Security Architecture

Haider Pasha, CISSP
SSEM, Emerging Central
Architectural Plays

hpasha@cisco.com
Traditional Corporate Border
Mobility and Collaboration Is Dissolving the Internet Border
Cloud Computing Is Dissolving the Data Center Border
Customers Want Business Without Borders
Cisco Security Architecture For Enterprise (SAFE)

Security Reference Architecture
Free Technical Design and Implementation Guide

- Collaboration between security and network devices
- Uses network intelligence
- Fully tested and validated
- Speeds implementation
- Modular design
- Unifies security policy
SAFE Strategy

Security Solutions
- PCI
- DLP
- Threat Control

Security Devices
- VPNs
- Firewall
- Admission Control
- Monitoring
- Email Filtering
- Intrusion Prevention

Network Devices
- Routers
- Servers
- Switches

Visibility
- Identify
- Harden
- Isolate

Control
- Monitor
- Correlate
- Enforce

Secured Mobility, Unified Communications, Network Virtualization

Network Foundation Protection
SAFE Security Architecture Modules

- Management
- WAN Edge
- Branch
- Partner
- Teleworker
- SensorBase
- LAN/Campus
- Core
- Internet Edge
- Internet
- Data Center
- E-Commerce
- Extranet
Securing the LAN
Campus/LAN

- Network Access Control
- Enhanced Availability and Resiliency
- Secure Unified Communications
- Secure Unified Wireless Network
- Endpoint Security

- Catalyst Integrated Security Features
- Threat Detection and Mitigation
- Network Foundation Protection
- Edge Protection
SAFE Threat Response

<table>
<thead>
<tr>
<th>• Service Disruption</th>
<th>• Unauthorized Access</th>
<th>• Data Leakage</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Data Disclosure and Modification</td>
<td>• Network Abuse</td>
<td>• Identity Theft and Fraud</td>
</tr>
</tbody>
</table>

### Increasing Visibility for the LAN

<table>
<thead>
<tr>
<th>Identify</th>
<th>Monitor</th>
<th>Correlate</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN/port Authentication</td>
<td>Intrusion Detection</td>
<td>Event Analysis and Correlation</td>
</tr>
<tr>
<td>User Authentication</td>
<td>Network Management</td>
<td></td>
</tr>
<tr>
<td>Firewall Deep Packet Inspection</td>
<td>Event Monitoring</td>
<td></td>
</tr>
<tr>
<td>Traffic Classification</td>
<td>Network Telemetry</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Syslog</td>
<td></td>
</tr>
</tbody>
</table>

### Increasing Control for the LAN

<table>
<thead>
<tr>
<th>Harden</th>
<th>Isolate</th>
<th>Enforce</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Foundation Protection</td>
<td>VLANs</td>
<td>Stateful Firewall Access Control</td>
</tr>
<tr>
<td>OS Hardening</td>
<td>Network Access Control</td>
<td>ACLs, uRPF, Antispoofing</td>
</tr>
<tr>
<td>CISF</td>
<td>IPS</td>
<td>DHCP Snooping</td>
</tr>
<tr>
<td>Endpoint Security</td>
<td></td>
<td>Port Security</td>
</tr>
<tr>
<td>Link and System Redundancy</td>
<td>Firewall Access Control</td>
<td>Intrusion Prevention</td>
</tr>
<tr>
<td></td>
<td></td>
<td>QoS Enforcement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Network Access Control</td>
</tr>
</tbody>
</table>
Protecting the Network Devices
Secure Device Access - Protecting Device Access

- **In-band, in the Clear (not recommended)**
  - Telnet, HTTP, FTP
  - TFTP, SNMPv2c

- **In-band, Secure (recommended)**
  - SSH, SSL, IPSec,
  - SNMPv3, SFTP

1. **Out-of-band management, (most secure)**
   - Dedicated interfaces & Network
   - Logically separate (VLAN, VRF)
   - Strongest security
Protecting the Network Devices
Device Resiliency & Survivability

- Disable Unnecessary Services
  - Identify open ports
  - Disable unneeded open ports
  - Disable CDP on interfaces where it may pose a risk (e.g. data-only user ports in the campus)
  - Ensure directed broadcasts are disabled on all interfaces
  - Disable MOP, IP redirects, and proxy ARP on access lines

- Implement Redundancy
  - Backup and redundant interfaces
  - Redundant processors and modules
  - Active-standby, active-active failover
  - Topological redundancy
1. A device can be trusted if it correctly classifies packets
2. For scalability, classification should be done as close to the edge as possible
3. The outermost trusted devices represent the Trust Boundary
4. 1 and 2 are optimal, 3 is acceptable (if access switch cannot perform classification)
Protecting the Control Plane
Control Plane Policing - Incoming Traffic

1. Hardware-based mechanisms
2. Rate limit CPU bound traffic
3. Protect from DoS attacks
4. Control Plane Policing ensures routing stability, reachability, & packet delivery
5. Filters and rate limits traffic headed to Control Plane
Monitoring and Telemetry
NetFlow

NetFlow’s 7 Key Fields

1. Inspect a packet’s 7 key fields and identify the values.
2. If the set of key field values is unique create a flow record or cache entry.
3. When the flow terminates export the flow to the collector.

NetFlow Benefits

- Distributed traffic monitoring
- Track each data flow that appears in the network (establish baseline)
- Detect anomalies by analyzing traffic characteristics and deviations from baseline
Internal Perimeter Access Control and Security – NAC

NAC Benefits:

1. Recognizes users, their devices, and their roles in the network
2. Evaluates whether machines are compliant with security policies
3. Enforces security policies by blocking, and isolating noncompliant machines

NAC Appliance Components

1. NAS
2. NAM
3. CCA
1. **Port Security** prevents MAC flooding, port access, rogue network extension, and DHCP starvation attacks.

2. **DHCP Snooping** prevents Rogue DHCP Server attacks and DHCP starvation attacks.

3. **Dynamic ARP Inspection** used with DHCP snooping to prevent ARP Spoofing Attacks & MiTM attacks.

4. **IP Source Guard** uses DHCP snooping table to mitigate IP Spoofing, impersonation attacks & unauthorized access.
Distributed Security
Infrastructure Protection & Monitoring

1. QoS Trust Boundary
2. Scavenger Class
3. Secure Management
4. NBAR
5. NetFlow
6. Control Plane Policing
7. Network Time Protocol
8. ACS
9. Cisco MARS
10. Syslog
Securing the Internet Edge
## Enterprise Internet Edge Service Breakdown

<table>
<thead>
<tr>
<th>Segment</th>
<th>Description</th>
</tr>
</thead>
</table>
| **DMZ - Network Services**                   | • Public facing services  
| Application Segment                          | • FTP, DNS, NTP etc.                                                       |
| **Corporate Internet Access**                | • Internet access for campus and branch users  
|                                             | • Web browsing, email & other common internet services, web and email security |
| **Firewall Based Teleworker**                | • Teleworker access to corporate resources  
|                                             | • Internet access via headquarters firewall  
|                                             | • Basic IP telephony service                                                   |
| **Branch Office WAN Backup**                 | • Internet backup for branches  
|                                             | • Access to corporate resources  
|                                             | • Web browsing, email & other common internet services                        |
Firewall Design Considerations

• Firewall Security Design Considerations
  – Firewall rules to implement network security
  – Integrating Email and Web Security Appliance with firewall
  – Configuring and implementing Infrastructure Security
  – Implementing and designing a secure public facing DMZ
  – Enabling features for optimum monitoring and management
Firewall Design

Internet

Web Traffic

Web Security Appliance

Corporate Network

Email Traffic

Email Security Appliance

Email Server

Corporate User

Public User

Remote User

Email Traffic

Web Traffic
IPS at the Internet Edge

1. FW in active/standby stateful FO
2. IPS selection based on STP
3. Requires STP tuning
4. Required bandwidth satisfied with single IPS and FW
Remote Access

- **Client-based SSL or IPSec VPN**
- **Clientless SSL VPN**
- **Mobile Workers**
  - Easy access to corporate network resources
- **Clientless SSL VPN**
- **Roamers**
  - Seamless access to applications from unmanaged endpoints
- **Partners / Consultants**
  - Controlled access to specific resources and applications
- **Day Extenders / Home Office**
  - Day extenders and mobile employees require consistent LAN-like, full-network access, to corporate resources and applications
- **ASA 5500**
Web Appliance (IronPort example)

Consolidated Web Gateway

Consolidated Functionality

Lower TCO

Higher Accuracy

IronPort Web Security Appliance
Securing the Data Center
Data Center Today: End-to-End Architecture

Enterprise and DC Edge
- SaaS Gateway in WSA
  - Access Control for Software as a Service Apps
- Firewall
  - Coarse Inbound Filtering

Security Services Layer
- Firewall
  - Enforce Per-zone segmentation of servers
  - Virtual Contexts enable scale
- IPS
  - Threat mitigation and Hypervisor protections

Secure Server Access Layer
- Network Segmentation
  - Per zone, enforced in Services Layer
- Virtual Access Layer Visibility
  - Flow visibility in the vSwitch
- Layer 2 Security
  - Consistent protections in virtual and physical switch

Operations
- CSM
Secure Borderless Data Center: Tomorrow’s Architecture

Cloud Services Security Layer
Enterprise- or Cloud-Provided
- Security for applications in the Cloud

Cloud Edge
Protecting the Cloud Provider Network

Enterprise and Data Center Edge
SaaS Gateway - In WSA
Firewall—Coarse Filtering

Security Services Layer
Firewall and IPS
- Identity-based policies
- Service chaining connects physical to virtual

Secure Virtual Access Layer
Virtual Layer 2 through 7 Security
- Nexus 1000v and virtual firewall platform
Real World Customer Example

**DATA CENTER MODULE**

- Layer 3 Switches in High Availability Mode
- Firewall Services Module (FWSM) to protect against Layer 2 to Layer 7 attacks
- FWSM set in Virtual Firewall Mode. VFW1 to protect Management Servers and VFW2 to protect Data Center Servers
- Network Intrusion Detection/Prevention for Monitoring
- Application Control Engine (ACE) used for Load Balancing, SSL Offloading, and Layer 7 Deep inspection
- ACE Module to be used for all Front-End Web and Application server SSL Offloading and Load Balancing (after Layer 7 Firewall)
- Traffic flow moves from Yellow, to Blue, to Orange VLANs
- Private VLAN design to be implemented within each Server farm to segment against DOS/DDOS and Network attacks.
- Cisco Security Agent to be used on each server to protect against Day Zero attacks like Worms/viruses and DOS/DDOS attacks.
- NAC Appliance Manager for network wide policy enforcement
- Cisco Security Manager to manage security devices
- Cisco Security MARS for event correlation, Dynamic Threat Mitigation, and Incident Logging
- Cisco Call Manager/Unity for Voice Services
- Cisco Access Control Server for AAA and TACACS+ services
- FCIP Server backup with Disaster Recovery and Backup Site
- DHCP Snooping, IP Source Guard, Dynamic ARP Inspection, Port Security & Advanced Security via ACL
- Catalyst Rate Limiting for Blasting Worm Protection/Remediation
- Optimized Routing Protocols
- Multicast Subsecond Convergence
- First Hop Redundancy Protocols
- Spanning Tree, EtherChannel/GigEChannel with Core switches in Campus Module
- Supervisor/Power Supply Redundancy Etc.
- HSRP for redundant gateway service
- Path Diversity Documentation
- Layer 3 Switching utilizing IGP
- Load balancing & Fast convergence
- Provide first-hop redundancy
- Protects the Core from High Density Peering
- Aggregates the Access Layer elements
- Policy Enforcement QoS, ToS, IP Precedence
- Efficient handling of multicastrs
- Network Trust or Policy Boundary
- Dual active links to Core switches in Campus Module
- Wire-Rate Application-Aware using ACE and FWSM
- IGS-Based Intelligent Network Services in Supervisor
- Traffic Detection/Classification using NETFLOW
- IP Multicast Support
- Admission control & Traffic Policing
- Advanced Security via Access Control Lists
- Load Balancing & Fast convergence
- Scalable High-Speed services
- No unnecessary features
- 10 Gigabit Scalability
- Normal Operations: ~20°C (68° F)

**CAMPUS MODULE**

**INTERNET MODULE**
SAFE Resources

Cisco SAFE and Design Guide:
http://www.cisco.com/go/safe

Cisco Design Zone:
http://www.cisco.com/go/cvd

Cisco Security Lifecycle Services:
http://www.cisco.com/go/services/security

Cisco’s Security Products:
http://www.cisco.com/go/security