Solucionar problemas de identidade SAML que não está sendo aplicada ao tráfego de gateway da Web seguro

Contents

Introdução

Este documento descreve como solucionar problemas de identidades SAML que não estão sendo aplicadas ao Tráfego de gateway da Web seguro.

Identidade SAML não aplicada para QUALQUER tráfego da Web

Se a identidade SAML não for aplicada a NENHUM tráfego da Web, consulte a documentação do Umbrella para garantir que a configuração foi concluída corretamente. Esses itens de configuração devem ser concluídos.

- Configurações de IdP definidas e testadas em 'Implantações > Configuração SAML'
- Lista de usuários/grupos provisionados em 'Implantações > Usuários e Grupos da Web'
- O SAML deve ser ativado na política relevante* em 'Políticas > Políticas da Web'.
- A Descriptografia HTTPS deve ser habilitada na política relevante em 'Políticas > Políticas da Web'

Habilitando SAML em Políticas da Web

A Descriptografia SAML e HTTPS deve ser habilitada na política que se aplica à identidade de Rede ou Túnel relevante. Esses recursos se aplicam antes que um usuário seja identificado, portanto, a política importante é aquela aplicada ao "método de conexão".

As políticas SAML devem ser ordenadas da seguinte forma:

1. HIGHER Priority - (Prioridade MAIS ALTA) A política se aplica a usuários/grupos. Essa política decide as configurações de conteúdo/segurança para os usuários autenticados.

2. LOWER Priority (Prioridade INFERIOR): a política se aplica à rede/túnel. Esta política tem SAML habilitado e aciona a autenticação inicial.

Identidade SAML não aplicada para tráfego da Web específico

Substitutos de IP (comportamento padrão)

Para melhorar a consistência da identificação do usuário, recomendamos ativar o novo recurso de substitutos de IP. Esse recurso é habilitado automaticamente para todos os novos clientes do Umbrella SAML, mas precisa ser habilitado manualmente para clientes existentes do Umbrella.

Os substitutos de IP usam um cache de informações de IP interno > Nome de usuário, o que significa que a identificação SAML pode ser aplicada a todos os tipos de solicitações: até mesmo o tráfego de navegador que não seja da Web, o tráfego que não suporta cookies e o tráfego que não está sujeito à Descriptografia SSL.

Os substitutos de IP podem melhorar muito a consistência da identificação do usuário e reduzir a carga administrativa.

Observe que os substitutos de IP têm estes requisitos:

- A visibilidade de IP interno deve ser fornecida usando um túnel de rede Umbrella ou implantação de cadeia de proxy e cabeçalhos X-Forwarded-For. Isso não funciona com o arquivo PAC hospedado do Umbrella
- Os substitutos de IP não podem ser usados em cenários de endereço IP compartilhado (Servidores de Terminal, Switching Rápida de Usuário)
- Os cookies devem ser ativados no navegador. Os cookies ainda são necessários para a etapa de autenticação inicial.

Cookies substitutos (IP substitutos desativados)

Com os substitutos de IP desabilitados, a identidade do usuário é aplicada somente a solicitações de navegadores da Web suportados e o navegador da Web DEVE suportar cookies. O SWG requer que o navegador suporte cookies para cada solicitação para rastrear a sessão dos usuários em um cookie. Infelizmente, isso significa que não se espera que cada solicitação da Web seja associada a um usuário nesse modo.

O SAML não é aplicado nessas circunstâncias e a política padrão atribuída à identidade de rede/túnel é usada:

- Tráfego de navegador não Web
- Navegadores da Web com cookies desabilitados ou Configuração de Segurança Reforçada do IE
- Verificações de OCSP/Revogação de Certificado que não dão suporte a cookies
- Solicitações da Web individuais que não dão suporte a cookies. Em alguns casos, os cookies são bloqueados para solicitações individuais devido à Política de Segurança de Conteúdo do site. Essa restrição se aplica a muitas redes de fornecimento de conteúdo

populares.
- Quando o domínio/categoria de destino tiver sido ignorado do SAML usando uma lista de desvio de SAML
- Quando o domínio/categoria de destino tiver sido ignorado da descriptografia HTTPS usando uma lista Umbrella Selective Decryption.

Devido a essas restrições, é importante configurar um nível mínimo de acesso apropriado na política de rede/túnel relevante. A política padrão deve permitir aplicativos/domínios/categorias críticos de negócios e redes de fornecimento de conteúdo.

Como alternativa, use o sistema IP Surrogates para melhorar a compatibilidade.

Ignorar SAML

Em casos raros, exceções são necessárias. Isso é necessário quando o SWG submete uma solicitação de autenticação SAML, mas o aplicativo ou site não pode suportá-la. Isso acontece quando:

- Um aplicativo que não seja navegador usa um agente de usuário que se parece com um navegador da Web
- Um script não pode manipular redirecionamentos HTTP executados por nossos testes de cookie
- A primeira solicitação em uma sessão de navegação é uma solicitação POST (por exemplo, URL de logon único) que não pode ser redirecionado corretamente para SAML

A lista de desvio SAML é a melhor maneira de excluir um domínio da autenticação enquanto ainda mantém a segurança (inspeção de arquivo).

- A exceção da lista de desvio SAML deve ser aplicada à política correta que afeta a rede/túnel usado para conectar
- A lista de desvio SAML não permite automaticamente o tráfego. O(s) domínio(s) ainda deve(m) ser permitido(s) por categoria ou listas de destinos na política relevante.

Desvio de SAML - Considerações

Ao adicionar exclusões para sites populares e "homepages", é importante considerar o impacto no SAML. O SAML funciona melhor quando a primeira solicitação em uma sessão de navegação é uma solicitação GET para uma página HTML. Por exemplo: http://www.myhomepage.tld. Esta solicitação é redirecionada para autenticação SAML e as solicitações subsequentes assumem a mesma identidade usando substitutos de IP ou cookies.

Ignorar as páginas iniciais do SAML pode acionar um problema em que a primeira solicitação vista pelo sistema SAML é para conteúdo em segundo plano. Por exemplo, http://homepage-content.tld/script.js. Isso é um problema porque o redirecionamento SAML para uma página de login SAML não é possível quando o navegador está carregando conteúdo incorporado (como arquivos JS). Isso significa que a página parece ser renderizada ou operar incorretamente até que o usuário vá para um site diferente para disparar o logon.

Ao considerar sites populares e páginas iniciais, considere estas opções:

- Não excluir páginas iniciais e sites populares da descriptografia SAML ou HTTPS, a menos que seja necessário
- Se excluir uma página inicial, todos os domínios usados por esse site (incluindo conteúdo de segundo plano) deverão ser excluídos para evitar incompatibilidades de SAML

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.