Identity Management and Network Admission Control

Riyadh
March 2004

Franjo Majstor
Consulting Engineer
Cisco Systems, Inc.

Agenda

Cisco.com

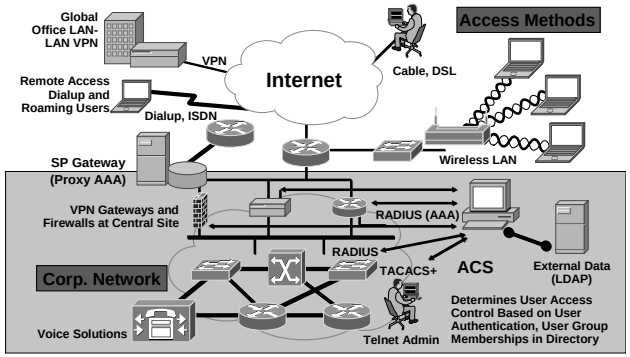
- IBNS Introduction
- Introduction to NAC
- Traditional Prevention Mechanisms
- Innovative approach
- Summary

Cisco.com

IBNS Introduction

Identity Based Networking Services

Cisco.com



IEEE 802.1x Defined

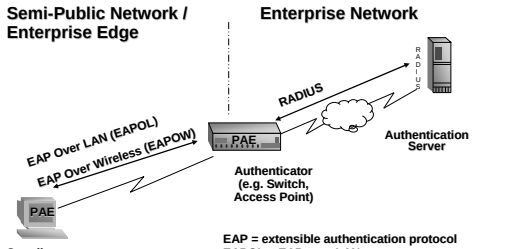
Port based network access control

Cisco.com

- 802.1x is an IEEE Standard for Port Based Network Access Control
- Falls under 802.1 NOT 802.11
- NETWORK standard, not a wireless standard
- Provides Network Authentication, NOT encryption
- Improved authentication: different methods
- Works on 802.3 LAN switch or 802.11b WLAN AP
- To be used for centralized user administration

IEEE 802.1x Terminology

Cisco.com

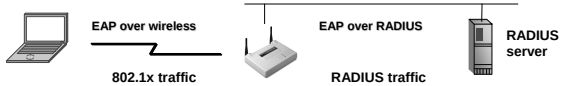


EAP = extensible authentication protocol
EAPOL = EAP over LANs
PAE = port access entity
Port = network access port
RADIUS = remote authentication dial in user service

Before EAP Start

Cisco.com

802.11 association complete; data blocked by AP



AP encapsulates 802.1x traffic into RADIUS traffic, and visa versa

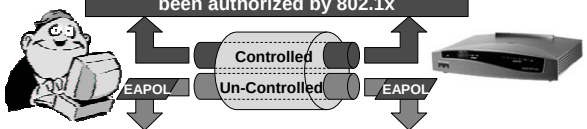
AP blocks everything but 802.1x-to-RADIUS authentication traffic

How Does 802.1x Work?

Cisco.com

For each 802.1x switch port, the switch creates TWO virtual access points at each port

The controlled port is open only when the device connected to the port has been authorized by 802.1x



Uncontrolled port provides a path for Extensible Authentication Protocol over LAN (EAPOL) traffic ONLY

EAP Defined - RFC 2284

Cisco.com

- Extensible Authentication Protocol is a extension of CHAP/PAP within PPP

  Support multiple "authentication" schemes:

  - plain password hash (MD5)
  - token cards
  - GSS-API (Kerberos)
  - TLS (based on X.509 certificates)

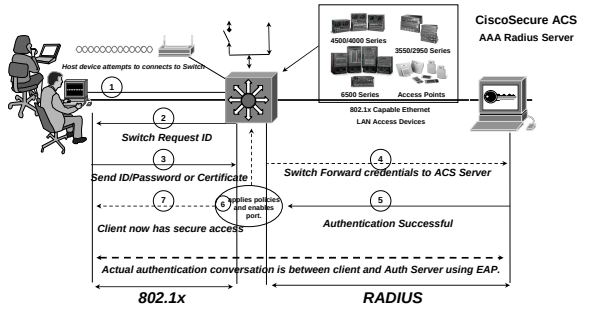
802.1x Extensible Authentication Protocols

Cisco.com

- **EAP-MD5 (Message Digest 5)**
  - Supported in Win 2K/XP and other Windows versions
  - Does ***not*** provide ***mutual*** authentication ***nor WEP key derivation***
- **EAP-Cisco Wireless, or LEAP**
  - Supported client in WinXP/2K/NT/ME/98/95/CE, Linux, Mac, DOS.
  - Provides ***mutual*** authentication and ***WEP key derivation***
- **EAP-TLS (mutual EAP-TLS)**
  - Supported in Win 2K/XP and other Windows versions
  - Requires ***client certificates*** and ***server certificates***
- **PEAP**
  - Supported in XP and W2K
  - Uses server-side TLS, which requires ***only server certificates***
- **EAP-MSCHAPv2**
  - Uses username/password MSCHAPv2 authentication
- …

Secure Identity-Based Network Access

Cisco.com



The switch detects the 802.1x compatible client, forces authentication, then acts as a middleman during the authentication, Upon successful authentication the switch sets the port to forwarding, and applies the designated policies.

IBNS - Secure Mobility & Workforce Optimization and Enhanced Productivity

Cisco IBNS Features and Benefits

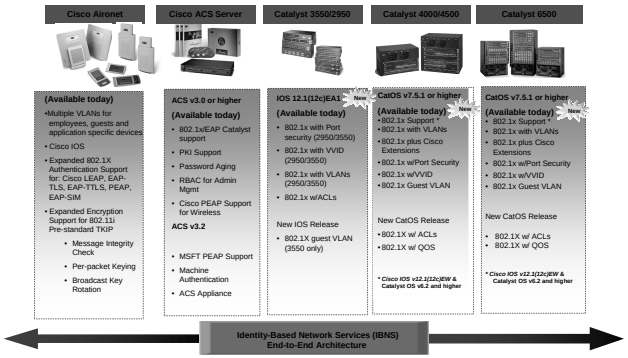
Cisco.com

- **IBNS Extensions**
  - Basic IEEE 802.1x Support
  - 802.1x with VLANs
  - 802.1x with Port Security
  - 802.1x with VVID
  - 802.1x Guest VLANs
  - 802.1x with Arp Inspection (New)
  - 802.1x with DHCP (New)
  - 802.1x with ACLs (3550)
  - 802.1x with Security Profile (Soon)
  - 802.1x Accounting Enhancements

- **Enhanced Port Based Access Control**
- **Greater flexibility and mobility for a stratified user community**
- **Enhanced User Productivity**
- **Added support for converged VoIP networks**

Identity Based Networking Services

Cisco.com



802.1x Client Support

Cisco.com

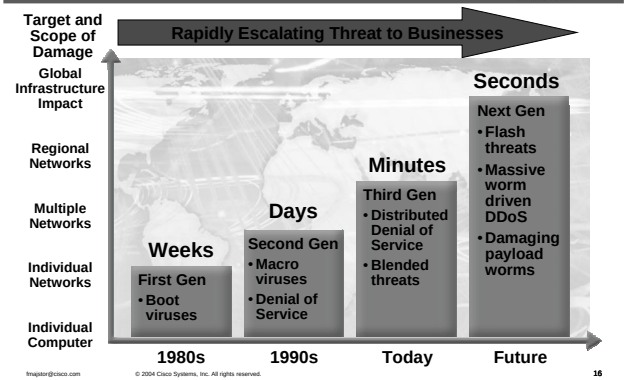
- **What endpoints are being covered?**
  - Windows XP - Yes
  - Windows 2000 - Yes
  - Linux - Yes
  - HP-UX - Yes
  - Solaris - Yes
  - HP Printers - Yes
  - Windows ME - Limited
  - Windows 98 - Limited
  - Windows NT4 - Limited
  - Apple - OS X v1.3
  - Pocket PC - New (Peap & TLS)
  - 3rd Party: Meeting House, Funk

Cisco.com

Introduction to NAC

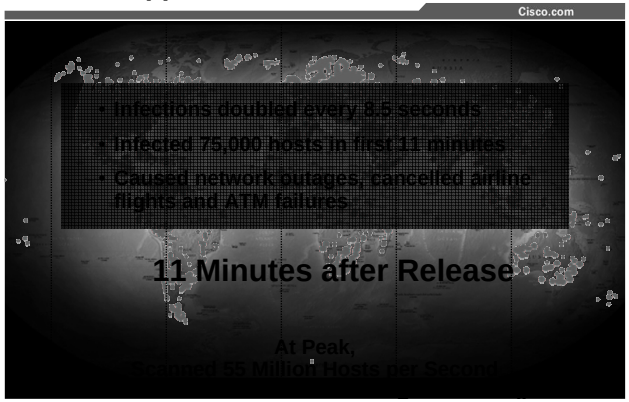
Threat Levels Evolution

Cisco.com



The Sapphire Worm or "Slammer"

Cisco.com



Problem Statement

Cisco.com

- **VU#980449 – Automatic Execution of Embedded MIME Types**
  - Sep 2001 – Nimda worm
  - Nov 2001 – W32/Badtrans
  - Apr 2002 – W32/Klez
  - Jul 2002 – W32/Frethem
  - Oct 2002 – W32/Bugbear

  Patch available in April 2001

- **VU#952336 – Buffer Overflow in IIS Indexing Service**
  - Jul 2001 – Code Red

  Patch available in June 2001

- **VU#484891 – Buffer Overflow in SQL Server Stack Buffer**
  - Jan 2003 – SQLSlammer
    W32.Slammer
    Sapphire worm

  Patch available in July 2002

Why is it the problem?

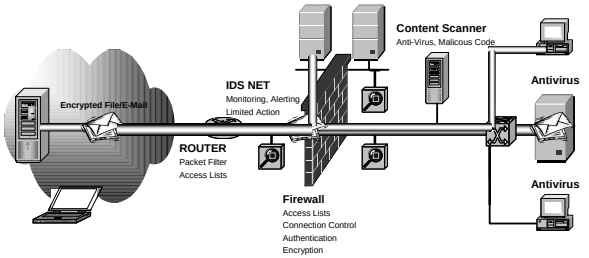
4129 vulnerabilities reported in 2002

- **To read the vulnerability description:**
  4129 x 20 min. to read *= 172 days in reading!*
- **Suppose 10% pertain to your environment:**
  413 vuls x 1 hour to install *= 51 days to install patches (per machine!)*
- **Just to read security news and patch a single system:**
  172+ 51 = 223 days (52 X 5 = 260 !!)

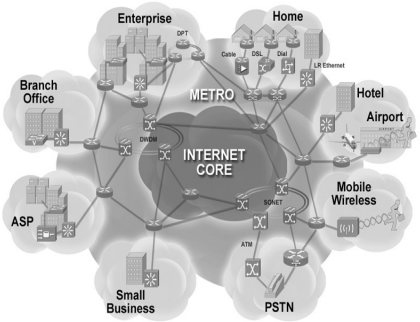
Even a 1% "hit rate" and 5 minutes to read new bulletins will cost almost 45 days, or about 20% of a perfectly efficient administrator.

Traditional Prevention Mechanisms

Traditional Security Concepts



Networks of the today

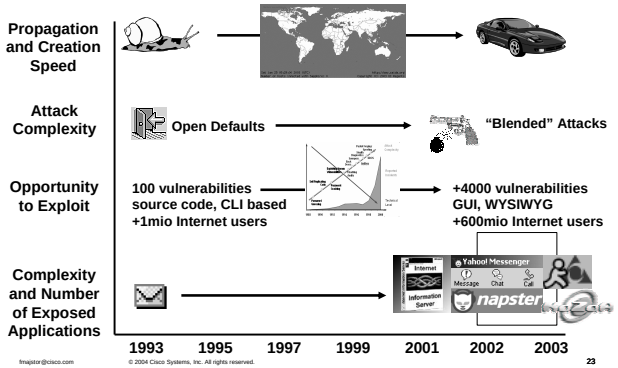


Characteristics

- Distributed Internet connections
- Need to open up data centers for more ubiquitous access
- Dramatic increase in employee mobility
- Increased use of new campus technologies like WLAN & IPT that provide more network access methods
- Growing damage due to viruses & worms

Evolution

…to fight against today's attacks?



Emerging Speed of Network Attacks

1980s-1990s
Usually had weeks or months to put defense in place.

2000-2002
Attacks progressed over hours, time to assess danger and impact. Time to implement defense.

2003-Future
Attacks progress on the timeline of seconds.

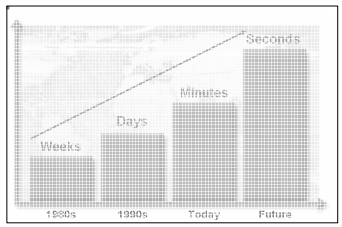
SQL Slammer Worm:
Doubled every 8.5 seconds
After 3 min : 55M scans/sec
1Gb Link is saturated after one minute

In 1/2 the time it took to read this slide, your network And all of your applications would have become unreachable!

SQL Slammer was a warning. Newer "Flash" worms are exponentially faster.

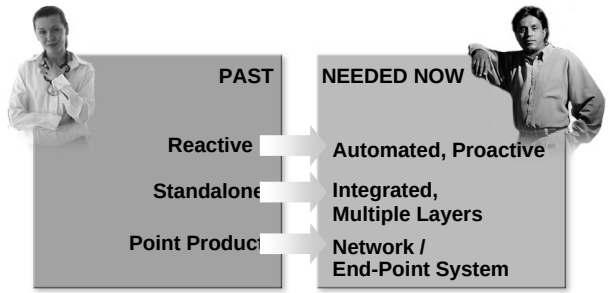
Threat Levels Escalating

- **Magnitude of infrastructure threats increasing**
- **Rapid worldwide propagation of attacks**
- **Current point product solutions can't keep up**



Innovative Approach

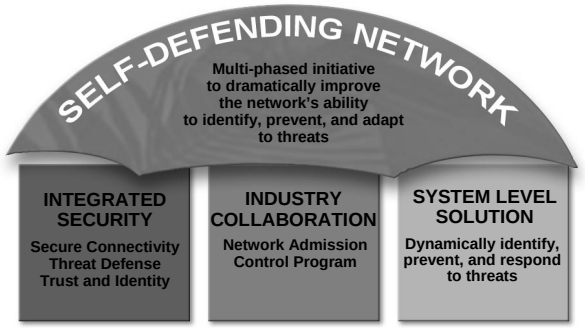
Approach to Security Must Change



A Collaborative Systems Approach

Self-Defending Network Solution

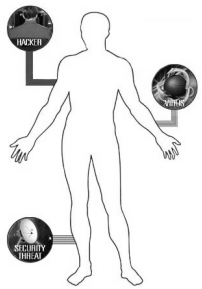
Cisco.com



The Network as the Human Body

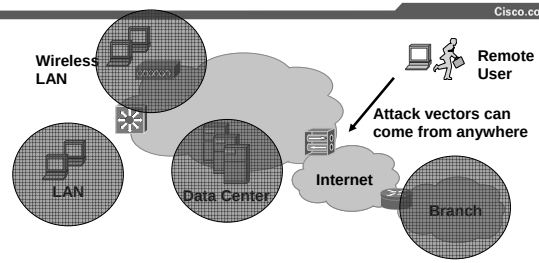
Cisco.com

- IT infrastructure (and network) needs to operate same as human body…
- Viruses… ever-present fact of life
  - We carry them with us
  - We pick them up from all sorts of contact
- Human body functions at high level even though we carry viruses and disease
- Self-Defending Network modeled around Autoimmune concept



Internet Worm Infection

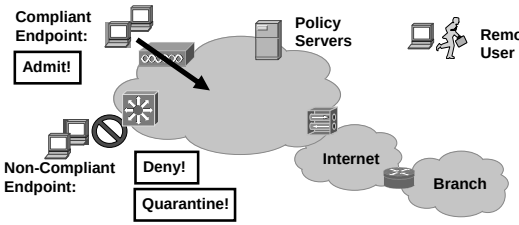
Cisco.com



- Self propagating worms continue to disrupt business, causing downtime and continual patching
- Locating and isolating infected systems is time and resource intensive
- Multiple types of users, access methods, and endpoints compound the problem

Ideal Solution: An Integrated System

Cisco.com

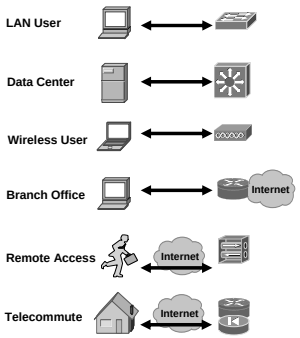


- Multiple components are required for a complete solution
  - Endpoint Security solutions knows security condition: type/compliance/etc
  - Policy Servers know compliance/access rules
  - Network access devices (routers, switches) enforce admission policy
- Virus/worm prevention and containment requires industry collaboration

Network Access Devices

Ubiquitous, Quarantine services, Transparency

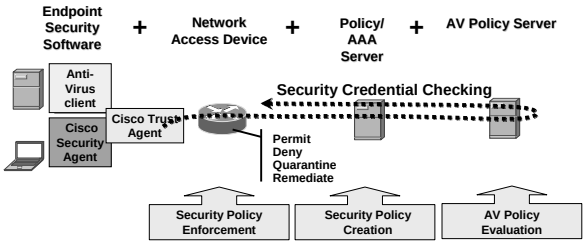
Cisco.com



- Ensure hosts comply to corporate policy (such as AV policy) before they can pass traffic to the network
  - Prevent attacks that start as soon as the device connects
  - Enforce on the network access device - no reliance on the host
  - Similar to 802.1x/AAA services
  - Isolate/quarantine hosts prior to access (L3/4 ACLs & L2 VLANS)
- Ensure all ways into and out of the network are covered
  - Cover wired, wireless, L3 gateways, dial-in, and IPsec remote access
  - Provide a consistent approach for all methods

Network Admission Control Elements

Cisco.com



Based on endpoint security posture, appropriate admission policy will be enforced in the network

Network, Hosts, and Policy are Symbiotic

Antivirus is just the beginning…

Cisco.com

Network Associates — symantec. — TREND MICRO

AV Client	CSA	Any App
EAP/TLV API		
Broker & Security		
Comms: L2/3 Service		
EAP/UDP	EAP/802.1X	

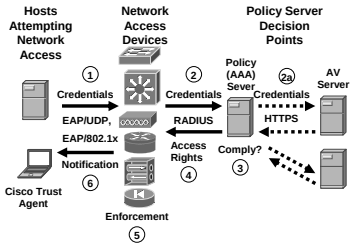
Cisco Trust Agent

- Initial focus on AV and OS/patches
  - Extensible model for host to network validation
  - Ensuring host OS patch and AV policy compliance
  - Built with Antivirus co-sponsors NAI, Symantec, TrendMicro
  - Support Microsoft Windows NT, XP, 2000
  - Use Cisco Trust Agent for comms, brokerage, and security
  - To be distributed by Cisco and partners, potentially bundled with AV solutions
- Expand to include other apps & policies
  - Security software: Personal firewall, HIPS
  - Application software: MS Office
  - Policies: no Kazaa
- Support wider range of platforms
  - Linux, Solaris, and other OSes will follow

Network Admission Control Solution

Cisco.com

NAC Solution: Leverage the network to intelligently enforce access privileges based on endpoint security posture



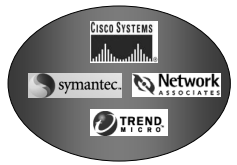
NAC Characteristics:

Ubiquitous solution for *all* connection methods
Validates *all* hosts
Leverages investments in network and AV solutions
Quarantine & remediation services
Scalability Deployment

Initial Component Details

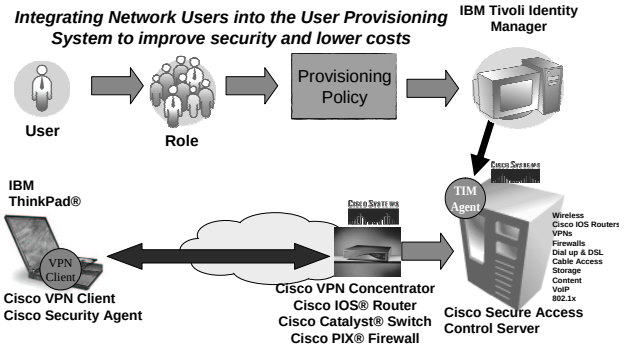
Cisco.com

- NAC-Enabled Applications
  - Cisco Security Agent
  - NAI McAfee Antivirus
  - Symantec Antivirus
  - Trend Micro Antivirus
- Cisco Trust Agent
  - No cost component
  - Support for Windows 2000, XP and NT
  - To be distributed by Cisco and partners, potentially bundled with AV solutions
- AAA Server - Cisco ACS v3.3
- Monitoring & Reporting - CiscoWorks SIMS

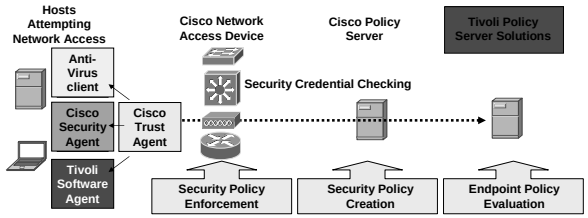


Announced: Unified User Provisioning
IBM & Cisco

Integrating Network Users into the User Provisioning System to improve security and lower costs



Announced: Tivoli & Cisco NAC
Extending Admission Control to Applications & Software



- Extends Cisco NAC beyond endpoint security posture to include application and software status
- Leverages existing customer investment in Tivoli and Cisco products
- Provides foundation for endpoint remediation

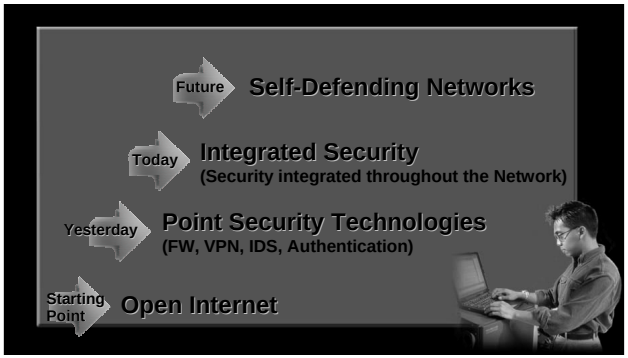
Network Admission Control Benefits

One Integrated System:

- Endpoint Security Solutions know security condition
- Policy Servers know compliance / access rules
- Network Access Devices enforce admission policy

Summary

Security Evolution



Q & A

Cisco Systems

Identity Management and Network Admission Control

Franjo Majstor
Consulting Engineer
Cisco Systems, Inc.

Cisco Systems