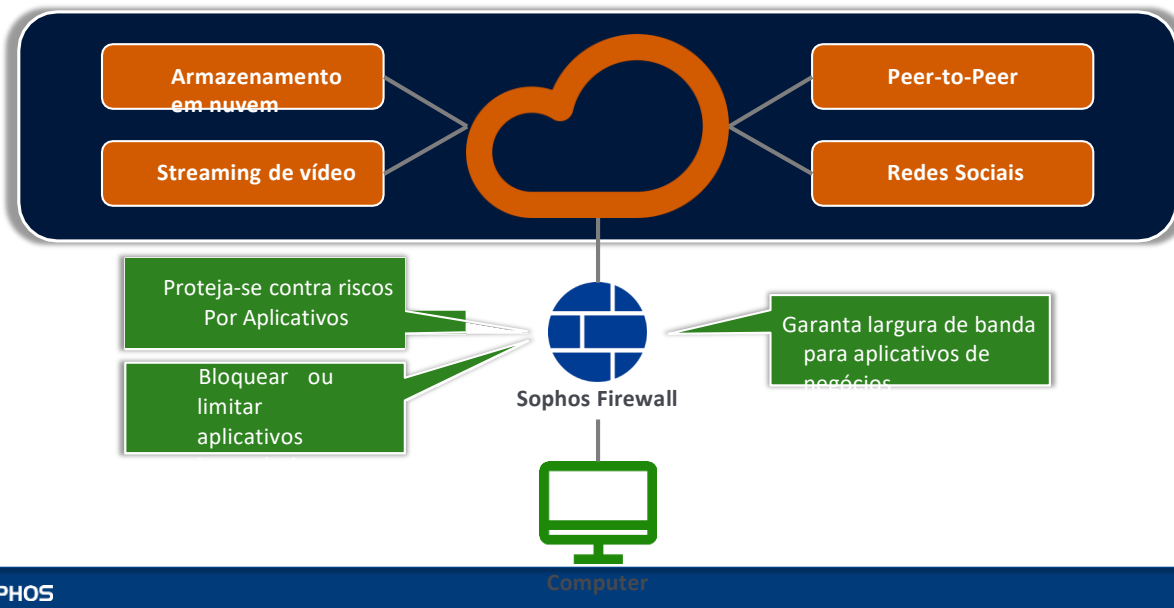




Getting Started with Application Control on Sophos Firewall

Sophos Firewall
Version: 19.0v1

Application Control Overview



Muitos aplicativos e ferramentas usados para negócios do dia-a-dia são fornecidos por meio de nuvem serviços, portanto, garantir uma boa conectividade com a Internet para os funcionários é vital.

Juntamente com esses aplicativos de negócios, há todos os outros tipos de aplicativos e serviços que podem ser imaginados, muitos dos quais são improdutivos ou podem expor os usuários e a rede da empresa a riscos.

O Sophos Firewall pode proteger contra aplicativos arriscados e bloquear ou limitar o acesso a aplicativos improdutivos e, ao mesmo tempo, garantir que os aplicativos de negócios tenham a largura de banda de que precisam.

Application List

Applications can be found in:
PROTECT > Applications > Application list

SOPHOS Firewall

Search

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

SYSTEM

- Sophos Central
- Profiles
- Hosts and services

Applications

Feedback How-to guides Log viewer Help admin@ny-gw.trainingdemo.xyz Sophos

Application filter Synchronized Application Control Cloud applications **Application list** Traffic shaping default Application object

Total applications: 3535

Name	Category	Risk	Technology	Characteristics	Classification
1 & 1 Webmail	Web Mail	2			
10000ft Plans	General Business	1			
100BAO P2P	P2P	High	P2P	Excessive Bandwidth, Loss of productivity, Vulnerabilities, Transfer files	
101 Network	Streaming Media	1			
123RF	E-commerce	1			
126 Mail	Web Mail	2 - Low	Browser Based	Transfer files, Widely Used	
163 Alumni	Social Networking	2 - Low	Browser Based	Loss of productivity, Widely Used	
163 BBS	Social Networking	2 - Low	Browser Based	Excessive Bandwidth, Loss of pr...	

Application Detail

Name 100BAO P2P

Category P2P

Risk High

Characteristics Excessive Bandwidth, Loss of productivity, Vulnerabilities, Transfer files

Technology P2P

Dependency None

Applicable on 16.01.0 Build 101 and above

Description 100bao is a Chinese peer to peer application specifically centered around users uploading media content for other users to view using their application.

O Sophos Firewall vem com definições para milhares de aplicativos conhecidos, que você pode filtrar e veja os detalhes do in **PROTECT > Applications > Application list**.

Live Connections

Current connections can be monitored in:
MONITOR & MANAGE > Current activities > Live connections

SOPHOS FW
Sophos Firewall

Search

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

SYSTEM

Sophos Central

Profiles

Hosts and services

Current activities

Feedback How-to guides Log viewer Help admin@ny-gw.trainingdemo.xyz Sophos

Live users

Live connections

Live connections IPv6

IPsec connections

Remote users

Live connections: 70

Live connections for Application

Automatic refresh interval Never Refresh

Application	Source IP address	Username	Upload transfer	Download transfer	Upstream bandwidth	Downstream bandwidth	Characteristics	Total
Other Applications	-	-	106.48 MB	80.60 MB	461 Bps	444 Bps	NA	45
Secure Socket Layer Protocol	-	-	1.69 MB	990.81 KB	357 Bps	194 Bps	Widely Used	6
Windows Remote Desktop	-	-	69 KB	651.75 KB	20 Bps	45 Bps	Excessive Bandwidth, Tunnels other apps	1
lsass.exe	-	-	644 Bytes	0 Bytes	0 Bps	0 Bps		2
dns.exe	-	-	1.26 KB	2.04 KB	0 Bps	0 Bps		9

A página Conexões em tempo real lista todos os aplicativos atuais que fazem conexões através do Sophos Firewall. Você pode usar o link na coluna 'Total' para obter informações mais detalhadas sobre todas as conexões para esse aplicativo.

As conexões em tempo real podem ser mostradas por aplicativo, nome de usuário ou endereço IP de origem, e a página pode ser opcionalmente configurada para atualizar automaticamente para fornecer uma visão em tempo real.

Application Filters

Applications can be found in:
PROTECT > Applications > Application filter

The screenshot shows the Sophos Firewall web interface. The left sidebar contains navigation menus for 'MONITOR & ANALYZE', 'PROTECT', 'CONFIGURE', and 'SYSTEM'. The 'Applications' menu item under 'PROTECT' is highlighted. The main content area is titled 'Applications' and has several tabs: 'Application filter' (selected), 'Synchronized Application Control', 'Cloud applications', 'Application list', 'Traffic shaping default', and 'Application object'. Below the tabs is a table of application filters. The table has columns for 'Name', 'Default action', and 'Description'. There are also 'Add' and 'Delete' buttons at the top right of the table. The table lists several filters, including 'Allow All', 'Block filter avoidance apps', 'Block generally unwanted apps', 'Block high risk (Risk Level 4 and 5) apps', 'Block peer to peer (P2P) networking apps', 'Block very high risk (Risk Level 5) apps', and 'Deny All'.

<input type="checkbox"/>	Name	Default action	Description	Manage
<input type="checkbox"/>	Allow All	Allow	Allow All Policy.	
<input type="checkbox"/>	Block filter avoidance apps	Allow	Drops traffic from applications that tunnels other apps, proxy and tunnel apps, and from apps that can bypass firewall policy. These applications allow users to anonymously browse Internet by connecting to servers on the Internet via encrypted SSL tunnels. This, in turn, enables users to bypass network security measures.	
<input type="checkbox"/>	Block generally unwanted apps	Allow	Drops generally unwanted applications traffic. This includes file transfer apps, proxy & tunnel apps, risk prone apps, peer to peer networking (P2P) apps and apps that causes loss of productivity.	
<input type="checkbox"/>	Block high risk (Risk Level 4 and 5) apps	Allow	Drops traffic that are classified under high risk apps (Risk Level- 4 and 5).	
<input type="checkbox"/>	Block peer to peer (P2P) networking apps	Allow	Drops traffic from applications that are categorized as P2P apps. P2P could be a mechanism for distributing Bots, Spywares, Adware, Trojans, Rootkits, Worms and other types of malwares. It is generally advised to have P2P application blocked in your network.	
<input type="checkbox"/>	Block very high risk (Risk Level 5) apps	Allow	Drops traffic that are classified under very high risk apps (Risk Level- 5).	
<input type="checkbox"/>	Deny All	Deny	Deny All Policy.	

Os filtros de aplicativo são conjuntos de regras que podem permitir ou negar acesso a aplicativos. Ao contrário das políticas da Web, as regras de filtro de aplicativo não são aplicadas a usuários e grupos, portanto, o filtro de aplicativo será aplicado a todos os usuários para a regra de firewall em que é usado.

Creating Application Filters

The screenshot shows the Sophos Firewall web interface. The left sidebar contains navigation menus for 'MONITOR & ANALYZE', 'PROTECT', 'CONFIGURE', and 'SYSTEM'. The 'Applications' section is highlighted under 'PROTECT'. The main content area is titled 'Applications' and has several tabs: 'Application filter' (selected), 'Synchronized Application Control', 'Cloud applications', 'Application list', 'Traffic shaping default', and 'Application object'. In the 'Application filter' tab, there are three input fields: 'Name *' (containing 'Training app filter'), 'Description', and 'Template'. The 'Template' dropdown menu is open, displaying a list of options: 'Allow All' (highlighted), 'Block generally unwanted apps', 'Block filter avoidance apps', 'Block peer to peer (P2P) networking apps', 'Block very high risk (Risk Level 5) apps', and 'Block high risk (Risk Level 4 and 5) apps'. An orange callout box with a pointer to the 'Allow All' option contains the text: 'You can optionally select an existing application filter as a template'.

Os filtros de aplicativo são criados em dois estágios.

Primeiro, você cria o filtro de aplicativo. Aqui, opcionalmente, você pode selecionar um filtro de aplicativo existente como um modelo.

Você salva o filtro de aplicativo e, se tiver selecionado um modelo, as regras serão copiadas para o novo filtro.

Creating Application Filters

The screenshot shows the Sophos Firewall 'Applications' page. The 'Application filter' tab is selected. The page has a sidebar on the left with navigation options: 'Control center', 'Current activities', 'Reports', 'Zero-day protection', 'Diagnostics', 'Rules and policies', 'Intrusion prevention', 'Web', 'Applications' (highlighted), 'Wireless', 'Email', 'Web server', 'Advanced protection', 'Remote access VPN', 'Site-to-site VPN', 'Network', 'Routing', 'Authentication', 'System services', 'Sophos Central', 'Profiles', and 'Hosts and services'. The main area has a header with 'Applications' and a search bar. Below the header, there are tabs: 'Application filter', 'Synchronized Application Control', 'Cloud applications', 'Application list', 'Traffic shaping default', and 'Application object'. The 'Application filter' tab is active. It contains a form with 'Name *' and 'Description' fields. Below the form, there is a table of applications. The first application is 'Manolito P2P Search, Piolet FileTransfer P2P, NapMX Retrieve P2P, Freenet P2P, Imesh P2P, Stealthnet P2P, Bearshare P2P, Ants IRC Connect P2P, MediaGet P2P, Gnutella P2P, DirectConnect P2P, Manolito P2P Download, Phex P2P, QQ Download P2P, DC++ Hub List P2P, Kugoo Playlist P2P, Piolet Initialization P2P, GoBoogy Login P2P, DC++ Connect P2P, Kite Initiation P2P, Ares P2P, Manolito P2P Connect, MP3 Rocket Download, Soulseek Retrieving P2P, Winny P2P, Soul Attempt P2P, LimeWire, VeryCD, Pando P2P, Morpheus P2P, Shareaza P2P, DC++ Download P2P, WinMX P2P, Ants Initialization P2P, Ants P2P, Tixati P2P, Miro P2P, Torrent Clients P2P, Mute P2P, PeerCast P2P, Manolito P2P GetServer List, 100BAO P2P, SoMud, Soulseek Download P2P, eMule P2P, Apple-Juice P2P, Vuze P2P, Flashget P2P, Napster P2P, Fileguri P2P'. The second application is 'Piolet FileTransfer P2P, Bronto, Tapin Radio, Contract Wars, DouBan FM, Zippyshare, Mixwit Website, Zoho WebMessenger, iMeet Central, Elixio Website, Zoom Meetings, Pearls Peril, Datawrapper, Shinniv Manana Orders, LinkedIn Videos, FarmVille 2, F Entertainment, 7share'. The table has columns for 'Application filter criteria', 'Schedule', 'Action', and 'Manage'. The first application has a checkbox, 'Category = P2P', 'All the Time', 'Deny', and a trash icon. The second application has a checkbox, 'Category = P2P', 'All the Time', 'Deny', and a trash icon. An annotation 'You can now add rules to your application filter' points to the 'Add' button. Another annotation 'Drag and drop to reorder' points to the application list.

Agora você pode abrir o filtro de aplicativo e começar a adicionar regras ou editar regras se tiver selecionado um modelo.

Por favor, note que as regras são processadas em ordem, e você pode reorganizá-las arrastando e soltando.

Application Filter Rules

SOPHOS Firewall

Applications

Feedback | How-to guides | Log viewer | Help | admin@ny-gw.trainingdemo.xyz | Sophos

Application filter | Synchronized Application Control | Cloud applications | Application list | Traffic shaping default | Application object

Add application filter policy rules

Category: [dropdown] Risk: [dropdown] Characteristics: [dropdown] Technology: [dropdown] Classification: [dropdown] Smart filter: [dropdown] Clear filter

Risk: High x Very High x Characteristics: Tunnels other apps x Vulnerabilities x Can bypass firewall policy x

☒ Select all ☐ Select individual application

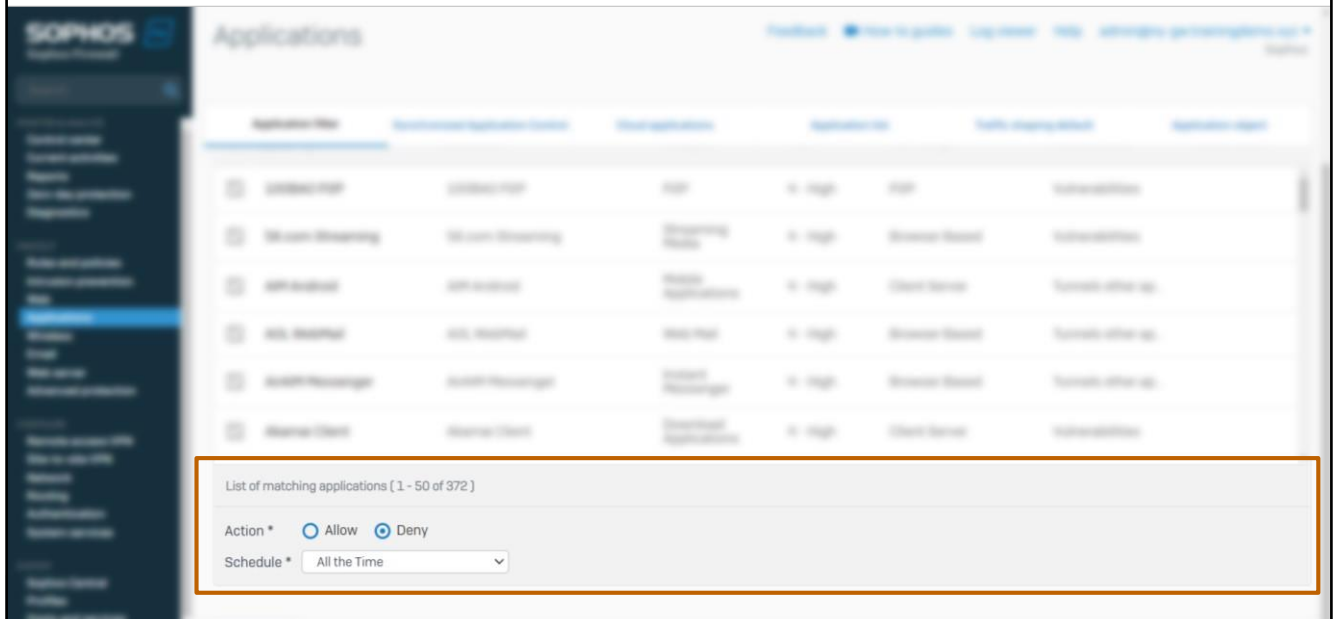
<input type="checkbox"/>	Name	Description	Category	Risk	Technology	Characteristics	Classification
<input checked="" type="checkbox"/>	100BA0 P2P	100BA0 P2P	P2P	4 - High	P2P	Vulnerabilities	
<input checked="" type="checkbox"/>	56.com Streaming	56.com Streaming	Streaming Media	4 - High	Browser Based	Vulnerabilities	
<input checked="" type="checkbox"/>	AIM Android	AIM Android	Mobile Applications	4 - High	Client Server	Tunnels other ap...	
<input checked="" type="checkbox"/>	AOL WebMail	AOL WebMail	Web Mail	4 - High	Browser Based	Tunnels other ap...	
<input checked="" type="checkbox"/>	AirAIM Messenger	AirAIM Messenger	Instant Messenger	4 - High	Browser Based	Tunnels other ap...	

Para cada regra de filtro de aplicativo, você seleciona a quais aplicativos ela será aplicada, define se a ação para esses aplicativos é permitida ou negada e, opcionalmente, seleciona uma agenda para quando a regra estará ativa.

A seleção dos aplicativos na regra é feita filtrando os aplicativos usando os critérios fornecidos ou usando um filtro inteligente de texto livre. Quando novos aplicativos são adicionados que correspondem aos filtros, eles serão automaticamente incluídos na regra.

Opcionalmente, você pode optar por selecionar aplicativos individuais em vez de todos os aplicativos incluídos nos resultados filtrados, nesse caso, os aplicativos recém-adicionados não serão adicionados automaticamente à regra.

Application Filter Rules



Abaixo dos aplicativos selecionados, você pode escolher se essa regra deve permitir ou negá-los. Você também pode selecionar quando essa regra está ativa com base em uma agenda.

Apply an Application Filter

The screenshot shows the 'Edit firewall rule' page in the Sophos Firewall management console. The left sidebar contains navigation menus for 'MONITOR & ANALYZE', 'PROTECT', 'CONFIGURE', and 'SYSTEM'. The main content area is titled 'Edit firewall rule' and includes a 'Default Policy' dropdown. A list of security features is shown with checkboxes: 'Apply web category-based traffic shaping' (unchecked), 'Block QUIC protocol' (checked), 'Scan HTTP and decrypted HTTPS' (checked), 'Use zero-day protection' (checked), 'Scan FTP for malware' (unchecked), 'Use web proxy instead of DPI engine' (unchecked), 'DPI engine or web proxy?' (info icon), 'Web proxy options' (unchecked), and 'Decrypt HTTPS during web proxy filtering' (unchecked). Below this, there is a section for 'Configure Synchronized Security Heartbeat'. The 'Other security features' section is highlighted with an orange box and contains three sub-sections: 'Identify and control applications (App control)' with a dropdown set to 'Training app filter' and 'Apply application-based traffic shaping policy' (checked); 'Shape traffic' with a dropdown set to 'None'; and 'DSCP marking' with a dropdown set to 'Select DSCP marking'. At the bottom, there is a section for 'Detect and prevent exploits (IPS)' with a dropdown set to 'lantowan_general' and a link to 'Scan email content'.

Depois de configurar o filtro do aplicativo, ele precisa ser selecionado em uma regra de firewall na Seção 'Outros recursos de segurança'.

Simulation: Create an Application Filter



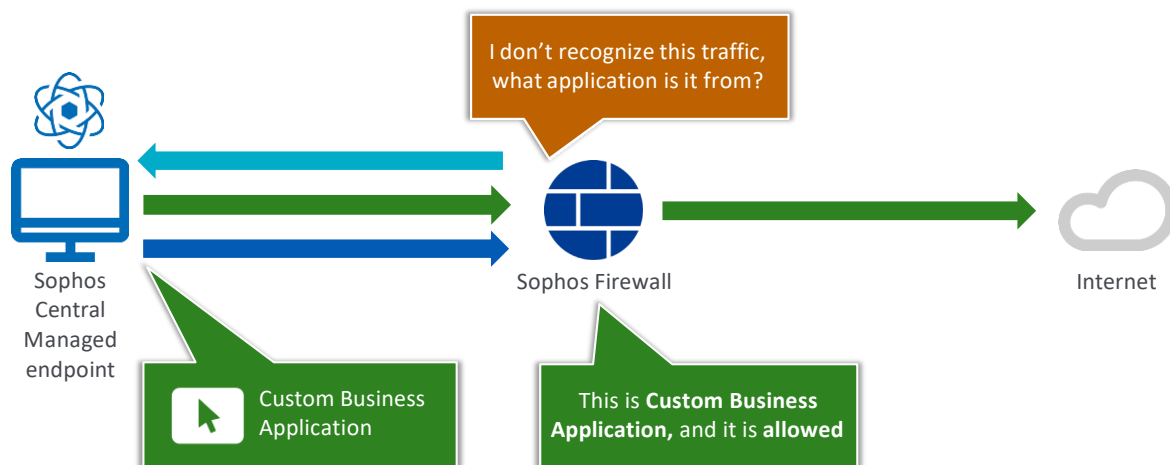
Nesta simulação, você criará um filtro de aplicativo personalizado, aplicá-lo a uma regra de firewall e, em seguida, testará os resultados.

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

SOPHOS

Nesta simulação, você criará um filtro de aplicativo personalizado, aplicá-lo a uma regra de firewall e, em seguida, testará o Resultados.

Synchronized App Control

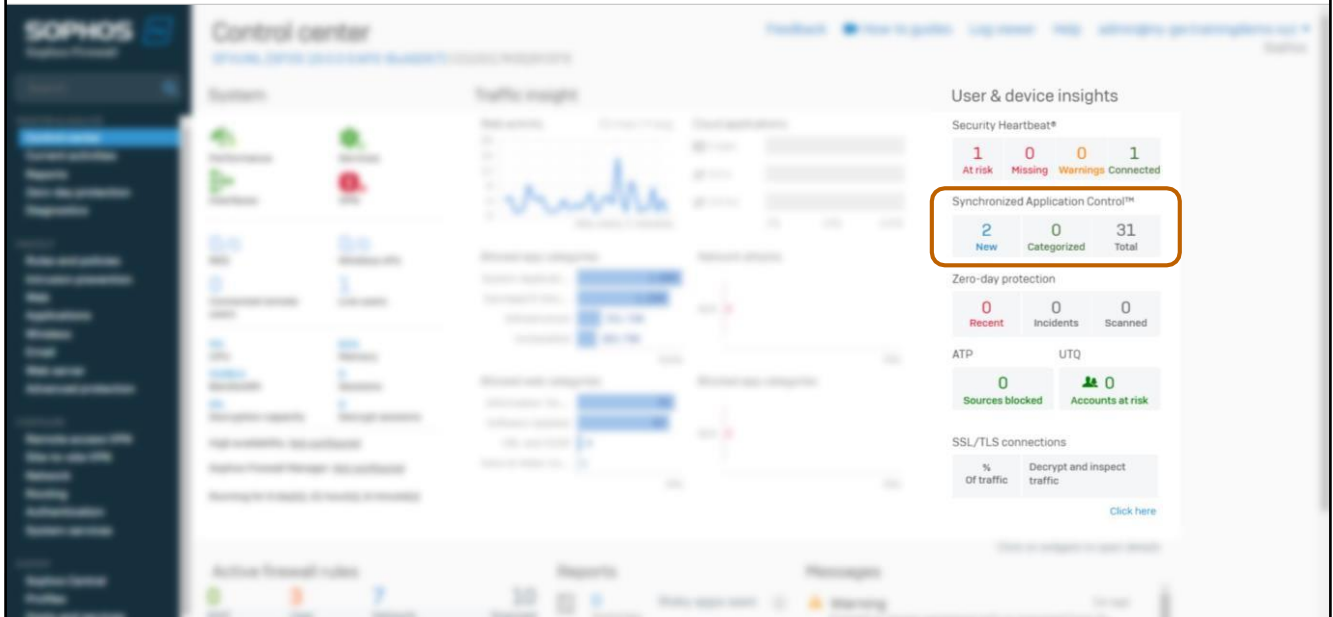


SOPHOS

O controle de aplicativo sincronizado pode identificar, classificar e controlar aplicativos anteriormente desconhecidos ativos na rede. Ele usa o Security Heartbeat para obter informações do ponto de extremidade sobre aplicativos que não têm assinaturas ou estão usando conexões HTTP ou HTTPS genéricas. Isso resolve um problema significativo que afeta o controle de aplicativos baseados em assinatura em todos os firewalls atuais, onde muitos aplicativos são classificados como "desconhecidos", "não classificados", "HTTP genérico" ou "SSL".

O controle de aplicativo sincronizado não tem suporte em implantações de alta disponibilidade ativo-ativo.

Managing Synchronized App Control



O controle de aplicativo sincronizado é ativado quando você registra o Sophos Firewall com o Sophos Central.

No Centro de controle, há um widget de controle de aplicativo sincronizado que fornece uma indicação rápida de novos aplicativos que foram identificados.

Categorizing Identified Applications

SOPHOS FW
Sophos Firewall

Search

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

SYSTEM

Sophos Central

Profiles

Hosts and services

Applications

Identified applications are managed in:
PROTECT > Applications > Synchronized Application Control

Application filter

Synchronized Application Control

Cloud applications

Application list

Traffic shaping default

Application object

Synchronized Application Control

On this page you can modify application details for applications discovered with Synchronized Security from Sophos managed devices. You can change the name and category for the applications, information for some applications is already provided automatically from Sophos. You can use these applications in the overall application control feature on Sophos Firewall or you can directly assign the discovered applications to application filters to control the applications.

Acknowledge

Hide

Delete

New applications

Apps, categories, and last occurrences

Filters: None

Add filter

Reset

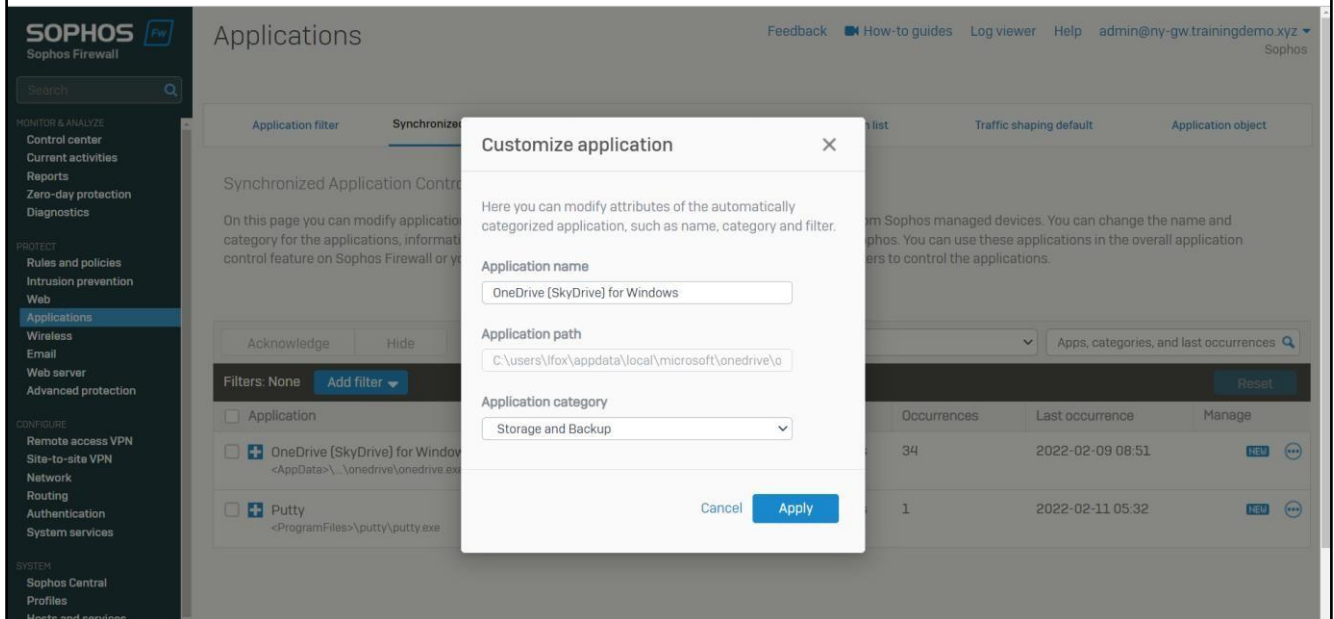
<input type="checkbox"/>	Application	Category	Endpoints	Occurrences	Last occurrence	Manage
<input type="checkbox"/>	<div>OneDrive [SkyDrive] for Windows</div> <div><AppData>\...\onedrive\onedrive.exe</div>	Storage and Backup	Found on 1 Endpoints	34	2022-02-09 08:51	<div>NEW</div> <div>...</div>
<input type="checkbox"/>	<div>Putty</div> <div><ProgramFiles>\putty\putty.exe</div>	Remote Access	Found on 1 Endpoints	1	2022-02-11 05:32	<div>Customize</div> <div>Hide</div> <div>Acknowledge</div> <div>Delete</div>

Sempre que possível, o Sophos Firewall classificará automaticamente os aplicativos identificados e eles serão controlado com base nos filtros de aplicativo atuais que você tem em vigor.

Através do menu para o aplicativo você personaliza a classificação.

Getting Started with Application Control on Sophos Firewall - 14

Categorizing Identified Applications



Aqui você pode ver que o OneDrive foi atribuído à categoria de aplicativo 'Armazenamento e Backup'. Se você estava bloqueando essa categoria, mas queria permitir o OneDrive, você poderia optar por movê-lo para outra categoria, como 'Negócios Gerais'.

Synchronized Application Control

The screenshot shows the Sophos Central web interface. The left sidebar contains navigation menus for 'MONITOR & ANALYZE', 'PROTECT', 'CONFIGURE', and 'SYSTEM'. The main content area displays 'Sophos Central registration' information, including device status, serial number, account, and email. Below this, there are three sections: 'Security Heartbeat' (ON), 'Synchronized Application Control' (ON), and 'Sophos Central services' (OFF). The 'Synchronized Application Control' section shows 31 total applications, 2 new applications discovered, and 0 categorized applications. A 'Clean up application database' button is highlighted with an orange box. A dialog box titled 'Clean up application database' is open, showing a checkbox for 'Clean up database automatically' (checked) and a dropdown menu for 'Elapsed time since last detection' set to '6 months'. The dropdown menu is expanded, showing options: 1 month, 3 months, 6 months, 9 months, and 12 months. The 'Save' button is highlighted in blue.

Você pode configurar a limpeza do banco de dados de controle de aplicativo sincronizado para remover obsoletos

aplicativos que não estão mais em uso; isso é feito em **PROTECT > Central synchronization**.

Você pode escolher por quanto tempo reter os aplicativos no banco de dados de 1 mês a 12 meses. O Sophos Firewall executará uma verificação diária de aplicativos mais antigos do que o limite e os removerá em lotes de 100 a cada 5 minutos. Os aplicativos também são excluídos das políticas de filtro de aplicativos se tiverem sido adicionados individualmente.

O tempo para o qual os aplicativos são retidos é desde que eles foram detectados pela última vez pelo controle de aplicativo sincronizado. Se o aplicativo for usado com frequência, a última data de detecção sempre será atualizada e o aplicativo não será limpo. Esse recurso foi projetado para limpar apenas aplicativos que não estão mais em uso e, portanto, não estão mais sendo detectados pelo controle de aplicativo sincronizado.

Simulation: Use Synchronized App Control to Block an Application



Nesta simulação, você reclassificará um aplicativo detectado pelo controle de aplicativo sincronizado e, em seguida, testará se ele está bloqueado.

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

SOPHOS

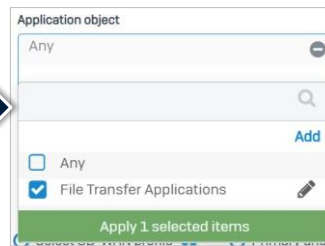
Nesta simulação você reclassificará um aplicativo detectado pelo aplicativo sincronizado em seguida, teste se ele está bloqueado.

[Additional Information]

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

Application Routing

Routing > SD-WAN Routing > Add



Application object

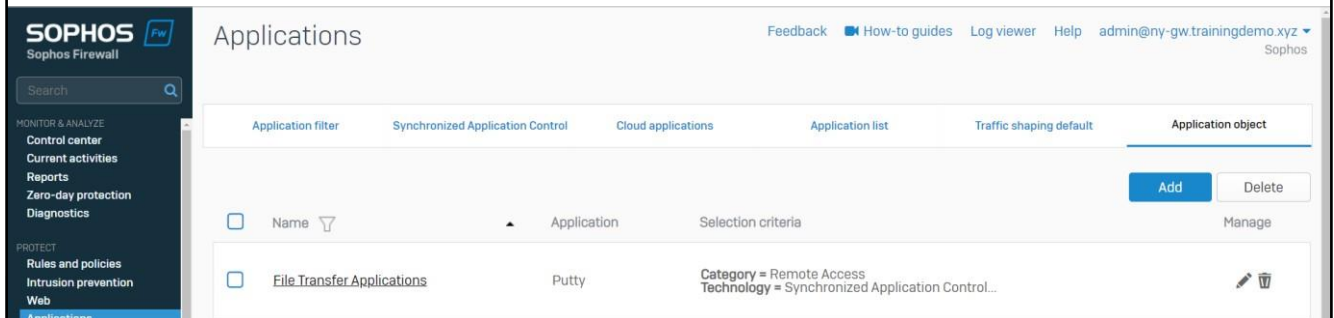
Any

Add

☐ Any

☒ File Transfer Applications

Apply 1 selected items



SOPHOS
Sophos Firewall

Search

MONITOR & ANALYZE
Control center
Current activities
Reports
Zero-day protection
Diagnostics

PROTECT
Rules and policies
Intrusion prevention
Web
Applications

Applications

Feedback How-to guides Log viewer Help admin@ny-gw.trainingdemo.xyz Sophos

Application filter Synchronized Application Control Cloud applications Application list Traffic shaping default Application object

Add Delete

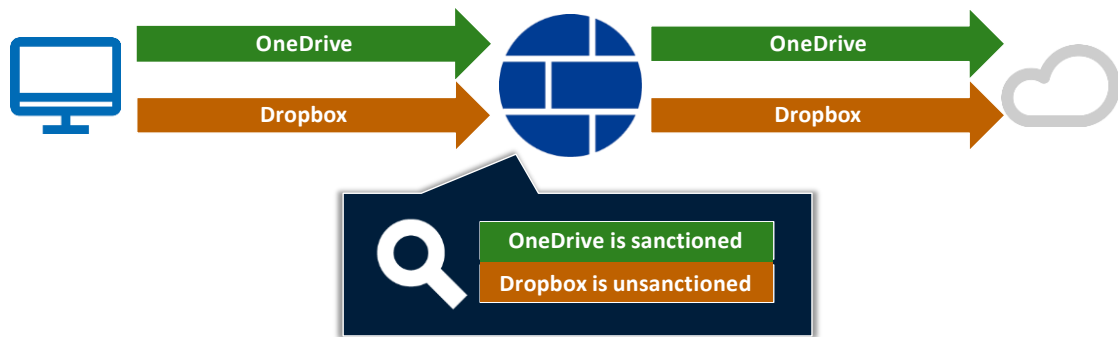
<input type="checkbox"/>	Name	Application	Selection criteria	Manage
<input type="checkbox"/>	File Transfer Applications	Putty	Category = Remote Access Technology = Synchronized Application Control...	

Os aplicativos podem ser adicionados como um seletor de tráfego para Rotas de política SD-WAN.

Para usar essa funcionalidade, você precisa criar um objeto de aplicativo. Um objeto de aplicativo é uma lista de aplicativos selecionados usando os mesmos critérios e opções de filtragem que para regras de filtro de aplicativo.

No exemplo aqui, selecionamos aplicativos de acesso remoto que foram detectados pelo controle de aplicativo sincronizado.

Cloud Applications



Identify cloud applications being used

Classify cloud applications

Apply traffic shaping rules

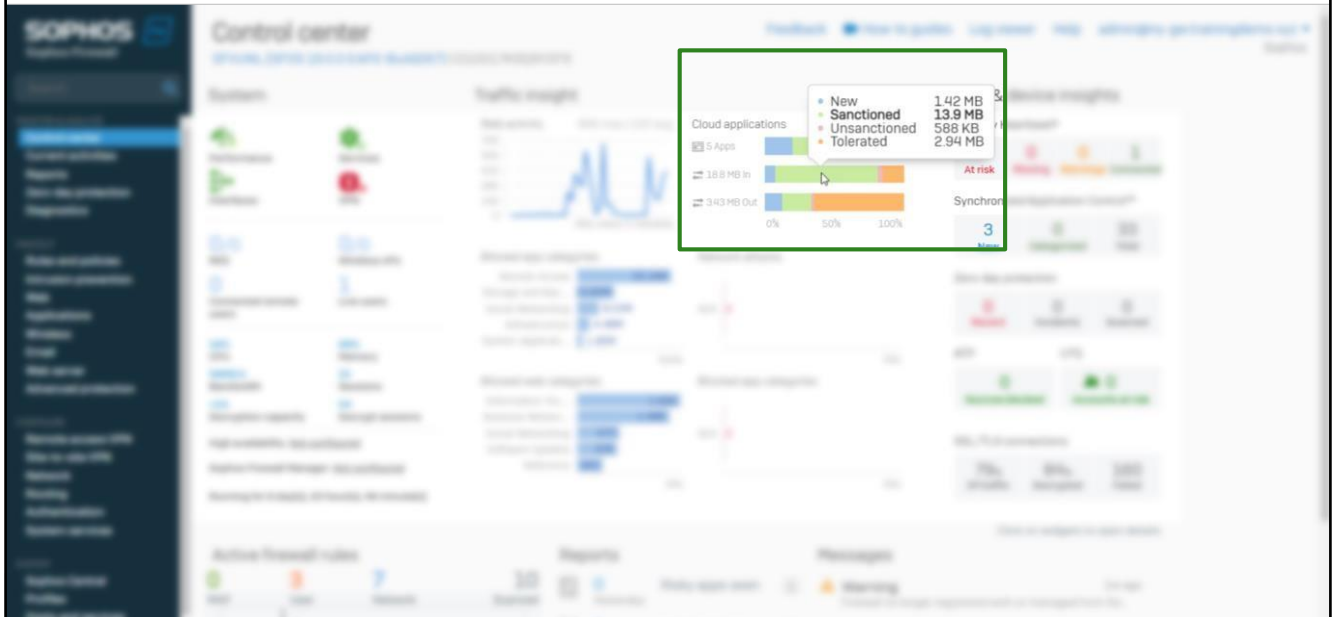
Block using application control

SOPHOS

O Sophos Firewall tem uma implementação de agente de segurança de acesso à nuvem lite, ou CASB, que ajuda a identificar comportamentos de risco, fornecendo insights sobre quais serviços em nuvem estão sendo usados. Em seguida, você pode tomar as medidas apropriadas educando os usuários ou implementando políticas de controle de aplicativos ou de modelagem de tráfego para controlar ou eliminar possíveis comportamentos arriscados ou indesejados.

Por exemplo, se sua empresa tiver um Microsoft 365 corporativo e usar o OneDrive para armazenamento de arquivos, e um usuário estiver carregando dados consistentemente para o Dropbox, isso pode ser um sinal de alerta que precisa de mais investigação ou aplicação de políticas. Essa prática de usar serviços de nuvem não sancionados é chamada de "Shadow IT", um termo que você geralmente ouvirá em associação com o CASB.

Cloud Applications in the Control Center



No Centro de controle, há um widget que fornece um resumo visual do uso do aplicativo em nuvem por classificação. Isso pode ser Novo, Sancionado, Não Sancionado ou Tolerado. As estatísticas mostram o número de aplicativos em nuvem e a quantidade de dados que entram e saem.

Clicar no widget leva você a **PROTECT > Applications > Cloud applications**, onde você pode obter informações mais detalhadas.

Cloud Applications

Cloud applications can be found in:
PROTECT > Applications > Cloud applications

The screenshot shows the Sophos Firewall web interface. The left sidebar contains navigation menus for 'MONITOR & ANALYZE', 'PROTECT', 'CONFIGURE', and 'SYSTEM'. The main content area is titled 'Applications' and has tabs for 'Application filter', 'Synchronized Application Control', 'Cloud applications' (selected), 'Application list', 'Traffic shaping default', and 'Application object'. Below the tabs, there are filters for date range (From: 2022-02-11 To: 2022-02-11), status (New), categories (All categories), and sorting (Sort by bytes transferred). The results show a list of cloud applications. The first application is 'GitHub', categorized as 'Storage and Backup' with a 'Very low risk' level. It shows 4.5 MB of traffic and 2 users. Below this is a table with columns 'User', 'Host', 'Upload data', and 'Download data'. The table lists two users: 'administrator' with 304 KB upload and 3.97 MB download, and 'Unauthenticated user' with 82.2 KB upload and 159 KB download. The second application is 'LinkedIn Website', categorized as 'Social Networking' with a 'Very low risk' level, showing 309 KB of traffic and 1 user. The third application is 'Twitter Website', categorized as 'Social Networking' with a 'Medium risk' level, showing 35.6 KB of traffic and 1 user.

User	Host	Upload data	Download data
administrator	10.16.16.10	304 KB	3.97 MB
Unauthenticated user	10.16.16.20	82.2 KB	159 KB

Aqui você pode ver todos os aplicativos em nuvem que foram detectados e filtrá-los por classificação e categoria, e pode ser classificado por volume de dados ou número de usuários.

Você pode expandir cada aplicativo para ver quais usuários o têm usado e quantos dados eles transferiram.

Classifying and Traffic Shaping

The screenshot displays the Sophos Firewall web interface. The left sidebar shows the 'Applications' menu item highlighted. The main content area is titled 'Applications' and includes a search bar, a date range filter (From: 2022-02-11 To: 2022-02-11), and a 'New' button. A table lists applications, with 'GitHub' selected. The 'Classify' button for GitHub is highlighted with a green box, and the 'Traffic Shaping' button is highlighted with an orange box. A green arrow points from the 'Classify' button to a 'Select classification' dialog box. An orange arrow points from the 'Traffic Shaping' button to a 'Traffic shaping policy' dialog box. The 'Select classification' dialog box shows the 'Name' as 'GitHub' and the 'Select classification' dropdown set to 'Sanctioned'. The 'Traffic shaping policy' dialog box shows the 'Name' as 'GitHub' and the 'Traffic shaping policy' dropdown set to 'QoS for GitHub'. Both dialog boxes have 'Save' and 'Cancel' buttons. The background table shows traffic statistics for various applications, including GitHub, with columns for Name, Size, and Users.

Para cada aplicativo detectado, você pode selecionar uma classificação e uma política de modelagem de tráfego.

Ao selecionar uma classificação para os aplicativos, você pode usá-la para personalizar relatórios para mostrar, por exemplo, o uso de aplicativos não sancionados em sua rede.

As políticas de modelagem de tráfego podem ser aplicadas para limitar ou garantir a largura de banda para aplicativos.

Simulation: Categorize Cloud Applications on Sophos Firewall



Nesta simulação você irá rever os aplicativos em nuvem detectados pelo Sophos Firewall e classificá-los.

SOPHOS

Nesta simulação você irá rever as aplicações em nuvem detectadas pelo Sophos Firewall e classificar eles.