Fachhochschule Gelsenkirchen

Sichere Einbindung von mobilen Endgeräten mit Hilfe von TNC → Trusted Network Connect

Prof. Dr. Norbert Pohlmann

Institut für Internet-Sicherheit
Fachhochschule Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet-sicherheit.

Heutige Aufgabenstellungen

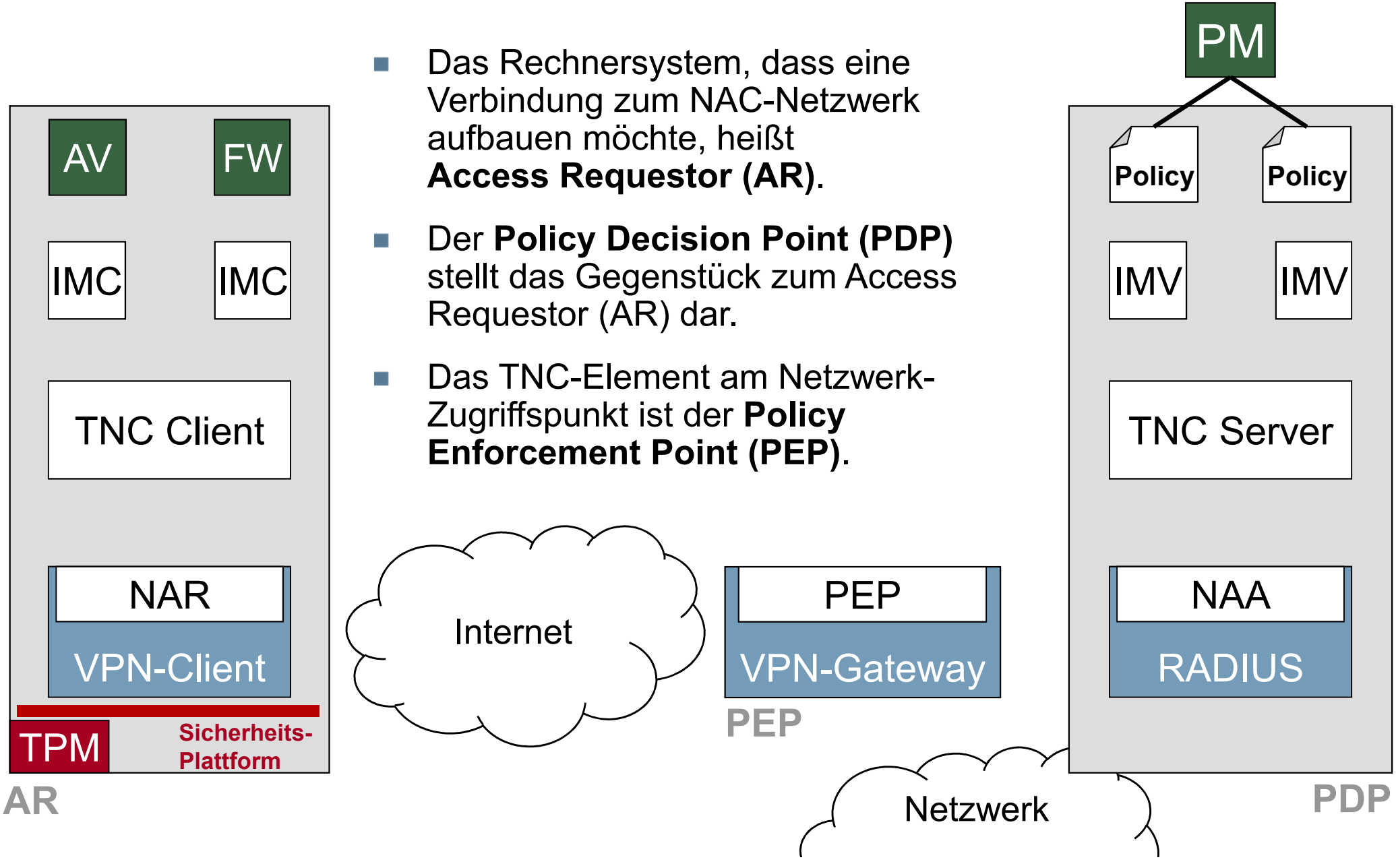
- **Außendienstmitarbeiter** nutzen ihre Rechnersysteme in vielen unterschiedlichen Umgebungen mit unterschiedlichen ***Sicherheitsanforderungen***.
- **Heimarbeiter** nutzen ihre PCs für ***private Zwecke***.
- **Mitarbeiter** nehmen ihre ***Notebooks*** mit ***nach Hause***.

- **Diese Rechnersysteme befinden sich außerhalb der Kontrolle der Firmen und können kompromittiert werden!**

- Deshalb wird ein Konzept benötigt, dass eine Integritäts-Prüfung entfernter Rechnersysteme erlaubt → **Network Access Control**!

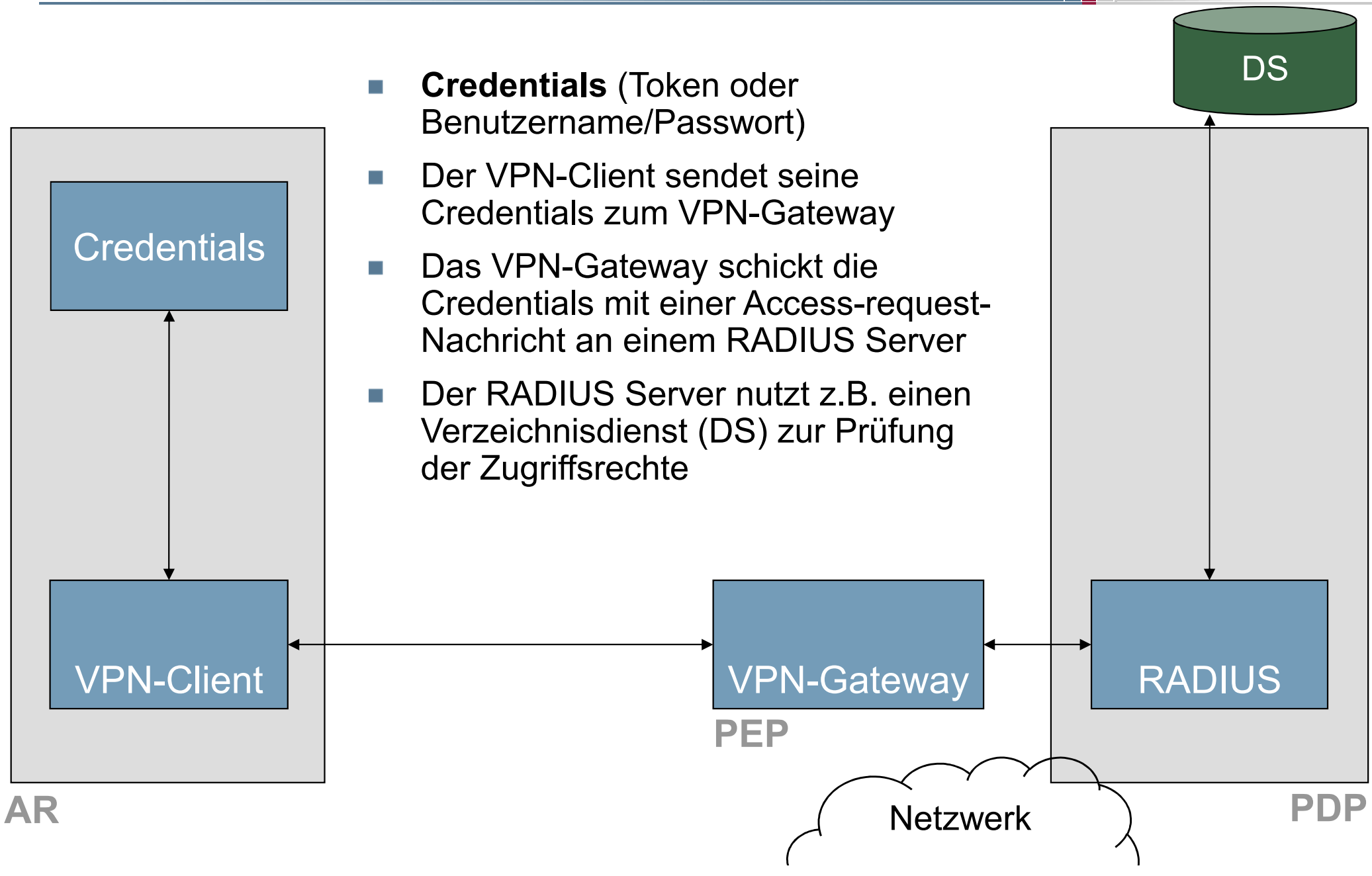
Übersicht
→ Trusted Network Connect (TNC)

- Das Rechnersystem, dass eine Verbindung zum NAC-Netzwerk aufbauen möchte, heißt **Access Requestor (AR)**.
- Der **Policy Decision Point (PDP)** stellt das Gegenstück zum Access Requestor (AR) dar.
- Das TNC-Element am Netzwerk-Zugriffspunkt ist der **Policy Enforcement Point (PEP)**.



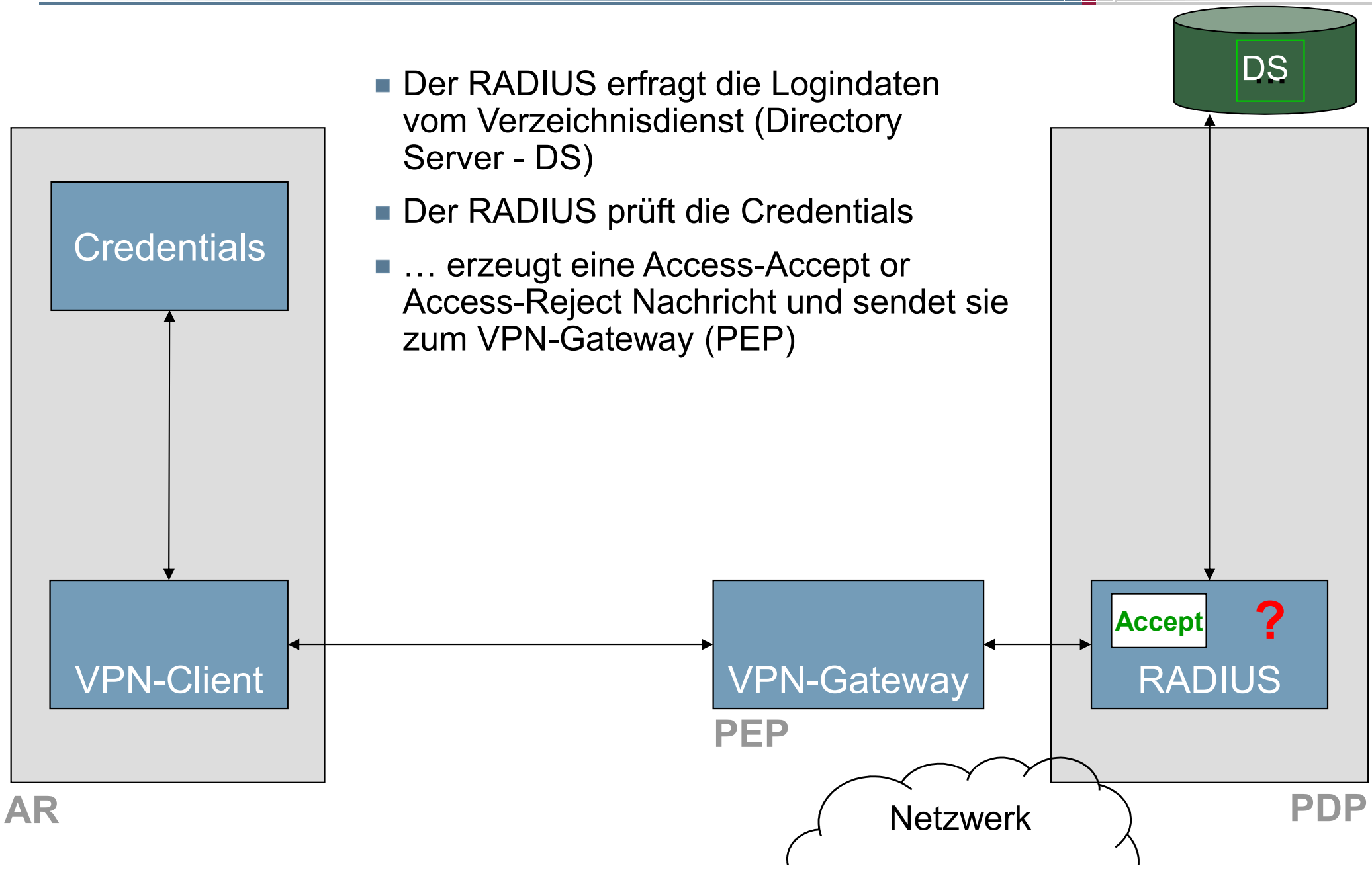
VPN-Kommunikation (1/6)
→ Authentifizierung/Autorisation (1/3)

- **Credentials** (Token oder Benutzername/Passwort)
- Der VPN-Client sendet seine Credentials zum VPN-Gateway
- Das VPN-Gateway schickt die Credentials mit einer Access-request-Nachricht an einem RADIUS Server
- Der RADIUS Server nutzt z.B. einen Verzeichnisdienst (DS) zur Prüfung der Zugriffsrechte



VPN-Kommunikation (2/6)
→ Authentifizierung/Autorisation (2/3)

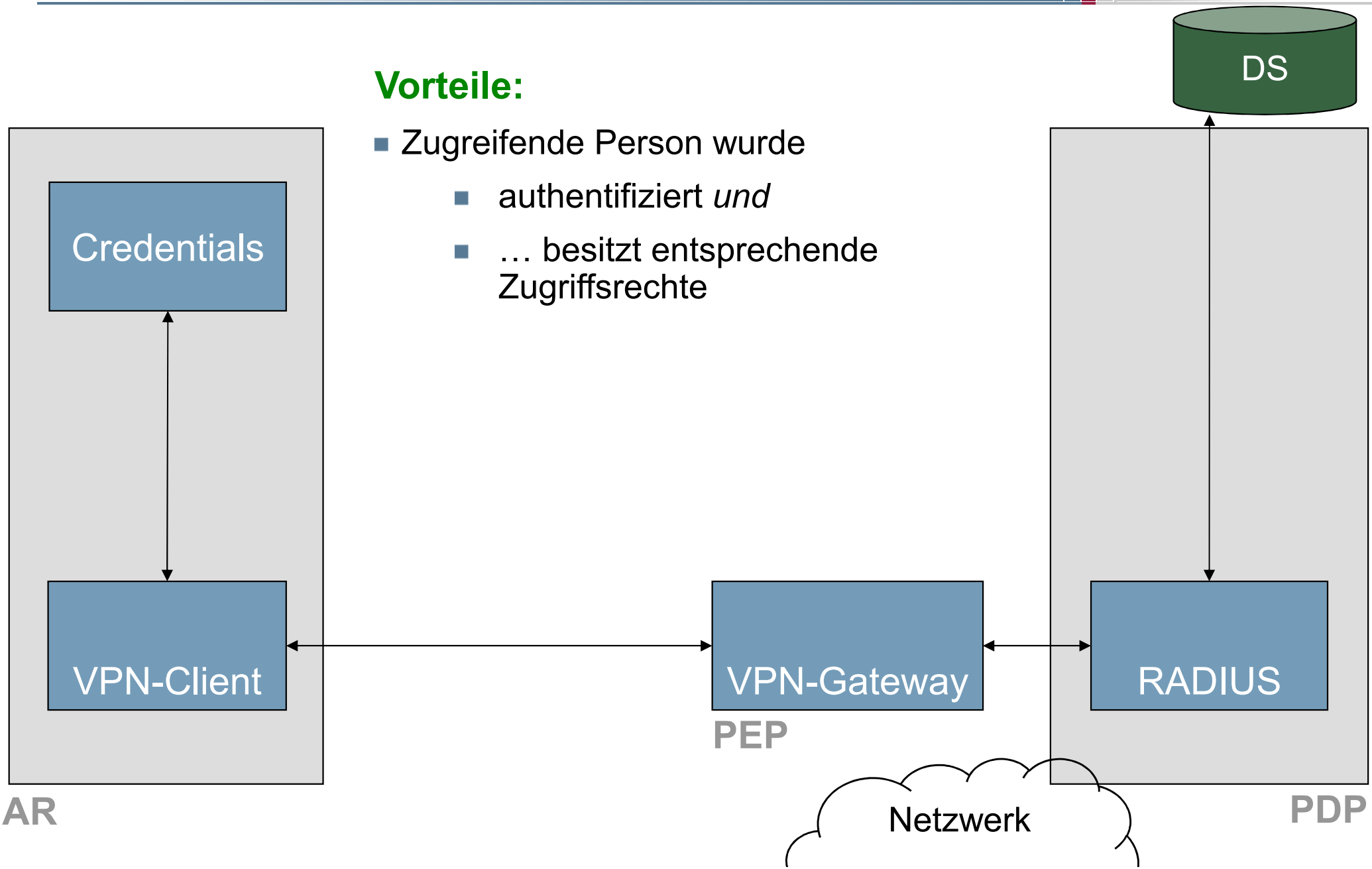
- Der RADIUS erfragt die Logindaten vom Verzeichnisdienst (Directory Server - DS)
- Der RADIUS prüft die Credentials
- … erzeugt eine Access-Accept or Access-Reject Nachricht und sendet sie zum VPN-Gateway (PEP)



VPN-Kommunikation (3/6)
→ Authentifizierung/Autorisation (3/3)

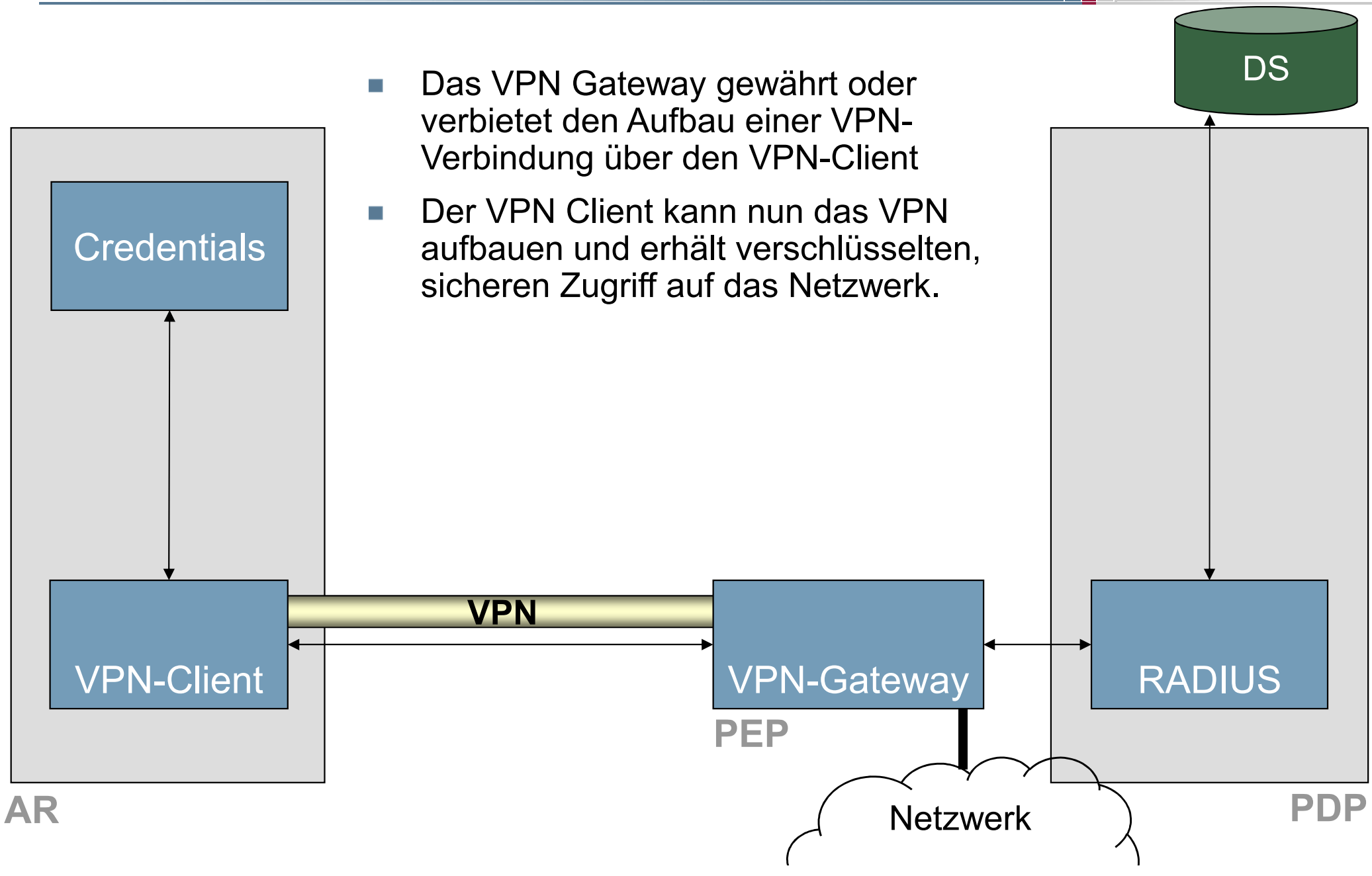
Vorteile:

- Zugreifende Person wurde
  - authentifiziert *und*
  - … besitzt entsprechende Zugriffsrechte



VPN-Kommunikation (4/6)
→Encrypted communication

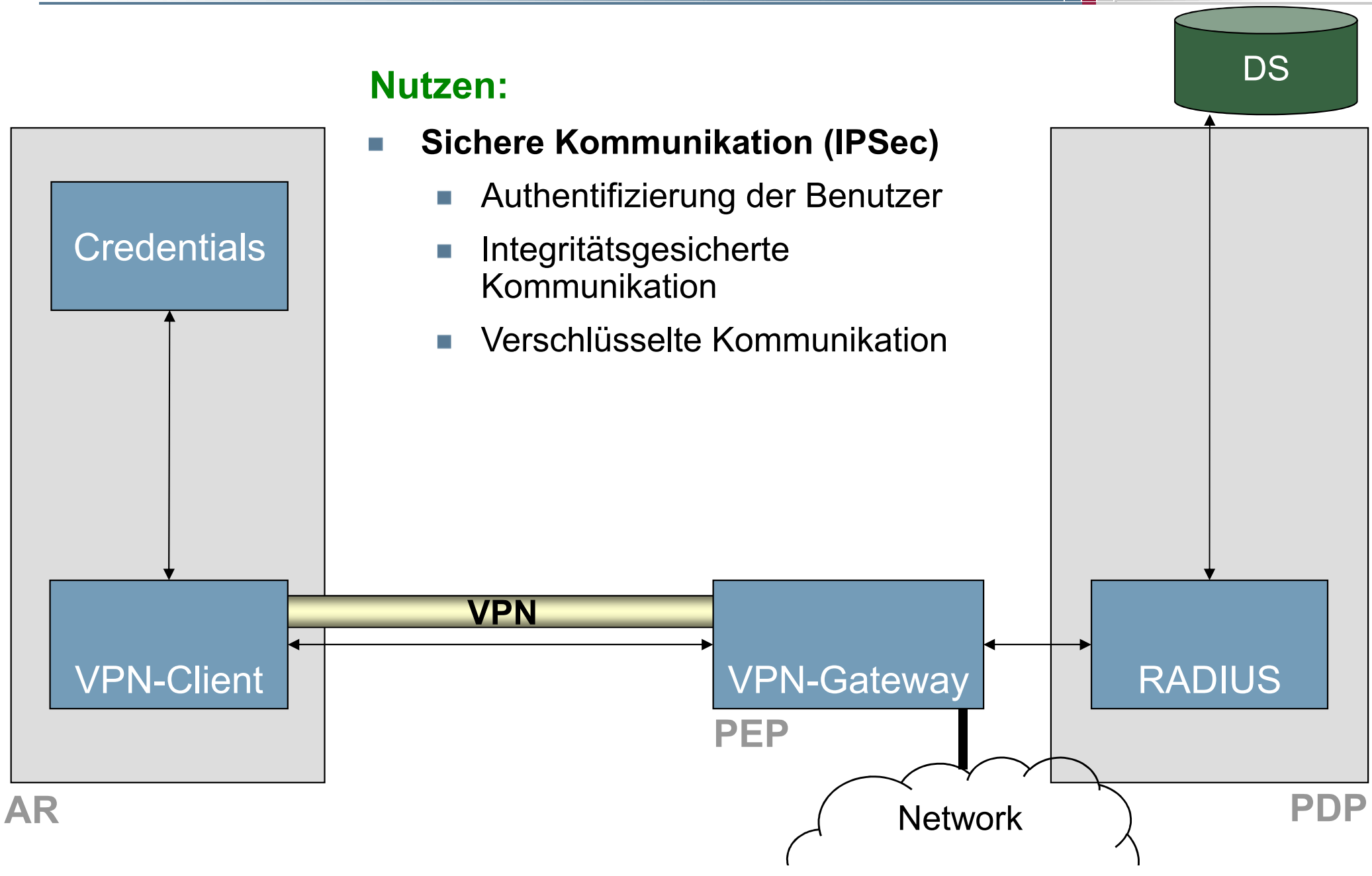
- Das VPN Gateway gewährt oder verbietet den Aufbau einer VPN-Verbindung über den VPN-Client
- Der VPN Client kann nun das VPN aufbauen und erhält verschlüsselten, sicheren Zugriff auf das Netzwerk.



VPN-Kommunikation (5/6)
→ Secure communication (IPSec)

Nutzen:

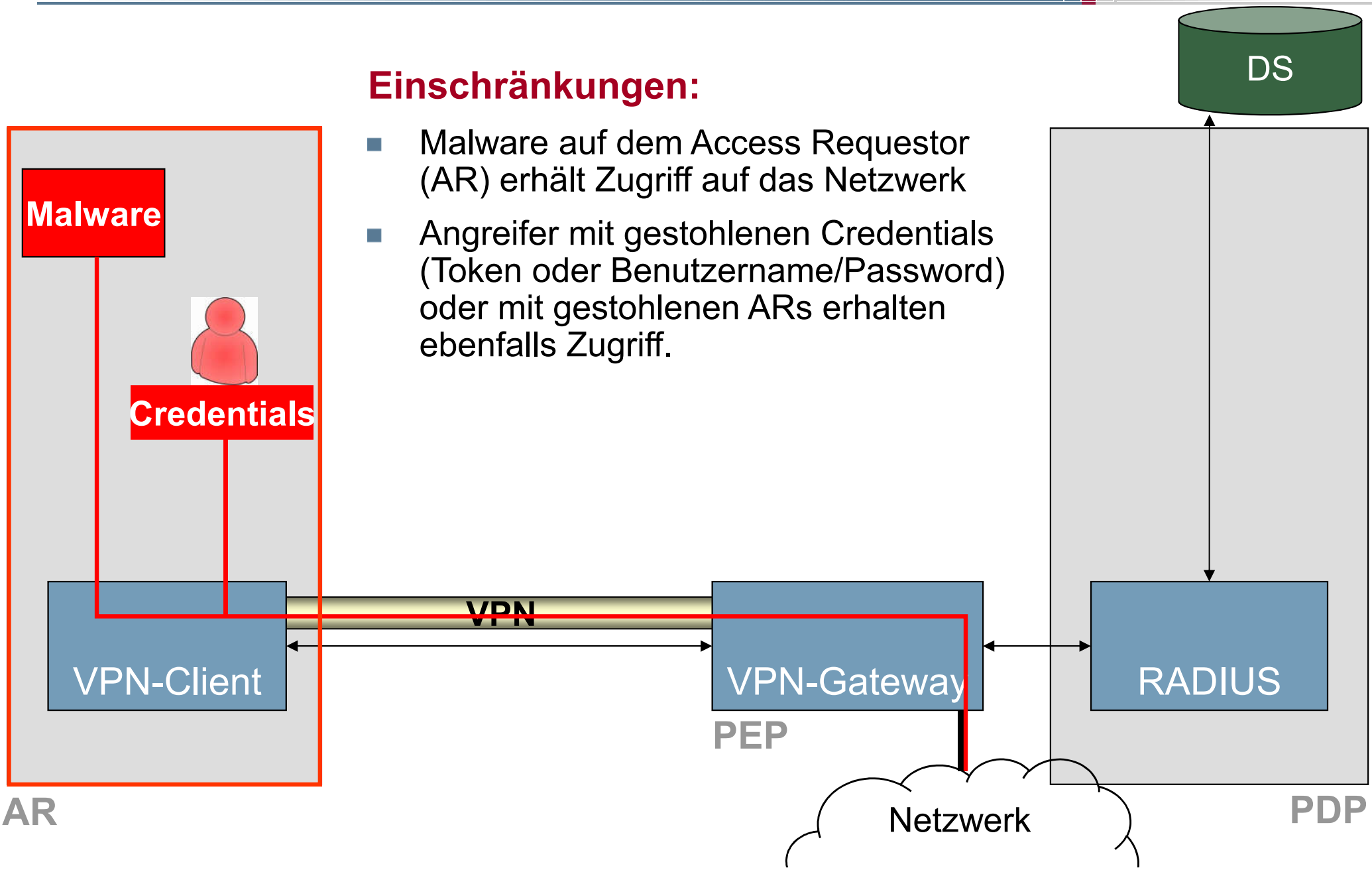
- **Sichere Kommunikation (IPSec)**
  - Authentifizierung der Benutzer
  - Integritätsgesicherte Kommunikation
  - Verschlüsselte Kommunikation



VPN-Kommunikation (6/6)
→ Offende Probleme von VPNs

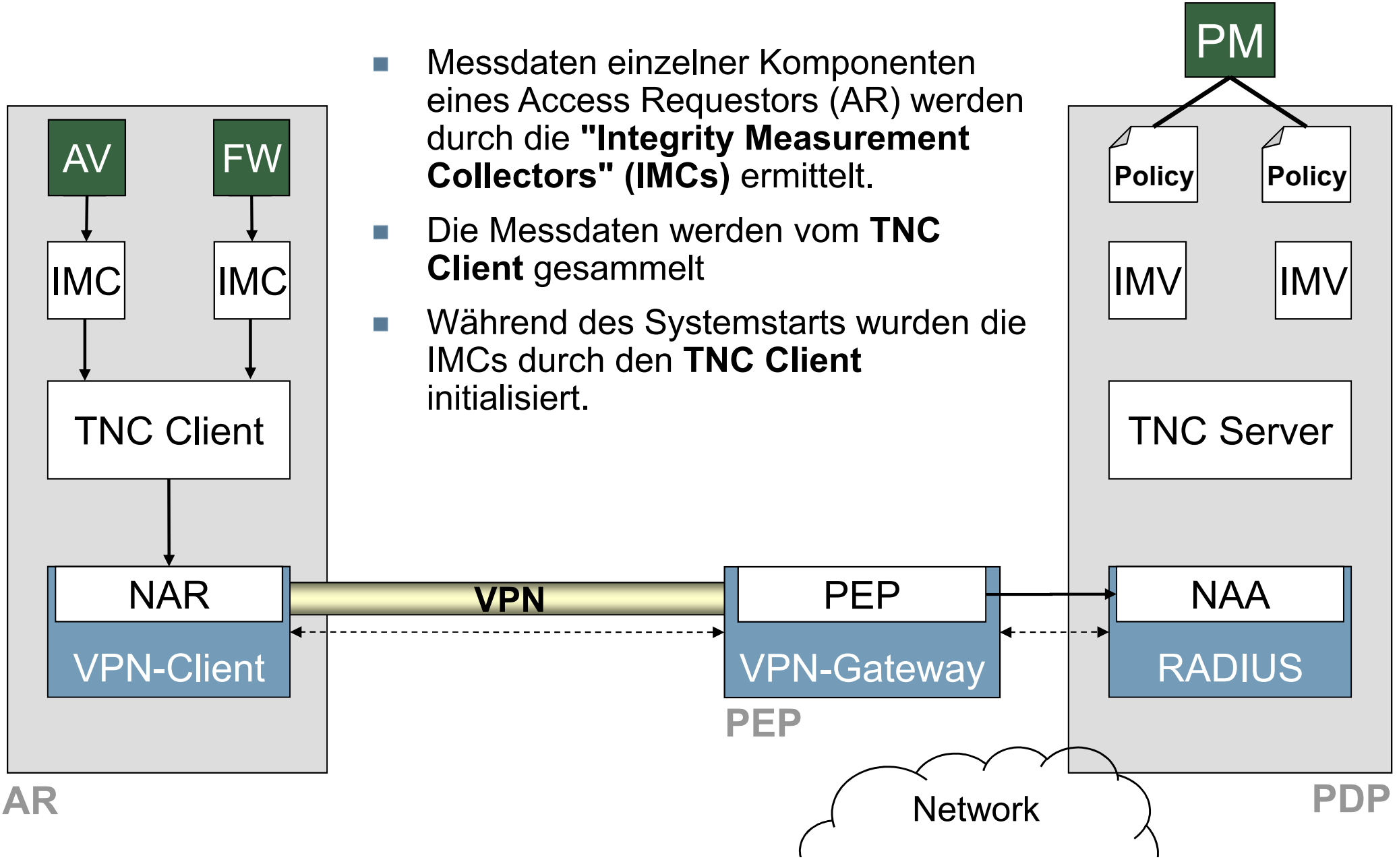
Einschränkungen:

- Malware auf dem Access Requestor (AR) erhält Zugriff auf das Netzwerk
- Angreifer mit gestohlenen Credentials (Token oder Benutzername/Password) oder mit gestohlenen ARs erhalten ebenfalls Zugriff.



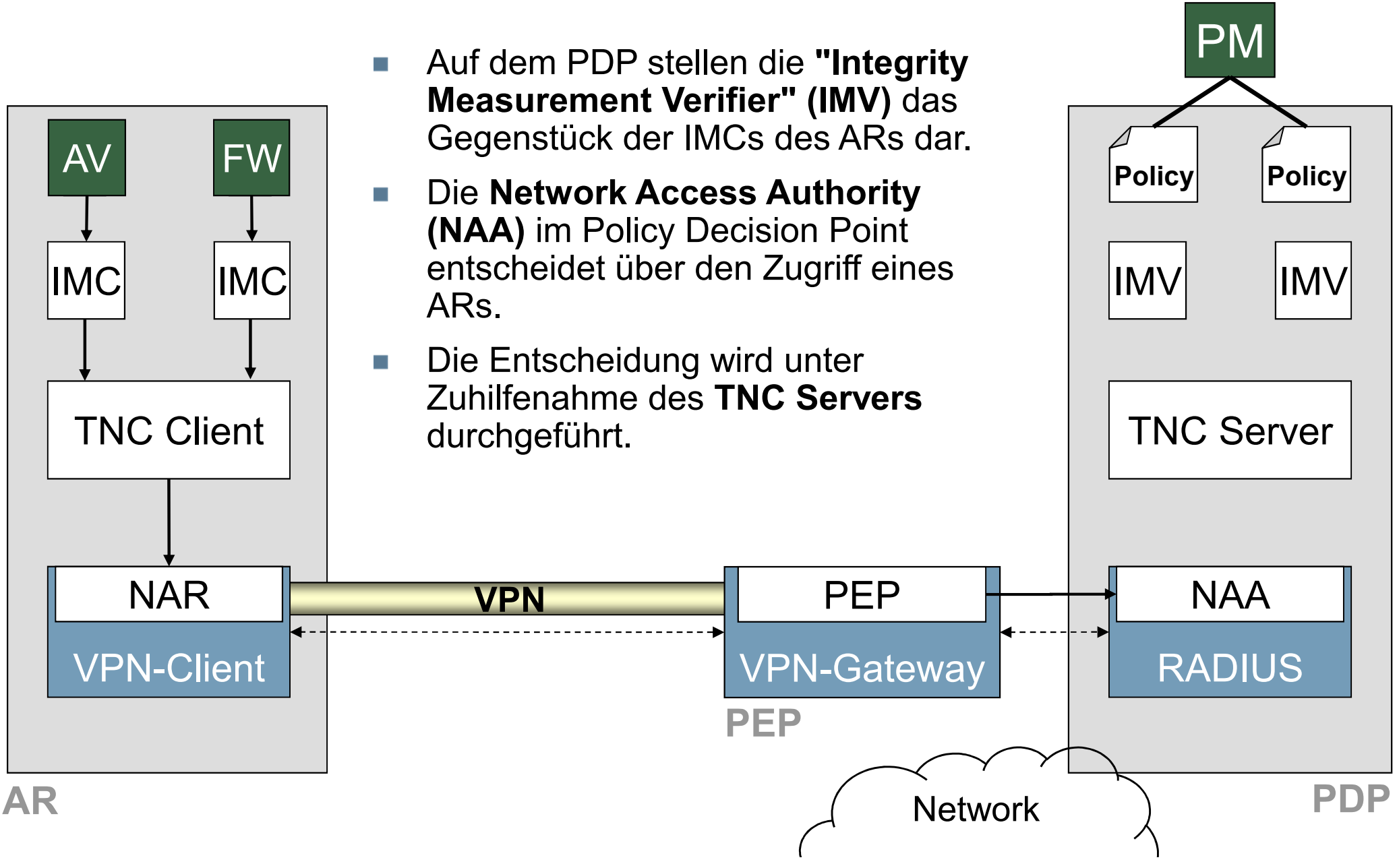
Trusted Network Connect (TNC)
→ Überblick: TNC-Funktionen (1/2)

- Messdaten einzelner Komponenten eines Access Requestors (AR) werden durch die **"Integrity Measurement Collectors" (IMCs)** ermittelt.
- Die Messdaten werden vom **TNC Client** gesammelt
- Während des Systemstarts wurden die IMCs durch den **TNC Client** initialisiert.



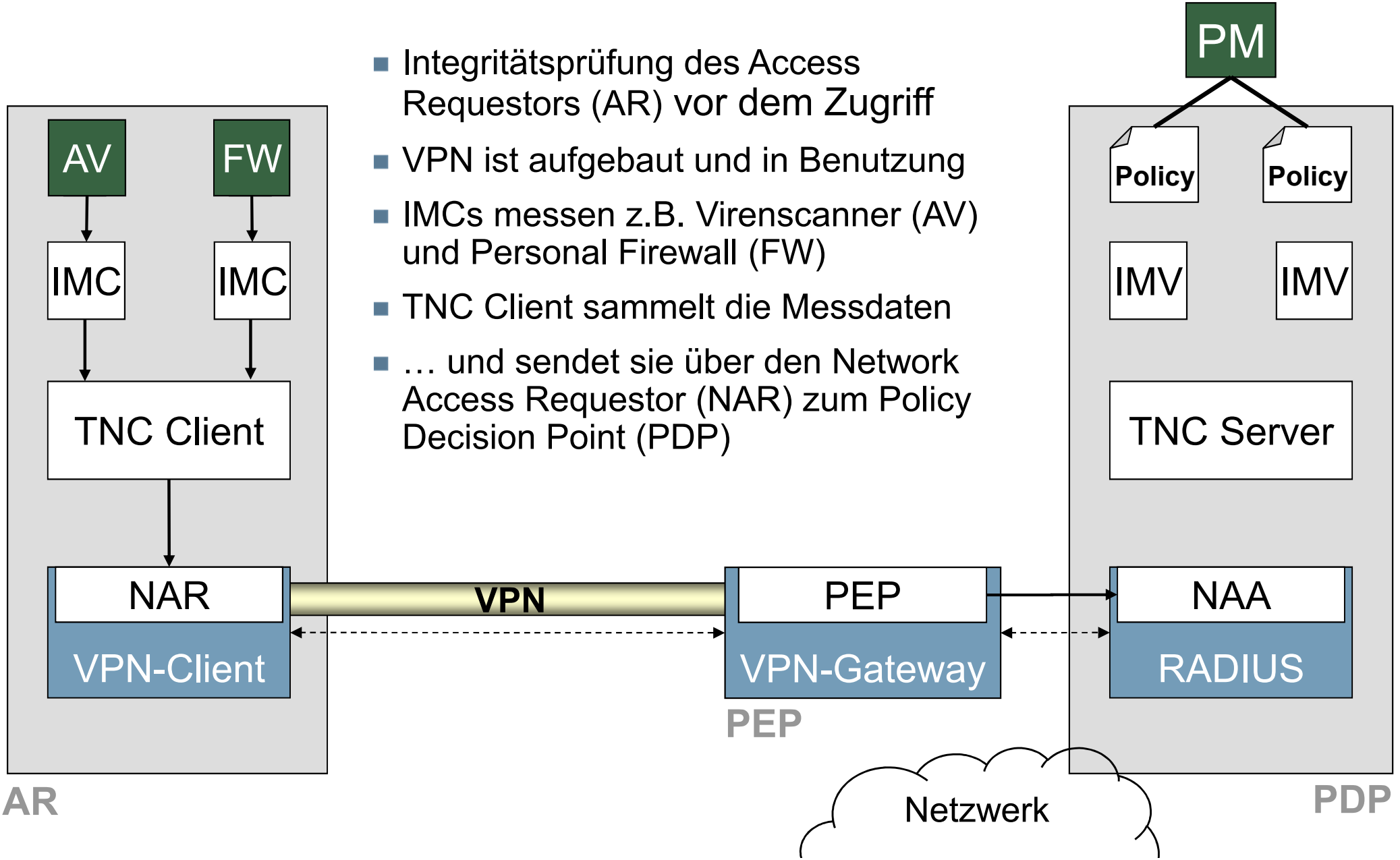
Trusted Network Connect (TNC)
→ Überblick: TNC-Funktionen (2/2)

- Auf dem PDP stellen die **"Integrity Measurement Verifier" (IMV)** das Gegenstück der IMCs des ARs dar.
- Die **Network Access Authority (NAA)** im Policy Decision Point entscheidet über den Zugriff eines ARs.
- Die Entscheidung wird unter Zuhilfenahme des **TNC Servers** durchgeführt.



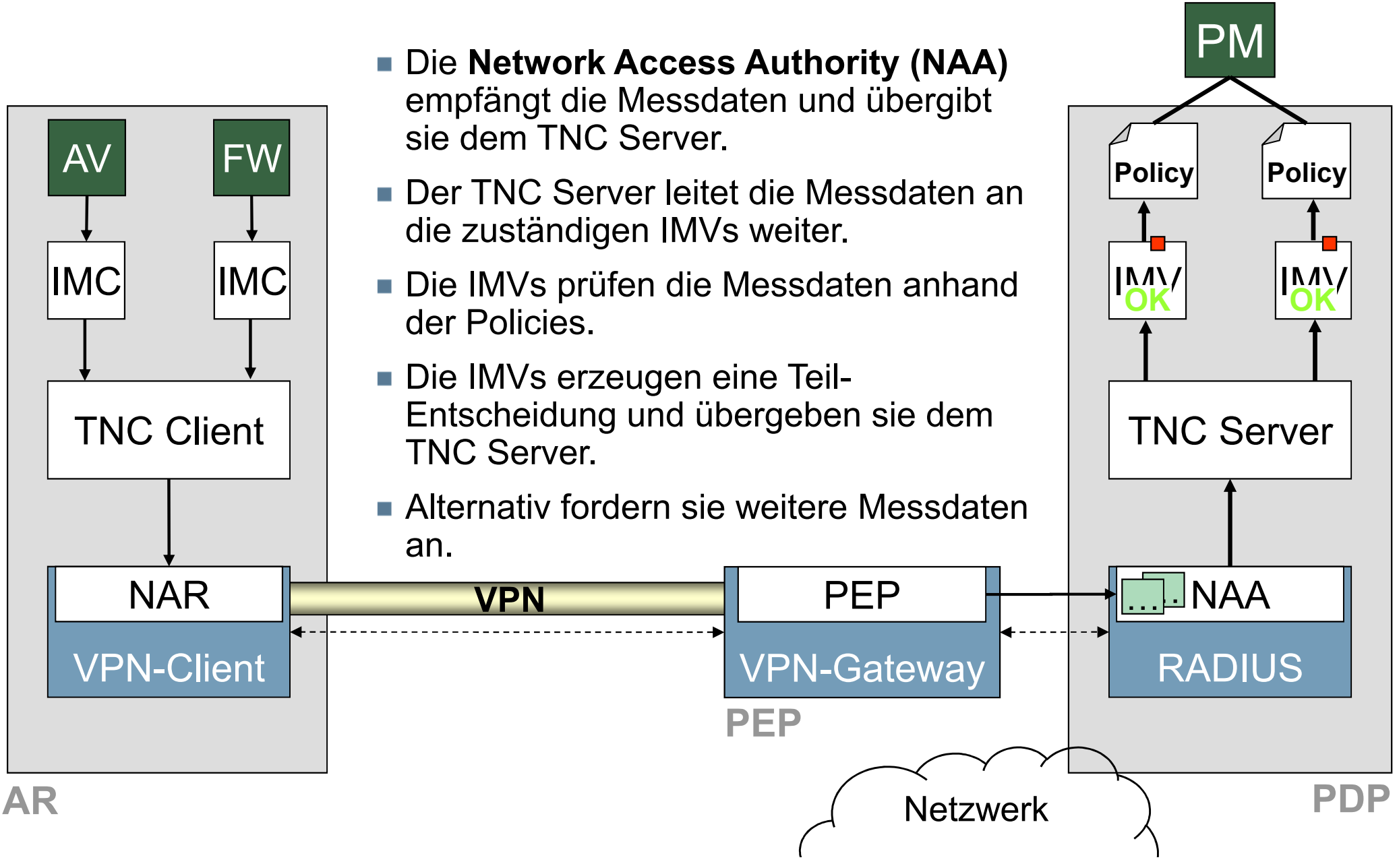
TNC – Phasen
→ Assessment Phase (1/3)

- Integritätsprüfung des Access Requestors (AR) vor dem Zugriff
- VPN ist aufgebaut und in Benutzung
- IMCs messen z.B. Virenscanner (AV) und Personal Firewall (FW)
- TNC Client sammelt die Messdaten
- … und sendet sie über den Network Access Requestor (NAR) zum Policy Decision Point (PDP)



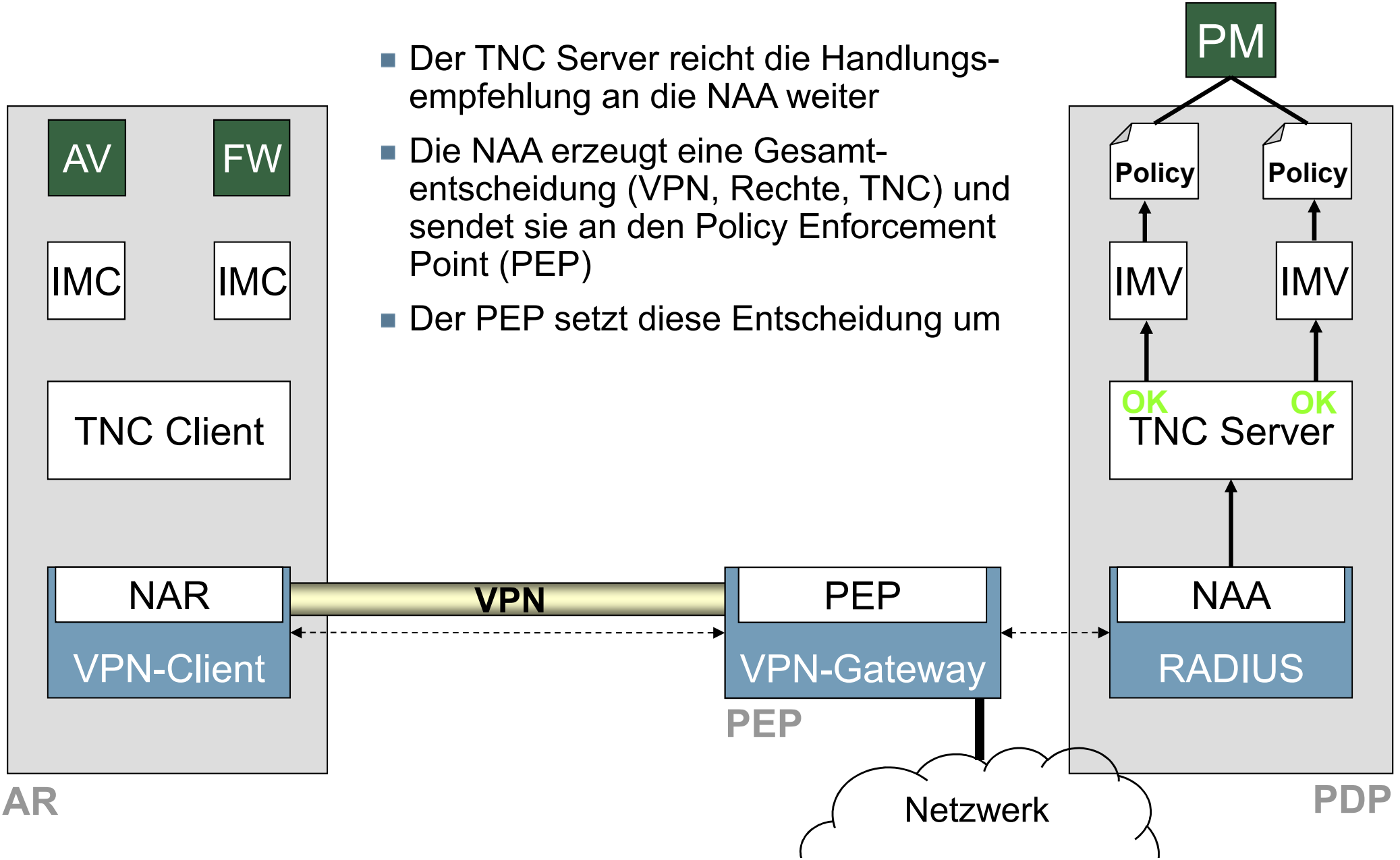
TNC – Phasen
→ Assessment Phase (2/3)

- Die **Network Access Authority (NAA)** empfängt die Messdaten und übergibt sie dem TNC Server.
- Der TNC Server leitet die Messdaten an die zuständigen IMVs weiter.
- Die IMVs prüfen die Messdaten anhand der Policies.
- Die IMVs erzeugen eine Teil-Entscheidung und übergeben sie dem TNC Server.
- Alternativ fordern sie weitere Messdaten an.



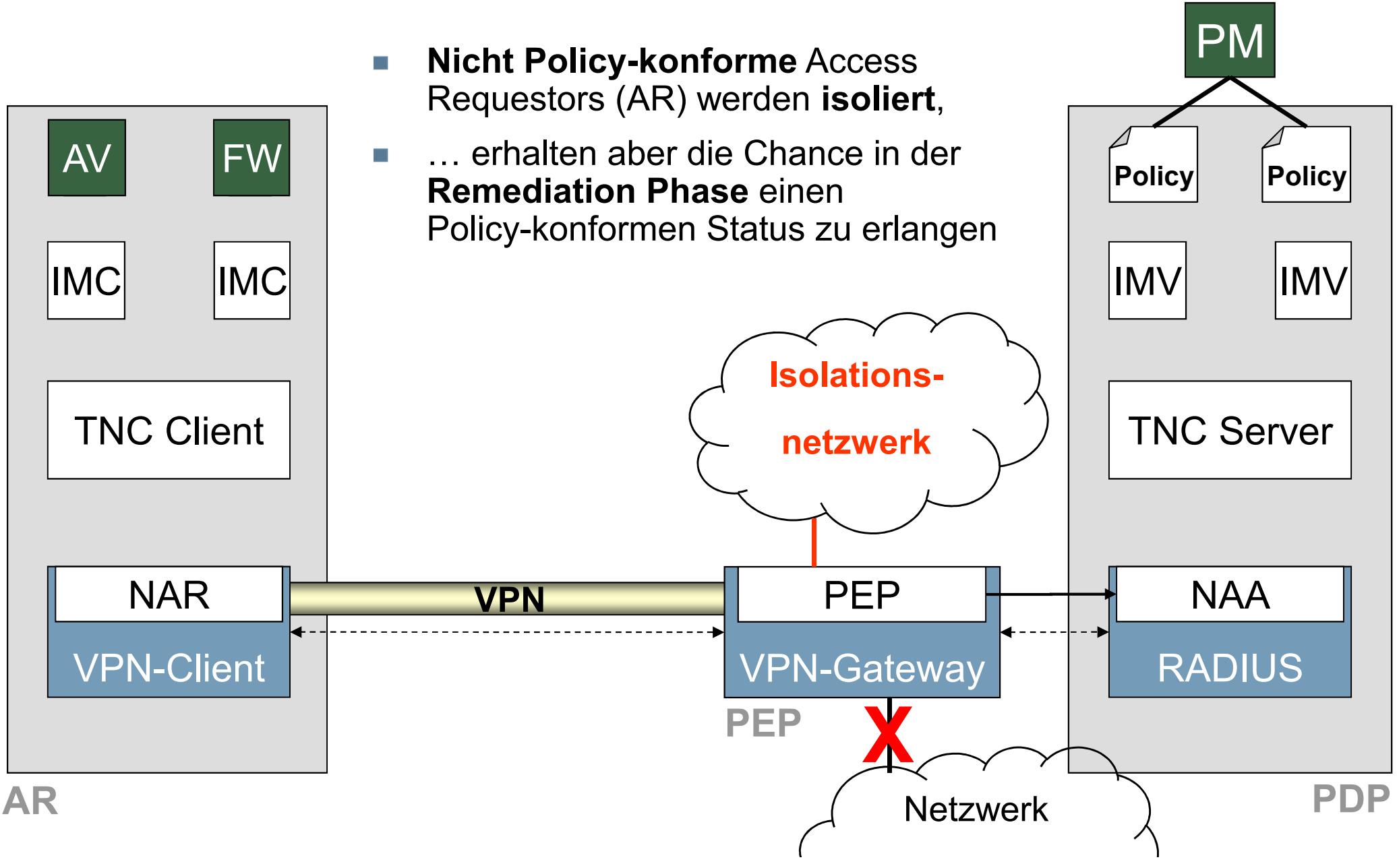
TNC – Phasen
→ Assessment Phase (3/3)

- Der TNC Server reicht die Handlungs-empfehlung an die NAA weiter
- Die NAA erzeugt eine Gesamt-entscheidung (VPN, Rechte, TNC) und sendet sie an den Policy Enforcement Point (PEP)
- Der PEP setzt diese Entscheidung um



TNC – Phasen
→ Isolation und Remediation Phase

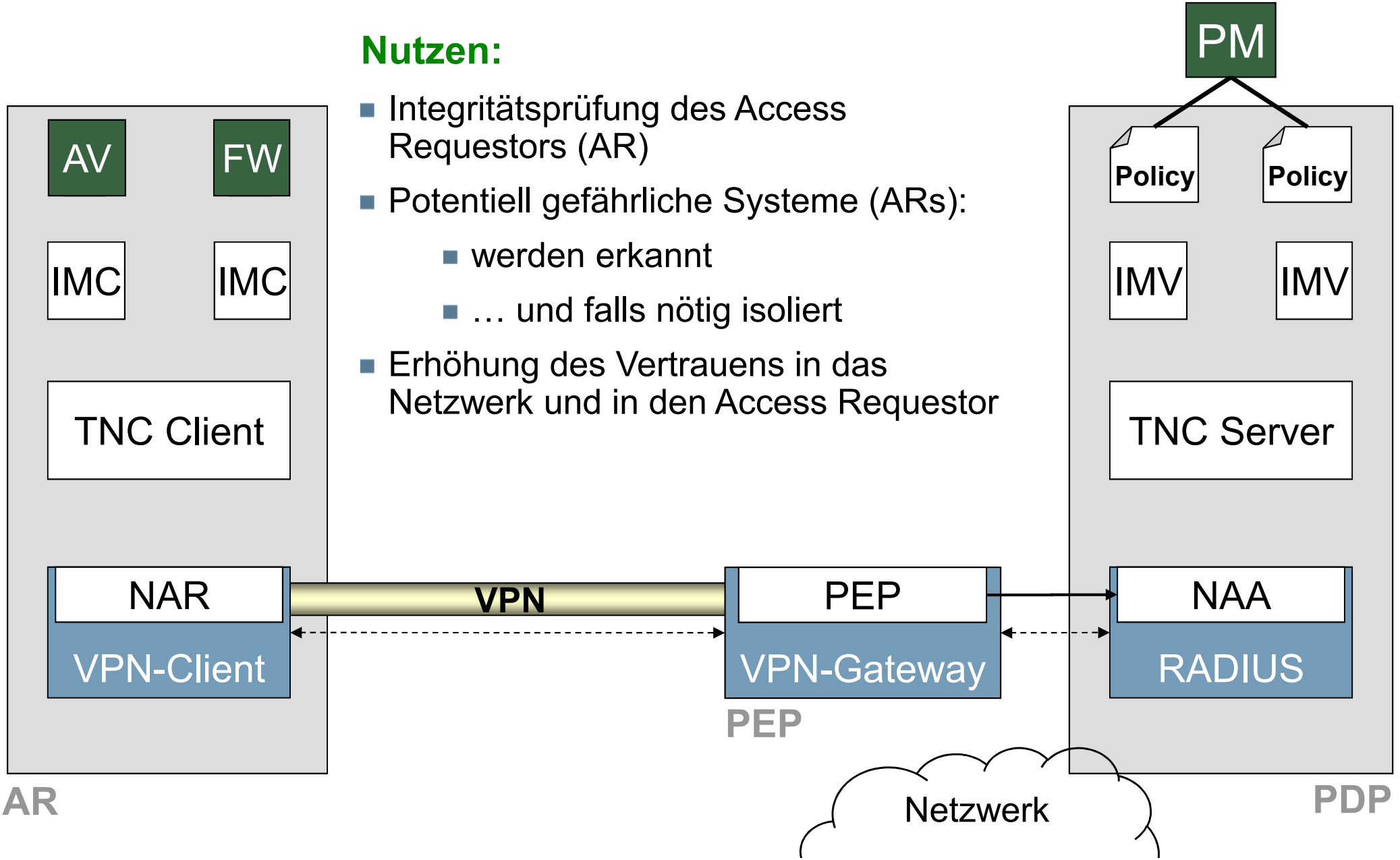
- **Nicht Policy-konforme** Access Requestors (AR) werden **isoliert**,
- … erhalten aber die Chance in der **Remediation Phase** einen Policy-konformen Status zu erlangen



TNC
→ Trusted Network Connect

Nutzen:

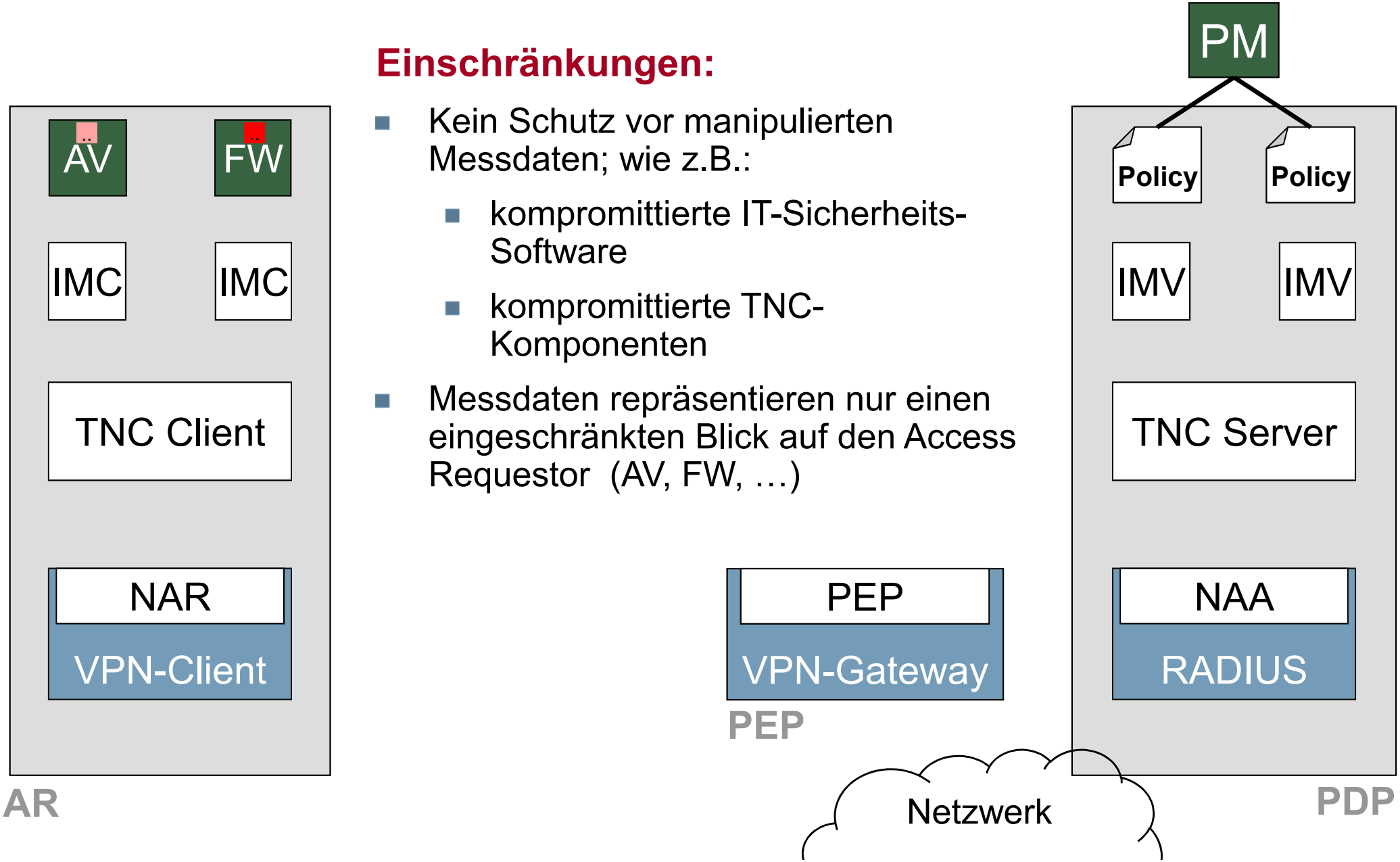
- Integritätsprüfung des Access Requestors (AR)
- Potentiell gefährliche Systeme (ARs):
  - werden erkannt
  - … und falls nötig isoliert
- Erhöhung des Vertrauens in das Netzwerk und in den Access Requestor



TNC
→ Offene Probleme bei TNC

Einschränkungen:

- Kein Schutz vor manipulierten Messdaten; wie z.B.:
  - kompromittierte IT-Sicherheits-Software
  - kompromittierte TNC-Komponenten
- Messdaten repräsentieren nur einen eingeschränkten Blick auf den Access Requestor (AV, FW, …)

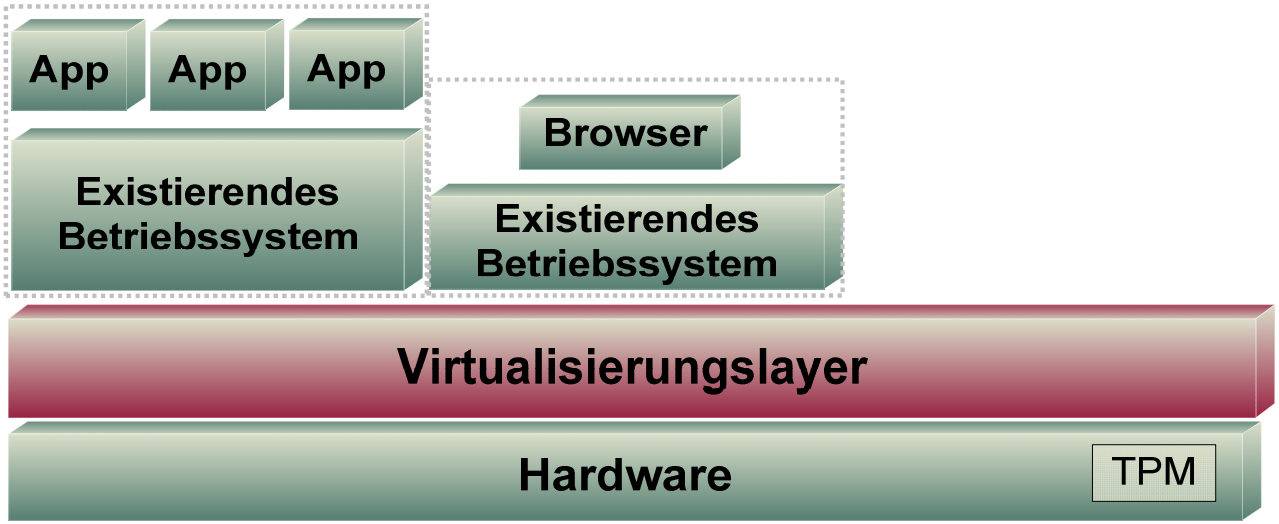


Sicherheitsplattform Turaya
→ Architektur und Technologie 1/3

- ***Herkömmliche Hardware***
  - CPU / Hardware Devices
- ***TPM***
  - Höchster Schutz durch hardwarebasierte Sicherheit
- ***Vorteile der Trusted-Computing-Technologie nutzen***

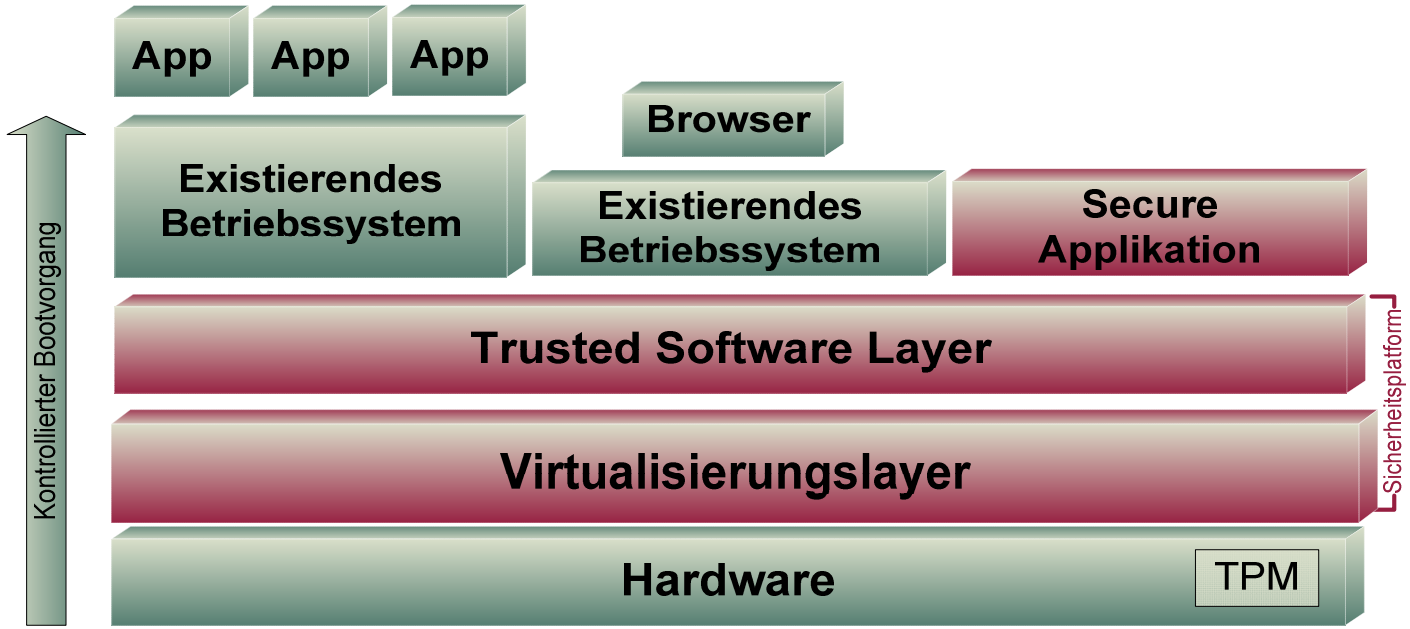
Sicherheitsplattform Turaya
→ Architektur und Technologie 2/3

- ***Virtualisierungslayer zur Isolation ...***
  - Schutz der Applikationen
  - Schutz der Anwenderdaten
  - Schutz vor Manipulationen einer Applikation (bspw.: Browser)
- ***... mittels moderner Virtualisierungstechniken***
  - Mikrokern-Architektur
  - Verwendbarkeit existierender Komponenten in Compartments



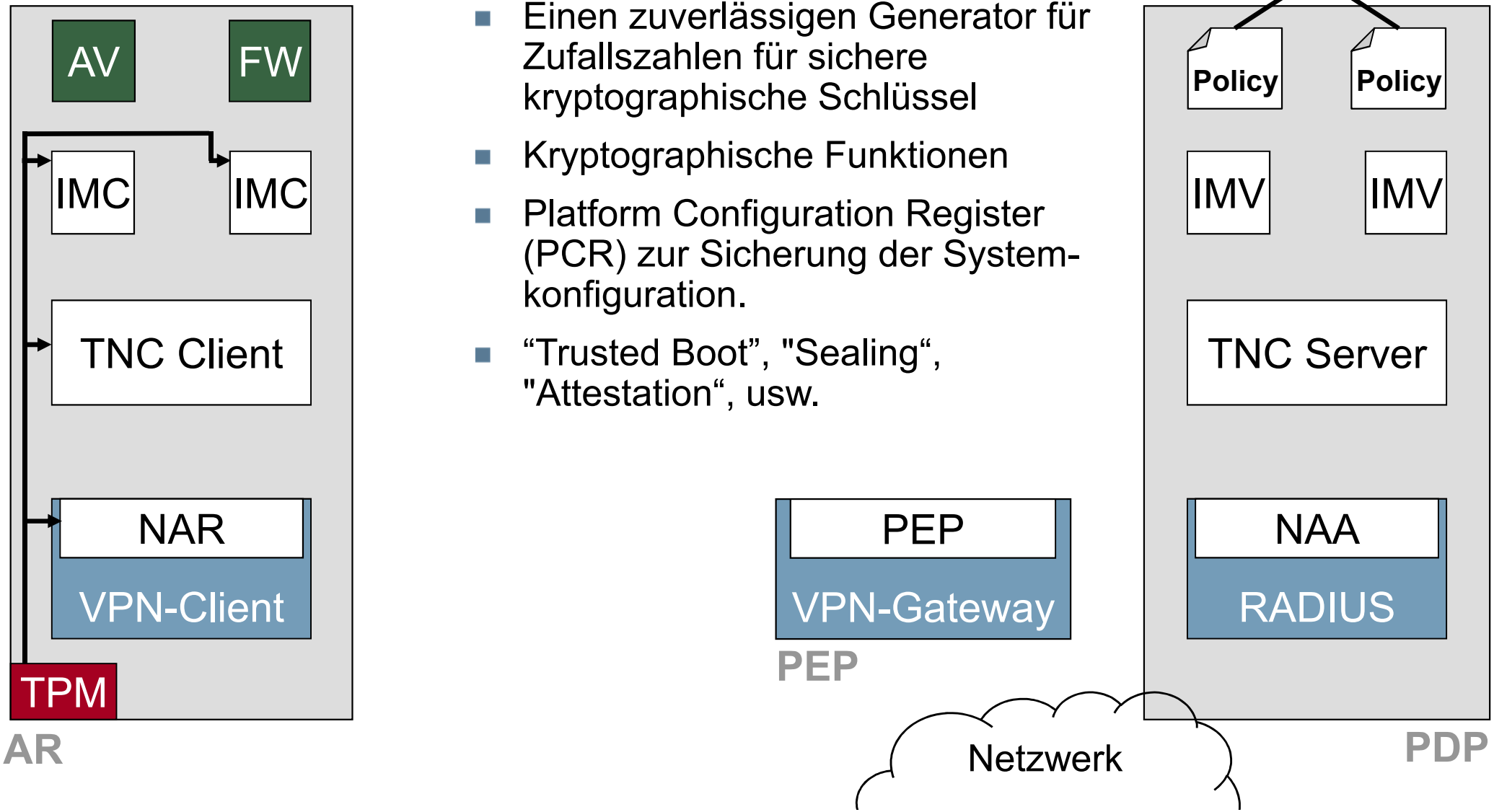
Sicherheitsplattform Turaya
→ Architektur und Technologie 3/3

- ***Sicherheitsplattform (Trusted Software Layer)***
  - **Authentifikation** einzelner Compartments
  - **Binden von Daten** an einzelne Compartments
  - **Trusted Path**
    - Zwischen Anwender & Applikation / Applikation & Smartcard
  - **Sicheres Policy Enforcement**



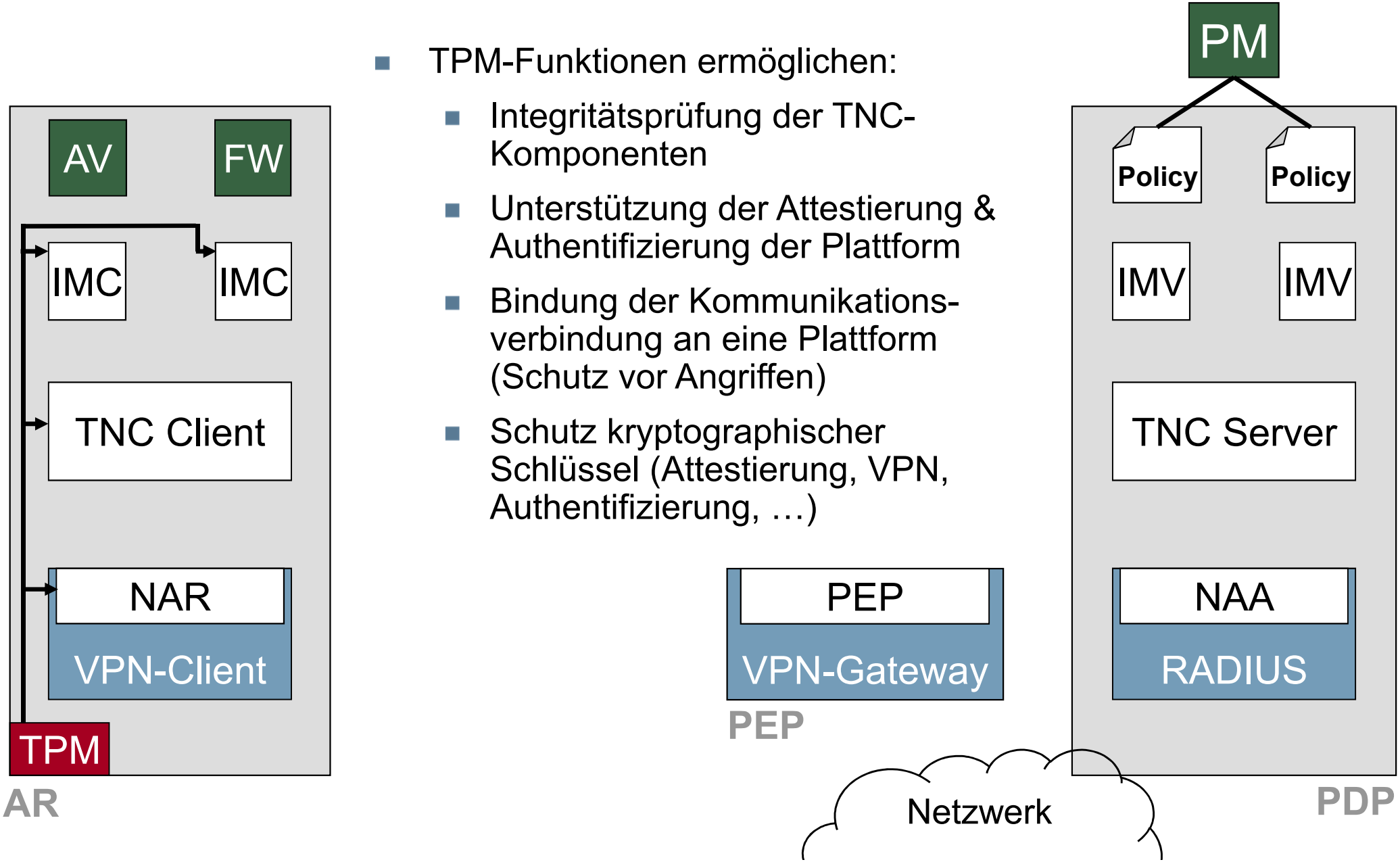
TNC+
→ TNC + TPM

- Was bietet ein TPM?
  - Einen zuverlässigen Generator für Zufallszahlen für sichere kryptographische Schlüssel
  - Kryptographische Funktionen
  - Platform Configuration Register (PCR) zur Sicherung der System-konfiguration.
  - “Trusted Boot”, "Sealing“, "Attestation“, usw.



TNC+
→ Mehrwert: TPM

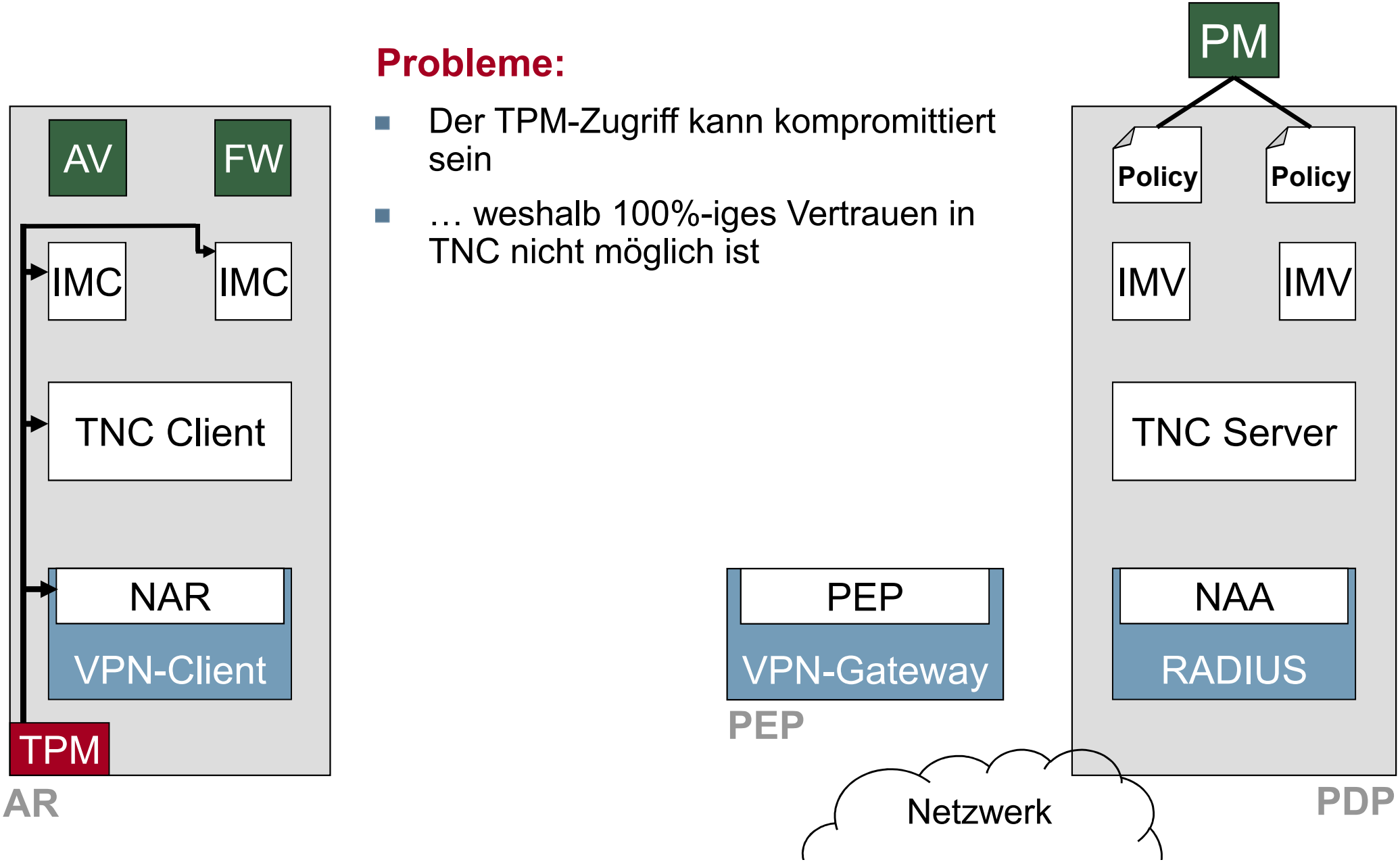
- TPM-Funktionen ermöglichen:
  - Integritätsprüfung der TNC-Komponenten
  - Unterstützung der Attestierung & Authentifizierung der Plattform
  - Bindung der Kommunikations-verbindung an eine Plattform (Schutz vor Angriffen)
  - Schutz kryptographischer Schlüssel (Attestierung, VPN, Authentifizierung, …)



TNC+
→ TPM: Einschränkungen

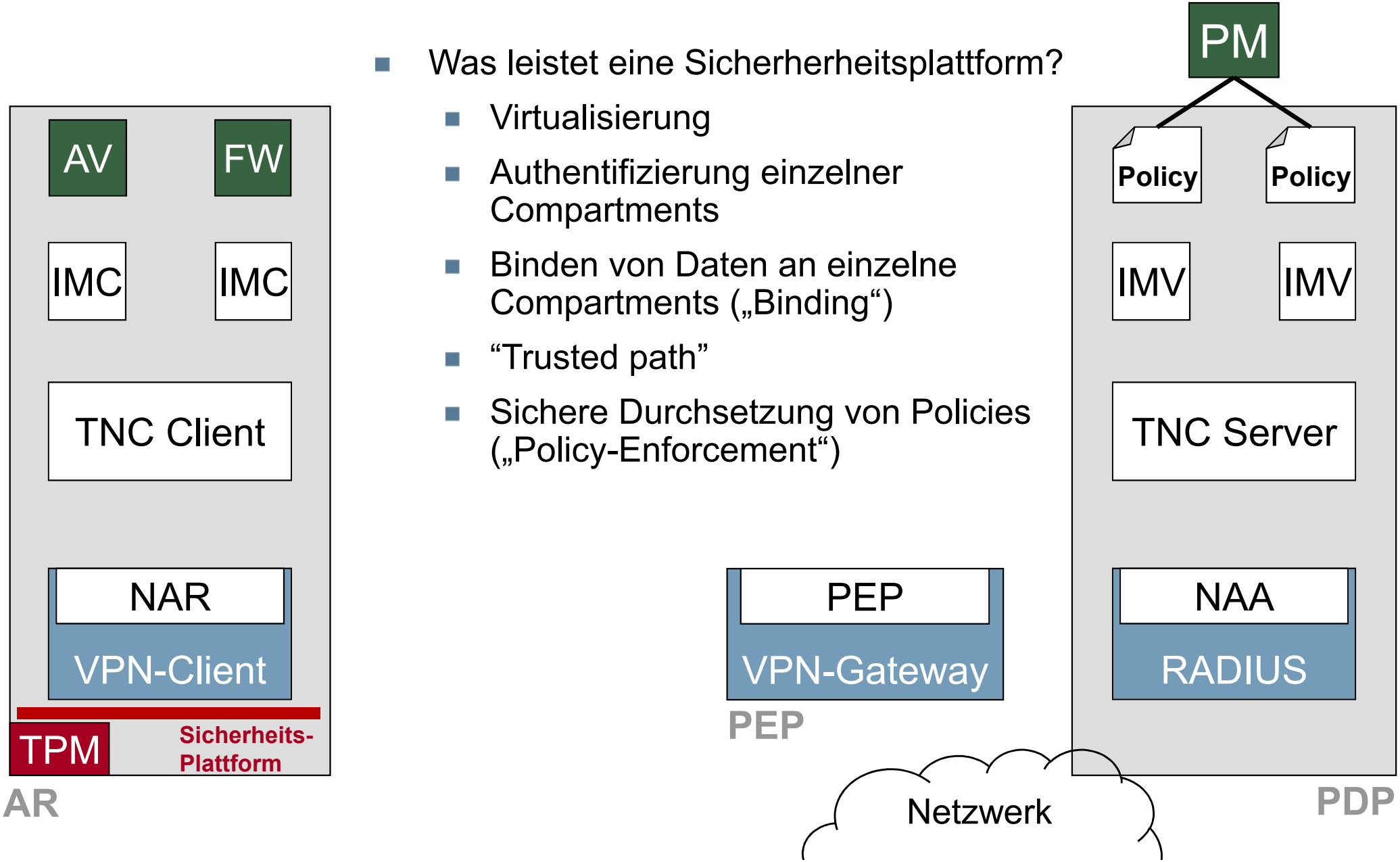
Probleme:

- Der TPM-Zugriff kann kompromittiert sein
- … weshalb 100%-iges Vertrauen in TNC nicht möglich ist



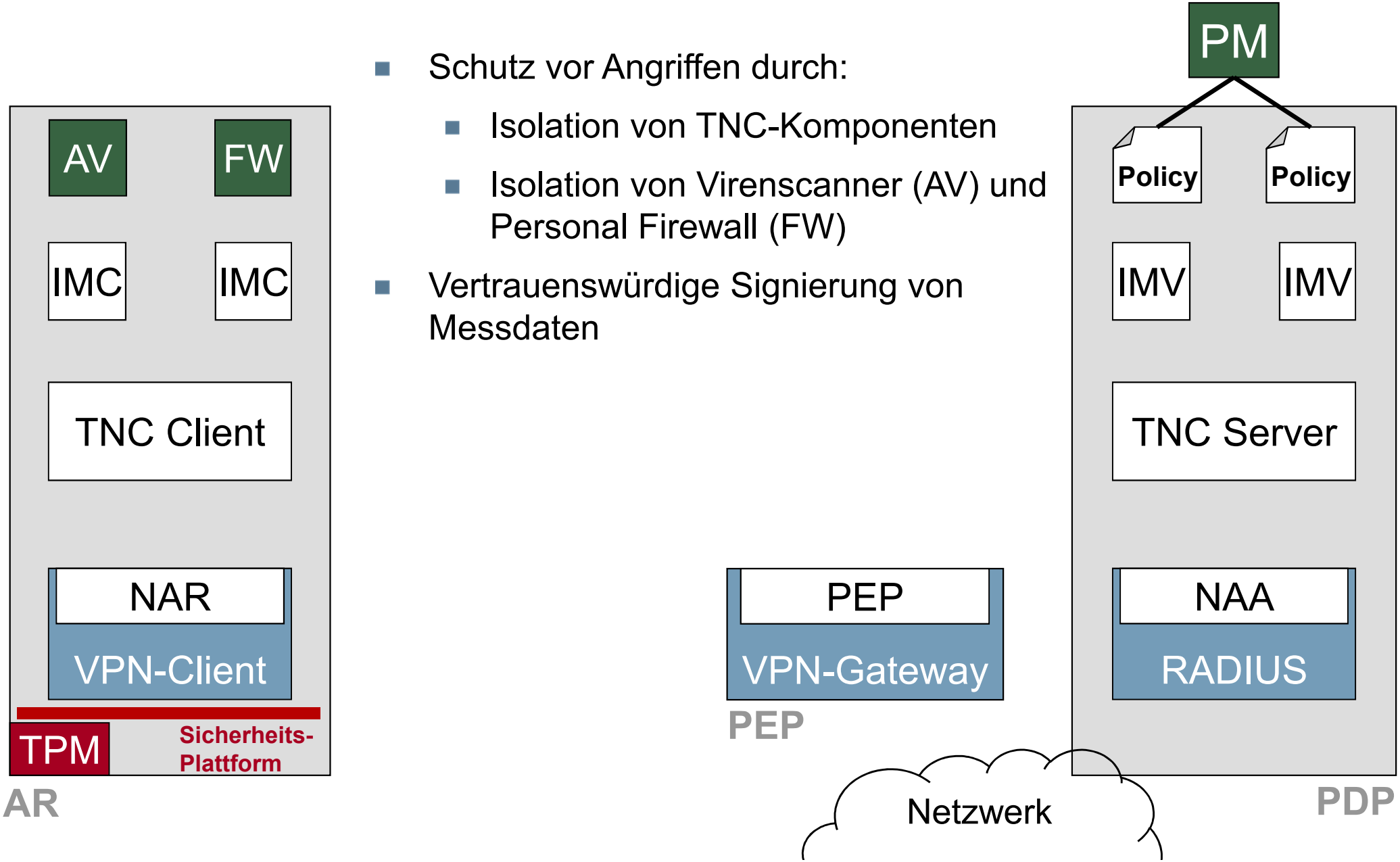
TNC++
→ TNC + TPM + Sicherheitsplattform

- Was leistet eine Sicherherheitsplattform?
  - Virtualisierung
  - Authentifizierung einzelner Compartments
  - Binden von Daten an einzelne Compartments („Binding“)
  - “Trusted path”
  - Sichere Durchsetzung von Policies („Policy-Enforcement“)



TNC++
→ Mehrwert: Sicherheitsplattform

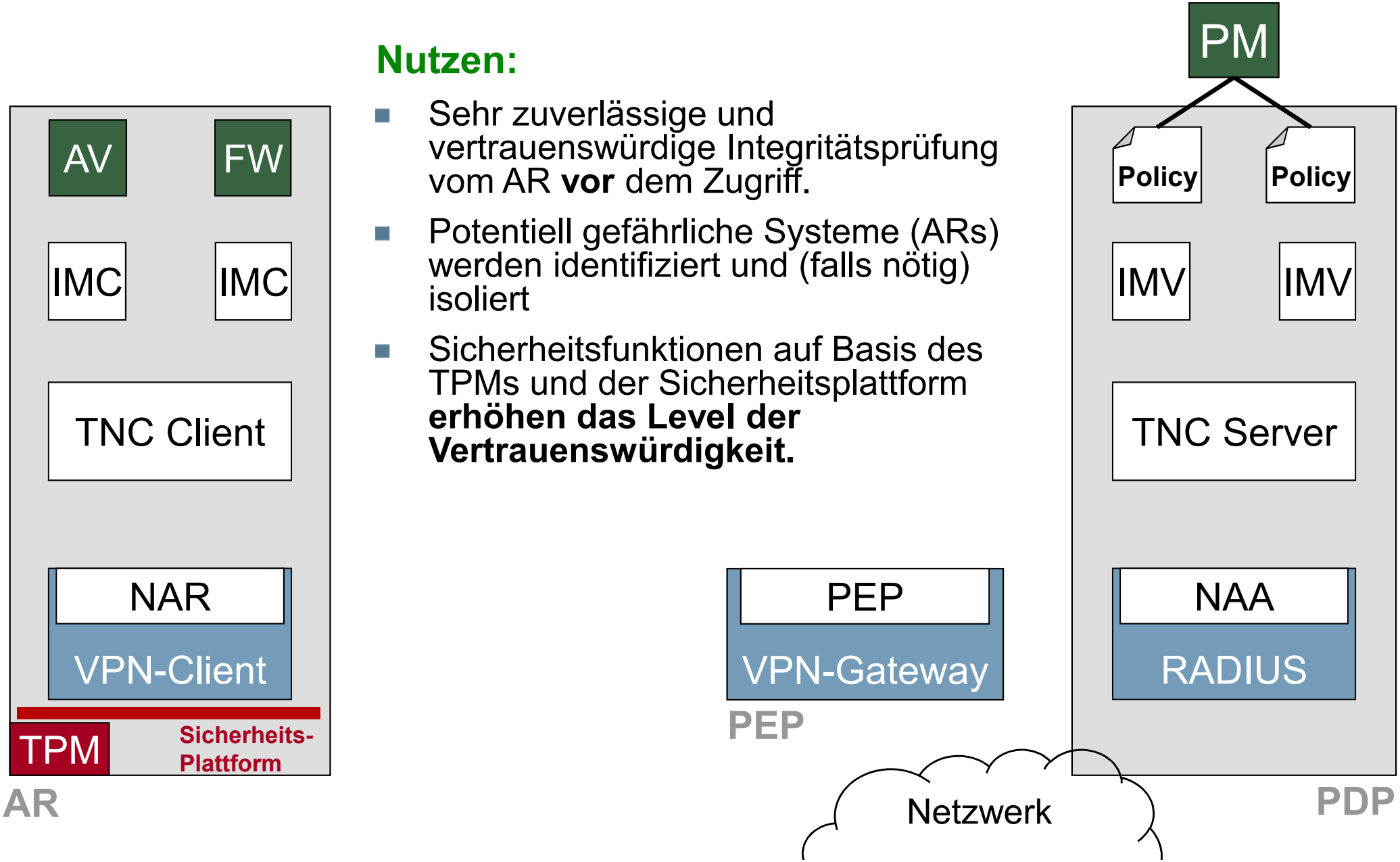
- Schutz vor Angriffen durch:
  - Isolation von TNC-Komponenten
  - Isolation von Virenscanner (AV) und Personal Firewall (FW)
- Vertrauenswürdige Signierung von Messdaten



TNC++
→ Mehrwert: Sicherheitsplattform

Nutzen:

- Sehr zuverlässige und vertrauenswürdige Integritätsprüfung vom AR **vor** dem Zugriff.
- Potentiell gefährliche Systeme (ARs) werden identifiziert und (falls nötig) isoliert
- Sicherheitsfunktionen auf Basis des TPMs und der Sicherheitsplattform **erhöhen das Level der Vertrauenswürdigkeit.**



Weitere Aufgabenstellungen (1/2)

- Wer definiert die Policies?
- Wer definiert welche Systemkonfiguration und welche IT-Sicherheitsprodukte vertrauenswürdig sind?
  - **Die Hersteller?**
    - Die Betriebssystem- und Software-Hersteller?
    - Die Anbieter von TNC-Lösungen?
    - Die Hersteller von IT-Sicherheitsprodukten; z.B. von IMCs und IMVs für Virenscanner (AV) und Personal Firewall (FW)?
  - **Die Betreiber?**
    - Aus strategischen Gründen?
    - Aus Erfahrung?
  - **Beide zusammen?**

Weitere Aufgabenstellungen (2/2)

- Benötigen wir einen “**TÜV**”**?**
  - Which makes a common criteria evaluation for IT-Systems
  - Erlaubnis des Verkaufs von Hard- und Software nur nach positiver Prüfung?
  -
- Benötigen wir eine **anwendernahe Organisation**, die sich um die Vertrauenswürdigkeit kümmert?
  - Verifikation neuer Technologien, Sicherheitsmechanismen, usw.
  - Sammlung der Nutzer-Erfahrungen.
  - Herausgabe von Nutzungs-Empfehlungen für die Integritätsprüfung entfernter Rechnersysteme

Zusammenfassung und Ausblick

- Vertrauenswürdigkeit ist kein Status!
- **Vertrauenswürdigkeit ist ein Prozess!**
- Lassen Sie uns einen gemeinsamen Schritt hin zu einem **höheren Level an Vertrauenswürdigkeit** gehen**!**
- **Network Access Control**, insb. **Trusted Network Connect,** scheinen der richtige Weg zu sein.

Fachhochschule Gelsenkirchen

Sichere Einbindung von mobilen Endgeräten mit Hilfe von TNC
→ Trusted Network Connect

Vielen Dank für Ihre Aufmerksamkeit
Fragen ?

Prof. Dr. Norbert Pohlmann

Institut für Internet-Sicherheit
Fachhochschule Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet-sicherheit.