Sophos

XG Firewall

This product is a UTM that bills itself as a next-generation firewall. This was one that rather took us aback because we don't tend to think of UTMs as firewalls. However, the argument is that a UTM really has a lot of traditional firewall functionality. So, if we add the next-generation functionality, the characterization makes sense. The functionality in this UTM includes, among other things, firewall, IPS, application security, wireless gateway and advanced threat protection.

We dropped into the landing page, what Sophos calls the Control Center, and got the usual top-level dashboard. From here there are extensive drill-downs. One particular feature that we liked was the User & Device Insight. This is a top-level view of a device being monitored. It gives a lot of detail about the device, including the Security Heartbeat. As one would expect, the Sophos anti-malware legacy shows up extensively with just about any type of malware identified and addressed.

This is a unique function that lets the endpoint communicate directly with the tool – resulting in a lot of endpoint information being sent for analysis. This includes analysis of suspicious files in the Sophos cloud-based sandbox, called Sandstorm. Sandstorm can simulate activity for a delay of up to six months for delayed detonation malware. This is more than just a passive look at the endpoint.

The User Threat Quotient – UTQ – identifies high-risk users based on their activities, such as suspicious file downloads. Setting rules is straightforward and the firewall rules look exactly as you would expect, which simplifies management for experienced engineers who are seeing what they expect to see. Editing rules is easy, consisting mostly of making selections from a menu page. However, if your selection is not there, you certainly can add your own.

Reporting is a strong suite for XG Firewall. There are over 1,000 reports available out of the box. Overall, we found this to be a useful tool. If you are a Sophos shop, reporting can aggregate across Cyberoam, XG and UTM 9 devices into a single report, a winning feature. Like the UTQ, the App Risk Analysis identifies high-risk applications.

Pricing on this product is very reasonable and there are multiple levels of support. There is a basic level of support at no cost during the first 90 days to cover the deployment period. After that there are two additional levels of fee-based support. The website has a good assistance portal that includes such things as a knowledge base and an FAQ. There also are forums along with some self-help guides.

So, next-generation firewalls as UTMs? We believe there is a very good case to be made for that. Time will tell, of course, but this is a marketspace that is certainly characterized by convergence.

– Peter Stephenson, technology editor

DETAILS

Vendor Sophos

Product XG Firewall

Website sophos.com/xgfirewall

Price Starting at $249/year on a three-year term for TotalProtect Plus & Enhanced Support on an XG 85.

Features	★★★★★
Performance	★★★★★
Documentation	★★★★★
Support	★★★★★
Value for money	★★★★★

OVERALL RATING ★★★★★

Strengths Very creative convergence of a lot of solid functionality. Documentation is presented in a novel way on the web portal.

Weaknesses None that we saw.

Verdict This demands your attention no matter what size your organization. There are models to cover most requirements.