



# ARCHITECT'S GUIDE: Mobile Security Using TNC Technology

---

December 2011

Trusted Computing Group  
3855 SW 153rd Drive  
Beaverton, OR 97006  
Tel (503) 619-0562  
Fax (503) 644-6708

[admin@trustedcomputinggroup.org](mailto:admin@trustedcomputinggroup.org)  
[www.trustedcomputinggroup.org](http://www.trustedcomputinggroup.org)

## Executive Summary and Action Items

**Mobility** means empowering staff to work when and where they want, not just when they are chained to their desk. The traditional desktop computer is no longer the center of the end-user's universe. Staff are using laptops, smart phones, and tablets in the office, at home, and on the road.

**Mobile Security** means managing access to corporate networks to maximize the value to staff, contractors, and even guests with mobile devices, while minimizing risk to the organization.

Both commercial and open source developers have embraced technology from the Trusted Computing Group's (TCG's) Trusted Network Connect (TNC) work group to build products ideally suited for implementing mobile security.

This Architect's Guide shows enterprise security architects how they can design and deploy successful mobile security solutions based on the open TNC architecture and standards.

## Critical strategies for architects include:

1. **Use a unified approach to mobile security.** Define access control policy, user authentication, and device compliance checks once, not for every access scenario. Enforce policies with re-usable tools, and focus on solutions that handle the entire universe of mobile security.
2. **Minimize special cases.** When considering mobile security, try to treat every type of user and every type of access consistently and within the same policy enforcement universe.
3. **Push access control enforcement as close to the end user as possible.** In-line enforcement close to the point of attachment gives fullest control and offers the best security.
4. **Trust, but verify.** Integrate profiling and IPS tools into mobile security solutions. This places additional layers of defense between mobile users and critical corporate assets.

## Introduction

The most valuable organizational workers have moved away from the desk and cubicle and towards collaborative teams, “work anywhere” attitudes, and a focus on the customer. Network managers are being bombarded by requests for mobile access to corporate networks, not just using corporate laptops but other mobile devices, such as smart phones and tablets.

Mobile security requires giving managed and unmanaged devices anytime/anywhere access to corporate resources, but securely and in a controlled fashion. Mobile security extends the trust boundary in the network to the end user, whether they are at their desk, in the company cafeteria, or on some wireless hotspot in Ouagadougou.

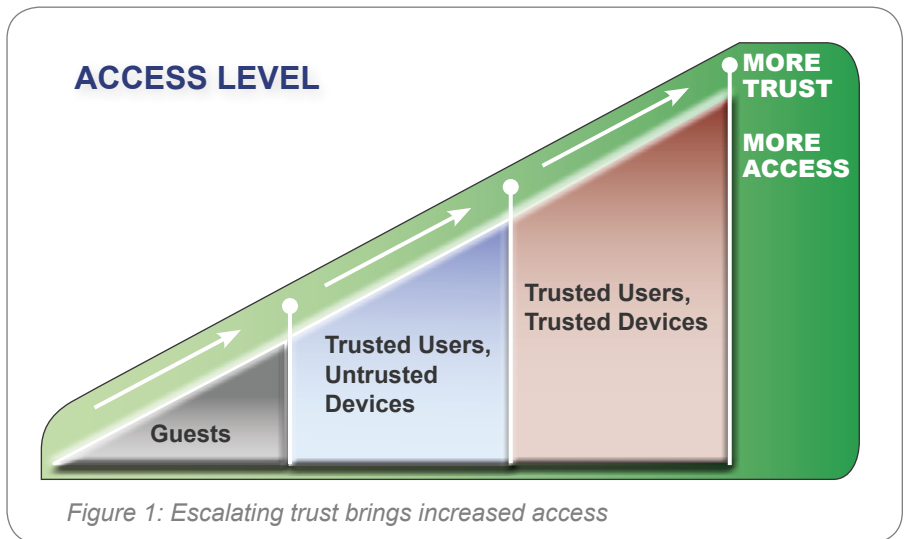
Technology from the Trusted Computing Group’s Trusted Network Connect (TNC) work group has been used by commercial vendors and open source developers to build a rich ecosystem of products, ideal for implementing mobile security in enterprise networks. Network managers can combine requirements for user authentication and endpoint integrity checking when writing access control rules to protect enterprise resources. The result is a win-win for all involved: end users are happy they can get their jobs done with minimum friction and frustration, while network and security teams are confident they are maintaining strict controls on network access and security of valuable enterprise systems.

TNC technologies are designed to help implement mobile security but they can also work with other TCG tools such as the TPM (Trusted Platform Module), which provides device identification and assists in device integrity checking, and TCG’s self-encrypting disk drive technology, which pushes encryption and access control technology within the hardware of the drive.

This Architect’s Guide gives a basic framework for mobile security based on industry-standard TNC technologies from the Trusted Computing Group. Network designers can use this as a starting point for their own deployment, and can see best practices learned from over five years of real-world deployment of network access control in organizational networks.

## Solution Overview

The solution in this Architect’s Guide is based on a simple requirements statement: **escalating trust brings increased access**. In Figure 1, different users are given different levels of access to corporate resources based on their trust. Guests, almost completely untrusted, get virtually no access. Trusted users with trusted devices (such as managed corporate laptops) are given the most access. In between are users at different levels of trust, such as staff with unmanaged devices such as smart phones, or contractors who should have only “need to know” access.



An important part of this solution is a unified approach to mobile security. Using a combination of international and industry standards, network managers can design and deploy solutions that provide seamless mobile services to users on the enterprise campus and while traveling. By re-using policy and enforcement elements across different networks and devices, security architects can mitigate the risk of something “falling through the cracks” with inconsistent application of policy, and reduce opportunities for human error.

## WHERE IS THE USER?

| SCENARIOS                                | CORPORATE CAMPUS  | OFF-CAMPUS (Home & Public Wi-Fi)   |
|--|---|--|
| Trusted User and Trusted Device          | User has full access as needed to enterprise network and Internet         | User has full access as needed to enterprise network, over secure connection, and Internet |
| Authenticated User, but Untrusted Device | User has restricted access to enterprise network, full access to Internet | User has restricted access to enterprise network, full access to Internet                  |
| Guest                                    | Internet access   | [does not apply]   |

## Elements of a Unified Solution

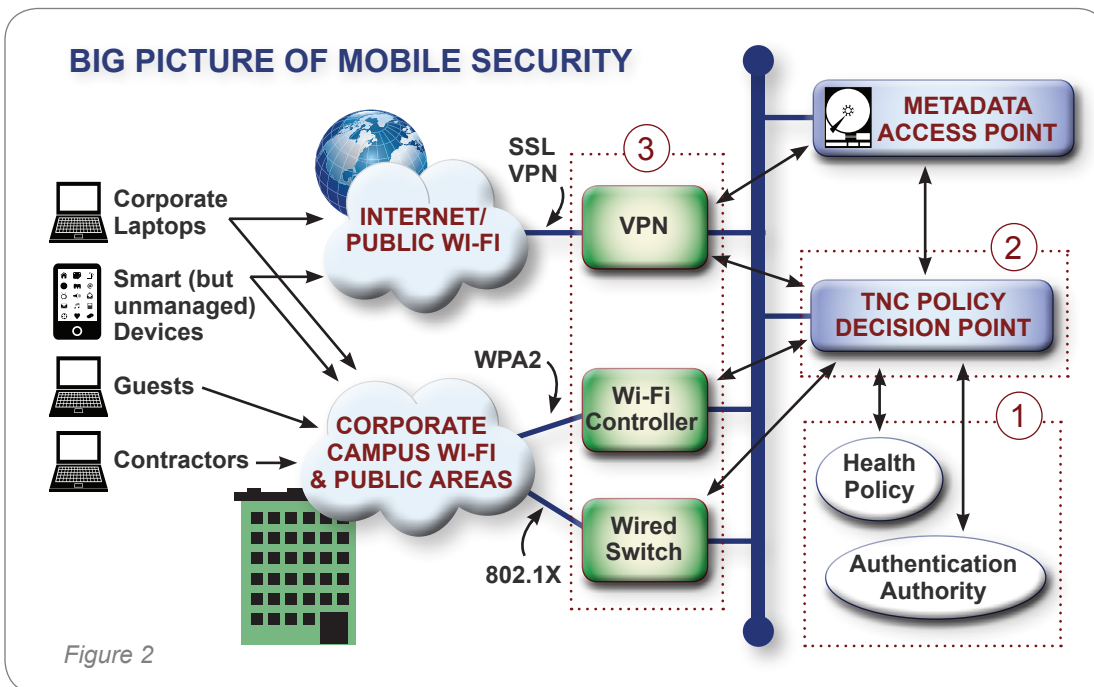


Figure 2

Any mobile security solution depends on three critical elements: user authentication and device compliance checks ①, policy evaluation ②, and access control enforcement ③. (See Figure 2.) In a unified solution, these elements can be assembled using off-the-shelf components, providing interoperability, scalability, and reusability. Solutions based on the TNC framework can take advantage of both protocols for mobile security as well as APIs between elements, resulting in a flexible design that can grow as needed.

① **User authentication and device compliance checks** are the first elements needed. Enterprises have long embraced centralized authentication and authorization systems, such as Windows Active Directory, so integrating these into mobile security designs is a clear goal. But checking user identity is often only one half of the problem; even trusted users can inadvertently bring viruses, and their malevolent behavior, from foreign networks. This makes health checks based on enterprise end-point security tools just as important, especially with highly-connected (and highly-attacked) laptops. Device health checks can include platform checks (such as particular mobile devices or operating system versions) as well as platform-specific checks, such as differentiating between user-provided Windows laptops and corporate managed Windows laptops. A key strategy here is to match the checks and access against the risk level presented by the platform. Treating mobile phones differently from laptops is a good risk management decision.

② Moving **policy evaluation** into Policy Decision Points separate from the enforcement points provides scalability and consistency in mobile solutions, and handles the network/

security boundary best. While network and security teams can work together, they have fundamentally different vocabularies: VLANs, subnets, and VPN tunnels don't usually map cleanly to security zones, user and group information, and application layer access controls. Separating policy evaluation from access control enforcement offers a critical bridge between network management and security management tools and terminology.

Behavioral profiling is closely related to policy evaluation. Traffic from mobile devices

can be assessed for unauthorized activity, and cause further restrictions in policy enforcement.

---

**A cornerstone of good mobile security solutions is ensuring that access control is pushed out as close to the end-user as possible, and is maintained in-line with the user's connection to the network.**

---

③ **Access control enforcement** in mobile security designs normally requires three separate types of devices to cover three different access methods: wired switches, wireless access points or controllers, and VPN gateways. In some cases, the Policy Enforcement Point is built into the access device and in others a traditional separate firewall is used. Security architects should leverage the capabilities of their existing equipment and only introduce new access control elements when required. A cornerstone of good mobile security solutions is ensuring that access control is pushed out as close to the end-user as possible, and is maintained in-line with the user's connection to the network. By using in-line enforcement mechanisms, security architects are assured that access control can be enforced in all circumstances and that edge cases, such as mobile device users "attacking" each other, are properly handled. At the same time, pushing access control enforcement towards the user ensures that access control occurs as transparently as possible, without requiring special client software or artificial network topologies.

## On Campus: Increasing Trust Brings Increasing Access

In the on-campus wireless environment, the best approach for mobile security is one that properly differentiates users and devices. The more trusted the user and the device, the greater the access. Less trusted devices or less trusted users should be given correspondingly less access to the network. For example, guest users—neither authenticated nor compliance-checked—would likely only have access to the Internet. Trusted users with fully trusted laptops would be on the other extreme, given the same access as you'd expect sitting down at a corporate desktop in someone's office.

This same approach of escalating access based on escalating trust works with easily accessible open wired network connections, such as in corporate conference rooms or other shared spaces.

### A Starting Point: Three Types of Access

The example architecture for mobile security in a campus wireless environment (Figure 3, page 5) shows an easy-to-deploy, but very powerful, configuration. This architectural diagram has been simplified to focus on the critical piece, the policy enforcement point, and the escalating trust model. Other components, such as the policy decision point and health checkers are visible in the “big picture” view (Figure 2, page 3).

This example architecture is based on three types of access:

**Lowest access level:** guest users

**Moderate access:** authenticated users with untrusted devices, such as smart phones or tablets, and

**Greatest network access:** trusted users with trusted devices, such as corporate-managed laptops.

Of course, you could have fewer or more access types, and different types of access, as fits the needs of your organization. For example, it would be very common to have a moderate access category for contractors, who might have fully compliant devices but who are given a lower level of trust than other trusted enterprise users. However, this division into three “buckets” is a very good starting point because it shows how to differentiate based on both authentication information and device trust information.

---

### What is Trusted Network Connect?

TCG's Trusted Network Connect (TNC) network security architecture and open standards enable intelligent policy decisions, dynamic security enforcement, and communication between security systems. TNC standards provide network and endpoint visibility, helping network managers know who and what is on their network, and whether devices are compliant and secure. TNC standards also include network-based access control enforcement—granting or blocking access based on authentication, device compliance, and user behavior. TNC provides pervasive security, Network Access Control (NAC) and interoperability in multi-vendor environments. Support for TNC standards is included in products from over two dozen commercial and open source vendors.

---

Using a combination of TNC-compliant policy enforcement devices with TNC-compliant endpoint security assessment clients, this type of mobile security solution is easy to design and to deploy. In this design, each of the different types of users is able to connect to the network with a minimum of fuss and configuration information, and gets the access they need.

Guest users, for example, will typically have either an unencrypted wireless connection or a “password of the day” WPA-Personal authentication. Guests would typically use a different SSID to connect to the wireless network, which makes differentiating and segmenting them easy, even when wireless is offered over a shared infrastructure. For wired guest users, the lack of any sort of authentication at the Ethernet layer (802.1X) is a signal to the network that this user should be treated as an unauthenticated, untrusted guest.

### USER + DEVICE = ACCESS

| USER AUTHENTICATION | DEVICE TRUST | ACCESS GRANTED  |
|---------------------|--------------|---|
| Authenticated       | Trusted      | “Corporate Laptop” Full access to corporate networks                      |
| Authenticated       | Untrusted    | “Smartphone” Moderate access to corporate networks: Intranet, email, etc. |
| Unauthenticated     | Untrusted    | “Guest” Internet only   |

Corporate users with a personal laptop, with a smart phone, or with a tablet, can use their corporate credentials to authenticate to the network. In the wireless environment, WPA-Enterprise allows them to pass their credentials securely to the network, with simple 802.1X port authentication in the wired environment. Because their device is not trusted, the Policy Decision Point sends a limited set of access controls to the Policy Enforcement Point. The user gets a lower level of access, such as the basic services you'd expect from a personal device: email, some corporate intranet pages, and so on. If the user (or their device) starts to misbehave, then behavior and profiling devices on the network can re-assess their access controls and push out a new set of controls to the Policy Enforcement Point, or move them completely off the corporate network.

Contractors and consultants are another common category. In this case, the user may have a fully-trusted device, but

not be a trusted user—the opposite of a trusted user with a personal device. Security architects can easily differentiate between these two cases and two trust levels if appropriate, giving different levels of role-based access to semi-trusted users with trusted devices.

Fully trusted users, such as corporate staff with enterprise-managed laptops, will have TNC clients which combine authentication and health check information into a single seamless experience. Whether on a wireless network, or a wired connection, the user can be given controlled access to the corporate network. At the same time, the client computing management team knows that endpoint security checks are keeping the laptop (or desktop) in compliance with corporate policy, while the security team knows that any actions the user performs on the corporate network can be tracked back not just to an IP address, but to an authenticated user.

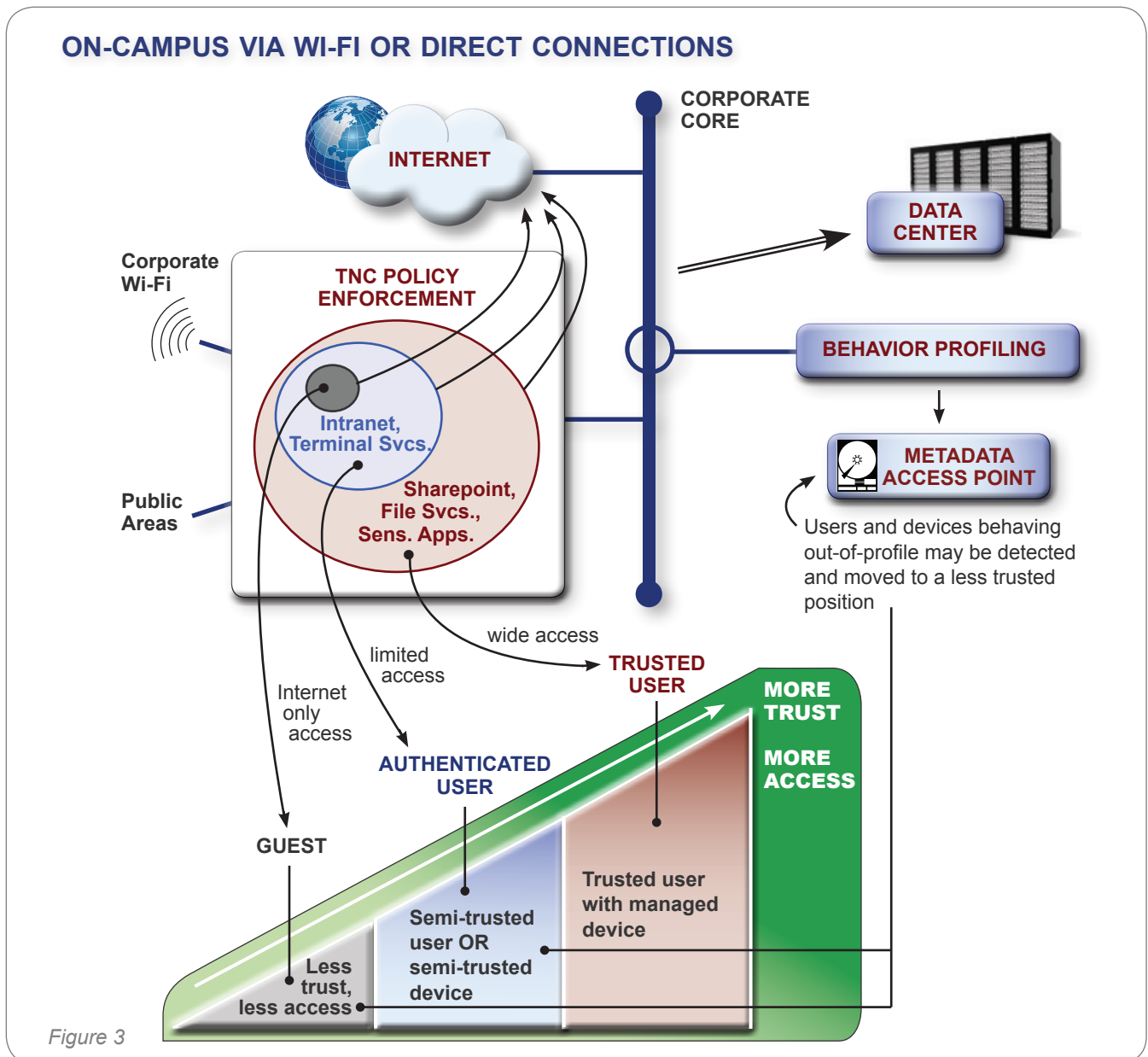
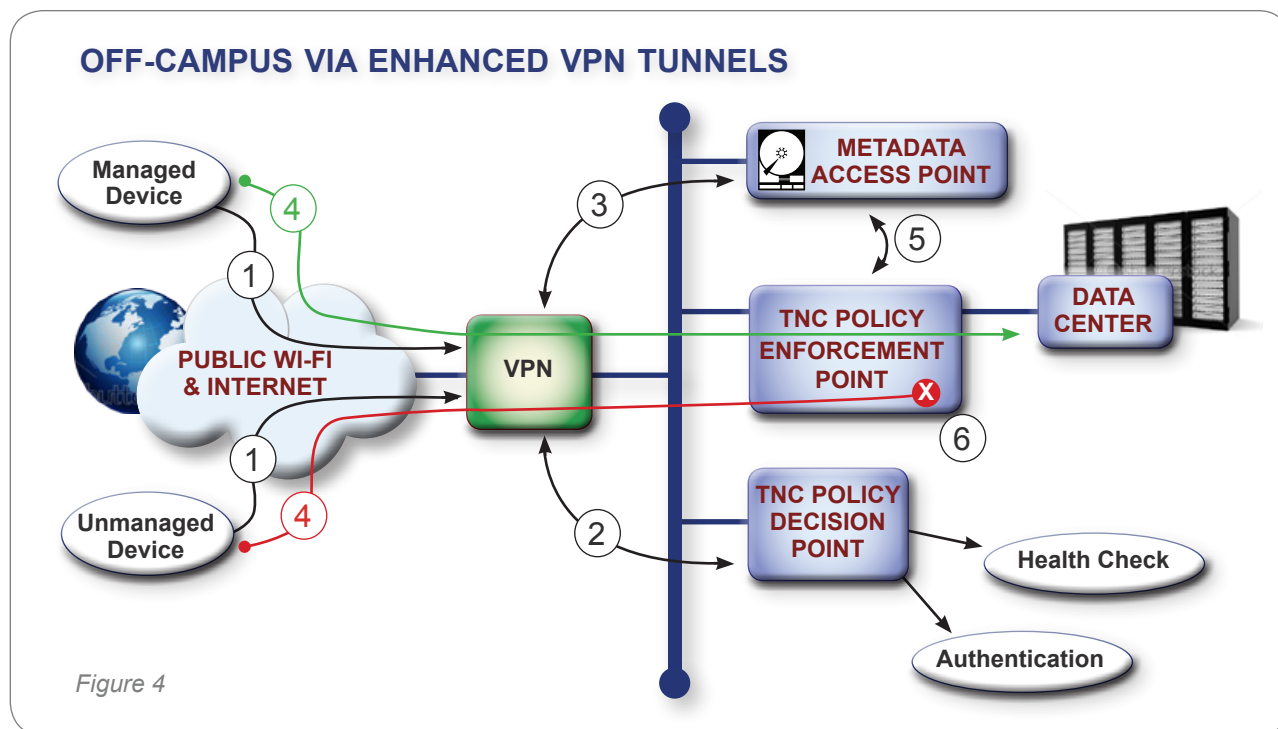


Figure 3

## Off Campus: Enhanced VPN Tunnels Differentiate Devices

A unified mobile security solution uses the same TNC-compatible client, Policy Enforcement Points, Policy Decision Point, compliance check and authentication store, whether the clients are on-campus or off-campus. When users are on public Wi-Fi networks or their home Internet connection, connecting to the enterprise over a secure connection such as a VPN, they have the same experience as when they are on the corporate campus.

In the diagram below, you can trace a connection both from trusted devices (such as corporate laptops) and untrusted devices (such as personal smart phones) as they connect to the corporate network through a VPN concentrator.



### Walking Through Scenarios

- (1) User on trusted or untrusted device connects to corporate VPN concentrator and tries to log in. If the device is TNC-compliant, then information about the platform and the posture of the device is also sent.
- (2) VPN concentrator contacts an authentication server via RADIUS and validates credentials. Access control information (such as user group) is passed back to VPN concentrator to apply proper access controls.
- (3) VPN concentrator updates MAP server using IF-MAP protocol with information on remote user IP and credentials, along with posture health check results.
- (4) Device attempts to go to restricted resource in data center protected by TNC Policy Enforcement Point (PEP).
- (5) TNC PEP contacts the Policy Decision Point (PDP) to retrieve policy. The PDP consults the MAP server to retrieve session information (credentials and roles), determines what policy to apply, and provisions appropriate access controls to the PEP.
- (6) TNC PEP applies appropriate access controls to user traffic based on authenticated credentials and posture check results.