

# Trusted Network Connect

## → Basis

Prof. Dr.  
**Norbert Pohlmann**

Institute for Internet Security - if(is)  
University of Applied Sciences Gelsenkirchen  
<http://www.internet-sicherheit.de>



if(is)  
internet security.

# Contents

- **Aim and outcomes of this lecture**
- **Introduction**
- **Network Access Control**
- **Trusted Network Connect**
- **Summary**

# Contents

- **Aim and outcomes of this lecture**
- Introduction
- Network Access Control
- Trusted Network Connect
- Summary

# TNC Basis

## → Aims and outcomes of this lecture

### Aims

- To introduce the topics Network Access Control (NAC) and Trusted Network Connect (TNC)
- To explore the general idea of Network Access Control (NAC) and Trusted Network Connect (TNC)
- To analyze the goals of Network Access Control (NAC) and Trusted Network Connect (TNC)
- To assess the concerns of Network Access Control (NAC) and Trusted Network Connect (TNC)

### At the end of this lecture you will be able to

- Understand what the basic idea of Network Access Control (NAC) and Trusted Network Connect (TNC) is.
- Know something about the approach of Network Access Control (NAC) and Trusted Network Connect (TNC).
- Understand the need of Network Access Control (NAC) and Trusted Network Connect (TNC).

# Contents

- Aim and outcomes of this lecture
- **Introduction**
- Network Access Control
- Trusted Network Connect
- Summary

# Introduction

## → What are the problems? (1/2)

### Networks

- Still increasing networking in and between companies
- Worldwide communication
  - use of public networks (Internet) which lead into multiple threats
- Growing demand for security critical applications with increasing need for trustworthy communication
  - B2B transactions, home banking and many more

### Company networks

Employees „carry“ security threats into the companies

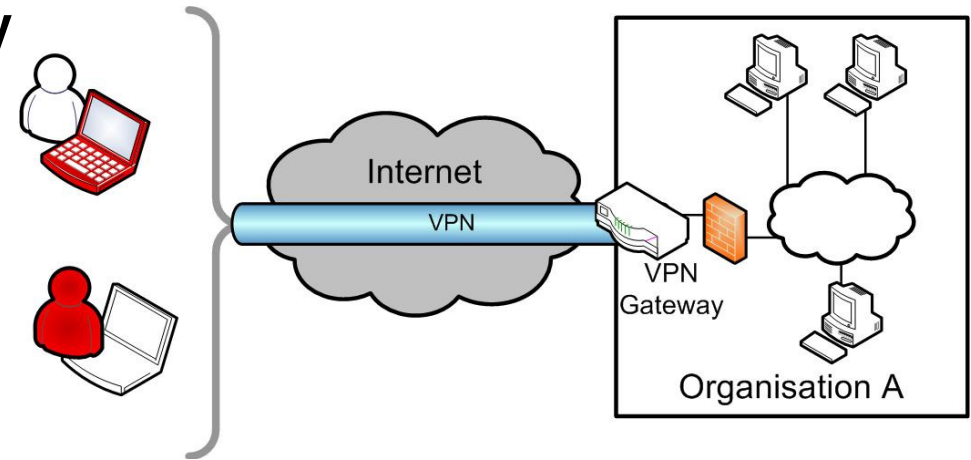
- as field workers (directly or over VPN connections)
  - as users who use notebooks at home and allow family members to access to it
  - ...
- 
- **Field workers** use their computer systems in many environments with ***various security requirements*** (e.g. insurance agents).

# Introduction

## → What are the problems? (2/2)

- Network access protected mainly by

- User authentication
- Firewalls,
- VPNs, ...



- But

- No integrity checks of connecting or connected **computer systems!**
- No difference between **trustworthy** and **not trustworthy** computer systems!

- Consequences

- Network connections are **not trustworthy**
  - Lack of trustworthy communication
  - **High probability of successful attacks!**

# Introduction

## → Need for new approaches

- There's a need for new technologies which
  - make an access decision as early as possible depending on the integrity (Trustworthiness) of any accessing device
  - **permit access** to computer systems with **trusted configuration**
  - **deny access** to computer systems with **untrusted configuration**

### Approach

## Network Access Control (NAC)



# Contents

- Aim and outcomes of this lecture
- Introduction
- **Network Access Control**
- Trusted Network Connect
- Summary

# Network Access Control

## → Functions (1/2)

- **User Authentication**
  - User Authentication  
(e.g. password / challenge-response / certificates management)
  - e.g. VPN and IEEE 802.1x
- **Configuration Assessment**
  - Configuration measurement **before** network access
    - e.g. installed software like Antivirus Scanner and Firewall
  - Compare the measurements to policies of the network to access
    - ➔ Integrity check of the computer system
  - Re-assess accepted computer systems in regular intervals
- **Policy Enforcement**
  - Enforce policies to non compliant (untrusted) computer systems

# Network Access Control

## → Functions (2/2)

### ■ Isolation

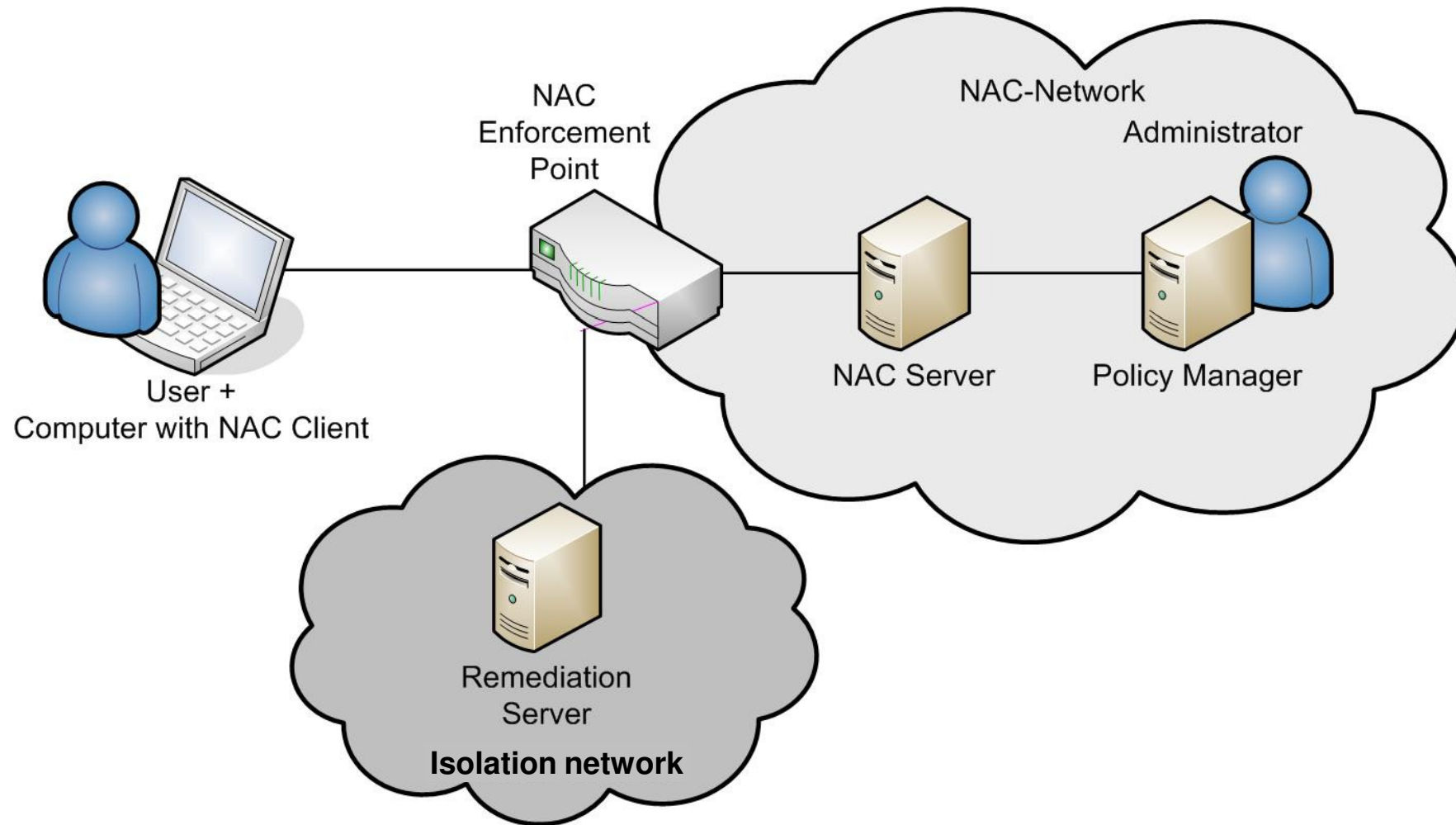
- Isolate non compliant computer systems in “Isolation networks”
- Instead of “access deny”
- Limited network access only
  - e.g. internet, update and remediation server

### ■ Remediation

- Allow non compliant computer systems to achieve a policy compliant configuration
- e.g., by updating their software to match the given Endpoint Policy Compliance
  - new signatures for anti malware scanners, OS patches, ...
- Access allow after re-assessment

# Network Access Control

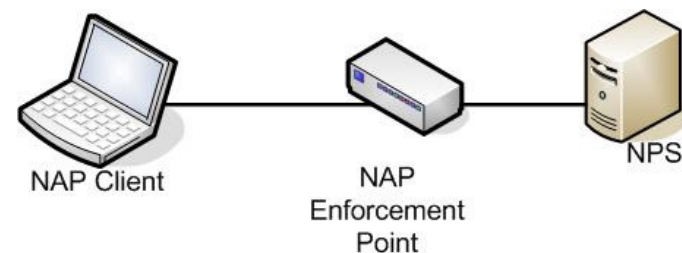
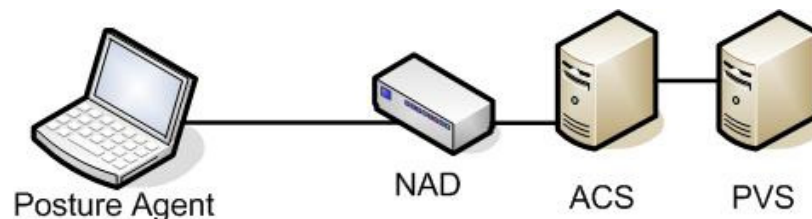
## → Topology



# Network Access Control

## → Solutions

- NAC solutions already available on the market
- The most prominent solutions
  - Cisco Network Admission Control (Cisco NAC)
  - Microsoft Network Access Protection (Microsoft NAP)
- And many more ...
  - Juniper Unified Access Control
  - StillSecure Safe Access
  - ...



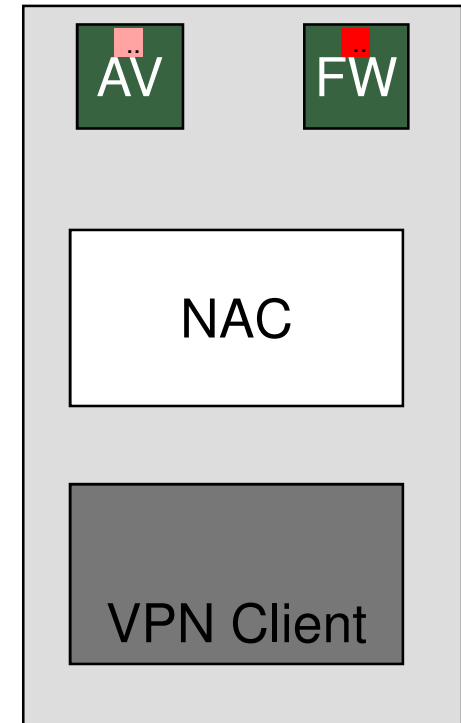
# Network Access Control

## → Limitations of current solutions (1/3)

### Lack of trust in the measurements

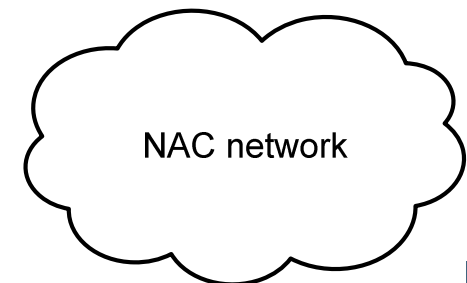
#### The “lying endpoint problem”

- Caused by current OS without isolation of components
- Measured components can get compromised
- NAC components can get compromised too
  - Shown on Cisco CTA at BlackHat conference 2007
- **Paradox:** Achieve more trustworthiness based on measurements which are not trustworthy?



### Lack of trust in NAC enabled networks

- User can't control collected data
- Possible privacy issues



# Network Access Control

## → Limitations of current solutions (2/3)

- **No standards, no compatibility by design**
- **First approaches**
  - Client sided compatibility of Cisco NAC and MS NAP
  - Microsoft opened their NAP-Client-Server-Protocol „SoH“
  - Compatibility of „smaller“ solutions to Cisco NAC, NAP or TNC
    - e.g. StillSecure Safe Access
- **Two approaches for standardization**
  - **TCG: Trusted Network Connect (TNC)**
  - **IETF: Network Endpoint Assessment (NEA)**
    - Goal: Standardize the Client-Server-Protocols

# Network Access Control

## → Limitations of current solutions (3/3)

- **Platform independence**
  - Support for every common OS is essential
  - Support of every IT devices (cars, TV, cell phone, ...) is required
  - Current NAC solutions support primarily Microsoft products
  - Need for exception management
    - e.g. MAC whitelist (which is not safe!!!)



# Network Access Control

## → Other names

---

- Endpoint Security
- Health System for IT Systems
- ...

# Contents

- Aim and outcomes of this lecture
- Introduction
- Network Access Control
- **Trusted Network Connect**
- Summary

# Trusted Network Connect

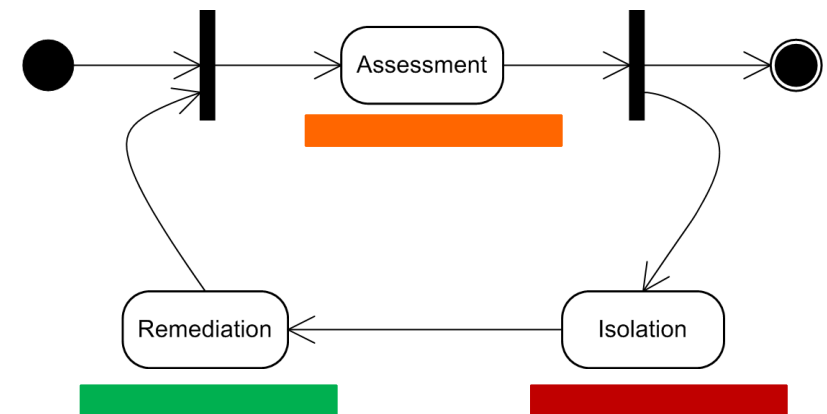
## → Overview

- **Open Architecture for NAC**
  - Specified by the TNC Subgroup of the TCG
  - All specifications are publicly available
    - Enables multi-vendor interoperability
  - Supports existing technologies (802.1x, EAP)



- **TNC Handshake consists of 3 phases**

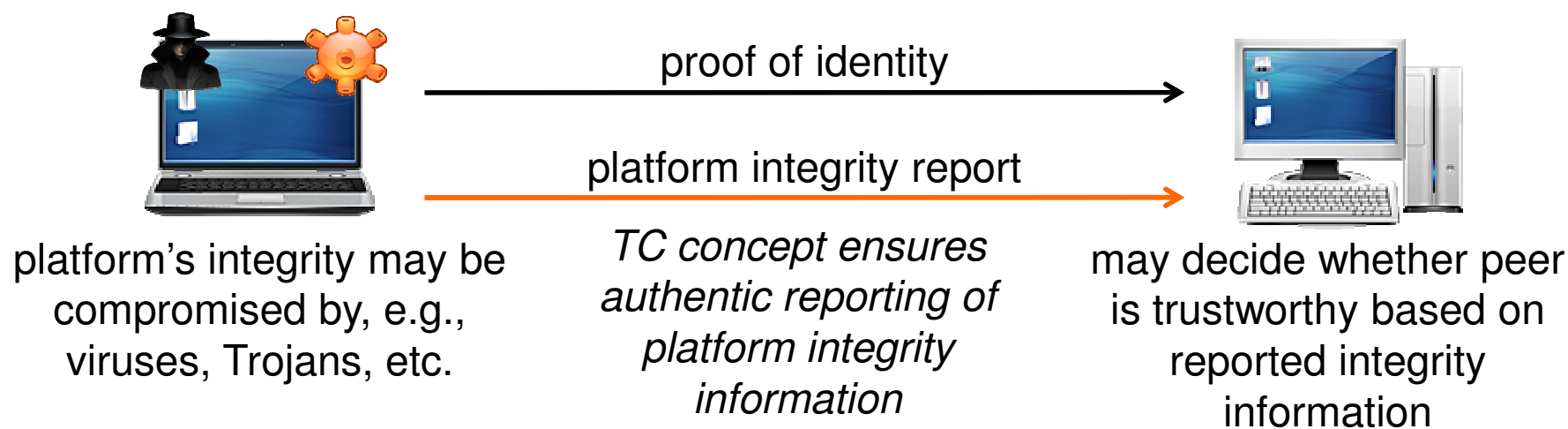
- **Assessment Phase**
  - TNC Platform Authentication
    - identity + integrity of platform
- **Isolation Phase**
  - Quarantine non-healthy endpoints
- **Remediation Phase**
  - Fixes problems and makes endpoint healthy again



# Trusted Network Connect

## → Overview

- TNC shall enhance existing network authentication protocols with Trusted Computing concepts [TNC2007]
- TNC enables verification of endpoint integrity additional to user/machine authentication
  - e.g., a user is only allowed to connect to a network via specific machines that are in a certain, probably secure configuration



# Trusted network Connect

## → Goals of TNC I

- **Interoperability of network access solutions of different vendors**
- **Platform-Authentication**
  - Platform Credential Authentication
    - Proof of the identity of a platform
    - e.g., via AIK certificates
  - Integrity Check Handshake of access requestor's platform
    - Verification of the integrity of a platform
    - e.g., via remote attestation (Trusted Computing – TCG)

# Trusted network Connect

## → Goals of TNC II

### ■ Endpoint Policy Compliance

- Assignment of a “level of trust” to the access requestor’s platform, e.g., according to the presence, integrity and version of software installed on AR’s platform
- e.g., a platform is allowed to access certain network services only if the latest patches for the operating system, virus scanner are installed and the personal firewall in the right configuration.

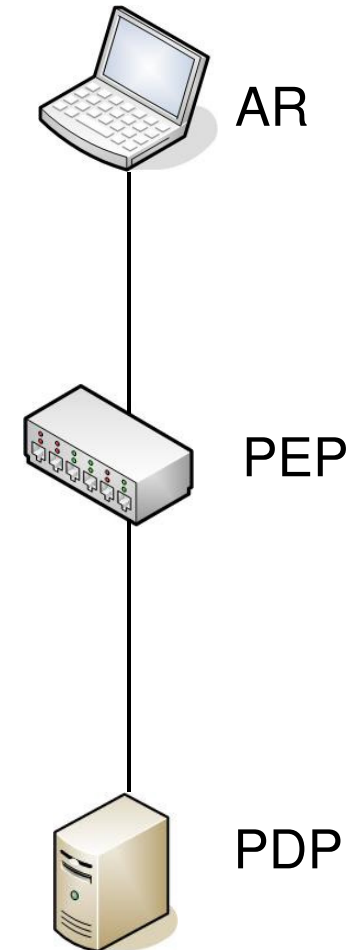
### ■ Access Policy

- Ensuring authentication of the access requestor and the
- disclosure of the access requestor’s security posture before granting access to the network

# Trusted network Connect

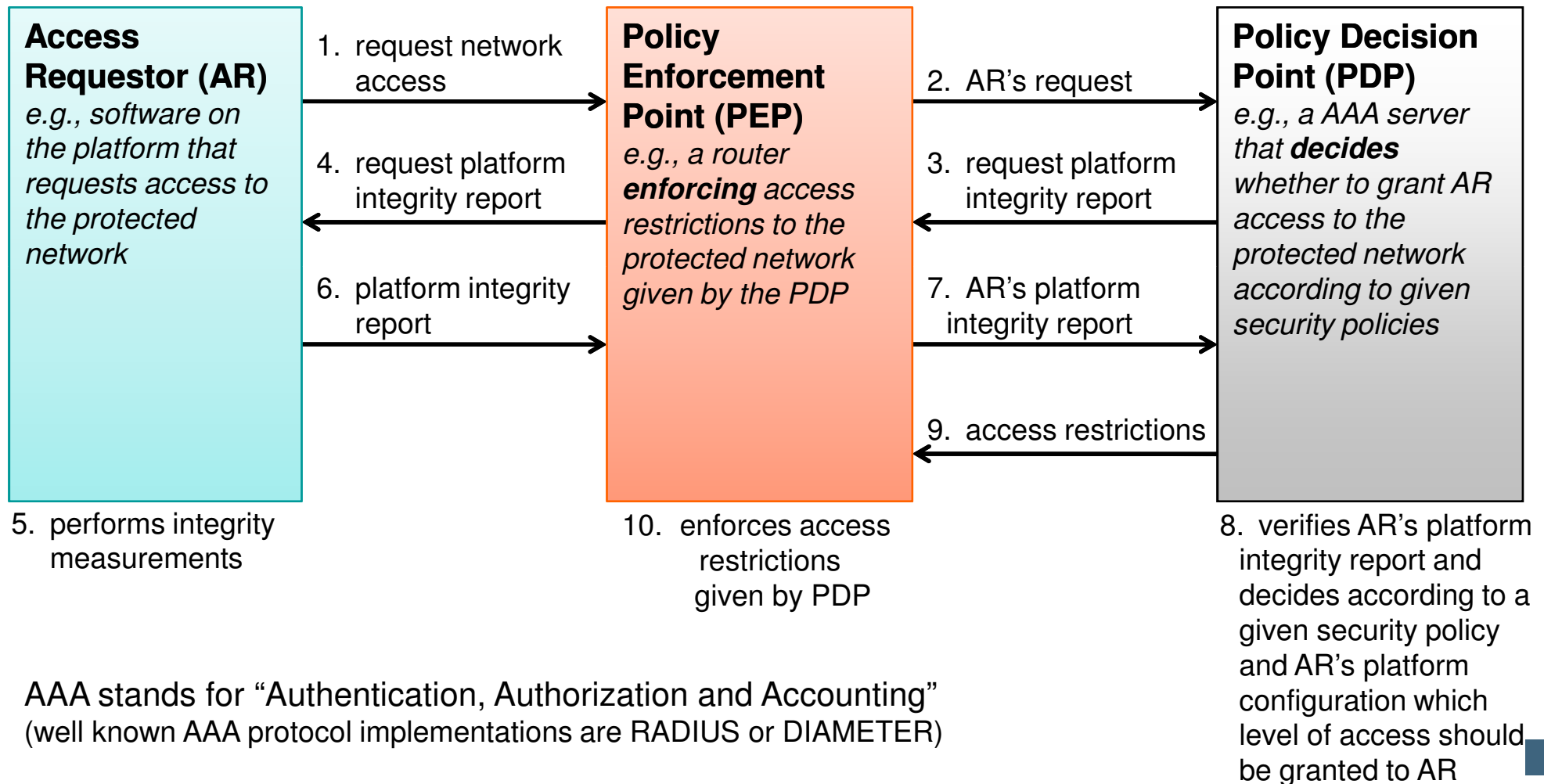
## → Topology

- **Access Requestor (AR)**
  - computer system with TNC client for system measurement
  - establishes the connection to the network
  - e.g. TNC enabled VPN-Client or IEEE 802.1x supplicant
- **Policy Enforcement Point (PEP)**
  - receives access request at the networks entry point
  - enforces the access decisions made by the PDP
  - e.g. TNC enabled VPN server or 802.1x switch
- **Policy Decision Point (PDP)**
  - decides whether to grant AR access to the protected network
  - according to given security policies
  - e.g. AAA Server (RADIUS)



# Trusted network Connect

## → Basic Message Flow

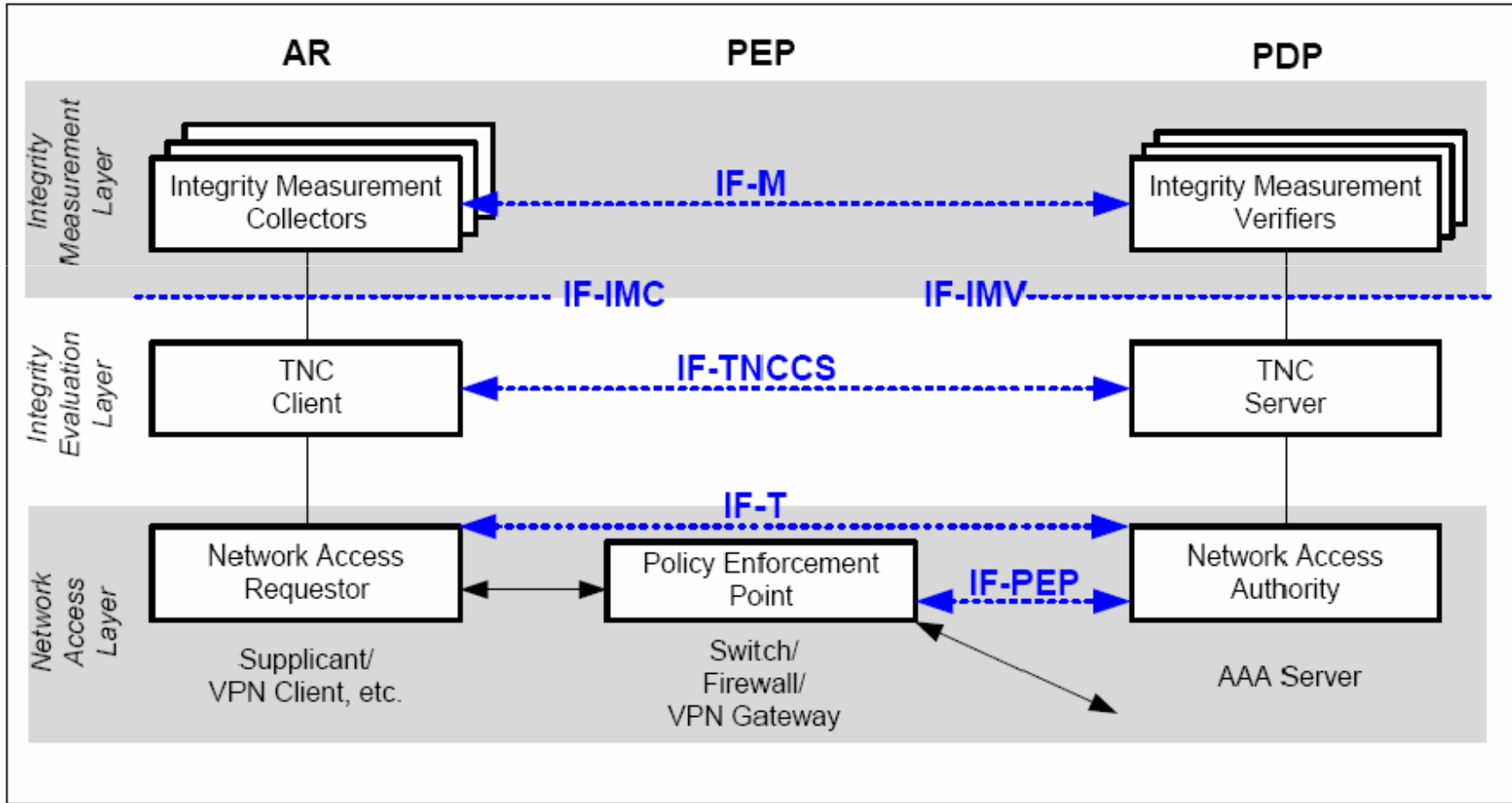
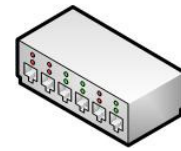


AAA stands for "Authentication, Authorization and Accounting"  
(well known AAA protocol implementations are RADIUS or DIAMETER)



# Trusted Network Connect

## → Architecture: Entities and Interfaces

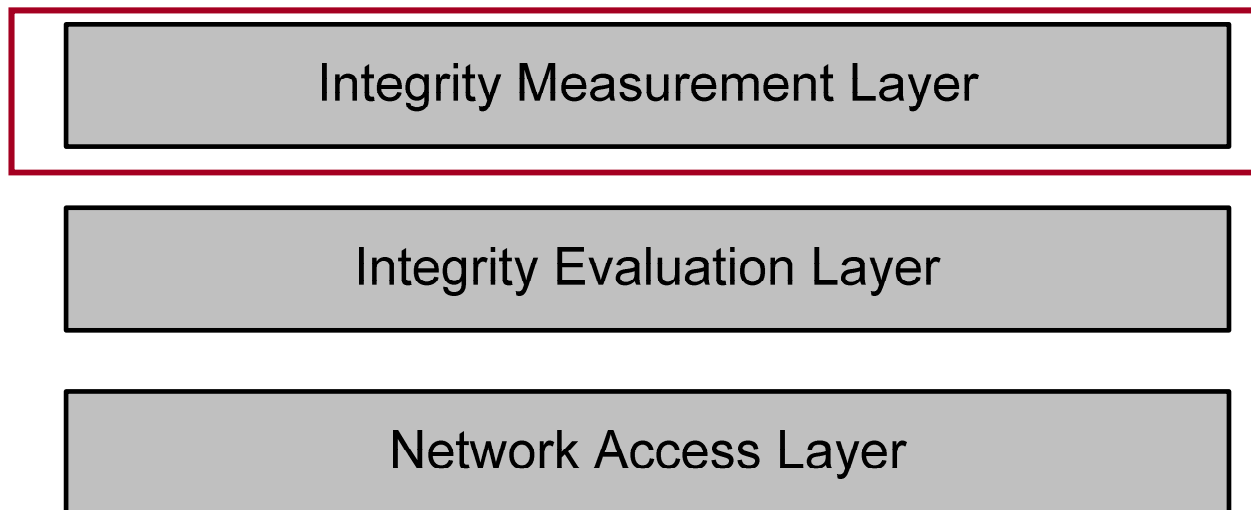


[TNC Architecture for Interoperability Specification version 1.3 revision 6]

# Trusted Network Connect

## → TNC Layers (1/3)

### Integrity Measurement Layer (IML)

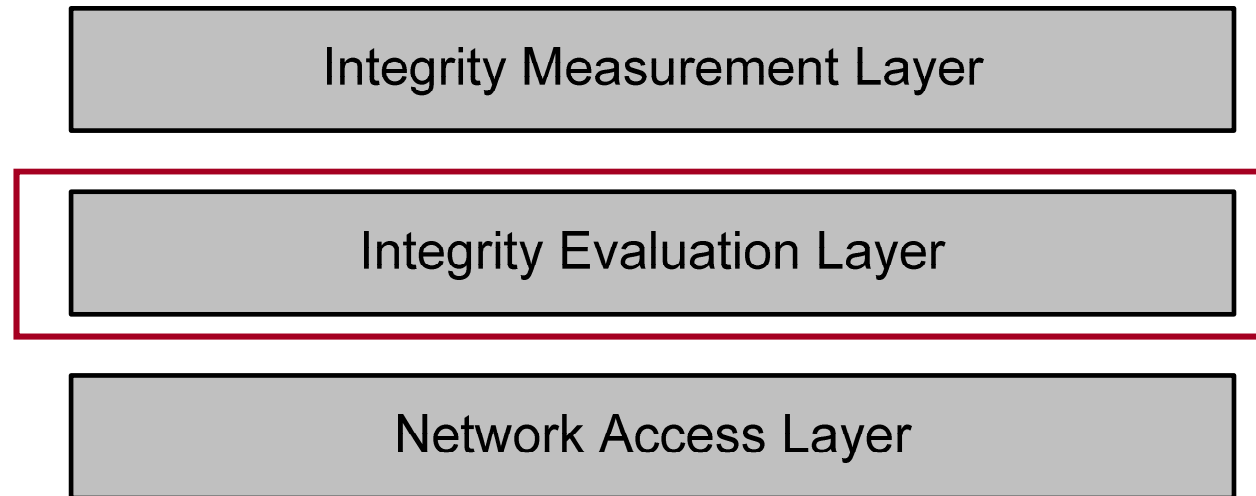


- **Functions handled on this layer**
  - Record current integrity state by collecting measurements
  - Request further measurements
  - Create “IMV action recommendations”
    - Which are sent to the TNCS

# Trusted Network Connect

## → TNC Layers (2/3)

### Integrity Evaluation Layer (IEL)

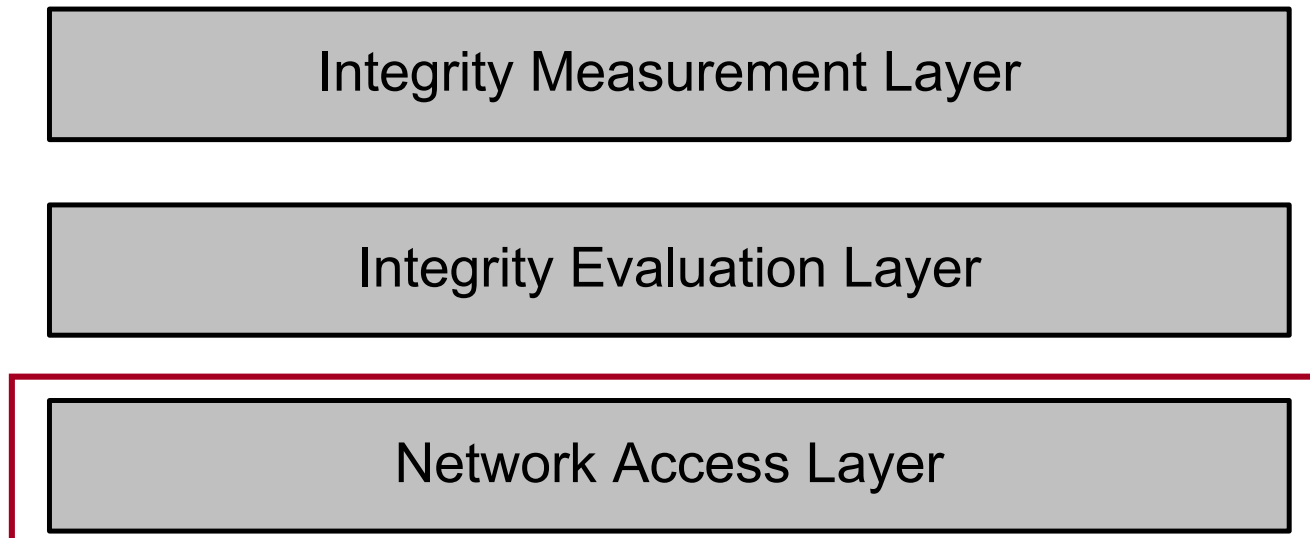


- **Functions handled on this layer**
  - Collect IMC measurements
  - Handle communication between IMCs and IMVs (logical)
  - Collect each “IMV action recommendation” received from the IML
  - Create a “TNCS recommendation” based on the IMV action recommendations
    - Send to the Network Access Layer

# Trusted Network Connect

## → TNC Layers (3/3)

### Network Access Layer (NAL)



- **Functions handled on this layer**
  - Establish, perform and close the communication
  - Receive, create and execute access decisions
  - Support existing technologies (like VPN or 802.1s)
    - e.g. VPN clients/VPN gateways

# Trusted Network Connect

## → Components: Access Requestor

- **Network Access Requestor (NAR)**

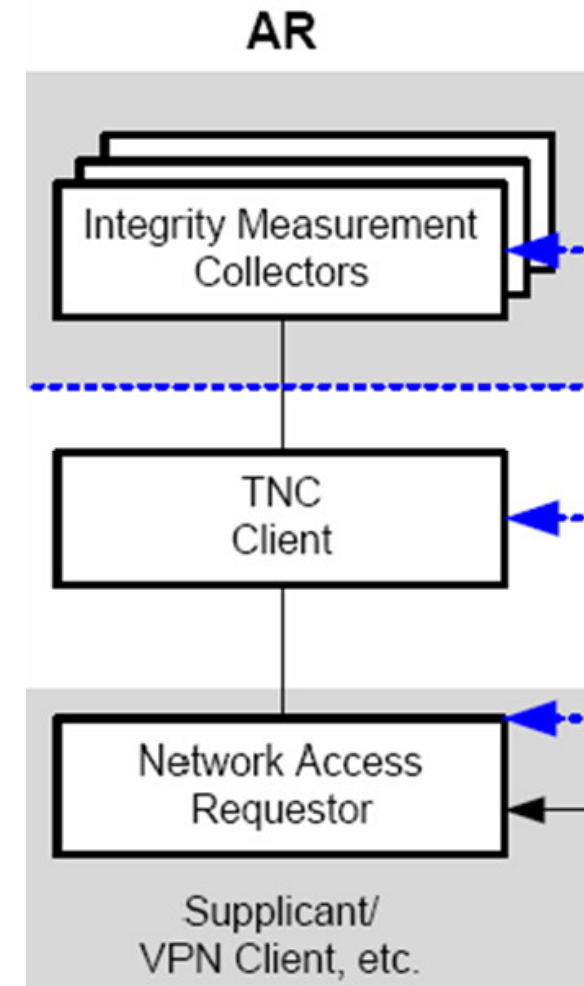
- Establishes network access
- Quantity: Multiple
  - one for each supported network access technology (e.g. VPN)

- **TNC Client (TNCC)**

- Software component which manages the integrity measures of the IMCs
- Quantity: 1

- **Integrity Measurement Collector (IMC)**

- Software which measures security related parameters of applications
- Quantity: Multiple
  - e.g. one for each security application like anti virus, personal firewall, OS patch level, ...

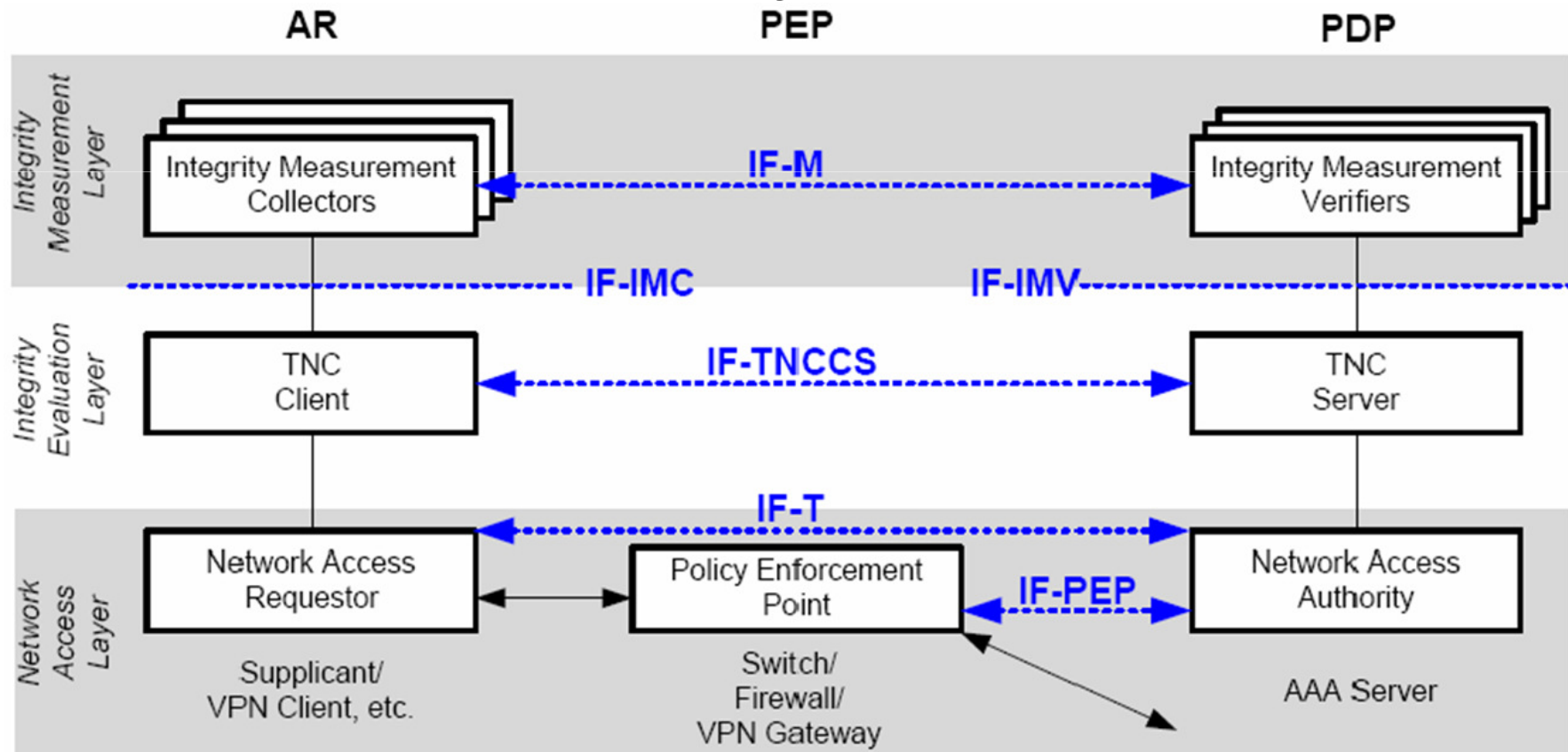


# Trusted Network Connect

## → Components: Policy Enforcement Point

### ■ Policy Enforcement Point (PEP)

- Controls the access to a TNC enabled network and enforces access decisions
- Asks the PDP whether access is granted or not



# Trusted Network Connect

## → Components: Policy Decision Point

### ■ Integrity Measurement Verifier (IMV)

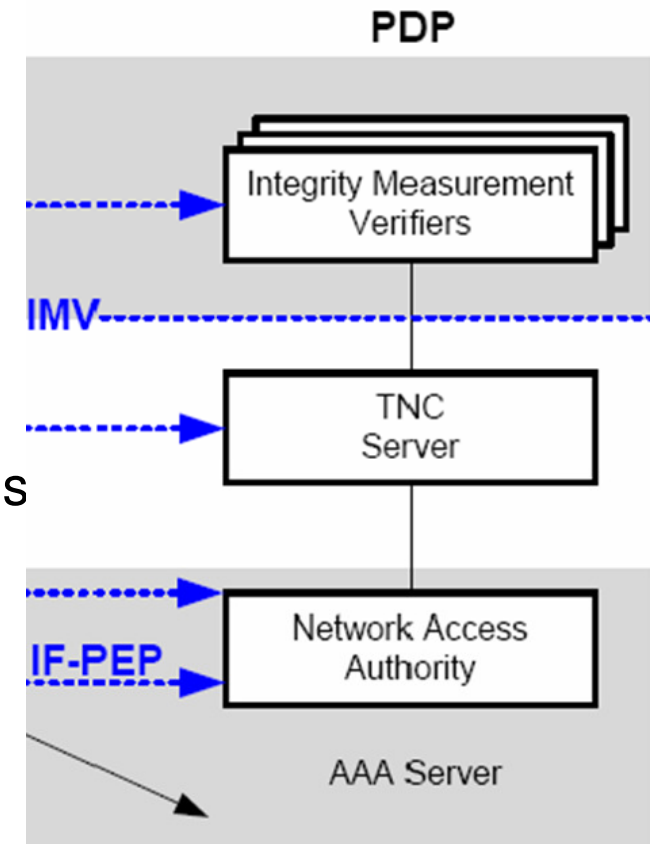
- Components which compare the received measurements to the policies
- Creates an **IMV action recommendation**
- Quantity: Multiple

### ■ TNC Server (TNCS)

- Manages the messages between IMVs and IMCs
- Collects each IMV action recommendations and aggregate these to a **TNCS recommendation** (policy based)
- Sends the TNCS recommendation to the NAA
- Quantity: 1

### ■ Network Access Authority (NAA)

- Asks the TNC Server whether the ARs state is policy compliant or not
- Creates final access decision which is enforced by the PEP
- Quantity: 1

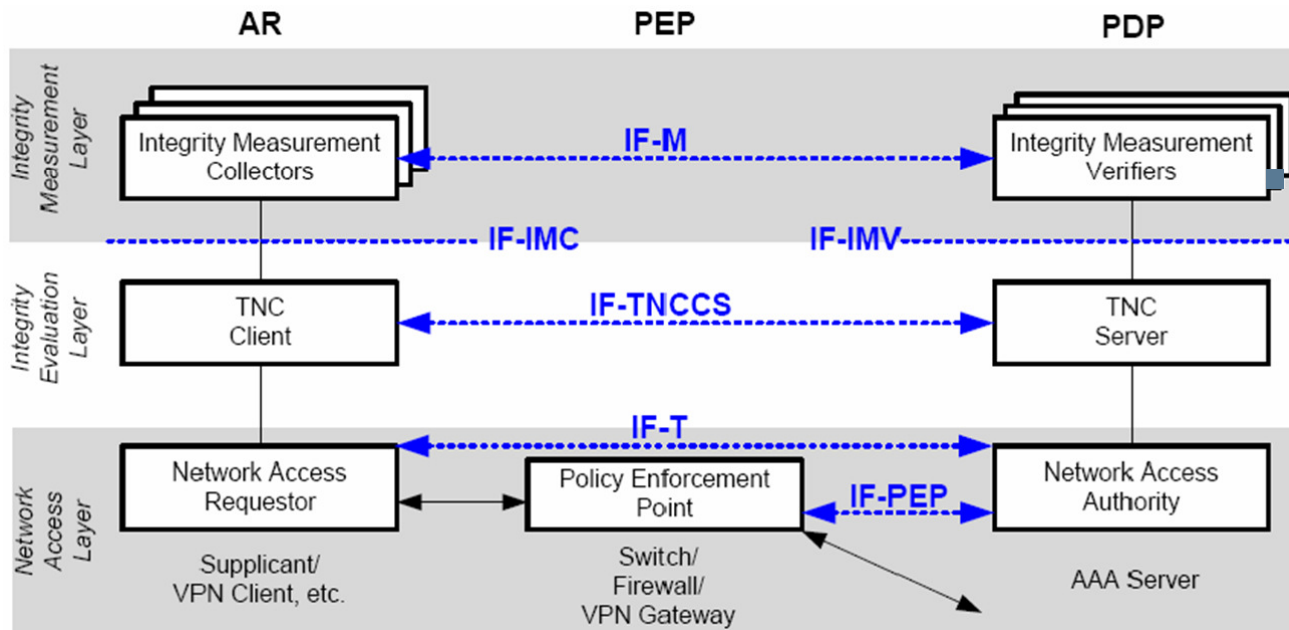


# Trusted Network Connect

## → TNC Interfaces (1/2)

- **Integrity Measurement Collector Interface (IF-IMC)**

- Used by the TNCC for forwarding:
  - measurements to the IMVs
  - IMV requests to the specific IMCs



### Integrity Measurement Verifier Interface (IF-IMV)

- Interface between TNCS and the IMVs

- **Policy Enforcement Point Interface (IF-PEP)**

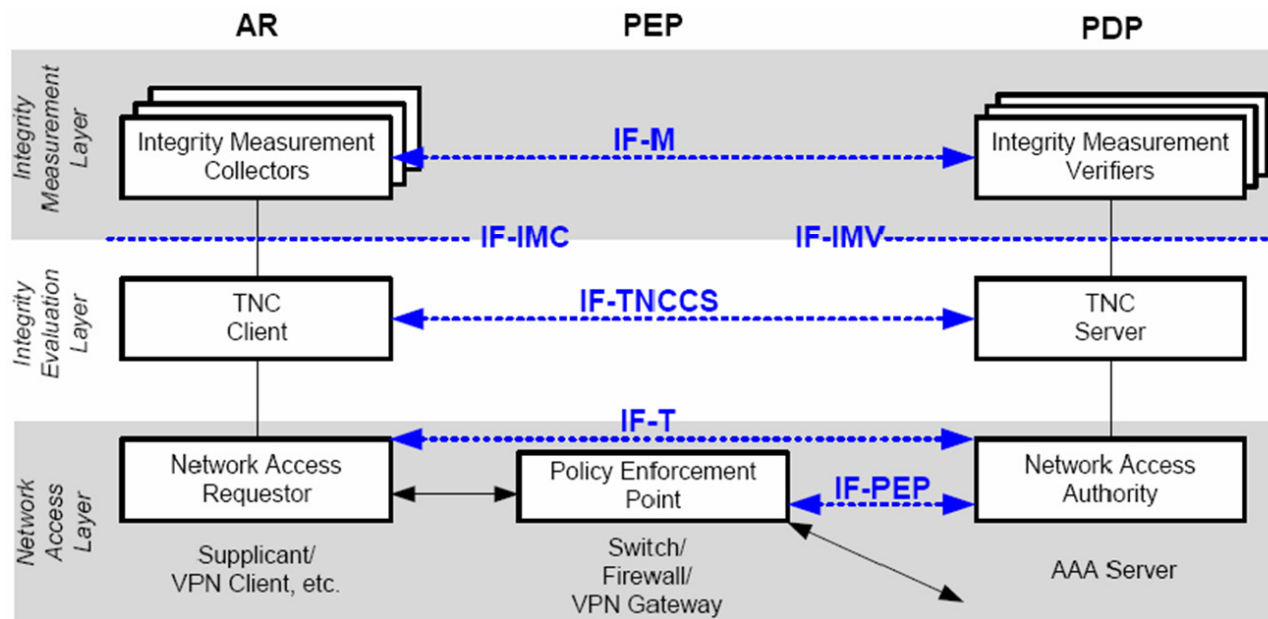
- enables the communication between PDP and PEP
- e.g.: PDP instructs the PEP to isolate an AR



# Trusted Network Connect

## → TNC Interfaces (2/2)

- **Vendor-Specific IMC-IMV Messages (IF-M)**
  - Interface between IMVs and IMCs
  - Communication of vendor specific messages



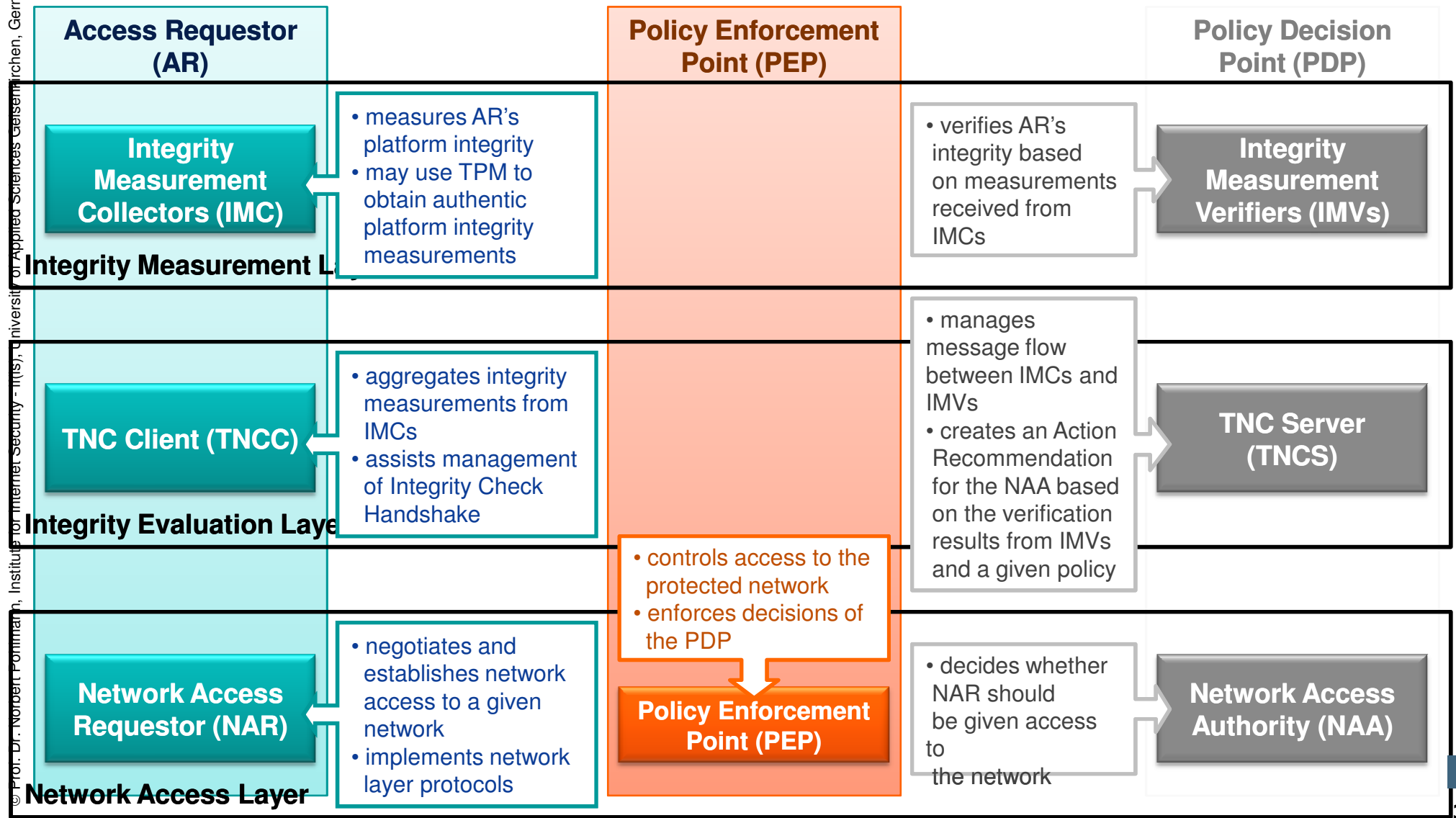
- **TNC Client-Server Interface (IF-TNCCS)**

- Enables message exchange between IMVs and IMCs

- **Network Authorization Transport Protocol (IF-T)**
  - Communication between AR and PDP
  - Utilize existing technologies (like EAP with IEEE 802.1x)

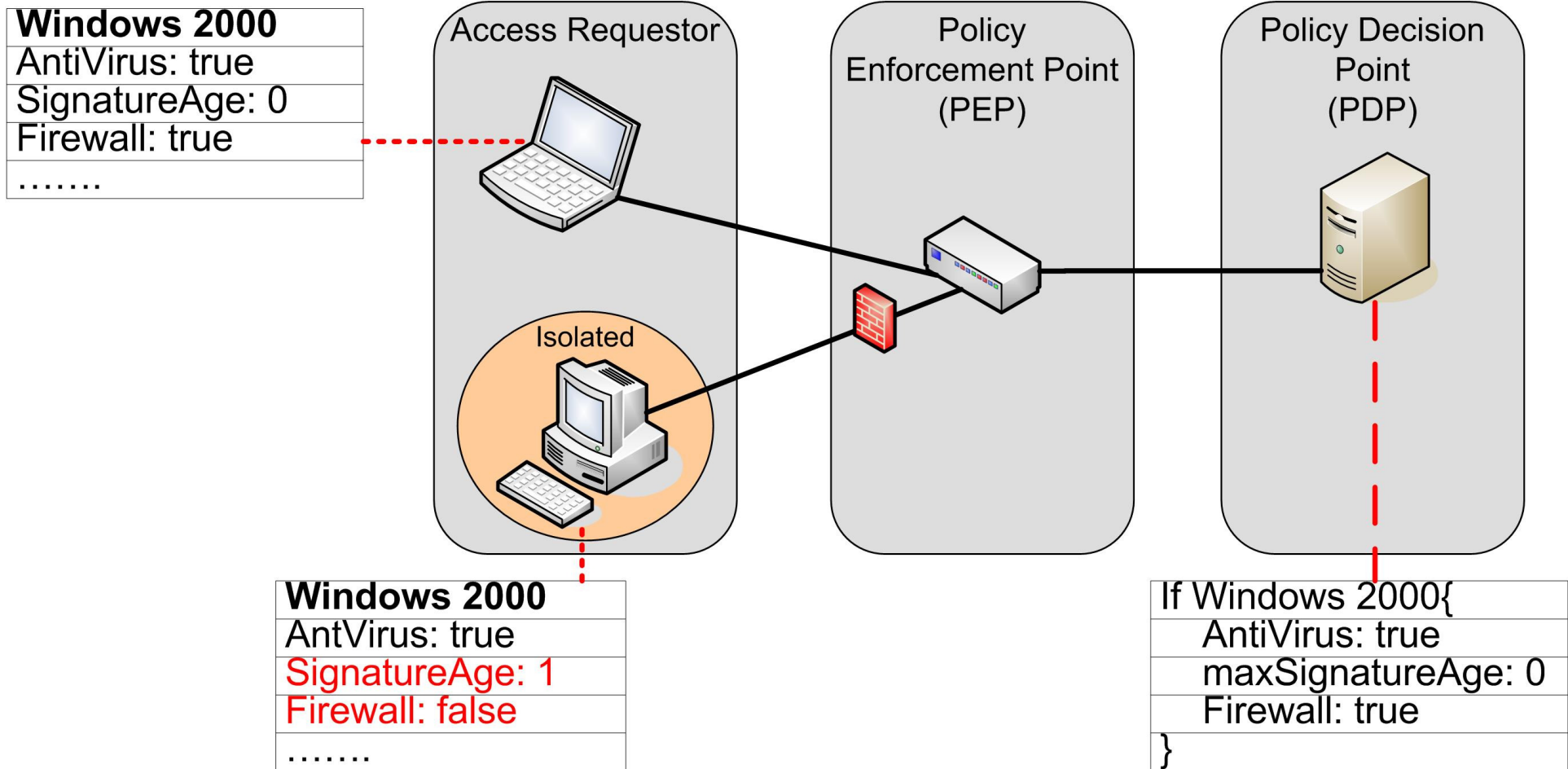
# Trusted Network Connect → TNC Architecture – Details

© Prof. Dr. Norbert Pommer, Institute for Internet Security - (iNS), University of Applied Sciences Geseirrhofen, Germany



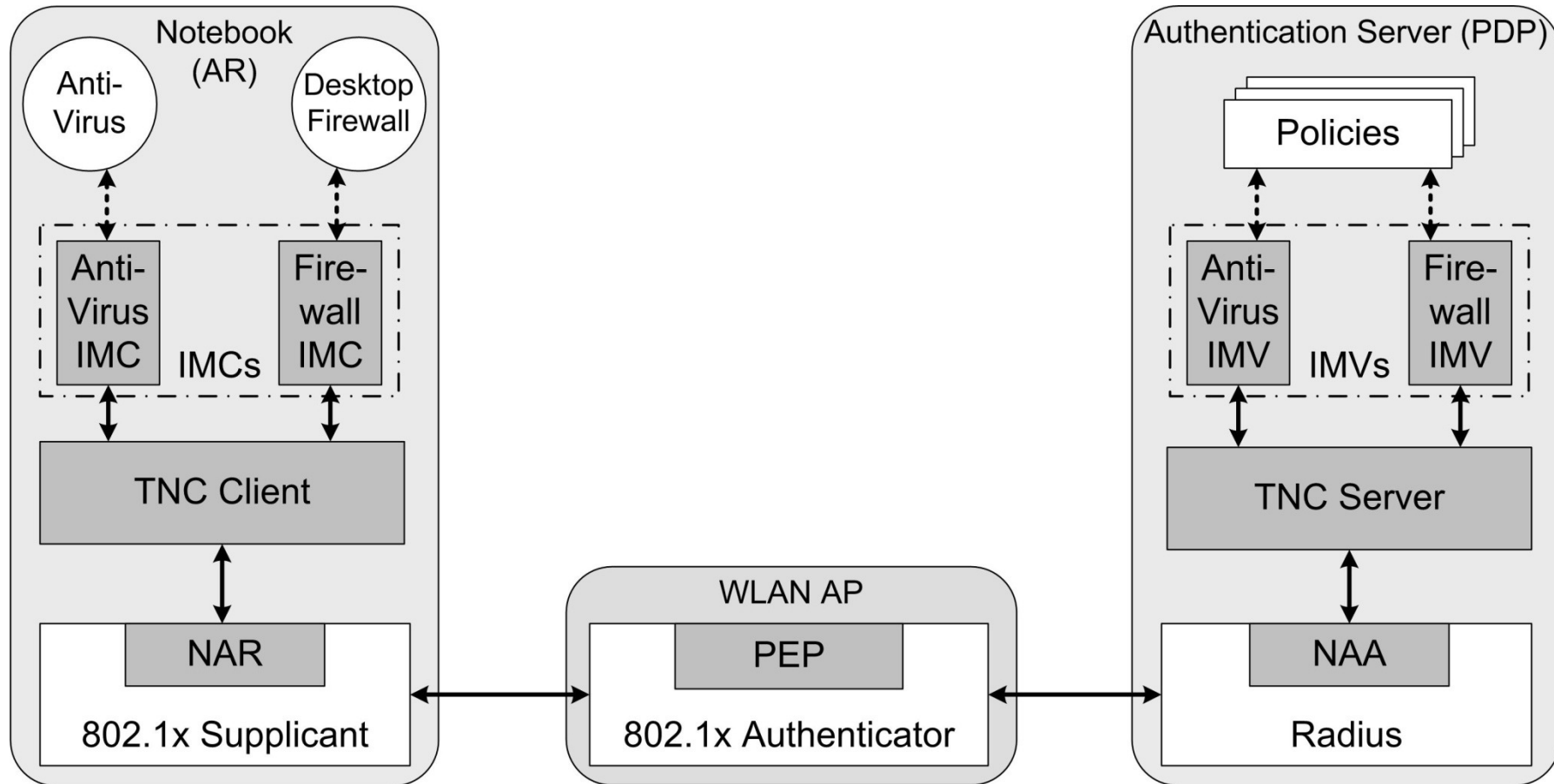
# Trusted Network Connect

## → Easy Example: Policy Enforcement



# Trusted Network Connect

## → Example: WLAN



# Trusted Network Connect

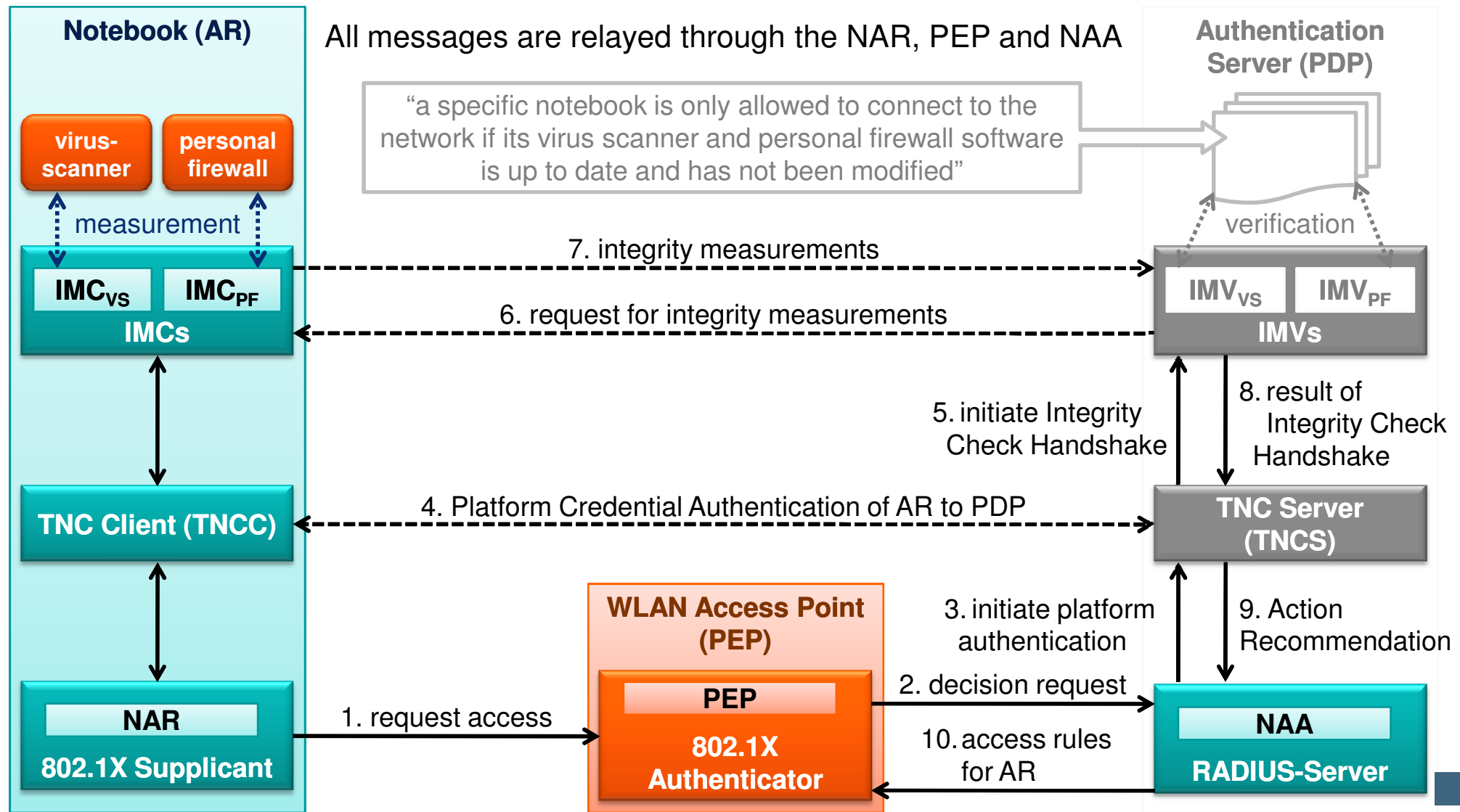
## → Example: WLAN

— direct communication

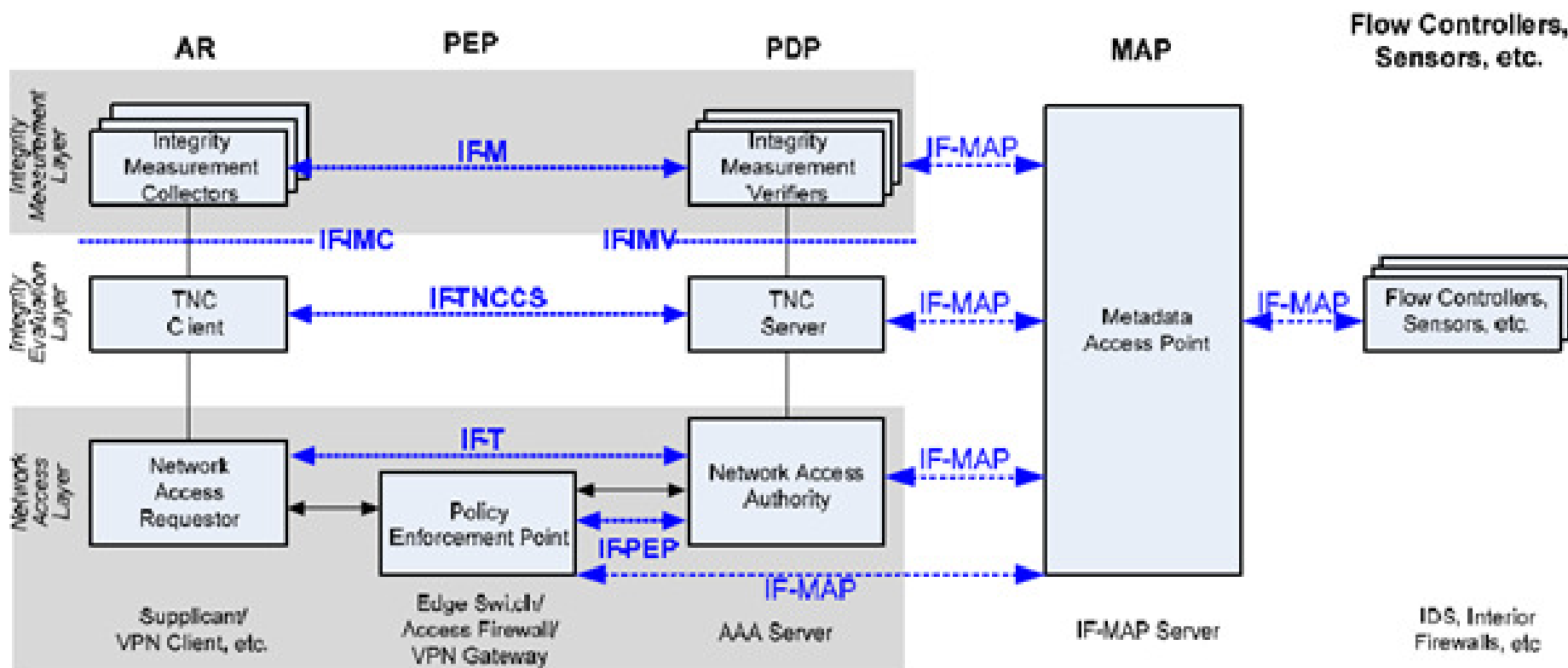
--- logical communication



© Prof. Dr. Norbert Pohlmann, Institute for Internet Security - if(is), University of Applied Sciences Gelsenkirchen, Germany



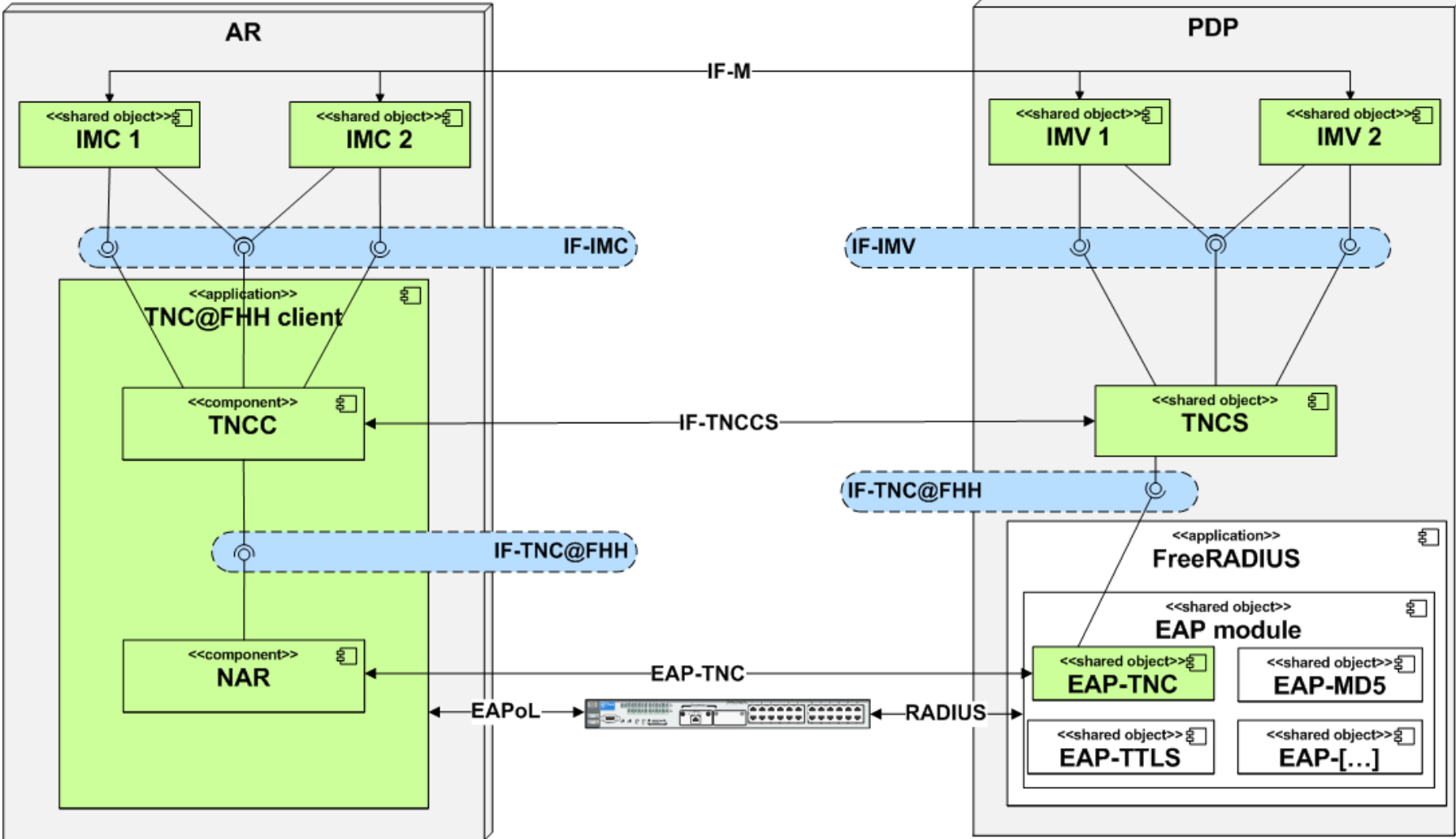
# Trusted Network Connect → Extension



- Metadata Access Point (MAP, storing and providing state information)
- Flow controllers, Sensors etc. (like IDS, Interior Firewalls).

# Trusted Network Connect

## → Example: TNC@FHH



# Trusted Network Connect

## → Example: IMC/IMV Pairs

- IMCs provided by the TNC@FHH project
- Currently “Windows only”
- **HostScanner**
  - Client-sided port scan
- **Registry**
  - Scans for specific registry entries
- **SecurityScanner**
  - IMC for the „Microsoft Security Center“
  - Collects data für Windows patch- , antivirus and firewall state
- **ClamWin**
  - IMC for the open source „Clam AntiVirus“ scanner

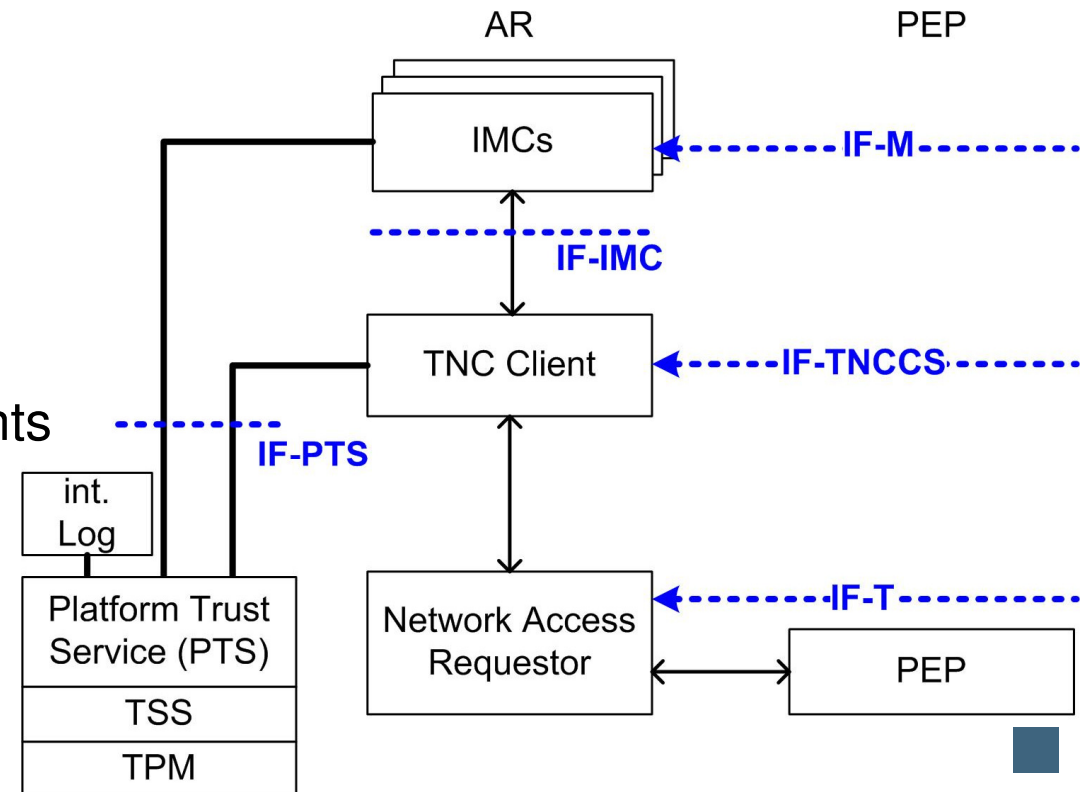


# Trusted Network Connect

## → TPM Support

- One main advantage of TNC compared to other NAC solutions
  - Supports use of the TPM during TNC Handshake
  - Promising approach to solve the „lying endpoint problem“
  - **Goal:** Ensure integrity of TNC subsystem located on the AR

- **New component:**  
**PTS (Platform Trust Services)**
  - System service on the AR
  - Exposes Trusted Platform capabilities to TNC components



# Trusted Network Connect

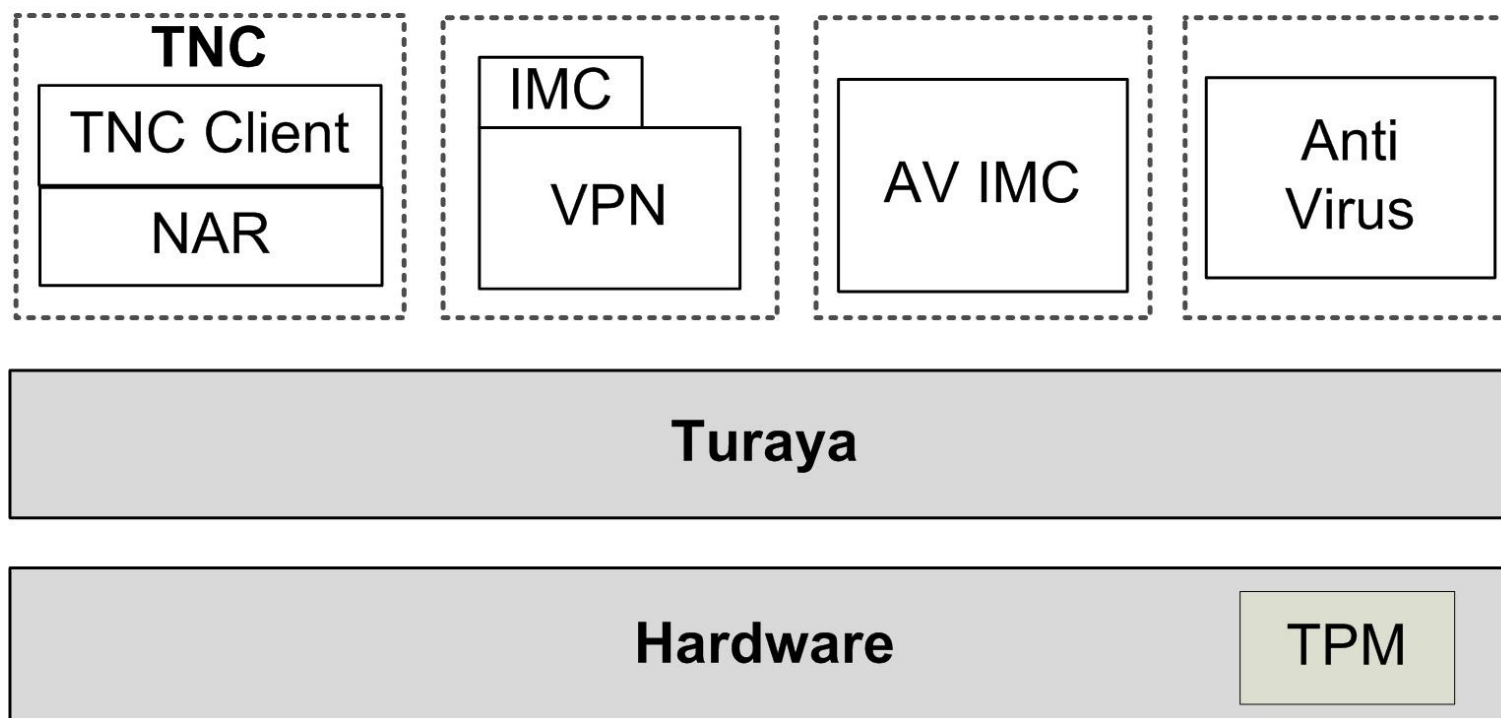
## → TPM Support

- **Idea: Use TPM capabilities during TNC Handshake**
  - Create integrity reports
    - Including signed PCR values
  - AR sends integrity report to PDP
  - Sign measurements
  - PDP compares received values to known good reference values
    - PDP can verify integrity of TNC subsystem
- **Limitation**
  - TPM components can still get compromised by malware
  - Every data which has to be signed can still get compromised
    - Exclusive use of the TPM cannot solve the lying endpoint problem
      - Due to the use of current OS
      - Only the use of **security platforms** can solve this problem

# Trusted Network Connect → TNC and Security Platforms (1/3)

## Example 1: Integration into Turaya

- Integrate TNC core components into one compartment
- IMCs part of compartments to measure or in isolated ones
- How to remote check Turaya?



# Trusted Network Connect

## → TNC and Security Platforms (2/3)

### Example 2: Integration into Turaya with Remote Attestation

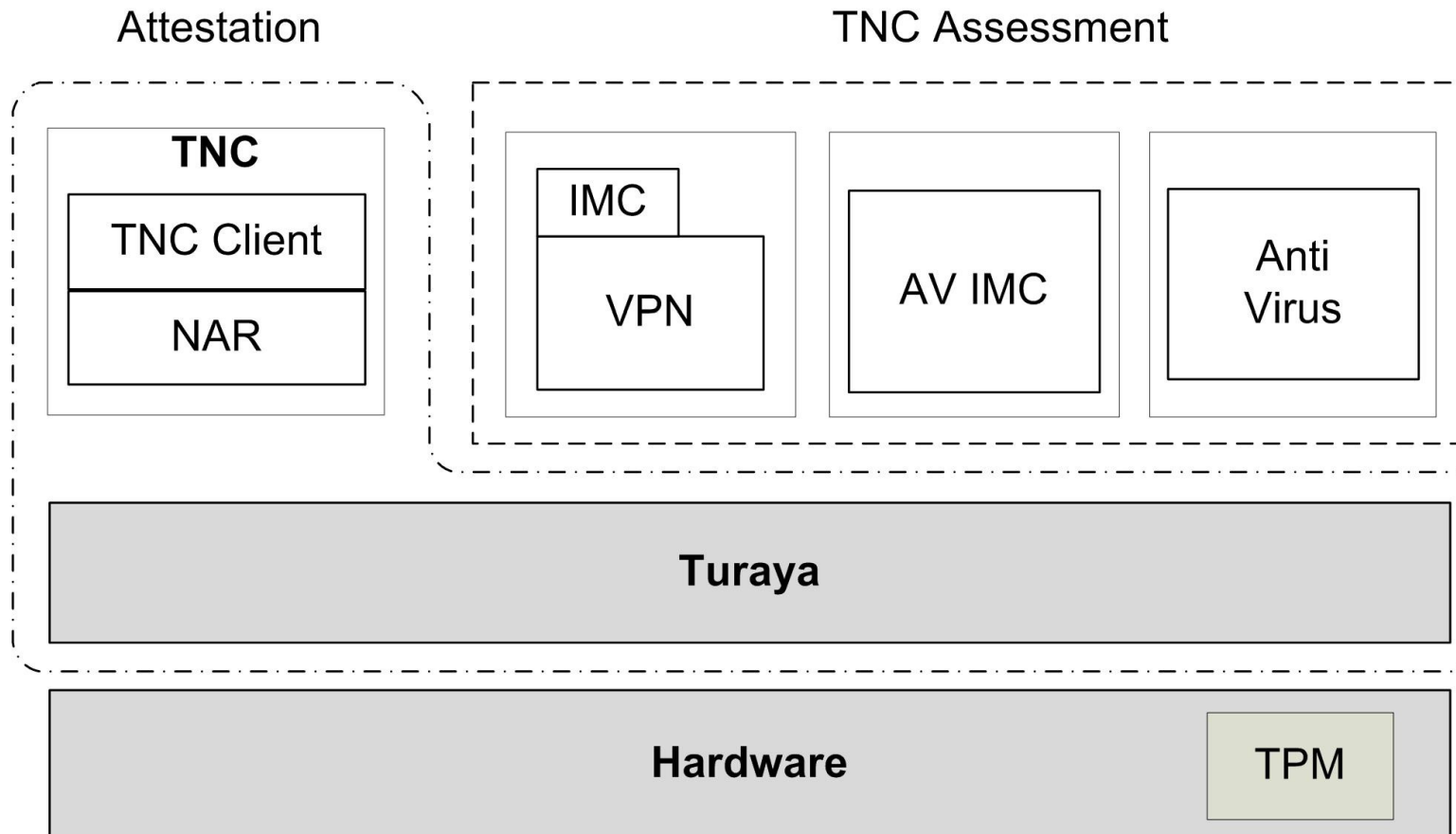
- Use Remote Attestation for attest Turaya and the TNC core components
- Use TNC to check frequently changing compartments

### Benefits

- Check Turaya and the TNC compartment at a high trust level
- Check frequently changing compartment
  - without the need for frequently re-certifications

# Trusted Network Connect

## → TNC and Security Platforms (3/3)



# Contents

- Aim and outcomes of this lecture
- Introduction
- Network Access Control
- Trusted Network Connect
- **Summary**

# TNC Basis

## → Summary

- TNS is a solution to check the trustworthiness of clients!
- TNC makes an access decision as early as possible depending on the trustworthiness level of any accessing device (healthy level).
- TNC proves the trustworthiness of SW and IT security components which change often (OS updates, signature for virus scanner, ...)
- The combination of TNC and security platform makes the trustworthiness level higher.

# Trusted Network Connect

## → Basis

Thank you for your attention!  
Questions?

Prof. Dr.  
**Norbert Pohlmann**

Institute for Internet Security - if(is)  
University of Applied Sciences Gelsenkirchen  
<http://www.internet-sicherheit.de>



if(is)  
internet security.



# TNC Basis

## → Literature

- [1] M. Jungbauer, N. Pohlmann: „Integrity Check of Remote Computer Systems - Trusted Network Connect“, in "ISSE/SECURE 2007 - Securing Electronic Business Processes - Highlights of the Information Security Solutions Europe/Secure 2007 Conference", Hrsg.: N. Pohlmann, H. Reimer, W. Schneider; Vieweg-Verlag, Wiesbaden 2007
- [2] M. Jungbauer, N. Pohlmann: „Trusted Network Connect Vertrauenswürdige Netzwerkverbindungen“, in "Trusted Computing - Ein Weg zu neuen IT-Sicherheitsarchitekturen“, Hrsg.: N. Pohlmann, H. Reimer; Vieweg-Verlag, Wiesbaden 2008

### Links:

Institute for Internet Security:

<http://www.internet-sicherheit.de/forschung/aktuelle-projekte/trusted-computing/>

<http://www.internet-sicherheit.de/forschung/aktuelle-projekte/tnac/>