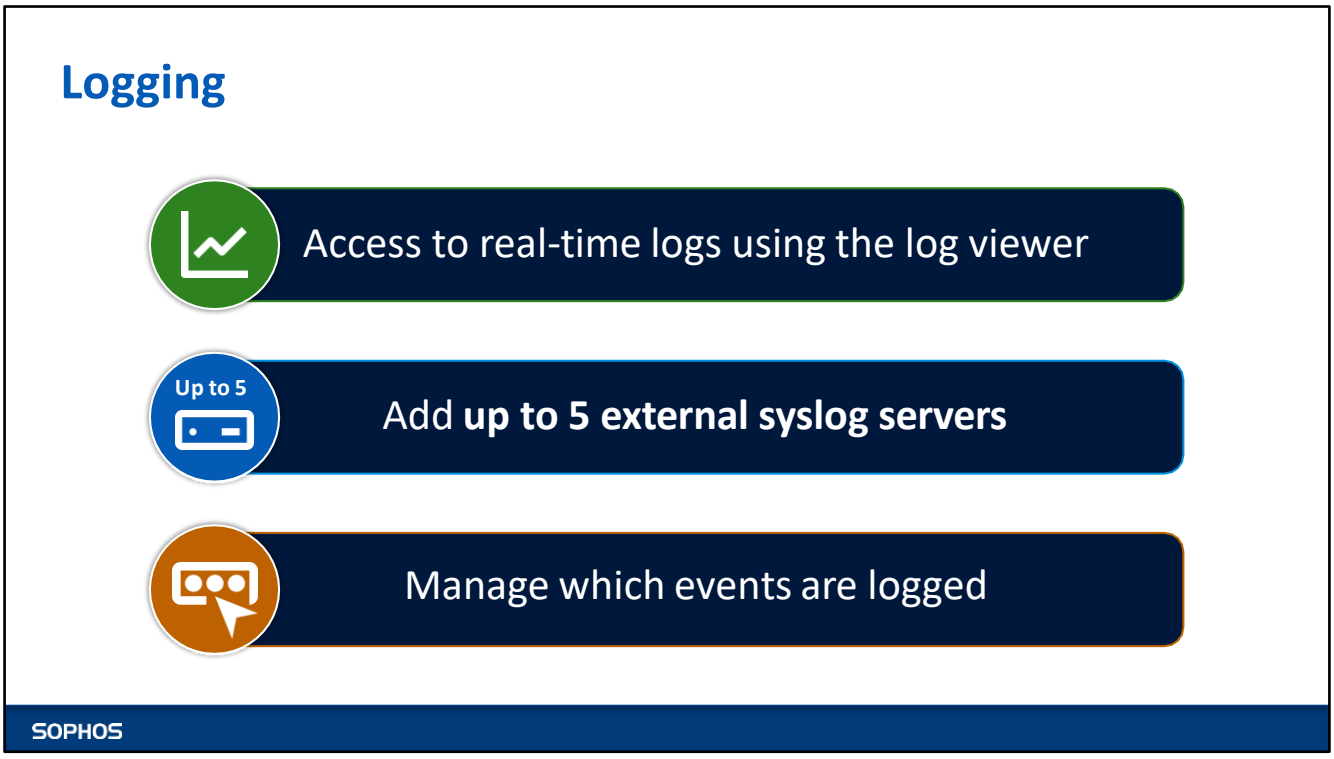
SOPHOS

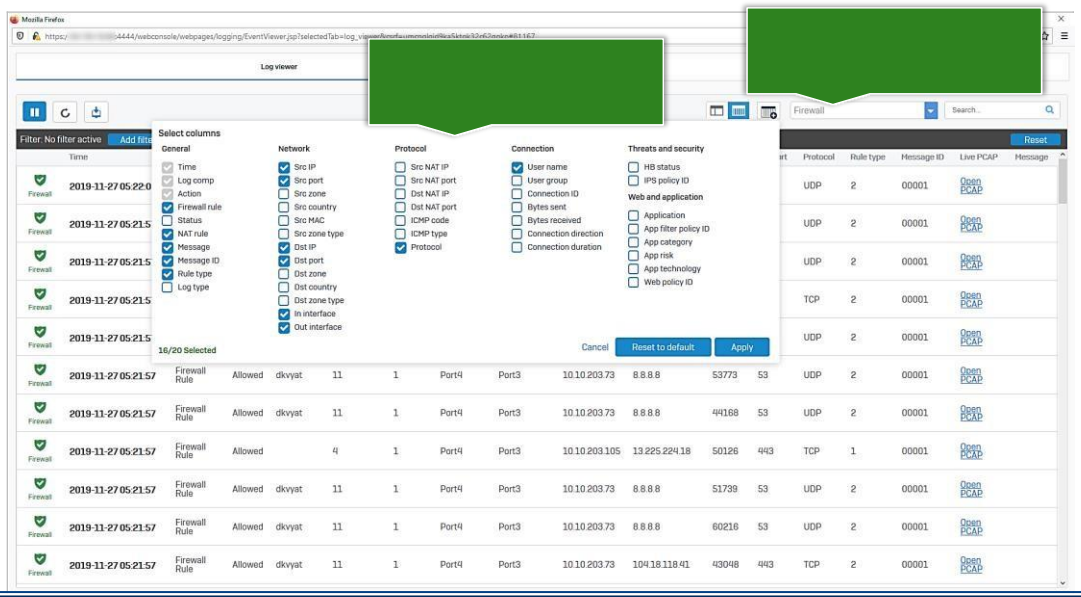
Managing Logs and Notifications on Sophos Firewall

Sophos Firewall
Version: 19.0v1



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



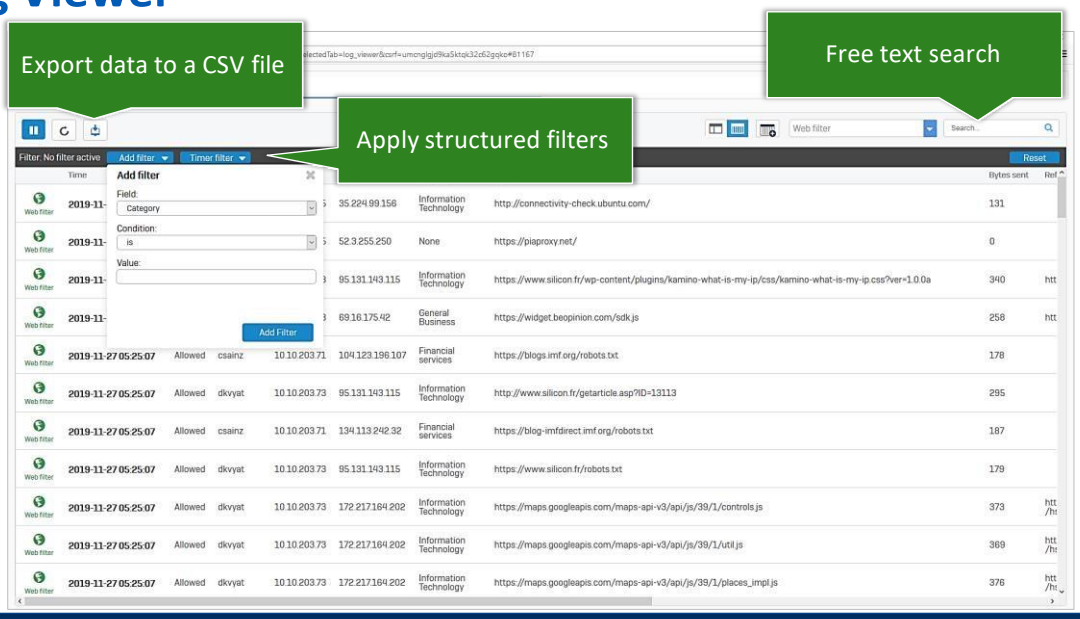
SOPHOS

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.

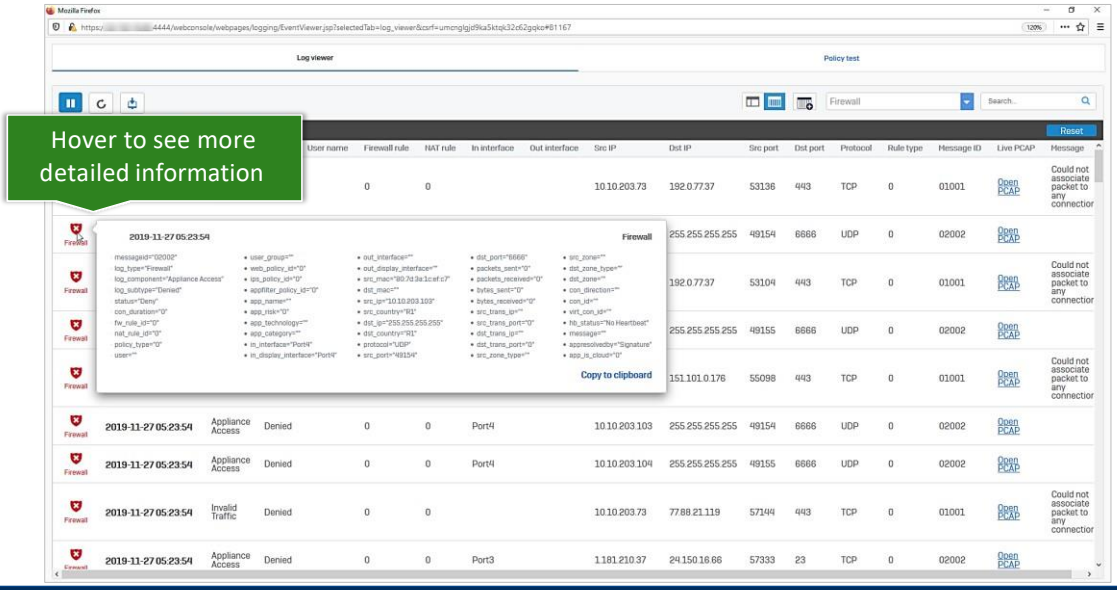
Log Viewer



SOPHOS

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.

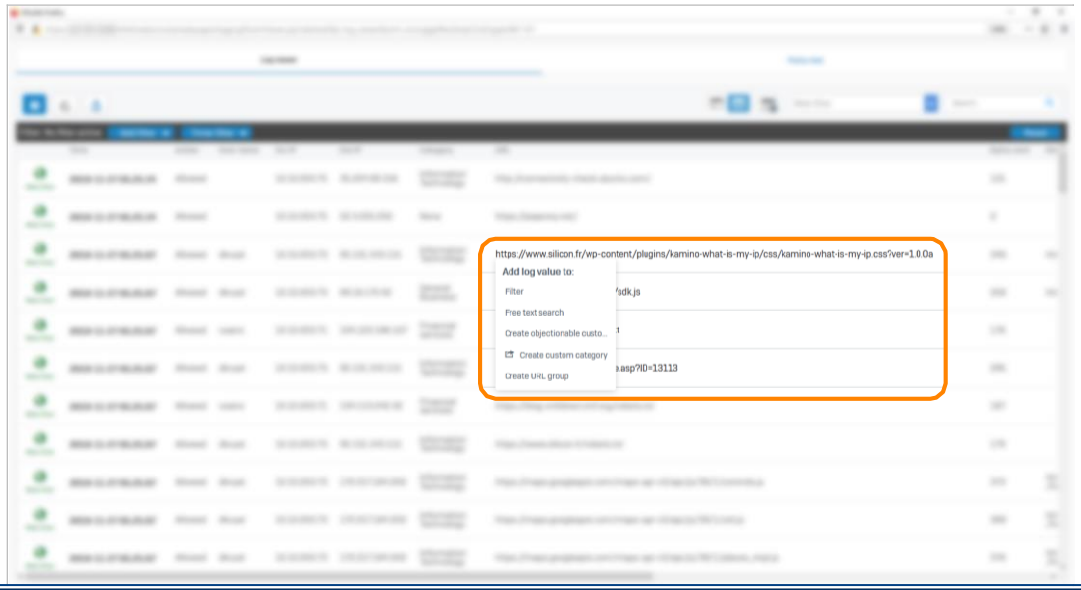
Log Viewer



SOPHOS

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

Log Viewer

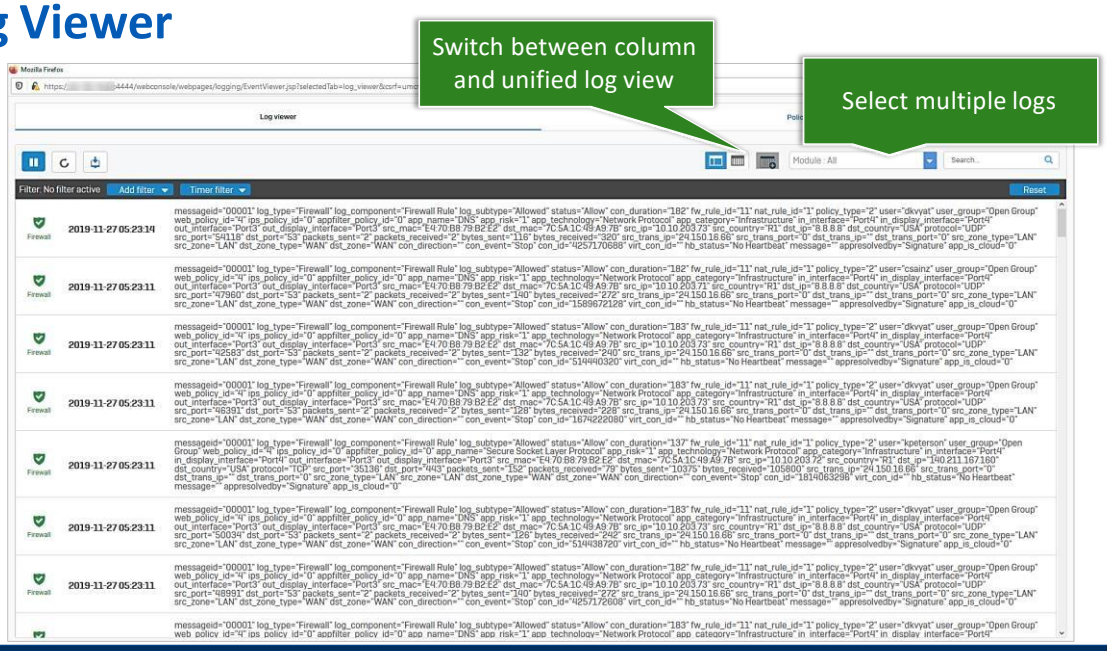


SOPHOS

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



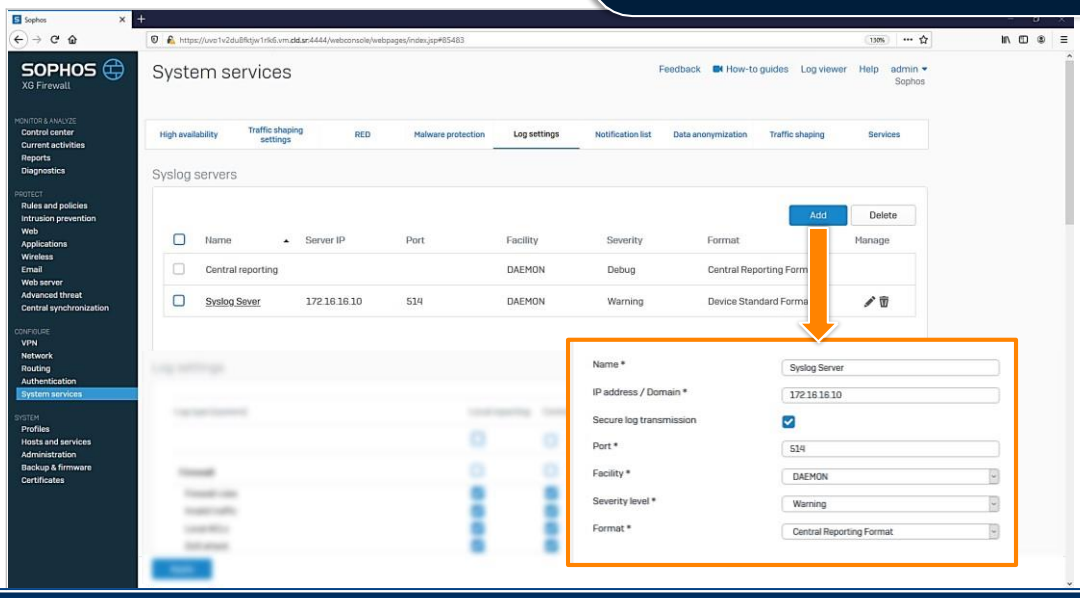
SOPHOS

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 pai navega automaticamente para esse local, tornando mais rápido e fácil revisar a configuração relevante para uma entrada de log.

Syslog



SOPHOS

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

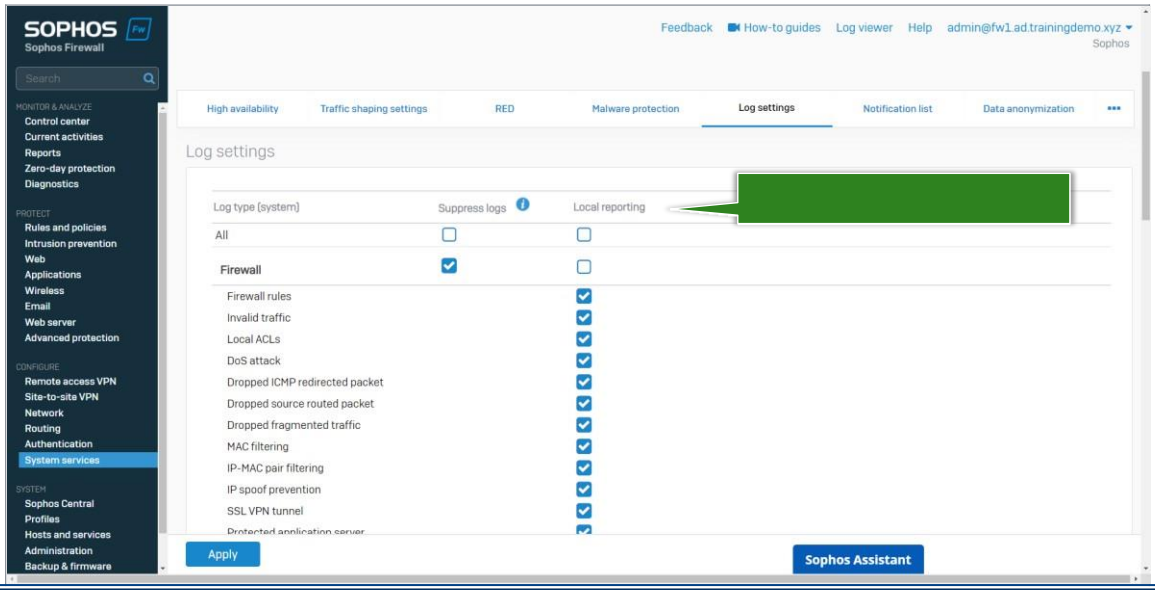
LOCAL0 – LOCAL7, para obter informações de um nível de log específico
USER, para registro em log com base em usuários que estão conectados ao servidor
Você também pode selecionar a gravidade dos eventos que deseja registrar. O firewall registrará todos os eventos para o nível selecionado e acima. Portanto,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

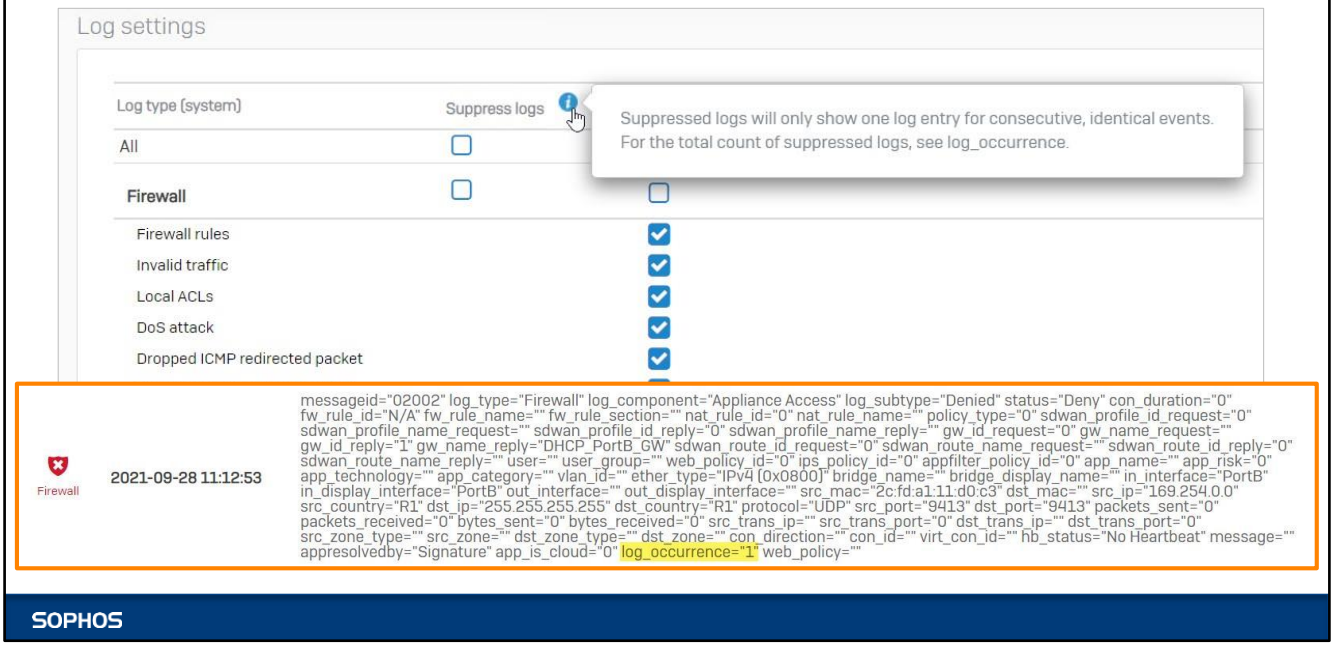
Log Configuration



SOPHOS

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



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

Additional information in the notes

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

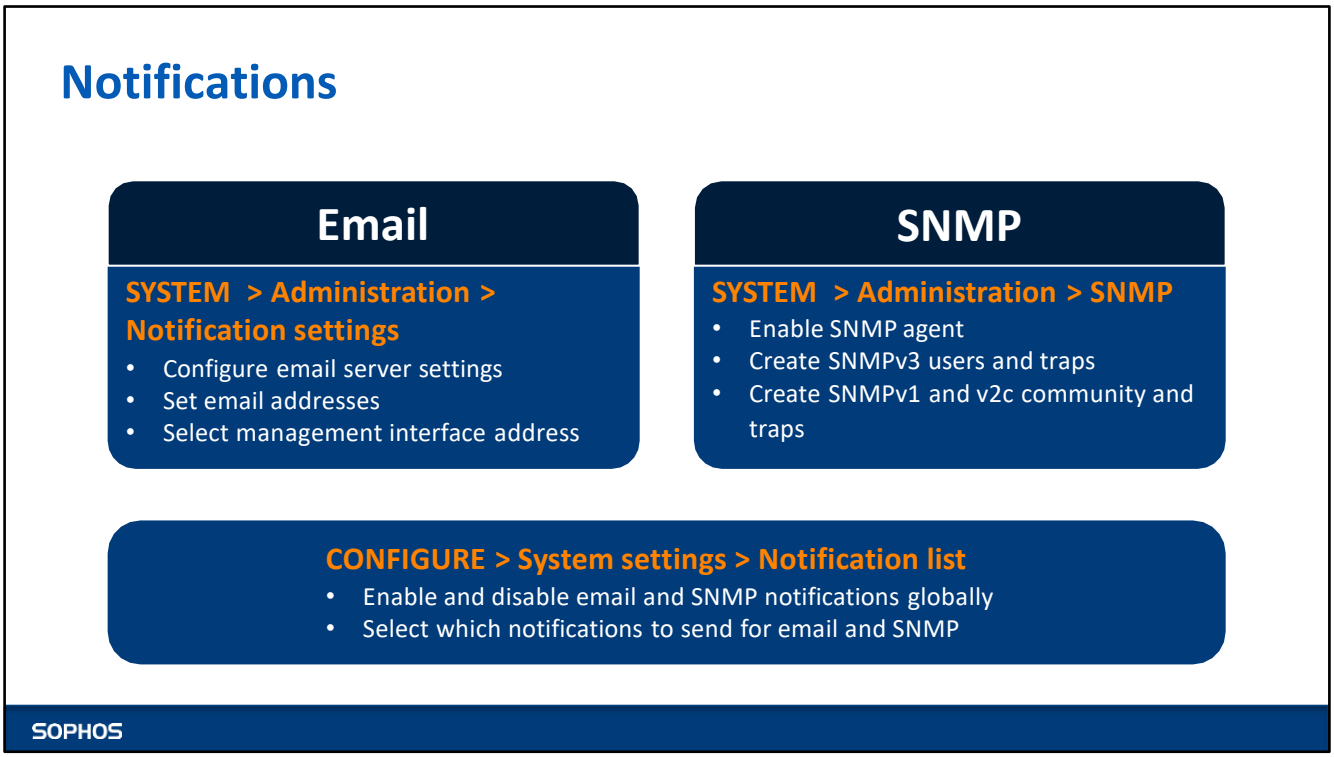
Pode haver um momento em que os arquivos precisem ser copiados de ou para o Sophos Firewall. Por exemplo, convém copiar alguns arquivos de log do dispositivo para retê-los por um período prolongado. Você pode fazer isso usando ftpput ou scp com os comandos mostrados aqui.

[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

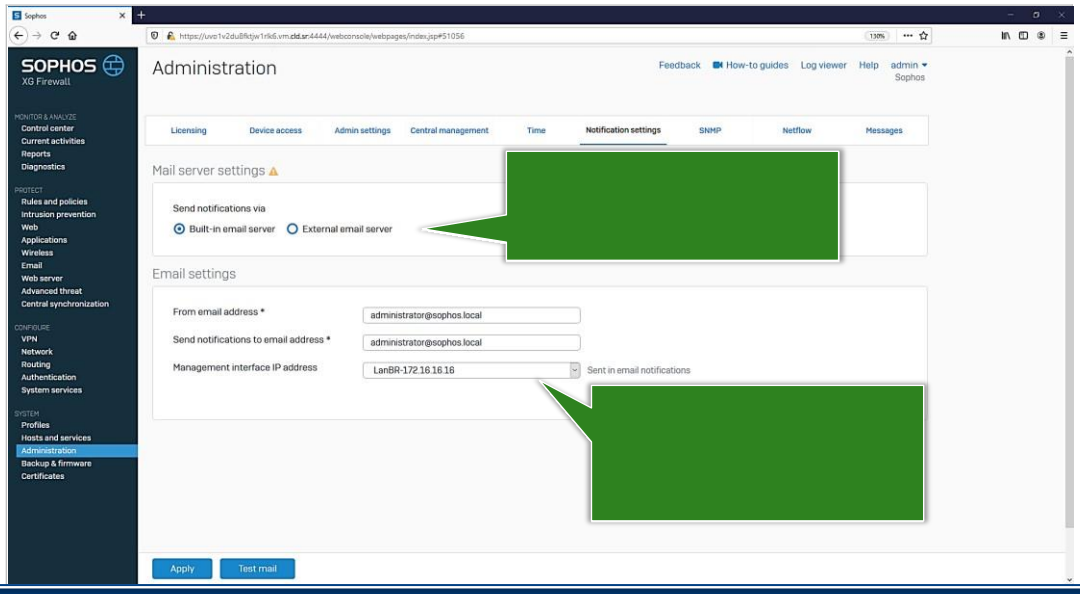


O Sophos Firewall pode enviar notificações por e-mail, SNMP ou ambos. Há duas etapas para configurar este:

Configurar o método de notificação, e-mail ou SNMP

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

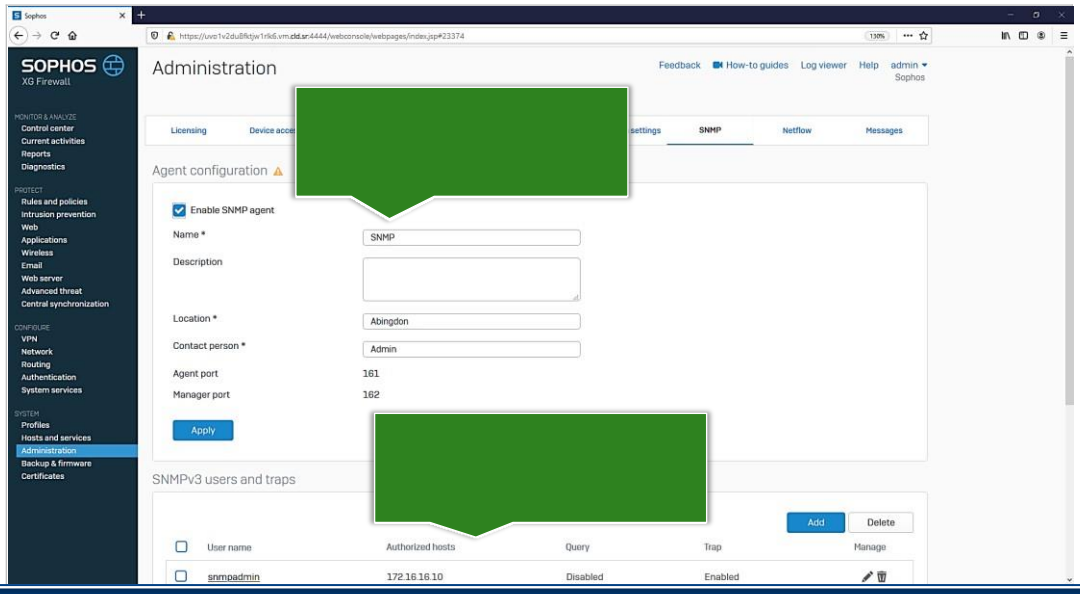
Email



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

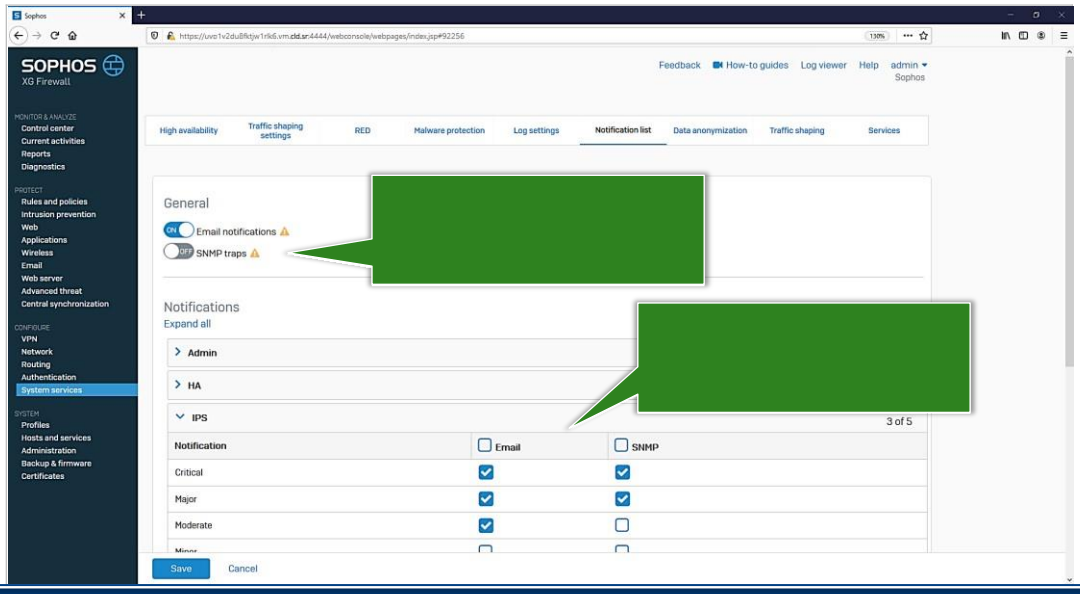


SOPHOS

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



SOPHOS

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.