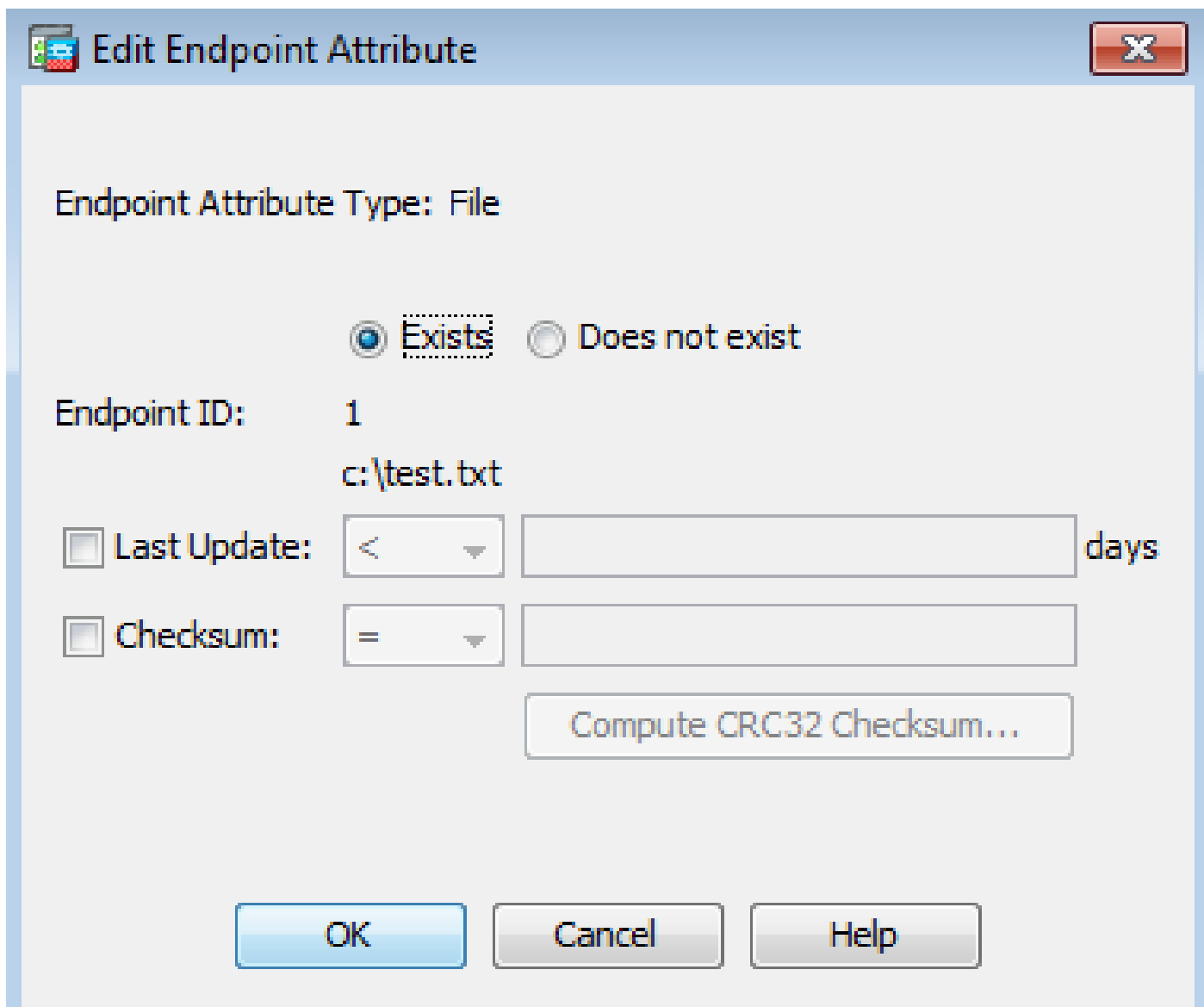


Il primo criterio (FileExists) controlla il nome del gruppo di tunnel utilizzato dal profilo VPN configurato (la configurazione del profilo VPN è stata omessa per chiarezza). Quindi, viene eseguito un ulteriore controllo per il file c:\test.txt, come mostrato nell'immagine.



Di conseguenza, non viene eseguita alcuna azione con l'impostazione predefinita per consentire la connettività. Non viene utilizzato alcun ACL. È disponibile l'accesso completo alla rete.

I dettagli per la verifica dei file sono come mostrato nell'immagine.



Il secondo criterio (FileNotExists) è simile, ma questa condizione temporale è valida se il file non esiste come mostrato nell'immagine.

Policy Name:

Description:

ACL Priority:

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... and the following endpoint attributes are satisfied.

AAA Attribute	Operation/Value	Endpoint ID	Name/Operation/Value
cisco.tunnelgroup	= TAC	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

ACL 1

Network ACLs

ACL 1

Per il risultato è stato configurato ACL1 con elenco accessi. Questa procedura è valida per gli utenti VPN non conformi con accesso di rete limitato.

Entrambi i criteri DAP richiedono l'accesso al client AnyConnect, come mostrato nell'immagine.

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 è utilizzato per l'autenticazione degli utenti. È necessario configurare solo il dispositivo di rete (ASA) e il nome utente corretto (cisco). Questa parte non è trattata in questo articolo.

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

CSD e provisioning di AnyConnect

All'inizio, all'utente non è stato assegnato un client AnyConnect. L'utente non è conforme ai criteri (il file c:\test.txt non esiste). Immettere <https://10.62.145.45> e l'utente viene immediatamente reindirizzato per l'installazione del CSD, come mostrato nell'immagine.



CISCO 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

A tale scopo, è possibile utilizzare Java o ActiveX. Una volta installato, il CSD viene segnalato come mostrato nell'immagine.



Cisco Secure Desktop



WebLaunch

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

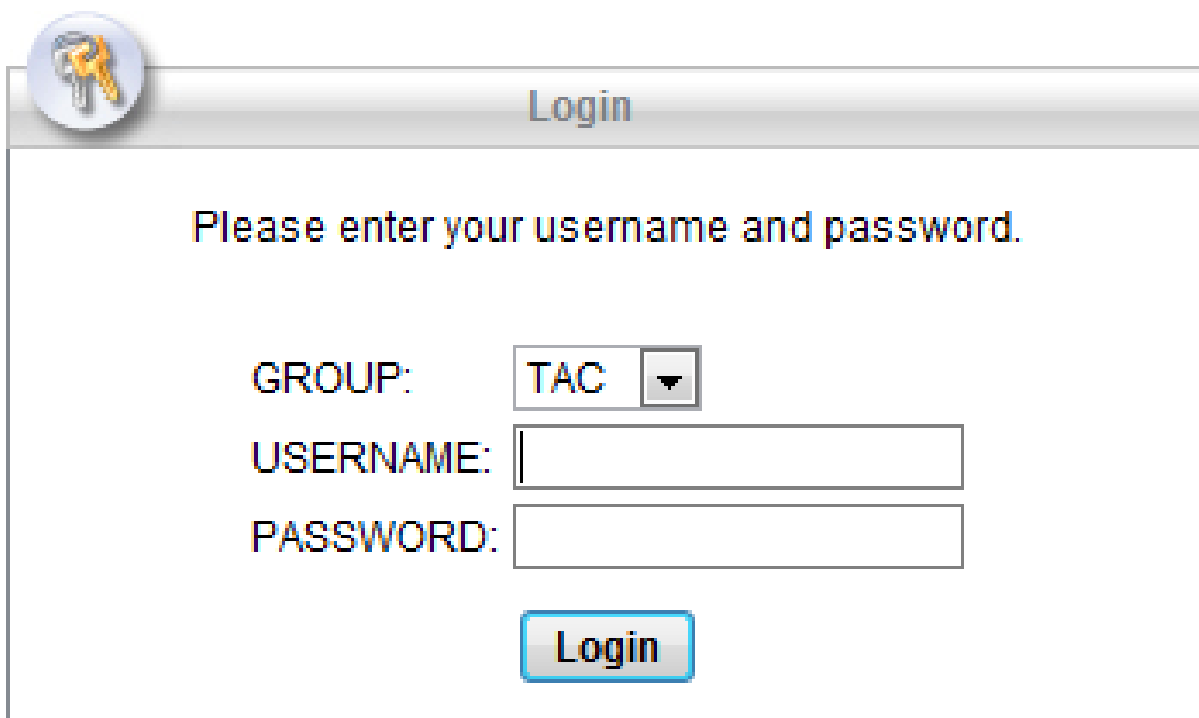
System Validated

Cisco Secure Desktop successfully validated your system.

Success. Reloading. Please wait...

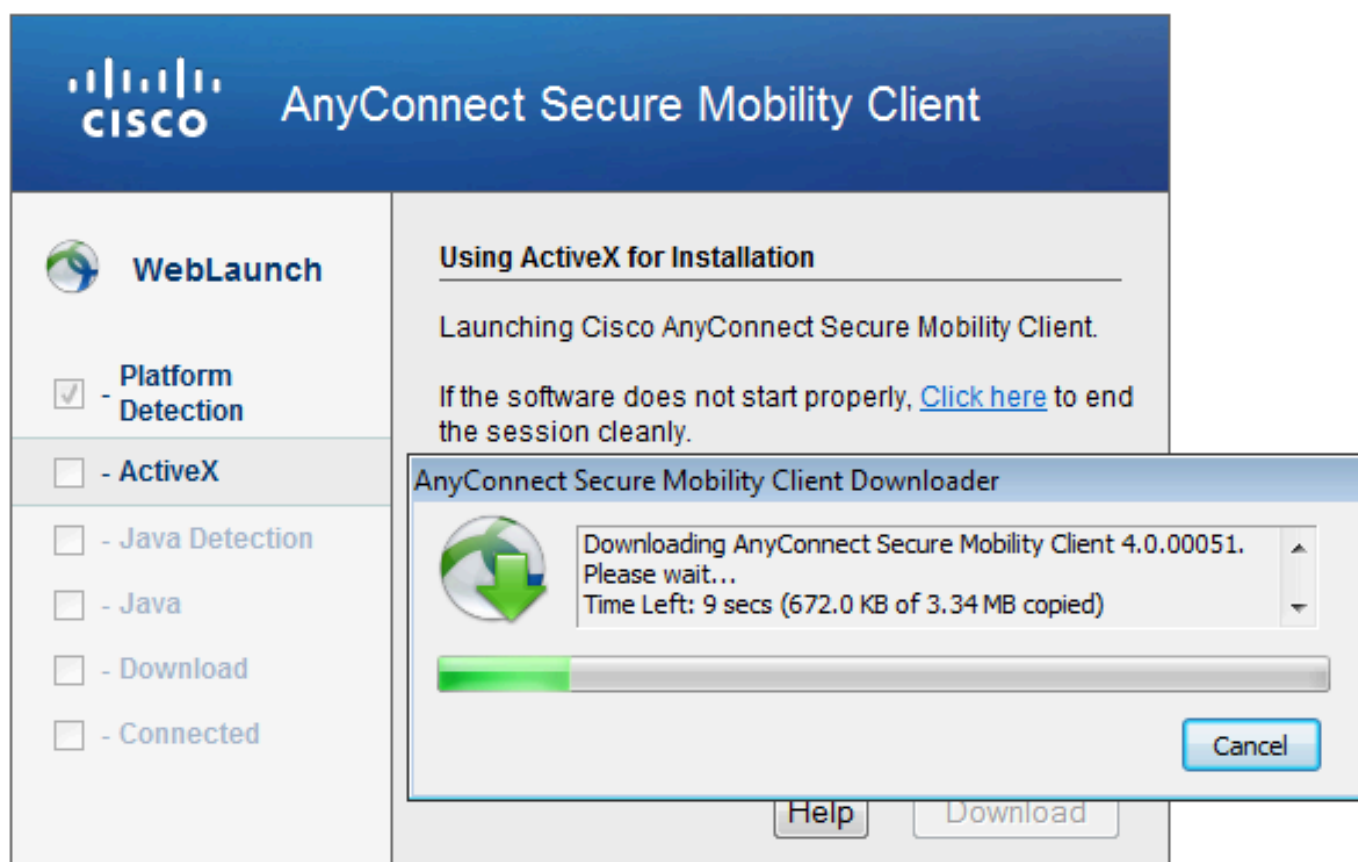
[Download](#)

Quindi l'utente viene reindirizzato per l'autenticazione come mostrato nell'immagine.



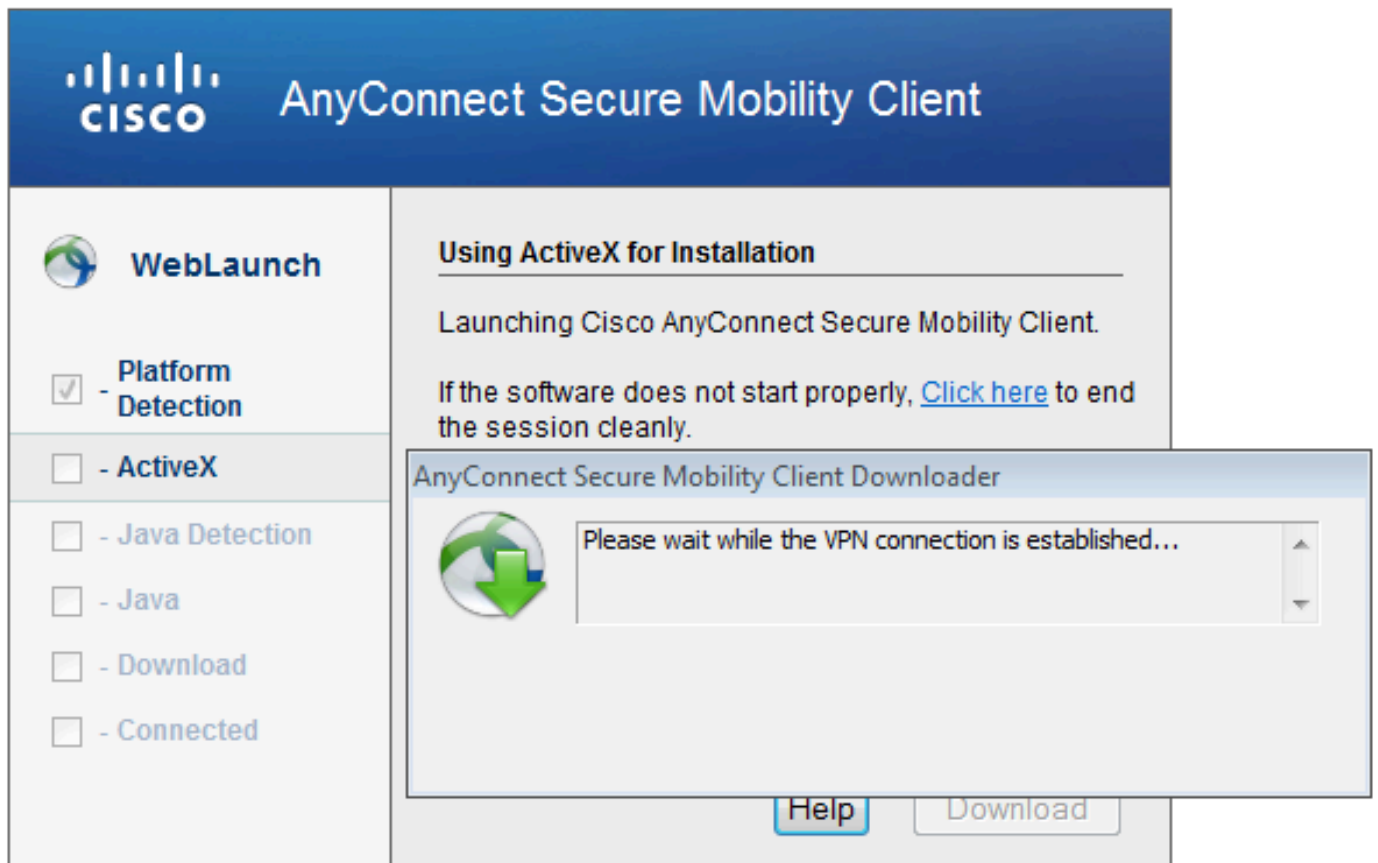
The image shows a 'Login' dialog box with a key icon in the top-left corner. The title bar reads 'Login'. The main text says 'Please enter your username and password.' Below this, there are three input fields: 'GROUP:' with a dropdown menu showing 'TAC', 'USERNAME:' with an empty text box, and 'PASSWORD:'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

Se il test ha esito positivo, viene distribuito AnyConnect con il profilo configurato. È possibile usare nuovamente ActiveX o Java, come mostrato nell'immagine.

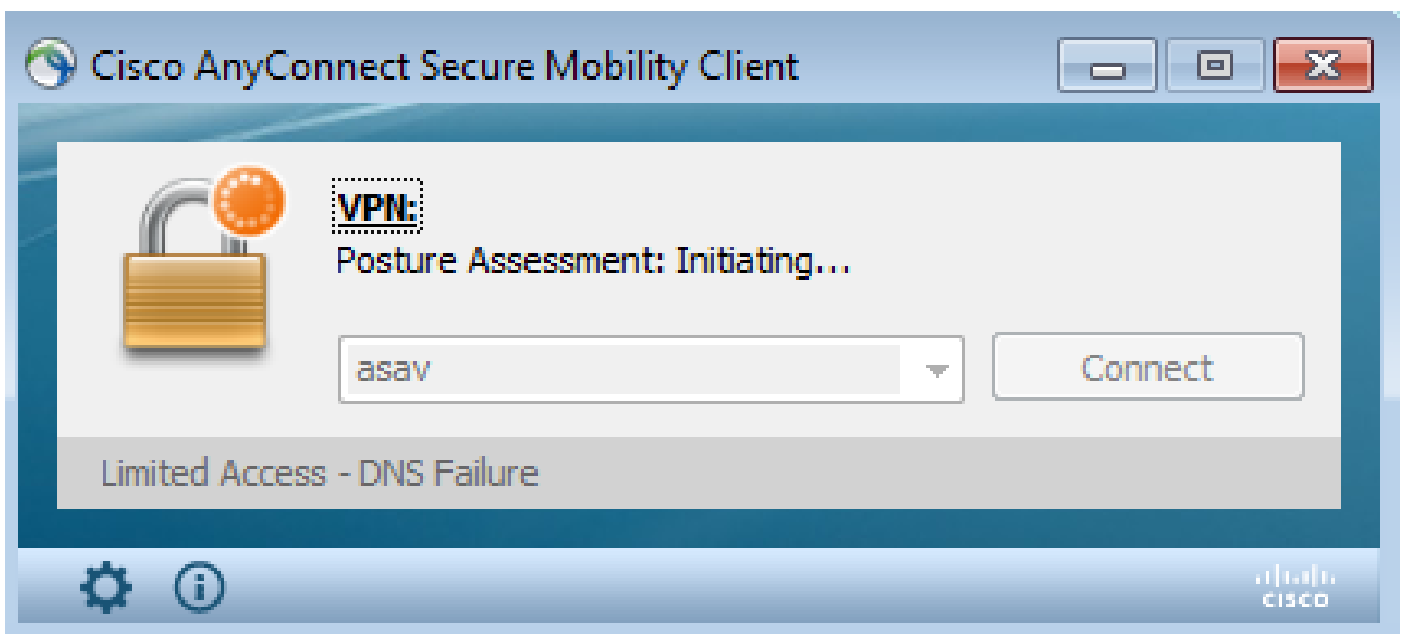


The image displays the Cisco AnyConnect Secure Mobility Client interface. The top header features the Cisco logo and the text 'AnyConnect Secure Mobility Client'. On the left side, there is a 'WebLaunch' section with a list of options: 'Platform Detection' (checked), 'ActiveX' (unchecked), 'Java Detection' (unchecked), 'Java' (unchecked), 'Download' (unchecked), and 'Connected' (unchecked). The main area is titled 'Using ActiveX for Installation' and contains the text: 'Launching Cisco AnyConnect Secure Mobility Client. If the software does not start properly, [Click here](#) to end the session cleanly.' A modal dialog box titled 'AnyConnect Secure Mobility Client Downloader' is overlaid on the main interface. It shows a progress bar and the text: 'Downloading AnyConnect Secure Mobility Client 4.0.00051. Please wait... Time Left: 9 secs (672.0 KB of 3.34 MB copied)'. A 'Cancel' button is located at the bottom right of the dialog box. At the bottom of the main interface, there are 'Help' and 'Download' buttons.

La connessione VPN viene stabilita come mostrato nell'immagine.



Il primo passo di AnyConnect è eseguire i controlli della postura (HostScan) e inviare i rapporti all'appliance ASA, come mostrato nell'immagine.

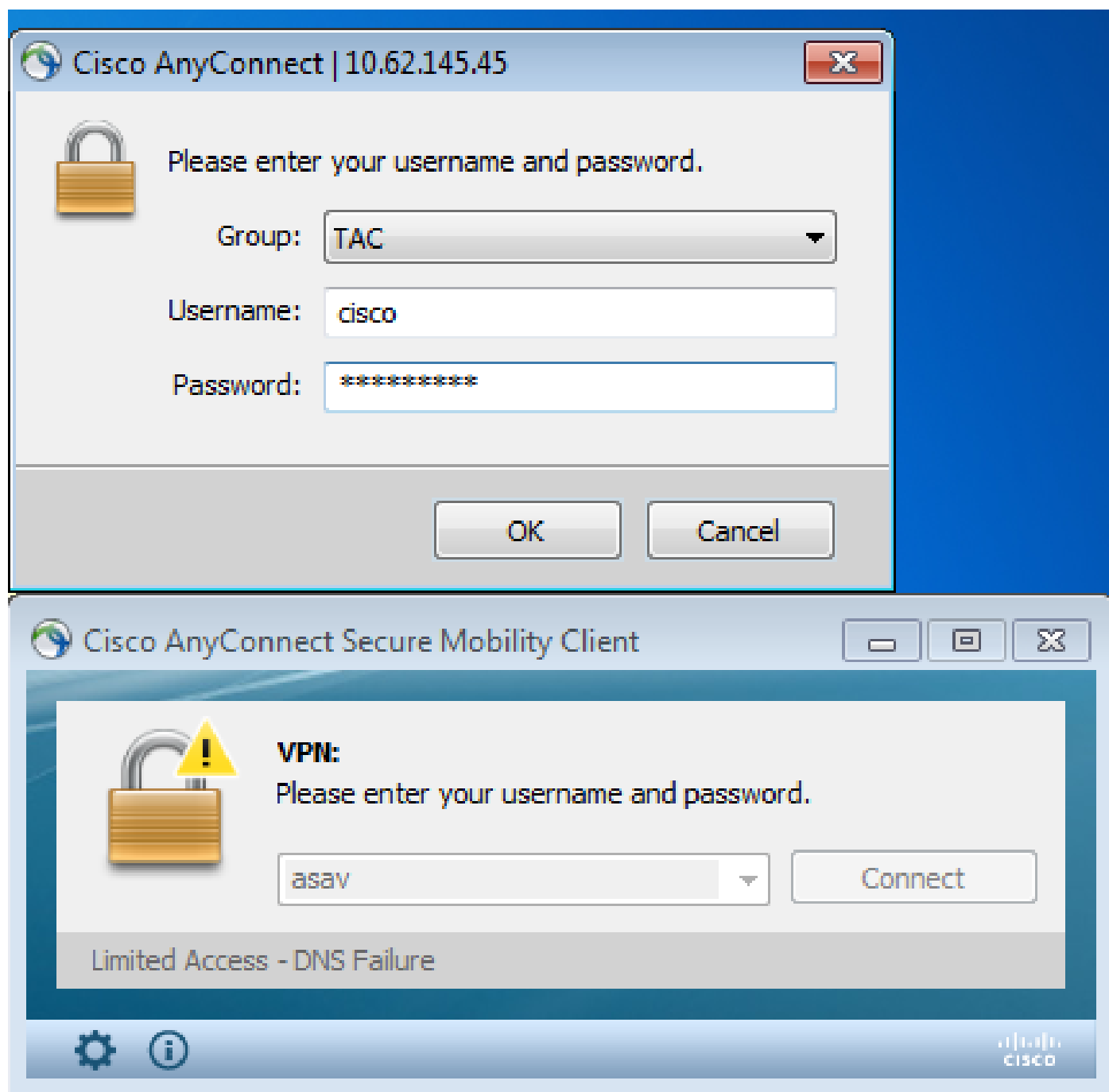


Quindi, AnyConnect autentica e termina la sessione VPN.

Sessione VPN AnyConnect con postura - Non conforme

Quando si stabilisce una nuova sessione VPN con AnyConnect, il primo passaggio è la postura (HostScan) come mostrato nello screenshot precedente. Quindi, viene eseguita l'autenticazione e

la sessione VPN viene stabilita come mostrato nelle immagini.



L'ASA segnala che il report HostScan è stato ricevuto:

```
<#root>
```

```
%ASA-7-716603:
```

```
Received 4 KB Hostscan data
```

```
from IP <10.61.87.251>
```

Esegui quindi l'autenticazione dell'utente:

<#root>

%ASA-6-113004:

AAA user authentication Successful

: server = 10.62.145.42 : user = cisco

E avvia l'autorizzazione per quella sessione VPN. Se "debug dap trace 255" è abilitato, vengono restituite le informazioni relative all'esistenza del file c:\test.txt:

<#root>

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"

Inoltre, informazioni relative a Microsoft Windows Firewall:

<#root>

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 Wind

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"

e Symantec AntiVirus (in base alle regole per la valutazione avanzata degli endpoint di HostScan configurate in precedenza).

Di conseguenza, il criterio DAP corrisponde:

```
<#root>
```

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

Questa policy impone l'uso di AnyConnect e applica anche l'ACL1 con elenco degli accessi che fornisce all'utente un accesso alla rete limitato (non conforme alla policy aziendale):

```
<#root>
```

```
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
```

I log presentano anche estensioni ACIDEX che possono essere utilizzate dai criteri DAP (o persino passate in Radius-Requests a ISE e utilizzate in Authorization Rules come condizioni):

```
<#root>
```

```
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
";
```

Di conseguenza, la sessione VPN è attiva ma con l'accesso di rete limitato:

```
<#root>
```

```
ASA#
```

```
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
```

La cronologia di AnyConnect mostra i passaggi dettagliati del processo di postura:

<#root>

```
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.

Sessione VPN con postura di AnyConnect - Conforme

Dopo aver creato il file c:\test.txt, il flusso è simile. Una volta avviata una nuova sessione AnyConnect, i log indicano l'esistenza del file:

```
<#root>
```

```
%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"
```

Di conseguenza viene utilizzato un altro criterio DAP:

```
<#root>
```

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

Il criterio non impone alcun ACL come restrizione per il traffico di rete.

E la sessione è attiva senza alcun ACL (accesso completo alla rete):

```
<#root>
```

```
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

Inoltre, Anyconnect segnala che HostScan è inattivo e in attesa della richiesta di analisi successiva:

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

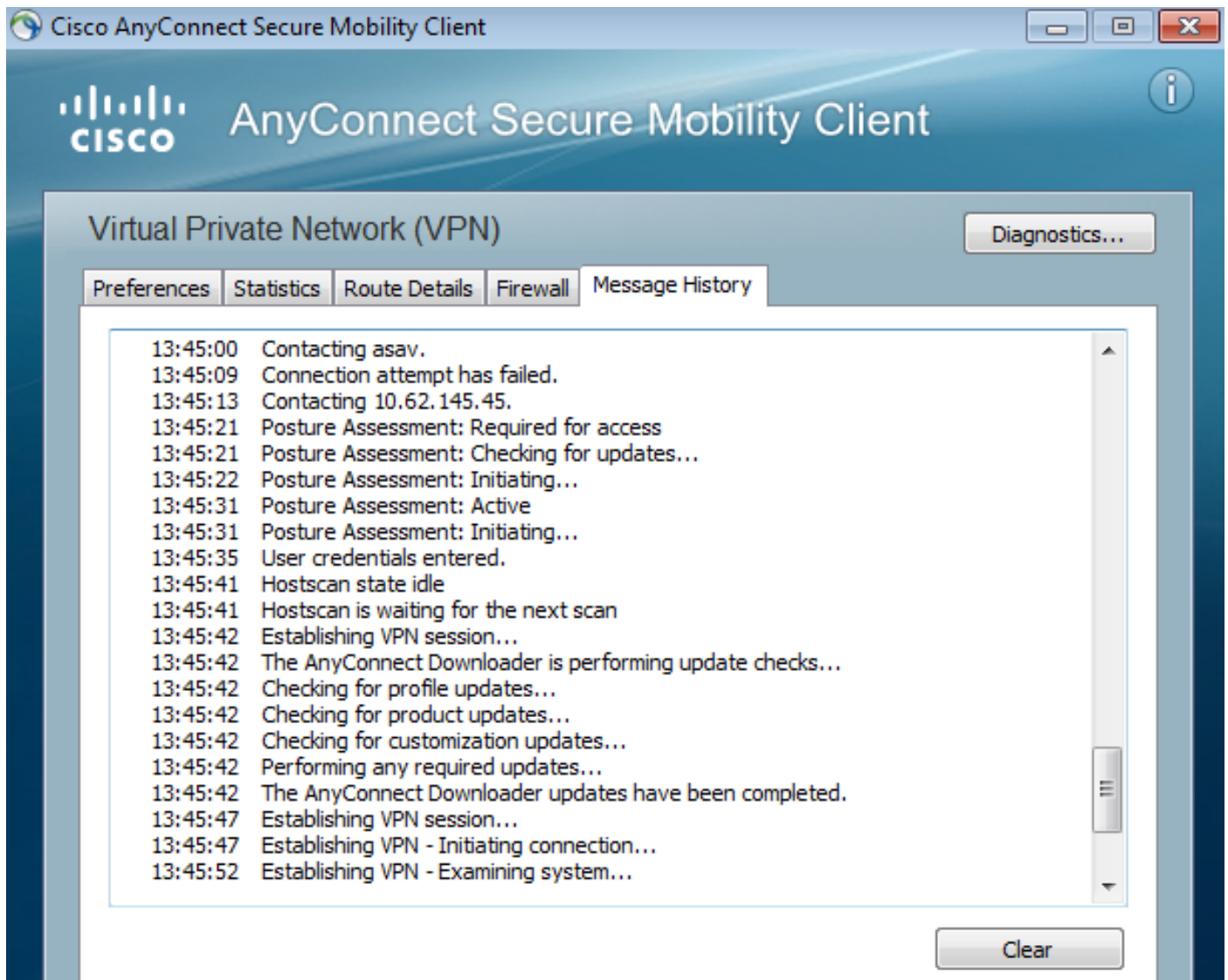
 Nota: per la rivalutazione, si consiglia di utilizzare un modulo di postura integrato con ISE.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

AnyConnect DART

AnyConnect fornisce la funzionalità Diagnostica, come mostrato nell'immagine.



The screenshot shows the Cisco AnyConnect Secure Mobility Client interface. The title bar reads "Cisco AnyConnect Secure Mobility Client". The main window title is "AnyConnect Secure Mobility Client". Below the title bar, there is a "Virtual Private Network (VPN)" section with a "Diagnostics..." button. The "Message History" tab is selected, displaying a list of log messages:

- 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...

At the bottom right of the message history window, there is a "Clear" button.

Che raccoglie e salva tutti i log di AnyConnect in un file zip sul desktop. Il file zip include i log di Cisco AnyConnect Secure Mobility Client/Anyconnect.txt.

In questo documento vengono fornite le informazioni sull'appliance ASA e viene richiesto a HostScan di raccogliere i dati:

<#root>

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.

In seguito, diversi altri registri rivelano che CSD è installato. Questo è l'esempio di un provisioning CSD e della successiva connessione AnyConnect con la postura:

<#root>

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...

La comunicazione tra ASA e AnyConnect è ottimizzata, l'ASA richiede di eseguire solo alcuni controlli specifici. AnyConnect scarica altri dati per poter eseguire questa operazione (ad esempio, la verifica antivirus specifica).

Quando si apre la richiesta con TAC, allegare i log Dart insieme a "show tech" e "debug dap trace 255" generati dall'ASA.

Informazioni correlate

- [Configurazione della scansione dell'host e del modulo postura - Guida dell'amministratore di Cisco AnyConnect Secure Mobility](#)
- [Guida alla configurazione dei servizi di postura di Cisco ISE](#)
- [Guida per l'amministratore di Cisco ISE 1.3](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).