

Configurer la posture pour les sessions VPN sur l'ASA avec CSD, DAP et AnyConnect 4.0

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Diagramme du réseau](#)

[ASA](#)

[Étape 1. Configuration VPN SSL de base](#)

[Étape 2. Installation du CSD](#)

[Étape 3. Politiques DAP](#)

[ISE](#)

[Vérification](#)

[Approvisionnement CSD et AnyConnect](#)

[Session VPN AnyConnect avec posture - Non conforme](#)

[Session VPN AnyConnect avec posture - Conforme](#)

[Dépannage](#)

[DART AnyConnect](#)

[Informations connexes](#)

Introduction

Ce document décrit comment effectuer la posture pour les sessions VPN à distance terminées sur l'appareil de sécurité adaptatif (ASA). La position est exécutée localement par ASA avec l'utilisation de Cisco Secure Desktop (CSD) avec le module HostScan. Une fois la session VPN établie, la station conforme est autorisée à accéder au réseau entier alors que la station non conforme a un accès réseau limité.

En outre, les flux d'approvisionnement CSD et AnyConnect 4.0 sont présentés.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration VPN Cisco ASA
- Client de mobilité sécurisée Cisco AnyConnect

Components Used

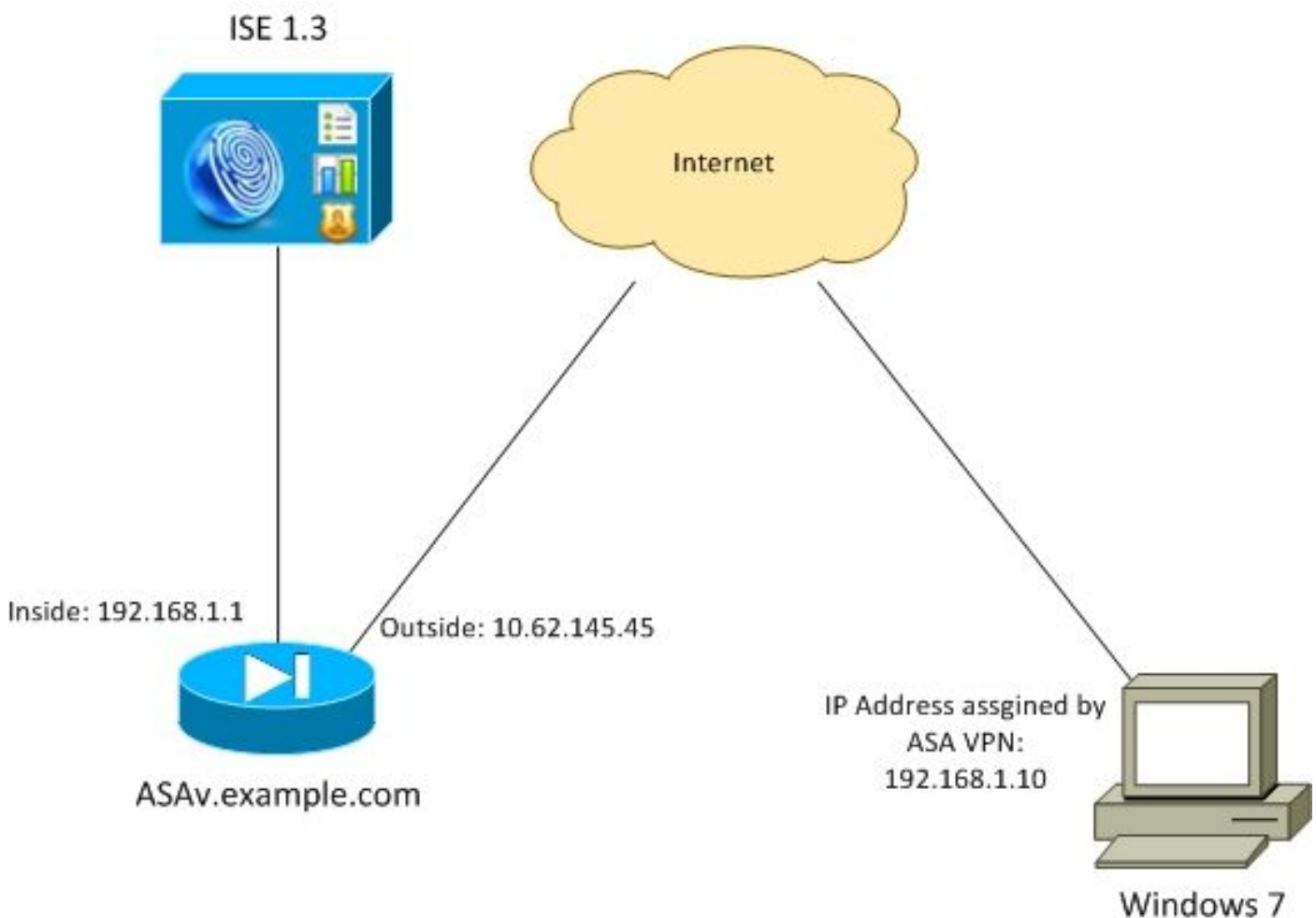
Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Microsoft Windows 7
- Cisco ASA, version 9.3 ou ultérieure
- Logiciel Cisco Identity Services Engine (ISE), versions 1.3 et ultérieures
- Client de mobilité sécurisée Cisco AnyConnect, versions 4.0 et ultérieures
- CSD, version 3.6 ou ultérieure

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration

Diagramme du réseau



La politique de l'entreprise est la suivante :

- Les utilisateurs VPN distants qui ont le fichier `c:\test.txt` (conforme) doivent avoir un accès réseau complet aux ressources internes de l'entreprise
- Les utilisateurs VPN distants qui n'ont pas de fichier `c:\test.txt` (non conforme) doivent avoir un accès réseau limité aux ressources internes de l'entreprise : seul l'accès au serveur de conversion 1.1.1.1 est fourni.

L'existence des fichiers en est l'exemple le plus simple. Toute autre condition (antivirus,

antispyware, processus, application, registre) peut être utilisée.

Le flux est le suivant :

- AnyConnect n'est pas installé sur les utilisateurs distants. Ils accèdent à la page Web ASA pour le provisionnement CSD et AnyConnect (avec le profil VPN)
- Une fois la connexion établie via AnyConnect, les utilisateurs non conformes sont autorisés avec un accès réseau limité. La stratégie d'accès dynamique (DAP) appelée **FileNotExists** correspond.
- L'utilisateur effectue la correction (installation manuelle du fichier **c:\test.txt**) et se connecte à nouveau à AnyConnect. Cette fois-ci, un accès réseau complet est fourni (la stratégie DAP appelée **FileExists** correspond).

Le module HostScan peut être installé manuellement sur le terminal. Les fichiers d'exemple (hostscan-win-4.0.00051-pre-Deployment-k9.msi) sont partagés sur Cisco Connection Online (CCO). Mais il pourrait aussi être poussé de l'ASA. HostScan fait partie du CSD qui peut être provisionné à partir d'ASA. Cette deuxième approche est utilisée dans cet exemple.

Pour les versions antérieures d'AnyConnect (3.1 et antérieures), un package distinct était disponible sur CCO (exemple : hostscan_3.1.06073-k9.pkg) qui aurait pu être configuré et provisionné séparément sur ASA (avec la commande **csd hostscan image**) - mais cette option n'existe plus pour AnyConnect version 4.0.

ASA

Étape 1. Configuration VPN SSL de base

ASA est préconfiguré avec un accès VPN distant de base (SSL (Secure Sockets Layer)) :

```
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

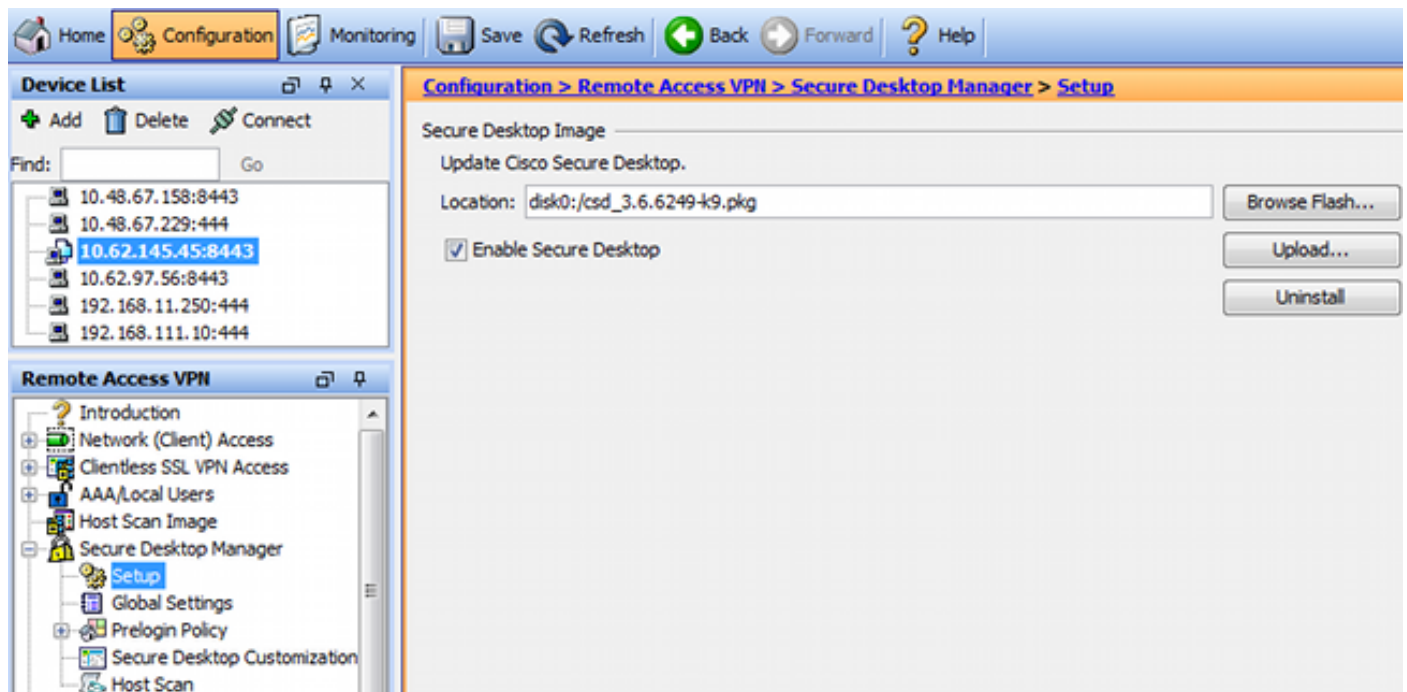
ip local pool POOL 192.168.1.10-192.168.1.20 mask 255.255.255.0

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

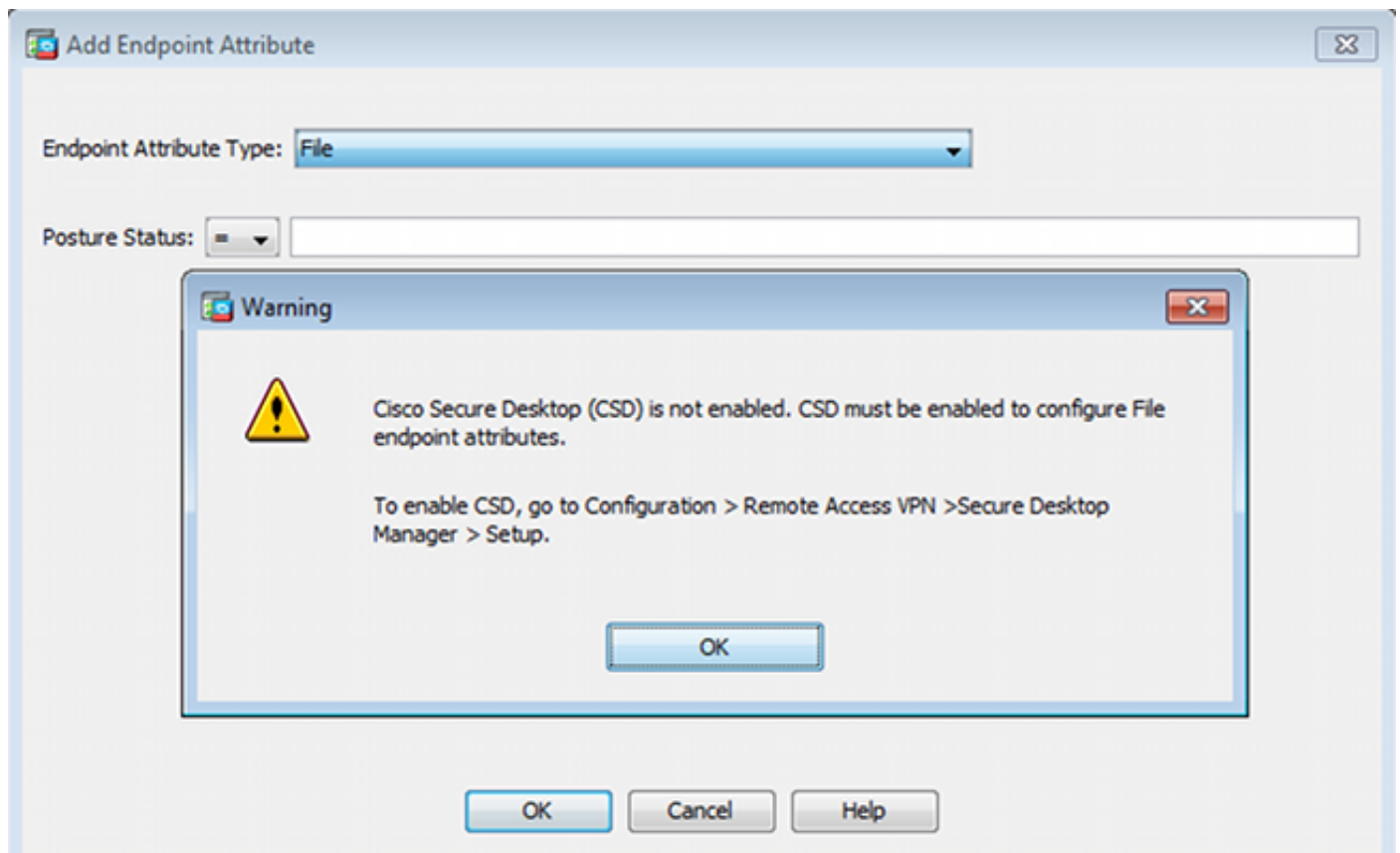
Le package AnyConnect a été téléchargé et utilisé.

Étape 2. Installation du CSD

La configuration suivante est effectuée avec Adaptive Security Device Manager (ASDM). Le package CSD doit être téléchargé afin de cliquer et de prendre la référence de la configuration comme indiqué dans l'image.



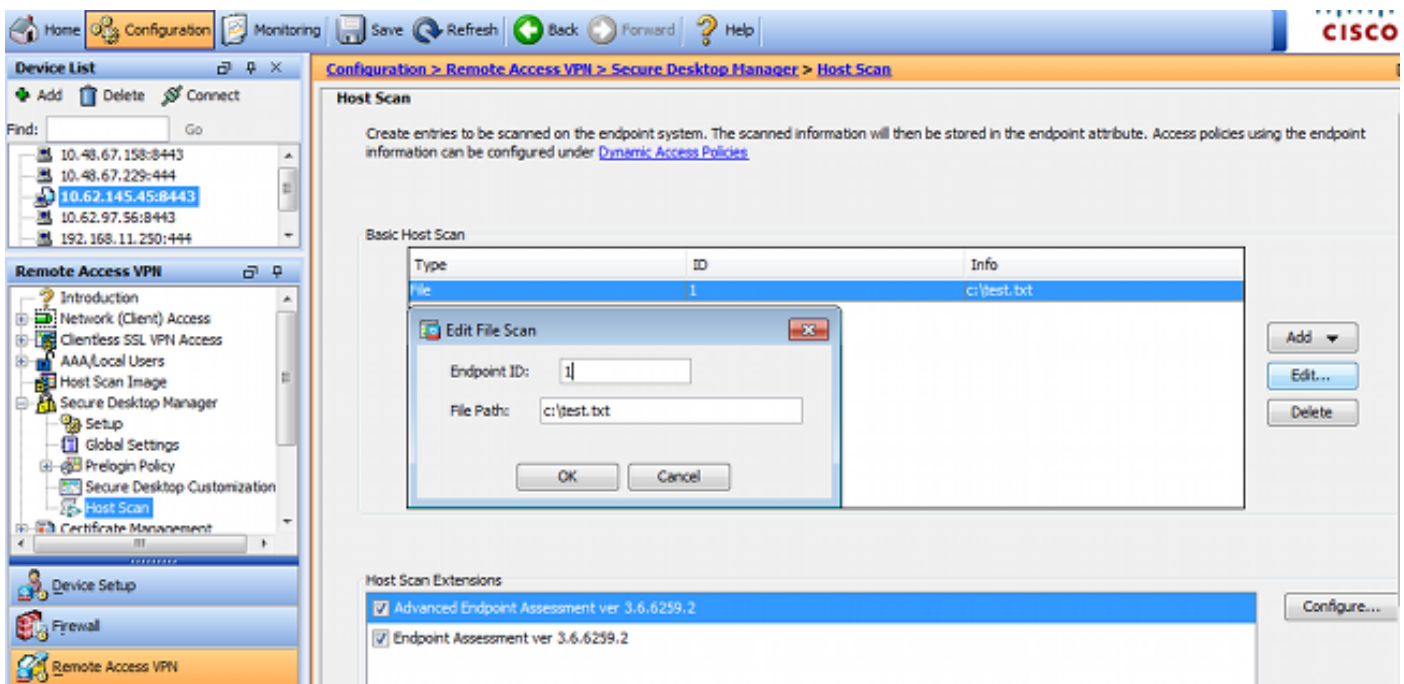
Sans l'activation de Secure Desktop, il ne serait pas possible d'utiliser les attributs CSD dans les politiques DAP comme le montre l'image.



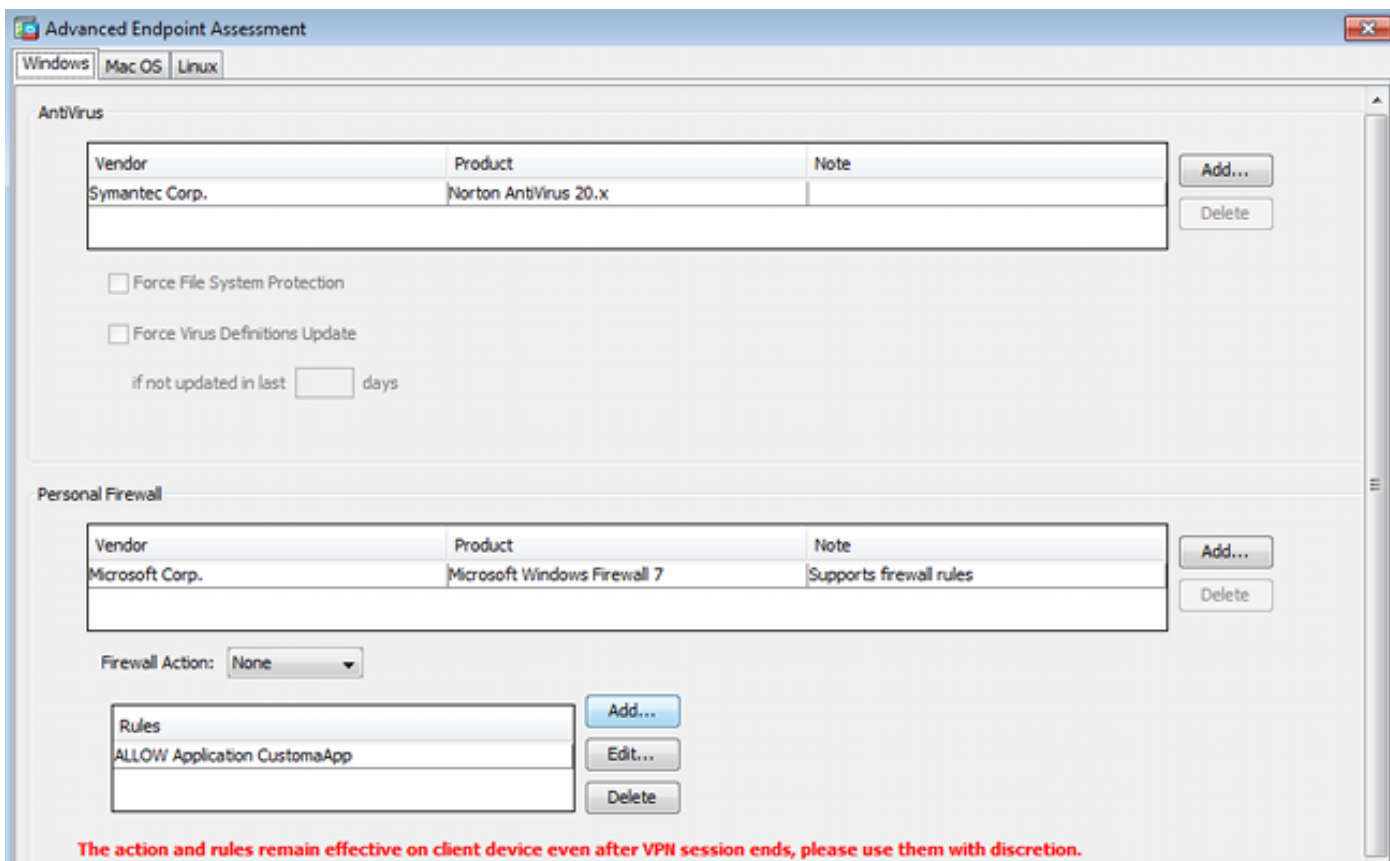
Après avoir activé le CSD, plusieurs options s'affichent sous Secure Desktop Manager.

Note: Soyez informé que certains d'entre eux sont déjà déconseillés. Vous trouverez plus d'informations sur les fonctionnalités déconseillées : [Avis de déviation des fonctionnalités pour Secure Desktop \(Vault\), Cache Cleaner, KeyAVC Logger Detection et Host Emulation Detection](#)

HostScan est toujours entièrement pris en charge, la nouvelle règle Basic HostScan est ajoutée. L'existence de `c:\test.txt` est vérifiée comme le montre l'image.



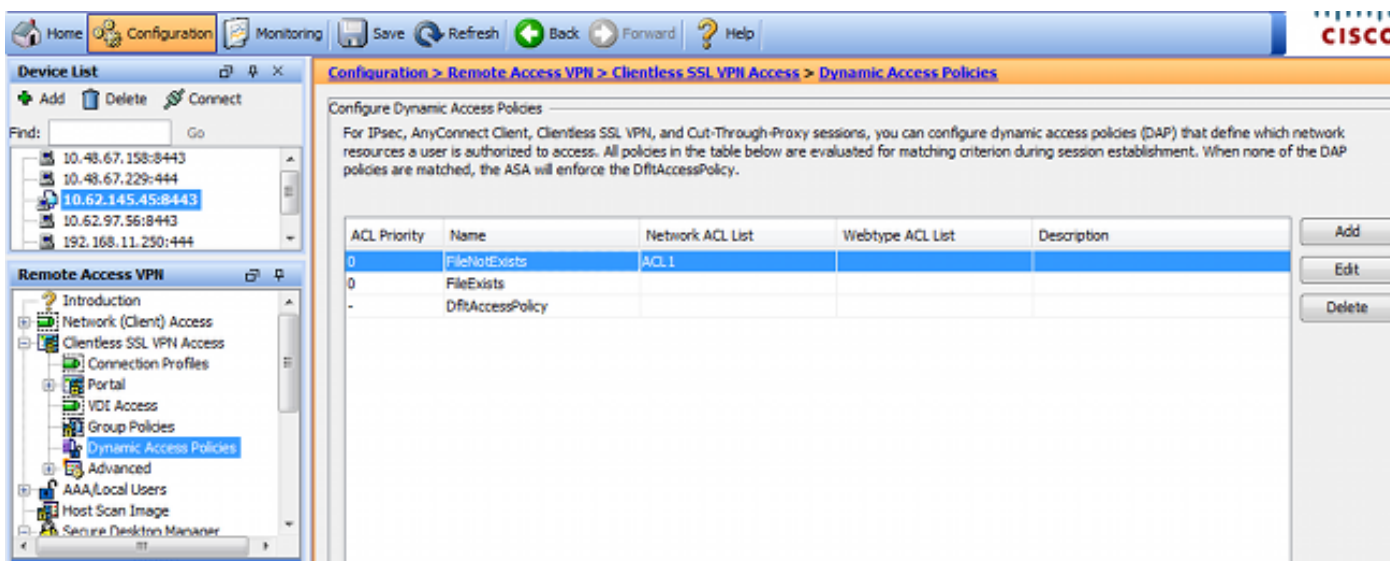
En outre, une règle d'évaluation avancée des points de terminaison supplémentaire est ajoutée, comme l'illustre l'image.



Celui-ci vérifie l'existence de Symantec Norton AntiVirus 20.x et de Microsoft Windows Firewall 7. Le module de posture (HostScan) vérifie ces valeurs mais il n'y aura aucune application (la politique DAP ne vérifie pas cela).

Étape 3. Politiques DAP

Les politiques DAP sont responsables d'utiliser les données collectées par HostScan comme conditions et d'appliquer des attributs spécifiques à la session VPN en conséquence. Afin de créer une stratégie DAP à partir d'ASDM, accédez à **Configuration > Remote Access VPN > Client less SSL VPN Access > Dynamic Access Policies** comme illustré dans l'image.



La première stratégie (FileExists) vérifie le nom du groupe de tunnels utilisé par le profil VPN configuré (la configuration du profil VPN a été omise pour plus de clarté). Ensuite, une vérification supplémentaire pour le fichier `c:\test.txt` est effectuée comme indiqué dans l'image.

Policy Name: ACL Priority:

Description:

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
isco.tunnelgroup	= TAC	file.1	exists = true

Buttons: Add, Edit, Delete, Logical Op.

Advanced

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

Port Forwarding Lists | Bookmarks | Access Method | AnyConnect | AnyConnect Custom Attributes

Action | Network ACL Filters (client) | Webtype ACL Filters (clientless) | Functions

Network ACLs

ACL 1 | Add >> | Manage... | Delete

Par conséquent, aucune action n'est effectuée avec le paramètre par défaut afin d'autoriser la connectivité. Aucune liste de contrôle d'accès n'est utilisée - un accès réseau complet est fourni.

Les détails de la vérification du fichier sont indiqués dans l'image.

Edit Endpoint Attribute

Endpoint Attribute Type: File

Exists Does not exist

Endpoint ID: 1
 c:\test.txt

Last Update: < [] days

Checksum: = []

Compute CRC32 Checksum...

OK Cancel Help

La deuxième stratégie (FileNotExists) est similaire, mais cette condition de temps est **si le fichier**

n'existe pas comme indiqué dans l'image.

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...

AAA Attribute	Operation/Value
cisco.tunnelgroup	= TAC

and the following endpoint attributes are satisfied.

Endpoint ID	Name/Operation/Value
file.1	exists != true

Advanced

Access/Authorization Policy Attributes

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

Port Forwarding Lists | Bookmarks | Access Method | AnyConnect | AnyConnect Custom Attributes

Action | Network ACL Filters (client) | Webtype ACL Filters (clientless) | Functions

ACL 1

Network ACLs

ACL 1

La liste de contrôle d'accès ACL1 est configurée pour le résultat. Cela s'applique aux utilisateurs VPN non conformes avec un accès réseau limité.

Les deux stratégies DAP poussent à l'accès **AnyConnect Client** comme l'illustre l'image.

Access/Authorization Policy Attributes

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

Action | Network ACL Filters (client) | Webtype ACL Filters (clientless) | Functions

Port Forwarding Lists | Bookmarks | Access Method | AnyConnect | AnyConnect Custom Attributes

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

ISE

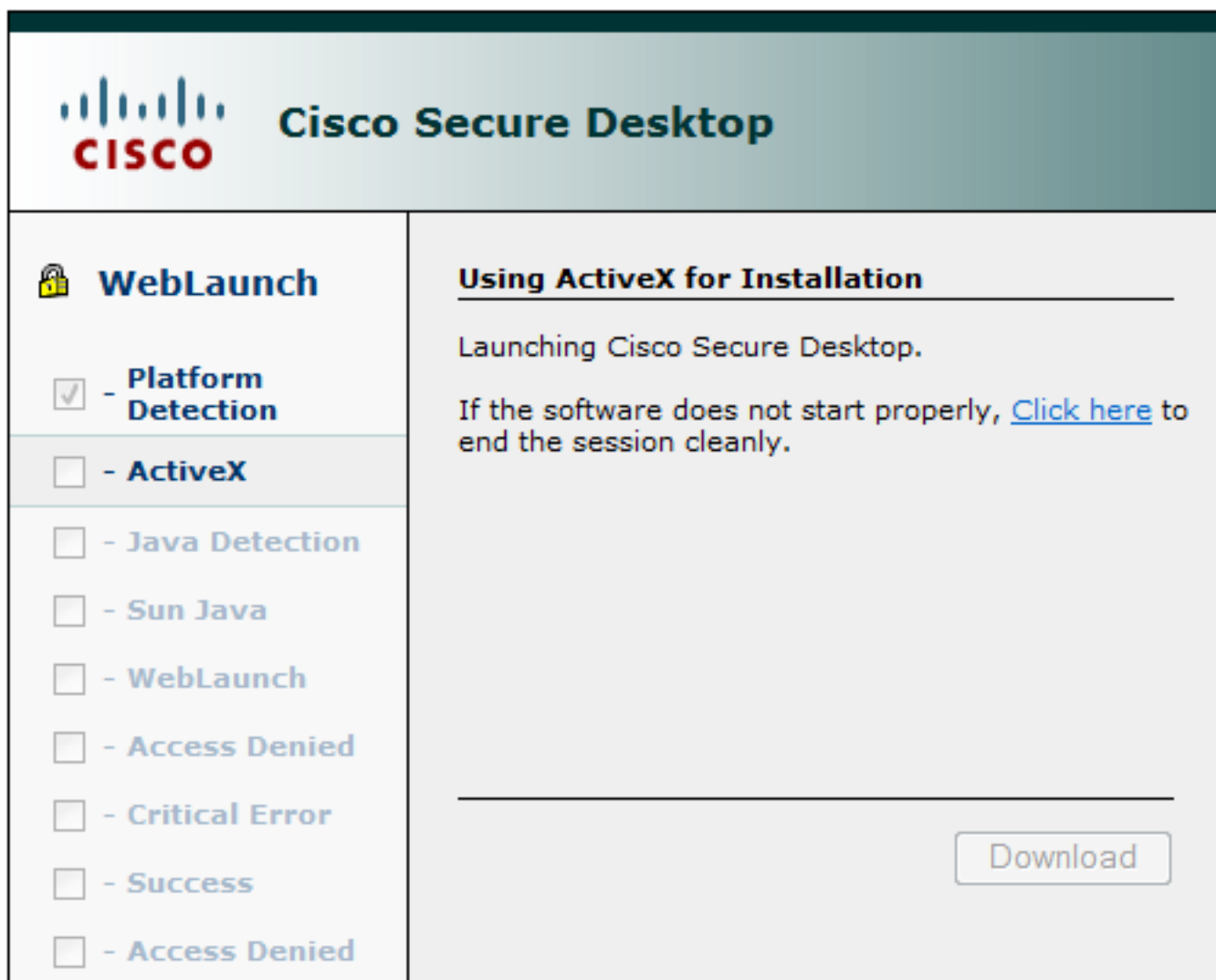
ISE est utilisé pour l'authentification des utilisateurs. Seul le périphérique réseau (ASA) et le nom d'utilisateur correct (cisco) doivent être configurés. Cette partie n'est pas traitée dans cet article.

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Approvisionnement CSD et AnyConnect

Initialement, l'utilisateur n'est pas approvisionné avec le client AnyConnect. L'utilisateur n'est pas non plus conforme à la stratégie (le fichier `c:\test.txt` n'existe pas). Entrez <https://10.62.145.45> et l'utilisateur est immédiatement redirigé pour l'installation de CSD comme indiqué dans l'image.



Cela peut être fait avec Java ou ActiveX. Une fois le CSD installé, il est signalé comme indiqué dans l'image.



Cisco Secure Desktop



WebLaunch

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

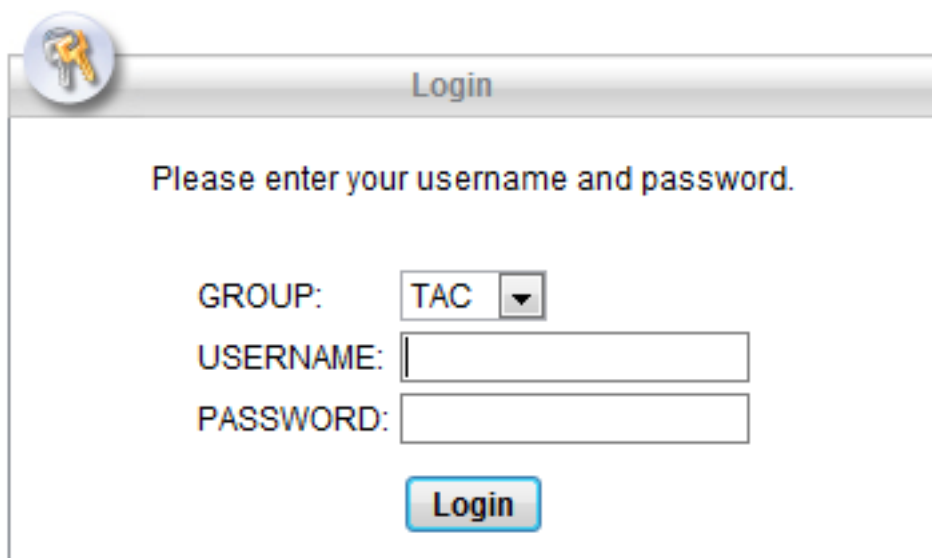
System Validated

Cisco Secure Desktop successfully validated your system.

Success. Reloading. Please wait...

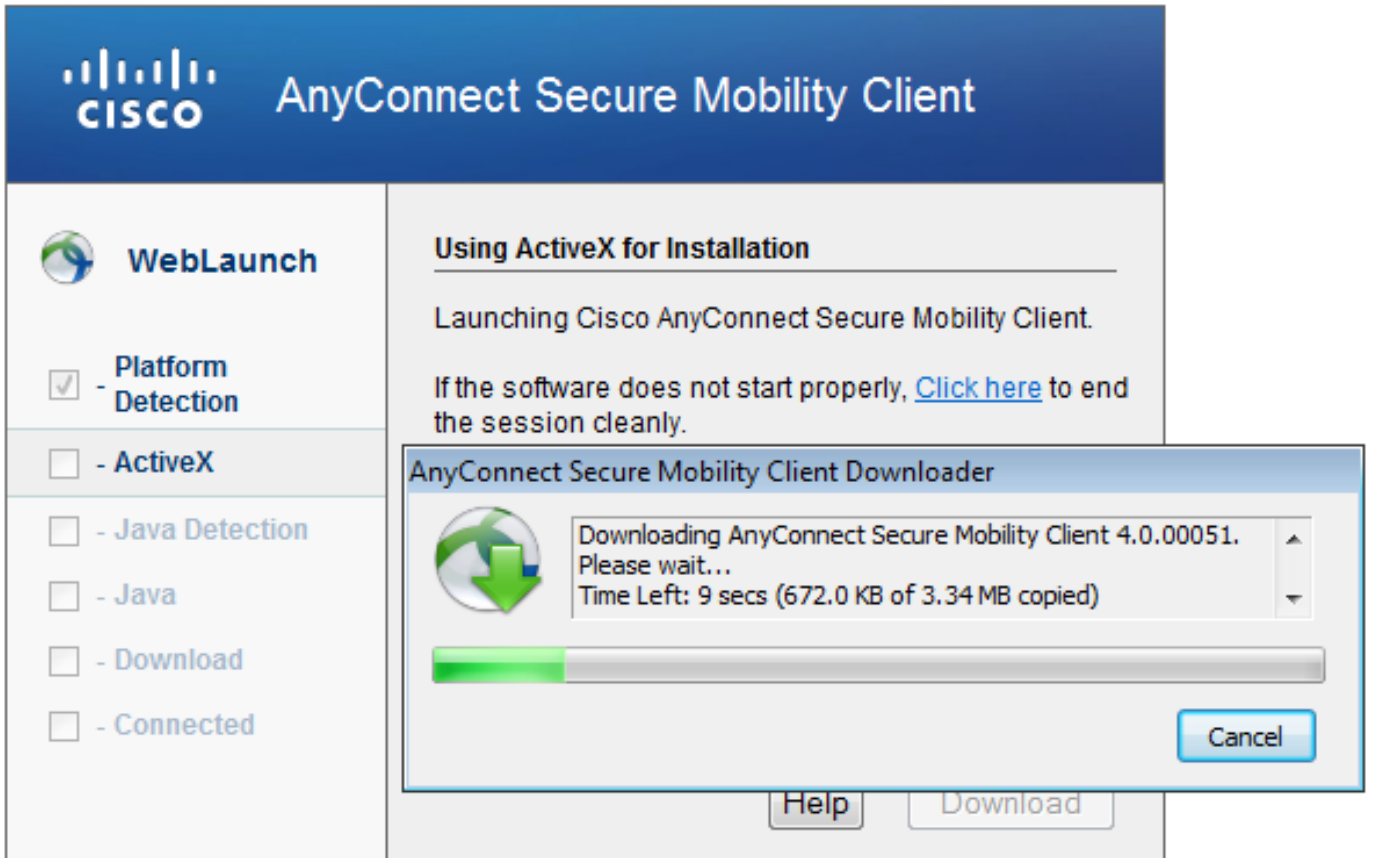
Download

L'utilisateur est ensuite redirigé vers l'authentification, comme l'illustre l'image.

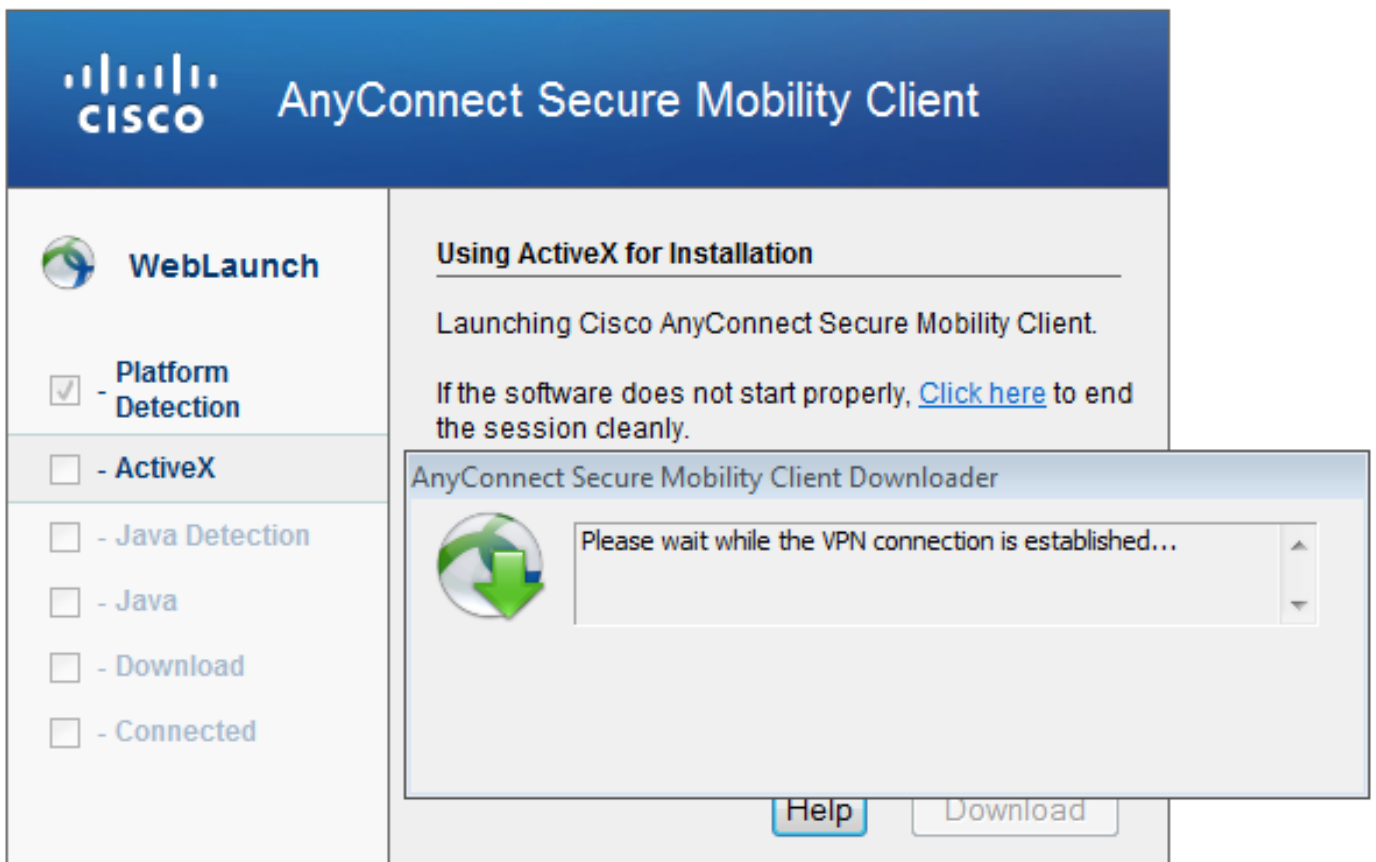


The image shows a 'Login' dialog box with a key icon in the top-left corner. The title bar reads 'Login'. The main text says 'Please enter your username and password.' Below this, there are three input fields: 'GROUP:' with a dropdown menu showing 'TAC', 'USERNAME:' with an empty text box, and 'PASSWORD:'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

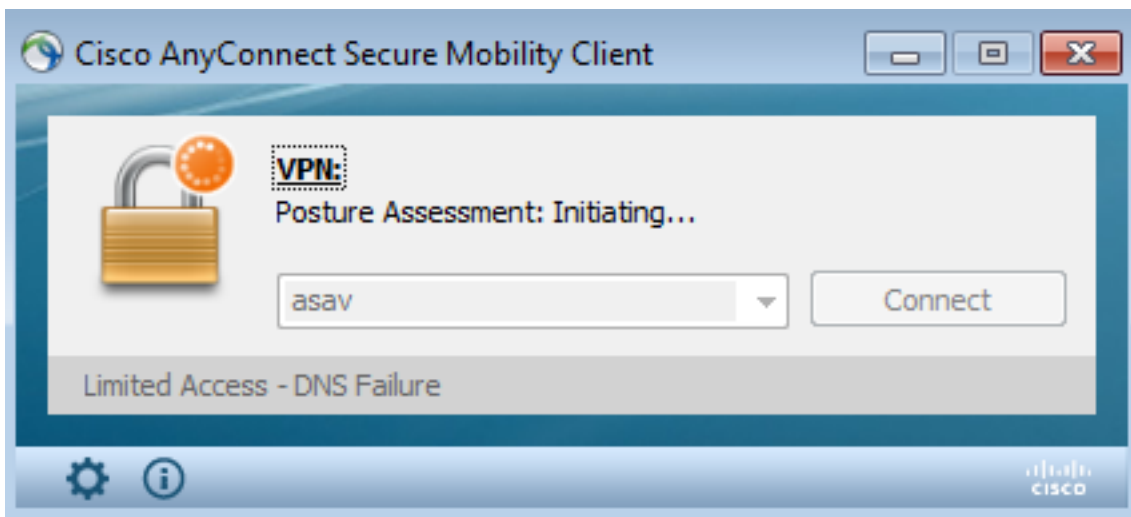
En cas de succès, AnyConnect et le profil configuré sont déployés. Une fois de plus, ActiveX ou Java peuvent être utilisés comme indiqué dans l'image.



De plus, la connexion VPN est établie comme le montre l'image.



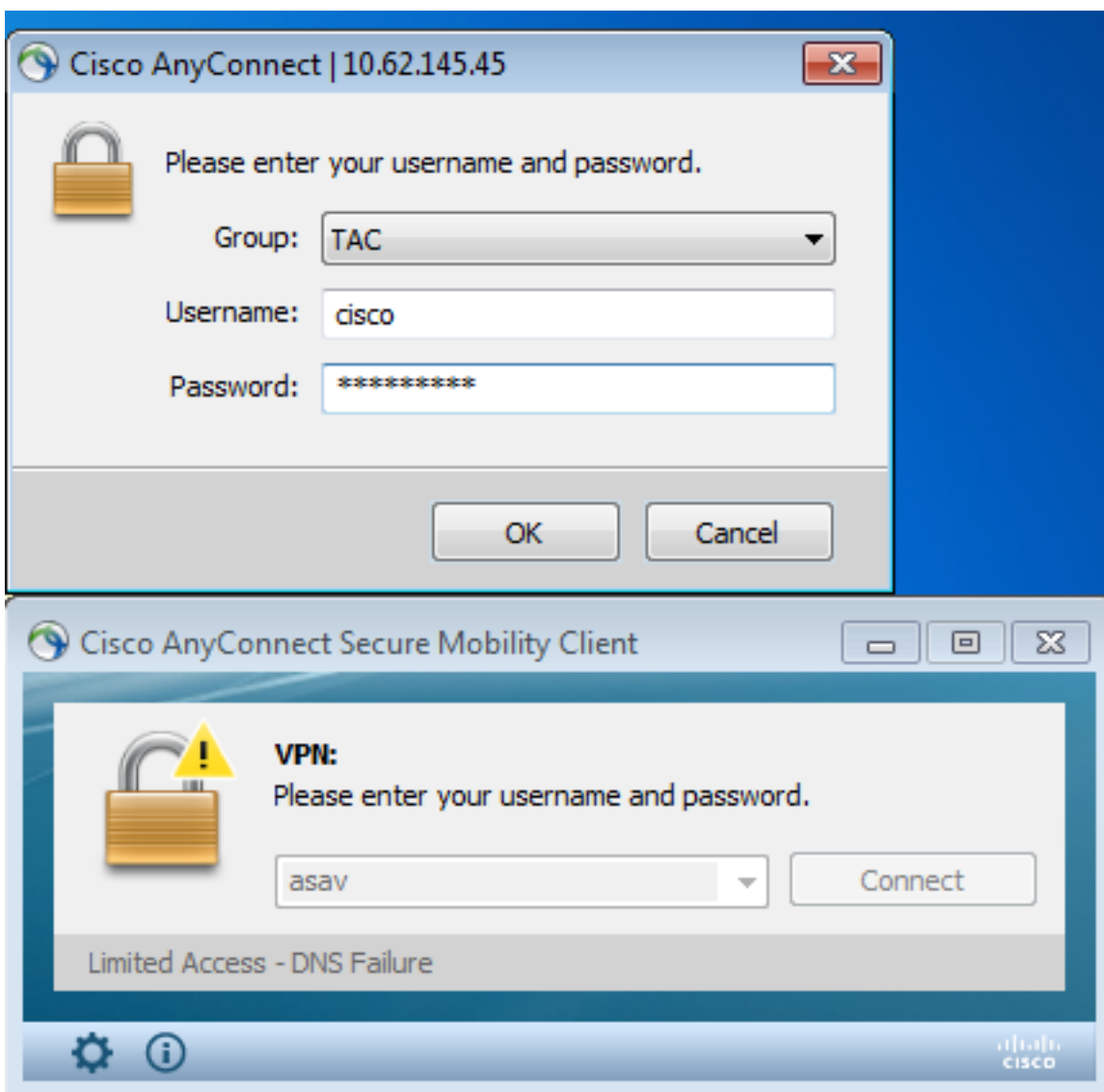
La première étape d'AnyConnect consiste à effectuer des contrôles de position (HostScan) et à envoyer les rapports à ASA comme l'illustre l'image.



Ensuite, AnyConnect authentifie et termine la session VPN.

Session VPN AnyConnect avec posture - Non conforme

Lorsque vous établissez une nouvelle session VPN avec AnyConnect, la première étape est la posture (HostScan) telle que présentée sur la capture d'écran précédente. Ensuite, l'authentification se produit et la session VPN est établie comme indiqué dans les images.



ASA signale que le rapport HostScan est reçu :

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

Effectue ensuite l'authentification des utilisateurs :

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

Et démarre l'autorisation pour cette session VPN. Lorsque vous avez « debug dap trace 255 » activé, les informations relatives à l'existence du fichier `c:\test.txt` sont retournées :

```
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"
```

En outre, informations relatives au pare-feu Microsoft Windows :

```
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"
```

Et Symantec AntiVirus (conformément aux règles d'évaluation avancée des terminaux de HostScan configurées précédemment).

En conséquence, la politique DAP est mise en correspondance :

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

Cette politique oblige à utiliser AnyConnect et applique également la liste de contrôle d'accès ACL1 qui fournit un accès réseau restreint à l'utilisateur (non conforme à la politique de l'entreprise) :

```
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
```

Les journaux présentent également des extensions ACIDEX qui peuvent être utilisées par la stratégie DAP (ou même passées dans Radius-Requests to ISE et utilisées dans les règles d'autorisation comme conditions) :

```
endpoint.anyconnect.clientversion = "4.0.00051";
endpoint.anyconnect.platform = "win";
endpoint.anyconnect.devicetype = "innotek GmbH VirtualBox";
endpoint.anyconnect.platformversion = "6.1.7600 ";
endpoint.anyconnect.deviceuniqueid =
```

```
"A1EDD2F14F17803779EB42C281C98DD892F7D34239AECDBB3FEA69D6567B2591";
endpoint.anyconnect.macaddress["0"] = "08-00-27-7f-5f-64";
endpoint.anyconnect.useragent = "AnyConnect Windows 4.0.00051";
```

Par conséquent, la session VPN est activée mais avec un accès réseau restreint :

```
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
```

L'historique d'AnyConnect présente les étapes détaillées du processus de posture :

```
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.
```

Session VPN AnyConnect avec posture - Conforme

Après avoir créé le fichier `c:\test.txt`, le flux est similaire. Une fois la nouvelle session AnyConnect lancée, les journaux indiquent l'existence du fichier :

```
%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"
```

En conséquence, une autre politique DAP est utilisée :

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

La stratégie n'impose aucune liste de contrôle d'accès comme restriction pour le trafic réseau.

Et la session est active sans liste de contrôle d'accès (accès réseau complet) :

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

En outre, Anyconnect signale que HostScan est inactif et attend la prochaine requête d'analyse :

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

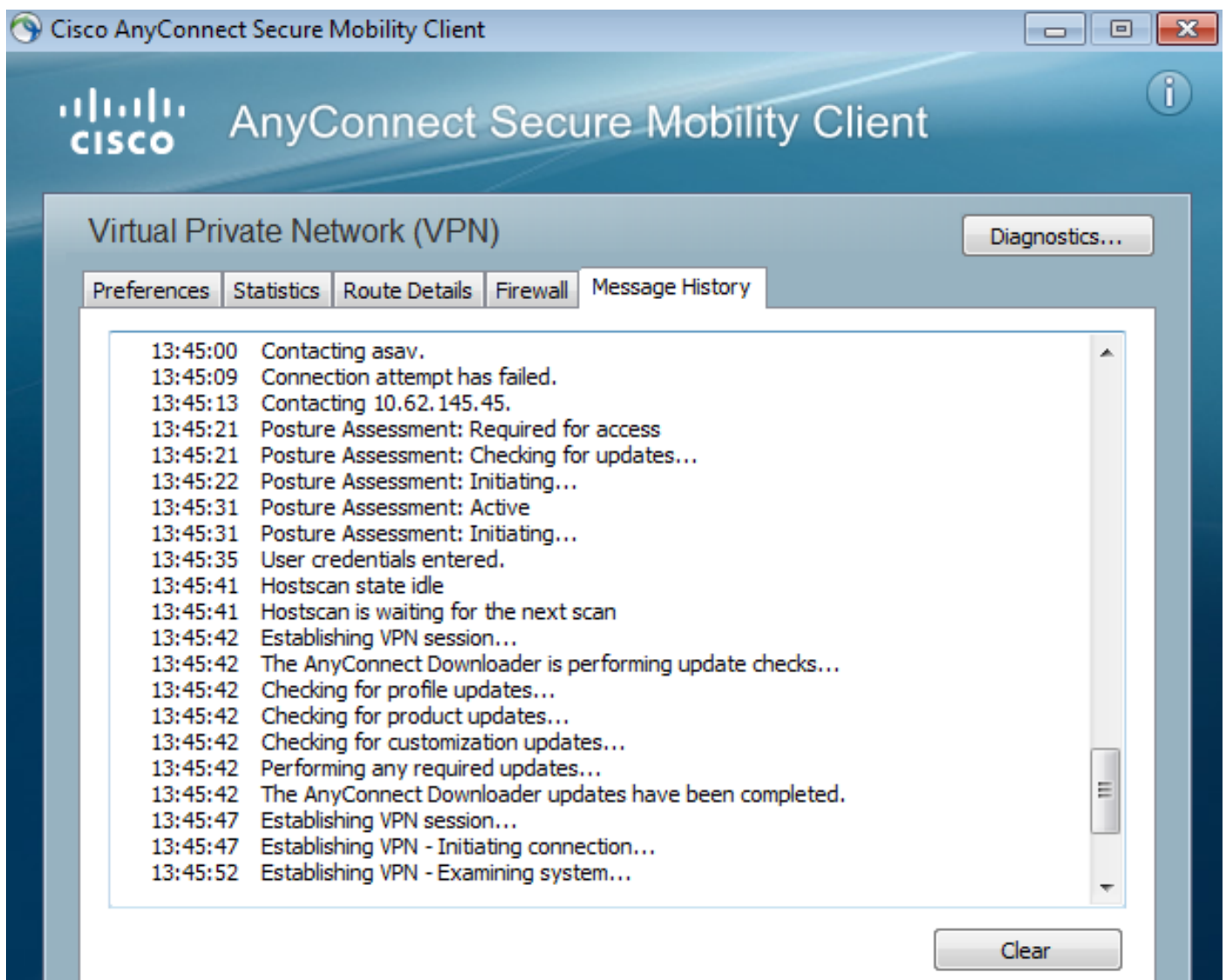
Note: Pour la réévaluation, il est conseillé d'utiliser un module de posture intégré à ISE.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

DART AnyConnect

AnyConnect fournit des diagnostics, comme l'illustre l'image.



qui collecte et enregistre tous les journaux AnyConnect dans un fichier zip sur le bureau. Ce fichier zip inclut les journaux de Cisco AnyConnect Secure Mobility Client/Anyconnect.txt.

Il fournit des informations sur ASA et demande à HostScan de collecter des données :

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.

Ensuite, plusieurs autres journaux indiquent que CSD est installé. Voici l'exemple d'un provisionnement CSD et d'une connexion AnyConnect subséquente avec posture :

CSD detected, launching CSD
Posture Assessment: Required for access
Gathering CSD version information.
Posture Assessment: Checking for updates...
CSD version file located
Downloading and launching CSD
Posture Assessment: Updating...
Downloading CSD update
CSD Stub located
Posture Assessment: Initiating...
Launching CSD
Initializing CSD
Performing CSD prelogin verification.
CSD prelogin verification finished with return code 0
Starting CSD system scan.
CSD successfully launched
Posture Assessment: Active
CSD launched, continuing until token is validated.
Posture Assessment: Initiating...

Checking CSD token for validity
Waiting for CSD token validity result
CSD token validity check completed
CSD Token is now valid
CSD Token validated successfully
Authentication succeeded
Establishing VPN session...

La communication entre ASA et AnyConnect est optimisée, les demandes ASA afin d'effectuer uniquement des contrôles spécifiques - AnyConnect télécharge des données supplémentaires afin de pouvoir effectuer cela (par exemple, la vérification spécifique de l'antivirus).

Lorsque vous ouvrez le boîtier avec le TAC, joignez les journaux Dart avec « show tech » et « debug dap trace 255 » à partir d'ASA.

Informations connexes

- [Configuration de l'analyse de l'hôte et du module Posture - Guide de l'administrateur du client de mobilité sécurisée Cisco AnyConnect](#)
- [Guide de configuration des services de positionnement sur Cisco ISE](#)
- [Guide d'administration de Cisco ISE 1.3](#)
- [Support et documentation techniques - Cisco Systems](#)