

Cisco IronPort S-Serie



Informationssuche im Internet, Web-Applikationen sowie Online-Meetings gehören heute zum Alltag in Unternehmen. Jedoch steigt mit der Zunahme des Webtraffics auch die Gefahr, sich mit schadhaften Code zu infizieren. Ein Großteil der PCs in Unternehmen ist bereits mit Malware infiziert. Dabei stellen sich zunehmend auch vertrauenswürdige Webpages als eine der größten Gefahrenquellen heraus: 87% der webbasierten Bedrohungen gehen von kompromittierten Internetseiten aus. Der alleinige Besuch führt dabei zum unweigerlichen Download des schadhaften

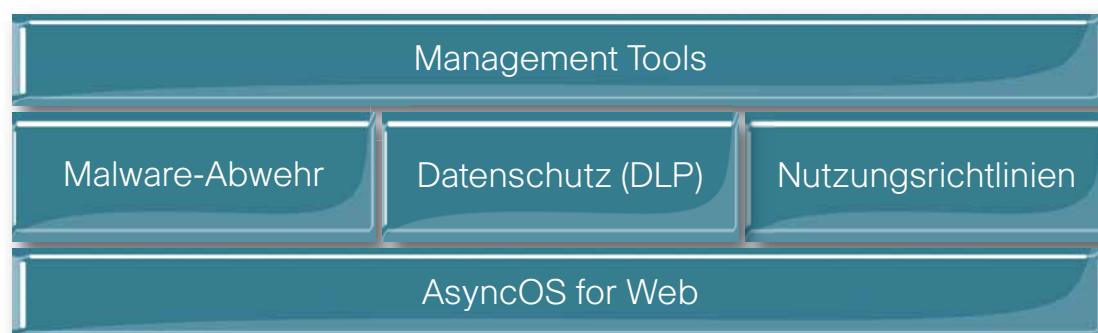
Codes. Auf diese Weise entstehen nicht nur erhebliche Sicherheitslücken im Netzwerk, auch können so sensitive Unternehmensdaten unbemerkt ausspioniert werden. Zudem gewinnt neben der Gefahrenabwehr zunehmend auch die Durchsetzung von Nutzungsrichtlinien des Internets im Unternehmen an Bedeutung. Bewahren Sie daher die Kontrolle über den gesamten ein- wie ausgehenden Internetverkehr und schützen Sie Ihr Unternehmensnetzwerk vor webbasierten Bedrohungen mit der Cisco IronPort Web Security Appliance.

Sicher im Netz mit der Cisco IronPort Web Security Appliance

Die Cisco IronPort Web Security Appliance wurde für Unternehmen jeglicher Größenordnung entwickelt. Als branchenweit erste Lösung kombiniert sie traditionelle Techniken der URL-Filterung mit innovativen Reputations- und Malwarefiltern auf einem einzigen Gerät. Dieses mehrschichtige System der Gefahrenabwehr in Verbindung mit einem extrem leistungsstarken

Web-Proxy gewährleistet nicht nur eine deutlich verbesserte Performance, sondern auch höhere Zuverlässigkeit als es traditionellen Systemen möglich ist. Die Cisco IronPort Web Security Appliance zählt damit zu den führenden Lösungen beim Schutz vor webbasierten Bedrohungen.

Die Cisco IronPort S-Serie gewährleistet mehrschichtigen Schutz vor webbasierten Bedrohungen. Dabei sind essentielle Sicherheitsfeatures auf einem leistungsstarken Proxy integriert.



Leistungsstarke Sicherheitsplattform

Ein **hochperformanter Web-Proxy** bildet die Grundlage für die Cisco IronPort Web Security Appliance. Basierend auf dem proprietären Betriebssystem AsyncOS for Web schafft der Proxy problemlos bis zu 100.000 gleichzeitig aktive TCP-Verbindungen. Damit wird ein besonders hohes Maß an Skalierbarkeit und Stabilität im Bereich der Websicherheit gewährleistet. Zudem garantiert der Proxy eine umfassende Kontrolle über HTTP-, HTTPS- sowie FTP-Verbindungen. Auf diese Weise wird eine sichere Kommunikation über die gängigsten Internet-

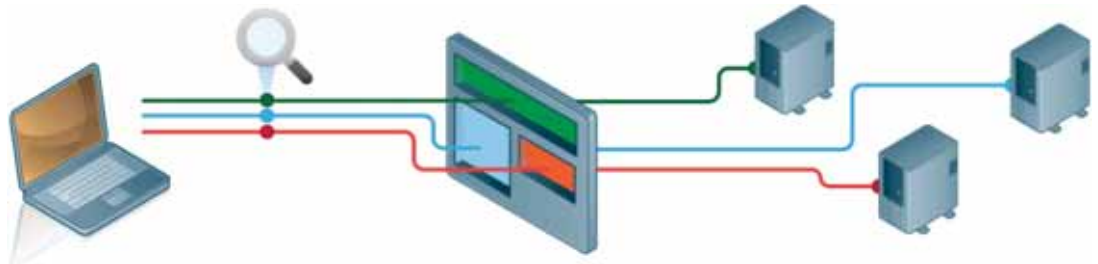
Protokolle im Geschäftsumfeld sichergestellt. Auch ist eine selektive Analyse von verschlüsselten Verbindungen über SSL möglich. Die Selektion kann dabei so eingestellt werden, dass lediglich jene Verbindungen zu Servern entschlüsselt werden, bei denen Verdacht auf schadhafte oder unzulässigen Inhalt besteht. Vertrauenswürdige Verbindungen hingegen können direkt an den Client übermittelt werden, wodurch Aspekte der Sicherheit des Unternehmensnetzwerkes mit datenschutzrechtlichen Bedenken einzelner Mitarbeiter in Einklang gebracht werden.

Malware-Abwehr

Cisco IronPort Web-Reputationsfilter stellt die erste Verteidigungslinie zur Abwehr von Malware-Attacken dar, bevor diese überhaupt ins Netzwerk gelangen können. Dabei wird die Vertrauenswürdigkeit von URLs basierend auf den Daten von SenderBase bewertet. SenderBase ist die größte Reputationsdatenbank im Internet und Teil von SensorBase der Cisco Security Intelligence Operations, welche Informationen und Daten von unterschiedlichsten Cisco Sicherheitssystemen und -lösungen analysiert. Der Web-Reputationsfilter nutzt diese Informationen, um URLs anhand von mehr als 200 verschiedenen gewichteten web- und netzwerkspezifischen

Parametern zu beurteilen. Auf Grundlage des errechneten Reputationswertes von -10 bis +10 werden URL-Anfragen in Echtzeit gefiltert. Je nach individueller Einstellung werden Webseiten mit schlechter Reputation geblockt, während alle anderen Anfragen zur weiteren Analyse übermittelt werden. Der Web-Reputationsfilter analysiert dabei nicht nur die ursprüngliche URL-Anfrage des Users, sondern auch alle folgenden Datenanfragen des Browsers wie beispielsweise zur Integration von Multimedia-Inhalten, die auf den unterschiedlichsten Webservern gehostet sein können.

Der Cisco IronPort Web-Reputationsfilter analysiert nicht nur die ursprüngliche URL-Anfrage, sondern jedes einzelne Objekt einer Site und bewertet dabei deren Vertrauenswürdigkeit.



Cisco IronPort Anti-Malware System scannt und überprüft Webinhalte anhand von Malware-Signaturen. Grundlage hierfür ist der kombinierte Einsatz marktführender signaturbasierter Virenscanner mit der einzigartigen Cisco IronPort Dynamic Vectoring and Streaming (DVS) Engine. Die DVS Engine nutzt neben ausgeklügelten Objektanalyse- und Vectoring-Techniken innovative Verfahren zum Lesen von Datenströmen sowie patentierte Funktionen für sinnvolles Caching. Auf diese Weise werden hohe Durchsatzleistung und kurze Latenzzeiten gewährleistet, die den Einsatz herstellerübergreifender Scan-Funktionen erstmals auch für HTTP-Gateways ermöglichen.

Layer 4 (L4) Traffic Monitor scannt sämtliche Ports und Protokolle in Echtzeit, um Downloads sowie „Phone-Home“-Aktivitäten von Spyware zu unterbinden. Durch die Überwachung aller 65.535 Netzwerk-Ports stoppt der L4 Traffic Monitor auch jene Malware-Attacken, bei denen versucht wird, den Port 80 zu umgehen. Dabei kann individuell eingestellt werden, ob die Aktivitäten über den L4 Traffic Monitor nur kontrolliert oder kontrolliert und geblockt werden sollen.

Datenschutz

Allgemeingültige Sicherheitsrichtlinien können schnell und einfach direkt on-box auf der Cisco IronPort Web Security Appliance definiert und durchgesetzt werden, um den ausgehenden Webverkehr über HTTP, HTTPS sowie FTP zu kontrollieren. Basierend auf der Analyse von File-Metadaten, URL-Kategorien, Nutzerdefinitionen sowie der Web-Reputation werden einzelne Anfragen schließlich durchgestellt, geblockt oder protokolliert.

Komplexe DLP-Systeme, die bereits im Unternehmen implementiert sind, können über ICAP nahtlos an die Cisco IronPort Web Security Appliance angebunden werden. Dieses Verfahren ermöglicht eine umfassende Inhaltsanalyse, wobei die externe DLP-Lösung Hand in Hand mit den definierten Sicherheitsrichtlinien auf der Appliance zusammenwirkt.

Nutzungsrichtlinien

Cisco IronPort Web Access Controls umfasst innovative Technologien zur dynamischen Filterung von URL-Anfragen. Dies ermöglicht nicht nur eine feinere Kategorisierung, auch können so Verbindungen zu nicht-kategorisierten Webseiten in Echtzeit klassifiziert werden. Welche URL-Kategorien schließlich geblockt oder erlaubt werden sollen, kann entsprechend der Authentifizierung im Active Directory spezifisch für verschiedene Gruppen sowie einzelne Individuen definiert werden. Zudem können bei der Implementierung der

Nutzungsrichtlinien des Internets auch zeitbasierte Einstellungen berücksichtigt werden. So beispielsweise kann der Zugriff auf bestimmte Webseiten in der Regelarbeitszeit geblockt werden, davor und danach jedoch erlaubt sein. Um die Mitarbeiter über eingeführte Richtlinien im Unternehmen zu informieren, ist die Einblendung von Warnhinweisen möglich. Auf diese Weise wird der Nutzer dazu aufgefordert, die Nutzungsbedingungen anzuerkennen, bevor die Freigabe der URL-Anfrage zur weiteren Bearbeitung erfolgt.

Order	Group	Applications	URL Categories	Objects	Anti-Malware	Content
1	QA	Block: FTP Block: User Agents	Block: 52 Monitor: 2 Allow: 0	Block: 236 Mb	(global policy)	
2	Engineering	Block: User Agents	Block: 52 Monitor: 2 Allow: 2	Block: No Max Size Block: Object Types Block: File Types	(global)	
3	Marketing	(disabled)	Block: 52 Monitor: 2 Allow: 2	Block: No Max Size Block: Object Types	Block: 22 Monitor: 2	
4	Dev	(global policy)	Block: 52 Monitor: 2 Allow: 2	Block: No Max Size	(global policy)	
Global Policy		Block: FTP, HTTPS Block: HTTP Block: User Agents Block: Ports 443, 21	Block: 45 Monitor: 2 Allow: 2	Block: 236 Mb Block: Object Types Block: File Types	Monitor: 22 Monitor: 0	

- Marketing**
 - FTP-Uploads geblockt
 - Media-Files erlaubt
- Sales**
 - Blocken von ausführbaren Dateien
 - HTTPS-Verbindungen entschlüsselt
- IT**
 - Zugriff auf sämtliche URL-Kategorien erlaubt
 - Adobe-Updates sind von Authentifizierung ausgeschlossen

Basierend auf einer Vielzahl an Parametern können dedizierte Richtlinien für die unterschiedlichsten Nutzergruppen definiert werden.

Management Tools

Cisco IronPort Web Security Manager bietet einen vollständigen Überblick über alle Zugriffs- und Sicherheitsrichtlinien, die auf der Cisco IronPort S-Serie eingerichtet sind. Auf diese Weise können Administratoren von einer zentralen Stelle aus Änderungen jeglicher Art vornehmen, so dass ein unternehmensweites Management gewährleistet wird.

Cisco IronPort Web Security Monitor trägt mittels Echtzeitberichten und historischen Analysen zur Transparenz des Internetverkehrs bei. Dies ermöglicht nicht nur eine gezielte Identifikation infizierter PCs im Netzwerk, auch sind regelmäßige Berichte sowie Trendanalysen abrufbar. Die benutzerfreundliche GUI unterstützt Sie dabei.

Cisco IronPort S-Serie

TECHNISCHE DATEN

S160

S360

S660

Gehäuse/Prozessor

Abmessung	1 HE (4,5 cm x 44,5 cm x 54,6 cm)	2 HE (8,9 cm x 44,5 cm x 74,9 cm)	2 HE (8,9 cm x 44,5 cm x 74,9 cm)
Gewicht	10 kg	26 kg	26 kg
Netzteil	750 Watt, 100/240 V	750 Watt, 100/240 V	750 Watt, 100/240 V
Wärmeenergie	546 – 853 BTU	redundantes Netzteil 820 – 1228 BTU	redundantes Netzteil 990 – 1478 BTU
CPU	1 Intel dual core	1 Intel quad core, 4 MB Cache	2 Intel quad core, 4 MB Cache
RAID	RAID 1 Konfiguration 256 MB Cache batteriegepuffert	RAID 10 Konfiguration 256 MB Cache batteriegepuffert	RAID 10 Konfiguration 256 MB Cache batteriegepuffert
Hot Swappable Laufwerke	–	Ja	Ja
Netzwerk	6x Gigabit NICs, RJ-45	6x Gigabit NICs, RJ-45	6x Gigabit NICs, RJ-45
Speicherplatz	500 GB (2x 250 GB SATA) 50 GB Cache	1,2 TB (4x 300 GB SAS) 100 GB Cache	1,8 TB (6x 300 GB SAS) 200 GB Cache

Anschlüsse

Seriell	1x RS-232 (DB-9)	1x RS-232 (DB-9)	1x RS-232 (DB-9)
Fiber	–	–	optional

Konfiguration/Logging/Monitoring

Web-Interface	zugänglich über HTTP oder HTTPS
Kommandozeile	zugänglich über SSH oder Telnet (Konfigurationsassistent oder Kommandozeile)
Logging	Squid, Apache, Syslog
Zentralisiertes Reporting	wird unterstützt bei allen Appliances
Datentransfer	SCP, FTP oder SYSLOG
Konfigurationsdaten	XML-basiert
Zentralisierte Konfiguration	wird unterstützt
Monitoring	SNMP, E-Mail-Alerts

PRODUKT-ÜBERSICHT

S160	Konzipiert für kleine bis mittelständische Unternehmen mit bis zu 1.000 Usern
S360	Empfohlen für Organisationen mit 1.000 bis 10.000 Usern
S660	Für große Unternehmen mit über 10.000 Usern

Nutzen Sie unser Angebot einer kostenlosen 30-Tage-Teststellung und unterziehen Sie, ganz unverbindlich, die Cisco IronPort Web Security Appliance dem Praxistest. Fordern Sie jetzt Ihre Appliance zu Evaluationszwecken an unter www.ironport.de/testen oder kontaktieren Sie uns per E-Mail an ironport-dach@cisco.com.



Cisco Systems GmbH
IronPort Europe
Am Söldnermoos 17
85399 Hallbergmoos
Deutschland

Cisco Systems, Inc. (NASDAQ: CSCO) mit Hauptsitz in San Jose (CA) ist mit 39,5 Milliarden US-Dollar Umsatz (26. Juli 2008) weltweit führender Anbieter von Networking-Lösungen für das Internet. Die deutsche Niederlassung Cisco Systems GmbH hat ihren Sitz in Hallbergmoos bei München und Büros in Eschborn bei Frankfurt am Main, Hamburg, Düsseldorf, Stuttgart und Berlin. Cisco-Produkte werden in Europa von der Cisco Systems International BV geliefert, eine Tochtergesellschaft im vollständigen Besitz der Cisco Systems, Inc. Cisco, Cisco Systems und das Cisco Systems-Logo sind eingetragene Marken oder Kennzeichen von Cisco Systems, Inc. und/oder deren verbundenen Unternehmen in den USA und in anderen Ländern. Alle anderen in diesem Dokument enthaltenen Marken sind Eigentum ihrer jeweiligen Inhaber. Die Verwendung des Worts "Partner" bedeutet nicht, dass eine Partnerschaft oder Gesellschaft zwischen Cisco und dem jeweils anderen Unternehmen besteht. Dieses Dokument ist eine Veröffentlichung von Cisco. Sitz der Gesellschaft: Am Söldnermoos 17, 85399 Hallbergmoos; Amtsgericht München HRB 102605; Geschäftsführer: Michael Ganser, Andreas Dohmen, Norbert Spinner; WEEE-Reg.-Nr. DE 65286400