Examinar o comportamento das consultas DNS e da resolução de nomes de domínio

Contents

Introdução

Este documento descreve como o Cisco OS® lida com consultas DNS e os efeitos na resolução de nomes de domínio com o Cisco AnyConnect e tunelamento dividido ou completo.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

DNS dividido versus padrão

Quando você usa o tunelamento split-include, estas são as três opções que você tem para o DNS (Domain Name System):

1. DNS dividido - As consultas DNS que correspondem aos nomes de domínio são configuradas no Cisco Adaptive Security Appliance (ASA). Eles se movem pelo túnel (para os servidores DNS que estão definidos no ASA, por exemplo) enquanto outros não.

2. Tunnel-all-DNS - Somente o tráfego DNS para os servidores DNS que são definidos pelo ASA é permitido. Essa configuração é definida na política de grupo.

3. DNS padrão - todas as consultas DNS se movem pelos servidores DNS que são definidos pelo ASA. No caso de uma resposta negativa, as consultas DNS também podem ir para os servidores DNS que estão configurados no adaptador físico.

Observação: o comando split-tunnel-all-dns foi implementado pela primeira vez no ASA versão 8.2(5). Antes desta versão, você só podia fazer DNS dividido ou DNS padrão.

Em todos os casos, as consultas DNS que são definidas para se mover pelo túnel, vão para qualquer servidor DNS que são definidos pelo ASA. Se não houver servidores DNS definidos pelo ASA, as configurações de DNS estarão em branco para o túnel. Se você não tiver o DNS dividido definido, todas as consultas DNS serão enviadas aos servidores DNS que são definidos pelo ASA. No entanto, os comportamentos descritos neste documento podem ser diferentes, com base no sistema operacional (SO).

Observação: evite o uso do NSLookup quando você testar a resolução de nomes no cliente. Em vez disso, confie em um navegador ou use o comando ping. Isso ocorre porque o NSLookup não depende do resolvedor DNS do SO. O AnyConnect não força a solicitação DNS por uma determinada interface, mas permite ou rejeita a solicitação dependendo da configuração DNS dividida. Para forçar o resolvedor de DNS a tentar um servidor DNS aceitável para uma solicitação, é importante que o teste de DNS dividido seja executado apenas com aplicativos que dependem do resolvedor de DNS nativo para a resolução de

---

nomes de domínio (todos os aplicativos, exceto NSLookup, Dig e aplicativos semelhantes que lidam com a resolução de DNS sozinhos, por exemplo).

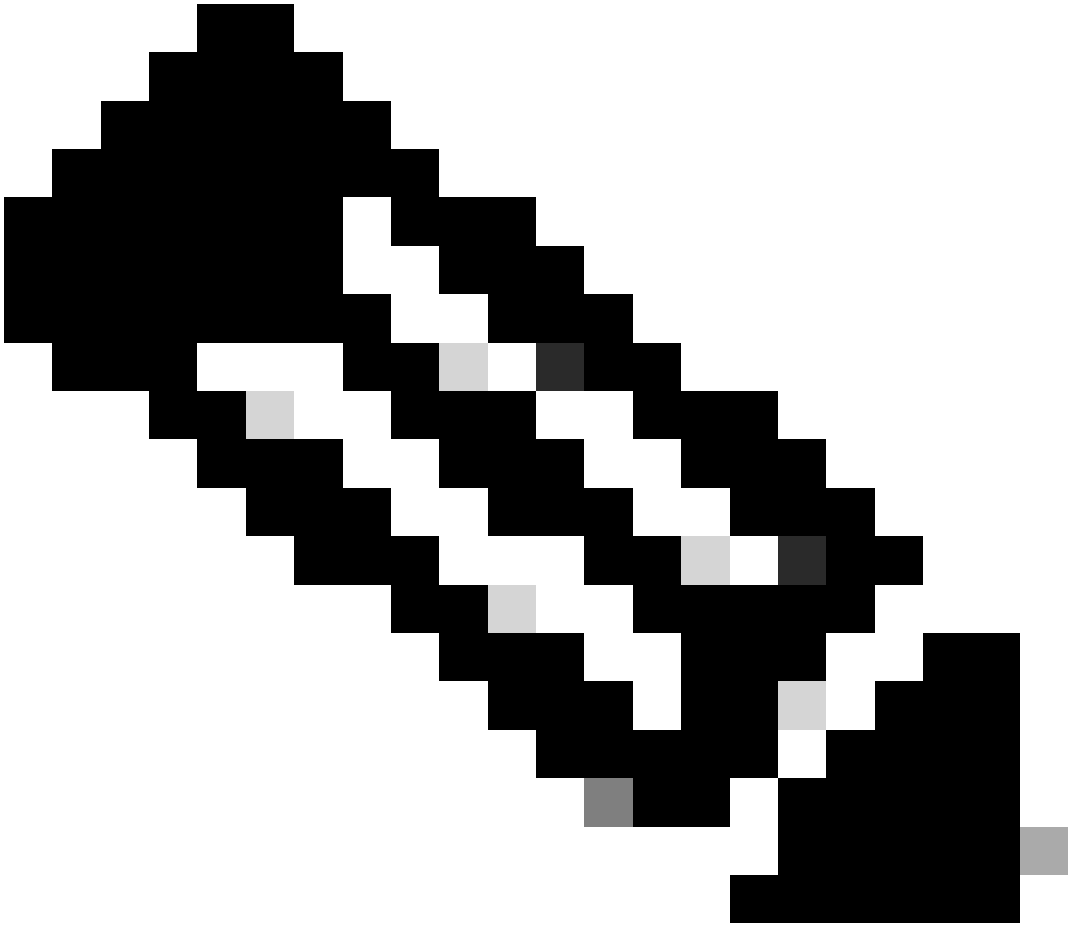
DNS verdadeiro versus DNS dividido por melhor esforço

O AnyConnect Versão 2.4 oferece suporte à split DNS Fallback (melhor esforço split DNS), que não é o DNS dividido verdadeiro e é encontrado no cliente IPsec legado. Se a solicitação corresponder a um domínio DNS dividido, o AnyConnect permitirá que a solicitação seja encapsulada no ASA. Se o servidor não puder resolver o nome do host, o resolvedor DNS continuará e enviará a mesma consulta ao servidor DNS que está mapeado para a interface física.

Por outro lado, se a solicitação não corresponder a nenhum dos domínios DNS divididos, o AnyConnect não a encapsulará no ASA. Em vez disso, ele cria uma resposta de DNS para que o resolvedor de DNS volte e envie a consulta para o servidor DNS que está mapeado para a interface física. É por isso que esse recurso não é chamado de DNS dividido, mas sim fallback de DNS para tunelamento dividido. O AnyConnect não só garante que somente as solicitações direcionadas a domínios DNS divididos sejam encapsuladas, como também depende do comportamento do resolvedor DNS do sistema operacional do cliente para a resolução de nomes de host.

Isso gera preocupações de segurança devido a um possível vazamento de nome de domínio privado. Por exemplo, o cliente DNS nativo pode enviar uma consulta para um nome de domínio privado para um servidor DNS público especificamente quando o servidor de nomes DNS da VPN não pôde resolver a consulta DNS.

Consulte o bug da Cisco ID CSCtn14578, atualmente resolvido somente no Microsoft Windows, a partir da versão 3.0(4235). A solução implementa DNS dividido verdadeiro, ela consulta estritamente os nomes de domínio configurados que correspondem e são permitidos para os servidores DNS VPN. Todas as outras consultas são permitidas somente para outros servidores DNS, como aqueles configurados no(s) adaptador(es) físico(s).



Observação: somente os usuários registrados da Cisco têm acesso às ferramentas e informações internas da Cisco.

DNS de Túnel Total e Túnel Total

Quando o tunelamento dividido está desabilitado (a configuração Tunnel-all), o tráfego DNS é permitido estritamente via túnel. A configuração Tunnel-all DNS (configurada na política de grupo) envia todas as pesquisas de DNS pelo túnel, junto com algum tipo de tunelamento dividido, e o tráfego DNS é permitido estritamente via túnel.

Isso é consistente entre as plataformas com uma advertência no Microsoft Windows: quando qualquer DNS Tunnel-all ou Tunnel-all é configurado, o AnyConnect permite o tráfego DNS estritamente para os servidores DNS que são configurados no gateway seguro (aplicado ao adaptador VPN). Este é um aprimoramento de segurança implementado junto com a solução de DNS dividido real mencionada anteriormente.

Se isso se revelar problemático em determinados cenários (por exemplo, as solicitações de

atualização/registro de DNS devem ser enviadas para servidores DNS não VPN), conclua estas etapas:

1. Se a configuração atual for Tunnel-all, habilite o tunelamento split-exclude . Qualquer rede de host único e com divisão de exclusão é aceitável para uso, como um endereço de link local.

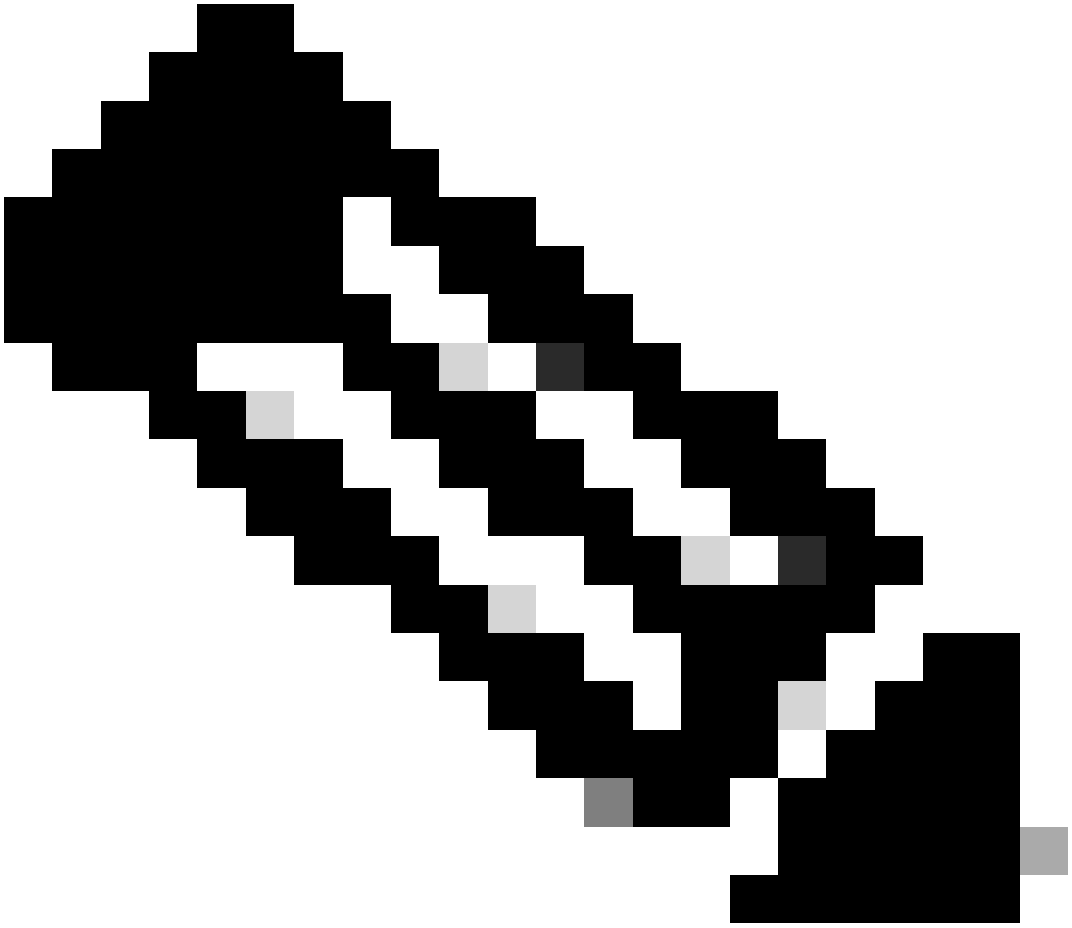
2. Certifique-se de que o DNS Tunnel-all não esteja configurado na política de grupo.

Problema de desempenho de DNS resolvido no AnyConnect versão 3.0(4235)

Esse problema do Microsoft Windows é predominante nas seguintes condições:

- Com a configuração do roteador residencial, os servidores DNS e DHCP recebem o mesmo endereço IP (o AnyConnect cria uma rota necessária para o servidor DHCP).
- Um grande número de domínios DNS está na política de grupo.
- Uma configuração Tunnel-all é usada.
- A resolução de nomes é executada por um nome de host não qualificado, o que implica que o resolvedor deve tentar vários sufixos DNS em todos os servidores DNS disponíveis até que o relevante para o nome de host consultado seja tentado. Esse problema ocorre devido ao cliente DNS nativo que tenta enviar consultas DNS através do adaptador físico, que o AnyConnect bloqueia (dada a configuração Tunnel-all). Isso leva a um atraso na resolução de nomes que pode ser significativo, especialmente se um grande número de sufixos DNS for enviado pelo headend. O cliente DNS deve percorrer todas as consultas e os servidores DNS disponíveis até receber uma resposta positiva.

Esse problema foi resolvido no AnyConnect versão 3.0(4235). Consulte as IDs de bug da Cisco CSCtq02141 e a ID de bug da Cisco CSCtn14578, juntamente com a introdução à solução DNS de divisão real mencionada anteriormente, para obter mais informações.



Observação: somente os usuários registrados da Cisco têm acesso às ferramentas e informações internas da Cisco.

Se uma atualização não puder ser implementada, estas são as possíveis soluções:

- Habilite o tunelamento split-exclude para um endereço IP, o que permite que as solicitações DNS locais fluam pelo adaptador físico. Você pode usar um endereço da sub-rede local de link 169.254.0.0/16 porque é improvável que qualquer dispositivo envie tráfego para um desses endereços IP através da VPN. Depois de habilitar o split-exclude tunnelingd, habilite o acesso à LAN local no perfil do cliente ou no próprio cliente e desabilite o Tunnel-all dDNS.

  No ASA, faça as seguintes 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 também pode ativar isso por cliente na GUI do cliente AnyConnect. Navegue até o menu Preferência do AnyConnect e marque a caixa de seleção Habilitar acesso à LAN local.

- Use os nomes de domínio totalmente qualificados (FQDNs) em vez dos nomes de host não qualificados para as resoluções de nome.
- Use um endereço IP diferente para o servidor DNS na interface física.

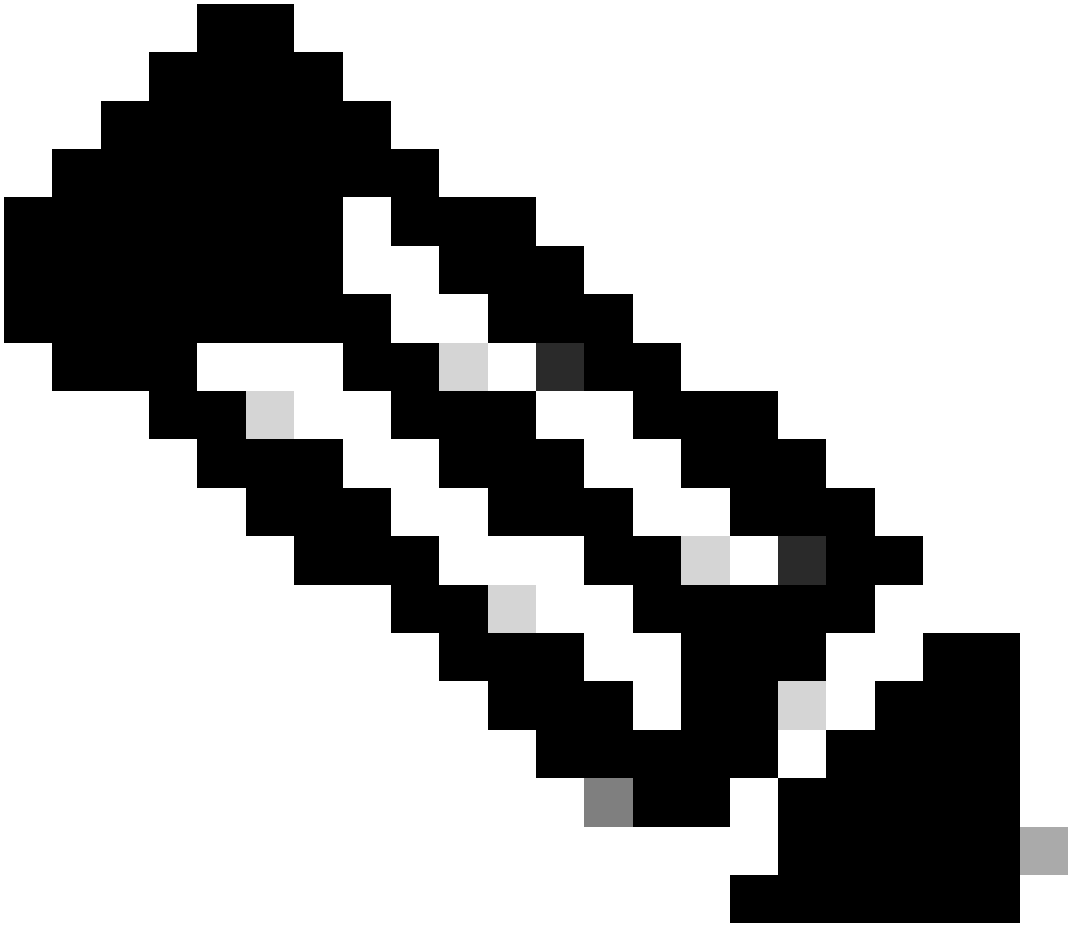
DNS com tunelamento dividido no sistema operacional Cisco diferente

Os diferentes sistemas operacionais da Cisco lidam com pesquisas DNS de maneiras diferentes quando usados com tunelamento dividido (sem DNS dividido) para o AnyConnect. Esta seção descreve essas diferenças.

Microsoft Windows

Em sistemas Microsoft Windows, as configurações DNS são por interface. Se o tunelamento dividido for usado, as consultas de DNS podem retornar aos servidores DNS do adaptador físico depois que eles falharem no adaptador de túnel VPN. Se o tunelamento dividido sem DNS dividido for definido, a resolução de DNS interno e externo funcionará porque ela retornará aos servidores DNS externos.

Houve uma mudança no comportamento no mecanismo DNS que trata disso no AnyConnect para Windows, na versão 4.2 após a correção do bug da Cisco ID CSCuf07885.



Observação: somente os usuários registrados da Cisco têm acesso às ferramentas e informações internas da Cisco.

Windows 7 e posteriores

Configuração de túnel completo (e separação de túneis com DNS de túnel completo habilitado)

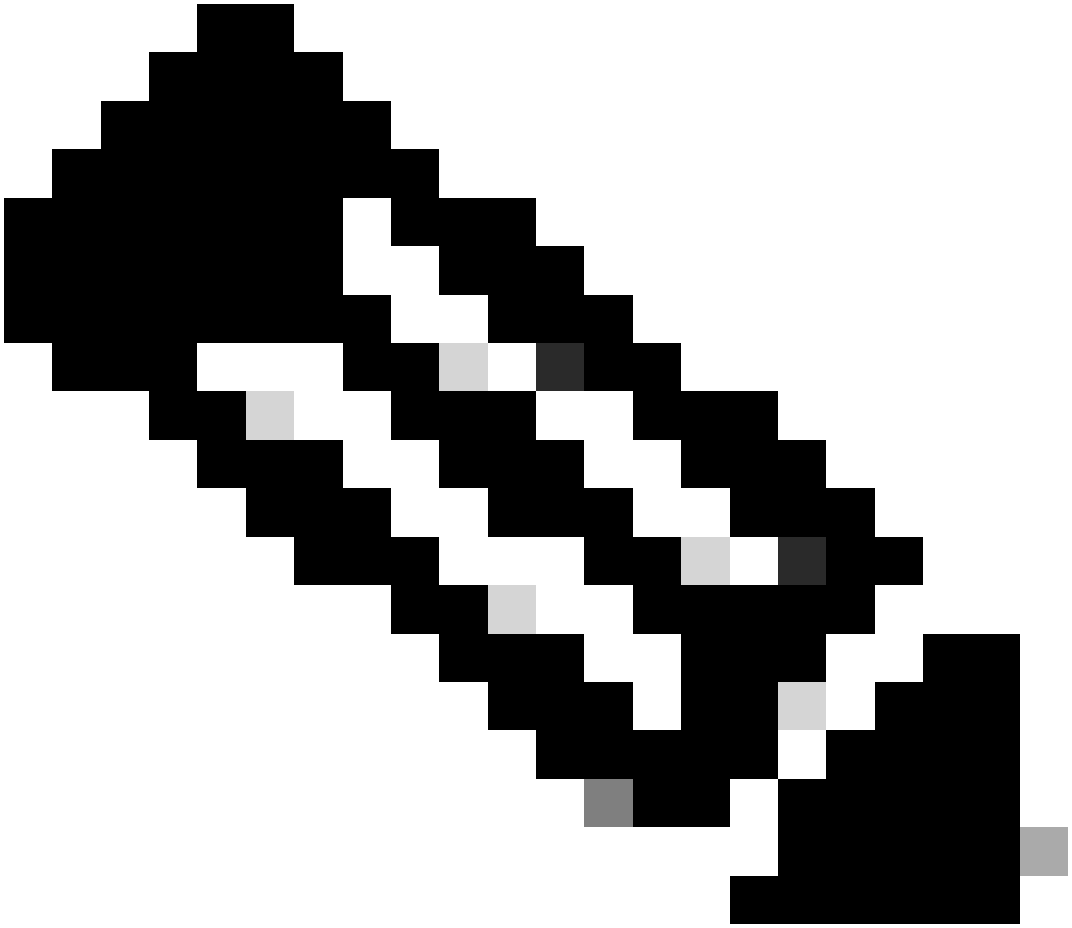
Antes do AnyConnect 4.2:

Somente solicitações DNS para servidores DNS configurados sob a política de grupo (servidores DNS de túnel) são permitidas. O driver do AnyConnect responde a todas as outras solicitações com uma resposta "no such name". Como resultado, a resolução DNS só pode ser executada com os servidores DNS do túnel.

AnyConnect 4.2 +

As solicitações DNS para qualquer servidor DNS são permitidas, desde que tenham origem no adaptador VPN e sejam enviadas pelo túnel. Todas as outras solicitações são respondidas sem esse nome , e a resolução DNS só pode ser executada através do túnel VPN.

Antes da correção do bug da Cisco ID CSCuf07885, o AC restringia os servidores DNS de destino; no entanto, com a correção desse bug, ele agora restringe quais adaptadores de rede podem iniciar solicitações DNS.



> Observação: somente os usuários registrados da Cisco têm acesso às ferramentas e informações internas da Cisco.

Configuração split-include (DNS tunnel-all desabilitado e sem DNS dividido)

O driver do AnyConnect não interfere no resolvedor de DNS nativo. Portanto, a resolução DNS é

executada com base na ordem dos adaptadores de rede em que o AnyConnect é sempre o adaptador preferencial quando a VPN está conectada. Além disso, uma consulta DNS é enviada primeiro pelo túnel e, se não for resolvida, o resolvedor tenta resolvê-la pela interface pública. A lista de acesso split-include inclui a sub-rede que cobre o(s) servidor(es) DNS do túnel. Para começar com o AnyConnect 4.2, as rotas de host para o(s) servidor(es) DNS de túnel são automaticamente adicionadas como redes com divisão de inclusão (rotas seguras) pelo cliente AnyConnect e, portanto, a lista de acesso com divisão de inclusão não exige mais a adição explícita da sub-rede do servidor DNS de túnel.

Configuração split-exclude (DNS de túnel total desabilitado e sem DNS dividido)

O driver do AnyConnect não interfere no resolvedor de DNS nativo. Portanto, a resolução DNS é executada com base na ordem dos adaptadores de rede em que o AnyConnect é sempre o adaptador preferencial quando a VPN está conectada. Além disso, uma consulta DNS é enviada primeiro pelo túnel e, se não for resolvida, o resolvedor tenta resolvê-la pela interface pública. A lista de acesso split-exclude não deve incluir a sub-rede que cobre o(s) servidor(es) DNS de túnel. Para começar com o AnyConnect 4.2, as rotas de host para o(s) servidor(es) DNS de túnel são automaticamente adicionadas como redes com divisão de inclusão (rotas seguras) pelo cliente AnyConnect e, portanto, impedem a configuração incorreta na lista de acesso com divisão de exclusão.

DNS dividido (DNS túnel-tudo desabilitado, split-include configurado)

Pré-AnyConnect 4.2

As solicitações DNS, que correspondem aos domínios split-dns, têm permissão para criar túneis de servidores DNS, mas não para outros servidores DNS. Para evitar que essas consultas de DNS interno vazem para fora do túnel, o driver do AnyConnect responde com "no such name" se a consulta for enviada para outros servidores DNS. Portanto, os domínios split-dns só podem ser resolvidos por meio de servidores DNS de túnel.

As solicitações DNS, que não correspondem aos domínios split-dns, são permitidas para outros servidores DNS, mas não podem criar túneis nos servidores DNS. Mesmo nesse caso, o driver do AnyConnect responde com "no such name" (sem esse nome) se uma consulta para domínios não split-dns for tentada por meio de túnel. Portanto, os domínios não split-dns só podem ser resolvidos por meio de servidores DNS públicos fora do túnel.

AnyConnect 4.2 +

As solicitações DNS, que correspondem aos domínios split-dns, são permitidas a qualquer servidor DNS, desde que se originem do adaptador VPN. Se a consulta for originada pela interface pública, o driver do AnyConnect responde com um "no such name" para forçar o resolvedor a sempre usar o túnel para a resolução de nomes. Portanto, os domínios split-dns só

podem ser resolvidos via túnel.

As solicitações DNS, que não correspondem aos domínios split-dns, são permitidas a qualquer servidor DNS desde que se originem do adaptador físico. Se a consulta for originada pelo adaptador VPN, o AnyConnect responde com "no such name" (sem nome) para forçar o resolvedor a sempre tentar a resolução de nome através da interface pública. Portanto, os domínios não split-dns só podem ser resolvidos por meio da interface pública.

Mac OSx

Em sistemas Macintosh, as configurações DNS são globais. Se o tunelamento dividido for usado, mas o DNS dividido não for usado, não será possível que as consultas DNS acessem os servidores DNS fora do túnel. Você só pode resolver internamente, não externamente.

Isso está documentado na ID de bug da Cisco CSCtf20226 e na ID de bug da Cisco CSCtz86314. Em ambos os casos, essa solução alternativa deve resolver o problema:

- Especifique um endereço IP de servidor DNS externo na política de grupo e use um FQDN para as consultas de DNS interno.

- Se os nomes externos puderem ser resolvidos através do túnel, navegue para Advanced > Split Tunneling e desabilite split DNS através da remoção dos nomes DNS configurados na política de grupo. Isso exige o uso de um FQDN para as consultas de DNS interno.

O caso DNS dividido é resolvido no AnyConnect versão 3.1. No entanto, você deve garantir que uma destas condições seja atendida:

- O DNS dividido deve ser habilitado para ambos os protocolos IP, o que requer o Cisco ASA versão 9.0 ou posterior.

- O DNS dividido deve ser habilitado para um protocolo IP. Se você executar o Cisco ASA versão 9.0 ou posterior, use o protocolo de desvio de cliente para o outro protocolo IP. Por exemplo, certifique-se de que não haja nenhum pool de endereços e que o Client Bypass Protocol esteja habilitado na política de grupo. Como alternativa, se você executar uma versão do ASA anterior à Versão 9.0, certifique-se de que não haja nenhum pool de endereços configurado para o outro protocolo IP. Isso implica que o outro protocolo IP é o IPv6.

Observação: o AnyConnect não altera o arquivo resolv.conf no Macintosh OS X, mas altera as configurações DNS específicas do OS X. O Macintosh OS X mantém o arquivo resolv.conf atualizado por razões de compatibilidade. Use o comando scutil —dns para exibir as configurações DNS no Macintosh OS X.

Configuração de túnel completo (e separação de túneis com DNS de túnel completo habilitado)

Quando o AnyConnect está conectado, somente os servidores DNS de túnel são mantidos na

configuração DNS do sistema e, portanto, as solicitações DNS só podem ser enviadas aos servidores DNS de túnel.

Configuração split-include (DNS tunnel-all desabilitado e sem DNS dividido)

O AnyConnect não interfere no resolvedor de DNS nativo. Os servidores DNS do túnel são configurados como resolvedores preferenciais, que têm precedência sobre os servidores DNS públicos, garantindo assim que a solicitação DNS inicial para uma resolução de nome seja enviada pelo túnel. Como as configurações de DNS são globais no Mac OS X, não é possível para consultas de DNS usar servidores DNS públicos fora do túnel, conforme documentado na ID de bug da Cisco CSCtf20226 . Para começar com o AnyConnect 4.2, as rotas de host para o(s) servidor(es) DNS de túnel são automaticamente adicionadas como redes com divisão de inclusão (rotas seguras) pelo cliente AnyConnect e, portanto, a lista de acesso com divisão de inclusão não exige mais a adição explícita da sub-rede do servidor DNS de túnel.

Configuração split-exclude (DNS de túnel total desabilitado e sem DNS dividido)

O AnyConnect não interfere no resolvedor de DNS nativo. Os servidores DNS do túnel são configurados como resolvedores preferenciais, eles têm precedência sobre os servidores DNS públicos, portanto isso garante que a solicitação DNS inicial para uma resolução de nome seja enviada pelo túnel. Como as configurações de DNS são globais no Mac OS X, não é possível para consultas de DNS usar servidores DNS públicos fora do túnel, conforme documentado na ID de bug da Cisco CSCtf20226 . Para começar com o AnyConnect 4.2, as rotas de host para o(s) servidor(es) DNS de túnel são automaticamente adicionadas como redes com divisão de inclusão (rotas seguras) pelo cliente AnyConnect e, portanto, a lista de acesso com divisão de inclusão não exige mais a adição explícita da sub-rede do servidor DNS de túnel.

DNS dividido (DNS túnel-tudo desabilitado, split-include configurado)

Se o DNS dividido estiver habilitado para ambos os protocolos IP (IPv4 e IPv6) ou estiver habilitado apenas para um protocolo e não houver nenhum pool de endereços configurado para o outro protocolo:
Um split-DNS real, semelhante ao do Windows, é aplicado. O DNS dividido verdadeiro significa que a solicitação que corresponde aos domínios DNS divididos só é resolvida através do túnel, eles não vazam para os servidores DNS fora do túnel.

Se o split-DNS está ativado para apenas um protocolo e um endereço de cliente é atribuído para o outro protocolo, apenas o fallback de DNS para split-tunneling é aplicado. Isso significa que a AC só permite solicitações de DNS que correspondam aos domínios split-DNS via túnel (outras solicitações são respondidas pela AC com resposta "recusada" para forçar o failover para servidores DNS públicos), mas não pode impor a solicitação que corresponde aos domínios split-DNS que não são enviados de forma limpa, através de adaptador público.

Linux

Configuração de túnel completo (e separação de túneis com DNS de túnel completo habilitado)

Quando o AnyConnect está conectado, somente os servidores DNS de túnel são mantidos na configuração DNS do sistema e, portanto, as solicitações DNS só podem ser enviadas aos servidores DNS de túnel.

Configuração split-include (DNS tunnel-all desabilitado e sem DNS dividido)

O AnyConnect não interfere no resolvedor de DNS nativo. Os servidores DNS do túnel são configurados como resolvedores preferenciais, que têm precedência sobre os servidores DNS públicos, garantindo assim que a solicitação DNS inicial para uma resolução de nome seja enviada pelo túnel.

Configuração split-exclude (DNS de túnel total desabilitado e sem DNS dividido)

O AnyConnect não interfere no resolvedor de DNS nativo. Os servidores DNS do túnel são configurados como resolvedores preferenciais, que têm precedência sobre os servidores DNS públicos, garantindo assim que a solicitação DNS inicial para uma resolução de nome seja enviada pelo túnel.

DNS dividido (DNS túnel-tudo desabilitado, split-include configurado)

Se split-DNS estiver habilitado, somente fallback de DNS para split-tunneling será imposto. Isso significa que a AC só permite solicitações de DNS que correspondam aos domínios split-DNS via túnel (outras solicitações são respondidas pela AC com resposta "recusada" para forçar o failover para servidores DNS públicos), mas não pode impor aquela solicitação que corresponde aos domínios split-DNS que não são enviados de forma limpa, através do adaptador público.

iPhone

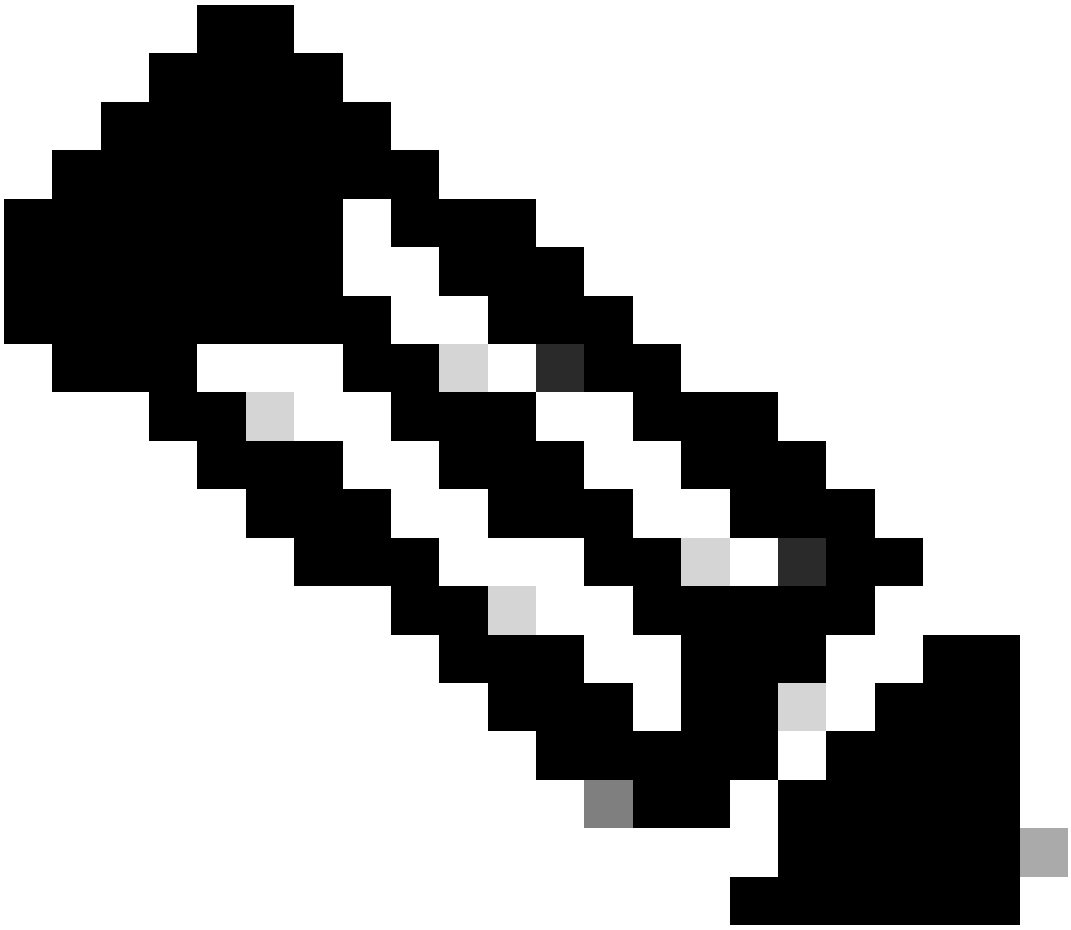
O iPhone é o oposto completo do sistema Macintosh e não é similar ao Microsoft Windows. Se o tunelamento dividido for definido, mas o DNS dividido não for definido, as consultas DNS serão encerradas por meio do servidor DNS global definido. Por exemplo, as entradas de domínio DNS divididas são obrigatórias para resolução interna. Esse comportamento é documentado na ID de bug da Cisco CSCtq09624 e é corrigido na versão 2.5.4038 para o cliente AnyConnect iOS da Apple.

Observação: esteja ciente de que as consultas de DNS do iPhone ignoram .domínios locais. Isso está documentado no bug da Cisco ID CSCts89292. Os engenheiros da Apple

---

confirmam que o problema é causado pela funcionalidade do SO. Este é o comportamento projetado, e a Apple confirma que não há nenhuma mudança para ele.

Informações de bug relacionadas



Observação: somente os usuários registrados da Cisco têm acesso às ferramentas e informações internas da Cisco.

- ID de bug Cisco CSCsv34395 - Adicione suporte no AnyConnect para proxies do FQDN para o servidor DHCP
- ID de bug Cisco CSCtn14578 - AnyConnect para suportar DNS dividido verdadeiro; não fallback
- ID de bug Cisco CSCtq02141 - Problema com o AnyConnect DNS quando o ISP DNS está na mesma sub-rede do IP público

- ID de bug da Cisco CSCtf20226 - Tornar o AnyConnect DNS com comportamento de túnel dividido para Mac igual ao Windows
- ID de bug Cisco CSCtz86314 - Mac: consultas DNS incorretamente não enviadas pelo túnel com DNS dividido
- ID de bug da Cisco CSCtq09624 - Tornar o AnyConnect iPhone DNS com comportamento de tunelamento dividido igual ao do Windows
- ID de bug Cisco CSCts89292 - AC para consultas de DNS do iPhone ignoram domínios .local

Informações Relacionadas

- Firewall Cisco IOS®
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.