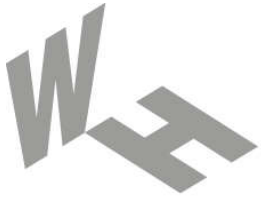


Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Trusted Network Connect → Process

Prof. Dr. (TU NN)
Norbert Pohlmann

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

if(is) internet security.

Content

- Aim and outcomes of this lecture
- What are the problems?
- TNC Process
- Definition of the Policies
- Summary

Content

- **Aim and outcomes of this lecture**
  - What are the problems?
  - TNC Process
  - Definition of the Policies
  - Summary

TNC Process
→ Aims and outcomes of this lecture

Aims

- To show the process of TNC
- To explore the idea of the combination of different security mechanisms
- To analyze who should define the policies

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

- Understand what the basic idea of network access control is
- Know something about the approach to TNC.
- Understand the need of the combination of TNC and Security Platform.

Content

- Aim and outcomes of this lecture
- **What are the problems?**
- TNC Process
- Definition of the Policies
- Summary

What are the problems?

- **Field workers** use their computer systems in many environments with ***various security requirements***.
- **Home workers** use their (company) PCs for ***private purposes***.
- **Employees** take their ***notebooks home***.

- **These computer systems can be compromised without control and knowledge of the company!**

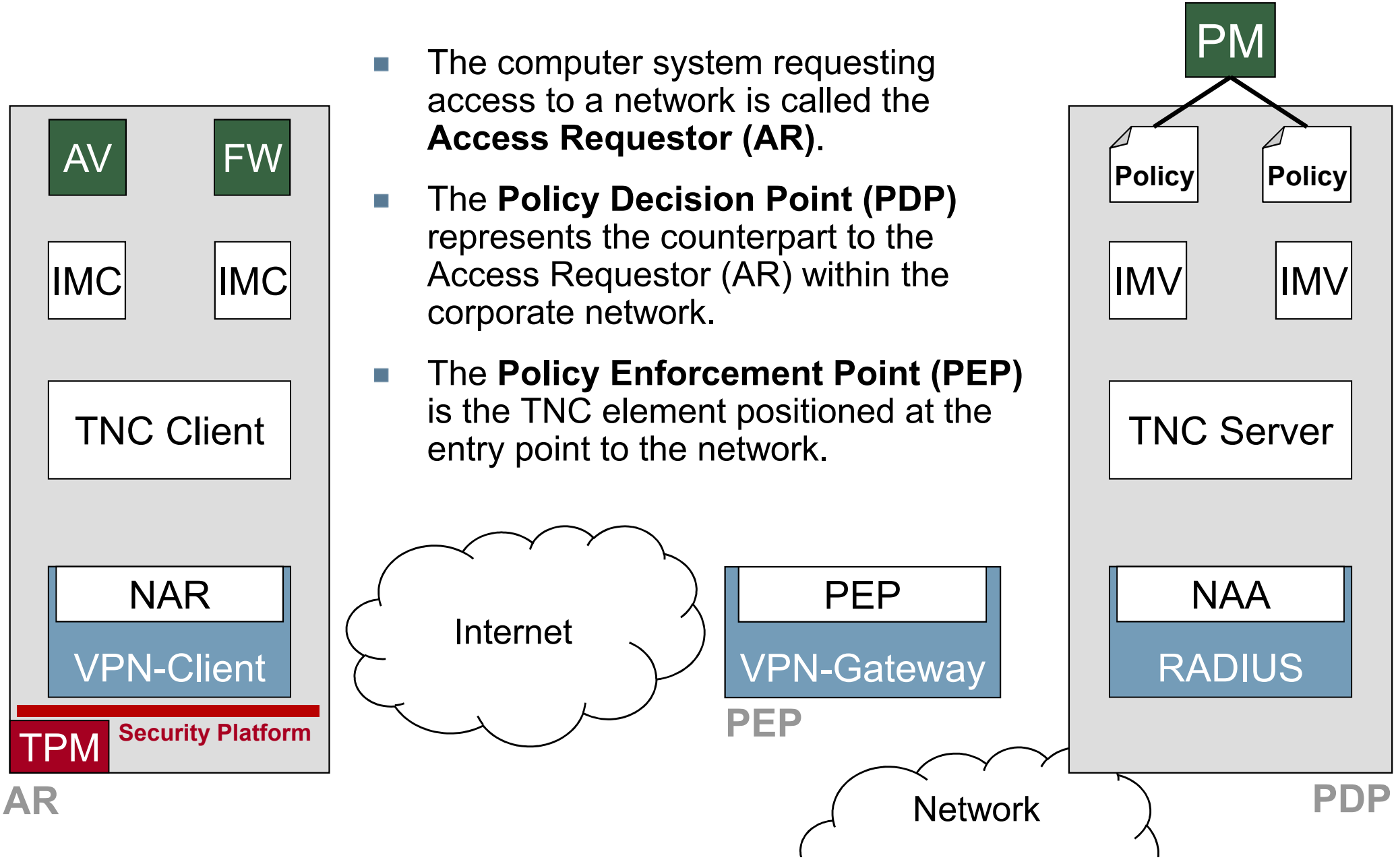
- Therefore, we need a **Network Access Control** concept, which allows an integrity check of remote computer systems!

Content

- Aim and outcomes of this lecture
- What are the problems?
- **TNC Process**
- Definition of the Policies
- Summary

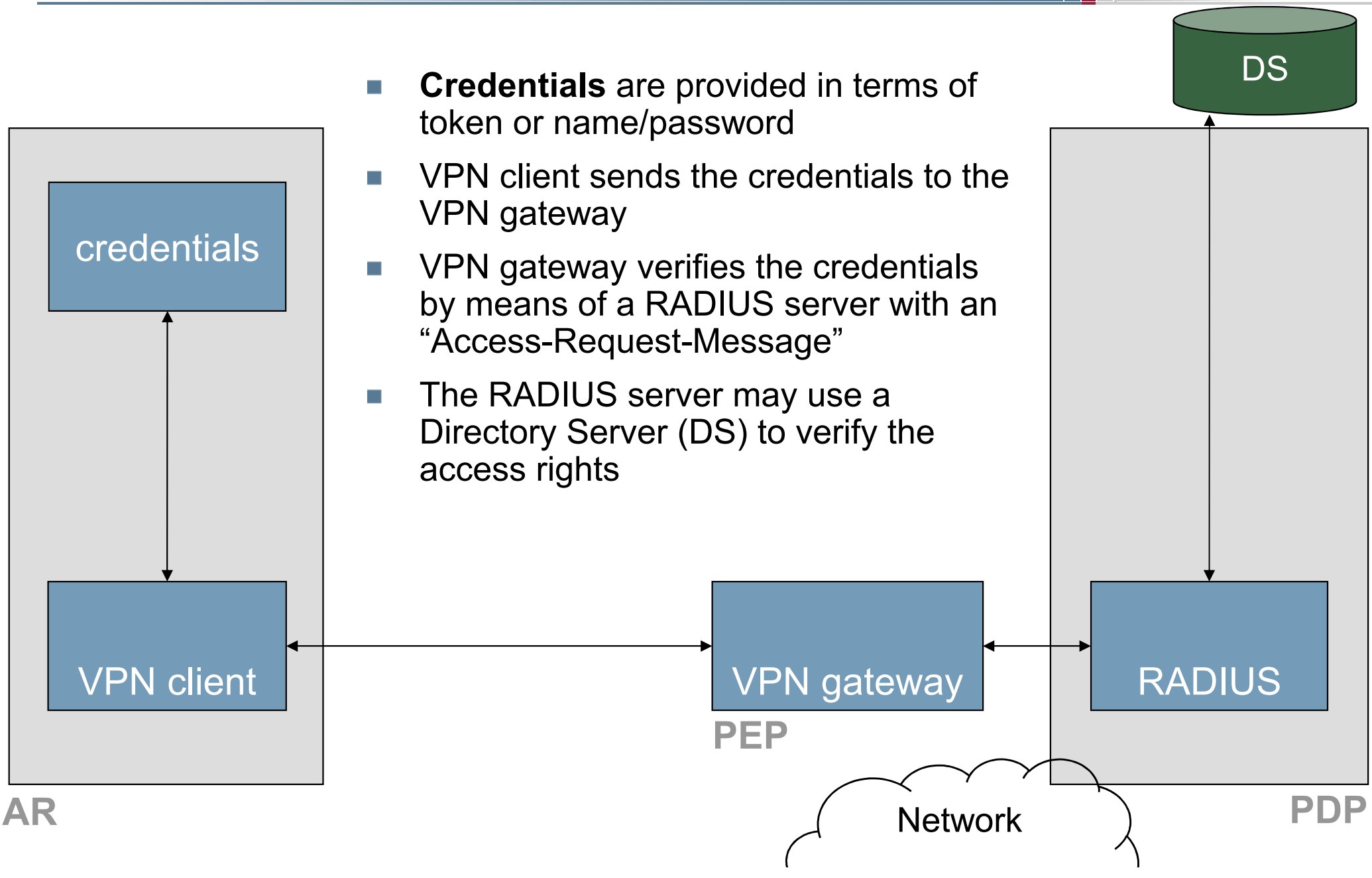
Overview
→ Trusted Network Connect (TNC)

- The computer system requesting access to a network is called the **Access Requestor (AR)**.
- The **Policy Decision Point (PDP)** represents the counterpart to the Access Requestor (AR) within the corporate network.
- The **Policy Enforcement Point (PEP)** is the TNC element positioned at the entry point to the network.



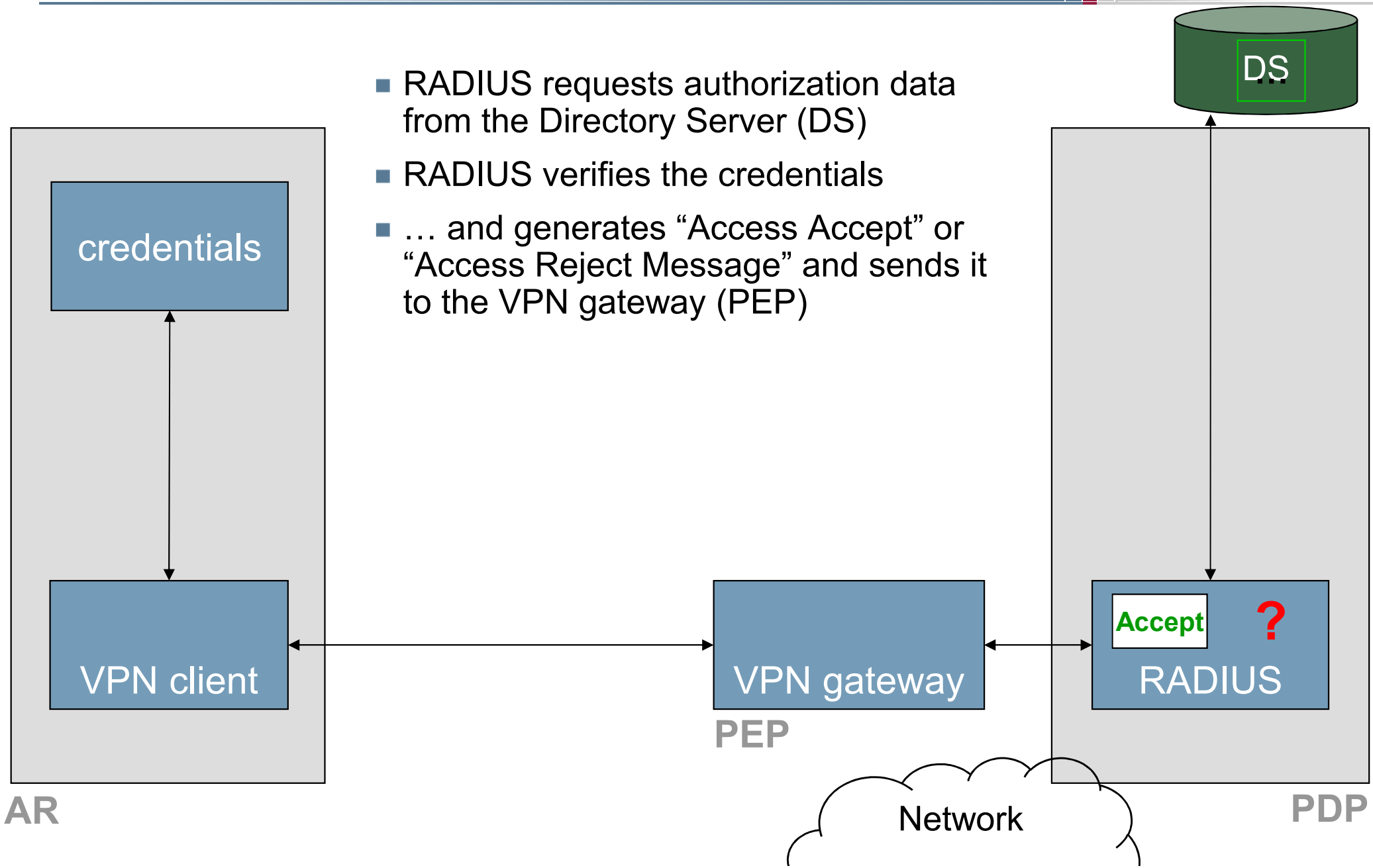
Communication via VPN (1/6)
→ Authentication/authorization (1/3)

- **Credentials** are provided in terms of token or name/password
- VPN client sends the credentials to the VPN gateway
- VPN gateway verifies the credentials by means of a RADIUS server with an “Access-Request-Message”
- The RADIUS server may use a Directory Server (DS) to verify the access rights



Communication via VPN (2/6)
→ Authentication/authorization (2/3)

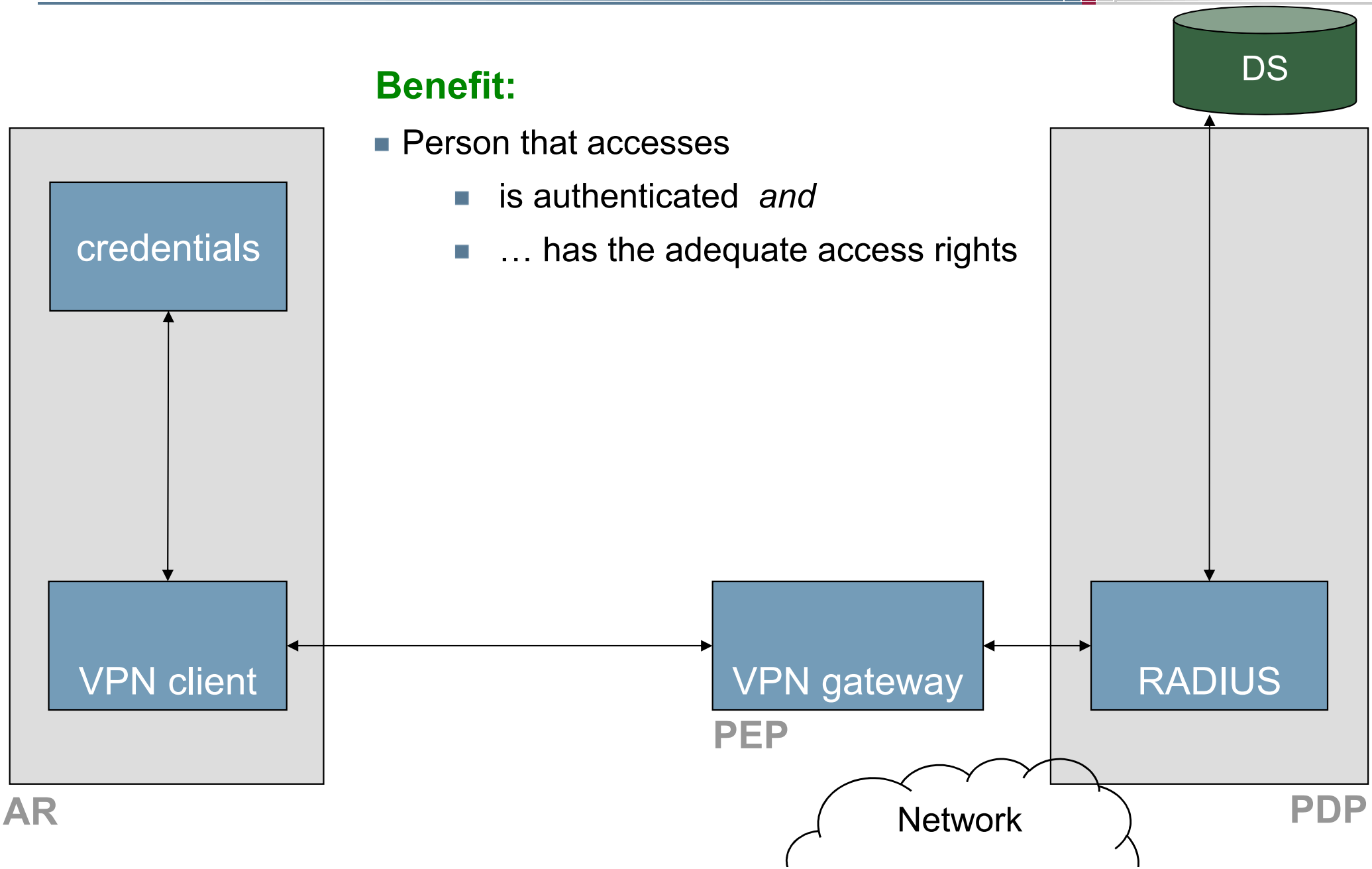
- RADIUS requests authorization data from the Directory Server (DS)
- RADIUS verifies the credentials
- … and generates “Access Accept” or “Access Reject Message” and sends it to the VPN gateway (PEP)



Communication via VPN (3/6)
→ Authentication/authorization (3/3)

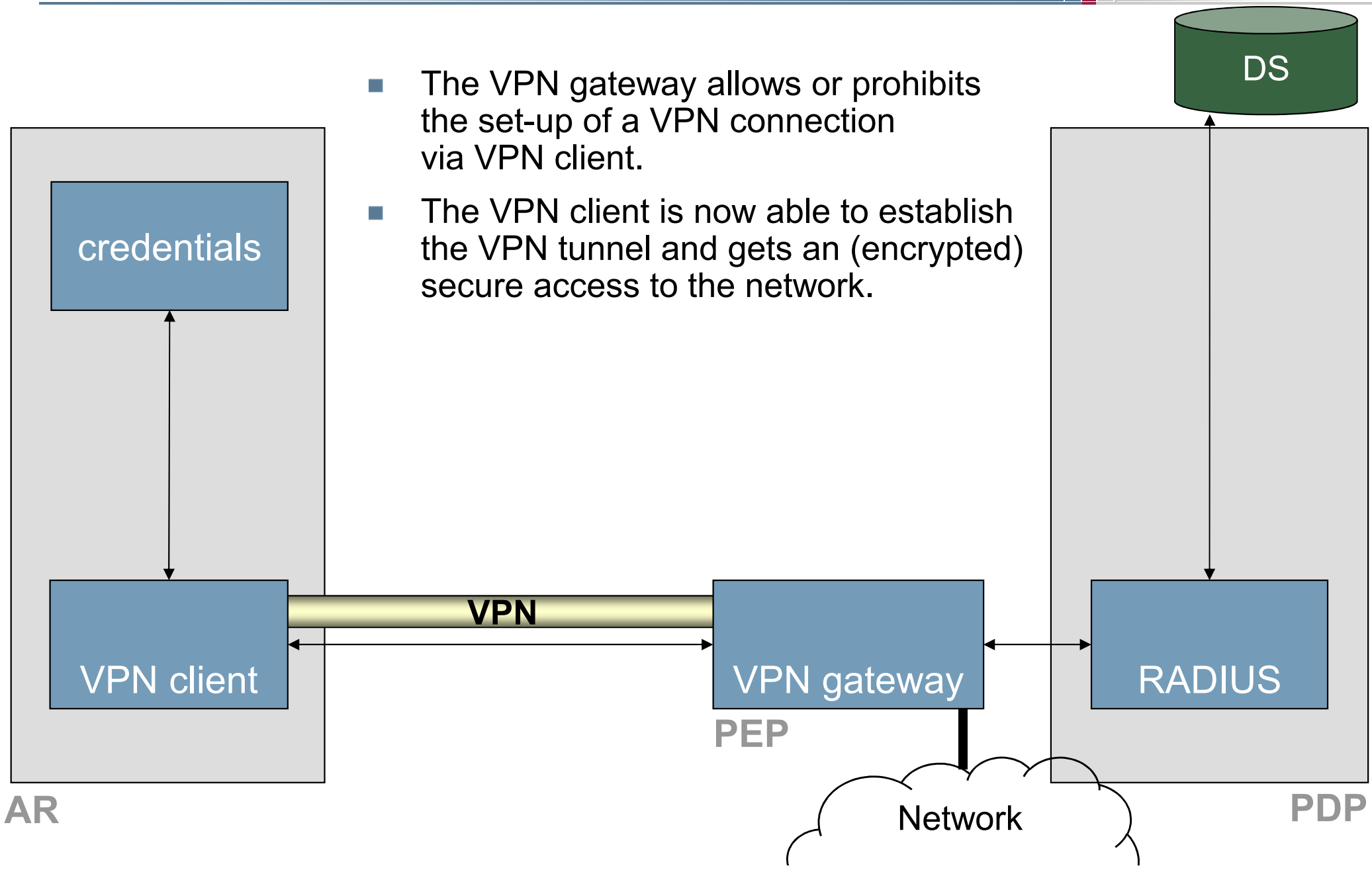
Benefit:

- Person that accesses
  - is authenticated *and*
  - … has the adequate access rights



Communication via VPN (4/6)
→Encrypted communication

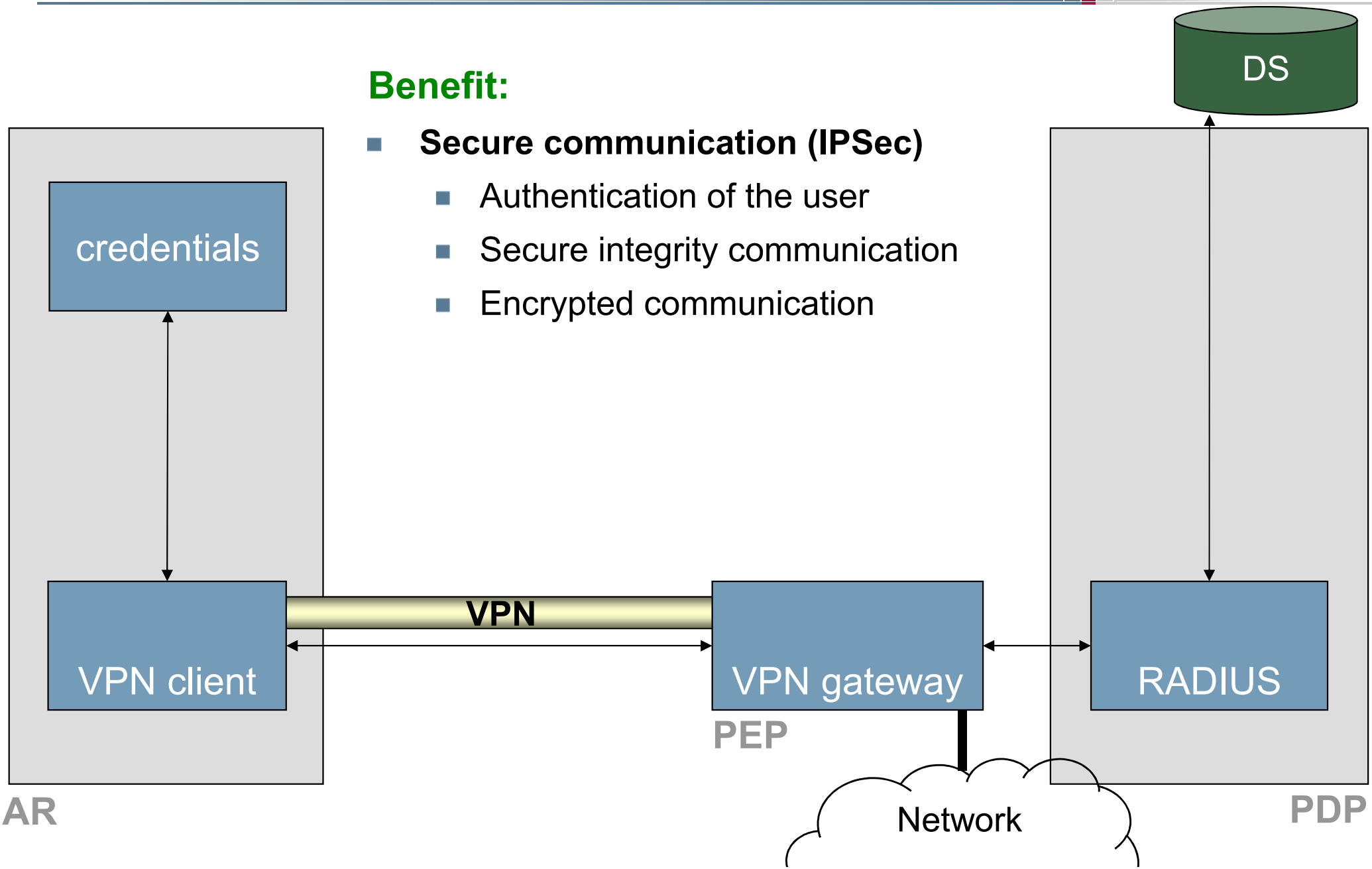
- The VPN gateway allows or prohibits the set-up of a VPN connection via VPN client.
- The VPN client is now able to establish the VPN tunnel and gets an (encrypted) secure access to the network.



Communication via VPN (5/6)
→ Secure communication (IPSec)

Benefit:

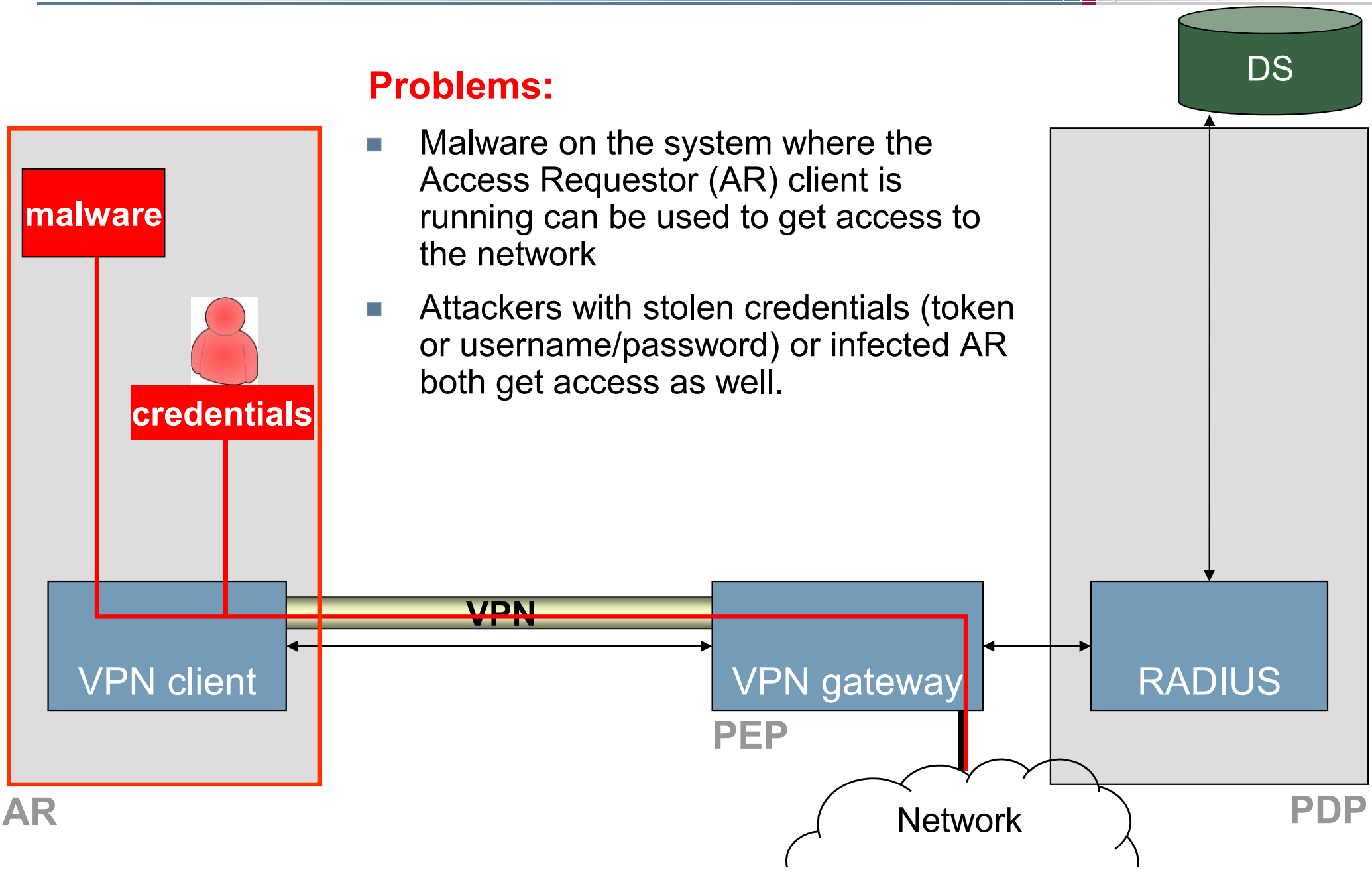
- **Secure communication (IPSec)**
  - Authentication of the user
  - Secure integrity communication
  - Encrypted communication



Communication via VPN (6/6)
→ Open problems with VPN

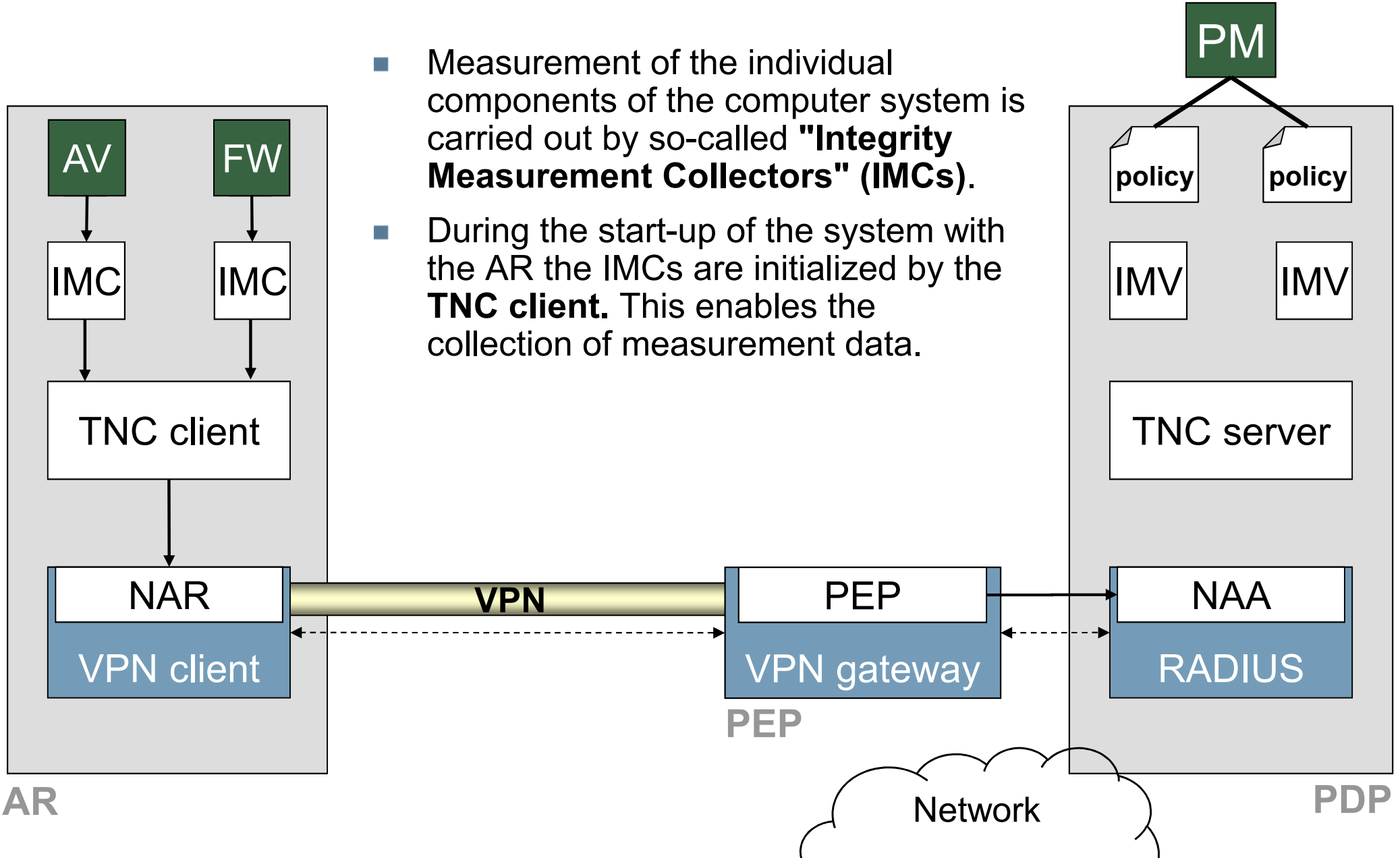
Problems:

- Malware on the system where the Access Requestor (AR) client is running can be used to get access to the network
- Attackers with stolen credentials (token or username/password) or infected AR both get access as well.



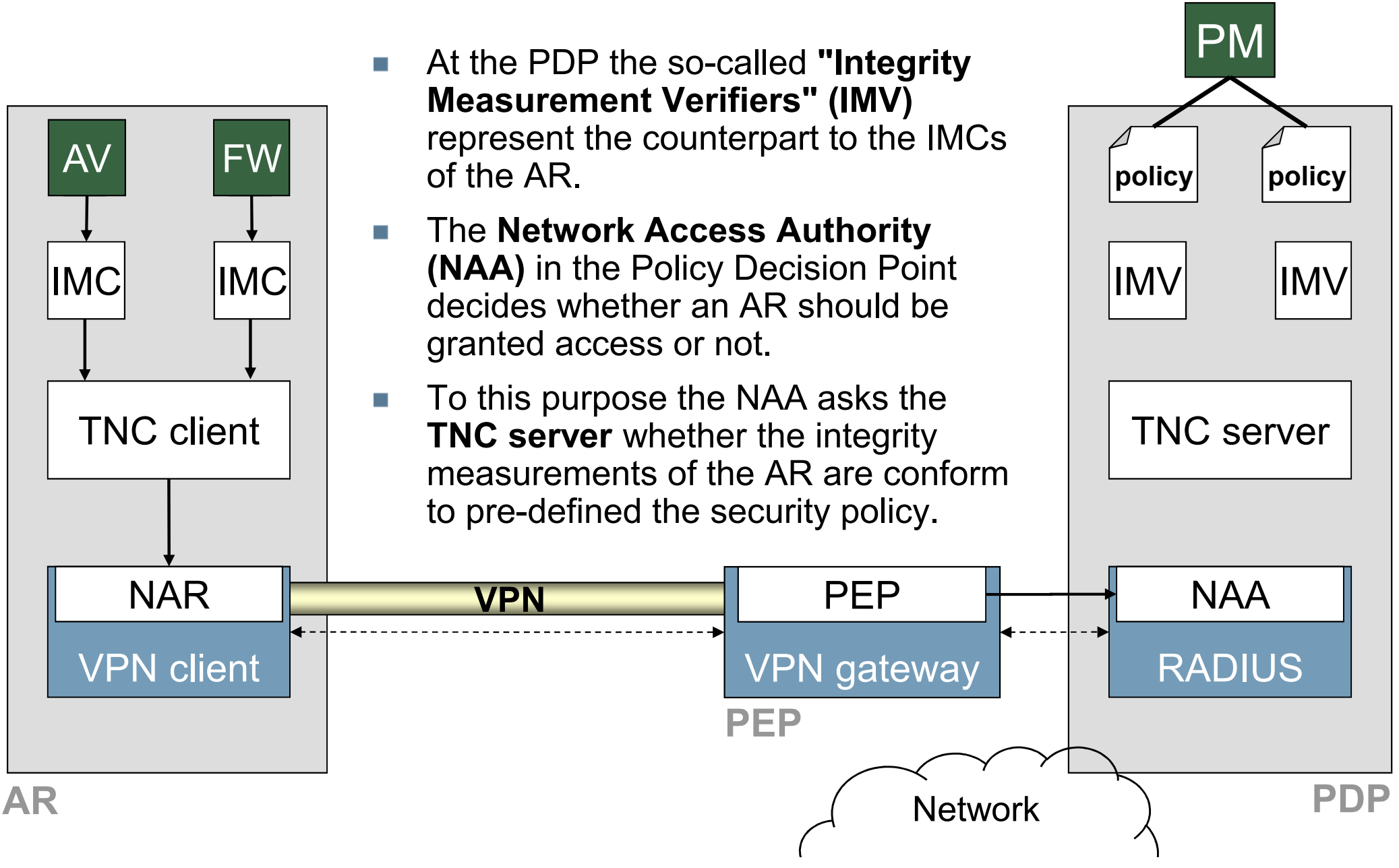
Trusted Network Connect (TNC)
→ Overview: TNC-functions (1/2)

- Measurement of the individual components of the computer system is carried out by so-called **"Integrity Measurement Collectors" (IMCs)**.
- During the start-up of the system with the AR the IMCs are initialized by the **TNC client.** This enables the collection of measurement data.



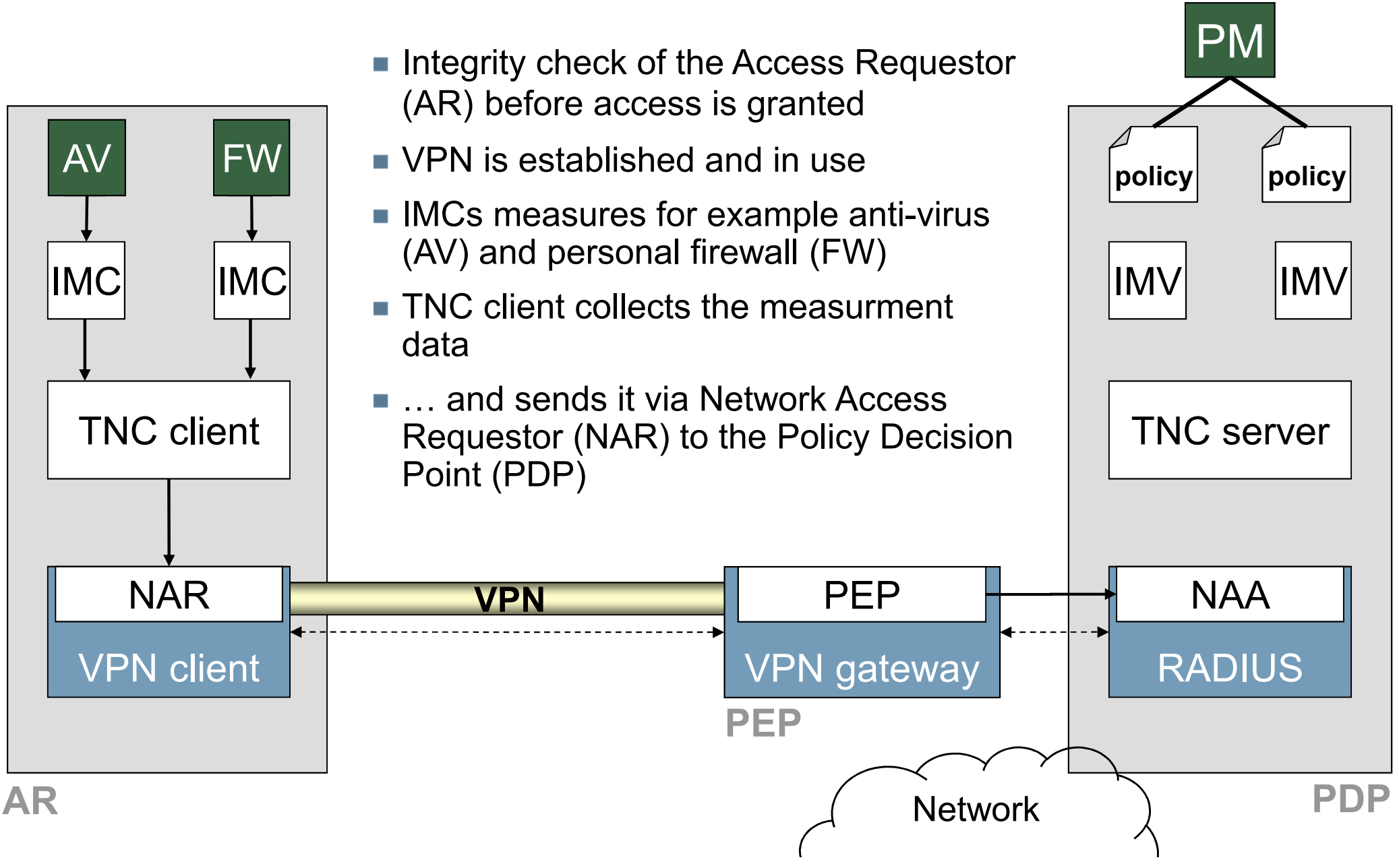
Trusted Network Connect (TNC)
→ Overview: TNC-functions (2/2)

- At the PDP the so-called **"Integrity Measurement Verifiers" (IMV)** represent the counterpart to the IMCs of the AR.
- The **Network Access Authority (NAA)** in the Policy Decision Point decides whether an AR should be granted access or not.
- To this purpose the NAA asks the **TNC server** whether the integrity measurements of the AR are conform to pre-defined the security policy.



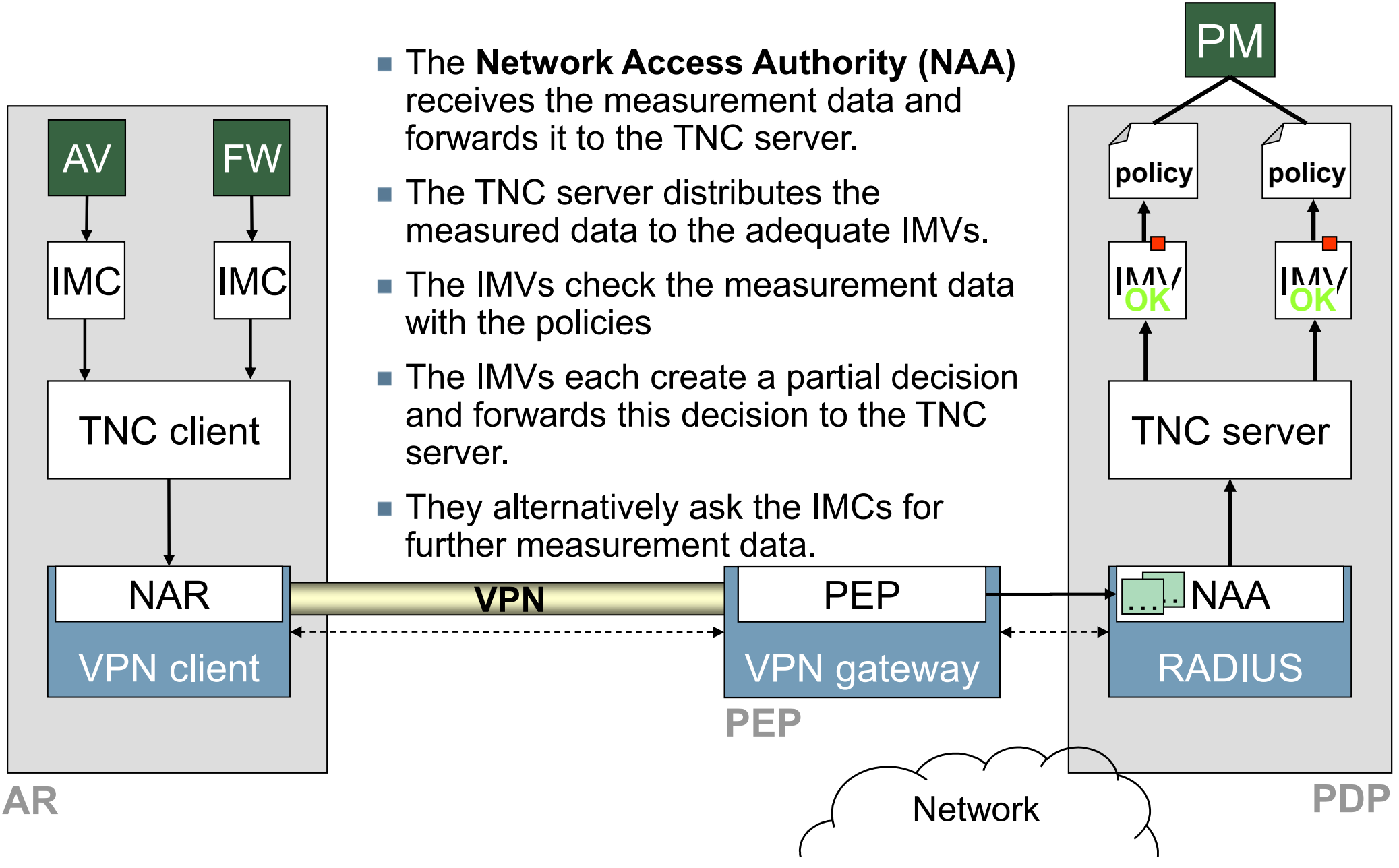
TNC – phases
→ Assessment phase (1/3)

- Integrity check of the Access Requestor (AR) before access is granted
- VPN is established and in use
- IMCs measures for example anti-virus (AV) and personal firewall (FW)
- TNC client collects the measurment data
- … and sends it via Network Access Requestor (NAR) to the Policy Decision Point (PDP)



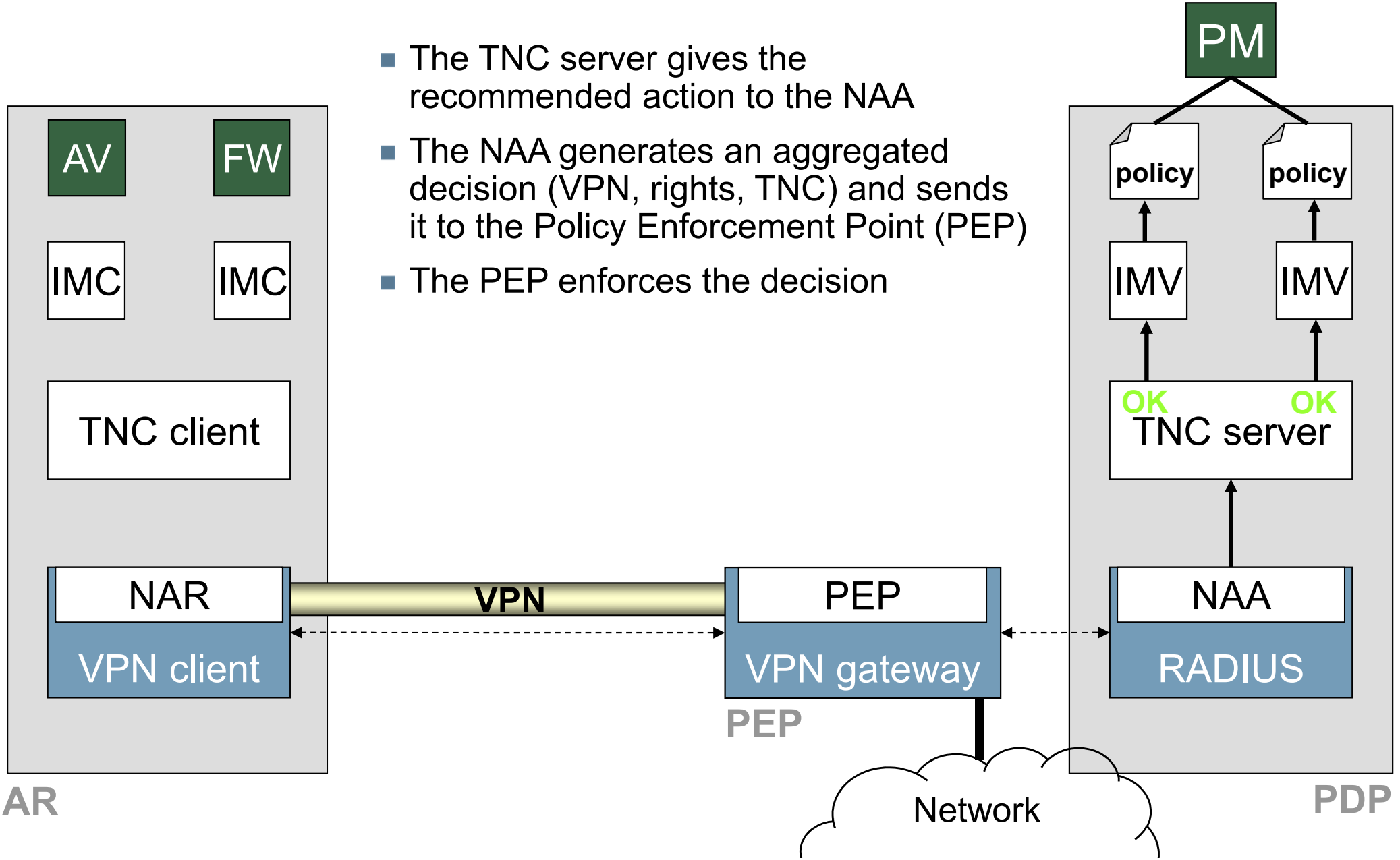
TNC – phases
→ Assessment phase (2/3)

- The **Network Access Authority (NAA)** receives the measurement data and forwards it to the TNC server.
- The TNC server distributes the measured data to the adequate IMVs.
- The IMVs check the measurement data with the policies
- The IMVs each create a partial decision and forwards this decision to the TNC server.
- They alternatively ask the IMCs for further measurement data.



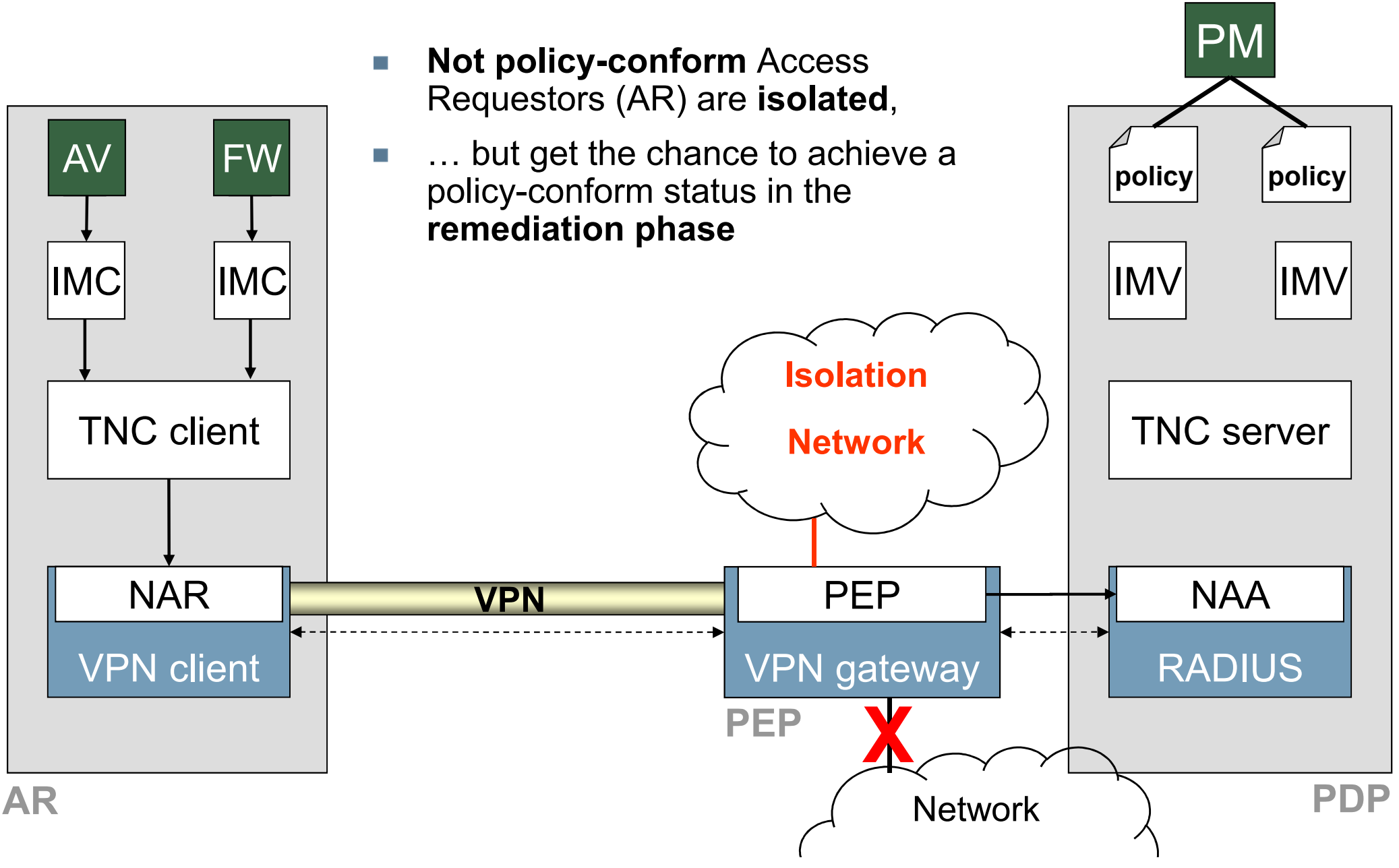
TNC – phases
→ Assessment phase (3/3)

- The TNC server gives the recommended action to the NAA
- The NAA generates an aggregated decision (VPN, rights, TNC) and sends it to the Policy Enforcement Point (PEP)
- The PEP enforces the decision



TNC – phases
→ Isolation and remediation phase

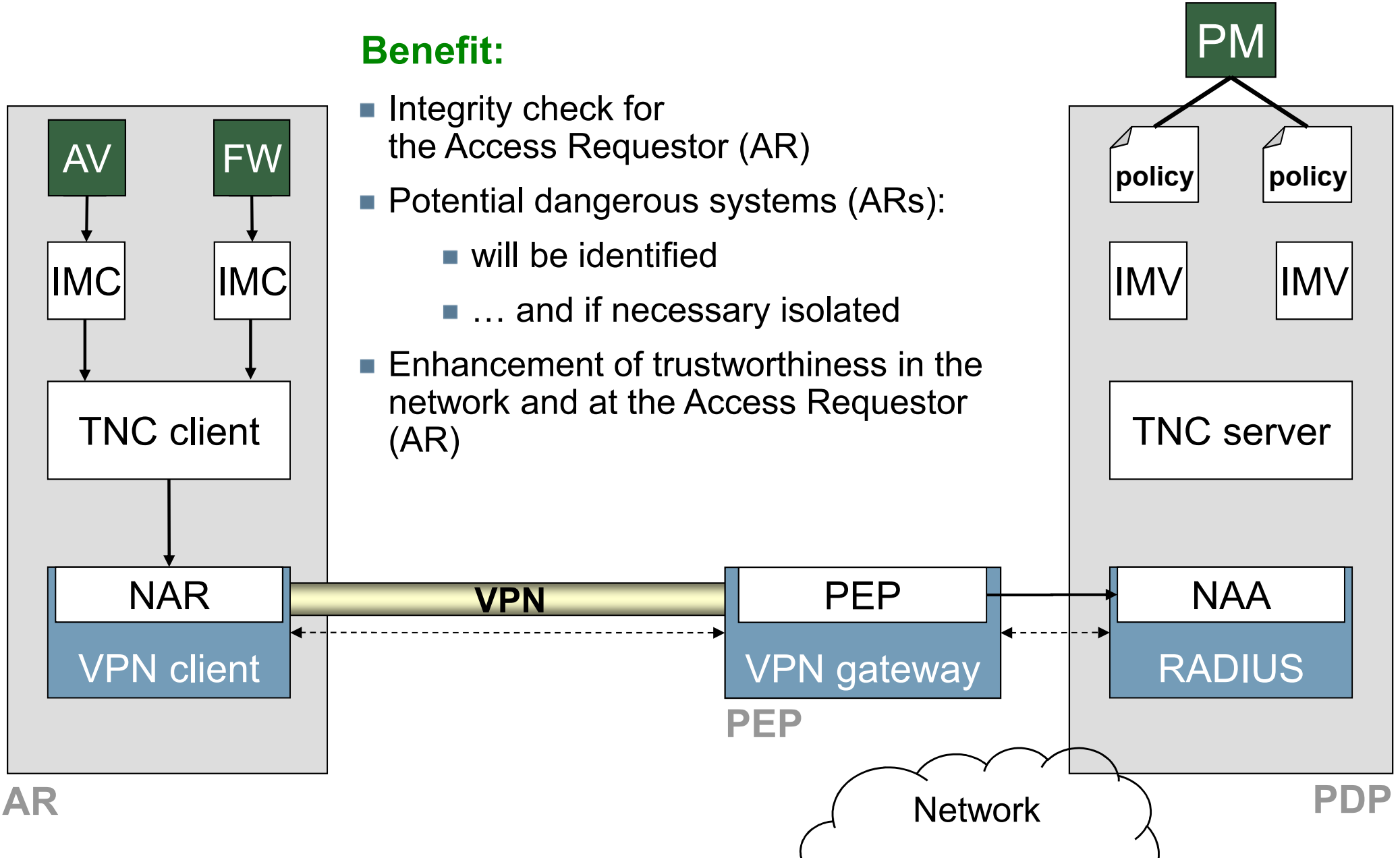
- **Not policy-conform** Access Requestors (AR) are **isolated**,
- … but get the chance to achieve a policy-conform status in the **remediation phase**



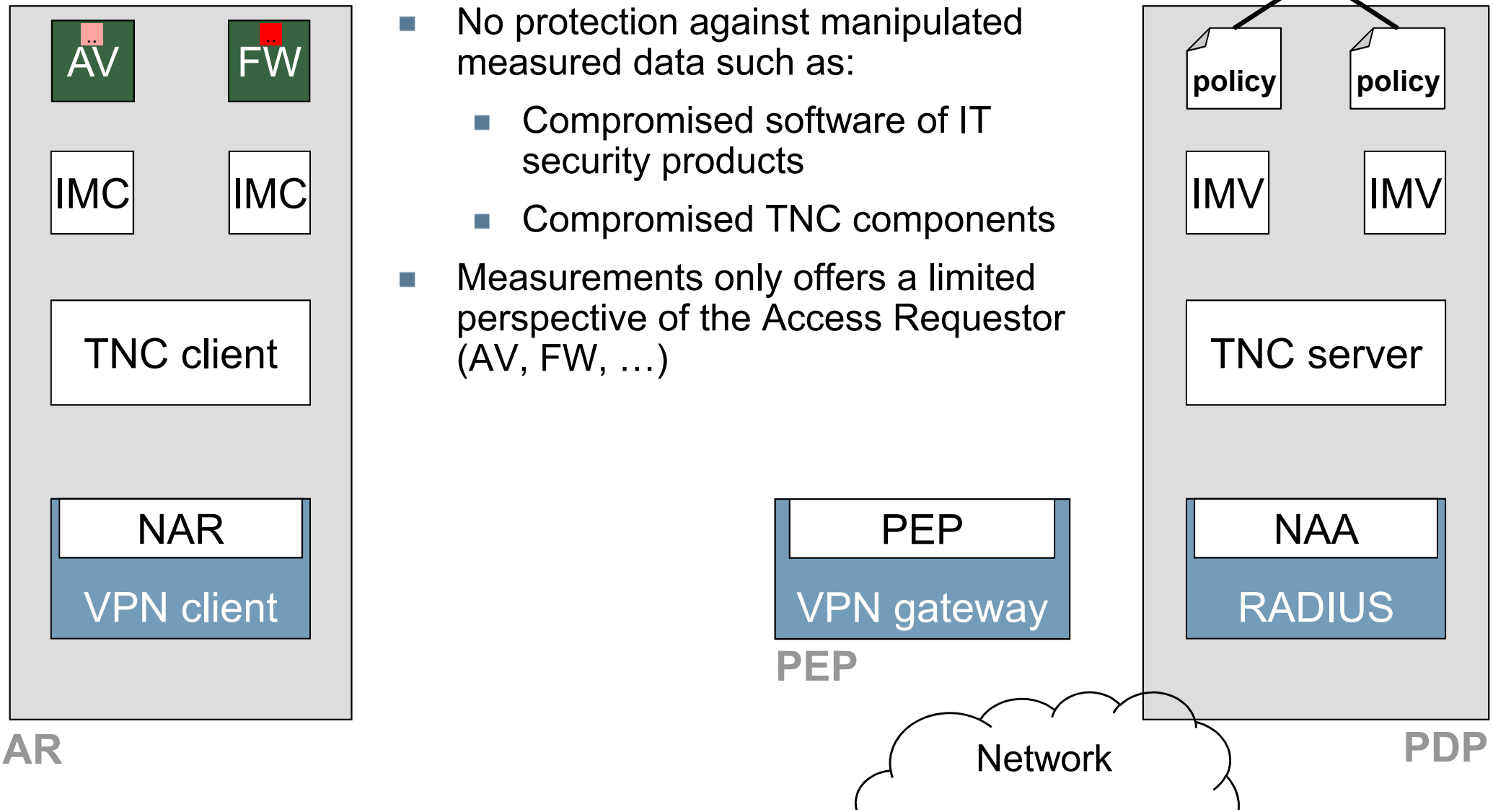
TNC
→ Trusted Network Connect

Benefit:

- Integrity check for the Access Requestor (AR)
- Potential dangerous systems (ARs):
  - will be identified
  - … and if necessary isolated
- Enhancement of trustworthiness in the network and at the Access Requestor (AR)



TNC
→ Open problems with TNC

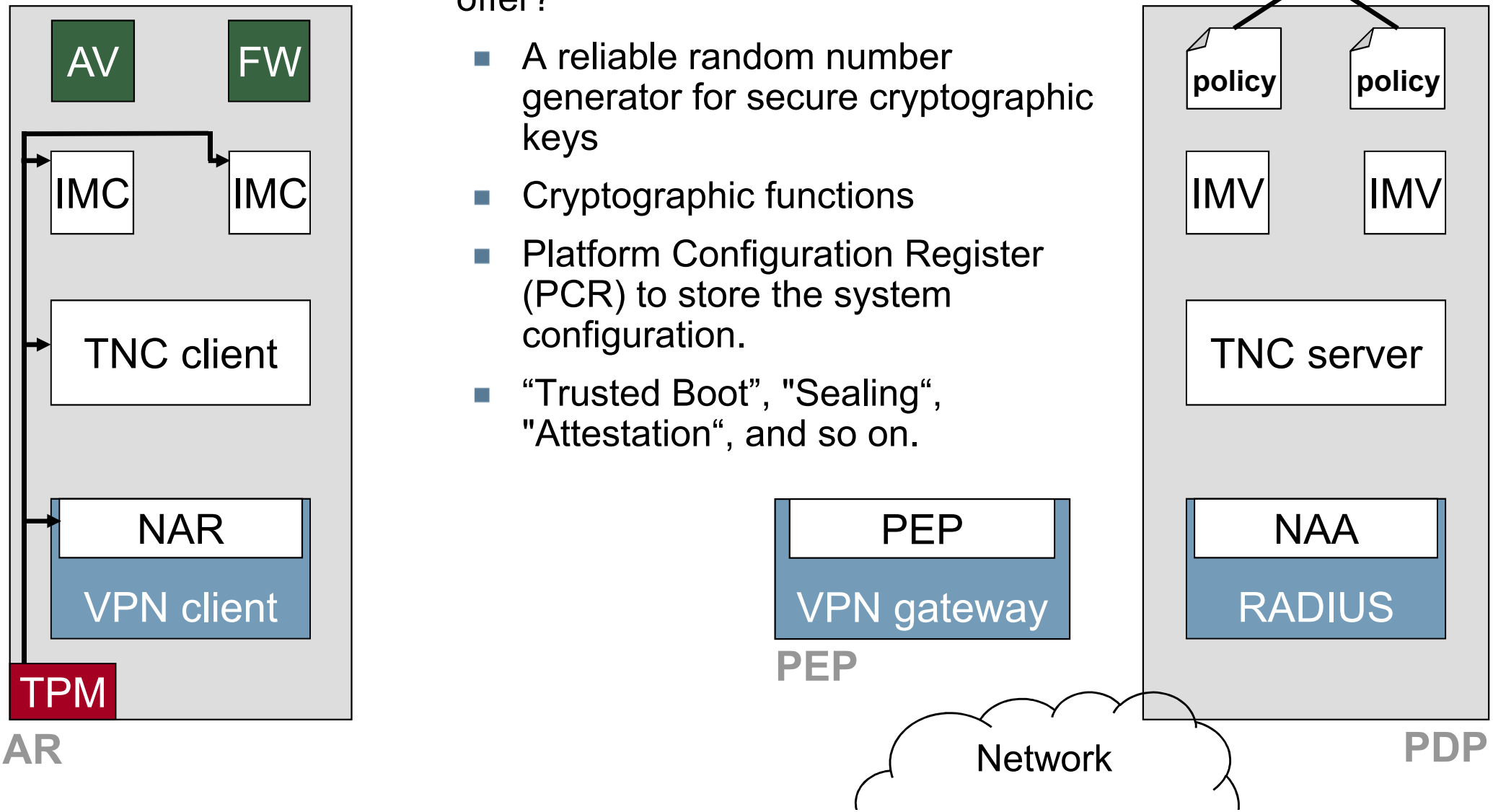


Problems:

- No protection against manipulated measured data such as:
  - Compromised software of IT security products
  - Compromised TNC components
- Measurements only offers a limited perspective of the Access Requestor (AV, FW, …)

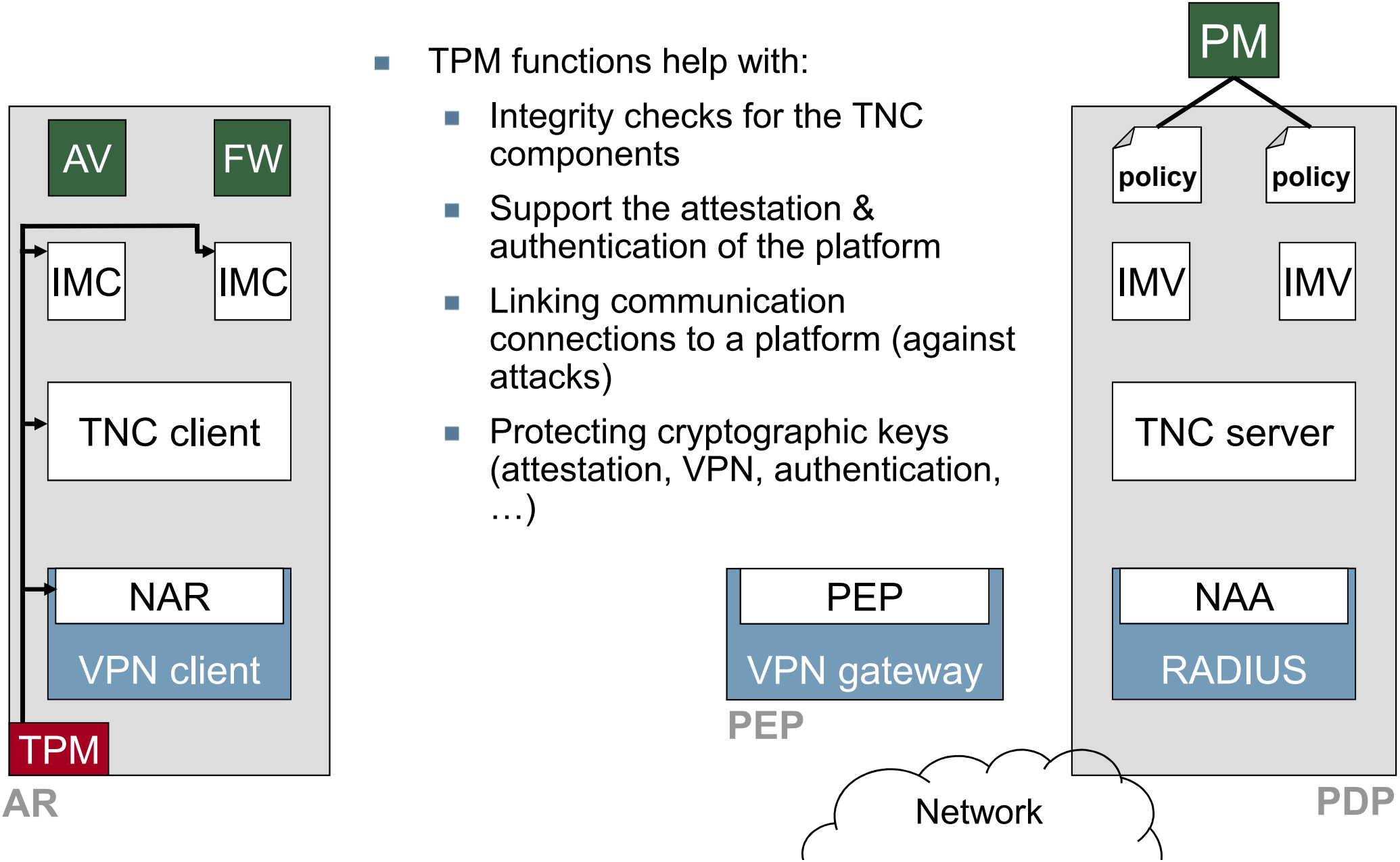
TNC+
→ TNC + TPM

- What additional benefit does the TPM offer?
  - A reliable random number generator for secure cryptographic keys
  - Cryptographic functions
  - Platform Configuration Register (PCR) to store the system configuration.
  - “Trusted Boot”, "Sealing“, "Attestation“, and so on.



TNC+
→ additional benefit: TPM

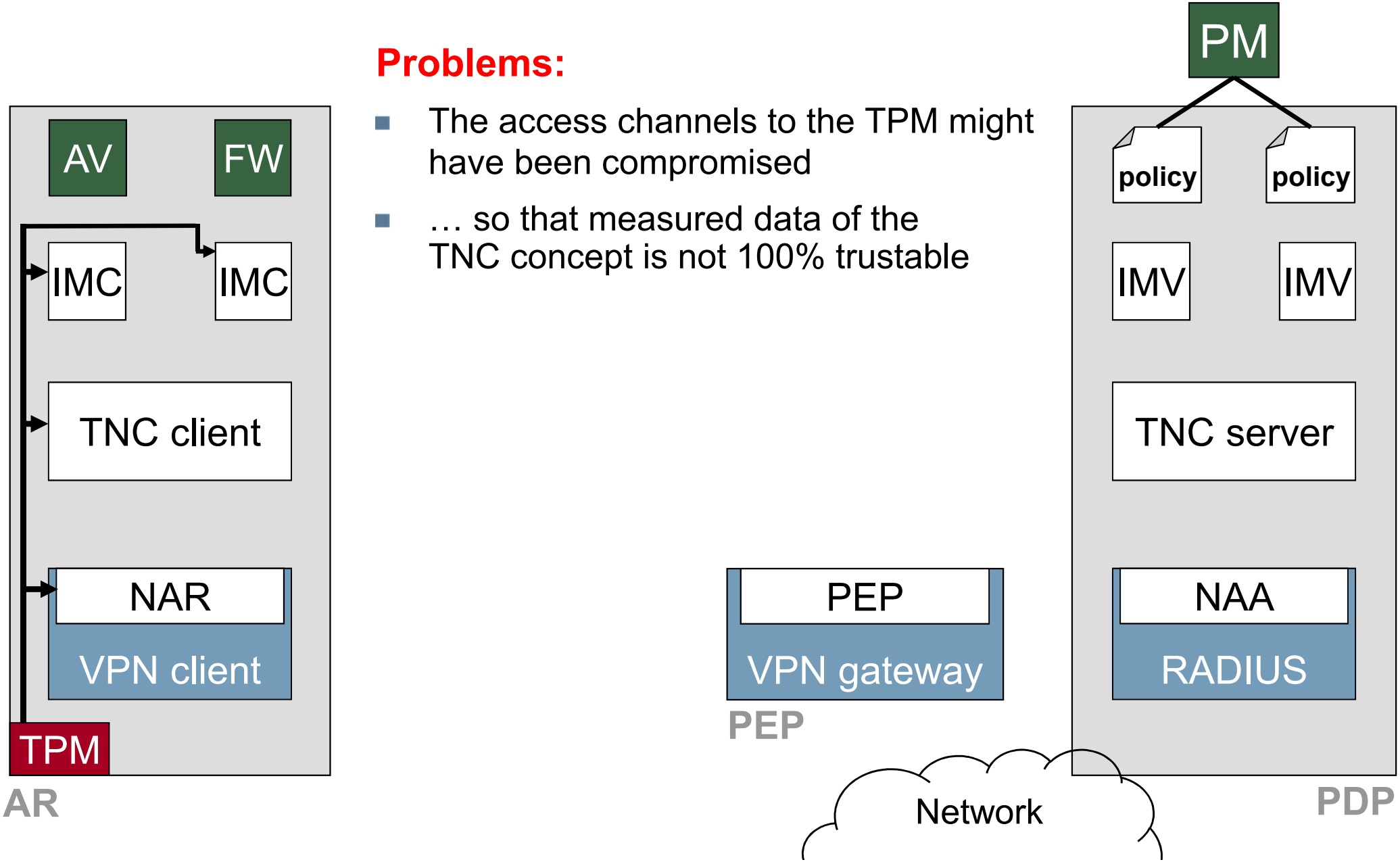
- TPM functions help with:
  - Integrity checks for the TNC components
  - Support the attestation & authentication of the platform
  - Linking communication connections to a platform (against attacks)
  - Protecting cryptographic keys (attestation, VPN, authentication, …)



TNC+
→ TPM: restrictions

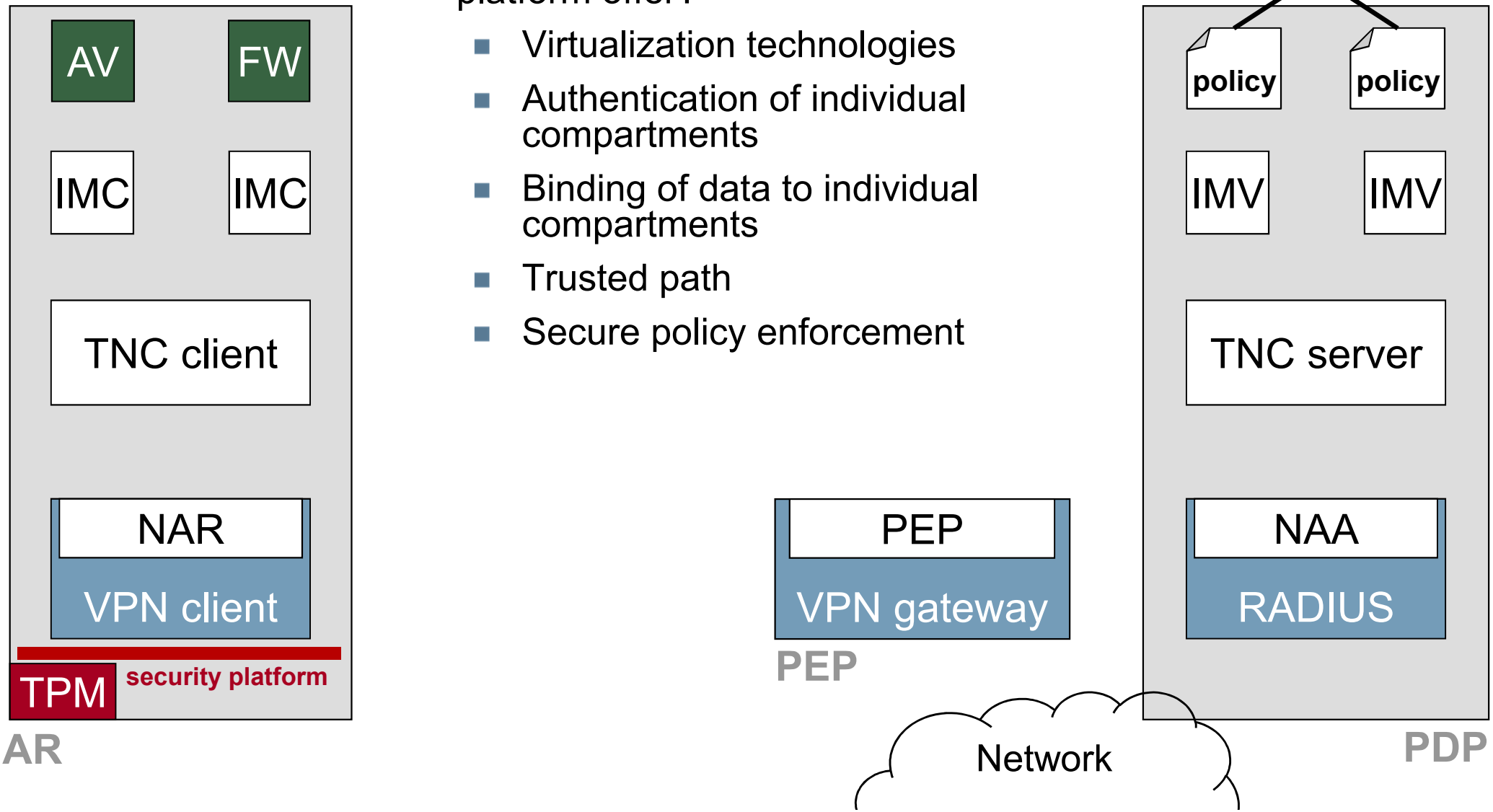
Problems:

- The access channels to the TPM might have been compromised
- … so that measured data of the TNC concept is not 100% trustable



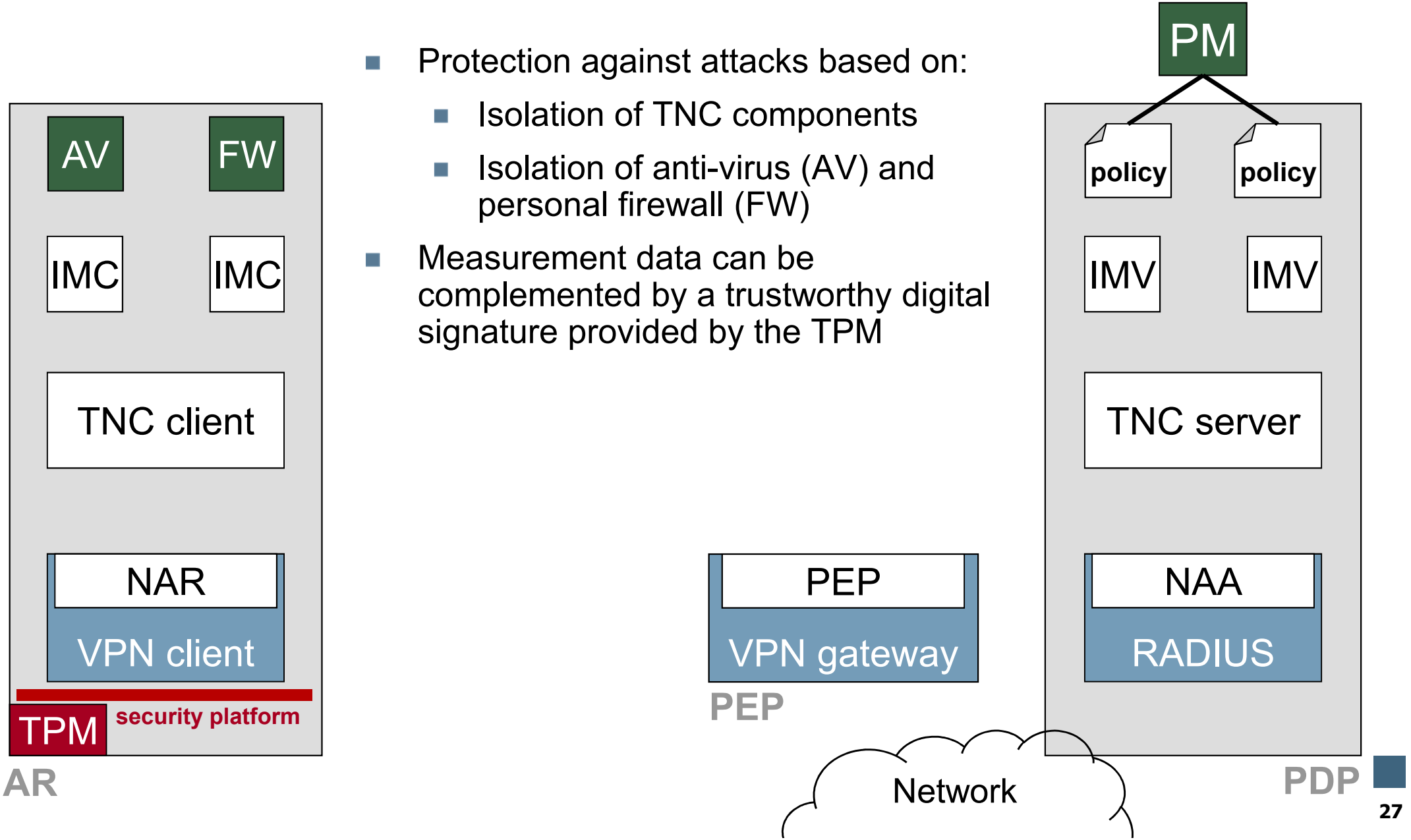
TNC++
→ TNC + TPM + security platform

- What additional benefit does a security platform offer?
  - Virtualization technologies
  - Authentication of individual compartments
  - Binding of data to individual compartments
  - Trusted path
  - Secure policy enforcement

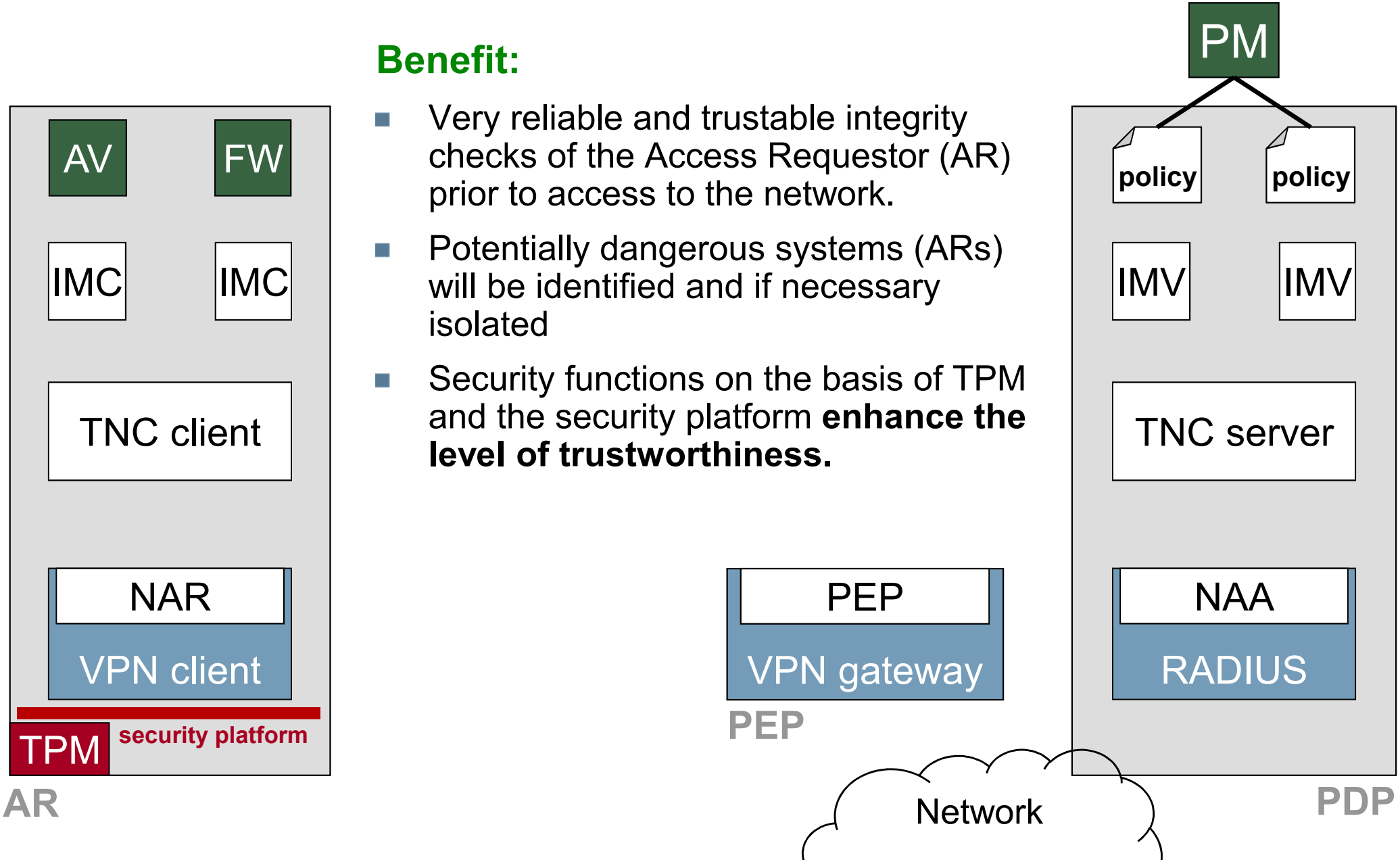


TNC++
→ Overvalue: security platform

- Protection against attacks based on:
  - Isolation of TNC components
  - Isolation of anti-virus (AV) and personal firewall (FW)
- Measurement data can be complemented by a trustworthy digital signature provided by the TPM



TNC++
→ Added value: security platform



Benefit:

- Very reliable and trustable integrity checks of the Access Requestor (AR) prior to access to the network.
- Potentially dangerous systems (ARs) will be identified and if necessary isolated
- Security functions on the basis of TPM and the security platform **enhance the level of trustworthiness.**

Content

- Aim and outcomes of this lecture
- What are the problems?
- TNC Process
- **Definition of the Policies**
- Summary

Open questions (1/2)

- **Who defines the policies?**
- Who defines which configuration of systems and IT security products can be credited as trustworthy?
  - **Vendors?**
    - Operating systems and applications vendors?
    - Software vendor of TNC solution?
    - Security software vendors of IT security products such as IMC and IMV for anti-virus (AV) and personal firewall (FW)?
  - **Operators?**
    - Strategic decision?
    - Experiences?
  - **Both together?**
    - How can we structure this cooperation?
    - Who takes the responsibility?

Open questions (2/2)

- Do we need a **Technical Inspection Authority?**
  - Which makes a common criteria evaluation for IT systems
  - And only if the evaluation is ok, companies can sell the hardware and software?

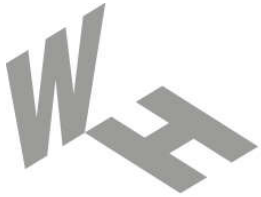
- Do we need a **user-oriented organization**, which takes care of the trustworthiness?
  - Verification of new technologies, security mechanisms, and so on
  - Collecting the experience of the user
  - Recommendation how to use integrity check of remote computer systems

Content

- Aim and outcomes of this lecture
- What are the problems?
- TNC Process
- Definition of the Policies
- **Summary**

TNC Process
→ Summary

- Trustworthiness is not a status!
- **Trustworthiness is a process!**
- Let us start the necessary process to reach a **higher level of trustworthiness**!
- **Network Access Control** and especially **Trusted Network Connect** seem to be the right concept.



Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Trusted Computing
→ Introduction

Thank you for your attention!
Questions?

Prof. Dr. (TU NN)
Norbert Pohlmann

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

if(is) internet security.

TNC Process
→ 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/