LISTA DE RECURSOS

Lista de recursos do Sophos Firewall

Sophos Firewall

Destaques

- A arquitetura Xstream oferece níveis extremos de visibilidade, proteção e desempenho por meio do processamento de pacotes baseado em fluxo.
- A inspeção TLS Xstream oferece alto desempenho, suporte para TLS 1.3 sem downgrade, independência de porta, políticas de nível empresarial com exceções pré-empacotadas, visibilidade exclusiva do painel de controle e solução de problemas de compatibilidade.
- O mecanismo DPI Xstream oferece proteção de varredura em streaming para IPS, AV, Web, controle de aplicativo e inspeção TLS em um único mecanismo de alto desempenho.
- O Xstream Network Flow FastPath oferece automaticamente aceleração inteligente e orientada por política do tráfego confiável.
- O Xstream SD-WAN oferece seleção de link baseada em desempenho com redirecionamento sem impacto, monitoramento SD-WAN, ferramentas de orquestração SD-WAN multissite e aceleração FastPath do tráfego do túnel de IPSec VPN.
- A interface de usuário dedicada com central de controle interativa utiliza indicadores semelhantes a um semáforo (vermelho, amarelo, verde) para identificar instantaneamente o que precisa de atenção.
- A central de controle oferece informações instantâneas sobre a integridade do endpoint, aplicativos Mac e Windows não identificados, aplicativos na nuvem e TI sombra, cargas suspeitas, usuários de risco, ameaças avançadas, ataques a redes, sites questionáveis e muito mais.
- Navegação otimizada de dois cliques para qualquer lugar com pesquisa inteligente
- O widget Central de Controle de Políticas monitora a atividade da política para empresas, usuários e políticas de rede, e rastreia políticas não utilizadas, desabilitadas, alteradas e novas.
- O modelo de política unificada combina todas as regras de inspeção TLS, firewall e NAT em uma única tela com opções de agrupamento, filtragem e pesquisa.
- Gerenciamento simplificado de regras de firewall para grandes conjuntos de regras com agrupamento automático e manual personalizado, além do recurso de passagem de mouse e indicadores de imposição.
- Todas as regras de firewall fornecem um resumo rápido da segurança e do controle aplicados para AV, sandbox, IPS, Web, aplicativos, modelagem de tráfego (QoS) e Heartbeat.
- Políticas de IPS, Web, aplicativo, TLS e modelagem de tráfego (QoS) pré-definidas permitem uma configuração rápida e personalização fácil de cenários de implantação comuns, como CIPA, políticas típicas do local de trabalho e outros mais.
- O Sophos Security HeartbeatTM conecta os Sophos Endpoints ao firewall para compartilhar o status de verificação de integridade e telemetria, permitindo a identificação instantânea de endpoints com problemas ou comprometidos.
- Resposta a ameaças ativas identifica, bloqueia e responde automaticamente a adversários ativos a partir de feeds de ameaças fornecidos por SophosLabs, analistas MDR ou terceiros
- Controle sincronizado de aplicativos identifica, classifica e habilita o controle de todos os aplicativos Mac/Windows desconhecidos na rede
- Visibilidade de aplicativos na nuvem permite a descoberta instantânea de TI em sombra e oferece modelagem de tráfego com um clique
- A ferramenta de simulação de testes de políticas permite simulação e teste de regras de firewall e políticas web por usuário, IP e hora do dia
- Princípios de design seguros garantem que o firewall seja endurecido contra ataques
- API de configuração para todas as funcionalidades para integração RMM/PSA

SOPHOS

- Integração NDR baseada na nuvem melhora a detecção adversária ativa
- Gateway ZTNA integrado em cada firewall facilita o acesso seguro às aplicações de qualquer lugar
- Sophos Central gerenciamento e relatórios baseados em nuvem para vários firewalls fornece gerenciamento de políticas de grupo e um console para todos os seus produtos de segurança de TI Sophos
- Assistente de configuração simplificada facilita implantação rápida em apenas alguns minutos
- Implantação e configuração sem toque no Sophos Central para novos firewalls
- Integração perfeita com Sophos MDR e XDR

Base Firewall

Gestão Geral

- Interface de usuário simplificada e gerenciamento de regras de firewall para grandes conjuntos de regras com agrupamento com recurso de regra de ponta e indicadores de aplicação
- Suporte à autenticação de dois fatores (senha única) para acesso de administrador, portal do usuário, IPsec, VPN SSL e WAF
- Ferramentas avançadas de logging e troubleshooting na GUI (por exemplo, captura de pacotes)
- A alta disponibilidade (HA) suporta agrupar dois dispositivos no modo ativo-ativo ou ativo-pasivo com plug-and-play Configuração rápida de HA que suporta múltiplos links de sincronização redundantes
- Interface de linha de comando completa (CLI) acessível a partir da GUI
- Administração baseada em funções com integração do Azure AD para login único
- Atualizações de firmware via SSL com fixação de certificado para máxima segurança
- Definições de objetos de sistema reutilizáveis e de pesquisa para redes, serviços, hosts, períodos de tempo, usuários e grupos, clientes e servidores
- Portal de Autoatendimento do Usuário
- Controle de alterações de configuração
- Controle de acesso de dispositivo flexível para serviços por zonas
- Opções de notificação de e-mail ou interceptação SNMP
- SNMP v3 (incluindo monitoramento de hardware) e monitoramento de Netflow/sFlow
- Suporte centralizado de gestão via Sophos Central (disponível apenas para clientes com suporte válido)
- Configurações de backup e restauração: localmente, via FTP ou e-mail; on-demand, diariamente, semanalmente ou mensalmente - com a opção de reformatar ports ao atualizar aparelhos de hardware
- Let's Encrypt suporte de certificado para WAF, SMTP, configuração TLS, login de hotspot, console de Web Admin, portal do usuário, portal cativo, portal VPN e portal SPX
- API para integração de terceiros
- Renomeamento da interface
- Opção de acesso remoto para Sophos Support
- Gestão de licenças baseada na nuvem via MySophos

Firewall, Redes e Roteamento

- Stateful inspeção profunda de pacotes firewall
- A arquitetura de processamento de pacotes Xstream fornece níveis extremos de visibilidade, proteção e desempenho através do processamento de pacotes baseado em stream
- Inspeção de TLS Xstream com alto desempenho, porta de suporte para TLS 1.3 sem downgrade, porta agnóstica, políticas de nível empresarial, visibilidade única do painel e solução de problemas de compatibilidade
- Xstream DPI Engine fornece proteção de scan de fluxo para IPS, AV, web, controle aplicativo e inspeção TLS em um único motor de alto desempenho
- O Xstream Network Flow FastPath fornece aceleração política e inteligente do tráfego de aplicativos confiáveis, tráfego VPN IPSec e tráfego criptografado TLS automaticamente
- Políticas baseadas em usuário, grupo, tempo ou rede
- Políticas de tempo de acesso por usuário/grupo
- Executar políticas entre zonas, redes ou por tipo de serviço
- isolamento de zona e apoio à política baseada em zona
- Zonas padrão para LAN, WAN, DMZ, LOCAL, VPN e Wi-Fi
- Zonas personalizadas em LAN ou DMZ

- Políticas NAT personalizáveis com mascaramento de IP e suporte a objetos completos para redirecionar ou redirecionar vários serviços em uma única regra com um assistente conveniente de regras NAT para criar regras NAT complexas rapidamente e facilmente em apenas alguns cliques
- Definições reutilizáveis de objetos de rede para todas as regras com pesquisa global inteligente de texto livre
- Proteção contra saturamento de dados: Bloqueio de DoS, DDoS e portscan
- Bloqueio de país por geo-IP
- Routing: estático, multicast (PIM-SM) e dinâmico: RIP, BGP, OSPFv3 (IPv6) BGPv6
- Clone rotas estáticas e ligá-las ou desligá-las, redistribuir rotas BGP dinâmicas para OSPFv3, utilizar opções de rota Blackhole e utilizar Equal-Cost Multi-Path (ECMP) para balanceamento de carga
- Suporte ao proxy upstream
- Rotação multicast independente de protocolo com IGMP snooping
- Conexão com suporte STP e ARP broadcast forwarding
- VLAN DHCP suporte e marcação
- Suporte de ponte VLAN
- Jumbo frame suporte
- Ativar/desativar interfaces físicas
- Suporte à WAN sem fio (N/A em implementações virtuais)
- 802.3ad agregação de links de interface
- Configuração completa de DNS, DHCP e NTP
- DNS dinâmico (DDNS)
- Certificação de aprovação do programa IPv6 Ready Logo
- Delegação de prefixo de IPv6 DHCP
- Suporte ao túnel IPv6 incluindo implantação rápida 6in4, 6to4, 4in6 e IPv6 (6a) através do IPsec

Xstream SD-WAN

- Os perfis SD-WAN Xstream suportam múltiplas opções de ligação WAN, incluindo VDSL, DSL, cabo, LTE/celular e MPLS
- SLAs baseados em desempenho selecionam automaticamente o melhor link WAN com base no jitter, latência ou perda de pacotes
- Balanço de carga SD-WAN em múltiplos links SD-WAN com ponderação redonda ou estratégias de persistência de sessão
- O reencaminhamento de impacto zero mantém as sessões de aplicativos quando o desempenho do link cai abaixo dos limiares e uma transição é feita para um link WAN com melhor desempenho
- Gráficos de monitoramento SD-WAN fornecem insights em tempo real sobre latência, jitter e perda de pacotes para todos os links WAN
- Aceleração Xstream FastPath do tráfego de túnel IPsec 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.
- Roteamento de aplicativos em links preferenciais por meio de regras de firewall ou roteamento baseado em políticas
- Suporte robusto de VPN, incluindo IPsec e SSL VPN
- Único túnel RED Layer 2 com roteamento

Modelagem de Tráfego Básica e Quotas

- Modelagem de tráfego flexível baseada em rede ou usuário (QoS) (opções de modelagem de tráfego web e aplicativo melhoradas incluídas na subscrição Web Protection)
- Defina quotas de tráfego baseadas no usuário no upload/download ou no tráfego total e ciclico ou não ciclico
- Otimização VoIP em tempo real
- Marcação de DSCP

Redes sem fio seguras

- Implantação simples de pontos de acesso Sophos Wireless (apenas APX Series) – aparecem automaticamente na central de controle do firewall
- Monitoramento e gerenciamento centralizados de APs e clientes sem fio através do controlador sem fio integrado
- Ponte APs para LAN, VLAN ou uma zona separada com opções de isolamento do cliente
- Suporte múltiplo SSID por rádio, incluindo SSIDs ocultos
- Suporte a diversos padrões de segurança e criptografia, incluindo WPA2 Personal e Enterprise
- Opção de seleção de largura do canal

- Suporte para IEEE 802.1X (autenticação RADIUS) com suporte ao servidor primário e secundário
- Suporte para 802.11r (transmissão rápida)
- Hotspot suporte para (custom) cupons, senha do dia, ou aceitação de T&C
- Acesso à Internet sem fios para hóspedes com opções de jardim murado
- Acesso de rede sem fios baseado no tempo
- Repetição sem fio e ponte de modo de rede em malha com APs suportados
- Automatic canal de seleção de otimização de fundo
- Suporte para login HTTPS

Autenticação

- O ID de usuário sincronizado utiliza Segurança sincronizada para compartilhar o ID de usuário atualmente logado no Active Directory entre os endpoints Sophos e o firewall sem um agente no servidor ou cliente do AD
- Autenticação via: Active Directory, eDirectory, RADIUS, LDAP e TACACS+
- Agentes de autenticação de servidor para Active Directory SSO, STAS, SATC
- Logon Único Active Directory, eDirectory, RADIUS Contabilidade
- Acesso único do Azure AD para acesso do administrador à consola Webadmin
- Acesso único do Azure AD para os usuários autenticarem o acesso à web através do portal cativo
- Transparente AD SSO com HSTS enforcado, possibilitando Kerberos e NTLM handshakes sobre HTTP ou HTTPS
- Azure AD Group Import e suporte RBAC
- Agentes de autenticação do cliente para Windows, Mac OS X, Linux 32/64
- Autenticação SSO do navegador: Autenticação proxy transparente (NTLM) e Kerberos
- Portal cativo do navegador
- Certificados de autenticação para iOS e Android
- Serviços de autenticação para IPsec, SSL, L2TP, PPTP
- Suporte à autenticação do Google Chromebook para ambientes com o Active Directory e o Google G Suite
- Integração do Google Workspace através do cliente LDAP com o Google Chromebook SSO
- Autenticação baseada em API

Usuário Self-Service & Portais VPN

- SNMP v3 (incluindo monitoramento de hardware) e monitoramento de Netflow/sFlow
- Baixe o cliente de autenticação Sophos
- Baixe o cliente de acesso remoto SSL (Windows) e os arquivos de configuração (outro sistema operacional)
- Informações de acesso Hotspot
- Alterar nome de usuário e senha
- Ver uso pessoal de internet
- Acessar mensagens em quarentena e gerenciar listas de bloqueio/permitir remetentes baseadas em usuário (requer proteção de e-mail)

Opções VPN básicas

- VPN site a site: certificados SSL, IPSec, AES/3DES de 256 bits, PFS, RSA, X.509, chave pré-compartilhada
- Sophos RED VPN de site a site túnel (robusto e leve)
- Aceleração do tráfego de túnel de IPSec (tanto site-to-site como de acesso remoto)
- Ferramentas de importação, monitoramento e gerenciamento do AWS VPC
- L2TP e PPTP
- VPN baseada em rota com seletores de tráfego
- Acesso remoto: Suporte a cliente SSL, IPsec, iPhone/iPad/Cisco/Android VPN
- Suporte IKEv2
- Conexão de IPsec HA Stateful failover para RBVPN, PBVPN e VPN de acesso remoto sem perder evento de sessão em cenários de failover HA
- IPsec VPN monitoramento de status de túnel via SNMP
- Suporte avançado IPsec para PSK exclusivo e DH-Group 27-30 / RFC6954
- Cliente SSL para Windows e download de configuração através do portal do usuário

Cliente Sophos Connect

- Autenticação: Chave pré-compartilhada (PSK), PKI (X.509), token e XAUTH
- Suporta login único do Entra ID (Azure AD)
- Ativa Segurança sincronizada e Security Heartbeat para usuários conectados remotos
- Encapsulamento split inteligente para roteamento de tráfego ideal
- Suporte NAT-transversal
- Cliente-monitor para visão geral gráfica do estado da conexão
- Suporte ao cliente Mac (IPsec) e Windows (SSL/IPsec)

Network Protection

Prevenção de Invasão (IPS)

- Motor de inspeção profunda de pacotes IPS de nova geração de alto desempenho com padrões IPS seletivos que podem ser aplicados com base em uma regra de firewall para o máximo desempenho e proteção
- Milhares de assinaturas
- Seleção de categoria granular
- Suporte para assinaturas IPS personalizadas
- Políticas de IPS Os filtros inteligentes permitem políticas dinâmicas que se atualizam automaticamente à medida que novos padrões são adicionados

Resposta a ameaças ativas e Security Heartbeat™

- Resposta a ameaças ativas monitora/bloqueia automaticamente o APT e outras ameaças identificadas através dos feeds de ameaças Sophos-X Ops para proteção contra ameaças avançadas contra bots e adversários ativos que tentam entrar em contato com destinos maliciosos usando detecção de DNS, AFC e firewall em várias camadas
- Resposta a ameaças ativas monitora/bloqueia automaticamente ameaças identificadas por feeds de ameaças MDR/XDR publicados por um Sophos ou por um analista SOC cliente/parceiro quando Sophos Firewall com proteção Xstream é combinado com Sophos MDR/XDR
- Resposta a ameaças ativas monitora/bloqueia automaticamente feeds de ameaças de terceiros de fontes de informação de ameaças industriais, verticais ou regionais com proteção Xstream
- O Sophos segurança sincronizada Heartbeat marca instantaneamente dispositivos comprometidos com status Heartbeat vermelho que estão tentando entrar em contato com qualquer indicador de ameaça identificado pela resposta a ameaças ativas e seus feeds de ameaças relacionados. O estado do ritmo cardíaco também é monitorado por endpoints gerenciados por Sophos e compartilhado com o firewall e incluirá detalhes como host, usuário, processo, contagem de incidentes e tempo de compromisso
- Condições Sophos Security Heartbeat podem ser anexadas a qualquer regra de firewall, limitando automaticamente o acesso a recursos de rede e segmentos para um dispositivo comprometido até que seja limpo
- O Sophos Firewall também inicia automaticamente a proteção contra acesso lateral no caso de um endpoint gerenciado ser comprometido, informando todos os endpoints gerenciados por Sophos saudáveis para rejeitar o tráfego do dispositivo comprometido.

Gerenciamento de Dispositivos RED

- Gerenciamento central de todos os dispositivos SD-RED
- Sem configuração: Conecta automaticamente através de um serviço de provisionamento baseado na nuvem
- Seguro túnel criptografado usando certificados digitais X.509 e criptografia AES de 256 bits
- Ethernet virtual para transferência confiável de todo o tráfego entre locais
- Gestão de Endereços IP com configuração de servidor DHCP e DNS centralizada
- Desautorizar remotamente dispositivos SD-RED após um período de inatividade selecionado
- Compressão do tráfego do túnel
- Opções de configuração de porta VLAN

VPN sem cliente

- Sophos único portal de self-service criptografado HTML5 com suporte para RDP, SSH, Telnet e VNC

Proteção da Web

Proteção e controle da Web

- Inspecção de modo de proteção web DPI ou proxy explícito
- Modo proxy explícito suporta autenticação por conexão para vários usuários no mesmo IP de origem

- Proteção contra ameaças avançadas
- URL Filter banco de dados com milhões de sites em 92 categorias, apoiado por SophosLabs
- Políticas de tempo de quota de navegação por usuário/grupo
- Políticas de tempo de acesso por usuário/grupo
- Varredura de malware: bloqueia todas as formas de vírus, malware web, trojans e spyware em HTTP/S, FTP e e-mails baseados na web
- Proteção avançada de web malware com emulação JavaScript
- Live Protection pesquisa em tempo real na nuvem para a mais recente inteligência de ameaças
- Segundo mecanismo de detecção independente de malware (Avira) para dupla verificação
- Escaneamento em tempo real ou batch mode
- Proteção contra pharming
- Executar restrições de inquilino para o O365
- Detecção e aplicação de túnel de protocolo SSL
- Validação do certificado
- Caching de conteúdo web de alto desempenho
- Caching forçado para atualizações de Endpoint Sophos
- Filtração de tipo de arquivo por tipo de mime, extensão e tipos de conteúdo ativo (por exemplo, Activex, applets, cookies, etc.)
- Aplicação do YouTube para Escolas por política (usuário/grupo)
- Aplicação de SafeSearch (baseada em DNS) para os principais motores de pesquisa por política (usuário/grupo)
- Monitoramento e aplicação de palavras-chave da Web para registar, reportar ou bloquear conteúdos da Web que correspondem a listas de palavras-chave com a opção de carregar listas aduaneiras
- Bloqueio de aplicativos potencialmente indesejados (PUA)
- Opção de supressão de política Web para professores ou funcionários para permitir temporariamente o acesso a sites ou categorias bloqueados que são totalmente personalizáveis e gerenciáveis por usuários selecionados
- Alertas instantâneos para qualquer usuário navegando em uma categoria restrita da Web (tanto frequentemente quanto a cada 5 minutos)

Visibilidade de aplicativos na nuvem

- O widget central de controle exibe a quantidade de dados carregados e baixados para aplicativos na nuvem categorizados como novos, sancionados, não sancionados ou tolerados
- Descubra Shadow IT em um olhar
- Examine para baixo para obter detalhes sobre usuários, tráfego e dados
- Acesso de um clique às políticas de modelagem de tráfego
- Filtrar uso aplicativo na nuvem por categoria ou volume
- Relatório detalhado de uso de aplicativo na nuvem personalizável para relatórios históricos completos

Proteção e controle de aplicativos

- Controle aplicativo sincronizado para identificar, classificar e controlar automaticamente todas as aplicações Windows e Mac desconhecidas na rede, compartilhando informações entre os endpoints gerenciados pela Sophos e o firewall
- Controle de aplicativos baseado em assinaturas com padrões para milhares de aplicações
- Visibilidade e controle aplicativos na nuvem para descobrir a TI sombria
- Filtros inteligentes que permitem políticas dinâmicas que se atualizam automaticamente à medida que novos padrões são adicionados
- Descoberta e controle de micro aplicativo
- Controle de aplicativos com base na categoria, características (por exemplo, consumo de largura de banda e produtividade), tecnologia (por exemplo, P2P) e nível de risco
- Aplicação de políticas de controle de aplicativo por usuário ou regra de rede

Modelagem de tráfego da Web e de aplicativos

- Opções melhoradas de modelagem de tráfego (QoS) por categoria web ou aplicação para limitar ou garantir a prioridade de upload/download ou de tráfego total e taxa de bits individualmente ou compartilhados

Proteção DNS

Serviço de DNS baseado em nuvem

- Serviço de resolução de nome de domínio:
- Serviço DNS baseado em nuvem de alto desempenho
- Powered by SophosLabs e AI

- Bloqueia URLs maliciosas na pesquisa de DNS
- Controles de conformidade detalhados para bloquear sites indesejados por categoria
- Gerenciado no Sophos Central

NDR Essentials

Network Detection and Response

- NDR baseado na nuvem
- Com o poder da IA
- Detecta comunicações de ameaças criptografadas sem descriptografia TLS
- Detecção por algoritmos de geração de domínios
- Pontua ameaças potenciais e alertas em qualquer ameaça que exceda seu limiar definido
- Suporte completo de relatórios e logging

Proteção de Dia Zero

Análise dinâmica de sandbox

- Integração completa no painel de soluções de segurança Sophos
- Inspecciona executáveis e documentos que contenham conteúdo executável (incluindo .exe, .com e .dll, .doc, .docx, docm e .rtf e PDF) e arquivos que contenham qualquer um dos tipos de arquivo listados acima (incluindo ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet)
- Análise agressiva de comportamento, rede e memória
- Detecta o comportamento de evasão de sandbox
- Tecnologia de aprendizado de máquina com Deep Learning analisa todos os arquivos executáveis perdidos
- Inclui prevenção de exploração e tecnologia de proteção CryptoGuard da Sophos Intercept X
- Relatórios de arquivos maliciosos em profundidade com capturas de tela e capacidade de liberação de arquivos do painel
- Seleção opcional de data center e opções de política de usuário e grupo flexíveis sobre tipo de arquivo, exclusões e ações de análise
- Suporta links de download de uma vez

Análise de inteligência de ameaça estática

- Todos os arquivos que contêm código ativo baixado pela web ou que entram no firewall como anexos de e-mail, como executáveis e documentos que contêm conteúdo executável (incluindo .exe, .com e .dll, .doc, .docx, docm e .rtf e PDF) e arquivos que contêm qualquer um dos tipos de arquivo listados acima (incluindo ZIP, BZIP, GZIP, RAR, TAR, LHA/LZH, 7Z, Microsoft Cabinet) são enviados automaticamente para análise de inteligência de ameaças
- Os arquivos são verificados com base na enorme base de dados de inteligência de ameaças da SophosLabs e submetidos a múltiplos modelos de aprendizado de máquina para identificar malware novo e desconhecido
- O extenso relatório inclui um widget de painel para arquivos analisados, uma lista detalhada dos arquivos que foram analisados e os resultados da análise, e um relatório detalhado que descreve o resultado de cada modelo de aprendizado de máquina

Central Orchestration

Orquestração SD-WAN

- Orquestração SD-WAN e VPN com a criação fácil e automatizada baseada em assistente de túneles VPN de site a site entre locais de rede usando uma arquitetura ideal (hub-and-spoke, rede completa ou alguma combinação)
- Suporta túneles IPsec, SSL ou RED VPN. Integra perfeitamente com recursos SD-WAN para priorização de aplicativos, otimização de roteamento e aproveitamento de múltiplos links WAN para resiliência e desempenho

Central Firewall Reporting avançado

- 30 dias de armazenamento de dados na nuvem para relatórios históricos de firewall com recursos avançados para salvar, agendar e exportar relatórios personalizados

Integração do XDR e MDR

- Integração com Sophos XDR e MDR para fornecer telemetria e inteligência de ameaças para caça a ameaças e análise
- Sophos Resposta a ameaças ativas utiliza feeds de ameaças dos analistas MDR e XDR para identificar, bloquear e isolar automaticamente ameaças ativas na rede
- Segurança sincronizada IoC telemetria recolhe informações importantes sobre qualquer ameaça, usuários, processo e dispositivo que foi comprometido

Email Protection

Proteção e controle de e-mails

- Escaneamento de e-mail com suporte para SMTP, POP3 e IMAP
- Serviço de reputação com monitoramento de surtos de spam baseado em tecnologia patenteada de detecção de padrões recorrentes
- Bloquear spam e malware durante a transação SMTP
- DKIM e BATV proteção anti-spam
- Proteção contra Spam Greelisting e Framework Política do Enviador (SPF)
- Verificação do destinatário para endereços de e-mail errados
- Segundo mecanismo de detecção independente de malware (Avira) para dupla verificação
- Live Protection pesquisa em tempo real na nuvem para a mais recente inteligência de ameaças
- Atualizações automáticas de assinatura e padrão
- Suporte de host inteligente para relés de saída
- Detecção/bloqueio/escaneamento de ficheiros anexados
- Aceitar, rejeitar ou soltar mensagens de tamanho excessivo
- Detecta URLs de phishing dentro de e-mails
- Use regras de varredura de conteúdo predefinidas ou crie suas próprias regras personalizadas com base em uma variedade de critérios com opções de política e exceções detalhadas
- Suporte à criptografia TLS para SMTP, POP e IMAP
- Adicionar assinatura automaticamente a todas as mensagens de saída
- Arquivador de Emails
- Bloqueie e permita que listas de remetentes sejam mantidas através do portal do usuário

Gerenciamento de quarentena de e-mails

- Resumo de quarentena de spam e opções de notificações
- Quarantena de malware e spam com opções de pesquisa e filtragem por data, remetente, destinatário, assunto e razão com opção para liberar e excluir mensagens
- Portal do usuário self-service para visualização e liberação de mensagens em quarentena

Encriptação e DLP de e-mails

- Criptografia SPX pendente de patente para criptografia de mensagem unidirecional
- Auto-registro do destinatário SPX password management
- Adicionar anexos a respostas seguras SPX
- Completamente transparente - nenhum software adicional ou cliente necessário
- Motor DLP com digitalização automática de e-mails e anexos para dados sensíveis
- Listas de controle de conteúdo (CCLs) de tipo de dados sensíveis pré-embaladas para PII, PCI, HIPAA e mais, mantidas pela SophosLabs

Proteção ao Servidor da Web

Proteção de firewalls de aplicativos da Web

- Proxy reverso
- Motor de hardening de URL com deep-linking e prevenção de traversal de diretórios
- Hardening de formulário motor
- Proteção de injeção SQL
- Proteção de script cross-site
- Motores antivírus duplos (Sophos e Avira)
- HTTPS (TLS/SSL) criptografia offloading
- Assinatura de cookies com assinaturas digitais
- Rotação baseada em caminho
- Aplicação da política Geo IP
- Configuração de criptografia personalizada e aplicação de versão TLS
- HSTS e X-Content-Type-Options Implementação
- Suporte ao protocolo Outlook em qualquer lugar
- Autenticação reversa (offloading) para autenticação baseada em formulário e básica para acesso ao servidor
- Abstração de servidor virtual e de servidor físico
- balanceador de carga integrado distribui visitantes em vários servidores

- Passe os controlos individuais de forma granular conforme necessário
- Solicitações de correspondência de redes de origem ou URLs de destino especificadas
- Suporte para lógica e/ou operadores
- Ajuda a compatibilidade com várias configurações e implementações não padrão
- Opções para alterar os parâmetros de desempenho do firewall da aplicação web
- Opção de limite de tamanho de digitalização
- Permitir/bloquear intervalos IP
- Suporte de Wildcard para caminhos de servidor e domínios
- Adicionar automaticamente um prefixo/sufixo para autenticação

Emissão de relatórios e logging

Central Firewall Reporting

- Relatórios pré-definidos com opções de personalização flexíveis
- Relatórios para Firewalls Sophos: hardware, software, virtual e cloud
- Interface de usuário intuitiva fornece representação gráfica de dados
- O painel de relatórios fornece uma visão panorâmica dos eventos das últimas 24 horas
- Identifique facilmente atividades de rede, tendências e ataques potenciais
- Fácil backup de logs com acesso rápido para fins de auditoria
- Implantação simplificada sem necessidade de conhecimentos técnicos

Central Firewall Reporting avançado

- Relatórios agregados multi-firewall
- Salvar modelos de relatórios personalizados
- Relatórios agendados
- Exportar relatórios em formato PDF, CFV ou HTML
- Até um ano de armazenamento de dados por firewall
- Conector de Data Lake MDRXDR para caça à ameaça

Relatórios on-box

- NOTA: O relatório Sophos Firewall está incluído sem custo adicional, mas a disponibilidade de logs, relatórios e widgets individuais pode depender das respectivas licenças do módulo de proteção.
- Centenas de relatórios on-box com opções de relatório personalizadas: Dashboards (Tráfego, Segurança e Quocientes de Ameaças de Usuários), Licitações Aplicacionais (Risco de Aplicações, Aplicações Bloqueadas, Aplicações Sincronizadas, Motores de Pesquisa, Servidores Web, Match de Palavras-Chave da Web, FTP), Rede e Ameaças (Resposta a Ameaças ativas e feeds de ameaças, Security Heartbeat, IPS, Proteção sem Fio, Proteção contra Ameaças de Dia Zero), VPN, E-mail, Compliance (HIPAA, GLBA, SOX, FISMA, PCI, NERC CIP v3, CIPA)
- Monitoramento de atividade atual: integridade do sistema, usuários ao vivo, conexões IPsec, usuários remotos, conexões ao vivo, clientes sem fio, quarentenas e ataques DoS
- Monitoramento de desempenho de link SD-WAN em tempo real baseado em jitter, latência e perda de pacote
- Anonimização de relatório
- Programação de relatórios para múltiplos destinatários por grupo de relatórios com opções de frequência flexíveis
- Exportar relatórios como HTML, PDF, Excel (XLS)
- marcadores de relatório
- Personalização de retenção de log por categoria
- Visualizador de log completo com visualização de coluna e visualização detalhada com poderosas opções de filtro e pesquisa, ID de regra hiperlinkada e personalização de visualização de dados

Gerenciamento central

Sophos Central

- Sophos Central gerenciamento e relatórios baseados em nuvem para vários firewalls fornece gerenciamento de políticas de grupo e um único console para todos os seus produtos de segurança de TI Sophos
- Gerenciamento de políticas de grupo permite que objetos, configurações e políticas sejam modificados uma vez e sincronizados automaticamente com todos os firewalls do grupo
- O Gerenciador de tarefas fornece um histórico completo de acompanhamento de auditoria e monitoramento de status de mudanças nas políticas do grupo
- Gerenciamento de firmware de backup em Sophos Central armazena os últimos cinco arquivos de backup de configuração para cada firewall com um que pode ser colado para armazenamento permanente e acesso fácil
- A programação de atualizações de firmware da Sophos Central permite que atualizações automáticas sejam aplicadas facilmente a qualquer momento
- A implantação zero-touch permite que a configuração inicial seja realizada no Sophos Central e depois exportada para upload no dispositivo usando uma unidade de memória flash na inicialização, reconectando o dispositivo automaticamente ao Sophos Central.

Zero Trust Network Access

- Integração Sophos gateway ZTNA para acesso seguro a aplicações alojadas atrás do firewall
- Gerenciado no Sophos Central

Segurança no design

Sophos Firewall Status de Integridade compara dezenas de configurações com as melhores práticas para identificar riscos potenciais com fácil análise para resolver problemas

- Capacidade automática de hotfix zero-touch over the air para corrigir vulnerabilidades sem tempo de inatividade
- Núcleo endurecido para maior segurança, desempenho e escalabilidade com isolamento e mitigação de processos apertados para ataques de canal lateral
- Monitoramento remoto da integridade por Sophos usando um sensor XDR integrado para permitir monitoramento em tempo real da integridade do sistema, incluindo configuração não autorizada, execução de código malicioso, manipulação de arquivos e muito mais, para identificar e responder rapidamente a ataques
- Arquitetura Xstream de nova geração com novo plano de controle para máxima segurança e escalabilidade
- Containerização dos principais limites de confiança e portais de usuário/VPN
- Gestão central criptografada e segura via Sophos Central eliminando qualquer necessidade de acesso remoto do administrador
- A autenticação multifacetada em todos os sistemas protege contra roubo de credenciais e ataques brutais
- Gateway ZTNA integrado para acesso remoto mais seguro e proteção de aplicativos
- Implementações seguras off-the-box garantem que as melhores práticas de segurança sejam implementadas com controles de acesso rigorosos

Características do Sophos Firewall por subscrição Sumário

	Pacote Xstream Protection							Disponível separadamente		
	Pacote Standard Protection					Disponível separadamente				
	Base Firewall	Network Protection	Proteção da Web	Proteção DNS	Funções do Bundle Only	Proteção de Dia Zero	Central Orchestration	Central Firewall Reporting Adv.	Email Protection	Proteção ao Servidor da Web
Gerenciamento geral (incl. HA)	✓									
Arquitetura Xstream	✓									
Firewall, Redes e Roteamento	✓									
Xstream SD-WAN	✓									
Modelagem de Tráfego Básica e Quotas	✓									
Redes sem fio seguras	✓									
Autenticação	✓									
Portal de Autoatendimento do Usuário	✓									
VPN (IPsec, SSL, etc)	✓									
VPN site a site RED	✓									
Cliente VPN do Sophos Connect	✓									
Prevenção de Invasão (IPS)		✓								
Resposta a ameaças ativas										
Feeds de ameaças do Sophos X-Ops		✓								
Feed de ameaças do MDR/XDR					✓					
Feeds de ameaças de terceiros					✓					
Pulsação de Segurança Sincronizada		✓								
Gerenciamento de Dispositivos RED		✓								
VPN sem cliente		✓								
Controle de aplicação sincronizada			✓							
Proteção e controle da Web			✓							
Proteção e controle de aplicativos			✓							
Visibilidade de aplicativos na nuvem			✓							
Modelagem de tráfego da Web e de aplicativos			✓							
Segurança e conformidade do DNS				✓						
NDR Essentials					✓					
Análise dinâmica de sandbox						✓				
Análise de inteligência de ameaças						✓				
Orquestração SD-WAN							✓			
Dados de relatório do firewall central**		7 dias	7 dias	7 dias	7 dias	7 dias	30 dias	Até 1 ano	7 dias	7 dias
Características avançadas do CFR							✓	✓		
Proteção e controle de e-mails									✓	
Gerenciamento de quarentena de e-mails									✓	
Encriptação e DLP de e-mails									✓	
Proteção de firewalls de aplicativos da Web										✓
Logs/Relatórios em caixa	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Sophos Central Management		✓	✓	✓	✓	✓	✓	✓	✓	✓
Gateway de ZTNA		✓	✓	✓	✓	✓	✓	✓	✓	✓
Segurança no design	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Nota: Algumas funcionalidades não são suportadas nos modelos XGS 87 e XGS 88 (reporting on-box, dupla varredura AV, varredura WAF AV e agente de transferência de mensagens de e-mail (MTA) funcionalidade)

Opções de licenciamento MSP diferem ligeiramente do acima

* O tempo de retenção de armazenamento de dados é uma estimativa baseada no uso médio da rede e variará dependendo do volume de dados de registro real. Ferramenta de Estimativa de Armazenamento.

**(Incluído com qualquer assinatura de proteção, suporte ou pacote*) Os clientes com uma licença base apenas precisam adicionar suporte para serem elegíveis para esses recursos.

SOPHOS

Características do Sophos Firewall por subscrição Sumário

	Suporte Aprimorado (Incluído nos pacotes Standard e Xstream Protection)	Suporte Aprimorado Plus (disponível como uma atualização do Suporte Enhanced)
Suporte multi-canal 24/7 (telefone, portal web, bate-papo) incluindo assistência remota e acesso de autoajuda a KB e fóruns de suporte	✓	✓
Downloads, atualizações e manutenção de firmware **	✓	✓
Sophos Central Management, Reporting e Gateway ZTNA	✓	✓
Substituição Advanced Hardware de dispositivos ativos	✓	✓
Substituição avançada de hardware para um dispositivo HA passivo*		✓
Substituição avançada de hardware para dispositivos SD-RED/APX		✓
Acesso VIP (chamadas encaminhadas para engenheiros seniores)		✓
Consultoria à distância (2-8 horas por ano)		✓

* Para habilitar cobertura RMA avançada para um dispositivo HA passivo, o dispositivo ativo deve ter uma licença de suporte Enhanced Plus
Consulte a Guia de Suporte Sophos para mais detalhes.

** Observação: Suporte deve ser adicionado a qualquer compra de módulo individual para receber atualizações de firmware

Vendas na América Latina
Email: latamsales@sophos.com

Vendas no Brasil
Email: brasil@sophos.com

2025-12-15 PTBR (DD)