Problema de Verificação de Integridade do Proxy de Upstream do WSA após Interrupção da Rede

Contents

Problema

Após uma interrupção prolongada da rede, um Cisco Web Security Appliance (WSA) configurado para usar um proxy de upstream especificado pelo FQDN pode falhar em retomar o tráfego de encaminhamento para um proxy de upstream e enviar o tráfego diretamente. Esse problema se manifesta quando o WSA marca o proxy de upstream como "inativo" durante a interrupção da rede, mas não reconhece quando o proxy de upstream se torna disponível novamente, mesmo depois que a conectividade de rede é restaurada.

Os sintomas específicos observados incluem:

- WSA configurado com proxy de upstream via FQDN e "Tratamento de falhas = ir direto"
- Interrupção da rede a longo prazo que afeta a conectividade com o proxy de upstream e o servidor DNS
- Após a recuperação da rede, os logs de acesso não mostram marcas DEFAULT_PARENT, indicando que o tráfego continua a ignorar o proxy de upstream
- Ocorre um problema em um dispositivo WSA enquanto outro, no mesmo ambiente, opera normalmente

Ambiente

- Cisco Web Security Appliance (WSA) série S
- AsyncOS 14.5.2-011 (versão afetada)
- Hardware: S695
- Proxy de Upstream Configurado com Especificação FQDN

- Tratamento de falhas configurado como "ir diretamente"
- Ambiente de rede com infraestrutura de switch L2

Resolução

Esse problema é resolvido com a atualização do AsyncOS para uma versão que contenha a correção para CSCwi13124. Esse erro foi corrigido nestas versões do AsyncOS:

- AsyncOS 15.5.0-566
- AsyncOS 15.5.0-710

Solução temporária para versões atuais

Para ambientes que não podem fazer upgrade imediatamente, uma mitigação temporária está disponível ajustando o timeout ocioso máximo para verificação de proxies upstream sem resposta:

Passo 1: Acesse a CLI e navegue até a configuração avançada de proxy:

```
cli -> advancedproxyconfig -> MISCELLANEOUS
```

Passo 2: Modifique a configuração de tempo limite máximo ocioso:

```
"Enter maximum idle timeout for checking unresponsive upstream proxy (in seconds)"
```

Passo 3: Reduza o valor máximo padrão (86400 segundos/24 horas) para um valor menor a fim de diminuir o tempo entre as verificações de integridade.

Método de Recuperação Imediata

Se o problema estiver afetando o fluxo de tráfego no momento, o próximo comando poderá restaurar imediatamente a funcionalidade do proxy de upstream:

Passo 1: Acesse o menu de diagnóstico:

```
CLI > diagnostic > PROXY > kick
```

Isso reinicia o processo de proxy e restaura as operações normais de proxy de upstream.

Procedimento de validação e teste

Para testar se o problema está presente ou foi resolvido após uma atualização, revise estas etapas:

Passo 1: Estabelecer monitoramento de linha de base

Monitore os logs de acesso e os logs de proxy para confirmar se o WSA está enviando tráfego para o proxy de upstream. Verifique se o tráfego está chegando ao lado do proxy de upstream.

Passo 2: Simular interrupção da rede

Após confirmar o fluxo de tráfego normal para o proxy de upstream, desconecte estas conexões:

- WSA para conexão de proxy upstream
- Conexão do WSA com o servidor DNS

Passo 3: Detecção de falha no monitor

Verifique os logs de proxy e os logs do sistema para obter estes indicadores:

- O log de proxy pode mostrar proxy de upstream como "... declarado inativo"
- O registro do sistema pode mostrar "Crítico: Máximo de falhas ao consultar o servidor DNS atingido..."

Passo 4: Manter Estado Interrompido

Sem reiniciar o processo de proxy, mantenha o estado desconectado da Etapa 2 e continue gerando solicitações por aproximadamente 10 horas.

Passo 5: Restaurar conectividade

Após aproximadamente 10 horas, restaure as conexões que foram desconectadas na Etapa 2.

Passo 6: Monitorar comportamento de recuperação

Após concluir a Etapa 5, monitore os logs de acesso e os logs de proxy sem reiniciar o processo de proxy:

- Em um sistema fixo: O tráfego continua fluindo pelo proxy de upstream e os logs de proxy mostram transições normais de status de integridade
- Em um sistema afetado: Os logs de acesso mostram o tráfego continuando a ignorar o proxy de upstream, e os logs de proxy não mostrarão mensagens "... estava doente, agora saudável" ou "... estava saudável, agora doente"

Causa

A causa raiz desse problema é uma falha lógica no mecanismo de verificação de integridade do proxy de upstream. Quando o WSA determina que um proxy de upstream configurado está "inativo" (sem resposta), ele implementa um algoritmo de backoff exponencial que dobra o intervalo de verificação de integridade após cada falha. Esse intervalo pode atingir um máximo de 24 horas (86400 segundos).

Esse problema ocorre quando o proxy de upstream torna-se disponível novamente durante um desses intervalos estendidos. Mesmo que o proxy tenha se recuperado e esteja respondendo normalmente, o WSA não executará uma verificação de integridade até que o intervalo de tempo configurado completo tenha decorrido. Isso pode resultar em até 24 horas de roteamento de tráfego direto contínuo em vez de retomar o uso de proxy de upstream.

Esse comportamento afeta as configurações do WSA, onde:

- O proxy de upstream é especificado pelo nome do host DNS/FQDN (não pelo endereço IP)

- O tratamento de falhas está definido como "ir direto"
- As interrupções prolongadas da rede afetam tanto o proxy de upstream quanto a conectividade do servidor DNS

ID de bug da Cisco: CSCwi13124

Conteúdo relacionado

- 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.