O cliente VPN não pode verificar com êxito o erro de modificação da tabela de encaminhamento de IP no cliente seguro RAVPN Split-Tunnel/DNS padrão

Contents

Problema

Os usuários do Mac experimentam falhas intermitentes ao tentar a autenticação CLI para aplicativos internos enquanto estão conectados ao Cisco Secure Client VPN. As falhas são apresentadas como erros "host not found" durante a autenticação CLI e ao usar comandos como `curl`. No entanto, os comandos de resolução DNS como `nslookup` e `dig` são bem-sucedidos. O problema ocorre aleatoriamente e pode ser temporariamente resolvido ao reconectar o VPN, após o qual a conectividade funciona por um curto período antes que o problema ocorra novamente. O VPN de túnel dividido está em uso e o Cisco Umbrella está ativo. O problema não ocorre ao usar o Palo Alto GlobalProtect VPN.

- Mensagem de erro: "host not found" nos comandos de autenticação e `curl` da CLI.
- Mensagem de erro: o cliente VPN não pode verificar com êxito as modificações da tabela de encaminhamento IP. Problema de resolução do servidor de nomes de domínio (DNS) ao conectar recursos privados
- Os comandos `nslookup` e `dig` foram bem-sucedidos
- Conectividade intermitente após reconectar a VPN
- VPN de acesso remoto de túnel dividido e módulo Umbrella ativados
- Problema reproduzível apenas com o Cisco Secure Client VPN em dispositivos MacOS

Ambiente

- Produto: Cisco Secure Client (CSC) com vários módulos
- Plataforma: dispositivos Mac corporativos
- Configuração do perfil de VPN: Perfil de VPN de acesso remoto - Ignorar acesso seguro - Modo de túnel dividido e modo DNS selecionados como "DNS padrão"
- Filtragem de DNS: Cisco Umbrella habilitado
- Versões do módulo:
    - Gerenciamento de nuvem v1.0.0.23
    - AnyConnect VPN v5.1.13.177
    - Guarda-chuva v5.1.13.177
    - DART v5.1.13.177

    - Postura de firewall segura v5.1.13.177
    - Módulo de visibilidade de rede v5.1.13.177
- Dados de diagnóstico: pacotes DART coletados para análise
- Observado apenas no Cisco Secure Client VPN (não no Palo Alto GlobalProtect)

Resolução

- Durante a depuração da configuração de túnel dividido do perfil de VPN (`naic.org`) e da tabela de roteamento do AnyConnect VPN no lado do cliente, esse comportamento foi observado:
    - Cenário de trabalho - Ao executar um `nslookup` para os domínios locais não produzidos do Vault, as solicitações DNS tratadas pelos servidores DNS configurados no perfil VPN resolveram corretamente para endereços 10.x. Da mesma forma, a tabela de roteamento foi atualizada com o IP resolvido (por exemplo, 10.59.130.193) em rotas não seguras.
    - Cenário Não Funcional - No entanto, quando as mesmas solicitações de DNS foram tratadas pelo DNS local do sistema macOS (192.168.x.x) configurado no adaptador untun4 e en0 em vez dos servidores DNS definidos no perfil VPN, esse comportamento foi observado claramente na captura de pacotes enquanto o problema foi observado.
    - os domínios privados resolveram o intervalo de IPs de 34.x.x.x , que levou ao problema de conectividade. A captura do Wireshark ajudou a identificar essa causa raiz subjacente do problema.
- Do ponto de vista do design e da configuração, com uma configuração de perfil VPN de túnel dividido, é recomendável usar DNS dividido em vez de depender de DNS do sistema local/DNS padrão.
- Além disso, a entrada `us-east-eks-amazonaws.com` foi adicionada para garantir que o tráfego desse cluster EKS seja direcionado corretamente através da interface de túnel remoto.
- Também foi discutido que a interface RAVPN deve ter precedência sobre o módulo Umbrella e não deve entrar em conflito com o arquivo `OrgInfo.json` que contém a ID da Organização Umbrella.
- Durante nosso processo de solução de problemas, fizemos uma nova instalação do cliente CSC sem o módulo Umbrella, com esse cenário, não conseguimos ver o problema. Eu também pude rever da perspectiva do Umbrella, o domínio raiz naic.org configurado na lista de domínios internos para ignorar o Umbrella, o que significa que as resoluções de domínio local são encaminhadas para o DNS do sistema configurado do MacOS, não interceptado pelo módulo DNS do Umbrella na interface de loopback no nível do kernel.

Isso se alinha com o problema resolvido quando não há um módulo Umbrella em vigor. Com a configuração de perfil de VPN adequada, incluindo domínios corretos na regra de direcionamento de tráfego e configuração DNS dividida, não devemos ver o problema mesmo com o modelo Umbrella ativado.

O usuário confirmou que o problema foi resolvido depois de modificar o modo DNS para Dividir o túnel e editou a configuração do perfil VPN.

Causa

Perfil de VPN - Ignorar acesso seguro - Modo DNS deve ser definido como Túnel dividido (opções mais comumente vistas de um caso de uso) e incluir todos os domínios de aplicação privada/interna na configuração de DNS dividido para resolver o problema.

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.