

Mehr Sicherheit im Netzwerk

Test - Blue Coat ProxyOne Security Appliance

von [Bernhard Haluschak](#), 02.03.2011 (publiziert)



Twittern

1



Gefällt mir

5

PDF | E-Book | Ranking ★★★★★



Blue Coat hat sein Security-Appliance-Portfolio um das System ProxyOne PR10 erweitert. Dieses bietet umfangreiche Sicherheitsfunktionen wie komfortables URL-Filtering und Virenerkennung sowie eine einfache Konfiguration. Wir haben die ProxyOne Security Appliance getestet.

Mit der Security Appliance ProxyOne will Blue Coat gezielt mittelständische Unternehmen ohne eigene IT-Abteilung ansprechen. Dabei erhält der Kunde ein System, das viele bekannte Sicherheitsfunktionen aus den Enterprise-Systemen bietet. Dazu zählen ein granularer URL-Filter, der den Zugang zu verdächtigen Websites sperrt, sowie ein Filter, der Webinhalte überprüft sowie *Malware* erkennt und blockiert.



Laut Blue Coat nutzen 70 Prozent aller kleinen und mittleren Unternehmen Social-Media-Dienste. Durch die steigende Verbreitung von Malware in diesen Angeboten droht der intern genutzten IT früher oder später der Befall mit Schadsoftware. Dabei sind oft die herkömmlichen lokalen Sicherungsmaßnahmen wie eine *Firewall* oder eine Desktop-Antiviren-Software gegen die Angreifer wirkungslos. Gerade in diesem Bereich soll Blue Coat ProxyOne ansetzen und Unternehmen schützen.

Der Preis der Appliance beläuft sich auf knapp 9000 Euro im ersten Nutzungsjahr für bis zu 100 angeschlossene Anwender. Das beinhaltet alle Softwarelizenzen, automatische Sicherheits-Updates und 24-x-7-Support für ein Jahr. Im zweiten Jahr reduziert sich die Summe auf knapp 4000 Euro. Darüber hinaus ist ein Upgrade auf bis zu 2000 User möglich.

In unserem Test muss die ProxyOne Appliance von Blue Coat beweisen, ob das Gerät das hält, was es verspricht.

Details der ProxyOne Security Appliance

Die ProxyOne Appliance von Blue Coat wird normalerweise zwischen Firewall und dem internen Router installiert, sodass das Gerät sämtlichen Webverkehr des Unternehmens auf unerlaubte Inhalte, gefährliche URLs und Malware durchsuchen kann. Verdächtige Daten werden damit vor dem Eintritt in die Unternehmens-IT abgewehrt. Aktuelle Informationen über die Gefahrenlagen, infizierte Webadressen und neue Malware bezieht die Appliance aus dem Rechenzentrum des Herstellers. Mit diesem Echtzeitdienst namens "Blue Coat WebPulse" erübrigt sich das Update der Security-Installation etwa um neue Virenmuster, wie es bei Desktop-basierter Schutzsoftware üblich ist. Basis des Dienstes ist die hausinterne, zentrale Security-Datenbank. Sie wird durch die Aktivitäten von rund 70 Millionen aktuellen Blue-Coat-Nutzern kontinuierlich um neue Erkenntnisse über sichere und unsichere Anlaufpunkte im Internet gespeist.



Hardware: Die Security Appliance verpackt der Hersteller in ein 19-Zoll-1HE-Rack-Gehäuse.

Die Appliance integriert darüber hinaus Caching-Funktionen, sodass ein mehrmaliger Scan von häufig angesteuerten Webseiten entfällt. Das beschleunigt die Webkommunikation, ohne die Leistung zu beeinträchtigen. Auch für Video-Streams hat sich der Hersteller eine Lösung einfallen lassen, die eine übermäßige Belastung der Internetverbindung verhindern soll. Das Gerät bezieht den Datenstrom nur einmalig aus dem Netz und verteilt ihn dann mehrfach an die angeschlossenen Anwender.

Das neue Produkt ist eine abgespeckte Version der URL-Filtering-Appliance "ProxySG". Sie erlaubt erfahrenen Anwendern eine granulare Konfiguration der Security-Regeln. Die Mittelstandslösung wird dagegen mit voreingestellten Richtlinien ausgeliefert. Ein Auswahlmü lässt den Anwendern die Wahl, welche Art von Inhalten gesperrt oder zugelassen werden sollen. Zudem integriert die kleine Ausführung einen Antivirenschutz. Im Enterprise-Umfeld gibt es für diese Funktion eine separate Box.

Die Kosten für ProxyOne beinhalten einen ständig erreichbaren Support, regelmäßige Software-Updates sowie die Schutzsoftware "ProxyClient" für Notebooks und Desktops der mobilen und entfernt tätigen Mitarbeiter. Sie ist nur in Verbindung mit der Appliance einsetzbar. Eine ergänzende Schutzsoftware für Smartphone-Nutzer gibt es bis dato nicht, soll aber folgen. Das Gerät lässt sich auf bis zu 2000 Anwender skalieren.

Die ProxyOne wird in einem Standard-19-Zoll-Rack-Gehäuse (1HE) geliefert. Im Innern des Systems verrichtet ein Intel-Quad-Core-Xeon-Prozessor des Typs E5540 seine Arbeit. Dem System stehen insgesamt 18 GByte Hauptspeicher zur Verfügung. Das Storage-Subsystem besteht aus zwei 1-TByte-SAS-Festplatten von Seagate, die im RAID-1-Verbund arbeiten.

Auf der Rückseite der Appliance befinden sich vier nutzbare Netzwerkanschlüsse. Ein Anschluss mit der Beschriftung INside kennzeichnet den Netzwerkausgang der Appliance, und OUTside ist entsprechend der Netzwerkeingang des Gerätes. Darüber hinaus besitzt es eine serielle Schnittstelle für den Anschluss einer Konsole. Da es sich im Prinzip um einen Server handelt, hat das System auch Anschlüsse für Tastatur, Maus und VGA-Monitor. Zudem sind zwei Onboard-Netzwerk-Ports vorhanden. Für die nötige Ausfallsicherheit sorgen zwei redundante 650-Watt Netzteile.

Im Frontbereich befinden sich die zwei Hotswap-fähigen TByte-SAS-Festplatten. Die Bedienung besteht aus einem Ein-/Ausschalter und einem ID-Taster. Drei Status-LEDs informieren den Anwender über den Betriebszustand, den Systemalarm und den ID-Zustand.

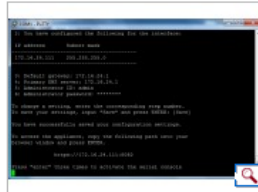
QUICKINFO

Produkt	ProxyOne Appliance PR10
Hersteller	Blue Coat
Prozessor	1 x Intel Xeon E5540 8ML2 (Quad Core), 2,53 GHz
Hauptspeicher	9 x 2048 MByte DDR3-1333 MHz , ECC
Storage-Subsystem	2 x TByte 3,5-Zoll-SAS-HDD (Seagate Constellation), RAID 1
Netzwerk	4 x 1 Gbit-Ethernet (Dual GbitE mit Bypass)
Weitere Optionen	2 x 650 Watt Netzteil (Failover)
Gehäuse	19-Zoll-Rack, 1HE , 697 x 430 x 43 mm (L x B x H)
Stromverbrauch	zirka 150 Watt (Betrieb)
Preis	9000 Euro, inklusive 100 Lizenzen und Support für ein Jahr

Erste Konfiguration der ProxyOne

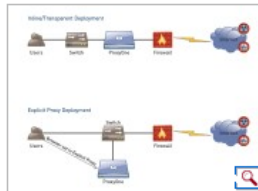
Die Verbindung mit einem Rechner zur initialen Konfiguration der ProxyOne Appliance erfolgt über die serielle Schnittstelle und eine entsprechende Terminal-Software wie HyperTerminal oder Putty auf einem Client-System.

Ist der serielle Kontakt zur ProxyOne erfolgt, meldet sich das Gerät mit dem Startbildschirm eines Konfigurations-Wizards. Im ersten Schritt wird festgelegt, wie das System arbeiten soll. Zur Auswahl stehen "*Physically in-path*" und "*Explicit proxy*".



Erstkontakt: Ist die IP-Adresse des Systems noch nicht bekannt, erfolgt die initiale Konfiguration der ProxyOne über die serielle Schnittstelle und ein Terminal-Programm.

Bei der "In-Path"-Verbindung wird das Gerät zwischen dem Netzwerk-Router und der Firewall installiert. Der gesamte Datenfluss erfolgt über die ProxyOne. Fällt diese zum Beispiel aus, läuft der Datenverkehr über einen internen Bypass ungeschützt, aber trotzdem weiter. Bei "Explicit Proxy" wird das Gerät nur an den Switch angeschlossen. Alle Benutzer müssen vom Administrator an der ProxyOne mit einer eigenen dedizierten IP-Adresse eingerichtet werden, damit sie den vollen Schutz genießen können. Ändert sich die IP-Adresse oder fällt das System aus, ist der Anwender ohne Schutz.



Entscheidungsfreiheit: Die ProxyOne beherrscht zwei verschiedene Deployment-Modi. Foto: Blue Coat

Nach dem Festlegen des Deployment-Modus muss der Anwender über die Konsole die IP-System-Adresse, die Subnet-Maske, das Default Gateway und die Administrator-ID sowie das Administratorpasswort festlegen. Mit der Eingabe des Wortes "Save" ist die Konfiguration über die serielle Verbindung abgeschlossen. Der Anwender kann jetzt das System durch Eingabe der festgelegten IP-Adresse komfortabel über einen Webbrowser erreichen.

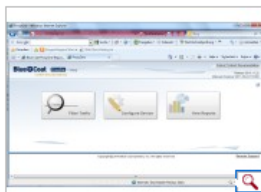
Konfiguration und Analyse über die Weboberfläche

Für das webbasierte Ansprechen der Security-Appliance ist Java erforderlich; falls die Software nicht vorhanden ist, muss sie nachinstalliert werden. Ist dies erfolgt, kann die Managementkonsole des Systems über einen beliebigen Webbrowser durch die Eingabe `https://<IP-Adresse des Systems>:8082` aufgerufen werden. Beim ersten Login fragt das Gerät nach dem Benutzernamen und dem Passwort. Standardmäßig haben wir "*admin*" und "*admin*" festgelegt. Es öffnet sich ein Browser-Fenster mit drei Auswahlbereichen:

Filter Traffic: Konfiguration von URL-Filtern

Configure Device: Konfiguration und Statusabfrage der ProxyOne

View Reports: Reporting und Monitoring des Datenverkehrs



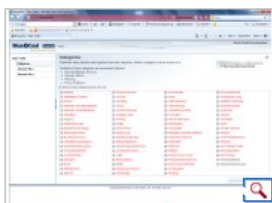
Begrüßung: Nach dem Login auf der GUI-Management-Konsole stehen dem Anwender drei Arbeitsbereiche zur Verfügung.

Wir widmen uns zuerst der Schaltfläche *Configuration Device*. Hier stehen dem Anwender die drei Navigationsreiter *Statistics*, *Configuration* und *Maintenance* zur Verfügung. Hier kann der Anwender sehr komfortabel und übersichtlich, da grafisch aufbereitet, Statistiken über Netzwerk- und System-Performance abrufen. Darüber hinaus kann der User auch erweiterte Netzwerkkonfigurationen vornehmen sowie Lizenz- und Servicerichtlinien für das System festlegen.

Die Appliance bietet gerade in diesem Bereich eine Fülle von verschiedenen Menüpunkten und komplexen Einstellungsmöglichkeiten in den Untermenüs. Die Navigation durch die Optionen hat der Hersteller mit der grafischen Weboberfläche zwar gut gelöst, entbindet den Anwender aber nicht davon, sich mit der komplexen Materie beziehungsweise Konfiguration detailliert auseinanderzusetzen. Diese benötigt er aber nur, wenn er weitere granulare Einstellungen vornehmen will oder muss.

URL-Filter und Malware-Filter

Im Arbeitsbereich des *Filter Traffic* erwartet den Anwender eine Übersichtseite der vorkonfigurierten URL-Kategorien, die von der Security Appliance geblockt werden sollen. Der Anwender kann hier einfach die entsprechende Kategorie auswählen. Was sich hinter den einzelnen Kategorien verbirgt, offenbart der Mauszeiger auf den Begriff. Wer weitere Details über die Zusammenstellung der Kategorien erfahren möchte, muss die Blue-Coat-Website bemühen.



Rundumschutz: Die Appliance bietet zahlreiche URL-Filtering-Funktionen, um das Netzwerk vor unberechtigtem Zugriff zu schützen.

Neben der sehr einfachen Auswahl der verschiedenen Kategorien kann der Anwender auch manuell URLs freigeben oder blockieren. Dies erfolgt in der linken Navigation durch *Allowed URLs* und *Blocked URLs*. Somit kann der User hier sehr detailliert und einfach seine entsprechenden Webeinstellungen durchführen. Darüber hinaus bietet Blue Coat einen Service an, der die Risikobewertung einer URL durchführt.



Gesperrt: Die ProxyOne sperrt entsprechend den Anwendervorgaben den Zugang zu den Webseiten.

Wir haben die Probe aufs Exempel gemacht und die Kategorie Pornography als Filter ausgewählt. Nach dem Bestätigen mit der *Apply*-Schaltfläche war es uns nicht mehr möglich, die Playboy- und ähnliche Webseiten aufzurufen. Sie wurden durch ProxyOne erfolgreich geblockt. Auch das Setzen von manuellen URL-Filtern (*Blocked URLs* und *Allowed URLs*) funktionierte in unserem Test einwandfrei.

Die Security Appliance überwacht im Hintergrund auch den Datenstrom auf mögliches Vorkommen von Viren und *Malware*. Laut Hersteller basiert dieser Dienst auf der Kaspersky-Engine, die automatisch und nahezu unbemerkt immer auf den neusten Stand gehalten wird. Auch die Überprüfung dieses Sicherheits-Features durch das Laden von einigen bekannten Virensignaturen verlief positiv.

Auswertung über Dashboard und Reports

In dem Bereich *View Reports* stellt die ProxyOne Appliance auf einer grafisch aufbereiteten Weboberfläche detaillierte Auswertungen über das Internetnutzungsverhalten der angeschlossenen Client-Rechner zur Verfügung.



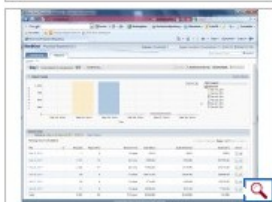
Alles auf einen Blick: Das Dashboard informiert über den Status des Netzwerkverkehrs.

So informiert die Security-Appliance unter dem Reiter *Dashboard* den Administrator zum Beispiel über die Top-10-Seiten auf der Basis von Page Views oder die vom System geblockten Webseiten. Mit *Edit* lassen sich die einzelnen Kategorien individuell konfigurieren. Darüber hinaus kann der Anwender die Blöcke je nach persönlichen Vorlieben anordnen.



Details: Die Security Appliance stellt dem Anwender umfangreiche Reporting-Funktionen zur Verfügung. Die einzelnen Auswertungskriterien werden grafisch aufbereitet.

Der Reiter *Reports* ermöglicht eine tiefere Analyse des Datenverkehrs, ohne jedoch Webanfragen einzelner Rechner darzustellen. Darüber hinaus sind eine zeitgesteuerte Erstellung und eine konfigurierbare Archivierung der Reports vorgesehen.



Anschaulich: Die einzelnen Auswertungskriterien werden grafisch aufbereitet.

Alles in allem bietet die Reporting-Funktion viele nützliche Funktionen, die sie nicht nur in reiner Textform offenbart, sondern auch in Form von Kuchengrafiken und Balkendiagrammen

Fazit

Die Security Appliance ProxyOne von Blue Coat eignet sich für kleine Unternehmen oder Zweigniederlassungen. Das System beinhaltet eine Menge nützlicher und interessanter Features, die in dieser Preisklasse nicht selbstverständlich sind. Neben einem breiten Funktions-Set an Sicherheitseinrichtungen fällt das Gerät durch sein klar strukturiertes Lizenzierungsmodell auf. Hinzu kommen eine strukturierte Bedienung und eine angenehme GUI, aber leider nur auf Englisch. Darüber hinaus ist die Einrichtung oder die Konfiguration ohne große Hürden durchführbar.

Wer also eine Security Appliance mit den entsprechenden Funktionen sucht, sollte sich dieses System näher anschauen. Es ist gerade für Unternehmen mit wenig internem IT-Know-how eine interessante Lösung. (hal)