Technical Update
Januar 2007

Adaptive Security Appliances
NAC Appliance

Niels Mogensen
Cisco ASA 5500 Series Adaptive Security Appliances

Niels Mogensen
Introducing Cisco Adaptive Security Appliances
Delivering Adaptive Threat Defense and VPN Solutions

Converged Adaptive Threat Defense and Flexible VPN Services
Application Security, Worm/Virus Mitigation,
Malware Protection, Threat-Protected VPN and Network Awareness

Minimize Deployment and Operations Costs
Platform Standardization, Unified Management

Technology Extensibility to Address New Threats
Purpose-Built Adaptive Identification and Mitigation Architecture Enables
Unprecedented Extensibility and Policy Control

The Cisco ASA 5500 Series
Cisco ASA 5500 Series
Convergence of Robust, Market-Proven Technologies

Market-Proven Technologies

- Firewall Technology
  - Cisco PIX
- IPS Technology
  - Cisco IPS
- Content Security
  - Trend Micro
- VPN Technology
  - Cisco VPN 3000
- Network Intelligence
  - Cisco Network Services

Adaptive Threat Defense, Secure Connectivity

- App Inspection, Use Enforcement, Web Control
  - Application Security
- Malware/Content Defense, Anomaly Detection
  - IPS & Anti-X Defenses
- Traffic/Admission Control, Proactive Response
  - Network Containment & Control
- Secure Connectivity
  - IPSec & SSL VPN
Cisco ASA 5500 Series Enterprise Editions

A Family of Tailored Packages for Location Specific Needs

- Enables standardization on the Cisco ASA 5500 Series to reduce costs in management, training, and sparing
- Superior protection by providing the right services for the right location
- Simplifies design and deployment by providing pre-packaged location-specific security solutions

Cisco ASA 5500 Firewall Edition
Cisco ASA 5500 SSL & IPSec VPN Edition
Cisco ASA 5500 IPS Edition
Cisco ASA 5500 Anti-X Edition
# Cisco ASA 5500 Series: Breadth and Depth

## Industry First Scalable, Multi-Function, Feature Rich Appliance

<table>
<thead>
<tr>
<th>Feature Category</th>
<th>Features</th>
</tr>
</thead>
</table>
| Firewall with Application Layer Security | - Multi-layer packet and traffic analysis  
- Advanced application and protocol inspection services  
- Network application controls  
- Advanced VoIP/multimedia security |
| IPS and Anti-X Defenses | - 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 |
| Access Control and Authentication | - 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 |
| SSL and IPSec Connectivity | - 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 |
| Cisco Intelligent Networking Services | - Low latency  
- Diverse topologies  
- Multicast support  
- Services virtualization  
- Network segmentation & partitioning  
- Routing, resiliency, load-balancing |
The Cisco ASA 5500 Series Modular Policy Framework allows business to adapt and extend the security services profile via Cisco-developed and partner-provide innovations delivering high current services performance and services extensibility.
Going IPS

- Event Severity: How urgent is the threat?
- Signature Fidelity: How prone to false positive?
- Attack Relevancy **: Is attack relevant to host being attacked?
- Asset Value of Target: How critical is this destination host?

RISK RATING Drives Mitigation Policy

Decision support balances attack urgency with business risk

<table>
<thead>
<tr>
<th>Event Action</th>
<th>Override</th>
<th>Enabled</th>
<th>Risk Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deny Attacker Inline</td>
<td></td>
<td>Yes/No</td>
<td>Minimum 85 - Maximum 100</td>
</tr>
</tbody>
</table>

Customizable Risk Rating Thresholds:
- 0 < RR < 35: Alarm
- 35 < RR < 85: Alarm & Log Packets
- 85 < RR < 100: Drop Packet
Accurate Prevention Technologies
Meta Event Generator Delivers Advanced Correlation

On-box correlation allows adaptation to new threats in real-time without user intervention

Links lower risk events into a high risk meta-event, triggering prevention actions

Models attack Behavior by Correlating:
- Event type
- Time span

A + B + C + D = WORM!

Event A
Event B
Event C
Event D

DROP Event D-Worm Stopped!
Content Security in the Cisco ASA 5500 Series

Introducing the
Content Security and Control
Security Services Modules

- Comprehensive Anti-X 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 mgmt with Trend TMCM
- Enables a single-box solution for all the needs of the SMB
Cisco ASA 5500 Series Anti-X Edition
Delivering Comprehensive Protection and Control

**THREAT TYPES**
- Unauthorized Access
- Intrusions & Attacks
- Insecure Comm.
- Viruses
- Spyware
- Malware
- Phishing
- Spam
- Inappropriate URLs
- Identity Theft
- Offensive Content

**NEW Anti-X Service Extensions**
- Resource & Information Access Protection
- Hacker Protection
- Client Protection
- DDoS Protection
- Protected Email Communication
- Protected Web Browsing
- Protected File Exchange
- Unwanted Visitor Control
- Audit & Regulatory Assistance
- Non-work Related Web Sites
- Identity Protection

Cisco ASA 5500 with CSC-SSM

Granular Policy Controls
Comprehensive Malware Protection
Advanced Content Filtering
Integrated Message Security
Easy to Use
Content Security and Control SSM

Product Details

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 & Blocking

Note: License Packages subject to change prior to FCS
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
Cisco ASA 5500 Series VPN Solutions
Enterprise-Class Site-to-Site VPN Capabilities

Network-aware site-to-site VPNs

QoS-Enabled VPN
Support for low latency queuing for latency-sensitive traffic such as VoIP

IPSec Stateful Failover
• Provides high performance Active-Standby failover with automatic key and SA information synchronization

Robust X.509 Certificate Support
• Manual enrollment support (PKCS 7/10)
• n-tiered X.509 certificate chaining support
• 4096-bit RSA keysizes support

OSPF Routing Over VPN
Remote Access VPN Technology Comparison
IPSec and SSL VPNs

There are 2 primary remote access VPN technologies: IPSec and SSL. SSL is the newer technology of choice, typically has lower support costs and provides better access to business partners and contractors than IPSec. SSL is growing faster than IPSec.

<table>
<thead>
<tr>
<th>IPSec VPN</th>
<th>SSL VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Widely deployed, well-proven technology</td>
<td>Extends secure network access to non-employees like contractors and temps</td>
</tr>
<tr>
<td>Operates well for extending access to employees using company-managed desktops</td>
<td>Simplifies provisioning and support for business partner access</td>
</tr>
<tr>
<td></td>
<td>Provides “anywhere” access to non-managed desktops such as Internet kiosks</td>
</tr>
<tr>
<td></td>
<td>Enables customized user access portals</td>
</tr>
<tr>
<td></td>
<td>Reduces operations costs associated with managing client software</td>
</tr>
</tbody>
</table>
Customizable Remote Application Access
Full Network Access: IPSec and SSL VPN

- Customizable access and streamlined management – comprehensive IPSec and SSL VPN solutions on one platform
- Ease of administration – dynamically downloadable SSL VPN client is centrally configured and easy to update
- Fast initiation and operation – multiple delivery methods and small download size ensures broad compatibility and rapid download

ASA 5500
Customizable Remote Application Access
Clientless Access

- Fully clientless web-based network access allows anywhere access to network resources
- Web content transformation provides excellent compatibility with web pages containing Java, ActiveX, complex HTML and JavaScript
- Multiple browser support ensures broad connection compatibility
- Uniform and efficient application delivery via fully clientless Citrix support
- Customizable user portal for ease of use and enhanced user experience
Optimizing SSL VPN Application Performance
Enhancing the End-User Experience

Optimized Application Access
Enhancing Performance of Resource-Intensive Applications like OWA and Lotus iNotes

Safe Caching
- Safe caching – head-end device and remote client cache non-security impacting information
- Improves application response times for end-users
- Improves application performance by reducing latency
- Increases performance for resource-intensive applications across SSL-VPN, such as Outlook Web Access (OWA) and Lotus iNotes

Compression
- GZIP compression support reduces bandwidth consumption
- Benefits both SSL VPN Client and Clientless modes
Endpoint Security for SSL VPN
Cisco Secure Desktop

Complete Pre-Connect Assessment:
- Location assessment – managed or unmanaged desktop?
- Security posture assessment – AV operational/up-to-date, personal firewall operational, malware present?

Comprehensive Session Protection:
- Data sandbox and encryption protects every aspect of session
- Malware detection with hooks to Microsoft free anti-spyware software

Post-Session Clean-Up:
- Encrypted partition overwrite (not just deletion) using DoD algorithm
- Cache, history and cookie overwrite
- File download and email attachment overwrite
- Auto-complete password overwrite

Works with Desktop Guest Permissions
No Admin Privileges Required
Virtualized Services and Transparent Operation 
Simplifies Deployment and Reduces Operational Costs

Scalable Security Services

- Adds support for Security Contexts (virtual firewalls) to lower operational costs
  - Enables device consolidation and segmentation
  - Supports separated policies and administration

Easy to Deploy Firewall and IPS Services

- Introduces transparent firewall capabilities for rapid deployment of security
  - Drops into existing networks without need for readdressing the network
  - Simplifies deployments of internal firewalls and security zoning – new applications
Advanced Network Integration
Maximizes Uptime and Supports Next-Gen Networks

Improved Network and Device Resiliency
- Introduces Active-Active failover for **enhanced resiliency** and asymmetric routing support
- Delivers new zero-downtime software upgrade capability for **improved uptime**

Intelligent Network Integration
- Provides **QoS traffic prioritization** for improved handling of latency sensitive traffic
- Adds IPv6 support for hybrid IPv4/IPv6 network environments
- Delivers **PIM sparse mode multicast** support for improved support for streaming data delivery services, video conferencing, and other mission-critical real-time enterprise applications
# Cisco ASA 5500 Series Product Lineup

Solutions Ranging from SOHO to Large Enterprise

## Target Market
- **SOHO and ROBO**
- **SMB and SME**
- **Enterprise**
- **Medium Enterprise**
- **Large Enterprise**

## List Price

<table>
<thead>
<tr>
<th>Model</th>
<th>SOHO and ROBO</th>
<th>SMB and SME</th>
<th>Enterprise</th>
<th>Medium Enterprise</th>
<th>Large Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco ASA 5505</strong></td>
<td>Starting at $595</td>
<td>Starting at $3,495</td>
<td>Starting at $7,995</td>
<td>Starting at $16,995</td>
<td>Starting at $19,995</td>
</tr>
<tr>
<td><strong>Cisco ASA 5510</strong></td>
<td>150 Mbps Future</td>
<td>300 Mbps</td>
<td>450 Mbps</td>
<td>650 Mbps</td>
<td>1.2 Gbps</td>
</tr>
<tr>
<td><strong>Cisco ASA 5520</strong></td>
<td>100 Mbps 25 / 25</td>
<td>170 Mbps 250 / 250</td>
<td>225 Mbps 750 / 750</td>
<td>325 Mbps 5000 / 2500</td>
<td>N/A</td>
</tr>
<tr>
<td><strong>Cisco ASA 5540</strong></td>
<td>300 Mbps</td>
<td>375 Mbps</td>
<td>450 Mbps</td>
<td>450 Mbps</td>
<td>425 Mbps</td>
</tr>
<tr>
<td><strong>Cisco ASA 5550</strong></td>
<td>425 Mbps</td>
<td>5000 / 5000</td>
<td>5000 / 5000</td>
<td>5000 / 2500</td>
<td>5000 / 5000</td>
</tr>
</tbody>
</table>

## Performance
- Max Firewall
- Max Firewall + IPS
- Max IPSec VPN
- Max IPSec / SSL VPN Peers

<table>
<thead>
<tr>
<th>Model</th>
<th>Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco ASA 5505</strong></td>
<td>10,000 / 25,000 3,000 8-port FE switch 3 / 3 (trunk) Stateless A/S (Sec Plus)</td>
</tr>
<tr>
<td><strong>Cisco ASA 5510</strong></td>
<td>50,000 / 130,000 6,000 3+1 FE / 5 FE 10 / 25 A/A &amp; A/S (Sec Plus)</td>
</tr>
<tr>
<td><strong>Cisco ASA 5520</strong></td>
<td>280,000 9,000 4 GE + 1 FE 100 A/A &amp; A/S</td>
</tr>
<tr>
<td><strong>Cisco ASA 5540</strong></td>
<td>400,000 20,000 4 GE + 1 FE 200 A/A &amp; A/S</td>
</tr>
<tr>
<td><strong>Cisco ASA 5550</strong></td>
<td>650,000 28,000 8 GE + 1 FE 200 A/A &amp; A/S</td>
</tr>
</tbody>
</table>

## Platform Capabilities
- Max Firewall ConnS
- Max Conns/Second
- Base I/O
- VLANs Supported
- HA Supported

<table>
<thead>
<tr>
<th>Model</th>
<th>Platform Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco ASA 5505</strong></td>
<td>10,000 / 25,000 3,000 8-port FE switch 3 / 3 (trunk) Stateless A/S (Sec Plus)</td>
</tr>
<tr>
<td><strong>Cisco ASA 5510</strong></td>
<td>50,000 / 130,000 6,000 3+1 FE / 5 FE 10 / 25 A/A &amp; A/S (Sec Plus)</td>
</tr>
<tr>
<td><strong>Cisco ASA 5520</strong></td>
<td>280,000 9,000 4 GE + 1 FE 100 A/A &amp; A/S</td>
</tr>
<tr>
<td><strong>Cisco ASA 5540</strong></td>
<td>400,000 20,000 4 GE + 1 FE 200 A/A &amp; A/S</td>
</tr>
<tr>
<td><strong>Cisco ASA 5550</strong></td>
<td>650,000 28,000 8 GE + 1 FE 200 A/A &amp; A/S</td>
</tr>
</tbody>
</table>

© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential
Introducing the Cisco ASA 5505
Next Generation SOHO / ROBO Security Appliance

Best-of-class Small Business, Branch Office, and Teleworker solution

Full-featured, High Performance, Market-proven Security Services, Including:

- Advanced Application Inspection and Control services
- Site-to-Site VPN / Cisco Easy VPN Server / Remote IPSec VPN Connectivity
- SSL VPN Connectivity
- Dual ISP support with object tracking and failback
- Hardware failover, PPPoE, dynamic DNS, and more!

Platform Highlights:

- Compact desktop form-factor
- Integrated VPN acceleration
- 8 x 10/100 ports with flexible port grouping
- VLANs: Home/Business/Outside
- Support for true DMZ & trunking
- Power over Ethernet (802.3af) ports for IP phones, external Wireless APs, etc.
- USB 2.0 ports for future use
- Wall and rack mountable
- Convection cooling (no fan)
Teleworker Deployment Model
Easy to Install Modern Home Networking Services

**Business VLAN**
- Secure access to both Home and Internet VLANs
- Power Over Ethernet for IP Phones and WiFi Access Points

**Internet VLAN**
- DHCP & Dynamic DNS services
- PPPoE support
- Backup ISP support (Security Plus)

**Home VLAN**
- Secure access for a wide range of applications through the Internet VLAN
- DHCP Server Services
Remote Office/SMB Deployment Model
High Performance, Resilient Security Services

Business/DMZ VLAN

Internet VLAN (Active)

- Site-to-Site IPSec VPN
- Remote Access VPN
- SSL VPN

Internet VLAN (Standby)

- Active/Standby design with Failback
- Support for DHCP, Dynamic DNS & PPPoE

Inside VLAN

- Web Server
- Email Server
- DNS Server
- VLAN Trunk
- Common Network Printer
- Power Over Ethernet WiFi Access Point
- Employee/Guest VLANs
Cisco ASA 5505 Licensing Model

- Similar to PIX 501 licensing, but with additional dimensions
- User Based Licensing
  - 10, 50, and Unlimited user licenses
- SSL VPN Licensing
  - Base includes 2 for free, 10 & 25 user upgrades available
- Security Plus License – offers many additional capabilities
  - **Increased system capacity**
    - Increases number of maximum connections (10K to 25K)
    - Increases IPSec peer count from 10 to 25
  - **Device and link-level redundancy**
    - Enables stateless Active/Standby failover
    - Enables redundant ISP support (dual ISP uplinks)
  - **Improved flexibility**
    - Enables full DMZ and 802.1q VLAN trunking support
    - Can be used with any user licensing level
Cisco ASA 5510/5520/5540/5550 Adaptive Security Appliances Product Tour

- Four 10/100/1000 Copper Gigabit Ports
- One 10/100 Out of Band Management Port*
- One Expansion Slot for Add’l Accelerated Services or I/O
- Sleek, High Performance 1 Rack Unit (RU) Design
- Diskless Architecture for High Reliability
- Single Field Upgradeable AC or DC Power Supply
- Two USB 2.0 Ports for Future Expansion (Credentials, Failover, and more)
- Compact Flash for Software, Config, and Log Storage
- Console and AUX Ports
- Five Status LEDs (Power, Status, Active, VPN, Flash)
- Diskless Architecture for High Reliability
- Single Field Upgradeable AC or DC Power Supply
Cisco Four-Port Gigabit Ethernet SSM

Product Tour

- High-Performance Module Adds More I/O Capacity
- Four Copper 10/100/1000 for Simplified Deployment
- Four SFP Gigabit Ports for Optical Connectivity
- Thumbscrews for Easy Insertion and Removal

Allows Customers to Choose Either Copper or Optical for Up to 4 Ports of Additional Connectivity

Ordering Information
Product ID: SSM-4GE=
List Price: $5,000
Cisco ASA Security Services Module (SSM)
Product Tour

- High Performance Module for Additional Services
- Diskless (Flash-Based) Design for Improved Reliability
- Gigabit Ethernet Port for Out-of-Band Management, etc.
- Thumbscrews for Easy Insertion and Removal
Cisco ASA Adaptive Security Appliances
Industry Certifications and Evaluations

- **Common Criteria**
  - In Process: EAL4+, v7.0.4 – ASA Family (FW)
  - In Process: EAL2, v5.1 – ASA SSM-10/20 (IPS)
  - In Process: EAL4, v7.2 – ASA Family (VPN)

- **FIPS 140**
  - Completed: Level 2, v7.0.4 – ASA Family

- **ICSA Firewall 4.1, Corporate Category**
  - Completed: v7.0.4 – ASA Family

- **ICSA IPSec 1.0D**
  - Completed: v7.0.4 – ASA Family

- **ICSA Anti-Virus Gateway**
  - Completed: v7.1 – ASA Family

- **ICSA Intrusion Prevention (IPS)**
  - In Process: v5.1 – ASA Family
Wide Range of Management Solutions
Provide Scalable, Cost Optimized Options for Businesses

Integrated Remote Management Capabilities Within ASA
- Configuration: Auto Update, SSH, Telnet, XML/HTTPS, and ASDM
- Real-time monitoring: Syslog, SNMP, HTTPS, and ASDM
- Software updates: Auto Update, SCP, HTTP, HTTPS, and TFTP

Cisco Security Manager (CS-Manager)
- Scalable management solution for wide range of Cisco security solutions including routers, switches, blades, and appliances
- Delivers centralized management of firewall, VPN, IPS/IDS, networking, and other services via flexible user interface
- Supports device grouping for simplified policy maintenance
- Provides role-based admin access and workflow capabilities
- Available on Windows (Linux version coming)

Cisco Monitoring and Response Solution (CS-MARS)
- Family of high performance appliances designed to provide automated analysis of security event information to help identify, manage, and counter attacks
- Supports getting events from wide range of Cisco and 3rd party solutions – and also analyzes NetFlow for additional intelligence
- Offers event correlation, visualization, rules engine, and reporting
Cisco Adaptive Security Device Manager (ASDM) v5.2
Dashboard Provides At-a-Glance View of System Status

- Dashboard provides instant status of items such as:
  - Software versions installed
  - Interface status and throughput
  - Platform uptime
  - Security Contexts
  - Real-time syslog viewer (last ten)
  - Powerful search capabilities
  - And more!
Now Available in ASDM 5.2: **New Rule Table**
Many Enhancements Coming to Primary Focus Area

- Redesigned rule table for streamlined policy creation
- Able to create objects, object-groups and rules from single UI
- Policy visualizer provides graphical view of actions
- Policy query in the rule table for advanced filtering
- "Show log" for a particular access rule in the real time log viewer
- Options to expand and display elements in an object group
- Ability to see attributes of an object or members of a group via tooltips
Now Available in ASDM 5.2: **Packet Tracer**
Live Tool to Determine Day In the Life of a Packet

**PACKET TRACING:** Enables the injection of arbitrary packets through the system to audit policy configuration and enforcement

**Benefits**
- Enables policy tuning and refining
- Enables rapid troubleshooting
- Simplifies fault isolation in complex policy environments
- First Pro-active Debugging Tool
Now Available in Cisco ASDM 5.2
Logging Enhancements

- Structured syslogs in Real time Log Viewer
- Parse all the syslogs and put into tabular structure
- Coloring of logs based on severity
- Integrated syslog guide within the Real time Log Viewer
- “Explanation” and “Recommended Action” for each syslog
- Single-Click Rule Creation from Syslog
- Ability to Show the access rule which created this Syslog

This message appears when the security appliance denies an attempt to connect to the interface service. For example, this message appears (with the service SNMP) when the security appliance receives an SNMP request from an unauthorized SNMP management station.
Cisco ASA / PIX Software v7.1 & ASDM v5.1
Syslog to ACL Correlation Features

Syslog messages now include unique hash and line number of ACL entry that created it

New buttons in ASDM Live Log Viewer allow admins to view/edit existing ACL, or create new ACL entry
Cisco Security Manager
“It Has to be Easy to Use and Flexible”

- Feature Rich front-end
- Different views for different administration preference
  - Device View
  - Topology View
  - Policy View
- Unified security service management independent of the enforcing device
  - Firewall, VPN, IPS...
- Supporting ASA, PIX, IPS Sensors, ISR’s and Catalyst Service modules
Device-Centric View

- Start with single device
- Clone and replicate
- Rapidly deploy the device settings
Policy-Centric View

- Centralized policy management
- Powerful scalability via inheritance, reuse, assignment, and sharing
Put devices on customizable maps, image backdrops
Build VPNs with right click
Launch FW rules and configure
Build maps-within-maps to scale
Mitigation and Response System (MARS)
Next Generation SIM/STM

- Leverage YOUR existing investment to build “pervasive security”
- Correlate data from across the Enterprise
  NIDS, Firewalls, Routers, Switches, CSA
  Syslog, SNMP, RDEP, SDEE, NetFlow, Endpoint event logs
- Rapidly locate and mitigate attacks

- Key Features
  Determines security incidents based on device messages, events, and “sessions”
  Incidents are topologically aware for visualization and replay
  Mitigation on L2 ports and L3 chokepoints
  Efficiently scales for real-time use across the Enterprise
Cisco Integrated Services Router Portfolio
Scalable From Small Business to Large Enterprise

Cisco® Integrated Services Routers (ISRs)

- Cisco 3800 Series ISR
  - High Density and Performance for Concurrent Services
- Cisco 2800 Series ISR
  - Embedded, Advanced Voice, Video, Data and Security Services
- Cisco 1800 Series ISR
- Cisco 800 Series ISR
  - Embedded Wireless, Security and Data

Branch Office | Small Branch | SMB | Small Office and Teleworker
Securing Complexity with Cisco Clean Access (NAC Appliance): A Technical View

Niels Mogensen
Agenda

1. Securing Complexity
2. Clean Access Product Overview
3. Clean Access Features In-Depth
4. Clean Access Technical Benefits
The Challenge of Securing Complexity

This is a story about network security.

Specifically, how you can have security without compromising productivity.

More to the point, your company may already be bristling with network defenses, but you still have one glaring vulnerability—your network users.
Productivity Causes Complexity

| WHAT SYSTEM IS IT?          | Windows, Mac or Linux
|                            | Laptop or desktop or PDA
|                            | Printer or other corporate asset |
| WHO OWNS IT?                | Company
|                            | Employee
|                            | Contractor
|                            | Guest
|                            | Unknown |
| WHERE IS IT COMING FROM?    | VPN
|                            | LAN
|                            | WLAN
|                            | WAN |
| WHAT’S ON IT? IS IT RUNNING? | Anti-virus, anti-spyware
|                            | Personal firewall
|                            | Patching tools |
| WHAT’S THE PREFERRED WAY TO CHECK/FIX IT? | Pre-configured checks
|                            | Customized checks
|                            | Self-remediation or auto-remediation
|                            | Third-party software |
Complexity Demands Defense-in-Depth

**Endpoint Securityalone fails:**
- 99% have AV, but infections persist!
- Host based apps are easily manipulated—even unintentionally
- Time gap between virus and virus def/repair

**Identity alone fails:**
- Protects against unauthorized access, but not malware
- Identifies user, but not device

**Network Security alone fails:**
- Firewalls cannot block legitimate ports
- VPNs cannot block legitimate users
- Malware signatures must be known
- Detection often occurs after-the-fact
What Is Network Admission Control?

Using the network to enforce policies ensures that incoming devices are compliant.

- Who is the user?
- Is s/he authorized?
- What role does s/he get?
- Is MS patched?
- Does A/V or A/S exist?
- Is it running?
- Are services on?
- Do required files exist?
- Is policy established?
- Are non-compliant devices quarantined?
- Is remediation required?
- Is remediation available?
Four Key Capabilities of NAC

- **SECURELY IDENTIFY DEVICE & USER**
  - What it means: Uniquely identifies users and devices, and creates associations between the two.
  - Without it: Critical to associate users and devices with roles to know which policies apply; prevents device spoofing.

- **ENFORCE CONSISTENT POLICY**
  - What it means: Assess and enforce a ubiquitous policy across the entire network.
  - Without it: A decentralized policy mechanism (e.g. on endpoint) can leave gaping security holes.

- **QUARANTINE AND REMEDIATE**
  - What it means: Acts on posture assessment results, isolates device, and brings it into compliance.
  - Without it: Just knowing a device is non-compliant is not enough—someone still needs to fix it.

- **CONFIGURE AND MANAGE**
  - What it means: Easily creates comprehensive, granular policies that map quickly to user groups and roles.
  - Without it: Policies that are too complex or difficult to create and use will lead to abandonment of project.

A robust NAC solution must have all four capabilities.
Agenda

1. Securing Complexity
2. Clean Access Product Overview
3. Clean Access Features In-Depth
4. Clean Access Technical Benefits
The Cisco Clean Access Advantage

1. One product for ALL use cases

2. 500+ customers across all use cases: No. 1 NAC solution

3. Most deployments ready under 5 days

4. Scales from 100 users to 100,000+ user, across 150+ locations

5. Does not require infrastructure upgrade
Clean Access Enforces Compliance

SECURELY
IDENTIFY
DEVICE & USER

Authenticates and authorizes users (local db, RADIUS, LDAP, Kerberos, AD, etc.)
Supports all access methods (LAN, wireless, remote/VPN, WAN)

ENFORCE
CONSISTENT
POLICIES

Centralized policy supports multiple user roles
Scans for infections, port vulnerabilities, hotfixes, AV, AS, services running, and files

QUARANTINE
AND REMEDIATE

Isolates non-compliant devices using MAC and IP addresses; effective at a per-user level
Network-based, self-guided remediation
Helpdesk integration

CONFIGURE
AND MANAGE

Pre-configured checks simplify policy configuration and rule creation
Web-based interface for easy management of roles, policies, and remediation steps

Who’s on? What’s on?

What are the requirements for access?

What are the steps to meet requirements?

How do I create or modify requirements?
Clean Access Components

- **Cisco Clean Access Server**
  Serves as an in-band or out-of-band device for network access control

- **Cisco Clean Access Manager**
  Centralizes management for administrators, support personnel, and operators

- **Cisco Clean Access Agent**
  Optional lightweight client for device-based registry scans in unmanaged environments

- **Rule-set Updates**
  Scheduled automatic updates for anti-virus, critical hot-fixes and other applications
Sampling of Pre-Configured Checks

Critical Windows Updates
Windows XP, Windows 2000, Windows 98, Windows ME

Anti-Virus Updates

Anti-Spyware Updates
Other 3rd Party Checks

Customers can easily add customized checks
Product User Flow Overview

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
User Experience with Agent

Login Screen

Scan is performed
(types of checks depend on user role)

Scan fails

Remediate

You have temporary access!

Your system does not meet the requirements enforced by the network administrator. You may only have limited access to the network until your system meets all the requirements.

There is approximately 0:03:59 left before your temporary access expires.

Please click on "Continue" and follow the instructions to satisfy network access requirements.

Required Software

Name: Anti-Spyware (Optional) Software
Version:
Location: http://www.lavasoft.com/support/download/
Description: Our security policy recommends that you download an anti-spyware program. Click Go To Link to download a free Anti-Spyware program or click Next to skip.
User Experience via Web Browser

Login Screen

Scan is performed (types of checks depend on user role/OS)

Guided self-remediation
Clean Access Sizing

Super Manager manages up to 40
Enterprise and Branch Servers

Standard Manager manages up to 20
Branch Office or SMB Servers

Manager Lite manages up to 3

Users = online, concurrent

1500 users each

100 users
250 users
500 users
1500 users each
Agenda

1. Securing Complexity
2. Clean Access Product Overview
3. Clean Access Features In-Depth
   - Management Console
   - Checks, Rules, Requirements
4. Clean Access Technical Benefits
Tour of Features: Management Console

- The Clean Access Manager (CAM) uses a GUI front-end for administration and management. Flat HTML, no Java or Active-X controls necessary.
- Changes are only made once in the active CAM, replication takes care of the rest.
- Communication between the CAS and the CAM is protected by SSL and shared passwords.
- Clean Access Server administration is controlled centrally through the Clean Access Manager.

(Make sure the Clean Access Server is on VLAN a before you set its management VLAN ID to a.)
CAM Manages All Clean Access Servers

Cisco Clean Access Manager - Microsoft Internet Explorer provided by Cisco Systems, Inc.

Device Management > Clean Access Servers > 192.168.3.2

Clean Access Server Type:
- Virtual Gateway
- Virtual Gateway
- Flex-IP Gateway
- NAT Gateway
- Out-of-Band Virtual Gateway
- Out-of-Band Flex-IP Gateway
- Out-of-Band NAT Gateway

Trusted Interface (to protected network):
- IP Address: 192.168.3.2
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.3.1
- Set management VLAN ID: 10

Untrusted Interface (to managed network):
- IP Address: 192.168.3.2
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.3.1
- Set management VLAN ID: 0

Pass through VLAN ID to managed network
Pass through VLAN ID to protected network

Make sure the Clean Access Server is on VLAN 10 before you set its management VLAN ID to 10.
Pre-Configured Checks

Updates of Clean Access Agent and pre-configured checks are downloaded automatically at designated intervals

- Proxy capabilities for customer who do not allow direct internet connections
- SSL encryption and certificates secure traffic between Cisco and the CAM
Clean Access posture validation is a hierarchical process with either pre-loaded or custom profiles.

**CHECKS**
- assess the state of a file, application, service, or registry key

**RULES**
- contain single or multiple Checks

**REQUIREMENTS**
- contain single or multiple Rules

**ROLES**
- have one or more Requirements
Checks and Rules: An Example

CHECKS
assess the state of a file, application, service, or registry key

- Is anti-spyware installed? (application present, file present)
- Is anti-spyware up-to-date? (file version > or =)
- Is anti-spyware running? (service / exe running)

RULES
assemble individual checks together to make a posture assessment

- Anti_Spyware_Installed_Check
- Anti_Spyware_UptoDate_Check
- Anti_Spyware_Running_Check
How Checks Look in the Manager

This is an example of a registry key CHECK for a Windows Hotfix:
# Cisco Clean Access Standard Manager

## Device Management > Clean Access

<table>
<thead>
<tr>
<th>Certified Devices</th>
<th>General Setup</th>
<th>Network Scanner</th>
<th>Clean Access Agent</th>
<th>Updates</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribution</td>
<td>Installation</td>
<td>Rules</td>
<td>Requirements</td>
<td>Reports</td>
</tr>
<tr>
<td>Check List</td>
<td>New Check</td>
<td>Rule List</td>
<td>New Rule</td>
<td>New AV Rule</td>
</tr>
<tr>
<td>Native Info</td>
<td></td>
<td></td>
<td>Role Requirements</td>
<td>New AS Rule</td>
</tr>
<tr>
<td>Support Info</td>
<td></td>
<td></td>
<td>Reports</td>
<td>AV/AS</td>
</tr>
</tbody>
</table>

### Check Category
- Service Check
- Registry Check
- File Check
- Application Check

### Check Type
- Service Status

### Check Description

### Operating System
- Windows All
  - Windows 2000
  - Windows ME
  - Windows 98
- Windows XP (All)
  - XP Pro/Home
  - XP Tablet PC
  - XP Media Center

- Automatically create rule based on this check

### Add Check
How Rules Look in the Manager

This is an example of a Windows Hotfix RULE with multi-level check logic:
Requirements and Roles

**REQUIREMENTS**
- Tie remediation actions directly to a rule

**ROLES**
- Determine which requirements and which security filters apply

Remediation methods include:
- File Distribution (“Download antispyware.exe”)
- Link Distribution (“windowsupdate.com”)
- Local Check (text instructions or messages)
- Definition Update (direct launch of supported AV or AS)

Option to dynamically assign VLANs
- Apply individual URL redirection per role, as well as Acceptable Usage Policies, User Pages, and more
How Requirements Look in the Manager

Remediation as required by REQUIREMENTS can be manual, automatic, optional, or enforced:
Cisco Clean Access Standard Manager Version 4.1.0

Device Management > Clean Access

Certified Devices  General Setup  Network Scanner  Clean Access Agent  Updates
Distribution  Installation  Rules  Requirements  Role Requirements  Reports
Requirement List  New Requirement  Requirement Rules

Requirement Type: AV Definition Update

Enforce Type: Man

Antivirus Vendor Name: None

AV Definition Update

AS Definition Update

Windows Update

Launch Programs

Requirement Name

Description

Operating System
- Windows All
  - Windows 2000
  - Windows ME
  - Windows 98
- Windows XP (All)
  - XP Pro/Home
  - XP Tablet PC
  - XP Media Center

Add Requirement

If the user has one of the following listed products installed, he/she can use the Update button provided by CCA Agent to update the virus definition file if this requirement fails.
How Roles Look in the Manager

Fine-tuning for timers, agents, and policies on a per-ROLE basis:
How Roles Look in the Manager

More options based on user ROLE (called “FTE” in this case):
 Filters and Bandwidth

SECURITY FILTERS behave the same as Access Control Lists with additional http://weblink and Layer 2 protocol capabilities.

Each role has its own filter, with access levels controlled by the system administrator.

BANDWIDTH CONTROLS allow for either per-user or per-role restrictions.

Common for remediation and guest access applications.
How Filters Look in the Manager

At-a-glance display of Filters by User Roles:
How Bandwidth Controls Look

Bandwidth control on a per-user and per-role basis:
Clean Access Manager: Back-end Authentication

Flexible back-end authentication options allow for fast integration to existing networks: Kerberos/NTLM, RADIUS, LDAP, AD, local db

- Map users attributes and rights directly to Roles and Filters
- Add operators and conditions to mapping rules to dial in the desired access rights
Admin Control with Real-Time Information

Logs can be viewed locally or sent via Syslog to an off-box collection engine for custom reports
Fine-Tuning Administrator Access

Multiple administrator user accounts for NOC, help desk operators, etc.
Clean Access Manager Benefits

Summary

- Centralized and scalable management and policy configuration
- Pre-configured checks drastically reduce “Day 2” support and maintenance
- Full access to the rules engine can create a posture assessment for any application
- Flexible remediation options give users as much power as desired to self-repair, reducing help desk dependence
Agenda

1. Securing Complexity
2. Clean Access Product Overview
3. Clean Access Features In-Depth
4. Clean Access Technical Benefits
## Clean Access Technical Benefits

<table>
<thead>
<tr>
<th>Product Experience</th>
<th>With 500+ deployments, Cisco understands the technical impact on your network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defense-in-Depth</td>
<td>Clean Access is a self-contained, proactive way to enforce policy compliance on all incoming devices</td>
</tr>
<tr>
<td>Rapid Setup Easy Mgmt</td>
<td>Pre-configured rulesets and checks make it easy to setup, maintain, modify, and expand</td>
</tr>
<tr>
<td>Flexible Deployment</td>
<td>Broad deployment options means that Clean Access fits into your network the way you need it to</td>
</tr>
<tr>
<td>Future Proof</td>
<td>Clean Access is core to Cisco’s strategic NAC vision and can be leveraged across all future deployment options</td>
</tr>
</tbody>
</table>