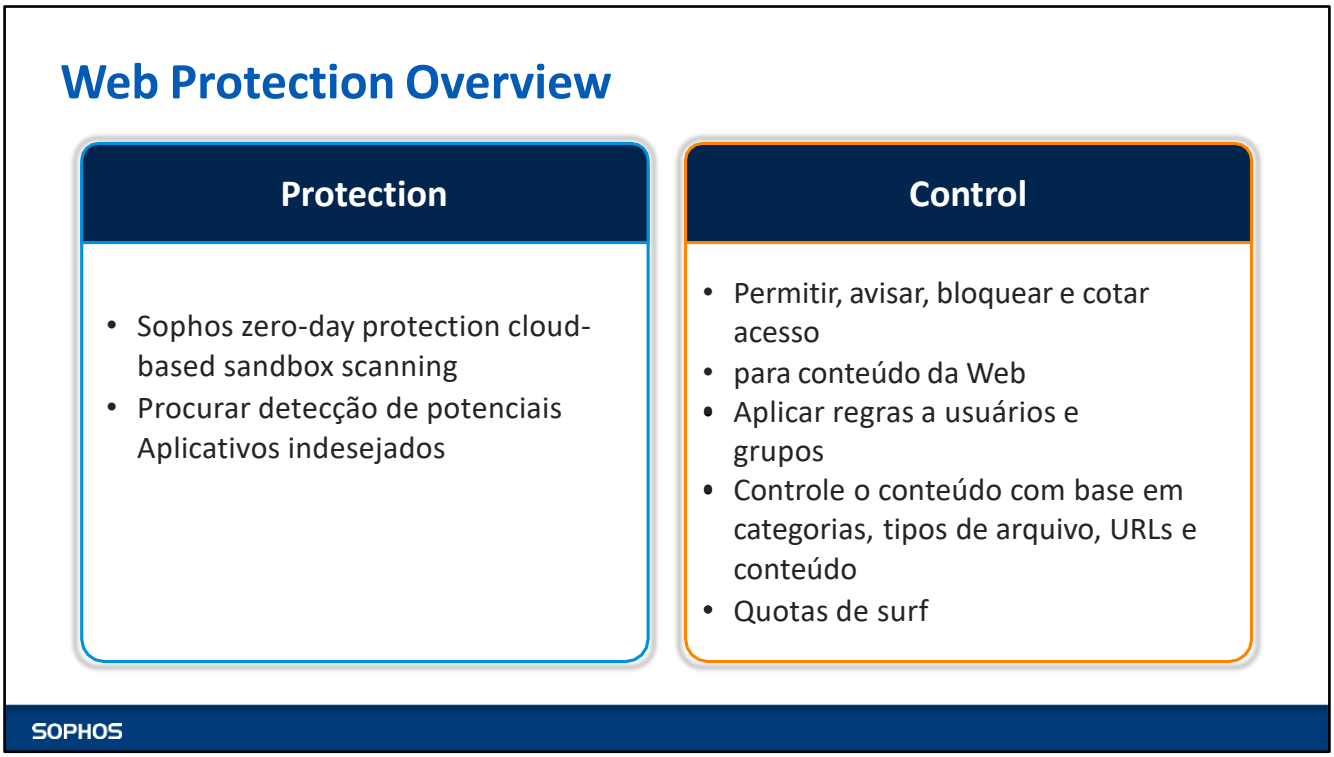
SOPHOS

Sophos Firewall Web Protection Overview

Sophos Firewall
Version: 19.0v1

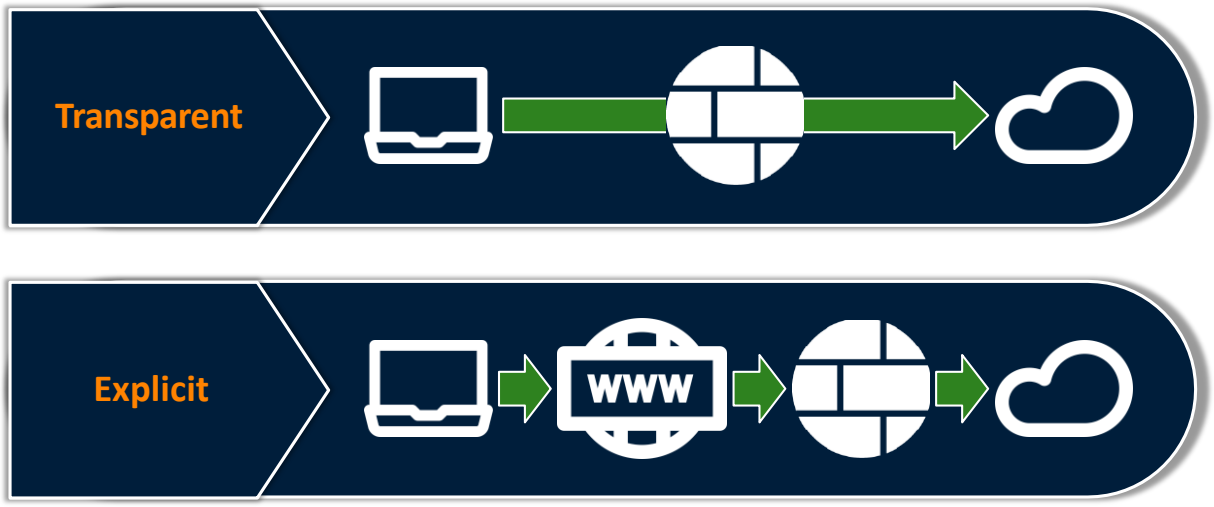


A Proteção da Web no Sophos Firewall pode ser usada para se defender contra malware e controlar o usuário comportamento.

O Sophos Firewall pode procurar conteúdo malicioso usando o mecanismos antivírus, Sophos, e se for necessária uma verificação adicional, ele pode aproveitar a proteção de dia zero, uma solução sandbox baseada em nuvem da Sophos. Além do conteúdo mal-intencionado, você também pode optar por bloquear o download de aplicativos potencialmente indesejados em sua rede.

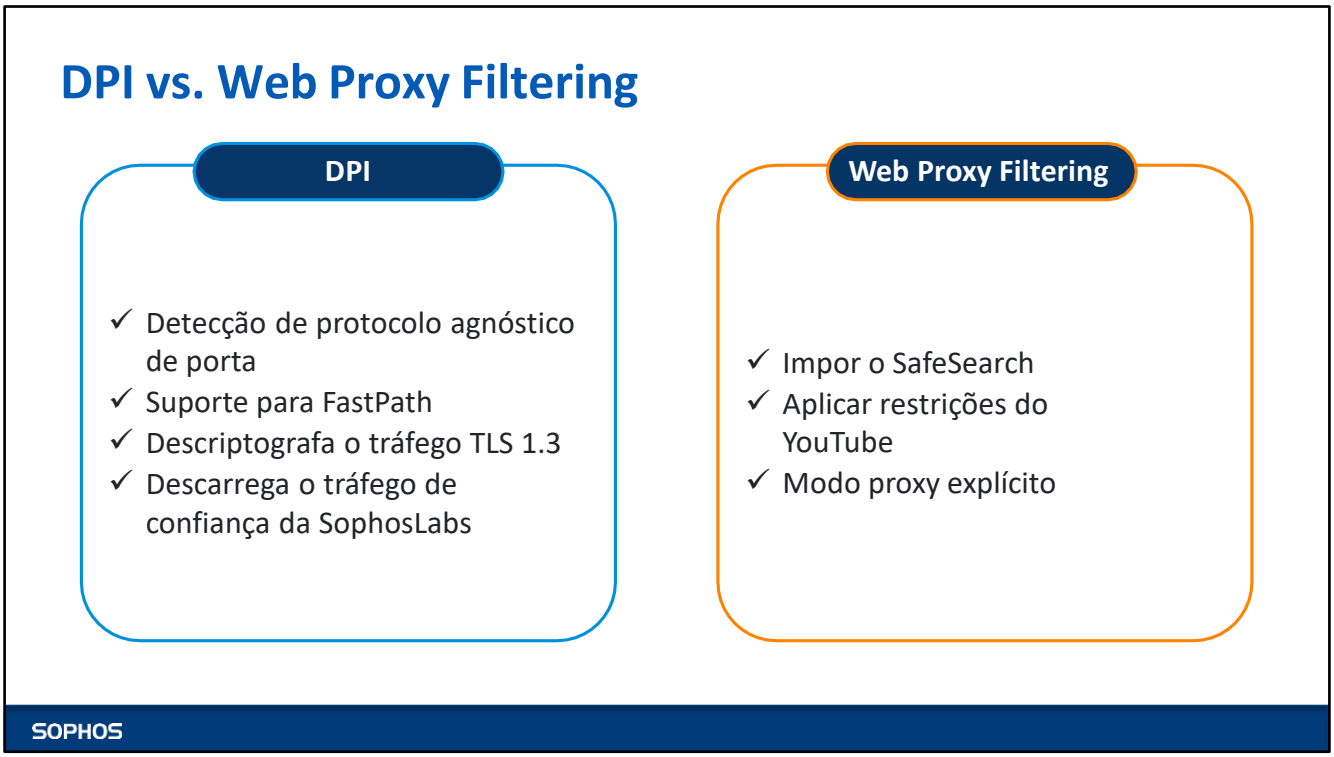
Você pode melhorar a segurança da sua rede bloqueando o acesso a sites de risco e aplicando controles ao comportamento de navegação dos usuários. O Sophos Firewall vem com várias políticas predefinidas para começar que podem ser personalizadas para atender às suas necessidades.

Web Protection Overview



SOPHOS

A filtragem da Web no Sophos Firewall pode ser feita de forma transparente, interceptando o tráfego à medida que passa, ou como um proxy explícito, onde os clientes são configurados para usar o Sophos Firewall como seu proxy da web.



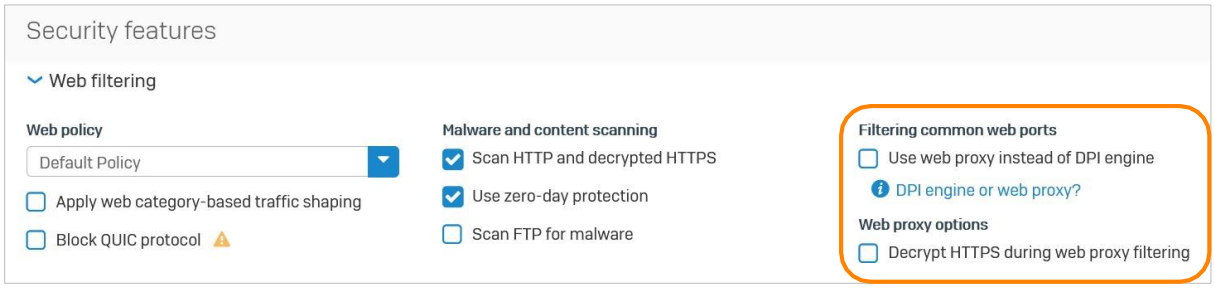
O mecanismo DPI (Deep Packet Inspection) pode executar a filtragem da Web para melhorar o desempenho, no entanto, você ainda pode optar por usar o proxy da Web herdado. Vamos dar uma olhada em algumas das diferenças entre DPI e filtragem de proxy da Web.

O DPI implementa a filtragem sem proxy manipulada pelo mecanismo IPS (Intrusion Prevention System). Ele fornece detecção de protocolo independente de porta e suporta o descarregamento parcial ou total de fluxos de tráfego para o FastPath de rede. Ele pode descriptografar e verificar o tráfego TLS 1.3 e descarrega o tráfego confiável pelo SophosLabs.

Em comparação, convém usar a filtragem de proxy da Web para impor o SafeSearch ou o YouTuberestrições ou porque seus clientes estão configurados para usar o Sophos Firewall como um proxy explícito.

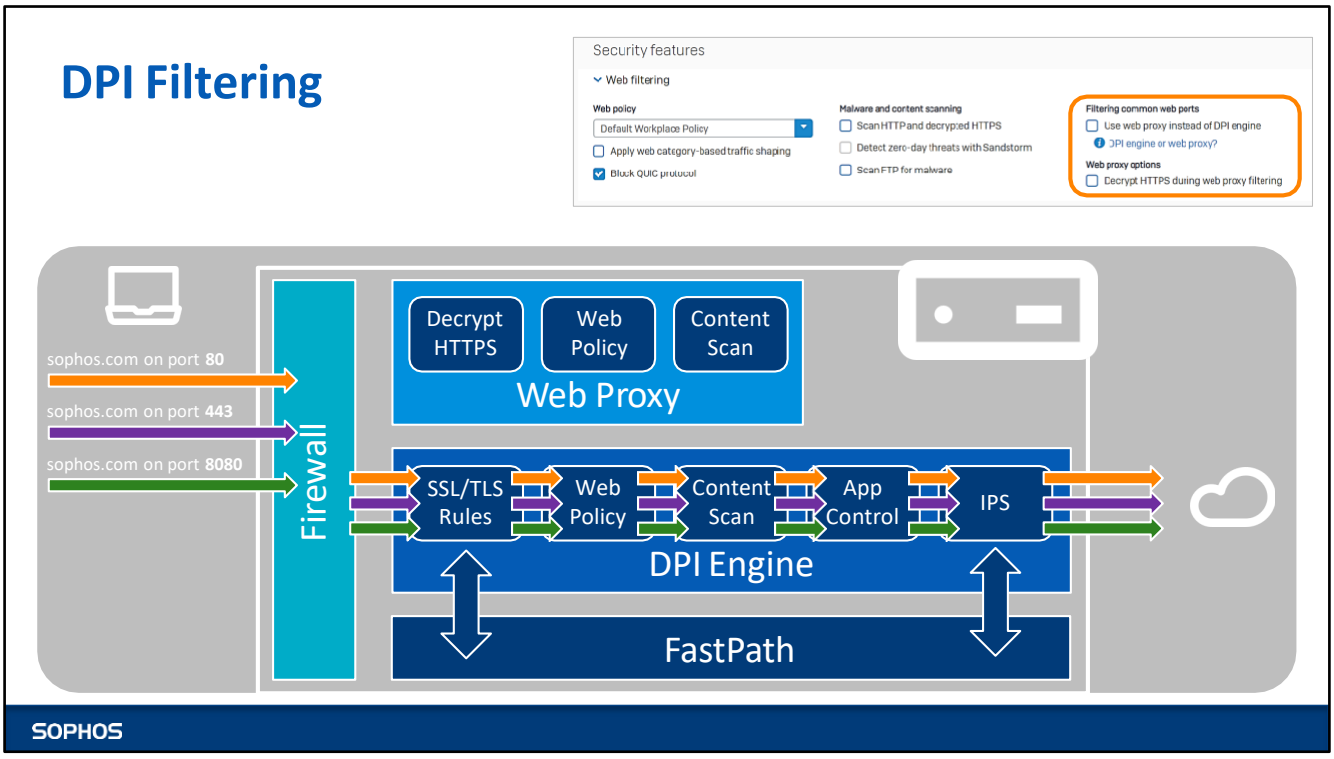
Vamos dar uma olhada mais de perto em como o tráfego é processado em cada um desses cenários.

Firewall Rule > Security Features



SOPHOS

A seção Recursos de Segurança das Regras de Firewall fornece configurações para escolher entre o DPI Mecanismo e Web Proxy para cada regra individual.

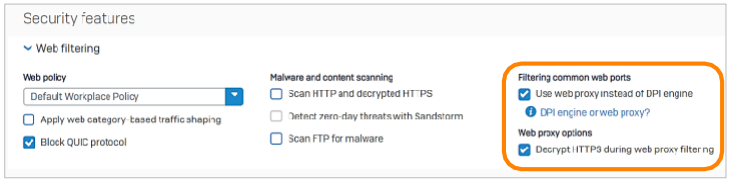


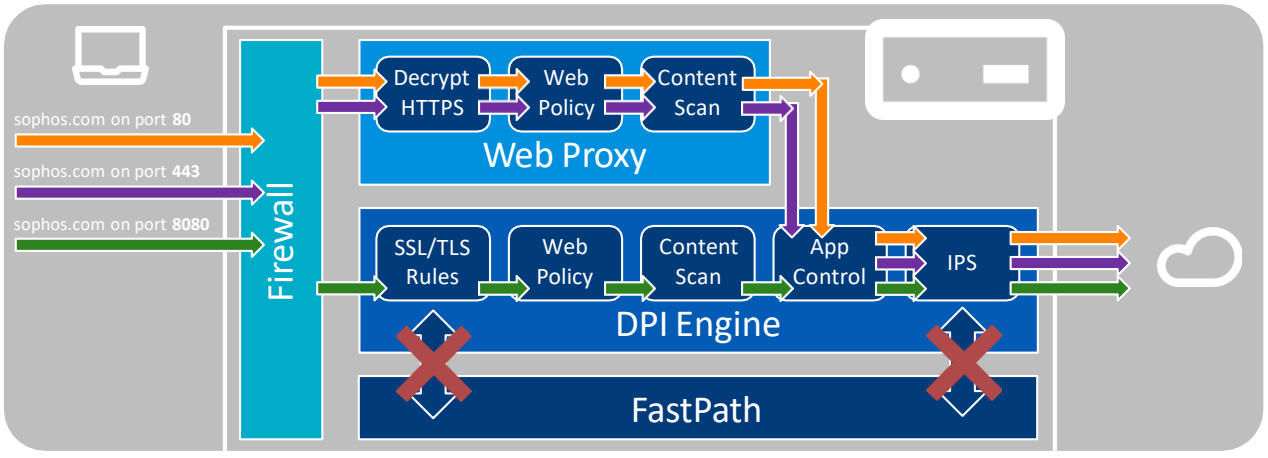
Usando a configuração mostrada aqui, todo o tráfego será tratado pelo mecanismo DPI mais rápido para IPS e filtragem da Web sem proxy e descriptografia SSL em qualquer porta para HTTP e HTTPS usando identificação de protocolo independente de porta.

Nessa configuração, as regras de inspeção SSL/TLS são usadas para gerenciar a descriptografia do tráfego seguro da Web.

O uso do mecanismo DPI permite que o Sophos Firewall descarregue o tráfego seguro para o FastPath. Isso é feito para o tráfego que o Sophos Firewall qualifica como sendo seguro ou que corresponde a identidades para o tráfego confiável do SophosLabs.

Web Proxy Filtering





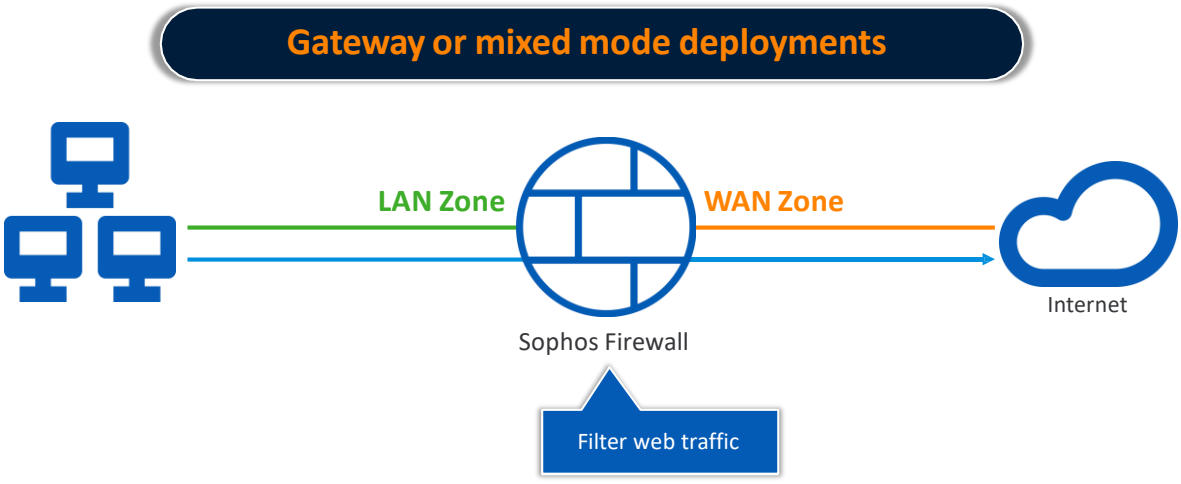
SOPHOS

Se você habilitar o proxy da Web, o tráfego HTTP e HTTPS nas portas 80 e 443 será processado pelo proxy da Web para descriptografia, política da Web e verificação de conteúdo, antes de ser entregue ao mecanismo DPI para controle de aplicativos e IPS.

O tráfego HTTP ou HTTPS em outras portas ainda será tratado pelo mecanismo DPI. O proxy da Web também é usado em configurações de proxy explícitas.

Quando o proxy da Web está sendo usado, nenhum tráfego pode ser descarregado para o FastPath.

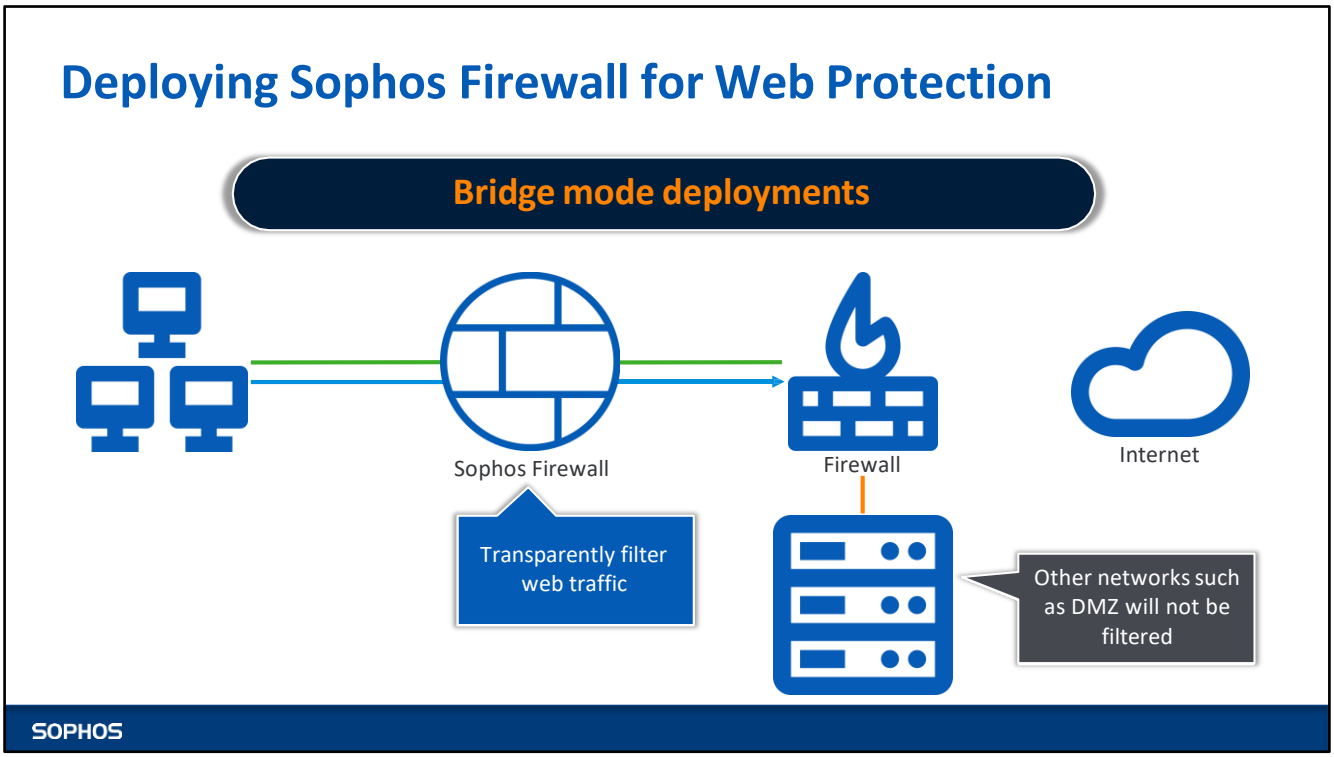
Deploying Sophos Firewall for Web Protection



Se o Sophos Firewall for o gateway de rede ou se estiver substituindo um gateway existente, então web a filtragem pode simplesmente ser ativada para o tráfego que passa por ela.

Esse cenário de implantação é ideal, pois todo o tráfego deve passar pelo Sophos Firewall antes de ser permitido na Internet. Como tal, todo o tráfego que entra na rede também deve passar pelo Sophos Firewall antes de chegar aos clientes. Ao implementar dessa maneira, todo o tráfego da Web pode ser verificado, descriptografado, enviado para proteção de dia zero, se necessário, e controlado para que os usuários não possam violar a política da empresa e os hackers não possam passar despercebidos.

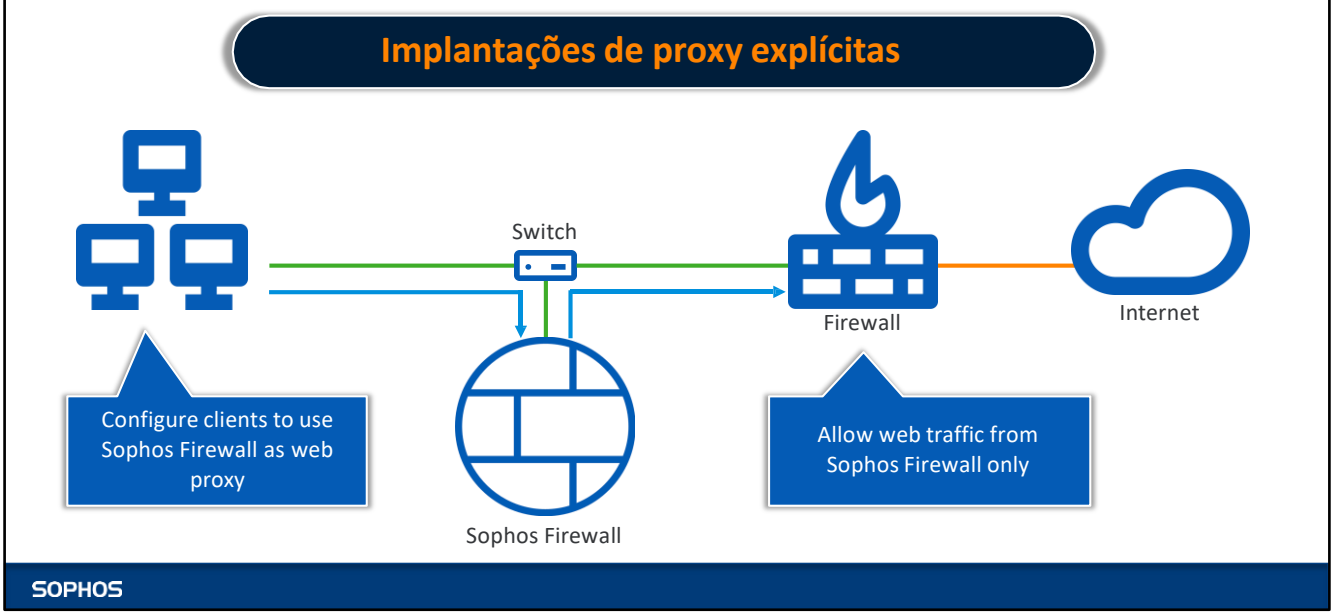
Nesse cenário de implantação, o Sophos Firewall pode ser usado como um ambiente transparente e explícito procuração.



Em cenários em que o Sophos Firewall não será o gateway de rede principal, há dois opções de implantação.

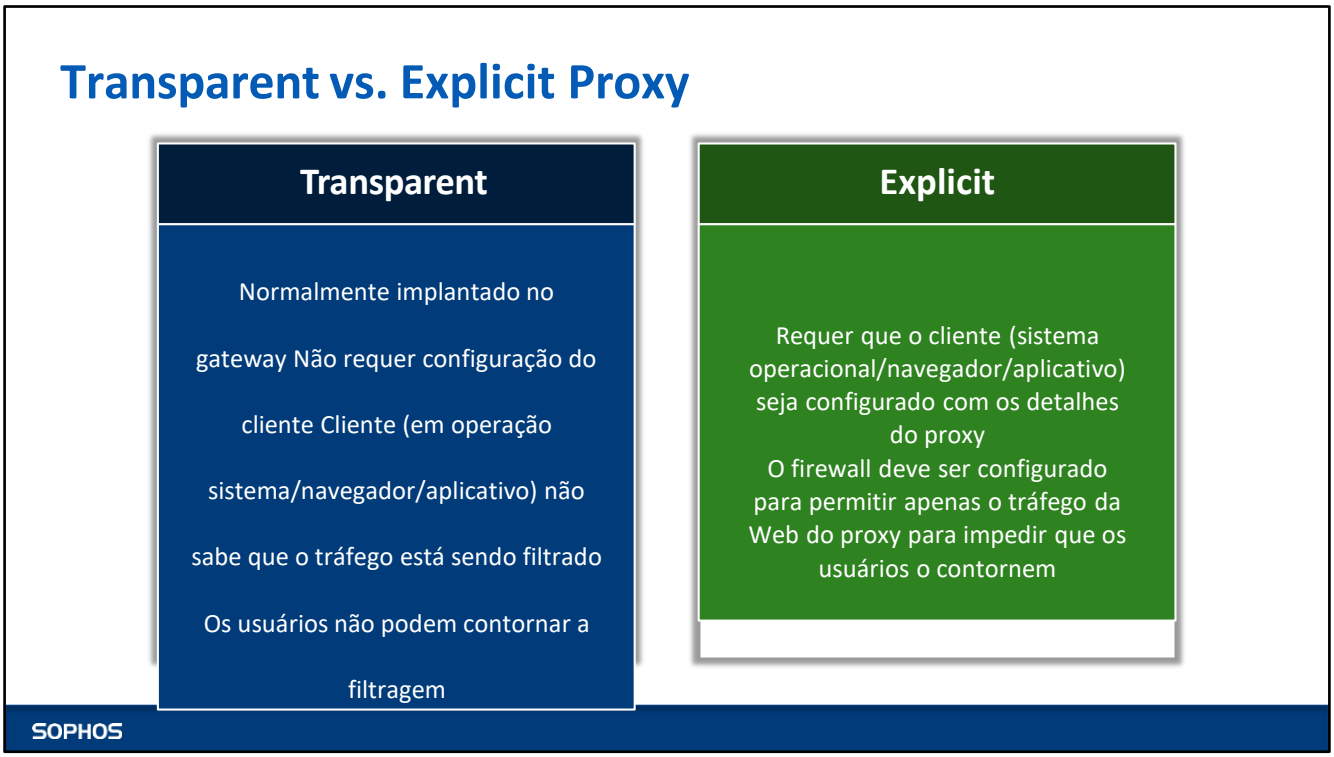
A primeira é adicionar o Sophos Firewall à rede no modo bridge, permitindo que ele filtre de forma transparente o tráfego da web. Esta é uma boa solução se o dispositivo de borda existente não for substituído. Da mesma forma, para a solução anterior, qualquer pessoa por trás do Sophos Firewall não poderá ignorar o filtro e terá seu tráfego inspecionado. A única exceção seria se houvesse outra rede, como uma DMZ hospedando servidores públicos, atrás do firewall de borda.

Deploying Sophos Firewall for Web Protection



A outra opção é que o Sophos Firewall esteja na rede, mas não no fluxo direto de e ter os clientes configurados para usá-lo como um proxy explícito.

Nessa configuração, o Sophos Firewall não tem nenhum controle sobre o tráfego que é enviado diretamente para o gateway padrão e, portanto, é importante que o dispositivo de borda esteja configurado para permitir apenas o tráfego da Web de dispositivos permitidos, incluindo o Sophos Firewall.



As principais diferenças entre a filtragem da Web de proxy transparente e explícita são:
Em uma configuração de proxy transparente, o proxy normalmente é implantado no gateway da Internet e o serviço de proxy é configurado para interceptar o tráfego de uma porta especificada.

O cliente (por exemplo, navegador, aplicativo de desktop, etc.) não está ciente de que o tráfego está sendo processado por um proxy. Por exemplo, um proxy HTTP transparente é configurado para interceptar todo o tráfego na porta 80/443. Isso fornece uma configuração corporativa padrão em que todos os clientes roteados para a Internet serão filtrados e protegidos, independentemente do que os usuários finais fizerem ou alterarem em suas máquinas. Um benefício adicional é a redução da solução de problemas de configuração cliente-proxy. Proxies transparentes também lidam com dispositivos móveis e convidados sem qualquer configuração adicional.

Em uma configuração de proxy explícita, o cliente é explicitamente configurado para usar um servidor proxy, o que significa que o cliente sabe que todas as solicitações passarão por um proxy. O cliente recebe o nome do host, o endereço IP e o número da porta do serviço proxy. Quando um usuário faz uma solicitação, o cliente se conecta ao serviço de proxy e envia a solicitação. A desvantagem do proxy explícito é que cada cliente deve ser configurado corretamente para usar o proxy.