SOPHOS

Security made simple.

UTM Network Protection

Für ein schnelles und sicheres Netzwerk – ohne Kompromisse

Sophos Network Protection kombiniert zahlreiche Schutztechnologien – für mehrschichtige Advanced Threat Protection. Mit Command-and-Control-Erkennung, Intrusion Prevention System (IPS) und VPN-Gateway sperren Sie gefährlichen ein- und ausgehenden Datenverkehr, damit befugte Benutzer sicher auf Ihr Netzwerk zugreifen können. Gleichzeitig halten Sie über Sophos UTM Sicherheitsrisiken unter Kontrolle und sorgen für eine optimale Performance, die genau auf das von Ihnen gewählte Bereitstellungsmodell zugeschnitten ist.

Highlights

- Als Hardware-, Software-, virtuelle oder cloudbasierte Appliance erhältlich
- Advanced Threat Protection stoppt gezielte Angriffe und APTs
- Integriertes Intrusion Prevention System (IPS)
- Standort-zu-Standort-VPN und Remotezugriff mit sicherem SSL oder IPsec
- Intuitive, browserbasierte Oberfläche zur einfachen Verwaltung
- Integrierte, modellübergreifende Reporterstellung

Bewährter Schutz vor Exploits und Eindringlingen

Unsere Advanced Threat Protection führt alle relevanten Ereignisse in ein gemeinsames Reporting zusammen und stoppt so selbst die gezieltesten Angriffe auf Ihr Netzwerk. Durch die Kombination von Command-and-Control- und Botnet-Erkennung, IPS-Mustern und Deep Packet Inspection werden anwendungs- und protokollbezogene Probes und Angriffe zuverlässig identifiziert und abgewehrt. Die umfangreiche Signaturdatenbank der SophosLabs mit Mustern und Regeln wird alle paar Minuten aktualisiert. Bei Aktivierung unserer Web Protection können Sie unbekannte Dateien außerdem mittels cloudbasiertem Sandboxing auf Schadinhalte untersuchen und Ihren Schutz stetig verbessern.

Optimierung Ihrer Netzwerkperformance

Unsere Software und Hardware sind speziell auf die von Ihnen gewünschten Durchsatzgeschwindigkeiten ausgelegt. Verteilen Sie Ihren Internetdatenverkehr kosteneffizient auf unterschiedliche WAN-Uplinks, und erweitern Sie Ihre Verbindungsoptionen durch den Einsatz von 3G- sowie UMTS-USB-Sticks. Individuelle Optionen garantieren eine ausreichende Bandbreite für definierten Netzwerkverkehr.

Anbindung von Außenstellen mit konfigurationsfreiem VPN

Mehrere Standort-zu-Standort-VPN-Tunnel mit gleichen Regeln für Lastenausgleich und Failover können einfach eingerichtet werden. Und mit unserem konfigurationsfreien Sophos RED-Gerät können Sie Computer in beiden Netzwerken vollständig freigeben oder den Datenverkehr im Tunnel beschränken. Für die Einrichtung in Außenstellen ist kein Fachpersonal erforderlich. Hostnamen für Tunnel mit integriertem Dynamic DNS-Client werden unterstützt.

Sicherer Zugriff für externe Mitarbeiter

Über unser UTM-Benutzerportal sind zahlreiche VPN-Technologien wie IPSec, SSL, Cisco VPN, iOS oder native Windows-VPN-Clients verfügbar. Unser exklusives HTML5 VPN Portal benötigt weder ActiveX oder Java noch eine Clientinstallation. Und es funktioniert auf allen Plattformen: von Windows und Macs bis hin zu iOS und Android. Bei der automatischen Anmeldung werden Zugangsdaten auf dem Gerät gespeichert.

„Sophos fährt eine einheitliche, klare Linie, und die Bedienung der Sophos UTM Appliances ist einfach und intuitiv."

Martin Wolf, CIO der Werke am Zürichsee AG

Technische Details

Abwehr von Eindringlingen

- Blockiert ausgehenden Datenverkehr zu Command-and-Control- und Botnet-Hosts
- Deep Packet Inspection mit über 18.000 Definitionen
- Schutz vor Netzwerküberflutungen (DoS, DDoS, Port-Scan)

Anbindung von Niederlassungen

- Unterstützung von SSL, IPsec
- RED-Technologie zur einfachen Anbindung von Außenstellen
- 256 Bit AES/3DES, PFS, RSA, x.509-Zertifikate, vorinstallierte Schlüssel

Zugriff für externe Mitarbeiter

- SSL, IPsec
- Cisco VPN (iOS-Unterstützung) und OpenVPN (iOS und Android)
- Browserbasiertes HTML5 VPN Portal ohne Plugin-Anforderungen

Sichere Benutzerauthentifizierung

- Sophos Authentifizierungs-Agent für Benutzer
- Unterstützung von Active Directory, eDirectory, RADIUS, LDAP, tacacs+
- Zwei-Faktor-Authentifizierung mit Einmalpasswort z. B. für Benutzerportal, IPSec, SSL, VPN – keine Infrastruktur notwendig

Einfache Verwaltung täglicher Aufgaben

- Self-Service-Benutzerportal
- Nachverfolgung von Konfigurationsänderungen
- On-Box-Protokollierung und identitätsbasierte Reporterstellung
- Planung und Archivierung von Reports

Zuverlässige Verbindung

- Statisch, OSPF, BGP, Multicast (PIM-SM)
- WAN Link Balancing für beliebige Kombinationen von 3G-/UMTS-/Ethernet-Ports
- Aktive/passive Hochverfügbarkeit ohne Konfiguration
- Active/Active-Cluster für bis zu 10 Appliances
- 802.3ad-Schnittstellen-Linkbündelung (LAG)
- Server Load Balancing

Erforderliche Subscriptions

UTM Network Protection. Auch enthalten, wenn Sie unsere Lizenz FullGuard UTM abonnieren.

Unsere Lizenz BasicGuard enthält einen Basisschutz für Ihr Netzwerk, der folgende Funktionen umfasst:

- Filterung von Datenverkehr im Netzwerk mittels Geo IP zum Blockieren von Aktivitäten aus bestimmten Ländern
- Remotezugriff für Benutzer über IPSec
- Standort-zu-Standort-VPNs mit IPSec oder SSL
- Verbindung mit Amazon VPC-Servern

Erweiterter Schutz

Erweitern Sie Ihre UTM Network Protection um UTM Web Protection, und Sie erhalten ausgereifte Next-Gen Firewall-Funktionen. Datenblatt Next-Gen Firewall.

Auszeichnungen und Preise

Jetzt kostenfrei testen

Kostenlose 30-Tage-Testversion unter sophos.de/utm-testen

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 (0) 611 5858-0 | +49 (0)721 255 16-0
E-Mail: sales@sophos.de

Oxford, UK | Boston, USA

1129-02.14DD.dsde.simple