SOPHOS
Cybersecurity delivered.

Sophos Firewall

Resumo da solução

Índice

Sophos Firewall

O Sophos Firewall foi concebido para abordar os principais problemas atuais com firewalls existentes, ao mesmo tempo que oferece uma verdadeira plataforma next-gen para lidar com o cenário moderno de Internet criptografada e de ameaças em constante evolução. O Sophos Firewall traz uma nova abordagem à maneira como você identifica riscos ocultos, se protege contra ameaças e responde a incidentes acompanhada de um ótimo desempenho. A Xstream Architecture for Sophos Firewall utiliza uma arquitetura de processamento em pacotes que oferece níveis extremos de visibilidade, proteção e desempenho.

O Sophos Firewall proporciona visibilidade incomparável de usuários de risco, aplicativos indesejáveis, cargas suspeitas e ameaças persistentes. Ele integra perfeitamente uma suíte completa de tecnologias de proteção contra ameaças que é fácil de configurar e manter. Diferentemente de firewalls legados, o Sophos Firewall se comunica com outros sistemas de segurança na rede, possibilitando que ele se torne seu ponto de aplicação confiável para conter ameaças e impedir que malwares se espalhem ou exfiltrem dados da rede – automaticamente – em tempo real.

O Sophos Firewall tem quatro grandes vantagens em relação aos outros firewalls de rede:

1. **Expõe riscos ocultos** – o Sophos Firewall é muito melhor em relação a outras soluções na exposição de riscos ocultos ao apresentar um painel para controle visual, relatórios detalhados integrados e baseados na nuvem e insights únicos sobre os riscos.
2. **Bloqueia ameaças desconhecidas** – o Sophos Firewall bloqueia as ameaças desconhecidas com mais rapidez e eficiência do que outros firewalls por meio de uma suíte completa de funcionalidades avançadas de proteção que são bastante fáceis de configurar e gerenciar.
3. **Responde automaticamente a incidentes** – o Sophos Firewall com Segurança Sincronizada responde automaticamente a incidentes na rede graças ao Sophos Security Heartbeat™, que compartilha inteligência em tempo real entre os seus endpoints e o seu firewall.
4. **Otimize a sua rede SD-WAN** – os recursos do Xstream SD-WAN no Sophos Firewall permitem instalar redes de sobreposição SD-WAN complexas bastando simplesmente apontar e clicar. Você pode também aproveitar a seleção automática de link WAN baseada no desempenho com transições instantâneas entre links com zero de impacto que otimiza o desempenho do seu aplicativo, a resiliência da rede e a continuidade dos negócios, além de promover a redução de custos de conectividade.

Exposição de riscos ocultos

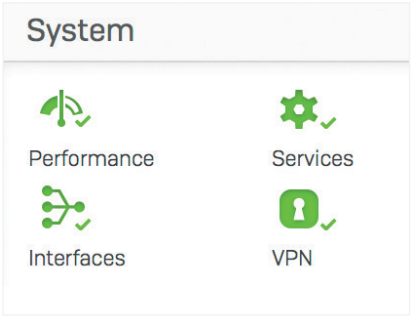
Para um firewall moderno é importante analisar a grande quantidade de informações que ele coleta, correlacionar dados sempre que possível e destacar somente as informações essenciais que requerem ação – antes que seja tarde.

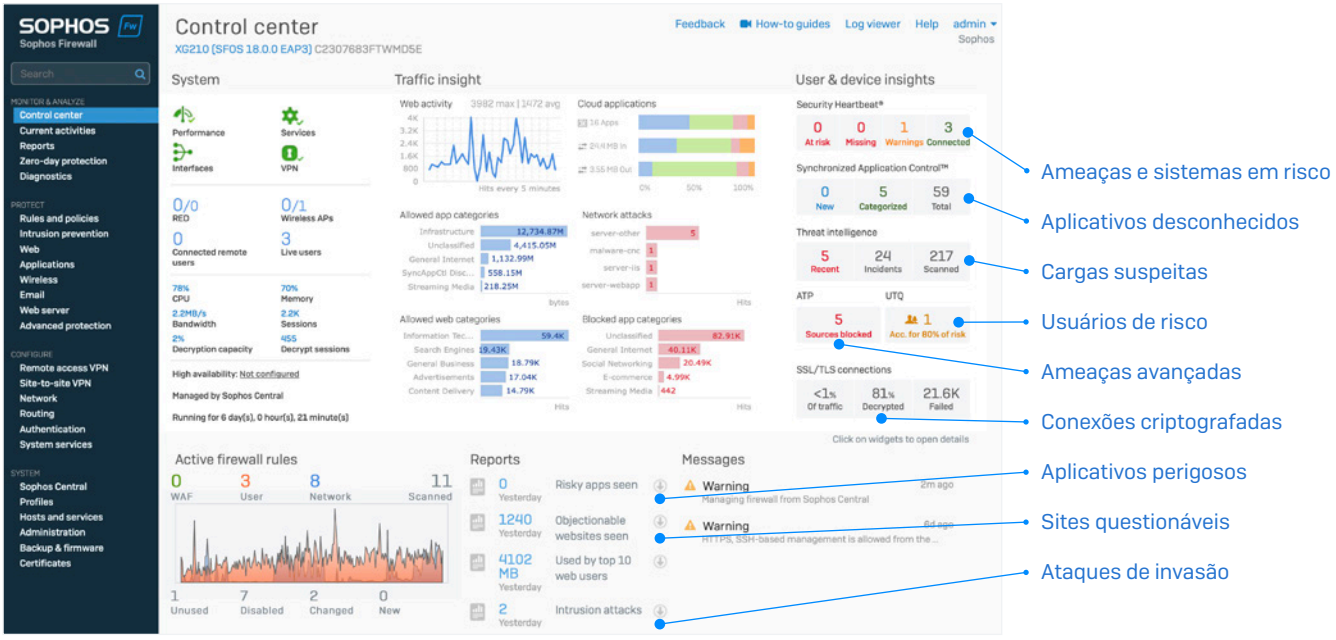
Central de Controle

A Central de Controle do Sophos Firewall oferece um nível jamais visto de visibilidade das atividades, riscos e ameaças em sua rede.

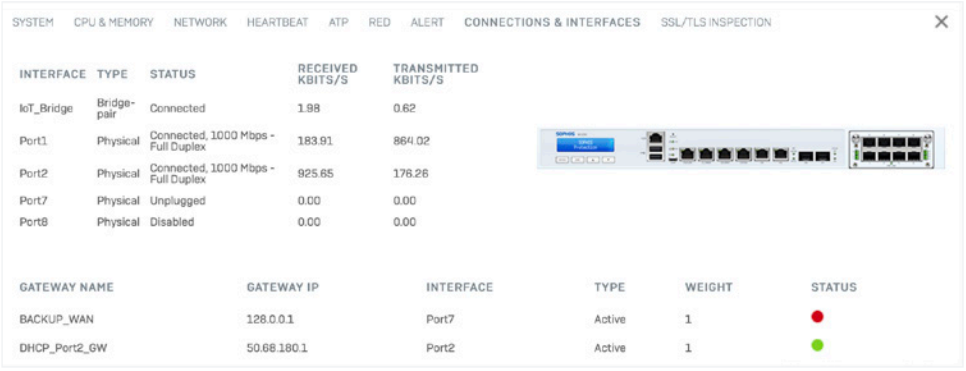
Ela utiliza indicadores no estilo "semáforo" (baseado em cores) para voltar sua atenção no que é mais importante para você.

Se algo está em vermelho, requer atenção imediata. Amarelo indica um possível problema.
E se tudo estiver em verde, não é necessária nenhuma outra ação.

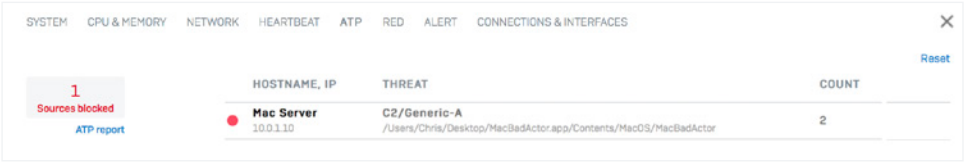




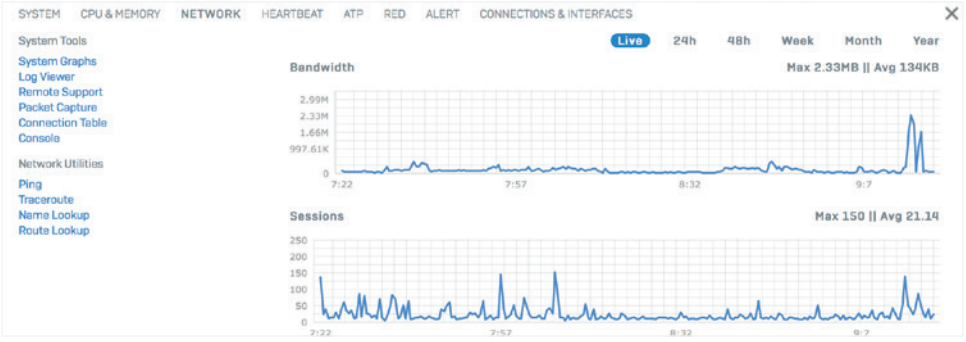
Cada widget na Central de Controle oferece informações adicionais, que são facilmente reveladas bastando clicar naquele widget. Por exemplo, o status das interfaces do dispositivo pode ser obtido clicando no widget "Interfaces" na Central de Controle.



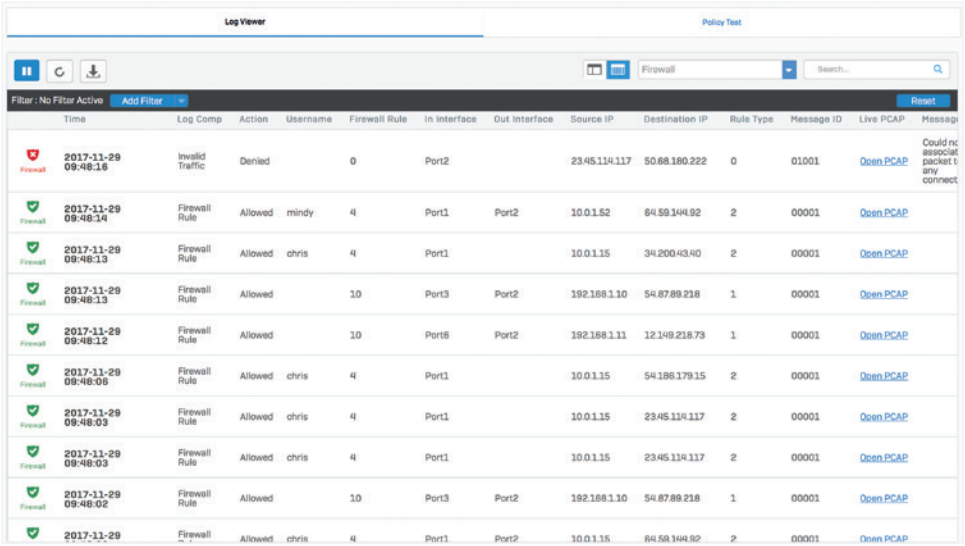
O host, usuário e origem de uma ameaça avançada são facilmente determinados com o simples clique do widget ATP (proteção contra ameaças avançadas) no painel de controle.



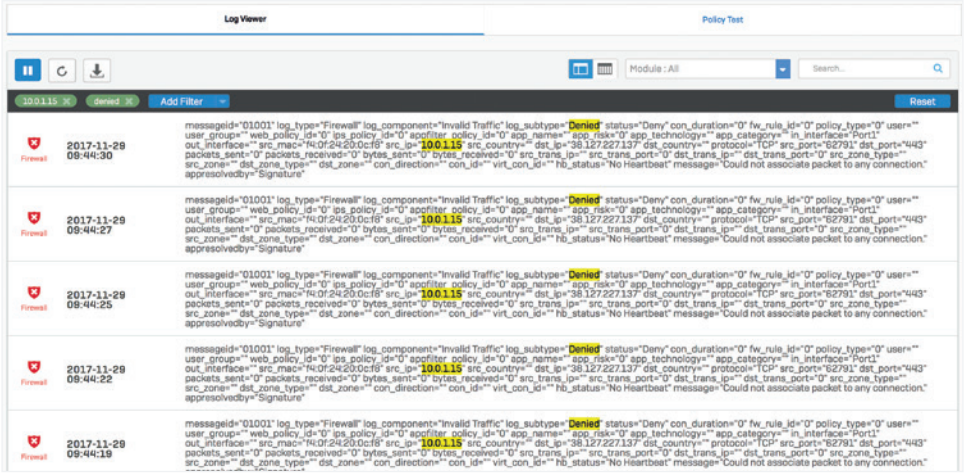
Gráficos do sistema também mostram o desempenho ao longo de períodos selecionáveis, caso deseje ver as últimas duas horas até o último mês ou ano. Além disso, eles oferecem acesso rápido a ferramentas de solução de problemas comumente usadas para resolver possíveis problemas.



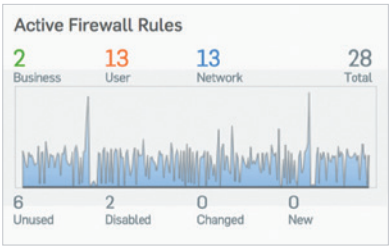
O visualizador de logs em tempo real encontra-se disponível em todas as telas, através de um simples clique. É possível abri-lo em uma nova janela para você manter um olho no log relevante, enquanto trabalha no painel de controle. Ele oferece duas vistas, uma mais simples, no formato de coluna, por módulo de firewall, e uma unificada mais detalhada, com filtros poderosos e opções de ordenação que agregam logs de todo o sistema em uma única vista em tempo real.



Se você é como a maioria dos administradores de rede, provavelmente ficou em dúvida se possui regras de firewall em demasia, e quais são realmente necessárias em relação às que não estão sendo usadas. Com o Sophos Firewall, você não precisa mais ficar em dúvida.



O widget de Regras Ativas de Firewall mostra um gráfico em tempo real do tráfego processado pelo firewall, por tipo de regra: Regras de Aplicativo de Negócios, Usuário e Rede. Ele também mostra uma contagem ativa das regras por status, inclusive as regras não utilizadas, dando-lhe a oportunidade de realizar uma manutenção. Assim como nas outras áreas da Central de Controle, clicar em qualquer uma delas expandirá, neste caso, a tabela de regras de firewall ordenadas pelo tipo ou status da regra.

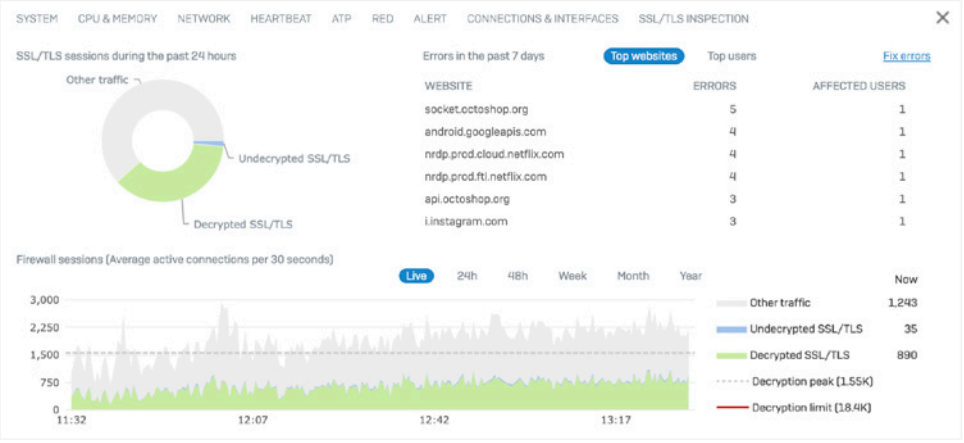


Inspeção TLS Xstream

Uma grande tempestade começa a envolver o tráfego criptografado. De acordo com a Google, o volume do tráfego criptografado nas redes cresceu para mais de 90%. Esse aumento representa uma oportunidade para os criminosos virtuais lançarem ataques que estão na espreita e, portanto, difíceis de detectar. Afinal de contas, você não pode parar o que não pode ver. Infelizmente, a maioria das organizações não consegue fazer muito contra isso porque o firewall que elas têm não oferece o desempenho necessário para utilizar inspeção TLS/SSL sem torná-lo drasticamente lento.

O Sophos Firewall, com o seu novo mecanismo de inspeção SSL Xstream, tem capacidade muito mais alta para conexões simultâneas e oferece ferramentas flexíveis de políticas para tomar decisões inteligentes sobre o que deve e pode ser verificado – e descartado quando apropriado. Ao utilizar ferramentas de políticas SSL, as organizações podem criar políticas TLS/SSL de grau Enterprise relacionadas a tráfego indecifrável, opções de imposição de cipher, certificados, protocolos e mais. O Sophos Firewall é compatível com TLS 1.3 e todas as suítes de criptografia modernas em todas as portas e aplicativos no sistema.

Ferramentas adicionais disponíveis diretamente no painel de controle permitem que os administradores vejam exatamente quanto tráfego de rede foi criptografado e como está sendo manipulado. O Sophos Firewall faz um trabalho muito melhor de exibição dessas informações do que qualquer outra solução, especialmente o modo como destaca os erros que são encontrados devidos a validação de certificado ou websites que não aceitam os padrões recentes de criptografia.



O Sophos Firewall oferece insights sobre os fluxos de tráfego criptografado e quaisquer problemas que possam surgir da inspeção TLS diretamente da central de controle

Os administradores podem exibir uma janela pop-up detalhada para ver exatamente quais sites são problemáticos e por que – além dos usuários que estão tendo problemas. A partir dessas informações eles podem agir diretamente para excluir o aplicativo ou site da decodificação para evitar problemas futuros. Nenhuma outra solução de inspeção SSL oferece a mesma acessibilidade a essas informações.

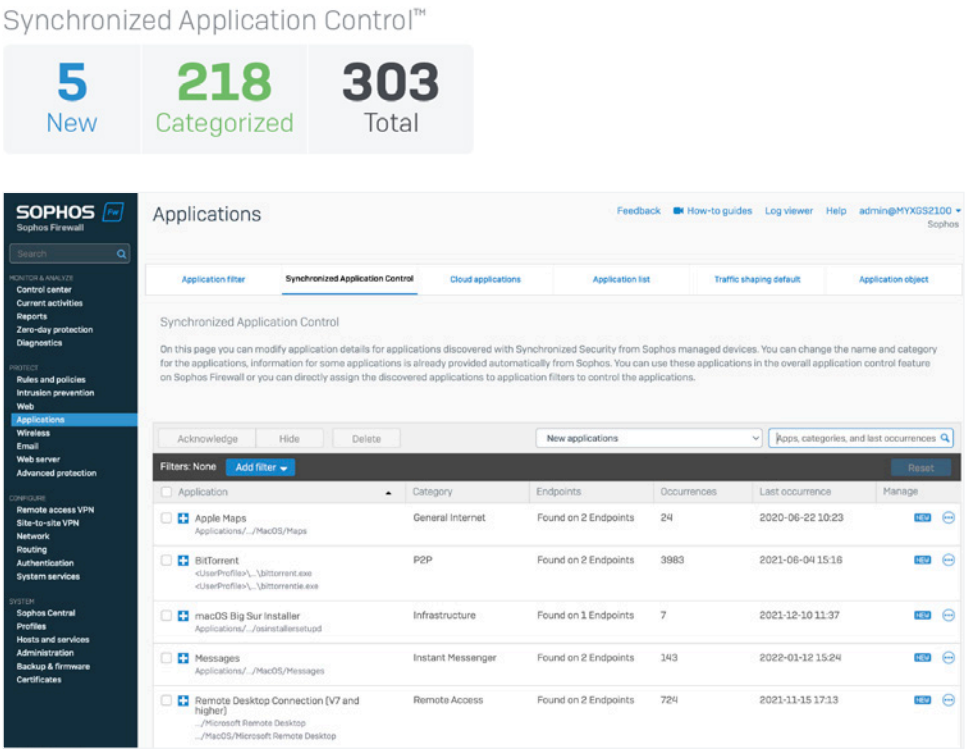
Controle Sincronizado de Aplicativos

O problema com o controle de aplicações nos firewalls next-gen de hoje em dia é que a maioria do tráfego de aplicativos passa sem ser identificado: sem classificação ou rotulado como desconhecido, HTTP genérico ou HTTPS genérico.

A razão disso é simples: todos os mecanismos de controle de aplicativo de firewall recorrem a assinaturas e padrões para identificar as aplicações. De modo geral, aplicações personalizadas de segmentos de mercado, como aplicativos médicos e financeiros, nunca terão assinaturas. Outros aplicativos evasivos, como os clientes BitTorrent e VoIP, além dos aplicativos de mensagens, estão constantemente mudando seu comportamento e assinatura para se evadir da detecção e controle. Muitos deles agora usam a criptografia para escapar da detecção, enquanto outros simplesmente se reclassificaram para usar conexões no estilo navegador da web porque as portas 80 e 443 geralmente ficam desbloqueadas na maioria dos firewalls.

O resultado é uma total falta de visibilidade dos aplicativos na rede, e você não pode controlar o que não pode ver. A solução para isso é tão refinada quanto eficaz: o Controle de Aplicação Sincronizada da Sophos, que faz uso da nossa exclusiva conexão de Segurança Sincronizada com endpoints Sophos gerenciados.

É assim que funciona: quando o Sophos Firewall vê o tráfego de aplicativos que não consegue identificar com assinaturas, ele indaga ao endpoint qual aplicativo está gerando o tráfego.



Aplicativos desconhecidos que foram descobertos pelo Controle Sincronizado de Aplicativos podem ser categorizados automática ou manualmente.

Dessa forma, o endpoint pode compartilhar o arquivo executável, o caminho e, geralmente, sua categoria, e passar essas informações de volta para o firewall. O firewall se utiliza dessas informações para classificar e controlar o aplicativo automaticamente na maioria das situações.

Se o Sophos Firewall não puder determinar a categoria apropriada do aplicativo automaticamente, o administrador pode definir a categoria desejada ou atribuir o aplicativo a uma política existente.

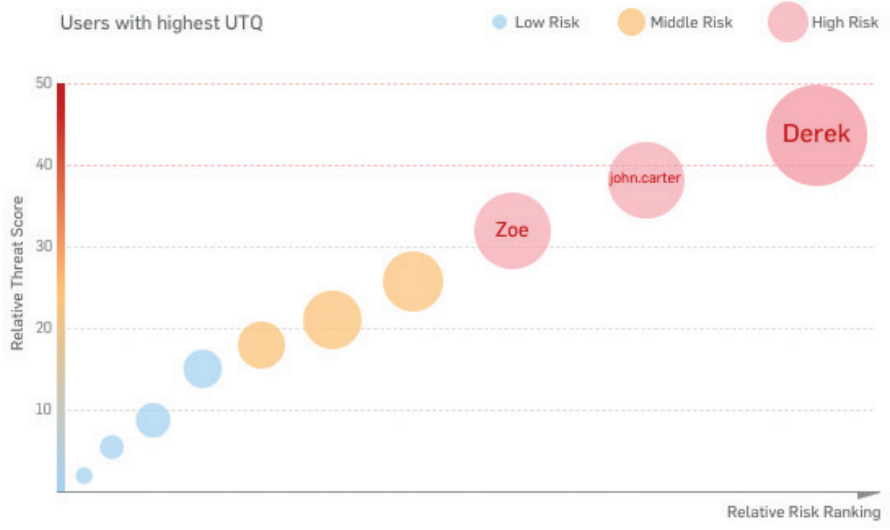
Uma vez que seja classificado – automaticamente ou pelo administrador da rede –, o aplicativo fica sujeito aos controles da mesma política que os outros aplicativos naquela categoria, o que permite bloquear facilmente os aplicativos indesejáveis e priorizar os necessários.

O Controle de Aplicação Sincronizada representa um avanço na visibilidade e controle de aplicativos, oferecendo absoluta clareza de cada aplicativo em uso na rede, inclusive aqueles que, anteriormente, ficaram sem identificação e controle.

Usuários de mais alto risco

Estudos comprovam que os usuários são o elo mais vulnerável na cadeia de segurança. Mas a boa notícia é que os padrões do comportamento humano podem ser usados para prever e prevenir ataques. Além disso, os padrões de uso podem ajudar a ilustrar a eficiência com a qual os recursos corporativos são usados e se as políticas de usuário precisam ser mais bem ajustadas.

O Quociente de Ameaça de Usuários (QAU) da Sophos ajuda os administradores de segurança a identificar os usuários que representam riscos, com base em comportamentos suspeitos na Web e no histórico de ameaças e infecções. Uma alta pontuação de risco QAU de um usuário pode indicar ações não intencionais devidas a uma falta de percepção de segurança, uma infecção por malware ou ações ilegítimas intencionais.

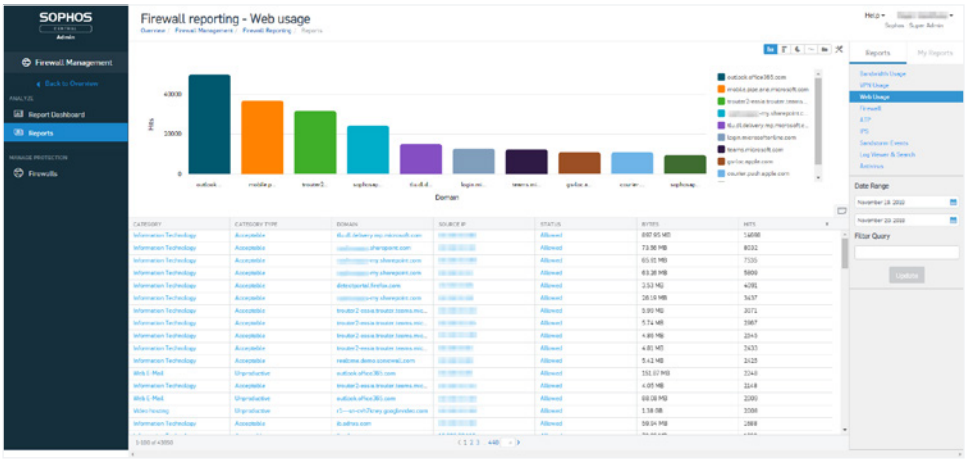


O Sophos Firewall identifica rapidamente os usuários de mais alto risco.

Saber quem é o usuário e as atividades que causaram o risco ajuda os administradores de segurança da rede a adotar as ações necessárias e a educar os usuários de alto risco ou impor políticas mais estritas ou mais adequadas para manter o controle do comportamento do usuário.

Opções flexíveis de relatórios

O Sophos Firewall é único entre os produtos NGFW e UTM, oferecendo opções flexíveis de relatórios na nuvem e integradas com um alto grau de detalhamento sem custos adicionais. O Sophos Central Firewall Reporting (CFR) permite que as organizações tenham um insight mais aprofundado da atividade da rede através de dados analíticos. Com abrangentes relatórios integrados e ferramentas para criar centenas de variações, o CFR oferece inteligência aplicável sobre comportamento de usuário, uso de aplicativo, eventos de segurança e mais. Relatórios interativos e painéis de visualização rápida permitem que os administradores analisem detalhadamente os dados de syslog armazenados na sua conta do Sophos Central para obter uma vista granular que é apresentada em um formato visual de fácil entendimento. Os dados podem ser analisados quanto a tendências que poderiam identificar lacunas na postura de segurança e destacar a necessidade de possíveis mudanças em políticas.



O Sophos Firewall fornece opções de relatórios completos já integrados e de relatórios baseados na nuvem.

O Sophos Firewall também oferece relatórios integrados. Escolha entre um conjunto abrangente de relatórios, convenientemente organizados por tipo, com vários painéis de controle embutidos. Existem centenas de relatórios com parâmetros personalizáveis em todas as áreas do firewall, inclusive atividade de tráfego, segurança, usuários, aplicativos, web, redes, ameaças, VPN, e-mail e conformidade. É possível facilmente agendar o envio por e-mail de relatórios periódicos para você ou seus destinatários designados, além de salvar relatórios em formato HTML, PDF ou CSV.

Bloquear ameaças desconhecidas

A proteção contra as mais modernas ameaças a redes requer uma sinfonia de tecnologias, todas trabalhando juntas e orquestradas por um grande maestro: o administrador da rede. Infelizmente, a maioria dos firewalls opera como um espetáculo independente: regras de firewall definidas em uma área, políticas da web em outra, inspeções TLS/SSL em outra ainda, e o controle de aplicativos em um local totalmente à parte do produto.

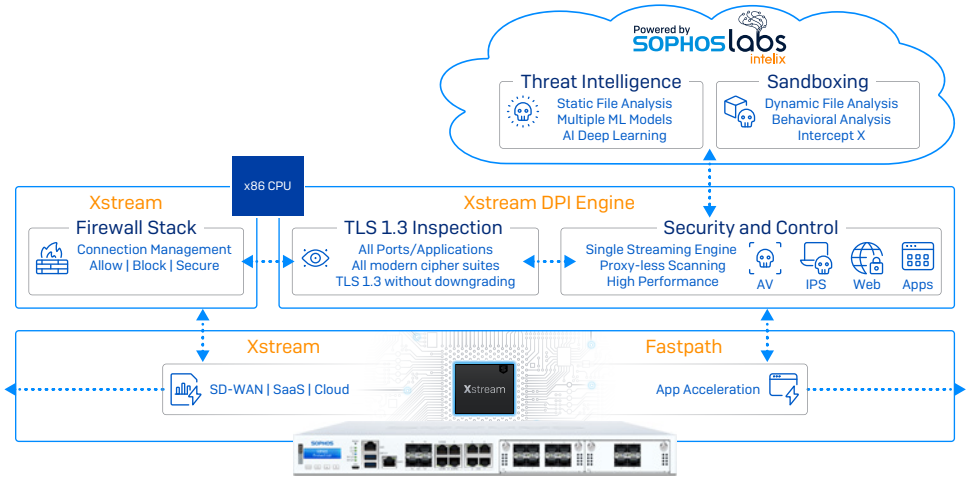
Na Sophos, não apenas acreditamos que você precisa da mais avançada tecnologia de proteção disponível, mas também entendemos a sua necessidade por simplicidade de configuração, implantação e gerenciamento diário – porque uma proteção configurada incorretamente pode ser pior do que nenhuma proteção.

O compromisso com a simplicidade sempre foi parte fundamental do DNA da Sophos. Porém, o mais importante, talvez, é que a Sophos possui uma rara disposição a adotar mudanças e fazer o que é preciso de forma diferente, com o intuito de oferecer uma melhor proteção e uma experiência suprema ao usuário.

O modo diferente de trabalhar do Sophos Firewall é que faz a grande diferença.

Proteção e desempenho Xstream

O desempenho do firewall nunca deveria ficar comprometido quando você aplica a segurança necessária para proteger a sua rede contra ameaças. Um dos componentes básicos da arquitetura de processamento do pacote Xstream do Sophos Firewall é a alta velocidade do mecanismo de Inspeção Profunda de Pacotes (DPI). O mecanismo DPI oferece varredura de segurança de passagem única sem proxy para IPS, Web, AV e Controle de aplicativo, além da nossa inspeção SSL Xstream.



A Arquitetura Xstream do Sophos Firewall com Xstream Flow Processors programáveis oferece poderosa proteção e desempenho.

Quando uma nova conexão é estabelecida, ela é processada pela pilha do firewall, que toma as decisões sobre permissão, bloqueio ou varredura do tráfego em busca de ameaças. Se o tráfego exigir varredura de segurança, ele encaminha os pacotes para o mecanismo DPI de fluxo de alto desempenho sem proxy que faz a varredura dos pacotes, mesmo se estiverem criptografados. Isso é usado apenas para os primeiros pacotes. Depois, a pilha de firewall sai do caminho e descarrega o processamento totalmente para o mecanismo DPI. Isso aumenta significativamente a latência e o desempenho.

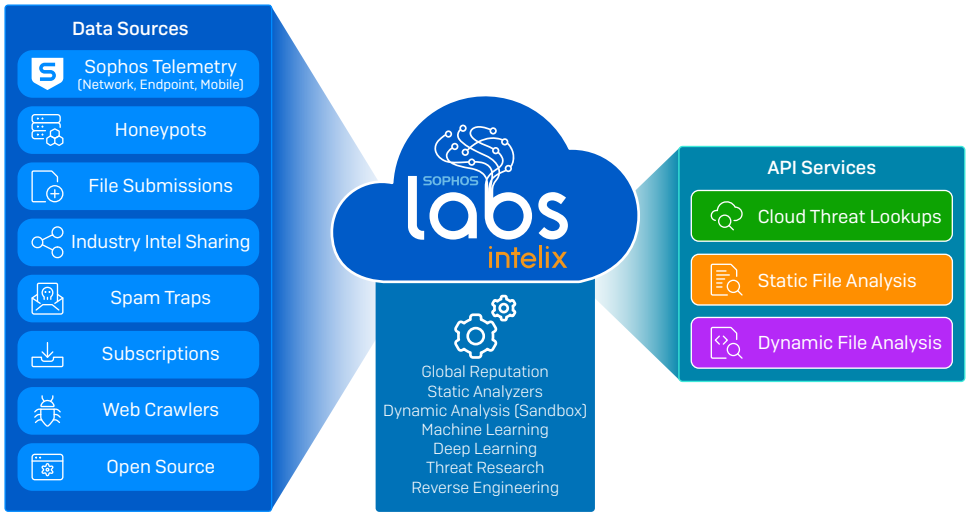
Depois, se o fluxo for considerado seguro e não mais exigir inspeção, o mecanismo DPI poderá descarregar o fluxo totalmente para o Sophos Network Flow FastPath, que oferece um caminho acelerado para o tráfego confiável. Isso aumenta drasticamente o desempenho ao liberar outros recursos da inspeção de tráfego que não a necessitam.

Proteção contra ameaças de dia zero

Conforme as ameaças avançadas, tais como o ransomware, vão se tornando mais direcionadas e evasivas, há uma necessidade crítica de identificar e se proteger prognosticamente contra ameaças de dia zero. A solução máxima para isso vem em duas metades:

1. **Análise estática de Machine Learning** – Oferece análise e detecção previsível através de vários modelos de Machine Learning de rede neural artificial, combinadas com reputação global e varredura de arquivo aprofundada, tudo isso sem precisar executar o arquivo em tempo real.
2. **Análise dinâmica de Sandbox em tempo de execução** – Detona um malware em tempo real em um ambiente sandbox na nuvem oferecendo insights inigualáveis da atividade do arquivo para revelar a verdadeira natureza e capacidade de uma ameaça desconhecida.

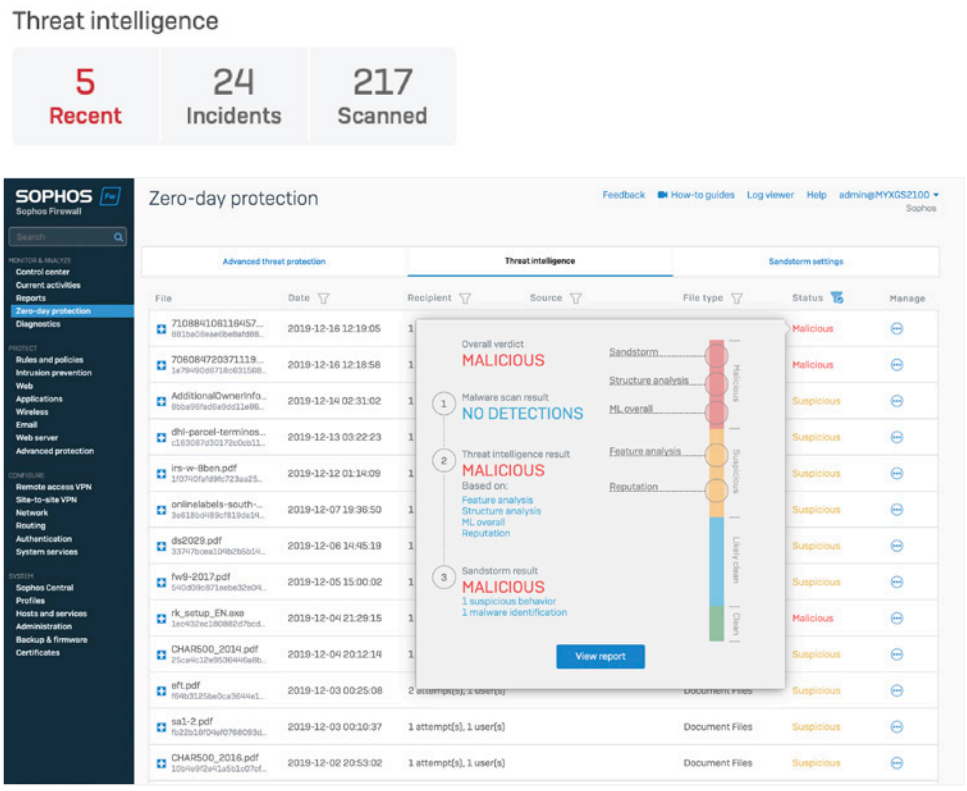
O Sophos Firewall inclui essas duas importantes tecnologias de proteção, alimentadas pelo SophosLabs Intelix. O SophosLabs, o nosso aclamado laboratório de pesquisa de ameaças em segurança cibernética de nível 1, desenvolveu a mais rica plataforma de inteligência e análise no SophosLabs Intelix. Utilizando a mais moderna tecnologia de Machine Learning, décadas de pesquisas em ameaças e petabytes de inteligência, oferece proteção inigualável contra ameaças nunca antes vistas.



A proteção de dia zero do Sophos Firewall é alimentada pelas análises de Machine Learning fornecidas pelo SophosLabs Intelix.

Quando o mecanismo DPI Xstream do Sophos Firewall realiza uma análise AV em um arquivo que entra na rede e determina que há um código ativo, ele retém o arquivo temporariamente e o envia para o serviço do SophosLabs Intelix na nuvem para as análises estática e dinâmica do arquivo. Ele cria um resumo dos resultados na Central de Controle do Sophos Firewall através do widget de Inteligência de Ameaças e este relatório de cliques (abaixo), e só libera o arquivo para o downloader ou para o destinatário do e-mail se o arquivo estiver limpo.

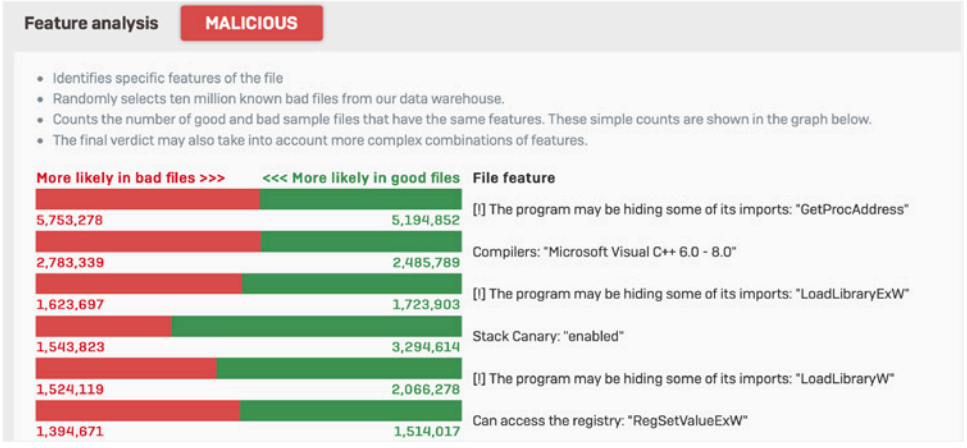
Esse último passo é importante, pois muitas soluções avançadas de malware de firewall frequentemente liberam o arquivo para o usuário final antes que a análise seja concluída, o que possivelmente resultará em uma limpeza confusa e dispendiosa se o arquivo foi rotulado como uma ameaça.



A proteção de dia zero do Sophos Firewall identifica ameaças novas nunca vistas em ação antes que causem danos à sua rede.

Análise estática de Machine Learning

A análise estática do arquivo utiliza vários modelos de machine learning para analisar as diferentes características, recursos, genética e elementos de reputação do arquivo, comparando-o com os milhões de arquivos sabidamente de boa e má reputação encontrados no banco de dados do SophosLabs para ditar um veredito em segundos sobre um arquivo novo e totalmente inédito. Identifica com rapidez e eficiência marcantes as novas ameaças e suas variantes, particularmente as ameaças que não são postas no sandbox com muita facilidade, como documentos protegidos por senha que carregam um malware.



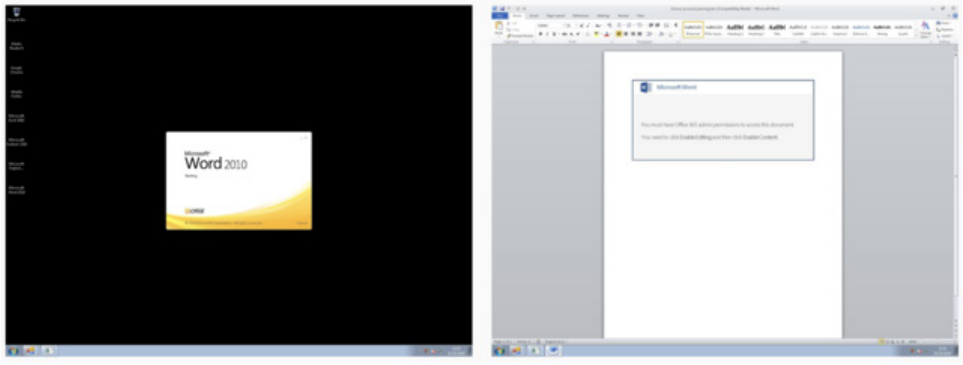
Diferentes modelos de Machine Learning são usados para analisar arquivos suspeitos em busca de ameaças de dia zero.

Análise dinâmica de sandbox em tempo de execução

Quando a tecnologia de sandbox surgiu, o conceito de área restrita era acessível apenas às grandes empresas. Só que agora, graças às soluções de sandbox em nuvem, tais como o Sophos Sandstorm, essa tecnologia ficou incrivelmente acessível até mesmo para as empresas menores. Pela primeira vez, as organizações de pequeno e médio porte têm acesso ao sandbox com a tecnologia Deep Learning que vai bem além da capacidade das soluções de sandbox dedicadas instaladas no local que as empresas implantavam por milhões de dólares, não muito tempo atrás.

Por estar na nuvem, não requer software ou hardware adicional e não causa impacto no desempenho do firewall. Qualquer arquivo que o mecanismo DPI Xstream determine conter código ativo, como um anexo de e-mail ou um download da web, é automaticamente carregado e detonado no sandbox do SophosLabs Intelix na nuvem em paralelo com uma análise estática (acima) para determinar o seu comportamento em tempo de execução antes de conseguir permissão para entrar na sua rede.

Para identificar ameaças, o SophosLabs integrou as mais recentes tecnologias de proteção do nosso produto de endpoint, também líder do setor, Intercept X Next-Gen, ao Sophos Sandstorm, incluindo Deep Learning, detecção de exploit e CryptoGuard (para deter arquivos criptografados por um ransomware ativo em tempo real). Ele também monitora toda a atividade do arquivo, memória, registro e rede em busca de características de alguma intenção maliciosa para dar o seu veredito. Nenhum outro firewall oferece esse tipo de análise em tempo de execução com a melhor proteção contra ameaças do mundo: Intercept X. E nenhum outro firewall oferece o nível de insights e relatórios que o Sophos Firewall proporciona, incluindo um conjunto completo de capturas de tela que exibe o que o arquivo divulgava enquanto era executado.

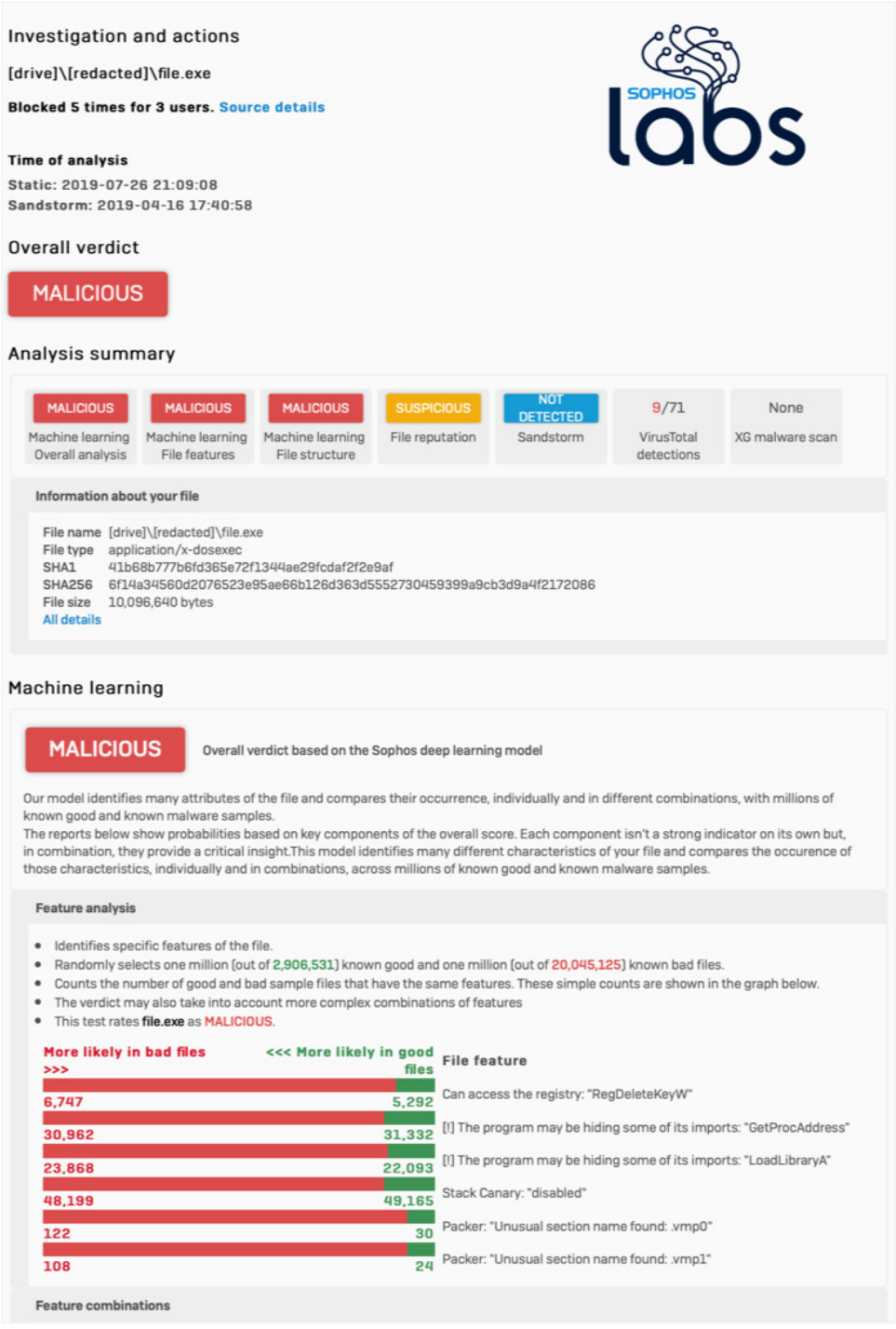


A análise em tempo de execução de sandbox detona os arquivos em um ambiente seguro, para determinar seu comportamento, e prepara capturas de tela para você poder rever a ação.

O sandbox é particularmente eficiente na detecção de ameaças que se entremeiam em arquivos normalmente benignos que talvez não tenham nenhuma característica maliciosa óbvia. Arquivos do Office com macros, ou executáveis benignos ou atualizações de aplicativos que foram minados.

Relatório do Threat Protection

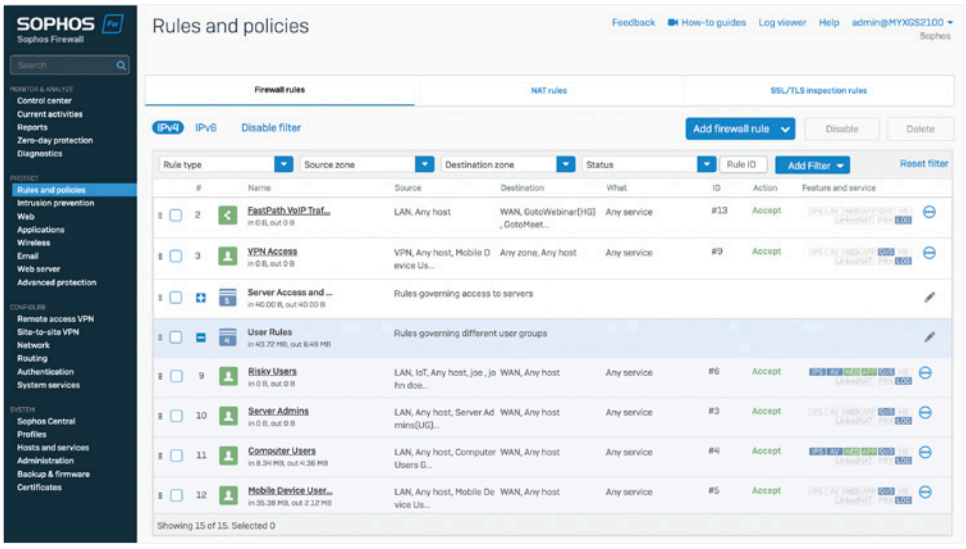
Cada arquivo que é analisado pelo Sophos Firewall apresenta um relatório que oferece detalhes completos sobre os resultados das várias análises e vereditos. Existem seis elementos diferentes no relatório, incluindo as várias análises de Machine Learning, reputação de arquivo, sandbox, além dos dados terceirizados do VirusTotal.



Gerenciamento unificado de regras

O gerenciamento de um firewall pode ser imensamente desafiador. Com a infinidade de regras, políticas e configurações de segurança distribuídas em várias áreas funcionais – e frequentemente sendo preciso várias regras diferentes para oferecer a proteção necessária –, ainda há muito o que fazer.

Com o Sophos Firewall, aproveitamos a oportunidade para repensar completamente a forma como as regras de firewall são organizadas e como a sua postura de segurança é gerenciada. Em vez de ter que ficar procurando no painel de gerenciamento pelas políticas certas, reunimos o gerenciamento de todas as regras de firewall e imposições em uma única tela, de forma unificada. Agora é possível visualizar, filtrar, pesquisar, editar, adicionar, modificar e organizar todas as suas regras de firewall em um único lugar.



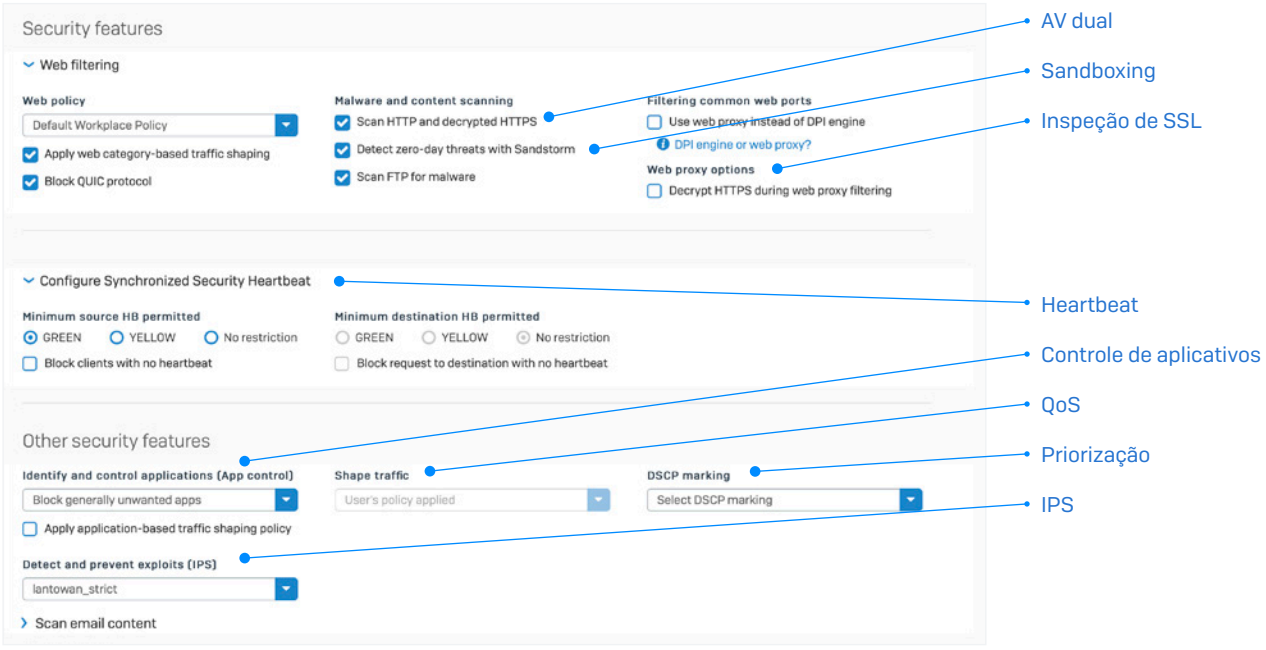
O Sophos Firewall coloca todas as suas regras de política de acesso, NAT e inspeção TLS juntas em um mesmo lugar para facilitar o gerenciamento.

As regras para usuários, aplicativos de negócios, NAT, inspeção TLS/SSL e redes facilitam visualizar apenas as políticas de que você precisa, proporcionando, ao mesmo tempo, uma tela conveniente para o gerenciamento.

Ícones indicadores proporcionam informações importantes sobre políticas, tais como, seu tipo, status, imposição e outras mais.

Vista rápida para o gerenciando da sua postura de segurança

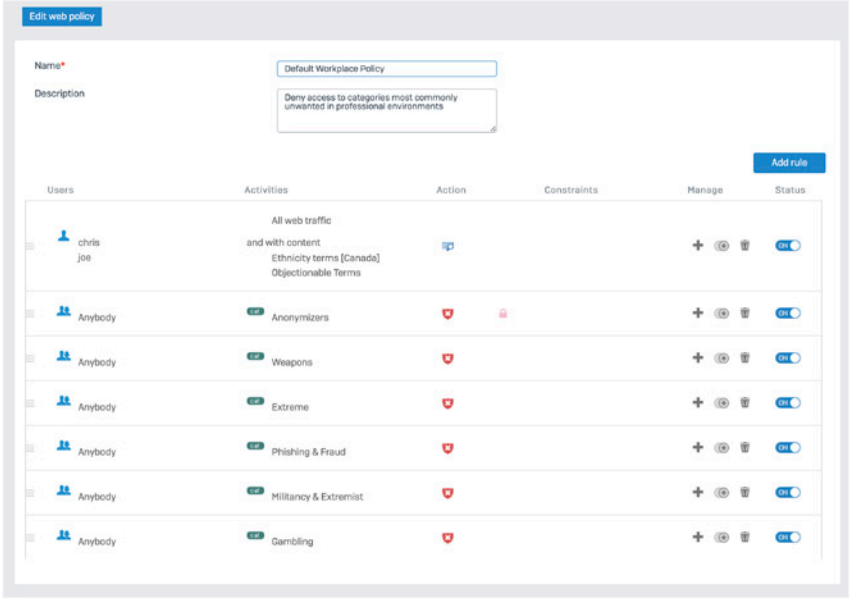
Seja usando a sua conta do Sophos Central na nuvem ou a interface de usuário do Sophos Firewall, a Sophos torna incrivelmente fácil configurar e gerenciar tudo o que é preciso para uma proteção moderna – e tudo em uma única tela.



Configure sua postura completa de segurança em uma única tela usando políticas personalizadas ou predefinidas.

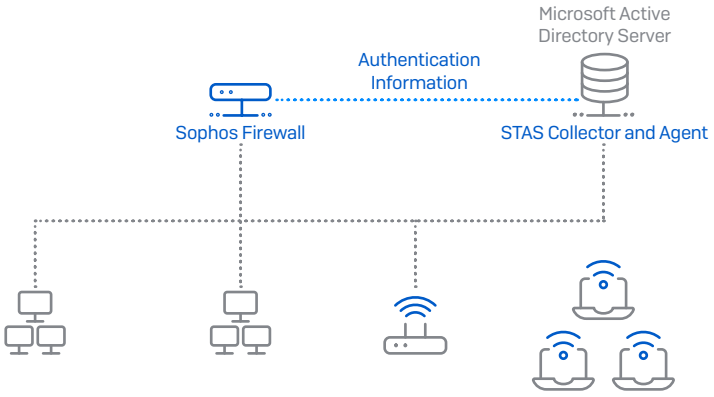
Você configura e monitora a segurança e o controle de antivírus, inspeção TLS, sandbox, IPS, modelagem de tráfego, controle da Web e de aplicativos, Security Heartbeat, NAT, roteamento e priorização em um mesmo lugar — tudo baseado em um modelo regra por regra, usuário por usuário ou grupo por grupo.

Se quiser ver exatamente o que uma de suas políticas está fazendo, ou mesmo fazer alterações nela, você pode editá-la sem precisar sair da regra de firewall e visitar outra parte do produto.



Veja detalhes da política instantaneamente e faça alterações sem sair da tela de regras do firewall.

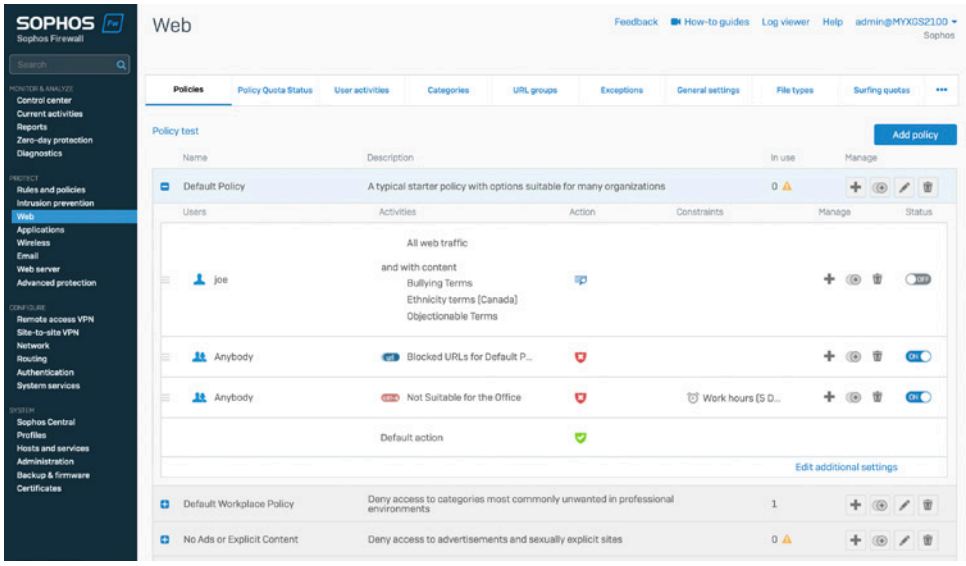
As opções de autenticação flexíveis permitem saber facilmente quem é quem, incluindo serviços de diretório, tais como o Active Directory, eDirectory e LDAP, bem como o NTLM, Kerberos, RADIUS, TACACS+, RSA, agentes de clientes ou um portal cativo. Além disso, o Sophos Transparent Authentication Suite (STAS) oferece integração com serviços de diretório, tais como o Microsoft Active Directory, para uma autenticação transparente de logon único fácil e confiável.



No client required on devices for SSO

Gateway de nível corporativo seguro à Web

A proteção e o controle da Web são itens básicos de qualquer firewall, mas, infelizmente, parece ser algo pensado apenas após as implementações de firewall. Nossa experiência com o desenvolvimento de soluções em proteção da Web de nível corporativo nos proporcionou a base e o conhecimento para implementar o tipo de controle de políticas da Web que você só encontraria em soluções corporativas de gateway seguro da web (SWG), que custam dez vezes mais. Implementamos um modelo de política de herança de cima para baixo que torna a criação de políticas sofisticadas uma tarefa fácil e intuitiva. Modelos predefinidos de políticas prontos para usar são incluídos nas implantações mais comuns, tais como ambientes de trabalho típicos, conformidade educacional da lei CIPA norte-americana e outros mais. Isso significa que você terá ao seu alcance fáceis opções de ajuste e personalização.



Poderosas políticas da Web de nível empresarial oferecem controles granulares.

Na verdade, sabemos que a política de Web é um dos elementos alterados diariamente (ou com maior frequência) em seu firewall e, por isso, investimos pesado para ajudar você a conseguir gerenciar e ajustar políticas com facilidade, de acordo com as necessidades de seus usuários e de sua empresa. É possível personalizar facilmente usuários e grupos, atividades (compreendidas por URLs, filtros de conteúdo, categorias e tipos de arquivos) e ações (bloquear, permitir ou alertar), além de adicionar ou ajustar restrições com base em horário e dia da semana.

Recursos de educação

O Sophos Firewall oferece vários recursos adaptados e otimizados para ambientes educacionais em que a conformidade e política da web são requisitos essenciais. Recursos específicos à educação incluem:

- Políticas da web predefinidas para atender à conformidade LPII educacional
- Filtros e relatórios de palavras-chave no conteúdo
- Configurações de Restrição do SafeSearch e YouTube com base em uma política de usuário/grupo
- Substituições de página de bloqueio podem ser gerenciadas por professores
- Relatório integrado abrangente para identificar problemas potenciais de antemão

As políticas agora incluem a opção de registrar, monitorar ou mesmo impor políticas pertinentes a conteúdo dinâmico baseado em listas de palavras-chave. Esse recurso é especialmente importante nos ambientes de ensino para garantir a segurança de crianças e adolescentes no ambiente online e oferecer insigths dos estudantes usando palavras-chave concernentes a autoflagelo, bullying ou extremismo, por exemplo. Bibliotecas de palavras-chave podem ser carregadas para o firewall e aplicadas a qualquer política de filtragem da web como critérios adicionais com ações para registrar, monitorar ou bloquear os resultados da pesquisa contendo palavras-chave de interesse.

Relatórios abrangentes são fornecidos para identificar correspondências entre palavras-chave e usuários que estão pesquisando ou consumindo conteúdo com tais palavras-chaves de interesse, permitindo a intervenção proativa antes que um usuário em risco se transforme em um problema real.

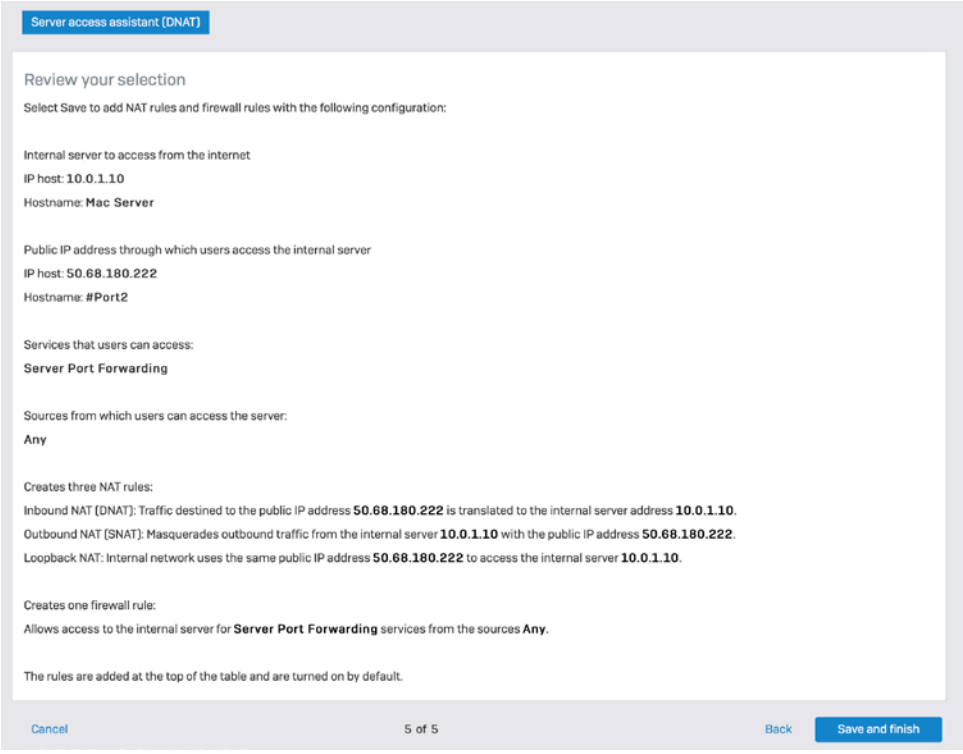
O Sophos Firewall ajuda com a conformidade da política de lei CIPA norte-americana, permitindo o seu rápido cumprimento. Também oferece controles flexíveis e poderosos das restrições do SafeSearch e do YouTube com base em uma política de usuário/grupo. Os professores podem ter a opção de configurar e gerenciar suas próprias substituições de políticas para permitir a seus alunos o acesso a websites que, do contrário, estariam bloqueados como parte do currículo disciplinar.

É a poderosa política de Web simplificada.

Configuração NAT simplificada

Qualquer pessoa que já tentou configurar as regras NAT de conversão de endereços de rede sabe como isso pode ser difícil. Mas não precisa ser assim. O Sophos Firewall inclui as funcionalidades NAT Enterprise completas para permitir configurações NAT poderosas e flexíveis, incluindo Source NAT (SNAT) e Destination NAT (DNAT) em uma única regra com critérios granulares de seleção. Para simplificar a complexidade de DNAT, um assistente fácil de usar o leva pelo processo de criação de uma configuração NAT completa com alguns poucos cliques.

Os administradores também podem se aproveitar da praticidade da opção NAT vinculada ao criar uma regra de firewall. A NAT vinculada automaticamente criará uma regra de configuração NAT correspondente, reduzindo ainda mais o tempo gasto com a criação e configuração de regras NAT.

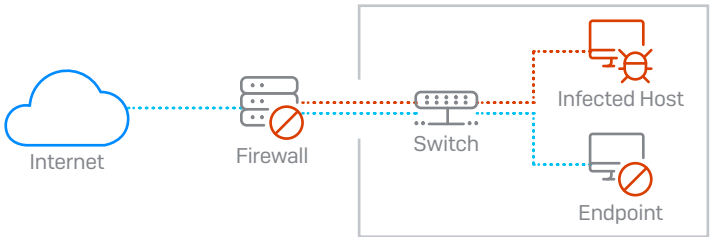


Aproveite as vantagens do poderoso e intuitivo assistente de regra de NAT para criar controles de acesso complexos com apenas alguns cliques.

Responde automática a incidentes

Um dos recursos de firewall mais requisitados aos administradores de redes é a capacidade de responder automaticamente aos incidentes de segurança na rede.

O Sophos Firewall é a única solução de segurança de rede que identifica totalmente a origem de uma infecção na sua rede e automaticamente limita, como resposta, o acesso do dispositivo infectado a outros recursos da rede. Isso é possível graças ao nosso exclusivo Sophos Security Heartbeat que compartilha informações de telemetria e do estado de integridade entre os endpoints gerenciados pela Sophos e o seu firewall.



O Sophos Firewall e o Security Heartbeat podem isolar automaticamente os hosts infectados na sua rede.

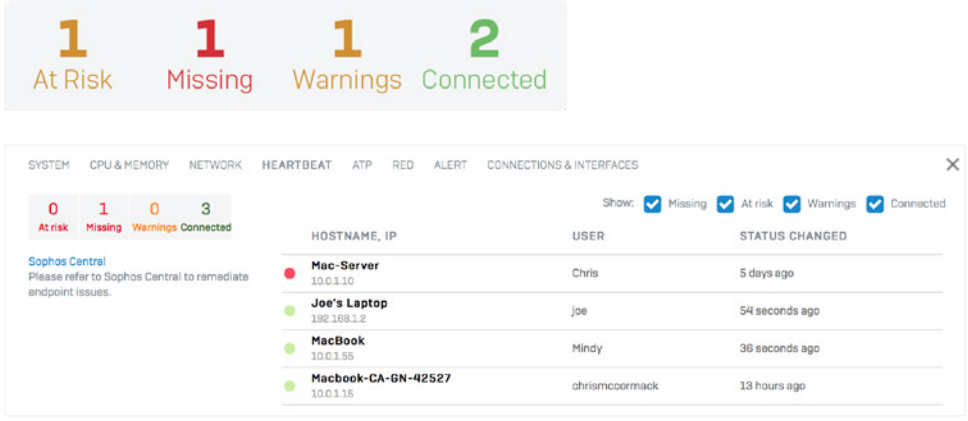
O Sophos Firewall integra exclusivamente os hosts conectados em suas regras de firewall, permitindo automaticamente limitar o seu acesso a recursos de rede sensíveis por parte de qualquer sistema comprometido, até que esteja descontaminado.

O Sophos Firewall pode não apenas isolar endpoints para evitar o acesso a outras partes da rede em um firewall, mas também pode requisitar o auxílio de todos os endpoints íntegros na rede para isolar um host comprometido no nível do endpoint.

Essa Proteção Contra Acesso mais Profundo à Rede, que é como a chamamos, isola e evita que ameaças ou invasores se movam para outros sistemas pela rede, mesmo que estejam no mesmo segmento de rede ou domínio de transmissão onde o firewall normalmente não pode intervir. Esta é uma solução extremamente simples e eficiente para combater os adversários ativos que operam na sua rede. Mas isso só é possível se o seu endpoint e firewall estiverem trabalhando juntos em uma defesa coordenada ou sincronizada.

Security Heartbeat

O Security Heartbeat da Sophos compartilha inteligência em tempo real, utilizando um link seguro entre os seus endpoints gerenciados pela Sophos e o Sophos Firewall. Esta etapa simples de sincronização de produtos de segurança, que antes eram operados de forma independente, cria uma proteção mais eficaz contra malware avançado e ataques direcionados.



O status do Security Heartbeat™ para a sua rede fica visível na central de controle.

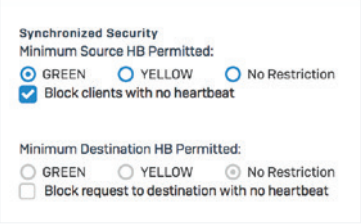
O Security Heartbeat não somente identifica a presença de ameaças avançadas instantaneamente como também pode ser usado para comunicar informações importantes sobre a natureza da ameaça, o sistema de hospedagem e o usuário. E, talvez o mais importante, o Security Heartbeat também pode agir automaticamente e isolar ou limitar o acesso a sistemas comprometidos até que estejam livres de malwares. Trata-se de uma fantástica tecnologia que revolucionou a forma de as soluções em segurança de TI identificarem e responderem às ameaças avançadas.

O Security Heartbeat para endpoints gerenciados por trás de seu firewall pode se encontrar em um dos três modelos seguintes:

O status **Sinal de Integridade Verde** indica que o dispositivo endpoint está íntegro e tem permissão de acessar todos os recursos de rede apropriados.

O status **Sinal de Integridade Amarelo** é um alerta de que um dispositivo pode ter um aplicativo potencialmente indesejado (PUA), estar descumprindo uma conformidade ou apresentar outro problema. É possível escolher a quais recursos de rede um sinal de integridade amarelo pode ter acesso até que o problema seja resolvido.

O status **Sinal de Integridade Vermelho** indica um dispositivo que está sob o risco de ser infectado por uma ameaça avançada e pode estar tentando fazer o call home conectando-se a um botnet ou servidor de comando e controle. Ao utilizar as configurações da política do Security Heartbeat em seu firewall, é possível isolar facilmente os sistemas com status de sinal de integridade vermelho até que possam ser limpos, a fim de reduzir o risco de perda de dados ou impedir que a infecção se propague.



Defina os requisitos do Security Heartbeat como parte de suas regras de firewall.

Somente a Sophos pode oferecer uma solução como o Security Heartbeat, uma vez que a empresa é líder em soluções de segurança de endpoint e de rede. Ainda que outros fornecedores estejam se conscientizando de que esse é o futuro da segurança de TI, eles apresentam uma desvantagem óbvia: não possuem uma solução de endpoint líder do setor e uma solução de firewall líder do setor que foram criadas pensando em integração.

O mundo é Zero Trust

O conceito de "confiável" se tornou algo perigoso em termos de tecnologia de informação, especialmente quando confiança deveria ser algo implícito. Criar um perímetro corporativo amplo e vedado e confiar em tudo o que adentra suas divisas demonstrou ser algo não tão confiável.

Zero Trust é uma abordagem holística de segurança que trata desses desafios e de como as organizações trabalham e respondem às ameaças. Uma filosofia e um modelo de como pensar sobre a segurança e colocá-la em prática.

Nada nem ninguém deve ser classificado como confiável à primeira vista, seja dentro ou fora da sua rede corporativa. Mas, no fim, precisamos confiar em algo. Com o Zero Trust, a confiança é temporária e é estabelecida a partir de múltiplas fontes de dados, sendo constantemente reavaliada.

O Zero Trust nos permite controlar toda a nossa instalação, partindo de dentro do escritório e percorrendo todas as plataformas da nuvem que usamos. Assim não há mais falta de controle fora do perímetro corporativo ou contendas com usuários remotos.

Como avançamos para o Zero Trust e aproveitamos todos os seus benefícios vantajosos? Ainda que ninguém possa oferecer o Zero Trust como uma solução singular, a Sophos tem um amplo portfólio de tecnologias e controles de segurança que aceleram e simplificam a sua jornada rumo à confiabilidade Zero Trust.

Sophos Central – A plataforma de segurança cibernética mais confiável do mundo coloca essas tecnologias díspares e complementares em um único painel de gerenciamento na nuvem para ajudá-lo a orquestrar e monitorar a sua rede Zero Trust.

Segurança Sincronizada – Segurança cibernética que continuamente compartilha informações entre endpoint, ZTNA, firewall e outros sistemas, promovendo insight e visibilidade entre eles.

Sophos ZTNA – Oferece uma solução Zero Trust Network Access verdadeiramente confiável para conectar usuários a aplicativos e dados com segurança.

Sophos Firewall Crie segmentos ou microperímetros sobre usuários, dispositivos, aplicativos, redes e mais.

Server Protection e Intercept X – Atribua um status de integridade a cada dispositivo de modo que na eventualidade de um deles ser comprometido, o dispositivo possa ser automaticamente isolado e bloqueado para que não estabeleça conexão com outros dispositivos.

Serviço MTR (Managed Threat Response) – Monitora toda a atividade do usuário em toda a rede e identifica as credenciais de usuário possivelmente comprometidas.

Otimizando a sua rede SD-WAN

Poucos termos sobre sistemas de rede geram tanta polêmica como SD-WAN (Software Defined Networking in a Wide Area Network). Toda essa polêmica é acompanhada, na mesma medida, por informações úteis e retórica confusa. Como resultado, o SD-WAN acabou tendo significados distintos para pessoas diferentes, enquanto alguns ainda tentam descobrir o que significa exatamente.

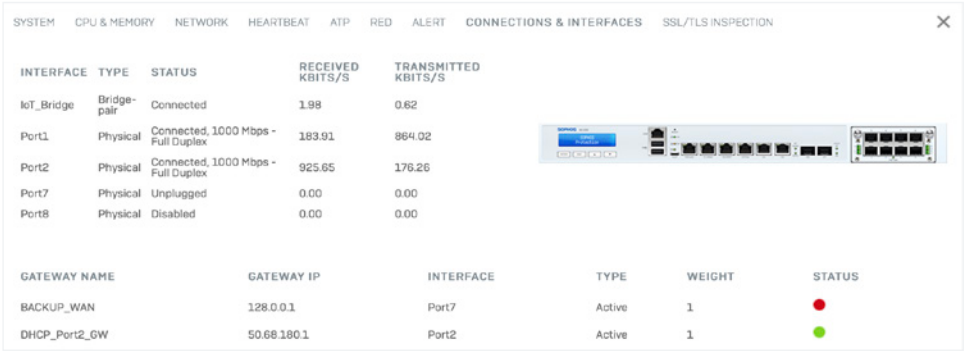
Fundamentalmente, SD-WAN se refere normalmente a como atingir um ou mais destes quatro objetivos de rede:

- **Reduza os custos de conectividade** – As conexões MPLS (Multi-Protocol Label Switching) tradicionais são caras, por isso as organizações estão mudando para opções de WAN de banda larga mais acessíveis, como cabo, DSL e 3G/4G/LTE
- **Continuidade dos negócios** – As organizações exigem soluções que forneçam redundância, roteamento, failover e preservação de sessão em caso de falha ou interrupção da WAN
- **Qualidade de aplicativos críticos** – As organizações buscam visibilidade em tempo real do tráfego e do desempenho dos aplicativos para manter a qualidade da sessão de aplicativos corporativos de missão crítica
- **Orquestração de VPN mais simples para filiais** – A orquestração de VPN entre locais costuma ser complexa e demorada, por isso é fundamental ter ferramentas que simplifiquem e automatizem a implantação e a configuração

Com o Sophos Firewall com Xstream SD-WAN você pode atingir as suas metas de SD-WAN mais audaciosas de modo simples e econômico com um conjunto que abrange orquestração, gerenciamento e desempenho de SD-WAN e opções de otimização confiáveis.

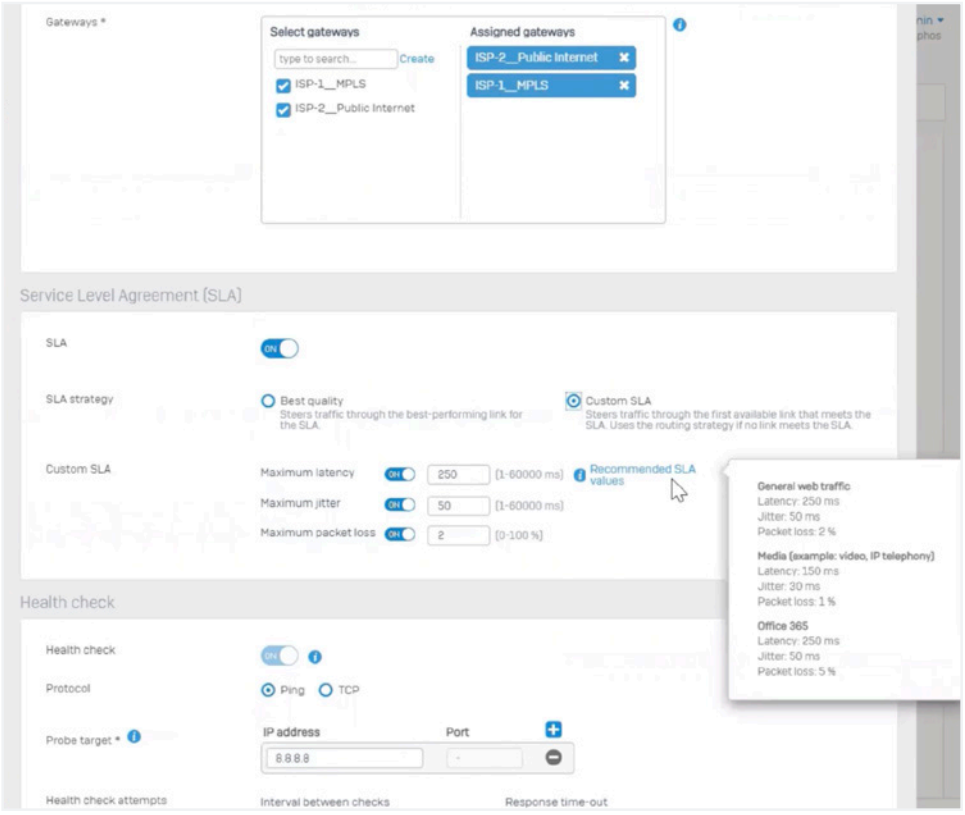
Xstream SD-WAN

Gerenciar a rota do tráfego do aplicativo através de muitos links de SD-WAN é um princípio básico da SD-WAN, e o Sophos Firewall com Xstream SD-WAN oferece uma solução de gerenciamento de links flexível e poderosa, seja usando múltiplas conexões MPLS, DSL, de cabo ou conexões celulares.



O status do Link WAN é mostrado na parte inferior deste widget de status da interface disponível no painel.

Os perfis SD-WAN definem uma estratégia de rota entre os vários gateways de link de WAN permitindo o redirecionamento eficiente das conexões do aplicativo com base no desempenho do link WAN.
As transições entre os links acontecem instantaneamente com zero de impacto nas sessões do aplicativo e nenhuma interrupção, proporcionando continuidade dos serviços, desempenho do aplicativo e a melhor experiência de usuário mesmo nos ambientes de ISP mais instáveis.



Criar perfis de SD-WAN é fácil e intuitivo.

As estratégias de roteamento de perfil SD-WAN podem se basear no primeiro critério de link disponível ou baseado no desempenho. O critério de monitoramento de desempenho inclui instabilidade, latência e perda de pacote, podendo utilizar vários destinos de sondagem para sondas de PING TCP.

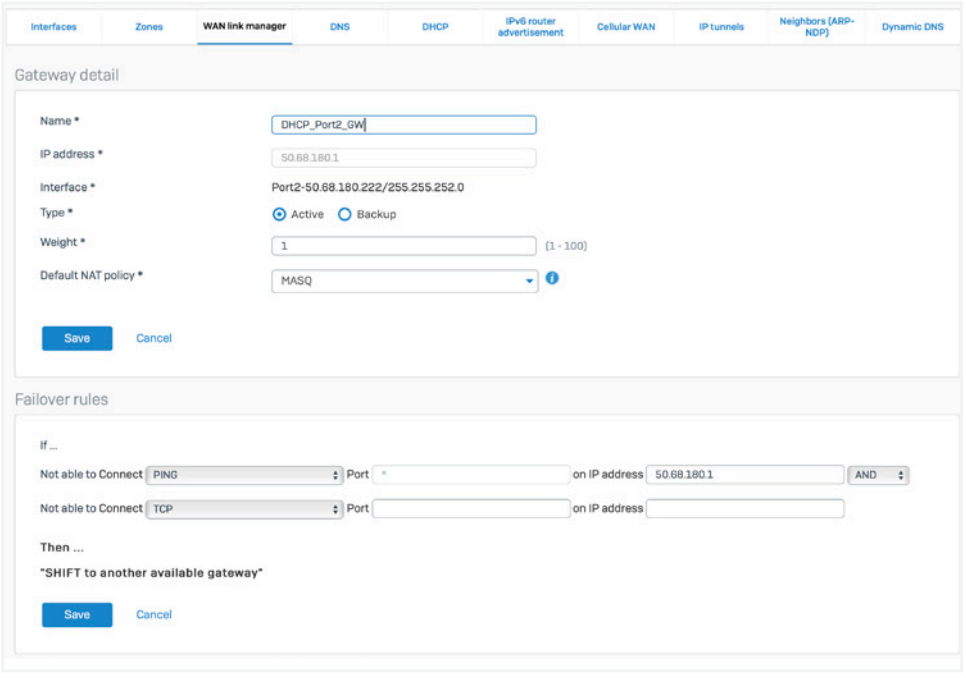
Os perfis de SD-WAN podem selecionar automaticamente o melhor link com base no desempenho ou de acordo com as suas políticas de SLA personalizadas que definem os valores específicos máximos para instabilidade, latência ou perda de pacote aceitáveis antes de redirecionar por um link de melhor desempenho com absolutamente zero de impacto a qualquer outra conexão.

O monitoramento do desempenho da sua rede SD-WAN é fácil com os gráficos com dados históricos e em tempo real de latência, instabilidade e perda de pacotes. As seleções cronológicas incluem tempo real, as últimas 24 ou 48 horas, ou a última semana ou mês corrido. O log avançado de roteamento e desempenho da SD-WAN também está incluído.

Monitore o desempenho dos seus vários links de WAN em tempo real.

Aceleração Xstream FastPath do tráfego de VPN da SD-WAN

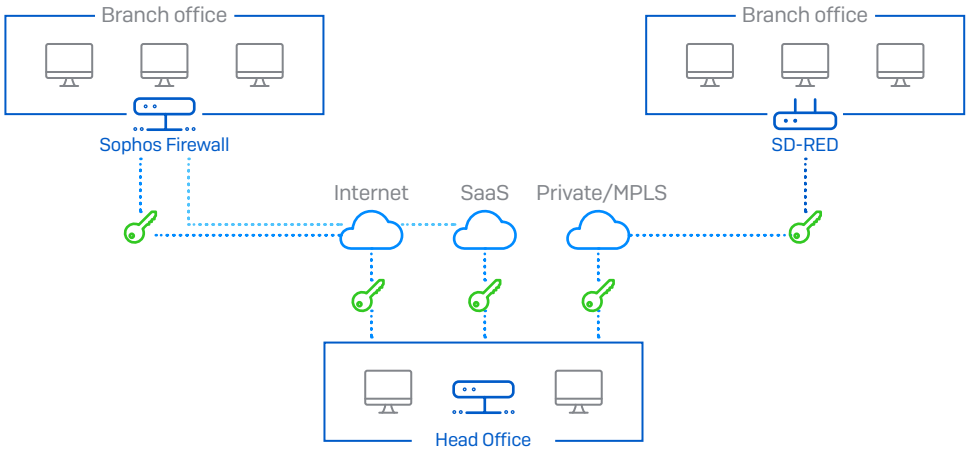
O Sophos Firewall utiliza os Xstream Flow Processors integrados nos dispositivos da Série XGS para oferecer aceleração de hardware do tráfego do túnel VPN de IPsec. Isso melhora o desempenho drasticamente, movendo parte do processamento com uso intenso da CPU pelos túneis de IPsec para o Xstream Flow Processor, como o encapsulamento/criptografia e desencapsulamento/descriptografia para ESP. Esse novo recurso aproveita ao máximo os recursos de criptografia de hardware no Xstream Flow Processor e oferece o benefício extra de liberar recursos de CPU para outras tarefas, como a inspeção profunda de pacote do tráfego que precisa dela. A aceleração Xstream FastPath para o tráfego de IPsec funciona para o tráfego de VPN site a site e de acesso remoto.



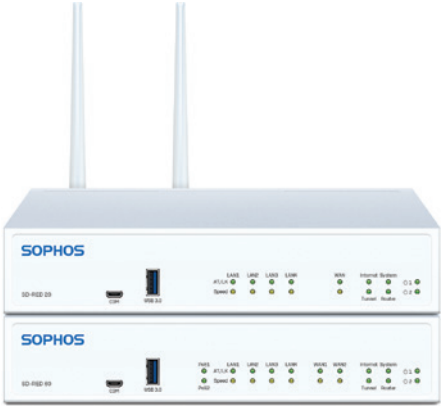
Gerenciamento de Link de WAN do Sophos Firewall, incluindo regras de failover e balanceamento.

Conectividade para filiais SD-Branch

A Sophos é pioneira na área de implantação e conectividade de filiais sem toque com nossos dispositivos SD-RED exclusivos. Esses dispositivos acessíveis são extremamente fáceis de serem implantados por uma pessoa não técnica e fornecem um túnel robusto e seguro de Layer-2 entre o dispositivo e um firewall central.

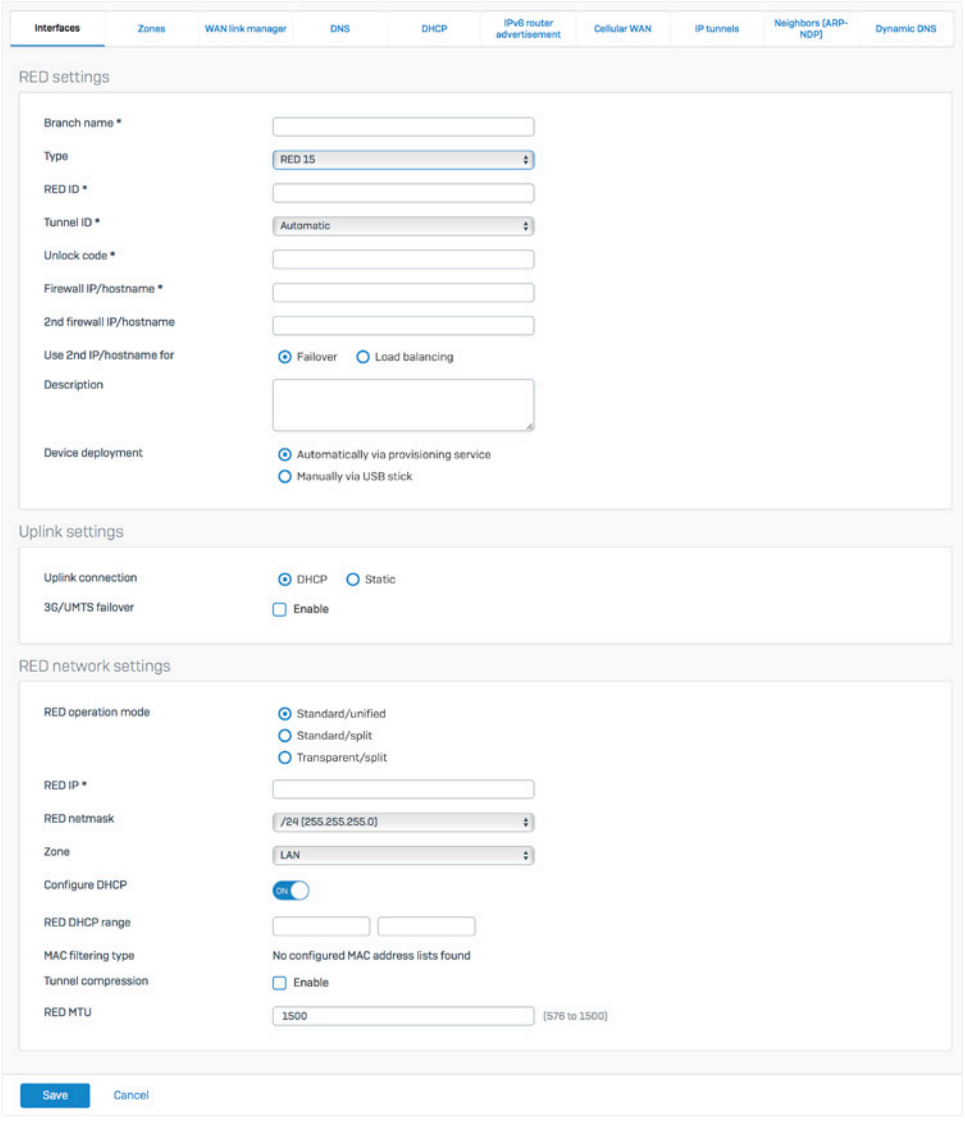


Os dispositivos Sophos Firewall e SD-RED oferecem opções de túnel para conectar filiais de maneira simples e econômica por meio do SD-WAN.



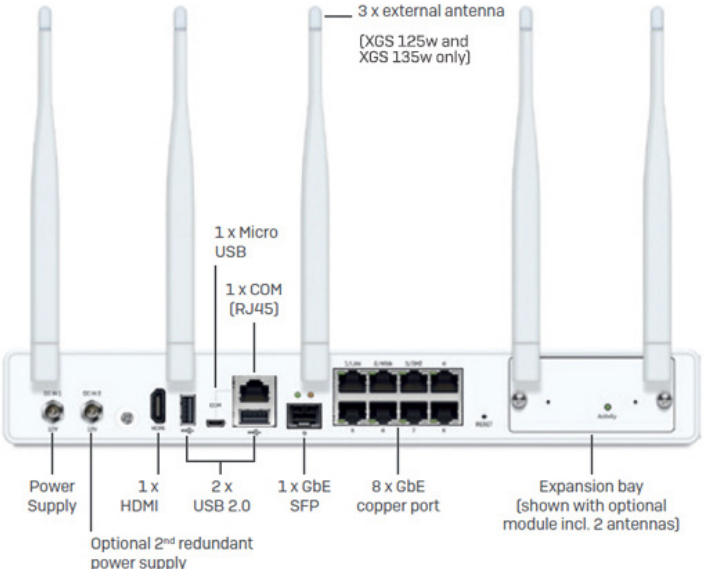
Os dispositivos Sophos SD-RED oferecem uma solução acessível e sem toque para conectividade de filial com SD-WAN.

A implantação de dispositivos SD-RED não poderia ser mais fácil: Basta incluir o número de série do dispositivo em seu firewall e enviar o dispositivo para o local remoto. Qualquer pessoa não técnica no local remoto simplesmente conecta o dispositivo e ele entrará em contato automaticamente com nosso serviço de provisionamento na nuvem para estabelecer uma conexão de túnel segura com o Firewall Sophos.



A Sophos SD-RED oferece uma solução de conectividade de filial SD-WAN flexível, segura e acessível.

Nossos dispositivos da Série XGS para desktop também são excelentes soluções de conectividade SD-WAN para filiais com opções de conectividade flexíveis, incluindo VDSL e celular, além de interfaces de cobre e fiber e suporte para nossos túneis SD-RED robustos.

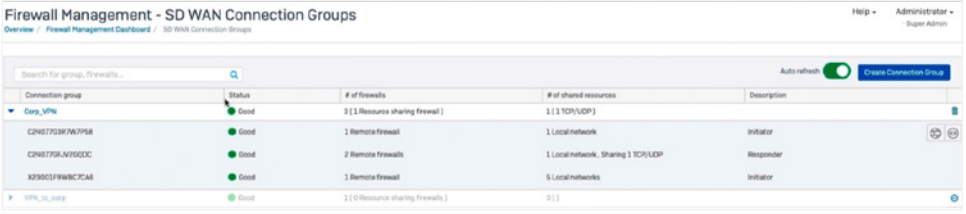


Alguns modelos para desktop, como o XGS 135w mostrado aqui, oferecem opções de conectividade LTE/celular, VDSL, cobre ou fiber WAN.

Suporte e orquestração de VPN

Se você já instalou mais do que um ou dois pares de túneis VPN entre diferentes firewalls, você sabe o quanto que esse processo consome do nosso tempo. O Sophos Firewalls suporta a orquestração SD-WAN no Sophos Central, o que faz da interconexão de vários túneis entre vários firewalls uma tarefa rápida e fácil.

Basta selecionar os firewalls sob o seu gerenciamento que você quer que participem dos grupos de conexão SD-WAN e selecionar os recursos de rede que deseja que cada site acesse. Com o simples girar de um botão, você vê a sua rede de sobreposição SD-WAN VPN entrar em ação, com todas as regras de acesso de firewall e túneis necessários, incluindo redundância, criados automaticamente.



Monte rapidamente as complexas redes de sobreposição de SD-WAN com alguns poucos cliques e monitore-as no Sophos Central.

Seja uma rede em malha completa, uma rede com topologia hub-and-spoke, ou similar, o Sophos Central cuidará automaticamente de todas as configurações necessárias de acesso a túneis e firewalls no backend para habilitar a sua rede de sobreposição SD-WAN.

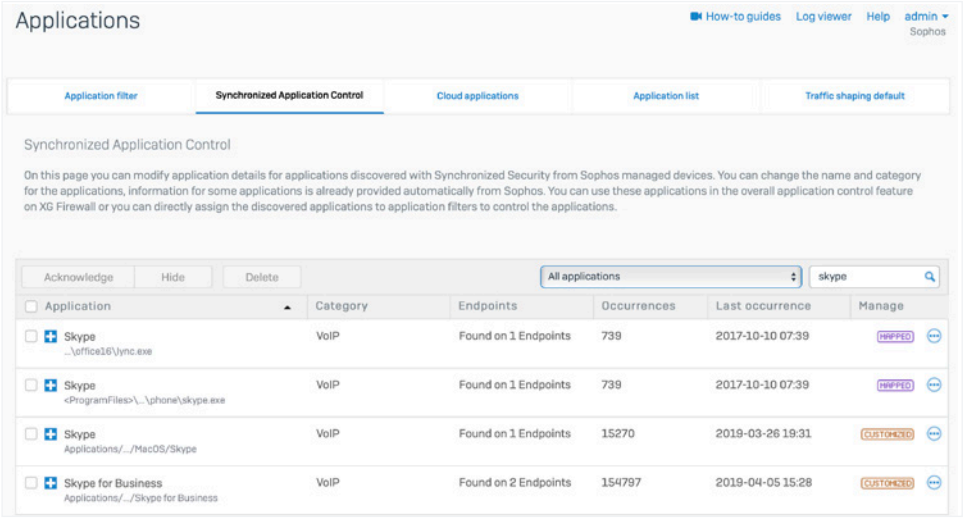
Logicamente, o Firewall Sophos aceita todas as opções VPN site a site padrão que você espera, incluindo IPsec e SSL. Oferecemos até mesmo nosso próprio túnel SD-RED de Layer-2 exclusivo com roteamento extremamente robusto e comprovadamente confiável em situações de alta latência, como em links de satélite.

Visibilidade e roteamento de aplicativos

Outro recurso importante para atingir os objetivos do SD-WAN é a seleção e o roteamento do caminho do aplicativo, que é usado para garantir a qualidade e minimizar a latência para aplicativos de missão crítica, como VoIP.

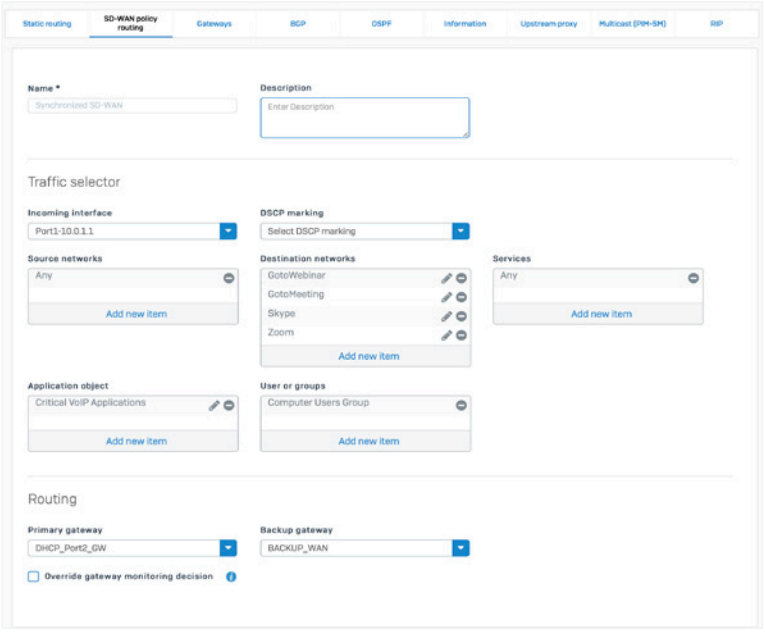
Claro, não é possível rotear o que não podemos identificar, portanto, a identificação e visibilidade precisas e confiáveis de aplicativos são essenciais. O Sophos Firewall e o Sophos Synchronized Security fornecem uma vantagem incrível nesses quesitos. O Controle Sincronizado de Aplicativos fornece 100% de clareza e visibilidade em relação a todos os aplicativos em rede, proporcionando uma vantagem significativa na identificação de aplicativos de missão crítica, especialmente aplicativos obscuros ou personalizados.

O SD-WAN Sincronizado, um recurso do Synchronized Security, oferece benefícios adicionais com o roteamento de aplicativos SD-WAN. O SD-WAN Sincronizado aproveita a clareza e a confiabilidade adicionais da identificação de aplicativos do compartilhamento de informações do Controle Sincronizado de Aplicativos entre endpoints gerenciados pelo Sophos e o Sophos Firewall. Agora, aplicativos que não eram identificados anteriormente também podem ser adicionados às políticas de roteamento do SD-WAN, fornecendo um nível de controle de roteamento e confiabilidade de aplicativos que outros firewalls não oferecem.



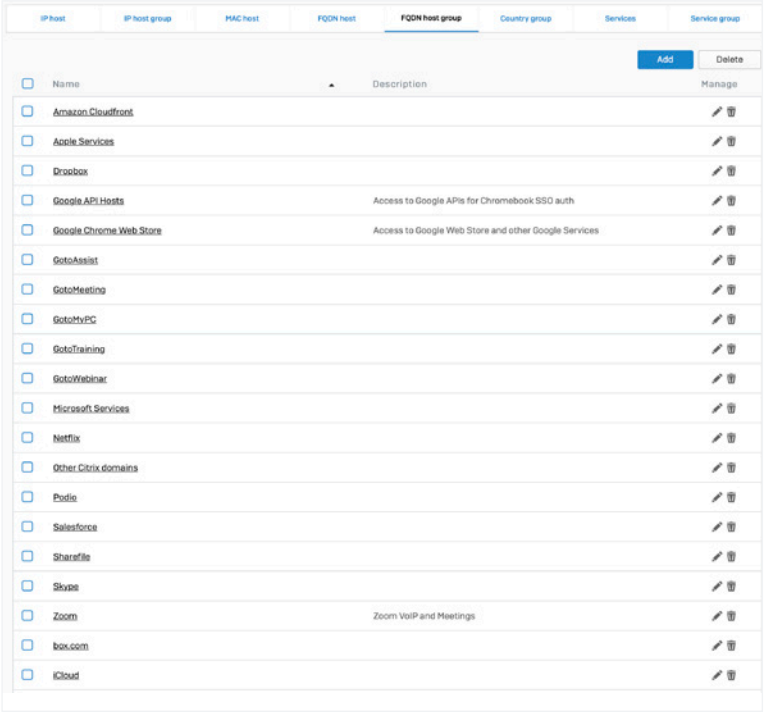
O Controle Sincronizado de Aplicativos identifica 100% de todos os aplicativos em rede, facilitando a priorização e o roteamento de aplicativos de missão crítica.

O Sophos Firewall também permite o roteamento baseado em aplicativos e a seleção de caminhos em cada regra de firewall, incluindo por usuário e grupo. Os controles granulares de roteamento baseado em política (PBR) oferecem a capacidade de definir o roteamento por meio da conexão WAN do gateway primário ou de backup e configurar a direção de reprodução. Juntos, esses recursos facilitam o direcionamento do tráfego de aplicativos importantes para a interface WAN ideal.



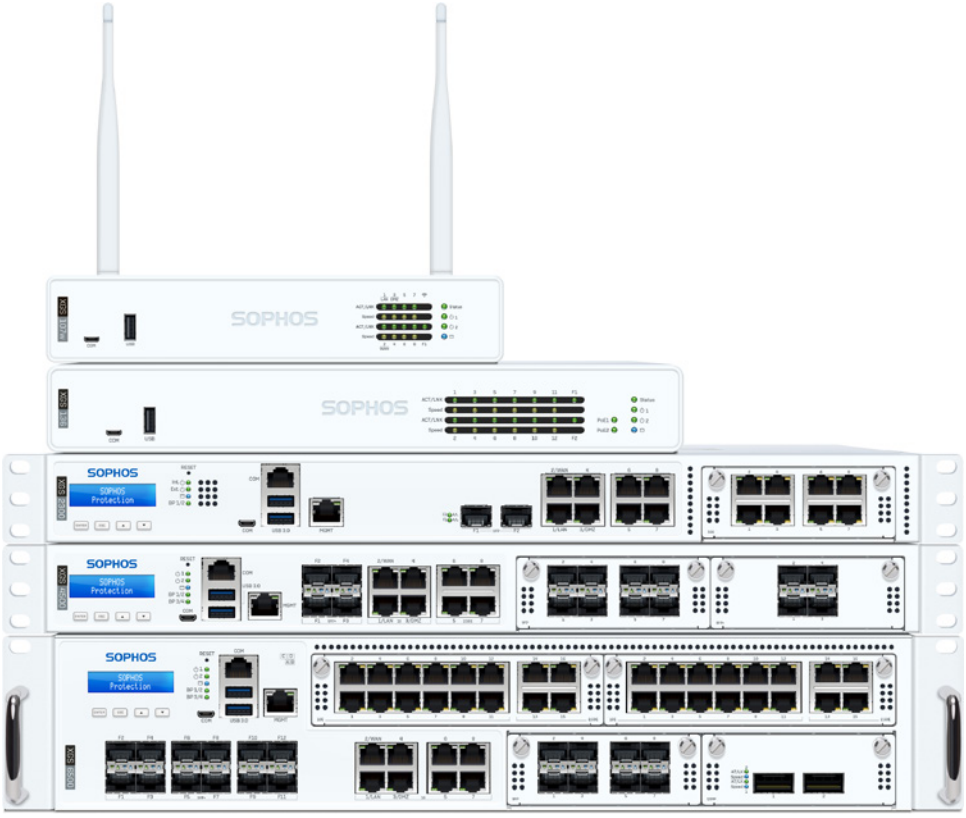
O roteamento baseado em política do SD-WAN oferece ferramentas flexíveis para roteamento do tráfego de aplicativos críticos.

O Sophos Firewall também inclui objetos predefinidos de nome de domínio totalmente qualificado (FQDN) para serviços SaaS populares na nuvem, com milhares de definições de hosts FQDN incluídas e a opção de adicionar mais com facilidade.



Os objetos predefinidos de host FQDN simplificam a seleção de caminhos e o roteamento baseado em aplicativos.

Adicione o Sophos Firewall a qualquer rede – Simplesmente



Os dispositivos de hardware da série Sophos Firewall oferecem opções flexíveis de implantação com portas fail-open bypass em todos os modelos 1U e disponíveis em módulos de portas Flexi para habilitar o recurso também em nossos dispositivos 2U. As portas de bypass permitem que o Sophos Firewall seja instalado no modo ponte em linha com os firewalls existentes. Se o Sophos Firewall precisar ser encerrado ou reinicializado para uma atualização de firmware, as portas de bypass proporcionam continuidade dos negócios ao permitir que o tráfego continue a fluir, garantindo que não haja rupturas na rede. Esse recurso possibilita novas opções de implantação que são totalmente isentas de riscos sem substituir nenhuma das redes existentes. Além disso, a nossa proteção de endpoint next-gen Intercept X trabalha com qualquer produto de desktop antivírus existente, criando uma solução completa do Sophos Synchronized Security para ser implementada em qualquer rede sem precisar fazer substituições.

Sophos Firewall: a segurança cibernética simplificada.

Solicitar orçamento

Solicite um orçamento sob medida para as suas necessidades sem compromisso em sophos.com/firewall-quote

Vendas na América Latina
E-mail: latamsales@sophos.com

Vendas no Brasil
E-mail: brasil@sophos.com

22-03-30 PTBR (DD)