



**BEDENKENLOS UND SICHER IM
INTERNET MIT DER IRONPORT
WEB SECURITY APPLIANCE™**

ÜBERBLICK

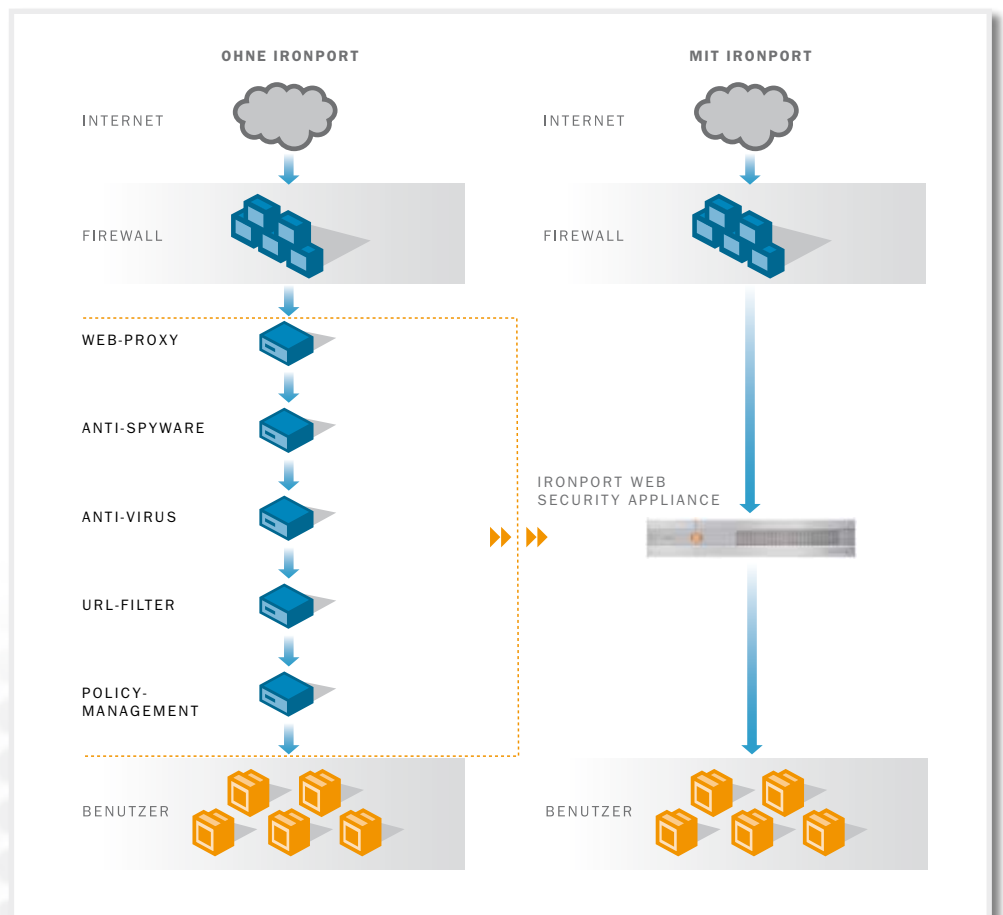
Malware, Spyware & Co. zählen mittlerweile zu den größten Sicherheitsproblemen hierzulande. Mehr als 75% der PCs in Unternehmen sind bereits mit schadhaftem Code infiziert. Dabei stellen sich zunehmend auch vertrauenswürdige Webpages als eine der größten Gefahrenquellen heraus. 70% der webbasierten Bedrohungen gehen von kompromittierten Internetseiten aus. Der alleinige Besuch führt dabei zur unweigerlichen Infektion des Rechners

mit Mal-, Spy- oder auch Adware. Auf diese Weise entstehen nicht nur erhebliche Sicherheitslücken im Netzwerk, auch können so sensitive Unternehmensdaten unbemerkt ausspioniert werden. Bewahren Sie die Kontrolle über den gesamten ein- wie ausgehenden Internetverkehr und schützen Sie Ihr Unternehmensnetzwerk vor webbasierten Bedrohungen mit der IronPort Web Security Appliance™.

Sicherheit im Webverkehr

Die 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 leistungs-

starken Web-Proxy gewährleistet nicht nur eine deutlich verbesserte Performance, sondern auch höhere Zuverlässigkeit als es traditionellen Systemen möglich ist. Die IronPort Web Security Appliance™ gehört damit zu den führenden Lösungen beim Schutz gegen webbasierte Bedrohungen.



Die S-Serie von IronPort bietet mehrschichtigen Schutz vor webbasierten Bedrohungen. Dabei sind Web-Reputationsfilter sowie führende Anti-Malwarelösungen auf einem schnellen Proxy integriert.

LEISTUNGS-
MERKMALE

Leistungsstarke Sicherheitsplattform

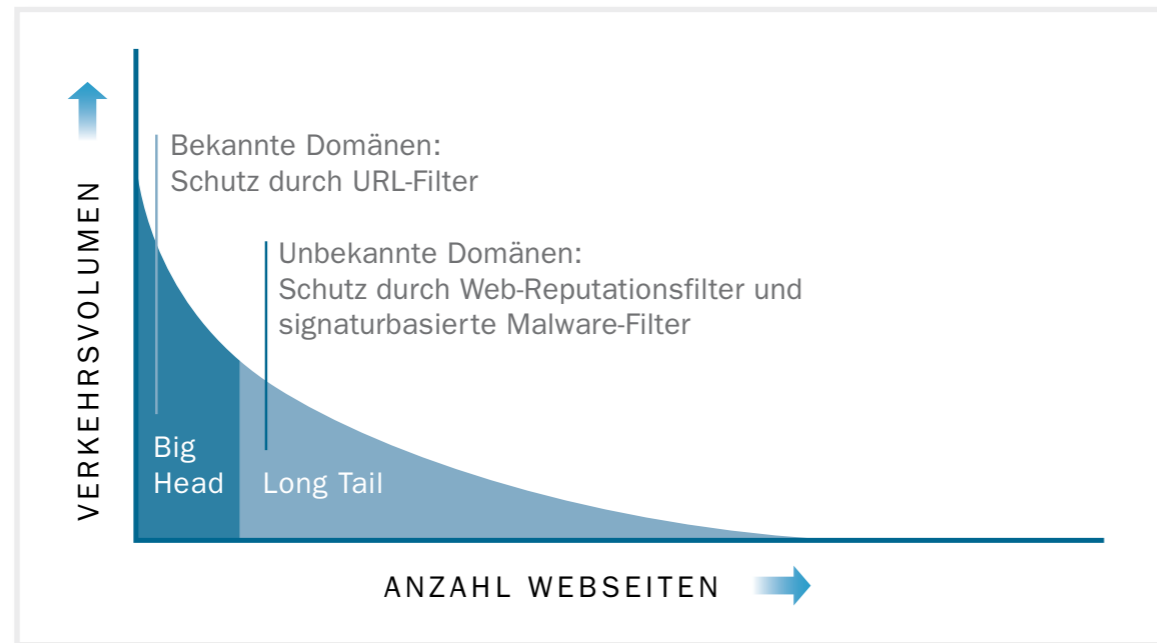
HTTP, HTTPS und FTP Application-Proxy ermöglichen eine tiefgreifende Inhaltsanalyse. Basierend auf IronPorts proprietärem Betriebssystem AsyncOS™ schafft der Proxy problemlos bis zu 100.000 gleichzeitig aktive TCP-Verbindungen. Damit wird ein besonders hohes Maß an Skalierbarkeit und Stabilität im Bereich der Websicherheit gewährleistet.

Layer 4 (L4) Traffic Monitor scannt sämtliche Ports und Protokolle in Echtzeit, um Downloads sowie „Phone-Home“-Aktivitäten von Spyware zu blockieren. Durch die Überwachung aller 65.535 Netzwerk-Ports stoppt der Layer 4 Traffic Monitor auch jene Malware-Attacken, bei denen versucht wird, den Port 80 zu umgehen.

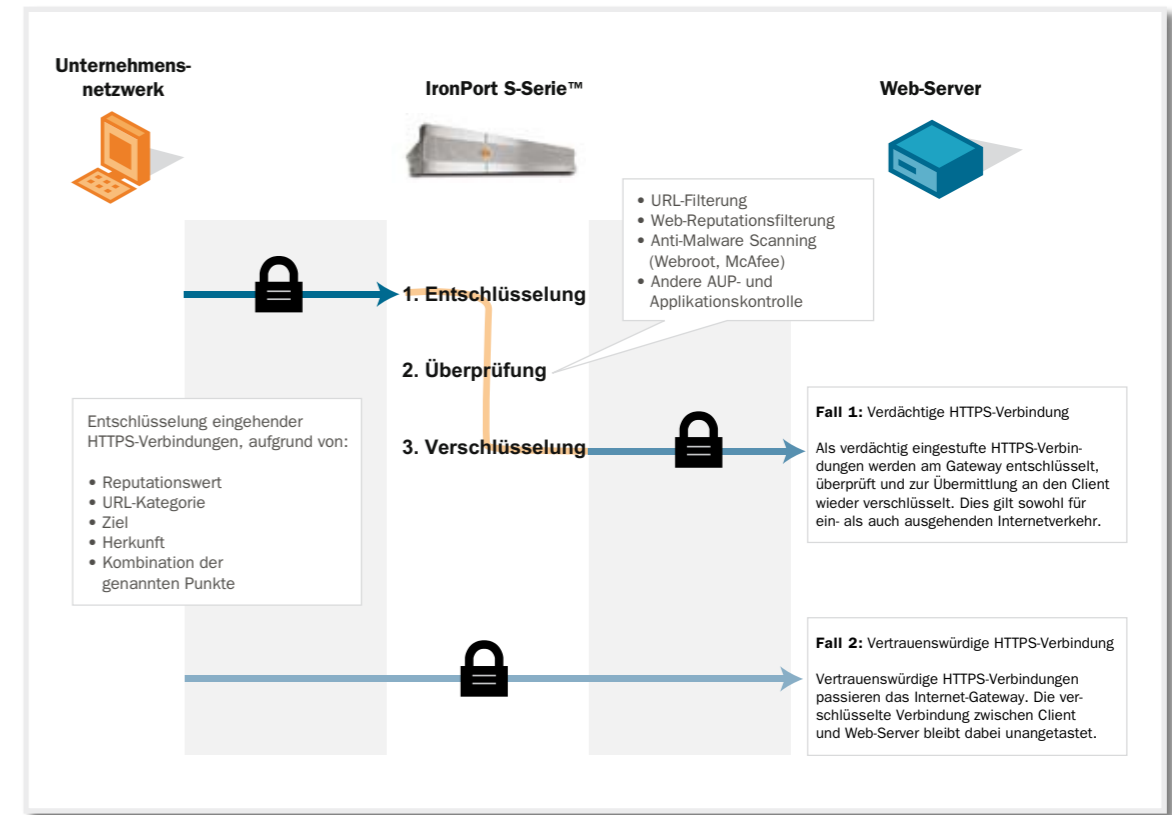
Mehrschichtiger Schutz

IronPort URL Filters™ bieten eine zuverlässige Filterung von Webinhalten gemäß unternehmensspezifischer Richtlinien zur Internetnutzung am Arbeitsplatz. Folglich können Sie nicht nur die mit der Internetnutzung potenziell verbundenen Produktivitätsverluste, sondern auch rechtliche Risiken auf ein Minimum reduzieren. Der URL-Filter von IronPort gewährleistet dabei ein unübertroffenes Maß an Qualität und Zuverlässigkeit. Nicht zuletzt auch aufgrund der dahinterstehenden Datenbank: Kontinuierlich wachsend und stetig aktualisiert umfasst sie über drei Milliarden Webseiten in mehr als 70 Sprachen und über 200 Länder hinweg.

IronPort Web Reputation Filter™ bewertet die Vertrauenswürdigkeit von URLs basierend auf den Daten von IronPort SenderBase™. Das weltweit größte Netzwerk zur Überwachung des E-Mail- und Webverkehrs analysiert über 30% der globalen Kommunikation im Internet. Der Web-Reputationsfilter nutzt diese Informationen, um URLs anhand 45 verschiedener gewichteter Parameter zu beurteilen. Auf Grundlage des errechneten Reputationswertes von -10 bis +10 werden URL-Anfragen in Echtzeit gefiltert: Je nach Einstellung werden Webseiten mit schlechter Reputation geblockt und alle anderen Anfragen zur weiteren Analyse frei gegeben.



Das größte Gefahrenpotenzial geht von den zahlreichen unbekanntem Webseiten aus, die sehr kurzfristig auftreten und sehr häufig Malware beherbergen.



Mit der IronPort HTTPS Scanning Engine bewahren Sie die Kontrolle auch über verschlüsselte Internet-Verbindungen, ohne dabei in datenschutzbedingte Belange Ihrer Mitarbeiter einzugreifen.

IronPort Anti-Malware System™ scannt und überprüft Webinhalte anhand von Malware-Signaturen. Grundlage hierfür ist der kombinierte Einsatz marktführender signaturbasierter Virens Scanner mit der einzigartigen 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.

IronPort HTTPS Scanning Engine nutzt die Informationen der Web-Reputations- und URL-Filter für ein selektives Analysieren der verschlüsselten Verbindungen. Dabei können Sie die Selektion so einstellen, dass lediglich HTTPS-Verbindungen zu Servern mit niedriger Reputation entschlüsselt werden, bei denen Verdacht auf schadhafte oder unzulässigen Inhalt besteht. Vertrauenswürdige HTTPS-Verbindungen hingegen können direkt an den Client übermittelt werden. Die IronPort HTTPS Scanning Engine ermöglicht es somit, Aspekte der Sicherheit des Unternehmensnetzwerkes mit datenschutzrechtlichen Bedenken einzelner Mitarbeiter in Einklang zu bringen.

Umfassendes Management und Reporting

IronPort Web Security Manager™ bietet einen vollständigen Überblick über alle Zugriffs- und Sicherheitsrichtlinien, die auf der IronPort Web Security Appliance™ eingerichtet sind. Administratoren können von hier aus Änderungen jeglicher Art wie beispielsweise User Policies vornehmen.

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

**PRODUKT-
ÜBERSICHT**

IronPort Systems bietet branchenführende Web Security Appliances für Unternehmen jeglicher Größenordnung:

IronPort S650™ bietet eine leistungsstarke, mehrschichtige sowie herstellerunabhängige Web-Sicherheitslösung für Unternehmen mit mehr als 5.000 Benutzern

IronPort S350™ mit den gleichen Funktionen wie die S650 entspricht diese Plattform den Sicherheitsanforderungen von Unternehmen mit bis zu 5.000 Benutzern

**TECHNISCHE
DATEN
(modellabhängig)****Gehäuse/Prozessor**

Abmessung 19 Zoll, 2 HU (3,5 Zoll x 19 Zoll x 29 Zoll)
CPU 2x Intel dual core, 4 MB Cache

Festplatten

RAID RAID 10 Konfiguration, 256 MB Cache batteriegepuffert
Laufwerke 6 x 146 GB SAS

Anschlüsse

Netzwerk 6 x Gigabit NICs, RJ-45
Seriell 1 x RS-232 (DB-9)

Interfaces/Konfiguration

Web-Interface zugänglich über HTTP oder HTTPS
Kommandozeile zugänglich über SSH oder Telnet;
Konfigurationsassistent oder Kommando-Zeile
Datentransfer SCP, FTP oder SYSLOG
Konfigurationsdaten XML-basierte Konfigurationsdatei



Nutzen Sie unser Angebot einer kostenlosen 30-Tage-Teststellung. Unterziehen Sie – ganz unverbindlich – die IronPort Web Security Appliance™ dem Praxistest. Besuchen Sie uns auf unserer Homepage www.ironport.com/de/how_to_buy oder rufen Sie uns einfach an unter **089-45 22 27-0**.

**IronPort Systems – A Cisco Business Unit**

Paul-Wassermann-Str. 3, 81829 München
TEL 089-45 22 27-0 **FAX** 089-45 22 27-10
E-MAIL de-info@ironport.com **WEB** www.ironport.de

IronPort Systems ist eine Geschäftseinheit von Cisco und ein führender Anbieter von Lösungen zum Schutz vor Spam, Viren und Spyware. Die Appliances von IronPort wurden für kleine Firmen bis hin zu Global-2000-Unternehmen entwickelt und spielen in der Netzinfrastruktur eines Unternehmens eine geschäftsentscheidende Rolle. Die innovativen Systeme sind einfach zu bedienen und bieten höchste Leistungsfähigkeit. Sie nutzen SenderBase™, die weltweit größte Datenbank zur Beobachtung und Bewertung von E-Mail- und Web-Bedrohungen. Mehr Informationen über Produkte, Lösungen und Services von IronPort finden Sie unter www.ironport.de

Copyright © 2008 Cisco Systems, Inc. Alle Rechte vorbehalten. IronPort, das IronPort-Logo und SenderBase sind eingetragene Warenzeichen von Cisco Systems, Inc. Alle anderen Warenzeichen sind Eigentum von Cisco Systems, Inc., oder ihrer jeweiligen Eigentümer. Es wird jede Anstrengung unternommen, um die Richtigkeit der Informationen sicherzustellen, doch übernimmt Cisco keine Haftung für Irrtümer oder Fehler, die auftreten könnten. Technische Daten und andere Informationen in diesem Dokument unterliegen eventuellen Änderungen.

IronPort is now
part of Cisco.

