Resolução ZTNA DNS de cliente seguro e perda de conectividade após hibernação de macOS

Contents

Problema

O Cisco SecureClient ZTNA em endpoints macOS apresenta falha na resolução de DNS e perda de conectividade ZTA depois que o sistema sai do modo de hibernação ou de suspensão. Esse problema afeta as funcionalidades ZTNA IA (Identity Access) e ZTNA PA (Private Access). Enquanto a conectividade IP básica permanece funcional (ping ICMP para endereços IP externos como 8.8.8.8 e 208.67.222.222 funciona com êxito), a resolução de nome DNS falha completamente, impedindo o acesso a recursos de internet e recursos privados configurados através de ZTNA.

Os sintomas específicos observados incluem:

- As pesquisas de DNS falham ao usar os comandos nslookup (como nslookup de www.cisco.com via 8.8.8.8 e 208.67.222.222 não funciona).
- As conexões ZTNA IA e ZTNA PA ficam indisponíveis.
- O problema ocorre consistentemente após a hibernação do endpoint e os ciclos de ativação.
- O problema também pode ocorrer aleatoriamente enquanto o dispositivo está em uso ativo.
- Eliminar o processo ZTNA resulta em reinicialização imediata, mas o problema de conectividade geralmente persiste.
- Somente uma reinicialização completa do sistema restaura a resolução DNS completa e a conectividade ZTNA.

Ambiente

- Sistema operacional: macOS (versão 26.3 documentada no caso)

- Cisco SecureClient: Versão 5.1.14.x (versões afetadas anteriores à 5.1.16)
- Módulo ZTNA: Ativo com configurações de Acesso de Identidade (IA) e Acesso Privado (PA)
- Monitoração de redes: Pode incluir soluções de segurança de terceiros, como o Sentinel One
- Software de segurança adicional: Pode incluir o Cisco Secure Endpoint
- Servidores DNS: Servidores DNS externos (8.8.8.8, 208.67.222.222) acessíveis via ICMP, mas a resolução DNS falha
- Módulo UMB: Não em uso

Resolução

O problema foi resolvido por meio de uma correção de software fornecida pela Engenharia da Cisco. O processo de resolução envolveu as etapas descritas nas próximas seções.

Passo 1: Identificação de problemas e rastreamento de erros

A Engenharia da Cisco identificou isso como um defeito conhecido e o registrou sob a ID de bug Cisco CSCwt24392 com a descrição "macOS: O DNS para de funcionar com ZTA SIA-all e NVM ative".

Passo 2: Coleta de Dados de Diagnóstico

Essas informações de diagnóstico foram coletadas para suportar a análise de engenharia:

- Pacotes DART (Diagnostic and Reporting Tool, Ferramenta de diagnóstico e geração de relatórios) de endpoints afetados.
- Arquivos de captura de pacote (ZTNA Issue1.pcapng).
- Capturas de tela que demonstram a falha de conectividade.

- Gravações de tela mostrando a reprodução do problema.
- Logs de interação do processo mostrando o comportamento do processo com.cisco.secureclient.zta.app.service e da extensão do sistema.

Passo 3: Desenvolvimento de correções de engenharia

A Cisco Engineering desenvolveu uma correção direcionada para o CSCwt24392 e a incluiu na versão 5.1.16 do SecureClient. A correção aborda especificamente a falha de resolução de DNS que ocorre quando o ZTA SIA-all e o NVM estão ativos em sistemas macOS após ciclos de espera/hibernação.

Passo 4: Instalação de atualização de software

Instale o Cisco SecureClient versão 5.1.16 ou posterior nos endpoints macOS afetados. Esta versão contém a correção para a resolução DNS e problemas de conectividade ZTA.

Passo 5: Teste de validação

Após instalar o SecureClient 5.1.16, execute estas etapas de validação:

1.- Permita que o terminal macOS entre no modo de hibernação ou de suspensão.

2.- Desperte o sistema do estado de suspensão ou hibernação.

3.- Teste a resolução DNS usando os comandos nslookup.

4.- Verifique a conectividade de ZTNA IA e ZTNA PA com os recursos configurados.

5.- Confirme se o acesso à Internet e o acesso a recursos privados funcionam corretamente sem exigir a reinicialização do sistema.

Solução alternativa para versões anteriores

Para ambientes em que a atualização imediata para o SecureClient 5.1.16 não é possível, esta solução temporária pode ser usada:

- Execute uma reinicialização completa do sistema após cada ciclo de suspensão/hibernação para restaurar a resolução DNS e a conectividade ZTNA.
- Considere cancelar o registro da ZTNA temporariamente se o problema de suspensão/hibernação afetar significativamente a produtividade (observe que isso remove a proteção ZTNA).

Causa

A causa raiz desse problema é um defeito de software nas versões do Cisco SecureClient anteriores à 5.1.16, especificamente rastreado como ID de bug Cisco CSCwt24392. O defeito ocorre quando os componentes ZTA (Zero Trust Access) SIA-all (Secure Internet Access) e NVM (Network Visibility Module) estão ativos em sistemas macOS. Durante o ciclo de suspensão ou hibernação e despertar, esses componentes não conseguem restaurar corretamente a funcionalidade de resolução DNS, enquanto mantêm a conectividade IP básica. Isso cria um estado em que o tráfego ICMP (ping) funciona normalmente, mas as consultas de DNS falham, bloqueando efetivamente o acesso a recursos de Internet e recursos privados protegidos por ZTNA. O problema envolve a interação imprópria entre o processo com.cisco.secureclient.zta.app.service e o processo de extensão do sistema durante as transições de estado do sistema.

Conteúdo relacionado

- ID de bug Cisco CSCwt24392 - macOS: O DNS para de funcionar com ZTA SIA-all e NVM ative
- 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.