Cisco Self Defending Network

Louis Senecal

November 2007
Why Cisco?
We Are Committed to Security

- Product and Technology Innovation
  - $500M in Security R&D Investment
  - 1500 security-focused engineers
  - Eight acquisitions added to our solution portfolio in last two years
  - 64+ NAC partners worked collaboratively with us to deliver an unprecedented security vision

- Responsible Leadership
  - NIAC Vulnerability Framework Committee
  - Critical Infrastructure Assurance Group
  - PSIRT—responsible disclosure
  - MySDN.com—intelligence and best practices sharing

“Because the network is a strategic customer asset, the protection of its business-critical applications and resources is a top priority.”

John Chambers, CEO, Cisco Systems®
Security Acquisitions

2004, DDOS Protection
2004, SSL VPN Client
2003, HIPS
2002, CTR (Technology)
2001, VPN (Technology)
2000, VPN (Enterprise)
2000, VPN (SP)
1998, IDS
1995, PIX

2004, NAC addition
2004, Event Correlation MARS
2005, Customer Advocacy
2005, VPN Technology
2005, Application-Acceleration and Security
2006
2006
2007, Messaging and Web Security Appliance
2007, XML Firewall
# Security Product Portfolio

<table>
<thead>
<tr>
<th>Integrated Services Router</th>
<th>800</th>
<th>1300</th>
<th>2800</th>
<th>3800</th>
<th>7000</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA Security appliance</td>
<td>5505</td>
<td>5510</td>
<td>5520</td>
<td>5540</td>
<td>5550</td>
</tr>
<tr>
<td>Intrusion Prevention System (IPS) Appliances</td>
<td>4215</td>
<td>4240</td>
<td>4255</td>
<td>4260</td>
<td>4270</td>
</tr>
<tr>
<td>Email and WEB Security Appliances</td>
<td>Ironport C-Series</td>
<td>Ironport S-Series</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anomaly Detection and Mitigation Appliances</td>
<td>XT 5600</td>
<td>XT 5650</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Catalyst® 6500 Series Service Modules and Data Center Security</td>
<td>Firewall</td>
<td>VPN</td>
<td>IPS</td>
<td>Anomaly Guard, Detector</td>
<td>ACE</td>
</tr>
<tr>
<td>Endpoint Protection</td>
<td>Security Agent</td>
<td>NAC Appliance: Clean Access</td>
<td>CSACS &amp; Meetinghouse</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Management</td>
<td>CSM</td>
<td>MARS</td>
<td>Device Manager</td>
<td>Network Compliance Manager</td>
<td></td>
</tr>
</tbody>
</table>
Cisco Self-Defending Network

Identify, Prevent and Adapt to Threats

INTEGRATED SECURITY
• Threat Defense
• Secure Connectivity
• Trust and Identity

INDUSTRY COLLABORATION
• Network Admission Control (NAC) Program
• Collaboration with antivirus vendors

SYSTEM LEVEL SOLUTION
• Dynamically identify, prevent and respond to threats
• Security-aware infrastructure

Continuous Risk Assessment & Proactive Regulatory Compliance
**SDN Architectural Philosophy**

- Technologies must span network from end-to-end including endpoints
  - Different elements have a larger or smaller role in specific locations
- Communication among devices is key to increasing contextual awareness of security entities
  - Host to network communication is critical step
- Support existing standards where mature (IPsec) and innovate where required (NAC)
- Defense-in-depth is key, each threat type needs more than one point of mitigation

- **Goal is a network security architecture greater than the sum of its parts**
SDN = Self-Defending Network – “The Ability for the **Network** to Identify, Adapt & Respond to Threats”

3 Pillars of SDN:
- Integrated Security
- Collaborative Security
- Adaptive Security

**Goal:** Stop Bad Stuff.

3 Requirements:
1. Transparency
2. Accuracy
3. Systems Approach
Properties of a Self-Defending Network

- **Network Availability**: remain active when under attack
- **Ubiquitous Access**: provide secure access from any location
- **Admission Control**: authenticate all users, devices, and their posture
- **Application Intelligence**: extend application visibility controls into the network
- **Day-Zero Protection**: ensure endpoints are immune to new threats
- **Infection Containment**: rapidly identify & contain virulent attacks
Network Availability

- **Traditional issue**: attacks consume bandwidth, endpoint, and control plane resources

- **SDN solution**: use anomaly guards, QoS, dynamic NIPS and firewall controls and CSA to protect these resources
Infection Containment
Cisco DDoS Solution

1. Detect
3. Divert Only Target’s Traffic
4. Identify and Filter the Malicious
5. Forward the Legitimate Traffic Destined to the Target
6. Non-Targeted Traffic Flows Freely

Protected Zone 1: Web
Protected Zone 2: Name Servers
Protected Zone 3: E-Commerce Application

BGP Announcement
Cisco Detector XT
Cisco Guard XT
Ubiquitous Access

- **Traditional issue**: access is arbitrarily open or restrictive

- **SDN Solution**: use authentication, privacy, and isolation facilities to provide secure access for any device from any location

![Diagram showing network components and connections](image-url)
Enterprise Class Teleworker

Raleigh Office

VPN Tunnel (V3PN)

Cisco Corporate Network

Internet

VolP GW

PSTN

Louis Home Office

Ottawa Office

Legacy PBX

Fax

Enterprise Class Teleworker

Raleigh Office

VPN Tunnel (V3PN)

Cisco Corporate Network

Internet

VolP GW

PSTN

Louis Home Office

Ottawa Office

Legacy PBX

Fax
## Network Admission Control

### THE GOAL

1. **End user attempts to access a Web page or uses an optional client**
   - Network access is blocked until wired or wireless end user provides login information.

2. **User is redirected to a login page**
   - Clean Access validates username and password, also performs device and network scans to assess vulnerabilities on the device.

3a. **Device is noncompliant or login is incorrect**
   - User is denied access and assigned to a quarantine role with access to online remediation resources.

3b. **Device is “clean”**
   - Machine gets on “certified devices list” and is granted access to network.
Application Intelligence

- **Traditional issue**: difficult to obtain and control application communication flows in a network

- **SDN Solution**: associates packets to applications, provides control mechanisms to enforce security policies

![Diagram of network traffic and application intelligence](image)
Day-Zero Protection

- **Traditional issue**: vulnerable to day-zero attacks, often resource intensive patching effort
- **SDN Solution**: assets protected against new and unknown attacks via behavioral-based technology
Day Zero Protection

- Cisco defines Host-Based Intrusion Prevention as the ability to stop day zero malicious code without reconfiguration or update.

- CSA has the industry’s best record of stopping Zero Day exploits, worms, and viruses over past 4 years:
  - 2001 – Code Red, Nimda (all 5 exploits), Pentagone (Gonner)
  - 2002 – Sircam, Debploit, SQL Snake, Bugbear,
  - 2003 – SQL Slammer, So Big, Blaster/Welchia, Fizzer
  - 2004 – MyDoom, Bagle, Sasser, JPEG browser exploit (MS04-028), RPC-DCOM exploit (MS03-039), Buffer Overflow in Workstation service (MS03-049)
  - 2005 – Internet Explorer Command Execution Vulnerability

- No reconfiguration of the CSA default configuration, or update to the CSA binaries were required
Infection Containment

- **Traditional issue:** isolating and dampening effects of outbreaks is a difficult, manual, time and resource intensive process
- **SDN Solution:** rapid visibility of infected systems, system-wide isolation and response controls