SOPHOS

新闻

Sophos Firewall

Sophos Firewall OS v21.5 的主要新功能

新增的保护与性能

Sophos NDR Essentials 与 Sophos Firewall 的集成

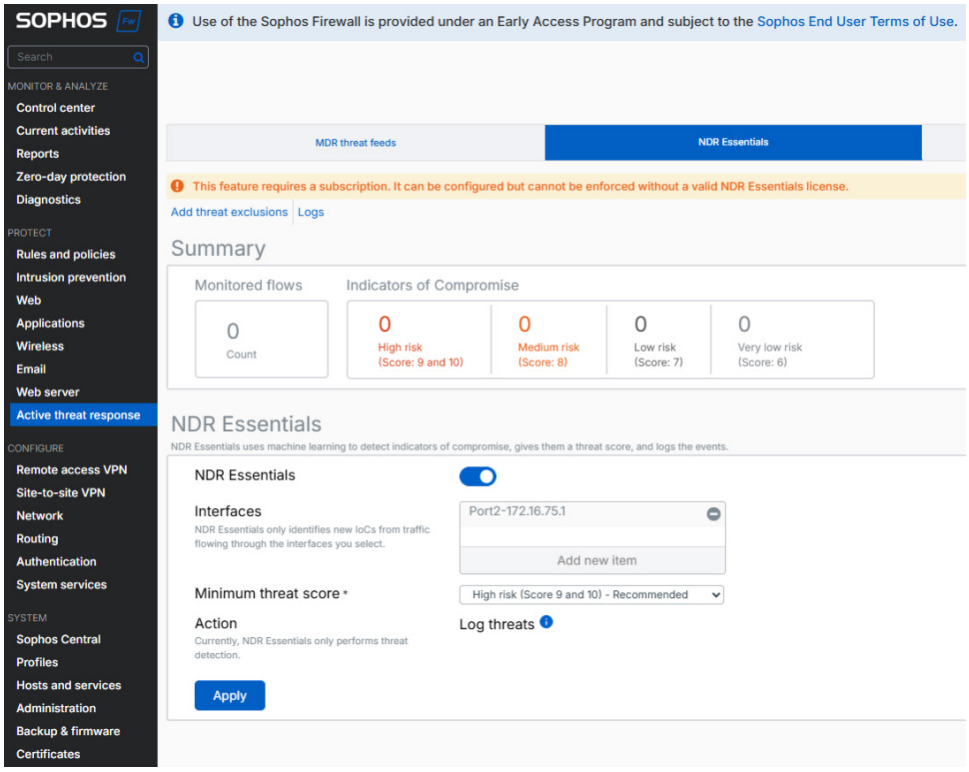
网络侦测与响应 (NDR) 是一类网络安全产品，旨在侦测异常流量行为，以帮助识别网络中操作的主动攻击敌手。技术娴熟的攻击者善于避开侦测，但最终他们需要在网络中横向移动或进行外部通信来执行攻击。NDR 通常部署在网络内部，通过传感器监控和分析网络流量，识别这类可疑活动。

NDR 产品已经问世多年，而 Sophos NDR 自 2023 年初以来已成为我们 MDR/XDR 产品组合的一部分。然而，随着 SFOS v21.5 的发布，我们业界首创将 NDR 与 Sophos Firewall 集成，并无需额外计费即为拥有 Xstream Protection 的 Sophos Firewall 客户提供。

将 NDR 与下一代防火墙集成似乎是理所当然的选择，但挑战在于如何在不影响防火墙性能的前提下实现这一目标。NDR 流量分析需要大量的处理能力。因此，我们采用创新方法，将 NDR 解决方案部署在 Sophos Cloud 中，将高负载任务从防火墙中卸载。

Sophos Firewall v21.5 引入了我们全新的 NDR Essentials 云交付网络侦测与响应平台。它利用最新的 AI 侦测技术，帮助识别主动攻击敌手，并通过 Sophos Firewall 威胁数据源 API 共享这些信息，作为 Active Threat Response 主动威胁响应的一部分，来让您随时掌握侦测结果及其相关风险。

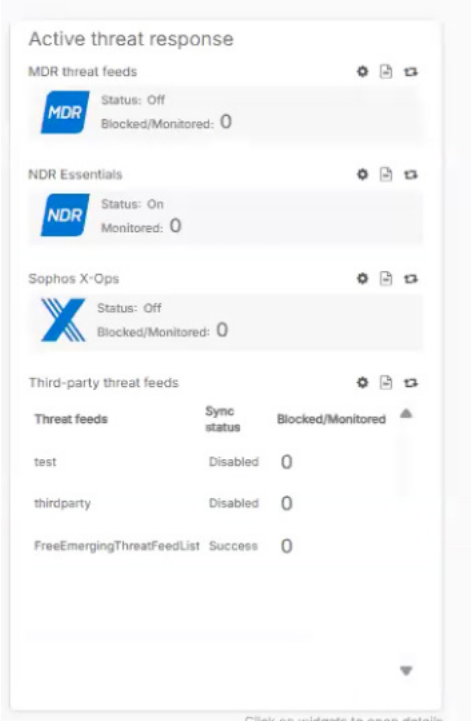
工作方式：Sophos Firewall 捕获来自 TLS 加密流量和 DNS 查询的元数据，并将之发送到 Sophos Cloud 中的 NDR Essentials，数据通过多个 AI 引擎进行分析。它能够在不进行 TLS 解密的情况下，侦测恶意加密负载，以及通过算法生成的新型和异常域名，这些往往是入侵的关键迹象。元数据提取由一个部署在 Xstream FastPath 上的新型轻量级引擎执行，因此仅在 XGS 系列硬件防火墙上提供。虚拟、软件和云防火墙未来可能会获得此 NDR 集成功能，但在 v21.5 版本中尚未提供。



在 Active threat response 下设置并监控您的 NDR Essentials 数据源，与其他威胁数据源一起管理。

新的 NDR Essentials 威胁数据源与其他威胁数据源（如 Sophos X-Ops、MDR 和第三方数据流）在防火墙的 Active Threat Response 区域一起进行管理，如上页屏幕截图所示。设置非常简单：只需切换开关启用它，选择要监控的内部界面，并设置最小的侦测风险阈值——就完成了！

NDR Essentials 的侦测结果范围由 1（低风险）到 10（高风险）。您可以根据您的环境决定触发警报的风险评分阈值。推荐的默认设置是高风险 (9-10)。所有评分大于或等于 6 的侦测结果都会被记录，但只有那些达到或超过您的阈值的侦测结果会触发通知，并在新的 Control Center 控制中心仪表微件中显示为警报。评分低于 6 的侦测结果可能为误报，因此不会被记录为结果。目前 NDR Essentials 侦测事件不会被封锁，但未来可能会加入此选项。所有侦测事件都可透过防火墙本机或 Sophos Central Firewall Reporting 防火墙报告中的 Active Threat Response 报告完整检视。



任何达到或超过您的风险阈值的 NDR Essentials 侦测结果，将显示在修订后的 Control Center 微件中。

如果您希望进一步了解侦测信息和威胁捕猎功能，强烈建议您查看 Sophos 扩展式侦测与响应 (XDR)，其内建完整 Sophos NDR 功能，并搭配全新的 NDR 调查控制台。您还可以考虑我们的 24/7 全天候侦测与响应服务托管式。所有这些产品和服务与您的 Sophos Firewall 协作、相辅相成，发挥更佳的保护效益。

远程访问 VPN SSO

Sophos Connect 客户端和 VPN 门户的 Entra ID (Azure AD) 单点登录

这是最受期待的功能之一，它简化了远程访问 VPN，让用户透过公司网络凭证登录 Sophos Connect 客户端与防火墙的 VPN 门户。Entra ID (Azure AD) 与 Sophos Connect 客户端和 VPN 门户的单点登录整合，现已包含在 SFOS v21.5 中。它通过行业标准的 OAuth 2.0 和 OpenID Connect 协议提供云原生集成，实现无缝体验。支持 Microsoft Windows 上的 Sophos Connect 客户端 2.4 及更高版本。

其他 VPN 和可扩展性增强

用户界面和可用性改进：连接类型名称已从“站对站”（site-to-site）重命名为“基于政策”（policy-based）；隧道接口已重命名为“基于路由”（route-based），使其更加直观易懂。

改进的 IP 租赁池验证：跨 SSLVPN、IPsec、L2TP 和 PPTP 远程访问 VPN，消除潜在的 IP 冲突。

严格的配置文件强制执行：对排除默认值的 IPsec 配置文件进行强制执行，确保成功的协商，消除潜在的封包碎裂和隧道无法妥当建立的情况。

基于路由的 VPN 可扩展性：基于路由的 VPN 容量翻倍，支持最多 3,000 个隧道。

SD-RED 可扩展性：Sophos Firewall 现在支持多达 1,000 个站对站的 RED 隧道和多达 650 个 SD-RED 设备。

Sophos DNS Protection

轻松使用 Sophos DNS Protection

去年，我们推出了 DNS Protection 服务，并为所有拥有 Xstream Protection 授权许可证的防火墙客户免费提供。通过此次发布，Sophos DNS Protection 进一步与 Sophos Firewall 集成，新增了用于指示服务状态的 control center 微件；并通过日志和通知提供新的故障排除洞察，还推出了一个新的引导教程，帮助用户轻松设置 Sophos DNS Protection。

简化管理和增强用户体验

与每个 Sophos Firewall 发布一样，这版本包含多个用户体验改进，使日常管理变得更加简便。

可调整大小的表格列：一直备受期待的功能，许多防火墙状态和配置屏幕现在支持可调整列宽，并且列宽会保存在浏览器内存中，方便下次访问时使用。诸如 SD-WAN、NAT、SSL、主机与服务、站对站 VPN 等多个屏幕均从这一新功能中获益。

扩展的自由文本搜索：SD-WAN 路由现在支持按路由名称、ID、对象、和对象值（如 IP 地址、域名或其他标准）进行搜索。本地 ACL 规则现在也支持按对象名称和值进行搜索，包括基于内容的搜索。

默认配置：应广泛需求，之前在设置新防火墙时创建的默认防火墙规则和规则组已被移除，仅在初始设置过程中提供默认网络规则和 MTA 规则。默认防火墙规则组和自定义网关的默认网关探测均设置为“无”。

新字体：Sophos Firewall 的用户界面现在采用了一种全新的字体，更加简洁、清晰，提升可读性并优化性能。

其他增强功能

虚拟、软件、云授权许可：所有 Sophos Firewall 的虚拟、软件和云授权许可证 (BYOL) 不再有 RAM 限制。授权许可证现在仅依据 CPU 核心数严格限制，没有内存限制。

WAF 中更大的文件大小限制：为 Web 应用程序防火墙 (WAF) 支持可配置请求（上传）文件大小限制，现在可以扫描最大 1 GB 的文件。

精心设计，成就安全：我们持续改进 Sophos Firewall 的安全性，在本次发布中，加入了实时遥测收集功能，通过安全哈希验证标记核心操作系统文件的任何未预期的更改。这将帮助我们的监控团队在问题发生之前主动识别潜在的安全事件，及时发现并避免问题的发生。

DHCP 前缀委派放宽：现在支持 /48 到 /64 的前缀，提高与 ISP 的互操作性。Router Advertisements (RA) 和 DHCPv6 服务器也默认启用。

路径 MTU 发现：此功能将解决由于浏览器中支持最新的 ML-KEM (Kyber) 密钥交换导致的 TLS 解密错误。Sophos Firewall 的深度数据包检查引擎现在会自动侦测并调整每个流的 MTU，确保根据特定网络条件实现最佳性能。

NAT64（IPv6 到 IPv4 流量）：在显式代理模式下，NAT64 支持 IPv6 到 IPv4 的流量。此模式下，仅 IPv6 的客户端可以访问 IPv4 网站。防火墙还为仅 IPv6 的客户端支持 IPv4 上游代理。

中国（大陆地区）销售咨询
电子邮件：salescn@sophos.com

2025-03-31 ZHCN (DD)

SOPHOS