2007 ISSE
INFORMATION SECURITY SOLUTIONS EUROPE

Integrity Check of Remote Computer Systems → Trusted Network Connect

Prof. Dr. Norbert Pohlmann

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

if(is) internet security.

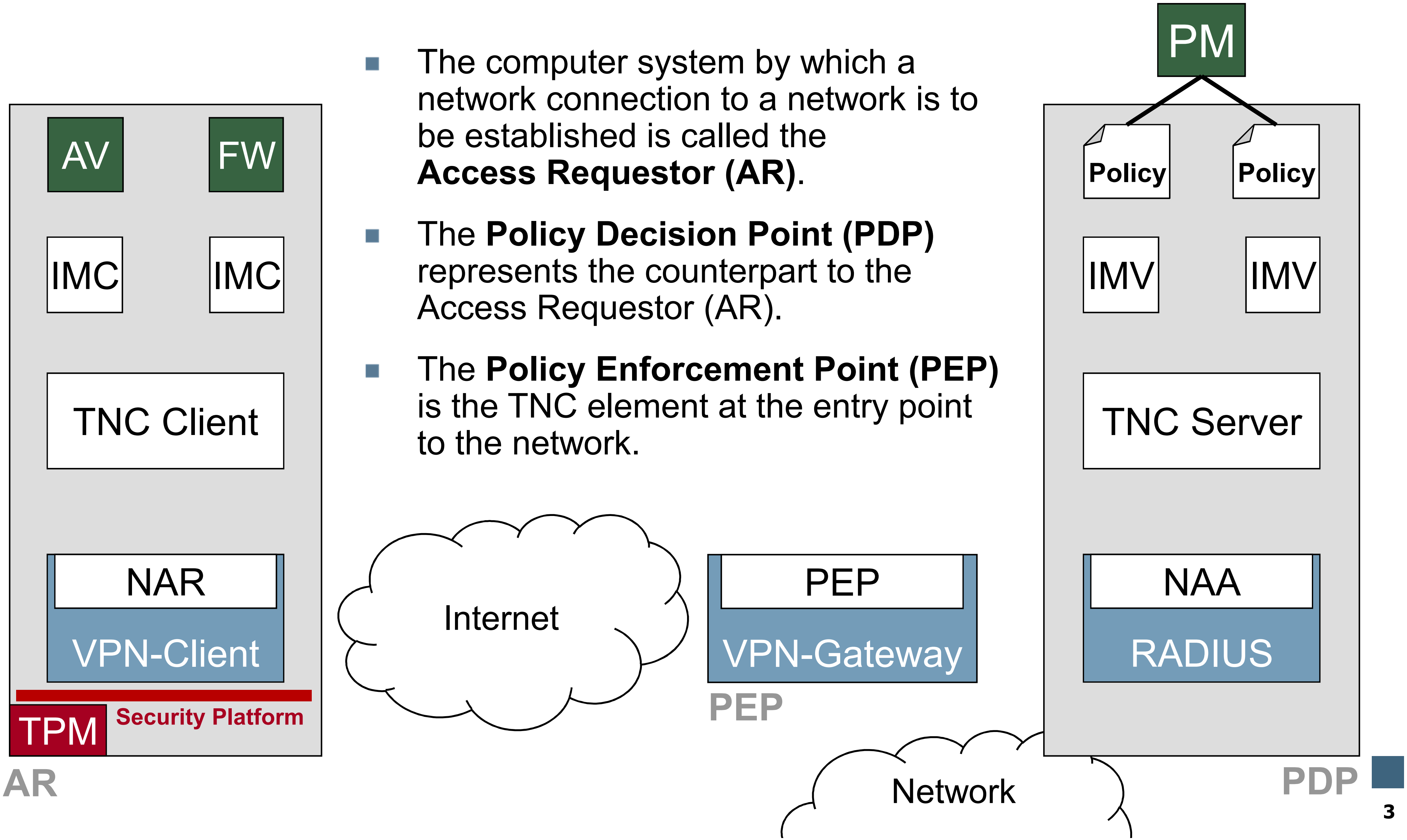
What are the problems?

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

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

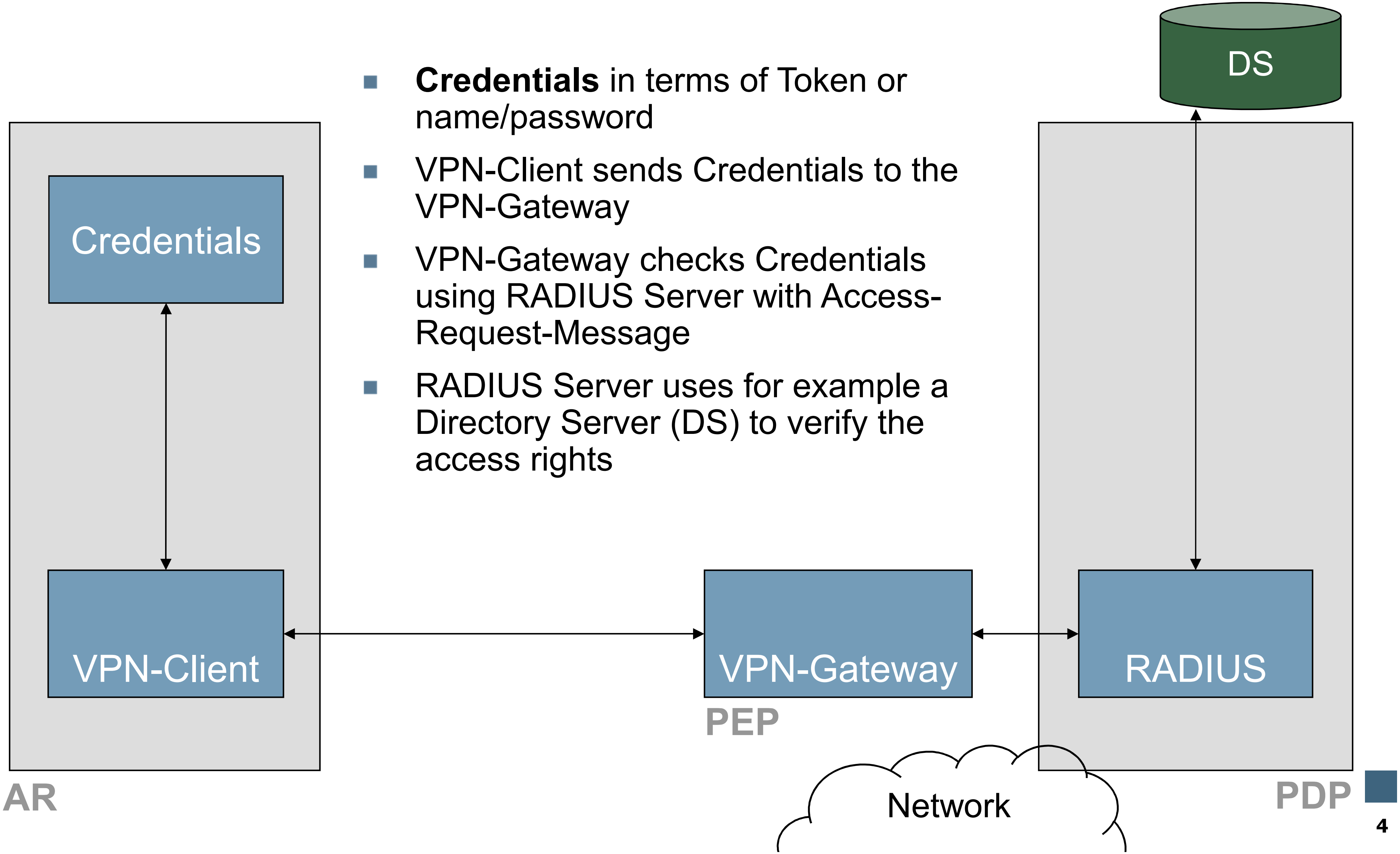
- Therefore we need a **Network Access Control** concept, which allows an integrity check of remote computer systems!

Overview
→ Trusted Network Connect (TNC)



- The computer system by which a network connection to a network is to be established is called the **Access Requestor (AR)**.
- The **Policy Decision Point (PDP)** represents the counterpart to the Access Requestor (AR).
- The **Policy Enforcement Point (PEP)** is the TNC element at the entry point to the network.

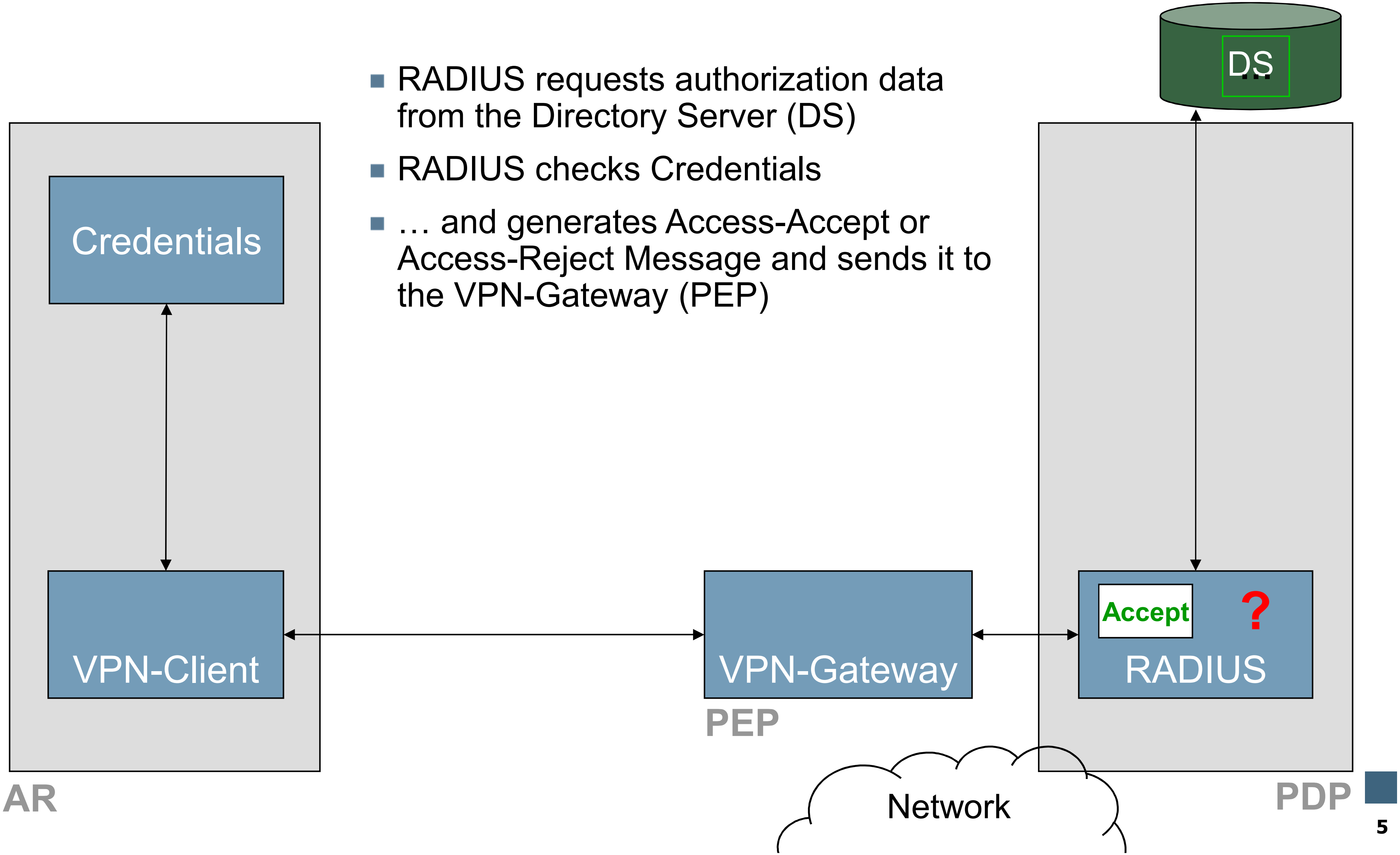
Communication via VPN (1/6)
→ Authentication/authorization (1/3)



- **Credentials** in terms of Token or name/password
- VPN-Client sends Credentials to the VPN-Gateway
- VPN-Gateway checks Credentials using RADIUS Server with Access-Request-Message
- RADIUS Server uses for example a Directory Server (DS) to verify the access rights

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

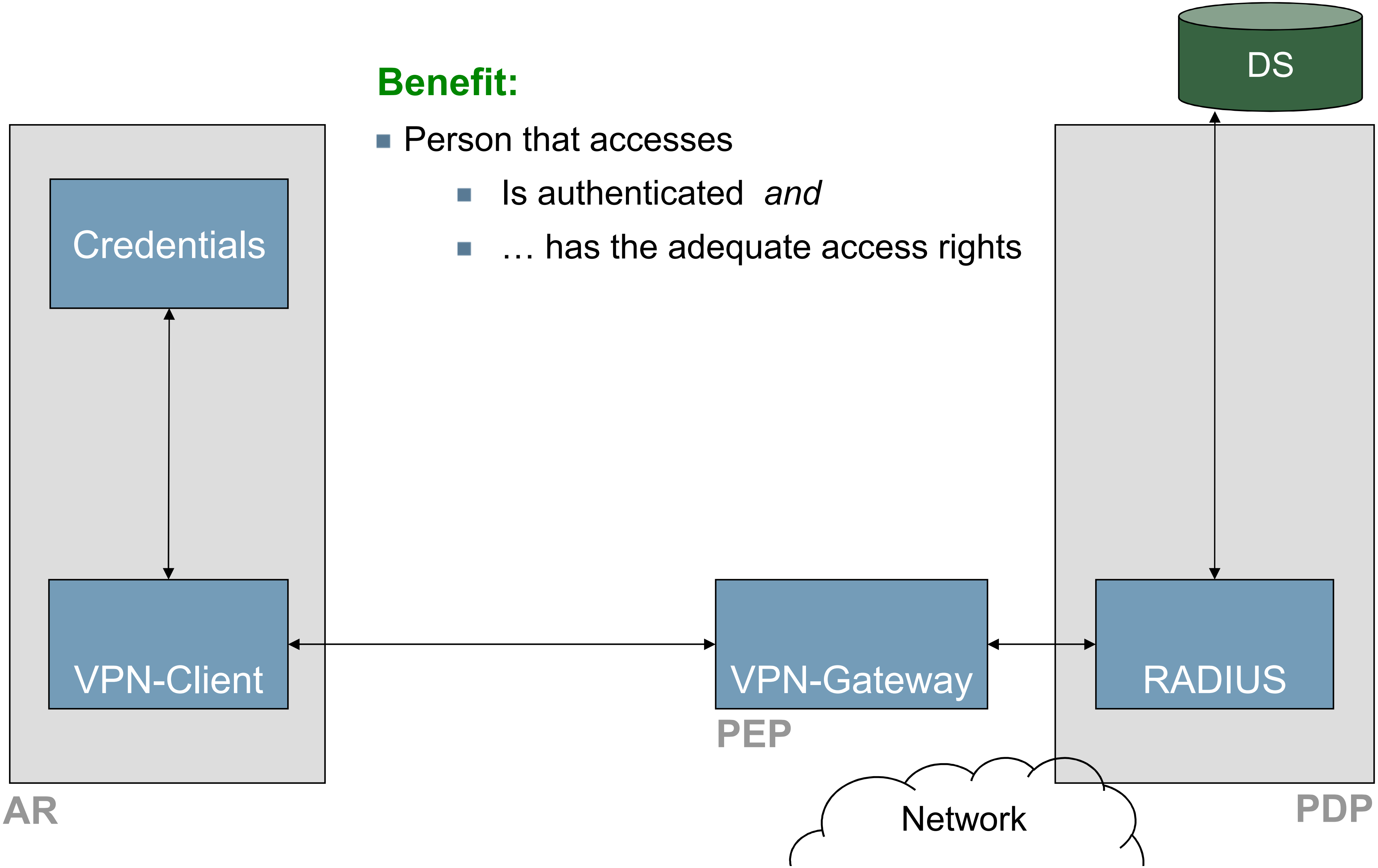
- RADIUS requests authorization data from the Directory Server (DS)
- RADIUS checks Credentials
- … and generates Access-Accept or Access-Reject Message and sends it to the VPN-Gateway (PEP)



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

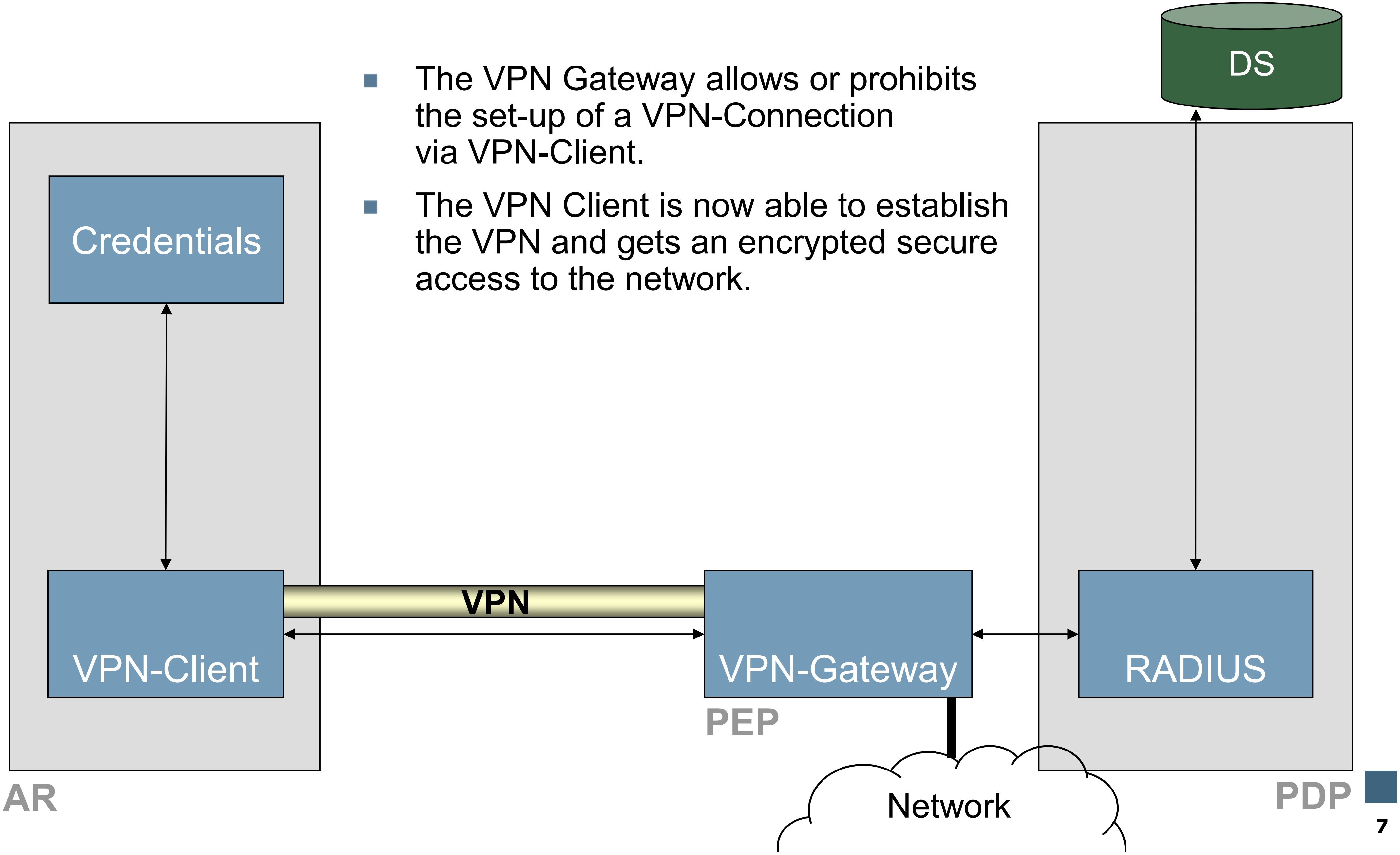
Benefit:

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



Communication via VPN (4/6)
→Encrypted communication

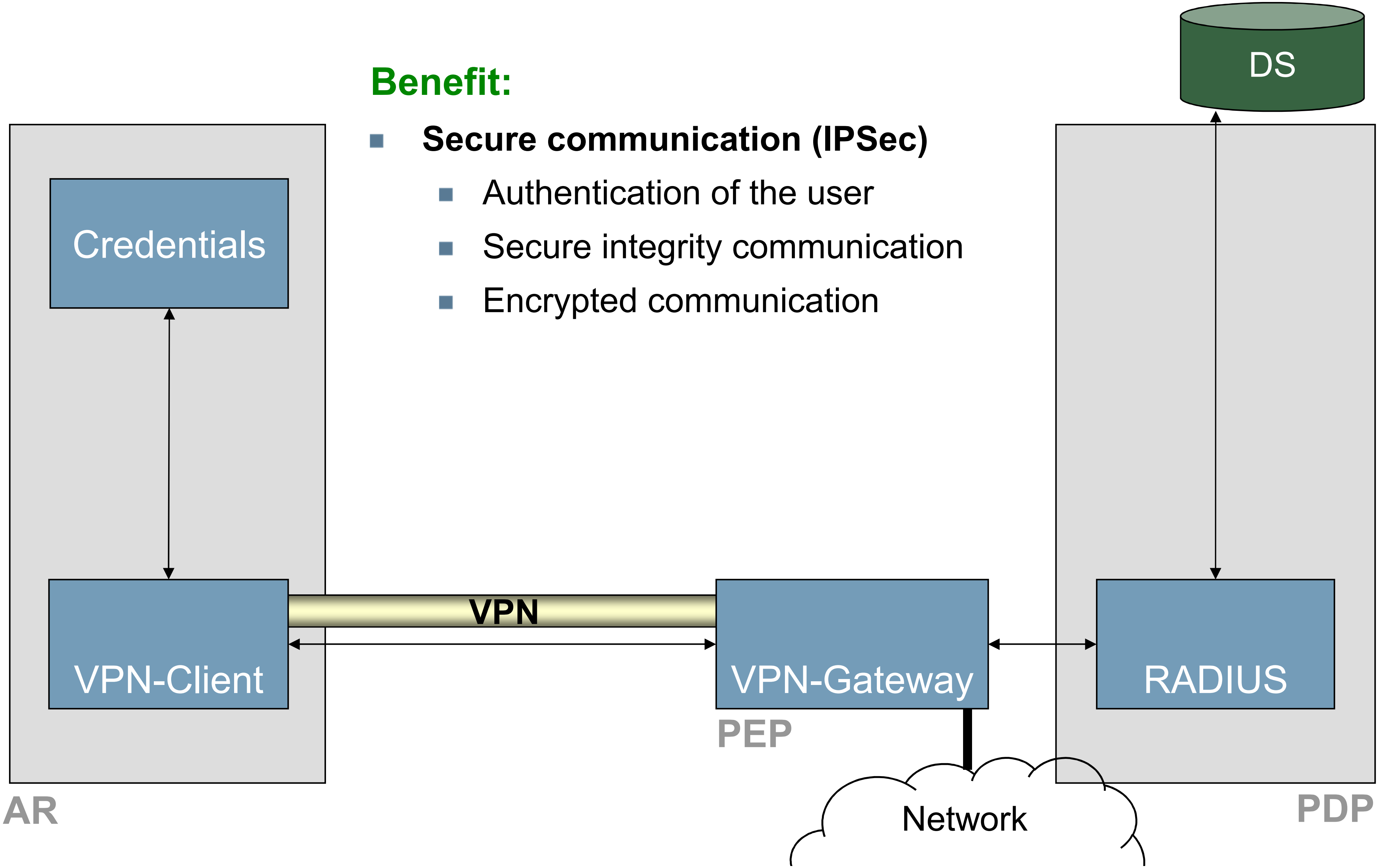
- The VPN Gateway allows or prohibits the set-up of a VPN-Connection via VPN-Client.
- The VPN Client is now able to establish the VPN and gets an encrypted secure access to the network.



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

Benefit:

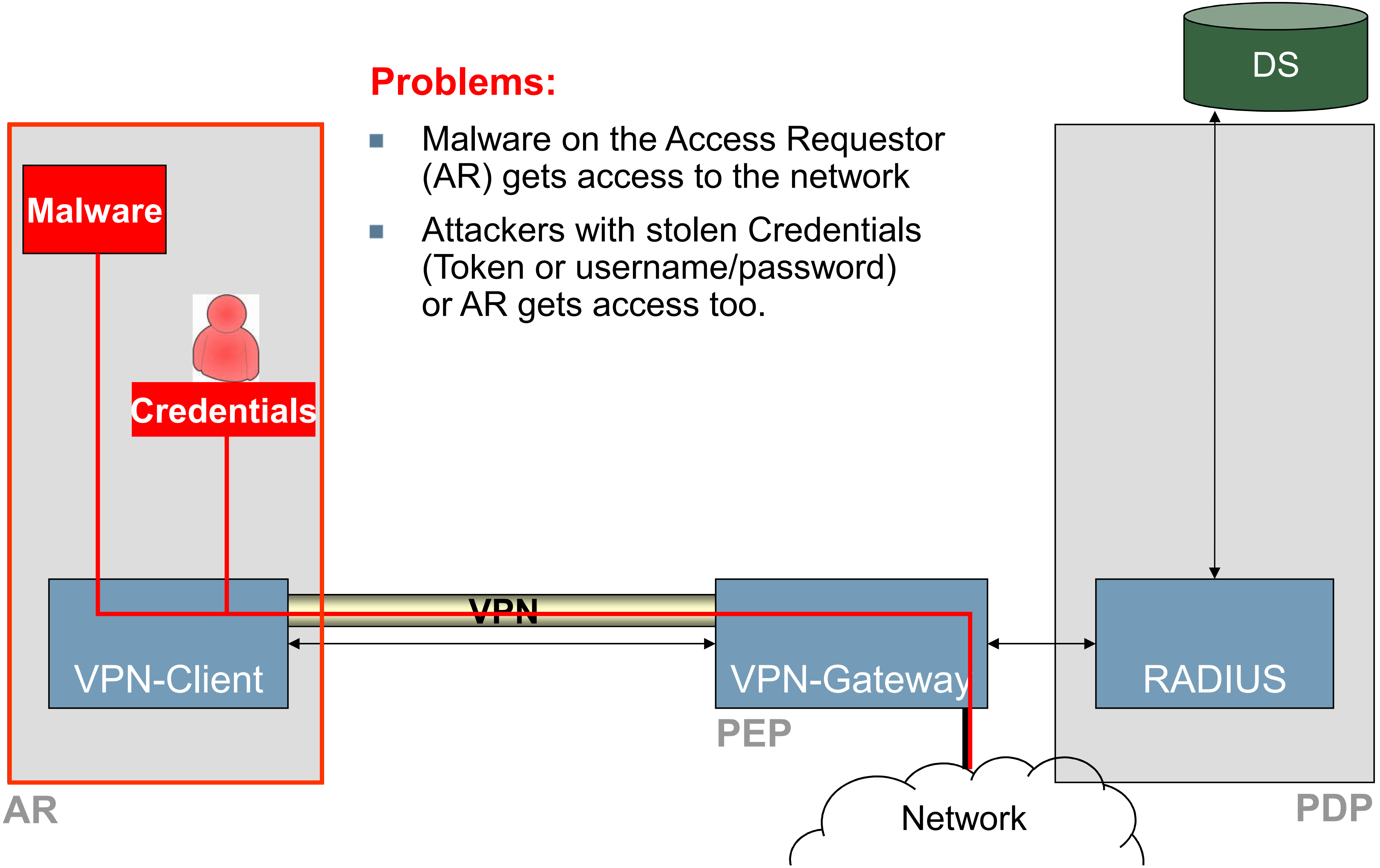
- **Secure communication (IPSec)**
  - Authentication of the user
  - Secure integrity communication
  - Encrypted communication



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

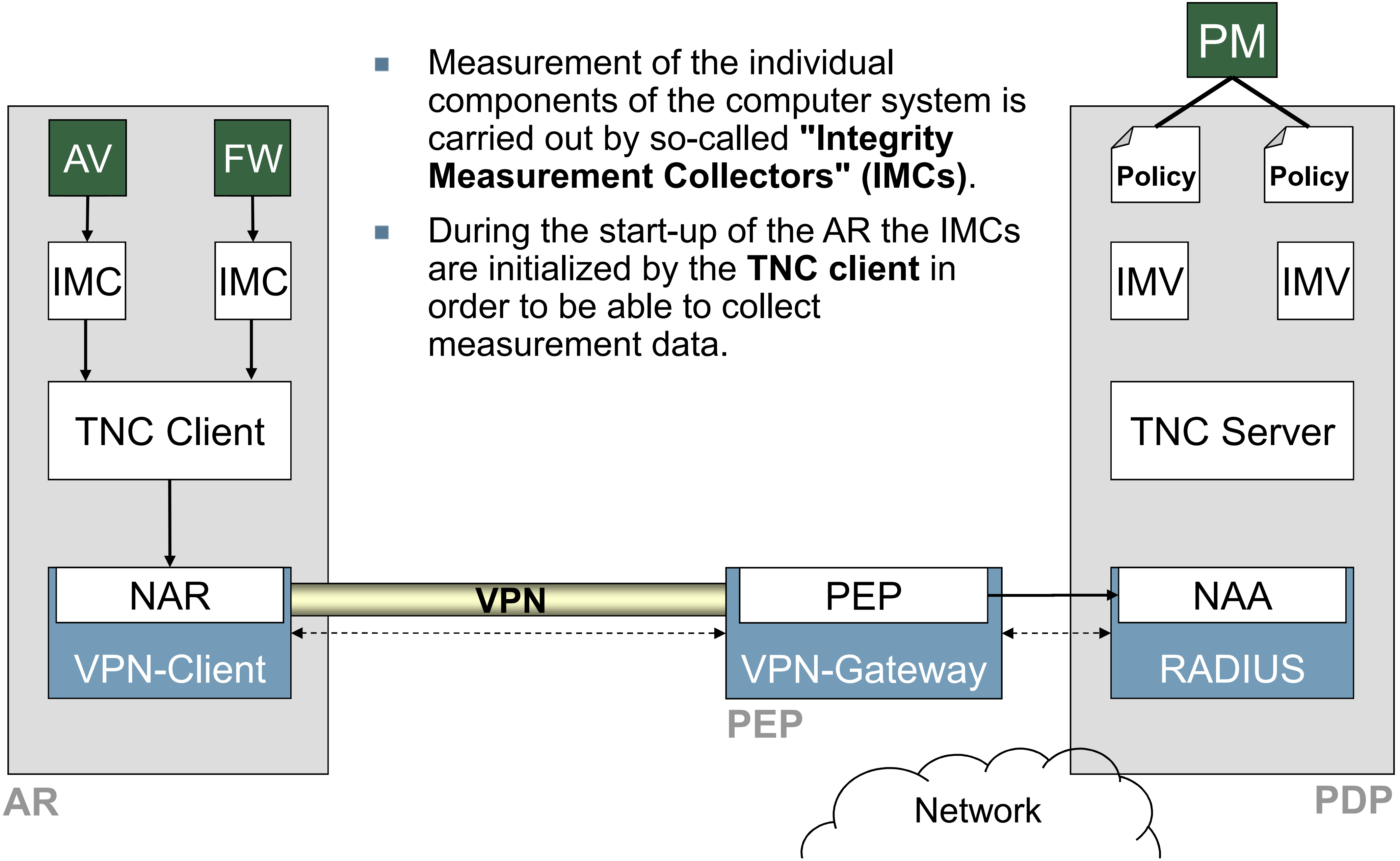
Problems:

- Malware on the Access Requestor (AR) gets access to the network
- Attackers with stolen Credentials (Token or username/password) or AR gets access too.



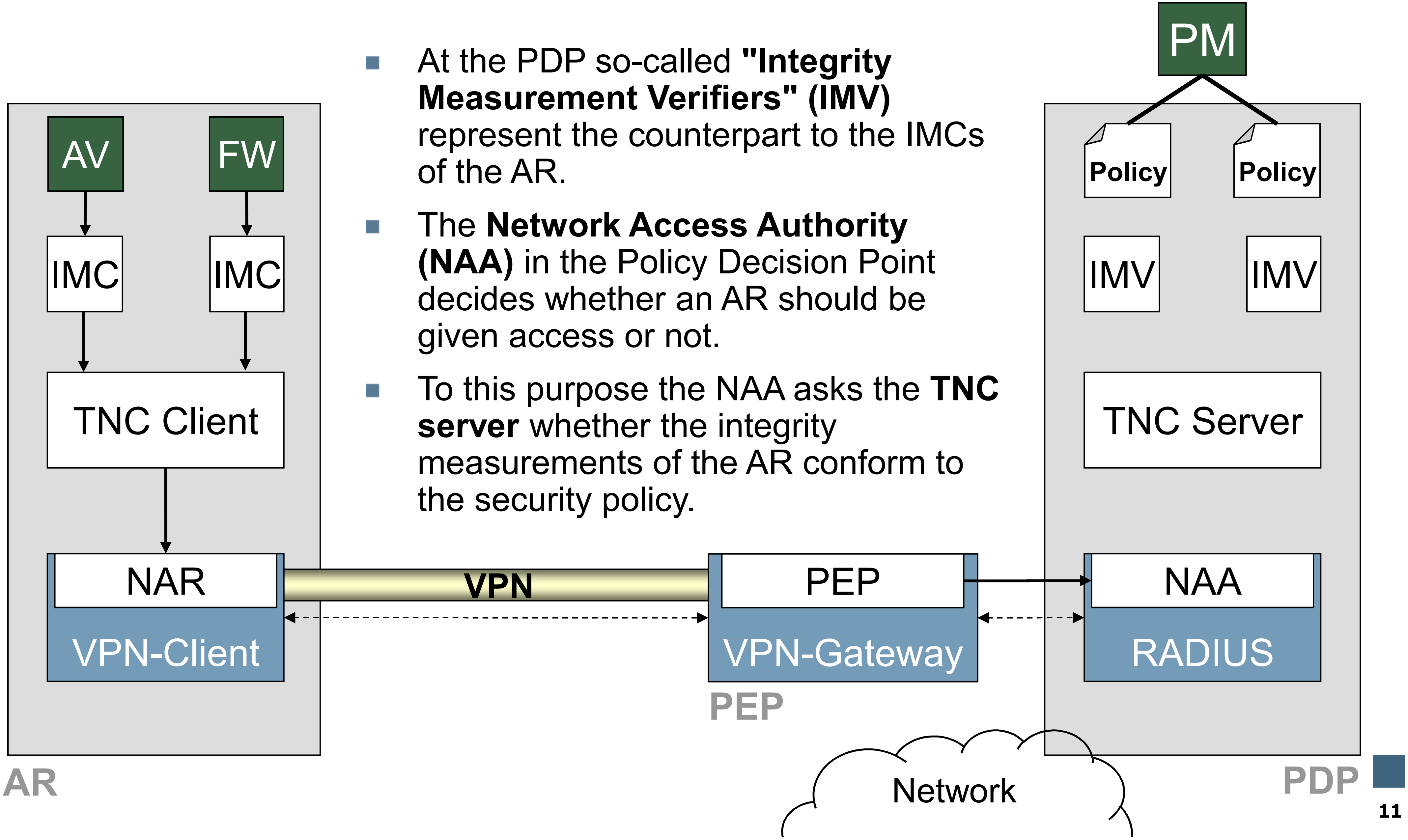
Trusted Network Connect (TNC)
→ Overview: TNC-functions (1/2)

- 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 AR the IMCs are initialized by the **TNC client** in order to be able to collect measurement data.



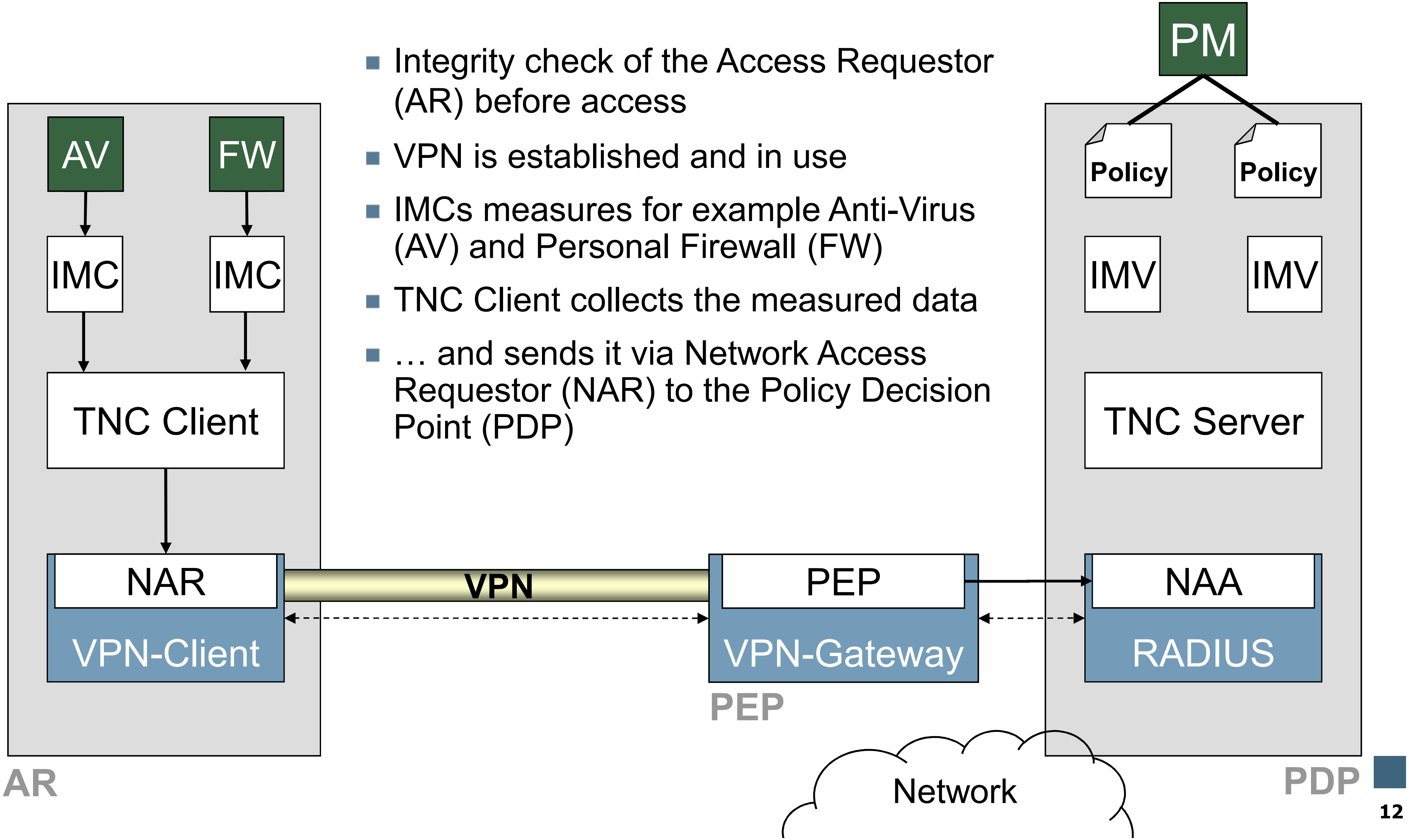
Trusted Network Connect (TNC)
→ Overview: TNC-functions (2/2)

- At the PDP 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 given access or not.
- To this purpose the NAA asks the **TNC server** whether the integrity measurements of the AR conform to the security policy.



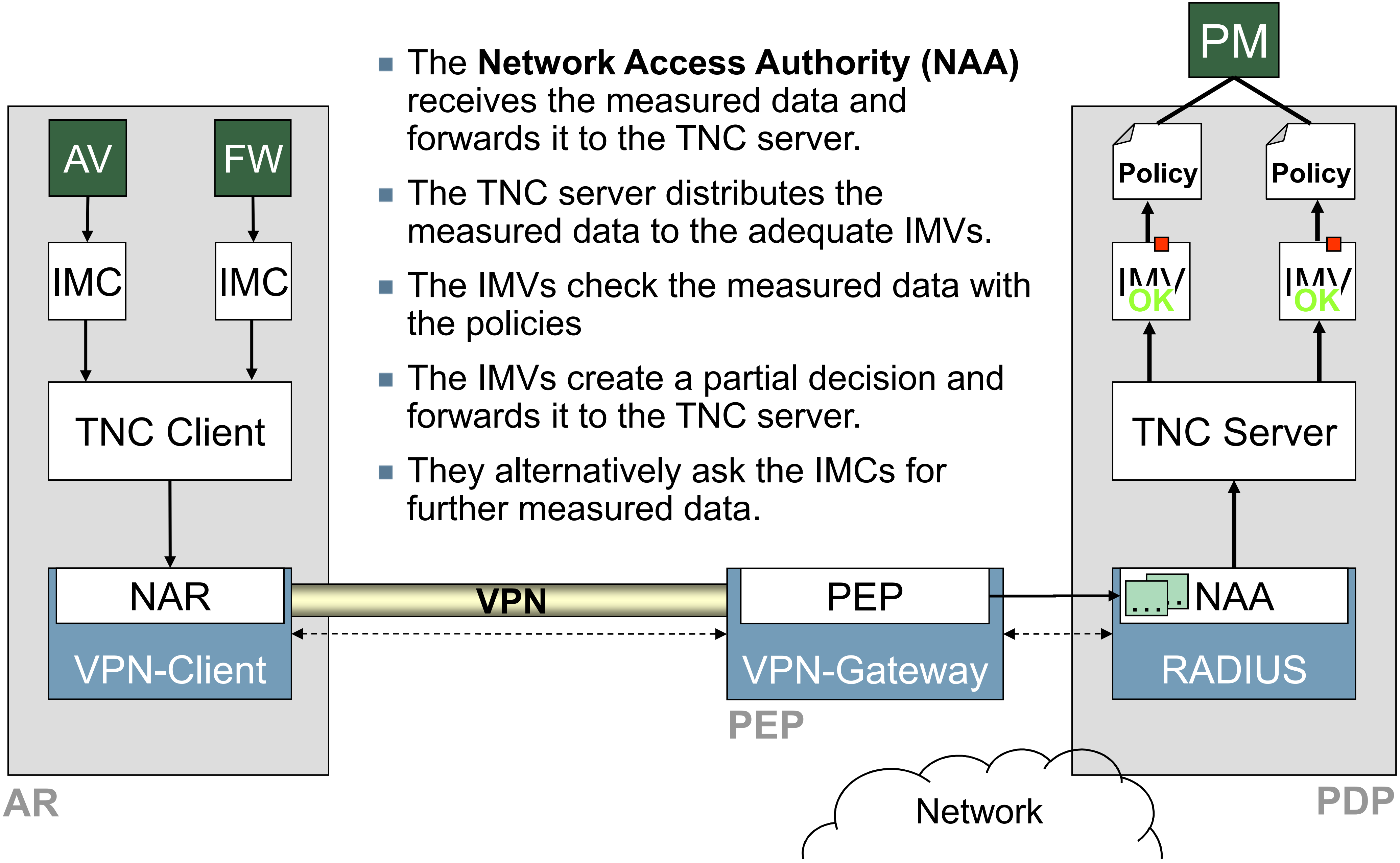
TNC – phases
→ Assessment phase (1/3)

- Integrity check of the Access Requestor (AR) before access
- VPN is established and in use
- IMCs measures for example Anti-Virus (AV) and Personal Firewall (FW)
- TNC Client collects the measured data
- … and sends it via Network Access Requestor (NAR) to the Policy Decision Point (PDP)



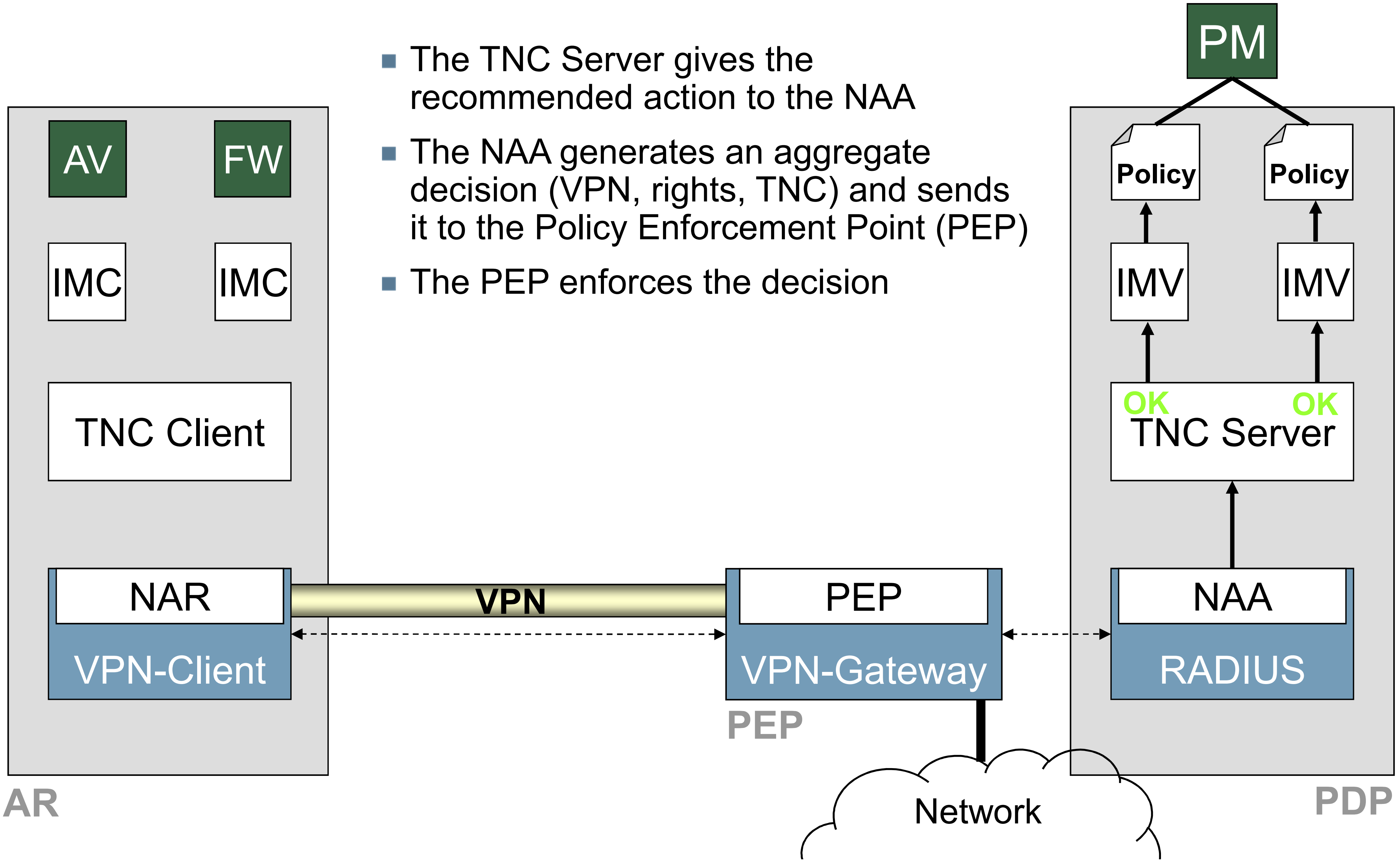
TNC – phases
→ Assessment phase (2/3)

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



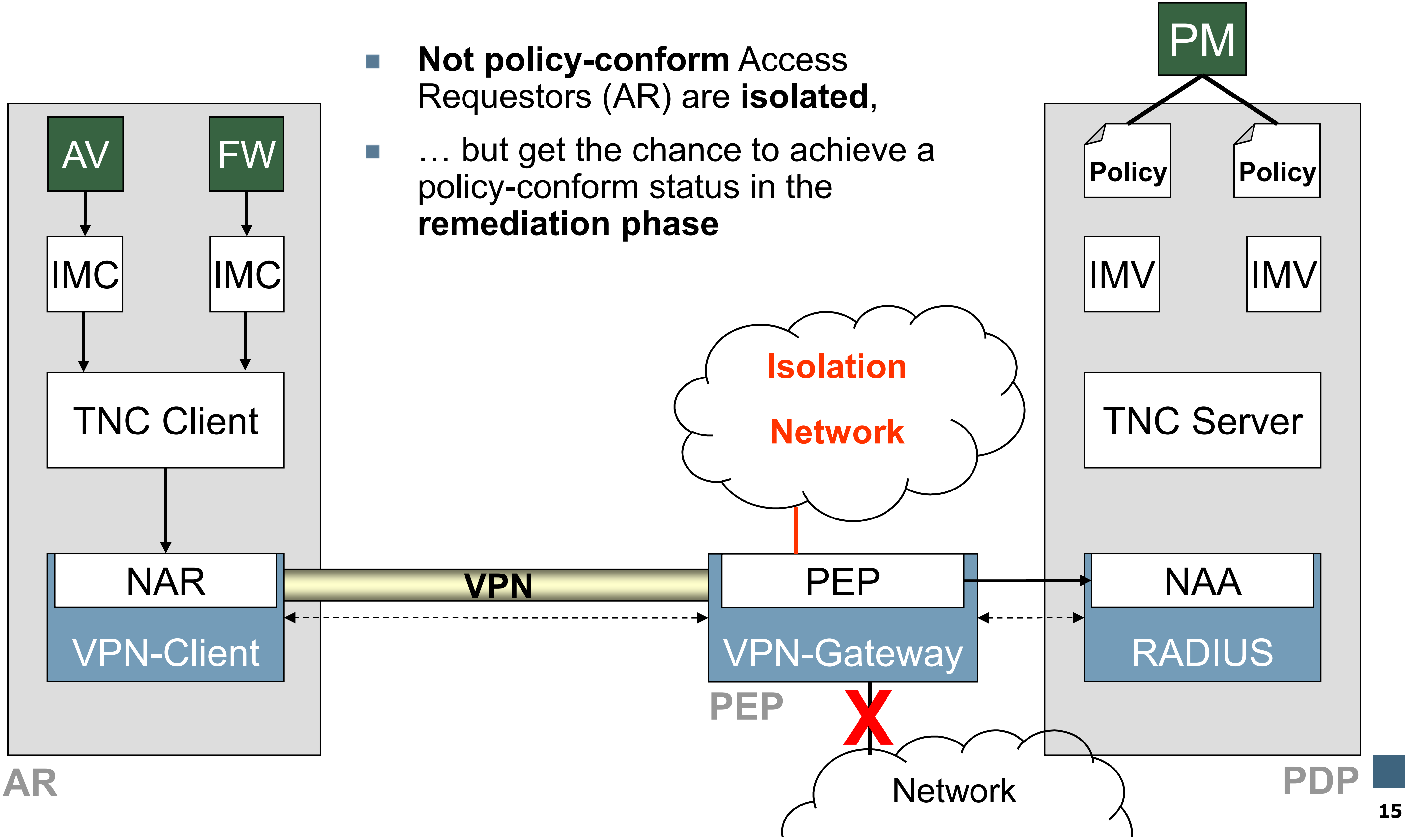
TNC – phases
→ Assessment phase (3/3)

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



TNC – phases
→ Isolation and remediation phase

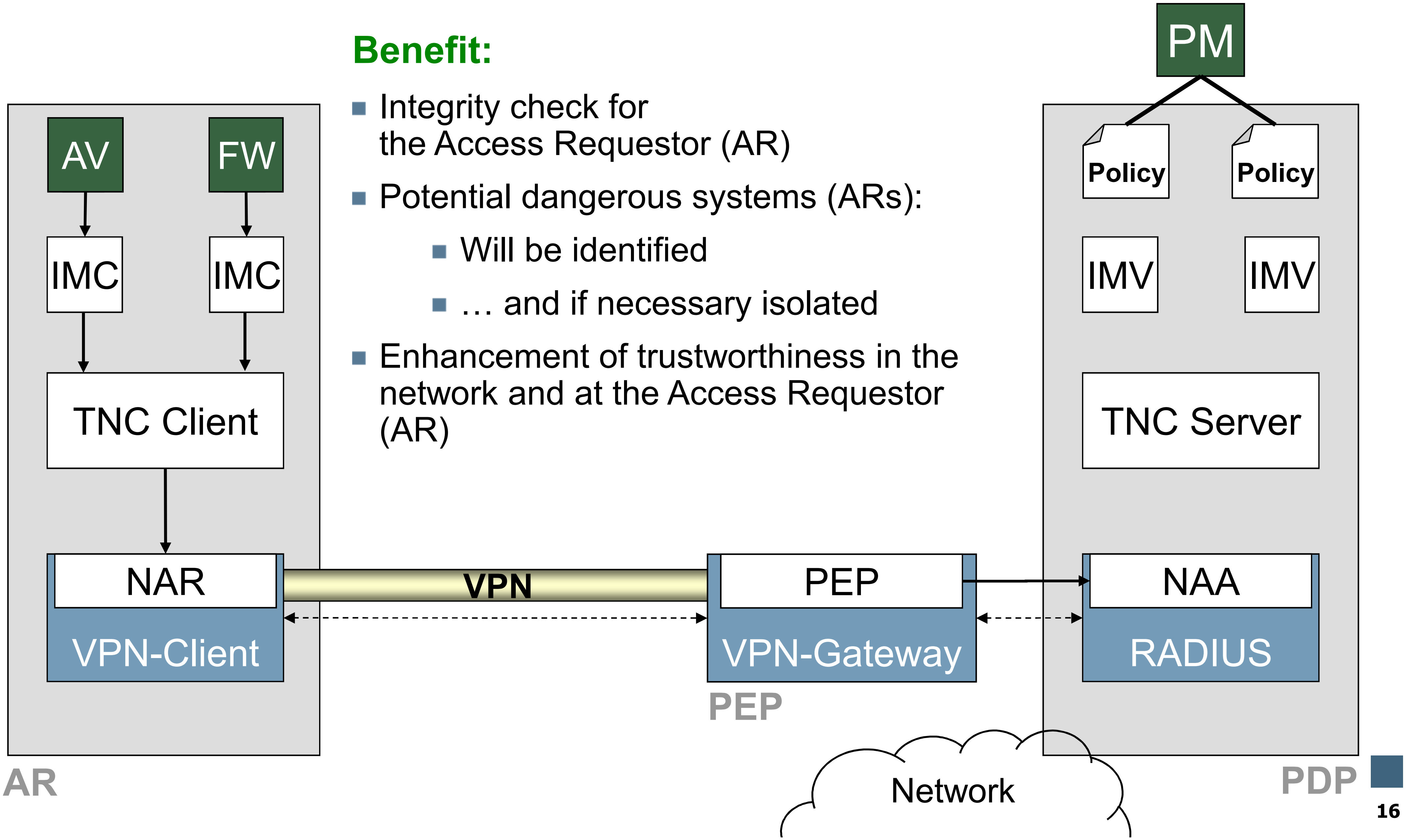
- **Not policy-conform** Access Requestors (AR) are **isolated**,
- … but get the chance to achieve a policy-conform status in the **remediation phase**



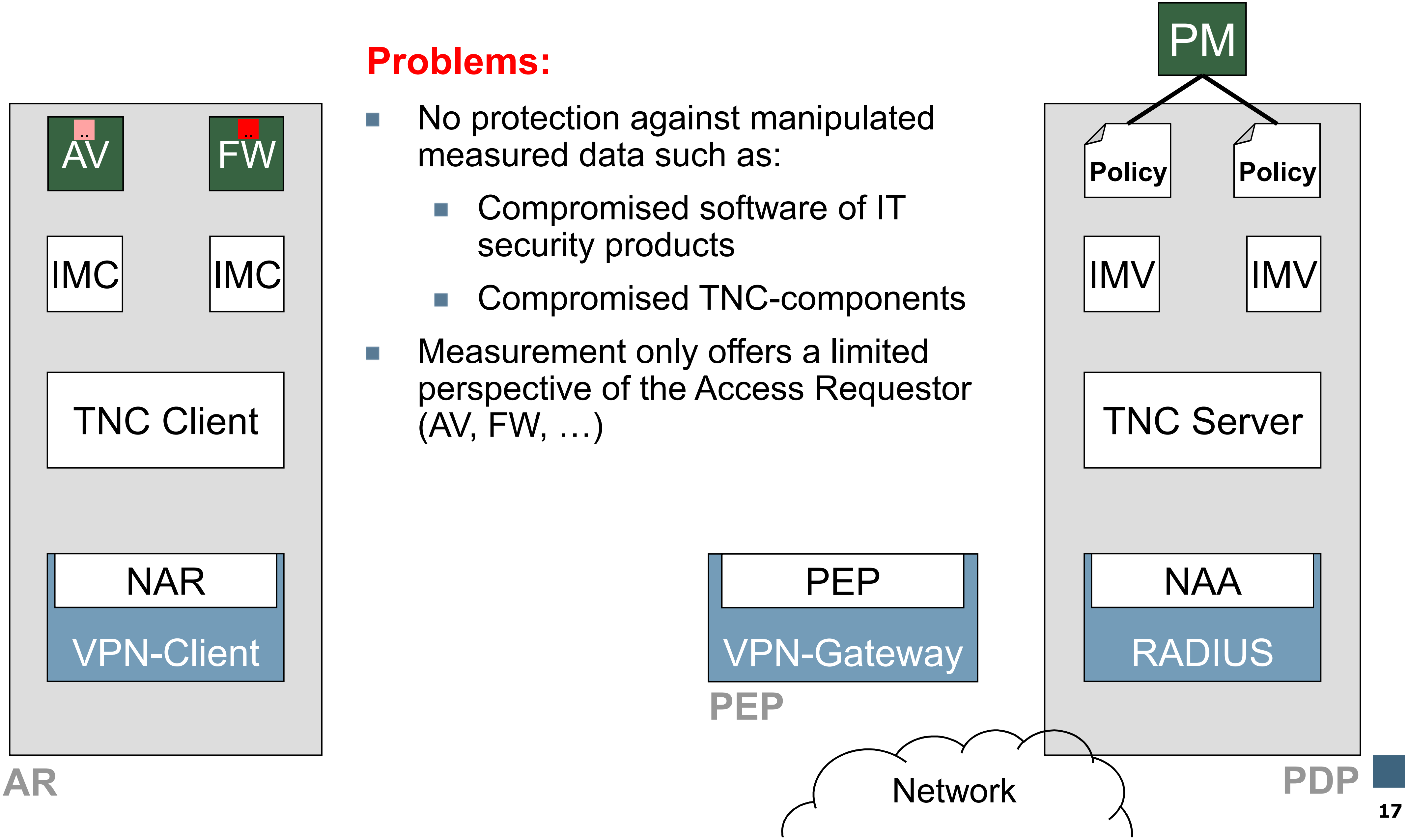
TNC
→ Trusted Network Connect

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)



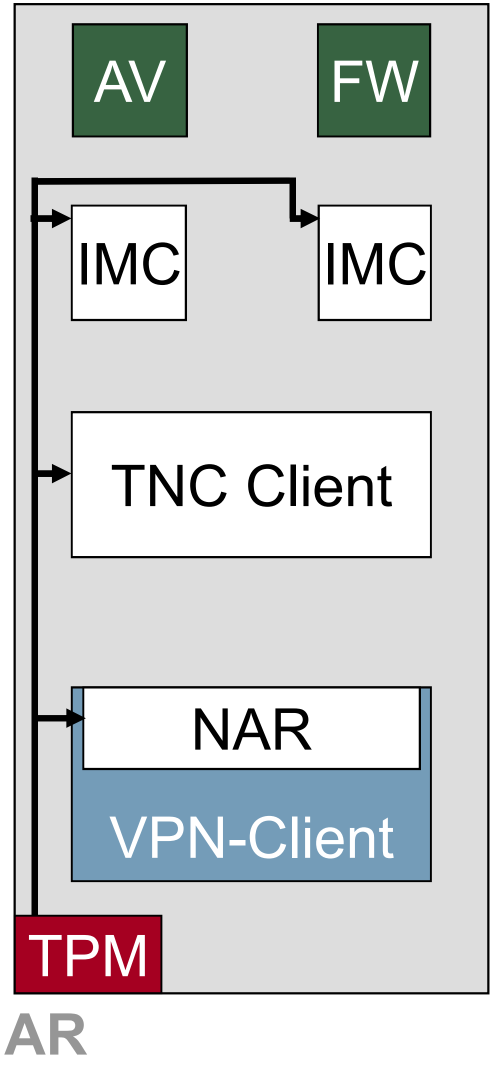
TNC
→ Open problems with TNC



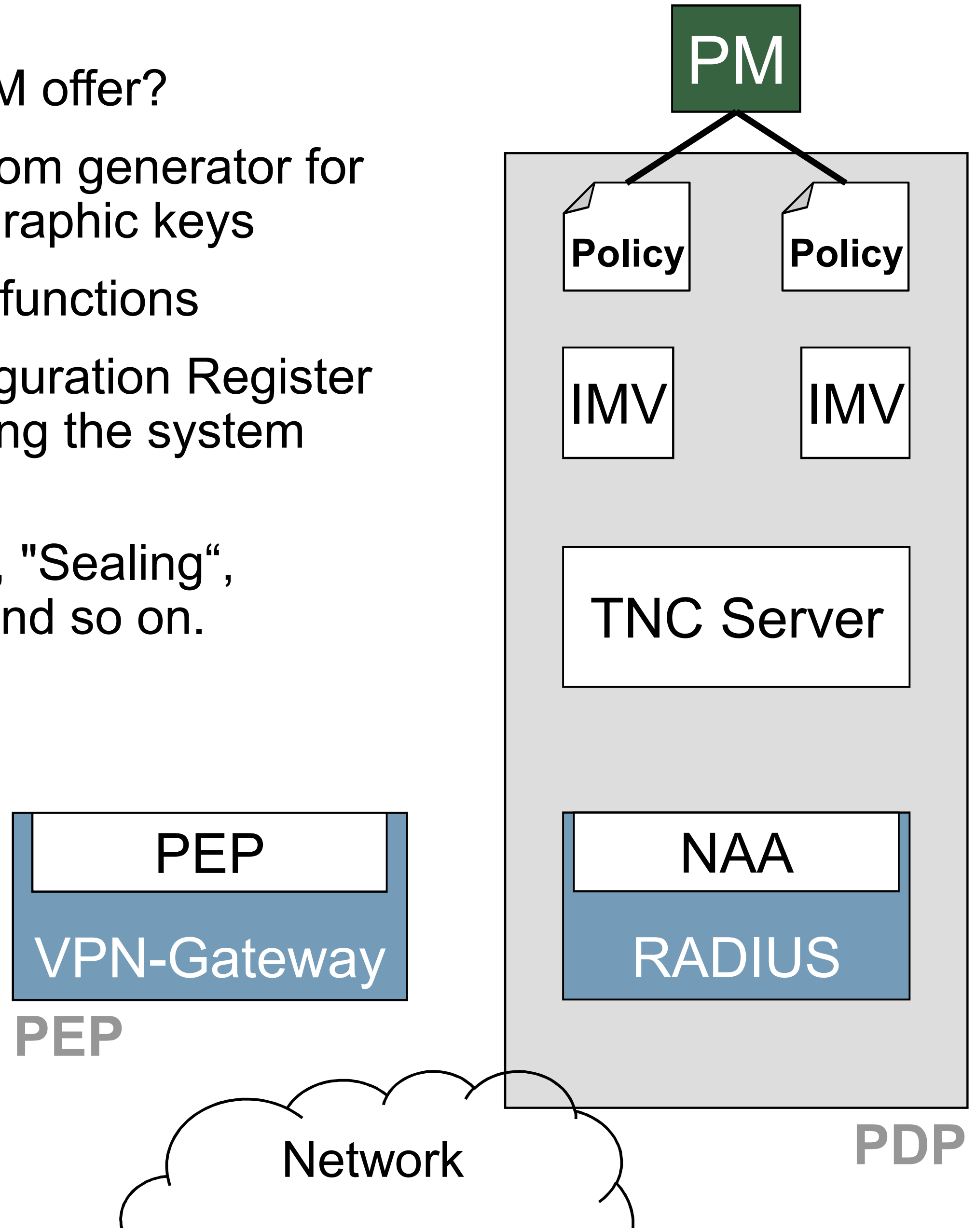
Problems:

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

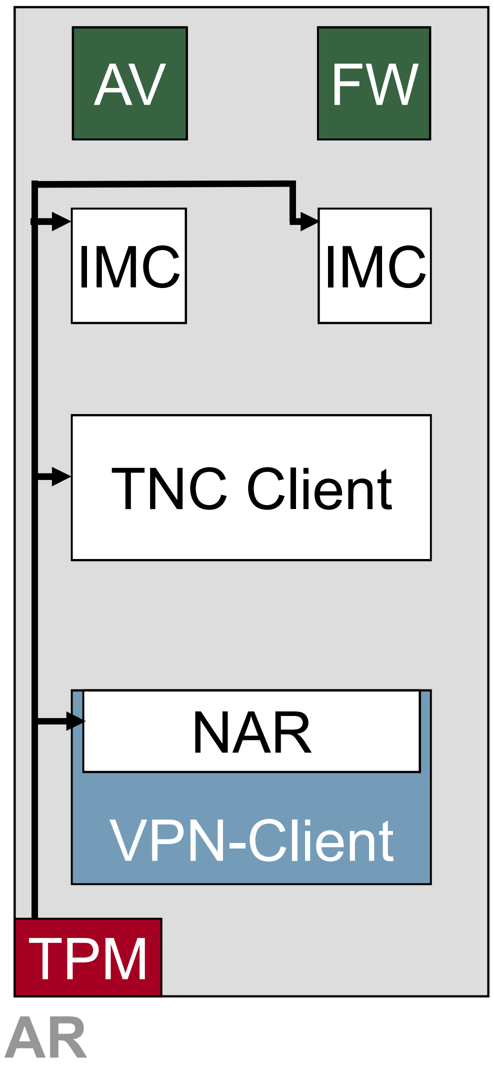
TNC+
→ TNC + TPM



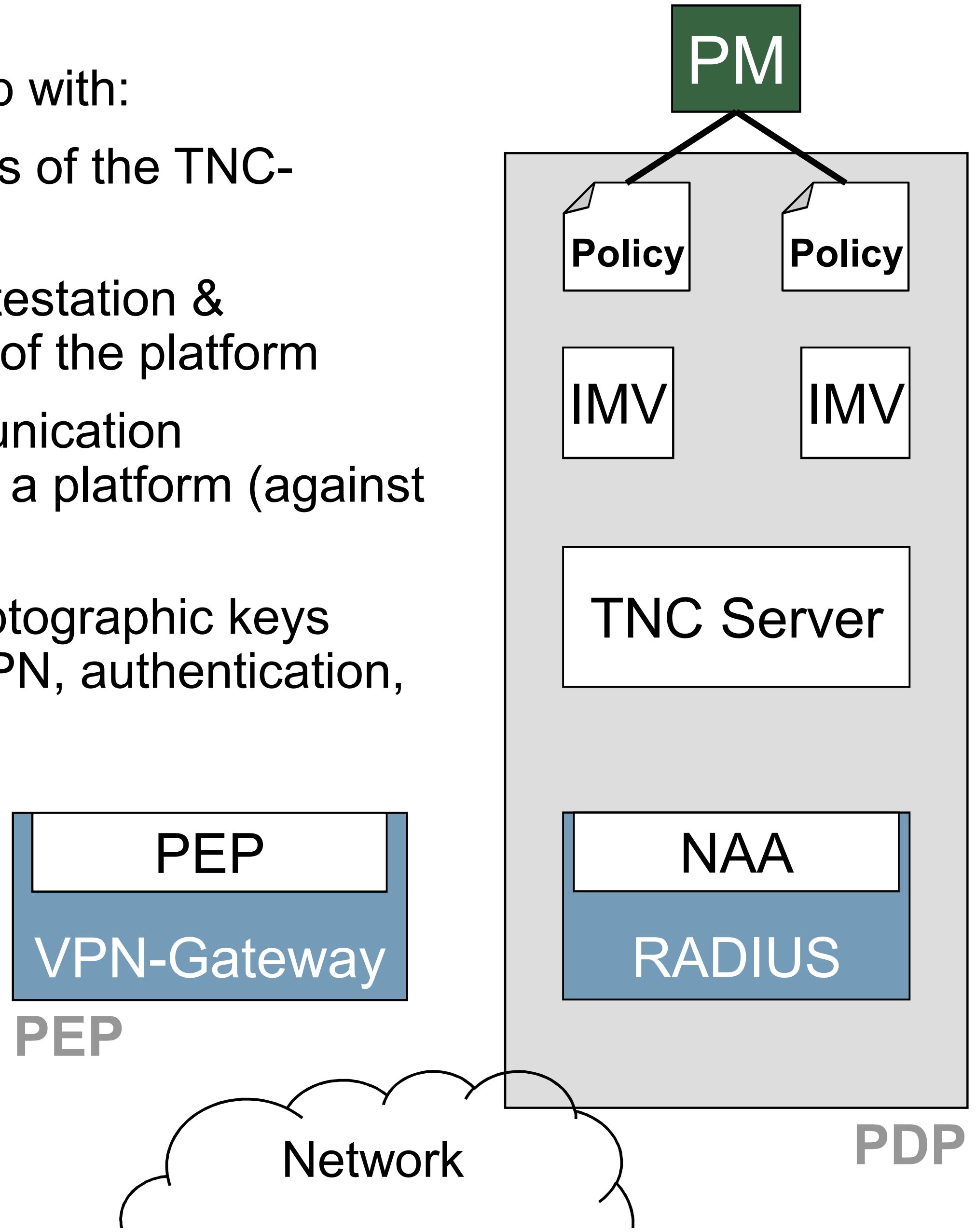
- What does the TPM offer?
  - A reliable random generator for secure cryptographic keys
  - Cryptographic functions
  - Platform Configuration Register (PCR) for storing the system configuration.
  - “Trusted Boot”, "Sealing“, "Attestation“, and so on.



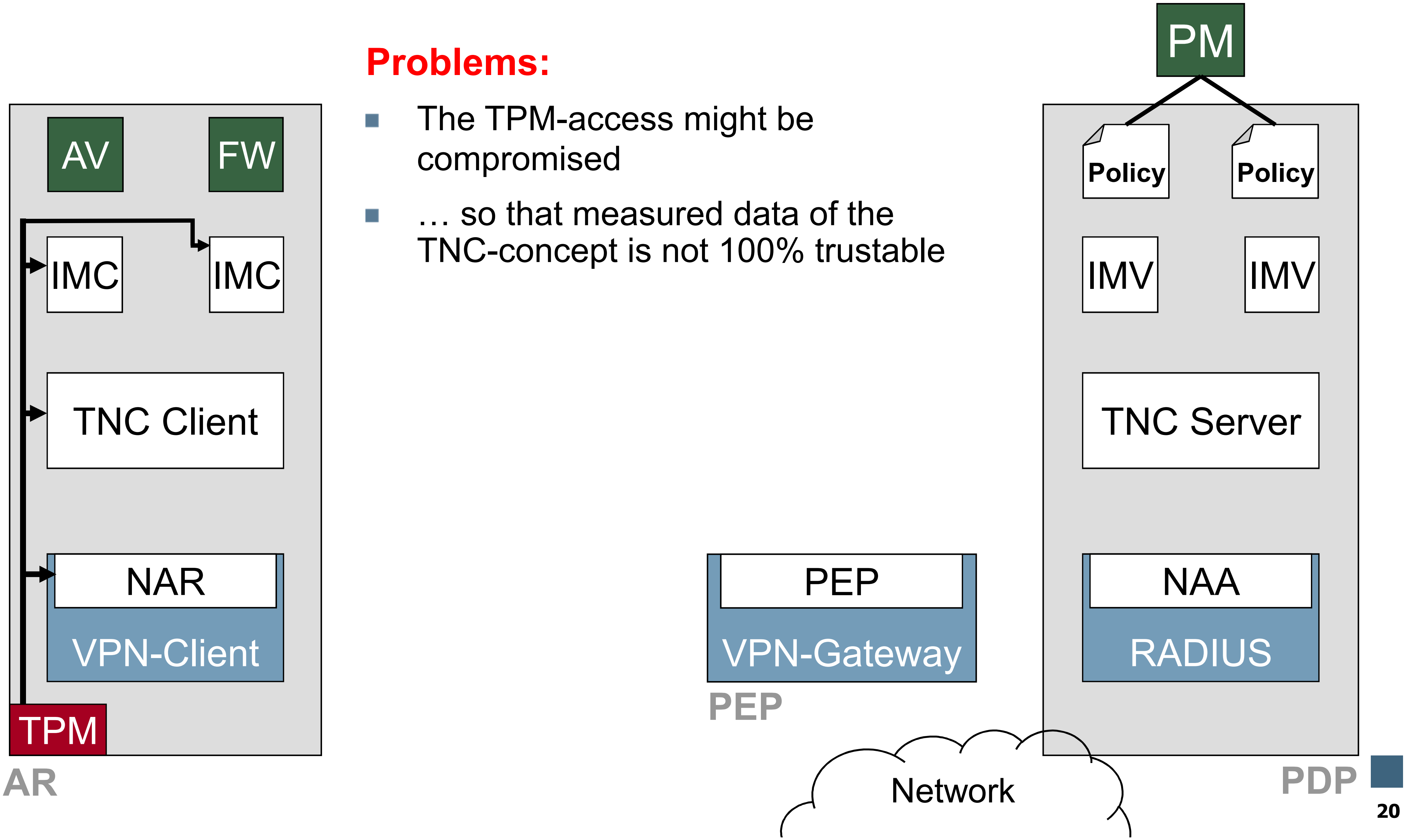
TNC+
→ Overvalue: TPM



- TPM functions help with:
  - Integrity checks of 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

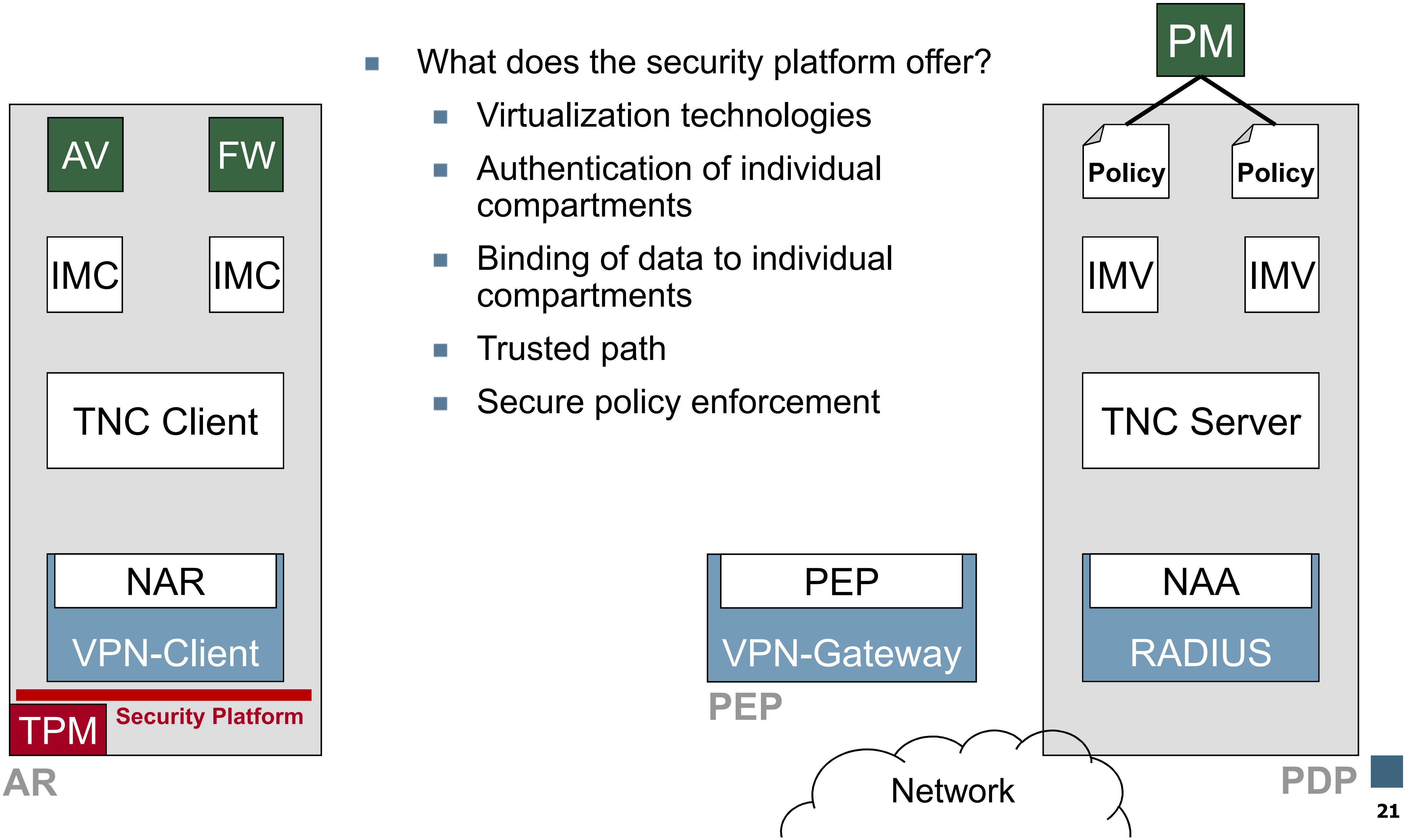


Problems:

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

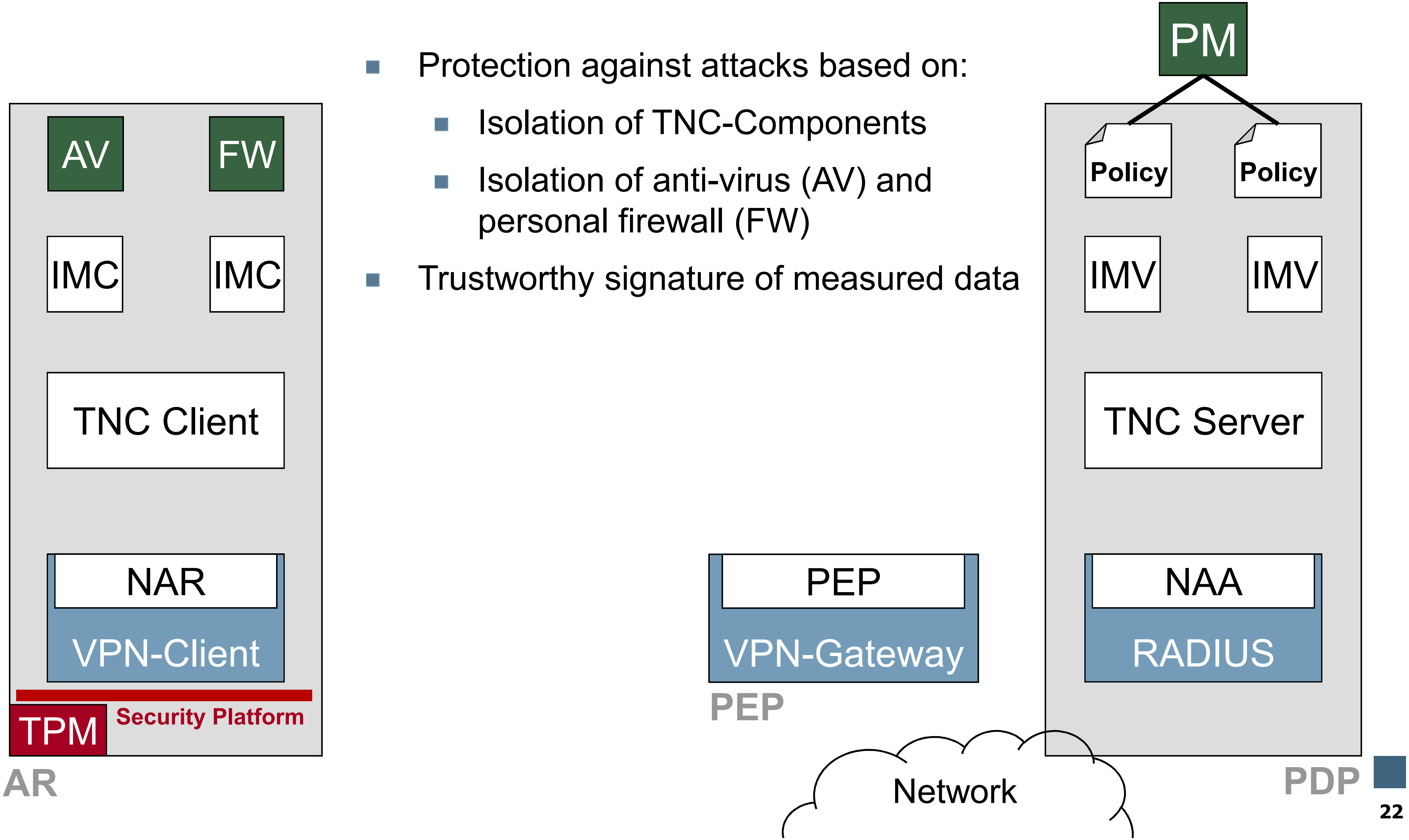
TNC++
→ TNC + TPM + security platform

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

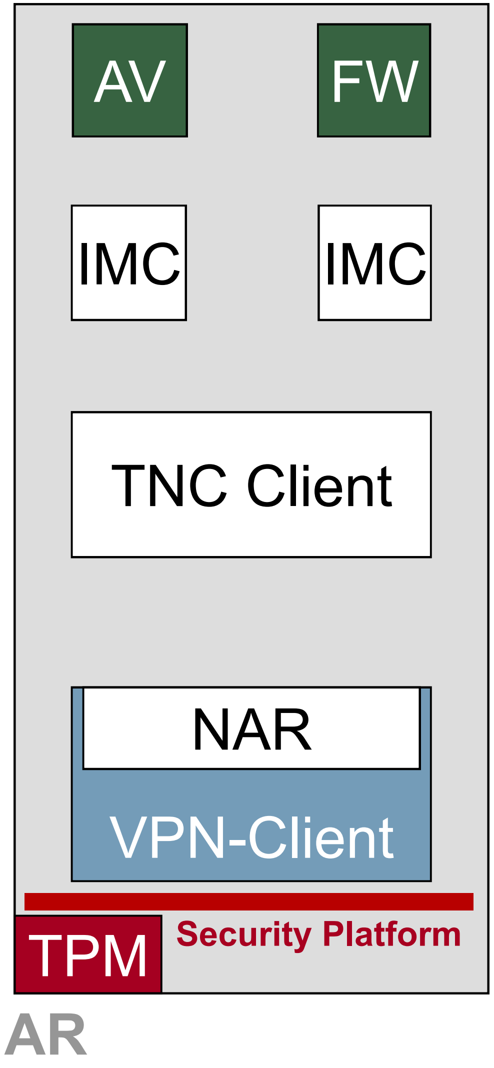


TNC++
→ Overvalue: security platform

- Protection against attacks based on:
  - Isolation of TNC-Components
  - Isolation of anti-virus (AV) and personal firewall (FW)
- Trustworthy signature of measured data

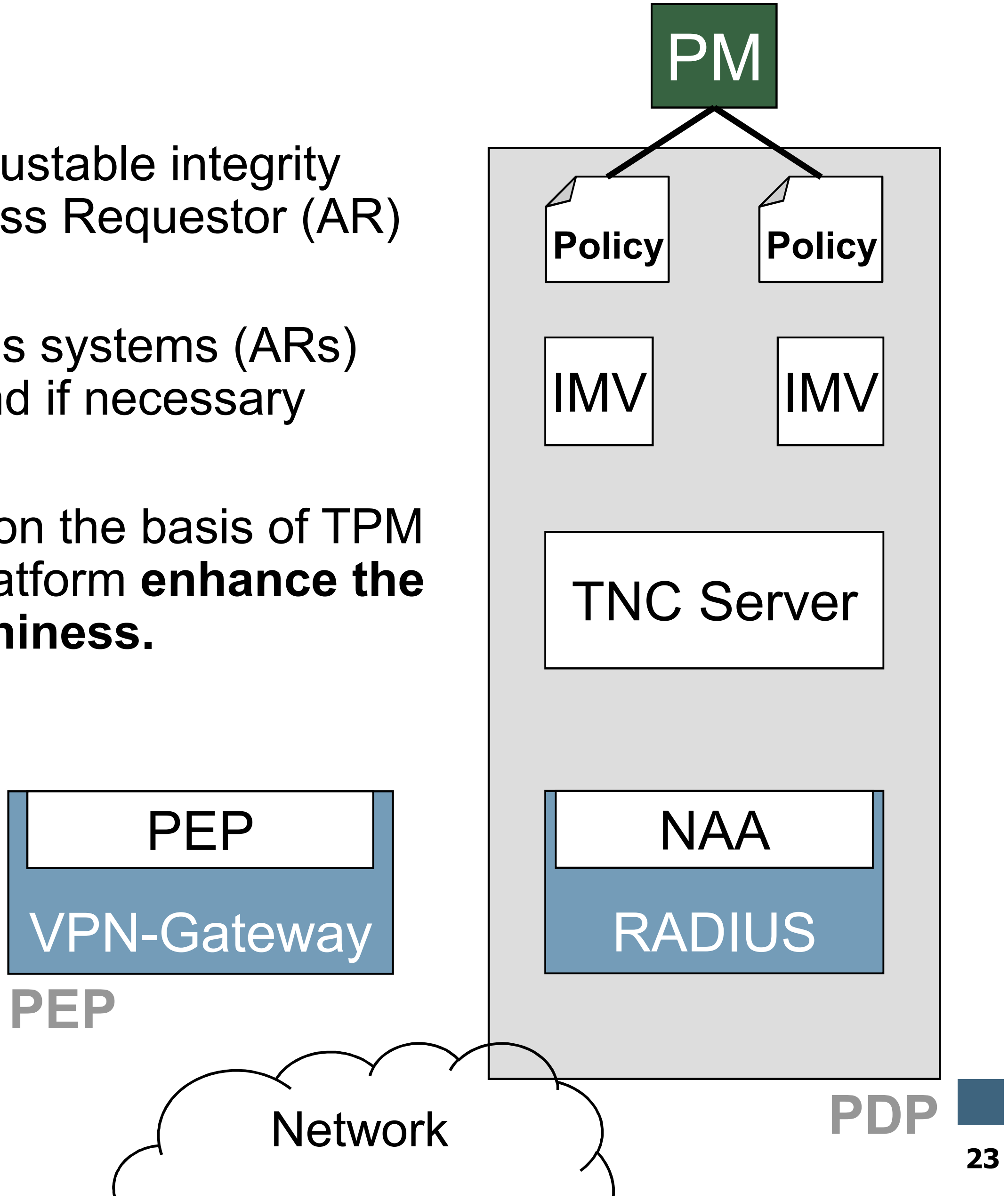


TNC++
→ Added value: security platform



Benefit:

- Very reliable and trustable integrity checks of the Access Requestor (AR) before access.
- Potential 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.**



Open questions (1/2)

- Who defines the policies?
- Who defines which configuration of systems and IT security products are 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?**

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

Integrity Check of Remote Computer Systems → 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.

Integrity Check of Remote Computer Systems → Trusted Network Connect

Thank you for your attention! Further questions?

Prof. Dr. Norbert Pohlmann

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