

MALWARE AM WEBGATEWAY STOPPEN

Blue Coat ProxyAV™ erkennt Malware am Gateway und ist somit ein wichtiger Bestandteil der ADN-Infrastruktur (Application Delivery Network), die für umfassende Anwendungstransparenz, -beschleunigung und -sicherheit sorgt. Die ProxyAV-Appliances sind auf die Verwendung mit ProxySG Secure Web Gateway-Appliances ausgerichtet und tragen so zum mehrschichtigen Sicherheitssystem von Blue Coat bei, das sowohl Schutz vor InlineBedrohungen als auch die Malwareprüfung von Webinhalten am Gateway umfasst. Die einzigartige High-Performance-Architektur von ProxyAV wird mit führenden Anti-Malware-Engines kombiniert, um auf effiziente Weise den Webverkehr zu sichern und Benutzer vor webbasierter Schadsoftware zu schützen. Gemeinsam bieten ProxyAV und ProxySG höchste Leistung bei minimalen Anforderungen an Hardware-Ressourcen und stellen somit eine umweltfreundliche und kostengünstige Lösung dar. Schützen Sie Ihre Benutzer und das gesamte Netzwerk vor Viren, Trojanern, Würmern, Spyware und anderen schädlichen Inhalten. Sogar Benutzer, die keine Virenschutzsoftware verwenden, sind damit in Sicherheit.

LEISTUNGSMERKMALE

Inline-Bedrohungsanalyse

ProxyAV unterstützt führende Malware-Engines von Kaspersky, Sophos, Trend Micro, Panda und McAfee mit Updates im Intervall von 5 Minuten und bietet so besseren Schutz als Desktop-Virenschutzlösungen.

Das nur von Blue Coat verwendete zeitversetzte Scannen schließt Objekte mit langer Ladedauer, wie Webradio und andere Medien, von der Threadverarbeitung aus, wodurch die Performance am Webgateway optimiert wird.

ProxyAV unterstützt vier Modi für die Inhaltsanalyse: herkömmliche Objektanalyse, Trickle-first- oder Last-Stream-Analyse und deferred Scan.

Bei der Konfiguration von ProxyAV können Sie festlegen, ob eingehender und ausgehender Datenverkehr analysiert werden soll und ob Dateien weitergeleitet werden sollen, wenn bei der Erkennung Fehler auftreten. Außerdem können Sie den Wert für die Zeitüberschreitung bestimmen und vertrauenswürdige Sites definieren. Für Zulassungs- und Sperrlisten können Richtlinien erstellt werden, die auf Dateierweiterungen sowie Größen- und Inhaltstypbeschränkungen basieren. Auch Warnungen und Protokolldateien sind individuell anpassbar.

Performance und Skalierbarkeit

ProxyAV wurde speziell für die effiziente Malware-Analyse am Gateway entwickelt. Lastverteilungs- und Clustering-Technologien erzielen eine höhere Effizienz – mit weniger Hardware als bei separaten Einzellösungen.

ProxyAV kommuniziert mit ProxySG über ICAP(S), ein standardisiertes Hochleistungsprotokoll.

Die Multi-Core-Architektur von ProxyAV in Kombination mit Lastausgleichs- und Clustering-Technologie steigert die Performance auf Durchsätze bis 1 Gbit/s und unterstützt so die Implementierung von Webgateways mit Hochverfügbarkeit.

Umfassender Scan

ProxyAV steht für erstklassige Malware-Scans – für Performance und Sicherheit.

ProxyAV kann Dateien mit einer Größe von bis zu 2 GB scannen und komprimierte Archive mit bis zu 99 Ebenen analysieren.

ProxyAV ist mit verschiedenen Clouds zur Bedrohungserkennung integrierbar, darunter Blue Coat WebPulse und Drittanbieter-Clouds. So kann der Cloud-Schutz am Gateway mehrere Anbieter umfassen.

ProxyAV 510

ProxyAV 510 ist die Einstiegs- und Mittelklasselösung für Zweigstellen und mittelständische Unternehmen.

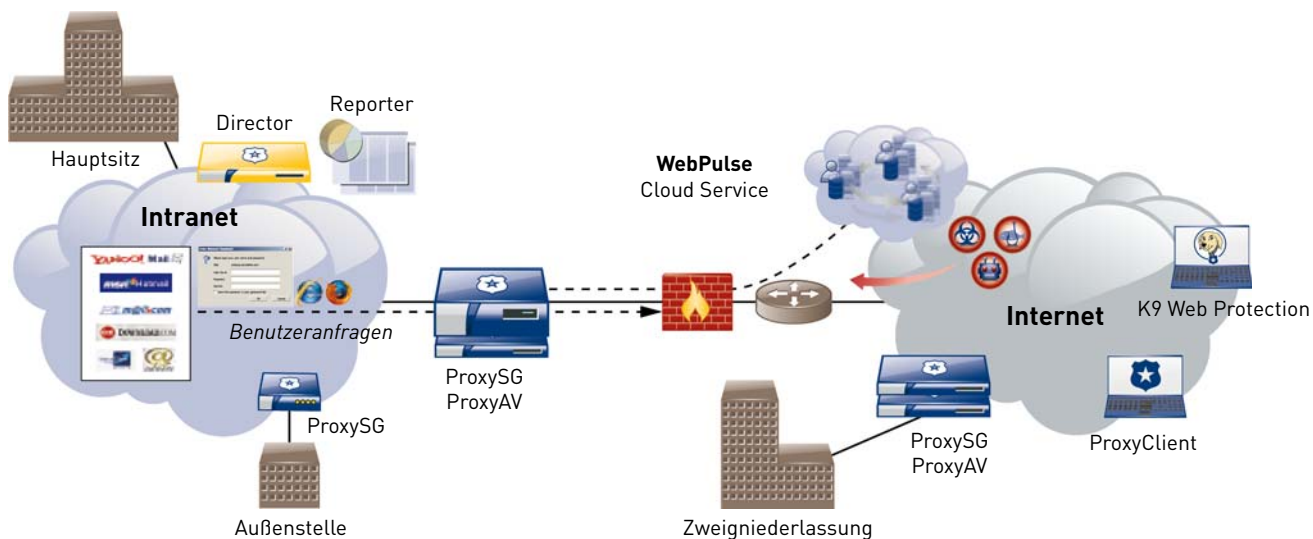
An große Unternehmen und Service Provider mit 10.000 oder mehr Benutzern richten sich hingegen ProxyAV 1400 und 2400, die 1:1 mit ProxySG 9000 integrierbar sind. ProxyAV 1200, die neueste Lösung aus der ProxyAV-Serie, wurde für mittelgroße Unternehmen entwickelt, beinhaltet jedoch dank ökonomischerem Prozessor alle Funktionen von ProxyAV 1400.

Integrierte Hardware-Servicefunktionen wie Montage-Gleitschienen reduzieren den Wartungszeitaufwand. Die doppelte, redundante Stromversorgung sichert hohe Verfügbarkeit.

Vorteile im Überblick

- Weniger Appliances bedeuten weniger Verwaltung und Platzbedarf und letztlich einen besseren ROI.
- Integrierter Investitionsschutz wird mit 4- oder 5-jährigen Serviceverträgen erzielt.
- Cloud-Schutzsysteme von verschiedenen Anbietern verstärken die Malware-Analyse um zusätzliche Ebenen.
- Sicherheit und Performance schließen einander nicht aus.





	AV510-A
System	
Prozessoren	1 CPU
Laufwerke	1 x 320-GB-SATA*
RAM	1 GB
Netzwerkschnittstelle	(2) integrierte 10/100/1000Base-T-Netzwerkkarten
Umgebungsbedingungen	
Stromversorgung	Netzbetrieb 100-240 V~, 50-60 Hz, 6,3-3,0 A
Max. Leistungsaufnahme	150 Watt
Wärmeleistung	150 W
Temperatur	5 °C bis 35 °C
Luftfeuchtigkeit	Bis 90 % relative Luftfeuchtigkeit (nicht kondensierend)
Höhe	Bis zu 3.048 m
Abmessungen und Gewicht	
Gehäuse	Montierbar in 19-Zoll-Rack
Abmessungen (L x B x H)	58 x 44 x 4,4 cm
Gewicht (maximal)	12,3 kg
Technische Standards	
Emissionen	FCC Klasse A, EN55022 Klasse A, VCCI Klasse A Nr. 1706609, BSMI, CCC, C-Tick
Sicherheit	CSA C22.2 Nr. 950 M95, UL 60950 3. Ausgabe, EN60950, TÜV-GS, TÜV-S, CCC, BSMI
Normen	UL/CSA, TÜV-S, BSMI, C-Tick, CCC, CE
Gewährleistung	
Es besteht für ein (1) Jahr ab Versanddatum eine beschränkte Gewährleistung, die nicht übertragbar ist. BlueTouch Support-Verträge für Software-Support rund um die Uhr und Optionen für Hardware-Support separat erhältlich.	

* Nur Geräte, die nach dem 7. 7. 2010 ausgeliefert wurden