Cisco IronPort
Email & Web Security

Frédéric HER, CISSP
Systems Engineer, Africa
Cisco IronPort Solutions
fher@cisco.com
Cisco IronPort
Unparalleled Market Leadership

IronPort funded in 2000, acquired by Cisco in 2007

- 20,000+ customers globally
- 400 million users protected
- 40% of Fortune 100 companies
- 8 of the 10 largest Service Providers
- 7 of the 10 largest Banks
- 99%+ customer renewal rates

Gartner
IronPort Positioned in the “Leaders” Quadrant in Magic Quadrant Report

IDC
IronPort is positioned as a leading player in the messaging security appliance market

The Radicati Group, Inc.
Named IronPort the market share leader in the email security appliance market
The Cisco IronPort Story
Application-Specific Security Gateways

BLOCK Incoming Threats:
- Spam, Phishing/Fraud
- Viruses, Trojans, Worms
- Spyware, Adware
- Unauthorized Access

APPLICATION-SPECIFIC SECURITY GATEWAYS

EMAIL Security Gateway
WEB Security Gateway

SENSORBASE
(The Common Security Database)
Cisco IronPort Email Security Appliance
Email Challenges

Standard Email does not natively offer what is expected

- Junk Mail
- Viruses
- Privacy & Control
- Regulations
Cisco IronPort Consolidates the Network Perimeter
For Security, Reliability and Lower Maintenance

Before Cisco IronPort

Internet

Firewall

Encryption Platform

MTA

Anti-Spam

Anti-Virus

Policy Enforcement

Mail Routing

Groupware

Users

After Cisco IronPort

Internet

Firewall

Cisco IronPort Email Security Appliance

Groupware

Users
Spam Trends

- Record spam volumes and criminal botnet activity
Spam Sophistication Increasing

2005

TEXT SPAM

2006

ATTACHMENT SPAM
(PDF, EXCEL, MP3)

2007

IMAGE SPAM

2008

TARGETED ATTACKS

Your Equitable Bank account is closed, call us now at (802)354-4250
Cisco IronPort SensorBase

- Statistics on more than 30% of the world’s e-mail traffic
- New threats & alerts detection
- More than 200 parameters to build reputation scores

E-Mail Reputation Filters
- Data Volume
- Message Structure
- Complaints
- Blacklists, whitelists
- Off-line data

Web Reputation Filters
- URL blacklists & whitelists
- HTML Content
- Domain Info
- Known “bad” URLs
- Website history…

Reputation Score
Email Security Architecture
Cisco IronPort Email Security Appliance

- INBOUND SECURITY
  - Spam Defense
  - Virus Defense

- MAIL TRANSFER AGENT
  - CISCO IRONPORT ASYNCOS EMAIL PLATFORM

- OUTBOUND CONTROL
  - Data Loss Prevention
  - Secure Messaging

Management
Cisco IronPort AsyncOS
Revolutionary Email Delivery Platform

Traditional Email Gateways and Other Appliances

- 200 Connections
- Disk I/O Bottlenecks
- Low Performance/Peak Delivery Issue
- Unable To Leverage Full Capability Components

Cisco IronPort Email Security Appliances

- 1K – 10K Connections
- CPU
- High Performance/Sure Delivery
- Limited Solely By CPU Capacity
Advanced Controls for Security and Efficiency
And to protect against the risk of being blacklisted

1. Protect internal servers
2. Rules per destination domain

IronPort Virtual Gateways
1. Protects the reputation of a domain
2. Relies on different IP addresses for sending messages

Email Authentication (DomainKeys, DKIM, SPF, SIDF)
Email Security Architecture
Cisco IronPort Email Security Appliance

INBOUND SECURITY
- Spam Defense
- Virus Defense

MAIL TRANSFER AGENT
- CISCO IRONPORT ASYNCOS EMAIL PLATFORM

OUTBOUND CONTROL
- Data Loss Prevention
- Secure Messaging

Management
Anti-Spam Defense in Depth

SensorBase Reputation Filtering

IronPort Anti-Spam

Spam Blocked Before Entering Network

> 99% Catch Rate < 1 in 1 million False Positives

Verdict
Who? How?
Where? What?
SensorBase Reputation Filtering

Real Time Threat Prevention

- Known good is delivered
- Suspicious is rate limited & spam filtered
- Known bad is blocked

Incoming Mail
Good, Bad, and Unknown Email

Reputation Filtering
IronPort Anti-Spam

Cisco’s Internal Email Experience:

<table>
<thead>
<tr>
<th>Message Category</th>
<th>%</th>
<th>Messages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stopped by Reputation Filtering</td>
<td>93.1%</td>
<td>700,876,217</td>
</tr>
<tr>
<td>Stopped as Invalid recipients</td>
<td>0.3%</td>
<td>2,280,104</td>
</tr>
<tr>
<td>Spam Detected</td>
<td>2.5%</td>
<td>18,617,700</td>
</tr>
<tr>
<td>Virus Detected</td>
<td>0.3%</td>
<td>2,144,793</td>
</tr>
<tr>
<td>Stopped by Content Filter</td>
<td>0.6%</td>
<td>4,878,312</td>
</tr>
<tr>
<td><strong>Total Threat Messages:</strong></td>
<td>96.8%</td>
<td>728,797,126</td>
</tr>
<tr>
<td>Clean Messages</td>
<td>3.2%</td>
<td>24,102,874</td>
</tr>
<tr>
<td><strong>Total Attempted Messages:</strong></td>
<td></td>
<td>752,900,000</td>
</tr>
</tbody>
</table>
Email Security Architecture
Cisco IronPort Email Security Appliance

- INBOUND SECURITY:
  - Spam Defense
  - Virus Defense

- MAIL TRANSFER AGENT:
  - Cisco IronPort Asyncos Email Platform

- OUTBOUND CONTROL:
  - Data Loss Prevention
  - Secure Messaging

Management
Cisco IronPort Virus Outbreak Filters

The First Line of Defense
Multi-Layer Virus Defense
Zero Hour Malware Prevention and AV Scanning

An analysis over one year:

Average lead time ....................... over 13 hours
Outbreaks blocked ...................... 291 outbreaks
Total incremental protection ............ over 157 days
Email Security Architecture
Cisco IronPort Email Security Appliance

INBOUND SECURITY

Spam Defense
Virus Defense

MAIL TRANSFER AGENT

CISCO IRONPORT ASYNCSOS EMAIL PLATFORM

OUTBOUND CONTROL

Data Loss Prevention
Secure Messaging

Management
Risks for the Organization

Top Risk: Employees

Biggest Impact: Customer Data

Top Data Loss Types

- Intellectual Property: 21%
- Personnel Information: 20%
- Information marked Confidential: 16%
- Personal client information: 44%
Data Loss Prevention
Comprehensive, Accurate, Easy

Comprehensive
- 100+ Pre-defined templates
- Regulatory compliance

Easy
- One-click activation
- Policy enable/disable

Accurate
- Multiple parameters
- Key words, proximity, etc.
Email Encryption
Instant Deployment, Zero Management Cost

- Automated key management
- No desktop software requirements
- No new hardware required
Email Security Architecture
Cisco IronPort Email Security Appliance

Inbound Security
- Spam Defense
- Virus Defense

Mail Transfer Agent
- Cisco IronPort Asyncos Email Platform

Outbound Control
- Data Loss Prevention
- Secure Messaging

Management
Cisco IronPort Email Security Manager
Single view of policies for the entire organization

“IronPort Email Security Manager serves as a single, versatile dashboard to manage all the services on the appliance.” – PC Magazine
Comprehensive Insight
Unified Business Reporting

- Single view across the organization
- Real Time insight into email traffic and security threats
- Actionable drill down reports
Visibility Into Email Messages

Message Tracking

What happened to the email I sent 2 hours ago?

✓ Track Individual Email Messages

Who else received similar emails?

✓ Forensics to Ensure Compliance
Email Security
Hosted Offerings

Cisco IronPort Hosted Email Security
Choice Maximizes Flexibility
*Full Continuum of Deployment Options*

**Appliances**
- Award-Winning Technology

**Hosted**
- Dedicated SaaS Infrastructure

**Hybrid Hosted**
- Best of Both Worlds

**Managed**
- Fully Managed on Premises

*Backed by Service Level Agreements*
Cisco IronPort Web Security Overview

Cisco IronPort Web Security Appliance
Malware Threat Distribution

Malware infection vectors are shifting from email to Web
Malware Evades Legacy Defenses

URL classification is reactive, has low coverage

Predictable, easy to classify

Hundreds of millions of sites
Thousands of new sites per hour

Signatures are reactive and CANNOT keep up
Exploited Websites
An Invisible Threat

Massive Attack: Half A Million Microsoft-Powered Sites Hit With SQL Injection
By Scott Gilbertson  April 28, 2008 | 8:04:40 AM  Categories: Security
Drive-By Scareware

- Full-screen pop-up simulates real AV software, asks you to buy full version to clean machine.
- Fakes scan of c: drive and pretends to find viruses even on Linux or Mac OS X!
The limits of legacy solutions

- Low Performance – not suitable for current usage of Web
- High Latency
- Low Security: often only URL filtering
- ….or only Antivirus and no efficient protection against Malware
Next Generation Secure Web Gateway

Before Cisco IronPort

Internet

Firewall

Web Proxy & Caching

Anti-Spyware

Anti-Virus

Anti-Phishing

URL Filtering

Policy Management

Users

After Cisco IronPort

Internet

Firewall

Cisco IronPort WSA

Users

All web security components in a single integrated platform
Web Security Architecture
Cisco IronPort Web Security Appliance
High-Performance Web Proxy
Connection Management & Optimized Storage

Maintain pool of persistent TCP connections (client and server side)

Handle extremely high traffic volumes

Co-related object storage and high-performance caching

Significantly improved response times

Facts & Figures:

– 100,000 simultaneous duplex TCP connections to easily handle traffic spikes
– Average latency introduced to end user: 5-15 milliseconds
Web Security Architecture
Cisco IronPort Web Security Appliance

- L4 Traffic Monitor
- URL Filters
- CISCO IRONPORT ASYNCOS WEB PLATFORM
- Web Reputation Filters
- Anti-Malware System

Management

PROXY CACHE
Detecting Existing Client Infections

- Cisco IronPort Layer 4 Traffic Monitor
  - Scans all traffic, all ports, all protocols
  - Detects malware bypassing Port 80
  - Prevents botnet traffic

- Powerful anti-malware data
  - Automatically updated rules
  - Real-time rule generation using “Dynamic Discovery”
Web Security Architecture
Cisco IronPort Web Security Appliance

- L4 Traffic Monitor
- URL Filters
- CISCO IRONPORT ASYNCS
  WEB PLATFORM
- Web Reputation Filters
- Anti-Malware System

PROXY CACHE
Web: Huge, Growing and Transient

- **1998**: 28 Million webpages
- **2000**: 1 Billion webpages
- **2008**: 1 Trillion webpages

**2005**: Web 2.0 tipping point

**Huge**
- 1 Trillion unique URLs

**Growing**
- 1 Billion new pages added every day

**Transient**
- 30% domain-level churn every year

Source: Multiple, including Cisco SIO, Google, Wikipedia
The Dark Web Challenge

Legacy URL Filtering Effectiveness is Decreasing

- Legacy URL filtering primarily focuses on crawling and manual review/classification
- Databases add thousands of new URLs per day...while the web adds a Billion
- 95% of the web will be uncategorized by 2015

URL Lookup in Database

www.sportsbook.com/ → Gambling → Uncategorized

- OBSCENE
- ADULT
- PORN
- GAMBLING
Cisco IronPort Web Usage Controls

Dynamic Categorization for the Dark Web

- Industry-leading URL database efficacy
  - 65 categories
  - Updated every 5 minutes
  - Powered by Cisco SIO

- Dynamic categorization identifies ~90% of Dark Web content in commonly blocked categories
Cisco Security Intelligence Operations (SIO)
Unmatched Visibility Drives Unparalleled Efficacy

Customer Administrators

Cisco IronPort Web Security Appliances on Customer Premises

Uncategorized URLs

URL Categorization Requests

Cisco SIO

Analysis and Processing

Master URL Database

External Feeds

Crowd Sourcing

Manual Categorization

Web Crawlers

Traffic Data from Cisco IronPort Email Security Appliances, Cisco IPS, and Cisco ASA sensors
Web Security Architecture
Cisco IronPort Web Security Appliance

- L4 Traffic Monitor
- URL Filters
- CISCO IRONPORT ASYNCOS WEB PLATFORM
- Web Reputation Filters
- Anti-Malware System
- PROXY CACHE
- Management
Protection For a Dynamic Web 2.0 World

Visibility Beyond the Initial Threat

- Web pages are made up of objects coming from different sources
- Objects can be images, executables, JavaScript...
- Compromised websites often grab malicious objects from external sources
- Security means looking at each object individually, not just the initial request
Cisco IronPort DVS Engine
Dynamic Vectoring and Streaming

- Multiple integrated verdict engines
  - McAfee and Webroot
- Decrypt & scan SSL traffic
  - Selectively, based on category & reputation
- Accelerated signature scanning
  - Parallel scans
  - Stream scanning
- Automated updates

~35% Additional Coverage
Cisco IronPort DVS Engine
*Multi-Layered Malware Defense*

- Deep content inspection
- High-performance scanning
  - Parallel scans
  - Stream scanning
- Multiple verdict engines
  - Integrated, on-box
  - Supported engines: Webroot, McAfee
Usage of Ports 80 & 443 has changed

- A lot of applications traversing port 80 are not “web browsing”
- A lot of applications using port 80 are not business-related
- Nearly all companies include **Webmail** users
  - Malicious attached files?
- **Instant Messaging** is found in all companies
  - How do you keep it open while ensuring your network is not at risk?
- **Web-based file transfer** is growing fast (MegaUpload, Rapidshare…)
- **Peer-to-Peer** is still used heavily
Web Application Controls

- Native control for HTTP, HTTP(s), FTP applications
- Selective decryption of SSL traffic for security and policy
- Policy enforcement for applications tunneled over HTTP—FTP, IM, video
- Application traversal using policy-based HTTP CONNECT

Understanding Web Traffic
HTTPS Scanning
Selective, Based on Trust

Decrypted • Inspected • Re-encrypted
Selectively on TRUST, Category, Source

Decrypted • Inspected • Re-encrypted
Selectively on Category, Source

Users

Cisco IronPort WSA

Internet

Web Server
Cisco IronPort WSA
Complete Data Security

- **On-box Common Sense Security**
  - Allow, block, log based on file metadata, URL category, user and web reputation
  - Multi-protocol: HTTP(s), FTP, HTTP tunneled

- **Off-box Advanced Data Security**
  - Deep content inspection: Structured and unstructured data matching
  - Performance optimized: Works in tandem with accelerated on-box policies
Web Security Architecture
Cisco IronPort Web Security Appliance

- L4 Traffic Monitor
- URL Filters
- CISCO IRONPORT ASYNCOS WEB PLATFORM
- Web Reputation Filters
- Anti-Malware System
Cisco IronPort Web Security Manager

Single View of Policies for the Entire Organization

- Block FTP
- Allow Media files
- Block all FTP sites
- Allow all FTP sites
- Block all malware
- Block all executables
- Block all protocols
- Monitor all traffic
- Allow all applications
- Allow Skype
- Allow all URL categories

Group by LDAP, Active Directory, Network

- Marketing
- Sales
- IT
Delegated Administration
Flexibility to Support Organizational Requirements

- Assign administrators for groups of users, appliances, subnets, or destinations
- Fine-grained, role-based access control

Global administrator defines roles and access permissions

Policy officer sets rules for users they manage

Policies are applied by group membership

No Media
IT

No FTP
SALES

No Webmail
LEGAL
Comprehensive Reporting

- **In-depth Threat Visibility**
  - Web Traffic Overview
  - Layer 4 Traffic Monitor
  - Anti-Malware Category and Threat Details
  - Client Malware Risk & Activity Detail
  - Website Activity and Detail

- **Extensive Forensic Capabilities**
  - Investigate acceptable use violations
  - Drill down for further analysis
  - Satisfy compliance requirements

- **Detailed off-box analysis**
  - Offload extensive data crunching
  - Top N and trend reporting for malware
  - Client, Source, Malware Name and Category
Web Security Hosted Offerings

ScanSafe SaaS Web Security

ScanSafe is now part of Cisco
The leading SaaS Web security solution

- Pioneer
- Leadership position: 34.5% Market Share (IDC)
- 30Bn Web requests monthly
- Millions of users
- Customers in 100+ countries
- 100% availability
- 200 million threats blocked monthly
- Award-winning

Awards

- Security product of the year 2008

Customers

- Shell
- Disney
- Bacardi
- ICI
- Standard Chartered
- Louis Vuitton
- IKEA
- Quintiles Transnational

Partners

- Orange Business Services
- at&t
- Google
- Sprint
- Telus
- NEC