Bloquear tráfego de upload no dispositivo da Web seguro

Contents

Introdução

Este documento descreve o processo de bloqueio do tráfego de upload para determinados sites no Secure Web Appliance (SWA).

Pré-requisitos

Requisitos

A Cisco recomenda o conhecimento destes tópicos:

- Acesso à interface gráfica do usuário (GUI) do SWA
- Acesso administrativo ao SWA.

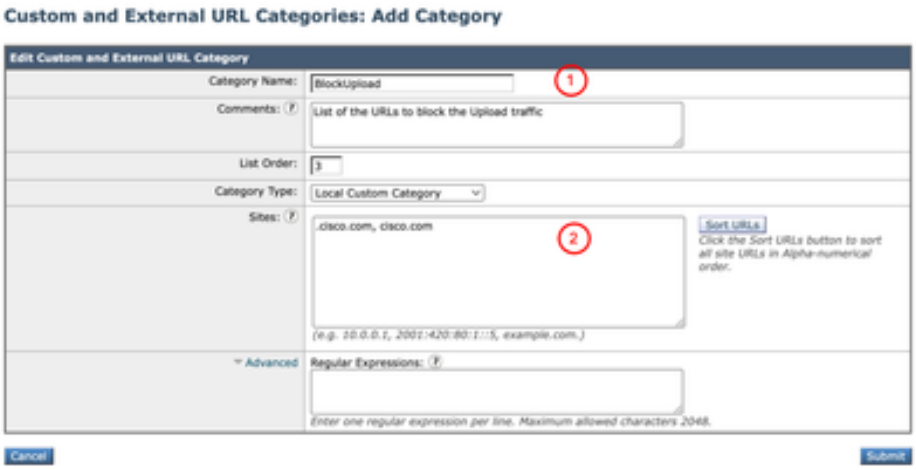
Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configuration Steps

Etapa 1. Crie uma Categoria	Etapa 1.1. Na GUI, navegue até Web Security Manager e

de URL Personalizada para o site.	escolha Custom and External URL Categories. Etapa 1.2. Clique em Adicionar categoria para criar uma nova Categoria de URL personalizada. Etapa 1.3. Digite Nome para a nova categoria. Etapa 1.4. Defina o domínio e/ou subdomínios do site que você está tentando bloquear o tráfego de upload (Neste exemplo, cisco.com e todos os seus subdomínios). Etapa 1.5.Envie as alterações.  Imagem - Criar categoria de URL personalizada Tip: Para obter mais informações sobre como configurar categorias de URL personalizadas, acesse: https://www.cisco.com/c/en/us/support/docs/security/secure-web-appliance-virtual/220557-configure-custom-url-categories-in-secur.html
Etapa 2. Descriptografar o tráfego do URL	Etapa 2.1. Na GUI, navegue até o Web Security Manager e escolha Políticas de descriptografia Etapa 2.2. Clique em Add Policy. Etapa 2.3. Digite Nome para a nova política. Etapa 2.4. (Opcional) Selecione o Perfil de identificação ao qual você precisa que essa política se aplique. Etapa 2.5. Na seção Definição de membro de política, clique nos links Categorias de URL para adicionar a Categoria de URL personalizada.

Etapa 2.6. Selecione a Categoria de URL que foi criada na Etapa 1.

Etapa 2.7. Clique em Submit.

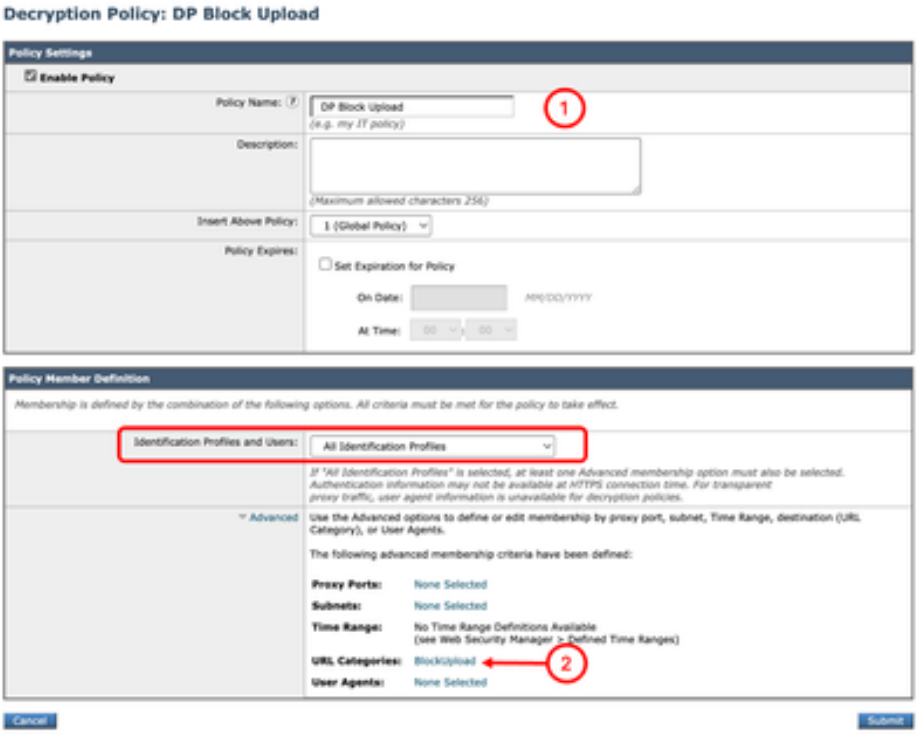


Imagem - Criar uma política de descriptografia

Etapa 2.8. Na página Políticas de descriptografia, clique no link de Filtragem de URL para a nova política.

Imagem - Selecione a filtragem de URL

Etapa 2.9. Escolha Descriptografar como a ação para Categoria de URL Personalizada.

Etapa 2.10. Clique em Submit.

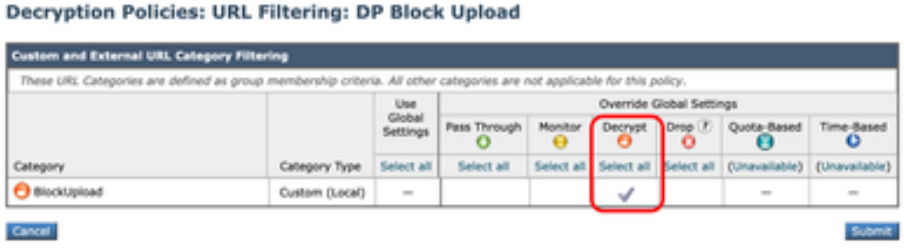


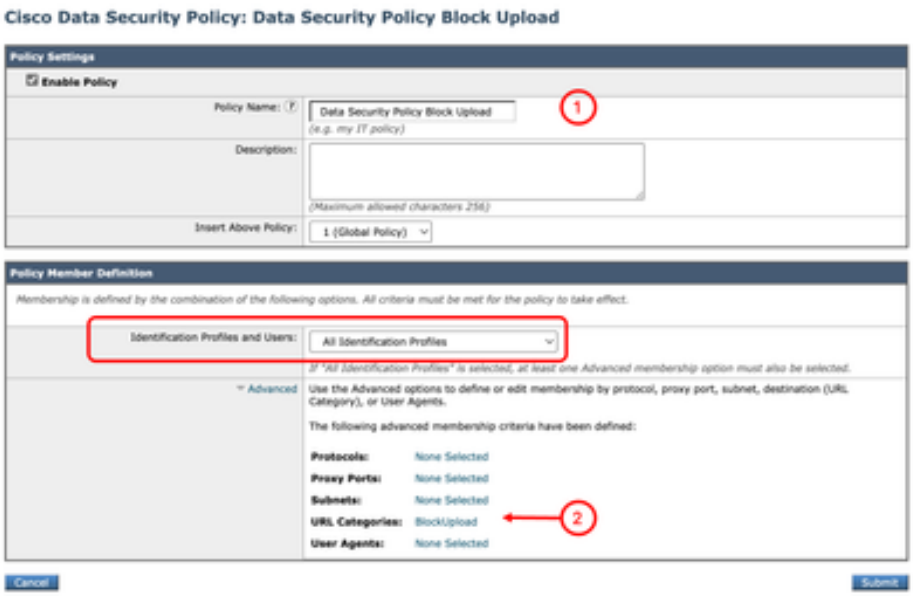
	Imagem - Definir descriptografia como ação
Etapa 3. Bloquear o tráfego de upload	Etapa 3.1. Na GUI, navegue até o Web Security Manager e escolha Cisco Data Security. Etapa 3.2. Clique em Add Policy. Etapa 3.3. Digite Nome para a nova política. Etapa 3.4. (Opcional) Selecione o Perfil de identificação ao qual você precisa que essa política se aplique. Etapa 3.5. Na seção Definição de membro de política, clique nos links Categorias de URL para adicionar a Categoria de URL personalizada. Etapa 3.6. Selecione a Categoria de URL que foi criada na Etapa 1. Etapa 3.7. Clique em Submit.  Imagem - Política de segurança de dados da Cisco Tip: Para fins de geração de relatórios, é melhor escolher um nome que não seja igual a nenhuma outra política de acesso/descriptografia. Etapa 3.8. Na página Cisco Date Security Policy, clique no link de URL Filtering para a nova política.

Imagem - Selecione a filtragem de URL

Etapa 3.9. Escolha Bloquear como a ação para Categoria de URL personalizada.

Etapa 3.10. Clique em Submit.

Imagem - Carregamento de bloco

Etapa 3.11. Confirmar alterações.

Relatórios e registros

Logs

Você pode exibir os logs relacionados ao tráfego de upload a partir do CLI escolhendo idsdataloss_logs, que é o nome de log padrão para Logs de segurança de dados.

Siga estas etapas para acessar os logs:

Etapa 1. Faça login no CLI

Etapa 2. Digite grep e pressione Enter.

Etapa 3. Localize e digite o número associado a idsdataloss_logs:

- Digite: "Logs de segurança de dados"
- Recuperação: FTP Poll e pressione Enter.

Etapa 4. (Opcional) Insira a expressão regular para grep você fã filtro por palavras-chave, ou você pode pressionar Enter, para exibir todos os logs

Etapa 5. (Opcional) Deseja que esta pesquisa não diferencie maiúsculas de minúsculas? [Y]> Se você selecionar qualquer palavra-chave na Etapa 4, poderá escolher se o filtro não diferencia maiúsculas de minúsculas ou não.

Etapa 6. (Opcional) Deseja pesquisar linhas não correspondentes? [N]> Caso precise filtrar todos os logs, exceto as palavras-chave selecionadas definidas na Etapa 4, você pode usar esta seção; caso contrário, você pode pressionar Enter.

Etapa 7. (Opcional) Deseja encerrar os logs? [N]> Se precisar exibir os logs dinâmicos, digite Y e pressione Enter. Caso contrário, pressione Enter para exibir todos os logs disponíveis.

Etapa 8. (Opcional) Deseja paginar a saída? [N]> Se precisar ver os resultados por página, você pode digitar Y e pressionar Enter; caso contrário, pressione Enter para usar o valor padrão [N].

Relatórios

Você pode gerar o relatório de rastreamento da Web para exibir os relatórios do tráfego de carregamento bloqueado pelo nome da política de segurança de dados da Cisco.

Siga estas etapas para gerar os relatórios:

Etapa 1. Na GUI, selecione Reporting e escolha Web Tracking.

Etapa 2. Escolha o intervalo de tempo desejado.

Etapa 3. Clique no link Avançado para pesquisar transações usando critérios avançados.

Etapa 4. Na seção Política, selecione Filtrar por política e digite o nome da Segurança de dados da Cisco que foi criada anteriormente.

Etapa 5. Clique em Pesquisar para revisar o relatório.

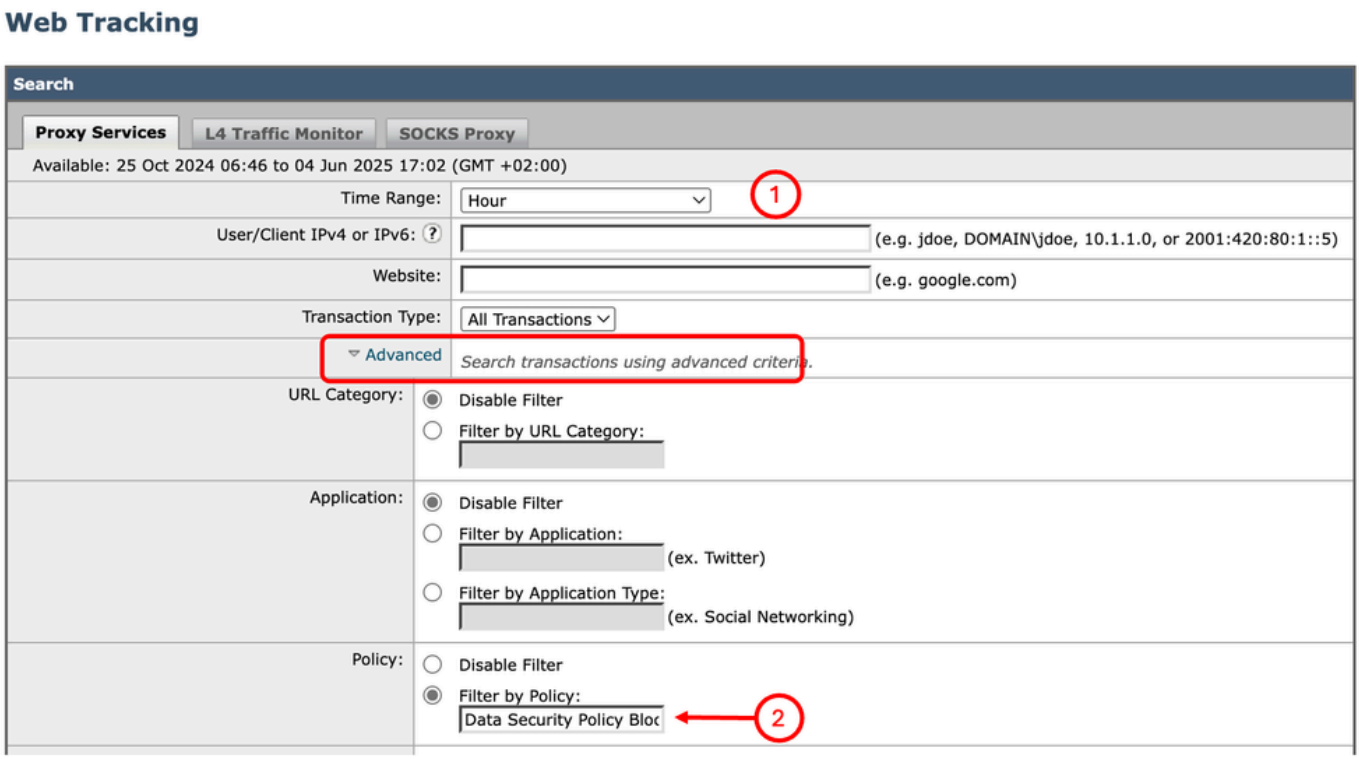


Imagem - Filtrando os relatórios de rastreamento na Web

Informações Relacionadas

- Manual do usuário do AsyncOS 15.2 para Cisco Secure Web Appliance
- Guia de instalação do Cisco Secure Email and Web Virtual Appliance
- Configurar categorias de URL personalizadas no Secure Web Appliance - Cisco
- Use as práticas recomendadas de dispositivos da Web seguros
- Configurar firewall para dispositivo seguro da Web
- Configurar certificado de descriptografia no aplicativo da Web seguro
- Configurar e solucionar problemas de SNMP em SWA
- Configurar logs de envio de SCP no Secure Web Appliance com o Microsoft Server
- Habilitar canal/vídeo específico do YouTube e bloquear o restante do YouTube no SWA
- Entender o formato do registro de acesso HTTPS no Secure Web Appliance
- Acessar logs do dispositivo da Web seguro
- Ignorar autenticação no Secure Web Appliance
- Bloquear o tráfego no Secure Web Appliance
- Ignorar o tráfego de atualizações da Microsoft no Secure Web Appliance

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.