

Port 80 Security Anwendungen

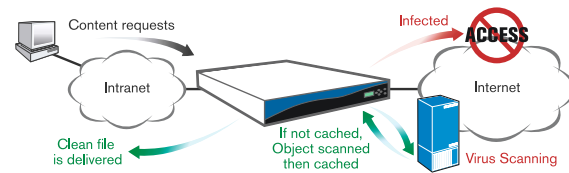
Sicherheit für Port 80 Datenverkehr mit Blue Coat Systems

The Web Security Authority.

Die Port 80 Appliances von Blue Coat Systems, die auf dem preisgekrönten Security Gateway OS (Betriebssystem) basieren, sind die ideale Lösung, um Unternehmensnetze gegen drohende Gefahren aus dem Internet zu schützen. Hierzu zählen Web Browsing, Mail-Würmer, Instant Messaging Dienste, personalisierte web-basierte E-Mail Postfächer (wie Yahoo! oder Hotmail) und bandbreiten-intensive Multimediainhalte. Mit den Systemen von Blue Coat Systems können Unternehmen den kompletten ein- und ausgehenden HTTP-Datenverkehr effektiv schützen:

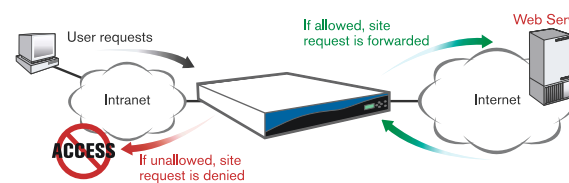
Web-Virenscreening

“Scan once, serve many” Modell ermöglicht Echtzeit-Scanning und Skalierbarkeit für effektives Scannen von Web-Inhalten.



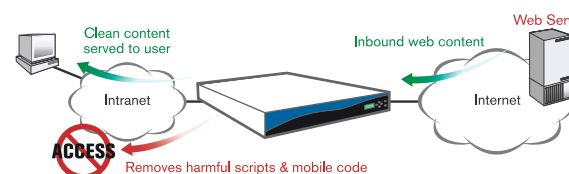
Inhaltsfilterung

Integrierte URL-Filterung ermöglicht es IT-Mitarbeitern, Zugang oder Ansicht von unerwünschten Inhalten zu beschränken und so unnötig die Unternehmensressourcen zu verbrauchen.



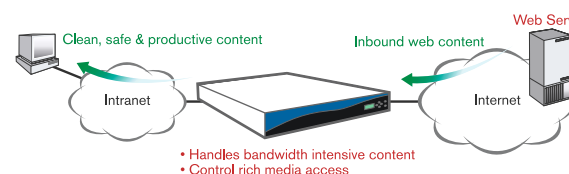
Content Security

Schützt und kontrolliert Up- und Downloads aus dem Web. Verteilt Web- und Multimediainhalte und entfernt bösartigen Mobile Code, aktive Inhalte oder spezielle Dateiarten, die von anderen Sicherheitsgeräten nicht überprüft werden.



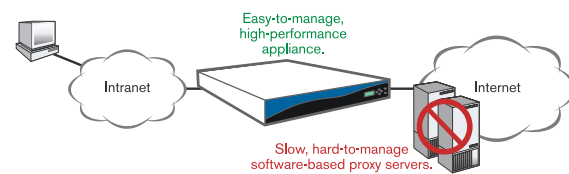
Bandbreitenmanagement

Bietet Kontrolle über Caching, Inhalts-Positionierung und Bandbreitenauslastung und gewährleistet, dass das Netzwerk optimal funktioniert und ausreichende Kapazitäten für geschäftskritische Anwendungen zur Verfügung stehen.



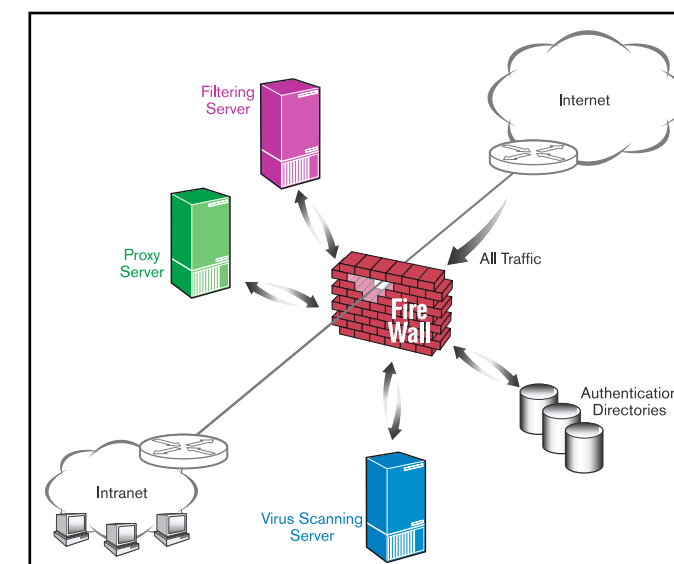
Hochleistungsfähige Proxy Server

Skalierbare Ersatzmöglichkeit für den Austausch bestehender Proxy Server ermöglicht es Administratoren, den Zugang der Nutzer zu Informationen aus dem Web zu sichern, zu verwalten und zu beschleunigen.



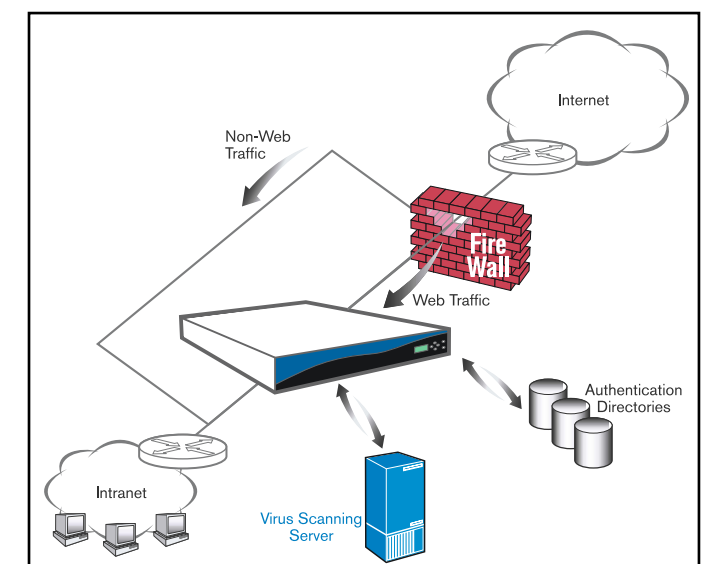
Inzwischen haben Unternehmen zwar Sicherheitsinfrastrukturen eingerichtet, um sich vor Gefahren auf Paketebene zu schützen, doch diese sind oftmals extrem anfällig für ausgeklügelte Angriffe auf Inhaltsebene. Derzeit tauchen solche Gefahren in Form von Web-Viren, Massenmailer-Würmern, gefährlichem Mobile Code und unerwünschten Web-Inhalten auf, die alle HTTP oder Port 80 als “offene Tür” zum Unternehmensnetz nutzen. Deshalb benötigen Firmen und Organisationen ein neues Internet-Sicherheitsmodell, das die Wirksamkeit des Schutzes einer Firewall auf Paketebene mit dem Schutz des Blue Coat Security Gateways für Port 80-Inhalte kombiniert.

Sicherheitsinfrastruktur OHNE Blue Coat Systems



Schützt gegen eine Reihe von Gefahren auf Paketebene. Schichtweiser Sicherheitsansatz, der Schutz auf Inhaltsebene hinzufügt, um web-basierte Gefahren zu bekämpfen, die HTTP und Port 80 für den Angriff nutzen. Policy-Entscheidungen werden separat auf Paketebene gemacht, was zu Überschneidungen und redundanten Regelungen führt, die aufwendig zu verwalten sind. Policy-Entscheidungen werden auf Inhalts- und/oder Paketebene gefällt, um optimalen Schutz und zentrale Verwaltung der Regelwerke zu gewährleisten. Überprüft Inhalte wie E-Mails nach dem Prinzip “Store and Forward”, ist aber nicht dafür ausgelegt, Web-Virenscreening in Echtzeit durchzuführen. Bietet hochskalierbares, regel-basiertes Virenscreening, optimiert für die Echtzeitüberprüfung auf web-basierte Gefahren. Blockiert bösartigen Mobile Code und aktive Inhalte, ist aber meist darauf beschränkt, in allen Instanzen entweder “passieren zu lassen” oder “abzulehnen”. Bietet Flexibilität für die Implementierung von individuellen Regelungen für Up- und

Sicherheitsinfrastruktur MIT Blue Coat Systems



Downloads von Inhalten je nach Art, Nutzer, Gruppe, Tageszeit, Ort, Protokollart, Browserversion und mehr. Nicht optimale Architektur für URL-Filterung außerhalb des Gerätes führt zu Leistungsverlusten der Firewall und längeren Antwortzeiten für die Nutzer. Skalierbare, policy-basierte URL-Filterung bietet umfangreiche Kontrolle über Web-Nutzungsverhalten und verkürzt Antwortzeiten für die Nutzer unabhängig von Onbox- oder Offbox-Installation. Bandbreitenmanagement erfordert Einsatz von mehreren Geräten, die separat verwaltet werden müssen. Integration von Caching, Inhaltspositionierung und Bandbreitenmanagement ermöglicht bessere Kontrolle von Web- und Multimediainhalten auf Nutzer-, Gruppen- und Protokollebene. Ältere Software-basierte Proxy Server bieten beschränkte Skalierbarkeit und sind in der Wartung recht teuer. Optimierte Appliance, die speziell für Sicherheitsüberprüfungen von Web-Inhalten entwickelt wurde und daher mehr Leistung und geringere Verwaltungskosten mit sich bringt.