مقایسه امکانات سوفوس

با محصولات امنیتی FortiGate

FORTINET

- یکی از تبلیغاتی که برای محصولات FortiGate می شود، استفاده از معماری سخت افزاری ASIC برای افزایش کارایی سیستم است. در محصولات امنیتی UTM، استفاده از معماری ASIC گرچه موجب افزایش کارایی می شود اما در مقابل ضریب امنیت را کاهش می دهد. سیستم های ASIC معمولا نمی توانند بانک های اطلاعاتی حجیم و پویای مورد نیاز برای سرویس های امنیتی مانند ضد ویروس و IPS را بطور کامل نگهداری کنند. به این دلیل مجبور به حذف بخشی از این اطلاعات می شوند و نتیجه آن نیز کاهش ضریب شناسایی ویروس و حملات است. بعنوان مثال تعداد حملات قابل شناسایی در FortiGate IPS حدود ۶ هزار مورد است، در حالیکه این عدد در تجهیزات Sophos به ۱۵ هزار می رسد.

- FortiGate برای شناسایی ویروس و هرزنامه از نرم افزارهای ساخت خود استفاده می کند که در رده بندی ها جایگاه بالایی ندارند. در حالیکه Sophos از ضدویروس های قدیمی و برتر جهان می باشد.

- واسط (interface) تحت web در محصولات FortiGate بسیار پیچیده طراحی شده است و پیدا کردن تنظیمات مورد نیاز در آن آسان نیست. ضمن اینکه تمام امکانات لازم را در اختیار مدیر شبکه قرار نمی دهد و مدیر شبکه برای پاره ای از کارها باید از Command Line استفاده کند. در حالیکه Sophos دارای واسط تحت web بسیار آسان و کاملی بوده و جوایزی نیز برای طراحی ویژه آن کسب کرده است.

- علاوه بر واسط مدیر شبکه، Sophos دارای واسط تحت web برای کاربر نیز می باشد (User Portal) که از طریق آن کاربران می توانند بسیاری از کارهای خود را از قبیل تغییر رمز عبور، آزاد کردن هرزنامه ها، دریافت تنظیمات VPN و ... انجام دهند. تجهیزات FortiGate فاقد این امکان هستند و زحمت تمام کارهای فوق به عهده مدیر شبکه می باشد.

- سیستم تشخیص نفوذ FortiGate IPS فقط قادر به شناسایی حملات متداول و شناخته شده است که حدود ۶ هزار حمله را شناسایی می کند و هیچگونه امکانی برای تجزیه و تحلیل ترافیک شبکه ندارد. در حالیکه سیستم تشخیص نفوذ Sophos قادر به شناسایی حدود ۱۵ هزار حمله می باشد و می تواند به روش Anomaly Detection هر گونه تغییری در ترافیک عادی شبکه را تشخیص دهد.

- تجهیزات Sophos در بخش "امنیت شبکه های بی سیم"، امکانات فراوانی را برای مدیریت شبکه بی سیم ارائه می دهند که از جمله می توان به امکان HotSpot و امکانات Accounting برای کنترل حجم و زمان استفاده کاربران از اینترنت بی سیم، امکان صدور مجوزهای ساعتی و روزانه برای دسترسی به اینترنت بی سیم و ... اشاره کرد. چنین امکاناتی در بخش بی سیم FortiGate موجود نیست.

- تجهیزات Sophos، امکان امنیتی Web Application Firewall را بصورت یکپارچه در UTM ارائه می دهند که در نتیجه هماهنگ کردن آن با امکانات امنیتی دیگر مانند Firewall و IPS از طریق مدیریت یکپارچه UTM، بسیار آسان تر و بهتر انجام می شود. در حالیکه FortiGate WAF بصورت یک دستگاه جداگانه ارائه می شود.

- شرکت Sophos تجهیزات RED (Remote Ethernet Device) را برای امنیت شعب و دفاتر نمایندگی ارائه می دهد که با استفاده از آن هزینه امنیت این دفاتر و مراکز کوچک بسیار کاهش می یابد. FortiGate فاقد چنین امکانی است و برای امنیت شعب باید دستگاه های UTM جداگانه خریداری کرد که مستلزم پرداخت هزینه اولیه و سالیانه بالا می باشد.

- Sophos امکانات گزارش گیری کاملی از ترافیک شبکه و تهدیدات امنیتی را بر روی دستگاه UTM ارائه می دهد که از طریق واسط تحت web آن به آسانی در دسترس است و امکان زمان بندی گزارشها و ارسال خودکار از طریق ایمیل نیز وجود دارد. در تجهیزات FortiGate برای داشتن گزارش های کامل باید یک دستگاه جداگانه به نام FortiAnalyzer خریداری شود.

- بدلیل محدودیت حافظه در معماری ASIC، تجهیزات FortiGate امکان ویرس یابی فایل های حجیم را ندارند.

- ضدهرزنامه FortiGate بسیار ساده بوده و تنها روشهای RBL و Black List را پشتیبانی می کند. در حالیکه ضدهرزنامه Sophos از ۹ روش مختلف برای شناسایی هرزنامه ها استفاده می کند. علاوه بر این، فهرستی از هرزنامه های شناسایی شده مربوط به هر کاربر برای وی ارسال می گردد تا به تشخیص خود، پیام های مورد نیاز احتمالی را بازیابی کند.

- در محصولات Sophos، تنظیمات سمت کاربر در VPN های IPSec و SSL بطور خودکار ساخته می شود و کاربر فقط باید فایل آن را دریافت و نصب کند. در تجهیزات FortiGate، کاربر باید تنظیمات پیچیده VPN را خودش انجام دهد.

- مدل های پایین FortiGate فاقد دیسک سخت داخلی بوده و لذا قادر به انجام مواردی نظیر قرنطینه هرزنامه ها و ثبت وقایع (log) نیستند. در حالیکه تمام مدل های Sophos دارای دیسک سخت با ظرفیت های بالا می باشند.

- ضد جاسوس افزار (Anti-Spyware) در محصولات FortiGate تنها محدود به ترافیک ورودی می شود. در حالیکه Sophos ترافیک ورودی و خروجی را از لحاظ جاسوس افزارها کنترل می کند.

- سیستم عامل محصولات FortiGate به طور خودکار به روز رسانی نمی شود و تنها به روز رسانی ضدویروس و IPS بطور خودکار صورت می گیرد و مابقی فایل های به روز رسانی باید بطور دستی دریافت و نصب گردند. بانک های اطلاعاتی و سیستم عامل محصولات Sophos کاملاً به طور خودکار به روز شده و هیچگونه محدودیتی نیز برای IP های ایران وجود ندارد.