Guia de distribuição vagueando do módulo da Segurança de AnyConnect OpenDNS

Índice

Introdução

Este documento descreve a instalação, a configuração, e os passos de Troubleshooting para o módulo vagueando de OpenDNS (guarda-chuva). Em AnyConnect 4.3.X e mais tarde, o cliente vagueando de OpenDNS está agora disponível como um módulo integrado. Igualmente sabe-se como o módulo da Segurança da nuvem e pode ser predeployed ao valor-limite com o instalador de AnyConnect, ou pode ser transferido da ferramenta de segurança adaptável (ASA) através de Web-distribui.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Mobilidade segura de Cisco AnyConnect
- OpenDNS/módulo vagueando do guarda-chuva
- Cisco ASA

Componentes Utilizados

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

- Versão ASA 9.3(3)7 de Cisco
- Cliente de mobilidade Cisco AnyConnect Secure 4.3.01095
- Módulo vagueando 4.3.01095 de OpenDNS
- Cisco Adaptive Security Device Manager (ASDM) 7.6.2 ou mais atrasado
- Microsoft Windows 8.1

- **Note**: Os requisitos mínimos para distribuir o módulo do guarda-chuva de OpenDNS são:
  - Versão 4.3.01095 ou mais recente do cliente VPN de AnyConnect
  - Cisco ASDM 7.6.2 ou mais atrasado
  O módulo vagueando de OpenDNS não é apoiado atualmente na plataforma Linux.

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 sua rede está viva, certifique-se de que você compreende o impacto potencial dos comandos any ou da configuração.

Informações de Apoio

OrgInfo.json

Para que o módulo vagueando de OpenDNS funcione corretamente, um arquivo OrgInfo.json deve ser transferido do painel de OpenDNS ou ser empurrado do ASA antes que o módulo esteja usado. Quando o arquivo é transferido primeiramente, salvar em um trajeto específico que dependa do sistema operacional.

Para Mac OS X, OrgInfo.json é transferido a /opt/cisco/anyconnect/Umbrella.
Para Microsoft Windows, OrgInfo.json é transferido ao cliente \ guarda-chuva seguros da mobilidade de C:\ProgramData\Cisco\Cisco AnyConnect.

```
{
"organizationId" : "XXXXXXX",
"fingerprint" : "XXXXXXXXXXXXXXXXXXXXXXXXXXXX",
"userId" : "XXXXXXX"
}
```

Como mostrado, o arquivo usa UTF-8 que codifica e contém um organizationId, uma impressão digital, e um userId. A identificação de organização representa a informação da organização para o usuário que é registrado atualmente no painel de OpenDNS. A identificação de organização é estática, original, e gerado automaticamente por OpenDNS para cada organização. A impressão digital é usada para validar o arquivo OrgInfo.json durante o registro do dispositivo e o usuário - a identificação representa um ID exclusivo para o usuário conectado.

Quando o módulo vagueando começa em Windows, o arquivo OrgInfo.json está copiado ao diretório de dados sob o diretório do guarda-chuva e usado como a cópia de funcionamento. Em

MAC OS X, a informação deste arquivo salvar a updater.plist no diretório de dados sob o diretório do guarda-chuva. Uma vez que o módulo leu com sucesso a informação do arquivo OrgInfo.json, tenta registrar-se com OpenDNS com uma nuvem API. Este registro conduz a OpenDNS que atribui a um identificador de dispositivo original à máquina esse registro tentado. Se um identificador de dispositivo do registro prévio está já disponível, o dispositivo salta o registro.

Depois que o registro está completo, o módulo vagueando executa uma operação de sincronização a fim recuperar a informação sobre a política para o valor-limite. Um identificador de dispositivo é necessário para que a operação de sincronização trabalhe. Os dados da sincronização incluem domínios syncInterval, whitelisted, e endereços IP de Um ou Mais Servidores Cisco ICM NT entre outras coisas. O intervalo da sincronização é o número de minutos depois do qual o módulo deve tentar ao resync.

Comportamento de sondagem DNS

Em cima do registro bem-sucedido e da sincronização, o módulo vagueando envia pontas de prova do Domain Name System (DNS) a seus resolvers locais. Estes pedidos DNS incluem perguntas TXT para debug.opendns.com. Baseado na resposta, o cliente pode determinar se um dispositivo virtual de OpenDNS dos em-locais (VA) existe na rede.

Se um dispositivo virtual (VA) esta presente, as transições do cliente a um modo “atrás-VA”, e a aplicação DNS não estão executadas no valor-limite. O cliente confia no VA para a aplicação DNS a nível de rede.

Se um VA não está atual, o cliente envia um pedido DNS aos resolvers públicos de OpenDNS (208.67.222.222) que usam UDP/443.

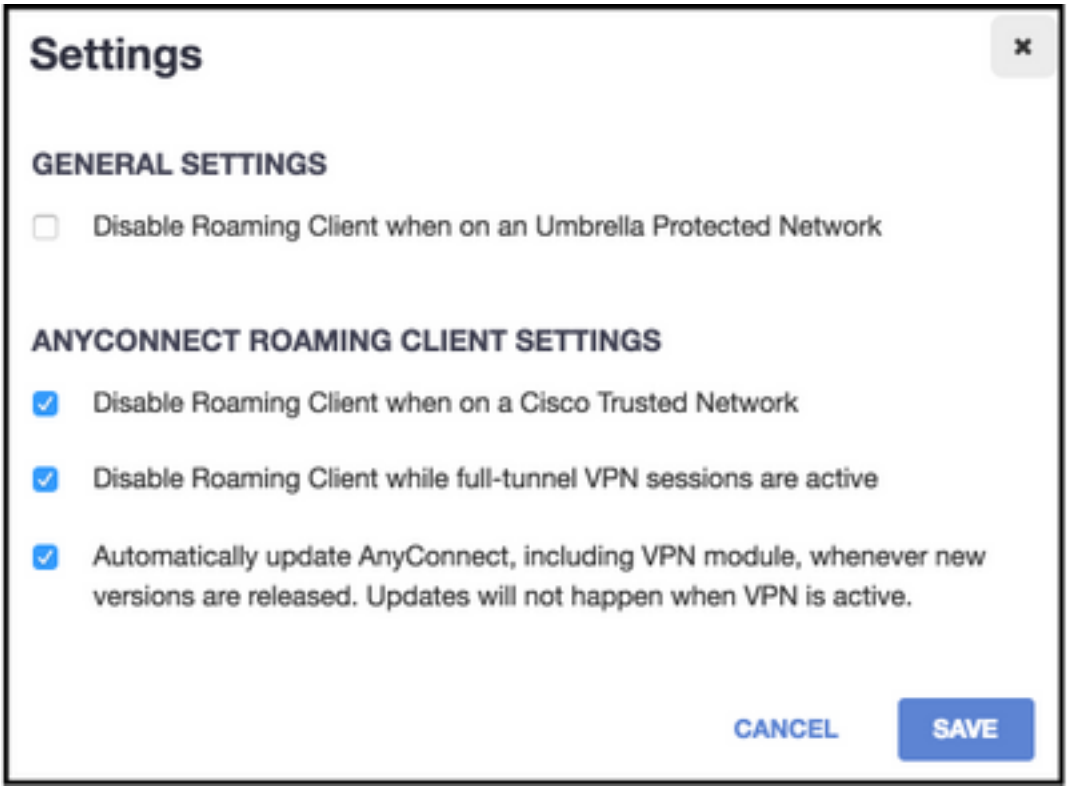
Uma resposta positiva indica que a criptografia DNS é possível. Se uma resposta negativa é recebida, o cliente envia um pedido DNS aos resolvers públicos de OpenDNS usando UDP/53.

Uma resposta positiva a esta pergunta indica que a proteção DNS é possível. Se uma resposta negativa é recebida, o cliente experimenta de novo a pergunta em alguns segundos.

Após recepção de um número do grupo de respostas negativas, as transições do cliente ao estado falha-aberto. Um estado falha-aberto significa que a criptografia e/ou a proteção DNS não são possíveis. Uma vez que o módulo vagueando tem com sucesso o concluiu a transição a um estado protegido e/ou cifrado, todas as perguntas DNS para domínios da busca fora dos domínios locais da busca e dos domínios do whitelist estão enviadas aos resolvers de OpenDNS para a resolução de nome. Com o estado cifrado permitido, todas as transações DNS são cifradas pelo processo do dnscrypt.

Comportamento de DNS com modos do Tunelamento de AnyConnect

1. Túnel-todo (ou túnel-todo-DNS permitido)



Note: Como mostrado, o comportamento padrão é para que o módulo vagueando desabilite a proteção DNS quando um túnel VPN com túnel-toda configuração for ativo. Para que o módulo seja ativo durante um AnyConnect túnel-toda configuração, o **desabilitação que vagueia o cliente quando as sessões de VPN do FULL-túnel forem opção ativa** deve ser desmarcado no portal de OpenDNS. A capacidade para permitir esta característica exige uma assinatura avançada em nível com OpenDNS. A informação abaixo supõe que a proteção DNS através do módulo vagueando está permitida.

Domínio perguntado parte de Whitelist

Os pedidos DNS que originam do adaptador do túnel são permitidos e enviados aos servidores DNS do túnel, através do túnel VPN. A pergunta permanecerá não resolvida se não pode ser resolvida pelos servidores DNS do túnel.

Domínio perguntado não parte de Whitelist

Os pedidos DNS que originam do adaptador do túnel são permitidos, e proxied aos resolvers públicos de OpenDNS através do módulo vagueando e serão enviados através do túnel VPN. Ao cliente de DNS parecerá como se a resolução de nome tinha ocorrido através do servidor DNS VPN. Se a resolução de nome através dos resolvers de OpenDNS não é bem sucedida, o módulo vagueando falha sobre aos servidores DNS localmente configurados, começando com o adaptador de VPN (que é o adaptador preferido quando o túnel estiver acima).

2. DNS em divisão (túnel-todo-DNS desabilitado)

Note: Todos os domínios do DNS em divisão são adicionados automaticamente ao whitelist vagueando do módulo em cima do estabelecimento de túnel. Isto é feito a fim fornecer um mecanismo de manipulação consistente DNS entre AnyConnect e o módulo vagueando. Assegure-se de que em uma configuração do DNS em divisão (com separação-inclua o Tunelamento) os resolvers públicos de OpenDNS não estejam incluídos nas redes

separação-incluir.

Note: Em Mac OS X, se o DNS em divisão é permitido para ambo o (IPv4 e IPv6) dos protocolos IP ou é permitido somente para um protocolo e não há nenhum conjunto de endereços configurado para o outro protocolo, o DNS em divisão verdadeiro similar a Windows é reforçado.
Se o DNS em divisão está permitido para somente um protocolo e um endereço de cliente está atribuído para o outro protocolo, simplesmente a reserva DNS para o split-tunneling está reforçada. Isto significa que AnyConnect permite somente os pedidos DNS que combinam os domínios do DNS em divisão através do túnel (outros pedidos são respondidos pelo AC com resposta recusada forçar o Failover aos servidores DNS públicos), mas não pode reforçar que os pedidos que combinam domínios do DNS em divisão não estão enviados na claro através do adaptador público.

Domínio perguntado parte de Whitelist e igualmente parte de domínios do DNS em divisão

Os pedidos DNS que originam do adaptador do túnel são permitidos e enviados aos servidores DNS do túnel, através do túnel VPN. Todos pedidos restantes para domínios de harmonização de outros adaptadores serão respondidos pelo direcionador de AnyConnect com “nenhum tal nome” para conseguir o DNS em divisão verdadeiro (impeça a reserva DNS). Consequentemente, somente o tráfego do NON-túnel DNS é protegido pelo módulo vagueando.

Domínio perguntado parte de Whitelist, mas não parte de domínios do DNS em divisão

Os pedidos DNS que originam do adaptador físico são permitidos e enviados aos servidores DNS públicos, fora do túnel VPN. Todos pedidos restantes para domínios de harmonização do adaptador do túnel serão respondidos pelo direcionador de AnyConnect com “nenhum tal nome” a fim impedir que a pergunta esteja enviada através do túnel VPN.

Domínio perguntado não parte de Whitelist ou domínios do DNS em divisão

Os pedidos DNS que originam do adaptador físico são permitidos e proxied aos resolvers públicos de OpenDNS, e enviados fora do túnel VPN. Ao cliente de DNS parecerá como se a resolução de nome tinha ocorrido através do servidor DNS público. Se a resolução de nome através dos resolvers de OpenDNS é mal sucedida, o módulo vagueando falha sobre aos servidores DNS localmente configurados, com exclusão de esses configurados no adaptador de VPN. Todos pedidos restantes para domínios de harmonização do adaptador do túnel serão respondidos pelo direcionador de AnyConnect sem tal nome a fim impedir que a pergunta esteja enviada através do túnel VPN.

3. Separação-inclua ou Separação-exclua o Tunelamento (nenhuns DNS em divisão e túnel-todo-DNS desabilitados)

Domínio perguntado parte de Whitelist

O resolver nativo do OS executa a resolução de DNS baseada na ordem dos adaptadores de rede, e AnyConnect é o adaptador preferido quando o VPN é ativo. Os pedidos DNS originarão do adaptador do túnel e serão enviados primeiramente aos servidores DNS do túnel, através do túnel VPN. Se a pergunta não pode ser resolvida pelos servidores DNS do túnel, o resolver do OS tentará resolvê-la através dos servidores DNS públicos.

Domínio perguntado não parte de Whitelist

O resolver nativo do OS executa a resolução de DNS baseada na ordem dos adaptadores de rede, e AnyConnect é o adaptador preferido quando o VPN é ativo. Os pedidos DNS originarão do adaptador do túnel e serão enviados primeiramente aos servidores DNS do túnel, através do túnel VPN. Se a pergunta não pode ser resolvida pelos servidores DNS do túnel, o resolver do OS tentará resolvê-la através dos servidores DNS públicos.

Se os resolvers públicos de OpenDNS são parte da lista separação-incluir ou não parte da lista da separação-exclusão, o pedido proxied está enviado através do túnel VPN.

Se os resolvers públicos de OpenDNS não são parte da lista separação-incluir ou parte da lista da separação-exclusão, o pedido proxied está enviado fora do túnel VPN.

Se a resolução de nome através dos resolvers de OpenDNS não é bem sucedida, o módulo vagueando falha sobre aos servidores DNS localmente configurados, começando com o adaptador de VPN (que é o adaptador preferido quando o túnel estiver acima). Se a resposta final retornada pelo módulo vagueando (e proxied de volta ao cliente de DNS nativo) não é bem sucedida, o cliente nativo tentará outros servidores DNS, se disponível.

Instale e configurar o módulo vagueando do guarda-chuva

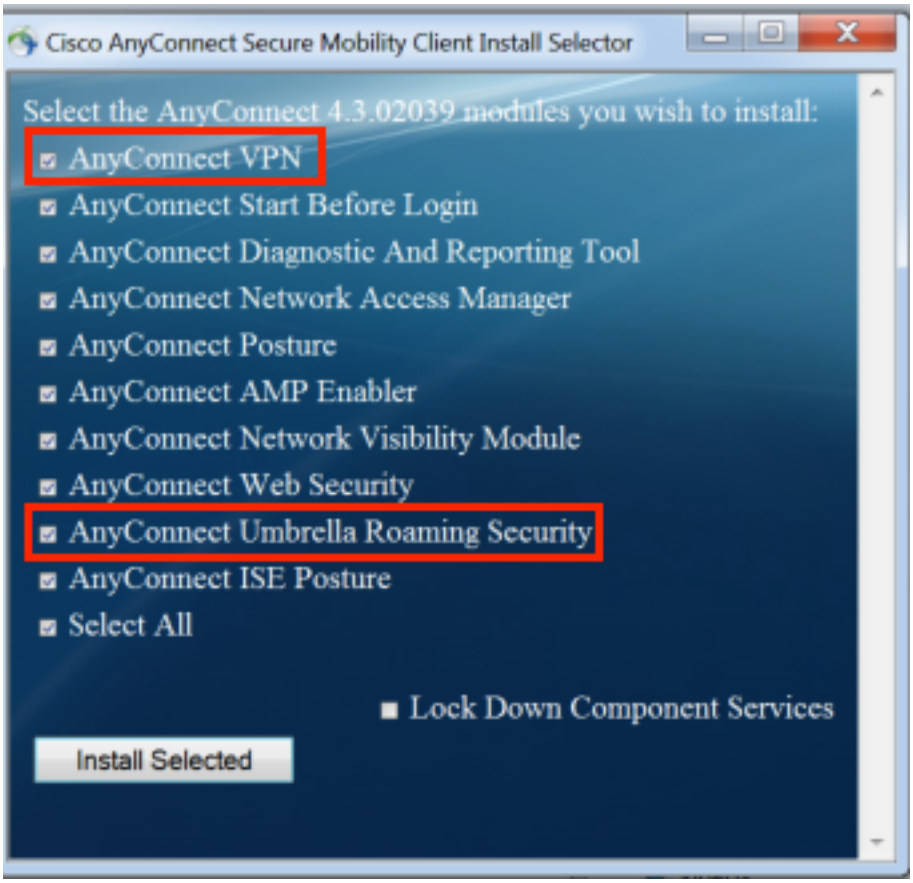
A fim integrar o módulo vagueando de OpenDNS com o cliente VPN de AnyConnect, o módulo precisa de ser instalado através do PRE-deplomento ou do método do desenvolvimento da Web:

método (manual) do PRE-desenvolvimento

o PRE-desenvolvimento exige a instalação manual do módulo de OpenDNS e do copi vagueando do arquivo OrgInfo.json na máquina do usuário. As distribuições em larga escala são conseguidas tipicamente com sistemas de administração do software de empreendimento (SMS).

Distribua o módulo vagueando de OpenDNS

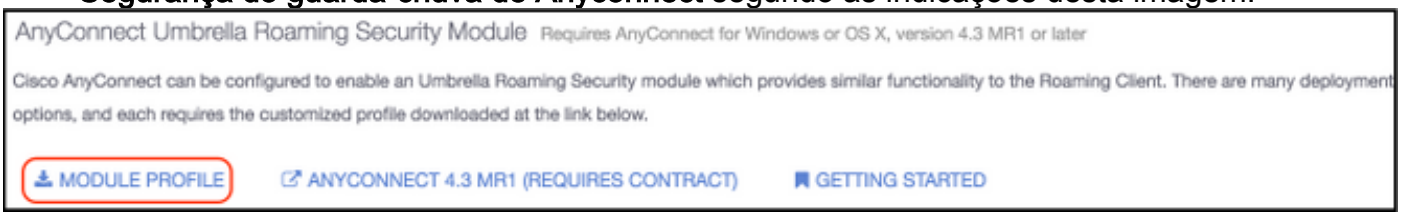
Durante a instalação do pacote de AnyConnect, escolha o **AnyConnect VPN** e os módulos **vagueando da Segurança do guarda-chuva de AnyConnect**:



Distribua OrgInfo.json

A fim transferir o arquivo OrgInfo.json, termine estas etapas:

1. Log no painel de OpenDNS.
2. Escolha a **configuração > as identidades > computadores vagueando.**
3. Clique **+** sinal.
4. Enrole para baixo e escolha o **perfil do módulo na seção de módulo vagueando da Segurança do guarda-chuva de Anyconnect** segundo as indicações desta imagem:



O arquivo é-lhe transferido uma vez deve ser salvar em um destes trajetos, que depende do sistema operacional.

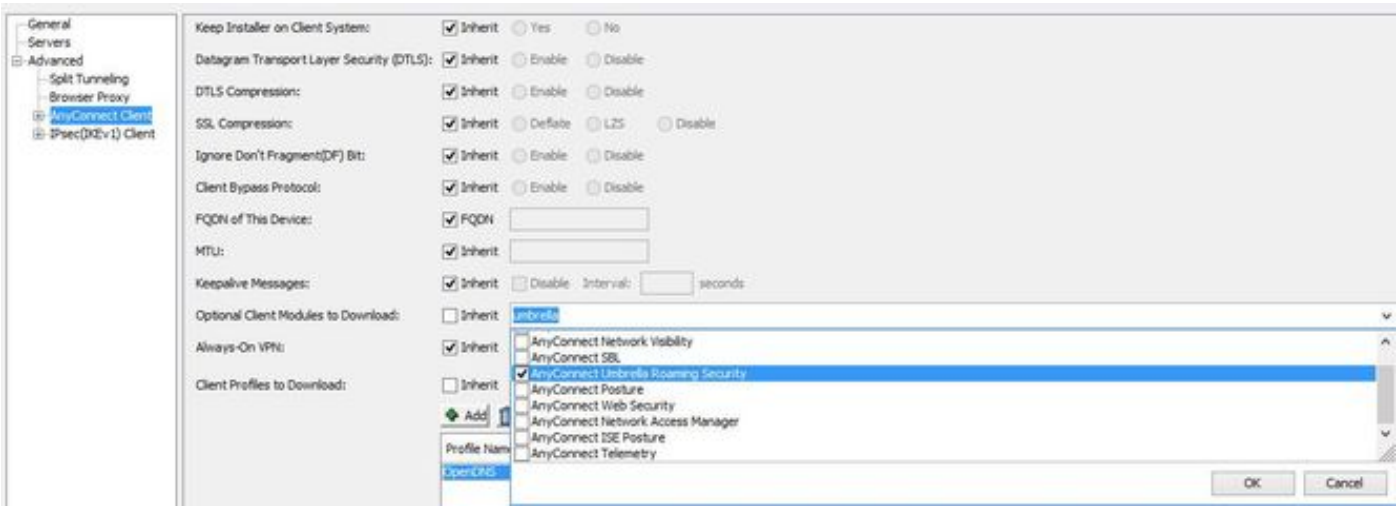
Para Mac OS X: /opt/cisco/anyconnect/Umbrella
Para Windows: Cliente \ guarda-chuva seguros da mobilidade de C:\ProgramData\Cisco\Cisco AnyConnect

Método do Web-desenvolvimento

Distribua o módulo vagueando de OpenDNS

Transfira o pacote do cliente da mobilidade da Segurança de Anyconnect (isto é, anyconnect-win-

4.3.02039-k9.pkg) da site da Cisco na Web e transfira-o arquivos pela rede ao flash do ASA. Uma vez que transferido arquivos pela rede, no ASDM, escolha a **política do grupo > avançou > cliente de AnyConnect > os módulos cliente opcionais para transferir** e escolher então a **Segurança vagueando do guarda-chuva.**

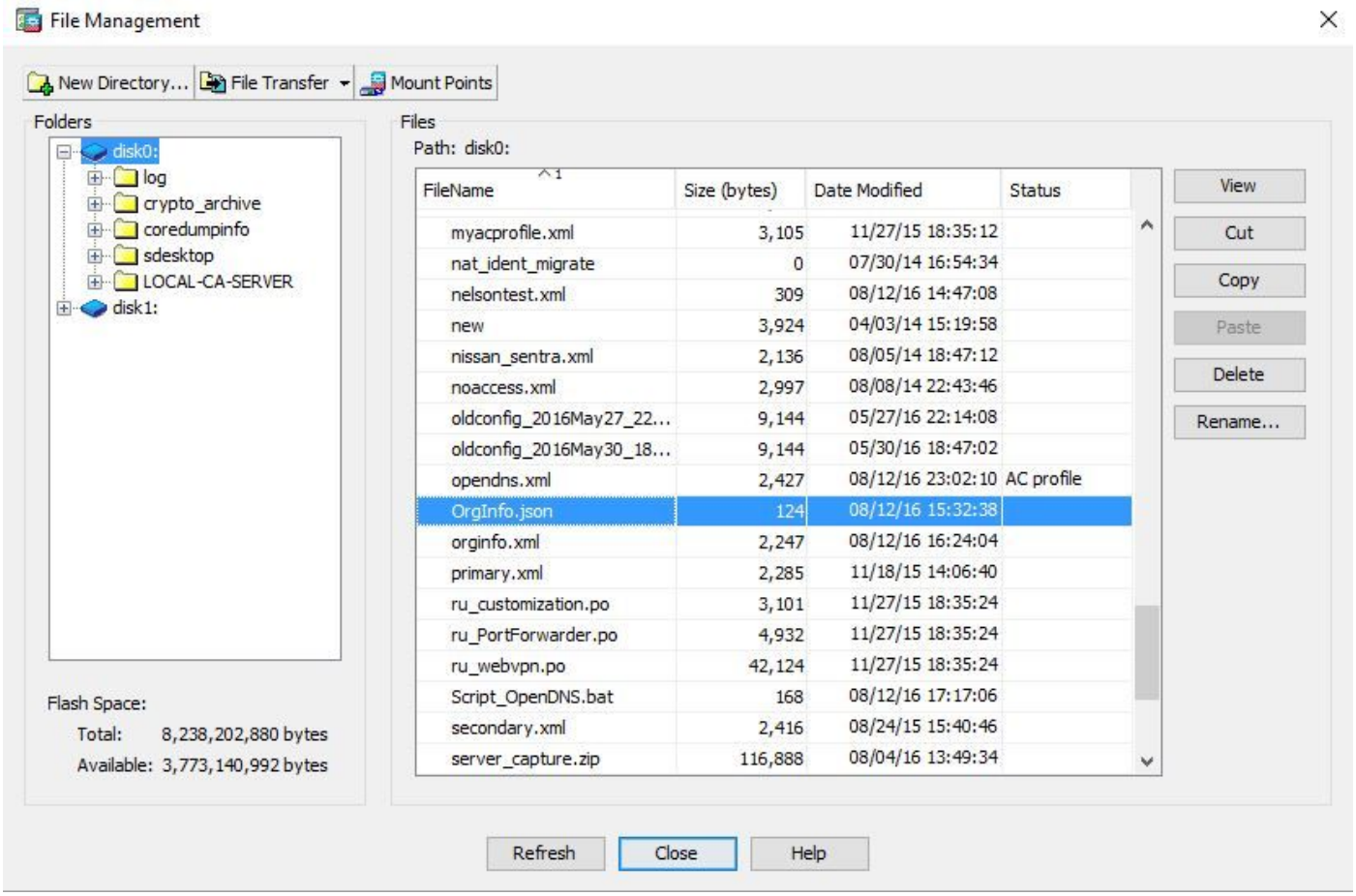


Equivalente CLI

```
group-policy <Group_Policy_Name> attributes
webvpn
anyconnect modules value umbrella
```

Distribua OrgInfo.json

1. Transfira o arquivo OrgInfo.json do painel de OpenDNS e transfira-o arquivos pela rede ao flash do ASA.



2. Configurar o ASA para empurrar o arquivo OrgInfo.json para pontos finais remotos.

```
webvpn
anyconnect profiles OpenDNS disk0:/OrgInfo.json
!
!
group-policy <Group_Policy_Name> attribute
webvpn
anyconnect profiles value OpenDNS type umbrella
```

> **Note**: Esta configuração pode somente ser executada com o CLI. A fim usar o ASDM para esta tarefa, a versão 7.6.2 ou mais recente ASDM precisa de ser instalada no ASA.

Uma vez que o cliente vagueando do guarda-chuva é instalado através de um dos métodos discutidos, deve aparecer como um módulo integrado dentro do AnyConnect GUI segundo as indicações desta imagem:

Até que o OrgInfo.json esteja distribuído no valor-limite no lugar correto, o módulo vagueando do guarda-chuva não estará inicializado.

Configurar

A seção mostra os snippet da configuração de CLI da amostra necessários operar o módulo vagueando de OpenDNS com os vários modos do Tunelamento de AnyConnect.

```
!--- ip local pool for vpn
ip local pool vpn_pool 198.51.100.1-198.51.100.9 mask 255.255.255.224

!--- Optional NAT Hairpin configuration to reach OpenDNS servers through VPN tunnel
object network OpenDNS
subnet 198.51.100.0 255.255.255.0
nat (outside,outside) source dynamic OpenDNS interface
!
same-security-traffic permit intra-interface

!--- Global Webvpn Configuration
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-4.3.01095-k9.pkg 1
anyconnect profiles Anyconnect disk0:/anyconnect.xml
 anyconnect profiles OpenDNS disk0:/OrgInfo.json
anyconnect enable
tunnel-group-list enable

!--- split-include Configuration
access-list Split_Include standard permit <host/subnet>

group-policy OpenDNS_Split_Include internal
group-policy OpenDNS_Split_Include attributes
wins-server none
dns-server value 198.51.100.11
vpn-tunnel-protocol ssl-client ssl-clientless
```

```
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value Split_Include
split-dns value <internal domains> (Optional Split-DNS Configuration)
webvpn
anyconnect profiles value AnyConnect type user
 anyconnect profiles value OpenDNS type umbrella
!
tunnel-group OpenDNS_Split_Include type remote-access
tunnel-group OpenDNS_Split_Include general-attributes
address-pool vpn_pool
default-group-policy OpenDNS_Split_Include
tunnel-group OpenDNS_Split_Include webvpn-attributes
group-alias OpenDNS_Split_Include enable


!--- Split-exclude Configuration
access-list Split_Exclude standard permit <host/subnet>

group-policy OpenDNS_Split_Exclude internal
group-policy OpenDNS_Split_Exclude attributes
wins-server none
dns-server value 198.51.100.11
vpn-tunnel-protocol ssl-client ssl-clientless
 split-tunnel-policy excludespecified
 split-tunnel-network-list value Split_Exclude
webvpn
anyconnect profiles value AnyConnect type user
 anyconnect profiles value OpenDNS type umbrella
!
tunnel-group OpenDNS_Split_Exclude type remote-access
tunnel-group OpenDNS_Split_Exclude general-attributes
address-pool vpn_pool
default-group-policy OpenDNS_Split_Exclude
tunnel-group OpenDNS_Split_Exclude webvpn-attributes
group-alias OpenDNS_Split_Exclude enable


!--- Tunnelall Configuration
group-policy OpenDNS_Tunnel_All internal
group-policy OpenDNS_Tunnel_All attributes
wins-server none
dns-server value 198.51.100.11
vpn-tunnel-protocol ssl-client ssl-clientless
 split-tunnel-policy tunnelall
webvpn
anyconnect profiles value AnyConnect type user
 anyconnect profiles value OpenDNS type umbrella
!
tunnel-group OpenDNS_Tunnel_All type remote-access
tunnel-group OpenDNS_Tunnel_All general-attributes
address-pool vpn_pool
default-group-policy OpenDNS_Tunnel_All
tunnel-group OpenDNS_Tunnel_All webvpn-attributes
group-alias OpenDNS_Tunnel_All enable
```

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

As etapas para pesquisar defeitos problemas relacionados de AnyConnect OpenDNS são:

1. Assegure-se de que o módulo vagueando da Segurança do guarda-chuva esteja instalado junto com o cliente seguro da mobilidade de Anyconnect.
2. Assegure-se de que OrgInfo.json este presente no valor-limite no trajeto correto baseado no sistema operacional e esteja no formato especificado neste documento.
3. Se as perguntas DNS aos resolvers de OpenDNS são pretendidas ir sobre o túnel de AnyConnect VPN, assegure-se de que o gancho de cabelo esteja configurado no ASA a fim permitir a alcançabilidade aos resolvers de OpenDNS.
4. Recolha capturas de pacote de informação (sem alguns filtros) no adaptador virtual e no adaptador físico de AnyConnect simultaneamente e note-as abaixo dos domínios que não resolvem.
5. Se o módulo vagueando se opera em um estado cifrado, recolha capturas de pacote de informação após ter obstruído UDP 443 localmente, para propósitos de Troubleshooting somente. Essa maneira lá é visibilidade nas transações DNS.
6. Execute o DARDO de AnyConnect, diagnósticos do guarda-chuva e note-o abaixo da época da falha de DNS. Veja como recolher o pacote do DARDO para Anyconnect para mais informação.
7. Recolha log de diagnóstico do guarda-chuva e envie a URL resultante a seu administrador de OpenDNS. Somente você e o administrador de OpenDNS têm o acesso a esta informação. Para Windows: C:\Program arquiva (cliente seguro da mobilidade x86)\Cisco\Cisco AnyConnect \ UmbrellaDiagnostic.exe
   Para o Mac OSX: /opt/cisco/anyconnect/bin/UmbrellaDiagnostic

Informações Relacionadas

- **Identificação de bug Cisco CSCvb34863: A latência em resolver o DNS quando AnyConnect configurou para separação-inclui o Tunelamento**
- **Suporte Técnico e Documentação - Cisco Systems**