



Integrale, netzwerkbasierte IT-Security bietet umfangreiche Sicherheit

Stoppt die Angriffe – bevor sie euch stoppen

Ob KMU oder Grosskonzern – die Aspekte der netzwerkbasierten IT-Security stellen vielerorts eine schier unlösbare Problematik dar. Die Notwendigkeit an uneingeschränkt hohen Datenraten, der Mangel an eigenen Sicherheitsexperten sowie eine nicht enden wollende Fülle an teuren Security-Komponenten, die allesamt administriert werden wollen, scheinen eine umfassende, hochgradige Sicherheit zu verunmöglichen. Integrale Security-Appliances schaffen Abhilfe.

Autor: Damian Suter, Captiva GmbH

Unternehmen und Internet-Service-Provider (ISPs), die den weit reichenden Aspekten einer umfassenden, netzwerk-basierten IT-Security das notwendige Gewicht beimessen, sind bzw. waren gezwungen, sich mit einer Vielzahl komplementärer Sicherheitskomponenten zu bestücken. Gilt es doch, den unzähligen Gefahren wie Viren, Würmer, Trojaner, DoS-Attacken (Denial of Service) oder unerwünschten Eindringlingen effektiv zu begegnen. Auf Grund der Tatsache jedoch, dass das Gros der heute erhältlichen Firewalls lediglich Teilaspekte der Netzwerksicherheit adressieren, wurde eine umfassende Security-Lösung für viele Firmen erst durch den Verbund mehrerer Einzelsysteme realisierbar.

Vielfältige Bedrohungen – unterschiedliche Lösungen

Die im Bereich der Netzwerksicherheit relevanten Bedürfnisse sind vielfältig und stellen an Firewalls und deren «Kompagnons» höchste Anforderungen. Sie lassen sich gliedern in die folgenden Themenbereiche und Kontrollverfahren:

- Paketfilter:** Statische Paketfilter-Firewalls prüfen die Send- und Empfangsadresse der einzelnen Datenpakete gemäss vordefinierten Regeln. Typische Vertreter dieser «Stateless Inspection»-Technologie sind kleinere Breitband- und ADSL-Router. Weiter gehen so genannte dynamische Paketfilter (Stateful Inspection). Auch sie überprüfen die Datenpakete auf Netzwerkebene, verwenden jedoch auch Kontext- und Zusatzinformationen des IP-Headers zur Prüfung von Kommunikationsbeziehungen. Allen Paketfilter-Firewalls gemeinsam ist die Über-

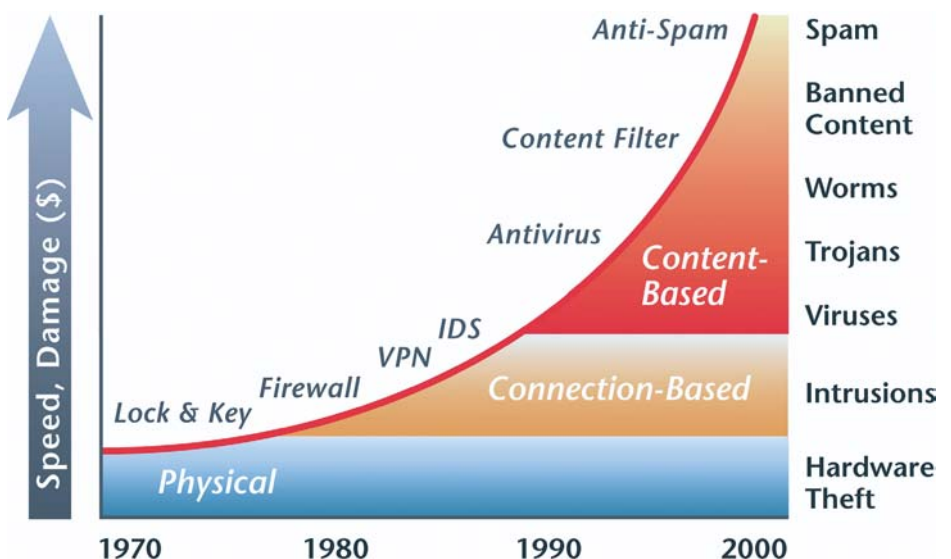


prüfung der Datenpakete in Echtzeit. Der Datenverkehr erfolgt also selbst bei hohem Datendurchsatz verzögerungsfrei. Allerdings sind Stateful-Inspection-Lösungen nicht in der Lage, die Datenpakete auf schädliche Inhalte wie z. B. Viren zu überprüfen, weshalb sie oft mit separaten Antivirus-Lösungen wie etwa der Virus-Wall von Trend Micro kombiniert werden.

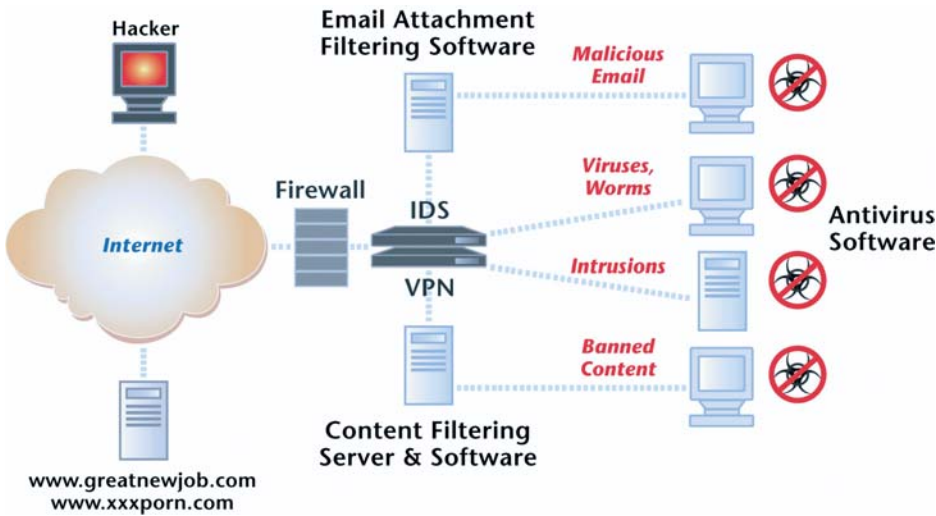
- Proxies bzw. Application-Gateways:** Im Gegensatz zu Paketfiltern überprüfen Proxy-Firewalls bestimmte Protokolle und Datenpakete auf ihren Inhalt. Sie bieten also ein limitiertes Content-Scanning und sind in der Lage, gewisse schädliche Elemente zu erkennen und abzuwehren. Da sich ein Grossteil der Gefahren aus dem Internet ausschliesslich innerhalb der Applikations-Proto-

kolle erkennen lässt, ist es notwendig, den gesamten Netzverkehr zu scannen. Proxy-Dienste bieten diesbezüglich zwar eine erhöhte Sicherheit, kommen aber trotzdem oft nicht zum Einsatz. Dies auf Grund der Tatsache, dass die rechenintensive Überprüfung der Daten bei allen konventionellen Firewalls zu einem stark reduzierten Datendurchsatz führt. Zahlreiche Benutzer stehen also vor der Wahl: Sicherheit versus Geschwindigkeit.

- Antivirus:** Proxy-Firewalls alleine reichen nicht aus, zerstörerische Viren, Trojaner und Würmer wirklich zu erkennen und abzuwehren. Erst durch die Verifikation der übertragenen Daten mit aktuellen Signaturen besteht Gewähr, dass der Datenstrom auf alle Gefahren hin überprüft wird. Firewalls, die Antivirus nur mit konventioneller, auf dem Arbeitsplatzrechner installierter Antivirus-Software unterstützen, bieten diesbezüglich keinen genügenden



Die Gefahren haben sich gewandelt: Inhaltsbasierende Angriffe via Internet werden durch konventionelle Firewalls nicht erkannt und verursachen unermessliche Schäden



Konventionelle Security-Lösungen basieren auf dem Verbund einzelner, teurer Systeme, die den aktuellen Sicherheitsbedürfnissen mehrheitlich nicht genügen

Schutz. Von einer zukunftsweisenden Security-Appliance darf erwartet werden, dass sie eine eigenständige «Signatur Scanning Engine» beinhaltet, die sämtliche via Internet übertragbare Viren kennt und eine Echtzeit-Überprüfung des Datenverkehrs erlaubt.

- VPN – Virtual Private Network:** Virtuelle private Netzwerke gewähren externen Mitarbeitenden, Aussendienstlern oder autorisierten Partnern via Internet einen sicheren Zugriff auf Firmendaten und Applikationen. Dabei werden die einzelnen Datenpakete verschlüsselt durch einen speziellen «Tunnel» sicher übertragen, sind für Dritte also nicht einsehbar. Heute beinhalten beinahe alle Firewalls ab einer mittleren Preisklasse VPN-Funktionalität.

- Intrusion Detection (IDS) und Intrusion Prevention (IDP):** Firmennetzwerke weisen immer offene Ports auf (so z. B. Port 80 für HTTP-Dienste). Diese bilden ideale Einstiegspforten für Attacken oder die Übermittlung von Trojanern. Zu den «gängigen» Angriffen zählen etwa Denial of Service-(DoS-)Attacken. Dabei werden einzelne IP-Adressen mit unzähligen Datenpaketen beschossen, bis sie unter der Last zusammenbrechen und ihren Dienst nicht mehr aufrechterhalten können. Als besonders perfide erweisen sich sogenannte distributed (verteilte) DoS-Attacken, die von mehreren Rechnern aus erfolgen und gut und gerne Tage oder gar Wochen dauern können. Die Schäden, die durch derartige Attacken ausgelöst werden, sind enorm – bei

ISPs führen sie bestenfalls zu einem grossen Image-Verlust. Um gefährliche Attacken dieser Art abzuwehren, werden Firewalls in der Regel mit speziellen Intrusion Detection Appliances ergänzt. Wichtig dabei ist allerdings, dass entsprechende Systeme mit IDP-Funktionalität ausgestattet sind. Nur so besteht die Gewähr, dass Angriffe nicht nur erkannt, sondern auch abgewehrt werden.

- Traffic Shaping:** Nicht alle via Netzwerk übertragenen Daten sind von derselben Wichtigkeit. Gewisse Dienste bedingen der Echtzeitübertragung (z. B. Sprache bzw. Voice over IP). Andere Daten wiederum sind auch mit einer verzögerten Übertragung uneingeschränkt nutzbar (z. B. E-Mail bzw. SMTP-Dienste). Traffic-Shaping-Systeme erlauben, einzelne Dienste priorisiert zu behandeln. Dadurch lassen sich wichtige Services auch bei hohen Datenvolumen in einer definierten Qualität übertragen (Quality of Service, QoS), was insbesondere für ISPs und deren angebotenen Dienste von zentraler Bedeutung ist.

Der klare Trend – integrale Lösungen

Security-Lösungen, die sämtlichen relevanten Sicherheitsaspekten gerecht werden, sind per dato mehrheitlich heterogene Gebilde. Die Verknüpfung unterschiedlichster Komponenten diverser Hersteller zu einer Gesamtlösung jedoch führt einerseits zu enorm hohen Kosten (Beschaffung und Unterhalt). Andererseits stellen Aspekte wie Konfiguration, Systemmanagement, Wartung und Up-Gr-

Firmenprofil

Boll Engineering mit Sitz in Wettingen ist Full-Service-Master-Distributor in den Bereichen IT-Security und Internet Access mit ausgeprägter System-Engineering-Kompetenz. Dazu zählen u. a. professionelle, kompetente Beratung sowie Konzept- und Implementierungsunterstützung.

Wichtigste Vertretungen:

- Fortinet:** ganzheitliche Anti-Virus Firewall-Appliance für sämtliche Unternehmensgrößen
- WatchGuard:** Firewall-Systeme für sämtliche Unternehmensgrößen
- DrayTek:** integrierte Breitband- und ADSL-Router
- Coyote Point Systems Inc.:** Geo Load Balancer für ISPs und ASPs

de kaum lösbare Probleme dar. Alternativen sind folglich gefragt. Allerdings: Integrale Lösungen – Security Appliances also, die sämtliche Dienste in einer Plattform vereinen – waren bis vor kurzem nicht erhältlich. Erst seit der Gründung der Firma Fortinet durch den visionären Security-Experten Ken Xie (ehemaliger Gründer und CEO von NetScreen) erfuhr der Security-Markt die notwendige Wende.

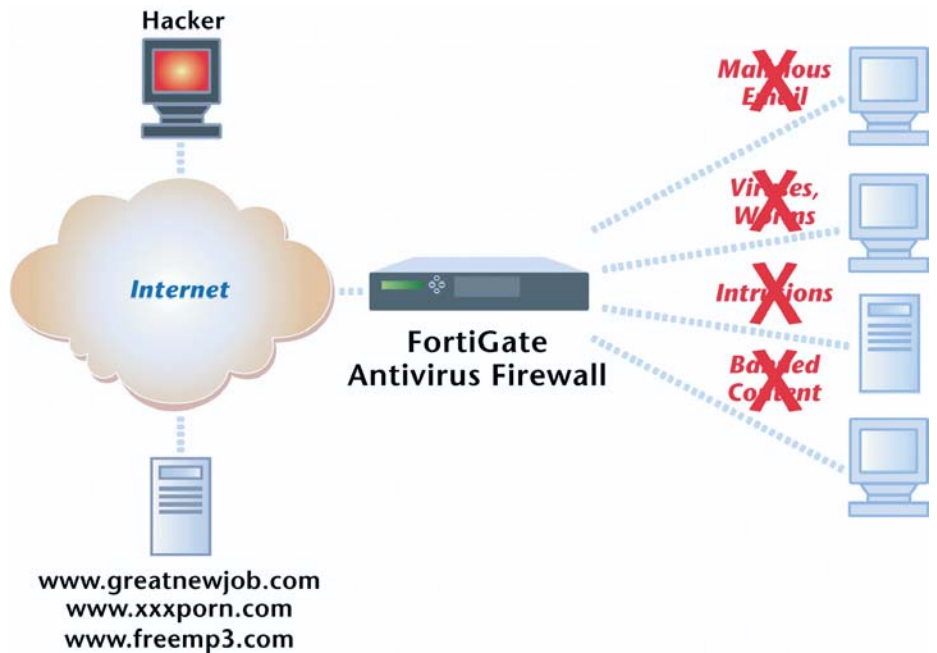
Heute darf die Security-Appliance FortiGate als wegweisende Firewall-Architektur bezeichnet werden. Dabei handelt es sich um eine ultraschnelle Firewall, die den gesamten Netzverkehr sowie den Inhalt der einzelnen Datenpakete in Echtzeit verifiziert (bis zu einer Geschwindigkeit von 4 GBit/s) sowie alle notwendigen Abwehrmechanismen beinhaltet.

Herzstück jeder FortiGate bildet ein eigens entwickelter ASIC-Prozessor (FortiASIC), der aus einer «Firewall Engine» sowie einer «Signature Scanning Engine» besteht und, je nach Modell, ein Cache Memory von 64 MByte bis 1 GByte beinhaltet. Er ist in der Lage, sowohl IP-Header als auch den gesamten Inhalt der IP-Pakete in Echtzeit zu scannen und mit den im systemeigenen Memory gehaltenen Signaturen zu vergleichen. Dadurch lassen sich sowohl inhaltsbezogene Funktionen wie Virenschanning, Web- und URL-Filtering als auch Dienste wie VPN-Verschlüsselung/Entschlüsselung oder Intrusion Prevention integrieren – ohne dabei den Datenfluss zu beeinträchtigen.

Von der Firewall zur Security Appliance

«Dass es sich bei jedem System von Fortinet um eine komplett umfassende Security-Lösung handelt, wird bei der Betrachtung weiterer Leistungsmerkmale deutlich», betont Urs Fink, Vertrieb des Schweizer Master-Distributors Boll Engineering. «So sind alle FortiGate Appliances von der ICSA für Antivirus, Firewall, VPN und Intrusion Detection zertifiziert. Zudem unterstützen die skalierbaren Security-Appliances wichtige Funktionen wie Traffic Shaping und Stateful Failover, um auch in anspruchsvollsten Netzwerkumgebungen einen umfassenden Schutz zu gewähren.» Auf die Frage der Vielseitigkeit antwortet er: «Auch bei bereits bestehenden Firewall-Infrastrukturen sind die FortiGate Appliances eine ideale Ergänzung, um Server und Clients zusätzlich mit Intrusion Prevention, AntiVirus und Content Filtering bereits am Perimeter umfassend zu schützen.»

Thomas Boll, Gründer und CEO des Netzwerkspezialisten Boll Engineering, macht ferner auf die Multi-Zonen-Unterstützung (Systeme mit bis zu 12 Ports) der FortiGate Security Appliances aufmerksam. «Damit lässt sich eine flexible Netzwerksegmentierung mit individuel-

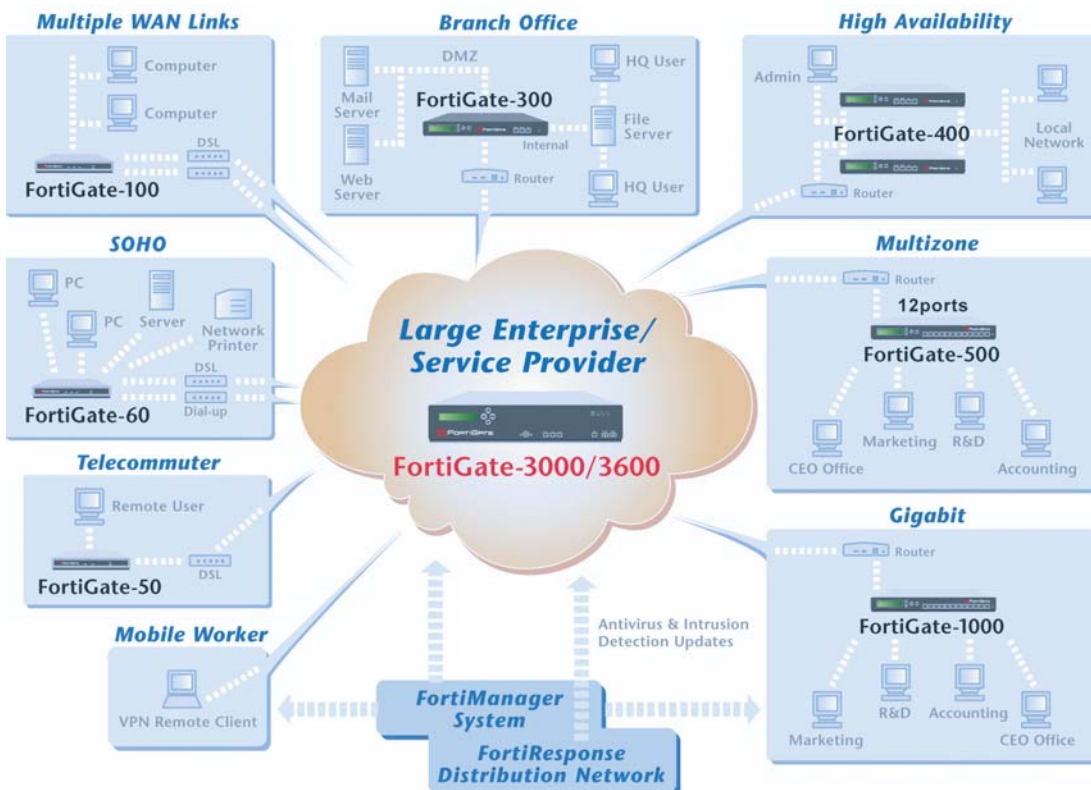


Die integralen Security-Appliances FortiGate von Fortinet vereinen sämtliche relevanten Sicherheitsmodule in einem System: Firewall, VPN, Intrusion Detection, Antivirus, Content Filtering (Mail/Web) und Traffic Shaping

len Sicherheits- und Zugriffsregeln realisieren.» Und er ergänzt: «Die Kombination aller relevanten Security-Funktionen in einem System führt zu einer drastisch vereinfachten Konfiguration sowie zu wesentlich geringeren Administrations-, Unterhalts- und Wartungskosten. Über das

zentrale Managementtool FortiManager lassen sich beliebig viele FortiGate-Einheiten intuitiv bedienen.»

Boll Engineering AG, Urs Fink
 Mythenstrasse 4, 5430 Wettingen
 Tel. 056 437 60 60, Fax 056 427 29 29
 urs.fink@boll.ch
 www.boll.ch, http://fortinet.boll.ch, www.fortinet.com



Die umfassende FortiGate Modellpalette bietet für KMUs wie für Grossunternehmen eine optimale Lösung. Sämtliche Basisfunktionen stehen bereits beim kleinsten Modell vollumfänglich zur Verfügung.