Erro Do Secure Access 502 Para Sites De Bancos Após A Autenticação

Contents

Problema

Os usuários relataram o recebimento de um código de erro 502 de HTTP de gateway inválido após a autenticação bem-sucedida no FCBanking. O processo de autenticação foi concluído com êxito, permitindo que os usuários digitem suas credenciais de login. No entanto, o navegador exibiu um erro de gateway incorreto 502 imediatamente após a autenticação.

O domínio do FCBanking e sua categoria relevante estavam isentos da descriptografia SSL e IPS e esta alteração de configuração não resolveu o erro HTTP 502. O problema ocorreu intermitentemente e só foi resolvido depois que o acesso seguro para o domínio FCBanking foi ignorado. A análise do arquivo HAR revelou 502 erros no destino para 'my.fcbanking.com' e os logs de pesquisa de atividades não mostraram os 502 erros que foram capturados no arquivo HAR, indicando que esses erros estavam ocorrendo em um nível de dispositivo intermediário.

Ambiente

- Cisco Secure Access - Acesso à Internet (Módulo de roaming, VA, DNS, SWG, PAC, IPS, Certificados)
- Topologia de rede: PC do usuário > Switch > Roteador Catalyst SD-WAN > Internet local ou túnel CSA
- Borda Catalyst SD-WAN configurada com regra de política de aplicativo para enviar todo o tráfego nas portas 80 e 443 através do acesso direto à Internet (DIA) ignorando o grupo de túnel de rede (NTG)
- O Cisco Secure Client depende de uma lista de desvio para determinar o roteamento de tráfego para o Secure Access
- Domínio bancário: fcbanking.com e subdomínios associados (my.fcbanking.com, treasury.fcbanking.com)

Resolução

A resolução primária envolve adicionar o domínio bancário para ignorar totalmente o acesso seguro, permitindo que o tráfego flua diretamente para a Internet enquanto mantém a segurança da camada DNS.

Passo 1: Adicionar domínio primário à lista de desvio

- Adicione fcbanking.com à lista bypass proxy only na configuração Secure Access. Isso garante que o tráfego da Web ignore o proxy de Acesso Seguro, enquanto a segurança da camada DNS permanece imposta e registrada na Pesquisa de Atividade.

Passo 2: Identificar e adicionar aliases de domínio

- Os sites bancários geralmente usam vários aliases que também devem ser adicionados à lista de desvio. Use a Verificação de Cache para identificar todos os aliases para o domínio bancário.
- Para fcbanking.com, esses aliases foram identificados e adicionados à lista de desvio:
    - treasury.fcbanking.com (também conhecido por: treasuryvanity.jackhenry.com)
    - my.fcbanking.com (também conhecido por: banno-online.jackhenry.bank)
    - treasuryvanity.jackhenry.com
    - banno-online.jackhenry.bank

Passo 3: Resolução alternativa usando endereços IP

- Como uma alternativa ao desvio baseado em domínio, os endereços IP resolvidos dos sites bancários podem ser adicionados à lista de desvio. O Cisco Secure Client converte os FQDNs encontrados na lista de desvio para endereços IP e roteia o tráfego da Web diretamente para a Internet.

Passo 4: Habilitar Log de Depuração para Solução de Problemas

- Para capturar logs detalhados para análise adicional, ative o log máximo de depuração:
- Crie um arquivo chamado 'SWGConfigOverride.json' com este conteúdo:

```
{"logLevel": "1"}
```

Coloque o arquivo SWGConfigOverride.json na pasta SWG:

```
C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\SWG\
```

Reinicie o serviço SWG ou Umbrella ou reinicie o sistema para aplicar a configuração de log de depuração.


Note: O log de depuração não afeta o desempenho do sistema, mas pode aumentar o tamanho do arquivo de log. Remova o arquivo SWGConfigOverride.json depois de obter o pacote DART para retornar aos níveis normais de registro em log.

Passo 5: Verificação

- Depois de implementar a configuração de desvio, os usuários não relataram mais nenhum erro 502 ao acessar o site bancário. O tráfego DNS continua a ser registrado na Pesquisa de atividades enquanto o tráfego da Web flui diretamente para a Internet.

Causa

Os sites bancários normalmente implementam medidas de segurança que detectam e bloqueiam o tráfego originado de servidores proxy ou intervalos de endereços IP compartilhados. O Cisco Secure Access usa intervalos de IP compartilhados (151.186.144.0/20 e 151.186.176.0/20) para tráfego proxy, que os sites bancários podem detectar e silenciosamente descartar ou responder com erros HTTP 502.

Quando os domínios são colocados na lista não descriptografar, o IP de origem ainda parece se originar do intervalo de IP compartilhado de acesso seguro, acionando os mecanismos de segurança do site bancário. Além disso, a inspeção de IPS no tráfego bancário e nos aliases de domínio que não estão devidamente isentos pode contribuir para falhas de conexão. A natureza intermitente desse problema e os erros 502 que aparecem nos arquivos HAR, mas não nos logs de pesquisa de atividades, indicam que os erros foram gerados pelo processamento de proxy intermediário em vez dos servidores bancários de destino.

Conteúdo relacionado

- Solucionar problemas de acesso ao site SWG
- Desabilite o protocolo QUIC para garantir a inspeção adequada do tráfego da Web
- Documentação de Intervalos IP de Acesso Seguro da Cisco
- 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.