



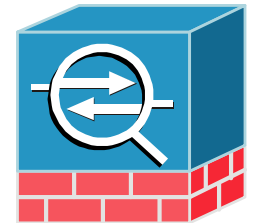
Technical Update

Januar 2007



Adaptive Security Appliances NAC Appliance

Niels Mogensen

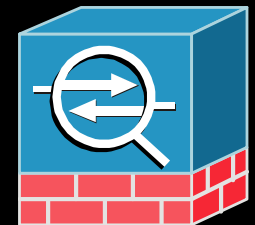




Cisco ASA 5500 Series Adaptive Security Appliances



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

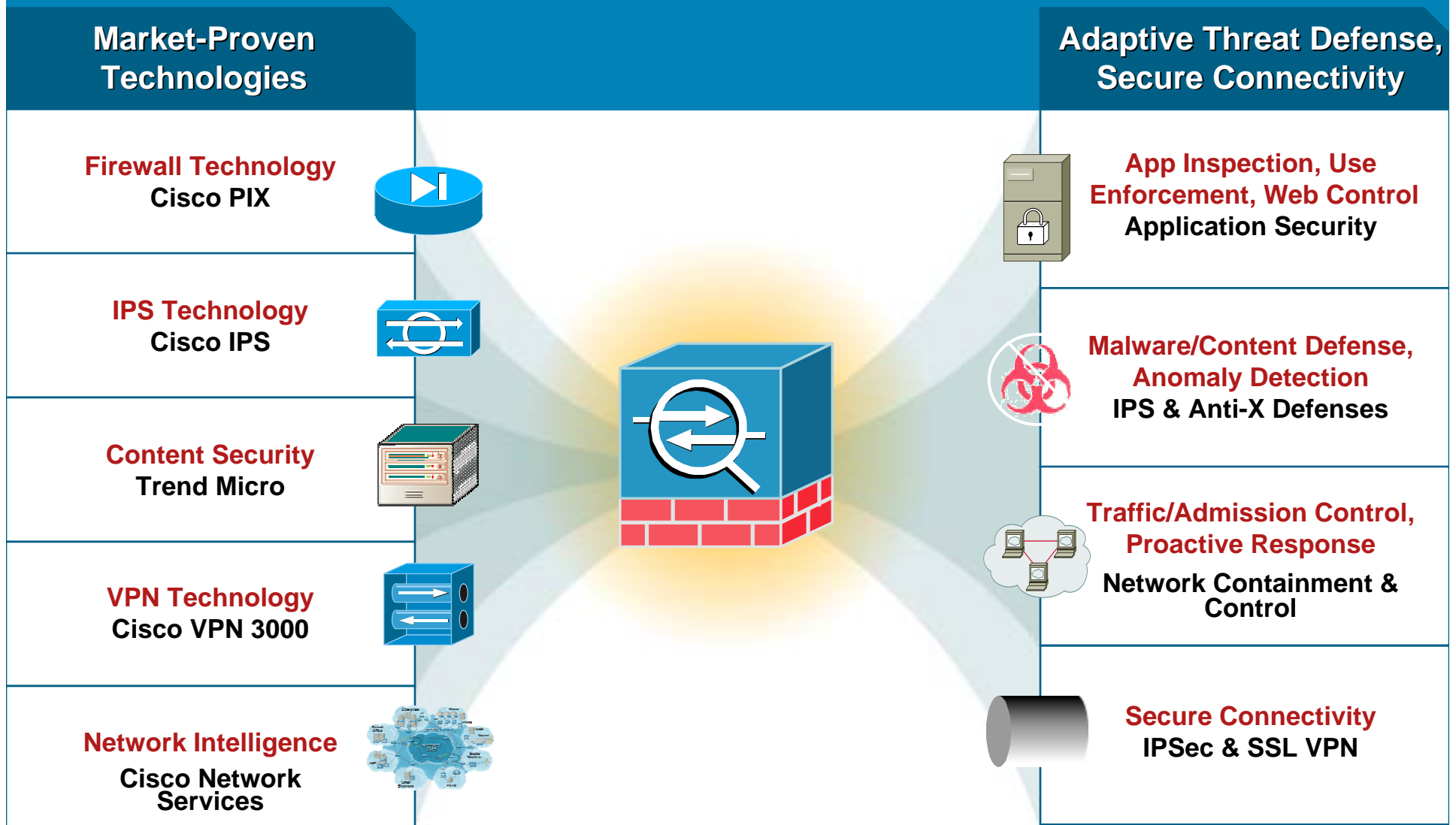
Purpose-Built Adaptive Identification and Mitigation Architecture Enables
Unprecedented Extensibility and Policy Control



The Cisco ASA 5500 Series

Cisco ASA 5500 Series

Convergence of Robust, Market-Proven Technologies



Cisco ASA 5500 Series Enterprise Editions

Cisco ASA 5500
Firewall Edition

Cisco ASA 5500
SSL & IPsec
VPN Edition



Cisco ASA 5500
IPS Edition

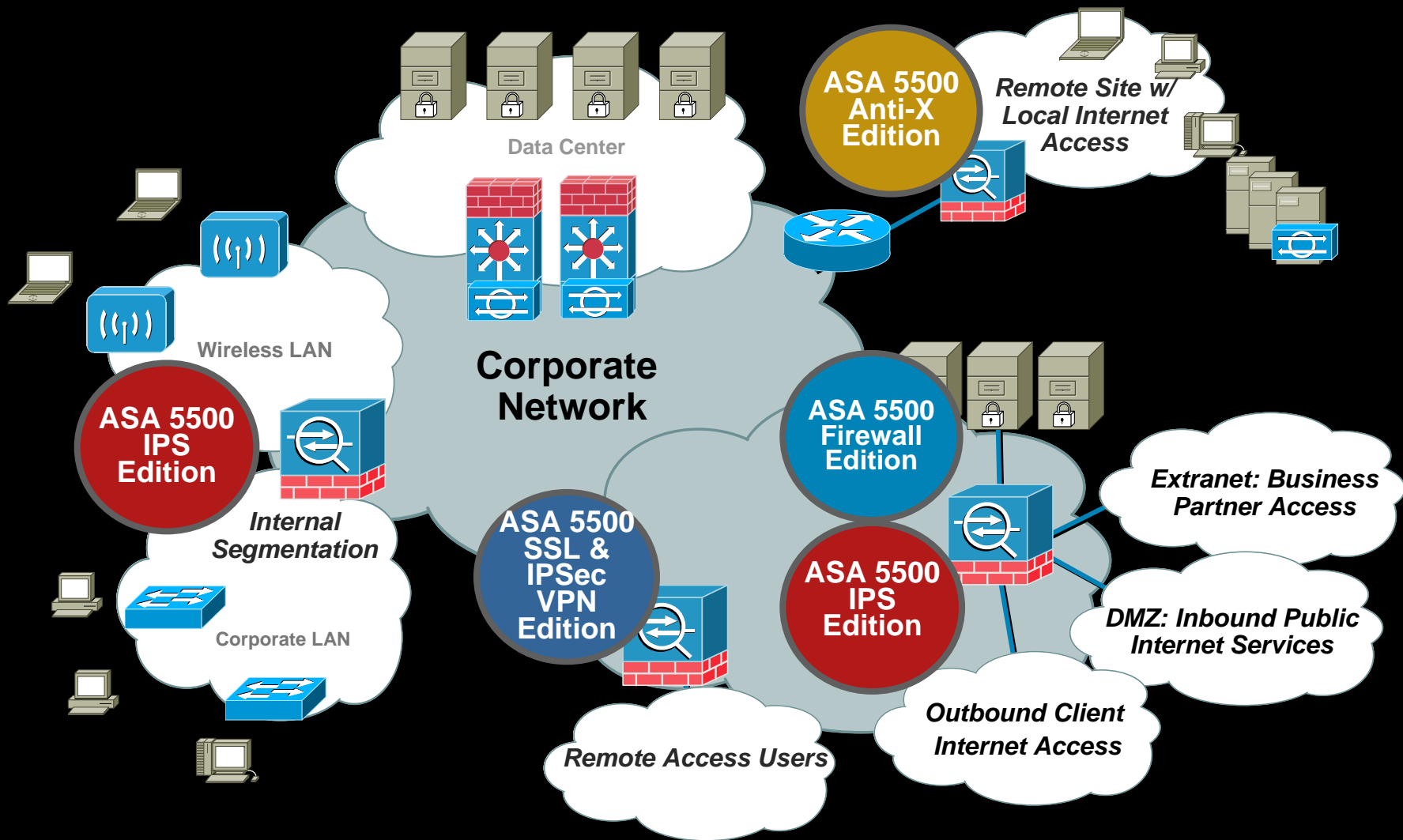
Cisco ASA 5500
Anti-X Edition

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 Series Solutions

Business Solutions and the Corporate Network



Cisco ASA 5500 Series: Breadth and Depth

Industry First Scalable, Multi-Function, Feature Rich Appliance

Firewall with Application Layer Security



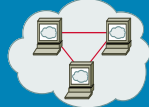
- **Multi-layer packet and traffic analysis**
- **Advanced application and protocol inspection services**
- **Network application controls**
- **Advanced VoIP/multimedia security**

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**

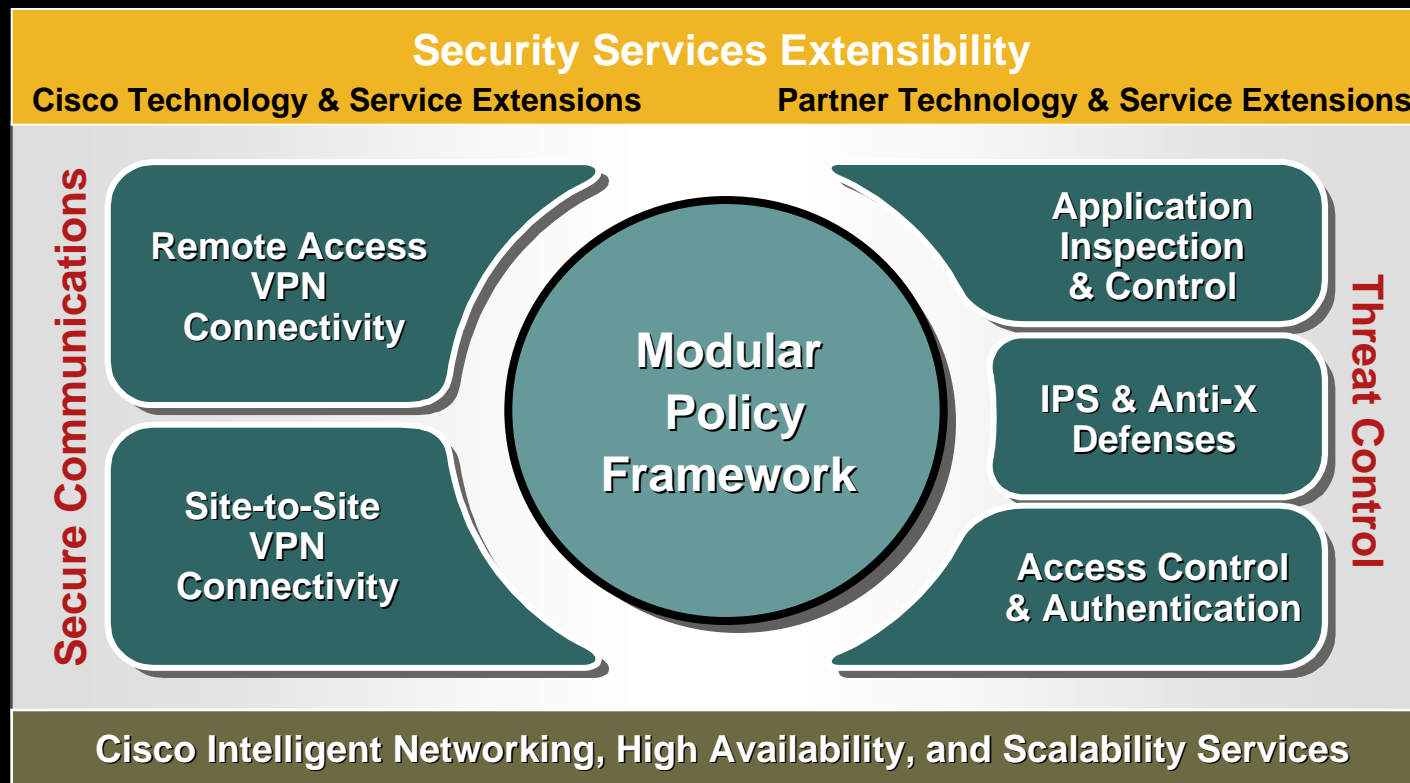
Cisco Intelligent Networking Services



- **Low latency**
- **Diverse topologies**
- **Multicast support**
- **Services virtualization**
- **Network segmentation & partitioning**
- **Routing, resiliency, load-balancing**

Cisco ASA 5500 Series Modular Policy Framework

Extensible Design Enables Flexible, Flow-Based Services Policies



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

Edit Event Action Override

Event Action: Deny Attacker Inline

Enabled: Yes No

Risk Rating: Minimum - Maximum

OK Cancel Help

Customizable Risk Rating Thresholds :

0 < RR < 35

Alarm

35 < RR < 85

Alarm & Log Packets

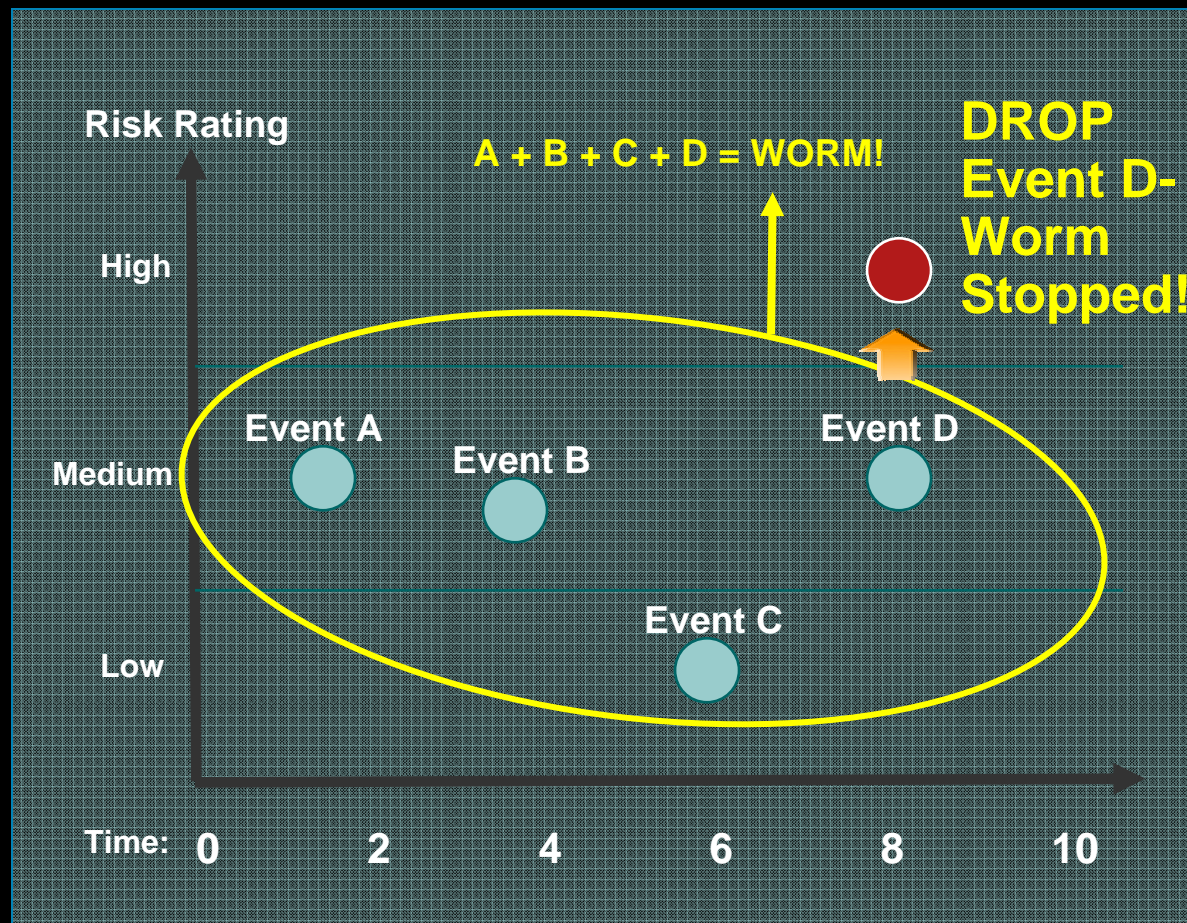
85 < RR < 100

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

Content Security in the Cisco ASA 5500 Series

All
New!

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 SYSTEMS



Cisco ASA 5500 Series Anti-X Edition

Delivering Comprehensive Protection and Control

➤ THREAT TYPES



Unauthorized Access



Intrusions & Attacks



Insecure Comms.

Viruses

New!

Spyware

Malware

Phishing

Spam

Inappropriate URLs

Identity Theft

Offensive Content

NEW Anti-X Service Extensions



Cisco ASA 5500 with CSC-SSM



Granular Policy Controls

Comprehensive Malware Protection

Advanced Content Filtering

Integrated Message Security

Easy to Use

➤ PROTECTION

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

Content Security and Control SSM

Product Details



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

Platforms / Subscription Levels

CSC SSM-10

- 50 User
- 100 User
- 250 User
- 500 User

CSC SSM-20

- 500 User
- 750 User
- 1,000 User

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

Multimedia / Voice over IP

SIP
SCCP (Skinny)
H.323 v1-4
GTP (3G Mobile Wireless)
MGCP
RTP / RTCP / RTSP
TAPI / JTAPI

Specific Applications

Microsoft Windows Messenger
Microsoft NetMeeting
Real Player
Cisco IP Phones
Cisco Softphones

Over 30
Engines

Core Internet Protocols

HTTP
FTP
TFTP
SMTP / ESMTP
DNS / EDNS
ICMP
TCP
UDP

Database / OS Services

ILS / LDAP
Oracle / SQL*Net (V1/V2)
Microsoft RPC / DCE RPC
Microsoft Networking
NFS
RSH
SunRPC / NIS+
X Windows (XDMCP)

Security Services

IKE
IPSec
PPTP

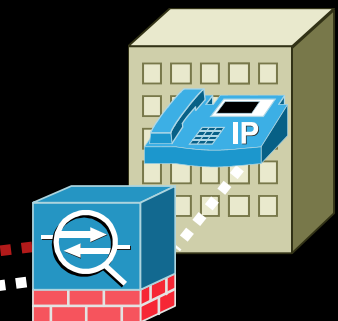
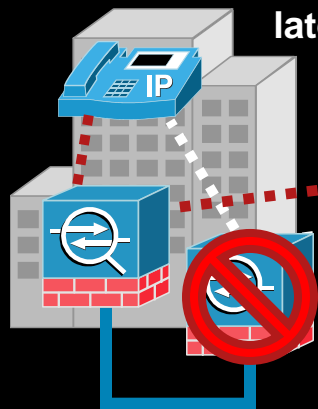
Cisco ASA 5500 Series VPN Solutions

Enterprise-Class Site-to-Site VPN Capabilities

Network-aware site-to-site VPNs

QoS-Enabled VPN

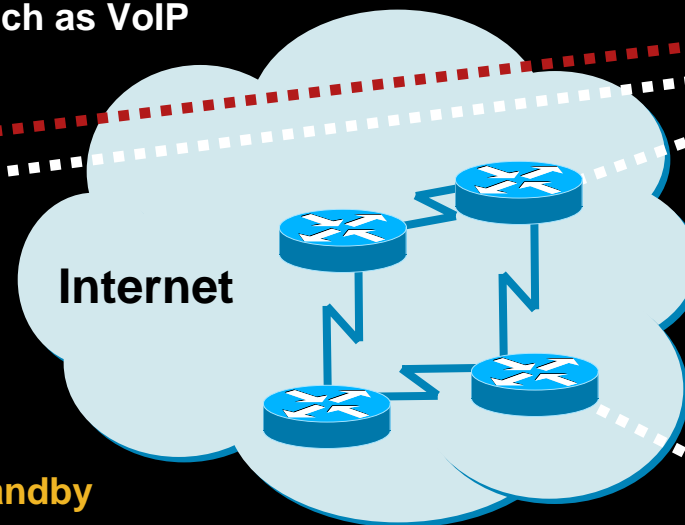
Support for low latency queuing for latency-sensitive traffic such as VoIP



OSPF Routing Over VPN

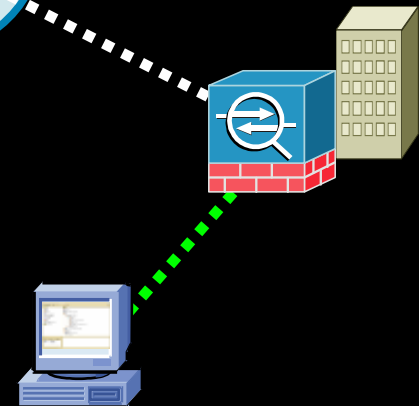
IPSec Stateful Failover

- 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** keysize support

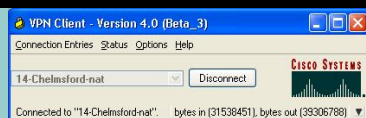


Remote Access VPN Technology Comparison

IPSec and SSL VPNs

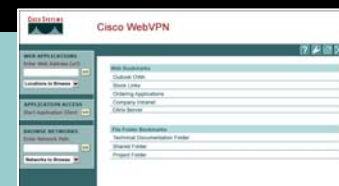
There are 2 primary remote access VPN technologies: IPSec and SSL. SSL is the newer technology of choice, typically has lower support costs and provides better access to business partners and contractors than IPSec. SSL is growing faster than IPSec.

IPSec VPN



- Widely deployed, well-proven technology
- Operates well for extending access to employees using company-managed desktops

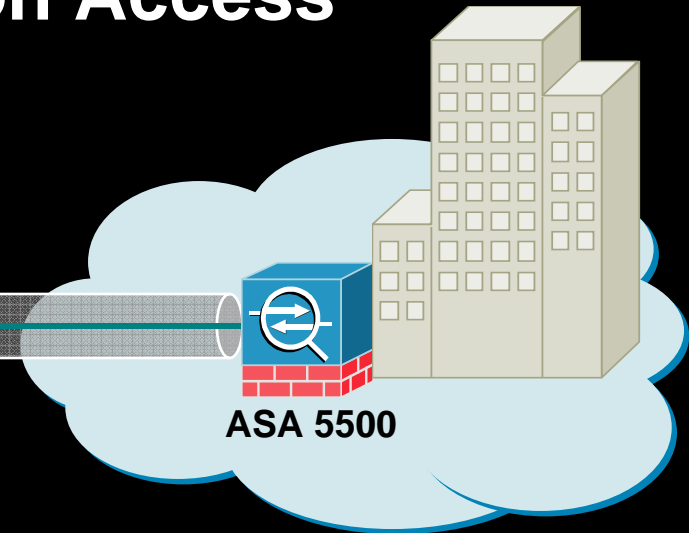
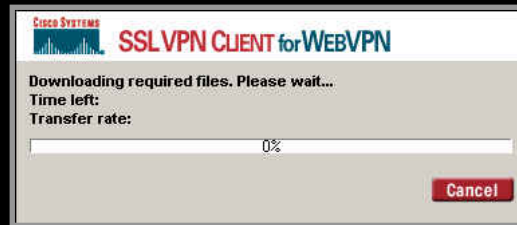
SSL VPN



- Extends secure network access to non-employees like contractors and temps
- Simplifies provisioning and support for business partner access
- Provides “anywhere” access to non-managed desktops such as Internet kiosks
- Enables customized user access portals
- Reduces operations costs associated with managing client software

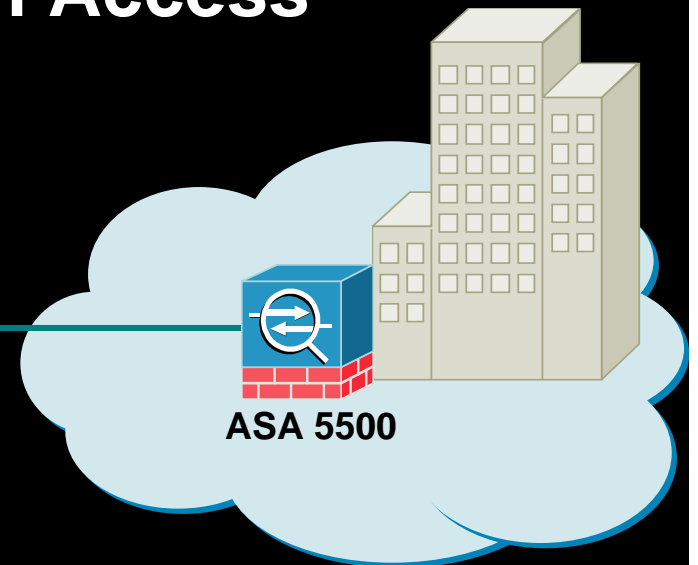
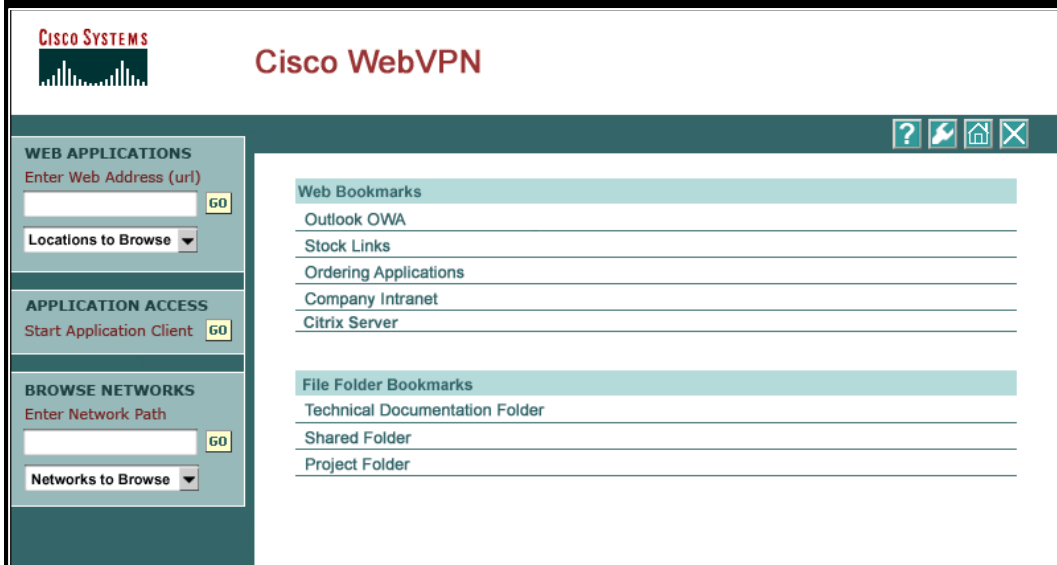
Customizable Remote Application Access

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

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



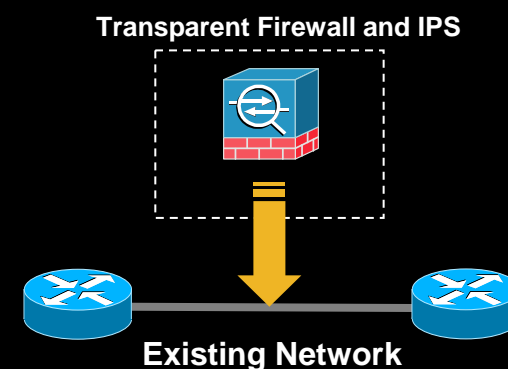
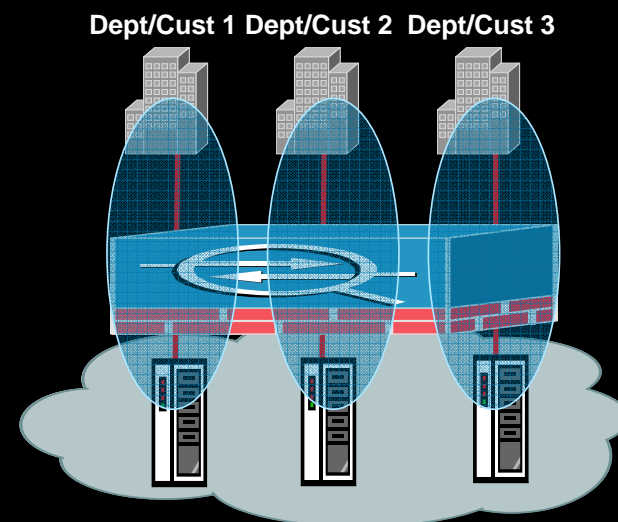
Virtualized Services and Transparent Operation Simplifies Deployment and Reduces Operational Costs

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 firewalling** and **security zoning** – new applications

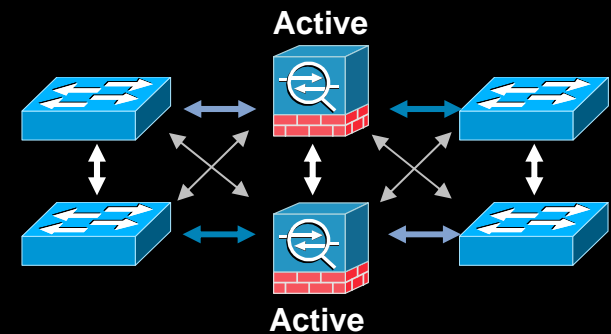


Advanced Network Integration

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**



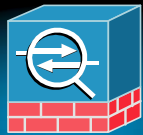
Intelligent Network Integration

- 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






List Price

Performance

Max Firewall
Max Firewall + IPS
Max IPSec VPN
Max IPSec / SSL VPN Peers

Platform Capabilities

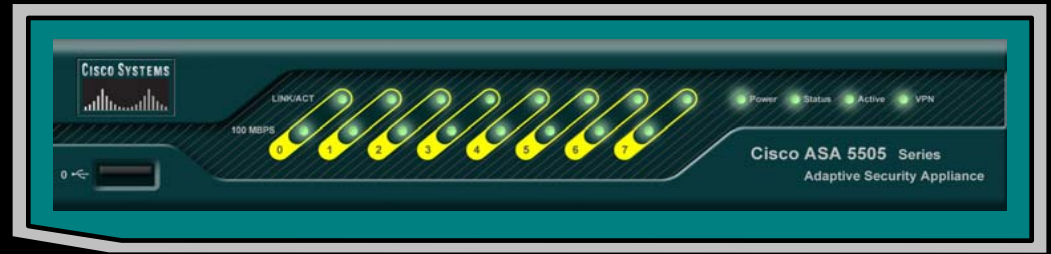
Max Firewall Conns
Max Conns/Second
Base I/O
VLANs Supported
HA Supported

	Cisco ASA 5505 <i>New!</i>	Cisco ASA 5510	Cisco ASA 5520	Cisco ASA 5540	Cisco ASA 5550 <i>New!</i>
					
Target Market	SOHO and ROBO	SMB and SME	Enterprise	Medium Enterprise	Large Enterprise
List Price	Starting at \$595	Starting at \$3,495	Starting at \$7,995	Starting at \$16,995	Starting at \$19,995
Performance	150 Mbps Future 100 Mbps 25 / 25	300 Mbps 300 Mbps 170 Mbps 250 / 250	450 Mbps 375 Mbps 225 Mbps 750 / 750	650 Mbps 450 Mbps 325 Mbps 5000 / 2500	1.2 Gbps N/A 425 Mbps 5000 / 5000
Platform Capabilities	10,000 / 25,000 3,000 8-port FE switch 3 / 3 (trunk) Stateless A/S (Sec Plus)	50,000 / 130,000 6,000 3+1 FE / 5 FE 10 / 25 A/A & A/S (Sec Plus)	280,000 9,000 4 GE + 1 FE 100 A/A & A/S	400,000 20,000 4 GE + 1 FE 200 A/A & A/S	650,000 28,000 8 GE + 1 FE 200 A/A & A/S

Introducing the Cisco ASA 5505

Next Generation SOHO / ROBO Security Appliance

Next Generation solution for small business, branch office and enterprise teleworker environments!



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)



- Secure access for a wide range of applications through the Internet VLAN
- DHCP Server Services

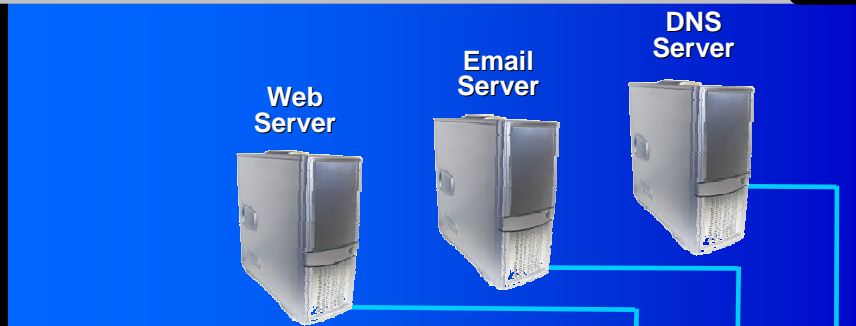
Home VLAN



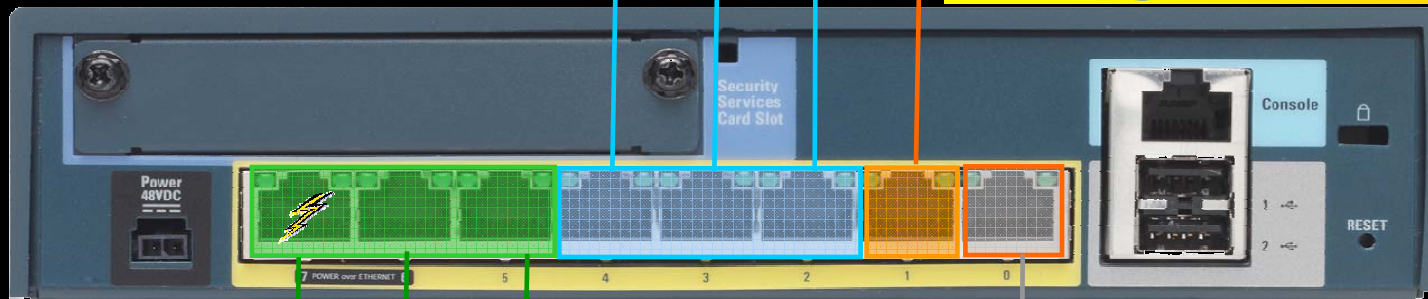
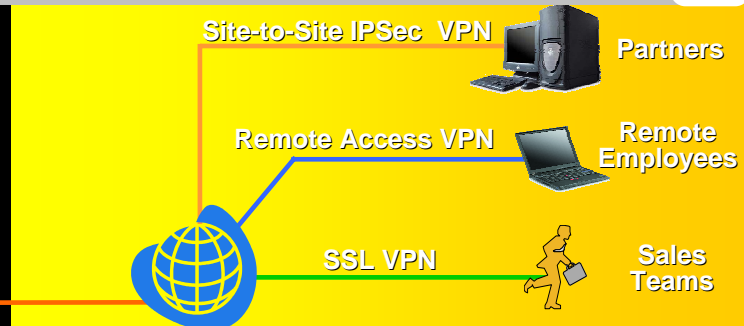
Remote Office/SMB Deployment Model

High Performance, Resilient Security Services

Business/DMZ VLAN



Internet VLAN (Active)



Inside VLAN



Internet VLAN (Standby)



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

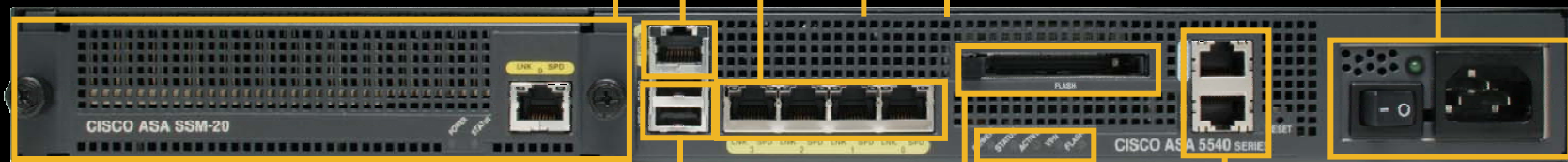
One 10/100 Out of Band
Management Port*

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



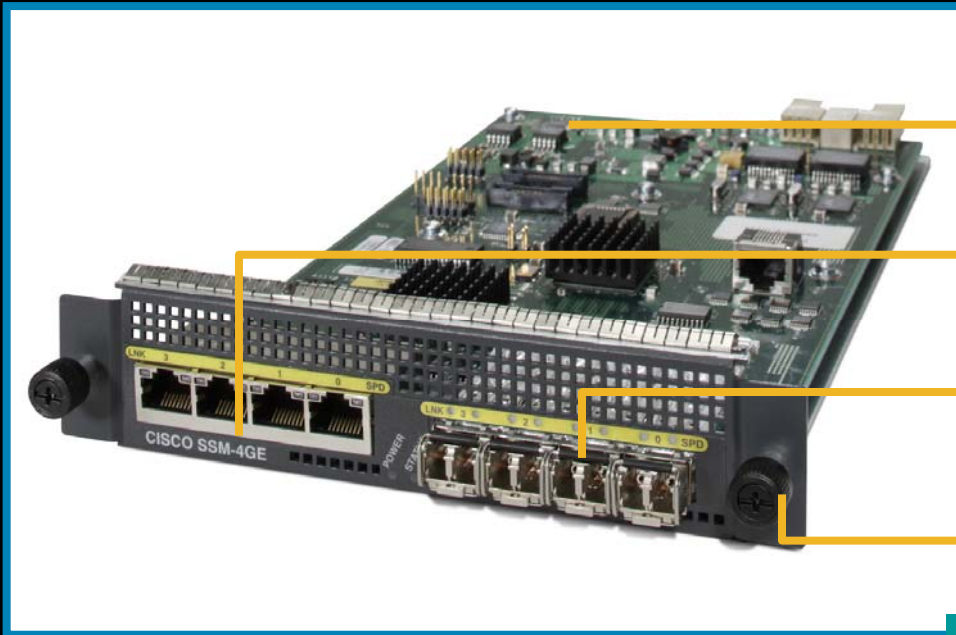
Two USB 2.0 Ports for
Future Expansion (Credentials,
Failover, and more)

Compact Flash for Software,
Config, and Log Storage

Console and AUX Ports

Five Status LEDs (Power,
Status, Active, VPN, Flash)

Cisco Four-Port Gigabit Ethernet SSM Product Tour



**High-Performance Module
Adds More I/O Capacity**

**Four Copper 10/100/1000
for Simplified Deployment**

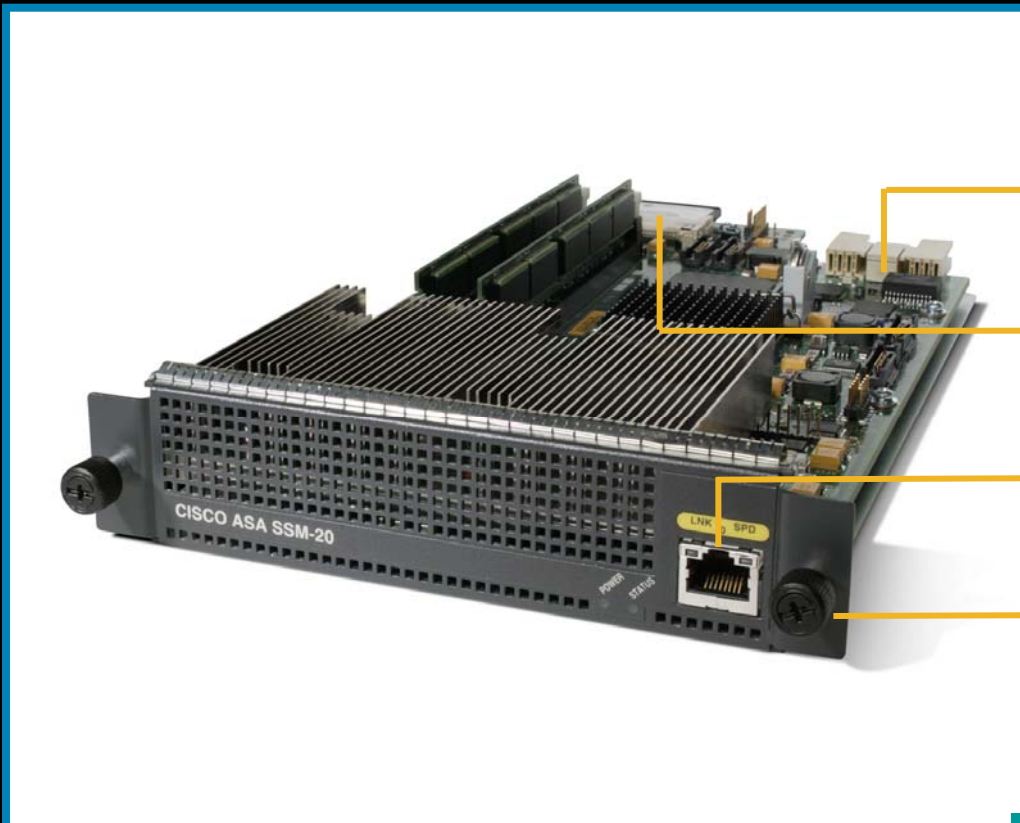
**Four SFP Gigabit Ports
for Optical Connectivity**

**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

New!

Completed: Level 2, v7.0.4 – ASA Family

ICSA Firewall 4.1, Corporate Category

New!

Completed: v7.0.4 – ASA Family

ICSA IPSec 1.0D

New!

Completed: v7.0.4 – ASA Family

ICSA Anti-Virus Gateway

New!

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

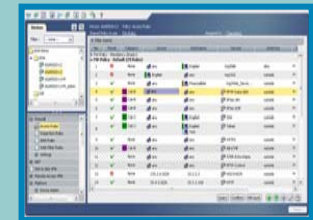
Integrated Remote Management Capabilities Within ASA

- 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

Device Information

General License

Host Name: **myFirewall.example.com**

ASA Version: **7.2(0)79** Device Uptime: **0d 4h 20m 59s**

ASDM Version: **5.2(1)** Device Type: **ASA 5520**

Firewall Mode: **Routed** Context Mode: **Single**

Total Flash: **64 MB** Total Memory: **1024 MB**

Interface Status

Interface	IP Address/Mask	Line	Link	Kbps
dmz	172.16.1.1/24	down	down	0
inside	192.168.1.1/24	up	up	0
mgmt	172.23.59.108/24	up	up	5
outside	198.52.1.1/24	up	up	0
partner-dmz	10.1.1.1/16	down	down	0

VPN Status

IKE Tunnels: **0** WebVPN Tunnels: **0** SVC Tunnels: **0**

System Resources Status

CPU Usage (percent): **27%**

Memory Usage (MB): **365MB**

Traffic Status

Connections Per Second Usage

'outside' Interface Traffic Usage (Kbps)

Input Kbps: **0** Output Kbps: **0**

Latest ASDM Syslog Messages (Stopped)

Severity	Date	Time	Syslog ID	Source IP	Destination IP	Description
6	Feb 16 2004	19:23:45	302013	10.21.104.41	172.23.59.108	Built inbound TCP connection 158 for mgmt:10.21.104.41/2973 (10.21.104.41/2973) to NP Identity Ifc
1	Feb 16 2004	19:23:44	106100	192.168.0.25	Mail_Server	access-list inside_access_in permitted tcp inside/192.168.0.25(10699) -> mgmt:Mail_Server(109) hit
6	Feb 16 2004	19:23:43	106015	10.21.104.41	172.23.59.108	Deny TCP (no connection) from 10.21.104.41/2908 to 172.23.59.108/443 flags RST on interface mg
6	Feb 16 2004	19:23:24	302013	10.21.104.41	172.23.59.108	Built inbound TCP connection 157 for mgmt:10.21.104.41/2959 (10.21.104.41/2959) to NP Identity Ifc
6	Feb 16 2004	19:23:24	302014	10.21.104.41	172.23.59.108	Teardown TCP connection 156 for mgmt:10.21.104.41/2958 to NP Identity Ifc:172.23.59.108/443 dur
6	Feb 16 2004	19:23:23	725001	10.21.104.41		Starting SSL handshake with client mgmt:10.21.104.41/2958 for TLSv1 session.
6	Feb 16 2004	19:23:23	302013	10.21.104.41	172.23.59.108	Built inbound TCP connection 156 for mgmt:10.21.104.41/2958 (10.21.104.41/2958) to NP Identity Ifc
6	Feb 16 2004	19:23:21	302014	10.21.104.41	172.23.59.108	Teardown TCP connection 155 for mgmt:10.21.104.41/2957 to NP Identity Ifc:172.23.59.108/443 dur
6	Feb 16 2004	19:23:21	725007	10.21.104.41		SSL session with client mgmt:10.21.104.41/2957 terminated.

• 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 a object or members of a group via tooltips

Object Selector: Can create, edit or delete network objects, services etc from the rule table itself

Show Logs: Show Logs fired ONLY from the selected rule in the Real Time Log Viewer

Packet Tracer: Run packet tracer on the selected rule, which will fill the appropriate values

Rule Flow Diagram: Rule Flow Diagram provides a snap-shot of the rule in a simple, nice view

Representation of system default rules: including "deny ip any any" rules

No.	Enabled	Source	Destination	Service	Action	Logging	Time	Description
dmz (2 implicit incoming rules)								
1		any	Any less secure net...	IP: ip	Permit			Implicit rule: Permit all traffic to
2		any	any	IP: ip	Deny			Implicit rule
inside (5 incoming rules)								
1	✓	FTP_Servers_inside	10.1.100.0/24	FTP: ftp	Permit			Sample Cisco CST (Checkers
		Web_server_group	10.1.101.0/24	SSH: ssh				
			10.1.102.0/24	HTTPS: https				
			10.1.103.0/24	HTTP: http				
			10.1.104.0/24					
2	✓	Inside-network/16	Mail_Server	Mail: Mail_Services	Permit	Alert...		
3	✓	192.0.0.0/8	172.16.0.0/16	any	Permit			allow all icmp to DMZ network
4	✓	192.16.210.0/24	198.52.1.100	any	Permit			
5		any	any	IP: ip	Deny			
mgmt (2 implicit incoming rules)								
1		any	Any less secure net...	IP: ip	Permit			Implicit rule: Permit all traffic to
2		any	any	IP: ip	Deny			Implicit rule
outside (7 incoming rules)								
1	✓	any	WWW_Server	HTTP: http	Permit			Allow anyone to access Wwe
2	✓	outside-network/24	192.168.1.100	HTTP: http	Permit	Alert...		Allow outside network to acc
3	✓	158.1.0.0/16	DMZ-networks	ping: ping-service	Permit			allow pings
4	✓	any	FTP_Servers_inside	FTP: ftp	Permit	Criti...		log any access to ftp server
5	✓	all_networks	DMZ-networks	UDP: all_udp-servic...	Deny			test rule to show tool-tip on t
6	✓	any	any	IP: ip	Deny			
7	✓	any	any	IP: ip	Deny			
partner-dmz (5 incoming rules)								

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

The screenshot shows the Cisco ASDM Packet Tracer interface. At the top, it prompts the user to select a packet type and supply parameters. The configuration is as follows:

- Interface: inside
- Packet Type: TCP
- Source IP: 10.1.1.100
- Destination IP: 100.1.1.100
- Source Port: 1025
- Destination Port: 80
- Show animation: checked

Below the configuration is a visual flow diagram showing the packet's path through various processing stages: inside, low Lookup, Route Lookup, Access list Lookup, IP Options Lookup, NAT Lookup, NAT Lookup, IP Options Lookup, and Flow creation Lookup.

The main part of the interface is a table showing the detailed phases of the packet's journey:

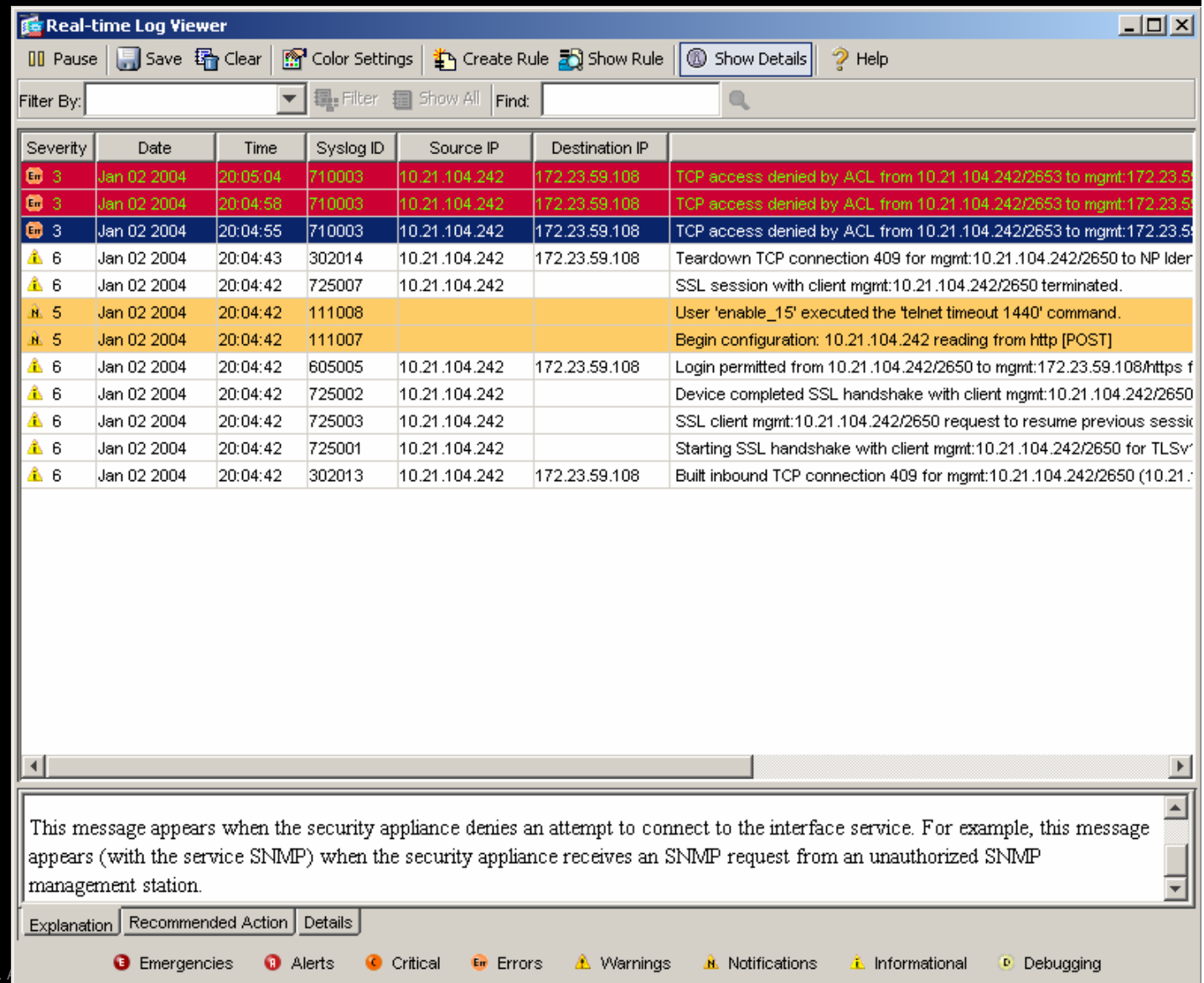
Phase	Action
ROUTE-LOOKUP	✓
ACCESS-LIST	✓
Type - ACCESS-LIST Action - ALLOW Show rule in Access Rules table.	
Config	
access-group inside_access_in in interface inside	
access-list inside_access_in extended permit tcp 10.1.1.0 255.255.255.0 100.1.1.0 255.255.255.0 eq www log emergencies	
IP-OPTIONS	✓
NAT	✓
NAT	✓
IP-OPTIONS	✓
FLOW-CREATION	✓
RESULT - The packet is forwarded.	✓

At the bottom of the window are 'Close' and 'Help' buttons.

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



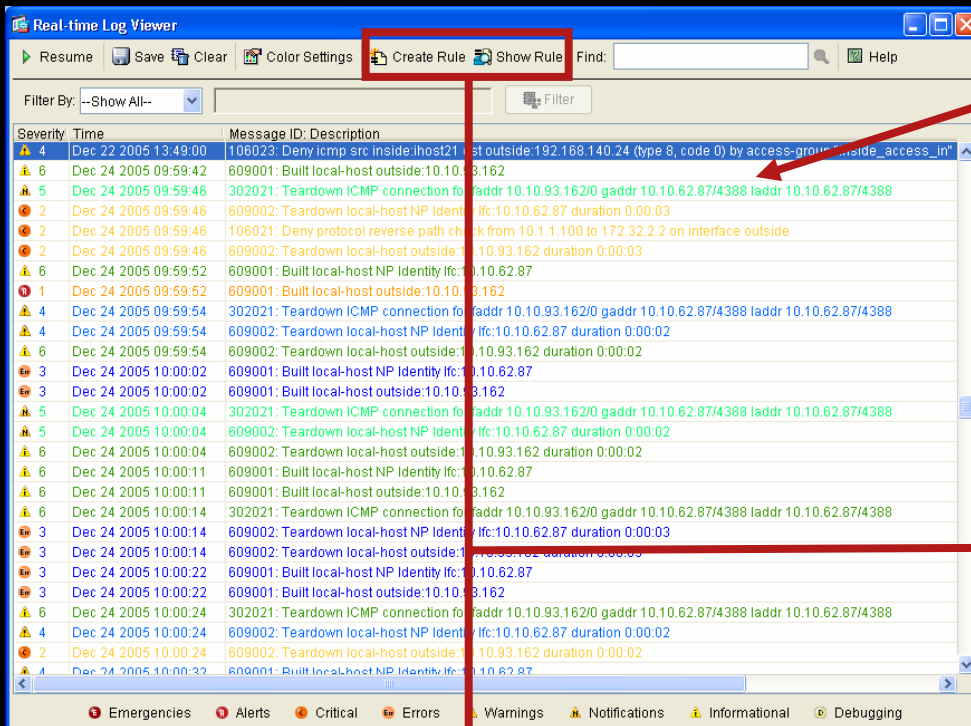
Severity	Date	Time	Syslog ID	Source IP	Destination IP	Message
Er 3	Jan 02 2004	20:05:04	710003	10.21.104.242	172.23.59.108	TCP access denied by ACL from 10.21.104.242/2653 to mgmt:172.23.59.108
Er 3	Jan 02 2004	20:04:58	710003	10.21.104.242	172.23.59.108	TCP access denied by ACL from 10.21.104.242/2653 to mgmt:172.23.59.108
Er 3	Jan 02 2004	20:04:55	710003	10.21.104.242	172.23.59.108	TCP access denied by ACL from 10.21.104.242/2653 to mgmt:172.23.59.108
W 6	Jan 02 2004	20:04:43	302014	10.21.104.242	172.23.59.108	Teardown TCP connection 409 for mgmt:10.21.104.242/2650 to NP Ider
W 6	Jan 02 2004	20:04:42	725007	10.21.104.242		SSL session with client mgmt:10.21.104.242/2650 terminated.
I 5	Jan 02 2004	20:04:42	111008			User 'enable_15' executed the 'telnet timeout 1440' command.
I 5	Jan 02 2004	20:04:42	111007			Begin configuration: 10.21.104.242 reading from http [POST]
W 6	Jan 02 2004	20:04:42	605005	10.21.104.242	172.23.59.108	Login permitted from 10.21.104.242/2650 to mgmt:172.23.59.108/https f
W 6	Jan 02 2004	20:04:42	725002	10.21.104.242		Device completed SSL handshake with client mgmt:10.21.104.242/2650
W 6	Jan 02 2004	20:04:42	725003	10.21.104.242		SSL client mgmt:10.21.104.242/2650 request to resume previous sessio
W 6	Jan 02 2004	20:04:42	725001	10.21.104.242		Starting SSL handshake with client mgmt:10.21.104.242/2650 for TLSv
W 6	Jan 02 2004	20:04:42	302013	10.21.104.242	172.23.59.108	Built inbound TCP connection 409 for mgmt:10.21.104.242/2650 (10.21.:

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.

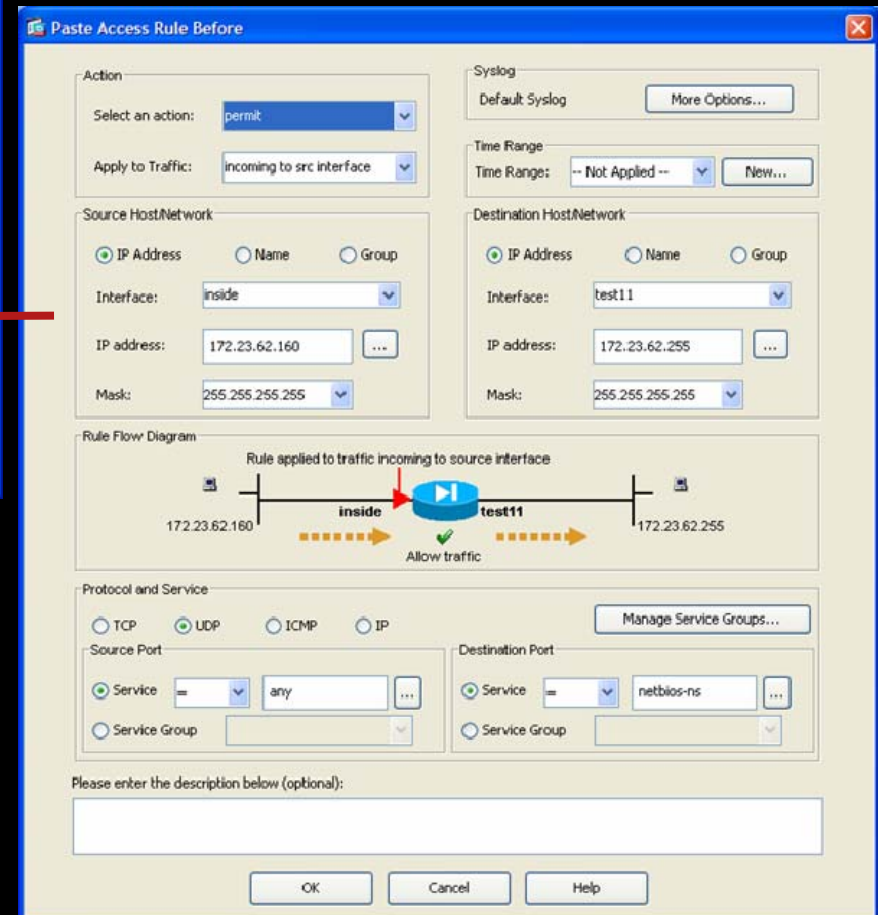
Explanation Recommended Action Details

E Emergencies R Alerts C Critical Er Errors W Warnings N Notifications I Informational D Debugging

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

Topology View

Policy View

No.	Permit	Category	Source	Destination	Direction	Action	
1	None	any	EngNet	tcp/588	dmz	in	
2	None	EngNet	any	tcp/322	outside	in	
3	None	any	FinancialNet	tcp/Web_Servic...	outside	in	
4	✓	Cat-B	any	PPTP-Data-GRE	outside	in	
5	✓	Cat-B	any	IPSec-AH	outside	in	
6	✓	Cat-B	any	IPSec-ESP	outside	in	
7	✓	any	EngNet	SSH	outside	in	
8	✓	Cat-C	any	EngNet	Telnet	outside	in
9	✓	any	any	HTTPS	outside	in	
10	✓	Cat-B	any	All-ICMP	outside	in	
11	✓	any	any	ICMP-Echo-Reply	outside	in	
12	✓	any	any	PPTP-Control	outside	in	
13	None	None	133.2.6.0/28	10.2.2.2	outside	in	
14	✓	None	10.4.3.0/26	10.1.1.100	outside	in	

Device View

Device-Centric View

Device: Cat6500_FW_4_fw-dragon Policy: Access Rules
Shared Policy in use : TestPolicy2 Assigned to : 5 Device(s)

Filter (none)

No.	Permit	Category	Source	Destination	Service	Interface	Dir.	Options	De
▶ TestPolicy - Mandatory (1 Rule)									
▶ TestPolicy2 - Mandatory (Empty)									
▼ TestPolicy2 - Default (29 Rules)									
1	⊘	None	any	TestNet	tcp/588	outside	in	LOG	
2	⊘	None	Tes...	any	tcp/322	outside	in	LOG	
3	✓	None	any	TestNet2	tcp/Web_Services.tcp...	outside	in	LOG	
	✓	Cat-B	any	any	PPTP-Data-GRE	outside	in	LOG	
	✓	Cat-B	any	any	IPSec-AH	outside	in	LOG	
	✓	Cat-B	any	any	IPSec-ESP	outside	in	LOG	
	✓	Cat-C	any	TestNet	SSH	outside	in	LOG	
	✓	Cat-C	any	TestNet	Telnet	outside	in	LOG	
	✓	None	any	any	HTTPS	outside	in	LOG	
	✓	Cat-B	any	any	All-ICMP	outside	in	LOG	
12	✓	None	any					LOG	
13	⊘	None	133...					LOG	
14	✓	None	10.4...					LOG	
15	✓	None	any					LOG	
16	✓	None	any					LOG	

Context Menu:

- Device Properties...
- Show in Map View
- Copy Policies Between Devices...
- Share Device Policies...
- Catalyst 6500/7600 Device Manager...
- Show Containment...
- Preview Configuration...
- Delete Device...
- Discover Policies on Device...

Callout Box:

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

Buttons: Query Conflicts HitCount Save

Policy-Centric View

The screenshot displays the Cisco CS Manager interface in a Policy-Centric View. The left pane shows a tree of Policy Types, including Firewall, Access Rules, Inspection Rules, AAA Rules, Web Filter Rules (PIX/FWSM), Web Filter Rules (IOS), Transparent Rules, Settings, and NAT (PIX). The main pane shows the details for the selected 'EngineeringPolicy' (Policy Type: Access Rules). The table below lists the rules for this policy, categorized into CorporatePolicy - Mandatory (2 Rules), EngineeringPolicy - Mandatory (2 Rules), EngineeringPolicy - Default (1 Rule), and CorporatePolicy - Default (Empty).

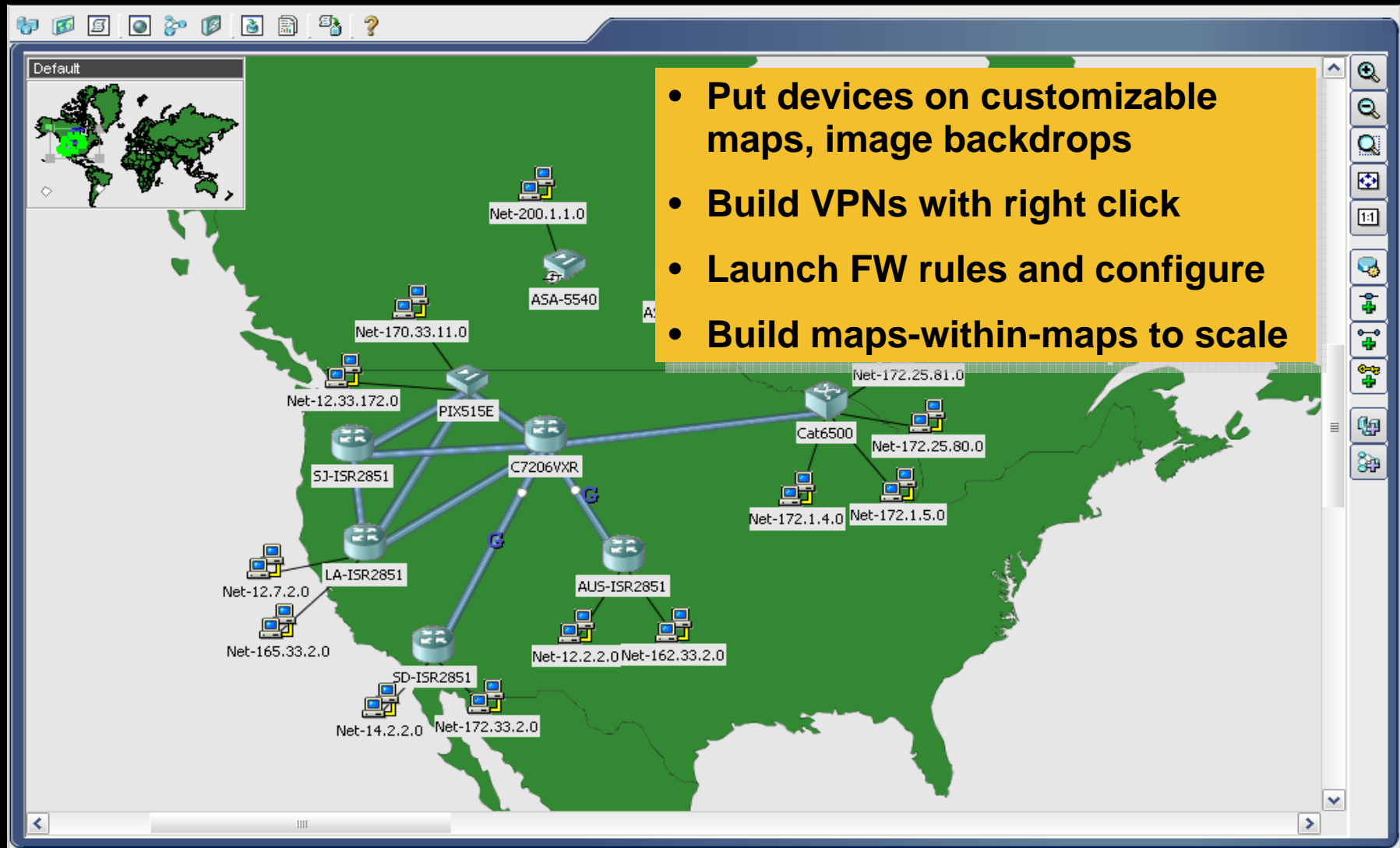
No.	Permit	Category	Source	Destination	Service	Interface	Dir.	Options	Description
CorporatePolicy - Mandatory (2 Rules)									
1	⊘	Cat-E	any	any	Telnet	All-Int...	in	LOG	
2	✓	Cat-E	any	any	HTTP HTTPS ICMP-Echo	All-Int...	in	LOG	
EngineeringPolicy - Mandatory (2 Rules)									
1	⊘	Cat-B	any	Engine...	FTP	All-Int...	in	LOG	
2	✓	Cat-B	any	any	NetMeeting	All-Int...	in	LOG	
EngineeringPolicy - Default (1 Rule)									
1	✓	Cat-C	any	any		All-Int...	in	LOG	
CorporatePolicy - Default (Empty)									

A context menu is open over the 'EngineeringPolicy' in the tree view, showing options: Save Policy As..., Rename Policy..., Edit Policy Inheritance..., New Access Rules Policy..., and Delete Policy... A yellow callout box points to this menu with the following text:

- Centralized policy management
- Powerful scalability via inheritance, reuse, assignment, and sharing

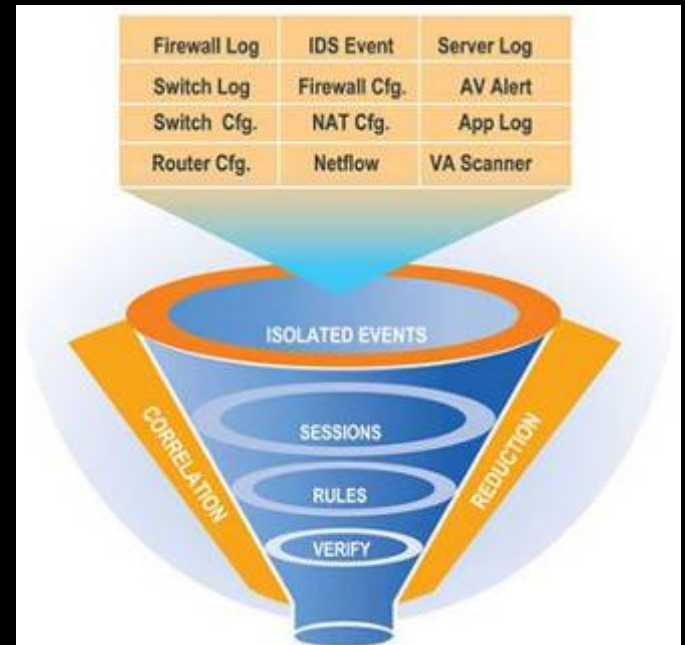
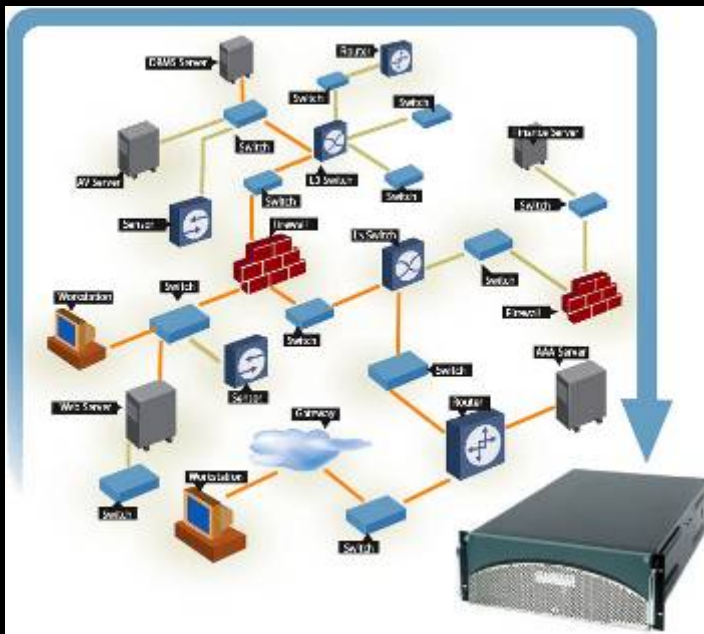
The bottom of the interface includes buttons for Query, Conflicts, HitCount, and a Save button.

Topology-Centric View



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

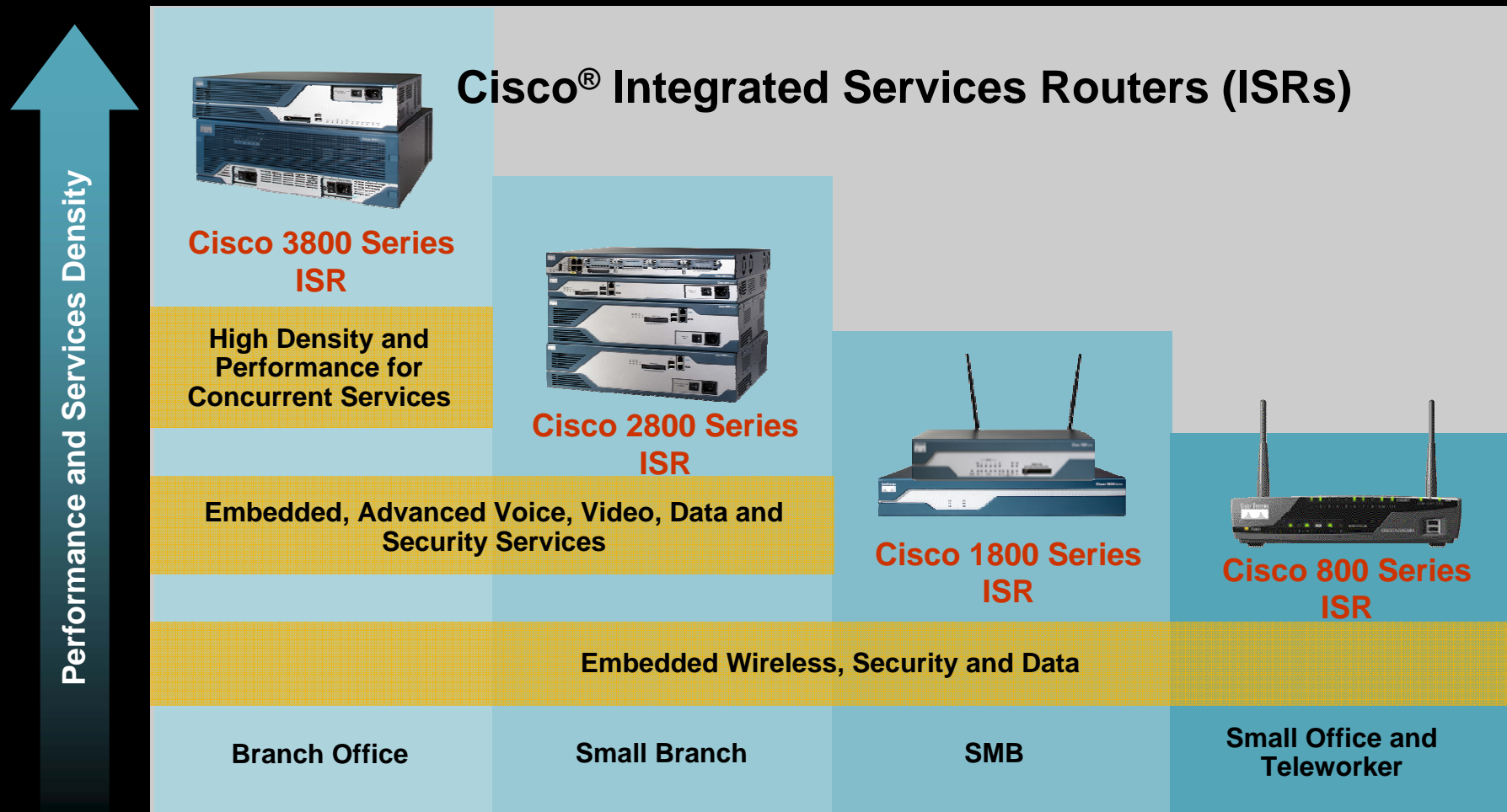


Key Features

- 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





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 compromising productivity.



security without

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

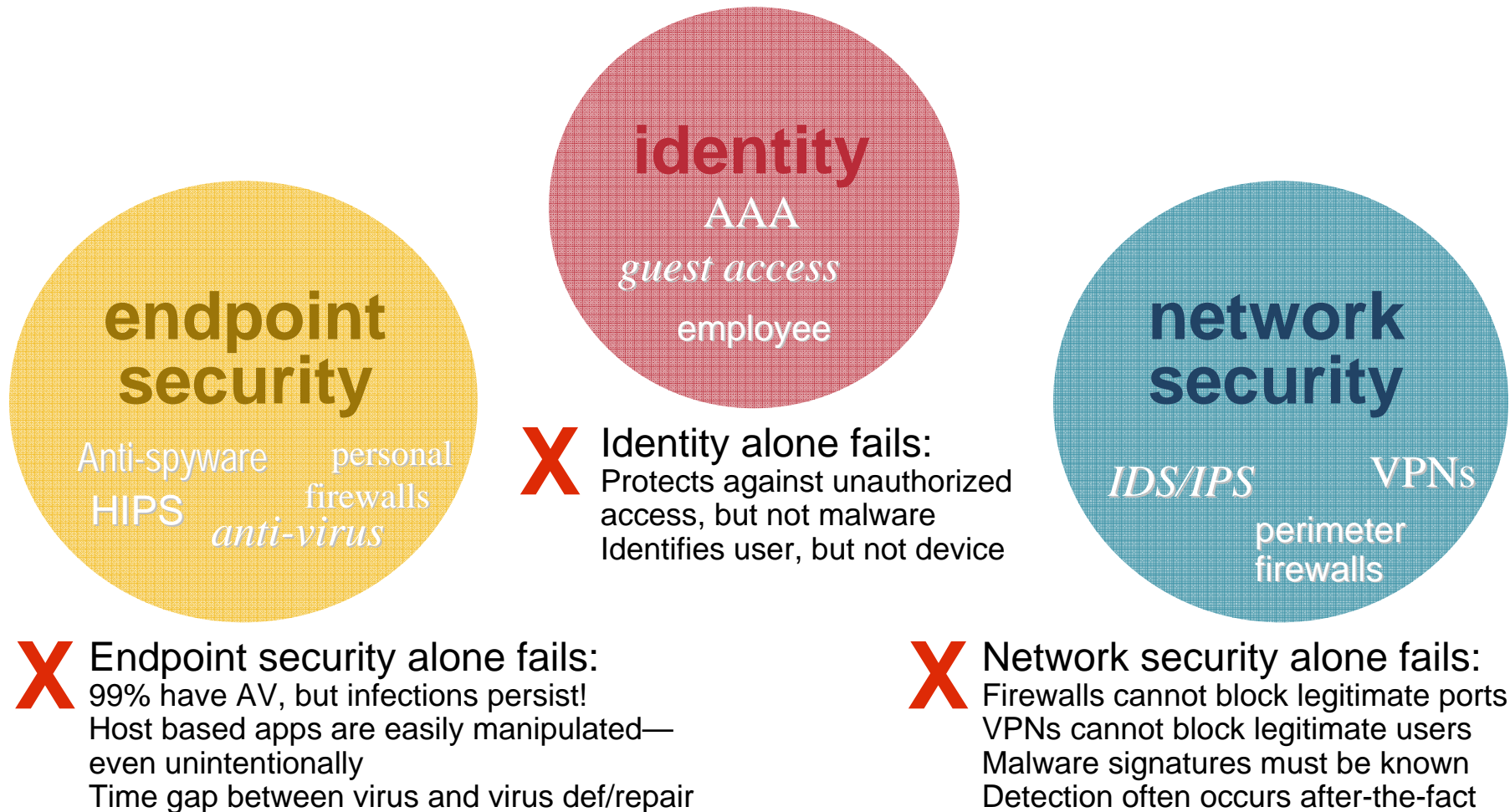
WHAT'S ON IT?
IS IT RUNNING?

Anti-virus, anti-spyware
Personal firewall
Patching tools

WHAT'S THE PREFERRED WAY TO CHECK/FIX IT?

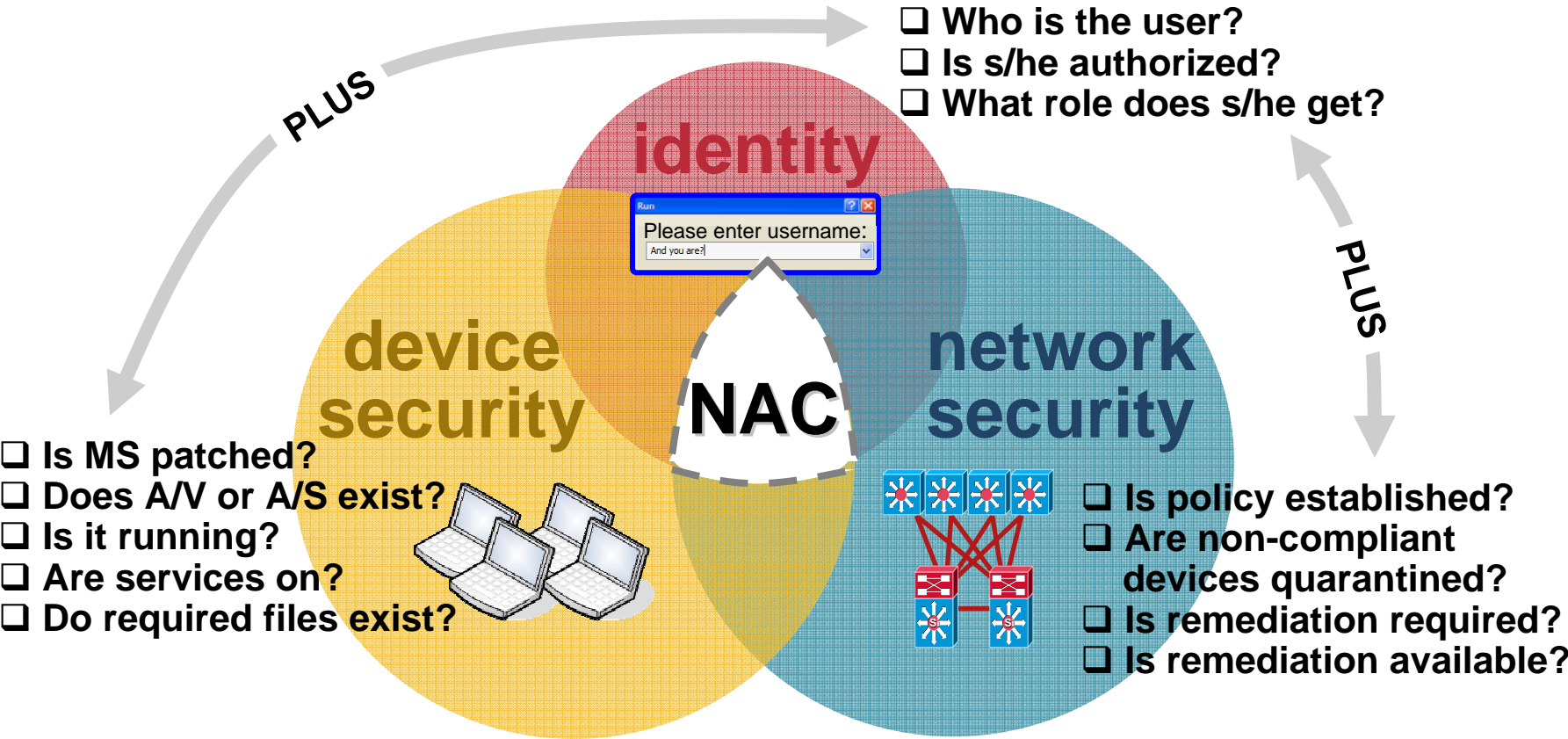
Pre-configured checks
Customized checks
Self-remediation or auto-remediation
Third-party software

Complexity Demands Defense-in-Depth



What Is Network Admission Control?

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



Four Key Capabilities of NAC

	SECURELY IDENTIFY DEVICE & USER	ENFORCE CONSISTENT POLICY	QUARANTINE AND REMEDIATE	CONFIGURE AND MANAGE
WHAT IT MEANS	Uniquely identifies users and devices, and creates associations between the two	Assess and enforce a ubiquitous policy across the entire network	Acts on posture assessment results, isolates device, and brings it into compliance	Easily creates comprehensive, granular policies that map quickly to user groups and roles
WITHOUT IT . . .	Critical to associate users and devices with roles to know which policies apply; prevents device spoofing.	A decentralized policy mechanism (e.g. on endpoint) can leave gaping security holes.	Just knowing a device is non-compliant is not enough—someone still needs to fix 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.

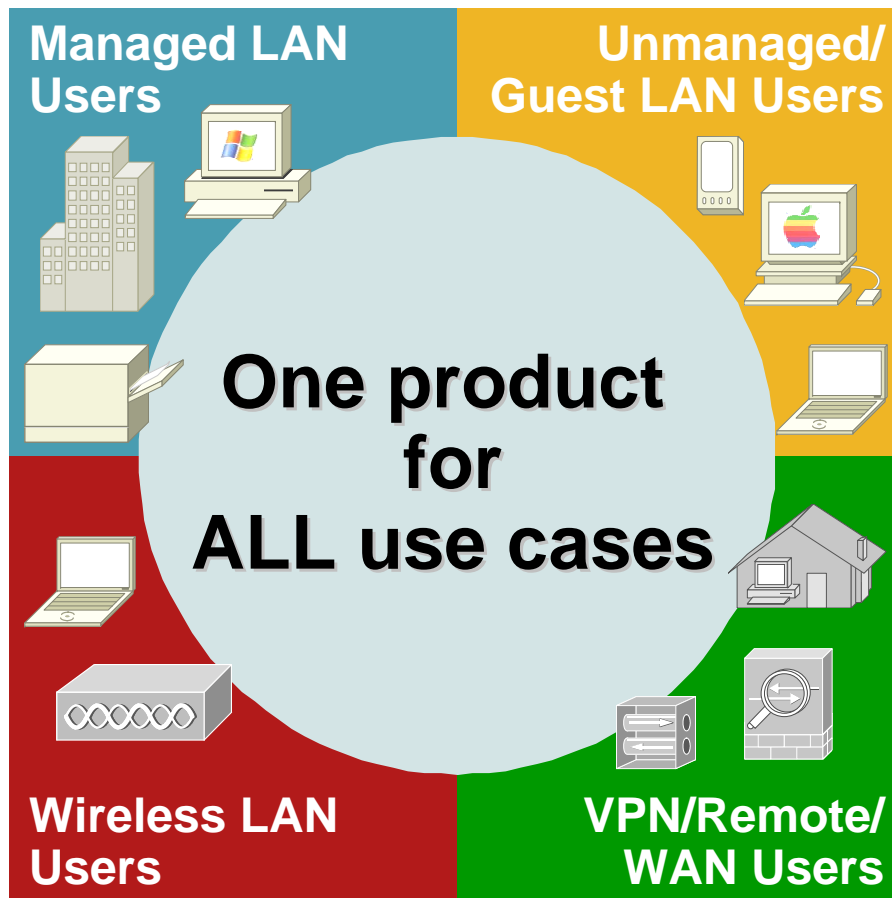
Agenda

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.



2.

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

3.

Most deployments ready under 5 days

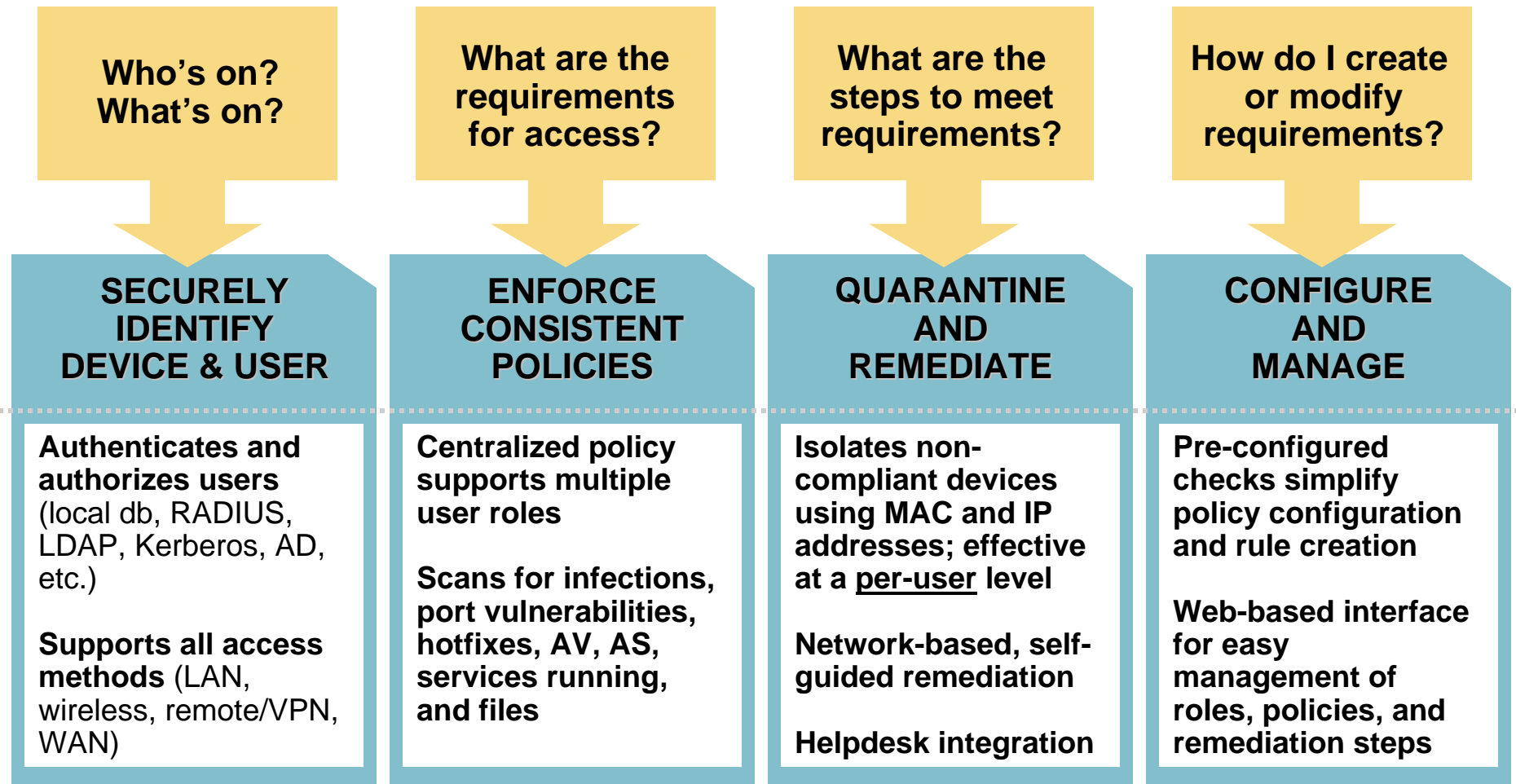
4.

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

5.

Does not require infrastructure upgrade

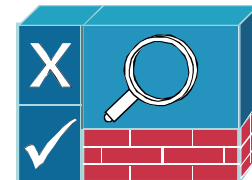
Clean Access Enforces Compliance



Clean Access Components

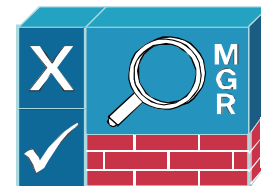
- Cisco Clean Access Server

Serves as an in-band or out-of-band device for network access control



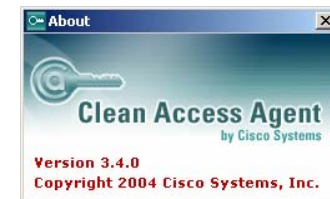
- Cisco Clean Access Manager

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



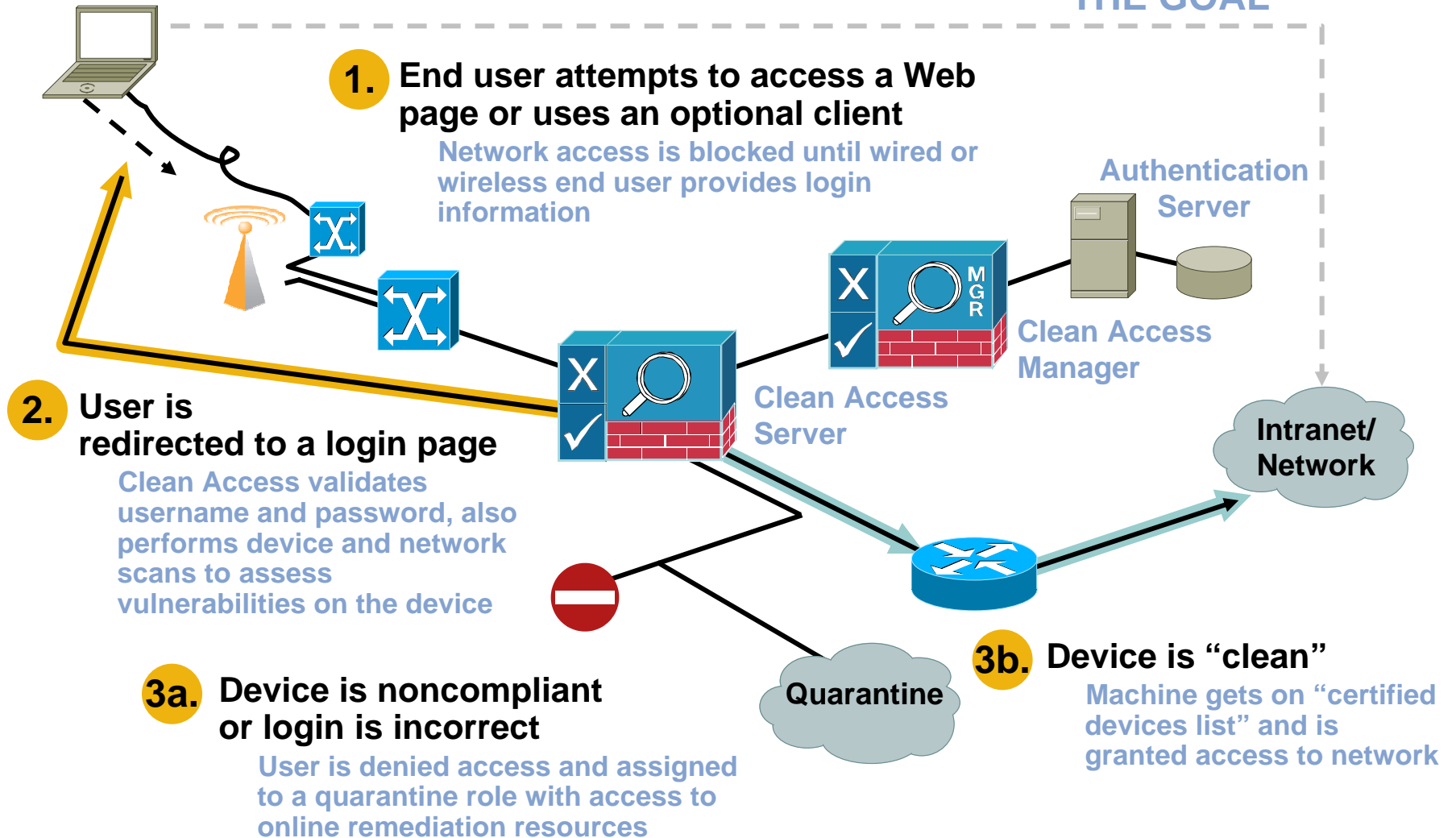
Anti-Spyware Updates
Other 3rd Party Checks



Customers can easily add customized checks

Product User Flow Overview

THE GOAL



User Experience with Agent

Login Screen



Cisco Clean Access Agent

Clean Access Agent

Please enter your user name and password:

User Name :

Password :

Remember Me

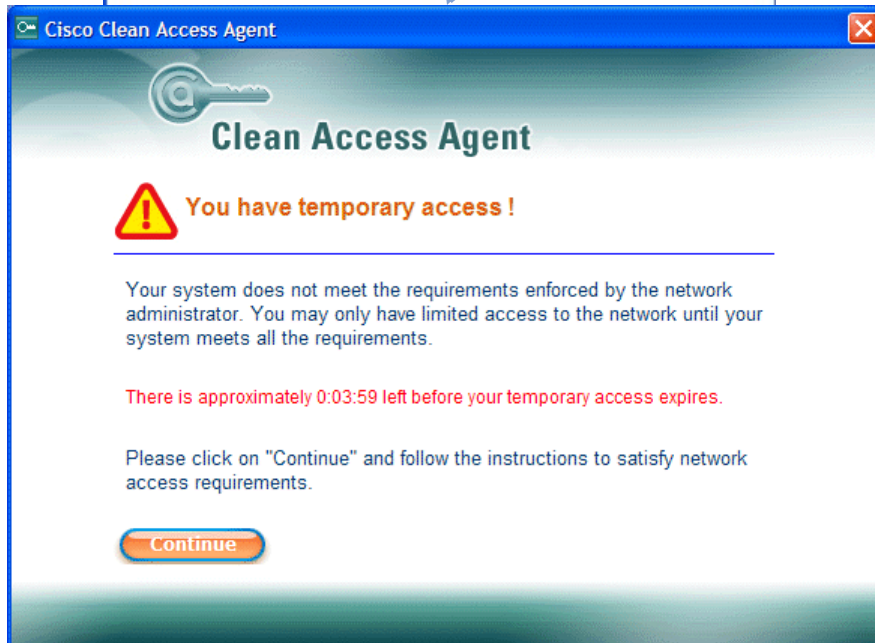
Please select your authentication provider:

Local DB

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

Scan fails

Remediate



Cisco Clean Access Agent

Clean Access Agent

⚠ 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.

Continue



Cisco Clean Access Agent

Clean Access Agent

⚠ Please download and install the required software before accessing the network.

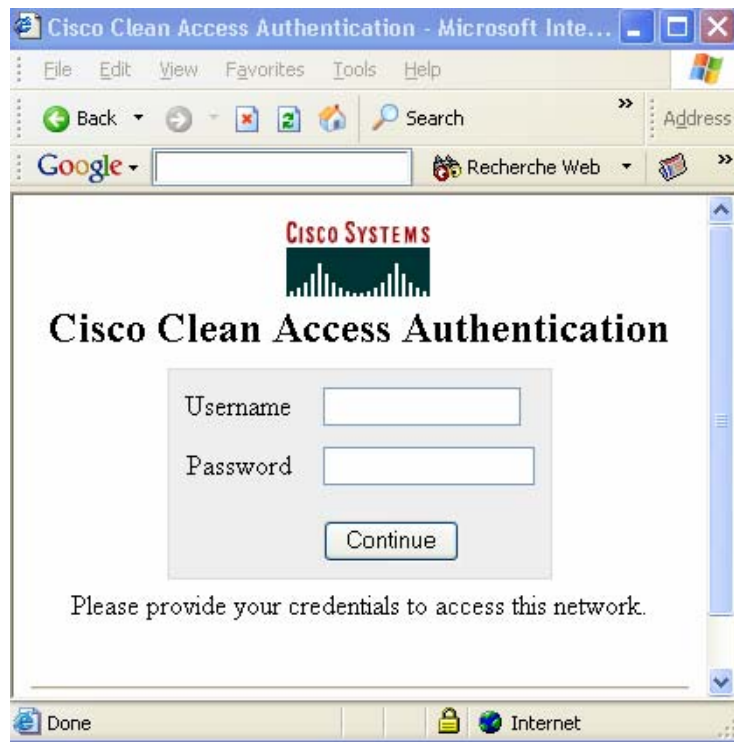
Required Software (0:03:10 left)

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.

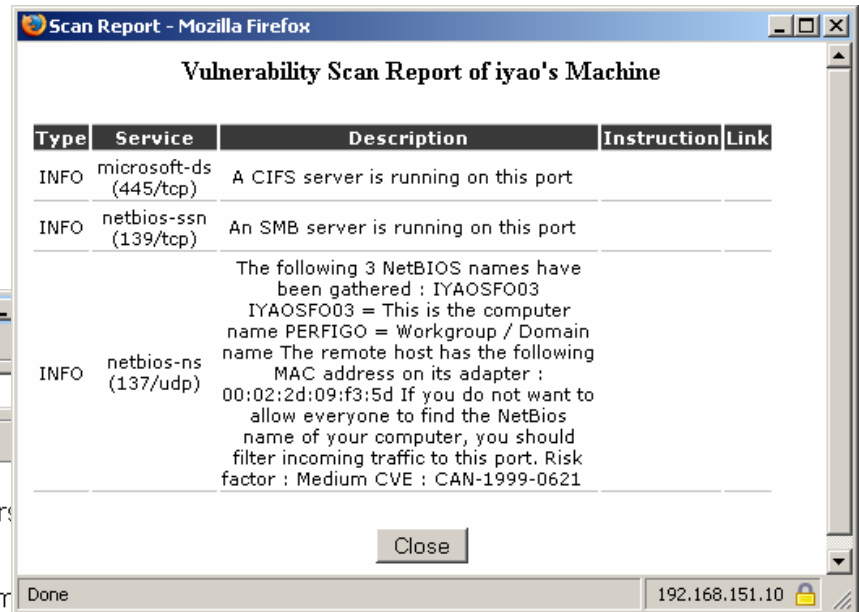
Go To Link **Next** **Cancel**

User Experience via Web Browser



Login Screen

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



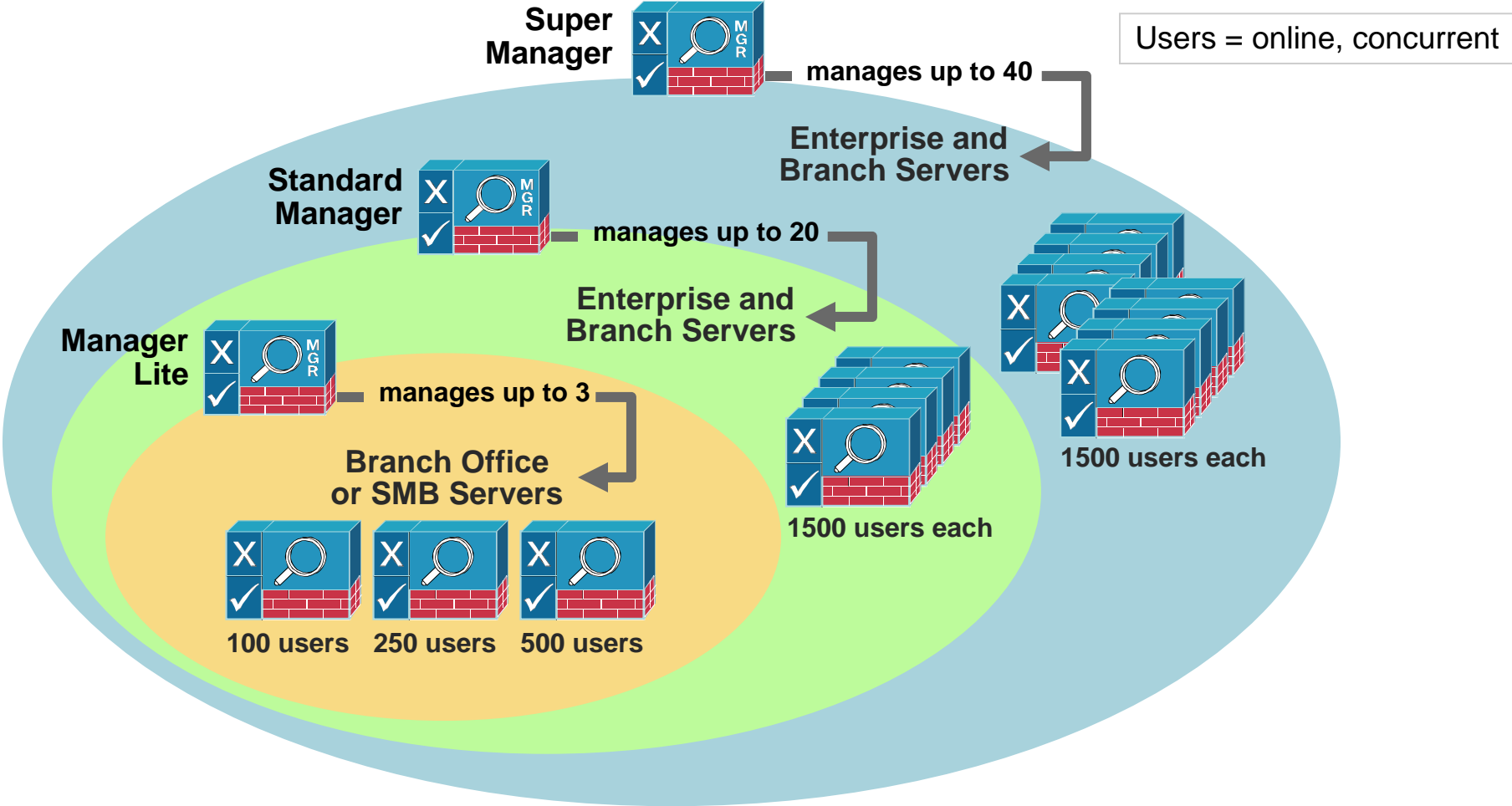
Guided self-remediation

Note that all existing anti-virus software should be removed from your computer before installing the Anti-Virus software. For complete installation instructions, see the How-To document.

The ITS Support Center will be delighted to answer any questions you have about the procedure. Contact

Accept Decline

Clean Access Sizing



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

Cisco Clean Access Manager Version 3.6.2

- 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

CAM Manages All Clean Access Servers

Cisco Clean Access Standard Manager Version 4.1.0

Device Management > Clean Access Servers > 192.168.3.2

Enable L3 support
 Enable L3 strict mode to ... Access Agent
 Enable L2 strict mode to ... ess Agent

Trusted Interface (to protected network)

IP Address	192.168.3.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.3.1
<input checked="" type="checkbox"/> Set management VLAN ID:	10
<input type="checkbox"/> Pass through VLAN ID to managed network	

Untrusted Interface (to managed network)

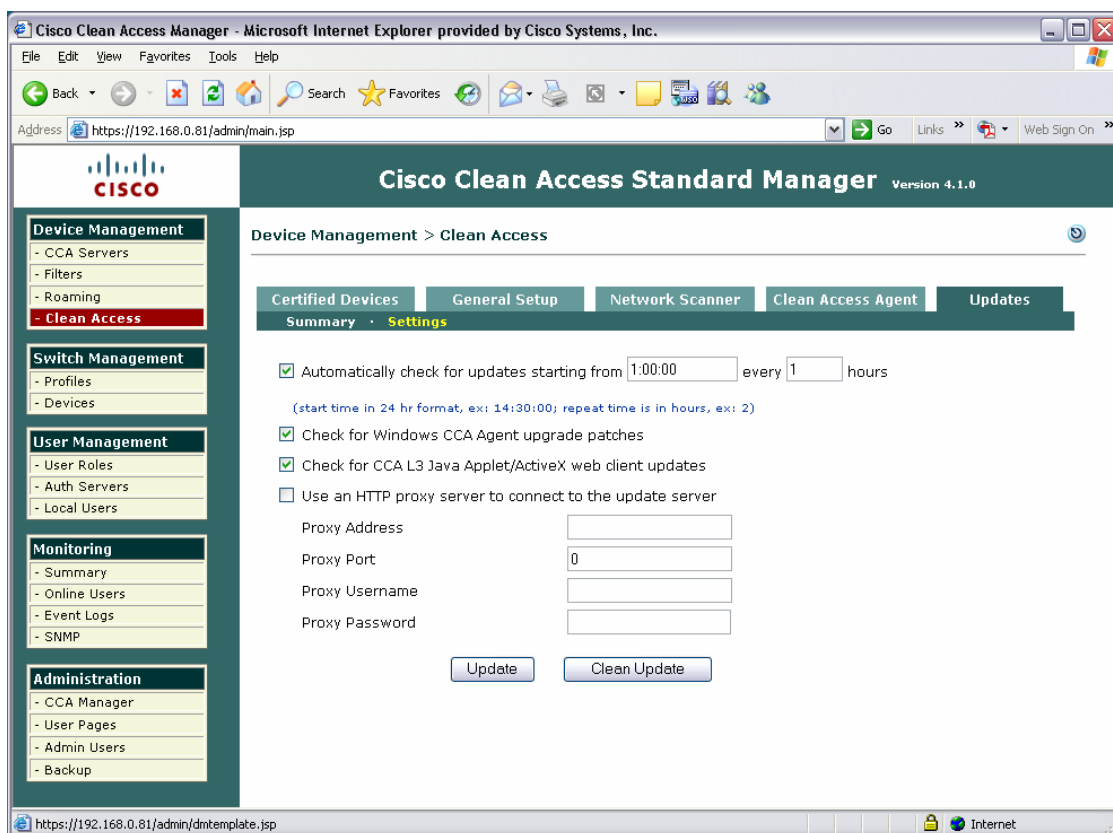
IP Address	192.168.3.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.3.1
<input type="checkbox"/> Set management VLAN ID:	0
<input type="checkbox"/> Pass through VLAN ID to protected network	

(Make sure the Clean Access Server is on VLAN n before you set its management VLAN ID to n.)

Update Reboot

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

Posture Validation Overview

Clean Access posture validation is a hierarchical process with either pre-loaded or custom profiles

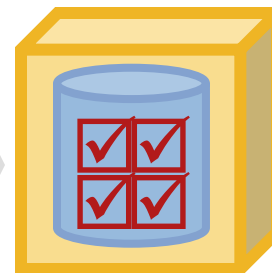
CHECKS
assess the state of a file, application, service, or registry key



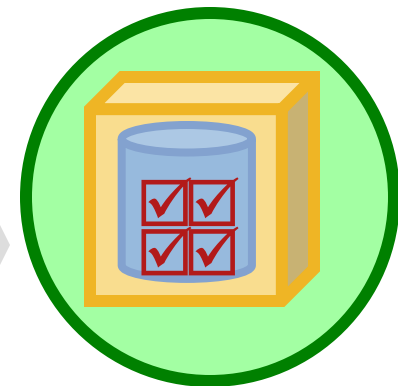
RULES
contain single or multiple **Checks**



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
AND
Anti_Spyware_UptoDate_Check
AND
Anti_Spyware_Running_Check

How Checks Look in the Manager

This is an example of a registry key CHECK for a Windows Hotfix:

The screenshot displays the Cisco Clean Access Standard Manager web interface. The browser window title is "Cisco Clean Access Manager - Microsoft Internet Explorer provided by Cisco Systems, Inc." and the address bar shows "https://192.168.0.81/admin/main.jsp". The page header includes the Cisco logo and "Cisco Clean Access Standard Manager Version 4.1.0". The main navigation menu on the left includes sections for Device Management, Switch Management, User Management, Monitoring, and Administration. The "Clean Access" option under Device Management is highlighted. The main content area shows the "Device Management > Clean Access" page with tabs for Certified Devices, General Setup, Network Scanner, Clean Access Agent, and Updates. The "Rules" tab is active, showing a "View Check" link. The check configuration form includes: Check Category: Registry Check; Check Type: Registry Key; Check Name: pc_Hotfix323255_98; Registry Key: HKLM \ Software\Microsoft\Active Setup\Installed Components; Operator: exists; Check Description: (empty); Operating System: Windows 98 (checked); and a note: "* Cisco created checks cannot be edited. Create a copy of the check if you intend to change it."

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

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites RSS Print Mail Stop

Address <https://192.168.0.81/admin/main.jsp> Go Links Web Sign On

CISCO

Cisco Clean Access Standard Manager Version 4.1.0

Device Management > Clean Access

- Device Management
 - CCA Servers
 - Filters
 - Roaming
 - **Clean Access**
- Switch Management
 - Profiles
 - Devices
- User Management
 - User Roles
 - Auth Servers
 - Local Users
- Monitoring
 - Summary
 - Online Users
 - Event Logs
 - SNMP
- Administration
 - CCA Manager
 - User Pages
 - Admin Users
 - Backup

Certified Devices | General Setup | Network Scanner | Clean Access Agent | Updates

Distribution · Installation · **Rules** · Requirements · Role-Requirements · Reports

Check List | **New Check** | Rule List | New Rule | New AV Rule | New AS Rule | AV/AS Support Info

Check Category: Service Check (dropdown)
Check Type: Service Status (dropdown)

Check Name:

Service Name:

Operator: running (dropdown)

Check Description:

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

Automatically create rule based on this check

Done Internet

How Rules Look in the Manager

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

The screenshot displays the Cisco Clean Access Standard Manager web interface. The browser window title is "Cisco Clean Access Manager - Microsoft Internet Explorer provided by Cisco Systems, Inc." and the address bar shows "https://192.168.0.81/admin/main.jsp". The page header includes the Cisco logo and "Cisco Clean Access Standard Manager Version 4.1.0".

The left sidebar contains navigation menus for Device Management, Switch Management, User Management, Monitoring, and Administration. The "Clean Access" option under Device Management is highlighted.

The main content area is titled "Device Management > Clean Access" and features a breadcrumb trail: "Distribution · Installation · Rules · Requirements · Role-Requirements · Reports". Below this is a "Support Info" section with links for "Check List", "New Check", "Rule List", "View Rule", "New AV Rule", "New AS Rule", and "AV/AS".

The "View Rule" configuration page shows the following details:

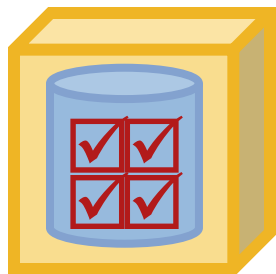
- Rule Name: pr_XP_Hotfixes
- Rule Description: Windows XP Hotfixes
- Operating System: Windows All, Windows 2000, Windows XP (All), Windows ME, XP Pro/Home, Windows 98, XP Tablet PC, XP Media Center
- Rule Expression: `pc_HotFix896423_XP&pc_HotFix901214_XP&pc_HotFix896424_XP&pc_HotFix896358_XP&pc_HotFix891781_XP&pc_HotFix902400_XP&pc_HotFix904706_XP&pc_HotFix912919_XP&pc_HotFix908519_XP&pc_KB908531_MS06-015_XP&pc_KB911280_MS06-025_XP&pc_KB914388_MS06-`

A help box on the right explains the rule expression syntax: "Use checks and operators to create an expression. If a rule condition is true, the client is considered in compliance with the rule. Operators are '&' (and), '|' (or), '!' (not), and '()' (eval priority parens). Ex: check1 & (check2 | check3)".

A note at the bottom states: "* Cisco created rules cannot be edited. Create a copy of the rule if you intend to change it." The page footer shows "Checks for Selected Operating System" and a status bar with "Done" and "Internet" icons.

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:

The screenshot displays the Cisco Clean Access Standard Manager web interface in Microsoft Internet Explorer. The browser title is "Cisco Clean Access Manager - Microsoft Internet Explorer provided by Cisco Systems, Inc." and the address bar shows "https://192.168.0.81/admin/main.jsp". The page header includes the Cisco logo and "Cisco Clean Access Standard Manager Version 4.1.0".

The left sidebar contains a navigation menu with the following sections:

- Device Management**
 - CCA Servers
 - Filters
 - Roaming
 - Clean Access
- Switch Management**
 - Profiles
 - Devices
- User Management**
 - User Roles
 - Auth Servers
 - Local Users
- Monitoring**
 - Summary
 - Online Users
 - Event Logs
 - SNMP
- Administration**
 - CCA Manager
 - User Pages
 - Admin Users
 - Backup

The main content area is titled "Device Management > Clean Access" and features several tabs: "Certified Devices", "General Setup", "Network Scanner", "Clean Access Agent", and "Updates". Under "Clean Access Agent", there are sub-tabs: "Distribution", "Installation", "Rules", "Requirements", "Role-Requirements", and "Reports". The "Requirements" sub-tab is active, showing a "Requirement List" and a "New Requirement" button.

The "New Requirement" form is filled out with the following details:

- Requirement Type: AV Definition Update
- Enforce Type: Mandatory
- Priority: 2
- Antivirus Vendor Name: McAfee, Inc.
- Requirement Name: McAfee AV Definition Update
- Description: You must download the latest McAfee Definition file
- Operating System: Windows All, Windows 2000, Windows XP (All), Windows ME, XP Pro/Home, Windows 98, XP Tablet PC, XP Media Center

An "Add Requirement" button is located at the bottom of the form. A note below the form states: "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."

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

File Edit View Favorites Tools Help

Address <https://192.168.0.81/admin/main.jsp> Go Links Web Sign On

Cisco Clean Access Standard Manager Version 4.1.0

Device Management

- CCA Servers
- Filters
- Roaming
- Clean Access

Switch Management

- Profiles
- Devices

User Management

- User Roles
- Auth Servers
- Local Users

Monitoring

- Summary
- Online Users
- Event Logs
- SNMP

Administration

- CCA Manager
- User Pages
- Admin Users
- Backup

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: AV Definition Update

*Note: Vendors without SOFTWIN, Zone Labs L requirement type (EarthLink, Inc., GData Software AG, Microsoft Corp., virus Vendor Name list.

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

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.

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

File Edit View Favorites Tools Help

Address: https://192.168.0.81/admin/main.jsp

Cisco Clean Access Standard Manager Version 4.1.0

Device Management

- CCA Servers
- Filters
- Roaming
- Clean Access

Switch Management

- Profiles
- Devices

User Management

- User Roles
- Auth Servers
- Local Users

Monitoring

- Summary
- Online Users
- Event Logs
- SNMP

Administration

- CCA Manager
- User Pages
- Admin Users
- Backup

Requirement Name: WindowsUpdate Operating System: Windows XP (All)

Requirement met if:

- WindowsUpdate succeeds
- McAfee succeeds
- CSA
- No selected rule succeeds

*Note: The service of providing regularly updated Spyware definition date/version is not available on the Cisco server yet. For AS Spyware Definition rules, the system has enforced the feature of allowing the definition file to be X days older than the current system date. Once the service is available, this note will be automatically removed.

For **AV Virus Definition rules**, allow definition file to be days older than

- the latest file date
- current system date

For **AS Spyware Definition rules**, allow definition file to be days older than

- the latest file date
- current system date

Rules for Selected Operating System Update

Select	Name	OS
<input checked="" type="checkbox"/>	pr_AutoUpdateCheck_Rule	Win (XP (All), 2000)
<input type="checkbox"/>	pr_Symantec_Client_Firewall_Enable	Win (XP (All))
<input type="checkbox"/>	pr_Symantec_Norton_Installation	Win (All)
<input type="checkbox"/>	pr_Symantec_Norton_Application	Win (All)
<input type="checkbox"/>	pr_Symantec_Norton_Update	Win (All)
<input type="checkbox"/>	pr_McAfee_Installation	Win (All)

Done Internet



Cisco Clean Access Standard Manager Version 4.1.0

Device Management

- CCA Servers
- Filters
- Roaming
- Clean Access**

Switch Management

- Profiles
- Devices

User Management

- User Roles
- Auth Servers
- Local Users

Monitoring

- Summary
- Online Users
- Event Logs
- SNMP

Administration

- CCA Manager
- User Pages
- Admin Users
- Backup

Device Management > Clean Access

- Certified Devices**
 - General Setup
 - Network Scanner
 - Clean Access Agent
 - Updates
- Distribution · Installation · Rules · Requirements · **Role-Requirements** · Reports

Role Type User Role

Select requirements to associate with the role

Select	Name	OS
<input checked="" type="checkbox"/>	WindowsUpdate	Win (XP (All))
<input checked="" type="checkbox"/>	McAfee	Win (All)
<input checked="" type="checkbox"/>	CSA	Win (All)

How Roles Look in the Manager

Fine-tuning for timers, agents, and policies on a per-ROLE basis:

The screenshot displays the Cisco Clean Access Standard Manager web interface in Microsoft Internet Explorer. The browser title is "Cisco Clean Access Manager - Microsoft Internet Explorer provided by Cisco Systems, Inc." and the address bar shows "https://192.168.0.81/admin/main.jsp". The page title is "Cisco Clean Access Standard Manager Version 4.1.0".

The interface features a left-hand navigation menu with the following sections:

- Device Management**
 - CCA Servers
 - Filters
 - Roaming
 - Clean Access
- Switch Management**
 - Profiles
 - Devices
- User Management**
 - User Roles
 - Auth Servers
 - Local Users
- Monitoring**
 - Summary
 - Online Users
 - Event Logs
 - SNMP
- Administration**
 - CCA Manager
 - User Pages
 - Admin Users
 - Backup

The main content area shows configuration options for a "Regular user" role. The "User Role" dropdown is set to "Regular user" and the "Operating System" dropdown is set to "ALL". A note states: "(By default, 'ALL' settings apply to all client operating systems if no OS-specific settings are specified.)"

The configuration options include:

- Require use of Clean Access Agent (for Windows & Macintosh OSX only)
 - Clean Access Agent Download Page Message (or URL): `Network Security Notice: This network is protected by the Clean Access Agent, a component of the Cisco Clean Access Suite. The Clean Access Agent ensures that your`
- Allow restricted network access in case user cannot use Clean Access Agent
 - Restricted Access User Role: Regular user
 - Restricted Access Button Text: Get Restricted Network Access
 - Restricted Network Access Message: `Restricted Network Access: If you cannot use the Clean Access Agent, you can obtain restricted network access temporarily by clicking the button below. Please`
- Show Network Policy to Clean Access Agent users (for Windows only)
 - Network Policy Link: [Empty field]
- Logoff Clean Access Agent users from network on their machine logoff or shutdown (for Windows & In-Band setup)
 - Refresh Windows domain group policy after login (for Windows only)
 - Automatically close login success screen after 0 SECS (for Windows only) (Setting the time to zero secs will not display the login success screen. Valid range: 0 - 300 secs.)
 - Automatically close logout success screen after 0 SECS (for Windows only) (Setting the time to zero secs will not display the logout success screen. Valid range: 0 - 300 secs.)

How Roles Look in the Manager

More options based on user **ROLE** (called "FTE" in this case):

The screenshot displays the Cisco Clean Access Standard Manager web interface in Microsoft Internet Explorer. The browser title is "Cisco Clean Access Manager - Microsoft Internet Explorer provided by Cisco Systems, Inc." and the address bar shows "https://192.168.0.81/admin/main.jsp". The page header includes the Cisco logo and "Cisco Clean Access Standard Manager Version 4.1.0".

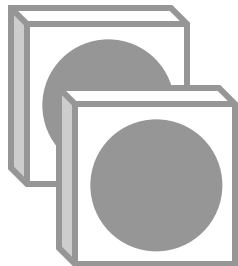
The left sidebar contains a navigation menu with the following sections:

- Device Management**
 - CCA Servers
 - Filters
 - Roaming
 - Clean Access
- Switch Management**
 - Profiles
 - Devices
- User Management**
 - **User Roles** (highlighted)
 - Auth Servers
 - Local Users
- Monitoring**
 - Summary
 - Online Users
 - Event Logs
 - SNMP
- Administration**
 - CCA Manager
 - User Pages
 - Admin Users
 - Backup

The main content area shows the configuration for a role named "FTE". The configuration includes:

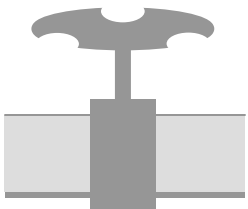
- Disable this role
- Role Name: FTE
- Role Description: Full Time Employees
- Role Type: Normal Login Role
- *VPN Policy: Deny
- *Dynamic IPSec Key: Enable Disable
- *Max Sessions per User Account (Case-Insensitive): 0 (1 - 255; 0 for unlimited)
- Retag Trusted-side Egress Traffic with VLAN (In-Band): (0 - 4095, or leave it blank)
- *Out-of-Band User Role VLAN: VLAN ID
- *After Successful Login Redirect to: previously requested URL
- this URL: (e.g. <http://www.cisco.com/>)
- Redirect Blocked Requests to: default access blocked page
- this URL or HTML message:
- *Roam Policy: Deny Allow
- *Show Logged-on Users: IPSec info PPP info
- User info Logout button

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:

The screenshot shows the Cisco Clean Access Standard Manager web interface. The left sidebar contains navigation menus for Device Management, Switch Management, User Management (with 'User Roles' selected), Monitoring, and Administration. The main content area displays a list of filters for the 'IP - Host' category, filtered by 'All Roles' and 'Untrusted -> Trusted'. The filters are organized into four sections: Unauthenticated Role, Temporary Role, Quarantine Role, and Regular user. Each section contains a table with columns for Action, Protocol, Untrusted, and Trusted, along with Enable, Edit, Del, and Move buttons.

Unauthenticated Role				Enable	Edit	Del	Move
Allow	UDP	DNS†					
Block	ALL						

Temporary Role				Enable	Edit	Del	Move
Allow	TCP	*,*	192.168.0.81 /255.255.255.255 :80	<input checked="" type="checkbox"/>			
Block	ALL						

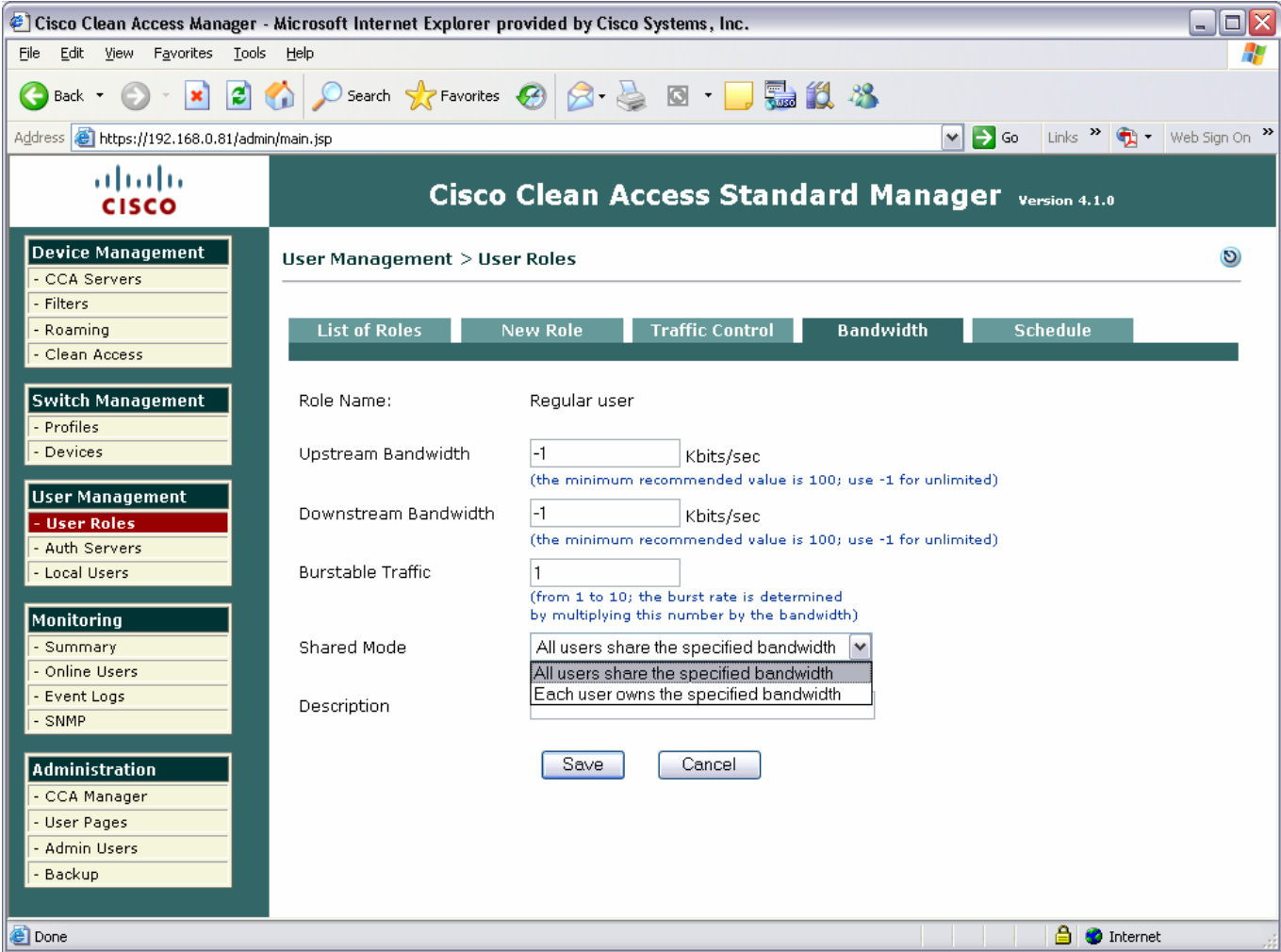
Quarantine Role				Enable	Edit	Del	Move
Block	ALL						

Regular user				Enable	Edit	Del	Move
Allow	ALL TRAFFIC	*	*	<input checked="" type="checkbox"/>			
Block	ALL						

(† DNS in Real-IP and NAT Gateway; DNS/DHCP in Virtual Gateway)
 (* All policies other than unauthenticated role)

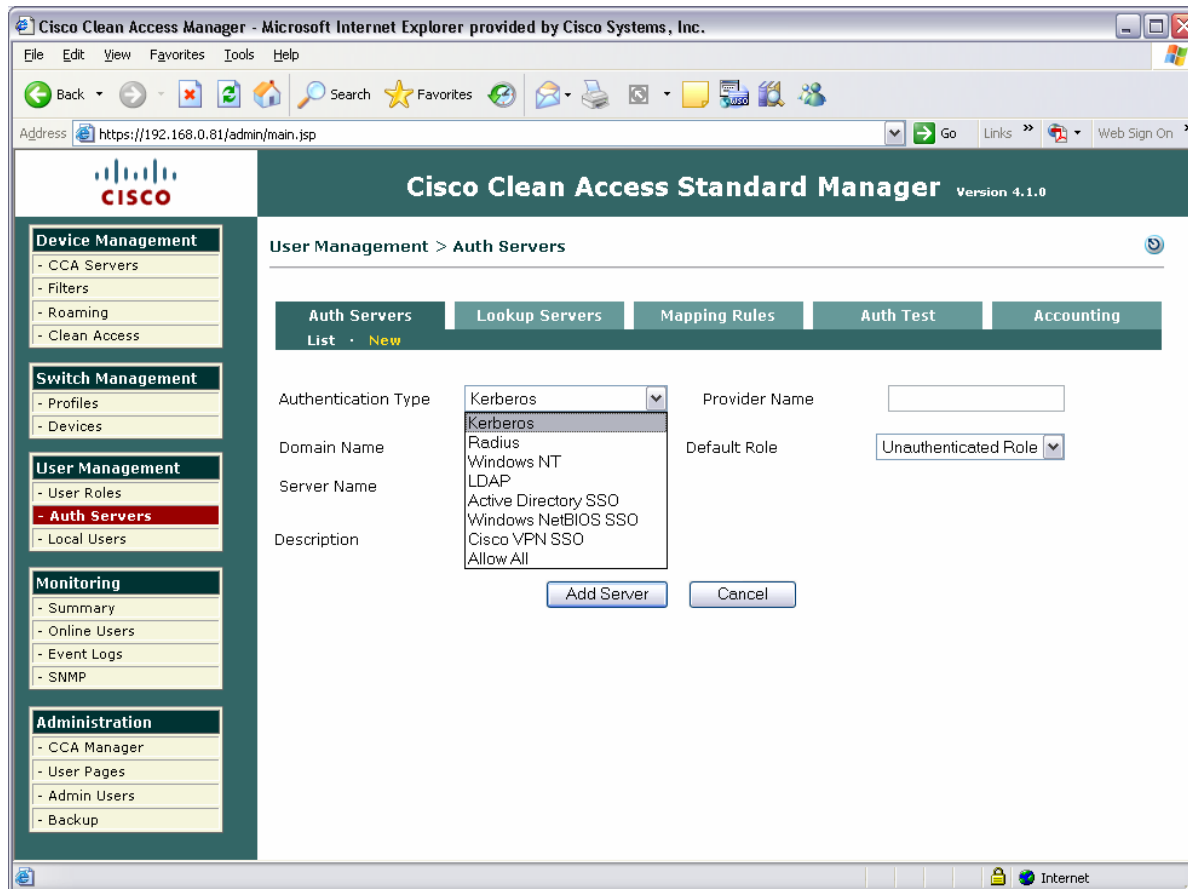
How Bandwidth Controls Look

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

USER

ADMIN

Cisco Clean Access Agent

Clean Access Agent

⚠ 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.

Continue

Cisco Clean Access Manager Version 3.5.2

Monitoring > Online Users

View Online Users | Display Settings

Any CCA Server | Any Provider | Any Role

Search For: - Select Field - | equals

View | Reset View | Kick Users

Active users: 1 (Max users since last reset: 1) | Reset Max Users

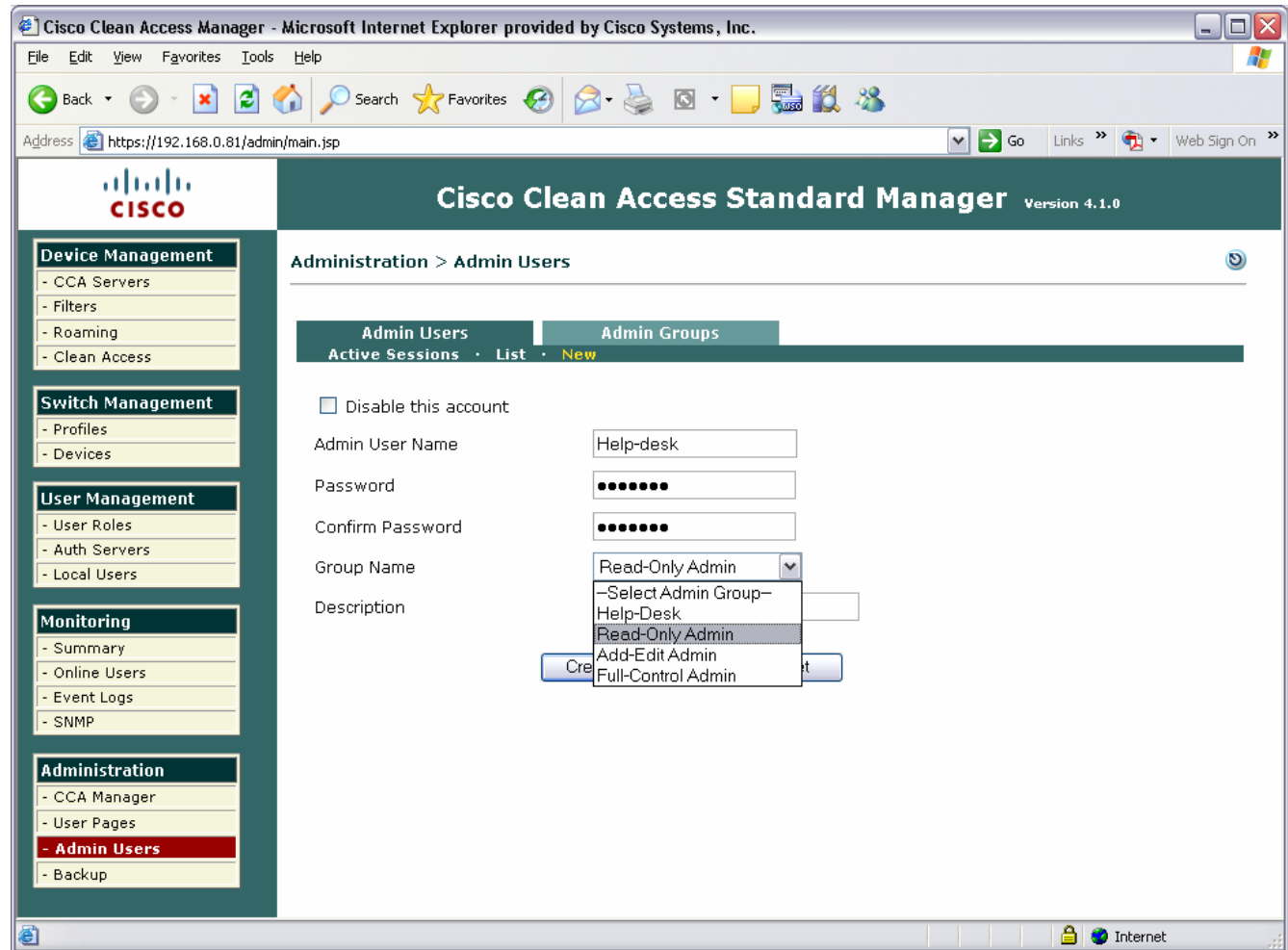
Online Users 1 - 1 of 1 | First | Previous | Next | Last |

User Name	User IP	User MAC	Provider	Role	VLAN	OS	
consultant	10.10.10.202	00:0C:29:72:46:90	Local DB	Quarantine Role	N/A	Windows XP	

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

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



Q&A

