Verificar recurso de comportamento de desvio para compatibilidade com o Secure Access Microsoft 365

Contents

Problema

Ao configurar o Cisco Secure Access com o recurso de Compatibilidade do Microsoft 365 habilitado, há incerteza sobre se FQDNs (Fully Qualified Domain Names) específicos relacionados à Microsoft serão automaticamente ignorados do processamento do Secure Web Gateway (SWG) e da descriptografia TLS. Especificamente, é necessário esclarecer o comportamento de desvio para esses domínios:

- do.dsp.mp.microsoft.com
- dl.delivery.mp.microsoft.com
- manage.microsoft.com

A principal preocupação se concentra em saber se esses domínios exigem adição manual à lista Não descriptografar ou se são excluídos automaticamente quando a compatibilidade com o Microsoft 365 está habilitada. Além disso, há confusão sobre a interação entre os desvios de nível SWG e as configurações de descriptografia de nível IPS, particularmente para manage.microsoft.com, que aparece na documentação sugerindo que a configuração manual do Do Not Decrypt List ainda pode ser necessária.

Ambiente

- Acesso seguro da Cisco
- Recurso de Compatibilidade do Microsoft 365 habilitado
- Inspeção do Secure Web Gateway (SWG) e descriptografia TLS configuradas
- Políticas de descriptografia de IPS em uso
- Serviços de gerenciamento e atualização da Microsoft que exigem conectividade

Resolução

O comportamento do recurso de compatibilidade do Microsoft 365 foi verificado através de testes laboratoriais com estas descobertas:

Escopo do Recurso de Compatibilidade do Microsoft 365

O recurso Compatibilidade do Microsoft 365 isenta domínios relacionados ao Microsoft 365 marcados como "Otimizar" e "Permitir" nas categorias de endpoint da Microsoft da inspeção de SWG e aplicação de política. Isso permite que o tráfego para esses domínios passe inalterado na camada SWG.

Resultados dos testes laboratoriais

Os testes foram realizados em um ambiente de laboratório controlado com compatibilidade com o Microsoft 365 ativada. Este comportamento foi observado para os FQDNs especificados:

Passo 1: Habilitar Recurso de Compatibilidade do Microsoft 365

O recurso de Compatibilidade do Microsoft 365 foi ativado na configuração de Acesso Seguro.

Passo 2: Testar tráfego para FQDNs de destino

O tráfego da Web foi gerado para cada um dos três FQDNs usando um navegador de Internet padrão:

- do.dsp.mp.microsoft.com
- dl.delivery.mp.microsoft.com
- manage.microsoft.com

Passo 3: Verificar o comportamento de desvio no painel

A análise do painel de controle do Secure Access confirmou que a inspeção e a descriptografia do tráfego da Web não estavam ocorrendo para o tráfego para esses destinos específicos quando o recurso de compatibilidade do Microsoft 365 foi habilitado.

Passo 4: Confirmar comportamento de direção DNS

O tráfego DNS para esses destinos continuou a ser direcionado pelo Secure Access, que se alinha ao comportamento documentado, a menos que uma isenção de DNS específica seja configurada.

Principais descobertas comportamentais

Com base nos resultados dos testes e na análise da documentação:

- Desvio de SWG: Os três FQDNs especificados são ignorados da inspeção de tráfego da Web quando a Compatibilidade com o Microsoft 365 está habilitada.
- Descriptografia TLS: A descriptografia é ignorada na camada SWG para esses domínios.
- Direção DNS: As consultas DNS continuam a ser processadas através do Secure Access, a menos que explicitamente isentas.
- Cobertura de domínio: Embora "*.microsoft.com" como um domínio inteiro não seja totalmente ignorado pela especificação, os URLs específicos testados são ignorados na prática.

Considerações sobre a camada de IPS

O recurso de compatibilidade do Microsoft 365 opera na camada SWG. Para o desvio de descriptografia no nível de IPS, a configuração manual ainda pode ser necessária:

- Se o desvio de descriptografia de IPS também for desejado para esses domínios, a adição manual à lista Não descriptografar poderá ser necessária.
- A lista Não descriptografar afeta principalmente a descriptografia do lado do IPS em vez do processamento SWG.
- Isso explica por que a documentação pode fazer referência à adição de manage.microsoft.com à lista Não descriptografar mesmo quando a compatibilidade com o

Microsoft 365 está habilitada.

Causa

A confusão surge da arquitetura em camadas do Cisco Secure Access, onde a Compatibilidade com o Microsoft 365 afeta o processamento no nível do SWG, enquanto a descriptografia do IPS opera como uma camada separada com seus próprios requisitos de configuração. O recurso de compatibilidade do Microsoft 365 manipula automaticamente o desvio SWG para qualificar domínios Microsoft, mas as políticas de descriptografia IPS podem exigir configuração separada por meio da lista Não descriptografar.

Conteúdo relacionado

- Documentação de compatibilidade do Cisco Secure Access com o Microsoft 365
- Crie uma lista Não descriptografar efetiva para o Cisco Secure Access
- 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.