



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

Name*

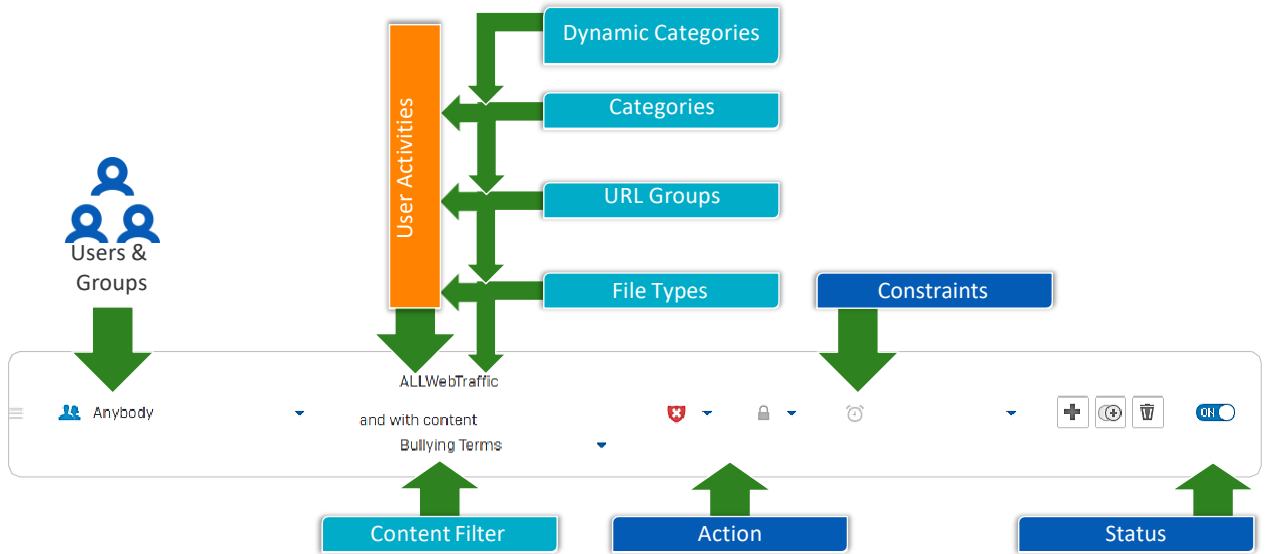
Description

Users	Activities	Action	Constraints	Manage	Status
IT	Information and Communi... IT Web Content and Servic... Private homepages	✓		<input type="button" value="+"/> <input type="button" value="⌂"/> <input type="button" value="🗑"/>	<input checked="" type="checkbox"/>
Anybody	Not Suitable for the Office Unproductive Browsing	⚠		<input type="button" value="+"/> <input type="button" value="⌂"/> <input type="button" value="🗑"/>	<input checked="" type="checkbox"/>
Anybody	Criminal Activities Drugs and Controlled Subs... Extreme or Violent Web Co... Nudity and Adult Content Risky Downloads <i>I more ...</i>	🛡		<input type="button" value="+"/> <input type="button" value="⌂"/> <input type="button" value="🗑"/>	<input checked="" type="checkbox"/>
Default action		✓			

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.

Creating and Editing Web Policies



SOPHOS

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

Search engine enforcement

☐ **Enforce SafeSearch**
Enforce additional image filters: Off

☐ **Enforce YouTube restrictions**
Restriction level: Moderate

Prevent potentially inappropriate images, videos, and text from appearing in Google, Yahoo, and Bing search results. You can reduce the risk of exposure to explicit content by enabling additional filters that display only images with a Creative Commons license.
⚠ This option can be enforced by the web proxy only.

Prevent access to potentially inappropriate content by restricting which videos are returned in YouTube search results.
⚠ This option can be enforced by the web proxy only.

Policy Quota Status

Allowed time quota: 1 Hours 0 Minutes

Set the maximum allowed time for a single user to browse web content that falls into categories restricted by a quota policy action.

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 descrição 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

Advanced settings

<input checked="" type="checkbox"/> Enable logging and reporting		
<input checked="" type="checkbox"/> Prevent download of files larger than <input type="text" value="50"/> MB	Values between 1 and 1536 MB are permitted	
<input type="checkbox"/> Add X-Forwarded-For header to outgoing HTTP requests	This can expose the user's internal IP address. Only use it with a properly configured upstream load balancer or proxy. ⚠ This option can be enforced by the web proxy only.	←
<input checked="" type="checkbox"/> Restrict login domains for Google apps		
Allowed domain(s) <input type="text" value="sophos.local"/>	A comma-separated list of allowed domains for Google apps ⚠ This option can be enforced by the web proxy only.	←
<input type="checkbox"/> Apply Microsoft Azure AD tenant restrictions		
Restrict-Access-To-Tenants <input type="text"/>	Comma-separated list of domain names and domain IDs in GUID format	
Restrict-Access-Context <input type="text"/>	Directory ID of the tenant setting the restrictions in GUID format ⚠ This option can be enforced by the web proxy only.	←

SOPHOS

As configurações avançadas permitem:

Inclua essa política em logs e relatórios.

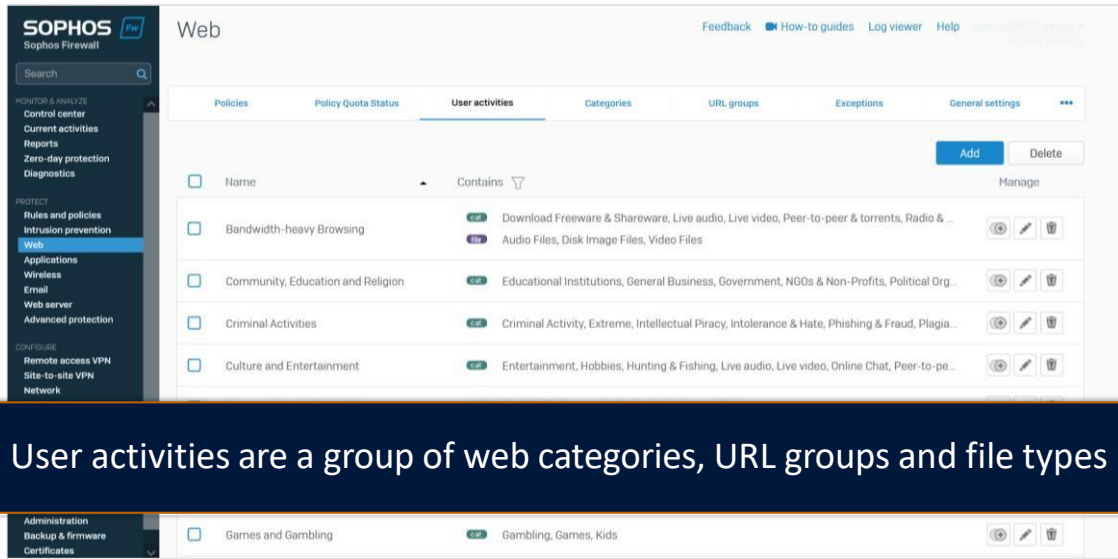
Impedir o download de arquivos maiores que o tamanho especificado.

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



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.



Additional information in the notes

Categories

Policies	Policy Quota Status	User activities	Categories	URL groups	Exceptions	General settings	...
				<div>AddDelete</div>			
<input type="checkbox"/>	Name ▾	Type ▲	Classification	Traffic shaping policy		Manage	
<input type="checkbox"/>	All web traffic	Default	Acceptable				
<input type="checkbox"/>	Activex	Default					
<input type="checkbox"/>	Advertisements	Default					
<input type="checkbox"/>	Alcohol & Tobacco	Default					
<input type="checkbox"/>	Anonymizers	Default					
<input type="checkbox"/>	Applets	Default					
<input type="checkbox"/>	Auctions & Classified Ads	Default					
<input type="checkbox"/>	Blogs & Forums	Default					
<input type="checkbox"/>	Business Cloud Apps	Default					

Name

Description

Classification *

Traffic shaping policy

Video hosting

This category includes URLs that provide video search.

Unproductive

Limit upload

Advanced settings ⓘ

Notification page

☐ Override default notification page

<div><h1>The administrator of this network has restricted access to content categorized as (category).</h1></div>

SOPHOS

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

Local TLS exclusion list

Managed TLS exclusion list (read only)

adobe.com, ecure.echosign.com, agni.lindenlab.com, atl.citrixonline.com, authentication.citrixonline.com, iad.citrixonline.com, citrixonlinecdn.com, las.citrixonline.com, live.citrixonline.com, ord.citrixonline.com, sjc.citrixonline.com, fra.citrixonline.com, ams.citrixonline.com, servers.citrixonline.com, play.google.com, tpncs.simpliflymedia.net, tpnxmmp.simpliflymedia.net, gotomeeting.com, icloud.com, apple.com, gsa.apple.com, gsas.apple.com, itunes.apple.com, ess.apple.com, gc.apple.com, appstore.com, courier.sandbox.push.apple.com, swscan.apple.com, itwin.com, livemeeting.com, logmein.com, secure.logmeinrescue.com, mozilla.org, packetix.net, pgiconnect.com, softether.com, telex.cc, vedivi.com, vudu.com, adobelogin.com, android.com, bitdefender.com, bitdefender.net, books.google.com, drive.google.com, cloudmosa.com, crsi.symantec.com, central.avsi.symantec.com, services-prod.symantec.com, shasta-mr-healthy.symantec.com, login.norton.com, nds.norton.com, stats.norton.com, zpi.nortonzone.com, central.nrsl.symantec.com, ent-shasta-mr-clean.symantec.com, ent-shasta-rs.symantec.com, vip.symantec.com, tses.symantec.com, www.nortonzone.com, dochub.com, dropbox.com, dropcam.com, fedoraproject.org, informaticloud.com, informaticloudemand.com, infra.lync.com, activation.sls.microsoft.com, messenger.live.com, lr.live.net, account.live.com, accounts.mesh.com, update.microsoft.com, storage.mesh.com, sls.microsoft.com, windowsupdate.microsoft.com, windowsupdate.com, phonefactor.com, logentries.com, mzstatic.com, onepagecrm.com, osdimg.com, pathviewcloud.com, periscope.tv, nortec.com, nortec.com, two.nortec.com, quip.com, the.redhat.com, zoom.hq.com

Domains known to be incompatible with TLS decryption. The content of this URL group is managed and may be changed by firmware updates. Sites in this group are excluded from

SOPHOS

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

Policies	Policy Quota Status	User activities	Categories	URL groups	Exceptions	File types	***
						<div>Add</div>	<div>Delete</div>
<input type="checkbox"/>	Name	File extensions	MIME headers	Description		Manage	
<input type="checkbox"/>	Audio Files	gsm, sd2, qcp, kar, smf, midi, mid, ulw, snd, aifc, aif, aiff, m3uri, m3u, wav, rm, ram, mp3, wmv	audio/x-gsm, audio/vnd.qcelp, audio/x-midi, application/x-midi, audio/midi, audio/x-mid, x-music/x-midi, audio/basic, audio/x-adpcm, audio/aiff, audio/x-aiff, audio/x-mpegurl, audio/wav, audio/x-wav, application/vnd.rn-realmedia, audio/x-au, audio/x-pn-realaudio, audio/mpeg3, audio/x-mpeg-3, audio/x-ms-wmv	Audio Files			
<input type="checkbox"/>	Backup Files	asd, bak, bkp, bup, dba, dbk, fbw, gho, nba, old, ori, sqb, tlg, tmp		The Backup Files category includes individual file backups and files related to backup software. Individual backup files are often generated automatically by software programs. Backup software files include incremental backups and full system backups.			
<input type="checkbox"/>	Compressed Files	7z, alz, deb, gz, pkg, pup, rar, rpm, sea, sfx, sit, sitx, tar.gz, tgz, war, zip, zipx	application/x-7z-compressed, application/x-alz, application/x-deb, application/x-gzip, application/x-newton-compatible-pkg, application/x-rar-compressed, application/sea, application/x-sea, application/x-sit, application/x-stuffit, application/gnutar, application/x-compressed, application/x-zip-compressed, application/zip, multipart/x-zip	Compressed files use file compression in order to save disk space. Compressed archive formats can also be used to compress multiple files into a single archive.			
<input type="checkbox"/>	Configuration Files	cfg, clg, dbb, ini, keychain, prf, prx, psf, rdt, reg, thmx, vmtx, wfc	application/pics-rules, application/vnd.ms-officetheme	Configuration files store settings for the operating system and applications. These files are not meant to be opened by the user, but are modified by the corresponding application when the program preferences are changed. Configuration files may also be called preference files or settings files.			

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.

Simulação: Criar categorias Web personalizadas no Sophos Firewall



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

<https://training.sophos.com/fw/simulation/WebCategories/1/start.html>

SOPHOS

Nesta simulação, você criará um filtro de palavras-chave, modificará o usuário existente de 'Navegação improdutiva' e criará 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

Policies	Policy Quota Status	User activities	Categories	URL groups	Exceptions	Content filters	***
							Add Content Filter
Name	Description	Key	Manage				
Ethnicity terms [Canada]	Terms used to describe ethnicity.	EthnicitytermsCA					
Ethnicity terms [UK]	Terms used to describe ethnicity.	EthnicitytermsUK					
Ethnicity terms [USA]	Terms used to describe ethnicity.	EthnicitytermsUSA					

Add content filter

Name

Bullying Terms

Description

Terms related to potential bullying behaviour

Upload file

Browse...

No file selected.

Apply

Cancel

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.

Simulação: Criar um filtro de conteúdo da Web no Sophos Firewall



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

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

SOPHOS

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

[Additional Information]

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

Applying Policies

Security features

Web filtering

Web policy

Default Workplace Policy

☐ Apply web category-based traffic shaping

☒ Block QUIC protocol

Malware and content scanning

☒ Scan HTTP and decrypted HTTPS

☒ Use zero-day protection

☐ Scan FTP for malware

Filtering common web ports

☐ Use web proxy instead of DPI engine

DPI engine or web proxy?

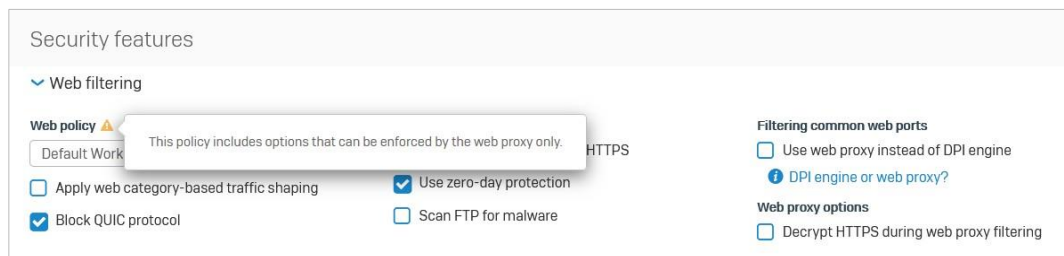
Web proxy options

☐ Decrypt HTTPS during web proxy filtering

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.

Simulação: Criar uma política da Web personalizada no Sophos Firewall



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

SOPHOS

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 irá:
Bloquear automaticamente sites identificados como contendo conteúdo de abuso sexual infantil pela Internet Watch Foundation (IWF)
Ocultar o nome de domínio em logs e relatórios
Não oferecer suporte a nenhuma política ou exclusão para permitir os sites



We minimize the availability of online sexual abuse content.
Specifically:

- Child sexual abuse content hosted anywhere in the world
- Non-photographic child sexual abuse images hosted in the UK

SOPHOS

Quando qualquer filtragem da Web estiver ativada, o Sophos Firewall bloqueará automaticamente os sites que estão identificados 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

Policies Policy Quota Status User activities Categories URL groups Exceptions **General settings** ***

Sophos Firewall protects you by scanning HTTP and HTTPS traffic for unwanted content or malware. Use this page to modify protection settings, as well as settings for the proxy and web cache.

Protection

Malware and content scanning

Scan engine selection
Single engine (optimal performance) ▼
Single scan engine is set to [Sophos](#).
Zero-day protection and content filters require use of the Sophos engine, either as the single scan engine or in dual engine mode.

Web proxy scanning mode
Batch (maximum protection) ▼
Real-time mode improves performance by allowing parts of a file to be downloaded before the scan is complete. DPI engine always uses real-time mode.

☐ Block potentially unwanted applications
Protect users against downloading potentially unwanted applications. For more information about PUAs, please refer to the [Sophos website](#).

Action on malware scan failure
Block (best protection) ▼
Files that cannot be fully scanned because they are encrypted or corrupted may contain undetected threats.

Do not scan files larger than
30 MB

Authorized PUAs
Search / Add +

Advanced settings ▼

Maximum file scan size for FTP
30 MB

☐ Scan audio and video files
Scan video and audio content for malware and threats. Scanning may cause issues with streaming audio and video players.

☒ Enable phishing protection
Protect users against domain name poisoning attacks by repeating DNS lookups before connecting.
⚠ This option can be enforced by the web proxy only.

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

HTTPS decryption and scanning

HTTPS scanning certificate authority (CA)

SecurityAppliance_SSL_CA

The scanning CA is used to secure scanned HTTPS connections.

☐

Block unrecognized SSL protocols

Stop traffic that avoids HTTPS scanning by using invalid SSL protocols.

☒

Block invalid certificates

Ensure HTTPS traffic is secure by connecting only to sites with a valid certificate.

For errors and block/warn policy actions on HTTPS connections when Decrypt & Scan is disabled

☒

Display user notifications

Browsers may show certificate warnings if the HTTPS CA is not installed.

☐

Drop connections without a user notification

Browsers may show connection failure messages.

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

The screenshot displays the Sophos Firewall management console. The left sidebar contains a navigation menu with sections: MONITOR & ANALYZE (Control center, Current activities, Reports, Zero-day protection, Diagnostics), PROTECT (Rules and policies, Intrusion prevention, Web, Applications, Wireless, Email, Web server, Advanced protection), CONFIGURE (Remote access VPN, Site-to-site VPN, Network, Routing, Authentication, System services), and SYSTEM (Sophos Central, Profiles, Hosts and services, Administration, Backup & firmware, Certificates). The main content area is titled 'Zero-day protection' and has tabs for 'Downloads and attachments' and 'Protection settings'. The 'Protection settings' tab is active, showing a 'Data center location' dropdown set to 'Let Sophos decide (recommended)', an 'Exclude file types' section with an 'Add new item' button, and a 'Security features' section. Under 'Web filtering', the 'Web policy' is 'Default Workplace Policy'. Under 'Malware and content scanning', 'Scan HTTP and decrypted HTTPS' and 'Use zero-day protection' are checked. Under 'Filtering common web ports', 'Use web proxy instead of DPI engine' is unchecked. A blue box highlights the 'Use zero-day protection' checkbox.

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

The screenshot shows the 'Advanced' settings page in the Sophos Firewall management console. The 'General settings' tab is selected. Two sections are highlighted with orange boxes:

- Web content caching:** Contains two checkboxes. The first, 'Enable web content cache', is unchecked and has a note: 'Reduce bandwidth consumption and improve performance on slower internet uplinks. This option can be enforced by the web proxy only.' The second, 'Always cache Sophos endpoint updates', is also unchecked and has a note: 'Reduce internet bandwidth required for Sophos product updates on your network.'
- Web proxy configuration:** Contains a 'Web proxy listening port' field set to '3128' with a note: 'The firewall can act as a web proxy for configured browsers as well as intercepting web traffic transparently.' Below it is a 'Minimum TLS version' dropdown set to 'TLS 1.1'. To the right is a list of 'Allowed destination ports' including 21, 70, 80, 88, 210, 443, and 563, each with a delete icon. A 'Search / Add' button and a plus icon are at the bottom of the list. A warning note at the bottom states: 'As a web proxy, the firewall may receive requests to connect to different ports on remote servers. Allowing ports not usually associated with web traffic may be a security risk.'

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

The screenshot shows the Sophos Firewall management interface. The left sidebar contains navigation menus for 'MONITOR & ANALYZE', 'PROTECT', 'CONFIGURE', and 'SYSTEM'. The 'Web' option under 'PROTECT' is selected. The main content area is titled 'Web' and includes a top navigation bar with tabs: Policies, Policy Quota Status, User activities, Categories, URL groups, Exceptions, and General settings. The 'General settings' tab is active, showing the 'Advanced' section for 'Web content caching'. In this section, the 'Enable web content cache' checkbox is checked, with a note that it can be enforced by the web proxy only. Below this, the 'Web proxy configuration' section is visible, showing the 'Web proxy listening port' set to 3128 and a list of 'Allowed destination ports' including 21, 70, 80, 88, and 3128. The 'Minimum TLS version' is set to TLS 1.1.

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

Policies **Policy Quota Status** **User activities** **Categories** **URL groups** **Exceptions** **User notifications** ***

The firewall displays notifications to users when "Web policy" is set to block or warn a website. Use this page to customize the appearance of those notifications.

Logo images on notification page

☐ Use custom images

Top image
Browse... No file selected.
Maximum size 125x70 pixels (.jpg or .jpeg)

Bottom image
Browse... No file selected.
Maximum size 70x60 pixels (.jpg or .jpeg)

Message for block action

☐ Use custom block message
[Preview block message](#)

☐ Use custom override message
[Preview override message](#)

☐ Use custom quota message
[Preview quota message](#)

SOPHOS

Stop!
This website is blocked

The administrator of this network has restricted access to sites categorized as {category}.

If you think this is incorrect, you may suggest a [different category](#).

[Return to previous page](#) [Login to network](#)

Protected by **SOPHOS**

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

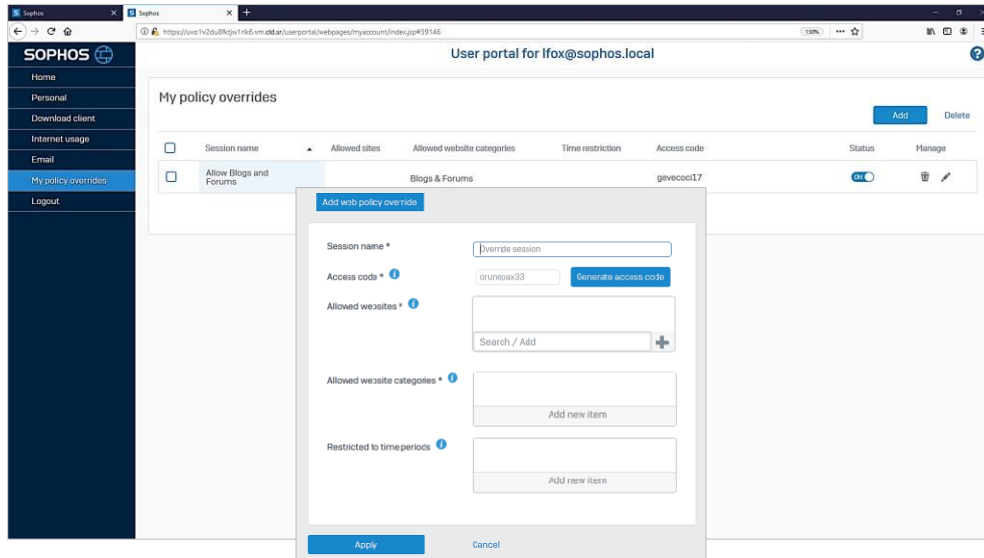
The screenshot shows the 'Policy Overrides' configuration page in the Sophos Firewall WebAdmin interface. At the top, there is a navigation bar with tabs: Policies, Policy Quota Status, User activities, Categories, URL groups, Exceptions, and General settings (which is currently selected). Below the navigation bar, the page title is 'Policy overrides'. The main content area is divided into two columns. On the left, there is a section titled 'Enable policy override' with a checked checkbox. Below this, there is a section titled 'Authorized users and groups' with a list containing 'Admins' and an 'Add new item' button. On the right, there is a section titled 'Blocked websites and categories' with a list containing 'Command & Control', 'Controlled substances', and 'Criminal Activity', along with an 'Add new item' button. To the right of this list is a checkbox for 'Allow manual access code entry' with a description. At the top right of the main content area, there is a link labeled 'View 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.

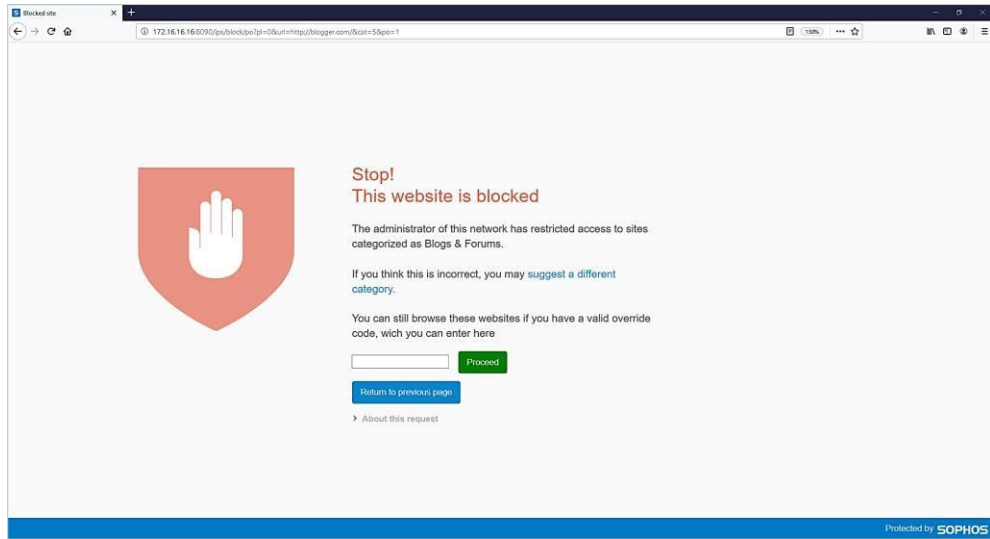
Policy Overrides



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.

Simulation: Delegate Web Policy Overrides on Sophos Firewall



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

SOPHOS

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

Policies	Policy Quota Status	User activities	Categories	URL groups	Exceptions	General settings	***
Add exception							
Name and description		Selection criteria		Skip			
Apple Update Allows Apple Update without content scanning side effects.		Matching URLs: ^([A-Za-z0-9-]*\.)*apple\.com\/?/ ^([A-Za-z0-9-]*\.)*cdn-apple\.com\/?/ ^([A-Za-z0-9-]*\.)*mzstatic\.com\/?/		HTTPS decryption HTTPS certificate validation Malware and content scanning Zero-day protection Policy checks			
Legacy HTTPS Exceptions URLs that were automatically skipped for HTTPS Decryption on earlier versions of XG Firewall.		Matching URLs: alicebusiness.it contacts.msn.com deluxe.com dropbox.com federalreserve.org iataindia.org login.live.com logmein.com 6 more ...		HTTPS decryption HTTPS certificate validation			
Microsoft Windows Update Allows Windows Update without content scanning side effects. Disable this exception if you're enforcing Microsoft tenant restrictions in web policy.		Matching URLs: ^([A-Za-z0-9-]*\.)*microsoft\.com/ ^([A-Za-z0-9-]*\.)*windowsupdate\.com/		HTTPS decryption HTTPS certificate validation Malware and content scanning Zero-day protection Policy checks			
Microsoft Windows Update with tenant re... Allows Windows Update without content scanning side effects. This exception is safe for use when enforcing Microsoft tenant restrictions in web policy.		Matching URLs: ^([?login_]([A-Za-z0-9-]*\.)*microsoft\.com/ ^([A-Za-z0-9-]*\.)*windowsupdate\.com/ ^([A-Za-z0-9-]*\.)*login\.microsoftonline\.com/		HTTPS decryption HTTPS certificate validation Malware and content scanning Zero-day protection Policy checks			

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

The screenshot shows the 'Exceptions' configuration window in the Sophos Firewall management console. At the top, there are fields for 'Name *' and 'Description'. Below these, a section titled 'For web traffic matching these criteria:' contains four options: 'URL pattern matches' (checked), 'Web site categories', 'Source IP addresses (end-user's address)', and 'Destination IP addresses (web site address)'. The 'URL pattern matches' option is expanded, showing a list with 'webapp.sophostaining.xyz' and a 'Search / Add' button. To the right, a section titled 'Skip the selected checks or actions:' contains five options: 'HTTPS decryption', 'HTTPS certificate validation', 'Malware and content scanning', 'Sandstorm', and 'Policy checks' (checked). At the bottom of the window are 'Save' and 'Cancel' buttons.

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.