Configurar o cliente seguro da mobilidade de AnyConnect com Split Tunneling em um ASA

Índice

Introdução

Este documento descreve como configurar o Cliente de mobilidade Cisco AnyConnect Secure através do Cisco Adaptive Security Device Manager (ASDM) em uma ferramenta de segurança adaptável de Cisco (ASA) essa versão de software das corridas 9.3(2).

Pré-requisitos

Requisitos

O pacote do desenvolvimento da Web do Cliente de mobilidade Cisco AnyConnect Secure deve ser transferido ao desktop local de que o acesso ASDM ao ASA esta presente. A fim transferir o pacote do cliente, refira o página da web do Cliente de mobilidade Cisco AnyConnect Secure. Os pacotes do desenvolvimento da Web para os vários sistemas operacionais (OS) podem ser

transferidos arquivos pela rede ao ASA ao mesmo tempo.

Estes são os nomes de arquivo do desenvolvimento da Web para os vários OS:

- *AnyConnect-win-<version>-k9.pkg do* Â do âÂ de **Microsoft Windows OS**
- *AnyConnect-macosx-i386-<version>-k9.pkg do* Â do âÂ de **Macintosh (MAC) OS**
- *AnyConnect-linux-<version>-k9.pkg do* Â do âÂ de **Linux OS**

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão ASA 9.3(2)
- Versão 7.3(1)101 ASDM
- Versão 3.1 de AnyConnect

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Este documento fornece detalhes passo a passo sobre como usar o wizard de configuração de Cisco AnyConnect através do ASDM a fim configurar o cliente de AnyConnect e permitir o Split Tunneling.

O split-tunneling é usado nas encenações onde somente o tráfego específico deve ser escavado um túnel, opostas às encenações onde todo o cliente máquina-gerou fluxos de tráfego através do VPN quando conectado. O uso do wizard de configuração de AnyConnect conduzirá à revelia a túnel-*toda* configuração no ASA. A escavação de um túnel rachada deve ser configurada separadamente, que é explicada em um detalhe mais adicional na seção do túnel em divisão deste documento.

Neste exemplo de configuração, a intenção é enviar o tráfego para a sub-rede 10.10.10.0/24, que é a sub-rede de LAN atrás do ASA, sobre o túnel VPN e todo tráfego restante da máquina cliente é enviado através de seu próprio circuito do Internet.

Informação de licença de AnyConnect

Estão aqui alguns links à informação util sobre as licenças do Cliente de mobilidade Cisco AnyConnect Secure:

- Refira os recursos de cliente, as licenças, e os OS seguros da mobilidade de AnyConnect, documento da liberação 3.1 a fim determinar as licenças que são exigidas para o cliente

seguro da mobilidade de AnyConnect e as características relacionadas.

- Refira o guia pedindo de Cisco AnyConnect para obter informações sobre do vértice de AnyConnect e mais licenças.
- Refira que licença ASA é precisada para o telefone IP e conexões de VPN móveis? documento para obter informações sobre das exigências adicionais da licença para o telefone IP e conexões móveis.

Configurar

Esta seção descreve como configurar o Cliente de mobilidade Cisco AnyConnect Secure no ASA.

> **Note**: Use a ferramenta de consulta de comandos (clientes registrados somente) a fim obter mais informação nos comandos que são usados nesta seção.

Diagrama de Rede

Esta é a topologia que é usada para os exemplos neste documento:

Wizard de configuração ASDM AnyConnect

O wizard de configuração de AnyConnect pode ser usado a fim configurar o cliente seguro da mobilidade de AnyConnect. Assegure-se de que um pacote do cliente de AnyConnect esteja transferido arquivos pela rede ao flash/disco do Firewall ASA antes que você continue.

Termine estas etapas a fim configurar o cliente seguro da mobilidade de AnyConnect através do wizard de configuração:

1. O log no ASDM, lança o **wizard de configuração**, e clica-o **em seguida**:

2. Dê entrada com o *nome do perfil de conexão*, escolha a relação em que o VPN será terminado da *interface de acesso VPN* deixa cair para baixo o menu, e o clica **em seguida**:

3. Verifique a caixa de verificação **SSL** a fim permitir o secure sockets layer (SSL). *O certificado do dispositivo* pode ser um certificado emitido Certificate Authority (CA) confiado da terceira parte (tal como Verisign, ou confie), ou um certificado auto-assinado. Se o certificado é instalado já no ASA, a seguir pode ser escolhido através do menu de gota para baixo.**Note**: Este certificado é o certificado do lado de servidor que será fornecido. Se não há nenhum Certificados instalado atualmente no ASA, e um certificado auto-assinado deve ser

gerado, a seguir clique **controlam**.A fim instalar um certificado da terceira, termine as etapas que são descritas no ASA 8.x instalam manualmente Certificados do vendedor da 3ª parte para o uso com documento Cisco do exemplo de configuração WebVPN.

4. O clique **adiciona**:

5. Datilografe um nome apropriado no *campo de nome do ponto confiável*, e clique **adicionar um** botão de rádio **novo do certificado de identidade**. Se não há nenhum par de chaves de Rivest-Shamir-Addleman (RSA) atual no dispositivo, clique **novo** a fim gerar um:

6. Clique o botão de rádio do **nome dos pares de chave padrão do uso**, ou clique o botão de rádio **novo do nome do par de chaves da entrada** e dê entrada com um novo nome. Selecione o tamanho para as chaves, e clique-o então **gerenciem agora**:

7. Depois que o par de chaves RSA é gerado, escolha a chave e verifique a caixa de verificação do **certificado auto-assinado da geração**. Incorpore o Domain Name sujeito desejado (DN) no campo do *assunto DN do certificado*, e clique-o então **adicionam o certificado**:

8. Uma vez que o registro está completo, **APROVAÇÃO do** clique, **APROVAÇÃO**, e então **em seguida**:

9. O clique **adiciona** a fim adicionar a imagem do cliente de AnyConnect (o arquivo *.package*) do PC ou do flash. O clique **consulta o flash** a fim adicionar a imagem da movimentação instantânea, ou a **transferência de arquivo pela rede do** clique a fim adicionar diretamente a imagem da máquina host:

10. Uma vez que a imagem é adicionada, clique **em seguida**:

11. A autenticação de usuário pode ser terminada através dos grupos de servidor do

Authentication, Authorization, and Accounting (AAA). Se os usuários são configurados já, a seguir escolha o **LOCAL** e clique-o **em seguida**. **Note**: Neste exemplo, a **autenticação local** é configurada, assim que significa que a base de dados de usuário local no ASA estará usada para a autenticação.

12. O conjunto de endereços para o cliente VPN deve ser configurado. Se se é configurado já, a seguir selecione-o do menu de gota para baixo. Se não, clique **novo** a fim configurar um novo. Uma vez que completo, clique **em seguida**:

13. Entre os server do Domain Name System (DNS) e os DN no *DNS* e no *Domain Name* colocam apropriadamente, e clicam então **em seguida**:

14. Nesta encenação, o objetivo é restringir o acesso sobre o VPN à rede **10.10.10.0/24** que é configurada como a sub-rede *interna* (ou LAN) atrás do ASA. O tráfego entre o cliente e a sub-rede interna deve ser isento de toda a tradução de endereço de rede dinâmica (NAT).

    Verifique o **tráfego isento VPN da** caixa de verificação da **tradução de endereço de rede** e configurar o LAN e as interfaces WAN que serão usados para a isenção:

15. Escolha as redes local que devem ser isentas:

16. Clique **em seguida**, **termine em seguida**, e então.

A configuração de cliente de AnyConnect está agora completa. Contudo, quando você configura AnyConnect através do wizard de configuração, configura a política do *túnel em divisão* como **Tunnelall** à revelia. A fim escavar um túnel o tráfego específico somente, o *split-tunneling* deve ser executado.

> **Note**: Se separação-escavando um túnel não é configurado, a política do túnel em divisão estará herdada da grupo-política do padrão (DfltGrpPolicy), que à revelia é ajustada a **Tunnelall.** Isto significa que uma vez que o cliente é conectado sobre o VPN, todo o tráfego (para incluir o tráfego à Web) está enviado sobre o túnel.

Somente o tráfego que é destinado ao endereço IP de Um ou Mais Servidores Cisco ICM NT MACILENTO ASA (ou *parte externa*) contorneará o Tunelamento na máquina cliente. Isto pode ser visto na saída do comando do **route print em** máquinas de Microsoft Windows.

Configuração do túnel em divisão

A escavação de um túnel rachada é uma característica que você possa usar a fim definir o tráfego para as sub-redes ou os anfitriões que devem ser cifrados. Isto envolve a configuração de um Access Control List (ACL) que seja associado com esta característica. O tráfego para as sub-redes ou os anfitriões que é definido neste ACL será cifrado sobre o túnel da extremidade de cliente, e as rotas para estas sub-redes é instalado na tabela de roteamento PC.

Termine estas etapas a fim mover-se de Túnel-*toda* configuração para a configuração do *túnel em divisão*:

1. Navegue às **políticas da configuração > do acesso remoto VPN > do grupo**:

2. O clique **edita**, e usa a árvore de navegação a fim navegar a **avançado > Split Tunneling**. Desmarcar a caixa de verificação **herdar na** *seção de política*, e selecione a **lista da rede de túnel abaixo do** menu de gota para baixo:

3. Desmarcar a caixa de verificação **herdar na** seção do *liste de redes*, e o clique **controla** a fim selecionar o ACL que especifica as redes LAN a que o cliente precisa o acesso:

4. Clique o **padrão ACL**, **adicionar**, **adicionar o nome ACL**, e então **ACL**:

5. O clique **adiciona o ACE** a fim adicionar a regra:

6. Click **OK**.

7. Clique em Apply.

Uma vez que conectadas, as rotas para as sub-redes ou os anfitriões na separação ACL são adicionados à tabela de roteamento da máquina cliente. Em máquinas de Microsoft Windows, isto pode ser visto na saída do comando do **route print**. O salto seguinte para estas rotas será um endereço IP de Um ou Mais Servidores Cisco ICM NT da sub-rede do pool do IP de cliente (geralmente o primeiro endereço IP de Um ou Mais Servidores Cisco ICM NT da sub-rede):

```
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.
```

Em máquinas do MAC OS, incorpore o **netstat - comando r** a fim ver a tabela de roteamento 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.
```

Transfira e instale o cliente de AnyConnect

Há dois métodos que você pode usar a fim distribuir o Cliente de mobilidade Cisco AnyConnect Secure na máquina do usuário:

- Desenvolvimento da Web
- Desenvolvimento autônomo

Both of these métodos são explicados em maiores detalhes nas seções que seguem.

Desenvolvimento da Web

A fim usar o método do desenvolvimento da Web, entre em **https:// <ASA FQDN>or<ASA IP>** URL em um navegador na máquina cliente, que o traz à página do portal *WebVPN*.

> **Note**: Se o internet explorer (IE) é usado, a instalação está terminada na maior parte através de ActiveX, a menos que você for forçado a usar Javas. Todos navegadores restantes usam Javas.

Registrado uma vez na página, a instalação deve começar na máquina cliente, e o cliente deve conectar ao ASA depois que a instalação está completa.

> **Note**: Você pôde ser alertado para que a permissão execute ActiveX ou Javas. Isto deve ser permitido a fim continuar com a instalação.

Desenvolvimento autônomo

Termine estas etapas a fim usar o método autônomo do desenvolvimento:

1. Transfira a imagem do cliente de AnyConnect da site da Cisco na Web. A fim escolher a imagem correta para a transferência, refira o página da web do Cliente de mobilidade Cisco AnyConnect Secure. Um link da transferência é fornecido nesta página. Navegue à página da transferência e selecione a versão apropriada. Execute uma busca para o **pacote completo da instalação - indicador/instalador autônomo (ISO)**.**Note**: Uma imagem do instalador ISO é transferida então (como *anyconnect-win-3.1.06073-pre-deploy-k9.iso*).
2. Use *WinRar* ou *7-Zip* a fim extrair os índices do pacote ISO:

3. Uma vez que os índices são extraídos, execute o **arquivo Setup.exe** e escolha os módulos que devem ser instalados junto com o Cliente de mobilidade Cisco AnyConnect Secure.

   Tip: A fim configurar ajustes adicionais para o VPN, consulte a seção configurando das conexões de cliente de VPN de AnyConnect do *manual de configuração do 5500 Series de Cisco ASA usando o CLI, os 8.4 e os 8.6*.

Configuração de CLI

Esta seção fornece a configuração de CLI para o Cliente de mobilidade Cisco AnyConnect Secure para finalidades da referência.

```
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
```

Verificar

Termine estas etapas a fim verificar a conexão de cliente e os vários parâmetros que são associadas a essa conexão:

1. Navegue à **monitoração > VPN no** ASDM:

2. Você pode usar o **filtro pela** opção a fim filtrar o tipo de VPN. Selecione o **cliente de AnyConnect do** menu de gota para baixo e as todas as sessões cliente de AnyConnect.**Tip**: As sessões podem mais ser filtradas com os outros critérios, tais como o *username* e o *endereço IP de Um ou Mais Servidores Cisco ICM NT*.

3. Fazer duplo clique uma sessão a fim obter uns detalhes mais adicionais sobre essa sessão particular:

4. Incorpore o comando do **anyconnect da mostra VPN-sessiondb no** CLI a fim obter os detalhes da sessão:

```
# 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. Você pode usar as outras opções de filtro a fim refinar os resultados:

```
# 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
```

Troubleshooting

Você pode usar os diagnósticos de AnyConnect e a ferramenta de relatório (DARDO) a fim

recolher os dados que são úteis para pesquisar defeitos a instalação e problemas de conexão de AnyConnect. O assistente do DARDO é usado no computador que executa AnyConnect. O DARDO monta os logs, o estado, e a informação de diagnóstico para a análise do centro de assistência técnica da Cisco (TAC) e não exige privilégios do administrado ser executado na máquina cliente.

Instale o DARDO

Termine estas etapas a fim instalar o DARDO:

1. Transfira a imagem do cliente de AnyConnect da site da Cisco na Web. A fim escolher a imagem correta para a transferência, refira o página da web do Cliente de mobilidade Cisco AnyConnect Secure. Um link da transferência é fornecido nesta página. Navegue à página da transferência e selecione a versão apropriada. Execute uma busca para o **pacote completo da instalação - indicador/instalador autônomo (ISO)**.**Note**: Uma imagem do instalador ISO é transferida então (como *anyconnect-win-3.1.06073-pre-deploy-k9.iso*).
2. Use *WinRar* ou *7-Zip* a fim extrair os índices do pacote ISO:

3. Consulte ao dobrador a que os índices foram extraídos.

4. Execute o **arquivo Setup.exe** e selecione somente AnyconnectDiagnostic **e ferramenta de relatório:**

Execute o DARDO

Está aqui alguma informação importante a considerar antes que você execute o DARDO:

- A edição deve ser recreada pelo menos uma vez antes que você execute o DARDO.

- A data e hora na máquina do usuário deve ser notada quando a edição é recreada.

Execute o *menu do* DARDO desde o início na máquina cliente:

O modo do *padrão* ou do *costume* pode ser selecionado. Cisco recomenda que você executa o DARDO no modo padrão de modo que toda a informação possa ser capturada em um único tiro.

Uma vez que terminada, a ferramenta salvar o arquivo do *.zip do* pacote do DARDO ao desktop de cliente. O pacote pode então ser enviado por correio eletrónico ao TAC (depois que você abre um caso de TAC) para a análise mais aprofundada.

Informações Relacionadas

- Guia do administrador do Cliente de mobilidade Cisco AnyConnect Secure, do Â do âÂ do 3.0 da liberação que controla, monitorando, e pesquisando defeitos sessões de AnyConnect

- Guia de Troubleshooting do cliente VPN de AnyConnect - Problemas comuns
- A Java 7 emite com AnyConnect, CSD/Hostscan, e WebVPN - guia de Troubleshooting
- Suporte Técnico e Documentação - Cisco Systems