Cisco IronPort E-mail Security Appliance

Deep dive - Hrvoje Dogan
Cisco IronPort Consolidates the Network Perimeter
For Security, Reliability and Lower Maintenance

Before IronPort

Internet

Firewall

Encryption Platform
MTA

Anti-Spam

Anti-Virus

Policy Enforcement

Mail Routing

Groupware

Users

After IronPort

Internet

Firewall

IronPort Email Security Appliance

DLP Policy Manager

DLP Scanner

Anti-Spam

Anti-Virus

Policy Enforcement

Mail Routing

Groupware

Users
Email Security Architecture
Inbound Security, Outbound Control

INBOUND SECURITY

Spam Defense

Virus Defense

CISCO IRONPORT ASYNCS™ EMAIL PLATFORM

OUTBOUND CONTROL

Data Loss Prevention

Secure Messaging
Processing the Email (Work Queue)

- **REPUTATION FILTERS**
- **MESSAGE FILTERS**
- **ANTI-SPAM**
- **ANTI-VIRUS**
- **CONTENT FILTERS**
- **VIRUS OUTBREAK FILTERS**

ASYNCOS EMAIL PLATFORM
Relationship Between Listeners, IP Interfaces, and Ethernet Interfaces

- **Listener**: An SMTP server awaiting connections from SMTP clients, typically on TCP port 25.
- **IP Interface**: The IP address binding of an IP address to a Physical Interface, VLAN, or Aggregated Link Pair.
- **VLAN**
- **Physical Ethernet Interface**
- **Data 1**
- **Data 2**

- **IronPort supports multiple interfaces and multiple listeners**

- **SMTP clients connect to the listener to send mail.**

- **A listener is an SMTP server awaiting connections from SMTP clients, typically on TCP port 25.**
Expanded Email Pipeline

Host Access Table (HAT)
- Default Domain
- Domain Map
- Recipient Access Table (RAT)
- Alias Tables
- LDAP Recipient Acceptance (SMTP-time)
- DKIM Verification
- SPF/SIDF Verification

Virtual Gateways
- Delivery Limits
- Received: Header
- Domain-based Limits
- Domain-based Routing
- Global Unsubscribe
- DKIM Signing
- Bounce Profiles

SMTP Server
- Work Queue
- SMTP client
- MTA
- Internet
- Accept Mail
- SMTP Receive
- Process Mail
- SMTP Delivery
- Exchange Server
- Deliver Mail

Per-Policy Scanning
- Anti-Spam
- Anti-Virus
- Content Filters
- Virus Outbreak Filters
Processing the Email (Work Queue)

ASYNCOS EMAIL PLATFORM