Im Test: Cyberoam CR50ia

Netzwerkverkehr unter Argusaugen

von Sandro Lucifora

Der beste Schutz vor externen Bedrohungen wäre es, das eigene Netzwerk nicht mit dem Internet zu verbinden – im heutigen Geschäftsumfeld eine undenkbare Variante. Andere Lösungen für den sicheren Aufenthalt im World Wide Web sind deshalb Pflicht. Cyberoam bietet mit dem Modell "CR50ia" eine UTM-Appliance an, die das Firmennetzwerk nicht nur gegen Gefahren aus dem Internet schützen soll, sondern auch das Einrichten von VPN-Tunneln und das Filtern des Datenverkehrs erlaubt. IT-Administrator hat für Sie ausführlich getestet, ob das Gerät all diese Funktionen zufriedenstellend erfüllen kann.

Um die Anforderungen verschiedener Netzwerke zu bedienen, hat Cyberoam seine UTM-Serie in verschiedene Leistungsmodelle gefasst. Die Dimensionierung für die eigene Absicherung ist dabei nicht nur von den im Netzwerk betriebenen Arbeitsplätzen abhängig, sondern muss vor allem den Anforderungen an den Datendurchsatz sowie den laufenden Datenverkehr gerecht werden. Unser Testgerät Cyberoam CR50ia siedelt sich im ersten Drittel der Leistungsklasse an und eignet sich als Torwächter von mittelgroßen Netzwerken.

Großzügige Ausstattung

Als Appliance zum Unified Threat Management (UTM) dient die CR50ia vorrangig als Inhalts-Filter im Datenaustausch und regelt durch die Firewall und den gesicherten VPN-Zugang den Zugriff von außen ins LAN. Zusätzlich will die Lösung die Auslastung der WAN-Verbindungen verbessern. Auf Basis von Fedora Linux, versehen mit einer Intel Celeron 1,6 GHz-CPU, 512 MByte Speicher und einer 80 GByte Festplatte, ist das Gerät für seine Aufgaben gut ausgestattet.

Auf den ersten Blick bietet die Appliance eine ganze Menge Funktionen. Dass das Gerät Routing und Firewall beherrscht, stellt keine Überraschung dar. Einen Mehrwert zu anderen Lösungen finden wir im Benutzer-basierten UTM: Dies bedeutet, dass der Administrator IP- und User-basiert Regeln aufstellen kann, die den Zugriff auf das Internet steuern. Vor der Internet-Nutzung muss sich jeder Anwender mit Benutzernamen und Kennwort autorisieren. Dabei ist es irrelevant, an welchem Computer und unter welchem Betriebssystem der User gerade arbeitet. Da ein Firmennetzwerk im Regelfall über ein zentrales Benutzermanagement verfügt und sich Mitarbeiter stets am PC anmelden müssen, kann diese Anmeldung auch mit dem Single Sign-On (SSO) gekoppelt werden. Dazu liefert der Hersteller eine entsprechende Software mit.

Ein weiteres Plus zu üblichen Firewalls und Routern zeigt sich im Content-Filter. Damit Nutzer auch wirklich nur auf die erlaubten Inhalte zugreifen, führt die CR50ia eine ständige Kontrolle des Datenverkehrs durch. So wird jeglicher Netzwerkverkehr entsprechend den eingestellten Firmen- oder Nutzerregeln geprüft und darauf reagiert. Außerdem rundet der Hersteller seine Appliance mit Load-Balancing- und Fail-Over-Gateway-Funktionen ab.

Inbetriebnahme mit leichten Hürden

Bis zur erfolgreichen Inbetriebnahme des Geräts war zu Beginn unseres Tests eine kleine Hürde zu überwinden: Da die Appliance über ein Webinterface administriert wird, galt es zunächst, dieses überhaupt aufzurufen. Leider holt sich das Gerät in der Grundkonfiguration seine IP-Adresse nicht über einen DHCP-Server, sondern lässt sich nur über eine statisch verankerte Zugriffsnummer aufrufen. Arbeitet das eigene Netzwerk nun in einem anderen IP-Bereich, bleibt nur die Möglichkeit, entweder mit einem Cross-Connect-Kabel und einem Standalone-Rechner oder dem mitgelieferten Konsolen-Kabel auf die Appliance zuzugreifen. Der zweite Weg setzt einen Computer mit serieller Schnittstelle vo-

raus und führte uns mit einem beliebigen SSH-Client schließlich auf die Konsole der CR50ia. Dort konnten wir dann die IP-Adresse ändern, um aus unserem regulären LAN heraus die Konfigurationsarbeiten aufzunehmen.

Bei der ersten Einrichtung hilft ein gut strukturierter Assistent. Im Test haben wir die Appliance im "Gateway Mode" eingerichtet. Das heißt, LAN und WAN sind über zwei separate Netzwerkports physisch getrennt. Dazu verbanden wir unser LAN mit Port A und den Router für das WAN mit Port B. An Port C schlossen wir einen separaten Server an, den wir in der DMZ einrichteten. Je nachdem, zu welchem Zweck die CR50ia genutzt wird, sollte auch die Policy gewählt werden. Wir entschieden uns für die General Internet Policy, die den Datenverkehr auf schädliche Informationen scannt und den HTTP-Traffic auf Viren prüft.

Als Alternativen existieren noch die Optionen "Monitor Only" – dabei wird der Datenverkehr unverändert durchgelassen – und "Strict Internet Policy", womit der Internetzugriff nur noch nach einer Autorisierung möglich ist. Nach einem Neustart greifen die eingestellten Schutzfunktionen. Nachdem wir die notwendigen Lizenzen für die Viren- und Spam-Signaturen aktiviert hatten, mussten wir uns der Firewall und dem Einrichten des Port Forwarding widmen. Wenn zum Beispiel der Exchange-Server im LAN und nicht der DMZ steht, lässt sich nur so weiterhin über Outlook Web Access auf die Daten zugreifen.

Dazu haben wir die Firewall-Regeln "WAN->LAN" erweitert. Im LAN benötigten wir daher zuerst einen virtuellen Host, den wir mit der Ziel-IP und den Ports definierten. Wichtig dabei ist, als externe IP-Adresse diejenige des Netzwerk-Anschlusses B der Appliance anzugeben und nicht die öffentliche IP-Adresse des Routers. Denn die Daten kommen ja über die Schnittstelle B. Im zweiten Schritt konfigurierten wir die Firewall so, dass über den WAN-Port und jede Client-IP (möglich wäre hier auch das Einschränken externer IP-Adressen) ins LAN an den zuvor eingetragenen virtuellen Host mit dem definierten Port zugegriffen werden darf. Diese Regel lässt sich noch zeitlich begrenzen und mit diversen Policies belegen.

Umfangreiche Inhaltsfilter

Wie bereits erwähnt bietet die CR50ia umfangreiche Möglichkeiten zum Content Filtering auf IP-, User- und Applikations-Ebene. Damit erlaubt der Hersteller eine Policy-basierte Blockade des Datenverkehrs. Die Regeln haben wir für verschiedene Benutzer und Gruppen erstellt. Die Definitionen trafen wir wahlweise IP- oder User-basiert. Darüber hinaus haben wir beim Content-Filter und dem Zugriff auf Internetseiten eine globale Regel erstellt, die unter anderem den Zugriff auf Spiele- und Pornoseiten blockiert.

Um den Inhaltsfilter zu überprüfen, installierten wir das Gerät für mehrere Wochen in einem realen Netzwerk. Hierbei konnten wir gute Leistung feststellen. Das System handelte nach den Richtlinien und war in der Lage, Benutzern den Zugriff auf bestimmte Websites zu blockieren. Zudem meldete es auf Wunsch Benutzer ab, wenn das zugeteilte Traffic- oder Zeit-Kontingent überschritten wurde. Neben Quota-Regelungen beim Surfen ließ sich über die Internet-Richtlinien einfach regeln, welche Benutzer überhaupt Zugriff auf die Websites oder Anwendungen haben.

Eine weitere Regel, die wir später nicht global, sondern userbasiert zuordneten, verhindert den Zugriff auf webbasierte E-Mail-Angebote und die klassischen Chat-Server. Die User-Level-Authentifizierung kann über die lokale Be-

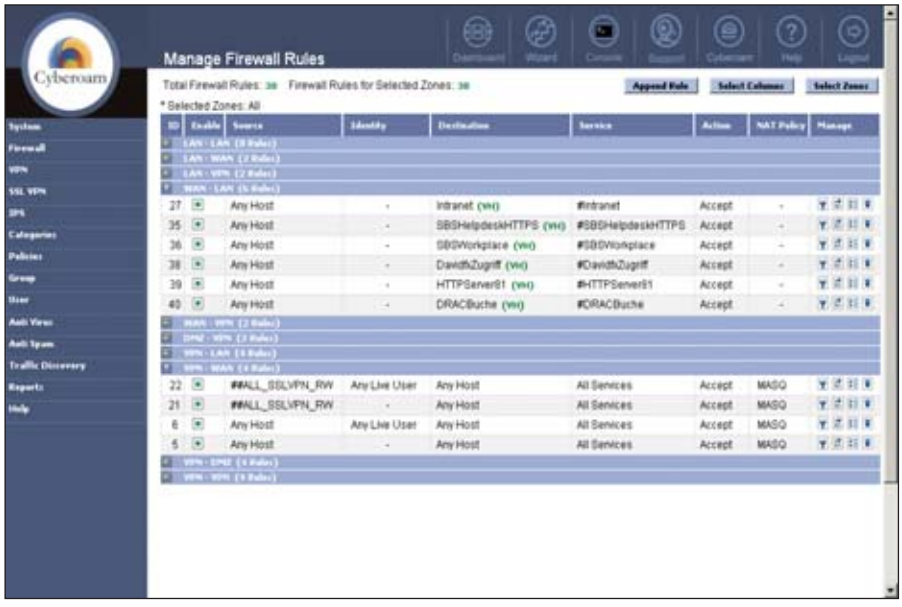

Bild 1: Die Firewall-Regeln steuern die Zugriffe vom WAN ins LAN und umgekehrt

Gateway versus Bridge

Um die volle Funktionsweise der Cyberoam CR50ia nutzen zu können, empfehlen wir die Einrichtung im Gateway-Modus. Dadurch wird das LAN und WAN physikalisch über zwei Netzwerkports der Appliance getrennt und geroutet. Der gesamte Datenverkehr vom und ins LAN läuft über die CR50ia.

Ist dagegen bereits eine Firewall im Einsatz, und Sie möchten die Konfiguration nicht ändern, bietet der Hersteller auch den Bridge-Modus an. Dabei ist die Appliance über einen Switch/Hub im Netzwerk, wie jedes andere Netzwerkgerät, eingebunden. In diesem Modus können die Routing-, Anti-Viren- und Anti-Spam-Funktionen nicht eingesetzt werden.

nutzer-Datenbank der Appliance oder einem mit Active Directory Service (ADS) und LDAP verbundenen User-Management erfolgen. Wir entschieden uns für das ADS und richteten auf den Arbeitsplätzen das Single Sign-On-Programm ein.

Verbesserungsfähiger Spam-Blocker

Wird die CR50ia wie in unserem Test im Gateway-Modus eingerichtet, fließt jeglicher Datenverkehr über das System. Mit einer gültigen Lizenz für Spam- und Viren-Schutz verwehrt die Appliance nicht nur den Zugriff auf ungewollte Internetseiten, sondern scannt zusätzlich den gesamten Datenstrom auf Spam-Nachrichten und Viren. Dabei beschränkt sich Letzteres nicht nur auf Anhänge von E-Mails, sondern auf jeglichen Code, der zum Beispiel durch einen regulären Download oder den Besuch einer Internetseite in das LAN übertragen wird. Ungebetenes wird so schon an der Eingangstüre zum Netzwerk abgelehnt.

Die Spam-Engine war im Test nicht so erfolgreich wie der Viren-Schutz. Während die CR50ia alle Viren entdeckt und in Quarantäne geschickt hat, machte die Spam-Engine einen etwas willkürlicheren Eindruck. Teilweise wurde Spam gar nicht erkannt, teilweise wurden ganz normale Nachrichten als Spam oder spamverdächtig deklariert. Die auf dem Exchange-Server im LAN betriebene alternative Anti-Spam-Lösung hatte weniger Probleme mit den Werbemails und hat die zuvor durch die Appliance durchgelassenen Nachrichten richtig klassifiziert und geblockt. Hier besteht also seitens des Herstellers noch Verbesserungsbedarf.

Guter Schutz vor DoS-Attacken

Mit dem Schutz vor Denial of Service (DoS)-Attacken verfügt die Appliance über ein besonderes Feature. Das Gerät lässt sich so konfigurieren, dass es Drop SYN Flood, UDP Flood und TCP-Traffic Flood-Attacken erkennt, wenn die Anzahl der Pakete die pro Minute definierte Quell-/Ziel-Paket-Rate übersteigt. Um die Firewall-Fähigkeiten zu testen, haben wir im Testumfeld über einen 1-GBit-Switch und das Tool "Nessus" DoS-Angriffe simuliert. Wir haben die Attacken über das LAN und den Switch simuliert, um Latenzen und Engpässen durch langsame ISP-Verbindungen vorzubeugen. Der so vorgetäuschte extreme Angriff wurde dennoch in Echtzeit erkannt und blockiert. Danach führten wir mit "Nmap Syn Stealth-Scan" und "TCP SYN" Ping-Attacken durch, die ebenfalls erfolgreich blockiert wurden.

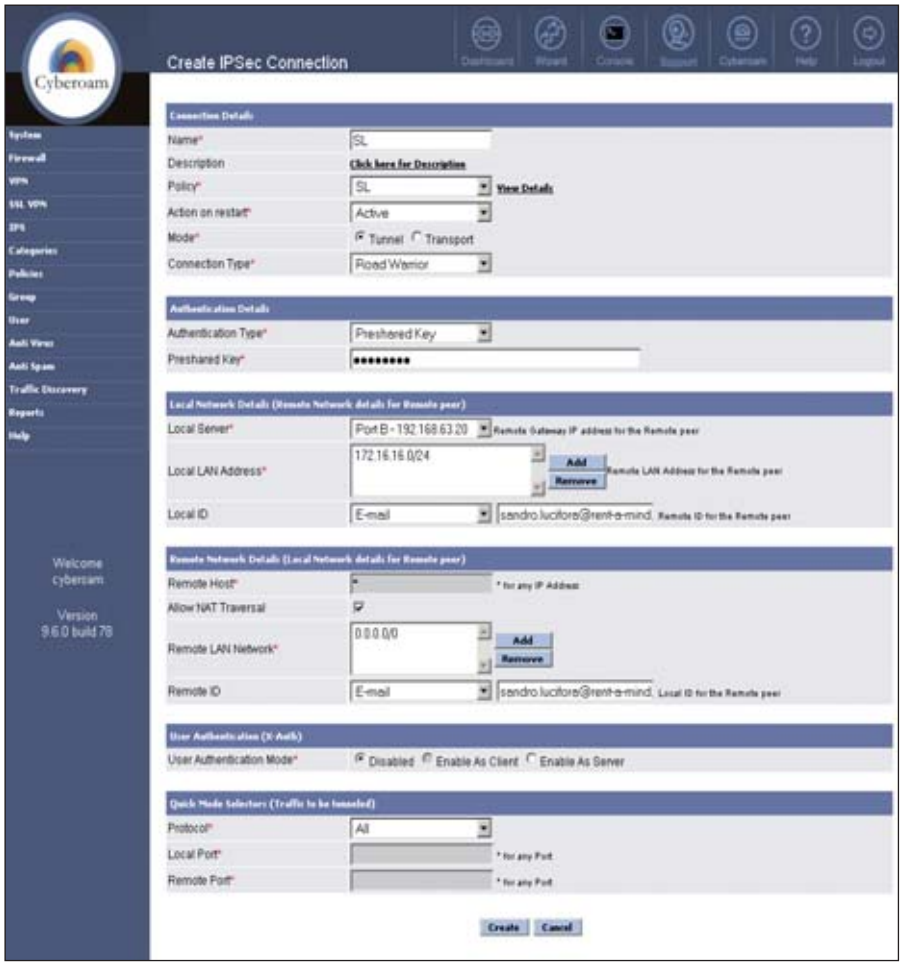

Bild 2: Die Einstellungen für die VPN-Regeln sind übersichtlich und einfach zu setzen

Remotezugriff per VPN

Mit dem VPN-Modul können mobile Benutzer und Telearbeiter über jedes Gerät einen sicheren Remote-Zugriff ins Netzwerk bekommen. Um Filialen, Home-Offices oder ein Notebook über feste oder dynamische Verbindung zu tunneln, ist ein VPN-Client nötig. Das Cyberoam-VPN unterstützt L2TP- und PPTP-Verbindungen sowie IPSec und kann so Net-to-Net- oder Host-to-Host-VPN-Verbindungen und Verbindungen für mobile Benutzer aufbauen. Der Client kann eine unter jedem Betriebssystem installierte VPN-Client-Software oder eine in einem Router integrierte VPN-Client-Lösung sein. Die VPNs von Cyberoam sind laut Hersteller von VPNC zertifiziert und sollten daher mit den meisten VPNs von Drittanbietern kommunizieren können.

Die wohl eleganteste Umsetzung für einen Remote-Client ist die in unserem Test eingesetzte Konfiguration mittels Preshared Key. Dazu haben wir die VPN-Policy unter dem entsprechenden

Menüpunkt erstellt. Danach wird eine IPSec-Verbindung auf Basis der VPN-Policy erstellt. Dabei wählten wir als Authentication Type "Preshared Key" aus. Nach der Erstellung dieses VPN-Zugangs muss dann der Schlüssel als TGB-Datei exportiert und im VPN-Client importiert werden. Als Client kam in unserem Test der Cyberoam-Client zum Einsatz.

Um sicherzustellen, dass auch durch einen VPN-Tunnel keine Malware oder Viren eingeschleust werden, sucht die Threat Free Tunneling (TFT)-Technologie im VPN-Datenverkehr nach unerwünschtem Code. Wer mehrere ISP-Gateways verbunden hat, nutzt den bei Cyberoam-VPN integrierten Failover der VPN-Konnektivität. Beim Ausfall einer ISP-Verbindung schaltet die Appliance auf die alternative VPN-Verbindung zum sekundären Gateway um.

Granulare Regeln erhöhen Komplexität

Die Appliance ermöglichte uns auch einen Echtzeiteinblick in die Verbindungen unseres Netzwerkes. Die Darstellung erfolgt wahlweise anwendungs- oder userbasiert. Auch nach IP-Adressen, der Datenübertragung oder der Bandbreiten-Nutzung werden Details der einzelnen Verbindung dargestellt. Voreingestellt generiert die CR50ia sieben ausführliche Berichte, die unter anderem Aufschluss geben über die Internet-Nutzung, die aufgerufenen Internetseiten, die Auslastung des Caches und den Mailzugriff. Die Berichte lassen sich ein Mal täglich per E-Mail an den Administrator senden. Im Laufe des Praxistests haben wir die Policies immer enger und genauer definiert. Dadurch steigerte sich die Leistung des Gerätes, was es aber auch immer schwieriger machte, mit der Appliance umzugehen. Denn schon kleine Änderungen und Anpassungen können große Wirkungen haben. Es zeigte sich, dass es sinnvoll ist, gerade zu Anfang eines der von Cyberoam vorkonfigurierten Regelwerke zum Bandbreiten-Management zu nutzen und darauf aufbauend individuelle Anpassungen vorzunehmen. Für fast jedes Szenario ist eine Policy verfügbar.

Fazit

Insgesamt ist der Funktionsumfang sehr gut und vielfältig. Und genau deshalb finden wir eine deutsche Benutzeroberfläche und Dokumentation unerlässlich. Die Konfiguration erschließt sich nicht sofort und die unstrukturierten Dokumentationen erleichtern das Vorhaben nicht wirklich. Der Hersteller hat jedoch für das nächste Update ein deutsches Interface angekündigt. Technisch gesehen ist die Appliance CR50ia ausgereift und hat auch im Härtetest gezeigt, dass sie die Anforderungen erfüllt. Die Konfiguration und Einrichtung sollte einem erfahrenen Administrator überlassen werden, da schnell das gesamte Netzwerk ohne Schutz dastehen kann oder, im Gegenteil, kein WAN-Zugriff mehr möglich ist. In Anbetracht der vielfältigen Management- und anderer Funktionen ist die CR50ia für mittelgroße Unternehmen sehr gut geeignet. *(ln)*

Produkt
UTM-Appliance mit VPN-Funktion und Bandbreitenmanagement.

Hersteller
Cyberoam – www.cyberoam.com/de/

Preis
Das Gerät selbst kostet rund 1.300 Euro. Das jährliche Abonnement für Webfilterung, Virenschutz und Spamabwehr schlägt mit etwa 1.200 Euro zu Buche.

Technische Daten
www.it-administrator.de/downloads/datenblaetter

So urteilt IT-Administrator *(max. 10 Punkte)*

Installation und Konfiguration	7
Content Filter-Funktionen	8
Schutz der Applikationen	10
Performance	8
VPN-Funktion	9

Dieses Produkt eignet sich

optimal für mittelgroße Netzwerke, die neben einem Content-Filter auch Remote-Anbindungen ans LAN benötigen.

bedingt für kleine Netzwerke, in denen IT-Verantwortlichen vor allem die Reglementierung des Internetzugriffs der Mitarbeiter und der Schutz des LAN wichtig ist.

nicht für den Schutz von kleinen Netzwerken mit wenigen Arbeitsplätzen, da dafür der administrative Aufwand zu groß ist.

Cyberoam CR50ia