SOPHOS

O que há de novo no

Sophos Firewall

As grandes novidades em recursos no Sophos Firewall OS v21.5

Proteção e desempenho adicionados

A integração do Sophos NDR Essentials ao Sophos Firewall

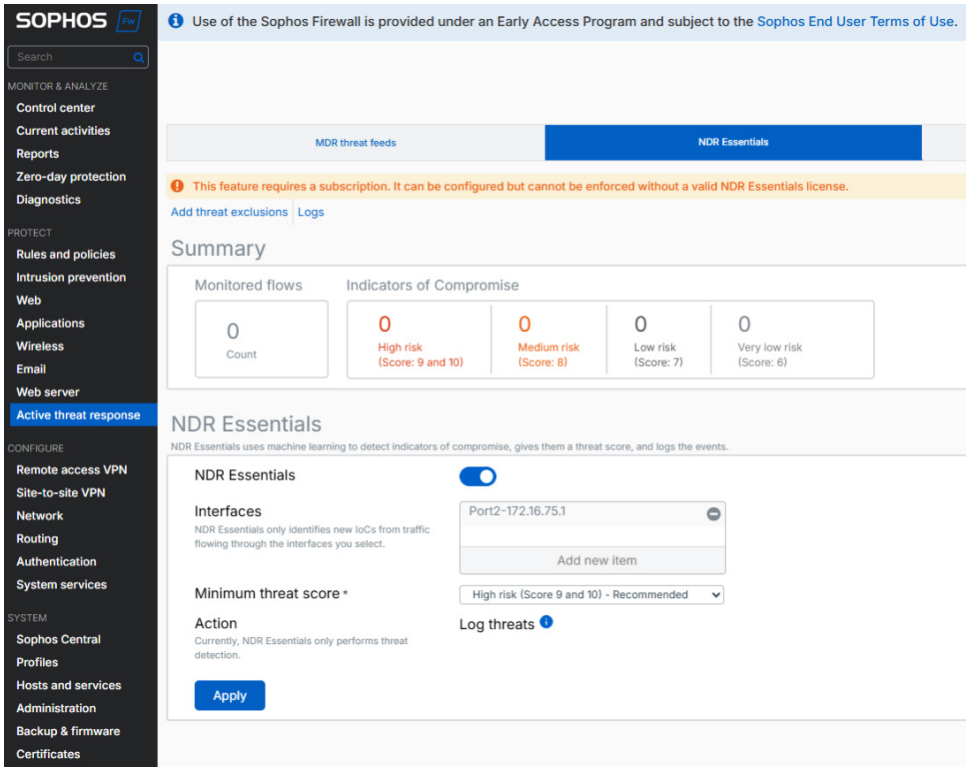
Network Detection and Response (NDR) é uma categoria de produtos de segurança de rede projetada para detectar o comportamento anormal de tráfego e ajudar a identificar adversários ativos operando na rede. Os invasores são bastante habilidosos para escapar da detecção, mas eles precisam se mover pela rede ou se comunicar externamente para executar um ataque. Normalmente, o NDR se posicionada na rede utilizando sensores que monitoram e analisam o tráfego de rede para identificar esse tipo de atividade suspeita.

Os produtos NDR já estão em uso há muitos anos, e o Sophos NDR tem sido parte do nosso portfólio de produtos MDR/XDR desde 2023. Contudo, com o SFOS v21.5, integramos o NDR ao Sophos Firewall, o primeiro do setor a promover essa iniciativa sem incorrer em custos extras aos clientes do Sophos Firewall com Xstream Protection.

A integração do NDR com um Firewall Next-Gen pode parecer uma escolha óbvia, mas o desafio maior é colocar isso em prática sem afetar o desempenho do firewall. A análise de tráfego NDR exige uma potência de processamento incrível. Consequentemente, estamos seguindo a abordagem de implantar uma solução NDR no Sophos Cloud para liberar a carga mais intensa do firewall.

O Sophos Firewall v21.5 introduz a nossa nova plataforma Network Detection and Response do NDR Essentials entregue pela nuvem. Ela utiliza as últimas detecções de IA para ajudar a identificar adversários ativos e compartilha as informações usando a API de feeds de ameaças do Sophos Firewall como parte da Resposta a Ameaças Ativas para manter você informado sobre as detecções e os seus riscos relacionados.

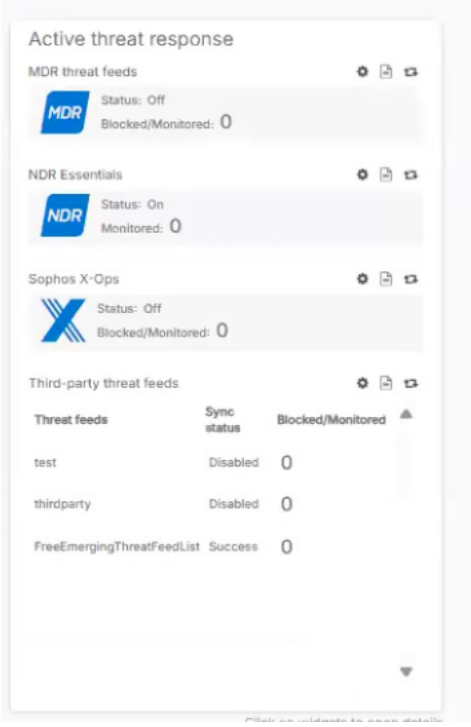
Como funciona: o Sophos Firewall captura metadados do tráfego criptografado por TLS e consultas DNS e envia essas informações para o NDR Essentials no Sophos Cloud, onde os dados são analisados usando diferentes mecanismos de IA. Ele pode detectar cargas criptografadas maliciosas sem realizar a descriptografia TLS, além de domínios novos e incomuns gerados através de algoritmos que são, muitas vezes, um indicador de comprometimento chave. A extração de metadados é realizada por um novo mecanismo leve implementado no Xstream FastPath, portanto, só se encontra disponível em firewalls em hardware da Série XGS. Firewalls em software, virtuais e na nuvem terão a funcionalidade NDR integrada futuramente, mas não na versão v21.5.



Instale e monitore o feed do NDR Essentials em Resposta a ameaças ativas, juntamente com os seus outros feeds de ameaças.

O novo feed de ameaças do NDR Essentials é gerenciado juntamente com os seus outros feeds de ameaças (Sophos X-Ops, MDR e feeds de terceiros) na área de Resposta a ameaças ativas do firewall, como mostra a captura de tela acima. A instalação é simples: ligue o interruptor, selecione quais interfaces internas monitorar, um limite mínimo para a detecção de risco e você está pronto para seguir!

As detecções do NDR Essentials são classificadas em um intervalo de 1 (baixo risco) a 10 (alto risco). Você decide qual classificação de risco estabelecer para o alerta de acordo com o seu ambiente. O padrão recomendado é alto risco (9-10). Todas as detecções com pontuações 6 ou acima são registradas, mas apenas aquelas com pontuação igual ou acima do limite disparam notificações e são exibidas com alertas no widget Central de Controle no painel. As detecções com pontuações abaixo de 6 podem representar falsos positivos e, portanto, não são registradas. No momento, nenhuma detecção do NDR Essentials é bloqueada, mas, futuramente, poderá se tornar uma opção. Todas as detecções são acessíveis completamente através do Relatório de resposta a ameaças ativas disponível com o produto e também via Sophos Central Firewall Reporting.



As detecções do NDR Essentials que atinjam ou ultrapassem o limite de risco definido são exibidas no widget Central de Controle revisado.

Se você deseja receber mais insights de detecção e trabalhar com os recursos de caça a ameaças, recomendamos que pondere o uso do Sophos Extended Detection and Response (XDR) com a implementação integral do Sophos NDR no novo Console de investigação NDR. Considere também os nossos Serviços Gerenciados de Detecção e Resposta 24/7 completos. Todos esses produtos e serviços trabalham melhor em conjunto com os seus Sophos Firewalls.

Acesso remoto por VPN com SSO

Logon único do Entra ID (Azure AD) para cliente Sophos Connect e portal de VPN

Um dos recursos mais solicitados foi tornar o acesso remoto por VPN mais fácil para os usuários finais, permitindo que utilizem suas credenciais de rede corporativa com o cliente Sophos Connect e o portal de VPN do firewall. Agora, o logon único do Entra ID (Azure AD) para a integração com o cliente Sophos Connect e o portal de VPN está incluído no SFOS v21.5. Ele oferece integração nativa na nuvem através dos protocolos OAuth 2.0 e OpenID Connect padrão do setor. Oferece também compatibilidade com o cliente Sophos Connect 2.4 e posteriores no Microsoft Windows.

Outras melhorias de escalabilidade e VPN

Melhorias à interface do usuário e usabilidade: tipos de conexão foram renomeados de "site a site" para "baseado em política" e interfaces de túnel foram renomeadas para "baseado em rota" para deixá-los mais intuitivos.

Melhorada a validação do pool de arrendamento de IP: VPN de acesso remoto entre SSLVPN, IPsec, L2TP e PPTP para eliminar possíveis conflitos de IP.

Aplicação de perfil estrito: em perfis IPsec que excluem valores padrão para assegurar o sucesso do handshake, eliminando a possível fragmentação de pacotes e a falha de túneis ao realizar o estabelecimento apropriado.

Escalabilidade da VPN baseada em rota: a capacidade de VPN baseada em rota é duplicada com o suporte a até 3.000 túneis.

Escalabilidade de SD-RED: agora, o Sophos Firewalls suporta até 1.000 túneis de RED site a site e até 650 dispositivos SD-RED.

Sophos DNS Protection

A simplicidade do Sophos DNS Protection

No ano passado, lançamos nosso serviço DNS Protection e o disponibilizamos gratuitamente a todos os clientes de firewall com a licença Xstream Protection. Com essa versão, o Sophos DNS Protection passa a se integrar com o Sophos Firewall na forma de um novo widget da Central de Controle para indicar o status do serviço, bem como novos insights para a resolução de problemas via log e notificações, e um novo tutorial guiado sobre como instalar o Sophos DNS Protection com facilidade.

Gerenciamento agilizado e melhorias de qualidade de vida

Como acontece em todos os novos lançamentos do Sophos Firewall, essa versão inclui várias melhorias de qualidade de vida que facilitam o gerenciamento diário.

Colunas de tabela redimensionáveis: um recurso há muito solicitado, agora várias telas de configuração e status do firewall aceitam o redimensionamento da largura das colunas, retendo a largura na memória do navegador para aplicá-la nas próximas visitas. São muitas telas que se beneficiam desse novo recurso, como SD-WAN, NAT, SSL, Hosts e serviços, e VPN de site a site.

Pesquisa de texto livre estendida: agora, as rotas de SD-WAN permitem a pesquisa pelo nome da rota, ID, objetos e valor de objetos, como endereços IP, domínios e outros critérios. Regras de ACL locais também aceitam a pesquisa por nome e valor do objeto, incluindo a pesquisa baseada em conteúdo.

Configuração padrão: por demanda popular, as regras de firewall padrão e o grupo de regras anteriormente criado ao instalar um novo firewall foram removidos, sendo agora apenas a regra de rede padrão e as regras de MTA que são fornecidas durante a instalação inicial. O grupo de regras de firewall e a sondagem de gateway padrão dos gateways personalizados estão ambos definidos, por padrão, como "Nenhum".

Novas fontes: a interface do usuário do Sophos Firewall apresenta agora uma fonte mais nítida, clara e precisa, aprimorando a legibilidade e o desempenho.

Outras melhorias

Licença virtual, no software e na nuvem: todas as licenças do Sophos Firewall, tanto virtual como de software e da nuvem (BYOL), não mais impõem limites de RAM. Agora as licenças são limitadas estritamente pela contagem de núcleos e não têm restrições de RAM.

Maior limite de tamanho de arquivo no WAF: suporta a solicitação (upload) configurável do limite de tamanho para o Web Application Firewall (WAF), que agora pode fazer a varredura de arquivos de até 1 GB.

Segurança no design: estamos continuamente melhorando a segurança do Sophos Firewall, e, neste lançamento, adicionamos a coleta de telemetria em tempo real para identificar mudanças inesperadas a arquivos de SO essenciais usando a validação de hash. Isso permitirá que nossas equipes de monitoramento identifiquem proativamente os possíveis incidentes de segurança antes que se tornem um verdadeiro problema.

Relaxamento da delegação de prefixo de DHCP: agora aceita prefixos de /48 a /64, melhorando a interoperabilidade com ISPs. Anúncios de roteador (RA) e o servidor DHCPv6 também estão habilitados por padrão.

Descoberta de MTU do caminho: isso resolve erros de descriptografia TLS devido ao recente suporte ao intercâmbio de chaves ML-KEM (Kyber) nos navegadores. O mecanismo de inspeção profunda de pacotes do Sophos Firewall detectará e ajustará automaticamente o MTU para cada fluxo, assegurando o desempenho ideal com base nas condições de rede específicas.

NAT64 (tráfego IPv6 para IPv4): NAT64 é suportado para o tráfego de IPv6 para IPv4 no modo de proxy explícito. Nesse modo, os clientes somente IPv6 podem acessar os sites IPv4. O firewall também suporta proxies upstream IPv4 para clientes somente IPv6.

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

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

2025-03-31 PTBR (DD)

SOPHOS