SOPHOS

Configuring Web Protection on Sophos Firewall

Sophos Firewall
Version: 19.5v1

Web Policies

Web Protection Policies

- Incluir opções para controlar os usuários finais
- navegação na Web
- O SafeSearch impede que imagens, vídeos e textos potencialmente inadequados apareçam nos resultados da pesquisa
- As restrições do YouTube também restringem os resultados da pesquisa
- As cotas de tempo podem permitir acesso limitado
- para sites restritos

Policy Rules

- Definir o tipo de uso a ser restrito
-
- Especificar filtros de conteúdo para restringir o conteúdo da Web que contém quaisquer termos nas listas
-
- Definir a ação a ser executada quando o firewall encontrar tráfego que corresponda aos critérios da regra
-

SOPHOS

As políticas da Web podem ser usadas para controlar as atividades de navegação na Web dos usuários finais. As políticas incluem opções para:

SafeSearch, que impede que imagens, vídeos e textos potencialmente inadequados apareçam nos resultados de pesquisa do Google, Yahoo e Bing.
Restrições do YouTube, que impedem o acesso a conteúdo potencialmente impróprio, restringindo os resultados de pesquisa do YouTube.

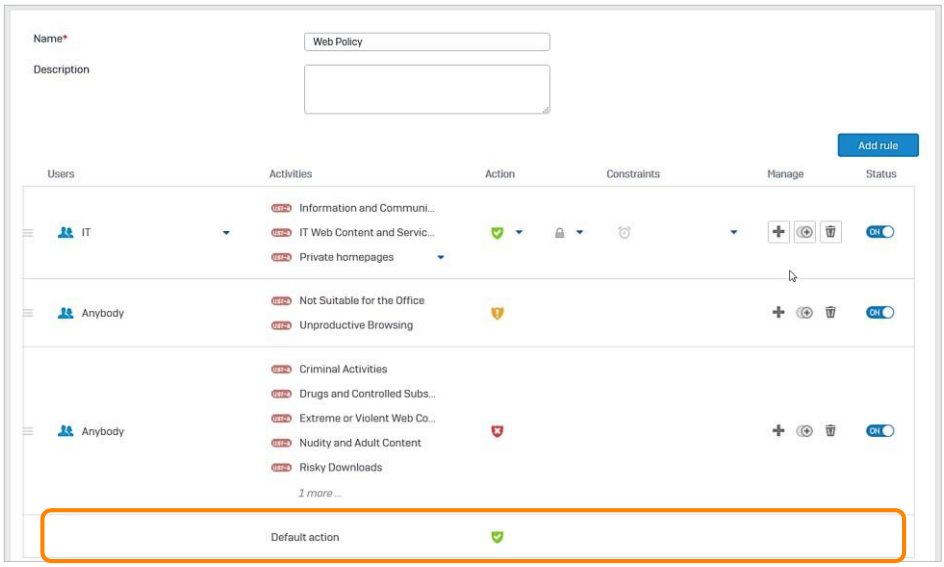
Cotas de tempo, que permitem o acesso a sites restritos, como compras on-line, por um período limitado.

As políticas incluem regras, que são usadas para:

Defina o tipo de uso a ser restringido. Isso pode incluir atividades do usuário, categorias, grupos de URL, arquivo tipos e categorias dinâmicas.
Especifique filtros de conteúdo para restringir o conteúdo da Web que contenha quaisquer termos nas listas.

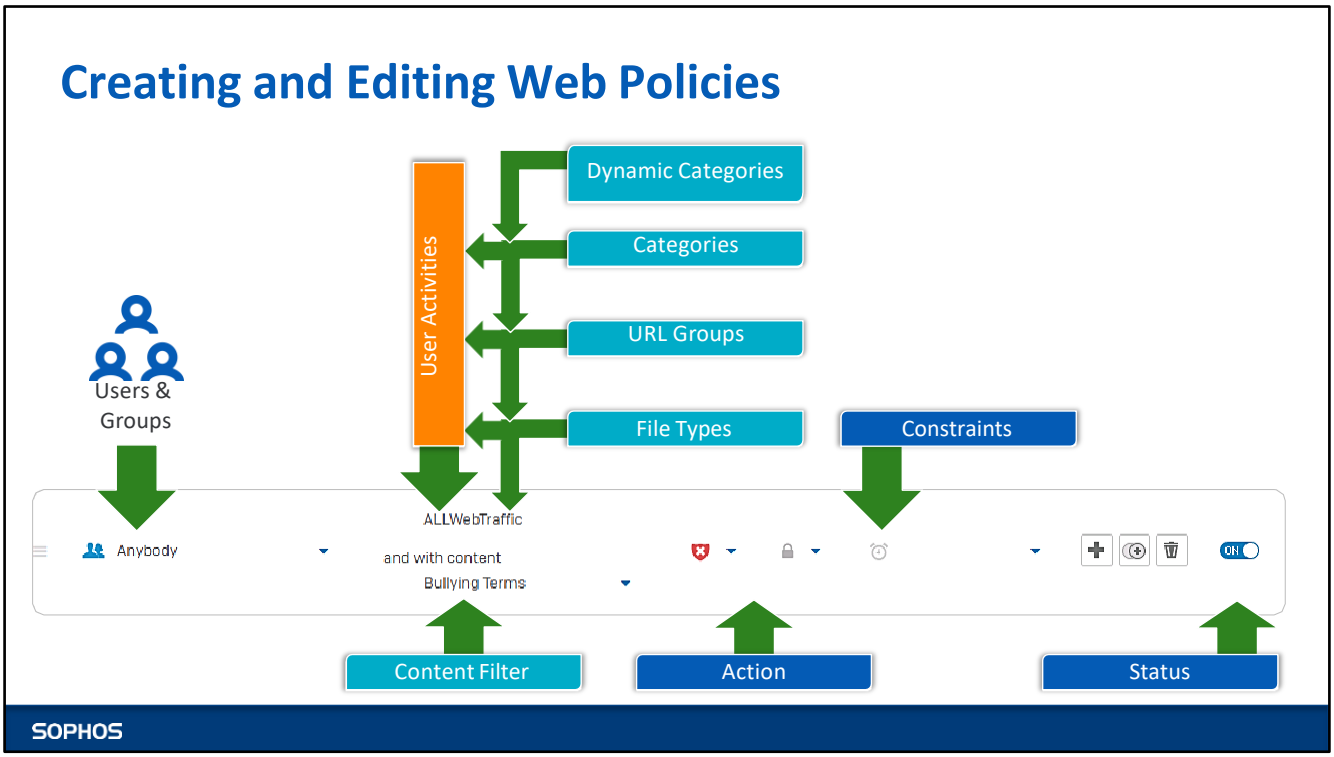
Defina a ação a ser executada quando o firewall encontrar tráfego HTTP que corresponda aos critérios da regra.

Creating and Editing Web Policies



SOPHOS

Isso mostra um exemplo de uma política da Web. Ele tem uma lista ordenada de regras e uma ação padrão, neste caso permitir, que determina o comportamento se o tráfego não corresponder a nenhuma das regras.



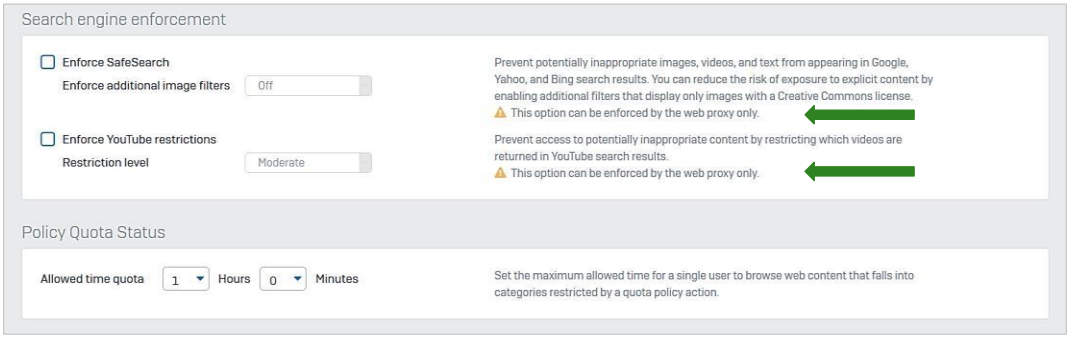
Cada regra de política da Web se aplica a usuários e grupos específicos ou a qualquer pessoa.
Você define as atividades ou os tipos de tráfego da Web que serão controlados pela regra e, opcionalmente, também pode aplicar um filtro de conteúdo de palavra-chave ao tráfego.

Cada regra tem uma ação, permitir, avisar, cotar ou bloquear, e isso pode ser substituído. Há também uma ação separada aplicada ao tráfego HTTPS.

Você pode definir restrições de tempo para a regra. Se nenhuma restrição de tempo for selecionada, a regra será ativo o tempo todo.

Finalmente, você pode habilitar e desabilitar regras individuais. Isso é especialmente útil ao criar novas regras e testes.

Web Policies



SOPHOS

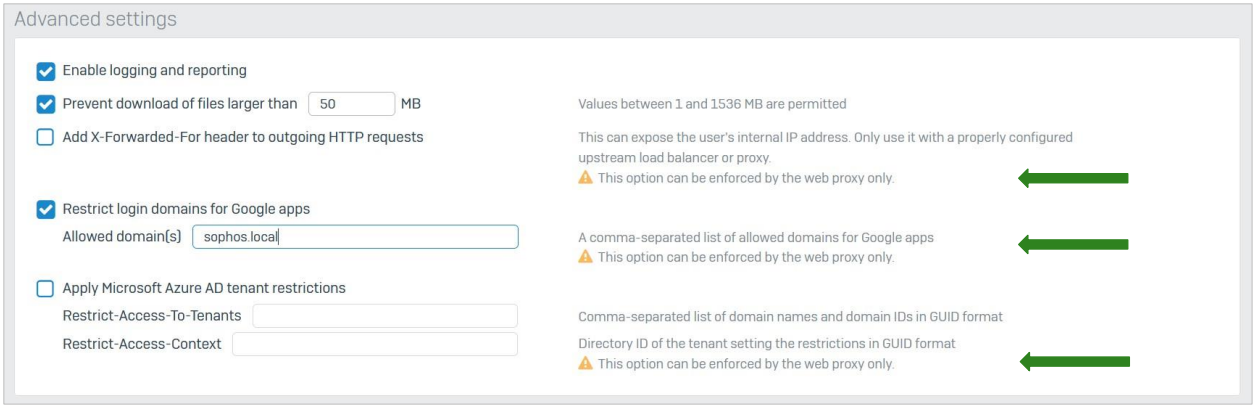
Abaixo das regras de política da Web estão outras opções, algumas das quais exigem que o proxy da Web seja aplicado. Estes são indicados com um aviso. Se essas opções forem selecionadas e usadas com o mecanismo DPI, elas não serão impostas.

As opções disponíveis são:

Aplique o SafeSearch em mecanismos de pesquisa comuns. Isso é feito modificando a solicitação para habilitar os recursos no mecanismo de pesquisa e requer a descriptografia do tráfego da Web.

Aplique as restrições do YouTube, o que é feito da mesma forma que a aplicação do SafeSearch. Configure quanto tempo de cota os usuários têm por dia.

Advanced Settings



SOPHOS

As configurações avançadas permitem:

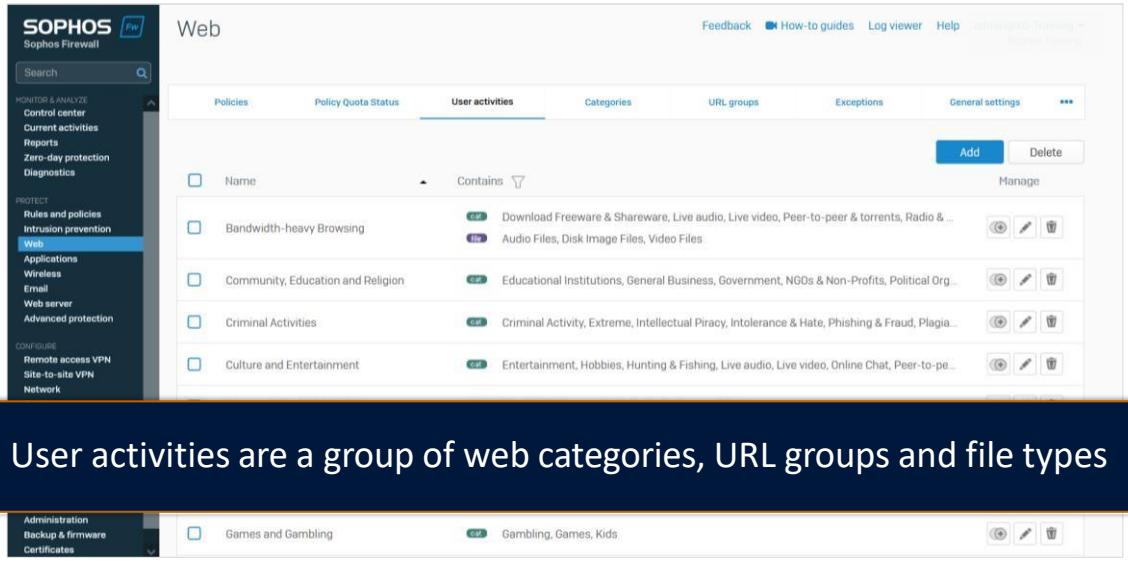
Inclua essa política em logs e relatórios.

Impedir o download de arquivos maiores que o tamanho especificado.

Adicione o cabeçalho X-Forwarded-For para transmitir o endereço IP da solicitação HTTP original.
Permita que os usuários façam login no Google Apps, como Gmail e Drive, somente com os domínios especificados.

Aplique restrições de locatário do Microsoft Azure AD.
Novamente, um aviso indica quais configurações exigem que o proxy da Web seja aplicado.

User Activities

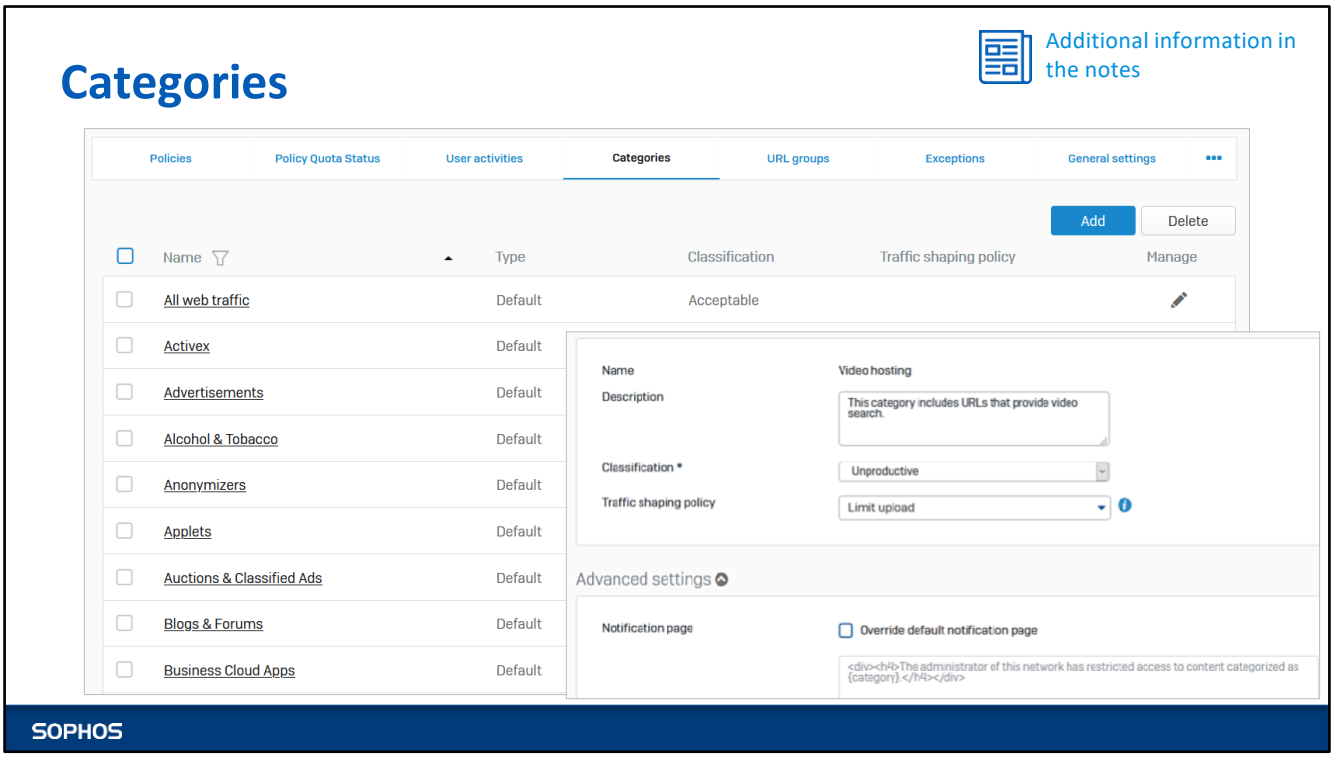


User activities are a group of web categories, URL groups and file types

SOPHOS

Vejamos os tipos de tráfego que você pode selecionar para controlar nas regras de política da Web, começando com Usuário Atividades.

As Atividades do Usuário são uma maneira de agrupar categorias da Web, grupos de URLs e tipos de arquivos em um único objeto para simplificar o gerenciamento.



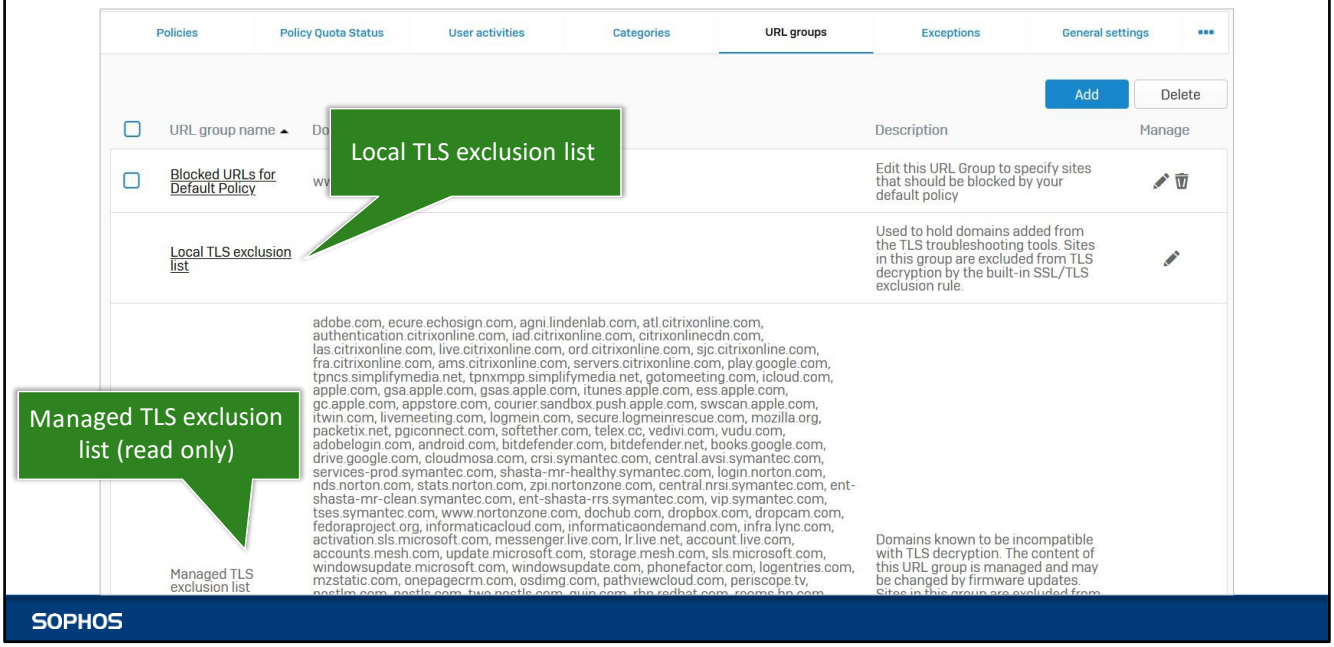
As categorias da Web são o que a maioria das pessoas pensa quando pensa em filtragem da Web. O Sophos Firewall vem com mais de 90 categorias da Web predefinidas, às quais você pode reclassificar e aplicar políticas de modelagem de tráfego.

Você também pode criar categorias da Web personalizadas com base em listas locais de domínios e palavras-chave ou em um banco de dados de URL externo.

[Informações adicionais]
Os bancos de dados de URL externos podem ser de um servidor HTTP ou FTP. O banco de dados deve estar em um dos os seguintes formatos:

..tar
.Ga
.Bz
.bz2
..txt
O banco de dados será verificado a cada duas horas para atualizações.

URL Groups

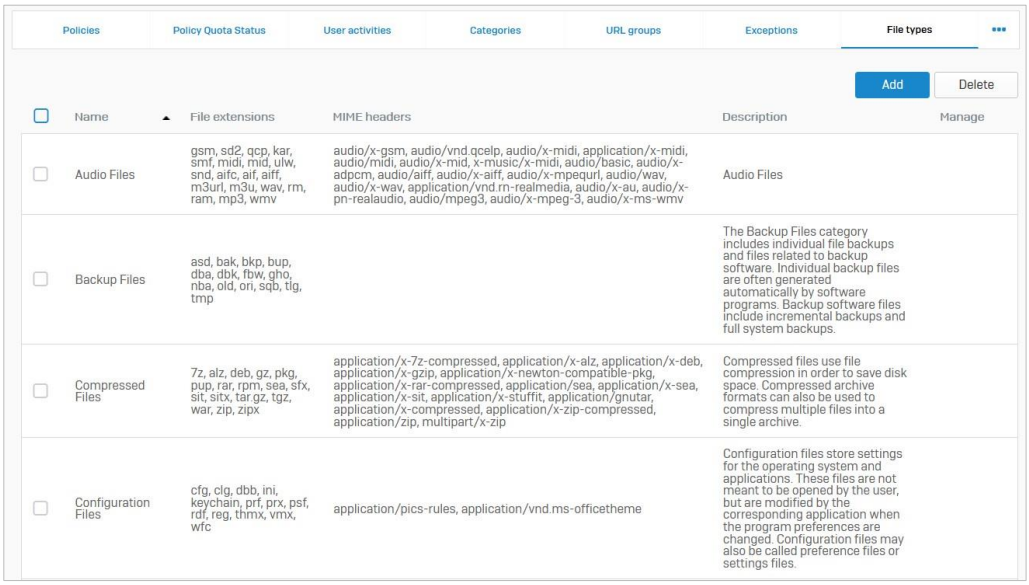


Os grupos de URLs são usados para criar uma lista de correspondência de domínios para os quais a configuração padrão deve não ser aplicado. Todos os subdomínios para os domínios inseridos também serão correspondidos.

Existem alguns grupos padrão importantes:
Lista de exclusão de TLS local, que você pode usar para gerenciar domínios para os quais não deseja descriptografar o tráfego.

Lista de exclusão de TLS gerenciado, que é uma lista gerenciada da Sophos de domínios excluídos da descriptografia de TLS. Nesta página você pode ver os domínios que estão incluídos, embora você não pode editar ou excluir este grupo.

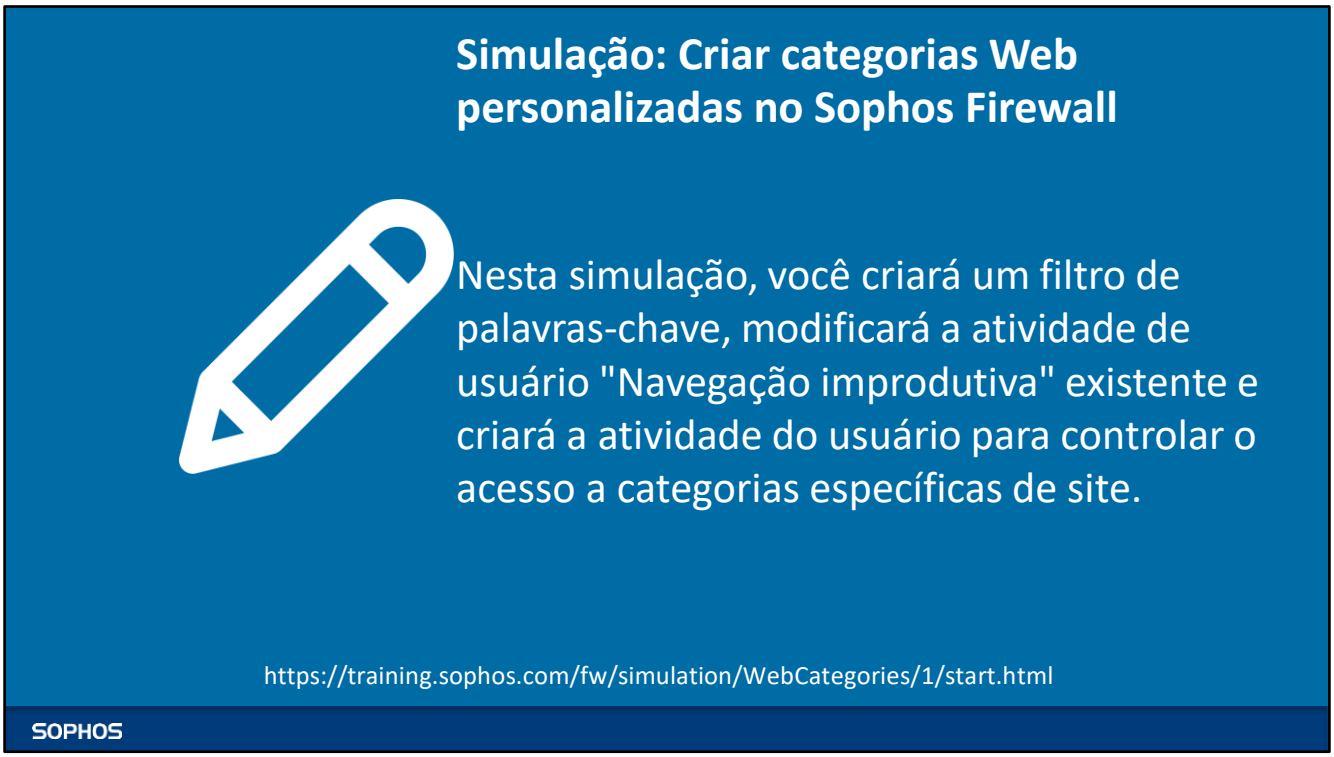
File Types



SOPHOS

Sophos Firewall pode gerenciar o acesso a arquivos através da política da web e vem com vários grupos de tipos de arquivo comuns definidos por extensão e tipo MIME.

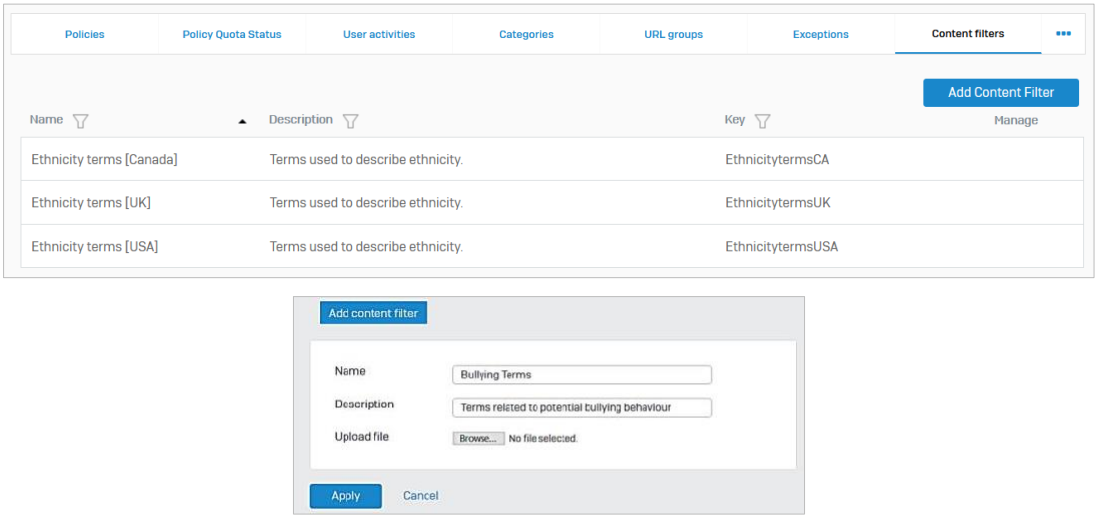
Você também pode criar tipos de arquivo personalizados, que podem usar um grupo existente como um modelo para importar tipos já definidos.



Nesta simulação, você criará um filtro de palavras-chave, modificará o usuário existente de 'Navegação improdutiva’ e criar atividade do usuário para controlar o acesso a categorias específicas do site.

[Informações adicionais]
https://training.sophos.com/fw/simulation/WebCategories/1/start.html

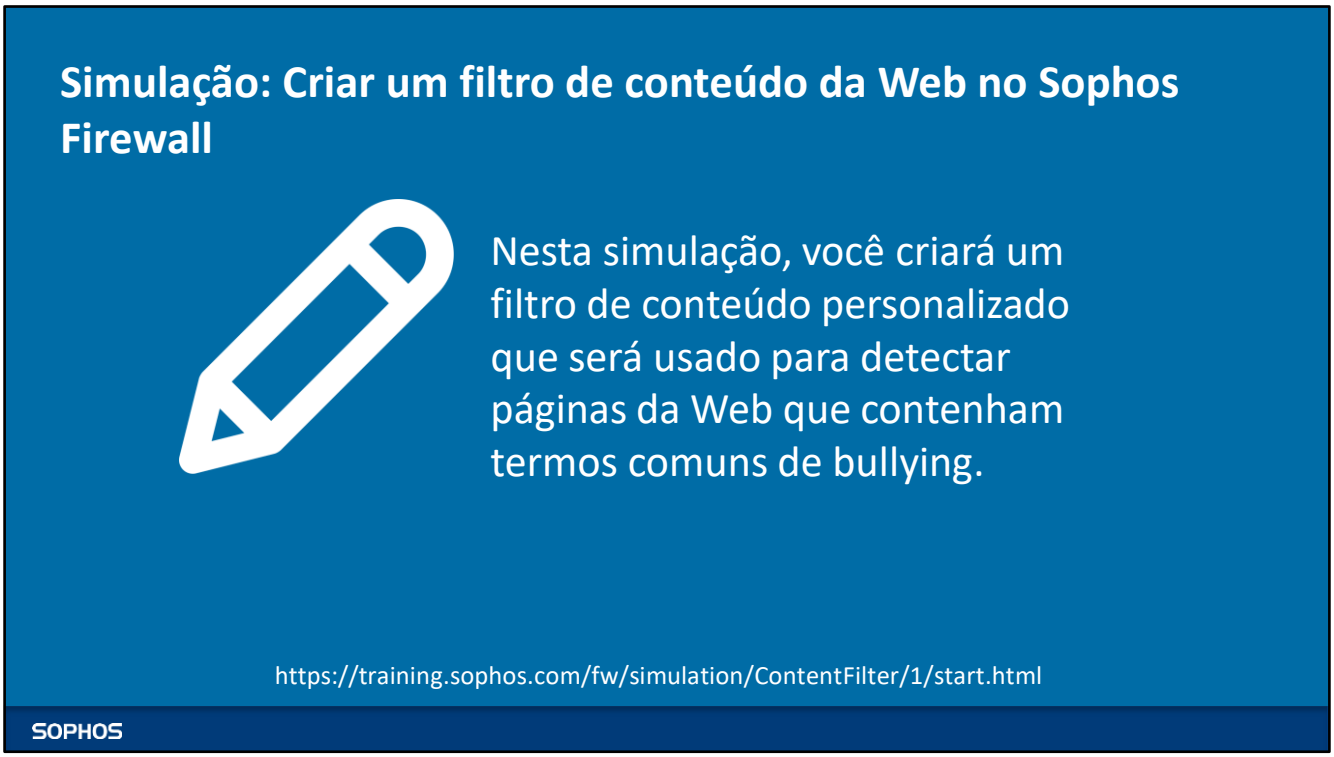
Content Filters



SOPHOS

As políticas da Web incluem a opção de registrar, monitorar e impor políticas relacionadas a listas de palavras-chave. Esse recurso é particularmente importante em ambientes educacionais para garantir a segurança infantil on-line e fornecer insights sobre os alunos usando palavras-chave relacionadas à automutilação, bullying, radicalização ou conteúdo inadequado. As bibliotecas de palavras-chave podem ser carregadas no Sophos Firewall e aplicadas a qualquer política de filtragem da Web como um critério adicional com ações para registrar e monitorar ou bloquear resultados de pesquisa ou sites que contenham as palavras-chave de interesse.

Relatórios abrangentes são fornecidos para identificar correspondências de palavras-chave e usuários que estão pesquisando ou consumindo conteúdo de palavras-chave de interesse, permitindo uma intervenção proativa antes que um usuário em risco se torne um problema real. As listas de palavras-chave são arquivos de texto sem formatação com um termo por linha.

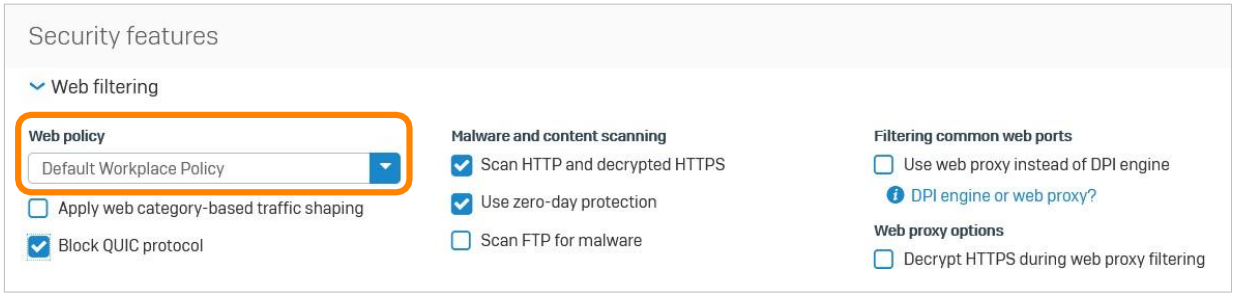


Nesta simulação, você criará um filtro de conteúdo personalizado que será usado para detectar páginas da Web quecontêm termos comuns de bullying.

[Additional Information]

https://training.sophos.com/fw/simulation/ContentFilter/1/start.html

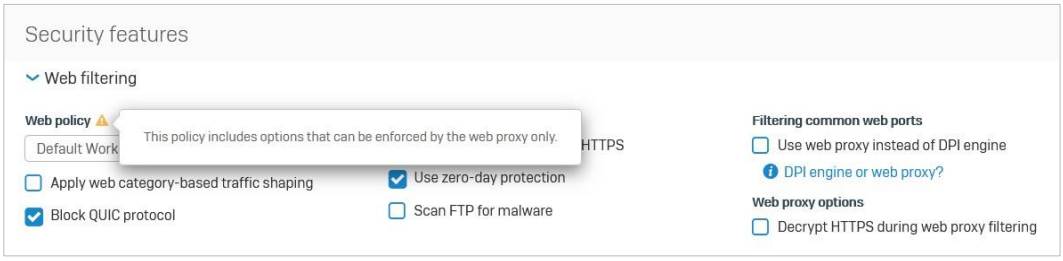
Applying Policies



SOPHOS

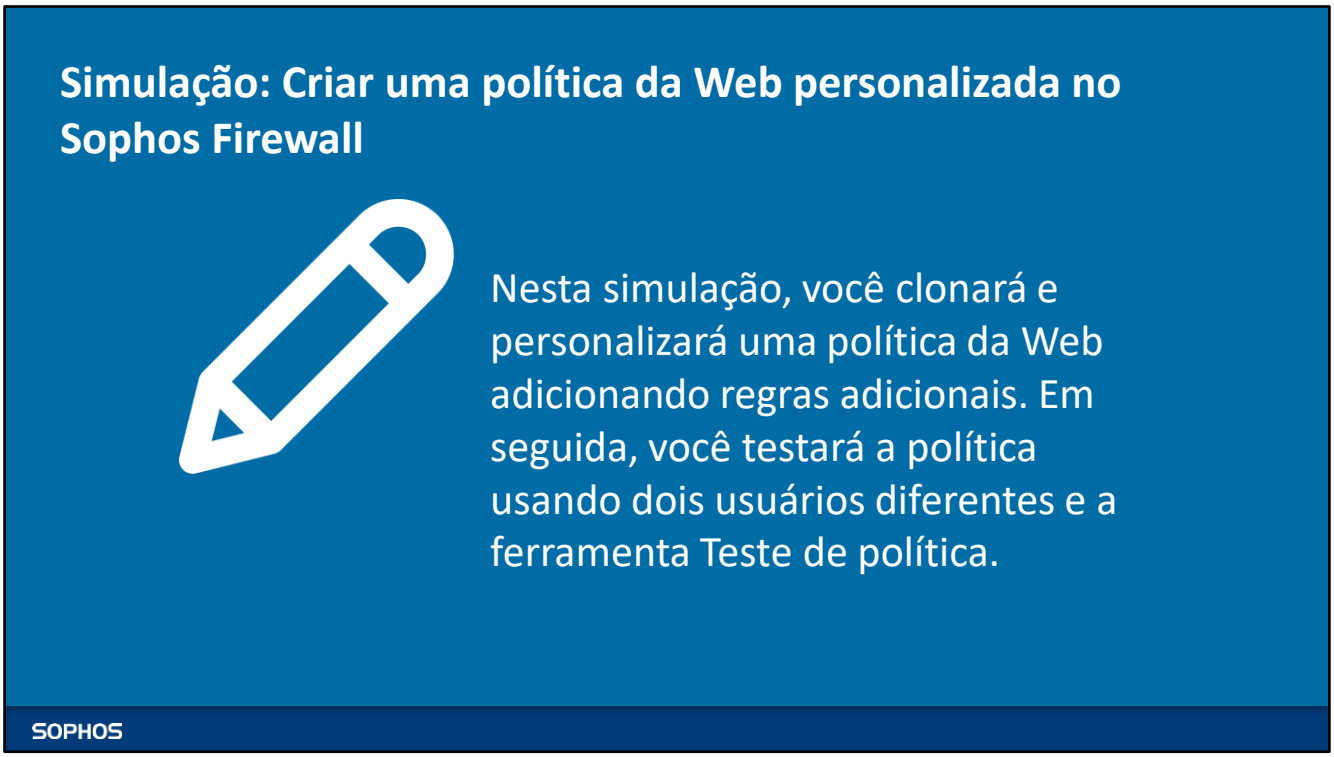
Depois de criar sua política da Web, você pode aplicá-la em regras de firewall.

Web Policies



SOPHOS

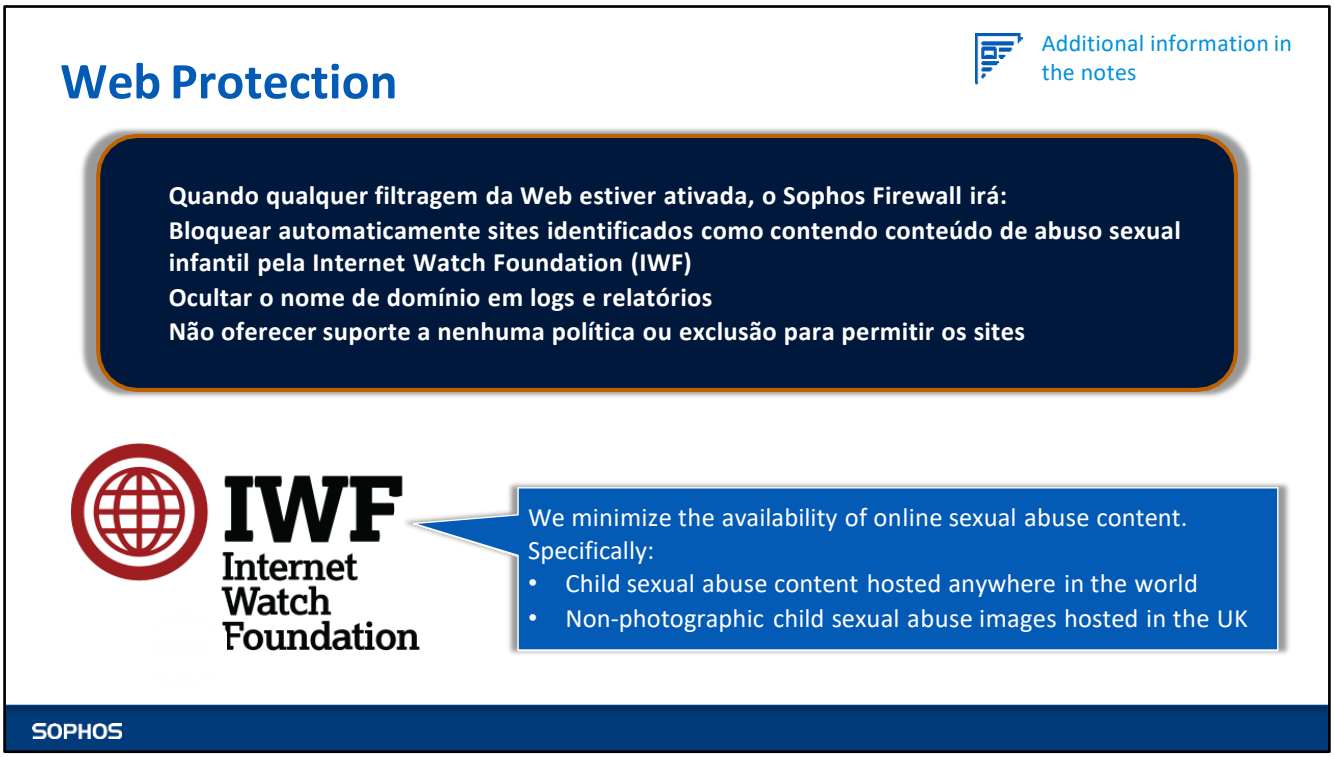
Se houver opções que não podem ser impostas, isso será indicado na regra de firewall com um triângulo de aviso. Passar o mouse sobre o aviso fornecerá informações adicionais.



Nesta simulação, você clonará e personalizará uma política da Web adicionando regras adicionais. Você vai em seguida, teste a política usando dois usuários diferentes e a ferramenta Teste de política.

[Additional Information]

https://training.sophos.com/fw/simulation/WebPolicy/1/start.html



Quando qualquer filtragem da Web estiver ativada, o Sophos Firewall bloqueará automaticamente os sites que estão identificado como contendo conteúdo de abuso sexual infantil pela Internet Watch Foundation.

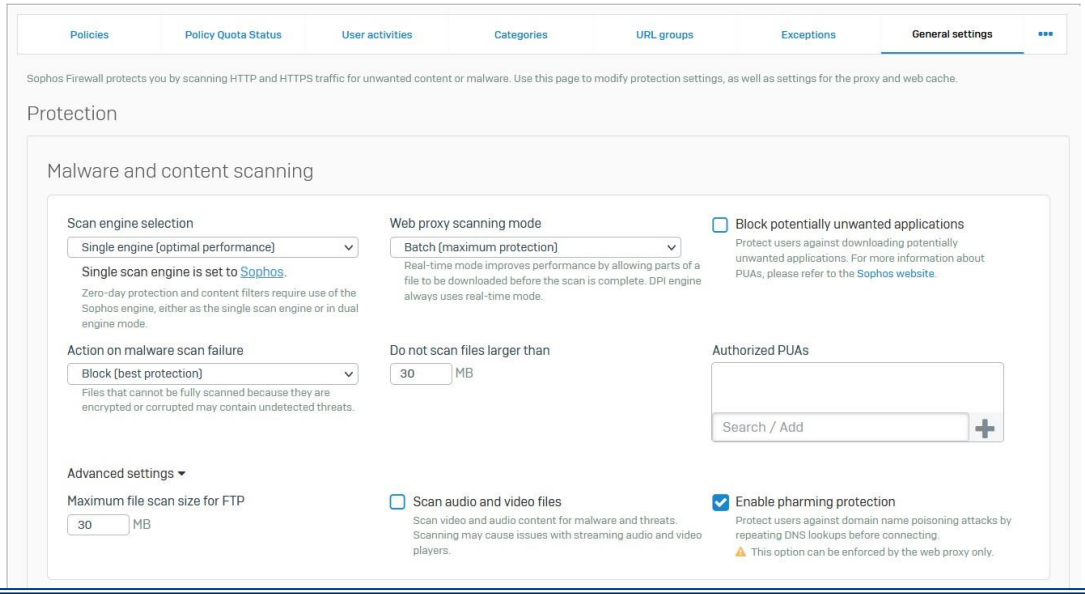
Nenhuma política ou exclusão pode ser configurada para permitir esses sites, e os nomes de domínio serão ocultos nos logs e relatórios.

[Additional Information]

Find out more about the IWF at https://www.iwf.org.uk

Protection Settings

Additional information in the notes



SOPHOS

Há várias configurações de proteção que podem ser gerenciadas nas configurações gerais do Web >, incluindo:

Seleção entre varredura de mecanismo único e duplo.
Modo de digitalização.

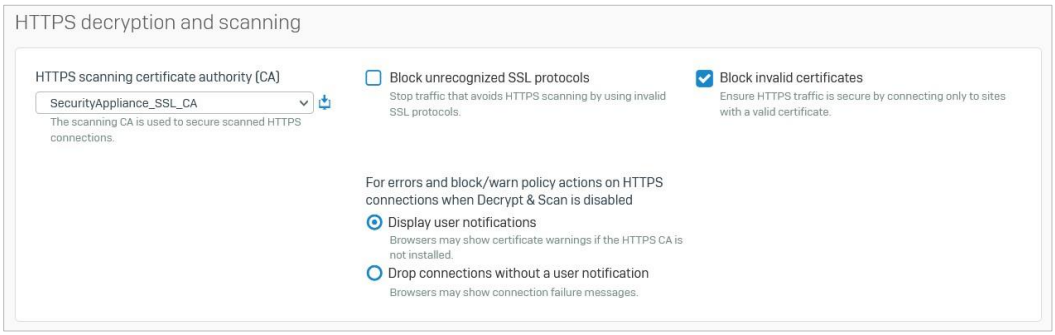
E a ação a ser tomada para conteúdo não escaneável e aplicativos potencialmente indesejados.
[Informações adicionais]

A proteção de dia zero requer o motor de digitalização Sophos; isso significa que você precisa selecionar o Sophos como o mecanismo de verificação primário (CONFIGURE > Serviços do sistema > Proteção contra malware) ou usar a verificação de mecanismo duplo.
O 'Modo de Verificação de Malware' pode ser definido como 'Tempo Real' para um processamento mais rápido ou 'Lote' para um mais
abordagem cautelosa.

Em seguida, devemos decidir sobre como lidar com o conteúdo que não pode ser verificado devido a fatores como criptografia ou proteção por senha. A opção mais segura é bloquear esse conteúdo, mas ele pode ser permitido se necessário.

Uma opção está disponível como parte da proteção da Web para bloquear o download de Aplicativos Potencialmente Indesejados. Aplicações específicas podem ser permitidas adicionando-as à lista de APIs autorizadas; e isso é aplicado como parte da proteção contra malware nas regras de firewall.

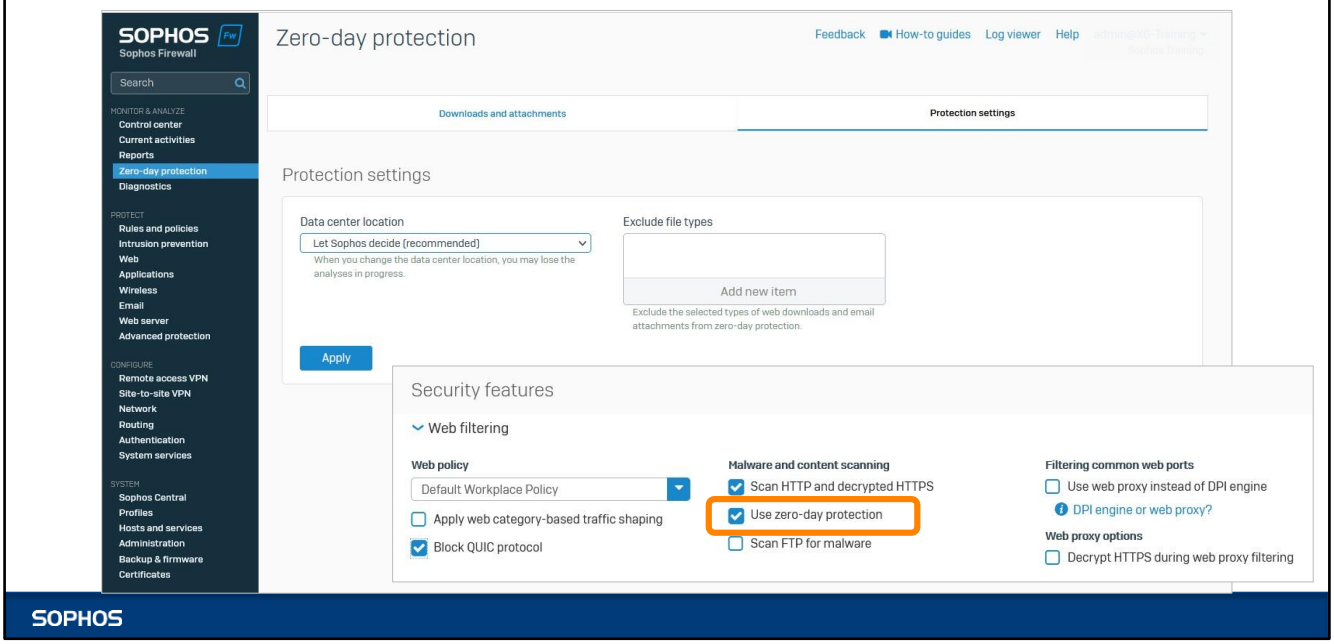
Protection Settings



SOPHOS

As configurações de descriptografia e varredura HTTPS nesta página permitem que você altere a autoridade de certificação de assinatura e modifique o comportamento de varredura do proxy da Web herdado. Essas configurações não afetam as regras de descriptografia TLS.

Zero-Day Protection



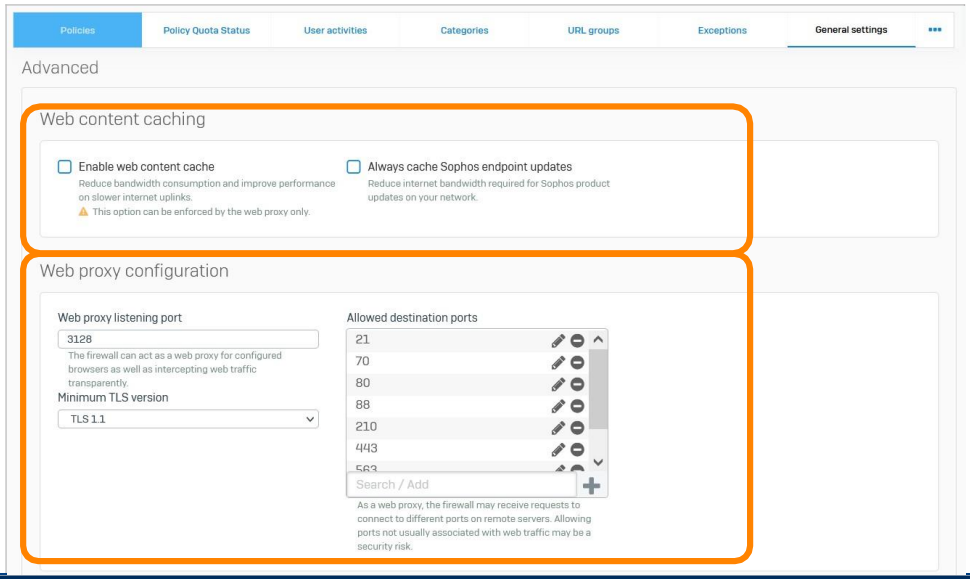
A configuração global de proteção de dia zero está em **PROTECT > Zero-day protection > Protection settings**.

Aqui você pode especificar se um datacenter da Ásia-Pacífico, Europa ou EUA será usado, ou deixar a Sophos decidir para onde enviar arquivos para análise com base em qual dará o melhor desempenho. Talvez seja necessário configurar isso para permanecer em conformidade com as leis de proteção de dados.

Você também pode optar por excluir determinados tipos de arquivo da proteção de dia zero usando as opções de tipo de arquivo predefinidas.

A verificação de proteção de dia zero está habilitada na seção Filtragem da Web das regras de firewall.

Advanced Settings



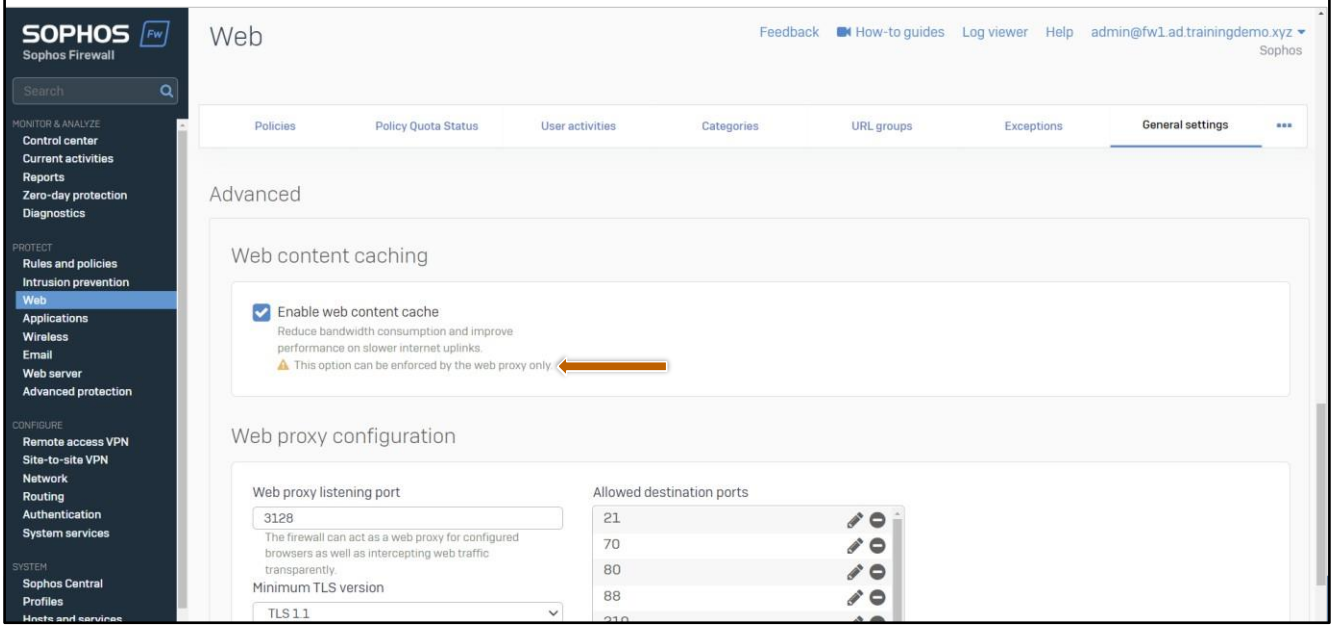
SOPHOS

Na guia Configurações gerais, também há algumas configurações avançadas nas quais você pode habilitar a Web cache e atualizações de ponto de extremidade Sophos.
Você também pode definir algumas configurações de proxy da Web:

A porta que os clientes devem usar para configurar o Sophos Firewall como um proxy explícito.
As portas às quais podem ser conectadas.

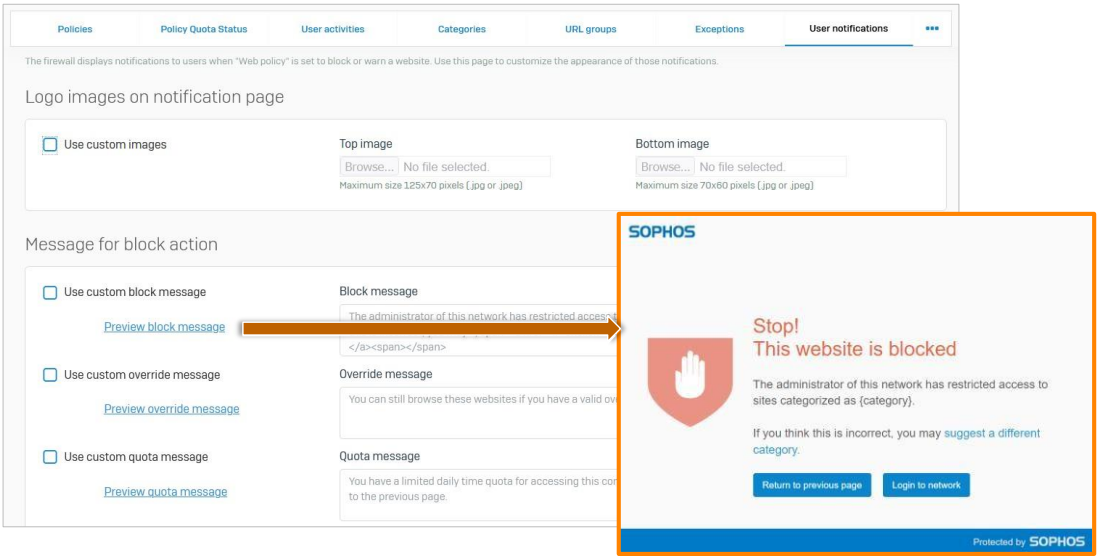
E a versão TLS mínima.

Web Proxy Content Caching



O Sophos Firewall pode ser configurado para armazenar em cache o conteúdo da Web, o que pode economizar largura de banda para sites com acesso limitado ou mais lento à Internet; no entanto, o proxy da Web é necessário para impor isso.

User Notifications

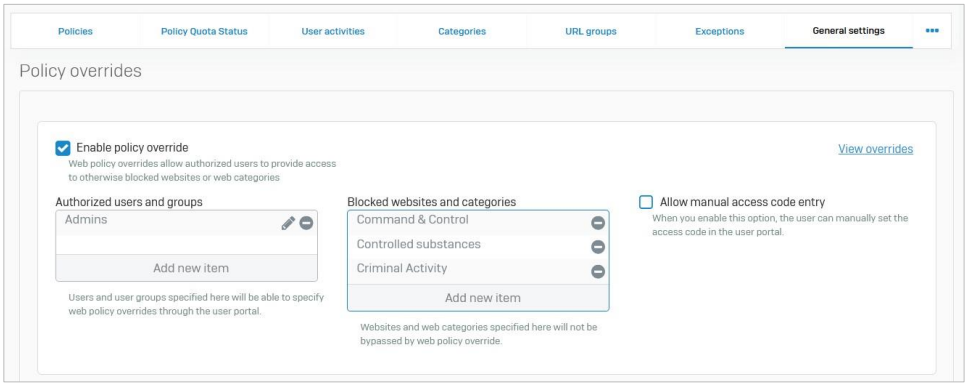


SOPHOS

Na guia Notificações do usuário, você pode modificar as imagens e o texto mostrados nas páginas de aviso e bloqueio. O texto pode incluir variáveis para exibir a categoria detectada e para vincular à sugestão de uma categoria diferente.

Você pode visualizar a aparência da mensagem quando os usuários a virem usando o link.

Policy Overrides

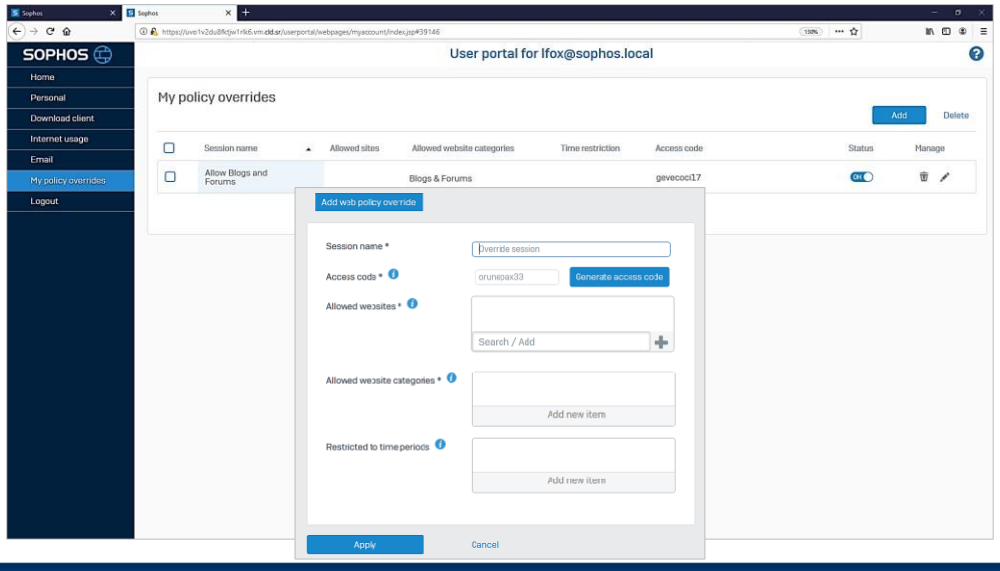


SOPHOS

As configurações de substituição de política da Web permitem que usuários autorizados substituam sites bloqueados em dispositivos de usuário, permitindo temporariamente o acesso.

Você define quais usuários (por exemplo, podem ser professores em uma configuração educacional) têm a opção de autorizar substituições de diretiva. Esses usuários podem então criar seus próprios códigos de substituição no Portal do Usuário do Sophos Firewall e definir regras sobre para quais sites eles podem ser usados. No WebAdmin, você pode ver uma lista completa de todos os códigos de substituição criados e desativá-los ou excluí-los, bem como definir sites ou categorias que nunca podem ser substituídos. Há também um relatório que fornece uma visão histórica completa sobre o uso de substituição da web.

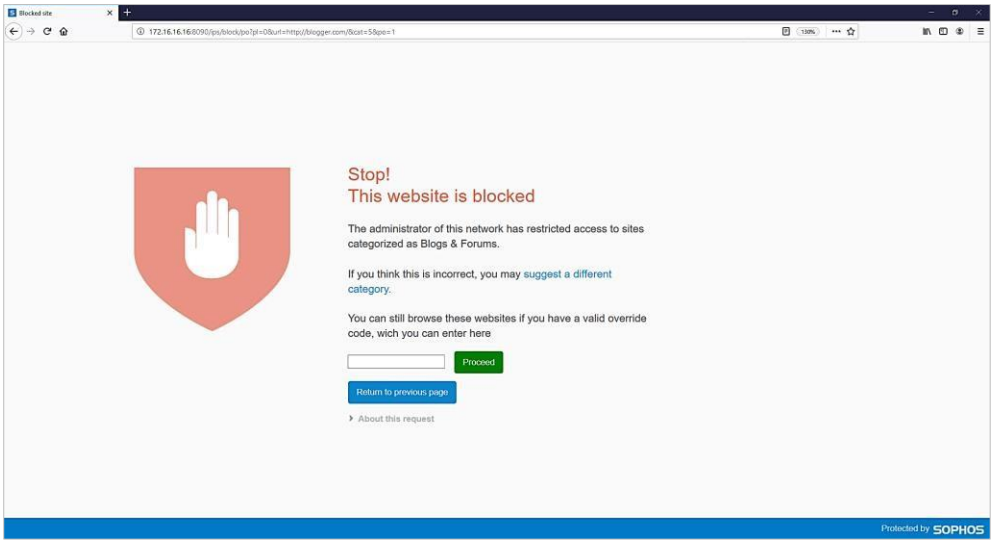
Policy Overrides



SOPHOS

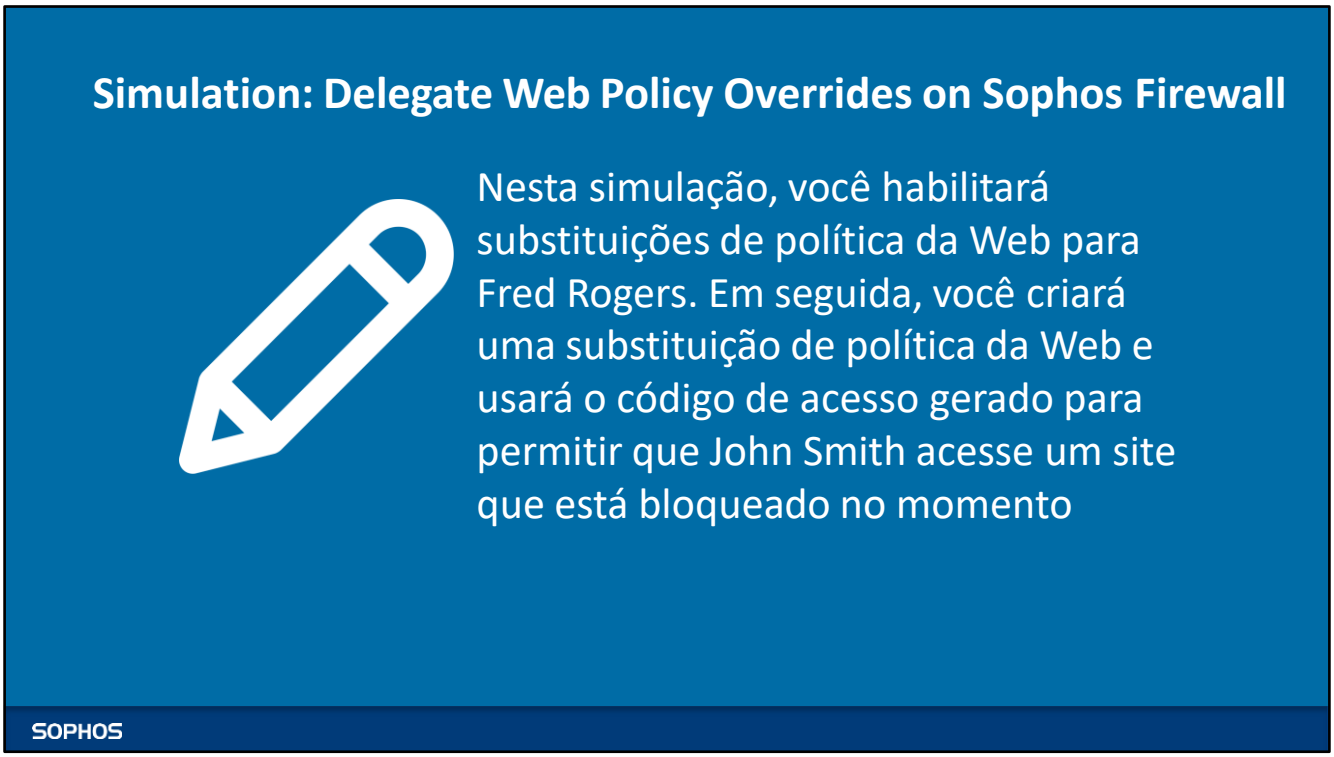
As regras de código de substituição podem ser amplas – permitindo qualquer tráfego ou categorias inteiras – ou mais restritas – permitindo apenas sites ou domínios individuais – e também podem ser limitadas por hora e dia. Para evitar abusos, os códigos podem ser facilmente alterados ou cancelados.

Policy Overrides



SOPHOS

Os códigos podem ser compartilhados com os usuários finais, que os inserem diretamente na página de bloqueio para permitir o acesso para um site bloqueado.

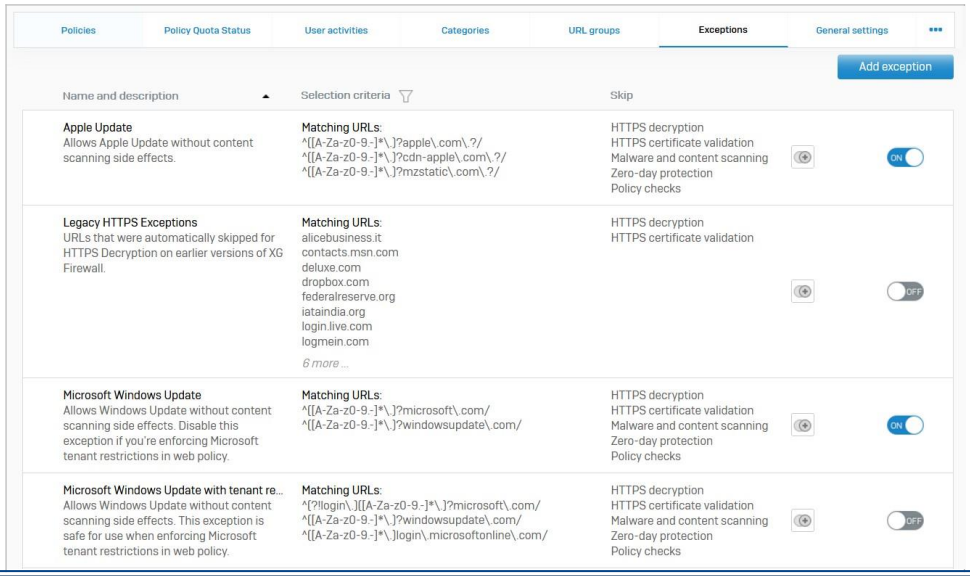


Nesta simulação, você habilitará substituições de política da Web para Fred Rogers. Em seguida, você criará uma substituição de política da Web e usará o código de acesso gerado para permitir que John Smith acesse um site que está bloqueado no momento.

[Informações adicionais]

https://training.sophos.com/fw/simulation/WebPolicyOverrides/1/start.html

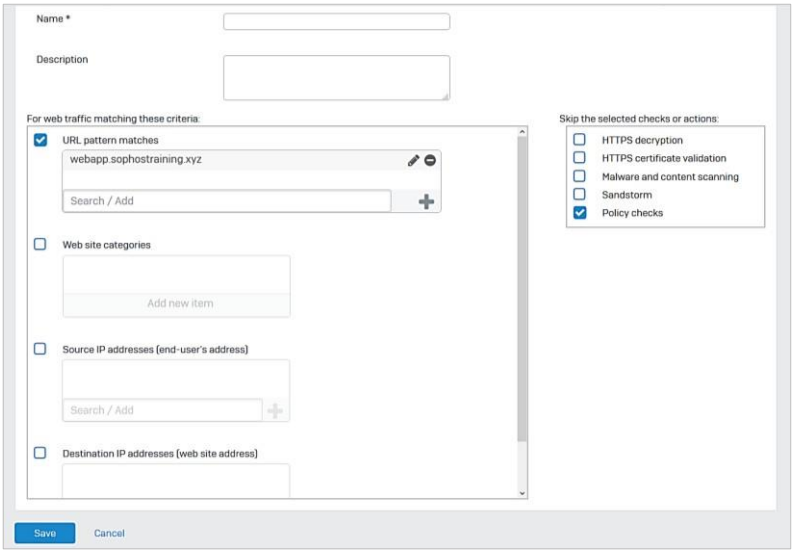
Exceptions



SOPHOS

As exceções encontradas na proteção da Web no Sophos Firewall podem ser usadas para ignorar determinadas verificações ou ações de segurança para quaisquer sites que correspondam aos critérios especificados na exceção. Existem algumas exceções predefinidas já no Sophos Firewall e mais podem ser criadas a critério do administrador. É importante observar que as exceções se aplicam a todas as políticas de proteção da Web, independentemente de onde elas são aplicadas no Sophos Firewall.

Exceptions



SOPHOS

As exceções podem ser correspondidas em qualquer combinação de:

Padrões de URL, que podem ser cadeias de caracteres simples ou expressões regulares.
Categorias do site.

Endereços IP de origem.

E endereços IP de destino.

Por favor, note que muitos sites têm vários endereços IP, e todos eles precisariam ser listados. Quando vários critérios de correspondência são usados, o tráfego deve corresponder a todos os critérios para corresponder com êxito. Em seguida, você pode selecionar quais verificações a exceção ignorará.