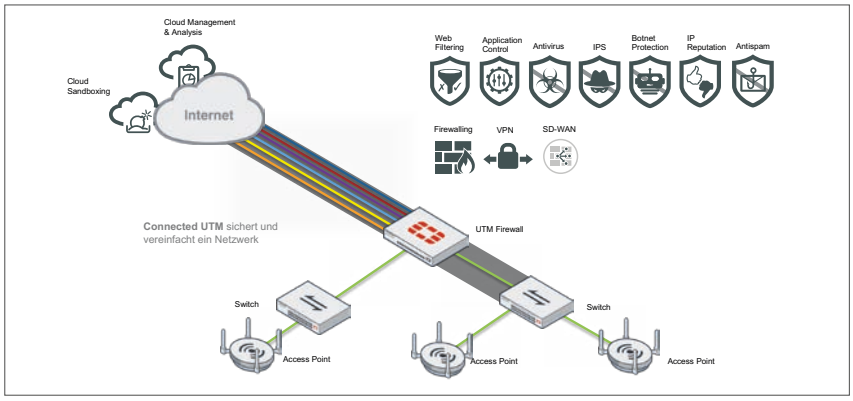
Total Security: die UTM-Evolution

UTM-Appliances erhalten laufend neue Funktionen. Über die Firewall hinaus gewähren moderne Lösungen umfassende Sicherheit, bieten integriertes WLAN-Management und werden zur Schaltzentrale für das gesamte Firmennetzwerk.



Netzwerksicherheit ist für alle Unternehmen matchentscheidend – egal, ob es sich um ein KMU oder einen Grosskonzern handelt. Den Grundstein jedes Sicherheitskonzepts bildet die Firewall: Herkömmliche Layer-4-Firewalls mit Stateful Inspection sperren oder öffnen anhand von Regeln für jede Verbindung bestimmte Netzwerk-Ports.

UTM bringt umfassende Sicherheit

Das Basic-Firewalling genügt jedoch nicht, um die immer raffinierteren Bedrohungen abzuwehren. Dafür braucht es UTM-Appliances (Unified Threat Management). Dabei werden möglichst viele Sicherheitsfunktionen in einem leistungsstarken System zusammengefasst. Typische UTM-Komponenten sind Antivirus und Antispam, VPN, Angriffserkennung und Angriffsabwehr (IDS/IPS) sowie URL-Filter zum Blockieren gefährlicher Webadressen. UTM-Appliances sind zum Beispiel von Fortinet und WatchGuard erhältlich, oft auch als virtuelle Appliance oder als Software-as-a-Service.

Im Laufe der Zeit sind zu den klassischen UTM-Features immer wieder neue Funktionen hinzugekommen. Dazu gehört etwa eine Application Firewall, auch Application Control oder Layer-7-Firewall genannt. Die UTM-Appliance sorgt in diesem Fall auch für die gezielte Freigabe oder Sperrung von Anwendungen, Webdiensten und Netzwerk-Services.

Verschlüsselte und unbekannte Schädlinge erkennen

Eine wichtige UTM-Funktion ist das SSL-Scanning. Beim Surfen, für E-Mails und bei Webanwendungen kommen praktisch nur noch SSL-verschlüsselte Verbindungen vor. Den verschlüsselten Verkehr inklusive Schadcode und gefährlicher URLs kann die Firewall jedoch nicht analysieren. Antivirus, Webfilter und Co. ergeben nur dann einen Sinn, wenn die Daten offen bereitstehen. Dazu muss die UTM-Appliance die SSL-Verschlüsselung aufbrechen und nach der Analyse die Daten wieder verschlüsseln. Diesen Vorgang nennt man SSL-Scanning.

Mit Sandboxing, einem weiteren neueren UTM-Feature, lässt sich auch Schadcode erkennen, der von der Antivirus-Engine nicht als schädlich erkannt wurde. Dateien mit aktivem Code werden dabei in einer abgeschotteten virtuellen Umgebung ausgeführt. Eine Datei wird nur dann weitergeleitet, wenn dabei nichts Gefährliches passiert ist. Sandboxing ist sehr rechenaufwendig. UTM-Appliances nutzen dazu meist einen Cloud-Service des Herstellers. Da der Vorgang Zeit in Anspruch nimmt, eignet sich Sandboxing vor allem für Anhänge von E-Mails, die ja ohnehin nicht in Echtzeit übermittelt werden.

Unerwünschte Gäste abwehren

Manche UTM-Appliances ermöglichen Geo-IP-Firewalling, auch als Geoblocking bekannt. Damit kann die Kommunikation aus bestimmten Ländern komplett abgeblockt werden.

Vergleichbar mit dem Geoblocking ist die Sperrung bestimmter IP-Adressen anhand ihrer Reputation. UTM-Hersteller pflegen dazu Listen von als gefährlich erkannten Systemen. Ein gutes Beispiel sind IP-Adressen von Botnetzen.

Das Netzwerk im Griff

Einige UTM-Hersteller wie Fortinet und WatchGuard haben zusätzlich zu den Sicherheitsfunktionen einen Wireless-Controller in ihre Geräte integriert. Die UTM-Appliance verwaltet so auch alle Aspekte des WLAN, das damit in den Genuss der gleichen Sicherheit wie das LAN kommt. Der Wireless-Controller erlaubt es beispielsweise, den Sicherheitsstandard WPA Enterprise zu nutzen. UTM-Appliances mit integriertem Wireless-Controller eignen sich besonders für KMU oder Zweigstellen.

Eine weitere Funktion von UTM-Appliances neueren Datums ist SD-WAN. Das Gerät kann mehrere Internetanschlüsse zu einer redundant ausgelegten, einfach zu konfigurierenden VPN-Verbindung mit automatischem Failover zusammenfassen. Damit lässt sich ein teures, MPLS-basiertes Privatnetzwerk durch günstige Internetzugänge ersetzen.

Fortinet geht als erster Hersteller noch einen Schritt weiter: Zusätzlich zur Sicherheit und zum Wireless-Controller ermöglicht integriertes Switch-Management, die gesamte Struktur des Netzwerks komplett über die Oberfläche der UTM-Appliance zu verwalten. So lassen sich etwa virtuelle Netzwerkunterteilungen (VLANs) direkt über die Oberfläche der UTM-Appliance definieren, und zwar gleichzeitig auf der Firewall und auf den Switches. Bisher musste ein VLAN auf beiden Systemen separat konfiguriert werden. Die Integration ermöglicht zudem, das gesamte Netzwerk bis hin zum einzelnen Client zu visualisieren. So entsteht eine bisher unerreichte Übersicht, und alle Umgebungen – LAN, WLAN und Sicherheit – lassen sich einheitlich bedienen.

BOLL
IT Security Distribution

BOLL Engineering AG

Jurastrasse 58
5430 Wettingen
Tel. 056 437 60 60
info@boll.ch | www.boll.ch