BATTLECARD

Fortinet vs. Sophos (SMB)

Why Fortinet Unified Threat Management?

Fortinet Unified Threat Management (UTM) devices are ideal for small and medium business (SMB) customers looking for strong security features with integrated access solutions. Fortinet UTM consolidates both FortiGate next-generation firewall (NGFW) security and FortiWiFi wireless access on a single device, while offering additional, easy-to-integrate network security products such as switches and network access control (NAC).

Fortinet was the only "Recommended" vendor with a security rating in the first NSS Labs software-defined wide-area network (SD-WAN) report. Fortinet again received a "Recommended" rating in the second NSS Labs independent SD-WAN test in 2019.

Fortinet UTM delivers:

- **Simplified management.** Offered as standalone and cloud-based (FortiGate, FortiGate Cloud, FortiSwitch, and FortiAP).
- **Security and performance.** Fortinet earned a high security rating of 99.3% and lowest total cost of ownership (TCO) in the NSS Labs 2019 NGFW test.
- **Security and performance.** FortiCloud scales easily for growth, making it an ideal solution for SMBs, distributed enterprises, and managed service providers (MSPs).

Sophos Background

Sophos is a network and endpoint security vendor headquartered in Abingdon, U.K. The vendor's portfolio includes firewalls (XG Series, SG Series, and CR Series), endpoint security (Sophos Endpoint Protection and Intercept X), mobile security, secure email gateway, email phishing training, secure web gateway, server security, encryption, wireless access points (Sophos AP), and unified endpoint management (Sophos Mobile). Sophos Firewall Manager is the name of the centralized management software, and Sophos Central is the cloud-based centralized management portal for all Sophos security products.

Sophos Target Account Priorities (Who They Target)

Sophos is a good fit for SMBs, especially for lower-midsize business and distributed-office use cases that value ease of use, security features, and firewall/endpoint integration. Target industries include: education, healthcare, retail, government, finance and banking, and the public sector.

Top Sophos Issues

1. **Performance.** Data sheet performance numbers are not supported by NSS Labs testing.
2. **Complex deployment.** After rebranding "Astaro" to Sophos UTM, it has challenges between XG and SG platforms with respect to deployment and migration without any proper documentation.
3. **Poor SD-WAN solution.** Sophos offers simple and basic SD-WAN features but no security.
4. **No SSL/TLS.** Sophos does not offer certificate validation or comprehensive cipher suite support.
5. **Limited reporting and management.** Sophos standard reporting is limited and occurs on-box. Additional licenses are required for iView for detailed reporting.

How to Win

Demonstrate Fortinet's cloud-managed solution for SMBs with easy management, configuration, and real-time application analytics on a single pane of glass.

- Demonstrate how easy it is to deploy FortiCloud and manage FortiGate, FortiSwitch, FortiAP, and FortiClient.
- Show HTTPS performance results with NSS Labs NGFW public testing.
- Mention that FortiGate Secure SD-WAN has been "Recommended" by NSS Labs in two out of two NSS Labs SD-WAN tests.
- Advise that Fortinet can offer significantly better security and performance than Sophos with controlled security policies and signatures. Explain why Fortinet can offer a more secure and effective option.
- Drive home the fact that Fortinet offers a cost-effective solution that includes highly rated security and access in an easy-to-use interface with multiple deployment options.
- Demonstrate the value of a security fabric.
- Highlight the value of SD-Branch.

Solution Comparison

Capabilities	Fortinet	Sophos
Security fabric	Yes	No
SD-WAN	Yes (Secure, fast, and certified by NSS Labs)	Limited (Primitive feature set and not certified)
SD-Branch	Yes	No (Switches)
Simplified security policies	Yes	No
SSL/TLS inspection	Yes	Yes (Subpar performance in NSS Labs testing)
Gartner UTM MQ 2018	Leader	Visionary
Simplified user and device configuration using a single management interface	Yes	Limited
Security validation (NSS Labs, ICSA)	Yes	Yes
On-box management	Yes	Yes

Feature Comparison

Features	Fortinet	Sophos
Cloud-managed	Yes	Limited
L3 routing	Yes	Yes
Security profiles	Yes	Yes
Application visibility	Yes	Yes
POE+	Yes	No
Network address translation (NAT)	Yes	Yes
Quality of service (QoS)	Yes	Very poor QoS
Integration with security fabric	Yes	No
Single-pane-of-glass management	Yes	Limited (Sophos Central)

Product Comparison*

	FortiGate 30E	FortiGate 50E	FortiGate 60E	FortiGate 80E	FortiGate 100E	Sophos XG 85	Sophos XG 105	Sophos XG 115	Sophos XG 125	Sophos XG 135
Firewall	950 Mbps	2.5 Gbps	3 Gbps	4 Gbps	7.4 Gbps	2 Gbps	3 Gbps	3.5 Gbps	5 Gbps	7 Gbps
Sessions	900,000	1,800,000	1,300,000	1,300,000	2,000,000	2,000,000	3,200,000	6,000,000	6,200,000	8,200,000
Sessions per second	15,000	21,000	30,000	30,000	30,000	12,000	27,500	27,500	35,000	82,000
IPsec VPN	75 Mbps	90 Mbps	2 Gbps	2.5 Gbps	4 Gbps	225 Mbps	360 Mbps	490 Mbps	700 Mbps	1,180 Mbps
SSL VPN	35 Mbps	100 Mbps	150 Mbps	200 Mbps	250 Mbps	x	x	x	x	x
IPS	300 Mbps	350 Mbps	400 Mbps	450 Mbps	500 Mbps	75 Mbps	86 Mbps	103 Mbps	180 Mbps	232 Mbps
SSL/TLS	125 Mbps	150 Mbps	135 Mbps	135 Mbps	130 Mbps	x	x	x	x	x
Application control	400 Mbps	450 Mbps	650 Mbps	900 Mbps	1 Gbps	x	x	x	x	x
NGFW	200 Mbps	220 Mbps	250 Mbps	360 Mbps	360 Mbps	31 Mbps	36 Mbps	42 Mbps	58 Mbps	95 Mbps
Threat prevention	150 Mbps	160 Mbps	200 Mbps	250 Mbps	250 Mbps	25 Mbps	27 Mbps	30 Mbps	75 Mbps	133 Mbps
Interfaces	5x GE RJ45	7x GE RJ45	10x GE RJ45	14x GE RJ45, 2x Shared Port Pairs	20x GE RJ45, 2x Shared Port Pairs	5x GE RJ45	5x GE RJ45	5x GE RJ45 w/1 shared SFP	5x GE RJ45 w/1 shared SFP	8x GE RJ45 w/1 shared SFP
List price	$430	$550	$650	$1,000	$2,000	$295	$440	$595	$795	$1,045

* The above numbers are published in data sheets. Sophos throughput numbers may be high in the data sheets, but the products failed to reach these numbers in NSS Labs performance testing.