Configurez le client sécurisé de mobilité d'AnyConnect avec la Segmentation de tunnel sur une ASA

Contenu

Introduction

Ce document décrit comment configurer le Client à mobilité sécurisé Cisco AnyConnect par l'intermédiaire du Cisco Adaptive Security Device Manager (ASDM) sur une appliance de sécurité adaptable Cisco (ASA) cette version de logiciel de passages 9.3(2).

Conditions préalables

Conditions requises

Le module de déploiement de Web de Client à mobilité sécurisé Cisco AnyConnect devrait être téléchargé à l'appareil de bureau local duquel l'accès ASDM à l'ASA est présent. Afin de

télécharger le module de client, référez-vous à la page Web de Client à mobilité sécurisé Cisco AnyConnect. Les modules de déploiement de Web pour différents systèmes d'exploitation (systèmes d'exploitation) peuvent être téléchargés à l'ASA en même temps.

Ce sont les noms de fichier de déploiement de Web pour les divers systèmes d'exploitation :

- *AnyConnect-win-<version>-k9.pkg du* Â d'âÂ de **systèmes d'exploitation de Microsoft Windows**
- *AnyConnect-macosx-i386-<version>-k9.pkg du* Â d'âÂ de **systèmes d'exploitation de Macintosh (MAC)**
- *AnyConnect-linux-<version>-k9.pkg du* Â d'âÂ de **systèmes d'exploitation linux**

Composants utilisés

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

- Version 9.3(2) ASA
- Version 7.3(1)101 ASDM
- Version 3.1 d'AnyConnect

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Ce document fournit les détails pas à pas au sujet de la façon utiliser l'assistant de configuration de Cisco AnyConnect par l'intermédiaire de l'ASDM afin de configurer la Segmentation de tunnel de client et d'enable d'AnyConnect.

La Segmentation de tunnel est utilisée dans les scénarios où seulement le trafic spécifique doit être percé un tunnel, opposés aux scénarios où toute les circulation produite par machine de client à travers le VPN une fois connectée. L'utilisation de l'assistant de configuration d'AnyConnect par résultat par défaut dans une tunnel-*toute* configuration sur l'ASA. Le perçage d'un tunnel fendu doit être configuré séparément, qui est expliqué dans davantage de détail dans la section de tunnel partagé de ce document.

Dans cet exemple de configuration, l'intention est d'envoyer le trafic pour le sous-réseau 10.10.10.0/24, qui est le sous-réseau LAN derrière l'ASA, au-dessus du tunnel VPN et tout autre trafic de la machine cliente est expédié par l'intermédiaire de son propre circuit d'Internet.

Données de licence d'AnyConnect

Voici quelques liens aux informations utiles au sujet des permis de Client à mobilité sécurisé Cisco AnyConnect :

- Référez-vous aux fonctionnalités client, aux permis, et à l'OSs sécurisés de mobilité d'AnyConnect, document de version 3.1 afin de déterminer les permis qui sont exigés pour le client sécurisé de mobilité d'AnyConnect et les caractéristiques relatives.
- Référez-vous au guide de commande de Cisco AnyConnect pour les informations au sujet de l'apex d'AnyConnect et plus des permis.
- Référez-vous au quel permis ASA est nécessaire pour le téléphone IP et les connexions VPN mobiles ? document pour des informations sur les conditions requises de licence supplémentaire pour le téléphone IP et les connexions mobiles.

Configurez

Cette section décrit comment configurer le Client à mobilité sécurisé Cisco AnyConnect sur l'ASA.

> **Note**: Utilisez le Command Lookup Tool (clients enregistrés seulement) afin d'obtenir plus d'informations sur les commandes qui sont utilisées dans cette section.

Diagramme du réseau

C'est la topologie qui est utilisée pour les exemples dans ce document :

Assistant de configuration ASDM AnyConnect

L'assistant de configuration d'AnyConnect peut être utilisé afin de configurer le client sécurisé de mobilité d'AnyConnect. Assurez-vous qu'un module de client d'AnyConnect a été téléchargé à l'éclair/au disque du Pare-feu ASA avant que vous poursuiviez.

Terminez-vous ces étapes afin de configurer le client sécurisé de mobilité d'AnyConnect par l'intermédiaire de l'assistant de configuration :

1. Connectez-vous dans l'ASDM, lancez l'**assistant de configuration**, et cliquez sur Next :

2. Écrivez le *nom de profil de connexion*, choisissez l'interface sur laquelle le VPN sera terminé de l'*interface d'accès VPN* relâchent vers le bas le menu, et cliquent sur Next :

3. Cochez la case **SSL** afin d'activer Secure Sockets Layer (SSL). *Le certificat de périphérique*

peut être un certificat délivré par Autorité de certification (CA) de confiance de tiers (tel que Verisign, ou confiez), ou un certificat auto-signé. Si le certificat est déjà installé sur l'ASA, alors il peut être choisi par l'intermédiaire du menu de baisse vers le bas.**Note**: Ce certificat est le certificat de côté serveur qui sera fourni. S'il n'y a aucun Certificats actuellement installé sur l'ASA, et un certificat auto-signé doit être généré, alors cliquez sur **gèrent**.Afin d'installer un tiers certificat, terminez-vous les étapes qui sont décrites dans l'ASA 8.x installent manuellement des Certificats de constructeur de tiers pour l'usage avec le document Cisco d'exemple de configuration de webvpn.

4. Cliquez sur Add :

5. Introduisez un nom approprié dans la zone d'*identification de point de confiance*, et cliquez sur l'**ajouter une nouvelle** case d'option de **certificat d'identité**. S'il n'y a aucune paire de clés de Rivest-Shamir-Addleman (RSA) actuelle sur le périphérique, cliquez sur New afin de générer un :

6. Cliquez sur la case d'option de **nom de paires de clé par défaut d'utilisation**, ou cliquez sur la **nouvelle** case d'option de **nom de paire de clés d'entrer** et écrivez un nouveau nom. Sélectionnez la taille pour les clés, et puis cliquez sur **se produisent maintenant** :

7. Après que la paire de clés RSA soit générée, choisissez la clé et cochez la case de **certificat auto-signée Generate**. Écrivez le nom de domaine soumis désiré (DN) dans le gisement de *DN de sujet de certificat*, et puis cliquez sur Add le **certificat** :

8. Une fois que l'inscription est complète, cliquez sur OK, **CORRECT**, et puis **ensuite** :

9. Cliquez sur Add afin d'ajouter l'image de client d'AnyConnect (le fichier *.package*) du PC ou de l'éclair. Cliquez sur **Browse Flash** afin d'ajouter l'image du lecteur flash, ou cliquez sur Upload afin d'ajouter l'image de l'ordinateur hôte directement :

10. Une fois que l'image est ajoutée, cliquez sur Next :

11. L'authentification de l'utilisateur peut être terminée par l'intermédiaire des groupes de serveurs d'Authentification, autorisation et comptabilité (AAA). Si les utilisateurs sont déjà configurés, alors choisissez les **GENS DU PAYS** et cliquez sur Next. **Note**: Dans cet exemple, l'**authentification locale** est configurée, ainsi il signifie que la base de données locale des utilisateurs sur l'ASA sera utilisée pour l'authentification.

12. Le pool d'adresses pour le client vpn doit être configuré. Si on est déjà configuré, alors sélectionnez-le du menu de baisse vers le bas. Sinon, cliquez sur New afin de configurer un neuf. Une fois terminez-vous, cliquez sur Next :

13. Entrez les serveurs de Système de noms de domaine (DNS) et les dn dans les *DN* et le *nom de domaine* met en place convenablement, et clique sur Next alors :

14. Dans ce scénario, l'objectif est de limiter l'accès au-dessus du VPN au réseau **10.10.10.0/24** qui est configuré comme sous-réseau *intérieur* (ou RÉSEAU LOCAL) derrière l'ASA. Le trafic entre le client et le sous-réseau intérieur doit être exempt de n'importe quelle traduction d'adresses de réseau dynamique (NAT).

    Cochez le **trafic VPN exempt de la** case de **traduction d'adresses réseau** et configurez les interfaces de LAN et WAN qui seront utilisées pour l'exemption :

15. Choisissez les réseaux locaux qui doivent être exempts :

16. Cliquez sur Next, **ensuite**, et puis **terminez**.

La configuration de client d'AnyConnect est maintenant complète. Cependant, quand vous configurez AnyConnect par l'intermédiaire de l'assistant de configuration, il configure la stratégie de *tunnel partagé* comme **Tunnelall** par défaut. Afin de percer un tunnel le trafic spécifique seulement, la *Segmentation de tunnel* doit être mise en application.

> **Note**: Si fractionnement-perçant un tunnel n'est pas configuré, la stratégie de tunnel partagé sera héritée de la stratégie de groupe par défaut (DfltGrpPolicy), qui est par l'ensemble par défaut à **Tunnelall.** Ceci signifie qu'une fois que le client est connecté au-dessus du VPN, tout les trafic (pour inclure le trafic au Web) est envoyé au-dessus du tunnel.

Seulement le trafic qui est destiné à l'adresse IP BLÊME ASA (ou *extérieur*) sautera le Tunnellisation sur la machine cliente. Ceci peut être vu dans la sortie de la commande print

d'**artère** sur des ordinateurs de Microsoft Windows.

Configuration de tunnel partagé

Le perçage d'un tunnel fendu est une caractéristique que vous pouvez employer afin de définir le trafic pour les sous-réseaux ou les hôtes qui doivent être chiffrés. Ceci implique la configuration d'une liste de contrôle d'accès (ACL) qui sera associée avec cette configuration. Le trafic pour les sous-réseaux ou les hôtes qui est défini sur cet ACL sera chiffré au-dessus du tunnel de l'extrémité client, et des artères pour ces sous-réseaux sont installés sur la table de routage PC.

Terminez-vous ces étapes afin de se déplacer de la Tunnel-*toute* configuration à la configuration de *tunnel partagé* :

1. Naviguez vers la **configuration > l'Accès à distance VPN > stratégies de groupe** :

2. Cliquez sur Edit, et utilisez l'arborescence afin de naviguer vers **avancé > Segmentation de tunnel**. Décochez la case d'**héritage** dans la section de *stratégie*, et sélectionnez la **liste des réseaux de tunnel ci-dessous du** menu de baisse vers le bas :

3. Décochez la case d'**héritage** dans la section de *liste des réseaux*, et le clic **parviennent** afin de sélectionner l'ACL qui spécifie les réseaux de RÉSEAU LOCAL auxquels les besoins de client accèdent à :

4. **L'ACL standard de** clic, **ajoutent**, **ajoutent le nom d'ACL**, et puis d'**ACL** :

5. Cliquez sur Add **ACE** afin d'ajouter la règle :

6. Cliquez sur **OK**.

7. Cliquez sur **Apply**.

Une fois que connectées, les artères pour les sous-réseaux ou des hôtes sur l'ACL fendu sont ajoutés à la table de routage de la machine cliente. Sur des ordinateurs de Microsoft Windows, ceci peut être visualisé dans la sortie de la commande print d'**artère**. Le prochain saut pour ces artères sera une adresse IP du sous-réseau de client ip pool (habituellement la première adresse IP du sous-réseau) :

```
C:\Users\admin>route print
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination Netmask Gateway Interface Metric
0.0.0.0 0.0.0.0 10.106.44.1 10.106.44.243 261
10.10.10.0      255.255.255.0    10.10.11.2  10.10.11.1     2

!! This is the split tunnel route.

10.106.44.0 255.255.255.0 On-link 10.106.44.243 261
172.16.21.1    255.255.255.255     On-link    10.106.44.243  6

!! This is the route for the ASA Public IP Address.
```

Sur des ordinateurs de MAC OS, entrez dans le **netstat -** commande **r** afin de visualiser la table de routage PC :

```
$ netstat -r
Routing tables
Internet:
Destination Gateway Flags Refs Use Netif Expire
default hsrp-64-103-236-1. UGSc 34 0 en1
10.10.10/24        10.10.11.2         UGSc    0   44   utun1

!! This is the split tunnel route.

10.10.11.2/32 localhost UGSc 1 0 lo0
172.16.21.1/32     hsrp-64-103-236-1. UGSc    1   0    en1

!! This is the route for the ASA Public IP Address.
```

Téléchargez et installez le client d'AnyConnect

Il y a deux méthodes que vous pouvez employer afin de déployer le Client à mobilité sécurisé Cisco AnyConnect sur l'ordinateur d'utilisateur :

- Déploiement de Web
- Déploiement autonome

Chacun des deux méthodes sont expliquées plus en détail dans les sections qui suivent.

Déploiement de Web

Afin d'utiliser la méthode de déploiement de Web, écrivez l'URL de **https:// <ASA FQDN>or<ASA IP>** dans un navigateur sur la machine cliente, qui vous amène à la page du portail de *webvpn*.

> **Note**: Si l'Internet Explorer (IE) est utilisé, l'installation est terminée en grande partie par l'intermédiaire d'ActiveX, à moins que vous soyez forcé pour utiliser Javas. Toutes autres Javas d'utilisation de navigateurs.

Une fois connecté dans la page, l'installation devrait commencer sur la machine cliente, et le client devrait se connecter à l'ASA après que l'installation soit complète.

Note: Vous pourriez être incité pour que l'autorisation exécute ActiveX ou Javas. Ceci doit être permis afin de procéder à l'installation.

Déploiement autonome

Terminez-vous ces étapes afin d'utiliser la méthode autonome de déploiement :

1. Téléchargez l'image de client d'AnyConnect du site Web Cisco. Afin de choisir l'image correcte pour le téléchargement, référez-vous à la page Web de Client à mobilité sécurisé Cisco AnyConnect. Un lien de téléchargement est fourni sur cette page. Naviguez vers la page de téléchargement et sélectionnez la version appropriée. Exécutez un **plein module d'installation de** rechercher **- Fenêtre/installateur autonome (OIN)**.**Note**: Une image d'installateur OIN est alors téléchargée (comme *anyconnect-win-3.1.06073-pre-deploy-k9.iso*).
2. Employez *WinRar* ou *7-Zip* afin d'extraire le contenu du module OIN :

3. Une fois que le contenu est extrait, exécutez le **fichier Setup.exe** et choisissez les modules qui doivent être installés avec le Client à mobilité sécurisé Cisco AnyConnect.

   Conseil : Afin de configurer les configurations supplémentaires pour le VPN, référez-vous la section de configuration de connexions AnyConnect VPN Client du *guide de configuration de gamme de Cisco ASA 5500 utilisant le CLI, les 8.4 et les 8.6*.

Configuration CLI

Cette section fournit la configuration CLI pour le Client à mobilité sécurisé Cisco AnyConnect pour la référence.

```
ASA Version 9.3(2)
!
hostname PeerASA-29
enable password 8Ry2YjIyt7RRXU24 encrypted
ip local pool SSL-Pool 10.10.11.1-10.10.11.20 mask 255.255.255.0
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.21.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.10.10.1 255.255.255.0
!
boot system disk0:/asa932-smp-k8.bin
ftp mode passive
object network NETWORK_OBJ_10.10.10.0_24
subnet 10.10.10.0 255.255.255.0
```

```
object network NETWORK_OBJ_10.10.11.0_27
subnet 10.10.11.0 255.255.255.224

access-list all extended permit ip any any

!***********Split ACL configuration***********

access-list Split-ACL standard permit 10.10.10.0 255.255.255.0
no pager
logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
mtu dmz 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-721.bin
no asdm history enable
arp timeout 14400
no arp permit-nonconnected

!************** NAT exemption Configuration *****************
!This will exempt traffic from Local LAN(s) to the
!Remote LAN(s) from getting NATted on any dynamic NAT rule.

nat (inside,outside) source static NETWORK_OBJ_10.10.10.0_24 NETWORK_OBJ_10.10.10.0_24
destination static NETWORK_OBJ_10.10.11.0_27 NETWORK_OBJ_10.10.11.0_27 no-proxy-arp
route-lookup
access-group all in interface outside
route outside 0.0.0.0 0.0.0.0 172.16.21.2 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
user-identity default-domain LOCAL
aaa authentication ssh console LOCAL
http server enable
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact

!********** Trustpoint for Selfsigned certificate***********
!Genarate the key pair and then configure the trustpoint
!Enroll the trustpoint genarate the self-signed certificate

crypto ca trustpoint SelfsignedCert
enrollment self
subject-name CN=anyconnect.cisco.com
keypair sslcert
crl configure
crypto ca trustpool policy
crypto ca certificate chain SelfsignedCert
certificate 4748e654
308202f0 308201d8 a0030201 02020447 48e65430 0d06092a 864886f7 0d010105
0500303a 311d301b 06035504 03131461 6e79636f 6e6e6563 742e6369 73636f2e
636f6d31 19301706 092a8648 86f70d01 0902160a 50656572 4153412d 3239301e
170d3135 30343032 32313534 30375a17 0d323530 33333032 31353430 375a303a
311d301b 06035504 03131461 6e79636f 6e6e6563 742e6369 73636f2e 636f6d31
19301706 092a8648 86f70d01 0902160a 50656572 4153412d 32393082 0122300d
```

```
06092a86 4886f70d 01010105 00038201 0f003082 010a0282 010100f6 a125d0d0
55a975ec a1f2133f 0a2c3960 0da670f8 bcb6dad7 efefe50a 482db3a9 7c6db7c4
ed327ec5 286594bc 29291d8f 15140bad d33bc492 02f5301e f615e7cd a72b60e0
7877042b b6980dc7 ccaa39c8 c34164d9 e2ddeea1 3c0b5bad 5a57ec4b d77ddb3c
75930fd9 888f92b8 9f424fd7 277e8f9e 15422b40 071ca02a 2a73cf23 28d14c93
5a084cf0 403267a6 23c18fa4 fca9463f aa76057a b07e4b19 c534c0bb 096626a7
53d17d9f 4c28a3fd 609891f7 3550c991 61ef0de8 67b6c7eb 97c3bff7 c9f9de34
03a5e788 94678f4d 7f273516 c471285f 4e23422e 6061f1e7 186bbf9c cf51aa36
19f99ab7 c2bedb68 6d182b82 7ecf39d5 1314c87b ffddff68 8231d302 03010001
300d0609 2a864886 f70d0101 05050003 82010100 d598c1c7 1e4d8a71 6cb43296
c09ea8da 314900e7 5fa36947 c0bc1778 d132a360 0f635e71 400e592d b27e29b1
64dfb267 51e8af22 0a6a8378 5ee6a734 b74e686c 6d983dde 54677465 7bf8fe41
daf46e34 bd9fd20a bacf86e1 3fac8165 fc94fe00 4c2eb983 1fc4ae60 55ea3928
f2a674e1 8b5d651f 760b7e8b f853822c 7b875f91 50113dfd f68933a2 c52fe8d9
4f9d9bda 7ae2f750 313c6b76 f8d00bf5 1f74cc65 7c079a2c 8cce91b0 a8cdd833
900a72a4 22c2b70d 111e1d92 62f90476 6611b88d ff58de5b fdaa6a80 6fe9f206
3fe4b836 6bd213d4 a6356a6c 2b020191 bf4c8e3d dd7bdd8b 8cc35f0b 9ad8852e
b2371ee4 23b16359 ba1a5541 ed719680 ee49abe8
quit
telnet timeout 5
ssh timeout 5
ssh key-exchange group dh-group1-sha1
console timeout 0
management-access inside
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
ssl server-version tlsv1-only
ssl encryption des-sha1 3des-sha1 aes128-sha1 aes256-sha1

!******** Bind the certificate to the outside interface********
ssl trust-point SelfsignedCert outside

!********Configure the Anyconnect Image and enable Anyconnect***
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-3.1.06073-k9.pkg 1
anyconnect enable
tunnel-group-list enable

!*******Group Policy configuration*********
!Tunnel protocol, Spit tunnel policy, Split
!ACL, etc. can be configured.

group-policy GroupPolicy_SSLClient internal
group-policy GroupPolicy_SSLClient attributes
wins-server none
dns-server value 10.10.10.23
vpn-tunnel-protocol ikev2 ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value Split-ACL
default-domain value Cisco.com

username User1 password PfeNk7qp9b4LbLV5 encrypted
username cisco password 3USUcOPFUiMCO4Jk encrypted privilege 15

!*******Tunnel-Group (Connection Profile) Configuraiton*****
tunnel-group SSLClient type remote-access
tunnel-group SSLClient general-attributes
address-pool SSL-Pool
default-group-policy GroupPolicy_SSLClient
tunnel-group SSLClient webvpn-attributes
group-alias SSLClient enable
!
```

```
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum client auto
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:8d492b10911d1a8fbcc93aa4405930a0
: end
```

Vérifiez

Terminez-vous ces étapes afin de vérifier la connexion client et les divers paramètres qui sont associées à cette connexion :

1. Naviguez vers la **surveillance > VPN** sur l'ASDM :

2. Vous pouvez utiliser le **filtre par l'**option afin de filtrer le type de VPN. **Client** choisi d'**AnyConnect de** baisse du menu vers le bas et toutes les sessions de client d'AnyConnect.**Conseil** : Les sessions peuvent être encore filtrées avec les autres critères, tels que le *nom d'utilisateur* et l'*adresse IP*.

3. Double-cliquer une session afin d'obtenir d'autres détails au sujet de cette session particulière :

4. Sélectionnez la commande d'**anyconnect de VPN-sessiondb d'exposition** dans le CLI afin d'obtenir les détails de session :

```
# show vpn-sessiondb anyconnect
Session Type : AnyConnect
Username : cisco Index : 14
Assigned IP : 10.10.11.1   Public IP : 172.16.21.1
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)3DES DTLS-Tunnel: (1)DES
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 11472 Bytes Rx : 39712
Group Policy : GroupPolicy_SSLClient   Tunnel Group : SSLClient
Login Time : 16:58:56 UTC Mon Apr 6 2015
Duration : 0h:49m:54s
Inactivity : 0h:00m:00s
```

```
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none
```

5. Vous pouvez employer les autres options de filtre afin d'affiner les résultats :

```
# show vpn-sessiondb detail anyconnect filter name cisco

Session Type: AnyConnect Detailed

Username : cisco Index : 19
Assigned IP : 10.10.11.1    Public IP : 10.106.44.243
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)3DES DTLS-Tunnel: (1)DES
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 11036 Bytes Rx : 4977
Pkts Tx : 8 Pkts Rx : 60
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : GroupPolicy_SSLClient  Tunnel Group : SSLClient
Login Time   : 20:33:34 UTC Mon Apr 6 2015
Duration : 0h:01m:19s

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 19.1
Public IP : 10.106.44.243
Encryption : none Hashing : none
TCP Src Port : 58311 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : AnyConnect
Client Ver   : Cisco AnyConnect VPN Agent for Windows 3.1.06073
Bytes Tx : 5518 Bytes Rx : 772
Pkts Tx : 4 Pkts Rx : 1
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 19.2
Assigned IP : 10.10.11.1 Public IP : 10.106.44.243
Encryption : 3DES Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 58315
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 3.1.06073
Bytes Tx : 5518 Bytes Rx : 190
Pkts Tx : 4 Pkts Rx : 2
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 19.3
Assigned IP : 10.10.11.1 Public IP : 10.106.44.243
Encryption : DES Hashing : SHA1
Encapsulation: DTLSv1.0 UDP Src Port : 58269
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 3.1.06073
Bytes Tx : 0 Bytes Rx : 4150
Pkts Tx : 0 Pkts Rx : 59
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

Dépannez

Vous pouvez utiliser les diagnostics d'AnyConnect et l'outil de génération de rapports (DART) afin de collecter les données qui sont utiles pour dépanner l'installation et les problèmes de connexion d'AnyConnect. L'assistant de DART est utilisé sur l'ordinateur qui exécute AnyConnect. Le DART compile les logs, l'état, et les informations de diagnostic pour l'analyse du centre d'assistance technique Cisco (TAC) et n'exige pas des privilèges d'administrateur de s'exécuter sur la machine cliente.

Installez le DART

Terminez-vous ces étapes afin d'installer le DART :

1. Téléchargez l'image de client d'AnyConnect du site Web Cisco. Afin de choisir l'image correcte pour le téléchargement, référez-vous à la page Web de Client à mobilité sécurisé Cisco AnyConnect. Un lien de téléchargement est fourni sur cette page. Naviguez vers la page de téléchargement et sélectionnez la version appropriée. Exécutez un **plein module d'installation de** rechercher **- Fenêtre/installateur autonome (OIN)**.**Note**: Une image d'installateur OIN est alors téléchargée (comme *anyconnect-win-3.1.06073-pre-deploy-k9.iso*).
2. Employez *WinRar* ou *7-Zip* afin d'extraire le contenu du module OIN :

3. Parcourez au répertoire auquel le contenu a été extrait.

4. Exécutez le **fichier Setup.exe** et sélectionnez seulement AnyconnectDiagnostic **et outil de génération de rapports :**

Exécutez le DART

Voici quelques informations importantes à considérer avant que vous exécutiez le DART :

- La question doit être recréée au moins une fois avant que vous exécutiez le DART.

- La date et l'heure sur l'ordinateur d'utilisateur doivent être notées quand la question est recréée.

Exécutez le *menu de* DART dès le début sur la machine cliente :

Ou *transférez* ou le mode *fait sur commande* peut être sélectionné. Cisco recommande que vous exécutiez le DART en mode par défaut de sorte que toutes les informations puissent être capturées dans un tir simple.

Une fois que terminé, l'outil enregistre le fichier du paquet *.zip de* DART à l'appareil de bureau de client. Le paquet peut alors être envoyé au TAC (après que vous ouvrez une valise TAC) pour l'analyse approfondie.

Informations connexes

- Guide de l'administrateur de Client à mobilité sécurisé Cisco AnyConnect, du Â d'âÂ de version 3.0 gérant, surveillant, et dépannage des sessions d'AnyConnect
- Guide de dépannage d'AnyConnect VPN Client - Problèmes courants
- Javas 7 questions avec AnyConnect, CSD/Hostscan, et webvpn - guide de dépannage
- Support et documentation techniques - Cisco Systems