Solucionar problemas de acesso ao site SWG

Contents

Introdução

Este documento descreve como solucionar problemas de acesso ao site vistos com o Umbrella Secure Web gateway (SWG) Proxy.

Informações de Apoio

Vamos supor que o site www.xyz.com não está acessível através do proxy SWG e quando os usuários tentam acessar a Internet diretamente (sem Umbrella SWG estar na imagem), funciona bem. Vamos analisar vários sintomas e diferentes tipos de mensagens de erro relatadas quando o site está inacessível via SWG. Os mais comuns são 502 gateway inválido, 502 não pôde retransmitir mensagem de erro de upstream, certificado de upstream revogado, acesso negado 403 proibido, incompatibilidade de cifras de upstream, o site atingiu o tempo limite após girar por algum tempo ou semelhante.

Erro "Acesso Negado 403" Devido ao Bloco Upstream

O servidor Web ou o lado upstream está bloqueando ou limitando os intervalos IP de saída do proxy SWG. Por exemplo, o Akamai WAF tem bloqueio listado alguns intervalos de IP de saída SWG. Para resolver esse problema, a única opção é entrar em contato com os administradores do site e pedir que eles desbloqueiem nossos intervalos de IP. Até lá, ignore o SWG usando a lista de gerenciamento de domínios externos para implantações de arquivos SWG e PAC do Anyconnect. Resumindo, esse tipo de problema não ocorre devido ao proxy em si, mas devido à incompatibilidade entre servidores proxy e Web. Este é o link para consultar o KB

especificamente sobre o erro "Access Denied 403" devido ao bloco do Egress IP.

Além disso, aqui está o link que cobre algumas razões possíveis pelas quais a Akamai bloqueou os endereços IP listados.

Erro "Acesso negado 403" devido a problema com Java

O site não está acessível e lançando "Acesso Negado ou 403 Proibido - Erro de gateway de segurança de nuvem Umbrella" quando a solicitação é enviada através do proxy MPS SWG com a configuração de inspeção de arquivo ativada. Mas se a Inspeção de arquivos estiver desativada, os sites serão carregados com êxito. Ou se colocarmos o site em descriptografia de desvio, sites são carregados com sucesso.

Causa básica do problema de alto nível

Qual é o problema relacionado ao Java com o MPS?

O site ou servidor Web em questão retorna um aviso TLS com relação a um alerta SNI ou SSL para o proxy depois que o proxy tenta se conectar ao servidor. Basicamente, isso acontece depois que o hello do cliente é enviado. Proxy MPS (que é baseado em Java e como tal) por design, ele trata todos os alertas TLS com "Nome não reconhecido" no campo de descrição como um erro durante a análise SNI e termina a transação. Mais detalhes encontrados aqui

Esteja ciente de que esse não é um problema de proxy SWG ou MPS. Essa é uma das incompatibilidades com o SWG ou com qualquer outro proxies devido à configuração incorreta no lado do servidor. Os navegadores normalmente ignoram esse aviso, mas o SWG ou outro filtro de segurança de conteúdo trata o aviso SSL como um erro fatal e encerra a sessão, o que resulta em 403 páginas de erro proibido para os usuários. Ele também pode relatar o erro 502 de Gateway Incorreto, mas com a maioria dos exemplos, o que vimos foi o erro 403 proibido, como mostrado nesta imagem.

Como o MPS funciona na camada de aplicação, ele tem pouco ou nenhum controle sobre como a camada TLS trata a transação com base nos alertas produzidos no protocolo TLS. É responsabilidade do servidor garantir que seus pontos de extremidade/certificados TLS sejam configurados corretamente. Consulte este link.

Para restringir ou solucionar o problema, ele pode ser facilmente apontado no laboratório SSL.

15152060146964

Quando o site é acessado sem o proxy SWG no meio ou ignora a inspeção HTTPS do SWG, o site funciona porque o navegador está ignorando o alerta de nome SNI não reconhecido e continua se comunicando com o servidor Web.

No momento em que este artigo foi escrito, a solução recomendada é a melhor atenuação que podemos sugerir a você. Em um futuro próximo, com a nova arquitetura de proxy, poderemos lidar com esses problemas de forma mais harmoniosa.

Resolução

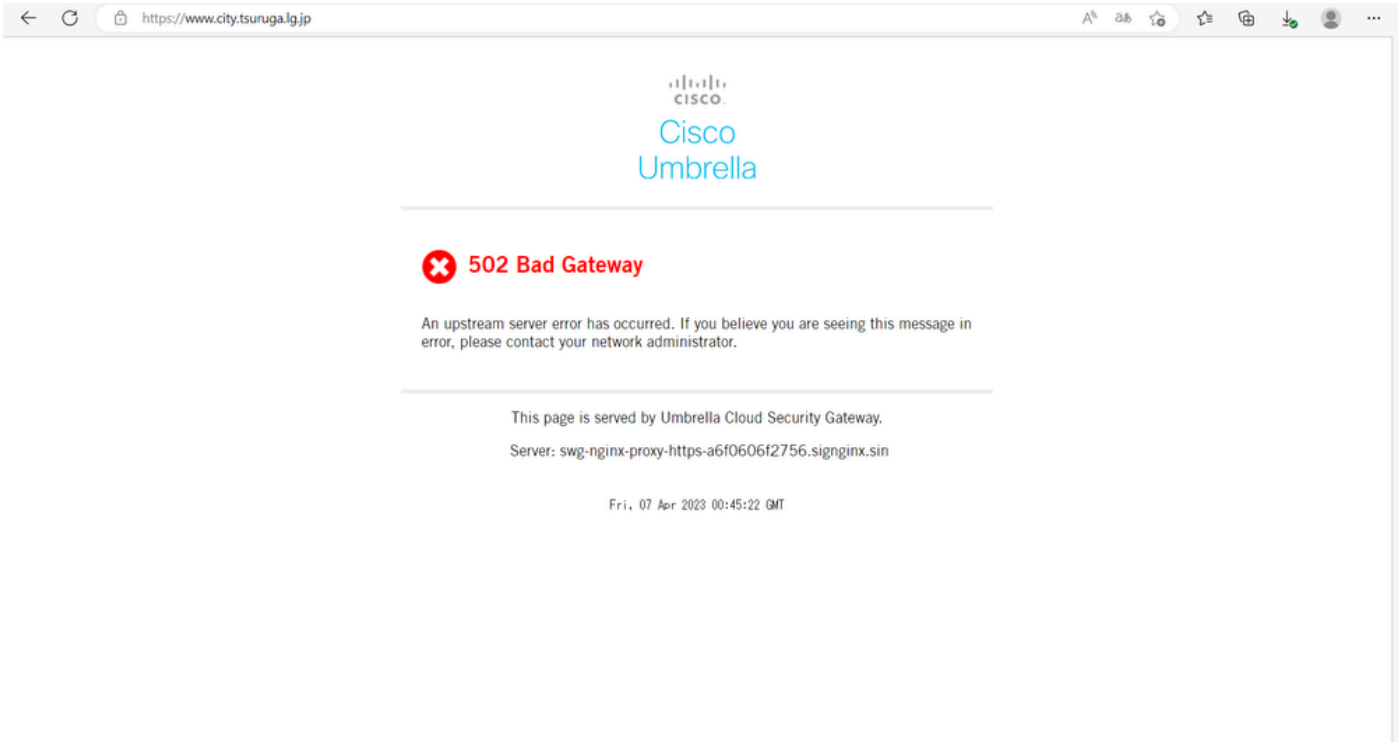
1. Desabilitar Descriptografia para os domínios afetados - OU
2. Adicione o domínio a uma lista de destino e associe uma regra de permissão (se você confiar no site)

O que é gateway incorreto 502?

Um erro de gateway incorreto 502 significa que o servidor estava agindo como um gateway ou proxy e recebeu uma resposta inválida do servidor upstream. Quando o usuário tenta acessar o site via proxy SWG, dois fluxos de comunicação ocorrem.

a) Cliente —> Conexão proxy (downstream)
b) Proxy—> Encerrar conexão do servidor Web (Upstream)

502 Erro de gateway incorreto entre o proxy SWG (MPS, Nginx) e a conexão do servidor final.



15026978020884

Fatores Comuns para Gateway 502 Ruim

1. Conjuntos de Cifras SWG sem Suporte

2. Solicitação de Autenticação de Certificado de Cliente

3. Cabeçalhos Adicionados ou Removidos pelo Proxy SWG

Conjuntos de criptografia SWG sem suporte

Vamos supor que um servidor Web informe pacotes de cifra SWG não suportados durante a negociação TLS. Observe que o proxy SWG MPS (Modular Proxy Service) não oferece suporte ao conjunto de cifras TLS_CHACHA20_POLY1305_SHA256. Esteja ciente de que há um artigo separado para abordar conjuntos de cifras e TLS suportados pelo SWG. Podemos identificar facilmente esse problema revisando outros pacotes capturados durante a troca de pacotes de codificação no hello do cliente e no hello do servidor. Como uma etapa de Troubleshooting, utilize o comando CURL que impõe o uso de cifras específicas para restringir o problema e confirmar se ele se deve a conjuntos de cifras, como mostrado nos exemplos 1 e 2.

Exemplo de Comandos Curl:

<#root>

```
curl -vvv "" --ciphers TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 >> /dev/null
curl -vvv "" --ciphers ECDHE-RSA-AES256-GCM-SHA384 >> /dev/null
```

Testing website With Proxy:

```
 - curl -x  proxy.sig.umbrella.com:80 -v  xyz.com:80
```

```
curl -x swg-url-proxy-https.sigproxy.qq.opendns.com:443 -vvv -k "https://www.cnn.com" >> null
```

Testing website without Proxy

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

Mac/Linux:

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

Windows:

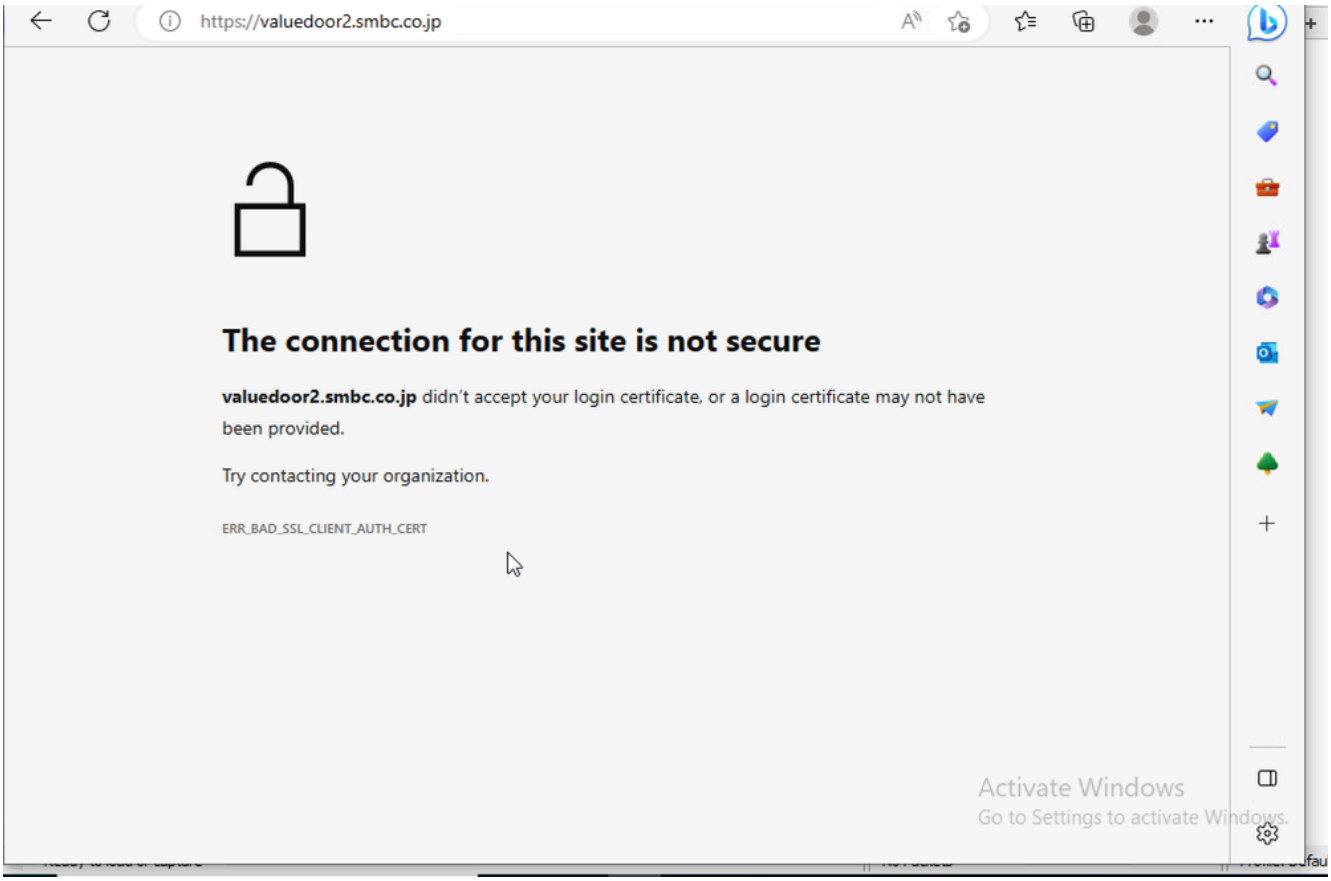
```
 - curl -vvv -o null -k -L www.cnn.com
```

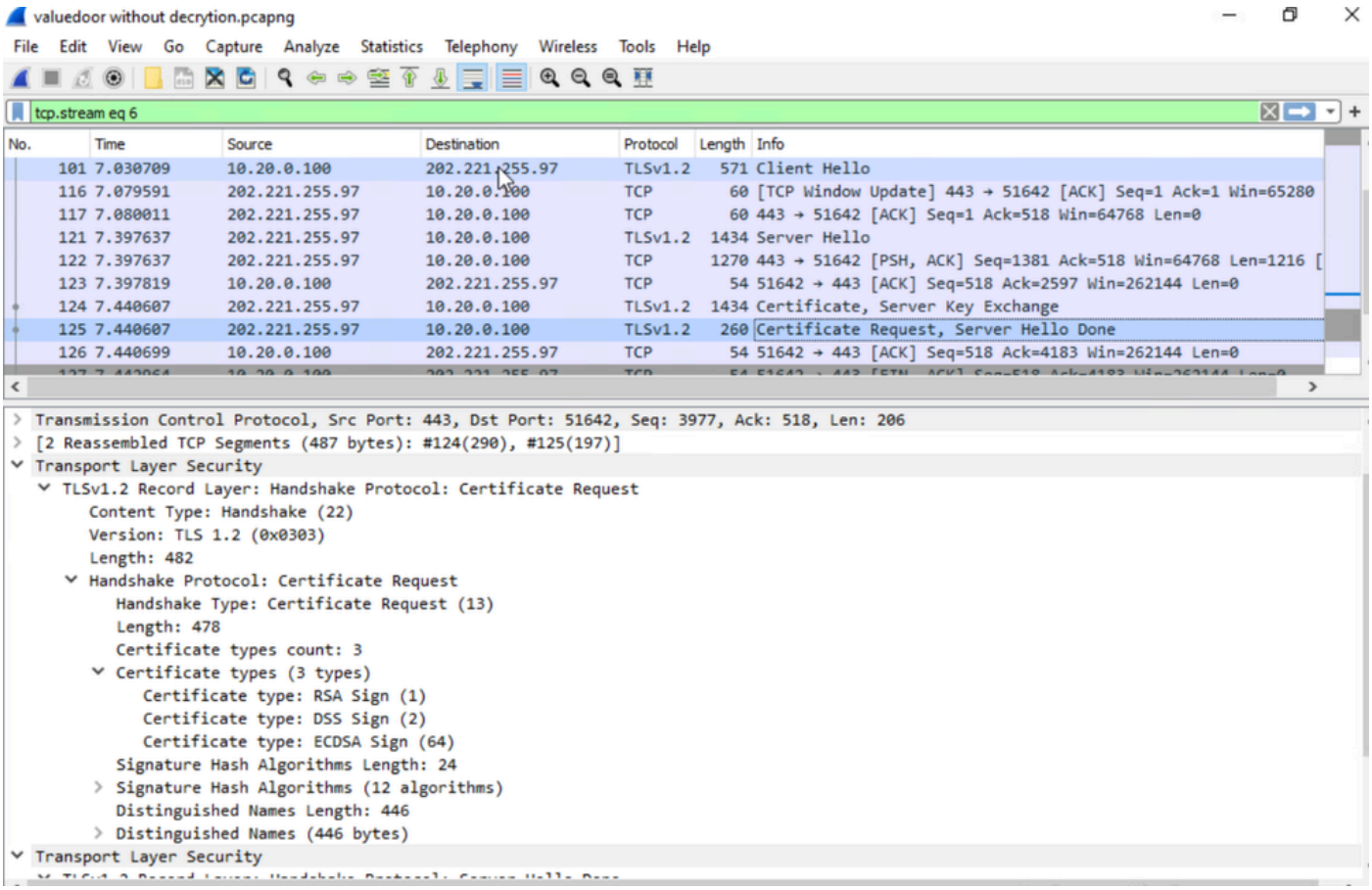
Resolução

Para resolver o problema, ignore a inspeção do site problemático usando a lista de descriptografia seletiva.

Solicitação de Autenticação de Certificado de Cliente

Durante o handshake TLS entre o proxy SWG e o upstream, o servidor web upstream espera a autenticação do certificado do cliente. Como a autenticação de certificado de cliente não é suportada, precisamos ignorar esses domínios do proxy usando a lista de gerenciamento de domínios externos, e ignorar apenas a inspeção https não é suficiente. Por exemplo: https://valuedoor2.smbc.co.jp.

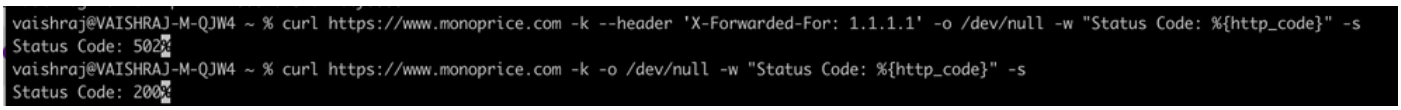




15027192992276

Cabeçalhos adicionados por proxy

O servidor Web está relatando um erro de gateway incorreto 502 devido ao cabeçalho X-Forward-For (XFF) adicionado pelo proxy SWG quando a inspeção https está habilitada. Podemos restringir facilmente a maioria dos 502 problemas de gateway inválido primeiro solucionando o problema com ou sem inspeção https e com ou sem inspeção de arquivo para descartar o problema de varredura de arquivos com o Proxy MPS.



15123666760340

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

Usamos o cabeçalho XFF quando a inspeção HTTPS é ativada, para que o servidor upstream possa fornecer conteúdo de localização geográfica ideal com base no IP do cliente (que fornece a localização física do usuário).

Quando a inspeção de HTTPS não está habilitada, esse cabeçalho não é adicionado pelo proxy, portanto não há um erro de Gateway Incorreto 502. Esse não é um problema de proxy do SWG . Este erro ocorre devido ao servidor Web upstream que está configurado incorretamente para não suportar o cabeçalho XFF padrão.

Resolução

Para resolver o problema, ignore a inspeção de HTTPS para domínios específicos usando listas de descriptografia seletivas.

- 517 Certificado Upstream Revogado
- Erros de certificado e protocolo TLS
- Selecionar SWG DC manualmente para teste interno

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.