Getting the Network Security Basics Right

Paul Bartock

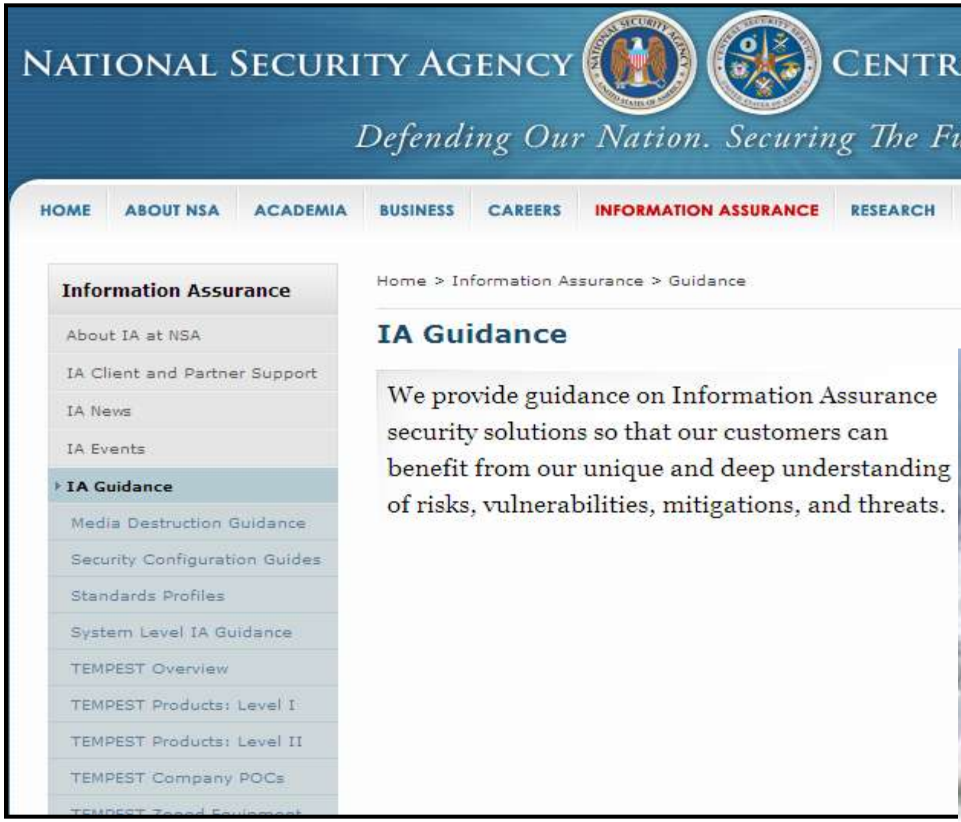
The Mitigations Group (I43)

Information Assurance Directorate

National Security Agency

1 Nov 2011

Who We Are



IA Guidance

We provide guidance on Information Assurance security solutions so that our customers can benefit from our unique and deep understanding of risks, vulnerabilities, mitigations, and threats.

UNCLASSIFIED

What We Do

- ***We Discover and Analyze*** vulnerabilities in…
  - in the core concepts of security
  - in emerging technologies and products
- ***We conduct operations*** *to find vulnerabilities…*
  - in the operational environment (networking, signals, space…);
  - as revealed thru content (e.g. log files)
- ***We Translate*** vulnerability knowledge*...*
  - into summaries, trends, root cause.
- ***We Lead*** the Community**...**
  - in the improvement of security practice;
  - in guidance, training, education, and standards development.

UNCLASSIFIED

Our Presence

- **We’re VERY public**
  - (Press) FCW/GCN, WTOP, Washington Post, SC Magazine, Information Week, Government Executive, etc…..
  - (Presentation) Blackhat/DEFCON, RSA, Lumension 360, IAWS, SC Forum, ITSEF, CISO, SANS
  - (Awards) SC Magazine, Fed 100, GovExec, SANS
- **We create and give away LOTS of great content**
  - FAM Folders
    - 4000+ given out
  - Security Configuration Guides
    - 75+ created and posted
    - 7 more in development this year

Lessons Learned

- The optimal place to solve a security problem is ...
- If it is happening to you today, then ...
- After you figure out what happened , there were ...
- Information Sharing is ...

UNCLASSIFIED

Lesson 1

The optimal place to solve a security problem is ...***never where you found it.***

--Corollary: the information for the solution is never in the right form for the solution

Lessons Learned

- The optimal place to solve a security problem is ...
- If it is happening to you today, then ...
- After you figure out what happened , there were ...
- Information Sharing is ...

UNCLASSIFIED

Lesson 2

If it is happening to you today, then ...

...***something very much like it happened to someone else yesterday, and will happen to someone else tomorrow.***

--Corollary: and you probably don’t know them

Lessons Learned

- The optimal place to solve a security problem is ...
- If it is happening to you today, then ...
- After you figure out what happened, there were ...
- Information Sharing is ...

Lesson 3

After you figure out what happened, there were…***plenty of signs that *could* have helped us prevent or manage this.***

--Corollary: but not all the signs are in "cyberspace", or available to "cyber defenders"

Lessons Learned

- The optimal place to solve a security problem is ...
- If it is happening to you today, then ...
- After you figure out what happened , there were ...
- Information Sharing is ...

UNCLASSIFIED

Lesson 4

Information Sharing is …

Over-rated!

--Corollary: until you think about Purpose, Content, Plumbing, and the Framework.

Information Sharing is ***over-rated***

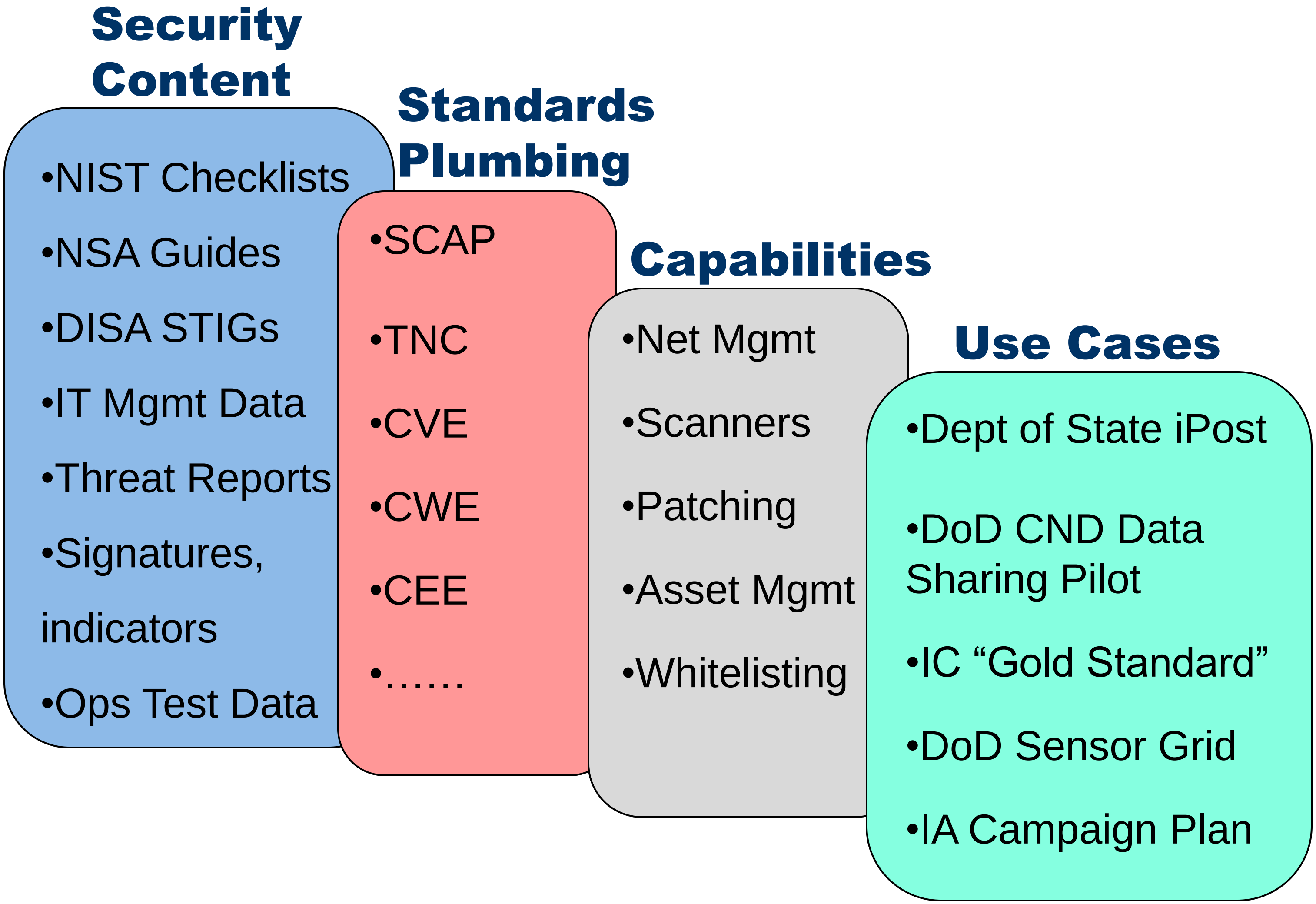
unless we decide on a shared PURPOSE,

which will determine the necessary CONTENT,

which we must move via standard PLUMBING,

which we must enforce within a FRAMEWORK.

Automation Landscape



Security Content

- NIST Checklists
- NSA Guides
- DISA STIGs
- IT Mgmt Data
- Threat Reports
- Signatures, indicators
- Ops Test Data

Standards Plumbing

- SCAP
- TNC
- CVE
- CWE
- CEE
- ……

Capabilities

- Net Mgmt
- Scanners
- Patching
- Asset Mgmt
- Whitelisting

Use Cases

- Dept of State iPost
- DoD CND Data Sharing Pilot
- IC “Gold Standard”
- DoD Sensor Grid
- IA Campaign Plan

TNC & SCAP Use Cases

- **Comply & Connect**: perform an SCAP based assessment using TNC protocols
- **Pro-active detection & monitoring & quarantine of assets** for un-authorize connections (detection of connection attempts to known bad IPs and domains, via router/ids black list connections)

TNC & SCAP Use Cases

Network sensing and Response. Security sensors detect suspicious activity (e.g. traffic sent to known bad IP addresses) and publish this information, which triggers further investigations such as checking caches on other devices to see if they have the same problem. This use case can be implemented through IF-MAP 2.0.

Trends. Administrators get visibility into warning signs by viewing activity on a console. This use case is enabled by IF-MAP 2.0 but nobody has implemented it yet.

TNC & SCAP Use Cases

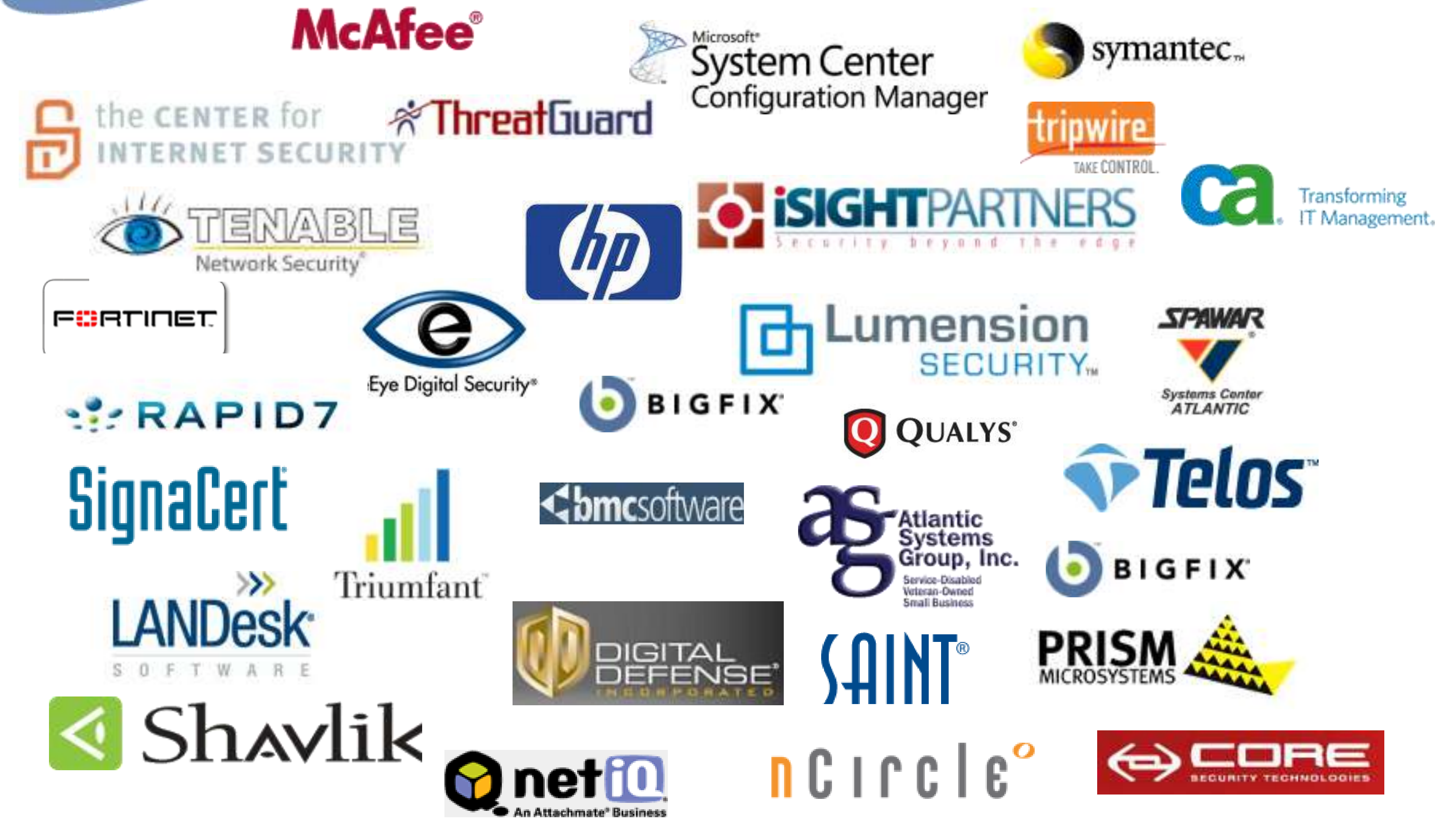
Rescan for new policy. When an SCAP policy changes, endpoints should be rescanned and their network access modified accordingly. For example, non-compliant endpoints might be quarantined until remediation can be completed.

Information sharing across administrators. The MAP provides a single shared database that allows administrators to have a common view of what's happening on their network. Tricky and interesting issues arise when sharing information across trust boundaries (i.e. from one organization to another). Information may be summarized.

TNC & SCAP Use Cases

Dashboard. Executives and commanders often want a global view of security issues. Which areas of the world are seeing the most attacks? The most compliance or non-compliance? They may also want to drill down to get more information. IF-MAP enables this sort of data to be amassed and exchanged among security systems in a standard way. Thinking is those executives generally view things from a risk perspective. Infections on a critical system are more important than those on a less important one.

SCAP Vendor Partners


McAfee®
Microsoft® System Center Configuration Manager
symantec™
the CENTER for INTERNET SECURITY
ThreatGuard
tripwire TAKE CONTROL.
TENABLE Network Security®
hp
iSIGHTPARTNERS Security beyond the edge
ca Transforming IT Management.
FORTINET
Eye Digital Security®
Lumension SECURITY™
SPAWAR® Systems Center ATLANTIC
RAPID7
BIGFIX®
QUALYS®
Telos™
SignaCert
Triumfant™
bmcsoftware
Atlantic Systems Group, Inc. Service-Disabled Veteran-Owned Small Business
BIGFIX®
LANDesk® SOFTWARE
DIGITAL DEFENSE® INCORPORATED
SAINT®
PRISM MICROSYSTEMS
Shavlik
netIQ® An Attachmate® Business
nCircle
CORE SECURITY TECHNOLOGIES

Trusted Network Connect Standards for Network Security

Agenda

Introduce TNC and TCG

Explanation of TNC

- What problems does TNC solve?
- How does TNC solve those problems?
- TNC Architecture and Standards
- TNC Adoption and Certification
- TNC Advantages
- Case Studies

Summary

For More Information

Trusted Network Connect

Open Architecture for Network Security

- Completely vendor-neutral
- Strong security through trusted computing
- Original focus on NAC, now expanded to Network Security

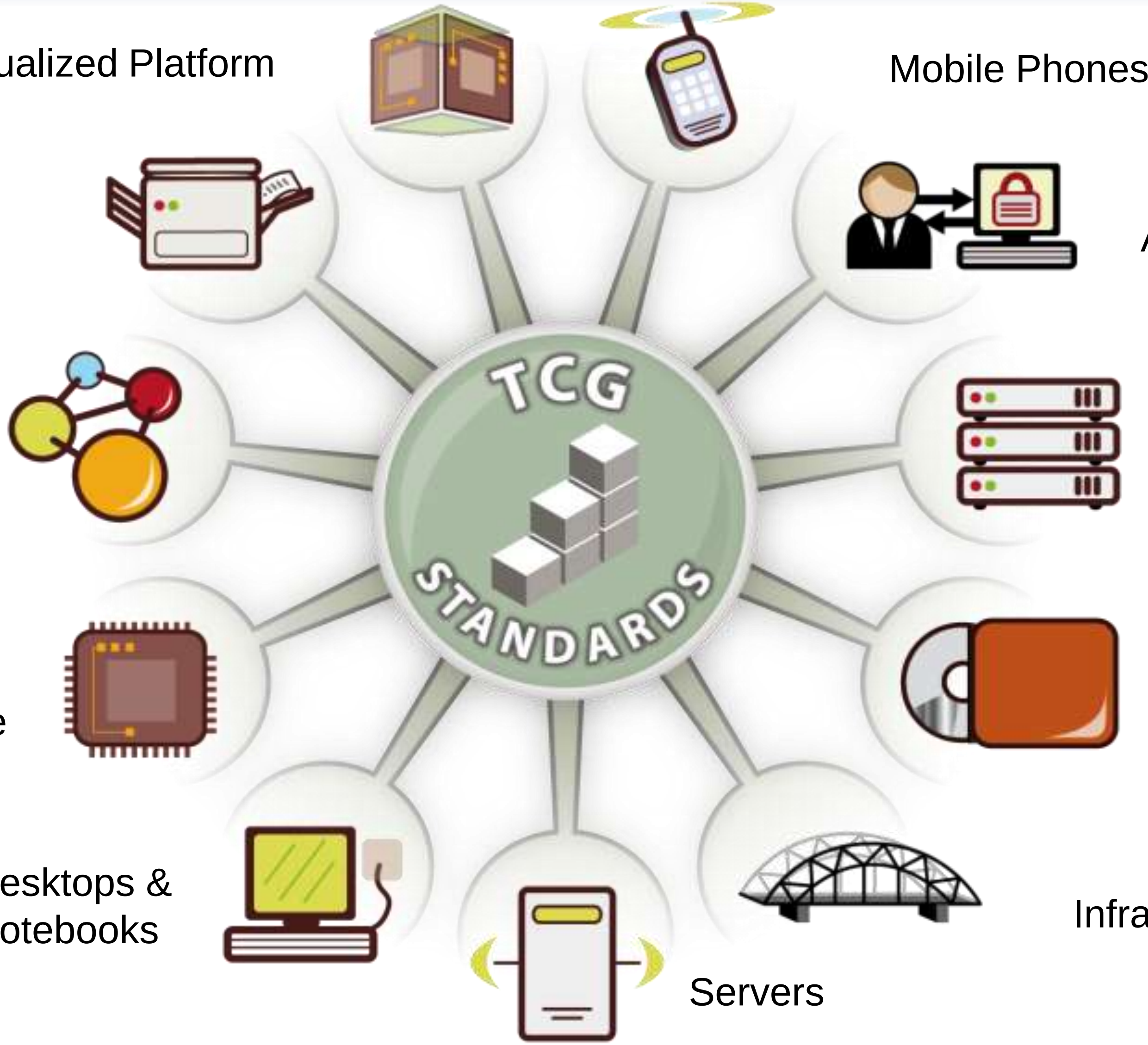
Open Standards for Network Security

- Full set of specifications available to all
- Products shipping since 2005

Developed by Trusted Computing Group (TCG)

- Industry standards group
- More than 100 member organizations
- Includes large vendors, small vendors, customers, etc.

TCG: Standards for Trusted Systems



Virtualized Platform

Mobile Phones

Printers & Hardcopy

Authentication

Network Security

Storage

Applications
- Software Stack
- Operating Systems
- Web Services
- Authentication
- Data Protection

Security Hardware

Desktops & Notebooks

Servers

Infrastructure

Trusted Platform Module (TPM)

Security hardware on motherboard

- Open specifications from TCG
- Resists tampering & software attacks

Now included in almost all enterprise PCs

- Off by default; opt in

Features

- Secure key storage
- Cryptographic functions
- Integrity checking & remote attestation

Applications

- Strong user and machine authentication
- Secure storage
- Trusted / secure boot

Problems Solved by TNC

Network and Endpoint Visibility

- Who and what's on my network?
- Are devices on my network secure? Is user/device behavior appropriate?

Network Enforcement

- Block unauthorized users, devices, or behavior
- Grant appropriate levels of access to authorized users/devices

Network Access Control (NAC)

Device Remediation

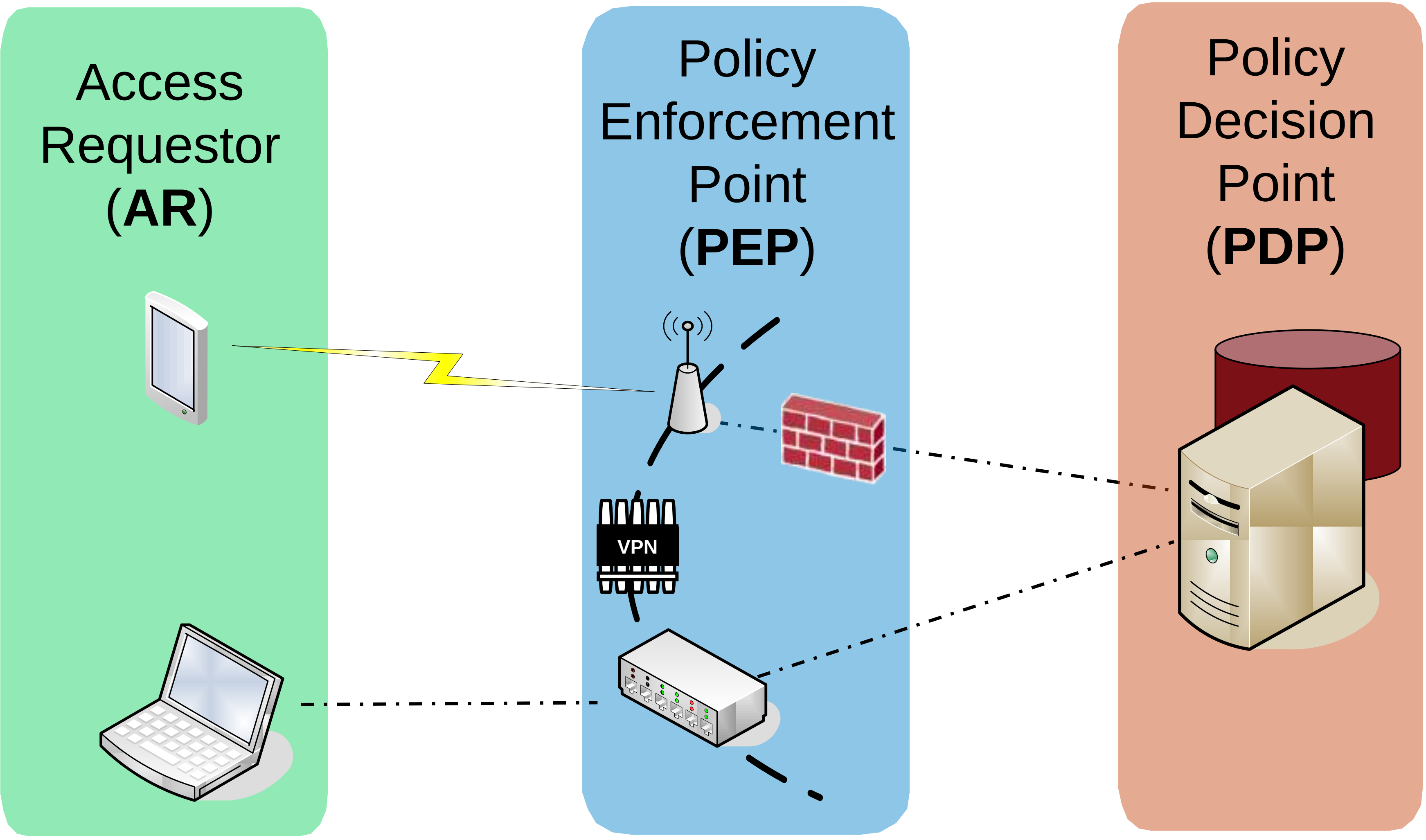
- Quarantine and repair unhealthy or vulnerable devices

Security System Integration

- Share real-time information about users, devices, threats, etc.

Coordinated Security

Basic NAC Architecture

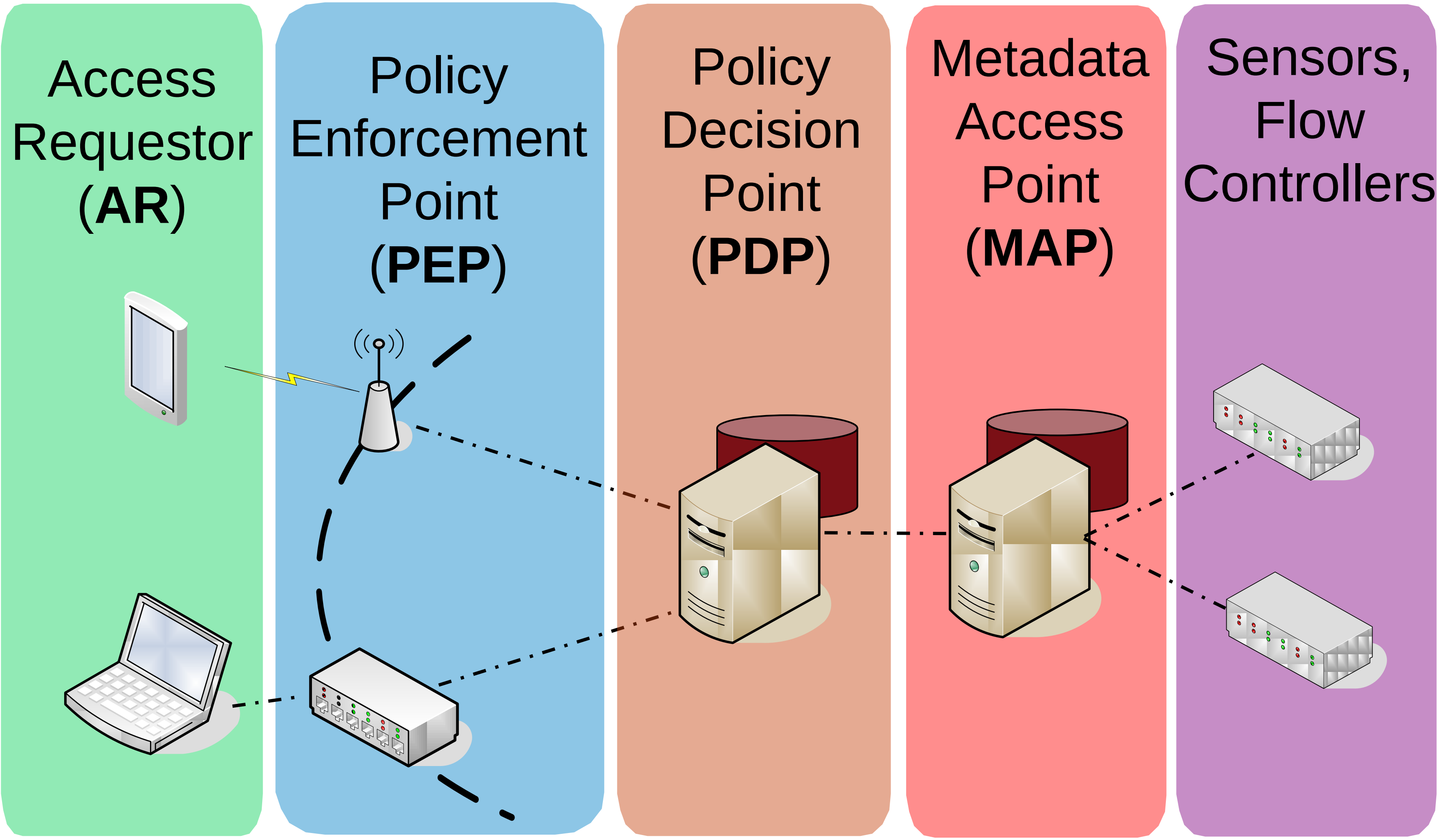


Access Requestor (**AR**)

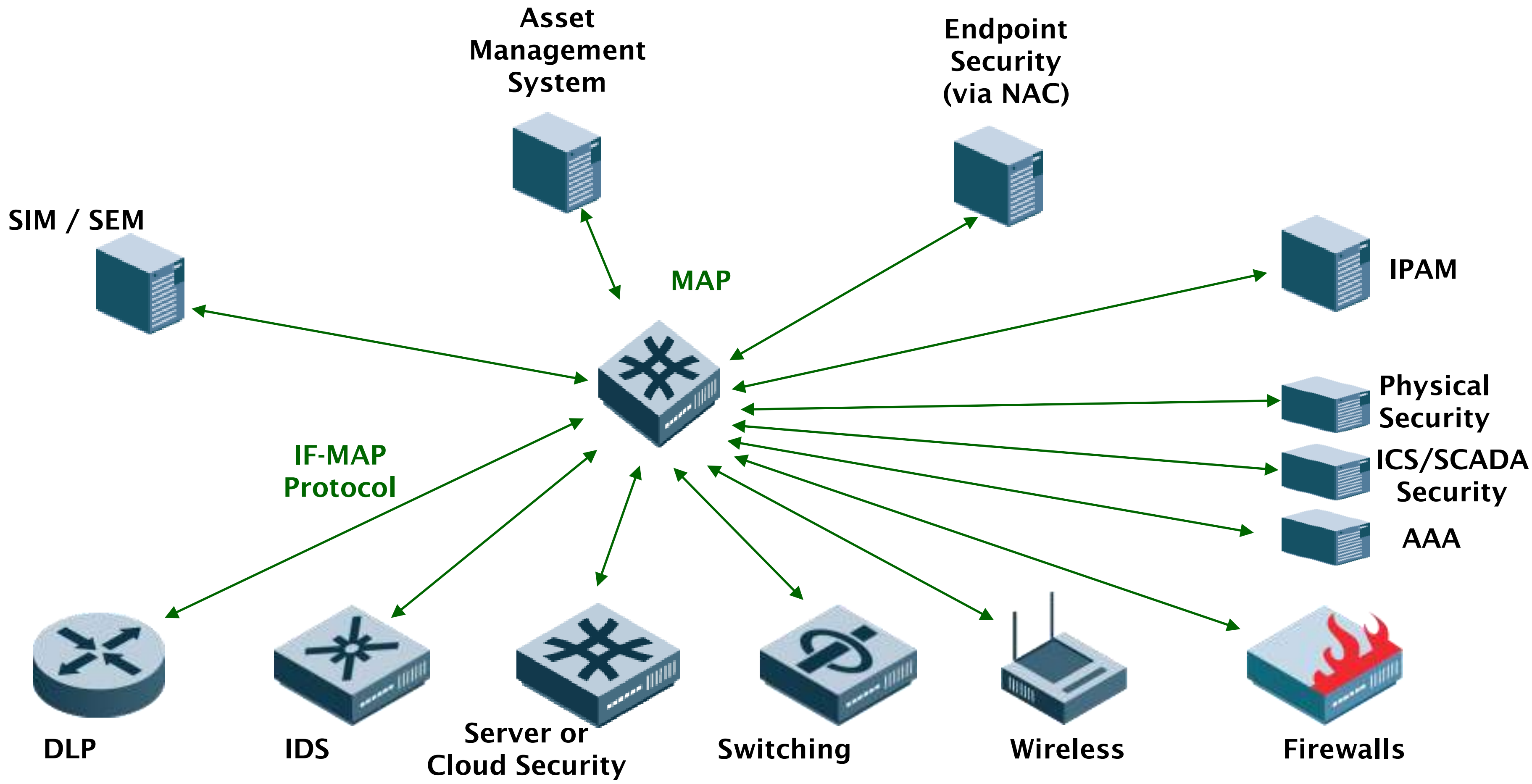
Policy Enforcement Point (**PEP**)

Policy Decision Point (**PDP**)

Integrating Other Security Devices


Access Requestor (**AR**)
Policy Enforcement Point (**PEP**)
Policy Decision Point (**PDP**)
Metadata Access Point (**MAP**)
Sensors, Flow Controllers

Coordinated Security



Typical TNC Deployments

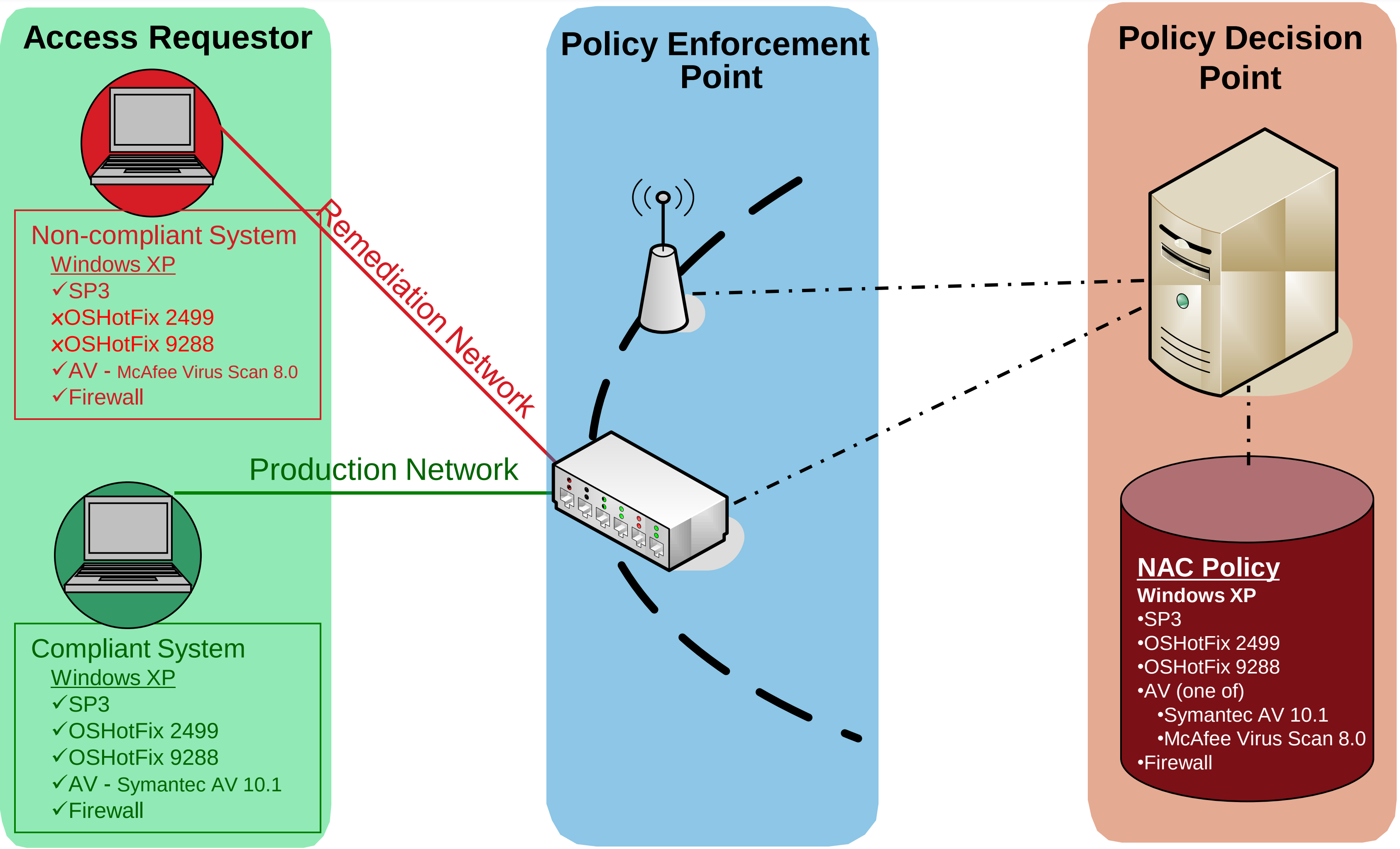
Health Check

Behavior Check

User-Specific Policies

TPM-Based Integrity Check

Health Check



Access Requestor

Non-compliant System

Windows XP

✓SP3

✗OSHotFix 2499

✗OSHotFix 9288

✓AV - McAfee Virus Scan 8.0

✓Firewall

Remediation Network

Production Network

Compliant System

Windows XP

✓SP3

✓OSHotFix 2499

✓OSHotFix 9288

✓AV - Symantec AV 10.1

✓Firewall

Policy Enforcement Point

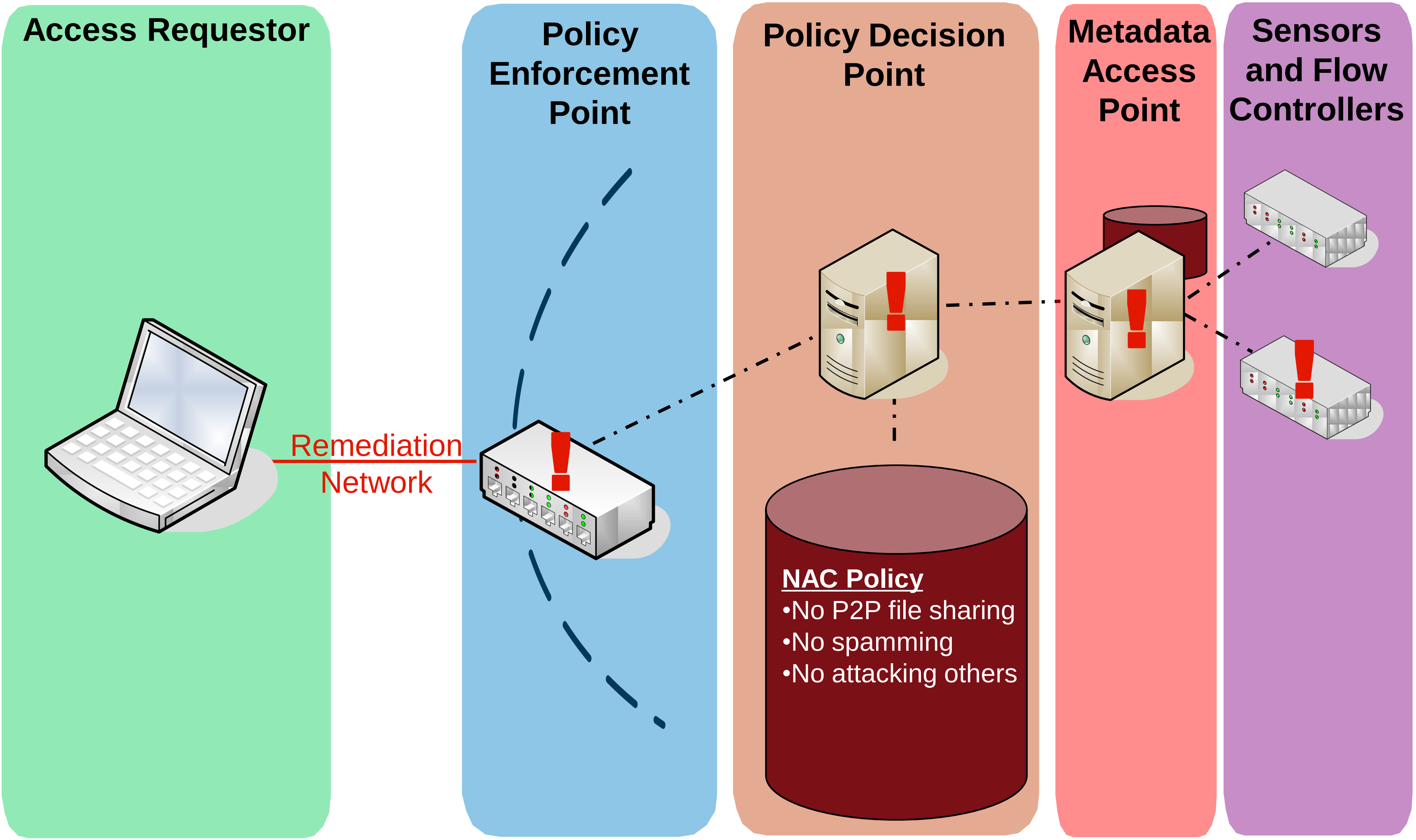
Policy Decision Point

NAC Policy

Windows XP

- SP3
- OSHotFix 2499
- OSHotFix 9288
- AV (one of)
  - Symantec AV 10.1
  - McAfee Virus Scan 8.0
- Firewall

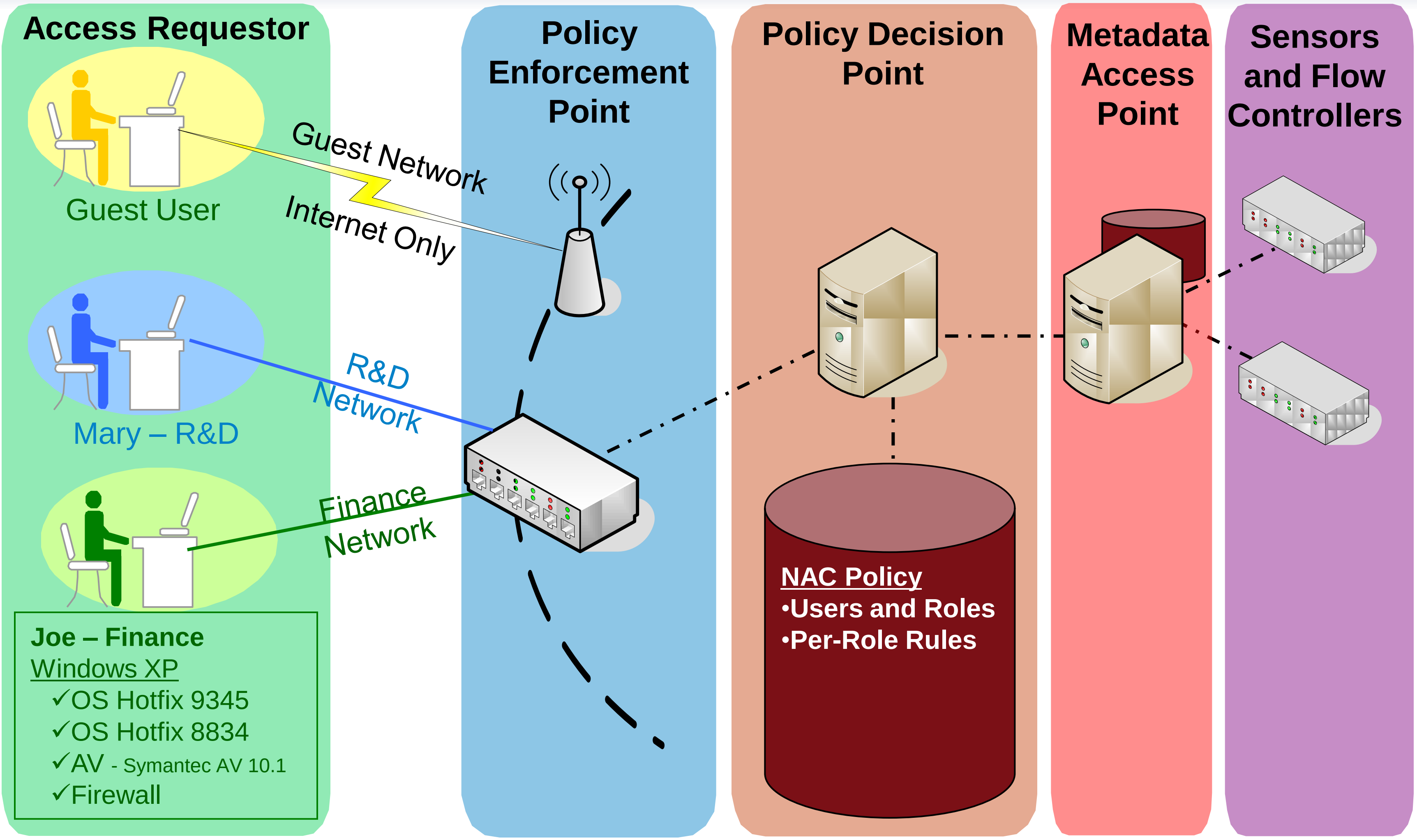
Behavior Check



NAC Policy

- No P2P file sharing
- No spamming
- No attacking others

User-Specific Policies



Access Requestor

Guest User

Mary – R&D

Joe – Finance
Windows XP
✓OS Hotfix 9345
✓OS Hotfix 8834
✓AV - Symantec AV 10.1
✓Firewall

Guest Network
Internet Only

R&D Network

Finance Network

Policy Enforcement Point

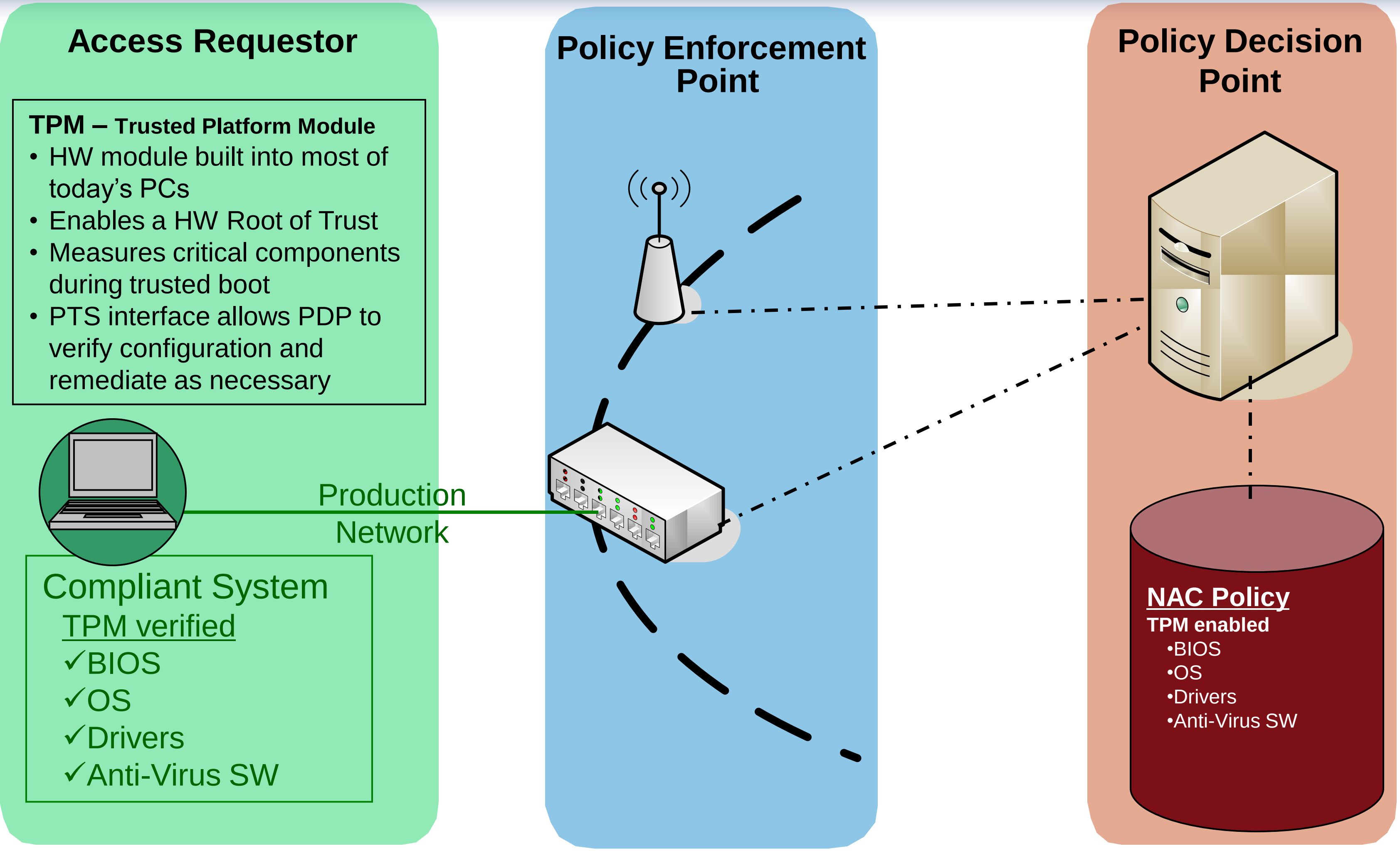
Policy Decision Point

NAC Policy
•Users and Roles
•Per-Role Rules

Metadata Access Point

Sensors and Flow Controllers

TPM-Based Integrity Check



Access Requestor

TPM – Trusted Platform Module
- HW module built into most of today's PCs
- Enables a HW Root of Trust
- Measures critical components during trusted boot
- PTS interface allows PDP to verify configuration and remediate as necessary

Production Network

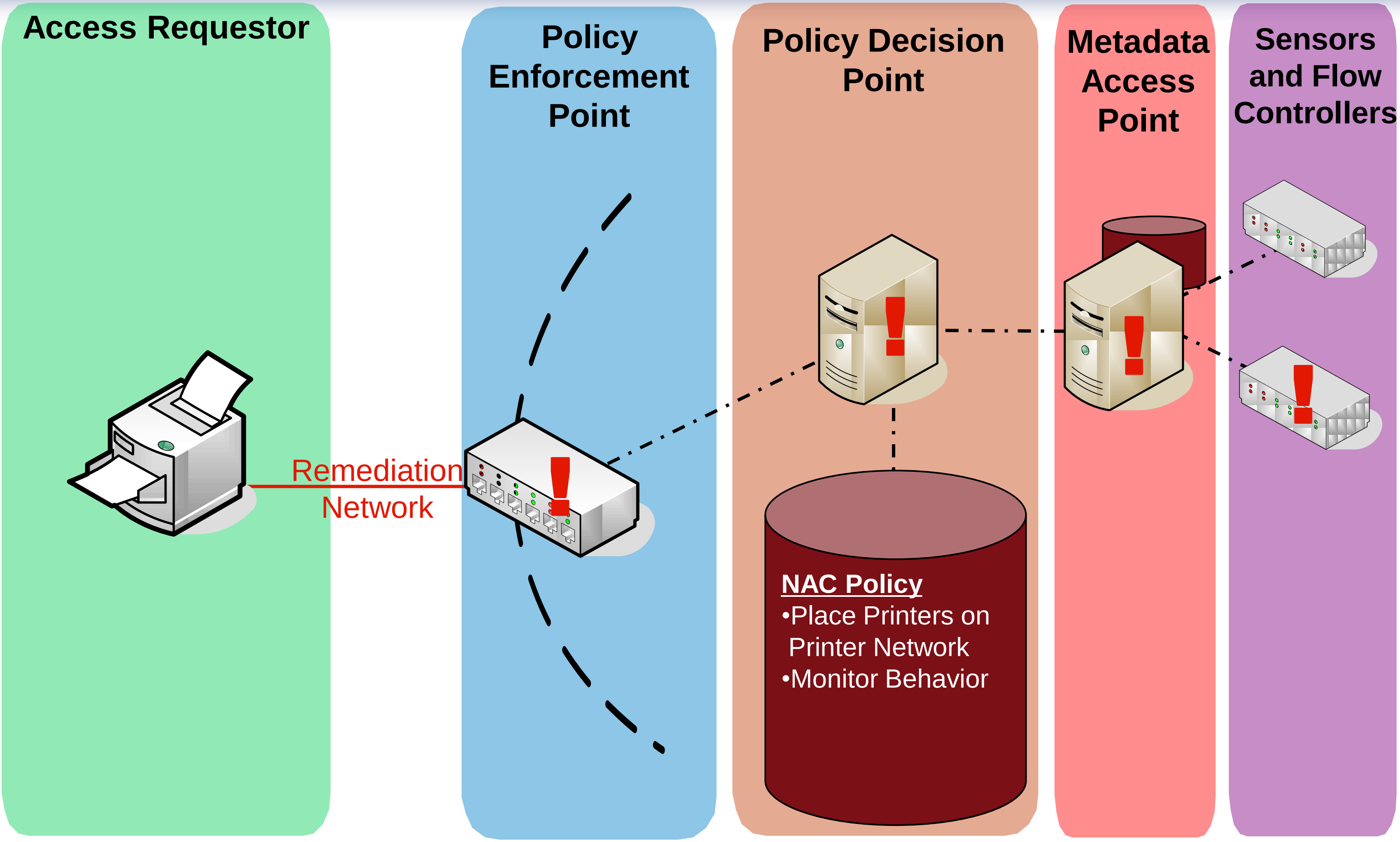
Compliant System
<u>TPM verified</u>
✓BIOS
✓OS
✓Drivers
✓Anti-Virus SW

Policy Enforcement Point

Policy Decision Point

<u>NAC Policy</u>
TPM enabled
•BIOS
•OS
•Drivers
•Anti-Virus SW

Clientless Endpoint Handling



NAC Policy

- Place Printers on Printer Network
- Monitor Behavior

Enforcement Options

Edge Enforcement

Inline Enforcement

Protocol-Based Enforcement

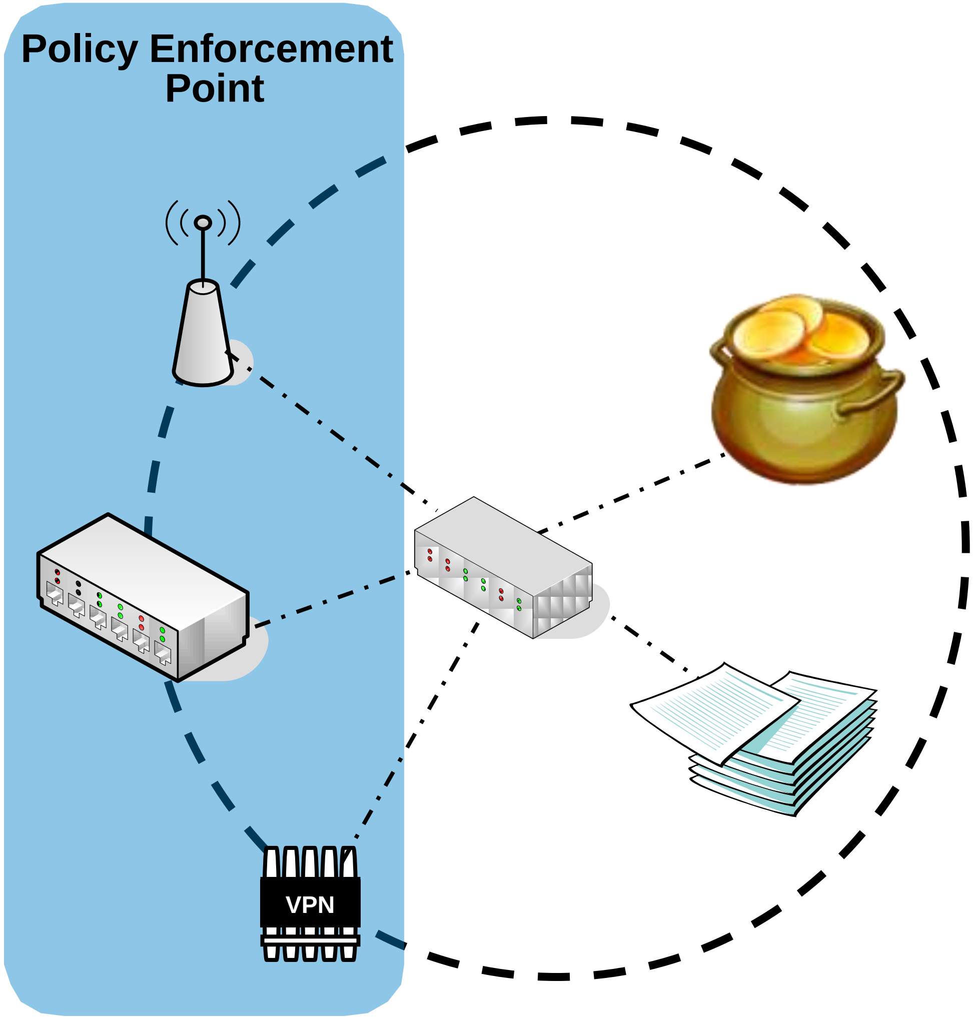
Edge Enforcement

Pros

- Simple

Cons

- Big change
- Hard for legacy endpoints



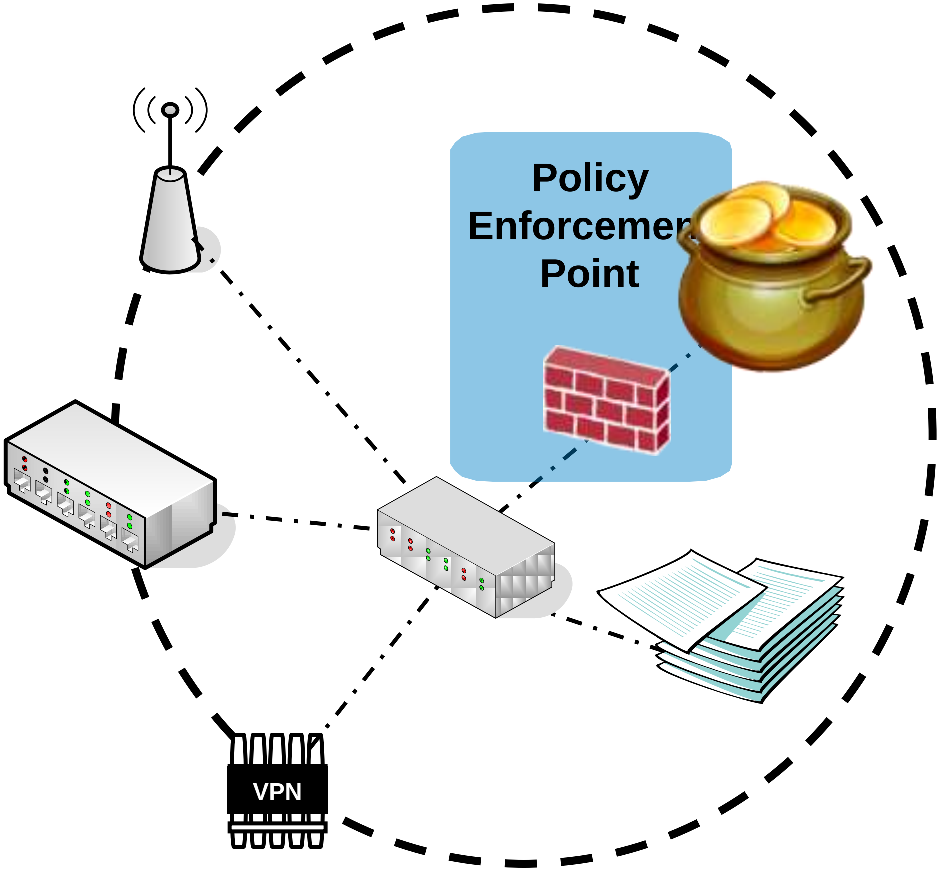
Inline Enforcement

Pros

- Gradual or partial deployment

Cons

- Security varies
  - IPsec/TLS vs. IP/MAC authn



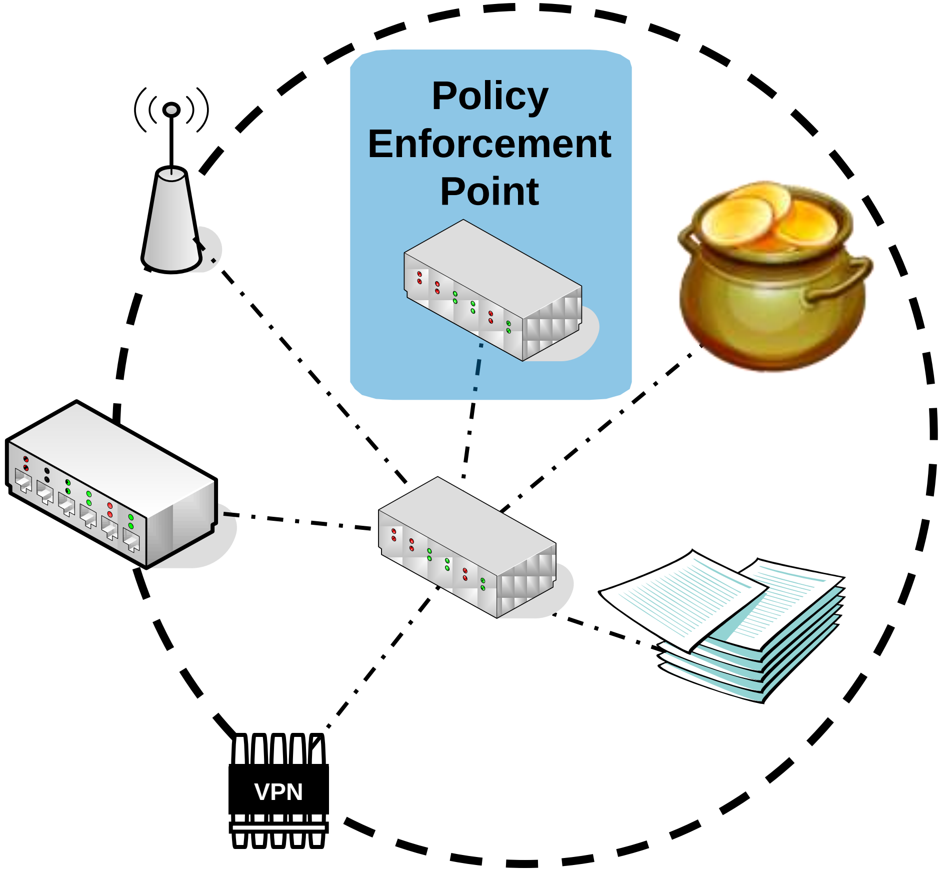
Protocol-Based Enforcement

Pros

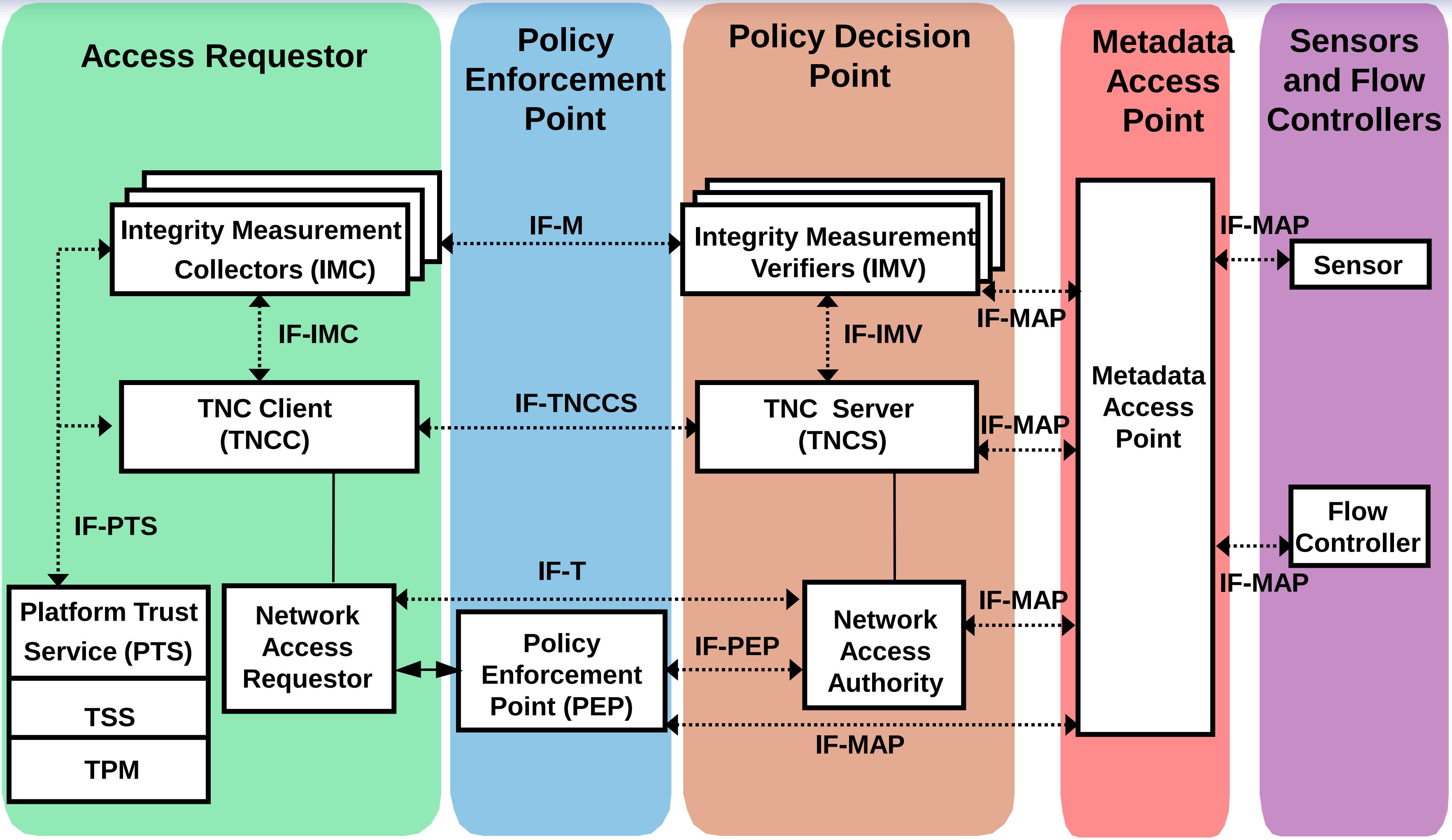
- Easy deployment

Cons

- Low security
  - Nothing inline
- Problematic



TNC Architecture



http://www.trustedcomputinggroup.org/developers/trusted_network_connect/specifications

Foiling Root Kits with TPM and TNC

Solves the critical “lying endpoint problem”

TPM Measures Software in Boot Sequence

- Hash software into PCR before running it
- PCR value cannot be reset except via hard reboot

During TNC Handshake...

- PDP engages in crypto handshake with TPM
- TPM securely sends PCR value to PDP
- PDP compares to good configurations
- If not listed, endpoint is quarantined and remediated

Federated TNC

Conveys TNC results between security domains

- Consortia, coalitions, partnerships, outsourcing, and alliances
- Large organizations

Supports

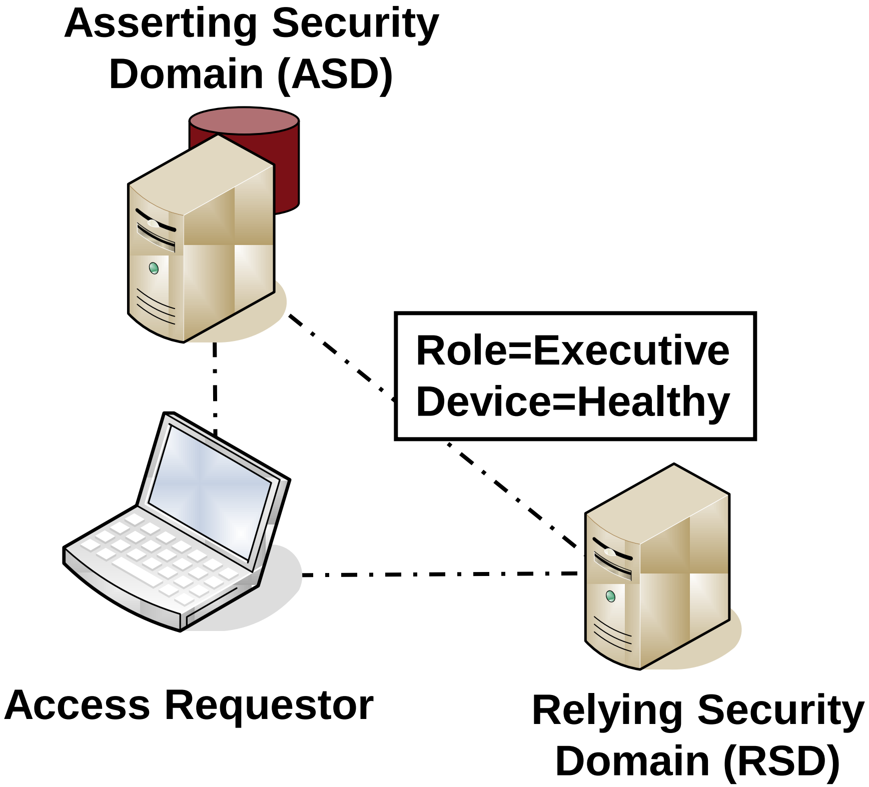
- Web SSO with health info
- Roaming with health check

How?

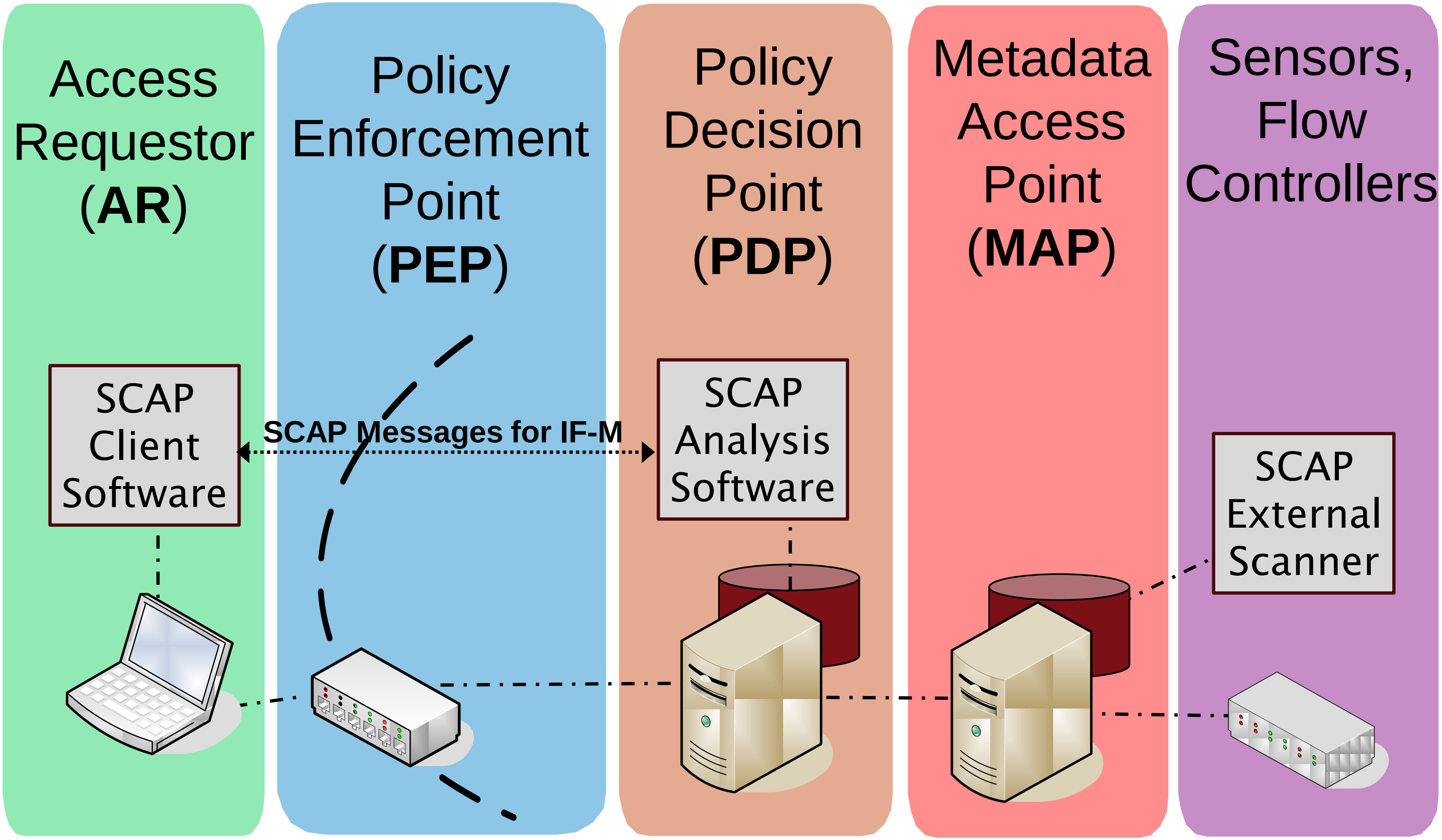
- SAML profiles for TNC

Applications

- Network roaming
- Coalitions, consortia
- Large organizations


Asserting Security Domain (ASD)
Role=Executive
Device=Healthy
Access Requestor
Relying Security Domain (RSD)

TNC and SCAP Together


Access Requestor (AR)
Policy Enforcement Point (PEP)
Policy Decision Point (PDP)
Metadata Access Point (MAP)
Sensors, Flow Controllers
SCAP Client Software
SCAP Messages for IF-M
SCAP Analysis Software
SCAP External Scanner

TNC: A Flexible Architecture

Assessment Options

- Identity, health, behavior, and/or location
- Optional hardware-based assessment with TPM
- Pre-admission, post-admission, or both

Enforcement Options

- 802.1X, firewalls, VPN gateways, DHCP, host software

Clientless endpoints

- No NAC capabilities built in
- Printers, phones, robots, guest laptops

Information sharing

- IF-MAP lets security devices share info on user identity, endpoint health, behavior, etc.
- Federated TNC supports federated environments

TNC Advantages

Open standards

- Non-proprietary – Supports multi-vendor compatibility
- Interoperability
- Enables customer choice
- Allows thorough and open technical review

Leverages existing network infrastructure

- Excellent Return-on-Investment (ROI)

Roadmap for the future

- Full suite of standards
- Supports Trusted Platform Module (TPM)

Products supporting TNC standards shipping today

TNC Adoption

Access Requestor

- McAfee®
- Microsoft®
- symantec.
- FUJITSU
- IBM
- JUNIPer NETWORKS
- Triumfant
- StillSecure
- GENERAL DYNAMICS C4 Systems
- wave

Policy Enforcement Point

- ARUBA networks
- hp
- Microsoft®
- enterasys Secure Networks
- JUNIPer NETWORKS
- NORTEL

Policy Decision Point

- symantec.
- Microsoft®
- FUJITSU
- IBM
- JUNIPer NETWORKS
- Q1 Labs
- wave
- enterasys Secure Networks
- Triumfant
- StillSecure
- GENERAL DYNAMICS C4 Systems
- McAfee®

Metadata Access Point

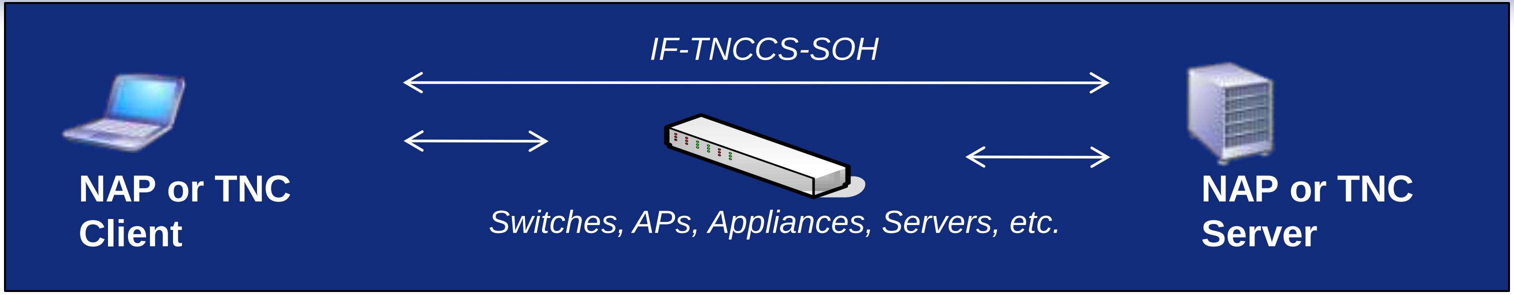
- Infoblox
- JUNIPer NETWORKS

Sensors, Flow Controllers

- ArcSight
- Great Bay Software Inc.
- ARUBA networks
- JUNIPer NETWORKS
- LUMETA®
- HIRSCH ELECTRONICS
- nSolutions Effortless Infrastructure
- insightix
- TOFINO™

TRUSTED COMPUTING GROUP™

Microsoft NAP Interoperability



IF-TNCCS-SOH Standard

- Developed by Microsoft as Statement of Health (SoH) protocol
- Donated to TCG by Microsoft
- Adopted by TCG and published as a new TNC standard, IF-TNCCS-SOH

Availability

- Built into Windows Vista, Windows 7, Windows Server 2008, and Windows XP SP 3
- Also built into products from other TNC vendors

Implications

- NAP servers can health check TNC clients without extra software
- NAP clients can be health checked by TNC servers without extra software
- As long as all parties implement the open IF-TNCCS-SOH standard

IETF and TNC

IETF NEA WG

- Goal: Universal Agreement on NAC Client-Server Protocols
  - Co-Chaired by Cisco employee and TNC-WG Chair

Published several TNC protocols as IETF RFCs

- PA-TNC (RFC 5792) and PB-TNC (RFC 5793)
- Equivalent to TCG’s IF-M 1.0 and IF-TNCCS 2.0
- Co-Editors from Cisco, Intel, Juniper, Microsoft, Symantec

Now working on getting IETF approval for IF-T

What About Open Source?

Lots of open source support for TNC

- University of Applied Arts and Sciences in Hannover, Germany (FHH)
  http://trust.inform.fh-hannover.de
- libtnc
  http://sourceforge.net/projects/libtnc
- OpenSEA 802.1X supplicant
  http://www.openseaalliance.org
- FreeRADIUS
  http://www.freeradius.org
- omapd IF-MAP Server
  http://code.google.com/p/omapd
- strongSwan IPsec
  http://www.strongswan.org
- Open Source TNC SDK (IF-IMV and IF-IMC)
  http://sourceforge.net/projects/tncsdk

TCG support for these efforts

- Liaison Memberships
- Open source licensing of TNC header files

TNC Certification Program

Certifies Products that Properly Implement TNC Standards

Certification Process

- Compliance testing using automated test suite from TCG
- Interoperability testing at Plugfest
- Add to list of certified products on TCG web site

Customer Benefits

- Confidence that products interoperate
- Easy to cite in procurement documents

TNC in the Real World

Widely Deployed

- Millions of Seats
- Thousands of Customers
- Dozens of Products

Across Many Sectors

- Government
- Finance
- Health Care
- Retail …

Case Study – St. Mary's County Public Schools

CHARTING A COURSE TO EXCELLENCE

St. Mary's County Public Schools

"Work Hard and Be Nice"

Who

- Public school district in Maryland
- 16,000 students, 2,100 staff
- 26 schools, Grades K-12
- New, intensive STEM academies
  - STEM = Science, Technology, Engineering, and Math
  - Grades 6-12

Problem

- Received grant for 60 wireless laptops for STEM academies
- Need strongest security
  - Only STEM laptops can connect
  - User-specific access controls
  - Strong health checks on laptops
  - All wireless traffic encrypted

TRUSTED COMPUTING GROUP™

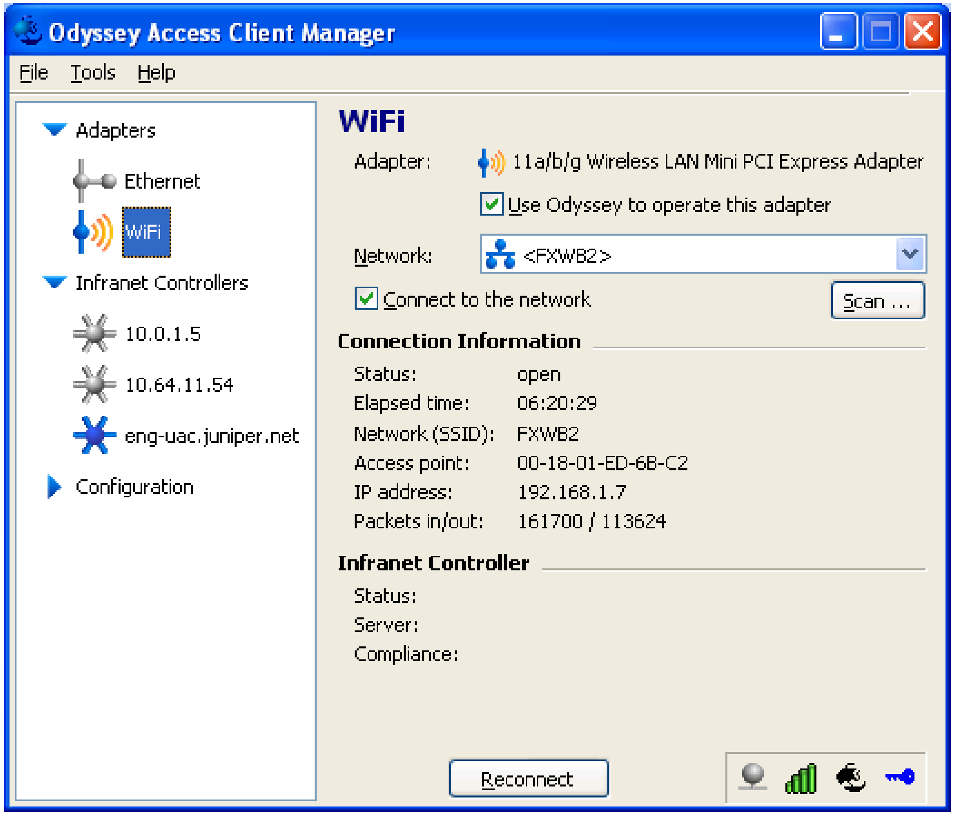
St. Mary's County Public Schools - Solution

Solution

- Juniper UAC with …
  - Permanently resident agent
  - Continuous health checks
- Non-Juniper wireless access points
  - 802.1X enforcement
  - Integrated via TNC's IF-PEP

Lessons Learned

- Design for the environment
  - Tightly controlled endpoints
  - Strong security requirements
  - Need constant health checking



WiFi

Adapter: 11a/b/g Wireless LAN Mini PCI Express Adapter

☑ Use Odyssey to operate this adapter

Network: <FXWB2>

☑ Connect to the network

Connection Information

Status: open
Elapsed time: 06:20:29
Network (SSID): FXWB2
Access point: 00-18-01-ED-6B-C2
IP address: 192.168.1.7
Packets in/out: 161700 / 113624

Infranet Controller

Status:
Server:
Compliance:

TRUSTED COMPUTING GROUP™

Case Study – Naperville Community School District

Who

- Public school district in Illinois
- 19,000 students, 2,500 staff
- 21 schools, Grades K-12
- Innovative teaching methods

Problem

- Increasing number and variety of network-connected devices
  - District-owned
  - Staff-owned
  - Student-owned
- Must provide network access for all
  - High-speed
  - Cost-effective
  - Secure

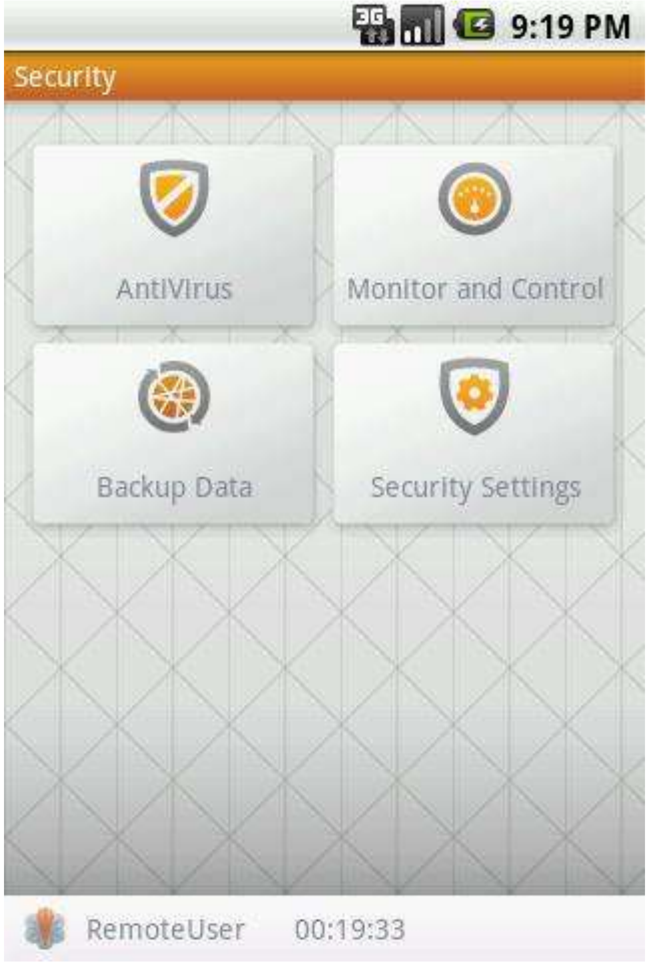
Naperville Community School District - Solution

Solution

- District-owned Devices
  - Strict permanent agent
- Non-district Devices
  - Web-based agent
  - Security policies
- Separate guest network
  - Enforced with 802.1X

Lessons Learned

- Design for the environment
  - Platform-independent
  - Lightweight for guests
  - Maintaining security policies



Summary

TNC solves today's security problems with growth for the future

- Flexible open architecture to accommodate rapid change
- Coordinated, automated security for lower costs and better security

TNC = open network security architecture and standards

- Enables multi-vendor interoperability
- Can reuse existing products to reduce costs and improve ROI
- Avoids vendor lock-in

TNC has strongest security

- Optional support for TPM to defeat rootkits
- Thorough and open technical review

Wide support for TNC standards

- Many vendors, open source, IETF

For More Information

TNC Web Site

- Technical
  - http://www.trustedcomputinggroup.org/developers/trusted_network_connect
- Business
  - http://www.trustedcomputinggroup.org/solutions/network_security

TNC-WG Co-Chairs

Steve Hanna

Distinguished Engineer, Juniper Networks

shanna@juniper.net

Paul Sangster

Chief Security Standards Officer, Symantec

Paul_Sangster@symantec.com