

Mit GateProtect die Sicherheit modellieren

Test: Grafisches Unified Threat Management

Firewalls und Unified Threat Management gibt es zuhauf auf dem Markt. Ihre Verwaltung ist meist regelbasiert. GateProtect liefert in seinen Appliances einen neuen Ansatz zur Verwaltung.

Von Johann Baumeister

Klein wie ein Buch

GateProtect liefert Sicherheitstools zum Schutz des Netzwerks. Das Produktportfolio reicht von den kleinen Firmen mit zehn Benutzern bis hinaus zu Unternehmen mit 10.000 Anwendern.

Damit adressiert GateProtect das gesamte Spektrum von SOHO-Markt bis hin zum gehobenen Mittelstand. Eines dieser Modelle, die GPO 125, haben wir uns in einem Test näher angesehen.



Die GPO 125 ist für 25 Benutzer ausgelegt und wird als kleine Appliance in der Größe eines Buches im Format A5 mit etwa 5 cm Höhe geliefert. Diese Box lässt sich damit recht unauffällig an jedem Arbeitsplatz unterbringen. Auf der Rückseite des Gerätes befinden sich vier Ethernet-Ports, zwei USB-Anschlüsse, ein VGA-Anschluss, eine Reset-Taste und der Anschluss für die Stromversorgung.

Auf der Vorderseite finden sich jeweils 2 LEDs für die vier Ethernet-Ports, 1 LED für die Harddisk und eine weitere, die Auskunft über die Stromversorgung gibt. Im Inneren der Appliance befindet sich ein vollständiger Rechner samt Festplatte.

Linux-basiertes UTM-Tool

Die Software von GateProtect ist auf einem Linux-System aufgebaut, doch davon sieht der Anwender in der Regel nichts. Als Unified-Threat-Management-Tool (UTM) konzipiert, wird die Box zwischen das interne Netz und das Internet geschaltet. Dazu dienen die Netzwerkschnittstellen auf der Rückseite. Die vier Ethernet-Ports sind wahlfrei zu belegen. In der Regel wird man eine davon für den Zugang nach außen verwenden. Die anderen drei erlauben die Definition von bis zu drei Subnetzen des Unternehmens-LAN.

Durch die VLAN-fähigen Switches lässt sich die Anzahl der Subnetze darüberhinaus noch erweitern.

Zur Verwaltung des UTM-Systems liefert der Hersteller eine grafische Konsole, den Admin-Client. Diesen haben wir von der Website des Herstellers bezogen und auf einen Rechner mit Windows XP eingerichtet. Das Setup ist schnell passiert und folgt den dabei üblichen Gepflogenheiten. Wird anschließend der Admin-Client gestartet, so baut er eine Verbindung mit der Appliance auf. Im Test verkabelten wir unseren Administrations-Rechner über einen Switch mit dem Port 1 (eth0).

Setup der Appliance durch USB-Stick

Nachdem wir einige Testkonfigurationen vorgenommen hatten, setzen wir das Gerät wieder in den Ursprungszustand zurück und richteten die Appliance neu ein. Hierzu ist von der Website des Herstellers ein Software-Modul zu laden. Dieses wird auf einem Standard-Windows-Rechner ausgeführt. Dabei erzeugt dieses Programm ein Boot-Image für einen USB-Stick. Mit diesem Stick ist dann die Appliance neu zu installieren.



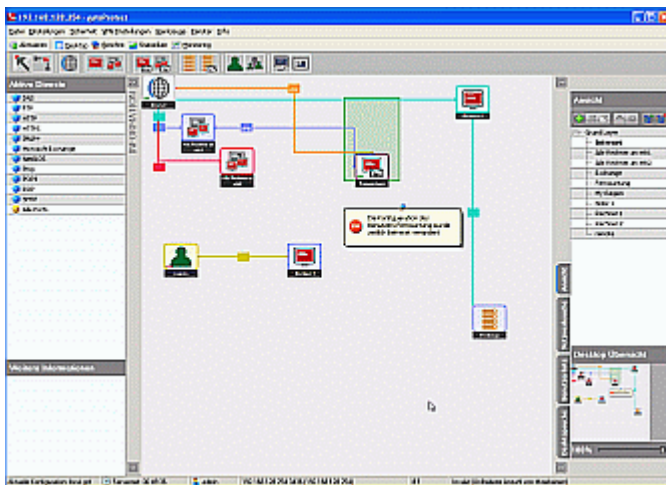
Das Einrichten der UTM verlangt im Wesentlichen nur die Angabe der IP-Adressen für die vier Ports. Diese nahmen wir anhand des im Testlabor vorherrschenden IP-Schemas vor.

Im Test ergaben sich Adressen, die wir so nicht wünschten. Wir entschieden uns daher das System erneut einzurichten und peinlichst auf die IP-Adressen zu achten, zumal dieser Vorgang in weniger als 15 Minuten durchlaufen ist.

In der Regel wird die Einrichtung der UTM-Firewall in das kundenspezifische Netzwerk von geschulten GateProtect Partnern übernommen, die solche Anfangsprobleme wie wir nicht mehr haben, versicherte uns der Hersteller.

Grafisches Verwaltungstool vereinfacht Administration

Bei der Arbeit mit der Verwaltungskonsole sticht die etwas ungewohnte Management-Oberfläche ins Auge. In der Regel erfolgt die Konfiguration von gängigen Firewalls durch Regeln, die in Tabellen zusammengefasst werden. GateProtect kennt zwar auch diese Regelsätze, unterlegt diese aber mit einer grafischen Darstellung. Die Grundlage dazu stellen verschiedene Verwaltungsobjekte dar. Dies sind Objekte für den Internetzugang, die Benutzer oder Benutzergruppen, Rechner oder Rechnergruppen, einen Server oder mehrere Server in einer DMZ und einen VPN-Rechner oder eine Gruppe mit VPN-Zugang.



(Bild: Zur Definition der Zugriffsrechte baut GateProtect auf eine grafische Modellierung. Zur Vergrößerung klicken: Links die freigegebenen Dienste, in der Mitte die grafisch dargestellte Netzstruktur, rechts die Ansteuerung mit Layers z.B. für Abteilungen oder Nutzergruppen)

Für all diese Objekte liefert GateProtect grafische Symbole. Diese platziert der Administrator auf einem Arbeitsblatt. Um beispielsweise einem Benutzer oder einer Gruppe einen Zugang zum Internet einzurichten, werden die beiden Objekte Benutzer(Gruppe) und Internet benötigt. Ferner sind diese Objekte durch eine Linie zu verbinden. Diese Linie symbolisiert die Kommunikationsverbindung zwischen dem Benutzer und dem Internet. Die Eigenschaften dieser Verbindung beschreiben dann die, durch GateProtect überwachte, Kommunikation zwischen den beiden Objekten. Diese Konfigurationsart ist intuitiv und per Drag-an-Drop gesteuert. Die Darstellung orientiert sich an jenen, wie es beispielweise bei Microsoft Visio verwendet wird.

Durch Doppelklick auf die Verbindungslinie zwischen zwei Objekten öffnet sich ein Regeleditor. In diesem werden nun die Firewall-Regeln erstellt und geändert. An dieser Stelle orientiert sich GateProtect an den gängigen Verfahren, denn diese Regelsätze sind mit jenen von anderen Produkten dieses Segments zu vergleichen. In den Regeln werden die Protokolle, die bei GateProtect »Dienst« heißen, verwaltet. Unter diesen Diensten befinden sich beispielsweise die folgenden bereits vordefinierten Kategorien, die bis auf User- oder IP-Ebene individuell konfiguriert werden können:

- Standard: darunter fallen die Protokolle IPX, DNS, LDAP , PING, Kerberos oder Exchange-Anbindung
- Internet, wie etwa HTTP, HTTPS, FTP, Pop3
- Datenbank-Zugriffs-Protokolle
- VPN-Verwaltung
- Fernwartung und die dazu notwendigen Kommunikationstechniken
- Eigene Protokolle deren Port explizit einzustellen ist

Im Rahmen des Tests definierten wir den http-Zugang eines Clients zum Internet und hinterlegten das Protokoll dafür. Anschließend erweiterten wird die Protokolle und Regeln um weitere Möglichkeiten wie Https, DSN und Ping. Ferner nahmen wir weitere Geräte und Gruppen dazu. Die Arbeitsweise des Sicherheits-Tools ist logisch und erlaubt eine flotte Konfiguration.

Ein Bündel an Sicherheitsfunktionen

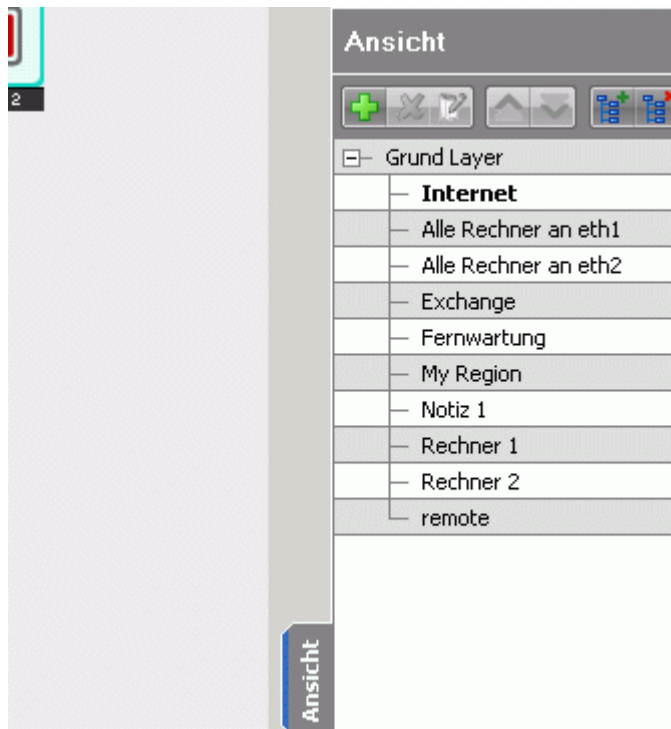
Nach diesen Basistests, die den Browserzugang zum Internet zum Ziele hatten, wandten wir uns den weiteren Sicherheitsfunktionen der Appliance zu. Dazu gehört auch ein Antivirus-Scanner. Dieser unterscheidet nach den Kommunikationsprotokollen http, FTP, POP3 und SMTP. Um dessen Funktionsweise zu prüfen, richteten wir einen Mailclient auf einem weiteren Gerät ein. Durch diesen holten wir mittels POP3 Emails von unserem Provider ab. Eine dieser Emails wurde mit einem Testvirus versehen. Diesen erkannte die GPO 125 korrekt und informierte uns darüber.

Ferner hat der Hersteller einen URL-Filter dazu gepackt. Durch die Definition von »White Lists« und »Black Lists« lassen sich die Zugriffe fein steuern. Der integrierte Content Filter überwacht den Zugriff auf die Webseiten. Zur Konfiguration der Filter dienen reguläre Ausdrücke, die sich dann an die jeweiligen Anforderungen anpassen lassen. Die Einstellungen lassen sich anhand unterschiedlicher Kriterien wie etwa der Zeit weiter verfeinern. Dadurch ist es beispielsweise möglich, Mitarbeitern nach Büroschluss den Zugang zum Internet zu gewähren, in den Bürozeiten aber zu unterbinden.

Außerdem verfügt die GPO 125 optional über einen Spam-Filter aus dem Hause Commtouch. Durch den Einsatz von Real Time Detection Centers werden Spam, Virus oder auch Phishing Attacken anhand von charakteristischen Mustern beim Ausbrechen erkannt.

Grafische Modellierung der Sicherheitseinrichtung

Die grafische Modellierung der Kommunikation ist eine Besonderheit des Werkzeugs. Das Schaubild erlaubt einen schnellen Überblick über die gesamte Konfiguration des Systems. Um nicht für jeden Kommunikationsweg ein eigenes Symbol und eine eigene Verbindung aufbauen zu müssen, werden Gruppen gebildet. Diese repräsentieren beispielsweise die Kommunikation für eine Fachabteilung. Aber auch dann kann das Schaubild recht umfangreich werden. Daher lassen sich die Kommunikationswege in der Anzeige in mehreren Ebenen modellieren. Diese Ebenen sind wahlfrei, wie zum Beispiel nach Standorten oder Gebäuden, zu gestalten der aufzubauen. Die Anzeigen und ihre Ebenen lassen sich auch ausblenden. Dies hilft, um den Überblick zu bewahren.



Durch die integrierte Zoomfunktion lassen sich die wichtigen Bereiche außerdem hervorheben. Für große und umfangreiche Netzwerkschaubilder kann sich der Administrator auch eigene Ansichten zusammenstellen. Ferner lassen sich die Verbindungen mit unterschiedlichen Farben versehen. Hinzu kommt außerdem, dass sich die Objekte auch übereinander lagern lassen und somit zu mehr Übersicht des Schaubilds beitragen.

Fazit: Angenehme Sicherheitsverwaltung

Die Arbeiten mit der GateProtect-Appliance sind, nachdem man sich mit den Konzepten der grafischen Verwaltung vertraut gemacht hat, intuitiv und angenehm.

Die Box liefert einen umfangreichen Schutz für mittelständische Unternehmen. Diese vereinfacht die Verwaltung des Systems, gerade für die Zielgruppe des Mittelstands, deren Administratoren als Allrounder unterschiedlichste IT-Geräte verwalten müssen.

Die Inbetriebnahme des Systems kann außerdem, um Fehler zu vermeiden, durch Unterstützung der GateProtect-Partner erfolgen.

<http://www.it-im-unternehmen.de/tests/2009/09/10/test-grafisches-unified-threat-management>