Cisco IronPort Web Security Appliance

Hrvoje Dogan
Consulting Systems Engineer, Emerging Markets East
Cisco Advanced Technologies
Cisco IronPort Secure Web Gateway
Addressing Business Challenges

- Secure Against Malware
- Web Business Challenges
- Prevent Data Breaches
- Control Web Traffic and Applications

Cisco IronPort S-Series
Cisco IronPort S-Series
A Powerful, Secure Web Gateway Solution

- Most effective defense against web-based malware
- Visibility and control for acceptable use and data loss
- High performance to ensure best end-user experience
- Integrated solution offering optimum TCO

Management and Reporting

Acceptable Use Policy  Malware Defense  Data Security

AsyncOS for Web
Acceptable Use Enforcement
Visibility and Control for the Web and Web Applications

Management and Reporting

Acceptable Use Policy
Malware Defense
Data Security

AsyncOS for Web

- Enterprise-class URL filtering
- Applications and object filtering
- Integrated identity and authentication
Introducing Cisco IronPort Web Usage Controls
A Spotlight for the Dark Web

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

- Real-time Dynamic Content Analysis Engine accurately identifies over 90% of Dark Web content in commonly blocked categories
Dynamic Content Analysis (DCA) Engine
Identifies 90% of Objectionable Dark Web Content

High performance
- Optimized verdict pipeline
- Categorization verdicts in less than 10 milliseconds
- Imperceptible to user

Tuned for commonly blocked content
- Pornography and Adult
- Hate
- Gambling
- Proxy Avoidance

Analyzes content in human terms
- Advanced heuristic analysis based on content concept modeling
- Improved accuracy vs. simplistic keyword approach

Stops 50% more objectionable content*

*Source: Cisco SIO, based on data from customer production traffic
Cisco IronPort Web Usage Controls
Leading Efficacy, Rich Controls, Comprehensive Visibility

**Control**
- Per user, per group policies
- Multiple actions: block, warn, monitor
- Time-based policies
- Unlimited custom categories
- Custom end-user notifications

**Visibility**
- Easy to understand reports
- Extensive logging
- Comprehensive alerting

**Efficacy**
- 200+ countries
- 50+ languages
- 65 categories
- Less than 1 in 1 million false positives

© 2009 Cisco Systems, Inc. All rights reserved. Cisco Public
Web Application Control

- 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

Collaboration

Software as a Service

Tunneled Applications

Integrated Identity and Authentication

User-Specific Acceptable Use and Data Security Policies

- Authentication against LDAP servers
- Transparent, single sign-on (SSO) authentication against Active Directory
- Multi-realm sequencing
- Multi-domain authentication
- Guest policies
- Re-Auth and Failed Auth policies

Define Acceptable Use and Data Security Policies using Rich Identity Constructs
Malware Defense
Multiple layers for Malware and Spyware Protection

- Malware landscape
- Multi-layered malware defense
- Network layer phone-home prevention
- Reputation filtering and signature scanning
Multi-Layered Malware Defense
Protection Against Today’s Threats

- Detects malicious botnet traffic across all ports
- Blocks 70 percent of known and unknown malware traffic at connection time
- Blocks malware based on deep content analysis
Detecting Existing Client Infections
Preventing “Phone-Home” Traffic

- **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 Reputation Filters
Predictive, Real-Time Threat Prevention

200+ Parameters
- URL Blacklists
- URL Whitelists
- Dynamic IP Addresses
- Bot Networks
- URL Behavior
- Global Volume Data
- Domain Registrar Information
- Compromised Host List
- Real-Time Cloud Analysis
- Network Owners
- Known Threat URLs

Cisco Security Intelligence Operations

SensorBase Network

Security Modeling

Web Reputation Scores (WBRS)
-10 to +10
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

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

- Data security imperative and reality
- Simple on-box data security
- Advanced off-box data security
Data Security
On-box Common Sense Security

- Content metadata inspection, along with visibility and forensics
- Allow, block, log
  Based on file metadata, URL category, user and web reputation
- Multi-protocol
  HTTP(s), FTP, HTTP tunneled
## Common Sense Policies
### Simple Approach for Avoiding Web Data Breaches

<table>
<thead>
<tr>
<th>Who?</th>
<th>John Smith, Finance</th>
<th>John Smith, Finance</th>
<th>Jane Doe, Sales</th>
</tr>
</thead>
<tbody>
<tr>
<td>Where?</td>
<td>Webmail.com</td>
<td>Taxfirm.com</td>
<td>Personal-site.com, -9 Reputation score</td>
</tr>
<tr>
<td>How?</td>
<td>HTTPS (Encrypted)</td>
<td>HTTPS (Encrypted)</td>
<td>FTP</td>
</tr>
<tr>
<td>Verdict</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
</tr>
</tbody>
</table>
Non-Human Initiated Data Breaches
Critical Data Security Element

Gozi Trojan
- Installs via PDF attachment
- Encrypts itself to evade detection
- Steals data from SSL streams

Layer 4 Traffic Monitor
Block data loss from malicious phone-home activity

Trojan.PWS.ChromInject.B
- Installs via Firefox plug-in
- Captures e-banking credentials

Web Reputation Filters
Prevent data-stealing malware from entering the network

Sinowal Trojan
- Over 500,000 bank accounts compromised
- Suspected ties to Russian Business Network

Dynamic Vectoring and Streaming Engine
## Management and Reporting

Enterprise-Wide Management and Visibility

<table>
<thead>
<tr>
<th>Management and Reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acceptable Use Policy</td>
</tr>
<tr>
<td>Malware Defense</td>
</tr>
<tr>
<td>Data Security</td>
</tr>
</tbody>
</table>

### AsyncOS for Web

- Enterprise-wide management
- Roles-based administration and delegation
- Detailed URL and threat reporting
- User-level tracking and forensics
Cisco IronPort Web Security Manager
Single View of Policies for the Entire Organization

Configure granular policies based on a variety of parameters

- Block FTP uploads
- Allow media files
- Route requests to partner site
- Block executables
- Block sports sites 9am-5pm M-F
- Decrypt HTTPS connections
- Allow all URL categories
- Exempt Adobe updates from authentication
- Block all malware
Critical Acceptable Use Reports

- **Real-time insights**
  - Visibility into web usage and trends
  - Monitor acceptable use trends
  - Identify risky user behavior

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

Purpose-Built Performance

- High-performance web proxy + cache
- Multi-core scanning
- Diverse form factors
- Flexible deployments
Right-Sized Hardware Platforms
Remote Office and Back Office (ROBO) to Enterprise

- Multiple network integration options (transparent L4 redirection options, PAC file, WPAD, WCCP)
- Built-in system redundancy – RAID 10, dual power supplies
- High availability – WCCP, DNS, L4
- Flexible network routing

<table>
<thead>
<tr>
<th>Capacity and Throughput</th>
<th>Cisco IronPort S160</th>
<th>Cisco IronPort S360</th>
<th>Cisco IronPort S660</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1,000 users</td>
<td>1,000-10,000 users</td>
<td>10,000-30,000 users</td>
<td></td>
</tr>
</tbody>
</table>

Market Segment

- ROBO
- Regional HQ / Mid-Market
- Corporate HQ