SOPHOS

Was ist neu in der

Sophos Firewall?

Die wichtigsten neuen Funktionen in Sophos Firewall OS v21.5

Mehr Schutz und stärkere Performance

Integration von Sophos NDR Essentials in die Sophos Firewall

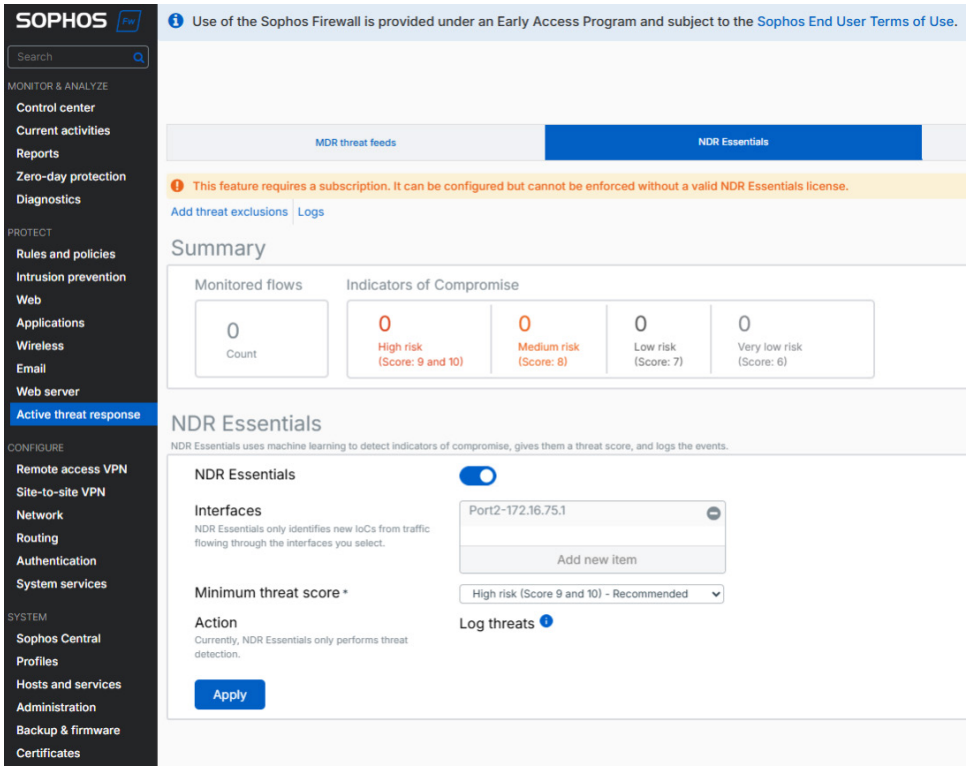
Network Detection and Response (NDR) ist eine Kategorie von Network-Security-Produkten, die Datenverkehrs-Anomalien erkennen können. Versierten Angreifern gelingt es oft, erste Erkennungen zu umgehen. Doch um einen Angriff durchzuführen, müssen sie sich irgendwann im Netzwerk bewegen oder nach außen kommunizieren. NDR ist in der Regel im Netzwerk implementiert und nutzt Sensoren, die den Netzwerkverkehr überwachen und analysieren, um solche verdächtigen Aktivitäten zu erkennen.

NDR-Produkte gibt es bereits seit vielen Jahren, und auch bei Sophos ist NDR seit Anfang 2023 in unserem MDR/XDR-Portfolio enthalten. Mit SFOS v21.5 integrieren wir NDR nun in die Sophos Firewall – als branchenweit erster Anbieter. Kunden der Sophos Firewall mit Xstream Protection erhalten diese neue Funktion ohne zusätzliche Kosten.

Die Integration von NDR in eine Next-Gen Firewall scheint naheliegend. Dabei besteht jedoch die Herausforderung, dies so umzusetzen, dass die Performance der Firewall nicht beeinträchtigt wird. NDR-Traffic-Analysen erfordern nämlich eine beträchtliche Rechenleistung. Deshalb haben wir uns entschlossen, unsere NDR-Lösung in der Sophos Cloud bereitzustellen, um eine zusätzliche Belastung der Firewall zu vermeiden.

Mit der Sophos Firewall v21.5 führen wir NDR Essentials ein – unsere neue cloudbasierte Network-Detection-and-Response-Plattform. Sie nutzt aktuelle KI-Erkennungen, um aktive Angreifer zu finden, und gibt diese Daten über die Sophos Firewall und die Bedrohungsfeed-API als Teil der Active Threat Response weiter. So bleiben Sie stets über alle Erkennungen und deren Risiken informiert.

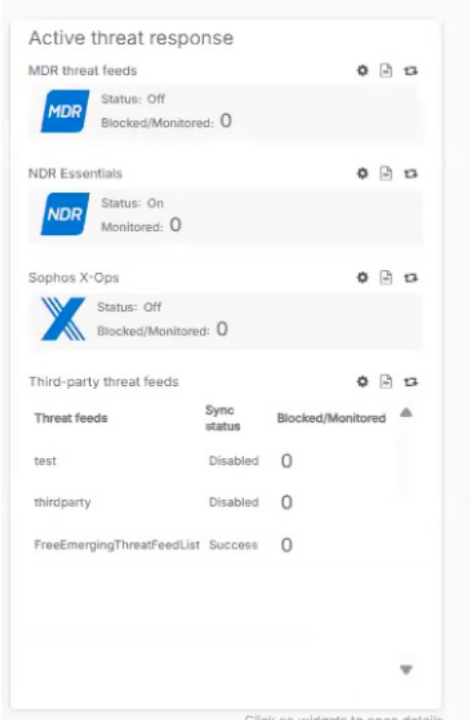
So funktioniert unsere Lösung: Die Sophos Firewall erfasst Metadaten des TLS-verschlüsselten Datenverkehrs sowie DNS-Abfragen und sendet diese Informationen an NDR Essentials in der Sophos Cloud, wo sie mit mehreren KI-Engines analysiert werden. Unsere neue Lösung erkennt schädliche verschlüsselte Payloads, ohne eine TLS-Verschlüsselung durchzuführen, sowie neue und unübliche Domains, die von Algorithmen erstellt wurden – das ist oft ein wichtiger Indikator für eine Kompromittierung. Diese Metadaten-Extrahierung erfolgt über eine neue, leichte Engine auf dem Xstream FastPath. Deshalb ist NDR Essentials derzeit auch nur für Hardware-Firewalls der XGS-Serie verfügbar. Für virtuelle, Software- und Cloud-Firewalls wird die neue NDR-Integration ggf. in Zukunft angeboten, jedoch noch nicht in v21.5.



Richten Sie Ihren NDR Essentials Feed unter Active Threat Response gemeinsam mit Ihren anderen Bedrohungsfeeds ein und überwachen Sie ihn.

Der neue NDR-Essentials-Bedrohungsfeed wird neben Ihren anderen Bedrohungsfeeds (Sophos X-Ops, MDR, Drittanbieter) im Bereich für die Active Threat Response der Firewall verwaltet, wie der Screenshot oben zeigt. Die Einrichtung ist ganz einfach: Zum Aktivieren legen Sie einen Schalter um. Dann wählen Sie aus, welche internen Schnittstellen überwacht werden und wo der untere Schwellenwert für die Erkennungsrisiken liegen soll.

NDR-Essentials-Erkennungen werden auf einer Skala von 1 (geringes Risiko) bis 10 (hohes Risiko) eingeordnet. Sie entscheiden für Ihre Umgebung, ab welchem Wert ein Alert ausgegeben werden soll. Empfohlen wird ein Wert, der einem hohen Risiko entspricht (9–10). Alle Erkennungen größer oder gleich 6 werden protokolliert, aber nur diejenigen, die den Schwellenwert erreichen, werden auf dem neuen Control Center Dashboard Widget als Alerts ausgegeben. Alle Erkennungen unter 6 können falsch positiv sein und werden deshalb nicht protokolliert. Derzeit werden keine NDR-Essentials-Erkennungen blockiert, in Zukunft könnte dies allerdings als Option angeboten werden. Alle Erkennungen sind vollständig über den Bericht zur Active Threat Response zugänglich, sowohl über das On-Box Reporting als auch das Sophos Central Firewall Reporting.



Alle Erkennungen von NDR Essentials, die den Risikoschwellenwert erreichen oder überschreiten, werden im überarbeiteten Control Center Widget angezeigt.

Wenn Sie Ihre Bedrohungserkennung verbessern und Threat-Hunting-Kapazitäten erweitern möchten, sollten Sie sich Sophos Extended Detection and Response (XDR) ansehen – unsere Lösung, bei der Sophos NDR von Anfang an implementiert wird. Auch unsere neue NDR-Analyse-Konsole ist einen Blick wert. Außerdem bieten wir 24/7 Managed Detection and Response Services an. All diese Produkte und Services funktionieren besser gemeinsam mit Ihren Sophos Firewalls.

Remote Access VPN SSO

Entra ID (Azure AD) Single-Sign On für Sophos Connect Client und VPN-Portal

Eine der am häufigsten angefragten Funktionen erleichtert Remote Access VPN für Endbenutzer, sodass sie ihre Zugangsdaten für das Unternehmensnetzwerk mit dem Sophos Connect Client und dem Firewall VPN-Portal verwenden können. Die Single-Sign-On-Integration über Entra ID (Azure AD) mit Sophos Connect und dem VPN-Portal ist jetzt in SFOS v21.5 enthalten. Sie bietet cloudnative Integration über die branchenüblichen Oauth 2.0- und OpenID Connect-Protokolle für nahtlosen Komfort. Unterstützt mit Sophos Connect Client 2.4 und höher unter Microsoft Windows.

Weitere Verbesserungen bei VPNs und Skalierbarkeit

Verbesserungen der Benutzeroberfläche und Benutzerfreundlichkeit: Die Verbindungsarten wurden umbenannt von „Site-to-Site" zu „Richtlinienbasiert", und Tunnel-Interfaces wurden umbenannt zu „Routenbasiert", um diese Begriffe intuitiver zu gestalten.

Verbesserte IP-Lease-Pool-Validierung: Über SSLVPN, IPsec, L2TP und PPTP Remote Access VPN, um potenzielle IP-Konflikte zu beseitigen.

Strikte Profildurchsetzung: Auf IPsec-Profilen, die Standardwerte ausschließen, um einen erfolgreichen Handshake zu gewährleisten, wodurch potenzielle Paketfragmentierung und Tunnels, die nicht ordnungsgemäß aufgebaut werden können, vermieden werden.

Routenbasierte VPN-Skalierbarkeit: Die routenbasierte VPN-Kapazität wird verdoppelt und unterstützt bis zu 3.000 Tunnel.

SD-RED-Skalierbarkeit: Sophos Firewalls unterstützen jetzt bis zu 1.000 Site-to-Site-RED-Tunnel und bis zu 650 SD-RED-Geräte.

Sophos DNS Protection

Einfache Sophos DNS Protection

Im letzten Jahr haben wir unseren DNS Protection-Service eingeführt und für alle Firewall-Kunden mit Xstream-Protection-Lizenz kostenlos bereitgestellt. Mit diesem Release wird Sophos DNS Protection noch besser in die Sophos Firewall integriert: Ein neues Control Center Widget zeigt den Dienststatus an und es stehen neue Informationen zur Fehlerbehebung durch Protokollierung und Benachrichtigungen und ein neues geführtes Tutorial zur einfachen Einrichtung von Sophos DNS Protection zur Verfügung.

Optimierte Verwaltung und mehr Benutzerfreundlichkeit

Wie bei jedem Sophos Firewall Release bietet diese Version Verbesserungen im Bereich Benutzerfreundlichkeit und User Experience, die die tägliche Verwaltung erleichtern.

Anpassbare Tabellenspalten: Viele Firewall-Status- und Konfigurationsbildschirme unterstützen jetzt anpassbare Spaltenbreiten, die für nachfolgende Besuche im Browser gespeichert werden. Viele Bildschirme wie SD-WAN, NAT, SSL, Hosts und Services sowie Site-to-Site VPN profitieren von dieser neuen Funktion.

Erweiterte Freitextsuche: SD-WAN-Routen ermöglichen jetzt die Suche nach Routenname, ID, Objekten und Objektwerten wie IP-Adressen, Domänen oder anderen Kriterien. Lokale ZSL-Regeln unterstützen jetzt auch die Suche nach dem Objektnamen und Wert, u. a. auch die inhaltsbasierte Suche.

Standardkonfiguration: Aufgrund der großen Nachfrage wurden die Standard-Firewallregeln und die zuvor beim Einrichten einer Firewall erstellte Regelgruppe entfernt. Während der Ersteinrichtung werden nur die Standard-Netzwerkregel und die MTA-Regeln angegeben. Die Standard-Firewallregelgruppe und die Standard-Gateway-Prüfung für benutzerdefinierte Gateways sind standardmäßig auf „Keine" gesetzt.

Neue Schriftart: Die Benutzeroberfläche der Sophos Firewall verfügt jetzt über eine neue Schriftart, die heller, klarer und schärfer ist und für mehr Lesbarkeit und eine verbesserte Performance sorgen soll.

Weitere Verbesserungen

Virtuelle, Software-, Cloud-Lizenzierung: Alle virtuellen, Software- und Cloud-Lizenzen (BYOL) der Sophos Firewall haben keine RAM-Beschränkungen mehr. Lizenzen sind jetzt streng nach Core-Anzahl begrenzt und unterliegen keinen RAM-Beschränkungen.

Größeres Dateigrößenlimit in WAF: Unterstützt ein konfigurierbares Dateigrößenlimit für Anfragen (Upload) für die Web Application Firewall (WAF), die jetzt Dateien von bis zu 1 GB scannen kann.

Konzipiert für maximale Sicherheit: Wir verbessern die Sicherheit der Sophos Firewall kontinuierlich und fügen in dieser Version Echtzeit-Telemetriedaten hinzu, über die unerwartete Änderungen an wichtigen Betriebssystemdateien mithilfe von Secure-Hash-Validierung sichtbar werden. So können unsere Überwachungsteams potenzielle Sicherheitsvorfälle frühzeitig erkennen, bevor sie zu einem echten Problem werden.

Lockerung der DHCP-Präfixdelegation: Unterstützt jetzt die Präfixe /48 bis /64, wodurch die Interoperabilität mit ISPs verbessert wird. Router Advertisements (RA) und der DHCPv6-Server sind jetzt ebenfalls standardmäßig aktiviert.

Path MTU Discovery: Dadurch werden TLS-Entschlüsselungsfehler behoben, die auf den neuesten ML-KEM (Kyber)-Schlüsselaustausch in Browsern zurückzuführen sind. Die Deep Packet Inspection Engine der Sophos Firewall erkennt und passt die MTU jetzt automatisch an jeden Datenfluss an und gewährleistet eine optimale Performance basierend auf spezifischen Netzwerkbedingungen.

NAT64 (IPv6-to-IPv4-Traffic): NAT64 wird für IPv6 to IPv4 Traffic im expliziten Proxy-Modus unterstützt. In diesem Modus können nur IPv6-Clients auf IPv4-Websites zugreifen. Die Firewall unterstützt auch IPv4 Upstream Proxies für reine IPv6 Clients.

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0
E-Mail: sales@sophos.de

2025-03-31 DE (DD)

SOPHOS