Diferenças comportáveis em relação às perguntas DNS e definição do Domain Name em OS diferentes

Índice

Introdução

Este documento descreve como perguntas diferentes do Domain Name System (DNS) do punho dos sistemas operacionais (OS) e as influências na definição do Domain Name com Cisco AnyConnect e Tunelamento rachado ou completo.

Separação contra o padrão DNS

Quando você se usa separação-inclua o Tunelamento, lá são três opções de DNS:

1. **DNS em divisão** - As perguntas DNS que combina os Domain Name, são configuradas na ferramenta de segurança adaptável de Cisco (ASA). Movem-se através do túnel (aos servidores DNS que são definidos no ASA, por exemplo) quando outro não fizerem.

2. **Túnel-todo-DNS** - Somente o tráfego DNS aos servidores DNS que são definidos pelo ASA é permitido. Este ajuste é configurado na política do grupo.

3. **Padrão DNS** - Todas as perguntas DNS movem-se através dos servidores DNS que são definidos pelo ASA. No caso de uma resposta negativa, as perguntas DNS puderam igualmente ir aos servidores DNS que são configurados no adaptador físico.

Nota: O comando separação-túnel-todo-**dns** foi executado primeiramente na versão ASA 8.2(5). Antes desta versão, você poderia somente fazer o DNS em divisão ou o padrão DNS.

Em todos os casos, as perguntas DNS que são definidas para se mover através do túnel, vão a todos os servidores DNS que forem definidos pelo ASA. Se não há nenhum servidor DNS definido pelo ASA, a seguir os ajustes DNS estão vazios para o túnel. Se você não tem o DNS em divisão definido, a seguir todas as perguntas DNS estão enviadas aos servidores DNS que são definidos pelo ASA. Contudo, os comportamentos que são descritos neste documento podem ser diferentes, segundo o operating system (OS).

Nota: Evite o uso do NSLookup quando você testa a resolução de nome no cliente. Em lugar de, confie em um navegador ou use o **comando ping**. Isto é porque NSLookup não confia no solucionador DNS do OS. AnyConnect não força o pedido DNS através de uma determinada interface mas permite-o ou rejeita-o dependente da configuração do DNS em divisão. A fim forçar o solucionador DNS para tentar um servidor DNS aceitável para um pedido, é importante que o teste do DNS em divisão está executado somente com os aplicativos que confiam no solucionador DNS nativo para a definição do Domain Name (todos os aplicativos exceto NSLookup, escavação, e os aplicativos similares que seguram a resolução de DNS sós, por exemplo).

Retifique contra o melhor DNS em divisão do esforço

A liberação 2.4 de AnyConnect apoia a reserva do DNS em divisão (o melhor DNS em divisão do esforço), que não é o DNS em divisão verdadeiro e é encontrada no cliente de IPSec do legado. Se o pedido combina um domínio do DNS em divisão, AnyConnect permite que o pedido esteja escavado um túnel no ASA. Se o server não pode resolver o nome de host, o solucionador DNS continua e envia a mesma pergunta ao servidor DNS que é traçado à interface física.

Por outro lado, se o pedido não combina alguns dos domínios do DNS em divisão, AnyConnect não o escava um túnel no ASA. Em lugar de, constrói uma resposta de DNS de modo que o solucionador DNS recue e envie a pergunta ao servidor DNS que é traçado à interface física. Esta característica não é chamada é por isso DNS em divisão, mas reserva DNS para o Split Tunneling. Não somente AnyConnect assegura que somente os pedidos que visam domínios do DNS em divisão estão escavados um túnel dentro, ele igualmente confia no comportamento do solucionador DNS do SO de cliente para a resolução de nome do host.

Isto levanta os interesses de segurança devido a um escape privado potencial do Domain Name. Por exemplo, o cliente de DNS nativo pode enviar uma pergunta para um Domain Name privado a um servidor DNS público especificamente quando o server de nome de DNS VPN não poderia resolver a pergunta DNS.

Refira a identificação de bug Cisco CSCtn14578, resolvida atualmente em Microsoft Windows somente, até à data da versão 3.0(4235). A solução executa o DNS em divisão verdadeiro, pergunta restritamente os Domain Name configurados que os fósforos e são permitidos aos servidores DNS VPN. Todas perguntas restantes são permitidas somente a outros servidores DNS, tais como aquelas configuradas no adaptador físico.

Escave um túnel tudo e escave um túnel todo o DNS

Quando o Split Tunneling estiver desabilitado (o **túnel toda a** configuração), o tráfego DNS está permitido restritamente através do túnel. **O túnel que toda a Configuração de DNS** (configurada na política do grupo) envia a todas as pesquisas de DNS através do túnel, junto com algum tipo de Split Tunneling, e a tráfego DNS é permitido restritamente através do túnel.

Isto é consistente através das Plataformas com a uma advertência em Microsoft Windows: quando todo o **túnel todo** ou **escavar um túnel todo o DNS** é configurado, AnyConnect permite o tráfego DNS restritamente aos servidores DNS que são configurados no gateway seguro (aplicado ao adaptador de VPN). Este é um aprimoramento de segurança executado junto com a solução verdadeira previamente mencionada do DNS em divisão.

Se isto prova problemático em determinadas encenações (por exemplo, a atualização DNS/requisições de registro deve ser enviada aos servidores DNS NON-VPN), termine então estas etapas:

1. Se a configuração atual é **túnel todo**, a seguir permita separação-**excluem o Tunelamento**. Todo o host único, separação-exclui a rede é aceitável para o uso, tal como um endereço local de link.

2. Assegure-se de que que **escava um túnel todo o DNS** não é configurado na política do grupo.

Edição de desempenho DNS resolvida na versão 3.0(4235) de AnyConnect

Esta edição de Microsoft Windows é na maior parte predominante sob estas condições:

- Com a instalação home do roteador, o DNS e os servidores DHCP são atribuídos o mesmo endereço IP de Um ou Mais Servidores Cisco ICM NT (AnyConnect cria uma rota necessária ao servidor DHCP).

- Um grande número domínios de DNS estão na política do grupo.

- **Túnel-toda** configuração é usada.

- A resolução de nome é executada por um nome de host NON-qualificado, que implique que o resolver deve tentar um número de sufixos DNS em todos os servidores DNS disponíveis até que esse relevante ao nome de host perguntado esteja tentado.

Esta edição é devido ao cliente de DNS nativo que tenta enviar perguntas DNS através do adaptador físico, que AnyConnect obstrui (dado túnel-**toda** configuração). Isto conduz a um atraso

da resolução de nome que possa ser significativo, especialmente se um grande número sufixos DNS são empurrados pelo final do cabeçalho. O cliente de DNS deve andar através de todas as perguntas e servidores DNS disponíveis até que receba uma resposta positiva.

Este problema é resolvido na versão 3.0(4235) de AnyConnect. Proveja o Bug da Cisco ID CSCtq02141 e CSCtn14578, junto com a introdução à solução verdadeira precedente-mencionada do DNS em divisão, para mais informação.

Se uma elevação não pode ser executada, a seguir estas são as alternativas possíveis:

- Enable separação-**exclui o Tunelamento** para um endereço IP de Um ou Mais Servidores Cisco ICM NT, que permita os pedidos do DNS local correr através do adaptador físico. Você pode usar um endereço da sub-rede linklocal **169.254.0.0/16** porque é improvável que qualquer dispositivo envia o tráfego a um daqueles endereços IP de Um ou Mais Servidores Cisco ICM NT sobre o VPN. Depois que você permite o **Tunelamento da separação-exclusão**, permita o acesso no perfil do cliente ou no cliente próprio do LAN local, e desabilite o **túnel todo o DNS**.

  No ASA, faça estas alterações de configuração:

  ```
  access-list acl_linklocal_169.254.1.1 standard permit host 169.254.1.1
  group-policy gp_access-14 attributes
  split-tunnel-policy excludespecified
  split-tunnel-network-list value acl_linklocal_169.254.1.1
  split-tunnel-all-dns disable
  exit
  ```

  No perfil do cliente, você deve adicionar esta linha:

  ```
  <LocalLanAccess UserControllable="true">true</LocalLanAccess>
  ```

  Você pode igualmente permitir este em uma base do por-cliente no cliente GUI de AnyConnect. Navegue ao menu da **preferência de AnyConnect**, e verifique a caixa de verificação do **acesso do LAN local da possibilidade**.

- Use os nomes de domínio totalmente qualificados (FQDNs) em vez dos nomes de host incompetentes para as resoluções de nome.

- Use um endereço IP de Um ou Mais Servidores Cisco ICM NT diferente para o servidor DNS na interface física.

DNS com o Split Tunneling em OS diferentes

O punho diferente DNS OS procura em maneiras diferentes quando usado com Split Tunneling (sem DNS em divisão) para AnyConnect. Esta seção descreve aquelas diferenças.

Microsoft Windows

Em sistemas de Microsoft Windows, os ajustes DNS são interface per. Se o Split Tunneling é usado, as perguntas DNS podem cair de volta aos servidores DNS físicos do adaptador depois que falham no adaptador do túnel VPN. Se o Split Tunneling sem DNS em divisão é definido, a seguir a resolução de DNS interna e externo trabalha porque cai de volta aos servidores DNS

externos.

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 onde AnyConnect é sempre o adaptador preferido quando o VPN é conectado. Além disso, uma pergunta DNS é enviada primeiramente através do túnel e se não obtém resolved, o resolver tenta resolvê-lo através da interface pública. A lista de acesso separação-incluir inclui a sub-rede que cobre os server DNS do túnel. Para começar 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 onde AnyConnect é sempre o adaptador preferido quando o VPN é conectado. Além disso, uma pergunta DNS é enviada primeiramente através do túnel e se não obtém resolved, o resolver tenta 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. Para começar 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 impedem consequentemente 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 combina com 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. Consequentemente, os domínios do DNS em divisão podem somente ser resolved através dos servidores DNS do túnel.

Os pedidos DNS, que não combina com os domínios do DNS em divisão são permitidos a outros servidores DNS, mas não permitidos 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. Consequentemente, 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 combina com 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. Consequentemente, os domínios do DNS em divisão podem somente ser resolved através do túnel.

Os pedidos DNS, que não combina com os domínios do DNS em divisão 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. Consequentemente, não os domínios do DNS em divisão podem somente ser resolved através da interface pública.

Mac OSx

Em sistemas macintosh, os ajustes DNS são globais. Se o Split Tunneling está usado, mas o DNS em divisão não está usado, não é possível para as perguntas DNS alcançar servidores DNS fora do túnel. Você pode somente resolver internamente, não externamente.

Isto é documentado no Bug da Cisco ID CSCtf20226 e CSCtz86314. Em ambos os casos, esta ação alternativa deve resolver a edição:

- Especifique um endereço IP de Um ou Mais Servidores Cisco ICM NT externo do servidor DNS sob a política do grupo e use um FQDN para as perguntas dos DN internos.

- Se os nomes externos são solucionáveis através do túnel, a seguir navegue a **avançado >**

Split Tunneling e desabilite o DNS em divisão através da remoção dos nomes de DNS que são configurados na política do grupo. Isto exige o uso de um FQDN para as perguntas dos DN internos.

O exemplo do DNS em divisão é resolvido na versão 3.1 de AnyConnect. Contudo, você deve assegurar-se de que uma destas circunstâncias esteja estado conforme:

- O DNS em divisão deve ser permitido para ambos os protocolos IP, que exige a versão ASA 9.0 de Cisco ou mais atrasado.

- O DNS em divisão deve ser permitido para um protocolo IP. Se você executa a versão ASA 9.0 de Cisco ou mais atrasado, a seguir use o protocolo do desvio do cliente para o outro protocolo IP. Por exemplo, assegure-se de que não haja nenhum conjunto de endereços e que o **protocolo do desvio do cliente** está permitido na política do grupo. Alternativamente, se você executa uma versão ASA que esteja mais adiantada do que a versão 9.0, assegure-se de que não haja nenhum conjunto de endereços configurado para o outro protocolo IP. Isto implica que o outro protocolo IP é IPv6.

Nota: AnyConnect não muda o **arquivo resolv.conf no** Macintosh OS X, mas muda um pouco ajustes X-específicos do OS DNS. O Macintosh OS X mantém o resolv.conffile atual para razões de compatibilidade. Use o scutil**--comando dns** a fim ver os ajustes DNS no Macintosh 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 resolvers preferidos, que toma a precedência sobre servidores DNS públicos, assim assegura-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. Para começar 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 enquanto os resolvers preferidos, tomando a precedência sobre servidores DNS públicos, assim assegura-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. Para começar 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 esse pedido que os fósforos com 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 o pedido DNS que combina 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 o pedido que combina com os domínios do DNS em divisão que não são 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 resolvers preferidos, que toma a precedência sobre servidores DNS públicos, assim assegura-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 resolvers preferidos, que toma a precedência sobre servidores DNS públicos, assim assegura-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 o pedido DNS que combina com 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 esse pedido que combina com os domínios do DNS em divisão que não são enviados na claro, através do adaptador público.

iPhone

O iPhone é o oposto completo do sistema macintosh e não é similar ao Microsoft windows. Se o Split Tunneling é definido mas o DNS em divisão não está definido, a seguir o DNS pergunta a saída através do servidor DNS global que é definido. Por exemplo, as entradas de domínio do DNS em divisão são imperativas para a definição interna. Este comportamento é documentado na identificação de bug Cisco CSCtq09624 e fixado na versão 2.5.4038 para o cliente iOS AnyConnect de Apple.

> Nota: Esteja ciente que as perguntas do iPhone DNS ignoram **domínios .local**. Isto é documentado na identificação de bug Cisco CSCts89292. Os coordenadores de Apple confirmam que a edição está causada pela funcionalidade do OS. Este é o comportamento projetado, e Apple não confirma lá é nenhuma mudança para ela.

Informações Relacionadas

- CSCsv34395 - Adicionar o apoio em AnyConnect para proxying o FQDN ao servidor DHCP
- CSCtn14578 - AnyConnect para apoiar o DNS em divisão verdadeiro; não reserva
- CSCtq02141 - Edição de AnyConnect DNS quando o ISP DNS estiver na mesma sub-rede como o IP do público
- CSCtn14578 - AnyConnect para apoiar o DNS em divisão verdadeiro; não reserva
- CSCtf20226 - Faça a AnyConnect DNS com o comportamento do túnel em divisão para o Mac mesmos que indicadores
- CSCtz86314 - Mac: Perguntas DNS incorretamente não enviadas através do túnel com DNS em divisão
- CSCtq09624 - Faça ao iPhone DNS de AnyConnect com o comportamento do Split Tunneling mesmos que Windows
- CSCts89292 - O AC para perguntas do iPhone DNS ignora domínios .local
- Cisco IOS Firewall

- Suporte Técnico e Documentação - Cisco Systems