TRUSTED COMPUTING GROUP™

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

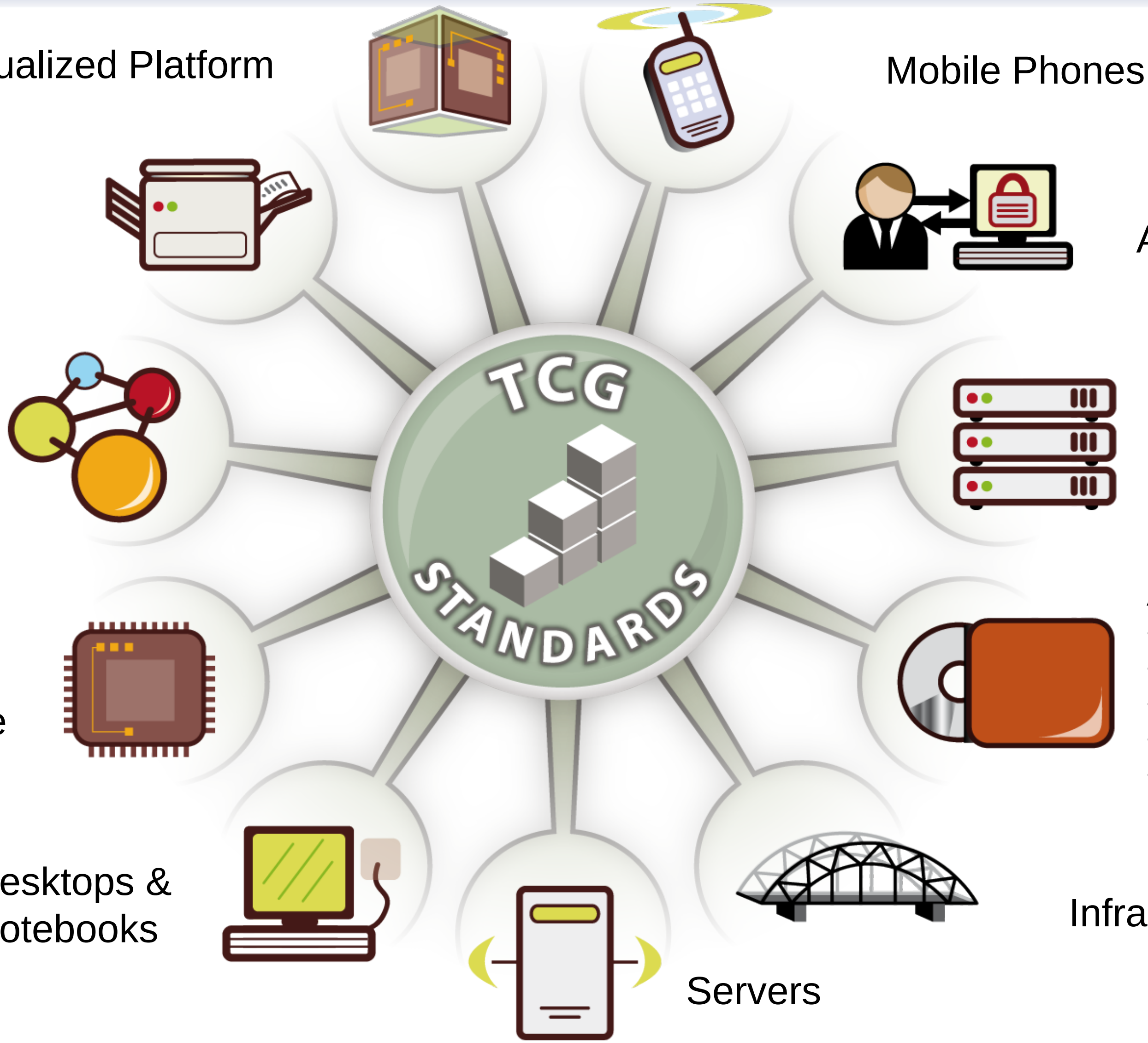
Open Standards for Network Security

- 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

Security Hardware

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

Desktops & Notebooks

Infrastructure

Servers

Trusted Platform Module (TPM)

Security hardware on motherboard

- Open specifications from TCG
- Resists tampering & software attacks

Now included in almost all enterprise PCs

- On by default
- Easy to provision and manage

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

Device Remediation

- Quarantine and repair unhealthy or vulnerable devices

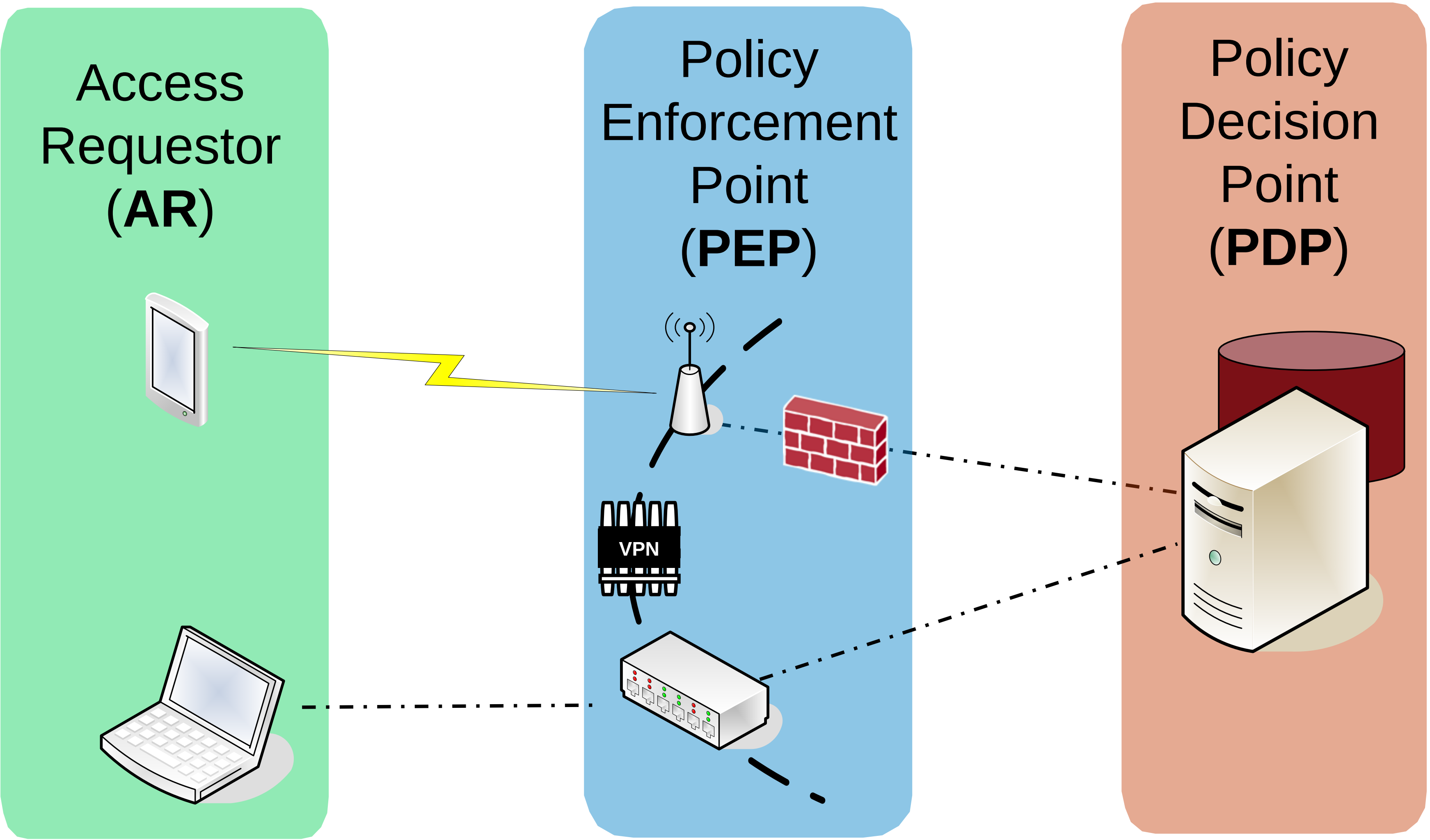
Network Access Control (NAC)

Security System Integration

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

Security Automation

Basic NAC Architecture

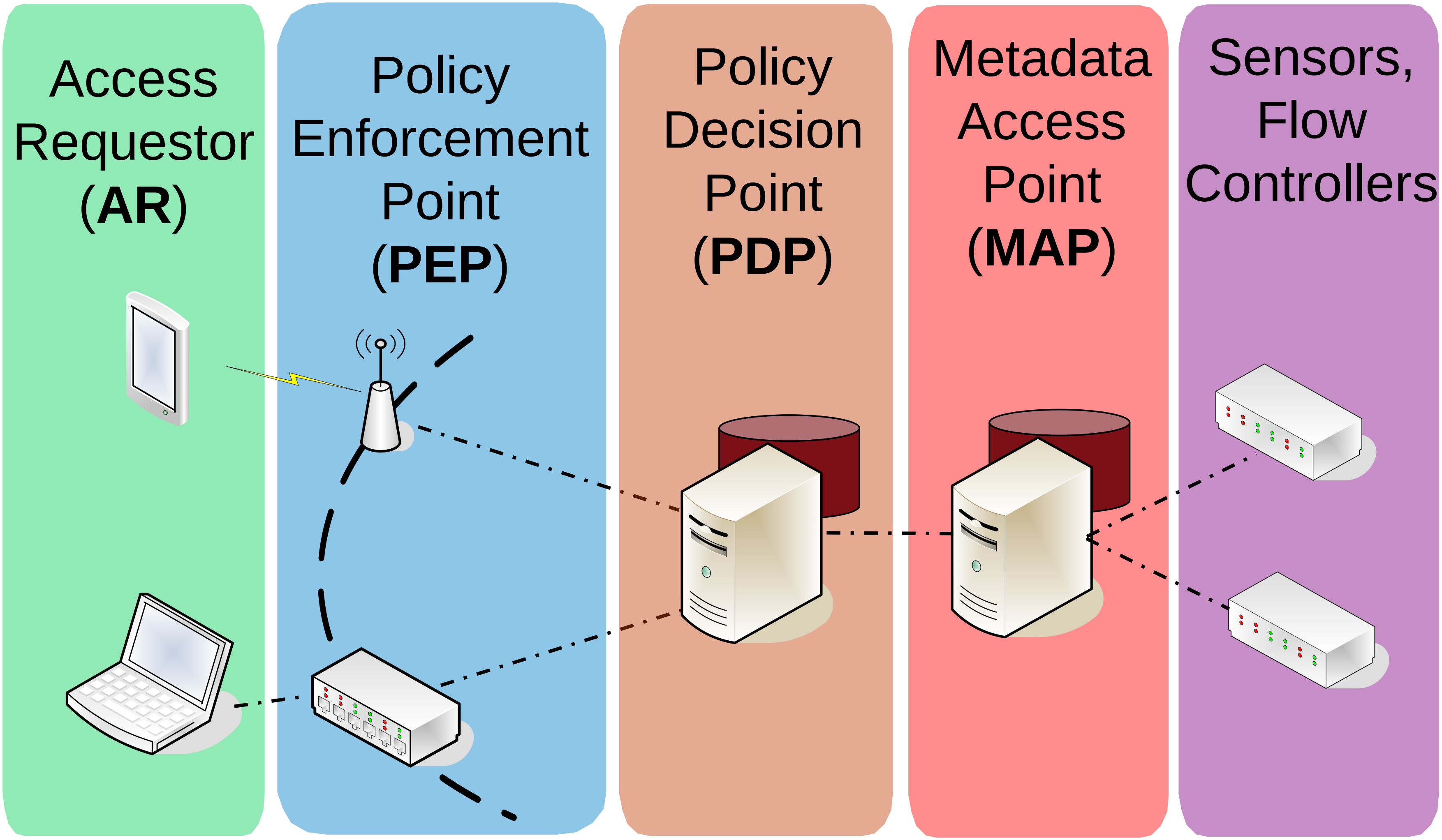


Access Requestor **(AR)**

Policy Enforcement Point **(PEP)**

Policy Decision Point **(PDP)**

Integrating Other Security Devices



Access Requestor (**AR**)

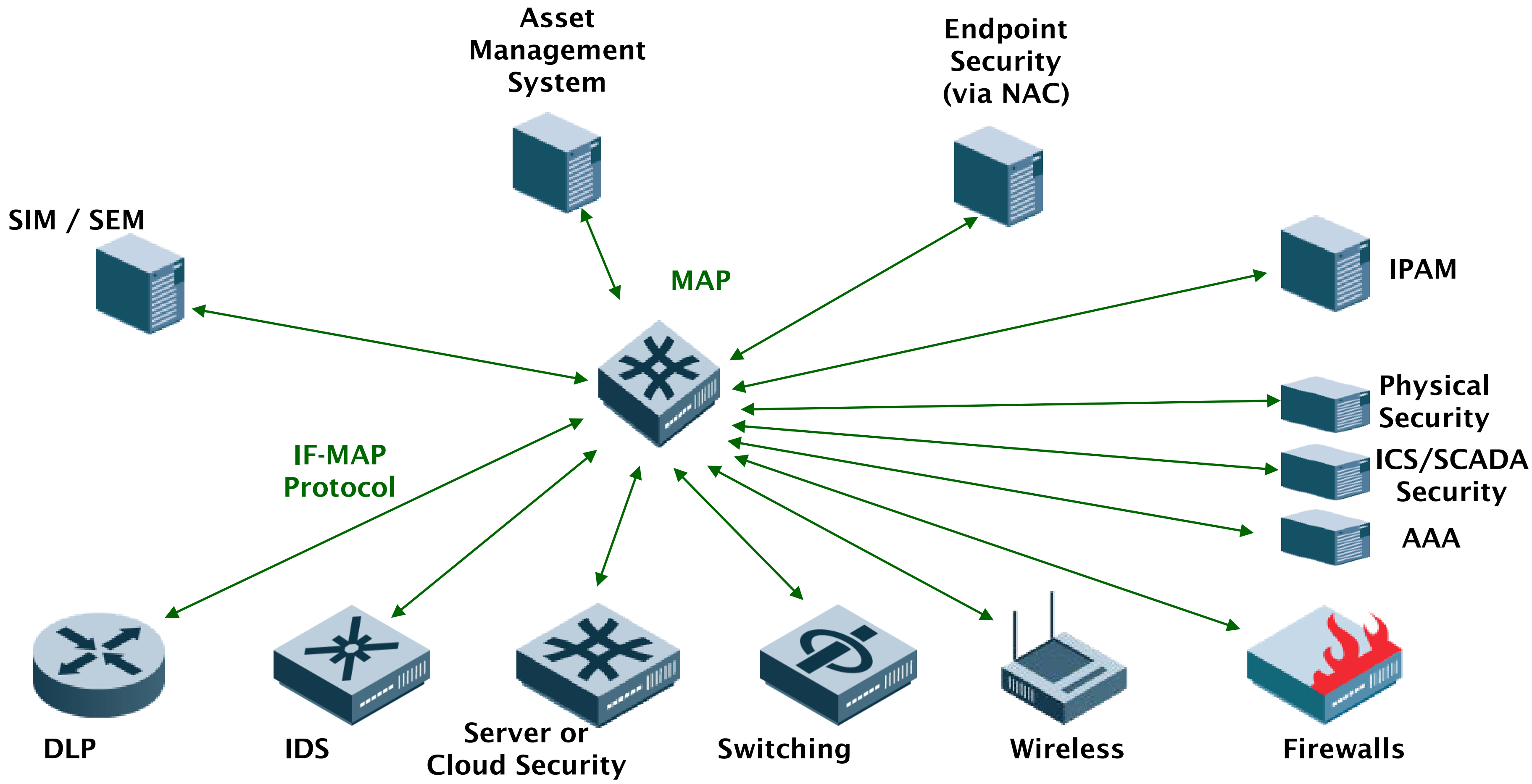
Policy Enforcement Point (**PEP**)

Policy Decision Point (**PDP**)

Metadata Access Point (**MAP**)

Sensors, Flow Controllers

Security Automation



Typical TNC Deployments

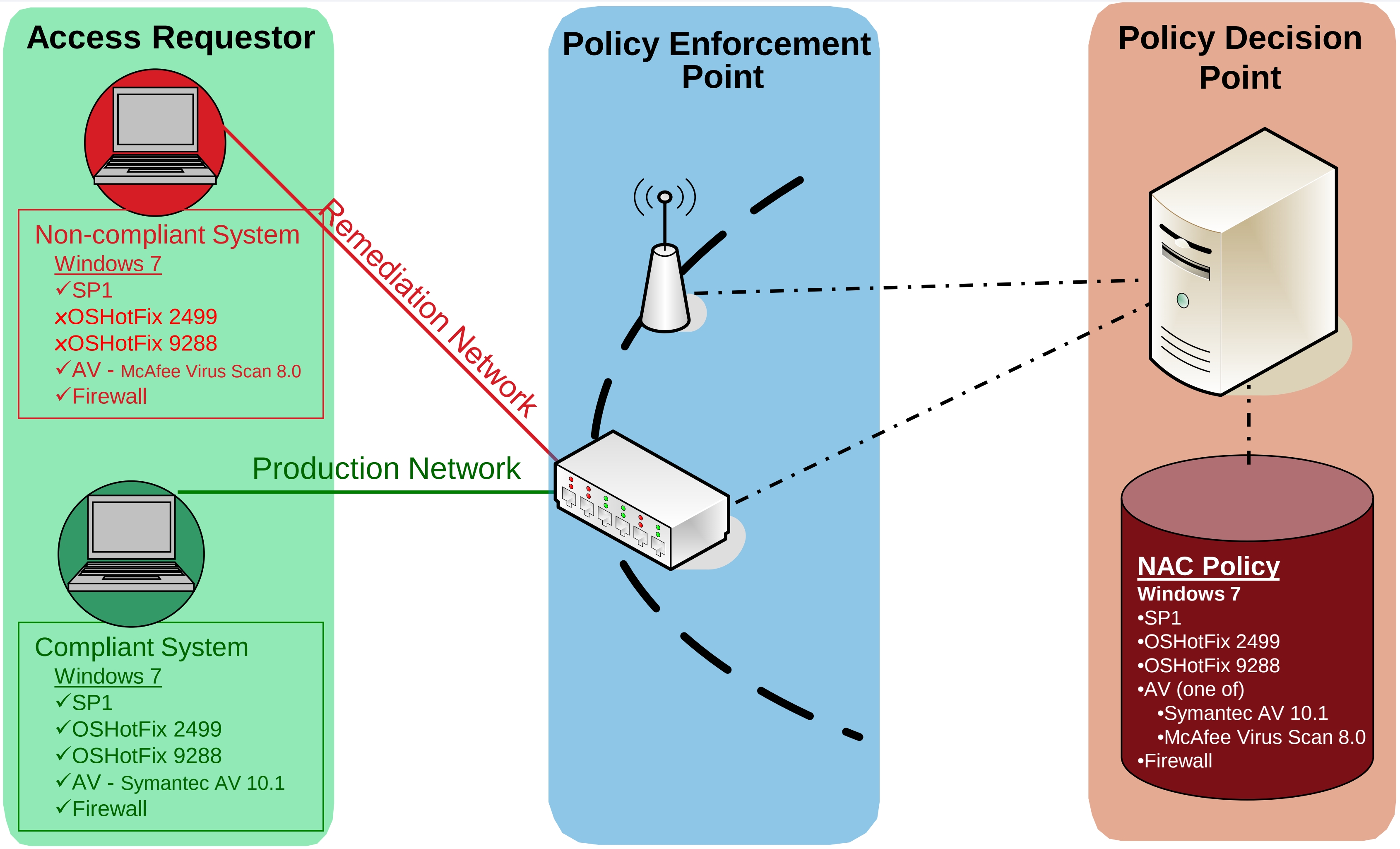
Health Check

Behavior Check

User-Specific Policies

TPM-Based Integrity Check

Health Check



Access Requestor

Non-compliant System

Windows 7
✓SP1
✗OSHotFix 2499
✗OSHotFix 9288
✓AV - McAfee Virus Scan 8.0
✓Firewall

Compliant System

Windows 7
✓SP1
✓OSHotFix 2499
✓OSHotFix 9288
✓AV - Symantec AV 10.1
✓Firewall

Policy Enforcement Point

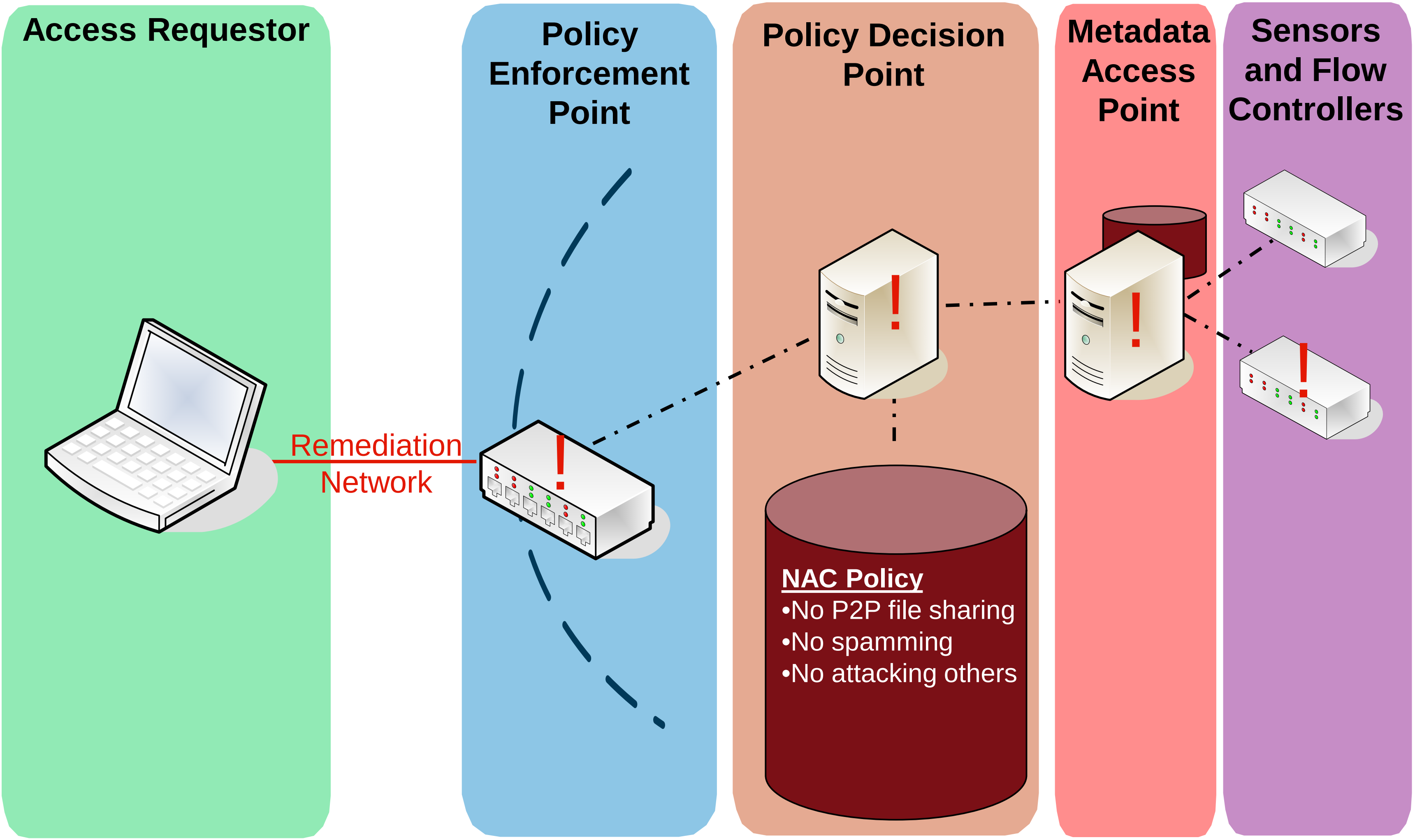
Policy Decision Point

NAC Policy

Windows 7
- SP1
- OSHotFix 2499
- OSHotFix 9288
- AV (one of)
  - Symantec AV 10.1
  - McAfee Virus Scan 8.0
- Firewall

TRUSTED COMPUTING GROUP™

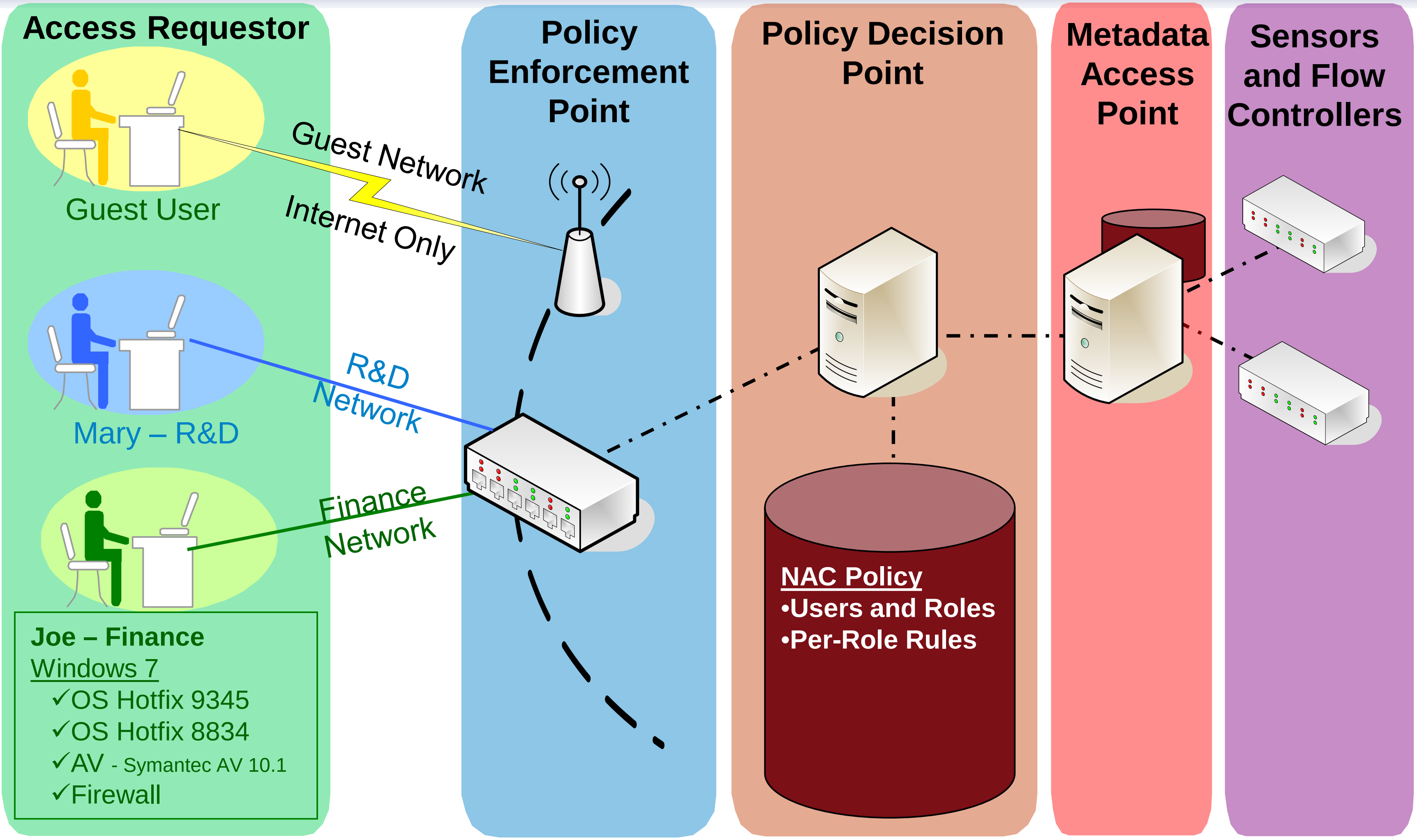
Behavior Check



NAC Policy

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

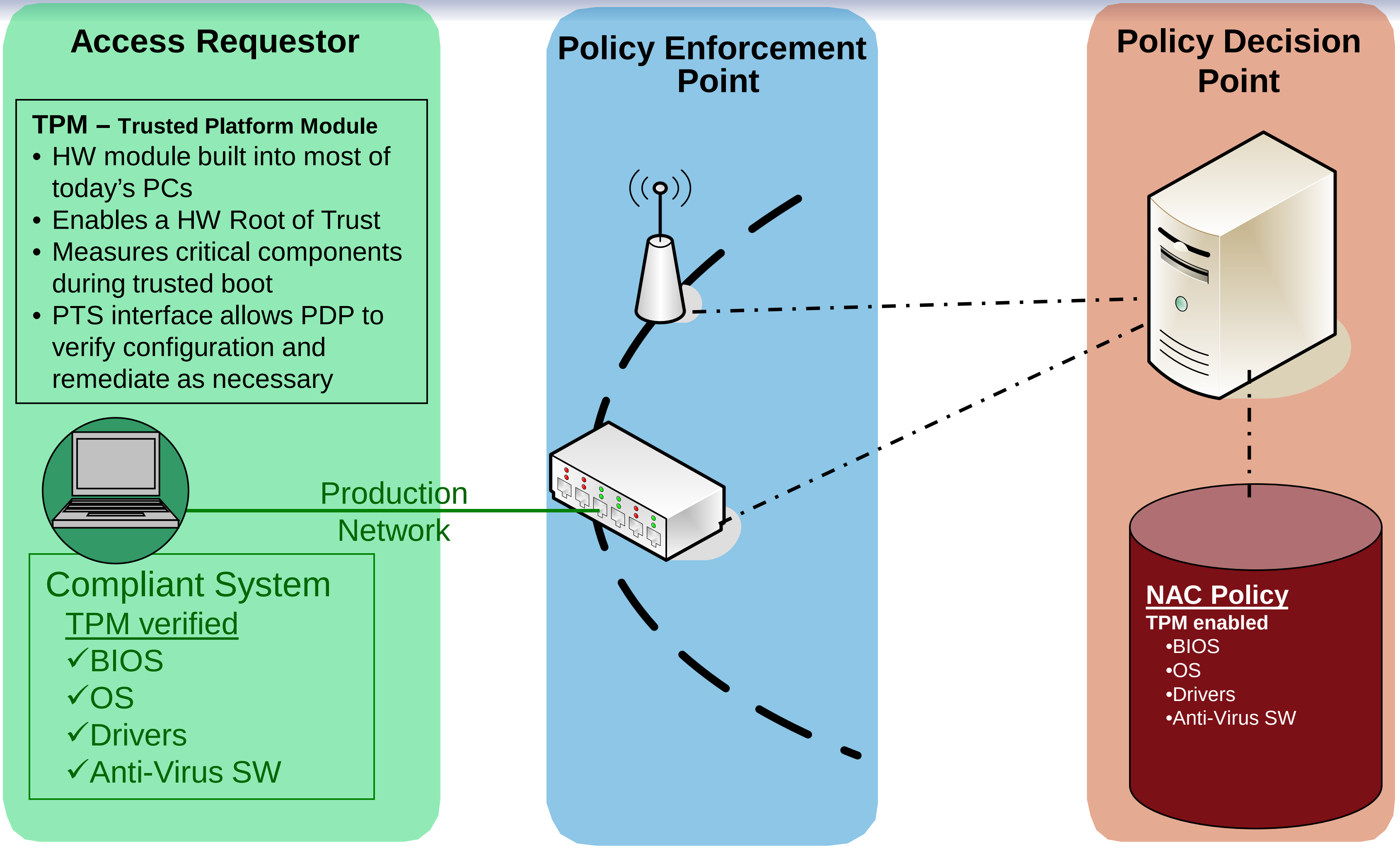
User-Specific Policies



Joe – Finance
Windows 7
✓OS Hotfix 9345
✓OS Hotfix 8834
✓AV - Symantec AV 10.1
✓Firewall

NAC Policy
•Users and Roles
•Per-Role Rules

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

TPM verified

✓BIOS

✓OS

✓Drivers

✓Anti-Virus SW

Policy Enforcement Point

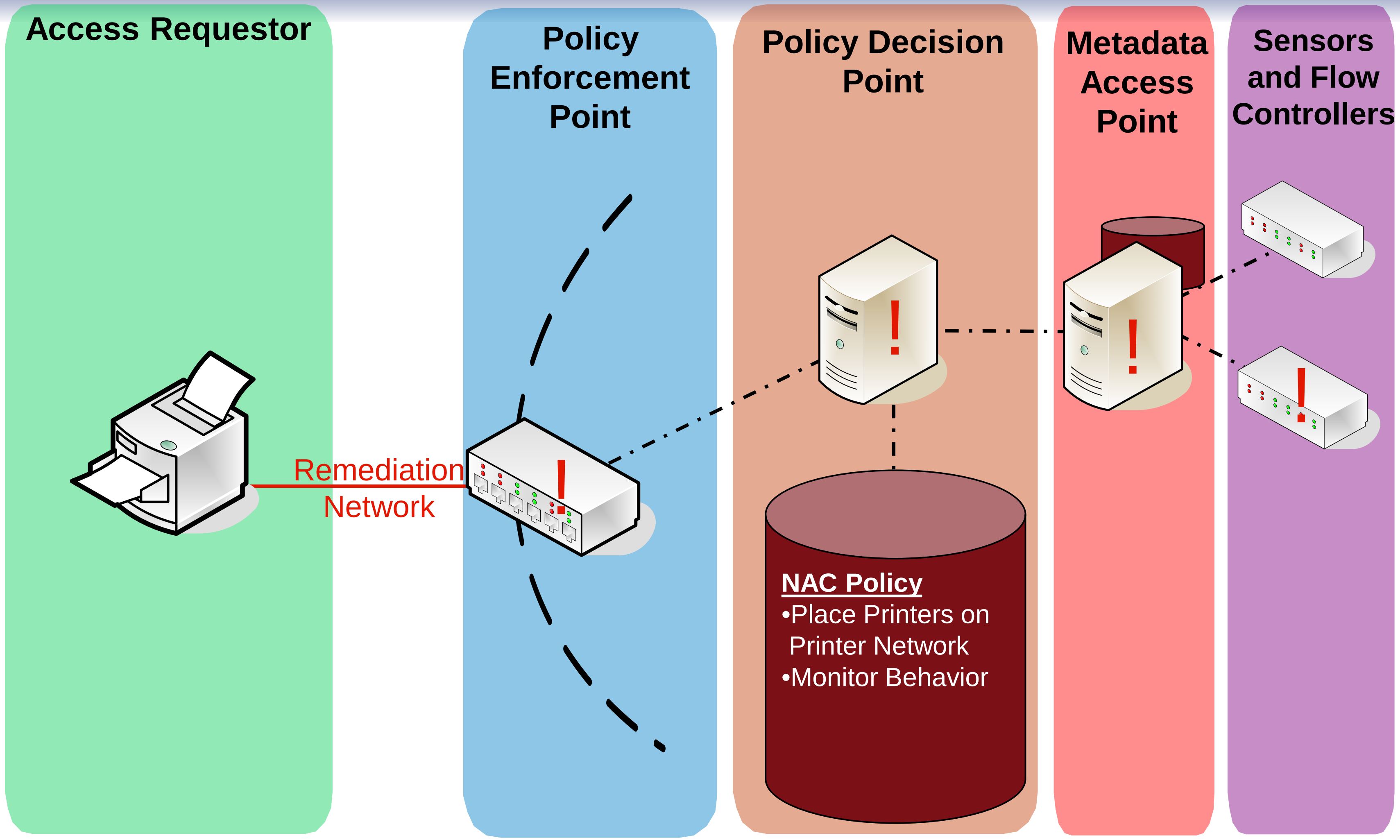
Policy Decision Point

NAC Policy

TPM enabled

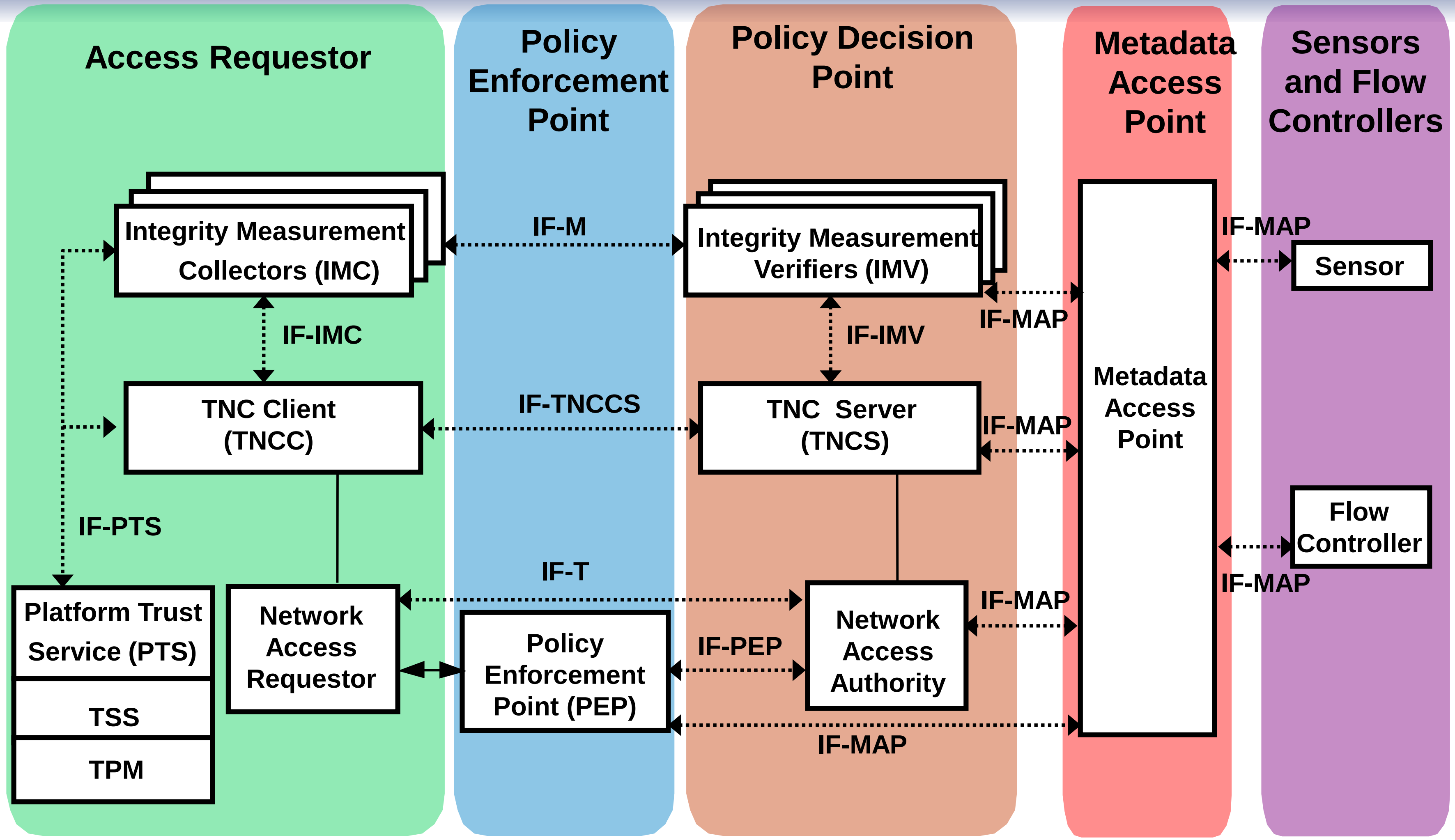
- •BIOS
- •OS
- •Drivers
- •Anti-Virus SW

Clientless Endpoint Handling



NAC Policy
- Place Printers on Printer Network
- Monitor Behavior

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

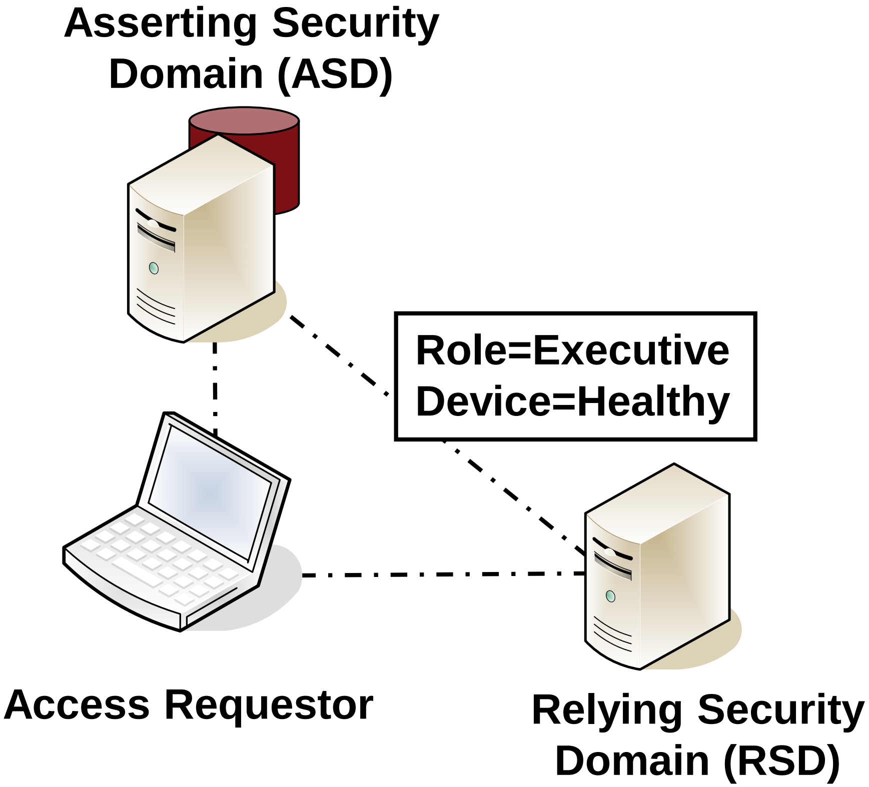
- Web SSO with health info
- Roaming with health check

How?

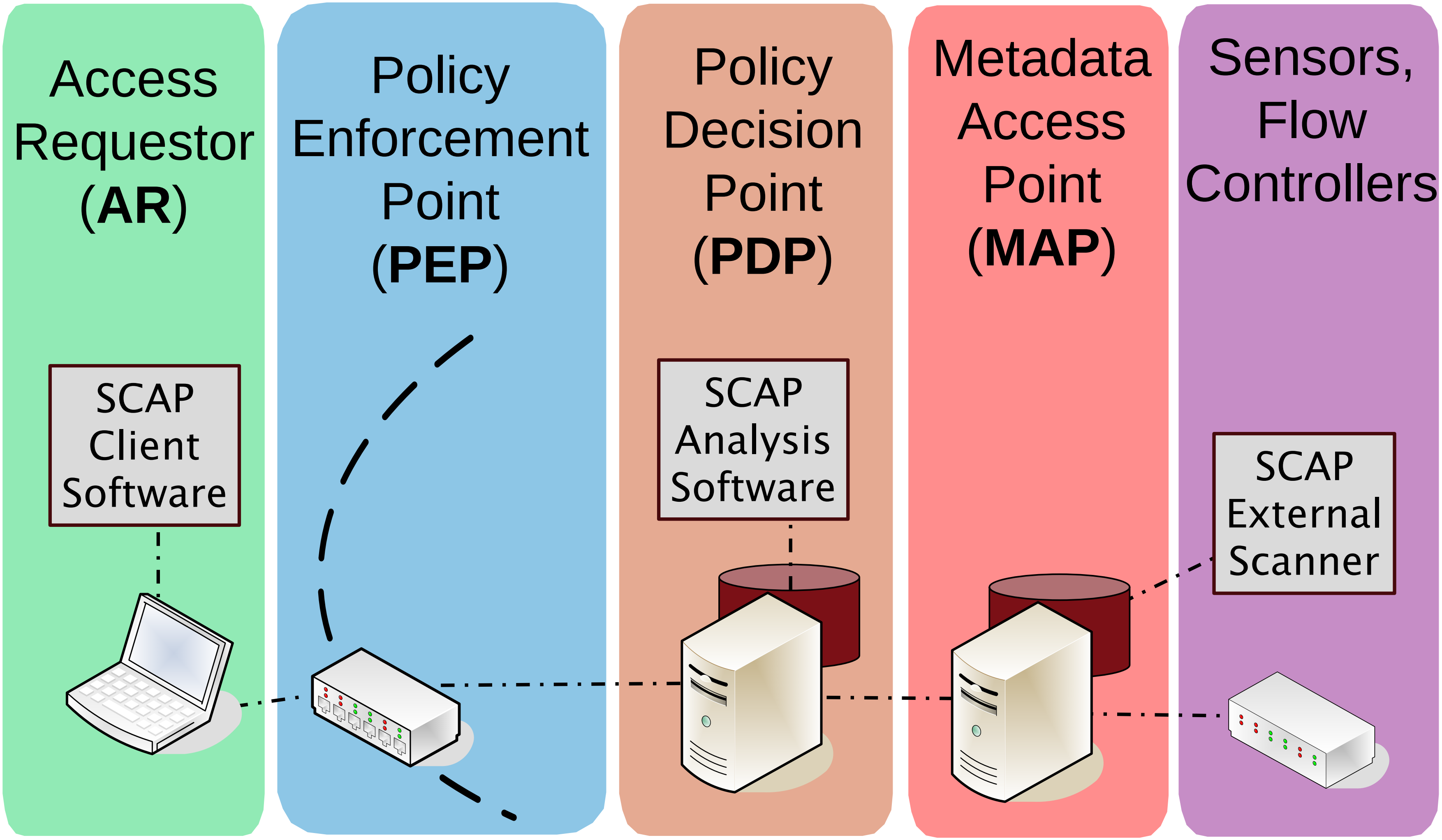
- SAML profiles for TNC

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 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
- CISCO.
- Microsoft
- enterasys® Secure Networks™
- JUNIPER NETWORKS
- IBM®

Policy Decision Point

- symantec.
- Microsoft
- FUJITSU
- IBM®
- JUNIPER NETWORKS
- Q1Labs
- wave®
- enterasys® Secure Networks™
- Triumfant™
- StillSecure®
- GENERAL DYNAMICS C4 Systems
- McAfee®

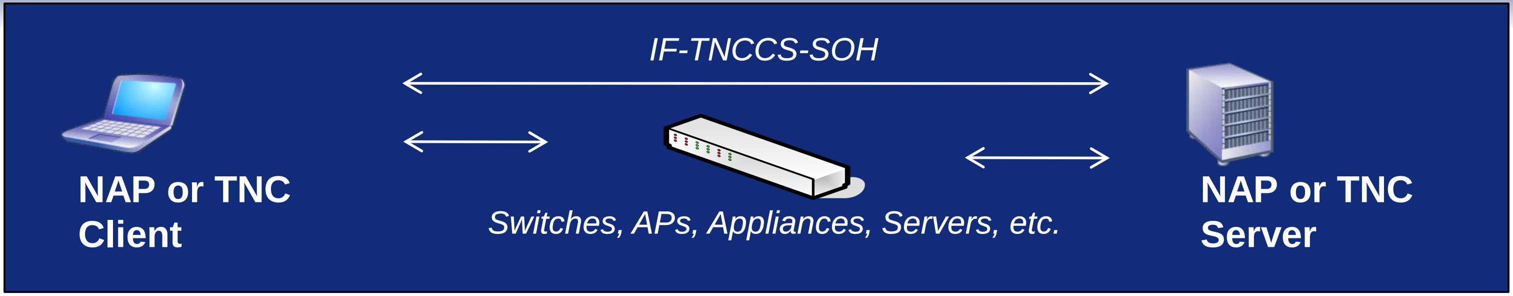
Metadata Access Point

- Infoblox
- JUNIPER NETWORKS

Sensors, Flow Controllers

- ArcSight
- Great Bay Software Inc.
- Asguard Networks
- ARUBA
- JUNIPER NETWORKS
- LUMETA®
- HIRSCH ELECTRONICS
- macmon®
- NCP SECURE COMMUNICATIONS
- insightiX
- TOFINO™

Windows Support



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 all supported versions of Microsoft Windows
- 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), PB-TNC (RFC 5793), PT-TLS (RFC 6876)
- Equivalent to TCG's IF-M 1.0, IF-TNCCS 2.0, and IF-T/TLS
- Co-Editors from Cisco, Intel, Juniper, Microsoft, Symantec

Now working on getting IETF approval for IF-T/EAP

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

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

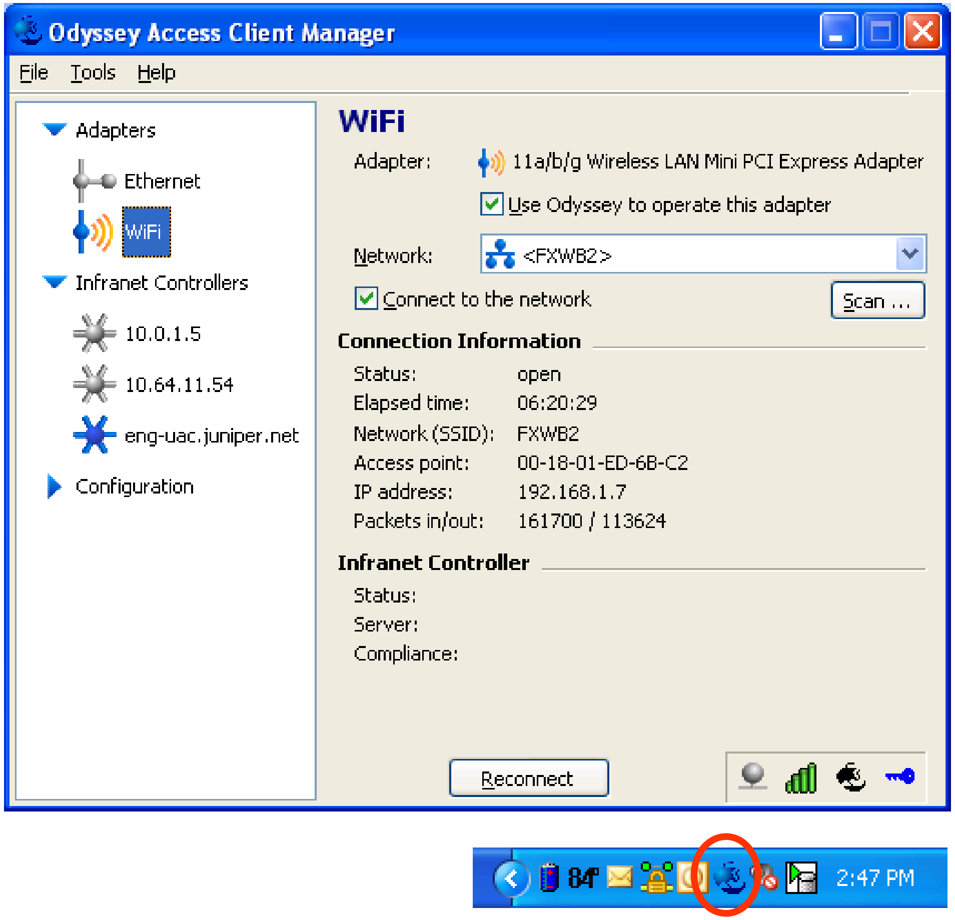
St. Mary’s County Public Schools - Solution

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:

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

Lisa Lorenzin

Principal Solutions Architect, Juniper Networks

llorenzin@juniper.net

Atul Shah

Senior Security Strategist, Microsoft

atuls@microsoft.com