

SOPHOS
Cybersecurity delivered.

Sophos Firewall

解决方案概要



目录

Sophos防火墙	2
暴露隐藏风险	3
控制中心	3
Xstream TLS 检查	6
Synchronized Application Control 同步应用程序控制	7
高风险用户	8
灵活的报告方式	9
阻止未知威胁	10
Xstream 防护和性能	10
零日威胁防护	11
静态机器学习分析	12
动态运行时沙箱分析	13
威胁防护报告	14
统一规则管理	15
管理安全一览	16
企业级安全 Web 网关	17
教育功能	18
简化 NAT 配置	19
自动应对事件	20
Security Heartbeat安全心跳	20
这是一个零信任的世界	22
优化您的 SD-WAN 网络	23
Xstream SD-WAN	23
Xstream FastPath 加速 SD-WAN VPN 流量	26
SD-分支办公室连接性	27
VPN 支持与协作	29
应用程序可见性与路由	30
将 Sophos Firewall 加入任何网络 – 简单	32

Sophos 防火墙

Sophos Firewall 设计伊始旨在解决现有防火墙的当前主要问题,同时提供一个真正的下一代平台,应对现代加密互联网和不断发展的威胁局面。Sophos Firewall 带来识别隐藏风险,防御威胁,应对事件同时提供最优性能的新方式。用于 Sophos Firewall 的 Xstream 架构采用数据包处理架构,实现极高可见性、防护和性能。

Sophos Firewall 提供高风险用户、有害应用程序、可疑载荷和持续威胁的无人能及的可见性。紧密集成全套现代威胁防护技术,方便设置和维护。和传统防火墙不同,Sophos Firewall 能够与网络上的其他安全系统通信,从而成为您可以信任的实施点,自动实时隔离威胁,并阻止恶意软件传播或数据渗透出网络。

Sophos Firewall 相比其他网络防火墙具有四个重要优势:

1. **暴露隐藏风险** - Sophos Firewall 在暴露隐藏风险方面比其他解决方案做的好很多,提供可视仪表盘、丰富的现场和云报告以及独有风险信息。
2. **阻止未知威胁** - Sophos Firewall 利用一整套非常容易设置和管理的高级防护功能,比其他防火墙更快更容易更有效阻止未知威胁。
3. **自动应对事件** - 采用 Synchronized Security 的 Sophos Firewall 利用 Sophos Security Heartbeat™ 在端点与防火墙之间共享实时情报,自动应对网络上的事件。
4. **优化 SD-WAN 网络** - Sophos Firewall 的 Xstream SD-WAN 功能只需指向单击,即可设置复杂的 SD-WAN 重叠网络。您还可以利用自动基于性能的 WAN 链接选择,以及链接之间即时零影响切换,优化您的应用程序性能、网络弹性和业务连续性,同时降低连接成本。

暴露隐藏风险

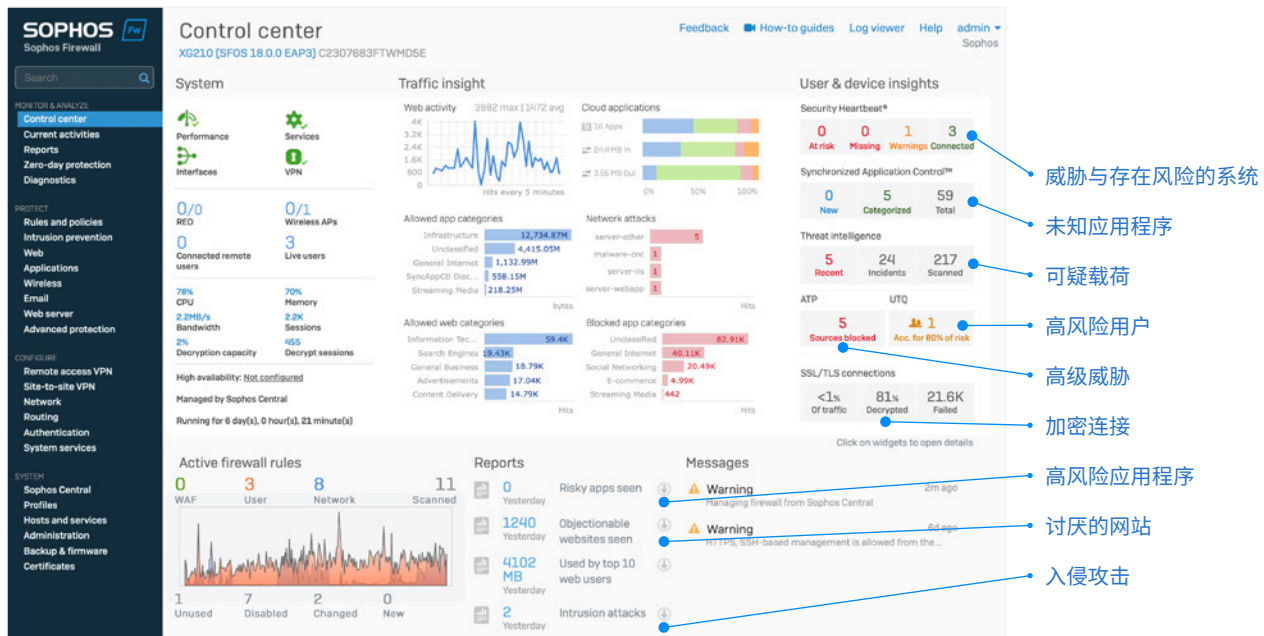
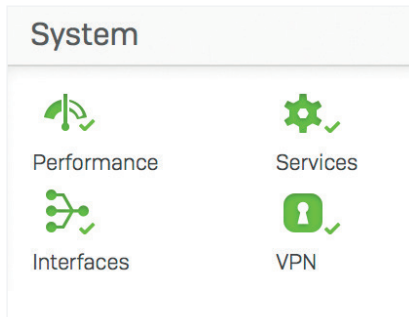
现代防火墙解析收集的海量信息,与数据关联,仅突出需要采取措施的最重要信息非常重要 - 最好不要为时已晚。

控制中心

Sophos Firewall 的控制中心为网络上的活动、风险和威胁提供前所未有的可见性。

利用“信号灯”式指示灯吸引您注意最重要的内容。

如果亮红灯,需要立刻注意。黄灯表示潜在问题。如果亮绿灯,无需其他操作。



The screenshot shows the Sophos Firewall Control Center interface. The dashboard is divided into several sections:

- System:** Overview of system health and configuration.
- Traffic insight:** Graphs showing web activity and network attacks.
- User & device insights:** Security heartbeat, synchronized application control, threat intelligence, and ATP (Advanced Threat Protection) status.
- Active firewall rules:** Overview of WAF, User, Network, and Scanned rules.
- Reports:** Summary of risky apps, objectionable websites, top 10 web users, and intrusion attacks.
- Messages:** Recent alerts and warnings.

Annotations in Chinese point to specific data points:

- 威胁与存在风险的系统 (Threats and systems at risk) - points to the Security Heartbeat section.
- 未知应用程序 (Unknown applications) - points to the Synchronized Application Control section.
- 可疑载荷 (Suspicious payloads) - points to the Threat Intelligence section.
- 高风险用户 (High-risk users) - points to the ATP section.
- 高级威胁 (Advanced threats) - points to the ATP section.
- 加密连接 (Encrypted connections) - points to the SSL/TLS connections section.
- 高风险应用程序 (High-risk applications) - points to the Reports section.
- 讨厌的网站 (Disliked websites) - points to the Reports section.
- 入侵攻击 (Intrusion attacks) - points to the Reports section.

控制中心的每个小工具提供额外信息,单击小工具即可轻松显示。例如,单击控制中心的“接口”小工具,可以轻松获得设备上的接口状态。

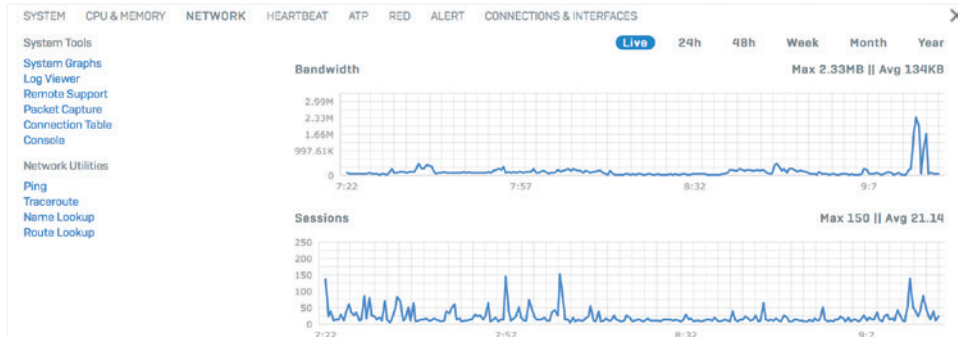
INTERFACE	TYPE	STATUS	RECEIVED KBITS/S	TRANSMITTED KBITS/S
IoT_Bridge	Bridge-pair	Connected	1.98	0.62
Port1	Physical	Connected, 1000 Mbps - Full Duplex	183.91	864.02
Port2	Physical	Connected, 1000 Mbps - Full Duplex	925.65	178.26
Port7	Physical	Unplugged	0.00	0.00
Port8	Physical	Disabled	0.00	0.00

GATEWAY NAME	GATEWAY IP	INTERFACE	TYPE	WEIGHT	STATUS
BACKUP_WAN	128.0.0.1	Port7	Active	1	●
DHCP_Port2_GW	50.68.180.1	Port2	Active	1	●

单击仪表板的 ATP (高级威胁防护) 小工具, 可以轻松确定高级威胁的主机、用户和来源。

HOSTNAME, IP	THREAT	COUNT
● Mac Server 10.0.1.10	C2/Generic-A /Users/Chris/Desktop/MacBadActor.app/Contents/MacOS/MacBadActor	2

系统图还显示性能时间图, 提供可选择的时间范围, 无论您是要查看最近两小时还是上个月或去年的信息。还提供常用故障排除工具的快捷方式以解决潜在问题。



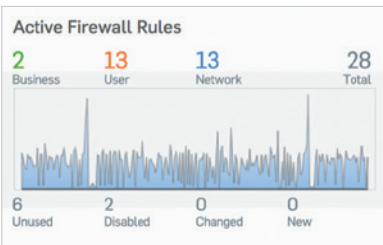
在每个屏幕单击一下, 都可以访问在线日志查看工具。您可以在新窗口中打开, 这样可以在控制台上工作的同时留意相关日志。提供两种视图, 一种较简单, 基于列按防火墙模块划分的格式, 一种是更详细的统一视图, 提供强大的筛选和排序选项, 将系统中的日志聚集在一个实时视图中。

Time	Log Comp	Action	Username	Firewall Rule	In Interface	Out Interface	Source IP	Destination IP	Rule Type	Message ID	Live PCAP	Message
2017-11-29 09:48:16	Invalid Traffic	Denied		0	Port2		23.45.114.117	50.68.180.222	0	01001	Open PCAP	Could not associate packet to any connection
2017-11-29 09:48:14	Firewall Rule	Allowed	mindy	4	Port1	Port2	10.0.1.52	64.58.144.92	2	00001	Open PCAP	
2017-11-29 09:48:13	Firewall Rule	Allowed	chris	4	Port1		10.0.1.15	34.200.43.40	2	00001	Open PCAP	
2017-11-29 09:48:13	Firewall Rule	Allowed		10	Port3	Port2	192.168.1.10	54.87.88.218	1	00001	Open PCAP	
2017-11-29 09:48:12	Firewall Rule	Allowed		10	Port6	Port2	192.168.1.11	12.148.218.73	1	00001	Open PCAP	
2017-11-29 09:48:08	Firewall Rule	Allowed	chris	4	Port1		10.0.1.15	54.186.179.15	2	00001	Open PCAP	
2017-11-29 09:48:03	Firewall Rule	Allowed	chris	4	Port1		10.0.1.15	23.45.114.117	2	00001	Open PCAP	
2017-11-29 09:48:03	Firewall Rule	Allowed	chris	4	Port1		10.0.1.15	23.45.114.117	2	00001	Open PCAP	
2017-11-29 09:48:02	Firewall Rule	Allowed		10	Port3	Port2	192.168.1.10	54.87.88.218	1	00001	Open PCAP	
2017-11-29	Firewall	Allowed	chris	4	Port1	Port2	10.0.1.15	64.58.144.92	2	00001	Open PCAP	

如果您和大多数网络管理员一样，您可能想知道防火墙规则是不是太多，哪些是真正需要的，哪些是实际用不到的。有了 Sophos Firewall，您再也不用考虑这些。

2017-11-29 08:44:30	messageid="01001" log_type="Firewall" log_component="Invalid Traffic" log_subtype="Denied" status="Deny" con_duration="0" fw_rule_id="0" policy_type="0" user="user_group" web_policy_id="0" ips_policy_id="0" appfilter_policy_id="0" app_name="app_risk="0" app_technology="app_category=" in_interface="Port1" out_interface="src_mac="fc0f24200c0f8" src_ip="100.115" src_country=" dst_ip="38.127.227.137" dst_country=" protocol="TCP" src_port="82791" dst_port="443" packets_sent="0" packets_received="0" bytes_sent="0" bytes_received="0" src_trans_ip=" src_trans_port="0" dst_trans_ip=" dst_trans_port="0" src_zone=" src_zone=" dst_zone=" dst_zone=" con_direction=" con_id=" virt_con_id=" hb_status="No Heartbeat" message="Could not associate packet to any connection" appresolvedby="Signature"
2017-11-29 08:44:27	messageid="01001" log_type="Firewall" log_component="Invalid Traffic" log_subtype="Denied" status="Deny" con_duration="0" fw_rule_id="0" policy_type="0" user="user_group" web_policy_id="0" ips_policy_id="0" appfilter_policy_id="0" app_name="app_risk="0" app_technology="app_category=" in_interface="Port1" out_interface="src_mac="fc0f24200c0f8" src_ip="100.115" src_country=" dst_ip="38.127.227.137" dst_country=" protocol="TCP" src_port="82791" dst_port="443" packets_sent="0" packets_received="0" bytes_sent="0" bytes_received="0" src_trans_ip=" src_trans_port="0" dst_trans_ip=" dst_trans_port="0" src_zone=" src_zone=" dst_zone=" dst_zone=" con_direction=" con_id=" virt_con_id=" hb_status="No Heartbeat" message="Could not associate packet to any connection" appresolvedby="Signature"
2017-11-29 08:44:25	messageid="01001" log_type="Firewall" log_component="Invalid Traffic" log_subtype="Denied" status="Deny" con_duration="0" fw_rule_id="0" policy_type="0" user="user_group" web_policy_id="0" ips_policy_id="0" appfilter_policy_id="0" app_name="app_risk="0" app_technology="app_category=" in_interface="Port1" out_interface="src_mac="fc0f24200c0f8" src_ip="100.115" src_country=" dst_ip="38.127.227.137" dst_country=" protocol="TCP" src_port="82791" dst_port="443" packets_sent="0" packets_received="0" bytes_sent="0" bytes_received="0" src_trans_ip=" src_trans_port="0" dst_trans_ip=" dst_trans_port="0" src_zone=" src_zone=" dst_zone=" dst_zone=" con_direction=" con_id=" virt_con_id=" hb_status="No Heartbeat" message="Could not associate packet to any connection" appresolvedby="Signature"
2017-11-29 08:44:22	messageid="01001" log_type="Firewall" log_component="Invalid Traffic" log_subtype="Denied" status="Deny" con_duration="0" fw_rule_id="0" policy_type="0" user="user_group" web_policy_id="0" ips_policy_id="0" appfilter_policy_id="0" app_name="app_risk="0" app_technology="app_category=" in_interface="Port1" out_interface="src_mac="fc0f24200c0f8" src_ip="100.115" src_country=" dst_ip="38.127.227.137" dst_country=" protocol="TCP" src_port="82791" dst_port="443" packets_sent="0" packets_received="0" bytes_sent="0" bytes_received="0" src_trans_ip=" src_trans_port="0" dst_trans_ip=" dst_trans_port="0" src_zone=" src_zone=" dst_zone=" dst_zone=" con_direction=" con_id=" virt_con_id=" hb_status="No Heartbeat" message="Could not associate packet to any connection" appresolvedby="Signature"
2017-11-29 08:44:19	messageid="01001" log_type="Firewall" log_component="Invalid Traffic" log_subtype="Denied" status="Deny" con_duration="0" fw_rule_id="0" policy_type="0" user="user_group" web_policy_id="0" ips_policy_id="0" appfilter_policy_id="0" app_name="app_risk="0" app_technology="app_category=" in_interface="Port1" out_interface="src_mac="fc0f24200c0f8" src_ip="100.115" src_country=" dst_ip="38.127.227.137" dst_country=" protocol="TCP" src_port="82791" dst_port="443" packets_sent="0" packets_received="0" bytes_sent="0" bytes_received="0" src_trans_ip=" src_trans_port="0" dst_trans_ip=" dst_trans_port="0" src_zone=" src_zone=" dst_zone=" dst_zone=" con_direction=" con_id=" virt_con_id=" hb_status="No Heartbeat" message="Could not associate packet to any connection" appresolvedby="Signature"

主动防火墙规则小工具按规则类型实时显示防火墙处理的流量图：企业应用程序、用户和网络规则。还按状态显示活跃规则计数，包括未使用的规则，这样您就可以进行整理。和控制中心的其他区域一样，单击任意部分将向下钻取，在此情况下，可以钻取到按规则类型或状态排序的防火墙规则表。



Xstream TLS 检查

围绕加密流量正在酝酿一场完美风暴。据 Google 称，网络上的加密流量数量已经增长至超过 90%。这给了网络罪犯机会发动隐蔽且难以发现的攻击。毕竟，您无法阻止看不到的攻击。遗憾的是，大多数企业对此无能为力，因为他们当前的防火墙缺乏必要性能，无法在不显著减慢速度的前提下进行 TLS/SSL 检查。

Sophos Firewall 采用新的 Xstream SSL 检查引擎，能够显著提高并发连接容量，提供灵活的政策工具，就应该扫描以及可以扫描哪些内容制定智能决策，并在必要时卸荷。企业可以使用 SSL 政策工具，创建与无法解密的流量、证书、协议、加密执行方法等有关的企业级 TLS/SSL 政策。Sophos Firewall 在系统的所有端口和应用程序上支持 TLS 1.3 和所有现代加密套件。

仪表板提供的其他工具支持管理员清晰了解网络流量的加密数量，以及应对方法。Sophos Firewall 在暴露这些信息方面比其他解决方案做的好很多，尤其是突出因证书验证或不支持最新加密标准的网站而遇到的错误。



Sophos Firewall 从控制中心提供加密流量以及 TLS 检查产生的任何问题的信息

管理员还可以弹出详细窗口，准确了解存在问题的站点和原因，以及遇到问题的用户。他们可以在这里直接采取措施，禁止应用程序或网站解密以避免更多问题。任何其他 SSL 检查解决方案都无法提供这种程度的信息。

Synchronized Application Control 同步应用程序控制

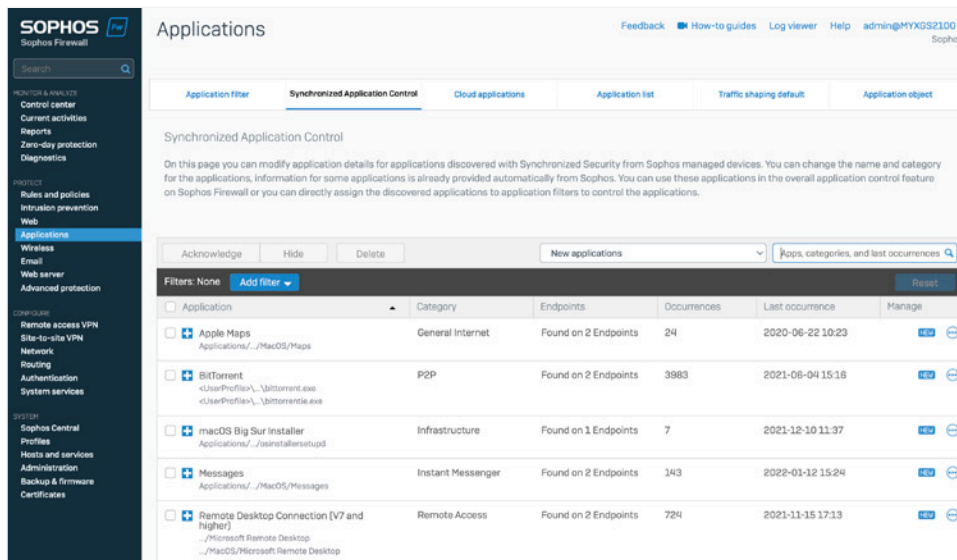
现在下一代防火墙中的应用程序控制存在一个问题，大多数应用程序流量不被识别：要么未分类，要么标记为未知、普通 HTTP 或普通 HTTPS。

理由很简单：所有防火墙应用程序控制引擎依赖特征码和模式识别应用程序。您可能猜到了，自定义垂直市场应用程序（如医疗和金融应用程序）从来都没有特征码。其他善于回避的应用程序（如 BitTorrent 客户端和 VoIP）以及通讯应用程序不断改变其行为和特征码以回避检测与控制。许多应用程序现在利用加密避开检测，其他应用程序则使用类似普通 Web 浏览器的连接穿过防火墙通信，因为大多数防火墙通常不阻止端口 80 和 443。

结果是完全缺乏对网络上应用程序的可见性，而您无法控制看不到的内容。对此的解决方案非常简单但有效：Sophos 同步应用程序控制，利用我们独有的与 Sophos 托管端点的 Synchronized Security 连接。

工作方式如下。当 Sophos Firewall 发现应用程序流量，并且无法通过特征码识别时，将询问端点哪个应用程序生成该流量。

Synchronized Application Control™



可以自动或手动分类 Synchronized Application Control 发现的未知应用程序。

然后端点可以分享可执行文件、路径和类别，将这些信息传送回防火墙。在大多数情况下，防火墙可以利用这些信息自动分类和控制应用程序。

如果 Sophos Firewall 无法自动确定合适的应用程序类别, 管理员可以设置所需类别或者为应用程序分配现有政策。

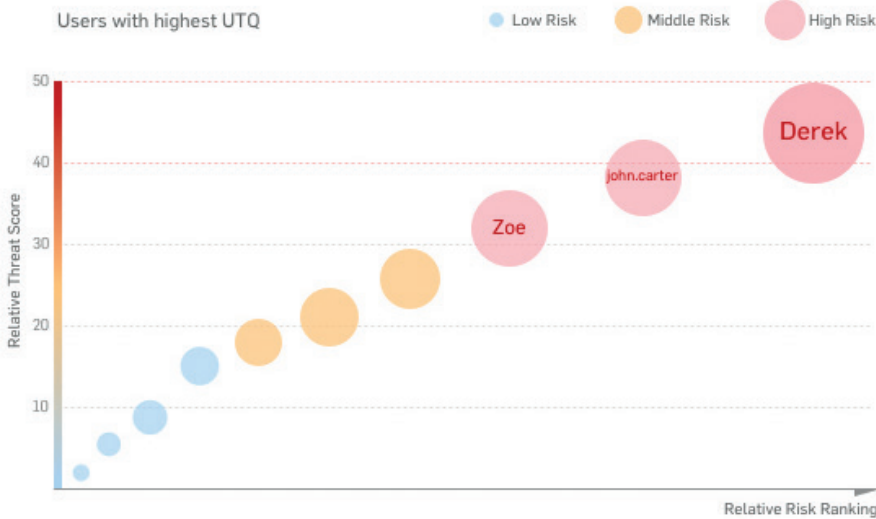
分类应用程序后, 自动或者由网络管理员分配, 应用程序受到和该类别所有其他应用程序相同的政策控制, 非常方便阻止您不需要的所有未识别应用程序, 优先安排您需要的应用程序。

同步应用程序控制是应用程序可见性和控制的突破, 提供网络上使用的所有应用程序的绝对透明度, 包括以前未识别或不受控制的应用程序。

高风险用户

研究证明, 用户是安全防护链中最薄弱的环节。好消息是, 我们可以分析并利用人类行为模式预测和阻止攻击。此外, 使用模式有助于说明企业资源的利用效率, 以及是否需要微调用户政策。

Sophos 用户威胁系数 (UTQ) 帮助安全管理员根据可疑 Web 行为和威胁以及感染历史, 发现存在风险的用户。用户的高 UTQ 风险分数可能说明用户缺乏安全意识导致非预期操作、恶意软件感染或有意欺诈行为。

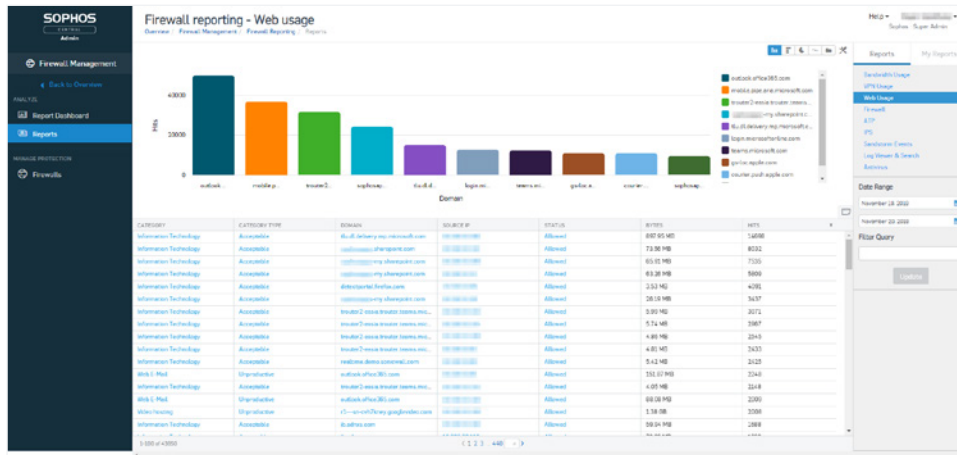


Sophos Firewall 在概览中突出显示最高风险用户。

了解导致风险的用户和活动可以帮助网络安全管理员采取必要措施, 教育高风险用户或实施更严格或更合适的政策以控制用户行为。

灵活的报告方式

Sophos Firewall 在 NGFW 和 UTM 产品中独一无二，提供灵活的云和现场报告方式，可高度定制，无需额外费用。Sophos Central Firewall Reporting (CFR) 为企业提供通过分析获得的更深入网络活动信息。CFR 具有丰富的内置报告和用于创建数百种报告的工具，可以提供关于用户行为、应用程序使用、安全事件等的可操作情报。交互式报告和概览报告仪表盘支持管理员在 Sophos Central 帐户中存储的 syslog 中向下钻取，以可视化格式呈现精细视图以方便理解。然后可以分析数据寻找趋势，发现安全状态的漏洞，突出可能需要改变的政策。



Sophos Firewall 提供丰富的现场和中央云报告选项。

Sophos Firewall 还提供现场报告。从丰富的报告中选择，报告按类型方便组织，并提供多个内置仪表盘。防火墙的所有区域提供数百个具有可自定义参数的报告，包括流量活动、安全、用户、应用程序、Web、联网、威胁、VPN、电子邮件和合规性。您可以轻松计划定期将报告通过电子邮件发送给您或指定收件人，将报告保存为 HTML、PDF 或 CSV 格式。

阻止未知威胁

防御最新网络威胁需要所有技术在一个指挥家 - 网络管理员 - 的指挥下, 像交响乐团一样工作。遗憾的是, 大多数防火墙产品更像一个人的乐队在耍杂耍, 防火墙规则设置在一个区域, Web 政策在另一个区域, SSL 检查在第三个区域, 应用程序控制在第四个区域。

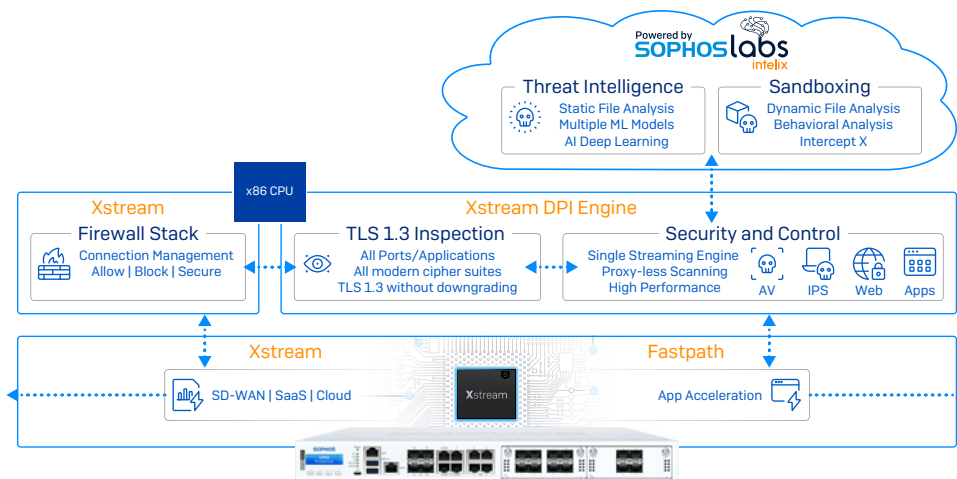
而在 Sophos, 我们不仅认为您需要最先进的防护技术, 而且需要能够简单配置部署和进行日常管理, 因为错误配置的防护通常比没有保护更糟糕。

对简单性的承诺一直是 Sophos DNA 的重要部分。更重要的是, Sophos 罕见地愿意支持改动, 采取必要的不同举措以提供更好的防护和更好的用户体验。

Sophos Firewall 的一些不同方式带来了巨大区别。

Xstream 防护和性能

开启保证网络安全不受威胁影响的安全功能后, 防火墙性能减慢。Sophos Firewall 的 Xstream 数据包处理架构的一个核心部分是高速深度数据包检查 (DPI) 引擎。DPI 引擎为 IPS、Web、AV 和应用程序控制以及 Xstream SSL 检查提供免代理一次性安全扫描。



Sophos Firewall 的 Xstream 架构和可编程 Xstream Flow Processors 提供强大的保护和性能。

建立新连接后, 防火墙堆栈进行处理, 做出允许、阻止或扫描流量威胁的决定。如果流量需要安全扫描, 将把数据包转发至免代理高性能流处理 DPI 引擎, 由后者扫描数据包, 即使已经加密。这仅用于最初的少数几个数据包。之后, 防火墙堆栈不再查收, 将处理完全交给 DPI 引擎, 这样限制改善延迟和性能。

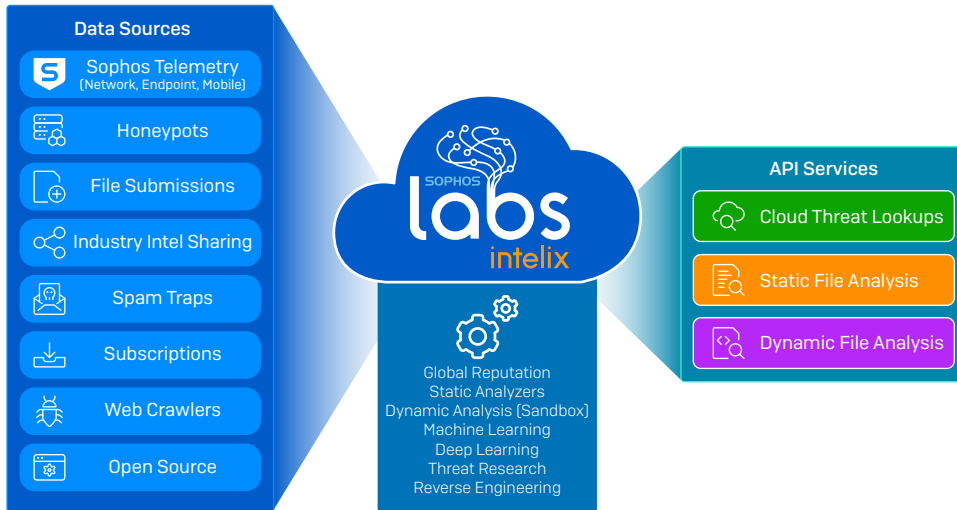
如果流视为安全, 不再需要进一步检查, DPI 引擎可以将工作流完全交给 Sophos Network Flow FastPath, 由后者为受信任流量提供加速通道。这样释放其他资源, 不再用于检查不需要的流量, 从而显著提升性能。

零日威胁防护

随着勒索软件等高级威胁越来越有针对性和回避性，迫切需要预测性零日威胁识别和防护功能。最终解决方案包括两层：

1. **静态机器学习分析** – 通过多个人工神经网络机器学习模型提供预测性分析和侦测，同时配备全局信誉和深度文件扫描，完全无需实时执行文件。
2. **动态运行时沙箱分析** – 在对文件活动具有无与伦比可见性的云沙箱环境中实时引爆恶意软件，揭露未知威胁的本性和功能。

Sophos Firewall 提供由 SophosLabs Intelix 支持的这两个重要防护技术。SophosLabs 是我们备受赞誉的 1 级网络安全威胁研究实验室，开发了 SophosLabs Intelix 中的终极威胁分析和智能平台。利用最新机器学习技术，数十年威胁研究，以及海量情报，提供针对前所未见的最新威胁的防护，效果无人能及。



Sophos Firewall 的零日防护由 SophosLabs Intelix 机器学习分析提供支持。

Sophos Firewall Xstream DPI 引擎对进入网络的文件执行 AV 分析，并确定存在活跃代码后，将暂时扣留文件，将文件发送至云端的 SophosLabs Intelix 服务，进行静态和动态文件分析。然后通过 Sophos Firewall 控制中心的威胁情报小工具和(下面的)可单击报告显示结果摘要，仅当文件清理干净后，才会发送到下载者或电子邮件收件人。

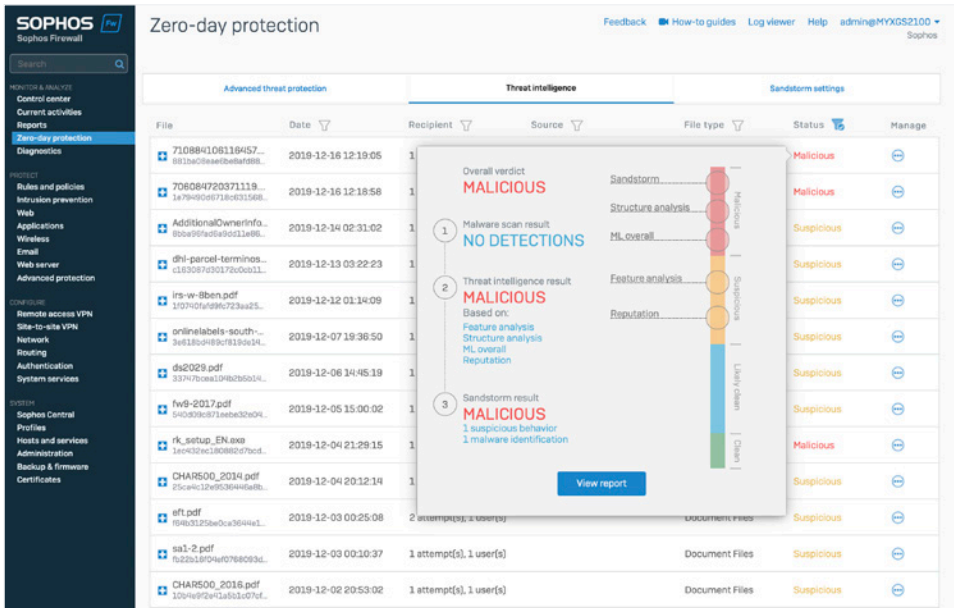
最后一部分很重要，许多防火墙高级恶意软件解决方案往往在完成分析前将文件发送给最终用户，如果文件最终被确定为威胁，可能给清理带来麻烦，增加成本。

Threat intelligence

5
Recent

24
Incidents

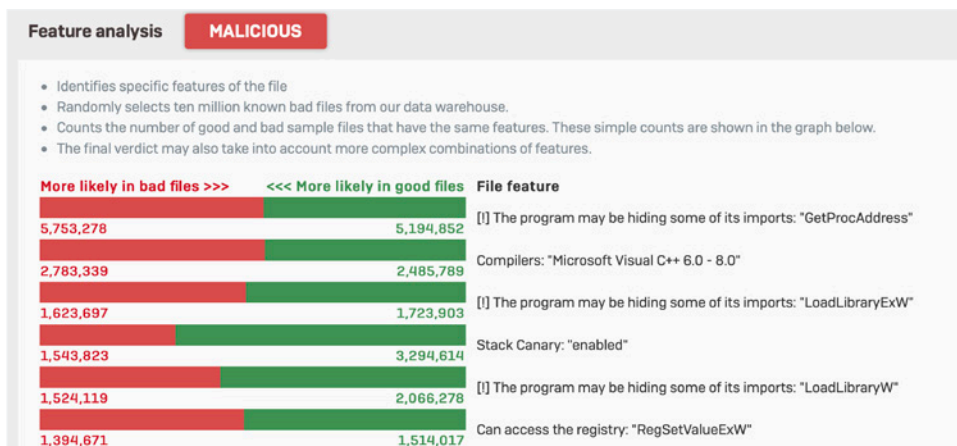
217
Scanned



Sophos Firewall 的零日防护识别以前没有见过的新威胁, 防止其进入网络。

静态机器学习分析

静态文件分析利用多个机器学习模型, 分析文件的各个特征、特性、起源和信誉要素, 并与 SophosLabs 数据库中数以百万的已知好文件和坏文件对比, 在数秒内对任何从未见过的新文件得出判断。识别新威胁和现有威胁变种的速度和效率极高, 尤其是不方便进行沙箱处理的威胁, 如含有恶意软件并受密码保护的文档。



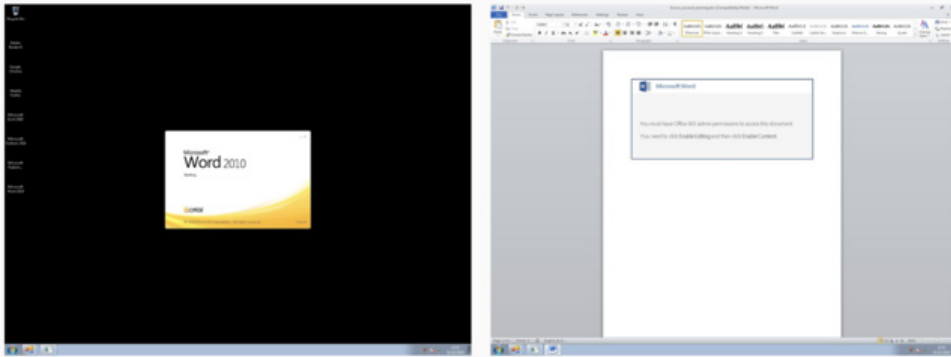
利用多个机器学习模型分析可疑文件的零日威胁。

动态运行时沙箱分析

沙箱技术最初问世时,只有最大型企业能够承担得起费用。但现在,借助 Sophos Sandstorm 等云沙箱解决方案,即使最小的企业也可以负担得起。中小型企业首次获得采用深度学习技术的沙箱,功能远胜于几年前企业用数百万美元部署的专用现场沙箱解决方案。

由于基于云技术,无需额外软件或硬件,并且不影响防火墙性能。Xstream DPI 引擎确定包含活跃代码的任何文件,如电子邮件附件或 Web 下载,将自动上传到 SophosLabs Intelix 云沙箱并引爆,同时进行静态分析(上文)以确定其运行时行为,之后才允许其进入您的网络。

为了识别威胁,SophosLabs 将行业领先的 Intercept X 下一代端点产品的最新防护集成集成在 Sophos Sandstorm 中,包括深度学习、漏洞攻击检测和 CryptoGuard (实时侦测活跃勒索软件加密文件的行为)。还可监视所有文件、内存、注册表和网络活动的恶意意图特征,作出判断。其他防火墙无法提供这种具有全球最佳威胁防护能力 – Intercept X 的实时分析,也不具备 Sophos Firewall 的可见性和报告水平 – 包括文件运行时发现内容的全套屏幕截图。



沙箱运行时分析在安全环境中引爆文件,确定行为,并提供屏幕截图供您检查。

沙箱对于发现没有任何明显恶意特征的通常良性文件中潜伏的威胁非常有效。带有宏的 Office 文件,或者被篡改的良性可执行文件或应用程序更新。

威胁防护报告

Sophos Firewall 分析的所有文件附带一个报告, 提供各种分析结果和判断的完整详细信息。报告具有 6 个不同要素, 包括各种机器学习分析、文件信誉、沙箱甚至第三方 VirusTotal 数据。

Investigation and actions


[drive]\[redacted]\file.exe

Blocked 5 times for 3 users. [Source details](#)

Time of analysis
 Static: 2019-07-26 21:09:08
 Sandstorm: 2019-04-16 17:40:58

Overall verdict

MALICIOUS



Analysis summary

MALICIOUS	MALICIOUS	MALICIOUS	SUSPICIOUS	NOT DETECTED	9/71	None
Machine learning Overall analysis	Machine learning File features	Machine learning File structure	File reputation	Sandstorm	VirusTotal detections	XG malware scan

Information about your file

File name [drive]\[redacted]\file.exe
 File type application/x-dosexec
 SHA1 41b68b777b6fd365e72f1344ae29fcdaf2f2e9af
 SHA256 6f14a34560d2076523ae95aee66b126d363d552730459399a9cb3d9a4f2172086
 File size 10,096,640 bytes
[All details](#)

Machine learning

MALICIOUS

Overall verdict based on the Sophos deep learning model

Our model identifies many attributes of the file and compares their occurrence, individually and in different combinations, with millions of known good and known malware samples. The reports below show probabilities based on key components of the overall score. Each component isn't a strong indicator on its own but, in combination, they provide a critical insight. This model identifies many different characteristics of your file and compares the occurrence of those characteristics, individually and in combinations, across millions of known good and known malware samples.

Feature analysis

- Identifies specific features of the file.
- Randomly selects one million (out of **2,906,531**) known good and one million (out of **20,045,125**) known bad files.
- Counts the number of good and bad sample files that have the same features. These simple counts are shown in the graph below.
- The verdict may also take into account more complex combinations of features
- This test rates **file.exe** as **MALICIOUS**.

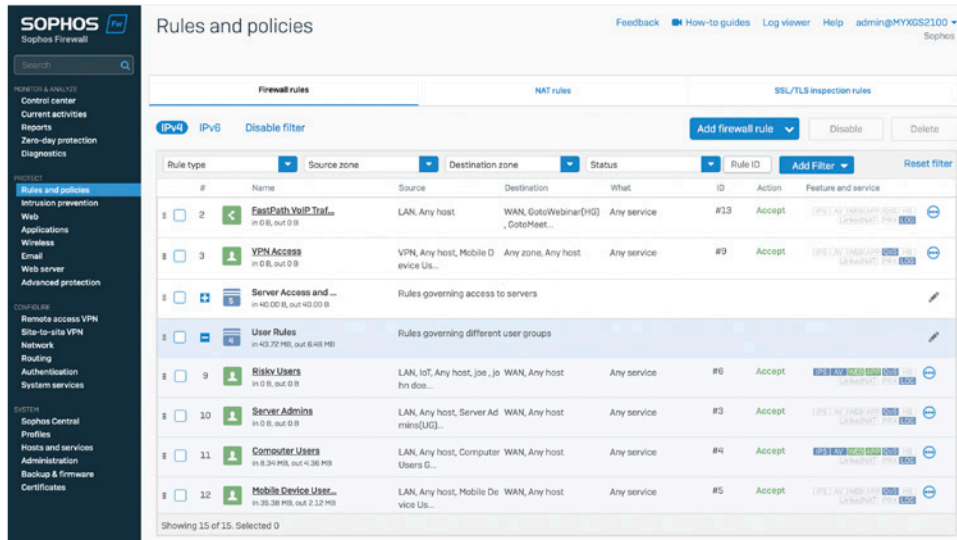
More likely in bad files	<<< More likely in good files	File feature
6,747	5,292	Can access the registry: "RegDeleteKeyW"
30,962	31,332	[!] The program may be hiding some of its imports: "GetProcAddress"
23,868	22,093	[!] The program may be hiding some of its imports: "LoadLibraryA"
48,199	49,165	Stack Canary: "disabled"
122	30	Packer: "Unusual section name found: .vmp0"
108	24	Packer: "Unusual section name found: .vmp1"

Feature combinations

统一规则管理

管理防火墙是一个充满挑战的工作。多个规则、政策和安全设置分布在各种功能区域，并且往往需要多个不同规则来提供所需防护，要做大量的工作。

利用 Sophos Firewall，我们有机会完全重新思考防火墙规则的组织方式以及管理安全状态的方式。无需在控制台上寻找合适政策，我们将所有防火墙规则和实施管理收集在一个统一屏幕中。您可以在一个地方查看、筛选、搜索、编辑、添加、修改和组织所有防火墙规则。



Sophos Firewall 将访问策略、NAT 和 TLS 检查的所有规则放在一个位置，方便管理。

针对用户、企业应用程序、NAT、TLS/SSL 检查和联网的规则方便仅查看需要的政策，同时提供一个方便的屏幕进行管理。

指示图标提供政策的重要信息，如它们的类型、状态、实施等。

管理安全一览

无论是通过云端的 Sophos Central 帐户还是 Sophos Firewall 用户界面, Sophos 都能非常轻松配置和管理现代防护需要的一切工作, 并且全部在一个屏幕中搞定。

The screenshot shows the 'Security features' configuration page. It is divided into several sections: 'Web filtering', 'Configure Synchronized Security Heartbeat', and 'Other security features'. Blue callout lines point to various settings with Chinese labels: '双 AV' (Dual AV) points to 'Scan HTTP and decrypted HTTPS'; '沙箱' (Sandbox) points to 'Detect zero-day threats with Sandstorm'; 'SSL 检查' (SSL Check) points to 'Scan FTP for malware'; '心跳' (Heartbeat) points to 'Configure Synchronized Security Heartbeat'; '应用控制' (Application Control) points to 'Identify and control applications (App control)'; 'QoS' (QoS) points to 'Shape traffic'; '优先级设置' (Priority Settings) points to 'DSCP marking'; and '入侵防御系统' (Intrusion Prevention System) points to 'Detect and prevent exploits (IPS)'. Other visible settings include 'Block QUIC protocol', 'Block clients with no heartbeat', 'Block request to destination with no heartbeat', 'Block generally unwanted apps', 'Apply application-based traffic shaping policy', and 'Scan email content'.

使用预定义或自定义策略, 在一个屏幕上配置全部安全状态。

您可以设置和整合防病毒、TLS 检查、沙箱、IPS、流量调整、Web 和应用程序控制、Security Heartbeat、NAT、路由和优先级的安全与控制, 全部在一个位置 — 逐个规则, 逐用户, 或逐组。

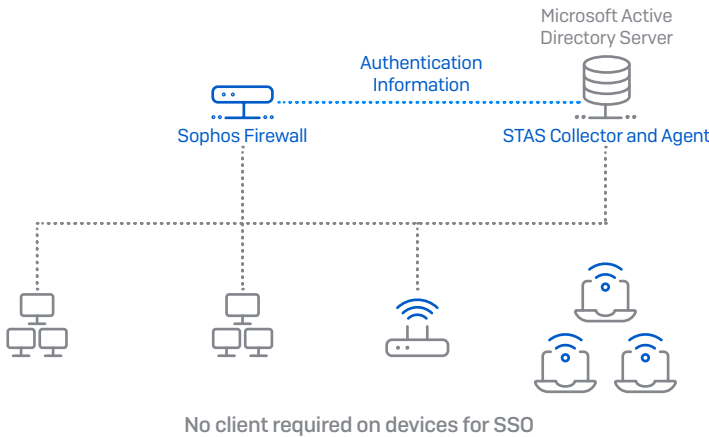
如果要查看任何整合政策的具体工作, 或者进行改动, 您可以就地编辑, 无需离开防火墙规则访问产品的其他部分。

The screenshot shows the 'Edit web policy' screen. At the top, there is a 'Name' field with 'Default Workplace Policy' and a 'Description' field with 'Deny access to categories most commonly unwanted in professional environments'. Below this is a table with columns: 'Users', 'Activities', 'Action', 'Constraints', 'Manage', and 'Status'. The table contains several rows of rules:

Users	Activities	Action	Constraints	Manage	Status
chris joe	All web traffic and with content Ethnicity terms [Canada] Objectionable Terms	Block		+ (i) (t)	ON
Anybody	Anonymizers	Block		+ (i) (t)	ON
Anybody	Weapons	Block		+ (i) (t)	ON
Anybody	Extreme	Block		+ (i) (t)	ON
Anybody	Phishing & Fraud	Block		+ (i) (t)	ON
Anybody	Militancy & Extremist	Block		+ (i) (t)	ON
Anybody	Gambling	Block		+ (i) (t)	ON

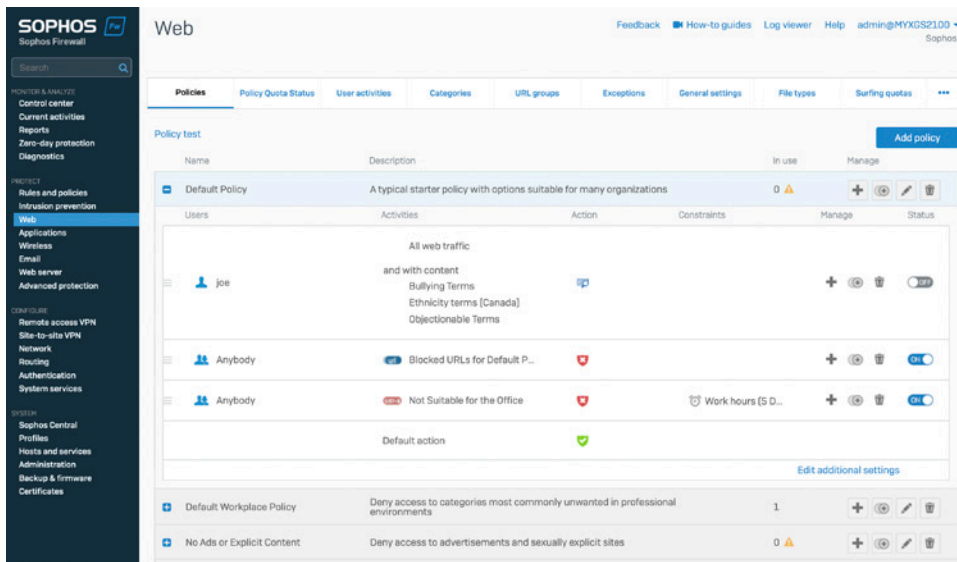
概览查看策略详细信息, 进行更改而不离开防火墙规则屏幕。

灵活的身份验证选项允许您轻松了解对方是谁, 加入目录服务, 如 Active Directory、eDirectory 和 LDAP, 以及 NTLM、Kerberos、RADIUS、TACACS+、RSA、客户端代理或强制网络门户。Sophos Transparent Authentication Suite (STAS) 提供与目录服务 (如 Microsoft Active Directory) 的集成, 实现方便、可靠、透明的单点登录身份验证。



企业级安全 Web 网关

Web 防护和控制是任何防火墙的主要功能, 遗憾的是, 在大多数防火墙实施中感觉都像事后增补的。我们打造企业级 Web 防护解决方案的经验为我们提供了背景和知识, 部署通常只有企业级安全 Web 网关 (SWG) 解决方案中才有的 Web 政策控制, 但后者成本是我们的十倍。我们实施了一个从上至下继承政策模型, 让制定复杂政策变得简单而直观。提供现成预定义政策模板用于最常用部署, 例如典型工作环境、教育 CIPA 合规等。这意味着可以立刻上线并合规, 轻松微调 and 定制选项就在您的指尖。



强大的企业级 Web 策略提供精细控制。

事实上, 我们知道 Web 政策是防火墙日常最经常改动的要素, 所以我们投入大量精力使其便于根据用户和企业需求进行管理和调整。您可以轻松自定义用户和组、活动 (由 URL、类别、内容过滤器和文件类型)、操作 (阻止、允许或警告) 组成, 添加或调整当天时间和星期约束。

教育功能

对于重视 Web 策略和合规性要求的教育环境，Sophos Firewall 提供多个非常适合的功能。特定于教育的功能包括：

- 预封装的 Web 政策，用于 CIPA 合规性
- 根据关键字进行内容过滤和报告
- 基于用户/组政策的 SafeSearch 和 YouTube 限制设置
- 可以由教师管理的阻止页面覆盖
- 综合内置报告，提前发现潜在问题

Web 政策现在提供记录和监测功能，甚至可以根据关键字列表实施与动态内容有关的政策。此功能在教育环境中尤其重要，可以利用与自残、欺凌、极端行为或其他不当内容有关的关键字，确保儿童在线安全，并提供学生相关信息。关键字库可以上传到防火墙，应用于任何 Web 过滤政策作为附加标准，并提供记录和监测操作，或者阻止包含相关关键字的搜索结果或网站。

提供全面报告用于识别关键字匹配以及搜索或消耗相关关键字内容的用户，在风险用户成为真正问题前实现主动干预。

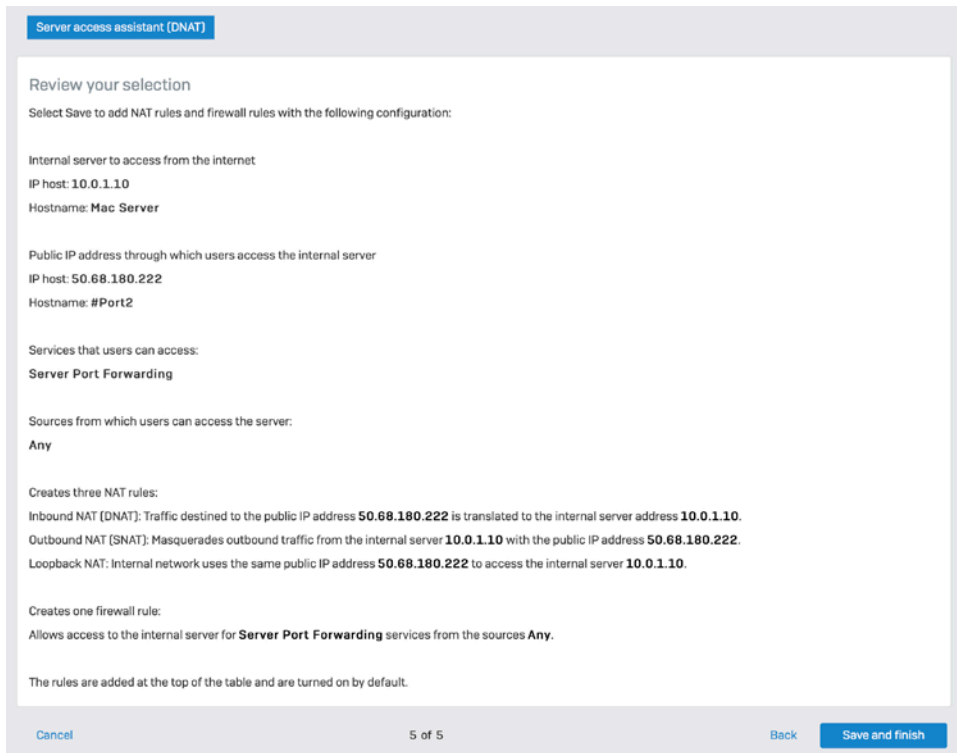
Sophos Firewall 提供现成 CIPA 政策合规性，实现快速合规。还根据用户/组策略，提供对 SafeSearch 和 YouTube 限制的灵活强大控制。可以允许教师设置和管理自己的政策覆盖，允许其教室访问通常在课程中阻止的网站。

强大的 Web 政策简化操作。

简化 NAT 配置

任何尝试配置 NAT (Network Address Translation) 规格的人都知道配置难度,但并不一定如此。Sophos Firewall 包含完整企业级 NAT 功能,在一个具有精细选择标准的规则中实现强大灵活的 NAT 配置,包括源 NAT (SNAT) 和目标 NAT。为了简化复杂 DNAT,易于使用的向导将指导您创建完整 NAT 配置,只需单击几下。

创建防火墙规则时,管理员还可以利用方便的链接 NAT 功能。链接 NAT 将自动创建相应 NAT 配置规则,进一步缩短用于创建和配置 NAT 规则的时间。

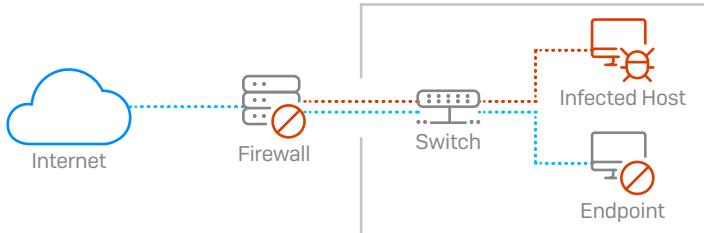


利用强大而直观的 NAT 规则向导,只需单击几下即可创建复杂访问控制。

自动应对事件

网络管理员要求最多的一个防火墙功能是自动应对网络安全事件的功能。

Sophos Firewall 是唯一能够完全识别网络感染来源, 并自动限制受感染设备访问其他网络资源的网络安全解决方案。这得益于我们独有的 Sophos Security Heartbeat, 在 Sophos 托管端点与防火墙之间共享遥测和运行状态。



Sophos Firewall 和 Security Heartbeat 可以自动隔离网络上被感染的主机。

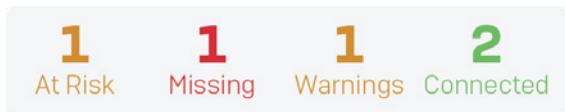
Sophos Firewall 将连接主机的运行状况独特集成在您的防火墙规则中, 允许您自动限制从任何隐患系统访问敏感网络资源直到清除。

Sophos Firewall 不仅在防火墙隔离端点, 禁止其访问网络其他部分, 而且可以协助网络上的所有健康端点在端点层面隔离存在隐患的主机。

我们称为横向移动防护, 可以隔离并阻止威胁或攻击者在网络内横向移动至其他系统, 即使他们位于防火墙通常无法干预的同一网段或广播域。该解决方案能够极为简单有效地解决网络上活跃对手带来的挑战。只有您的端点和防火墙采用协作或同步防御时才能实现这一点。

Security Heartbeat安全心跳

Sophos Security Heartbeat 使用 Sophos 托管端点与 Sophos Firewall 之间的安全链接实时共享情报。只需简单同步以前独立工作的安全产品, 就可形成对高级恶意软件和针对性攻击的更有效防护。



The screenshot shows the 'HEARTBEAT' tab in the Sophos Firewall management console. It features a summary bar at the top with counts for 'At risk', 'Missing', 'Warnings', and 'Connected'. Below this is a table listing monitored hosts with their status and last update time.

HOSTNAME, IP	USER	STATUS CHANGED
Mac-Server 10.0.1.10	Chris	5 days ago
Joe's Laptop 192.168.1.2	joe	54 seconds ago
MacBook 10.0.1.55	Mindy	36 seconds ago
Macbook-CA-6N-42527 10.0.1.18	chrismcpermack	13 hours ago

网络的 Security Heartbeat™ 状态显示在控制中心。

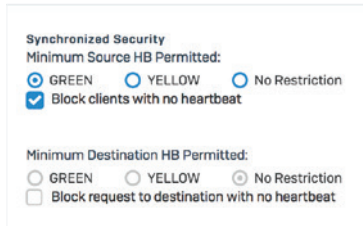
Security Heartbeat 不仅可以及时发现高级威胁的存在,还可用于传递威胁性质、主机系统和用户等重要信息。最重要的是, Security Heartbeat 还可自动采取措施,隔离或限制访问存在隐患的系统直到没有恶意软件。这项有意义的技术革新了 IT 安全解决方案识别和应对高级威胁的方式。

用于防火墙背后托管端点的 Security Heartbeat 具有三种状态:

绿色心跳状态表示端点设备健康,允许访问所有合适网络资源。

黄色心跳状态表示警告,设备可能具有潜在有害应用程序 (PUA),不合规,或存在其他问题。您可以选择解决问题前黄色心跳可以访问的网络资源。

红色心跳状态表示设备存在感染高级威胁的风险,可能尝试报障至僵尸网络或指挥控制服务器。在防火墙中使用 Security Heartbeat 政策设置,可以用红色心跳状态轻松隔离系统直到可以清除,以减少数据丢失的风险或阻止传播感染。



设置 Security Heartbeat 要求作为任何防火墙规则的一部分。

只有 Sophos 可以提供类似 Security Heartbeat 的解决方案,因为只有 Sophos 同时是端点和网络安全解决方案领域的领军企业。虽然其他供应商开始认识到这是 IT 安全的未来,并开始想办法实现类似功能,但他们都存在一个决定性的劣势:他们不同时具备行业领先的端点解决方案和行业领先的防火墙解决方案以集成二者。

这是一个零信任的世界

信任在 IT 行业是一个危险的词语,尤其当信任具有隐含意义时。建立庞大隔离的企业外围并信任内部的所有内容已经证明是一种存在缺陷的设计。

零信任是一种全盘方法,能够解决这些变化,以及企业工作和应对威胁的方式。这是与安全思维和执行方式有关的模型和理念。

不应自动信任任何人或任何事,无论是企业网络内外。但最终,需要信任有些东西。有了零信任,这种信任是临时性的,根据多个数据来源确定,并且不断重新评估。

零信任让我们可以控制整个资产,从办公室内部到使用的云平台。不再缺乏对企业外围以外的控制,也不再出现远程用户的窘迫。

我们如何向零信任过渡,发挥其全部优点?虽然还没有公司可以提供单独的零信任解决方案,但 Sophos 提供广泛的安全技术和控制,加速并简化向零信任的过渡。

Sophos Central - 全球最受信任的网络安全平台将这些孤立互补的技术组合在一个云管理控制台,帮助您协调和监测零信任网络。

Synchronized Security - 在端点、ZTNA、防火墙和其他系统之间持续共享信息的网络安全,提供信息和彼此之间的可见性。

Sophos ZTNA - 提供真正的零信任网络访问解决方案,将客户安全连接至应用程序和数据。

Sophos Firewall 围绕用户、设备、应用程序、网络等建立区域划分或微外围。

Server Protection and Intercept X - 为每个设备分配设备运行状态,这样如果受到威胁,可以自动隔离该设备,并阻止其连接其他设备。

Managed Threat Response (MTR) service - 监测网络内的所有用户活动,发现存在潜在隐患的用户凭据。

优化您的 SD-WAN 网络

在网络行业,很少有像 SD-WAN (软件定义广域网, Software Defined Networking in a Wide Area Network) 引起如此大热议的事物。在热烈的讨论中,有用信息和夸大吹嘘各占一半。因此,不同的人对于 SD-WAN 有着不同的看法,有些人仍在试图了解其到底是什么。

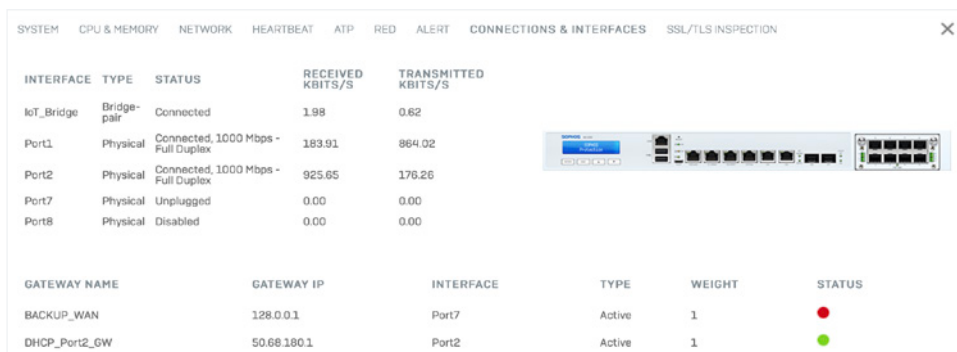
从根本上来说,SD-WAN 通常在于实现以下四个联网目标中的一个或多个:

- **降低连接成本** – 传统 MPLS (Multi-Protocol Label Switching) 连接技术昂贵,因此企业转向更廉价的宽带 WAN 方案,如电缆、DSL 和 3G/4G/LTE
- **业务连续性** – 企业需要解决方案在发生 WAN 故障和断电时提供冗余、路由、故障转移和会话保留功能
- **关键应用程序的质量** – 企业寻求应用程序流量和性能的实时可见性,以保持使命关键型业务应用程序的会话质量
- **简化分支办事处 VPN 协同** – 不同地点之间的 VPN 协作往往复杂而耗时,所以提供能够简化和自动完成部署与设置的工具很关键

Sophos Firewall 和 Xstream SD-WAN 帮助您轻松而价格合理地实现最高的 SD-WAN 目标,提供全面的 SD-WAN 协同、管理和性能以及可靠性优化选择。

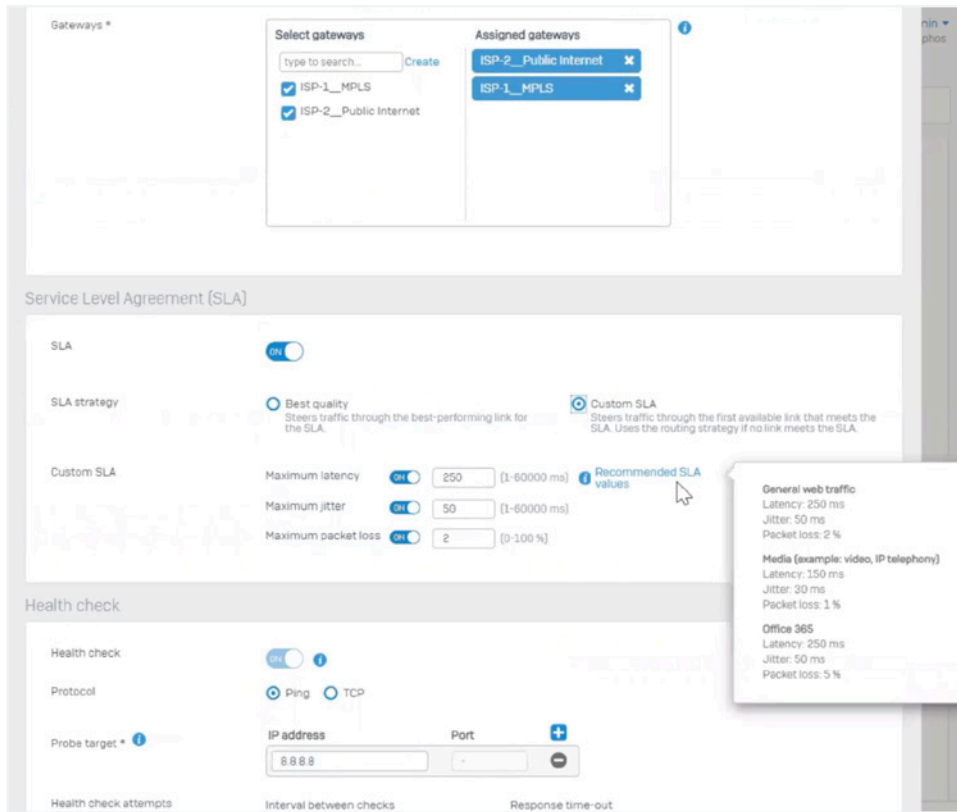
Xstream SD-WAN

管理多个 WAN 链接上的应用程序流量路由是 SD-WAN 的主要任务, Sophos Firewall 和 Xstream SD-WAN 提供一个强大而灵活的链接管理解决方案,无论您使用多个 MPLS、DSL、有线还是无线连接。



WAN 链路状态显示在仪表板的此接口状态小工具底部。

SD-WAN 配置文件定义多个 WAN 链路网关之间的路由策略,根据 WAN 链路性能实现无缝高效重新路由应用程序连接。链路之间切换即时发生,对应用程序会话零影响,即使在中断最多或最不稳定的 ISP 环境中也能不中断提供无缝连续性、应用程序性能和最佳最终用户体验。



直观轻松设置基于性能的 SD-WAN 配置文件。

SD-WAN 配置文件路由策略可以基于第一个可用或基于性能的链接条件。性能监测标准包括抖动、延迟和数据包丢失，可以对 PING 和 TCP 探测使用多个探测策略。

SD-WAN 配置文件可以根据性能或您自己的自定义 SLA 策略选择最佳链路，定义最大可接受抖动、延迟或数据包丢失的具体值，然后重新路由到性能更好的链路，对任何活跃连接绝对零影响。

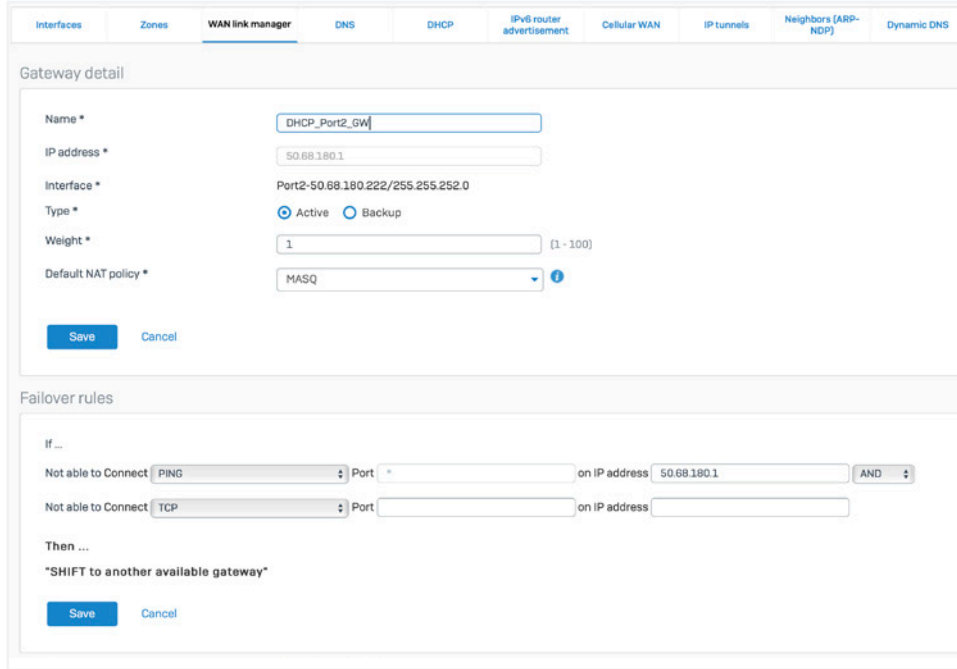
轻松监测 SD-WAN 网络的性能, 提供延迟、抖动和数据包丢失的实时和历史图形。时间线选择包括实时、最近 24 或 48 小时, 或者上周或上月。还提供 SD-WAN 性能和路由的高级记录。



实时监测各个 WAN 链路的性能。

Xstream FastPath 加速 SD-WAN VPN 流量

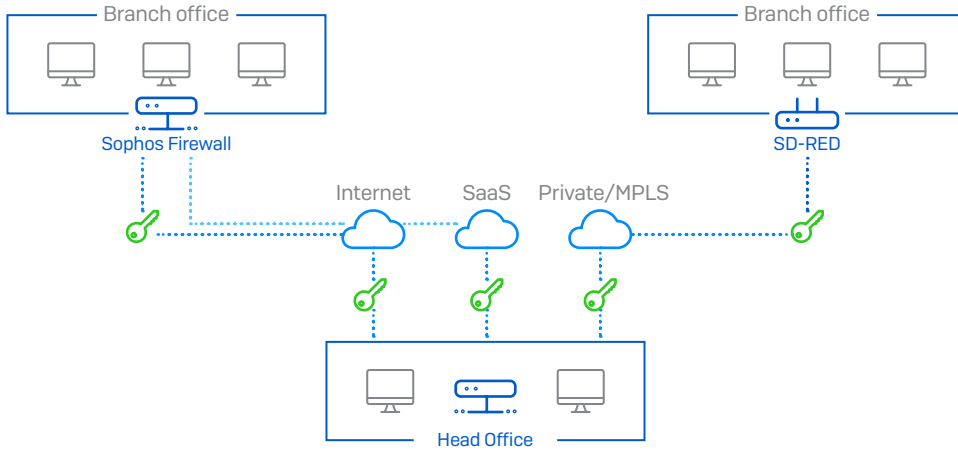
Sophos Firewall 利用 XGS 系列设备集成的 Xstream Flow Processors 提供 IPsec VPN 隧道流量的硬件加速。这显著提高了性能, 将 IPsec 隧道需要的一些 CPU 繁重处理转移到 Xstream Flow Processor, 例如 ESP- 封装/加密和解封/解密。这一新功能充分利用 Xstream Flow Processor 内的硬件加密功能, 而且释放 CPU 资源用于其他任务, 如对需要的流量进行深度数据包检查。Xstream FastPath 加密 IPsec 流量适合点对点 and 远程访问 VPN 流量。



Sophos Firewall WAN 链路管理, 包括平衡和故障转移规则。

SD-分支办公室连接性

凭借独有的 SD-RED 设备, Sophos 一直是零接触分支办公室部署和连接领域的先锋。此类廉价设备非常方便非技术人员部署, 在设备与中央防火墙之间提供强大而安全的 Layer 2 通道。



Sophos Firewall 和 SD-RED 设备提供通道选择, 通过 SD-WAN 简单廉价连接分支办公室。



Sophos SD-RED 设备提供 SD-WAN 分支办公室连接的廉价零接触解决方案。

SD-RED 设备部署再简单不过:您只需记下防火墙中的设备序列号,将设备运送至远程地点。远程地点的任何非技术人员只需连接设备,设备将自动联系云配置服务,与 Sophos Firewall 建立安全的通道连接。

The screenshot shows the configuration interface for a Sophos Firewall RED device. The top navigation bar includes tabs for Interfaces, Zones, WAN link manager, DNS, DHCP, IPv6 router advertisement, Cellular WAN, IP tunnels, Neighbors (ARP-NDP), and Dynamic DNS. The main configuration area is divided into three sections: RED settings, Uplink settings, and RED network settings. At the bottom, there are 'Save' and 'Cancel' buttons.

RED settings

- Branch name * [Text input]
- Type: RED 15 [Dropdown menu]
- RED ID * [Text input]
- Tunnel ID * [Dropdown menu: Automatic]
- Unlock code * [Text input]
- Firewall IP/hostname * [Text input]
- 2nd firewall IP/hostname [Text input]
- Use 2nd IP/hostname for: Failover Load balancing
- Description [Text area]
- Device deployment: Automatically via provisioning service Manually via USB stick

Uplink settings

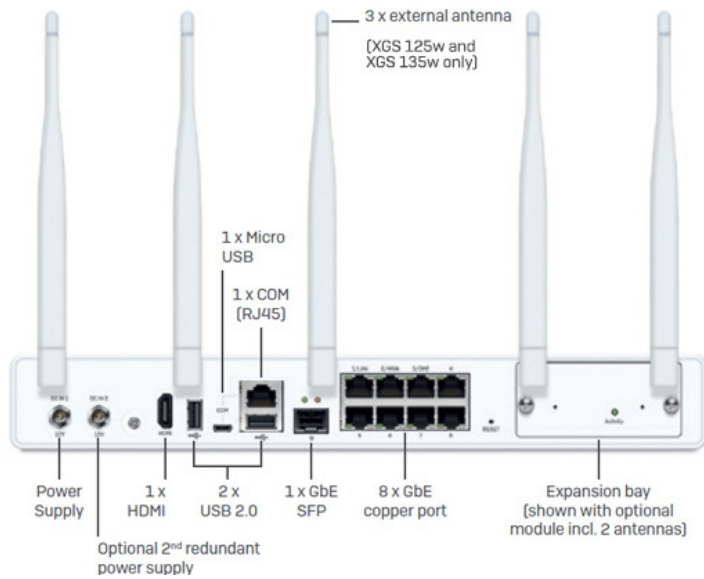
- Uplink connection: DHCP Static
- 3G/UMTS failover: Enable

RED network settings

- RED operation mode: Standard/unified Standard/split Transparent/split
- RED IP * [Text input]
- RED netmask: /24 (255.255.255.0) [Dropdown menu]
- Zone: LAN [Dropdown menu]
- Configure DHCP: ON
- RED DHCP range: [Text input] [Text input]
- MAC filtering type: No configured MAC address lists found
- Tunnel compression: Enable
- RED MTU: 1500 [Text input] (576 to 1500)

Sophos SD-RED 提供灵活安全廉价的 SD-WAN 分支办公室连接解决方案。

我们的台式 XGS Series 设备也是出色的分支办公室 SD-WAN 连接解决方案, 提供灵活的连接选择, 包括 VDSL、无线以及铜线和光纤接口, 支持强大的 SD-RED 通道。

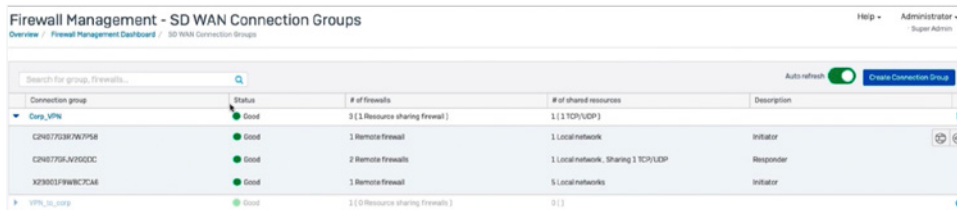


部分台式型号 (如这里显示的 XGS 135w) 提供 LTE/无线、VDSL、铜线或光纤 WAN 连接选择。

VPN 支持与协作

如果您在不同防火墙之间设置两个以上 VPN 隧道, 您知道这个工作有多费时和繁琐。Sophos Firewalls 在 Sophos Central 中支持丰富的 SD-WAN 协同, 快速轻松实现多个防火墙之间的多隧道互连。

您只需选择已经管理的, 需要加入 SD-WAN 连接组的防火墙, 然后选择希望每个地点可以访问的网络资源。只需开启开关, 即可看到 SD-WAN VPN 重叠网络成为现实, 将为您自动创建所有所需防火墙访问规则和隧道, 包括冗余。



只需单击几下, 即可设置复杂 SD-WAN 重叠网络, 从 Sophos Central 监测。

无论需要完整网状网络、辐射拓扑或者介于二者之间的结构, Sophos Central 都将在后端自动配置所有需要的隧道和防火墙设置, 实现您的 SD-WAN 重叠网络。

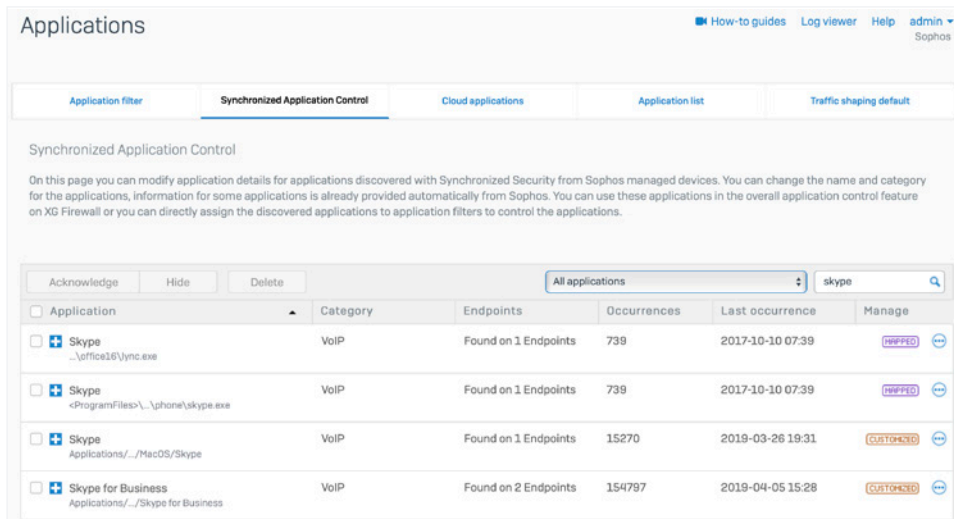
当前 Sophos Firewall 支持您想要的所有标准点对点 VPN 功能, 包括 IPSec 和 SSL。我们甚至提供带路由功能的独有 SD-RED Layer 2 通道, 极为强大, 且在高延迟场景 (如卫星链路) 中证明了可靠性。

应用程序可见性与路由

实现 SD-WAN 目标的另一个重要功能是应用程序路径选择和路由，用于确保使命关键型应用程序(如 VoIP)的质量和降低延迟。

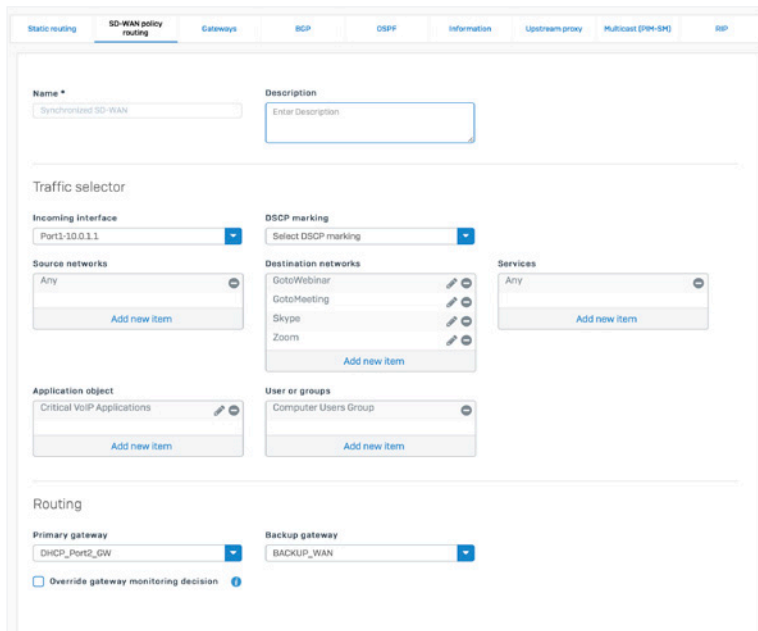
当然，您无法路由无法识别的内容，因此准确可靠的应用程序识别和可见性很关键。这是 Sophos Firewall 和 Sophos Synchronized Security 提供宝贵优势的方面。同步应用程序控制提供所有联网应用程序的 100% 透明度和可见性，在识别使命关键型应用程序，尤其是模糊或自定义应用程序方面，具有显著优势。

同步 SD-WAN (另一个 Synchronized Security 功能) 为 SD-WAN 应用程序路由提供额外好处。同步 SD-WAN 在 Sophos 托管端点与 Sophos Firewall 之间共享同步应用程序控制信息，提高应用程序识别的透明度和可靠性。现在，还可以将以前未识别的应用程序加入 SD-WAN 路由策略，提供其他防火墙无法匹敌的应用程序路由控制和可靠性。



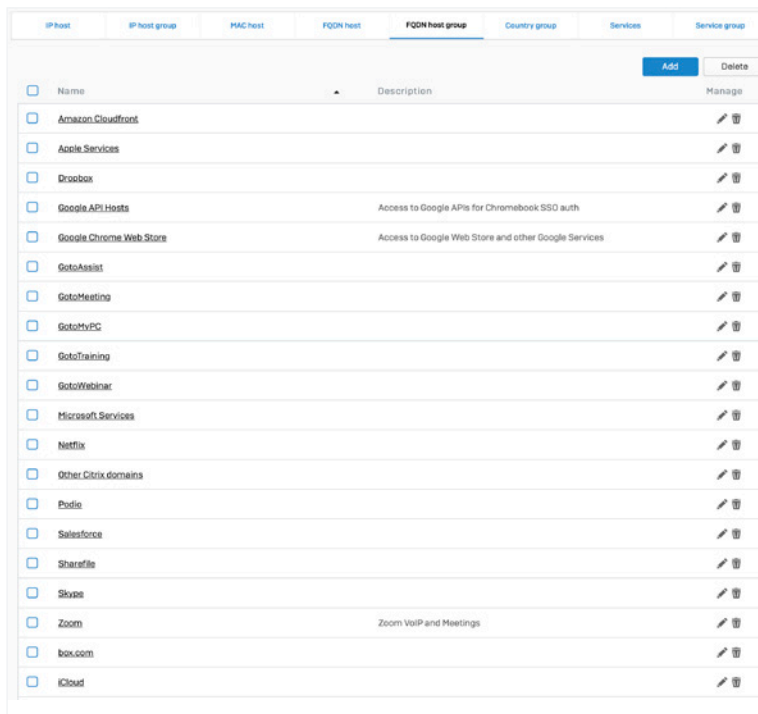
同步应用程序控制 100% 识别所有联网应用程序，方便设定优先级和路由使命关键型应用程序。

Sophos Firewall 还支持在所有防火墙规则中按用户和组选择的基于应用程序的路由与路径。精细的基于策略的路由 (PBR) 控制能够定义通过主要或备用网关 WAN 连接的路由，配置重放方向。这些功能组合在一起，能够轻松引导重要应用程序流量通过最优 WAN 接口发出。



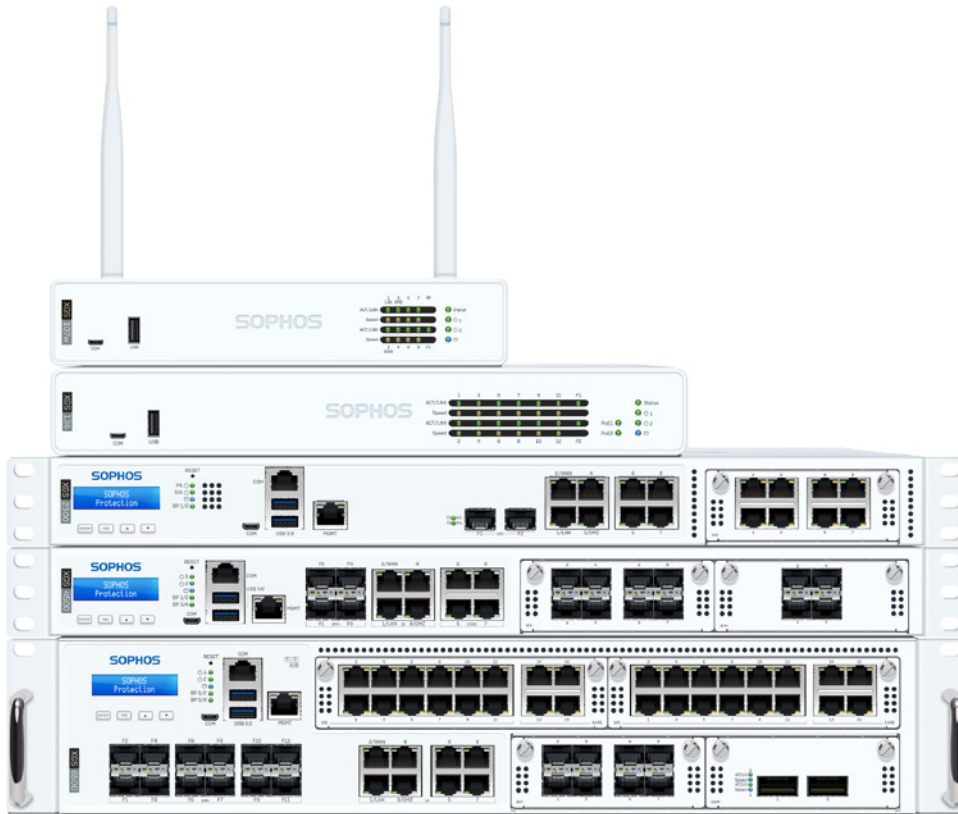
SD-WAN 基于策略的路由提供路由关键应用程序流量的灵活工具。

Sophos Firewall 还为受欢迎的 SaaS 云服务提供预定义完全限定域名 (FQDN) 对象, 以及数千个现成 FQDN 主机定义和轻松添加更多定义的功能。



预定义 FQDN 主机对象简化路径选择和基于应用程序的路由。

将 Sophos Firewall 加入任何网络 – 简单



Sophos Firewall 系列硬件设备提供灵活部署功能,故障打开旁路端口现在是在所有 1U 型号的标准配备,并在 Flexi Port 模块中提供,以便在 2U 设备上启用此功能。旁路端口支持以桥接模式并行安装 Sophos Firewall 和现有防火墙。如果需要关闭或重启 Sophos Firewall 以更新固件,旁路端口允许流量继续通过而不中断网络,从而提供业务连续性。此功能使新部署选项完全没有风险,无需更换任何现有网络基础设施。此外,我们的下一代端点防护 Intercept X 可以与任何现有台式机防病毒产品一起运行,支持在任何网络中部署完整 Sophos Synchronized Security 解决方案,不会取代任何产品。

Sophos Firewall: 简化网络安全。

申请报价

访问 www.sophos.cn/firewall-quote, 申请根据您的需求定制的非强制性报价

中国(大陆地区)销售咨询
电子邮件: salescn@sophos.com