Solucionar problemas de acesso ao site do Secure Web Gateway SWG

Contents

Introdução

Este documento descreve a metodologia estruturada para diagnosticar problemas de acesso ao site quando roteado por meio de um proxy baseado em nuvem (Secure Web Gateway/SWG), mas não quando se usa o Direct Internet Access (DIA).

- Escopo: Aplica-se ao Cisco Umbrella SIG e ao Cisco Secure Access.

Pré-requisitos e avisos importantes

- Verifique se toda a solução de problemas é executada em problemas reproduzíveis.
- Colete um arquivo HAR (Arquivo HTTP) e uma Captura de Pacotes simultânea (PCAP) para fornecer dados precisos para análise.
- Alterações nas políticas de proxy (por exemplo, contornar a descriptografia ou a inspeção) podem afetar a postura de segurança; se aplica somente à solução de problemas ou conforme recomendado.

Identificar erros em nível de proxy

Os indicadores comuns de interferência de proxy incluem:

- 502 Gateway com problema
- 515 Certificado de Upstream Não Confiável
- 517 Certificado Upstream Revogado
- 403 Proibido
- Certificados revogados
- Incompatibilidade do conjunto de cifras
- Tempos limite de conexão do site

Metodologia de Troubleshooting

Passo 1: Confirmar se o tráfego atravessa o proxy

- Levantamento de dados: Gere um arquivo HAR e um PCAP quando o problema ocorrer.
- Análise de cabeçalho: Inspecione o cabeçalho Via nas respostas HTTP. A presença de `s_proxy` (proxy Nginx) ou `m_proxy` (Serviço de Proxy Modular/MPS) confirma que o tráfego está com proxy aplicado.
- Fluxo TCP: No Wireshark, siga o fluxo TCP para garantir que a conexão seja com o IP do proxy, não com o IP de destino.

Passo 2: Verificar o status da descriptografia TLS

- Inspeção do navegador: Clique no ícone de cadeado na barra de endereços do navegador. Se o Certificado raiz de acesso seguro da Cisco for exibido na cadeia de certificados, a inspeção HTTPS estará ativa.
- Validação: Faça referência cruzada dos cabeçalhos Via em arquivos HAR/PCAP.
- Comando do OpenSSL: Para inspecionar cadeias de certificados:
  `openssl s_client -connect www.example.com:443 -showcerts`
  Este comando verifica a cadeia de certificados apresentada pelo servidor. Execute-o em uma máquina que atravessa o proxy para validação direta.

Passo 3: Isolamento e processo de eliminação

1. Fase A - Testar a inspeção HTTPS (camada Nginx):
   - Adicione o domínio problemático à lista "Do Not Decrypt" do SWG.
   - Manter Inspeção de Arquivo habilitada.
   - Se o problema for resolvido: A causa raiz provavelmente é a inspeção Nginx SSL/TLS. Analise o PCAP quanto a incompatibilidades de cifra ou problemas de SNI. Use `curl` com e sem proxy para comparar o comportamento.
   - Se o problema persistir: Continue na Fase B.
2. Fase B - Testar a inspeção do arquivo (camada de digitalização):
   - Desabilite a Inspeção de Arquivo para o tráfego específico.
   - Se o problema for resolvido: A causa raiz está no mecanismo de varredura de arquivos. Reveja o PCAP e o HAR, reproduza-o no laboratório e determine se um arquivo específico ou assinatura de varredura causa o problema.
   - Se não for resolvido: entre em contato com o suporte com registros e descobertas abrangentes.

Problemas comuns e códigos de erro

515 Certificado de Upstream Não Confiável

Esse erro ocorre quando o proxy SWG não pode validar o certificado do servidor de destino. As causas incluem cadeias de certificados expiradas, autoassinadas ou incompletas.

- Inspeção HTTPS ATIVADA + Inspeção de Arquivo ATIVADA: Trabalhos em sítios Web; nenhum erro de certificado.
- Inspeção HTTPS ATIVADA + Inspeção de Arquivo DESATIVADA: erro 515 observado, relatório de usuário correspondente.
- Inspeção HTTPS DESATIVADA + Inspeção de arquivo DESATIVADA (domínio na lista Não descriptografar): Nenhum problema foi observado.

Detalhes técnicos: O proxy Nginx poderá falhar se o servidor upstream depender da busca de AIA (Authority Information Access) para certificados intermediários ausentes, já que o Nginx não lida com o AIA de forma tão harmoniosa quanto o serviço proxy de verificação de arquivos. As incompatibilidades de SNI e SAN durante o handshake TLS também podem acionar falhas.

517 Certificado Upstream Revogado

O erro 517 significa que a verificação de CRL ou OCSP do proxy SWG detectou que o certificado do servidor upstream foi revogado.

- Troubleshooting: Use ferramentas externas, como SSL Labs ou OpenSSL para confirmar o status de revogação.
- Documentação:
  - Erro 517 de solução de problemas da Cisco - Certificado de upstream revogado
  - Entender erros comuns de certificado e protocolo

Opções de Tratamento de Erros de Certificado

O Cisco Secure Access introduzirá um novo recurso chamado "Opções de tratamento de erro de certificado" para desvio de erro granular sem desabilitar totalmente a descriptografia. Os domínios que disparam erros de certificado devido à inspeção podem ser gerenciados usando esse recurso, em vez de listas amplas de "Não descriptografar".
Esta característica existe no Umbrella SIG a partir de hoje. Detalhes de solicitações de recurso para CSA.

502 Gateway com problema

O erro 502 indica que o proxy SWG recebeu uma resposta inválida do servidor upstream enquanto atuava como um intermediário.

-Downstream: Cliente para proxy SWG
-Upstream: Proxy SWG para servidor de destino

O erro está sempre na conexão upstream—devido a erros de protocolo, reinicializações de TCP ou cabeçalhos malformados.

Causas 502 Comuns

- Conjuntos de criptografia SWG sem suporte
- Solicitação de Autenticação de Certificado de Cliente
- Cabeçalhos adicionados pelo proxy SWG

Conjuntos de Cifras sem Suporte

Causa: O servidor requer uma cifra não suportada pelo SWG (por exemplo, TLS_CHACHA20_POLY1305_SHA256).
Resolução: Adicione o domínio à lista Descriptografia seletiva.

Testando comandos:
Com proxy:

```
curl -x proxy.sig.umbrella.com:80 -v xyz.com:80
curl -x swg-url-proxy-https.sigproxy.qq.opendns.com:443 -vv -k "https://www.cnn.com" >> nulo
```

Sem proxy:

```
curl -v www.xyz.com:80
```

Mac/Linux:

```
curl -vv -o /dev/null -k -L www.cnn.com
```

Windows:

```
curl -vv -o null -k -L www.cnn.com
```

Solicitação de Autenticação de Certificado de Cliente

Causa: O servidor upstream requer certificados do lado do cliente, que o SWG não suporta.
Resolução: Ignore o domínio do proxy usando a lista de gerenciamento de Domínios externos (Umbrella SIG) ou Ignore o proxy seguro (Cisco Secure Access). Ignorar a inspeção HTTPS sozinha é insuficiente.

Cabeçalhos adicionados por proxy

Causa: Alguns servidores rejeitam solicitações com o cabeçalho X-Forwarded-For (XFF) adicionado pelo SWG quando a inspeção HTTPS está habilitada.
Resolução: Comparar o comportamento com/sem HTTPS e inspeção de arquivos. Se o erro ocorrer somente quando XFF estiver presente, o servidor Web provavelmente está configurado incorretamente.

Exemplo:
`curl https://www.xyz.com -k – header 'X-Forwarded-For: 1.1.1.1' -o /dev/null -w "Código de Status: %{http_code}" -s`
Código de status: 502
`curl https://www.xyz.com -k -o /dev/null -w "Código de Status: %{http_code}" -s`
Código de status: 200

O cabeçalho XFF é adicionado para geolocalização. Se o servidor não puder processá-lo, ocorrerá um erro 502.

PUA potencialmente indesejado ou arquivos corrompidos

Se o SWG não puder examinar um arquivo usando a inspeção de arquivos (por exemplo, arquivos protegidos, solicitados por intervalo ou corrompidos), ele bloqueará o download e os relatórios - Bloqueado - Aplicativo potencialmente indesejado (Arquivo protegido)

- Troubleshooting: Capturar um HAR durante o evento de bloqueio. Use Substituir segurança como uma solução temporária. Se o arquivo estiver corrompido ou for mal-intencionado, ele deverá ser corrigido na origem.

Categorias e blocos de reputação potencialmente prejudiciais

- Use o Talos para verificar a reputação da Web (WBRS). Se um domínio for categorizado incorretamente, envie uma solicitação COG Jira ao Talos para revisão. Talos categorizados como seguros ou favoráveis, mas ainda bloco SWG, então precisamos verificar a partir do serviço Beaker do SWG.

Acesso negado pela Akamai para IPs de saída SWG

- O SWG usa IPs de saída compartilhados. Se eles estiverem na lista negra dos serviços de reputação de IP (por exemplo, Brightcloud), o acesso a determinados sites poderá ser negado.

Problemas conhecidos: Inicialização de Entrada do Youtube e Vídeo Indisponível

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.