Security for Small Medium Businesses

Tore Olav Amundsen
Systems Engineer
Evolution of Threats

- **Consequence**
  - **Mass-attack**
  - **Targeted attack**

- **Testing the Waters:** Simple penetration & virus
- **Fame:** Virus & malicious code
- **Fortune:** Adware
- **Financial:** Theft and other criminal activity

Timeline:
- 1990
- 1995
- 2000
- 2005
- What's next?

Image: Wanted poster.
Self-Defending Network Defined

Efficient security management, control, and response

Advanced technologies and security services to
- Mitigate the effects of outbreaks
- Protect critical assets
- Ensure privacy

Security as an integral, fundamental network feature

Operational Control and Policy Management

Threat Control and Containment

Confidential Communications

Secure Transactions
Network Security Checklist

Which of the following tools do we have in place?

- Firewall
- Virtual Private Networking (VPN)
- Intrusion prevention (IPS)
- Virus protection
- Secured wireless network (WLAN)
- Anomaly detection
- Policy & Identity management
- Compliance validation
Cisco ASA 5500 Series
Adaptive Security Appliances
Cisco ASA 5500 Adaptive Security Appliances

Provides Converged Threat Defense, Flexible Secure Connectivity, Minimized Operation Costs, and Unique Adaptive Design to Combat Future Threats

**Market-Leading Firewall Services**
- Integrates and extends the #1 deployed firewall technology from Cisco PIX Security Appliances
- Built upon the experience of over one million PIX deployed worldwide and 10+ years of innovation

**Market-Leading IPS Services**
- Integrates and extends the #1 deployed IPS and IDS technology from the Cisco IPS 4200 Series
- Provides comprehensive security from directed attacks and many other threats

**Market-Leading VPN Services**
- Integrates and extends the #1 deployed remote access VPN technology from Cisco VPN 3000 Concentrators and Cisco PIX Security Appliances, offering both SSL and IPsec VPN services

**Market-Leading Content Security**
- Integrates and extends the #1 deployed gateway content security technology to protect from viruses, spyware, spam, phishing, and employee productivity impacting websites

**Market-Leading Secure Unified Communications**
- Comprehensive access control, threat protection, network policies, service protection and voice/video confidentiality for real-time Unified Communications traffic
Cisco ASA 5500 Adaptive Security Appliances

Provides Converged Threat Defense, Flexible Secure Connectivity, Minimized Operation Costs, and Unique Adaptive Design to Combat Future Threats

Market-Leading Firewall Services
- Integrates and extends the #1 deployed firewall technology from Cisco PIX Security Appliances
- Built upon the experience of over one million PIX deployed worldwide and 10+ years of innovation

Market-Leading IPS Services
- Integrates and extends the #1 deployed IPS and IDS technology from the Cisco IPS 4200 Series
- Provides comprehensive security from directed attacks and many other threats

Optional Module for:
- ASA 5510, 5520, 5540

Market-Leading Content Security
- Integrates and extends the #1 deployed gateway content security technology to protect from viruses, spyware, spam, phishing, and employee productivity impacting websites

Optional feature license for SSL VPN

- Integrates and extends the #1 deployed remote access VPN technology from Cisco VPN 3000 Security Appliances, offering both SSL and IPsec VPN services

- Integrates and extends the #1 deployed firewall technology from Cisco PIX Security Appliances
- Built upon the experience of over one million PIX deployed worldwide and 10+ years of innovation

Optional Module for:
- ASA 5510, 5520, 5540

Market-Leading Secure Unified Communications
- Comprehensive access control, threat protection, network policies, service protection and voice/video confidentiality for real-time Unified Communications traffic
Cisco ASA 5500 Series Platforms
Cisco ASA 5500 Series Adaptive Security Appliances
Solutions Ranging from Desktop to Data Center
Cisco ASA 5500 Series
Security Services Overview
Cisco ASA 5500 Series: Breadth and Depth
Industry First Scalable, Multi-Function, Feature Rich Appliance

- Multi-layer packet and traffic analysis
- Advanced application and protocol inspection services
- Network application controls
- Advanced VoIP/multimedia security
- Real-time protection from application and OS level attacks
- Network-based worm and virus mitigation
- Spyware, adware, malware detection and control
- On-box event correlation and proactive response
- Flexible user and network based access control services
- Stateful packet inspection
- Integration with popular authentication sources including Microsoft Active Directory, LDAP, Kerberos, and RSA SecurID
- Threat protected SSL and IPSec VPN services
- Zero-touch, automatically updateable IPSec remote access
- Flexible clientless and full tunneling client SSL VPN services
- QoS/routing-enabled site-to-site VPN
- Low latency
- Diverse topologies
- Multicast support
- Services virtualization
- Network segmentation & partitioning
- Routing, resiliency, load-balancing
Application Inspection & Control Engines
Provide Control over Application Usage & Network Access

- Application and protocol-aware inspection services provide strong application-layer security and detailed policy controls
- Perform conformance checking, state tracking, security checks, NAT/PAT, dynamic port allocation, and offer a wide range of controls for businesses to set application-layer policies

<table>
<thead>
<tr>
<th>Unified Communications</th>
<th>Database/OS Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP</td>
<td>ILS/LDAP</td>
</tr>
<tr>
<td>SCCP (Skinny)</td>
<td>Oracle/SQL*Net (V1/V2)</td>
</tr>
<tr>
<td>H.323 v1–4</td>
<td>Microsoft RPC/DCE RPC</td>
</tr>
<tr>
<td>GTP (3G Mobile Wireless)</td>
<td>Microsoft Networking</td>
</tr>
<tr>
<td>MGCP</td>
<td>NFS</td>
</tr>
<tr>
<td>TRP/RTCP/RTSP</td>
<td>RSH</td>
</tr>
<tr>
<td>TAPI/JTAPI</td>
<td>SunRPC/NIS+</td>
</tr>
<tr>
<td></td>
<td>X Windows (XDMCP)</td>
</tr>
</tbody>
</table>

| Over 30 Engines as of sw 8.0 |
| Core Internet Protocols |

<table>
<thead>
<tr>
<th>HTTP</th>
<th>FTP</th>
<th>TFTP</th>
<th>SMTP/ESMTP</th>
<th>DNS/EDNS</th>
<th>ICMP</th>
<th>TCP</th>
<th>UDP</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Specific Applications</th>
<th>Security Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows Messenger</td>
<td>IKE</td>
</tr>
<tr>
<td>Microsoft NetMeeting</td>
<td>IPSec</td>
</tr>
<tr>
<td>Real Player</td>
<td>PPTP</td>
</tr>
<tr>
<td>Cisco IP Phones</td>
<td></td>
</tr>
<tr>
<td>Cisco Softphones</td>
<td></td>
</tr>
</tbody>
</table>
Secure Remote Access (Virtual Private Network)
Cisco ASA 5500 Series
Setting the Standard in **Secure** Remote Access VPN’s

- Integrated SSL VPN, IPSec Remote Access and IPSec Site-2-Site VPN solution
- Self-Defending VPN leverages on-board endpoint and network security to guard the VPN threat vector
- Integrated load-balancing enables multi-chassis scaling without expensive external load-balancers
- Stateful failover features for high availability
- Easily integrates into the network – VLANs, QoS, OSFP and EIGRP routing
- Simple and cost-effective pricing – SSL VPN / WebVPN functionality in a single feature license
Remote Access Using IPSec VPN
ASA 5500 Remote Access IPSec VPN

- All ASA 5500 Series models have IPSec VPN support included
- Clients supported
  - Cisco VPN Client 4.x and higher
  - Microsoft Windows L2TP over IPSec using Windows 2000 & XP L2TP Client
- Client Authentication
  - Username & Password, Digital Certificate or both
  - Local user database, RADIUS, TACACS+, NT Domain, Kerberos, LDAP, HTTP
  - Form and RSA SecurID (SDI)
- IKE Authentication: Pre-shared key, Identity Certificate, Mutual Group Authentication
- IPSec Encryption: DES, 3DES, AES-128 and AES-256
- Supported CA Servers
  - Verisign, Entrust, Baltimore, MS Windows, Cisco IOS CA Server and ASA 5500 version 8.0 embedded CA Server
- High Availability
  - VPN Load Balancing across multiple ASA 5500 in a cluster
  - Active / Standby Failover
Remote Access Using SSL VPN

Clientless
Thin Client
Full Tunnel
ASA 5500 Remote Access SSL VPN

- All ASA 5500 Series models support SSL VPN as a licensed option.
  VPN Edition Bundles include SSL VPN License.
  License options for 10, 25, 50, 100, 250 peers and more are available.

- Clients supported:
  - Clientless aka. WebVPN
  - Thin Client
  - Cisco AnyConnect 2.0 (aka. Full Tunnel SSL VPN Client)

- Client Authentication:
  - Username & Password, Digital Certificate, or both.
  - Local user database, RADIUS, TACACS+, NT Domain, Kerberos, LDAP, HTTP, Form and RSA SecurID (SDI)

- Encryption: SSL (TLS) up to and including AES.

- Supported CA Servers:
  - Verisign, Entrust, Baltimore, MS Windows, Cisco IOS CA Server, and ASA 5500 version 8.0 embedded CA Server.

- High Availability:
  - VPN Load Balancing across multiple ASA 5500 using AnyConnect Client.
  - Active / Standby Failover.
Remote Access Using SSL VPN

**Clientless**
Thin Client
Full Tunnel
SSL VPN Clientless Login

[Image of SSL VPN Clientless Login interface with a login page requiring username and password]
SSL VPN Clientless Portal
SSL VPN Clientless

- Uses standard browser
- Concentrator proxies HTTP(S) over SSL connection
- Limited to web pages
  - HTML pages
  - Web-based (webified) applications
- For application translation, VPN appliance “webifies” application
  - Translates protocol to HTTP
  - Delivers HTML look-and-feel
  - Expands use to some non-web applications
  - CIFS (NT and Active Directory file sharing)
SSL VPN Clientless Application Support
Clientless SSL VPN: Client/Server Plug-ins

The VNC plugin allows access to the corporate VNC servers, and Mac OS X shared desktops from any Sun Java 1.4+ equipped browser.

The format of the URL is:
```
vnc://[server[:port]/]/{parameters}
```

TightVNC Java viewer supports a number of parameters allowing you to customize its behaviour. Most parameter names carry settings available from the Options frame in the Java viewer. Both parameter names and their values are case-insensitive, with one exception for the "PASSWORD" parameter. Here is the full list of parameters supported in TightVNC Java viewer:

- "HOST" (no GUI equivalent): Value: host name or IP address of the VNC server. Default: in applet mode, the host from which the applet was loaded. This parameter tells the viewer which server to connect to. Normally, it's not needed, because default Java security policy allow connections from applets to the only one host anyway, and that is the host from which the applet was loaded.
- "PORT" (no GUI equivalent): Value: TCP port number on the VNC server. Default: none. This parameter is required in all cases. Note that this port is not the one used for HTTP connection from the browser, it is the port used for RFB connection. Usually, VNC servers use ports 5900 for HTTP connections, and ports 5901 for RFB connections. Thus, most likely, this parameter should be set to something like 5900, 5901 etc.
- "PASSWORD" Value: session password in plain text. Default: none, ask user DO NOT EVER USE THIS PARAMETER, unless you really know what you are doing. It’s extremely dangerous from the security point of view. When this parameter is set, the viewer won’t ever ask for a password.
- "Encoding" Values: "Auto", "Raw", "RRE", "CORRE", "Textile", "ZIP", "Tight". Default: "Auto". The preferred encoding. If the value is "Auto", then this viewer will continuously estimate average network throughput and request encodings that are appropriate for current connection speed. "Textile" is an encoding that was designed for fast networks, while "Tight" is better suited for low-bandwidth connections. From the other side, "Tight" decoder in the TightVNC Java viewer seems to be more efficient than "Textile" decoder so it may be ok for fast networks too. Other encodings are not efficient and provided for compatibility reasons.
- "Compression level" Values: Default: "1", "2", "3", "4", "5", "6", "7", "8", "9". Default: "2". Use specified compression level for "Tight" and "ZIP" encodings. Level 9 offers best compression but may be slow in terms of CPU time consumption on the server side. Use high levels with very slow network connections, and low levels when working over higher-speed networks. The "Default" value means that the server’s default compression level should be used.
- "JPEG Image quality" Values: "JPEG off", "0", "1", "2", "3", "4", "5", "6", "7", "8", "9", "10", "11", "12", "13", "14", "15", "16", "17", "18", "19", "20". Default: "0". Use the specified image quality level in "Tight" encoding. Quality level 0 denotes bad image quality but very impressive compression ratios, while level 20 offers very good image quality at lower compression ratios. If this value is "JPEG off", the.

Presentation_ID © 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential
Clientless SSL VPN: Client/Server Plug-ins

Microsoft RDP
Clientless SSL VPN: Client/Server Plug-ins

VNC

VNC connection will open in a popup window.

Please don’t close this page or go back to the portal page until you are finished with the VNC session.

Click here if you want to open another window with the portal page.
Remote Access Using SSL VPN

- Clientless
- Thin Client
- Full Tunnel
SSL VPN Full Tunnel
Cisco AnyConnect 2.0 Client

- **Next generation VPN client** available on following platforms:
  - Windows Vista 32- and 64-bit
  - Windows XP 32- and 64-bit
  - Windows 2000
  - Mac OS X 10.4 (Intel and PPC)
  - Intel-based Linux

- **Stand-alone, Web Launch, and Portal Connection Modes**

- **Start before Login (SBL)*** and DTLS support
  - *) Windows 2000 and XP only

*New as of sw 8.0!
Remote Access Using SSL VPN

Clientless

Thin Client

Full Tunnel
SSL VPN Thin Client (aka. Smart Tunnel)

- Enables specific application access without using a Full Tunnel Client
- Local Smart Tunnel “thin” client acts as proxy
  Tunnels and forwards selected application traffic
  Configured on ASA 5500
- Used with Clientless SSL VPN as a helper application
- Delivered via Java from ASA 5500 VPN appliance
- Supports Windows 2000 and XP (32-bits)
SSL VPN Thin Client (aka. Smart Tunnel)

Client Workstation

Web Browser

Java Applet WinSock2 Wrapper *)

Client Program

HTTPS Connection to VPN Appliance

VPN Appliance

Protocol Connection to Remote Server

Remote Server

*) WinSock2 TCP only
Comprehensive End Point Security
Cisco Secure Desktop
Comprehensive End Point Security

- Cisco Secure Desktop (CSD) now supports hundreds of pre-defined products, updated frequently
  - Anti-virus, anti-spyware, personal firewall, and more
- Administrators can define custom checks including running processes
- Posture policy presented visually to simplify configuration and troubleshooting (Pre-login sequence and Dynamic Access Policies)
- Four features available:
  - Host Scan (Windows)
  - Advanced Endpoint Assessment provides remediation and periodic rechecking capabilities (licensed option)
  - Cache Cleaner (Windows, Mac OS X, and Linux)
Cisco Secure Desktop
Configuring Pre-login Decision Tree

- Supported Checks
  Registry check
  File check
  Certificate check
  Windows version check
  IP address check

- Leaf Nodes
  Login denied
  Location
  Subsequence
Enhanced Remote Access Security

- Enhanced authorization using policies and group information
- Extended use of credentials
- Embedded Certificate Authority (CA)
- Virtual keyboard option
- SAML Single Sign-On (SSO) verified with RSA Access Manager (was ClearTrust)
- Group/User-to-VLAN mapping support
Content Security
(Anti-X / UTM)
Cisco Anti-X / UTM
Content Security Module in the Cisco ASA 5500

- Comprehensive content security services on a single module
- Incorporates security technology from Trend Micro’s award-winning InterScan VirusWall suite
- Seamless management and monitoring through Cisco ASDM, multi-device management with Trend TMCM
- Enables a single-box solution for all the needs of the SMB
Cisco ASA 5500 Content Security
Delivering Comprehensive Protection and Control

Threat Types
- Unauthorized Access
- Intrusions and Attacks
- Insecure Comms.
- Viruses
- Spyware
- Malware
- Phishing
- Spam
- Inappropriate URLs
- Identity Theft
- Offensive Content

NEW Anti-X Service Extensions

Protection
- Resource and Information Access Protection
- Hacker Protection
- Client Protection
- DDoS Protection
- Protected Email Communication
- Protected Web Browsing
- Protected File Exchange
- Unwanted Visitor Control
- Audit and Regulatory Assistance
- Non-work Related Web Sites
- Identity Protection

Granular Policy Controls

Comprehensive Malware Protection

Advanced Content Filtering

Integrated Message Security

Easy to Use
Content Security and Control SSM

Cisco ASA 5500 Series
Content Security and Control Module (CSC-SSM)

Platforms/Subscription Levels

<table>
<thead>
<tr>
<th>CSC-SSM-10</th>
<th>CSC-SSM-20</th>
</tr>
</thead>
<tbody>
<tr>
<td>50 User</td>
<td>500 User</td>
</tr>
<tr>
<td>100 User</td>
<td>750 User</td>
</tr>
<tr>
<td>250 User</td>
<td>1,000 User</td>
</tr>
<tr>
<td>500 User</td>
<td></td>
</tr>
</tbody>
</table>

Feature Sets

**Base Services**
- File-based Anti-Virus and malware filtering;
- Anti-Spyware

**Plus License**
- Anti-Spam,
- Content Filtering,
- Anti-Phishing,
- URL Filtering
  and Blocking
Intrusion Prevention Systems (IPS)
Cisco IPS Offers Multi-Vector Threat Identification
Delivers Broad Attack and Malware Protection

**Spyware/Adware**
- Prevents installation of malware and blocks “phone home” communications
- Frees network bandwidth and controls the transmission of confidential data

**Network Worms & Viruses**
- Stops the infection and propagation of malware
- Leverages internal development and partnership with Trend Micro

**Directed Attacks**
- Controls corporate espionage
- Stops web defacing by preventing web attacks
- Prevents zombie, backdoor, and bot placement thus stopping automated attacks (e.g., denial of service (DoS))

**Traffic Cleansing**
- Removes traffic ambiguities such as overwritten fragments, TCP segment overwrites, TTL discrepancies
- Simulates end host behavior to increase inspection accuracy
Cisco Intrusion Protection System
Cisco IOS IPS

Protect Branch PCs from Internet Worms

Move Worm Protection to the Network Edge

Protect Branch-Office Servers

1. Protect Branch PCs from Internet Worms
2. Move Worm Protection to the Network Edge
3. Protect Branch-Office Servers
Latest Improvements in Cisco IOS IPS
Cisco IOS 12.4(11)T2 and Later

- Automated signature updates
  - local TFTP or HTTP(S) server
- Risk Rating (RR) value in IPS alarms based on
  - signature severity
  - fidelity
  - target value rating
- Supports Signature Event Action Processor (SEAP)
- Signature provisioning using
  - Cisco IOS CLI
  - Cisco Secur Router Device Manager (SDM)
- Same signature format as the Cisco IPS 6.0
Cisco Intrusion Prevention System
Advanced Integration Module

Accelerated Threat Control for Cisco Integrated Services Router
- Enable Cisco intrusion prevention in the Branch
- Runs same software (Cisco IPS 6.0) as Cisco IPS series
- Hardware accelerated IPS:
  - Up to 45 Mbps on Cisco 3845
  - Dedicated CPU and DRAM to offload host CPU
- Managed via Cisco IPS Device Manager and Cisco Security Manager (CSM 3.2)
- Supported by Cisco Security MARS for event monitoring and correlation
## IPS Solutions on Cisco ISRs

<table>
<thead>
<tr>
<th>Feature</th>
<th>Cisco IOS IPS</th>
<th>Cisco IPS AIM</th>
<th>Cisco NM-CIDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dedicated CPU/DRAM for IPS</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Inline and Promiscuous Detection and Mitigation</td>
<td>Yes</td>
<td>Yes</td>
<td>No, Promiscuous Mode Only</td>
</tr>
<tr>
<td>Signature Supported</td>
<td>Superset of 2000+ Signatures, Subject to Available Memory</td>
<td>Full Set Signatures (2200+)</td>
<td>Full Set Signatures (2200+)</td>
</tr>
<tr>
<td>Automatic Signature Updates</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Day-zero Anomaly Detection</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Rate Limiting</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Cisco Security Agent and Cisco IPS Collaboration</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Meta Event Generator</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Event Notification</td>
<td>Syslog, SDEE</td>
<td>SNMP and SDEE</td>
<td>SNMP and SDEE</td>
</tr>
<tr>
<td>Device Management</td>
<td>CLI, SDM</td>
<td>IOS CLI, IDM</td>
<td>IPS CLI, IDM</td>
</tr>
<tr>
<td>System/Network Management</td>
<td>CSM</td>
<td>CSM</td>
<td>CSM</td>
</tr>
<tr>
<td>Event Monitoring and Correlation</td>
<td>IEV, CS-MARS</td>
<td>IEV, CS-MARS, On-box Meta Event Generator</td>
<td>IEV, CS-MARS, On-box Meta Event Generator</td>
</tr>
</tbody>
</table>

**NOTE:** Only One IPS Solution May Be Active in the Router.
Cisco Intrusion Prevention System Security Services Module in the ASA 5500 Series

- Comprehensive IPS services on a single module
- Incorporates and extends security technology from Cisco IPS 4200 Series
- Runs same software (Cisco IPS 6.0) as Cisco IPS 4200 series
- Managed via Cisco IPS Device Manager and Cisco ASDM
- Installs in the Service Module slot in ASA 5510, 5520 and 5540
- Enables a single-box solution
Responding to Security Events as They Occur

- Full Disclosure
- CERT
- "Back-channel"
- SANS
- BugTrack
- Other Sources

Cisco Security Intelligence Services
Responding to Security Events as They Occur
Example: Microsoft Patch Tuesday

Cisco Security Center & Event Response Page
IntelliShield Alerts for new Vulnerabilities
IPS Signature Updates
Cisco Applied Mitigation Bulletin
Cisco Response to Microsoft Bulletin Summary e-mail
Responding to Security Events as They Occur
Example: Microsoft Patch Tuesday

Cisco Security Center & Event Response Page
IntelliShield Alerts for new Vulnerabilities
IPS Signature Updates
Cisco Applied Mitigation Bulletin
Cisco Response to Microsoft Bulletin Summary e-mail
MS Tuesday Timeline – October 2007

- **MS Bulletin Published**: 10:07 PST
- **First IntelliShield Alert Published**: 11:03 PST
- **Cisco Security Center Event Response Page Goes Live**: 12:55 PST
- **CSM-managed sensors up-to-date with latest IPS Signatures**: 13:30 PST
- **STG Teams Notified**: 10:20 PST
- **Applied Mitigation Bulletin Published**: 12:40 PST
- **IPS Signatures Published**: 13:19 PST
- **Cisco Response to MS Bulletin E-mail**: 14:25 PST
End point Security
Cisco Security Agent (CSA) 5.2
Intercepting Operating System Calls

The Cisco Security Agent intercepts application OS calls and invokes an allow/deny response.

Interceptors monitor calls for resource access:

- File system
- Network (inbound/outbound)
- Registry
- Execution (process creation, library access, executable invocation)

“Zero Update” architecture – behavior based control means you don’t need a new signature to stop the next attack.
CSA Benefits

- **Device Security**
  - Day Zero Attack Protection
  - Defense against Targeted Attacks, Spyware
  - System Integrity Assurance + Patch Relief

- **Transaction Assurance**
  - Per-Application network Prioritization (QoS)
  - Wireless bandwidth optimization (QoS - WMM)

- **Compliance Enforcement**
  - Wireless NIC security configuration
  - Removable media control
  - Acceptable Use control
CSA + IPS Collaboration with Cisco IPS Version 6.0

- Enhanced contextual analysis of endpoint
- Ability to use CSA inputs to influence IPS actions
- Correlation of info. contained in CSA watch list
- Host Quarantining

Service Provider

OS = WindowsXP

Management Console
CSA + IPS Collaboration with Cisco IPS Version 6.0

- Enhanced contextual analysis of endpoint
- Ability to use CSA inputs to influence IPS actions
- Correlation of info. contained in CSA watch list
- Host Quarantining
CSA + IPS Collaboration with Cisco IPS Version 6.0

- Enhanced contextual analysis of endpoint
- Ability to use CSA inputs to influence IPS actions
- Correlation of info. contained in CSA watch list

- Host Quarantining

Source 10.1.10.2 initiates a port scan destined for internal servers

Port Scan from IP not in Watch List: Alarm Only

Management Console
CSA + IPS Collaboration with Cisco IPS Version 6.0

- Enhanced contextual analysis of endpoint
- Ability to use CSA inputs to influence IPS actions
- Correlation of info. contained in CSA watch list

- Host Quarantining

Watch List Source 10.1.10.1 initiates a port scan destined for internal servers

Port Scan from IP on Watch List: Drop Packet
Cisco IPS Summary

- **IPS functionality**
  - Cisco IOS IPS for ISR routers
  - Cisco AIM-IPS for ISR routers
  - Cisco IPS Services Module for ASA 5500
  - Cisco IPS 4200 Series appliances

- **Host based IPS**
  - Cisco Security Agent (CSA) 5.2

- **Cisco Services for IPS** - Comprehensive Security Services
  - Signature Updates
  - Software support
  - Application updates
Adaptive Security Device Manager - ASDM 6.0
For Administrators, Visual Management
Smart ASDM management tool reduces overhead and TCO

- **Visual management**
  - Intuitive, familiar, user-friendly interface
  - Wizards guide and simplify SSL VPN setup, even for novice users
  - Visual policy editor for setting access control policies and posture checking, including CSD
  - Expanded on-screen help

- **Easily control access**
  - Configurable user and group permissions
  - Easy to provision, secure access when and where needed
Identity & Policy Management - Cisco Secure ACS Express 5.0
Cisco Secure ACS Express 5.0

- Entry-level RADIUS and TACACS+ authentication, authorization, and accounting (AAA) server for small-medium-sized businesses (SMBs)
  - Supports up to 350 users
  - Maximum 50 AAA devices
  - Simplified GUI and policy management
- First of the next-gen ACS’
  - Native access to AD
  - Linux OS appliance
- Controls user and machine access to:
  - Wireless networks
  - Wired networks
  - Virtual private networks (VPN)
- Controls administrative access to network devices using RADIUS and TACACS+
- Hardware appliance comes preloaded with Cisco Secure ACS Express
- [http://www.cisco.com/go/acsexp](http://www.cisco.com/go/acsexp)
Cisco Secure ACS Express 5.0

Configuration Summary

**Network Resources**
- Devices: 18
- Device Groups: 8

**Users & Identity Stores**
- Internal Users: 1385
- Internal User Groups: 7
- External Databases: AD, LDAP, OTP

**Access Policies**
- RADIUS Access Services: 3
- TACACS+ Access Services: 3 Rules
- Radius Responses: 6
- Time of Days: 4

**System Administration**
- Replication: Disabled
- SNMP Agent: Disabled

**Server Information**
- Host Name: bhashik-inx
- IP Address: 171.69.74.222
- Version: 4.0
- Total Memory: 1010MB
- /root Disk: 72G Total, 30G In-Use
- /localdisk Disk: 0 Total, 0 In-Use
- Uptime: 149 days, 1:21 hours

**Server Status**
- CPU: 0%
- Mem: 31%
- Root Disk: 44%
Security Planning Tips
Security Planning Tips

- Focus on return on value rather than return on investment
- Never assume network attacks will only come from outsiders
- Don't be tempted to confront security concerns with a piecemeal approach rather than a single, unified strategy
- Work with others within your company to develop and implement security strategies, focusing on technology, training, physical site security, and more
- Find the right balance between security and usability
Q and A
Please Complete Your Session Evaluation!