

«Next Generation UTM Appliances» der Enterprise-Klasse

Modern Malware, professionelle Hackergruppen, die vermehrte Einbindung mobiler Devices, verletzte Systeme ... Die IT-Security ist ein anspruchsvolles Unterfangen. Eine Herausforderung, der Next Generation UTM Appliances ganzheitlich begegnen.

IT-Security-Verantwortliche sind mit stetig komplexer werdenden Rahmenbedingungen konfrontiert. Einerseits mit einer Vielzahl an Systemen, Technologien und Applikationen, die allesamt geschützt sein wollen. Andererseits mit ausgeklügelten Angriffsmethoden (Modern Malware), der vermehrten Nutzung von Virtualisierungstechnologien sowie mit cloudbasierten Services und Web-2.0-Anwendungen, die neue Schwachstellen schaffen. Vor dem Hintergrund, dass sich User, Systeme und Programme nicht mehr klar definierten IP-Adressen oder TCP-Ports zuordnen lassen, reichen konventionelle Technologien wie Paketfilter, Content Filter oder IDS/IPS nicht mehr aus, um Gefahren zu erkennen und abzuwehren.

Auch die Nutzung (privater) mobiler Devices (BYOD) sowie die entsprechende Einbindung von WLANs ins Firmennetz bringen konventionelle Security-Appliances und statische Security-Policies an ihre Grenzen. Technologien wie «Secure WLAN», Benutzer- und Geräte-Authentifizierung, IPSEC und SSL VPN, Datenverschlüsselung, Verschleierung, Konformitätsüberprüfung etc. werden zur Notwendigkeit.

Umfassende Kontrolle von Usern, Applikationen und Devices

Um den aktuellen und zukünftigen Gefahren am Perimeter wirksam begegnen zu können, ist ein breit gefächertes Abwehrdispositiv notwendig. Dieses besteht einerseits idealerweise aus UTM-Appliances, die neben «klassischen» «Stateful Inspection Firewall»-Funktionen auch Leis-



Die Next Generation UTM Appliances von Fortinet bilden die zentrale Instanz zur Gewährung einer umfassenden IT-Security.

tungsmerkmale wie VPN, SSL VPN, Antivirus (AV), Antispam, Webfilter, IPS, DLP und teilweise auch E-Mail-Security in einem System vereinen. Andererseits aus Next Generation Firewalls, die sich namentlich durch «Application Control»-Funktionen auszeichnen. Sie sind in der Lage,

Integrale Gesamtlösung von Fortinet

Mit den Next Generation UTM Appliances von Fortinet stehen nun integrale Gesamtlösungen zur Verfügung, die den ganzen LAN- und WLAN-Datenverkehr sowie User, Devices und Applikationen in Echtzeit überwachen,



User, Applikationen und Devices zu erkennen und zu kontrollieren. Zudem ermöglichen sie eine granulare Definition, welche Applikationen – oder Teile davon – wann und für wen zugelassen oder gesperrt sind (User based Policy Enforcement). So ist es beispielsweise möglich, HTTPS firmenweit freizugeben, hingegen Online-Browser-Spiele zu blockieren und die Freigabe von Social-Media-Applikationen zeitabhängig zu steuern.

visualisieren und – wenn nötig – auf Basis der definierten Security-Policies und stets aktualisierter Signatures aktiv ins Geschehen eingreifen. Selbst verschlüsselter Code, der über Protokolle wie HTTPS, POP3S, SMTPS und IMAPS transportiert wird, kann analysiert werden.

Die Leistungsmerkmale der hochperformanten Enterprise- und Data-Center-Plattform FortiGate 3600C stehen stellvertretend für das breite Fortinet-Lösungsangebot:

- Hoch performante Next Generation UTM Appliance – geeignet für Grossunternehmen, Data Center und Anbieter von Managed Security Services
- Nahtlose Einbindung bzw. Absicherung von LAN- und WLAN-Infrastrukturen (Secure WLAN)
- WLAN-Einbindung über eigene Thin Access Points (FortiAP), welche pro SSID auf der Firewall virtuelle Interfaces generieren
- Maximierte Performance dank ASIC-basierten Beschleunigungskarten der neuesten Generation (spezifische Security-Aufgaben wie IPS, AV-Inspection, SSL-Entschlüsselung oder User- und Application-Control werden in einer dedizierten Umgebung parallel ausgeführt und beschleunigt)
- Hohe Portdichte (physische Ports) inkl. 10 GBit Ethernet Ports
- Virtualisierte Ports (VLAN)
- Virtualisierte, komplett getrennte Domains (VDM)
- Bis zu 500 virtualisierte Firewall-Instanzen
- Geringste Latenzzeit von lediglich 4 µs (Firewall Latency)
- Bis zu 28 Mio. gleichzeitige Sessions
- Intrusion Prevention (IPS) von 14 Gbps
- Maximale Verfügbarkeit (High Availability) dank Features wie Cluster-Installationen, geografische Redundanz und unterbrechungsfreie Upgrades

BOLL Engineering AG
 Jurastrasse 58
 5430 Wettingen
 Tel. 056 437 60 60
 info@boll.ch, www.boll.ch