Registro de DNS e comportamento de registro de dispositivo com o Cisco Secure Client no iOS para VPN de acesso remoto

Contents

Problema

Ao usar o Cisco Secure Client no iOS (iPad) para estabelecer VPN de acesso remoto com o Cisco Secure Access usando a autenticação SAML via Microsoft Entra ID, os logs DNS não são exibidos no Secure Access após a conexão VPN bem-sucedida, mesmo que os logs de firewall e da Web sejam gerados corretamente. Além disso, o iPad não aparece em Roaming Devices > Mobile Devices no painel Secure Access após estabelecer a conexão VPN.

Os sintomas específicos observados incluem:

- Os registros de acesso remoto mostram eventos de "conexão" bem-sucedidos no Secure Access
- Os logs do firewall e da Web são gerados e exibem a identidade do usuário autenticado SAML
- Os logs DNS estão completamente ausentes do log de acesso seguro
- As informações do dispositivo iPad não são preenchidas na seção de dispositivos móveis de acesso seguro
- Todo o tráfego flui pelo túnel VPN (nenhum tunelamento dividido configurado)

Ambiente

- iPad executando iOS 26.2
- Cisco Secure Client

- Provedor de identidade: ID do Microsoft Entra
- Conector de segurança: Não instalado
- Cisco Secure Access com autenticação SSO configurada
- implementação de autenticação SAML
- Perfil VPN configurado com o modo DNS definido como padrão
- Nenhum tunelamento dividido configurado (todo o tráfego é roteado através da VPN)
- Gerenciamento de dispositivos móveis (MDM) usado para distribuição de perfis

Resolução

O comportamento observado é esperado para a configuração documentada. O Cisco Secure Client no iOS funciona como um cliente VPN (equivalente ao AnyConnect) e não inclui a funcionalidade equivalente ao RSM por padrão. O conector de segurança é o componente equivalente de RSM no iOS que é necessário para preenchimento de identidade de endpoint e controle DNS no estilo Umbrella.

Entendendo a arquitetura

A ausência de registros DNS e registro de dispositivo ocorre porque:

- O Cisco Secure Client fornece conectividade VPN sozinha, mas não tem a funcionalidade de agente de endpoint necessária para visibilidade de DNS
- O conector de segurança (equivalente ao RSM no Windows) é necessário para o controle DNS e o registro de dispositivo no acesso seguro
- Sem o conector de segurança, as consultas de DNS são tratadas pelos servidores DNS obtidos por VPN sem visibilidade do Umbrella/Secure Access

Solução de registro de DNS via Traffic Steering

Para habilitar o registro de DNS sem instalar o conector de segurança, configure a direção de tráfego para direcionar consultas de DNS para servidores DNS Umbrella:

Passo 1: Configurar o tráfego direcionado no acesso seguro

Navegue para Traffic Steering > Add > Add a source e especifique o IP do servidor DNS como uma origem.

Passo 2: Tráfego DNS direto para servidores Umbrella

Configure o perfil VPN para usar servidores DNS Umbrella (208.67.222.222 e 208.67.220.220) para garantir que as consultas DNS sejam visíveis para o Acesso Seguro.

Passo 3: Validar Log DNS

Depois de implementar a configuração de direcionamento de tráfego, os logs DNS devem ficar visíveis no painel de controle de acesso seguro para sessões VPN.

Configuração do Modo DNS do Perfil VPN

A configuração "DNS Mode" (Modo DNS) no perfil VPN não está relacionada à ausência de logs DNS nessa configuração. As sessões RAVPN (Remote Access VPN) usam os servidores DNS obtidos por VPN independentemente dessa configuração, e a visibilidade do registro depende se o tráfego DNS é direcionado à infraestrutura DNS monitorada.

Opção de instalação do conector de segurança

A instalação do Conector de Segurança no iOS habilitará:

- Visibilidade de registro de DNS no Secure Access
- Recursos aprimorados de identidade de endpoint e registro de dispositivo
- Controle e proteção DNS em estilo guarda-chuva

O conector de segurança pode ser usado em conjunto com o cliente seguro, mas a exclusão de

tráfego e as considerações de projeto apropriadas são necessárias para evitar conflitos entre os dois componentes.

Causa

A causa básica é a arquitetura: O Cisco Secure Client no iOS fornece conectividade VPN, mas não inclui a funcionalidade de agente de endpoint necessária para visibilidade de DNS e registro de dispositivo no Secure Access. Essa funcionalidade requer a instalação do conector de segurança ou a configuração de direcionamento de tráfego para direcionar consultas de DNS através da infraestrutura monitorada. Sem esses componentes, as consultas de DNS ignoram o monitoramento de acesso seguro e as informações de identidade do dispositivo não são preenchidas na seção de dispositivos móveis.

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.