



Managing Logs and Notifications on Sophos Firewall

Sophos Firewall

Version: 19.0v1

Logging



Access to real-time logs using the log viewer



Add **up to 5** external syslog servers

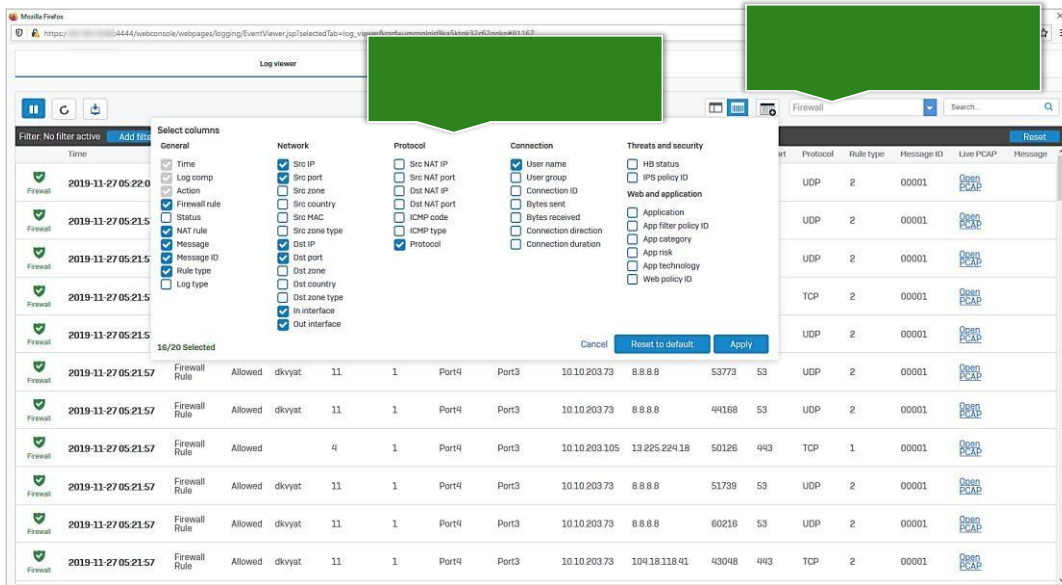


Manage which events are logged

SOPHOS

O Sophos Firewall fornece acesso a logs em tempo real no WebAdmin para que você possa monitorar facilmente o impacto das alterações e solucionar problemas. Os dados de log também podem ser relatados a servidores syslog externos e há controle granular sobre quais eventos são registrados.

Log Viewer



SOPHOS

Disponível no canto superior direito de cada página, o link Visualizador de log abre uma nova janela com o registro ao vivo para Sophos Firewall.

Na exibição de coluna padrão, o visualizador de log exibirá um único log e você poderá usar o menu suspenso para selecionar qual log será exibido.

Você pode personalizar quais colunas são exibidas, selecionando até 20, com tempo, componente de log e ação sendo obrigatórios.

Log Viewer

The screenshot displays the Sophos Log Viewer interface. A green callout box at the top left points to the 'Export data to a CSV file' button. Another green callout box at the top right points to the 'Free text search' input field. A third green callout box in the center points to the 'Add filter' button and the filter configuration panel. The main area shows a table of logs with columns for Time, Action, Category, IP, Port, Service, URL, and Bytes sent. The table is filtered to show logs from 2019-11-27 05:25:07.

Time	Action	Category	IP	Port	Service	URL	Bytes sent
2019-11-27 05:25:07	Allowed	csainz	10.10.203.71	104	123	196	107
2019-11-27 05:25:07	Allowed	dkvyat	10.10.203.73	95	131	143	115
2019-11-27 05:25:07	Allowed	csainz	10.10.203.71	134	113	242	32
2019-11-27 05:25:07	Allowed	dkvyat	10.10.203.73	95	131	143	115
2019-11-27 05:25:07	Allowed	dkvyat	10.10.203.73	172	217	164	202
2019-11-27 05:25:07	Allowed	dkvyat	10.10.203.73	172	217	164	202
2019-11-27 05:25:07	Allowed	dkvyat	10.10.203.73	172	217	164	202

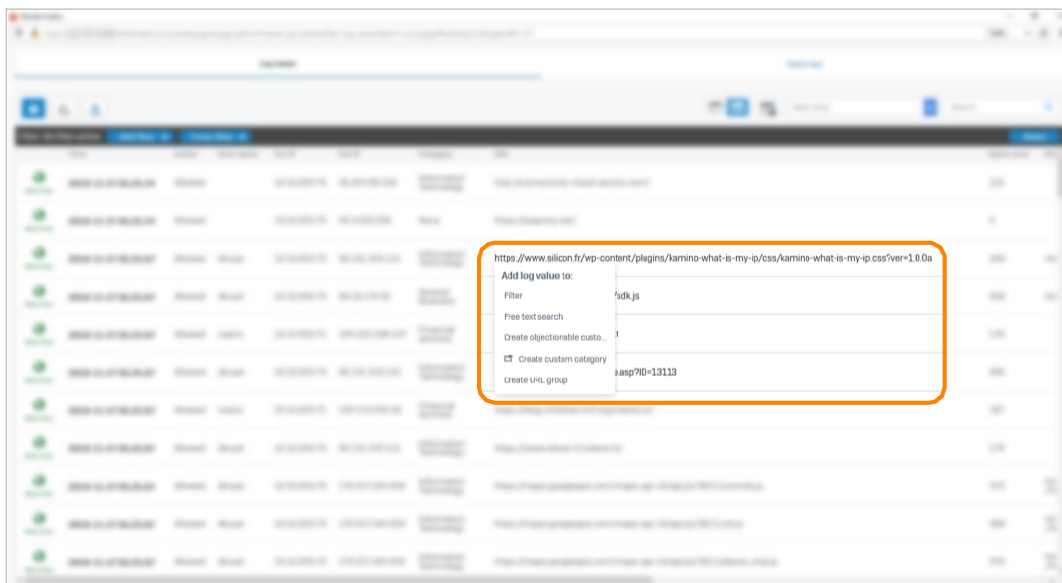
Você pode aplicar filtros estruturados aos logs e realizar pesquisas de texto livre, em ambos os casos o os termos correspondentes serão realçados. A qualquer momento, você pode optar por exportar os dados para um arquivo CSV.

Log Viewer

Hover to see more detailed information

Ao passar o mouse sobre a entrada de log, você também pode ver informações mais detalhadas.

Log Viewer



SOPHOS

Ao clicar nos dados nos logs, você obterá ações sensíveis ao contexto. Você sempre terá a opção de filtrar usando os dados como um filtro estruturado ou pesquisa de texto livre, mas em muitos casos, você também poderá editar regras e políticas ou criar novas configurações.

O exemplo aqui inclui a opção de criar uma categoria de URL personalizada censurável incluindo esses dados, porque era permitido. Se tivesse sido bloqueado, a opção teria sido criar uma categoria de URL personalizada aceitável.

Log Viewer

Switch between column and unified log view

Select multiple logs

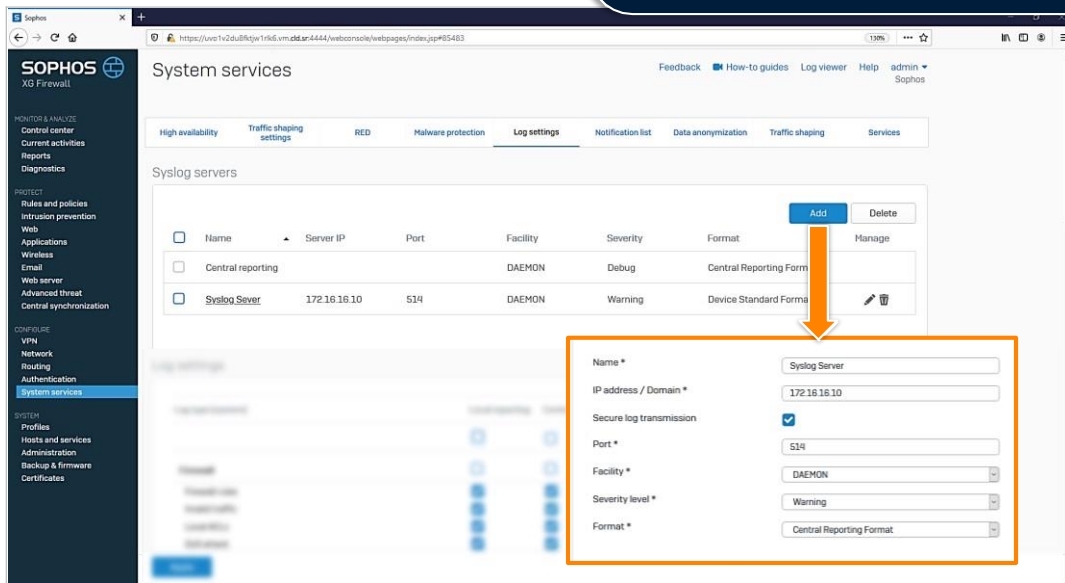
The screenshot shows the Sophos Log Viewer interface. At the top, there are buttons for switching between column and unified log views, and a button for selecting multiple logs. Below these are search and filter options. The main area displays a list of logs, each with a status icon (green checkmark), a date, and a detailed log entry. The logs are filtered by 'No filter active' and 'Add filter' is available. The interface is clean and professional, with a blue header and a white body.

SOPHOS

Você pode alternar para a exibição de log unificada detalhada usando os botões na parte superior. Esse modo de exibição tem as mesmas opções de pesquisa e filtragem que o modo de exibição padrão, mas pode agregar os logs de vários módulos.

Por padrão, quando você alterna para esse modo de exibição, todos os logs serão mostrados. Você pode usar o menu suspenso para selecionar para quais módulos deseja exibir os logs.

Quando você clica nos links para regras e políticas de firewall, a janela WebAdmin vai navegar automaticamente para esse local, tornando mais rápido e fácil revisar a configuração relevante para uma entrada de log.



Além dos logs locais em tempo real, o Sophos Firewall pode ser configurado para registrar até 5 logs externos servidores syslog, geralmente na porta UDP 514, embora isso possa ser personalizado.

Na configuração do servidor syslog, você pode selecionar para qual recurso deseja registrar: DAEMON, que inclui informações de serviços em execução no firewall
KERNEL, para o log do kernel

LOCAL0 – LOCAL7, para obter informações de um nível de log específico
USER, para registro em log com base em usuários que estão conectados ao servidor
Você também pode selecionar a gravidade dos eventos que deseja registrar. O firewall registrará todos os eventos para o nível selecionado e acima. Portanto, se você selecionar CRÍTICO, ele também registrará eventos de ALERTA e EMERGÊNCIA.

Há dois formatos de log que podem ser selecionados:

Formato de Relatório Central, que é um formato syslog padrão e é usado para registrar no Sophos Central

Formato padrão do dispositivo, que é um formato proprietário e é usado ao registrar no iView

Log Configuration

The screenshot displays the Sophos Firewall web interface for log configuration. The sidebar on the left includes sections for 'MONITOR & ANALYZE', 'PROTECT', 'CONFIGURE', and 'SYSTEM'. The 'CONFIGURE' section is expanded, showing 'System services' as the selected option. The main content area is titled 'Log settings' and features a table with the following columns: 'Log type (system)', 'Suppress logs', and 'Local reporting'. A green arrow points to the 'Local reporting' column header. The table lists various log types, with 'Firewall' and its sub-items having checkboxes in the 'Local reporting' column. An 'Apply' button is located at the bottom left, and a 'Sophos Assistant' button is at the bottom right.

Log type (system)	Suppress logs	Local reporting
All	<input type="checkbox"/>	<input type="checkbox"/>
Firewall	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Firewall rules		<input checked="" type="checkbox"/>
Invalid traffic		<input checked="" type="checkbox"/>
Local ACLs		<input checked="" type="checkbox"/>
DoS attack		<input checked="" type="checkbox"/>
Dropped ICMP redirected packet		<input checked="" type="checkbox"/>
Dropped source routed packet		<input checked="" type="checkbox"/>
Dropped fragmented traffic		<input checked="" type="checkbox"/>
MAC filtering		<input checked="" type="checkbox"/>
IP-MAC pair filtering		<input checked="" type="checkbox"/>
IP spoof prevention		<input checked="" type="checkbox"/>
SSL VPN tunnel		<input checked="" type="checkbox"/>
Protected application server		<input checked="" type="checkbox"/>

Você pode habilitar e desabilitar tipos de eventos específicos dentro de cada módulo ou do próprio módulo inteiro, e isso pode ser feito independentemente para o log local, Sophos Central e cada servidor syslog.

Firewall Log Suppression

Log settings

Log type (system)

Suppress logs



Suppressed logs will only show one log entry for consecutive, identical events. For the total count of suppressed logs, see log_occurrence.

All

☐

Firewall

☐☐

Firewall rules

☒

Invalid traffic

☒

Local ACLs

☒

DoS attack

☒

Dropped ICMP redirected packet

☒

2021-09-28 11:12:53

```
messageid="02002" log_type="Firewall" log_component="Appliance Access" log_subtype="Denied" status="Deny" con_duration="0"
fw_rule_id="N/A" fw_rule_name="" fw_rule_section="" nat_rule_id="0" nat_rule_name="" policy_type="0" sdwan_profile_id_request="0"
sdwan_profile_name_request="" sdwan_profile_id_reply="0" sdwan_profile_name_reply="" gw_id_request="0" gw_name_request=""
gw_id_reply="1" gw_name_reply="DHCP PortB GW" sdwan_route_id_request="0" sdwan_route_name_request="" sdwan_route_id_reply="0"
sdwan_route_name_reply="" user_group="" web_policy_id="0" ips_policy_id="0" appfilter_policy_id="0" app_name="" app_risk="0"
app_technology="" app_category="" vlan_id="" ether_type="IPv4 (0x0800)" bridge_name="" bridge_display_name="" in_interface="PortB"
in_display_interface="PortB" out_interface="" out_display_interface="" src_mac="2c:fd:a1:11:d0:c3" dst_mac="" src_ip="169.254.0.0"
src_country="R1" dst_ip="255.255.255.255" dst_country="R1" protocol="UDP" src_port="9413" dst_port="9413" packets_sent="0"
packets_received="0" bytes_sent="0" bytes_received="0" src_trans_ip="" src_trans_port="0" dst_trans_ip="" dst_trans_port="0"
src_zone_type="" src_zone="" dst_zone_type="" dst_zone="" con_direction="" con_id="" virt_con_id="" hb_status="No Heartbeat" message=""
appresolvedby="Signature" app_is_cloud="0" log_occurrence="1" web_policy=""
```

SOPHOS

Entradas repetidas no log do firewall podem ser suprimidas para torná-las menos barulhentas e mais fáceis de ler. Somente eventos idênticos consecutivos serão suprimidos e as entradas de log do firewall terão um novo campo para mostrar quantas ocorrências houve dessa entrada.



Retrieving Log Files

Upload a file from Sophos Firewall using FTP

```
ftpput -u <username> -p <password> host ip <Remote file name>  
<Local file name>
```

Upload a file from Sophos Firewall using SCP

```
scp <Local file name> <username>@<host>:/path/to/remote/file
```

SOPHOS

Pode haver um momento em que os arquivos precisem ser copiados de ou para o Sophos Firewall. Por exemplo, convém copiar alguns arquivos de log do dispositivo para retê-los por um período prolongado. Você pode fazer isso usando ftpput ou scp com os comandos mostrados aqui.

[Additional Information]

To use FTP, you can use the following commands in advanced shell:

- Get file : ftpget -u <username> -p <password> host ip <Local file name> <Remote file name>
- Put file : ftpput -u <username> -p <password> host ip <Remote file name> <Local file name>

To use SCP, you can use the following command in the advanced shell:

- scp <local file name> <username>@<host>:/path/to/remote/file

Notifications

Email

SYSTEM > Administration > Notification settings

- Configure email server settings
- Set email addresses
- Select management interface address

SNMP

SYSTEM > Administration > SNMP

- Enable SNMP agent
- Create SNMPv3 users and traps
- Create SNMPv1 and v2c community and traps

CONFIGURE > System settings > Notification list

- Enable and disable email and SNMP notifications globally
- Select which notifications to send for email and SNMP

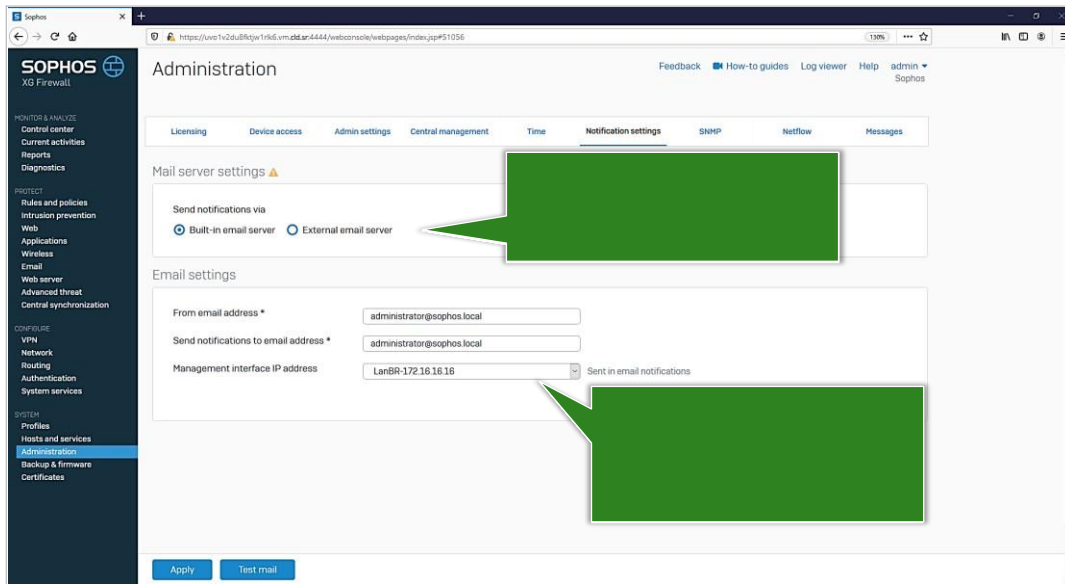
SOPHOS

O Sophos Firewall pode enviar notificações por e-mail, SNMP ou ambos. Há duas etapas para configurar este:

Configurar o método de notificação, e-mail ou SNMP

Selecione quais notificações você deseja enviar por e-mail e SNMP

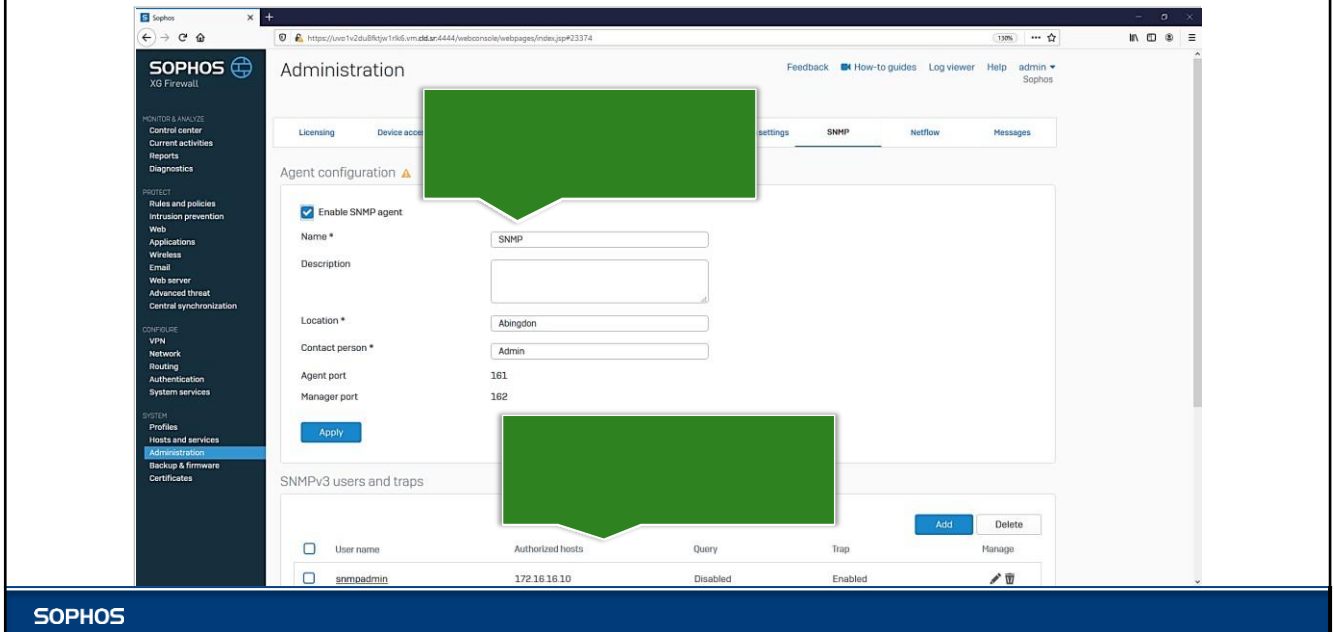
Email



SOPHOS

Durante a configuração inicial, você define algumas configurações básicas para alertas de e-mail para que você receba notificações para o novo firmware e quando o status dos gateways mudar. Você pode modificar ainda mais as configurações de e-mail em **SYSTEM > Administration > Notification settings**.

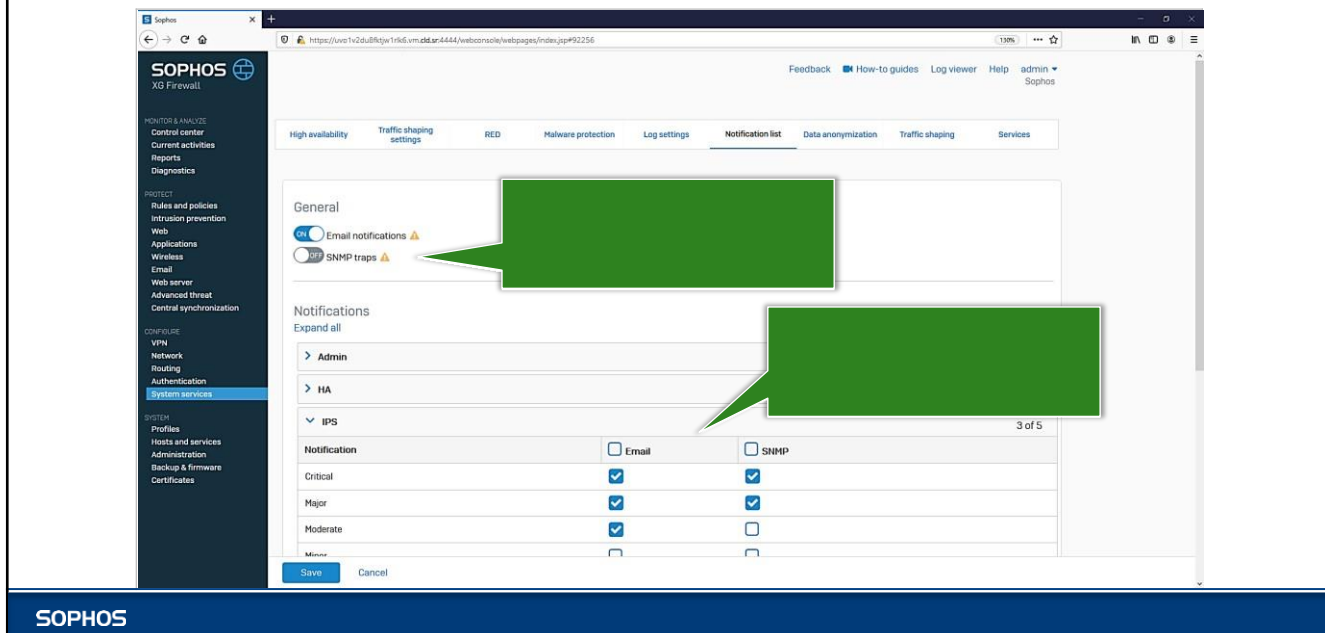
SNMP



O SNMP pode ser configurado em **SYSTEM > Administration > SNMP**.

Aqui você habilita e configura o agente SNMP no Sophos Firewall e cria usuários e traps SNMPv3 e comunidades SNMP e traps para v1 e v2c.

Notification list



Depois que o e-mail e o SNMP estiverem configurados, vá para **CONFIGURE > System services > Notification list**.

Você pode habilitar e desativar globalmente as notificações para e-mail e SNMP e controlar separadamente quais notificações são enviadas por meio de cada canal.