Putting Trust Into The Network

Securing Your Network Through Trusted Access Control

Steve Hanna, Juniper Networks
Co-Chair, Trusted Network Connect Sub Group
of Trusted Computing Group

ACSAC
December 2006

Talk Outline

- Problem Statement
- Various Solutions
- Trusted Access Control
- Q & A

TRUSTED COMPUTING GROUP™

Problem: Reduce Endpoint Attacks

- Motivated Attackers
  - Extortion, Identity Theft, Bank Fraud, Corporate Espionage
- Increasingly Sophisticated and Serious Attacks
  - Viruses, Worms, Spyware, Rootkits, Back Doors, Botnets
  - Zero-Day Exploits, Targeted Attacks, Rapid Infection Speed
- Exponential Growth in Malware
  - >40,000,000 Infected Machines, >35,000 Malware Varieties
- Dissolving Network Boundaries
  - Mobile workforce, partners, contractors, outsourcing
- Regulatory Requirements

TRUSTED COMPUTING GROUP™

Various Solutions

- More Secure Endpoints
  - AV, Personal Firewall, Patch Management
  - Better Coding Practices, Anti-Spyware, HIPS
- Stronger Network Protection
  - Firewalls, IDS, IPS, Vulnerability Scanners
  - Network Access Control (NAC)
- But Endpoints Still Get Compromised
  - And then what?

TRUSTED COMPUTING GROUP™

Trusted Access Control =

Trusted Platform Module

+

Network Access Control

Trusted Platform Module

- Hardware Security Component
  - Key storage
  - Signing and encryption
  - Secure and Trusted Boot
  - Remote attestation
- Open Standards for Features and APIs
  - Developed by Trusted Computing Group
- Included on all new commercial laptops, increasing number of desktops and servers

TRUSTED COMPUTING GROUP™

Network Access Control

- Check Endpoint Health against Policy
  - At or After Network Connection
  - If Unhealthy, Quarantine and Remediate
- But what about lying endpoints?
  - Need Trusted Boot and Remote Attestation

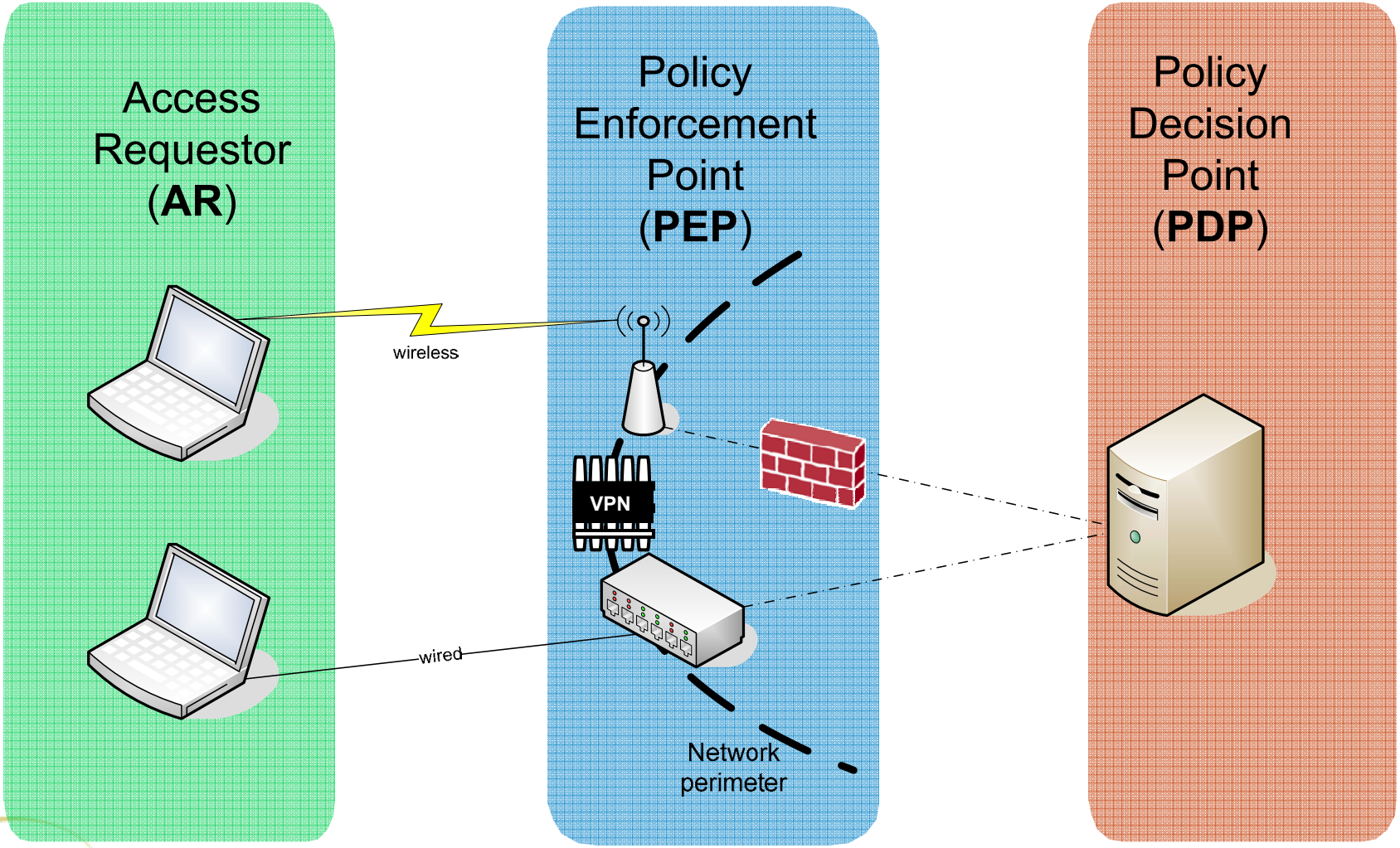
TRUSTED COMPUTING GROUP™

Trusted Network Connect (TNC)

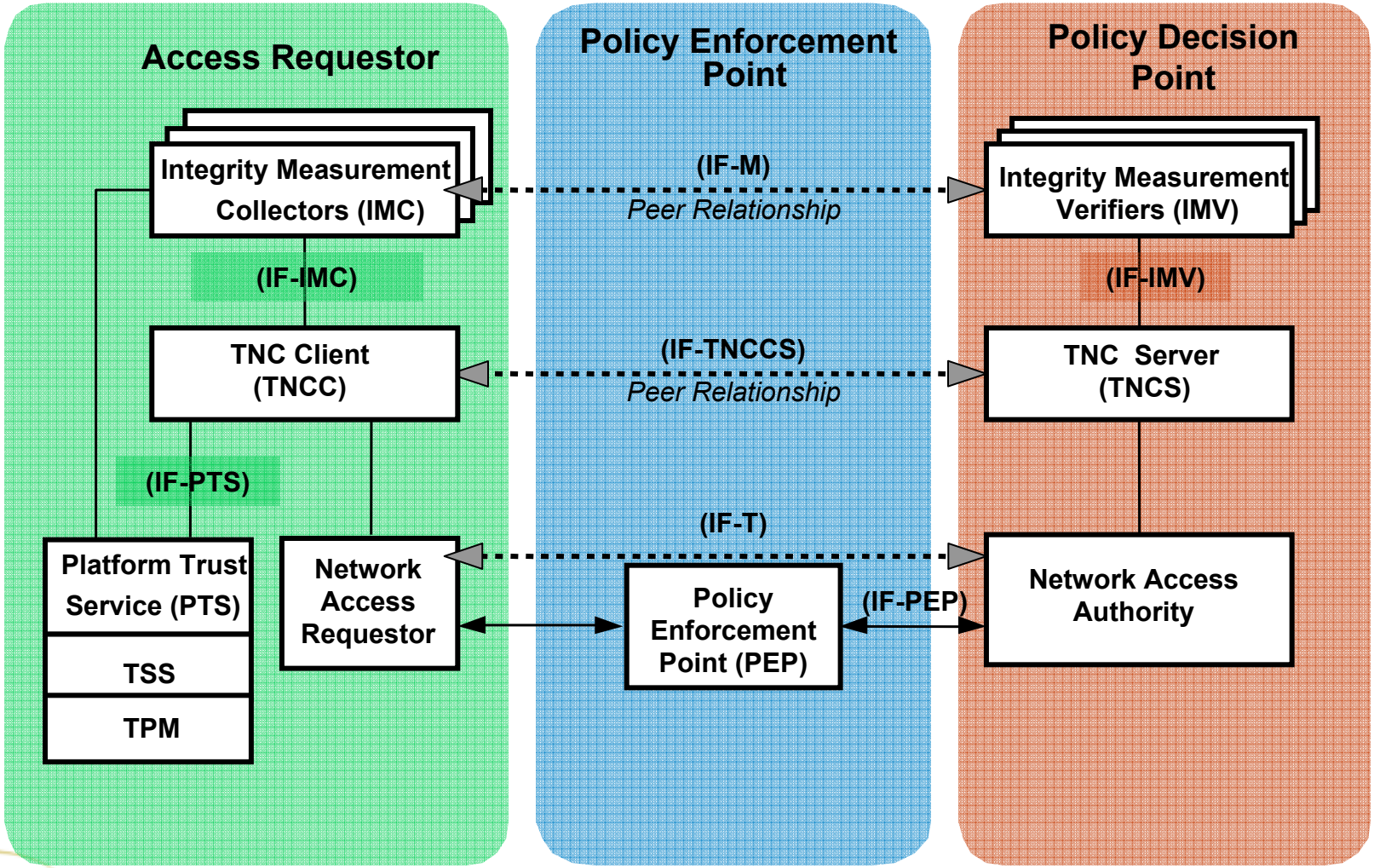
- Open Architecture for Network Access Control (NAC)
- Suite of Standards
- Developed by Trusted Computing Group
- Supports Trusted Access Control

TRUSTED COMPUTING GROUP™

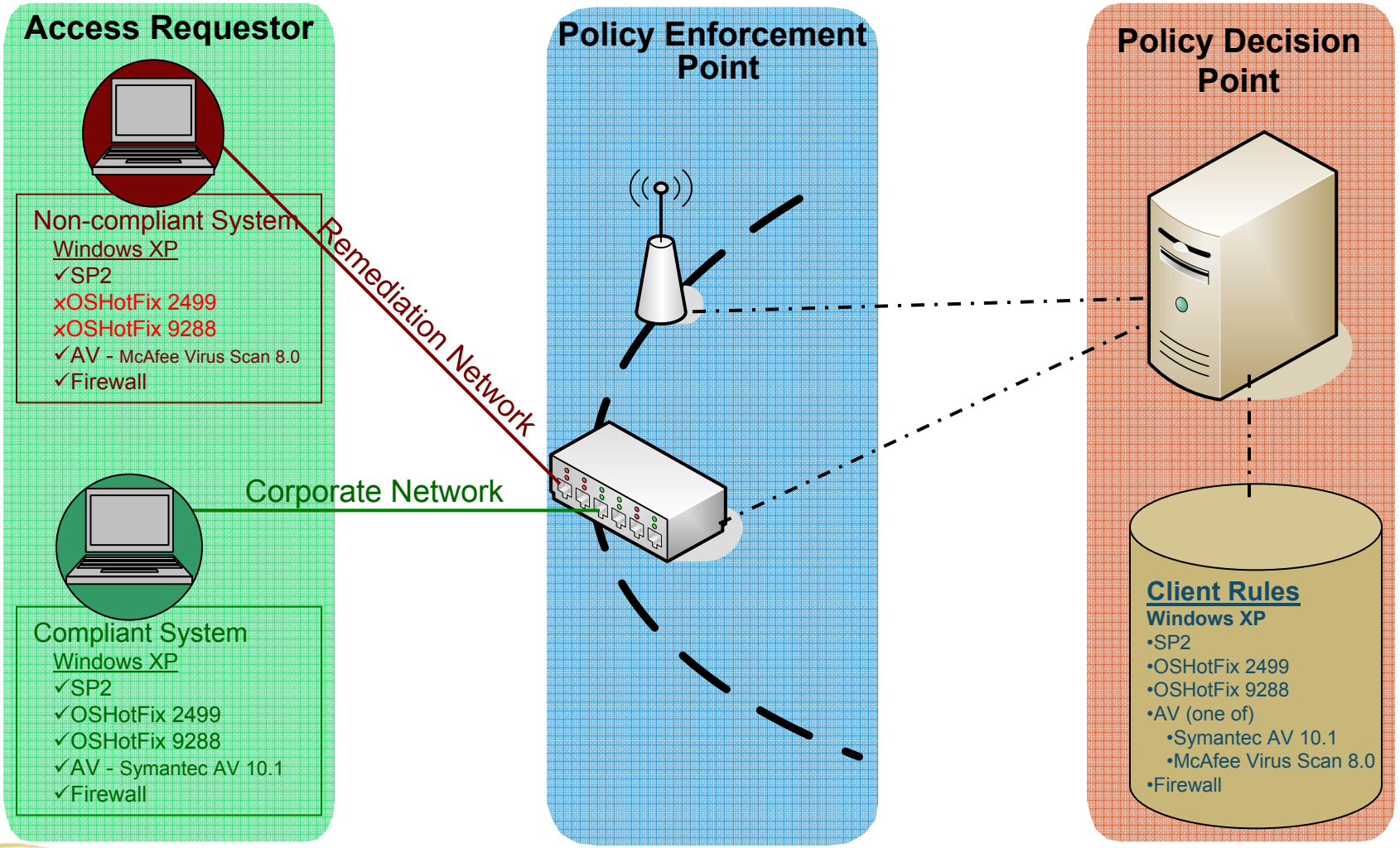
TNC Architecture



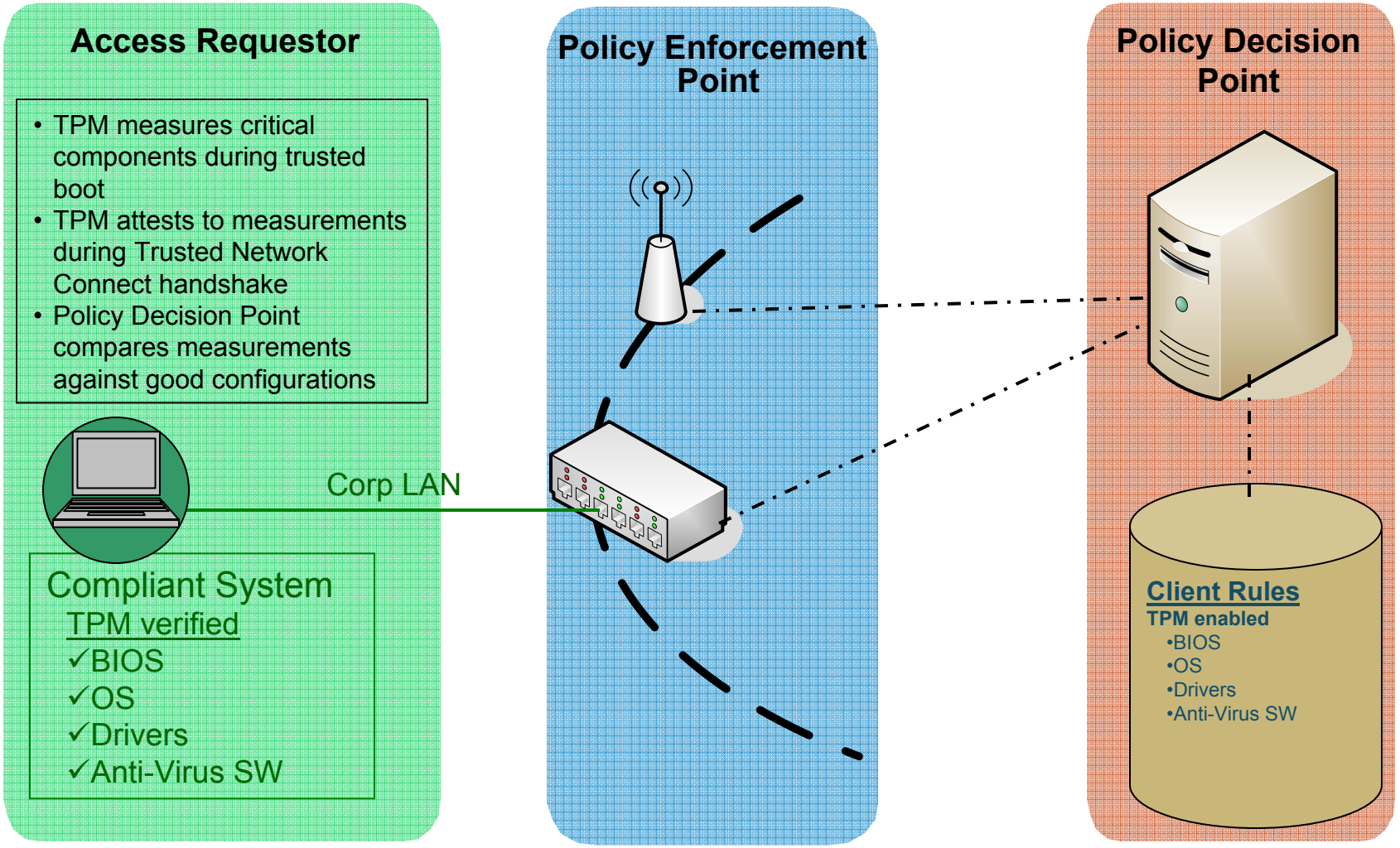
TNC Standards



Network Access Control Use Case



Trusted Access Control Use Case

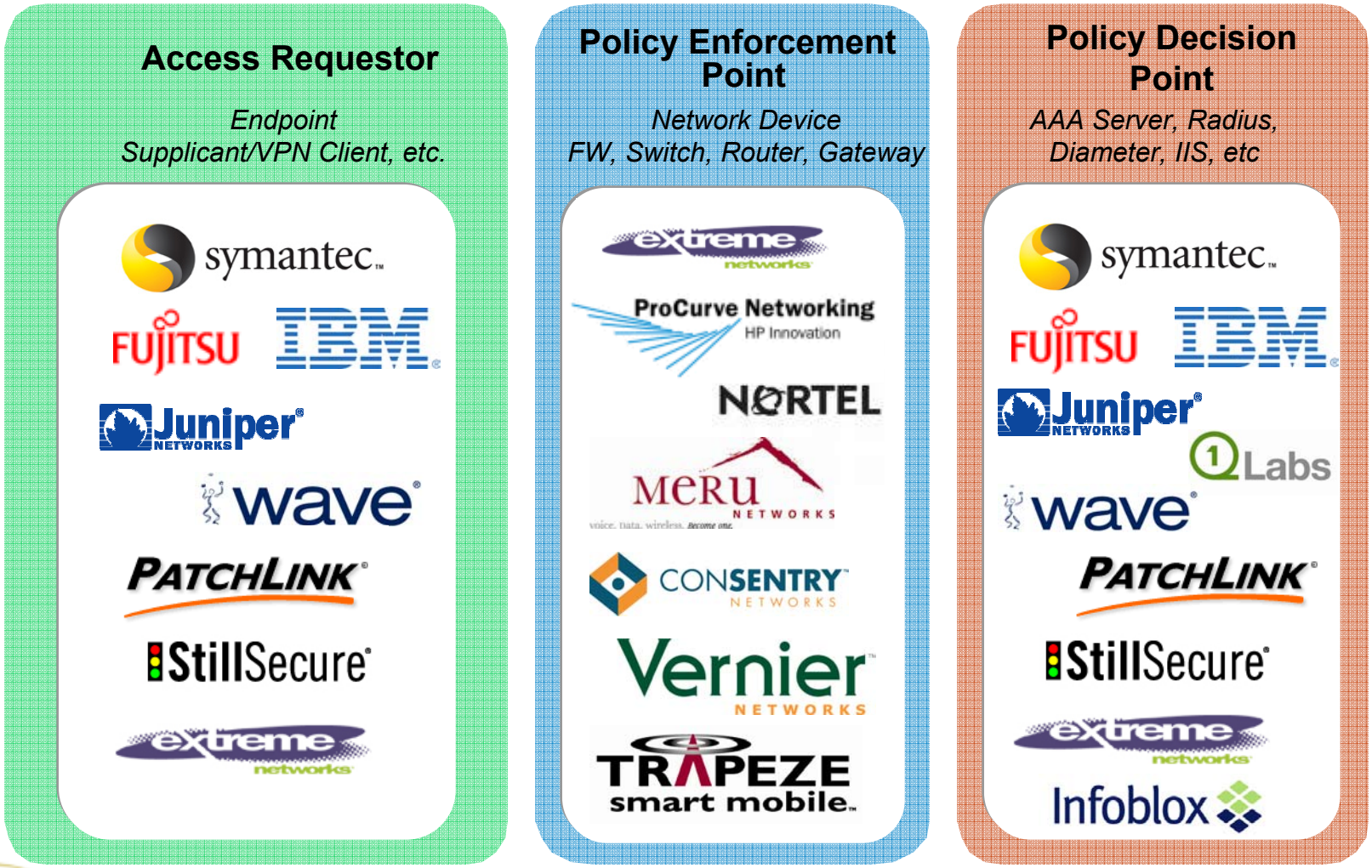


Trusted Network Connect (TNC) Advantages

- Open standards
  - Non-proprietary – Supports multi-vendor compatibility
  - Enables customer choice
  - Allows thorough and open technical review
- Leverages existing network infrastructure
  - Excellent Return-on-Investment (ROI)
- Strong security
  - Trusted Platform Module (TPM)
  - Solves lying endpoint problem
- Products supporting TNC standards shipping today
  - Including open source implementations

TRUSTED COMPUTING GROUP™

TNC Vendor Support



TRUSTED COMPUTING GROUP™

Q & A