Interop entre AnyConnect e o cliente vagueando de OpenDNS

Índice

Introdução

Este documento descreve algumas das limitações atual e as ações alternativas disponíveis para fazer AnyConnect e o cliente vagueando de OpenDNS trabalham junto. Os clientes Cisco confiam no cliente VPN de AnyConnect para seguro e uma comunicação codificada a suas redes corporativas. Similarmente, o cliente vagueando de OpenDNS dá a usuários a capacidade para usar firmemente serviços DNS com a ajuda dos server do público de OpenDNS. Ambos estes clientes adicionam um conjunto rico de recursos de segurança no valor-limite, e consequentemente é importante para eles interoperar um com o otro.

Pré-requisitos

Conhecimento em funcionamento do cliente vagueando de AnyConnect e de OpenDNS.

Familiaridade com a configuração do final do cabeçalho ASA ou IOS/IOS-XE (grupo de túneis/política) para AnyConnect VPN.

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Final do cabeçalho ASA ou IOS/IOS-XE
- Valor-limite que executa o cliente vagueando do cliente VPN e do OpenDNS de AnyConnect

Componentes Utilizados

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

- Liberação 9.4 do corredor do final do cabeçalho ASA
- Windows 7
- Cliente 4.2.00096 de AnyConnect
- Cliente vagueando 2.0.154 de OpenDNS

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

OpenDNS está desenvolvendo um AnyConnect de encaixe com a equipe de Cisco AnyConnect para estar disponível no futuro. Quando nenhuma data for ajustada, esta integração permitirá que o cliente vagueando trabalhe com o cliente de AnyConnect sem as ações alternativas endereçadas. Isto igualmente permitirá AnyConnect de ser um mecanismo de entrega para o cliente vagueando.

Funcionalidade

Manipulação de AnyConnect DNS

O fim de cabeçalho de VPN pode ser configurado em maneiras diferentes de um par de segurar o tráfego do cliente de AnyConnect.

1. Configuração de túnel completa (túnel-toda): Isto força todo o tráfego do valor-limite para ser enviado através do túnel VPN cifrado, e consequentemente o tráfego nunca deixa o adaptador de interface pública no texto claro
2. Configuração do túnel em divisão:

a. Separação-inclua o Tunelamento: Trafique destinado somente às sub-redes específicas ou os anfitriões definidos no fim de cabeçalho de VPN são enviados através do túnel, todo tráfego restante são enviados fora do túnel no texto claro

b. Separação-exclua o Tunelamento: Trafique destinado somente às sub-redes específicas ou os anfitriões definidos no fim de cabeçalho de VPN são excluídos da criptografia e deixam a interface pública no texto claro, todo tráfego restante é cifrado e enviado somente através do túnel

Cada um destas configurações determina como a resolução de DNS é segurada pelo cliente de AnyConnect, segundo o sistema operacional no valor-limite. Houve uma mudança no comportamento no mecanismo de manipulação DNS em AnyConnect para Windows, na liberação 4.2 após o reparo para CSCuf07885.

Windows 7+

Túnel-toda configuração (e split-tunneling com túnel-todo DNS permitido)

Pre AnyConnect 4.2:

Somente os pedidos DNS aos servidores DNS configurados sob a grupo-política (servidores DNS do túnel) são permitidos. O direcionador de AnyConnect responde a todos pedidos restantes com de “uma resposta nenhum tal nome”. Em consequência, a resolução de DNS pode somente ser executada usando os servidores DNS do túnel.

AnyConnect 4.2 +

Os pedidos DNS a todos os servidores DNS estão permitidos, enquanto são originados do adaptador de VPN e enviados através do túnel. Todos pedidos restantes são respondidos com de “resposta nenhum tal nome”, e a resolução de DNS pode somente ser executada através do túnel VPN

Antes do reparo CSCuf07885, o AC restringe os servidores DNS do alvo, porém com o reparo para CSCuf07885, restringe que adaptadores de rede podem iniciar pedidos DNS.

Separação-não inclua a configuração (túnel-todo DNS desabilitado e o nenhum DNS em divisão)

O direcionador de AnyConnect não interfere com o solucionador DNS nativo. Consequentemente, a resolução de DNS é executada baseou na ordem dos adaptadores de rede, e AnyConnect é sempre o adaptador preferido quando o VPN é conectado. Uma pergunta DNS será enviada assim primeiramente através do túnel e se não obtém resolved, o resolver tentará resolvê-lo através da interface pública. A lista de acesso separação-incluir terá que incluir a sub-rede que cobre os server DNS do túnel. Começando com AnyConnect 4.2, as rotas do host para os server DNS do túnel são adicionadas automaticamente como separação-incluem redes (fixe rotas) pelo cliente de AnyConnect, e consequentemente a lista de acesso separação-incluir já não exige a adição explícita da sub-rede do servidor DNS do túnel.

Separação-não exclua a configuração (túnel-todo DNS desabilitado e o nenhum DNS em divisão)

O direcionador de AnyConnect não interfere com o solucionador DNS nativo. Consequentemente, a resolução de DNS é executada baseou na ordem dos adaptadores de rede, e AnyConnect é sempre o adaptador preferido quando o VPN é conectado. Uma pergunta DNS será enviada assim primeiramente através do túnel e se não obtém resolved, o resolver tentará resolvê-lo através da interface pública. A lista de acesso da separação-exclusão não deve incluir a sub-rede que cobre os server DNS do túnel. Começando com AnyConnect 4.2, as rotas do host para os server DNS do túnel são adicionadas automaticamente como separação-incluem redes (fixe rotas) pelo cliente de AnyConnect, e consequentemente que impedirá o misconfiguration na lista de acesso da separação-exclusão.

DNS em divisão (túnel-todo DNS desabilitado, separação-inclui configurado)

Pre AnyConnect 4.2

Os pedidos DNS que combinam os domínios do DNS em divisão são permitidos escavar um túnel servidores DNS, mas não permitidos a outros servidores DNS. Para impedir que tais perguntas dos DN internos escapem para fora o túnel, o direcionador de AnyConnect responde com “nenhum tal nome” se a pergunta é enviada a outros servidores DNS. Assim os domínios do DNS em divisão podem somente ser resolved através dos servidores DNS do túnel.

O DNS pede a harmonização do DNS em divisão que os domínios são permitidos a outros servidores DNS, mas não reservado escavar um túnel servidores DNS. Mesmo neste caso, o direcionador de AnyConnect responde com “nenhum tal nome” se uma pergunta para domínios do DNS em divisão é tentada não através do túnel. Tão não os domínios do DNS em divisão podem somente ser resolved através dos servidores DNS públicos fora do túnel.

AnyConnect 4.2 +

Os pedidos DNS que combinam os domínios do DNS em divisão estão permitidos a todos os servidores DNS, enquanto originam do adaptador de VPN. Se a pergunta é originada pela interface pública, o direcionador de AnyConnect responde com “nenhum tal nome” para forçar o resolver para usar sempre o túnel para a resolução de nome. Assim os domínios do DNS em divisão podem somente ser resolved através do túnel.

O DNS pede a harmonização do DNS em divisão que os domínios estão permitidos a todos os servidores DNS enquanto originam do adaptador físico. Se a pergunta é originada pelo adaptador de VPN, AnyConnect responde com “nenhum tal nome” para forçar o resolver para tentar sempre a resolução de nome através da interface pública. Tão não os domínios do DNS em divisão podem somente ser resolved através da interface pública.

Mac OS X

Túnel-toda configuração (e split-tunneling com túnel-todo DNS permitido)

Quando AnyConnect é conectado, simplesmente os servidores DNS do túnel estão mantidos na Configuração de DNS do sistema, e consequentemente em pedidos DNS pode somente ser enviado aos server DNS do túnel.

Separação-não inclua a configuração (túnel-todo DNS desabilitado e o nenhum DNS em divisão)

AnyConnect não interfere com o solucionador DNS nativo. Os servidores DNS do túnel são configurados como os resolvers preferidos, tomando a precedência sobre servidores DNS públicos, assim assegurando-se de que o pedido inicial DNS para uma resolução de nome esteja enviado sobre o túnel. Desde que os ajustes DNS são globais em Mac OS X, não é possível para perguntas DNS usar servidores DNS públicos fora do túnel como documentado em CSCtf20226. Começando com AnyConnect 4.2, as rotas do host para os server DNS do túnel são adicionadas automaticamente como separação-incluem redes (fixe rotas) pelo cliente de AnyConnect, e consequentemente a lista de acesso separação-incluir já não exige a adição explícita da sub-rede do servidor DNS do túnel.

Separação-não exclua a configuração (túnel-todo DNS desabilitado e o nenhum DNS em divisão)

AnyConnect não interfere com o solucionador DNS nativo. Os servidores DNS do túnel são configurados como os resolvers preferidos, tomando a precedência sobre servidores DNS públicos, assim assegurando-se de que o pedido inicial DNS para uma resolução de nome esteja enviado sobre o túnel. Desde que os ajustes DNS são globais em Mac OS X, não é possível para perguntas DNS usar servidores DNS públicos fora do túnel como documentado em CSCtf20226. Começando com AnyConnect 4.2, as rotas do host para os server DNS do túnel são adicionadas automaticamente como separação-incluem redes (fixe rotas) pelo cliente de AnyConnect, e consequentemente a lista de acesso separação-incluir já não exige a adição explícita da sub-rede do servidor DNS do túnel.

DNS em divisão (túnel-todo DNS desabilitado, separação-inclui configurado)

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. O DNS em divisão verdadeiro significa que os pedidos que combinam os domínios do DNS em divisão são somente resolved através do túnel, ele não é escapado aos servidores DNS fora do túnel.

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 o AC 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.

Linux

Túnel-toda configuração (e split-tunneling com túnel-todo DNS permitido)

Quando AnyConnect é conectado, simplesmente os servidores DNS do túnel estão mantidos na Configuração de DNS do sistema, e consequentemente em pedidos DNS pode somente ser enviado aos server DNS do túnel.

Separação-não inclua a configuração (túnel-todo DNS desabilitado e o nenhum DNS em divisão)

AnyConnect não interfere com o solucionador DNS nativo. Os servidores DNS do túnel são configurados como os resolvers preferidos, tomando a precedência sobre servidores DNS públicos, assim assegurando-se de que o pedido inicial DNS para uma resolução de nome esteja enviado sobre o túnel.

Separação-não exclua a configuração (túnel-todo DNS desabilitado e o nenhum DNS em divisão)

AnyConnect não interfere com o solucionador DNS nativo. Os servidores DNS do túnel são configurados como os resolvers preferidos, tomando a precedência sobre servidores DNS públicos, assim assegurando-se de que o pedido inicial DNS para uma resolução de nome esteja enviado sobre o túnel.

DNS em divisão (túnel-todo DNS desabilitado, separação-inclui configurado)

Se o DNS em divisão é permitido, simplesmente “a reserva DNS para o split-tunneling” está reforçada. Isto significa que o AC 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.

Cliente vagueando de OpenDNS

O cliente vagueando é uma parte de software que controle serviços DNS no valor-limite, e utiliza os servidores DNS públicos de OpenDNS para fixar e cifrar o tráfego DNS.

Idealmente, o cliente deve estar em um estado protegido e cifrado. Contudo, se o cliente é incapaz de estabelecer uma sessão TLS com o server público do resolver de OpenDNS (208.67.222.222), tenta enviar tráfego DNS unencrypted na porta 53 UDP a 208.67.222.222. O cliente vagueando usa exclusivamente o endereço IP 208.67.222.222 público do resolver de OpenDNS (há algum outro tal como 208.67.220.220, 208.67.222.220, e 208.67.220.222). O cliente vagueando instalado uma vez, ajusta 127.0.0.1 (host local) como o servidor DNS local e cancela os ajustes atuais da interface per. DNS. Os ajustes atuais DNS são armazenados em arquivos locais resolv.conf (mesmo em Windows) dentro do dobrador vagueando da configuração de cliente. OpenDNS alternativo mesmo aqueles servidores DNS que são instruídos através do adaptador de AnyConnect. Por exemplo, se 192.168.92.2 é o servidor

DNS no adaptador público, OpenDNS criará o resolv.conf no seguinte lugar:

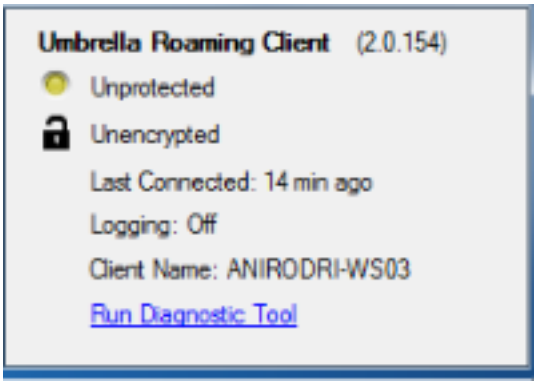
C:\ProgramData\OpenDNS\ERC\Resolver1-LocalAreaConnection-resolv.conf
servidor de nome 192.168.92.2

O cliente vagueando cifrará cada pacote ajustado a OpenDNS; contudo, não liga nem usa um túnel de criptografia a 208.67.222.222. O cliente vagueando tem uma característica opcional da aplicação da camada IP que abra uma conexão IPSec para que as finalidades não-DNS obstruam endereços IP de Um ou Mais Servidores Cisco ICM NT. Isto desabilitará automaticamente na presença de uma conexão ativa de AnyConnect. Igualmente liga a 127.0.0.1:53 para receber as perguntas geradas localmente no computador. Quando o valor-limite precisa de resolver um nome, as perguntas locais estão dirigidas a 127.0.0.1 devido à ultrapassagem, e então ao processo subjacente do dnscrypt-proxy do cliente vagueando para a frente eles aos server públicos de OpenDNS sobre o canal cifrado.

Se o DNS não é permitido para fluir a 127.0.0.1:53, a seguir o cliente vagueando não poderá funcionar e o seguinte ocorrerá. Se o cliente é incapaz de alcançar os servidores DNS públicos ou o endereço encadernado de 127.0.0.1:53, transição a um estado falha-aberto e para restaurar os ajustes DNS nos adaptadores locais. No fundo, continua a enviar pontas de prova a 208.67.222.222 e pode transição ao modo ativo se a conexão segura é restabelecida.

Limitações

Olhando a funcionalidade de nível elevado de ambos os clientes, é evidente que o cliente vagueando precisa de ter a capacidade para mudar os ajustes do DNS local e para os ligar a 127.0.0.1:53 para enviar perguntas através do canal seguro. Quando o VPN é conectado, as únicas configurações onde AnyConnect não interfere com o solucionador DNS nativo são separação-incluir e separação-para excluir (com separação-túnel-todo DNS desabilitado). Consequentemente, recomenda-se atualmente usar uma daquelas configurações, quando o cliente vagueando é igualmente dentro uso. O cliente vagueando permanecerá estado desprotegido/unencrypted se túnel-toda configuração está usada, ou separação-túnel-todo DNS está permitido, segundo as indicações da imagem.



Solução

Se a intenção é proteger uma comunicação entre o cliente e os server vagueando de OpenDNS

usando o túnel VPN, a seguir um manequim separação-exclui a lista de acesso pode ser usado no fim de cabeçalho de VPN. Esta será a coisa a mais próxima a uma configuração de túnel completa. Se não há nenhuma tal exigência, a seguir separação-inclua pode ser usado onde a lista de acesso não inclui os server públicos de OpenDNS, ou separação-excluem pode ser usado onde a lista de acesso inclui os server do público de OpenDNS.

Adicionalmente, ao usar o cliente vagueando, os modos do DNS em divisão não podem ser usados porque este conduzirá a uma perda de definição do DNS local. Separação-túnel-todo DNS deve igualmente permanecer deficiente; contudo, parcialmente é apoiado e deve permitir que o cliente vagueando transforme-se cargo-Failover cifrado.

Configurações

Tráfego de OpenDNS do túnel

Este exemplo usa um endereço IP de Um ou Mais Servidores Cisco ICM NT do manequim na lista de acesso da separação-exclusão. Com esta configuração, toda a comunicação com 208.67.222.222 acontece através do túnel VPN, e o cliente vagueando opera-se em um estado cifrado e protegido.

```
ciscoasa# sh run access-li split
access-list split standard permit host 2.2.2.2

ciscoasa# sh run group-policy
group-policy GroupPolicy-OpenDNS internal
group-policy GroupPolicy-OpenDNS attributes
 wins-server none
 dns-server value 1.1.1.1
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy excludespecified
 split-tunnel-network-list value split
 default-domain value cisco.com
 address-pools value acpool
 webvpn
 anyconnect profiles value AnyConnect type user
ciscoasa#
```

Exclua o tráfego de OpenDNS do túnel VPN

Este exemplo usa o endereço do resolver de OpenDNS na lista de acesso da separação-exclusão. Com esta configuração, toda a comunicação com 208.67.222.222 acontece fora do túnel VPN, e o cliente vagueando opera-se em um estado cifrado e protegido.

```
ciscoasa# sh run access-li split
access-list split standard permit host 208.67.222.222

ciscoasa# sh run group-policy
group-policy GroupPolicy-OpenDNS internal
group-policy GroupPolicy-OpenDNS attributes
 wins-server none
 dns-server value 1.1.1.1
 vpn-tunnel-protocol ssl-client
```

```
 split-tunnel-policy excludespecified
 split-tunnel-network-list value split
 default-domain value cisco.com
 address-pools value acpool
 webvpn
 anyconnect profiles value AnyConnect type user
ciscoasa#
```

Este exemplo mostra uma configuração separação-incluir para uma sub-rede 192.168.1.0/24 interna. Com esta configuração, o cliente vagueando ainda operar-se-á em um estado cifrado e protegido desde que o tráfego a 208.67.222.222 não é enviado através do túnel.

```
ciscoasa# sh run access-li split
access-list split standard permit 192.168.1.0 255.255.255.0

ciscoasa# sh run group-policy
group-policy GroupPolicy-OpenDNS internal
group-policy GroupPolicy-OpenDNS attributes
 wins-server none
 dns-server value 1.1.1.1
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value split
 default-domain value cisco.com
 address-pools value acpool
 webvpn
 anyconnect profiles value AnyConnect type user
ciscoasa#

Note: Split-tunnel-all-dns must be disabled in all of the  scenarios
```

Verificar

Quando o VPN é conectado, o cliente vagueando deve mostrar protegido e cifrado segundo as indicações desta imagem: