Conflitos de resolução de DNS entre o Cisco Secure Access e o aplicativo Banyan Security

Contents

Problema

Quando o Cisco Secure Access é implantado simultaneamente com o aplicativo Banyan Security em endpoints do Windows, os usuários experimentam lentidões e timeouts significativos na resolução de DNS. Os sintomas específicos incluem:

- A resolução DNS começa a expirar quando o Aplicativo de Segurança Banyan está conectado.
- As páginas da Web são carregadas muito lentamente, apesar da resolução.
- O aplicativo Banyan inicia um proxy DNS local em uma interface de loopback, semelhante ao comportamento Umbrella.
- Essa configuração de proxy DNS interfere no comportamento normal de resolução DNS.

O problema afeta especialmente os usuários que devem acessar ambientes externos enquanto o Cisco Secure Access é implantado para a segurança de rede principal.

Ambiente

- Cisco Secure Access implantado com componentes de acesso à Internet (módulo de roaming, VA, DNS, SWG, PAC, IPS, certificados)
- Aplicativo Banyan Security em execução em endpoints do Windows
- Usuários que precisam de acesso a ambientes externos por meio do Banyan, mantendo a conectividade de acesso seguro
- Serviços proxy DNS executados em interfaces de loopback de ambos os aplicativos

- Desvio de domínio interno já configurado no Acesso Seguro para resolução de FQDN

Resolução

Para resolver os conflitos de resolução de DNS entre o Cisco Secure Access e o Banyan Security App, implemente estas abordagens:

Etapas de Resolução Primárias

Este é um bug Cisco ID CSCwr21575 conhecido que trata de conflitos de proxy DNS conhecidos entre o Cisco Secure Access e aplicativos de segurança de terceiros que implementam proxies DNS locais.

Sintoma

A resolução DNS expira ou está significativamente atrasada.

Condições

- Consulta DNS interceptada pelo módulo Cisco Secure Client Umbrella.
- O servidor DNS primário é configurado para um endereço IP do intervalo de loopback 127.0.0.0/8 e a consulta DNS é direcionada a esse servidor.
- Há pelo menos um outro servidor DNS IPv4 sem loopback no mesmo ou em outro adaptador.

Solução

Defina o servidor DNS primário como um endereço IP sem loopback. A correção permanente é atualizar o Cisco Secure Client para 5.1.13 e superior.

Verificação e teste

Após implementar as etapas de resolução, execute esta validação:

- Teste a velocidade da resolução DNS com o Cisco Secure Access e o aplicativo Banyan Security ativos
- Verificar se os tempos de carregamento da página da Web retornam a níveis aceitáveis
- Confirme se o acesso a ambientes externos por meio do Banyan continua a funcionar
- Validar que a resolução de domínio interno por meio do bypass de Acesso Seguro permanece operacional

Causa

A lentidão da resolução de DNS é causada por implementações de proxy de DNS conflitantes entre o Cisco Secure Access e o Banyan Security App. Ambos os aplicativos estabelecem proxies DNS locais em interfaces de loopback, criando caminhos de resolução DNS concorrentes que resultam em tempos limite e respostas atrasadas.

O comportamento do proxy DNS do Aplicativo de Segurança Banyan interfere no tratamento do DNS do Cisco Secure Access, afetando particularmente a ordem e a prioridade do processamento de consultas DNS em endpoints do Windows.

O bug da Cisco ID CSCwr21575 trata desse problema específico de compatibilidade.

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.