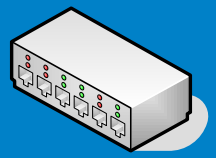
Copyright © 2011 Trusted Computing Group

Access Requestor (**AR**)

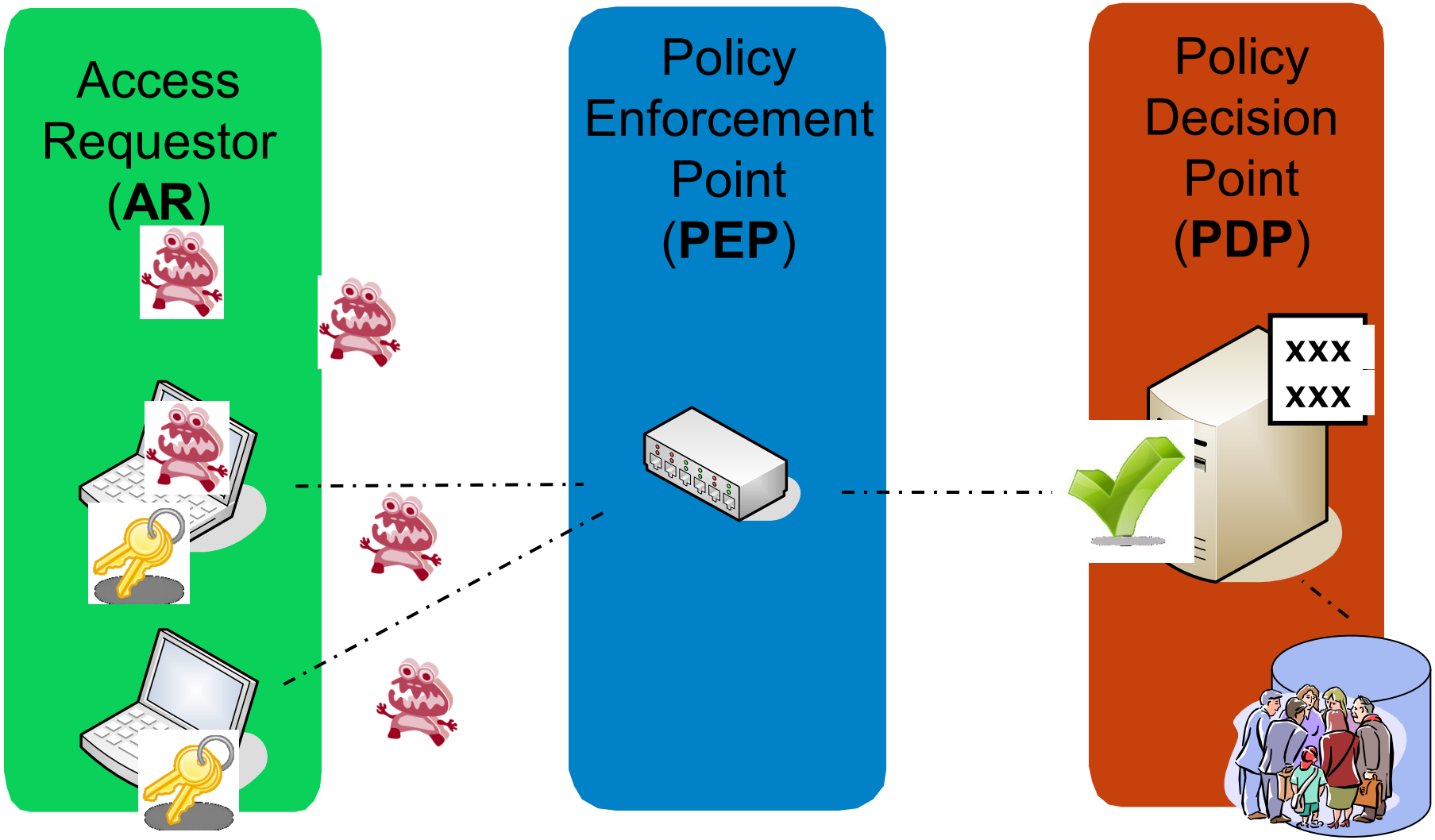
Policy Enforcement Point (**PEP**)



Policy Decision Point (**PDP**)

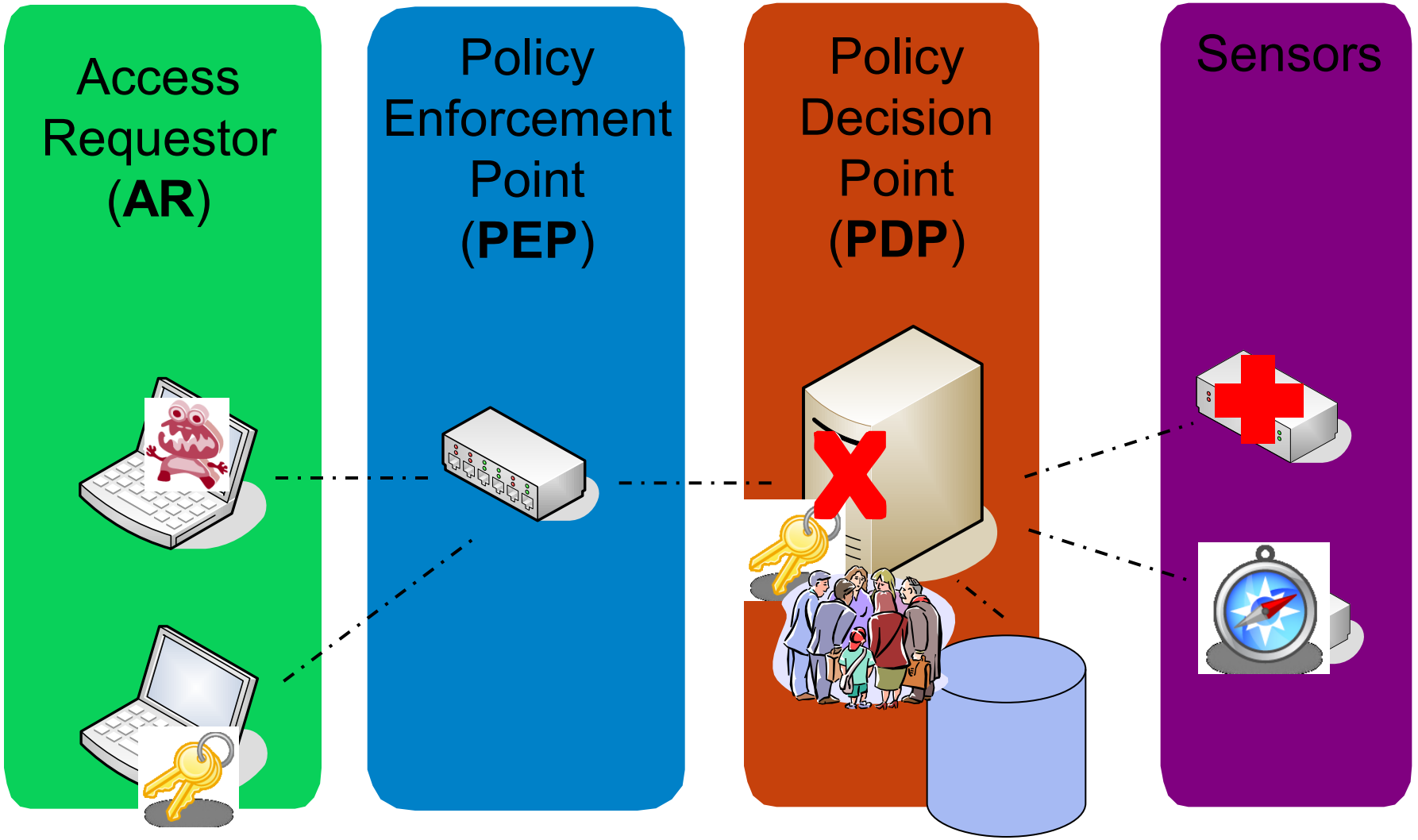
TRUSTED COMPUTING GROUP™

Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.



TRUSTED COMPUTING GROUP™

Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.



TRUSTED COMPUTING GROUP™

Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.

But How?

Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.

Open Standards for Gathering Additional Factors

- Device Health
- Location
- Behavior

Works at Application Layer or at Network Layer

- Enables Many Implementation Options

Strong Security

- Confidentiality – Sensitive Information
- Integrity – Accurate Information is Essential

Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.

Briefing on TNC

Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.

Open Architecture for Network Security

- Completely vendor-neutral
- Strong security through trusted computing

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

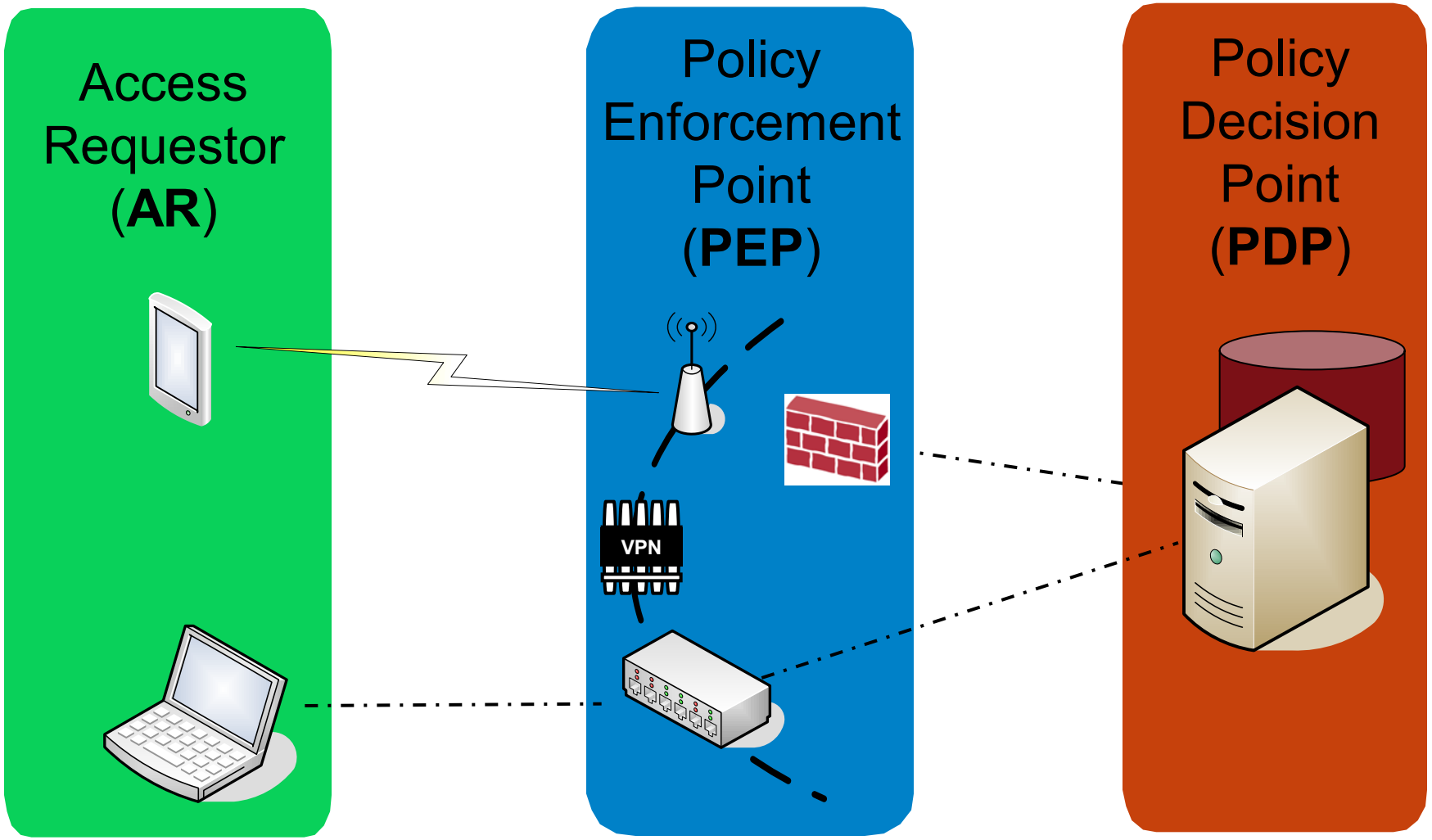
Also Approved by IETF

Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.

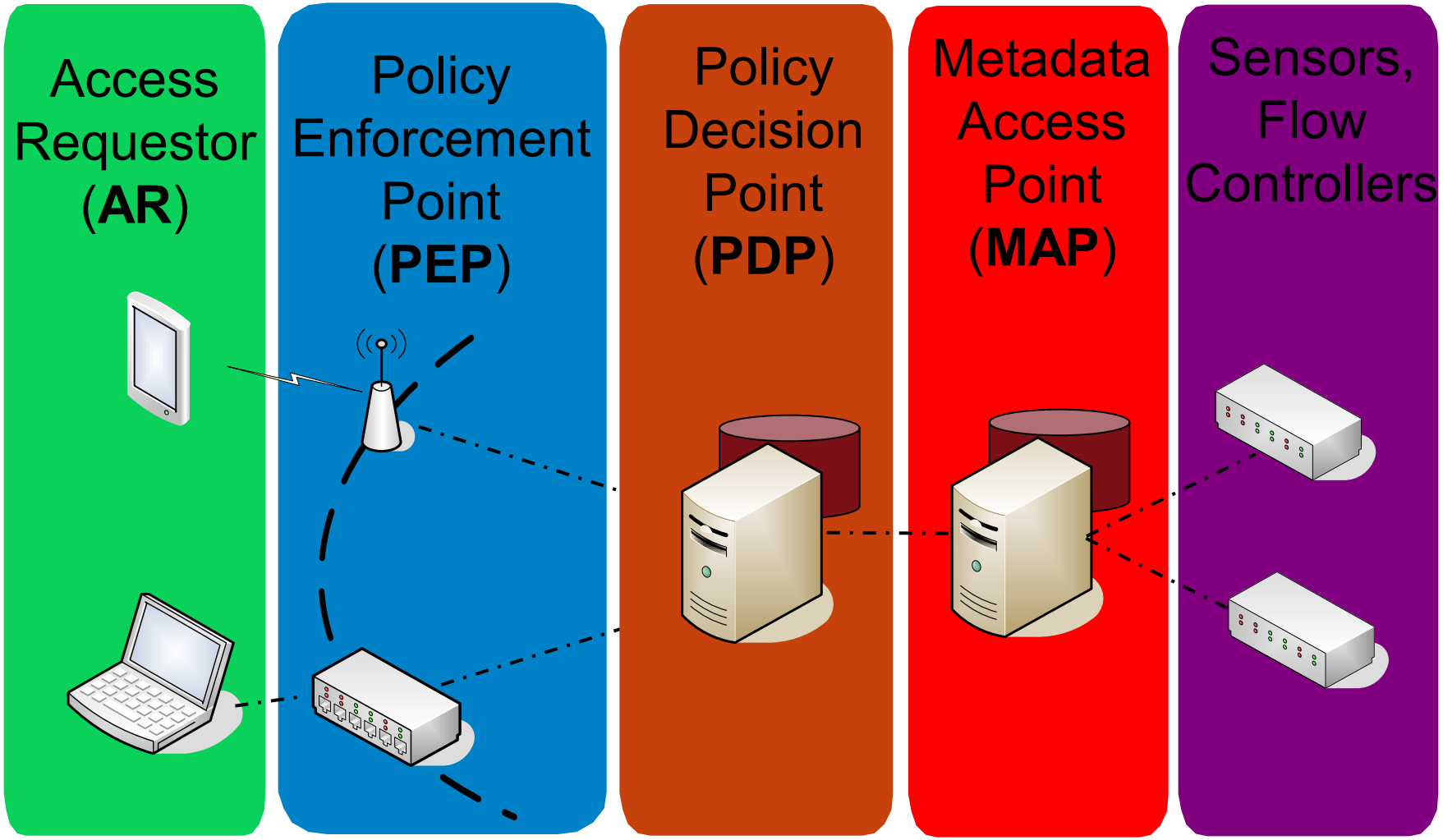
Network Access Control (NAC)

Coordinated Security

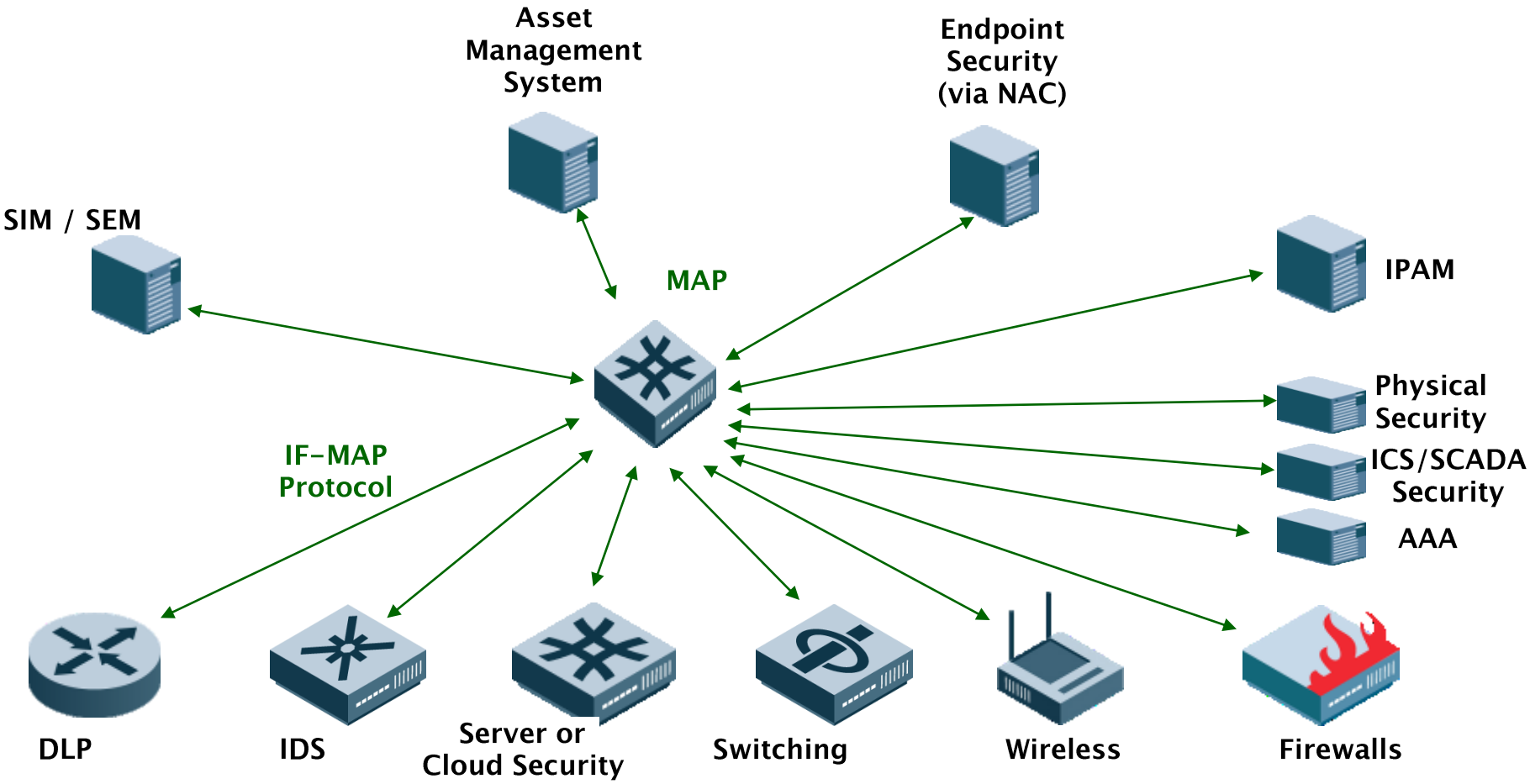
Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.



TRUSTED COMPUTING GROUP™
Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.



TRUSTED COMPUTING GROUP™
Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.



Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.

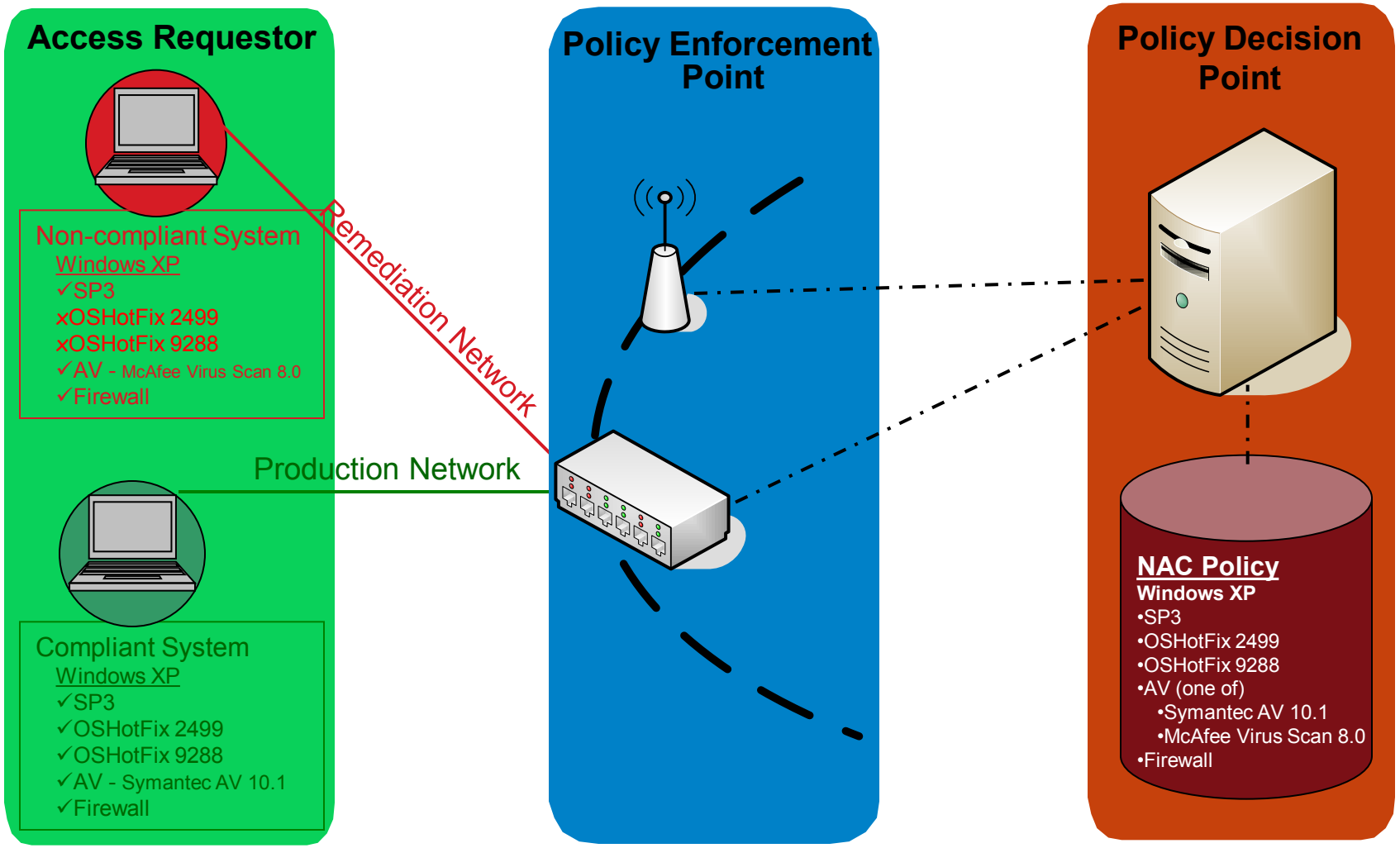
Health Check

Behavior Check

User-Specific Policies

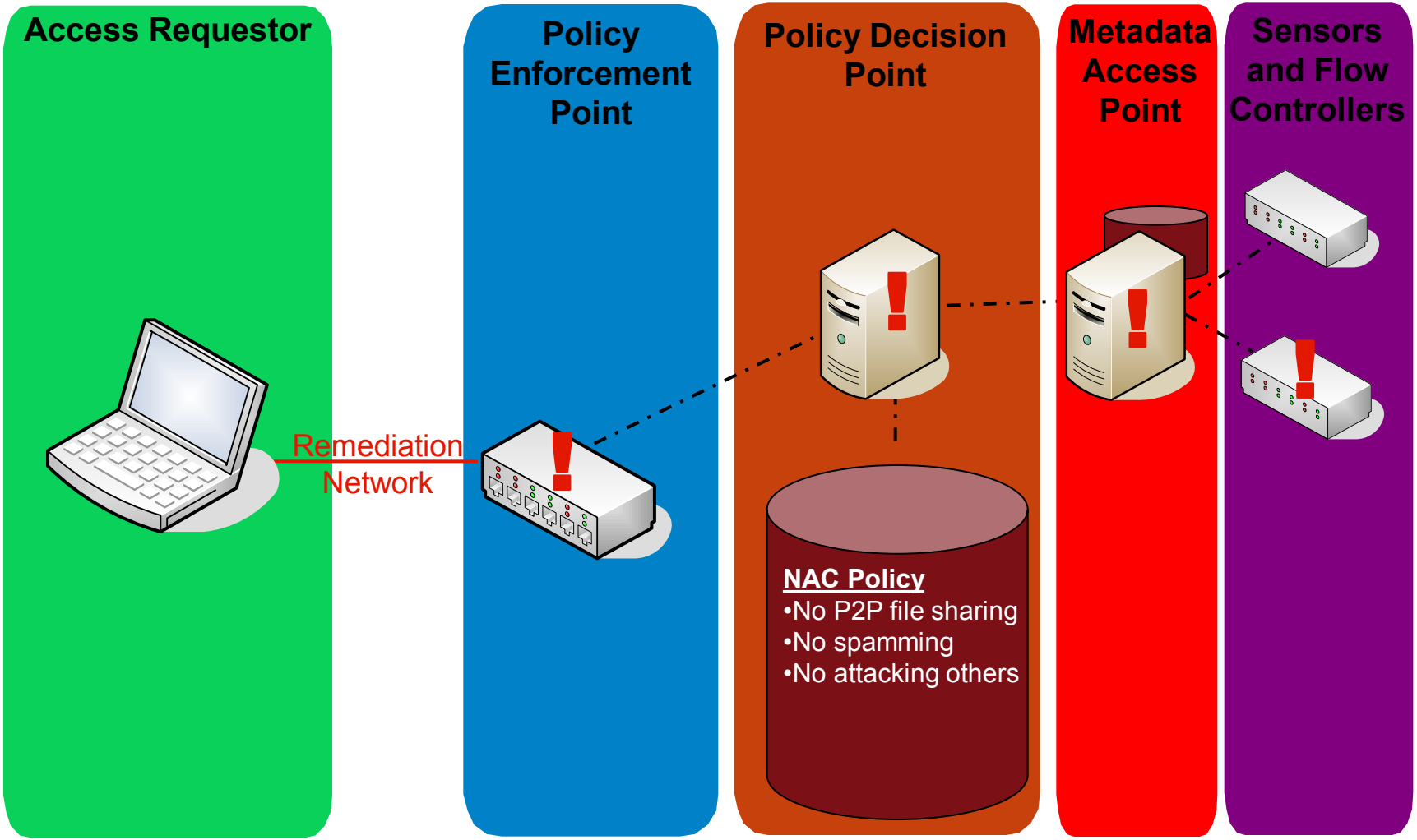
TPM-Based Integrity Check

TRUSTED COMPUTING GROUP™ Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.

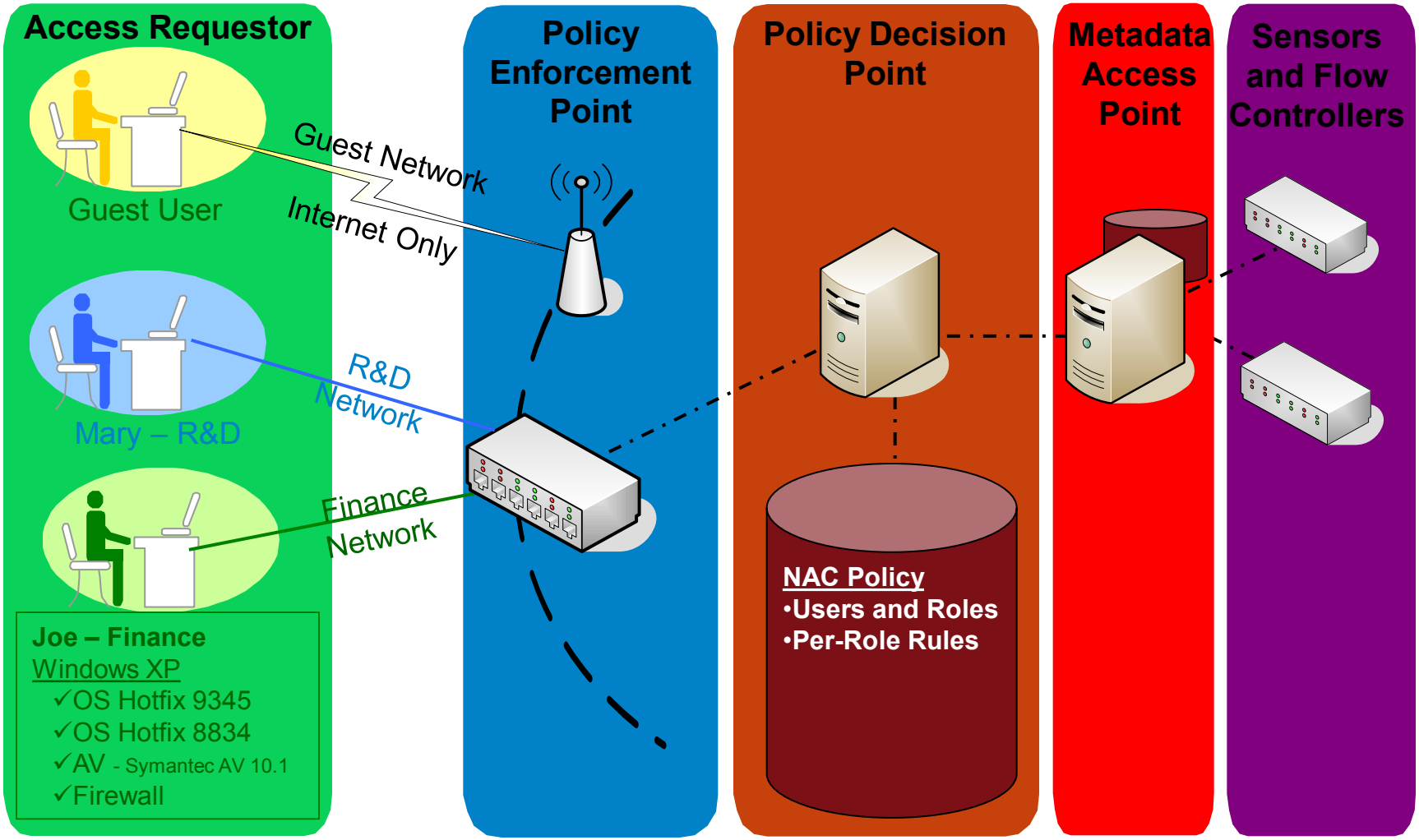


TRUSTED COMPUTING GROUP™

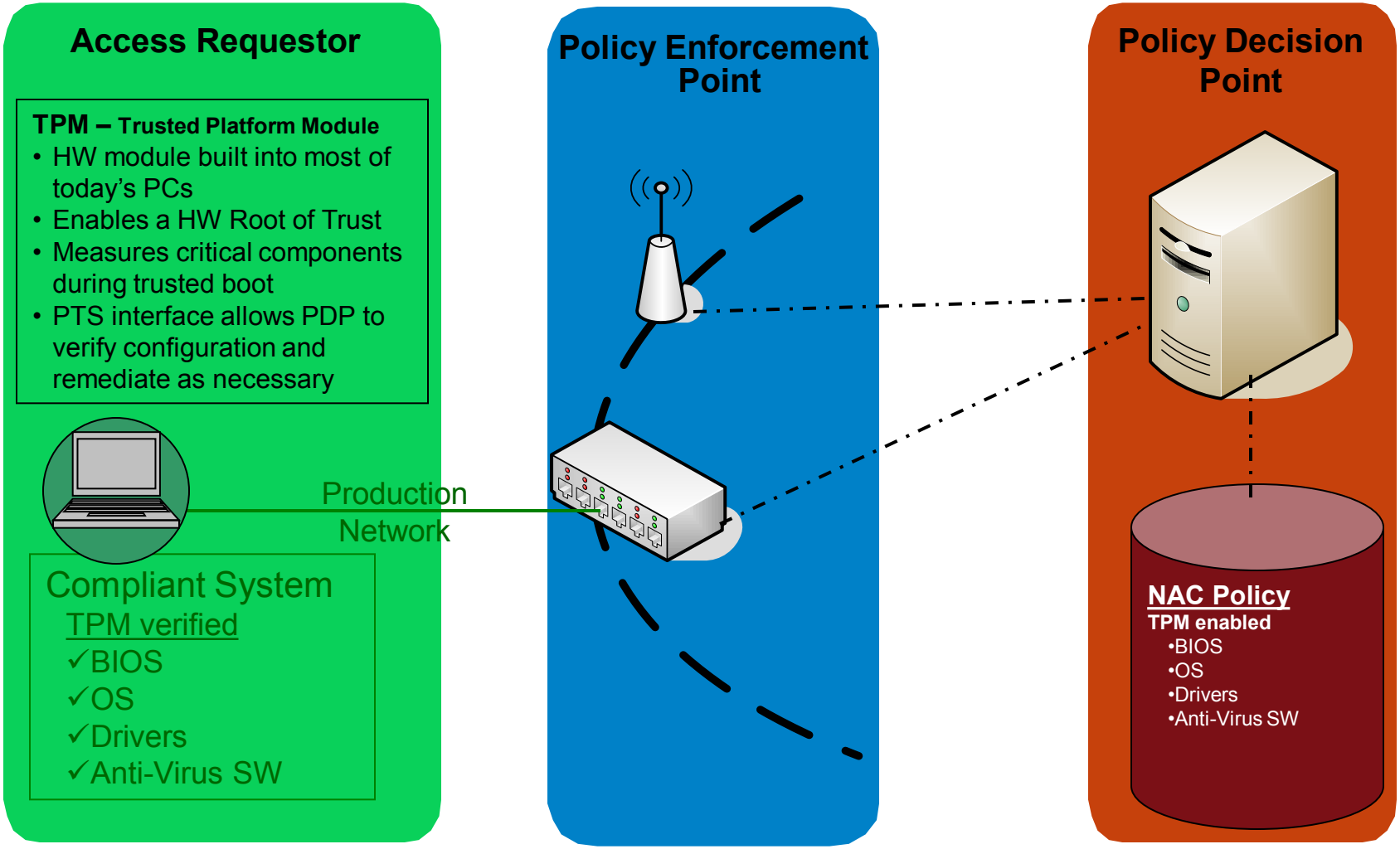
Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.



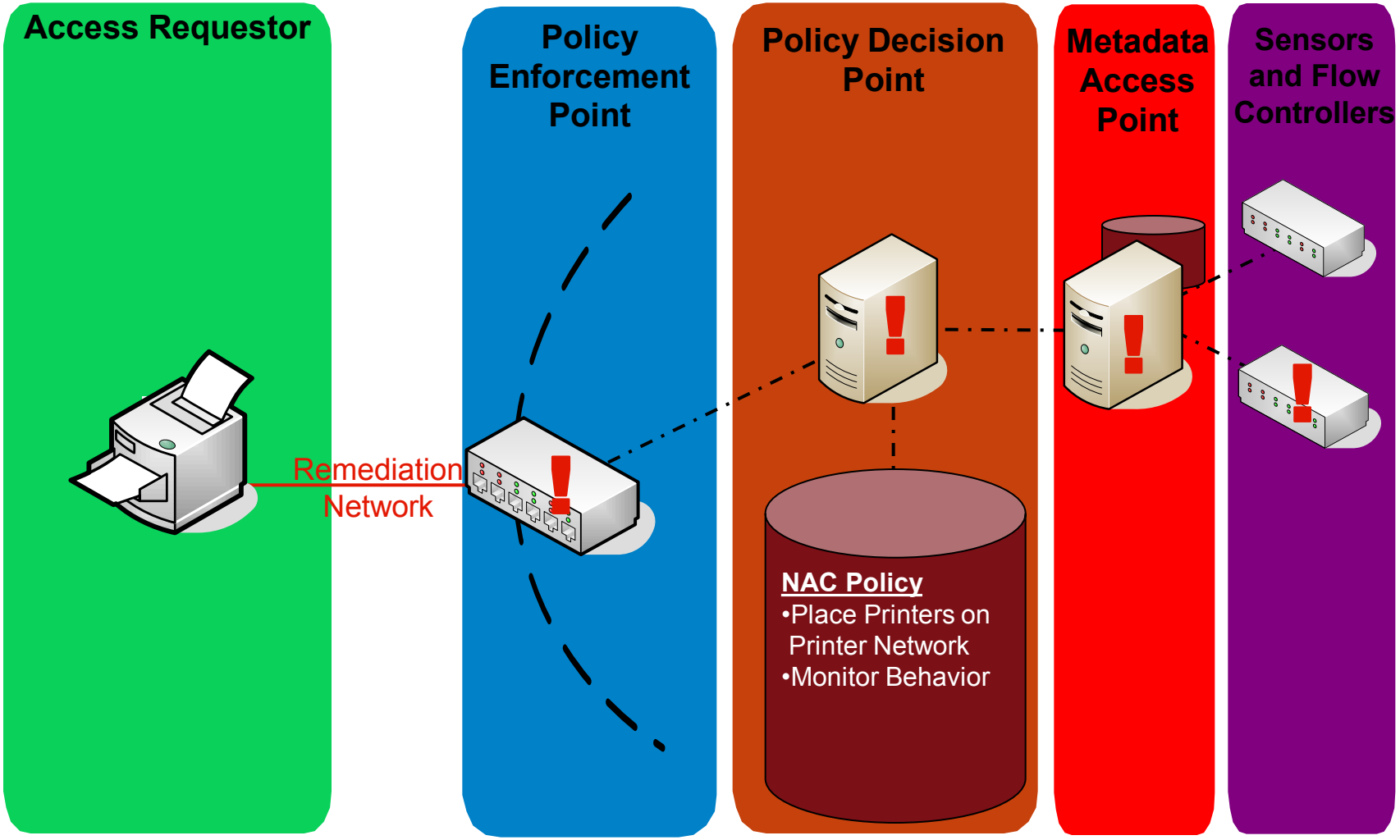
TRUSTED COMPUTING GROUP™
Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.



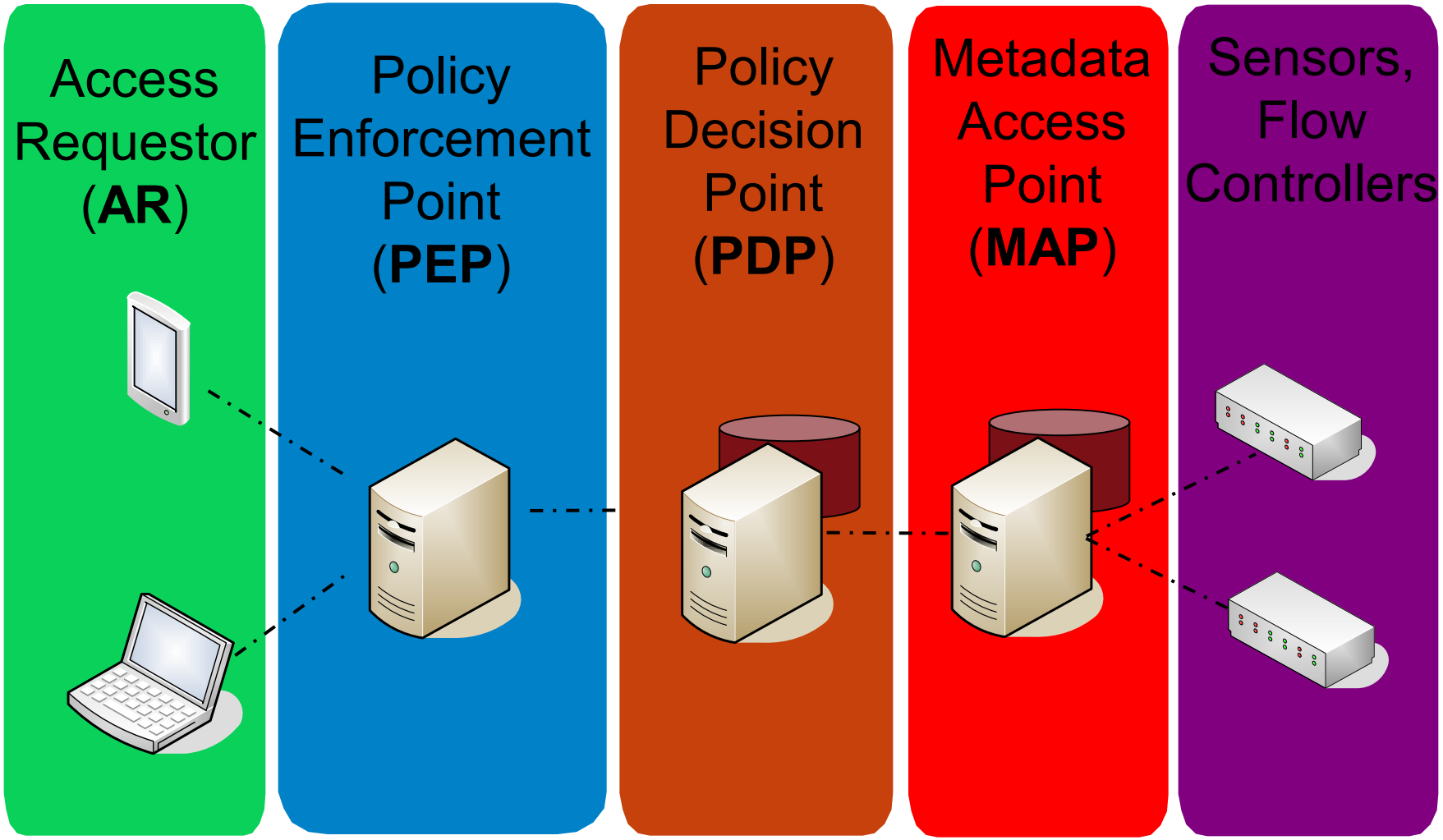
Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.



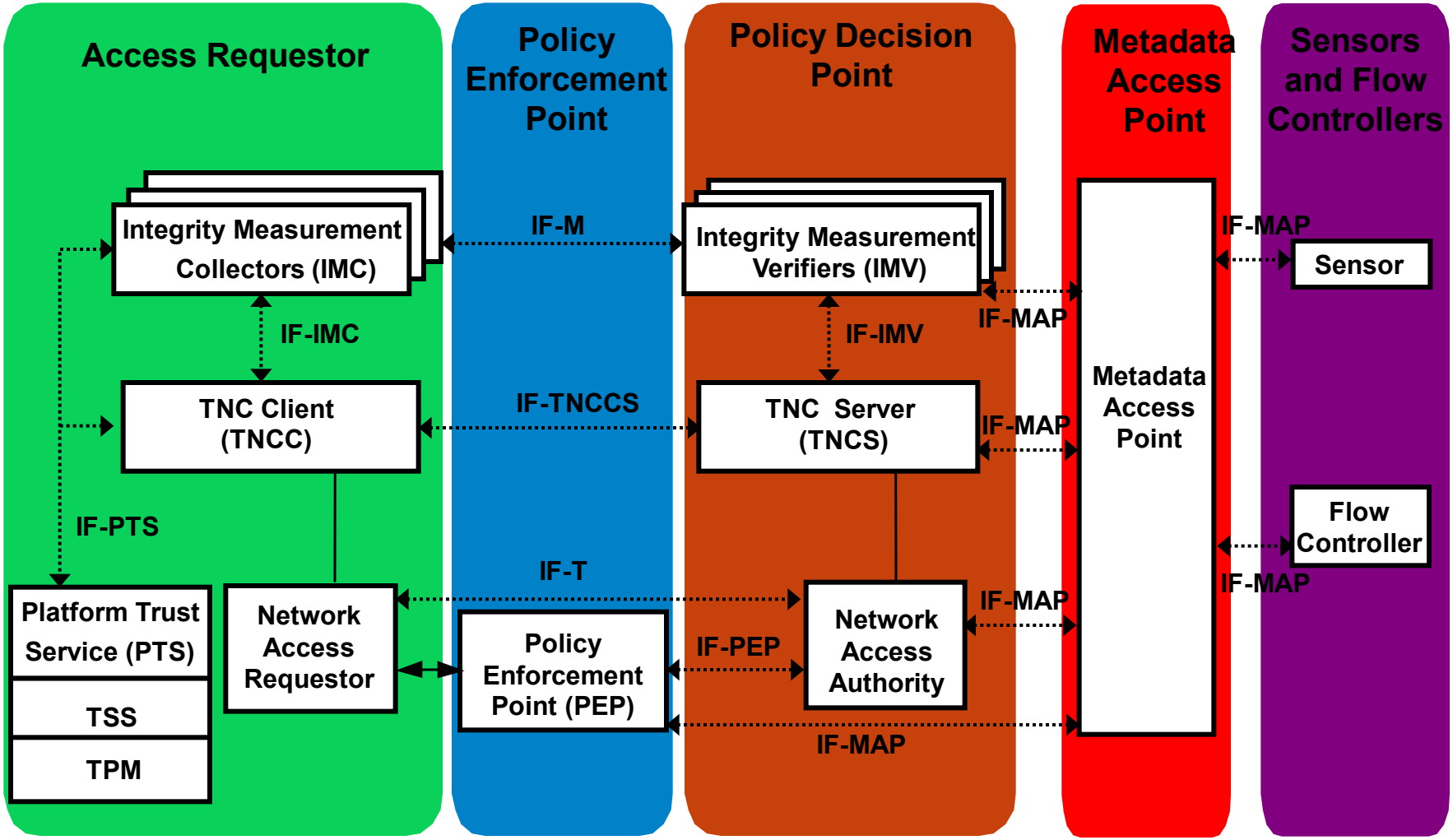
Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.



TRUSTED COMPUTING GROUP™
Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.



TRUSTED COMPUTING GROUP™
Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.



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

TRUSTED COMPUTING GROUP™ Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.

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

Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.

Conveys TNC results between security domains

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

Supports

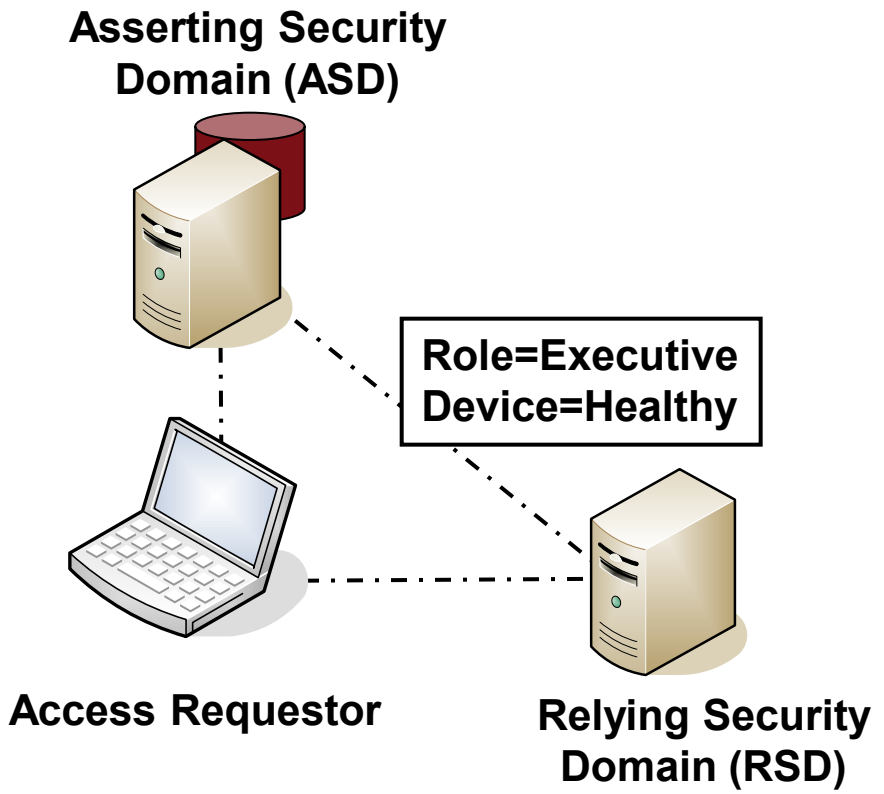
- Web SSO with health info
- Roaming with health check

How?

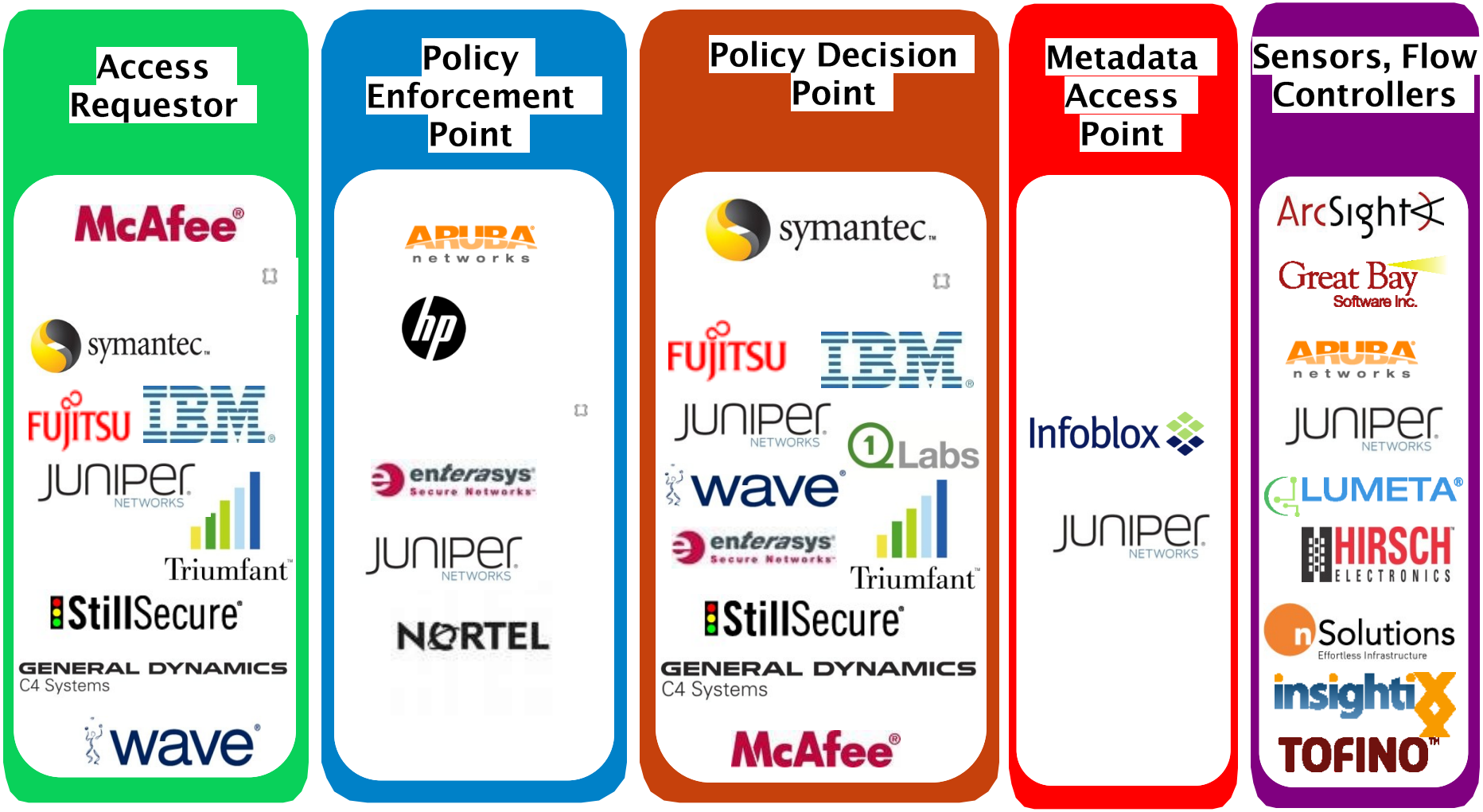
- SAML profiles for TNC

Applications

- Network roaming
- Coalitions, consortia
- Large organizations

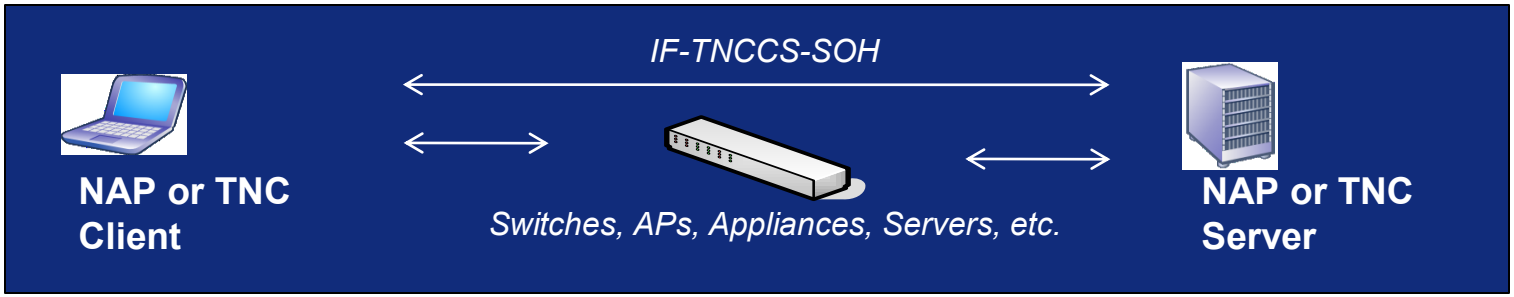


Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.



TRUSTED COMPUTING GROUP™

Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.



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

TRUSTED COMPUTING GROUP™ Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.

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

Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.

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

TRUSTED COMPUTING GROUP™ Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.

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

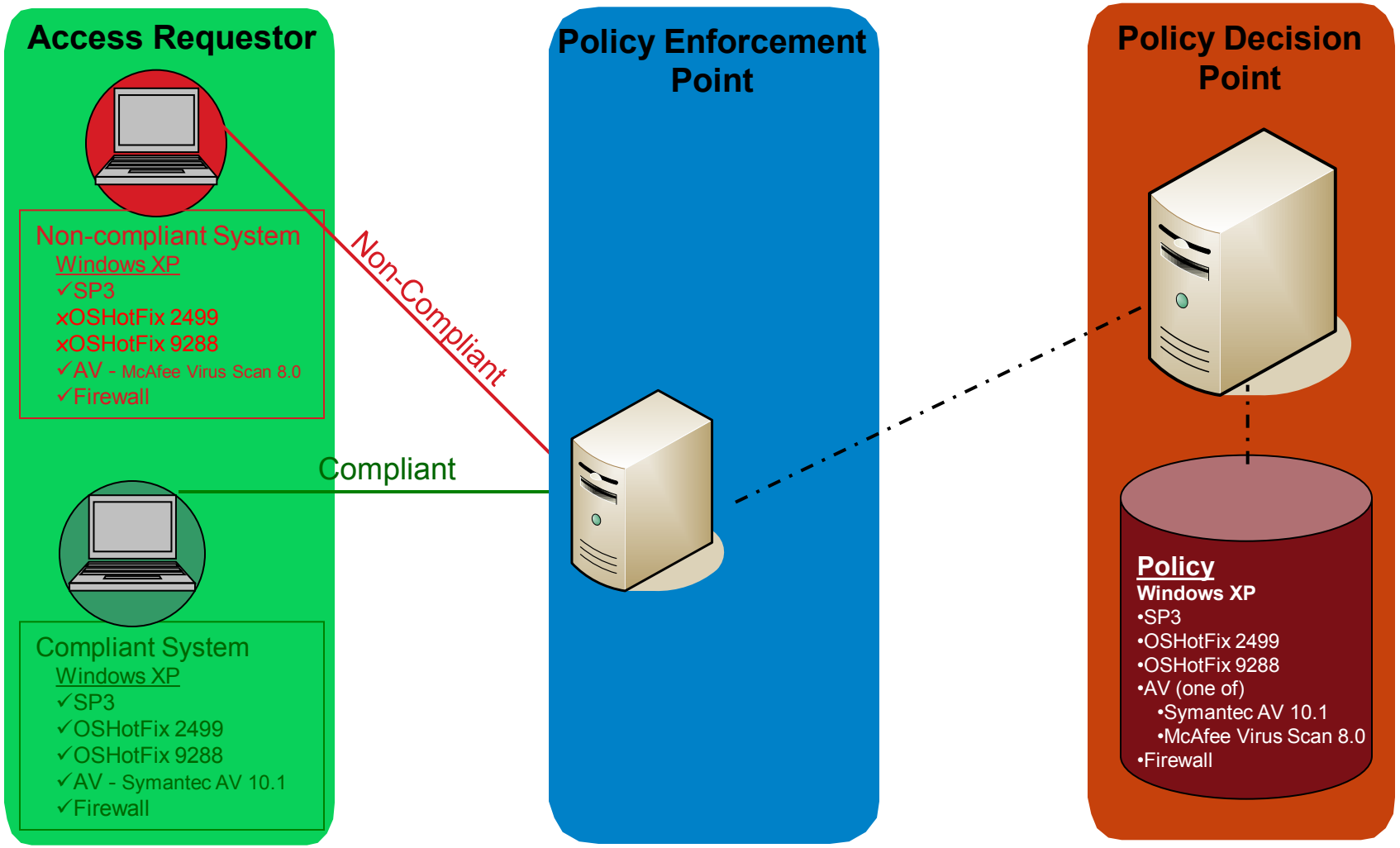
Customer Benefits

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

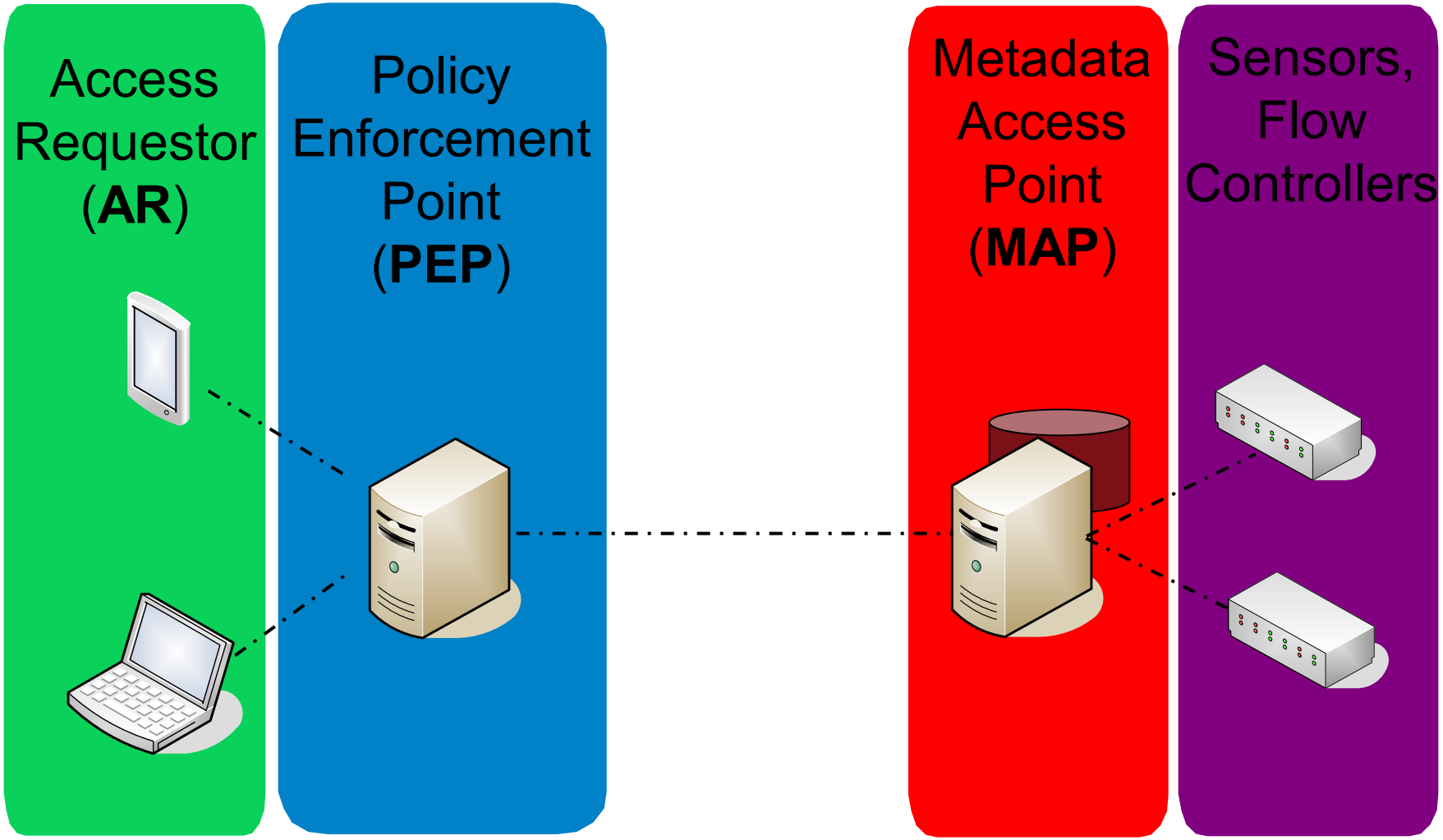
TRUSTED COMPUTING GROUP™ Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.

Options for Application Enforcement with TNC

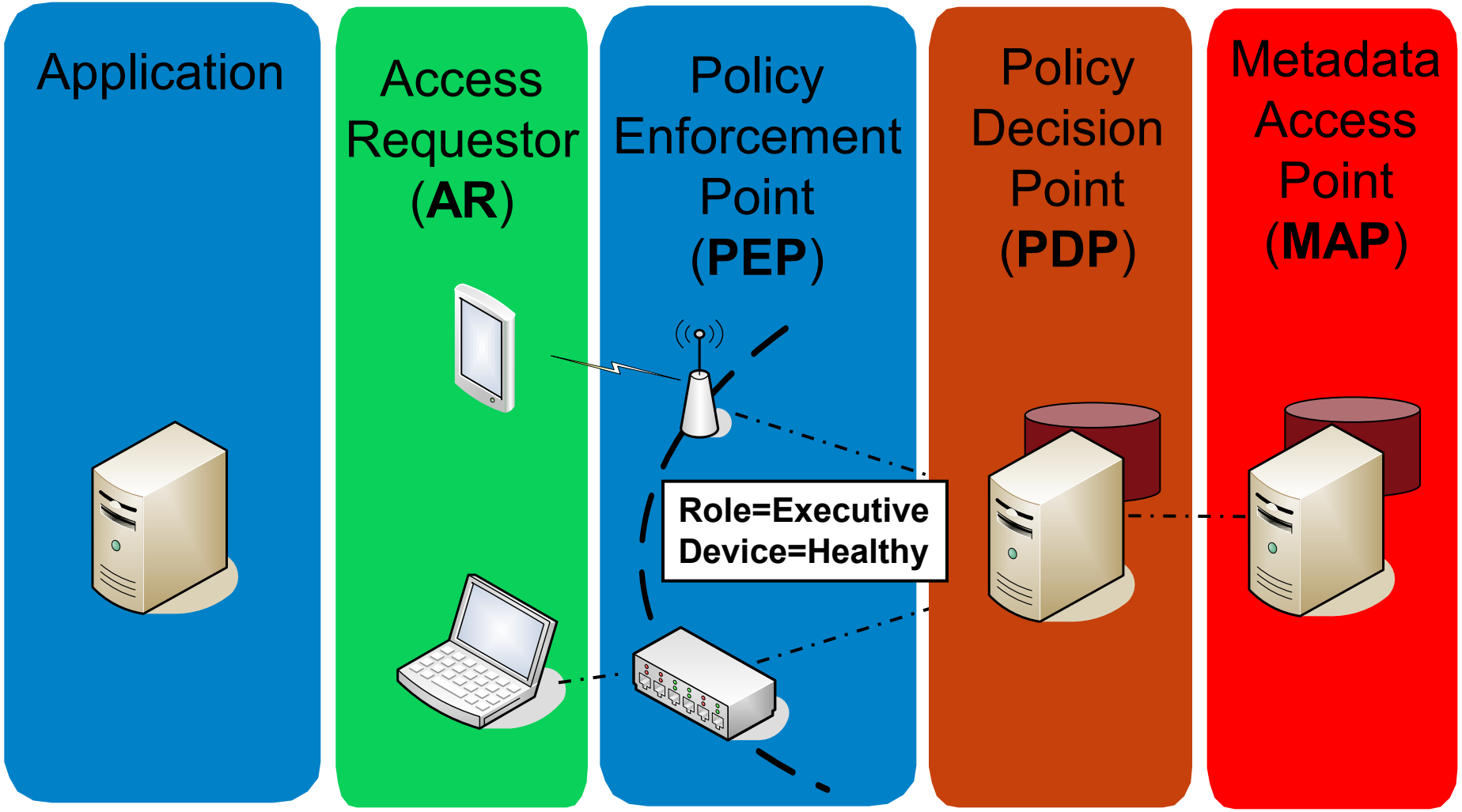
Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.



Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.



TRUSTED COMPUTING GROUP™
Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.



TRUSTED COMPUTING GROUP™
Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.

Copyright© 2011 Trusted Computing Group – Other names and brands are properties of their respective owners.

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

TRUSTED COMPUTING GROUP™

Copyright© 2011 Trusted Computing Group - Other names and brands are properties of their respective owners.