IRON: Intelligent Reaction on Network Events

Sichere Netzwerke durch Korrelation von Metadaten

Ingo Bente Jörg Vieweg

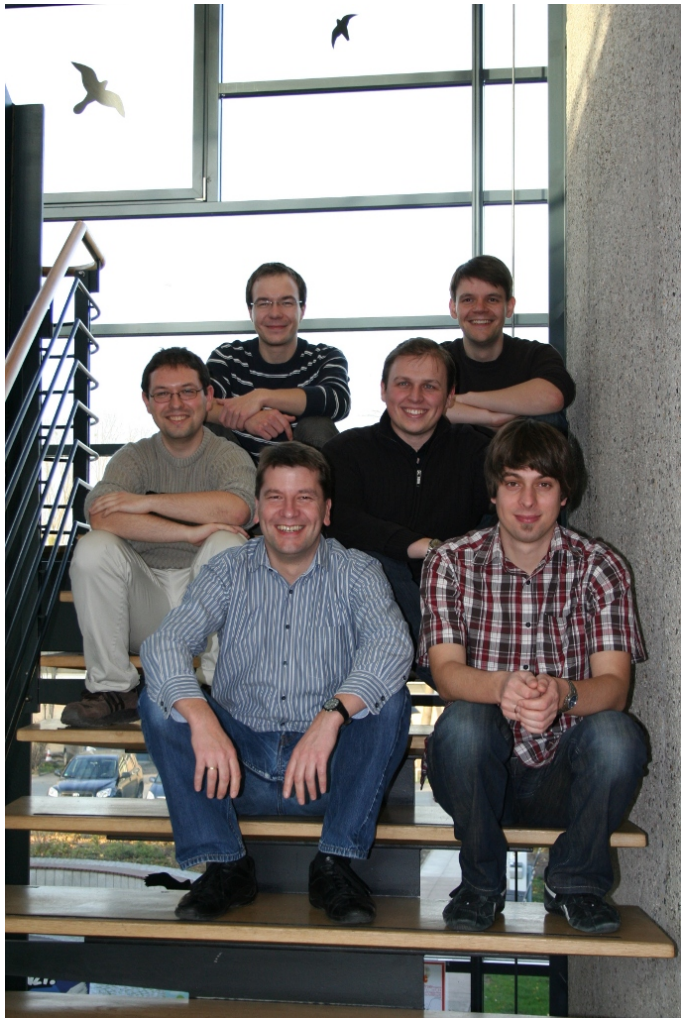
Forschungsgruppe Trust@FHH
Fachhochschule Hannover

16. April 2010
4. Essener Workshop
"Neue Herausforderungen in der Netzsicherheit"

Trust@FHH
Fachhochschule Hannover
University of Applied Sciences and Arts

Trust@FHH ... ?

- Forschungsgruppe an der Fachhochschule Hannover
- Fakultät IV - Wirtschaft und Informatik
- Themen
  - Trusted Computing
  - Network Access Control
  - Integration obiger Konzepte



- `http://trust.inform.fh-hannover.de`

Gliederung

Gliederung

Einleitung

Aktuelle Bedrohungslage für IT-Infrastrukturen

- IT-Infrastrukturen attraktives Angriffsziel
- Bedrohungslage verschärft sich stetig
  - dynamische Struktur moderner Netze
  - steigende Professionalität der Hacker
  - Underground Economy *etabliert* Wirtschaftsspionage[1]

Grundlegende Sicherheitsmechanismen

- Absicherung des Netz Perimeters
  - Firewall, VPN, Network Access Control
- *Interne* Sicherheitsmechanismen
  - IDS, IPS, Netzwerk Monitoring u. Management Tools

[1] http://online.wsj.com/article/SB125616872684400273.html

Nachteil aktueller Sicherheitsmechanismen

Tools arbeiten isoliert voneinander

- Funktionsweise basierend auf eigenem Datenbestand
- Jedes Tool hat eigene *Sicht* auf Netzwerk
- $\rightarrow$ Wissens-Inseln

Integration vorhandener Tools wünschenswert

- Austausch von Daten $\rightarrow$ Erweiterung der Funktionalität
- Anwendungsbeispiel: Reaktion auf IDS Alarme
- Bisher:
  - Log-Meldung / E-Mail an Admin
- Ziel:
  - NAC Lösung wird informiert $\rightarrow$ Isolation des Endgerätes
  - Firewall wird informiert $\rightarrow$ Anpassung der Konfiguration

Gliederung

IF-MAP Grundlagen

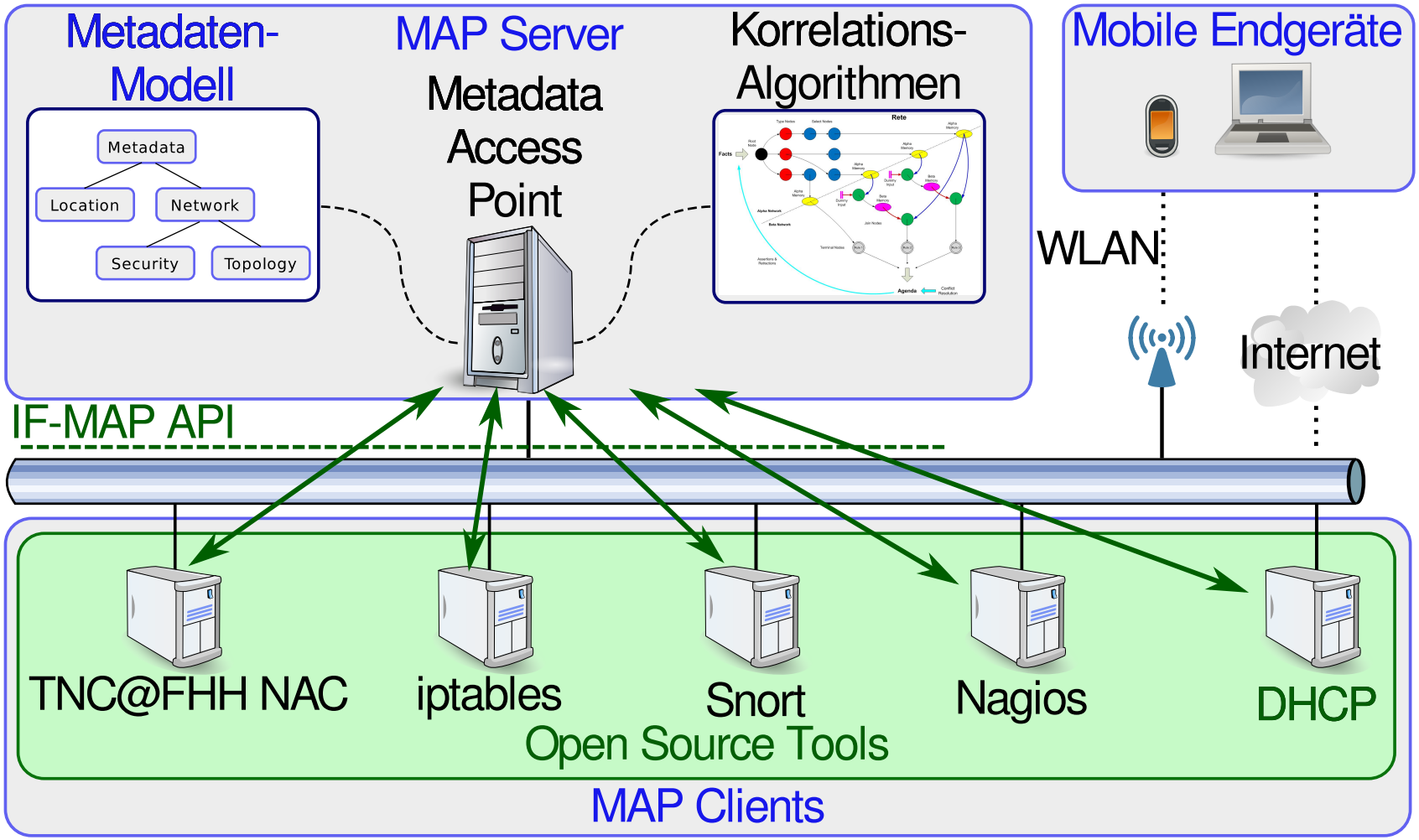
IF-MAP Spezifikationen der Trusted Computing Group

- Ansatz zur Integration beliebiger Netzwerkkomponenten
- Bestandteil des TNC Frameworks
- Kernanforderungen
  1. einheitliches, erweiterbares Datenformat
  2. interoperable Schnittstelle
- Integration basierend auf Metadaten des Netzwerkes

IF-MAP Architektur

- Zentraler MAP Server verwaltet Metadaten (MAPS)
- MAP Clients senden/empfangen Metadaten über MAPS
- Standardisierung: Format der Metadaten und IF-MAP API/Protokoll
- $\longrightarrow$ Interoperable Integration von Netzwerkkomponenten

Architektur einer IF-MAP Infrastruktur



Metadatenformat

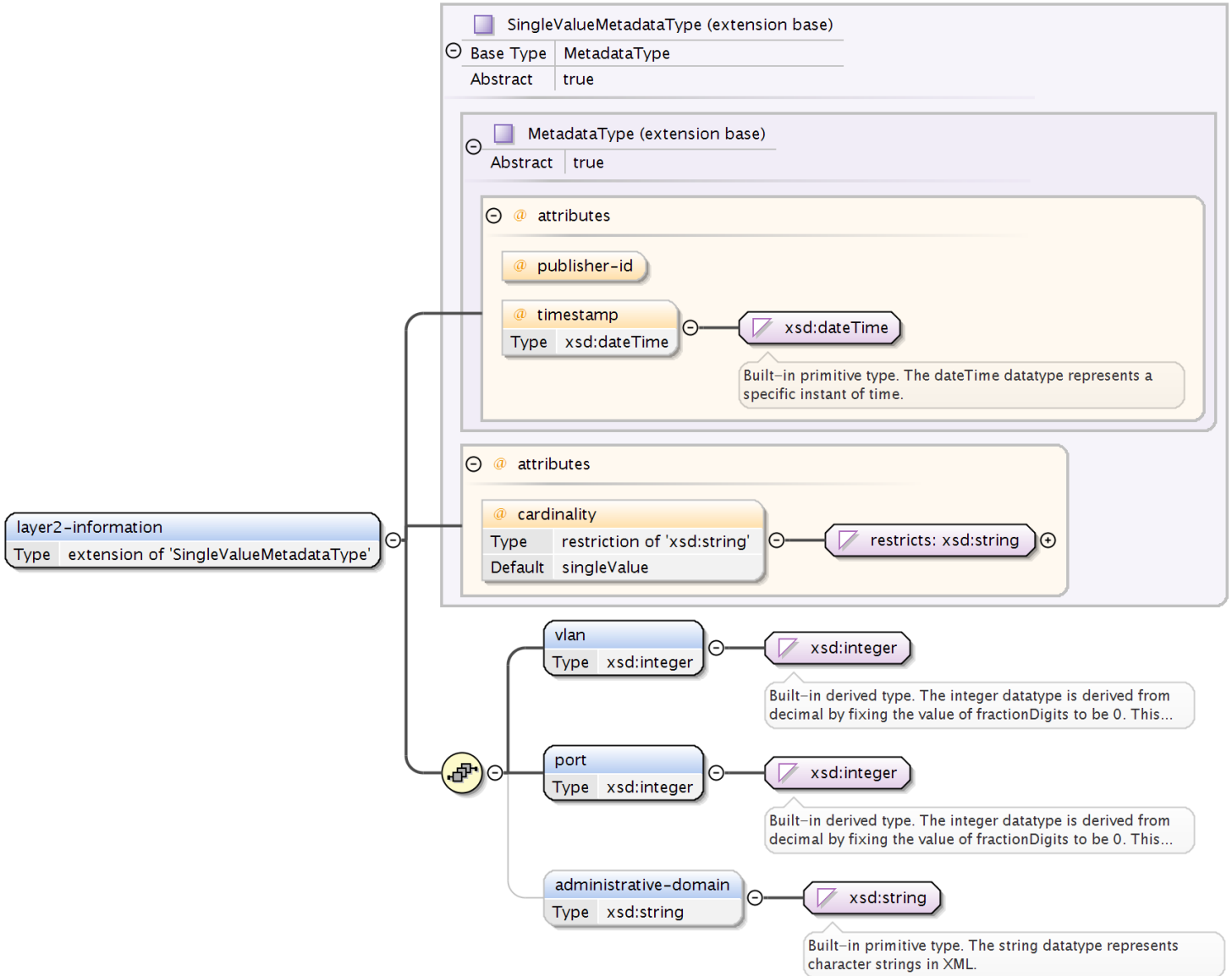
Interoperables, erweiterbares Format für Metadaten

- Definiert durch XML Schema Dokumente
- Addressiert zurzeit Use Cases für Netzwerksicherheit/Management
- Beispiele: Benutzer, Rolle, IP-Adresse, IDS-Alarm

Bestandteile und interne Repräsentation

- *Identifier*: IP-Adresse, Access-Request
- *Link*: verbindet zwei Identifier
- *Metadata*: User, Role, Layer2-Information
- Metadaten für Links und Identifier anwendbar
- Interne Repräsentation: ungerichteter Graph

Metadaten Beispiel: Layer 2 Information



IF-MAP Kommunikationsmodell

- Unterstützt wird (a)synchrone Kommunikation

Drei Grundoperationen

- publish: veröffentliche/aktualisiere Metadaten (synchron)
- search: Suche Metadaten (synchron)
- subscribe: Observiere Metadaten (asynchron)
- search/subscribe: Auswahl von Metadaten durch Filter
- `meta:layer2-information[ administrative-domain="Main Campus" and vlan > 30]`

Technologische Basis

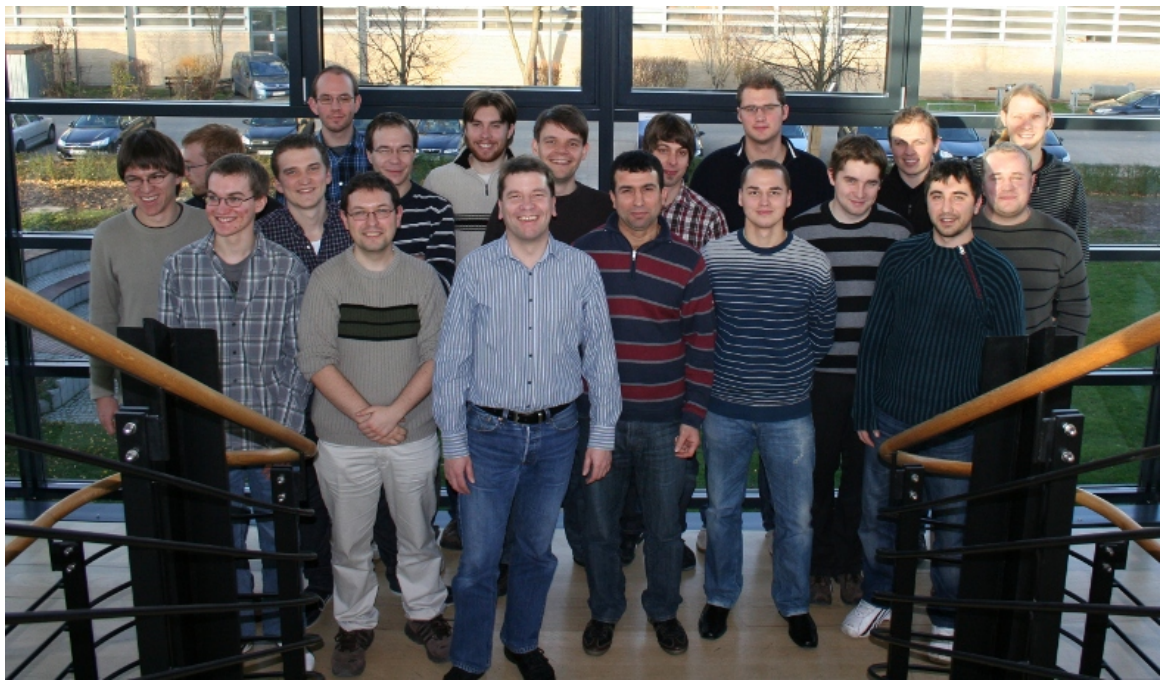
- SOAP über http(s), IF-MAP WSDL Beschreibung verfügbar

Gliederung

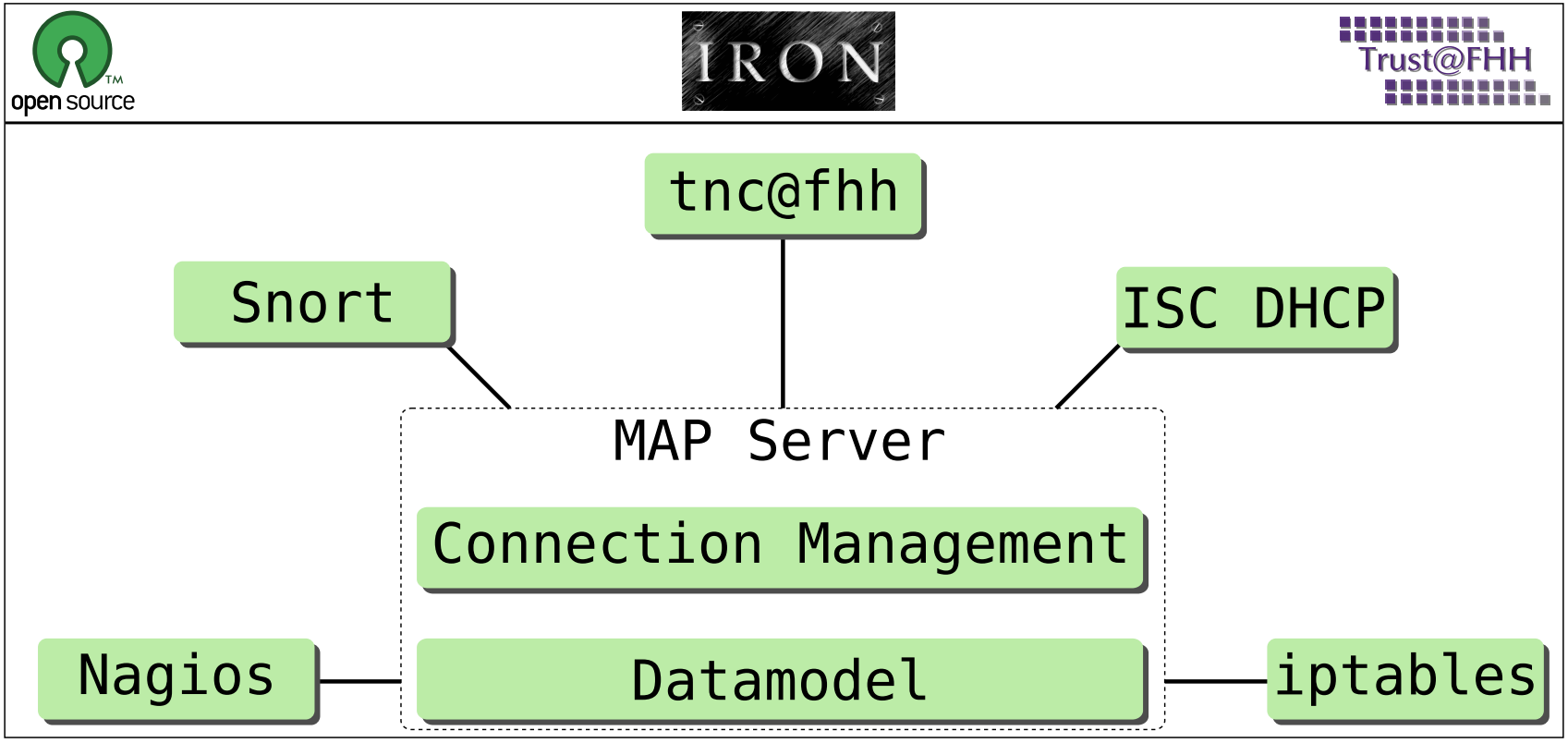
IRON - Intelligent Reaction on Network Events

Allgemeines

- Forschungsprojekt, Start: September 2009
- Beteiligung von Bachelor Studenten (5./6. Semester)
- 1. Ziel: Referenzimplementierung einer IF-MAP Infrastruktur



Projektstruktur



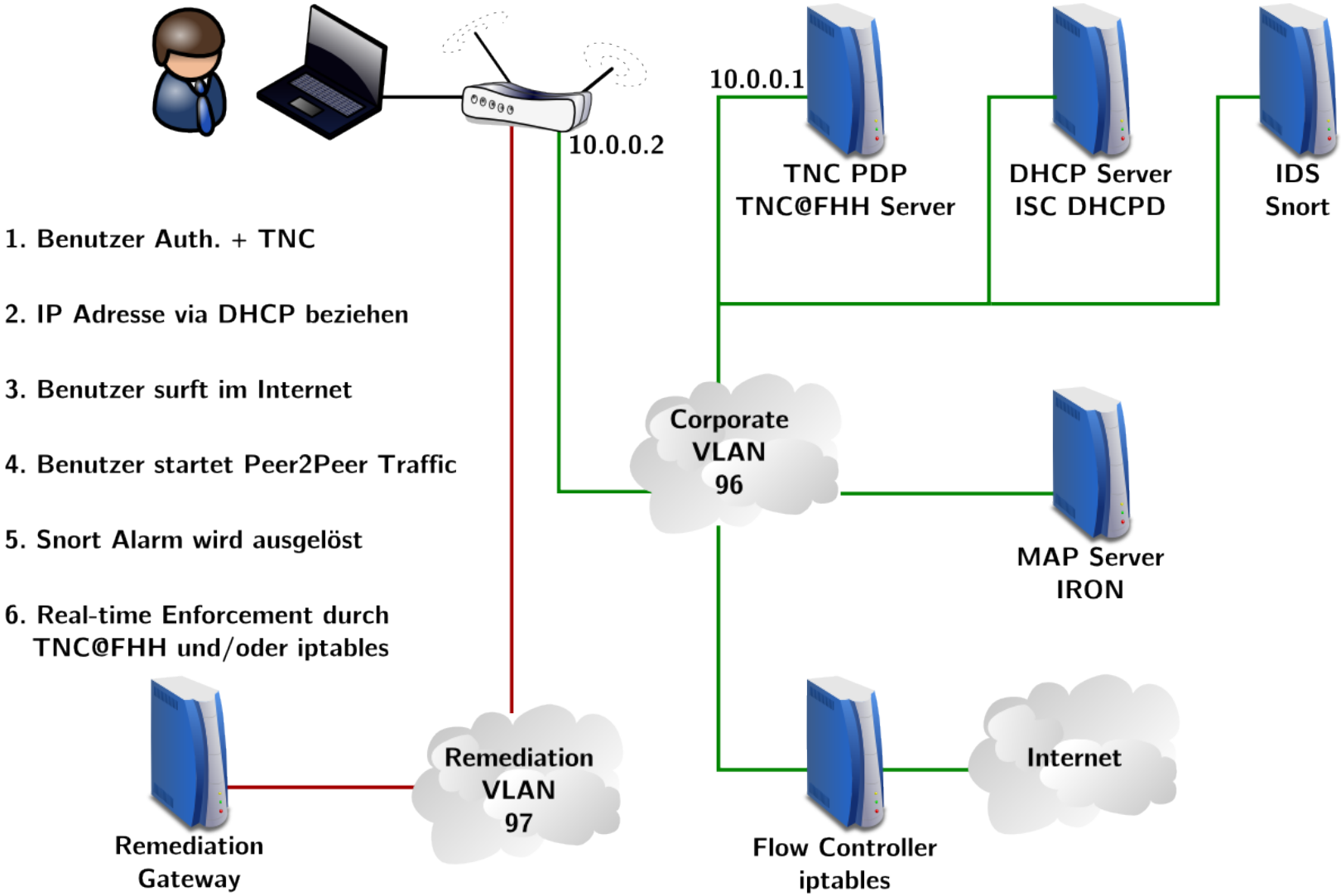
Beispielszenario

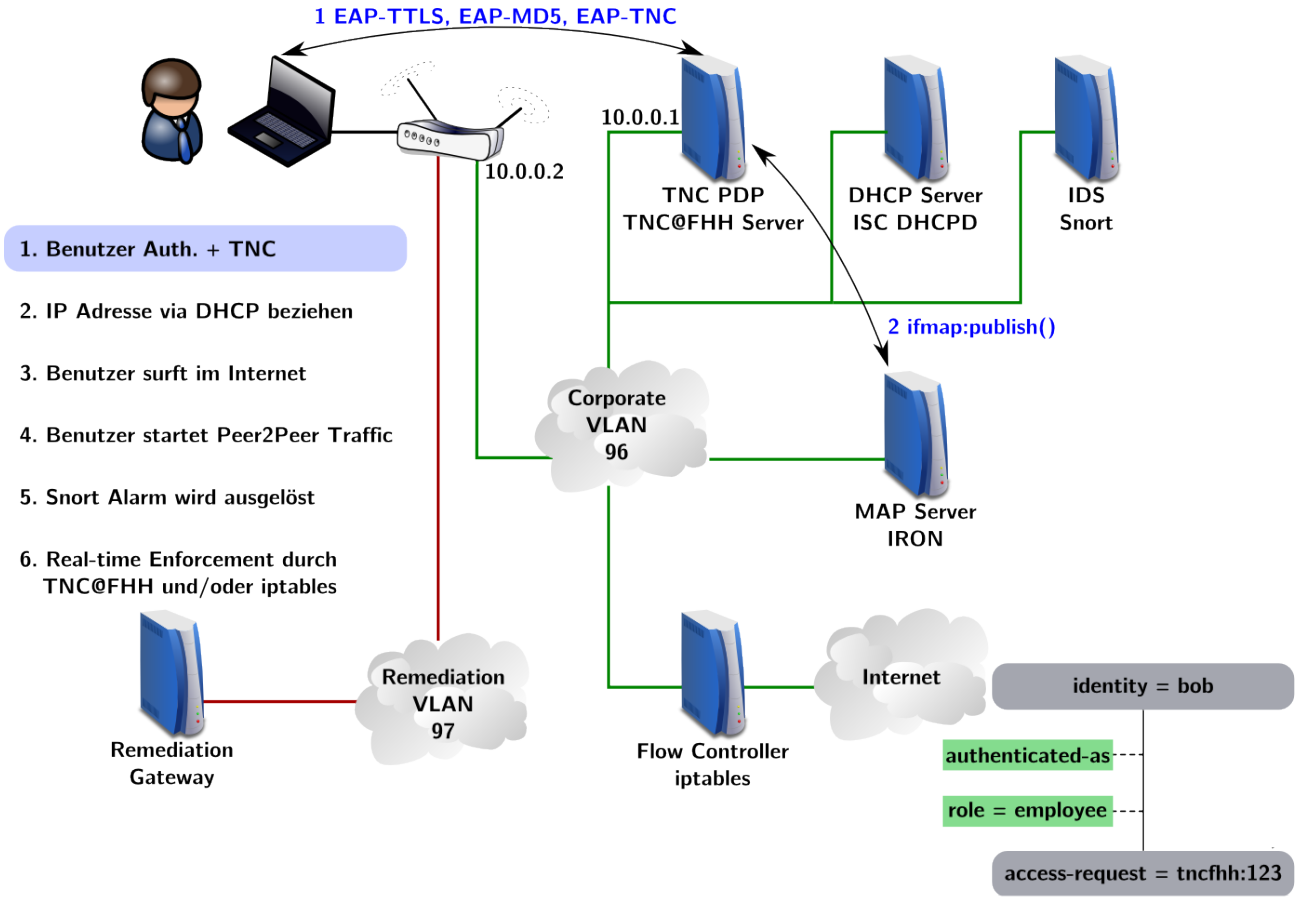
Use Case 1: Identity-Awareness

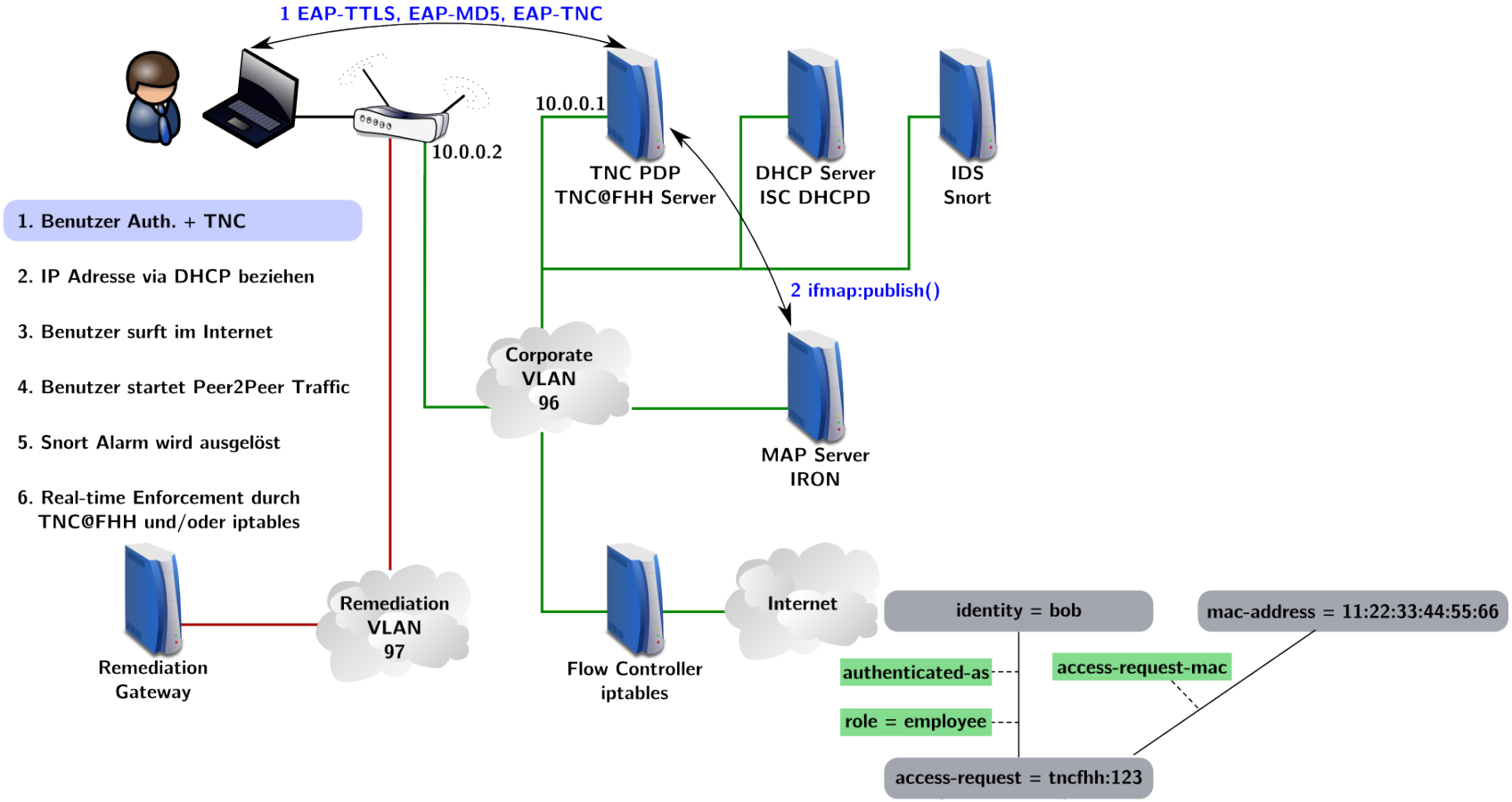
- Benutzer erhält Zugriff auf LAN
- Paket Filter erlaubt Zugriff auf Internet basierend auf Benutzeridentität

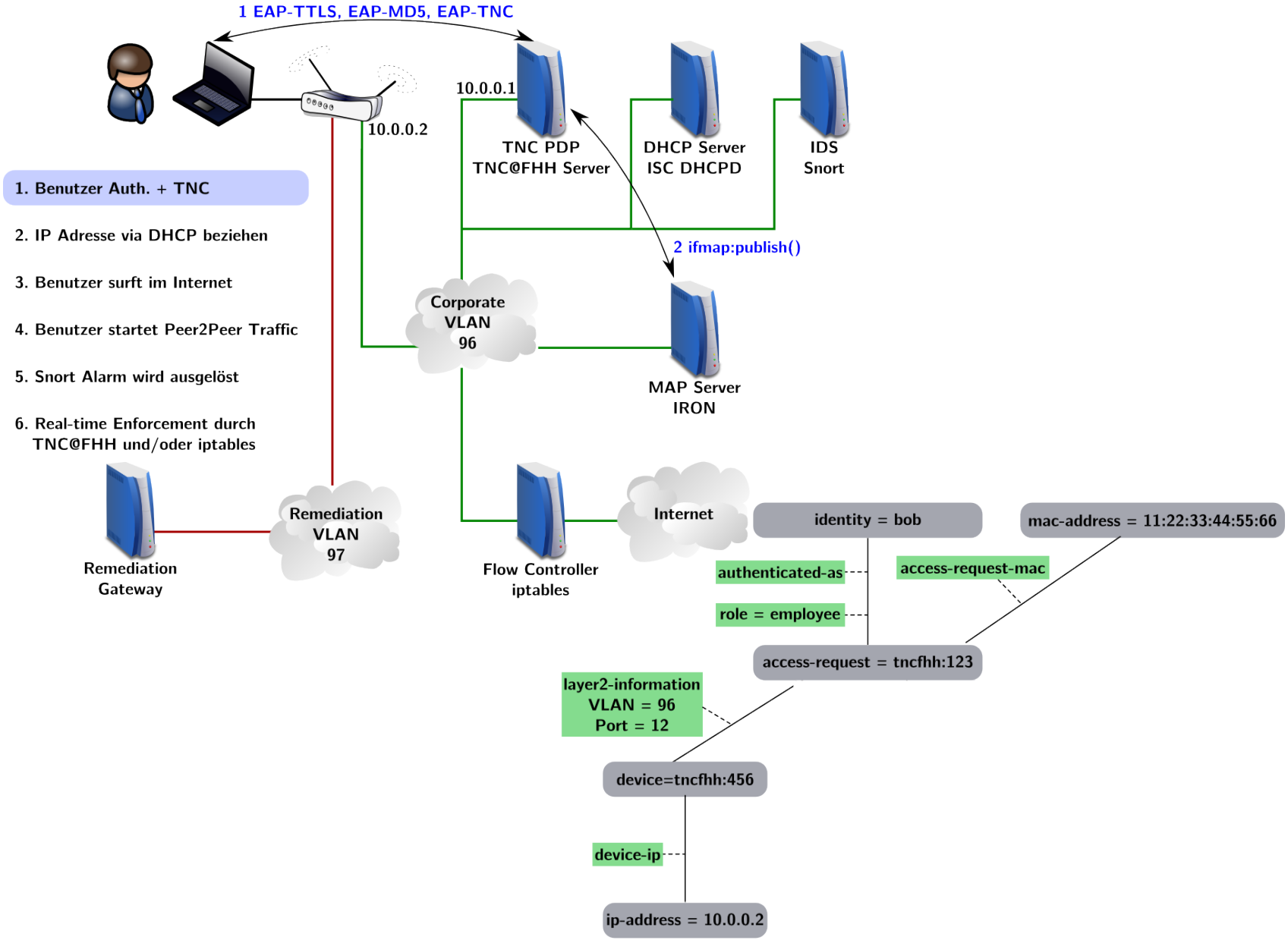
Use Case 2: Real-Time Enforcement

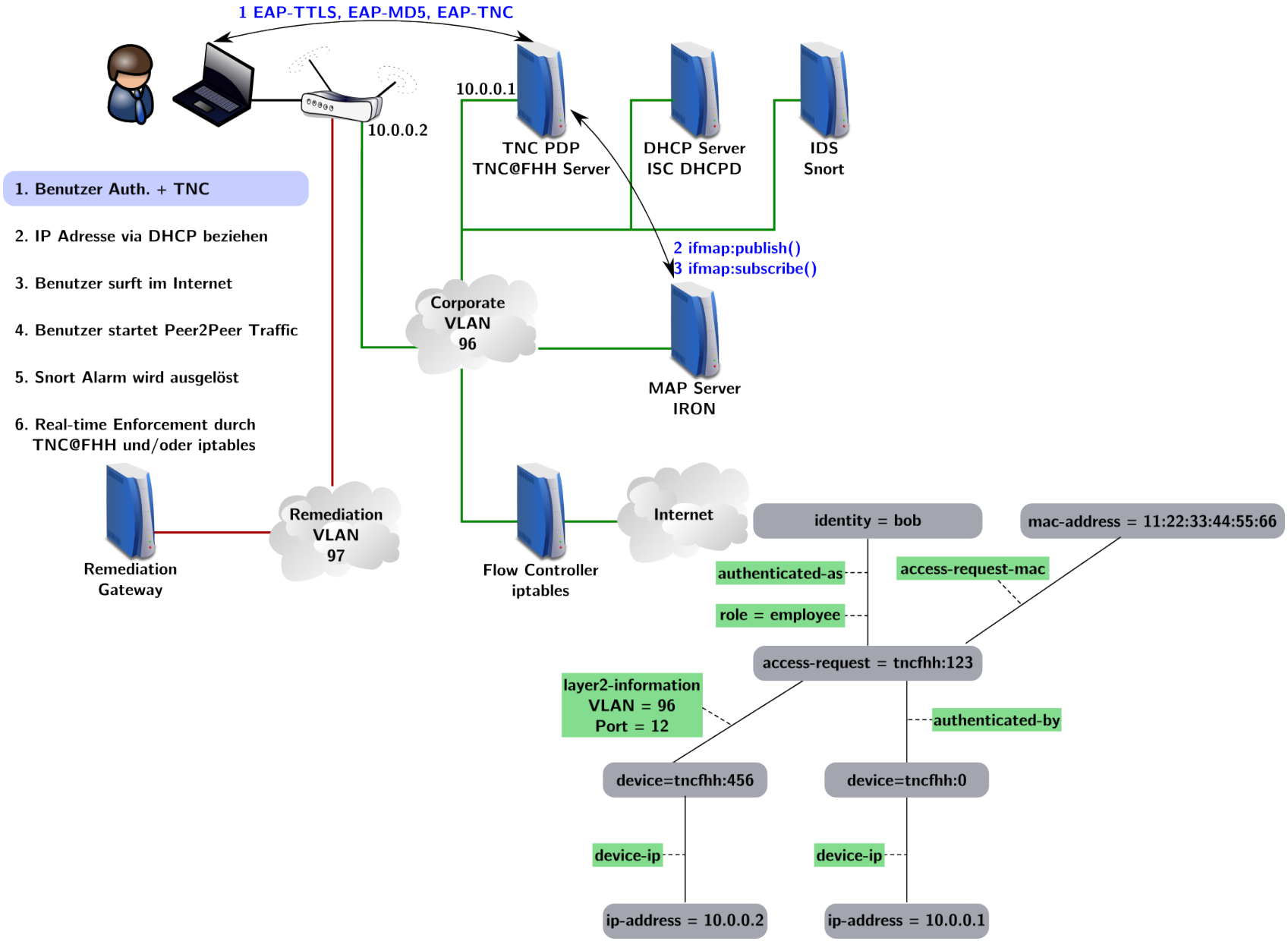
- Benutzer verstößt gegen lokale Policy (p2p Traffic)
- Automatische Isolation des Endgerätes

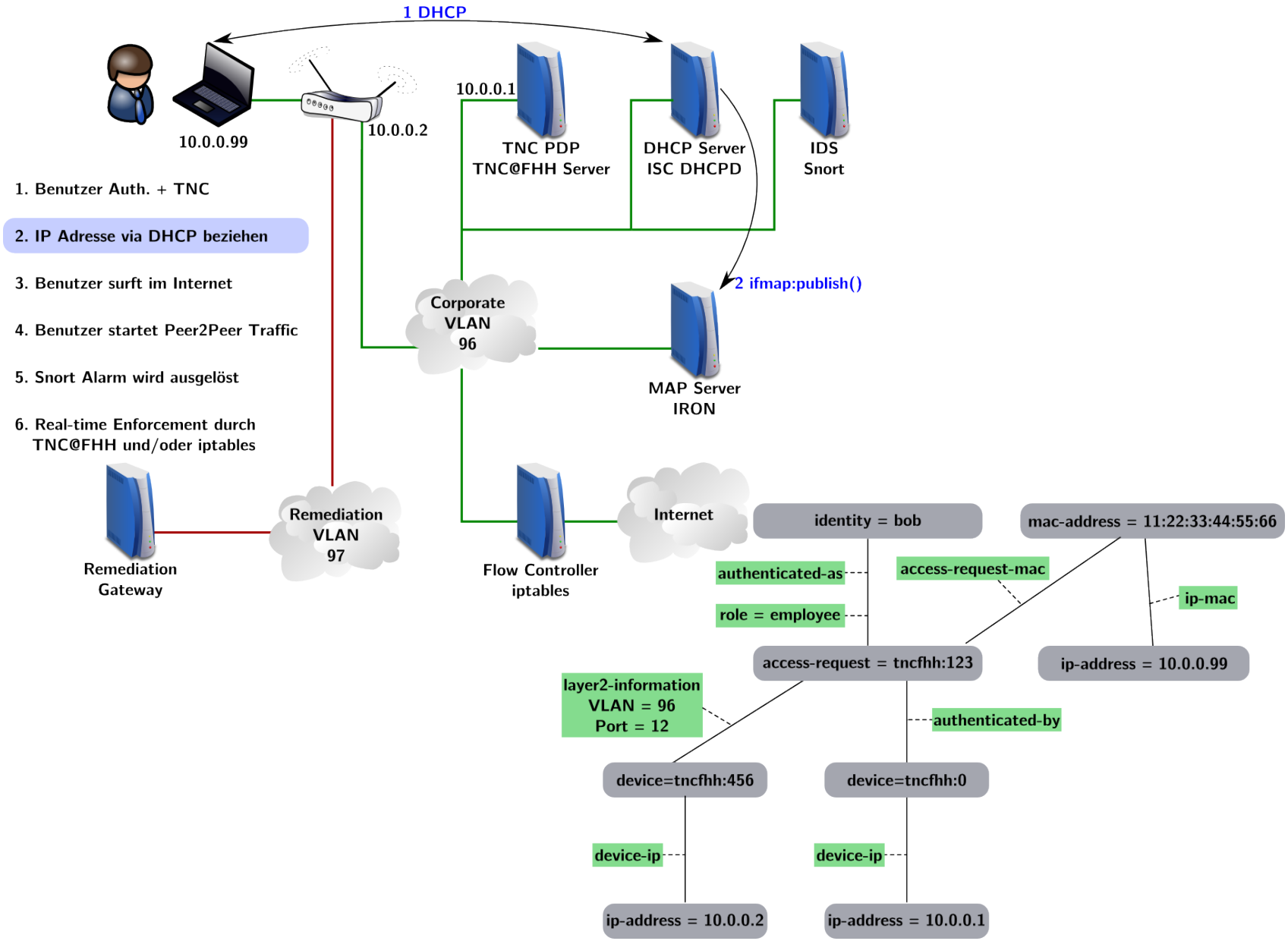

10.0.0.1
10.0.0.2
TNC PDP
TNC@FHH Server
DHCP Server
ISC DHCPD
IDS
Snort
1. Benutzer Auth. + TNC
2. IP Adresse via DHCP beziehen
3. Benutzer surft im Internet
4. Benutzer startet Peer2Peer Traffic
5. Snort Alarm wird ausgelöst
6. Real-time Enforcement durch
TNC@FHH und/oder iptables
Corporate
VLAN
96
MAP Server
IRON
Remediation
VLAN
97
Internet
Remediation
Gateway
Flow Controller
iptables

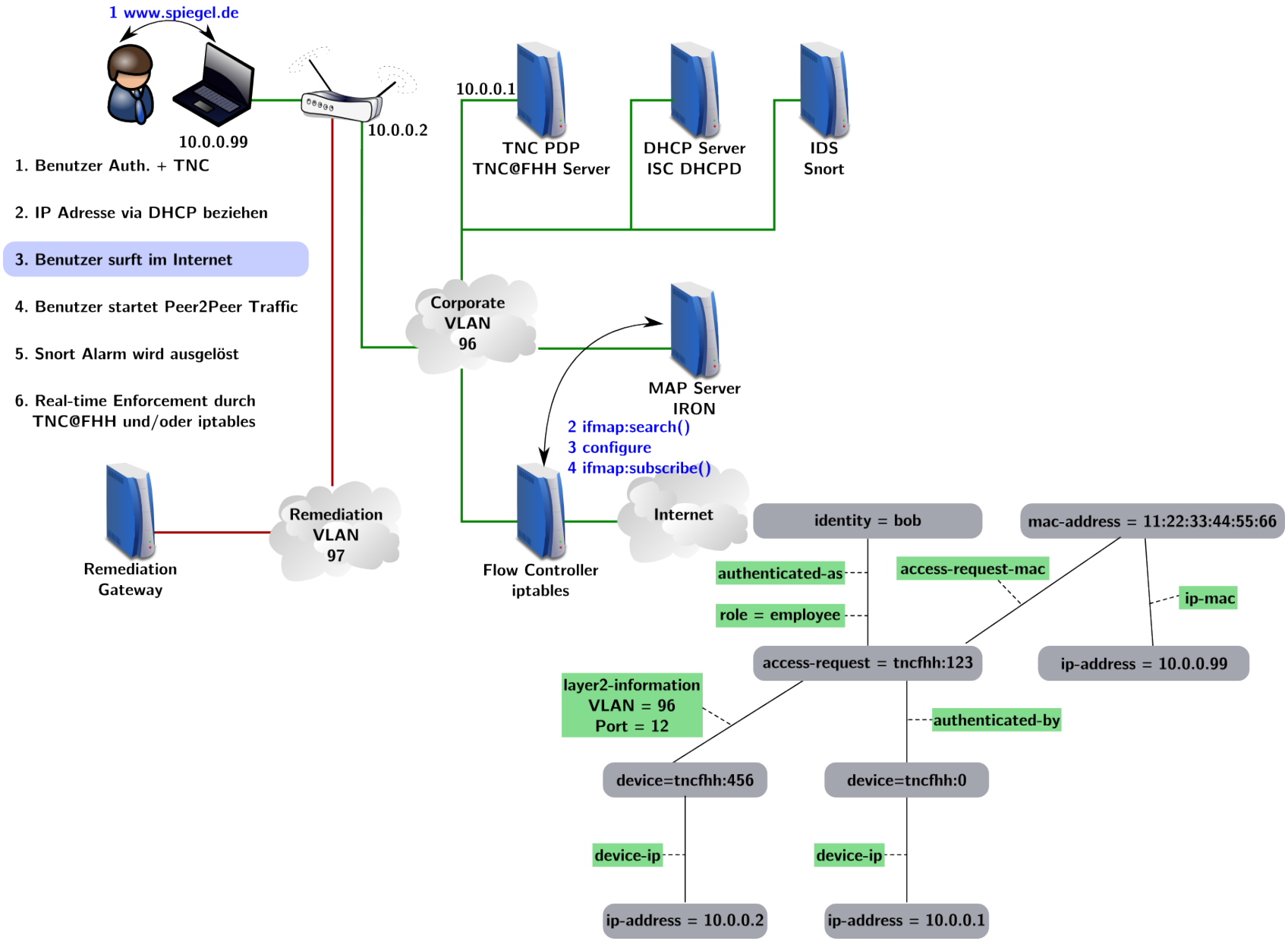

1 EAP-TTLS, EAP-MD5, EAP-TNC
10.0.0.1
10.0.0.2
TNC PDP
TNC@FHH Server
DHCP Server
ISC DHCPD
IDS
Snort
1. Benutzer Auth. + TNC
2. IP Adresse via DHCP beziehen
3. Benutzer surft im Internet
4. Benutzer startet Peer2Peer Traffic
5. Snort Alarm wird ausgelöst
6. Real-time Enforcement durch TNC@FHH und/oder iptables
2 ifmap:publish()
Corporate
VLAN
96
MAP Server
IRON
Remediation
VLAN
97
Remediation
Gateway
Flow Controller
iptables
Internet
identity = bob
authenticated-as
role = employee
access-request = tncfhh:123

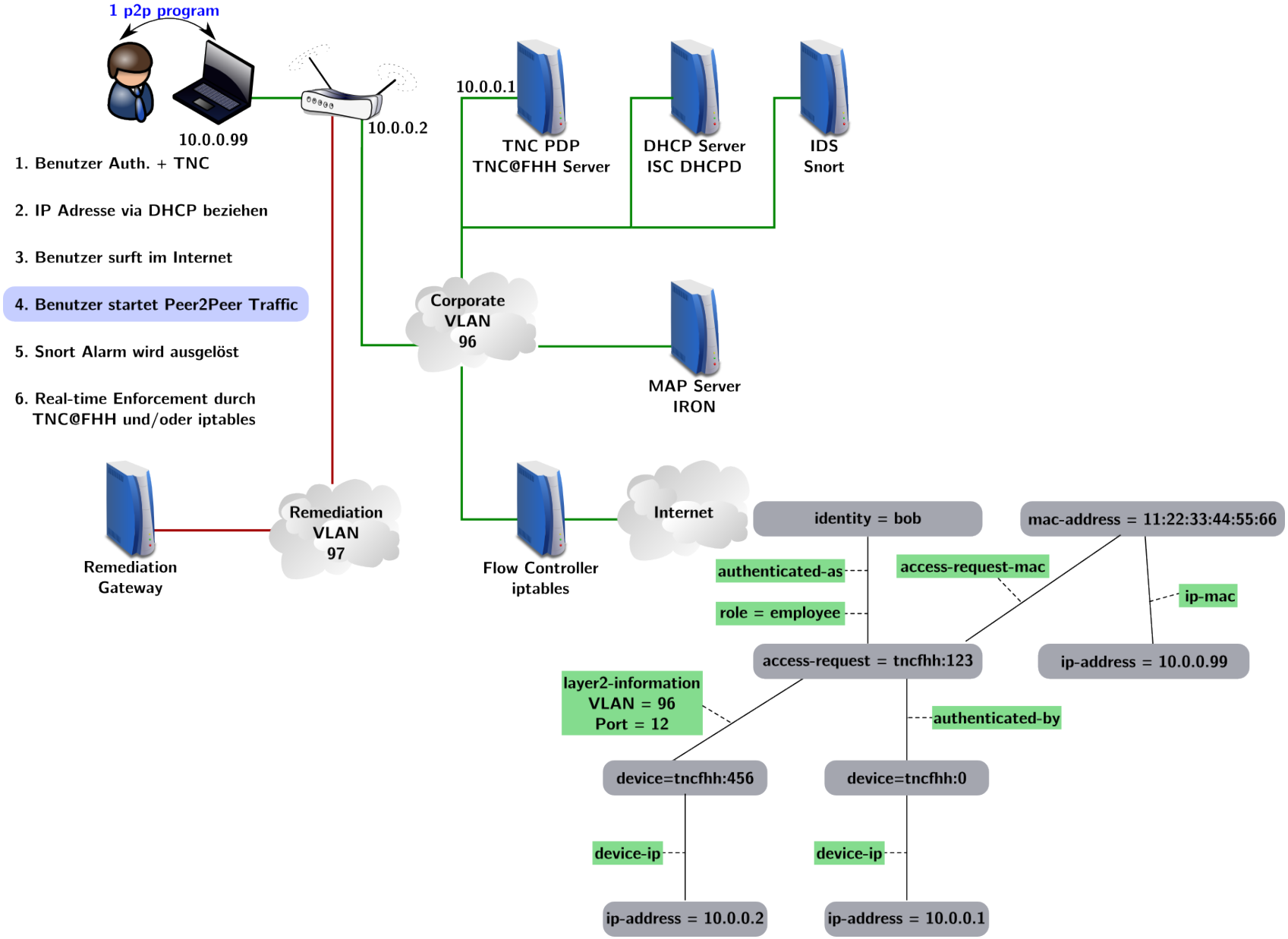

1 EAP-TTLS, EAP-MD5, EAP-TNC
10.0.0.1
10.0.0.2
TNC PDP
TNC@FHH Server
DHCP Server
ISC DHCPD
IDS
Snort
1. Benutzer Auth. + TNC
2. IP Adresse via DHCP beziehen
3. Benutzer surft im Internet
4. Benutzer startet Peer2Peer Traffic
5. Snort Alarm wird ausgelöst
6. Real-time Enforcement durch TNC@FHH und/oder iptables
2 ifmap:publish()
Corporate VLAN 96
MAP Server
IRON
Remediation Gateway
Remediation VLAN 97
Flow Controller
iptables
Internet
identity = bob
mac-address = 11:22:33:44:55:66
authenticated-as
access-request-mac
role = employee
access-request = tncfhh:123

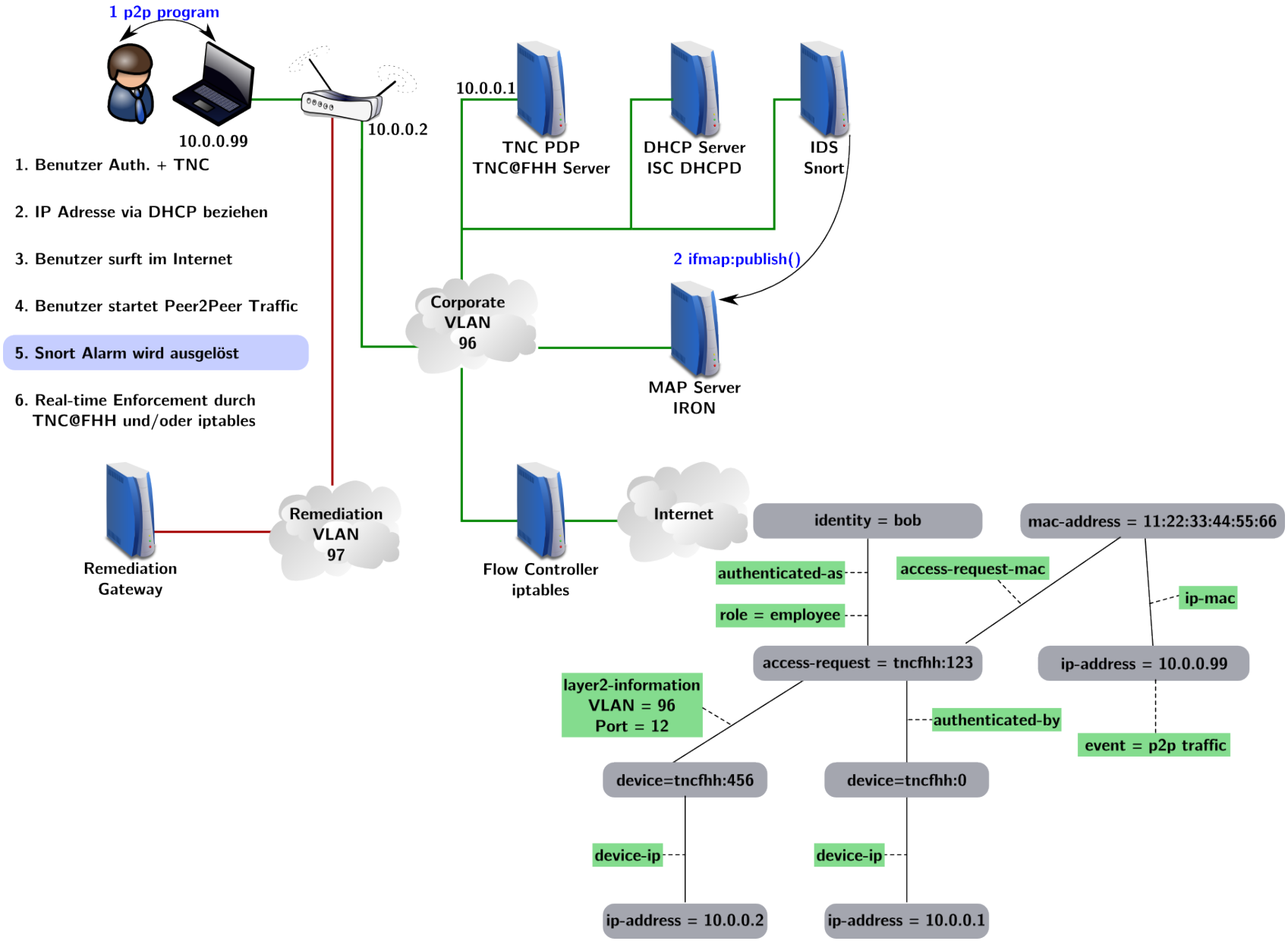

1 EAP-TTLS, EAP-MD5, EAP-TNC
10.0.0.1
10.0.0.2
TNC PDP
TNC@FHH Server
DHCP Server
ISC DHCPD
IDS
Snort
1. Benutzer Auth. + TNC
2. IP Adresse via DHCP beziehen
3. Benutzer surft im Internet
4. Benutzer startet Peer2Peer Traffic
5. Snort Alarm wird ausgelöst
6. Real-time Enforcement durch TNC@FHH und/oder iptables
2 ifmap:publish()
Corporate VLAN 96
MAP Server
IRON
Remediation Gateway
Remediation VLAN 97
Flow Controller
iptables
Internet
identity = bob
mac-address = 11:22:33:44:55:66
authenticated-as
access-request-mac
role = employee
access-request = tncfhh:123
layer2-information
VLAN = 96
Port = 12
device=tncfhh:456
device-ip
ip-address = 10.0.0.2

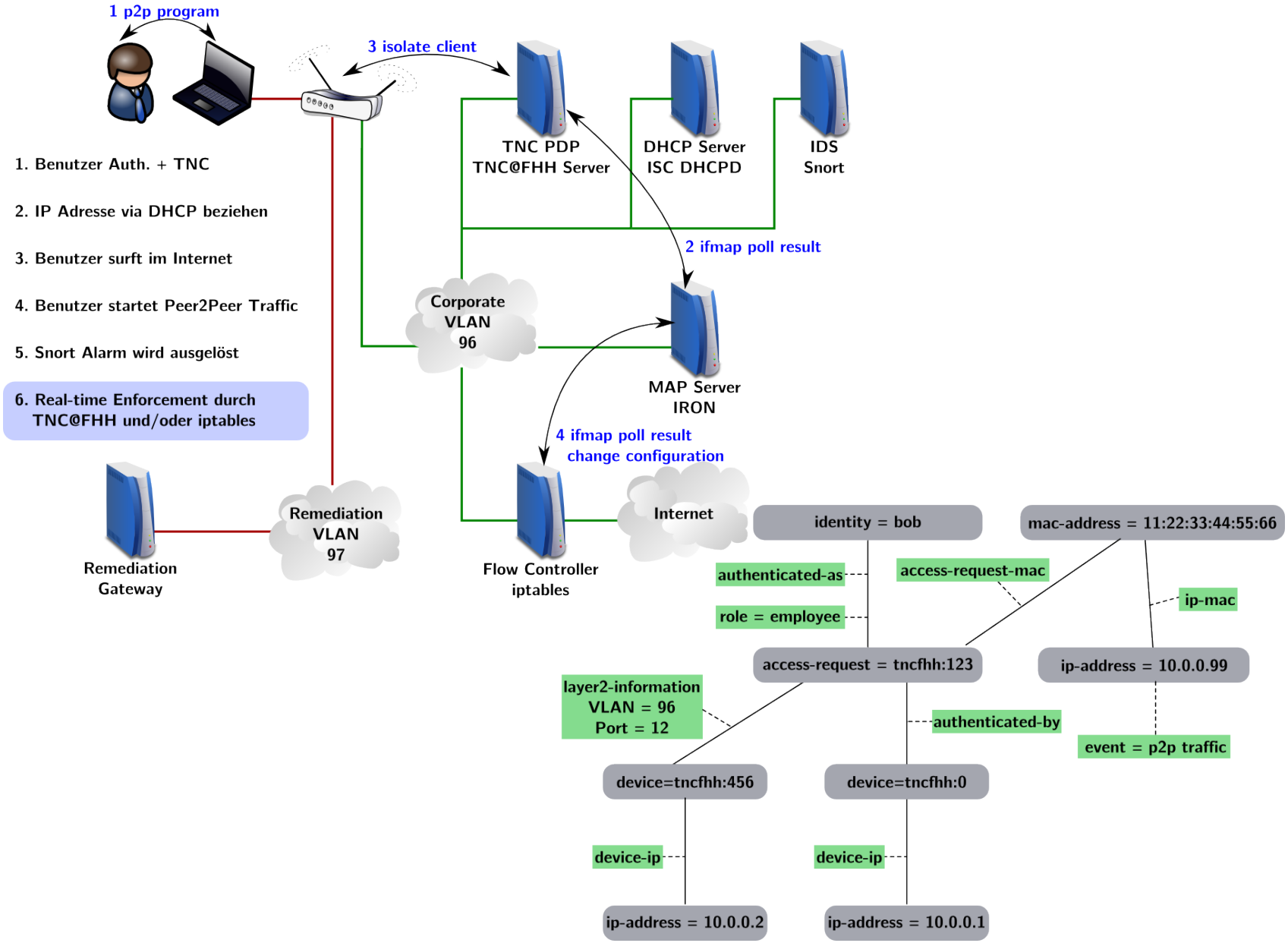

1 EAP-TTLS, EAP-MD5, EAP-TNC
10.0.0.1
10.0.0.2
TNC PDP
TNC@FHH Server
DHCP Server
ISC DHCPD
IDS
Snort
1. Benutzer Auth. + TNC
2. IP Adresse via DHCP beziehen
3. Benutzer surft im Internet
4. Benutzer startet Peer2Peer Traffic
5. Snort Alarm wird ausgelöst
6. Real-time Enforcement durch TNC@FHH und/oder iptables
2 ifmap:publish()
3 ifmap:subscribe()
Corporate VLAN 96
MAP Server
IRON
Remediation VLAN 97
Remediation Gateway
Flow Controller
iptables
Internet
identity = bob
mac-address = 11:22:33:44:55:66
authenticated-as
access-request-mac
role = employee
access-request = tncfhh:123
layer2-information
VLAN = 96
Port = 12
authenticated-by
device=tncfhh:456
device=tncfhh:0
device-ip
device-ip
ip-address = 10.0.0.2
ip-address = 10.0.0.1


1 DHCP
10.0.0.99
10.0.0.2
10.0.0.1
TNC PDP
TNC@FHH Server
DHCP Server
ISC DHCPD
IDS
Snort
1. Benutzer Auth. + TNC
2. IP Adresse via DHCP beziehen
3. Benutzer surft im Internet
4. Benutzer startet Peer2Peer Traffic
5. Snort Alarm wird ausgelöst
6. Real-time Enforcement durch TNC@FHH und/oder iptables
2 ifmap:publish()
Corporate VLAN 96
MAP Server IRON
Remediation VLAN 97
Remediation Gateway
Flow Controller iptables
Internet
identity = bob
mac-address = 11:22:33:44:55:66
authenticated-as
access-request-mac
role = employee
ip-mac
access-request = tncfhh:123
ip-address = 10.0.0.99
layer2-information VLAN = 96 Port = 12
authenticated-by
device=tncfhh:456
device=tncfhh:0
device-ip
device-ip
ip-address = 10.0.0.2
ip-address = 10.0.0.1


1 www.spiegel.de
10.0.0.99
10.0.0.2
10.0.0.1
TNC PDP
TNC@FHH Server
DHCP Server
ISC DHCPD
IDS
Snort
1. Benutzer Auth. + TNC
2. IP Adresse via DHCP beziehen
3. Benutzer surft im Internet
4. Benutzer startet Peer2Peer Traffic
5. Snort Alarm wird ausgelöst
6. Real-time Enforcement durch TNC@FHH und/oder iptables
Corporate VLAN 96
MAP Server IRON
2 ifmap:search()
3 configure
4 ifmap:subscribe()
Remediation VLAN 97
Remediation Gateway
Flow Controller iptables
Internet
identity = bob
mac-address = 11:22:33:44:55:66
authenticated-as
access-request-mac
role = employee
ip-mac
access-request = tncfhh:123
ip-address = 10.0.0.99
layer2-information VLAN = 96 Port = 12
authenticated-by
device=tncfhh:456
device=tncfhh:0
device-ip
device-ip
ip-address = 10.0.0.2
ip-address = 10.0.0.1


1 p2p program
10.0.0.99
10.0.0.2
10.0.0.1
TNC PDP
TNC@FHH Server
DHCP Server
ISC DHCPD
IDS
Snort
1. Benutzer Auth. + TNC
2. IP Adresse via DHCP beziehen
3. Benutzer surft im Internet
4. Benutzer startet Peer2Peer Traffic
5. Snort Alarm wird ausgelöst
6. Real-time Enforcement durch TNC@FHH und/oder iptables
Corporate VLAN 96
MAP Server
IRON
Remediation VLAN 97
Remediation Gateway
Flow Controller
iptables
Internet
identity = bob
mac-address = 11:22:33:44:55:66
authenticated-as
access-request-mac
role = employee
ip-mac
access-request = tncfhh:123
ip-address = 10.0.0.99
layer2-information
VLAN = 96
Port = 12
authenticated-by
device=tncfhh:456
device=tncfhh:0
device-ip
device-ip
ip-address = 10.0.0.2
ip-address = 10.0.0.1


1 p2p program
10.0.0.99
10.0.0.2
10.0.0.1
TNC PDP
TNC@FHH Server
DHCP Server
ISC DHCPD
IDS
Snort
2 ifmap:publish()
1. Benutzer Auth. + TNC
2. IP Adresse via DHCP beziehen
3. Benutzer surft im Internet
4. Benutzer startet Peer2Peer Traffic
5. Snort Alarm wird ausgelöst
6. Real-time Enforcement durch TNC@FHH und/oder iptables
Corporate VLAN 96
MAP Server
IRON
Remediation VLAN 97
Remediation Gateway
Flow Controller
iptables
Internet
identity = bob
mac-address = 11:22:33:44:55:66
authenticated-as
access-request-mac
role = employee
ip-mac
access-request = tncfhh:123
ip-address = 10.0.0.99
layer2-information
VLAN = 96
Port = 12
authenticated-by
event = p2p traffic
device=tncfhh:456
device=tncfhh:0
device-ip
device-ip
ip-address = 10.0.0.2
ip-address = 10.0.0.1


1 p2p program
3 isolate client
TNC PDP
TNC@FHH Server
DHCP Server
ISC DHCPD
IDS
Snort
1. Benutzer Auth. + TNC
2. IP Adresse via DHCP beziehen
3. Benutzer surft im Internet
4. Benutzer startet Peer2Peer Traffic
5. Snort Alarm wird ausgelöst
6. Real-time Enforcement durch TNC@FHH und/oder iptables
2 ifmap poll result
Corporate VLAN 96
MAP Server IRON
4 ifmap poll result
change configuration
Remediation VLAN 97
Remediation Gateway
Flow Controller iptables
Internet
identity = bob
mac-address = 11:22:33:44:55:66
authenticated-as
access-request-mac
role = employee
ip-mac
access-request = tncfhh:123
ip-address = 10.0.0.99
layer2-information
VLAN = 96
Port = 12
authenticated-by
event = p2p traffic
device=tncfhh:456
device=tncfhh:0
device-ip
device-ip
ip-address = 10.0.0.2
ip-address = 10.0.0.1

Stand der aktuellen Implementierung

- MAP Server
  - funktional vollständig (fast ...)
  - aktuelles Arbeitspaket: Subscriptions
- MAP Clients
  - publish mit *echten* Daten
  - rudimentäre search Anfragen
  - aktuelles Arbeitspaket: Subscriptions

Gliederung

Forschungsbedarf: IF-MAP++

Metadaten-Vokabularien

- Use Cases fokussiert auf Netzwerke/Sicherheit

Korrelations-Algorithmen

- Herausforderung: Korrekte Auswertung großer Metadaten-Graphen

Interdomain MAP

- Kommunikation zwischen MAP-Server verschiedener Domänen

Sicherheit und Beherrschbarkeit von IF-MAP?

- MAP-Komponenten selbst als Angriffsziel

Gliederung

Zusammenfassung

- Aktuelle Sicherheitsmechanismen arbeiten isoliert voneinander.
- IF-MAP ist ein Ansatz zur Integration beliebiger Netzkomponenten.
- IRON ist eine Open-Source Referenzimplementierung einer IF-MAP Infrastruktur.

- Ausblick
  - IF-MAP++ Forschungsbedarf notwendig.
  - Beherrschbarkeit/Auswirkungen von IF-MAP noch unklar.

Vielen Dank!

Fragen?