

Cisco IronPort C-Serie



Ob Spam, Malware oder Phishing – die Bedrohungen, die von E-Mails ausgehen, sind weiterhin im Anstieg. Dabei nimmt nicht nur die Anzahl der Angriffe zu, auch werden die einzelnen Attacken zunehmend komplexer und professioneller. So werden mittlerweile bis zu 180 Mrd. Spam-Nachrichten pro Tag versandt. Viele Unternehmen berichten, dass bereits mehr als 90% ihrer eingehenden E-Mails unerwünscht sind. Während die traditionelle Spam-Nachricht den schadhafte Code beispielsweise als PDF-, Excel- oder

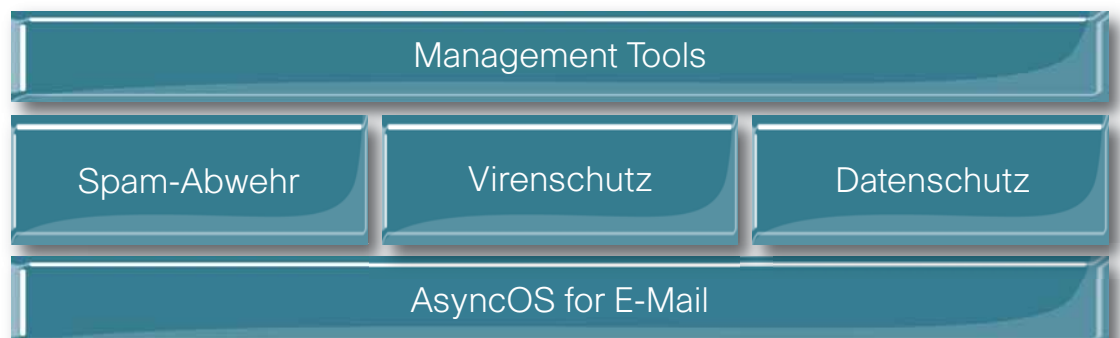
auch MP3-Anhang gleich mit übertragen hatte, ist heutzutage meist nur noch ein Link auf eine mit Malware verseuchte Internetseite beinhaltet. Jedoch stellt nicht nur der eingehende E-Mail-Verkehr ein Problem dar. Auch können sensitive Unternehmensdaten über E-Mail nach außen an unbefugte Dritte gesandt werden. Bewahren Sie daher die Kontrolle über den gesamten ein- wie ausgehenden E-Mail-Verkehr im Unternehmensnetzwerk mit den Cisco IronPort E-Mail Security Appliances und Services.

E-Mails im Griff mit der Cisco IronPort E-Mail Security Appliance

Die Cisco IronPort E-Mail Security Appliance ist bei Unternehmen jeglicher Größenordnung im Einsatz. Das mehrschichtige System zeichnet sich insbesondere durch die Kombination erstklassiger E-Mail- und Web-Reputationsfilter mit anschließender Spam- und Virenanalyse aus. Das Zusammenspiel präventiver und reaktiver Schutzmechanismen sowie der Einsatz des hochperformanten Betriebssystems AsyncOS gewährleisten dabei ein Höchstmaß an Leistungsfähigkeit und Zuverlässigkeit. So wird allein durch den IronPort Reputationsfilter der Großteil der unerwünschten E-Mails aufgrund schlechter

Reputationswerte bereits direkt am Gateway abgeblockt. Die selben Sicherheitstechnologien mit denen IronPort bereits im Segment für Security Appliances die weltweite Marktführerschaft erzielt hat, stehen nun auch als Managed, Hosted und Hybrid Hosted E-Mail Security Services zur Verfügung. Die Auswahl an Implementierungsmodellen ermöglicht es Kunden frei zu entscheiden, in welcher Art und Weise die Absicherung des E-Mail-Verkehrs geschehen soll – ob direkt vor Ort, komplett gemanagt, Cloud-basiert oder durch eine Kombination aller drei Möglichkeiten.

Die Cisco IronPort C-Serie basiert auf einem mehrschichtigen System und gewährleistet so eine umfassende Absicherung des ein- sowie ausgehenden E-Mail-Verkehrs.



Leistungsstarke Sicherheitsplattform

Die Cisco IronPort E-Mail Security Appliances sind speziell für die Absicherung des ein- und ausgehenden E-Mail-Verkehrs konstruiert. Basis hierfür bildet das proprietäre Betriebssystem **AsyncOS**, welches 2001 gemäß den Anforderungen der weltweit größten Infrastrukturen entwickelt worden ist. Neben 10.000 gleichzeitig aktiven Verbindungen bietet AsyncOS for E-Mail

fortschrittliche Funktionen wie dynamisches Queue-Management und Bounce-Handling. Zudem ist auch die gedrosselte Annahme von verdächtigen E-Mails möglich. Auf diese Weise wird gewährleistet, dass die E-Mail-Infrastruktur selbst bei massiven Viren- und Spam-Angriffen zu keinem Zeitpunkt überlastet ist.

Spam-Abwehr

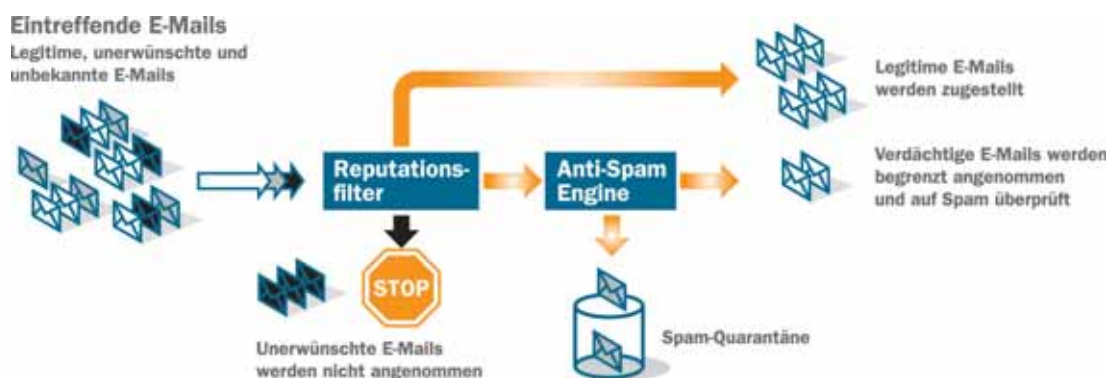
Cisco IronPort Reputationsfilter blockt als äußerer Schutzwall unerwünschte E-Mails bereits vor der Annahme ab. Grundlage hierfür sind die Echtzeit-Daten von SenderBase, der weltweit größten Reputationsdatenbank im Internet. SenderBase wird seit seiner Entstehung in 2002 kontinuierlich weiterentwickelt und analysiert als Teil von SensorBase der Cisco Security Intelligence Operations über 30% der globalen Kommunikation im Internet. Der Reputationsfilter nutzt diese Informationen der über 200 verschie-

den gewichteten Parameter, um spezifische Reputationswerte von -10 bis +10 zu errechnen. Bis zu welchem Wert eine E-Mail direkt am Gateway abgeblockt wird und ab wann eine Übermittlung zur weiteren Analyse bzw. eine direkte Zustellung der E-Mail ermöglicht ist, kann individuell auf der Appliance definiert werden. Je nachdem wie aggressiv die E-Mail-Policies eingestellt sind, können so bereits bis über 90% des unerwünschten Nachrichtenverkehrs direkt am Gateway abgewehrt werden.

Cisco IronPort Anti-Spam schließt nahtlos an den Reputationsfilter an und bietet mit der Context Adaptive Scanning Engine (CASE) ein innovatives System, das den gesamten Kontext einer E-Mail analysiert. Dabei werden Attribute zur Herkunft der Nachricht, zum Inhalt und Aufbau der E-Mail sowie über möglicherweise

verwendete URLs näher untersucht. So wird das Ergebnis der Spam-Filterung äußerst präzise: Unerwünschte E-Mails werden zuverlässig von legitimen E-Mails unterschieden und das mit einer branchenweit führenden Trefferquote sowie geringster False-Positive-Rate von 1:1.000.000.

Der Cisco IronPort Reputationsfilter blockt über 90% der eingehenden Spam-Mails bereits am Perimeter Ihres Netzwerkes ab und verbessert so die Gesamtwirksamkeit bedeutend.



Virenschutz

Cisco IronPort Virus Outbreak Filter dient der präventiven Abwehr bisher unbekannter Viren. Den Ausbruch neuer Viren registriert Sender-Base anhand der entstehenden Anomalien im weltweiten Datenverkehr. Verdächtige E-Mails werden daraufhin vom Virus Outbreak Filter in eine dynamische Quarantäne gestellt.

Cisco IronPort Anti-Virus Filter nutzt die bewährten Anti-Virenfilter von McAfee und Sophos. Die Integration dieser beiden signaturbasierten Virenfilter am Gateway gewährleistet in Kombination mit dem IronPort Virus Outbreak Filter einen äußerst wirksamen Schutz selbst bei extrem komplexen Angriffen.



Die dynamische Quarantäne stellt sicher, dass die kritische Zeit zwischen Virenausbruch und Veröffentlichung der entsprechenden Signatur des Anti-Virencanners überbrückt wird.

Datenschutz

Data Loss Prevention umfasst den Schutz vertrauenswürdiger Unternehmensdaten. Um den Datenverlust über den Versand von E-Mails zu verhindern, überprüft der Cisco IronPort Contentfilter die Inhalte aller ausgehenden Nachrichten inklusive Header und Dateianhänge nach spezifischen Suchbegriffen oder regulären Ausdrücken. Nachrichten mit sensitiven Daten werden je nach Regelvorgaben in Quarantäne gestellt, modifiziert, archiviert oder direkt verschlüsselt – ohne dass der Versender darauf Einfluss nehmen muss bzw. kann. Mittels vordefinierter Wörterbücher wie HIPAA, GLB und SOX werden zudem auch Compliance-Richtlinien von Unternehmen eingehalten. Ergänzt wird der IronPort Contentfilter mit weiterführenden DLP-Funktionen des Herstellers RSA, die über eine vollständig integrierte Softwarelizenz als zusätzliches Feature eingebunden werden können.

Cisco IronPort PXE Encryption ist eine einzigartige Methode der E-Mail-Verschlüsselung, die weder eine Softwareinstallation noch besondere Kenntnisse beim Endanwender erfordert und unabhängig von S/MIME oder Open-PGP funktioniert. Die Entschlüsselung der Nachricht erfolgt direkt am Arbeitsplatz des Empfängers ohne zusätzliche Software direkt im Webbrowser. Als Absender können Sie Ihre Nachrichten zeitlich befristen, ungelesene E-Mails problemlos zurückrufen sowie den Versand großer Dateien steuern. Als weitere Funktion können Sie zudem das Senden von Empfangs- und Lesebestätigungen einstellen und es dem Empfänger ermöglichen, auch verschlüsselt zu antworten.

Management Tools

Zentralisiertes Management ermöglicht auch bei Installationen mit mehreren Appliances eine extrem einfache, sichere und zuverlässige Verwaltung der Systeme. Dabei können lokale Adaptionen unter Berücksichtigung der global definierten Richtlinien vorgenommen werden. Je nach Berechtigung des Administrators kann dieser Einstellungen für spezifische Individuen und Gruppen im Unternehmen, einzelne Geräte oder aber auch für die Gesamtheit aller installierten E-Mail Security Appliances ändern. Die Konfigurationen sind dabei wahlweise über die benutzerfreundliche GUI oder auch per Kommandozeile möglich.

Reporting- und Tracking-Funktionalitäten sind auf allen IronPort E-Mail Security Appliances integriert. So beispielsweise können mit dem IronPort Message Tracking einzelne E-Mails sekunden-schnell per Mausklick über Suchkriterien wie Absender, Empfänger, Domäne, IP-Adresse oder spezifischen Wörtern aufgefunden werden. Darüber hinaus stehen über die in Echtzeit gelieferten Berichte alle Informationen zu den installierten Appliances stets zur Verfügung. Ein automatischer Versand der Reports per E-Mail an ausgewählte Empfänger ist ebenfalls einstellbar.



Cisco IronPort C-Serie

TECHNISCHE DATEN

C160

C360

C360D

C660

X1060

Gehäuse/Prozessor

Abmessung	1 HE (5,5 x 44,5 x 54,6 cm)	2 HE (8,9 x 44,5 x 74,9 cm)	2 HE (8,9 x 44,5 x 74,9 cm)	2 HE (8,9 x 44,5 x 74,9 cm)	2 HE (8,9 x 44,5 x 74,9 cm)
Gewicht	9,5 kg	23,5 kg	23,5 kg	23,5 kg	25,4 kg
Netzteil	750 Watt, 100/240 V	750 Watt, 100/240 V	750 Watt, 100/240 V	750 Watt, 100/240 V	750 Watt, 100/240 V
Wärmeenergie	546 – 853 BTU	820 – 1228 BTU	820 – 1228 BTU	891 – 1330 BTU	990 – 1478 BTU
CPU	1 Intel	1 Intel multi core	1 Intel multi core	2 Intel multi core	2 Intel multi core
Speicher	2 x 80 GB 7200 RPM SATA	2 x 146 GB 10.000 RPM U320 SCSI	2 x 146 GB 10.000 RPM U320 SCSI	4 x 146 GB 10.000 RPM U320 SCSI	4 x 146 GB 10.000 RPM U320 SCSI
RAID	RAID 1	RAID 1	RAID 1	RAID 10	RAID 10
Netzwerk	2 x 10/100/1000 BaseT Ethernet	3 x 10/100/1000 BaseT Ethernet	3 x 10/100/1000 BaseT Ethernet	3 x 10/100/1000 BaseT Ethernet	3 x 10/100/1000 BaseT Ethernet
Kapazität	10 GB Queue	35 GB Queue	35 GB Queue	70 GB Queue	70 GB Queue

Unterstützte Standards

E-Mail-Protokolle	SMTP, ESMTP, Secure SMTP über TLS
DNS	Interner Resolver/Cache; Auflösung unter Nutzung lokaler DNS oder Internet-DNS-Server
LDAP	U. a. Integration mit Active Directory, Notes, Domino und OpenLDAP-Server

Interfaces/Konfiguration

Web-Interface	Zugänglich über HTTP oder HTTPS
Kommandozeile	Zugänglich über SSH oder DB-9 Serial Port, Konfigurationsassistent und Kommandozeile
Datentransfer	SCP oder FTP
Monitoring	XML über HTTPS, SNMP
Konfigurationsdaten	XML-basierte Konfigurationsdatei

PRODUKT-ÜBERSICHT

C160	Benutzerfreundliche Komplettlösung für kleine bis mittelständische Unternehmen
C360	Für mittelständische bis große Unternehmen
C360D	Für alle Unternehmen mit besonderen Anforderungen an die ausgehende E-Mail-Kommunikation
C660	Für große Unternehmen und Service-Provider
X1060	Speziell für die Anforderungen der anspruchsvollsten Netzwerke
Hosted Services	Schutz über eine dedizierte E-Mail-Infrastruktur, die in einem Netzwerk von Cisco-Rechenzentren betrieben wird
Hybrid Hosted Service	Kombination der Vorteile von Inhouse- und Cloud-basierten Lösungen
Managed Services	Externe Verwaltung und Überwachung der E-Mail-Infrastruktur durch Cisco-Sicherheitsexperten

Nutzen Sie unser Angebot einer kostenlosen 30-Tage-Teststellung und unterziehen Sie, ganz unverbindlich, die Cisco IronPort E-Mail 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