

Usuários de Acesso Remoto Incapazes de Acessar Serviços Internos através de RAVPN

Contents

Problema

Os usuários de Acesso Remoto que usam Acesso Seguro não puderam acessar os serviços internos, incluindo o Controlador de Domínio na sede, enquanto o acesso à Internet continuou a funcionar normalmente. Os usuários podem navegar na Internet com êxito, mas não podem acessar recursos internos, como o Controlador de Domínio sobre RAVPN (Remote Access VPN).

Ambiente

- Cisco Secure Access - Acesso remoto seguro ao cliente (VPN, postura, recurso privado)
- Túneis RAVPN (Remote Access VPN) relatados como ativos e íntegros
- Infraestrutura SD-WAN em uso
- Servidores DNS internos na matriz
- Serviços de controlador de domínio no local da matriz
- Várias redes de filiais conectadas através da infraestrutura

Resolução

As seguintes etapas de solução de problemas e solução de problemas foram executadas para solucionar o problema de conectividade do Acesso Remoto:

Passo 1: Análise de captura de pacotes

Colete a Captura de pacotes simultânea do cliente e do seu dispositivo de borda (bidirecional) para analisar padrões de fluxo de tráfego.

Fluxo:

Cliente VPN RA -----túnel Cisco Secure Access -----Ipsec ----- dispositivo de borda ----
-----recurso privado

- Confirme se as consultas DNS dos clientes estavam alcançando com êxito o Dispositivo de Borda e sendo enviadas para o servidor DNS.
- Verifique se nenhuma resposta DNS foi observada retornando do servidor DNS local para os clientes
- O servidor DNS local estava enviando uma resposta, mas essas respostas nunca voltaram para a interface de túnel.

Passo 2: Identificação da causa raiz

Com base na análise de captura de pacotes, o problema foi identificado como um problema de roteamento de caminho de retorno. A análise de tráfego indicou que, embora as consultas DNS estivessem alcançando com êxito o servidor DNS local por meio da infraestrutura do Cisco Secure Access, o tráfego de retorno contendo respostas DNS não estava chegando aos clientes do Remote Access devido a problemas de roteamento ou configuração em sua infraestrutura.

Passo 3: Revisão e correção da configuração

Revisar e corrigir a configuração de rede interna e a configuração de rede externa, com foco especificamente em:

- Configuração DNS e roteamento de tráfego de retorno
- Políticas internas de roteamento para tráfego de retorno de VPN
- Configuração de roteamento de rede interna

- Elementos de configuração ausentes no lado do dispositivo de borda

Passo 4: Verificação da Restauração do Serviço

Após a revisão e as correções da configuração, a funcionalidade do Secure Access foi restaurada em grande parte. A maioria dos usuários de acesso remoto recuperou o acesso aos serviços internos, incluindo o Controlador de Domínio na sede.

Causa

A causa raiz foi identificada como um problema de roteamento do caminho de retorno dentro da infraestrutura de rede interna. Enquanto as consultas DNS dos clientes de Acesso Remoto estavam acessando com êxito o servidor DNS local através da Infraestrutura de Acesso Seguro da Cisco, o tráfego de retorno contendo respostas DNS não foi roteado corretamente de volta para os clientes. Isso foi causado pela configuração ausente ou incorreta no lado da infraestrutura da rede interna que impediu que as respostas DNS e TCP alcançassem os clientes de Acesso Remoto através da conexão VPN.

Conteúdo relacionado

- [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.