Configurar solicitação de intervalo para tráfego do Microsoft Update em SWA

Contents

Introdução

Este documento descreve as etapas para permitir que o Tráfego de Atualizações da Microsoft use a Solicitação de Intervalo no Secure Web Appliance (SWA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Administração SWA.

A Cisco recomenda que você tenha estas ferramentas instaladas:

- SWA físico ou virtual
- Acesso administrativo à interface gráfica do usuário (GUI) do 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.

Solicitação de Intervalo

Uma solicitação de intervalo é um recurso do protocolo HTTP que permite que um cliente (como um navegador da Web ou gerenciador de download) solicite apenas uma parte específica de um arquivo de um servidor, em vez de fazer o download do arquivo inteiro de uma vez. Isso é particularmente útil para retomar downloads interrompidos, transmitir mídia ou acessar arquivos grandes de forma eficiente. O cliente especifica o intervalo de bytes desejado no cabeçalho Range (Intervalo) da solicitação HTTP e o servidor responde com um código de status 206 Partial Content (Conteúdo Parcial) se suportar solicitações de intervalo, entregando somente o segmento solicitado do arquivo.

Esse mecanismo melhora o desempenho e a experiência do usuário em vários cenários. Por exemplo, na transmissão de vídeo, as solicitações de intervalo permitem que os jogadores busquem apenas os segmentos necessários para reprodução, reduzindo o uso da largura de banda e melhorando a capacidade de resposta. Da mesma forma, os gerenciadores de download usam solicitações de intervalo para dividir um arquivo em blocos e baixá-los em paralelo, acelerando o processo. As solicitações de intervalo também desempenham um papel importante nos sistemas de cache e proxy, permitindo atualizações parciais e reduzindo transferências de dados redundantes.

Solicitação de Intervalo no Ambiente Proxy

Em um ambiente proxy, as solicitações de intervalo desempenham um papel crucial na otimização do uso da largura de banda e na melhoria da eficiência de fornecimento de conteúdo. Quando as solicitações de intervalo estão habilitadas, o servidor proxy pode buscar somente os segmentos de byte necessários do servidor de origem e armazená-los localmente em cache. Isso permite que os clientes solicitem conteúdo parcial, como segmentos específicos de um vídeo ou um arquivo grande, e o recebam rapidamente do cache de proxy, se disponível. Também permite downloads paralelos e recursos de retomada, que são especialmente benéficos em ambientes com largura de banda limitada ou alta latência.

No entanto, quando as solicitações de intervalo são desabilitadas, o proxy deve buscar o arquivo inteiro do servidor de origem, mesmo que o cliente precise apenas de uma pequena parte. Isso leva a transferência desnecessária de dados, aumento de carga nos servidores proxy e origem e tempos de resposta mais lentos para os clientes. Ele também evita estratégias de cache eficientes, pois o proxy não pode armazenar ou servir conteúdo parcial. Em cenários de fluxo, isso pode resultar em atrasos de buffer ou experiência de usuário degradada. A desativação de

solicitações de intervalo pode ser feita por motivos de segurança ou de política, mas geralmente isso ocorre ao custo de desempenho e flexibilidade.

Por exemplo, considere um cenário em que 10 usuários estejam tentando fazer download de 1 MB cada de um arquivo de 100 MB através de um servidor proxy.

Solicitações de intervalo desativadas:

Quando as solicitações de intervalo estão desabilitadas, o proxy não pode buscar apenas o segmento de 1MB de que cada usuário precisa. Em vez disso, ele deve fazer o download de todo o arquivo de 100 MB do servidor de origem para cada solicitação. Isso resulta em:

Tráfego total da origem para o proxy: 10 × 100 MB = 1000 MB (1 GB)

Apenas 10MB desses dados são realmente usados pelos clientes.

Os 990 MB restantes são desperdiçados, o que leva ao uso ineficiente da largura de banda e ao aumento da carga nos servidores proxy e de origem.

Solicitações de intervalo ativadas:

Com as solicitações de intervalo ativadas, o proxy busca somente os 1MB solicitados por usuário:

Tráfego total da origem para o proxy: 10 × 1 MB = 10 MB

O proxy pode armazenar esses segmentos em cache e fornecê-los a outros usuários, se necessário.

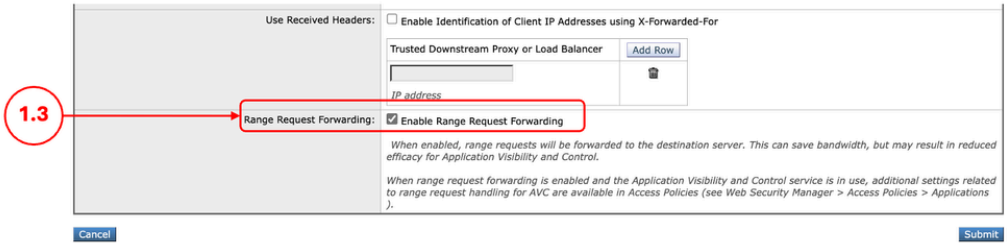
Isso resulta em 90 vezes menos tráfego, tempos de resposta mais rápidos e utilização de recursos significativamente melhor.

Habilitando Solicitação de Intervalo para Atualizações da Microsoft

Embora as solicitações de alcance melhorem o desempenho, elas impedem a verificação de segurança e a aplicação de políticas em ambientes SWA, pois esses sistemas não podem inspecionar totalmente o conteúdo parcial. Este artigo limita o uso da solicitação de intervalo exclusivamente ao tráfego do Microsoft Update.

⚠ Cuidado: a habilitação do encaminhamento de solicitação de intervalo pode interferir na eficiência do Application Visibility and Control (AVC) baseado em políticas e pode comprometer a segurança.

Etapas para Habilitar a Solicitação de Intervalo somente para Atualizações da Microsoft

Etapa 1. Ativar a Solicitação de Intervalo	Etapa 1.1. Na GUI, clique em Serviços de segurança e escolha Web Proxy. Etapa 1.2. Clique em Edit Settings. Etapa 1.3. Marque a caixa de seleção Ativar encaminhamento de solicitação de intervalo. Etapa 1.4. Clique em Submit.  Imagem - Habilitar encaminhamento de solicitação de intervalo
Etapa 2. Criar uma Categoria de URL Personalizada para URLs de Atualizações da Microsoft	Etapa 2.1.FromGUI, ChooseWeb Security Manager e clique em Categorias de URL personalizadas e externas. Etapa 2.2.Clique em Adicionar categoria para adicionar uma categoria de URL personalizada. Etapa 2.3.Atribua um CategoryName exclusivo. Etapa 2.4. (Opcional) Adicione Descrição. Etapa 2.5. Em Ordem da lista, escolha a primeira categoria a ser posicionada na parte superior. Etapa 2.6. Na lista suspensa Tipo de categoria, selecione Categoria personalizada local. Etapa 2.7. Adicionar URLs de atualizações da Microsoft na seção Sites. Tip: Você pode verificar a lista de atualizações da Microsoft neste link: Etapa 2 - Configurar o WSUS | Aprendizado da Microsoft Caution: Não copie/cole os URLs como estão nos documentos da Microsoft; formate-os corretamente como formato SWA. Para obter mais informações, visite: Configurar categorias de URL personalizadas no Secure Web Appliance - Cisco

Aqui está um exemplo:

```
http://windowsupdate.microsoft.com     ===>  windowsupdate.microsoft.com
http://*.windowsupdate.microsoft.com   ===>   .windowsupdate.microsoft.com
```

Etapa 2.8. Clique em Submit.

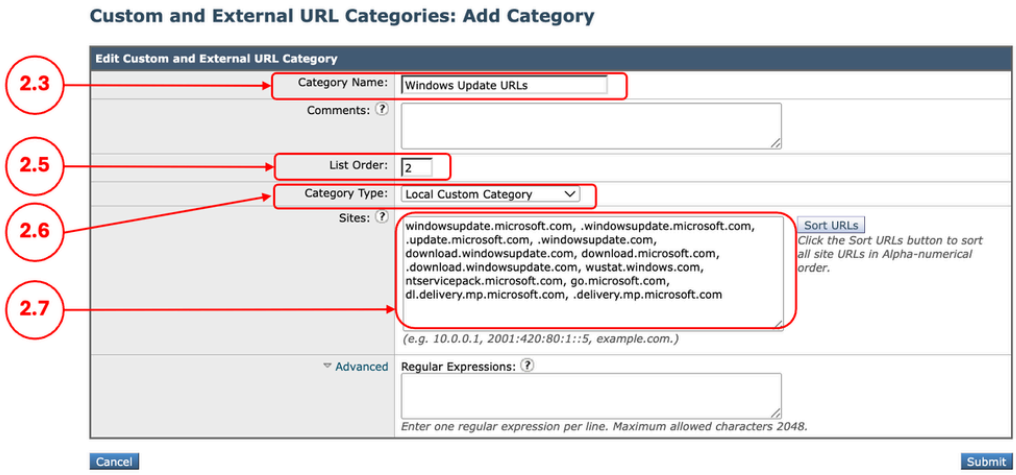


Imagem - Criar uma Categoria de URL Personalizada

Etapa 3. (Opcional) Criar um Perfil de Identificação para isentar o tráfego de Atualizações da Microsoft da Autenticação

Etapa 3.1.FromGUI, ChooseWeb Security Manager e clique em Identification Profiles.
Etapa 3.2.Clique emAdd Profile para adicionar um perfil.
Etapa 3.3.Certifique-se de que a caixa de seleçãoAtivar perfil de identificação esteja marcada.
Etapa 3.4.Atribua um profileName exclusivo.
Etapa 3.5. (Opcional) Adicione Descrição.
Etapa 3.6.Na lista suspensa InserirAcima, escolha onde esse perfil deve aparecer na tabela.

Note: Esta ação é para reduzir a carga de autenticação no SWA para o tráfego para as atualizações da Microsoft.

Etapa 3.7. Na seção Método de identificação de usuário, escolhaIsentar de autenticação/identificação.

Etapa 3.8.No campo Definir membros por sub-rede, se você quiser Passar através do tráfego da Microsoft para alguns usuários específicos, insira os endereços IP ou sub-redes que se aplicam, ou deixe este campo em branco para incluir todos os endereços IP.

Etapa 3.9. Na seção Avançado, escolha Categorias de URL personalizadas.

Etapa 3.10. Adicione a categoria de URL personalizada que foi criada para atualizações da Microsoft.

Etapa 3.11. Clique em Concluído.

Etapa 3.12. Clique em Enviar.

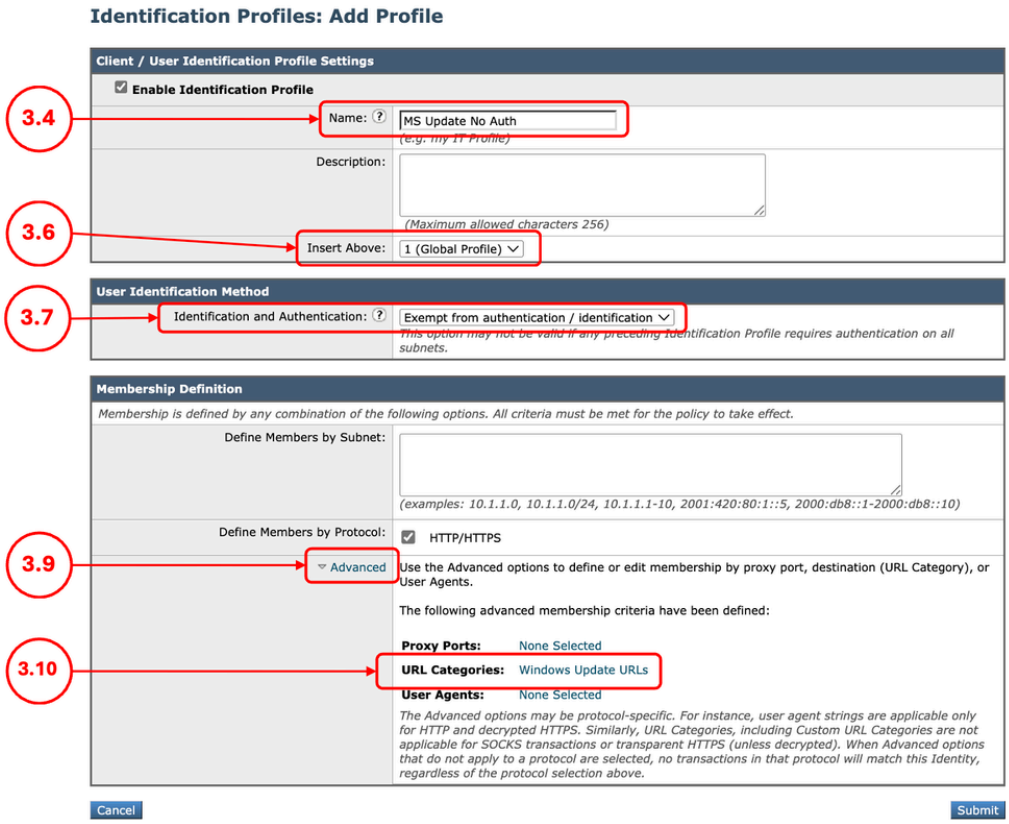


Imagem - Criar perfil de identificação

Etapa 4. (Opcional) Criar uma Política de Descriptografia para Passar pelo Tráfego de Atualizações da Microsoft

Note: Microsoft Atualiza, usa HTTP e o tráfego HTTPS é para enviar os links de atualizações. Esta ação é para reduzir a carga de descriptografia no SWA.

Etapa 4.1.FromGUI, ChooseWeb Security Manager e clique emDecryption Policy.

Etapa 4.2. Clique em Adicionar política para adicionar uma política de descriptografia.

Etapa 4.3.Atribua um PolicyName exclusivo.
Etapa 4.4. (Opcional) Adicione Descrição.
Etapa 4.5.Na lista suspensa Inserir política acima, escolha a primeira política.

Etapa 4.6.Em Perfis de identificação e usuários, escolha Selecionar um ou mais perfis de identificação.

Etapa 4.7. Selecione o Perfil de identificação criado na Etapa 3 e vá para a Etapa 4.11.

Etapa 4.8. Se você não criou nenhum perfil de ID para as atualizações do Windows, na seção Avançado, escolha Categorias de URL personalizadas.

Etapa 4.9. Adicione a Categoria de URL personalizada que foi criada para atualizações da Microsoft na Etapa 2.

Etapa 4.10. Clique em Concluído.

Etapa 4.11. Clique em Submit.

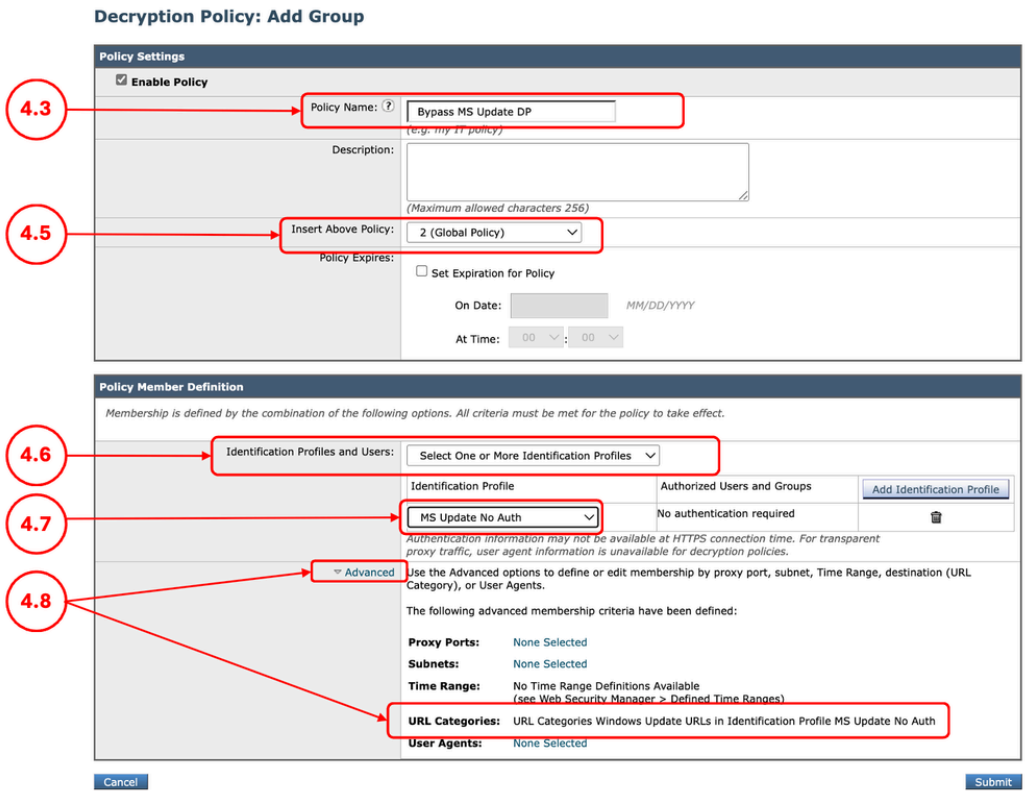


Imagem - Criar uma política de descriptografia

Etapa 4.12.Na página Descriptografia Políticas, emFiltragem de URL, clique no link associado a essa nova Política de Descriptografia.

Etapa 4.13.SelecionarAprovação Através da ação para a categoria de URL de Atualizações da Microsoft.

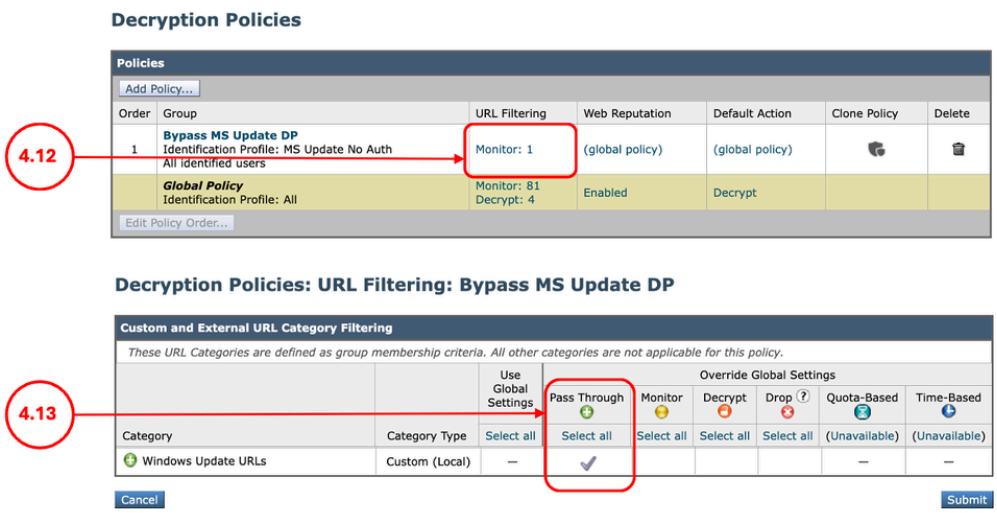


	Imagem - Definir a ação de passagem para a categoria de URL Etapa 4.12. Clique em Enviar.
Etapa 5. Criar uma Política de Acesso para Permitir Solicitação de Intervalo para Tráfego de Atualizações da Microsoft	Etapa 5.1.FromGUI, clique emWeb Security Manager e escolhaAccess Policy. Etapa 5.2. Clique em Adicionar política para adicionar uma política de acesso. Etapa 5.3.Atribua um PolicyName exclusivo. Etapa 5.4. (Opcional) Adicione Descrição. Etapa 5.5.Na lista suspensa Inserir política acima, escolha a primeira política. Etapa 5.6.Em Perfis de identificação e usuários, escolha Selecionar um ou mais perfis de identificação. Etapa 5.7. Selecione o Perfil de identificação que você criou na Etapa 3 e vá para a Etapa 5.11. Etapa 5.8. Se você não criou nenhum perfil de ID para as atualizações do Windows, na seção Avançado, escolha Categorias de URL personalizadas. Etapa 5.9. Adicione a Categoria de URL personalizada que foi criada para atualizações da Microsoft na Etapa 2. Etapa 5.10. Clique em Concluído. Etapa 5.11. Enviar.

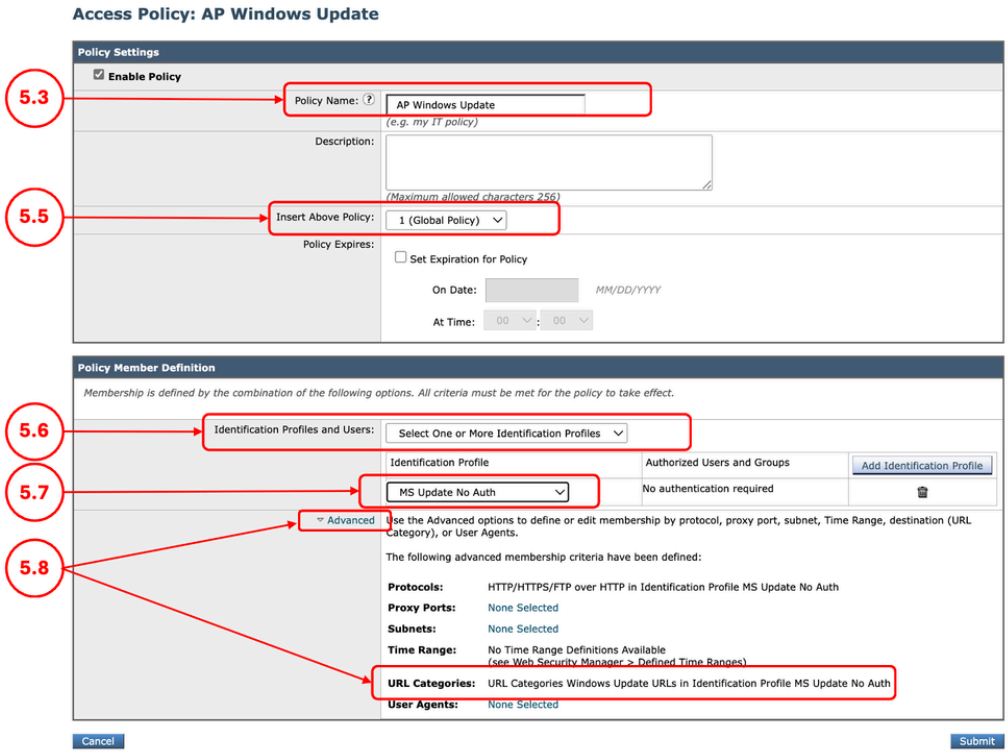


Imagem - Criar a política de acesso

Etapa 5.12. Na página Access Policies, em URL Filtering, clique no link associado a esta nova Access Policy

Etapa 5.13.Selecione Permitir como a ação para a categoria de URL personalizada criada para as atualizações da Microsoft.

Etapa 5.14. Clique em Enviar.

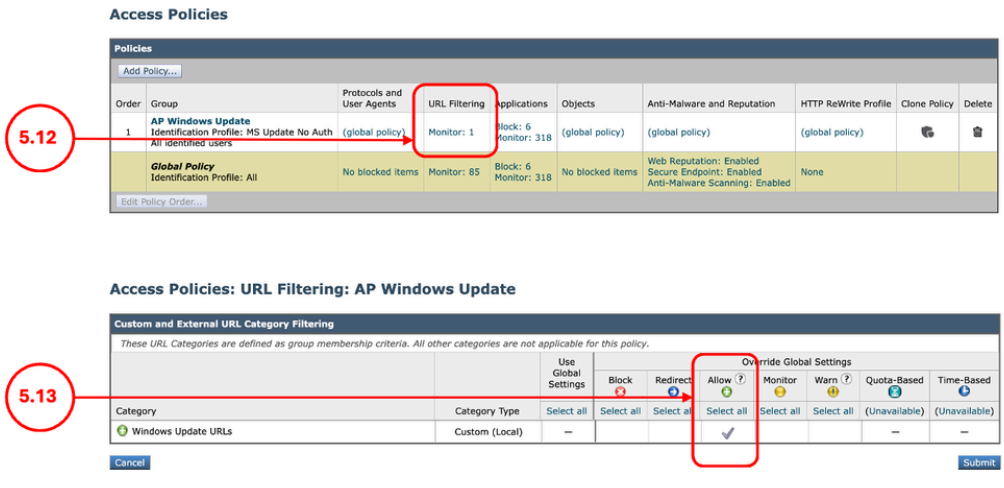


Imagem - Definir a ação Permitir para a categoria de URL

Etapa 5.15. Na página Access Policies, em Applications, clique no link associado a esta nova Access Policy

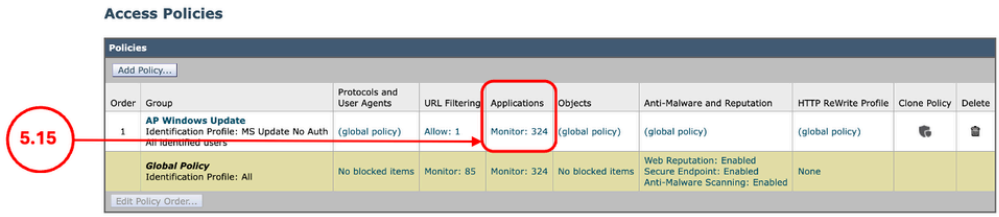


Imagem - Editar visibilidade e controle do aplicativo

Etapa 5.16. Na seção Edit Applications Settings, selecione Define Applications Custom Settings.

Etapa 5.17. Na seção Configurações dos aplicativos, clique no aplicativo Editar tudo para Jogos e defina a ação como Bloquear.

Etapa 5.18. Clique em Apply (Aplicar).

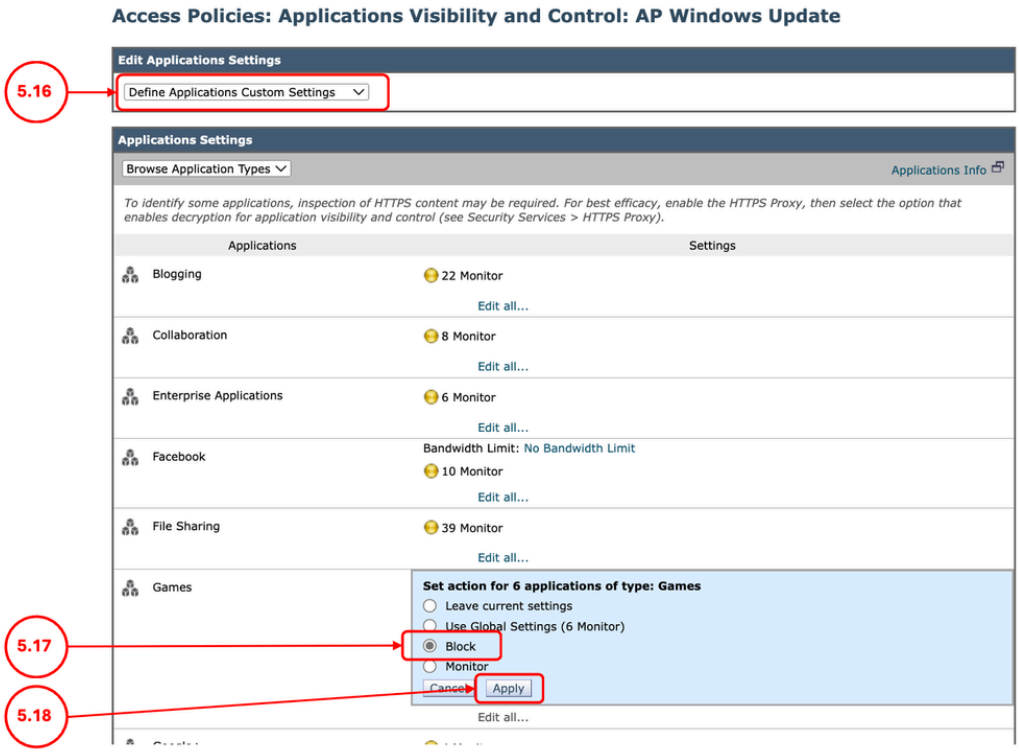


Imagem - Definir uma ação do aplicativo para bloquear

Etapa 5.19. Role para baixo até a seção Range Request Settings for Policy, verifique se Forward range requests está selecionado,

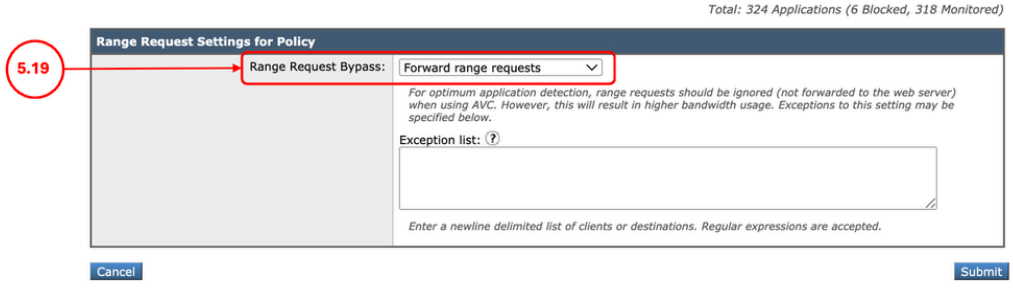


Imagem - Definições de Solicitação de Intervalo para Política

Etapa 5.20. Enviar.

Etapa 5.21. Na página Access Policies, em Applications, clique no link associado à Política Global.

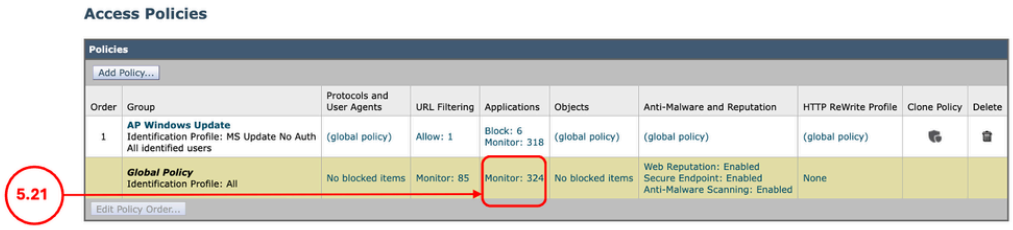


Imagem - Configurações de Aplicação da Política de Acesso Padrão

Etapa 5.22. Role para baixo até a seção Range Request Settings for Policy, certifique-se de que Do Not Forward range requests esteja selecionado,

Etapa 5.23. Confirmar alterações.

Modificando os logs de acesso

Para ter mais visibilidade das Solicitações de intervalo nos Logs de acesso, você pode adicionar estes campos personalizados:

[Intervalo do cliente = %<Intervalo:]	Mostra o intervalo, solicitado pelo cliente (Bytes)
[content= %>Comprimento do Conteúdo:]	Mostra o tamanho do conteúdo baixado (Bytes)

Para obter mais informações para adicionar um campo personalizado aos logs de acesso SWA, acesse este link: Configurar parâmetro de desempenho em logs de acesso

Verificação

Use este comando CURL para enviar uma solicitação de intervalo ao SWA:

```
curl -vvvk -H "Pragma: no-cache" -x 10.48.48.181:3128 -H 'Range: bytes=0-100' 'http://catalog.sf.dl.del
```

Na saída do CURL, você pode ver que a resposta HTTP é HTTP/1.1 206:

```
> GET http://catalog.sf.dl.delivery.mp.microsoft.com/filestreamingservice/files/f263aa64-f367-42f0-9cad
> Host: catalog.sf.dl.delivery.mp.microsoft.com
> User-Agent: curl/8.7.1
> Accept: */*
> Proxy-Connection: Keep-Alive
> Pragma: no-cache
> Range: bytes=0-100
>
* Request completely sent off
< HTTP/1.1 206 Partial Content
```

Nos Logs de acesso, você pode ver que a Ação é TCP_CLIENT_REFRESH_MISS/206:

```
1773942471.096 14 10.190.0.206 TCP_CLIENT_REFRESH_MISS/206 860 GET http://catalog.sf.dl.delivery.mp.mic
```

Informações Relacionadas

- Guia do usuário do AsyncOS 15.0 para Cisco Secure Web Appliance - GD (General Deployment) - Classifique os usuários finais para aplicação de política [Cisco Secure Web Appliance] - Cisco
- Configurar categorias de URL personalizadas no Secure Web Appliance - Cisco
- Como isentar o tráfego do Office 365 da autenticação e descriptografia no Cisco Web Security Appliance (WSA) - Cisco
- Configurar Parâmetro de Desempenho em Logs de Acesso
- Use as práticas recomendadas de dispositivos da Web seguros - Cisco
- Autenticação de desvio no Secure Web Appliance - 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.