Falha de confiança SSL/TLS do Secure Client Umbrella Module durante o registro do dispositivo

Contents

Problema

Durante a implantação do Cisco Secure Client com o módulo Umbrella, os dispositivos pararam de sincronizar com o Painel e foram relatados como "Inativos". Os clientes afetados apresentaram falhas de confiança SSL/TLS ao tentar se registrar em devices.api.sse.cisco.com, impedindo o registro bem-sucedido do dispositivo e a cobertura de proteção.

A interface do usuário mostrou o Umbrella como inativo com estas mensagens de status:

- O guarda-chuva está inativo.
- No momento, você não está protegido por um gateway da Web seguro.
- O gateway da Web seguro não está licenciado/está desabilitado.

As descobertas do diagnóstico revelaram uma falha de confiança SSL/TLS consistente durante o registro com esta mensagem de erro nos registros do Secure Client:

```
[ERROR] < 10> Device Registration: Registration failed against https://devices.api.sse.cisco.com/deploy
```

Ambiente

- Cisco Secure Client com implantação de módulo Umbrella em mais de 2.000 endpoints
- Infraestrutura SD-WAN com políticas de rota

- Túneis Umbrella antigos em vigor
- Configuração de rede que permite todos os destinos exigidos por documentação da Cisco
- Nenhuma descriptografia SSL ativa para destinos Cisco no perímetro

Resolução

A resolução envolvia a identificação e correção de um problema de configuração de roteamento que estava fazendo com que o tráfego de registro do dispositivo fosse direcionado incorretamente através de túneis Umbrella legados.

Identificação da causa raiz

A análise dos dados de captura de pacotes revelou que o certificado TLS apresentado para a conexão de API era um certificado Cisco Umbrella em vez do certificado Cisco Secure Access/Let's Encrypt esperado. Identifique o endereço IP para devices.api.sse.cisco.com.

Uma investigação mais profunda identificou uma política de rota SD-WAN que correspondia à sub-rede 146.112.0.0/16, fazendo com que o tráfego para devices.api.sse.cisco.com fosse roteado para túneis Umbrella legados em vez do destino pretendido.

Alterações de configuração

Estas etapas foram executadas para resolver o problema:

- Passo 1: Remova as rotas estáticas problemáticas. As rotas estáticas apontando 146.112.0.0/16 para os túneis Umbrella herdados foram removidas da configuração SD-WAN.
- Passo 2: Valide a conectividade. Após a remoção das rotas estáticas, os clientes afetados foram testados para garantir que conseguissem se conectar e se registrar com êxito em devices.api.sse.cisco.com.

Verificação

A cadeia de certificados esperada para devices.api.sse.cisco.com deve aparecer como mostrado:

```
openssl s_client -connect devices.api.sse.cisco.com:443
CONNECTED(00000003)
depth=2 C = US, O = Internet Security Research Group, CN = ISRG Root X1
verify return:1
depth=1 C = US, O = Let's Encrypt, CN = R13
verify return:1
depth=0 CN = api.sse.cisco.com
verify return:1
---
Certificate chain
 0 s:CN = api.sse.cisco.com
   i:C = US, O = Let's Encrypt, CN = R13
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Mar  5 14:13:56 2026 GMT; NotAfter: Jun  3 14:13:55 2026 GMT
 1 s:C = US, O = Let's Encrypt, CN = R13
   i:C = US, O = Internet Security Research Group, CN = ISRG Root X1
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Mar 13 00:00:00 2024 GMT; NotAfter: Mar 12 23:59:59 2027 GMT
```

Depois de implementar as alterações de configuração, os clientes afetados se conectaram e registraram com êxito e a implantação foi concluída com êxito.

Causa

A causa raiz foi uma política de rota SD-WAN que correspondeu à sub-rede 146.112.0.0/16, fazendo com que o tráfego de registro de dispositivo destinado a devices.api.sse.cisco.com (146.112.59.104) fosse roteado incorretamente através de túneis Umbrella legados. Isso resultou na apresentação de um certificado TLS incorreto (certificado Cisco Umbrella em vez do certificado Cisco Secure Access/Let's Encrypt esperado), levando a falhas de confiança SSL/TLS durante o processo de registro do dispositivo.

Conteúdo relacionado

- Documentação dos requisitos de rede do Cisco Secure Client

- 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.