NOVEMBER 2018

# ARCHITECT'S GUIDE

## Portable Device Security Using TNC Technology

Trusted Computing Group
3855 SW 153rd Drive
Beaverton, OR 97003
Tel (503) 619-0505
Fax (503) 644-6708
admin@trustedcomputinggroup.org
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 office computer is no longer the center of the end-user's universe. Staff are using laptops, smart phones, and tablets, not only in the office but also at home and on the road.

**Portable Device Security** means managing access to corporate networks to maximize the value to staff, contractors, and even guests with portable 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 Communications (TNC) work group to build products ideally suited for implementing portable device security.

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

### CRITICAL STRATEGIES FOR ARCHITECTS INCLUDE:

1. USE A UNIFIED APPROACH TO PORTABLE DEVICE SECURITY
2. MINIMIZE SPECIAL CASES
3. PUSH ACCESS CONTROL ENFORCEMENT TO END USER
4. TRUST BUT VERIFY

1. Use a unified approach to portable device 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 portable device security.

2. Minimize special cases. When considering portable device 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 portable device security solutions. This places additional layers of defense between portable device users and critical corporate assets.

### INTRODUCTION

Many 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 portable device access to corporate networks, not just using corporate laptops but also other devices, such as smart phones and tablets.

Portable device security requires giving managed and unmanaged devices anytime/anywhere access to corporate resources, but securely and in a controlled fashion. Portable device 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 TCG's TNC work group has been used by commercial vendors and open source developers to build a rich ecosystem of products, ideal for implementing portable device 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 portable device security but they can also work with other TCG tools such as the Trusted Platform Module (TPM), 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 of the laptop.

This Architect's Guide gives a basic framework for portable device security based on industry-standard TNC technologies from the TCG. Network designers can use this as a starting point for their own deployment and can see best practices learned from over ten 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 the least 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 access to a subset of enterprise resources.

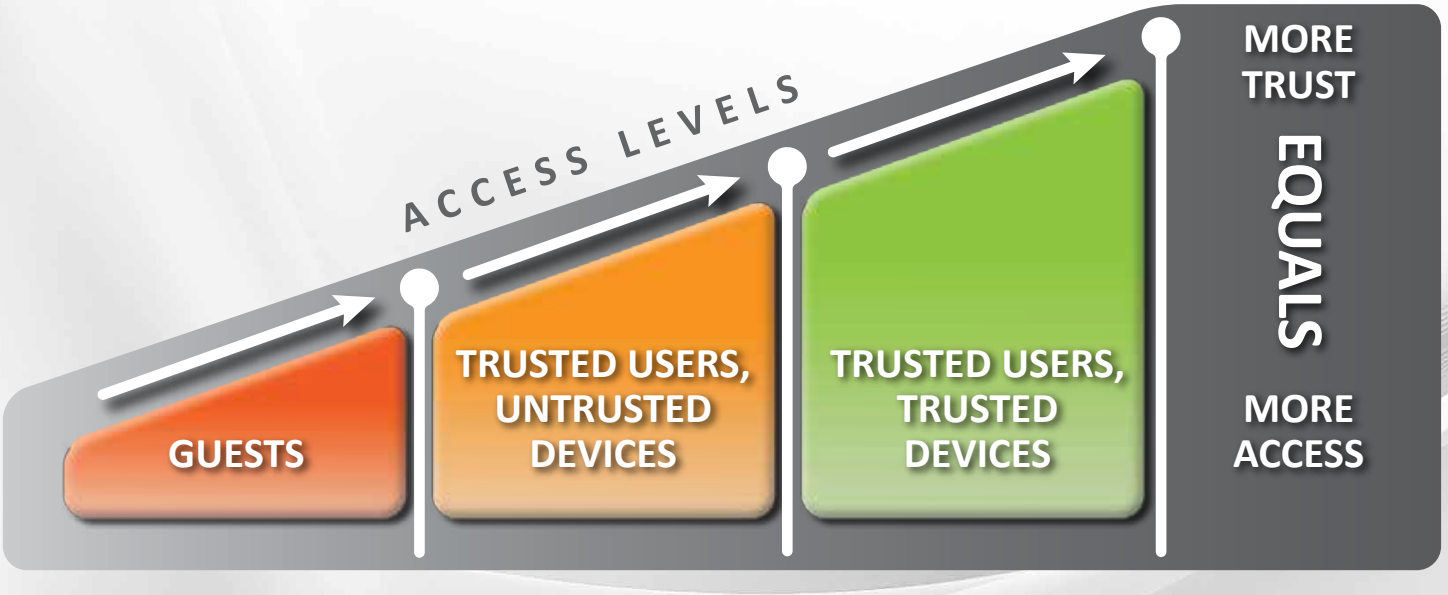


*Figure 1: Escalating trust brings increased access.*

An important part of this solution is a unified approach to portable device security. Using a combination of international and industry standards, network managers can design and deploy solutions that provide seamless portable device 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 | User has full access as needed to enterprise network, over secure connection |
| AUTHENTICATED USER, BUT UNTRUSTED DEVICE | User has restricted access to enterprise network | User has restricted access to enterprise network |
| GUEST | Public-level access | [Does not apply] |

Any portable device security solution depends on four critical elements: (1) user authentication and device compliance checks, (2) policy evaluation, (3) access control enforcement, and (4) data orchestration. (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 portable device security as well as APIs between elements, resulting in a flexible design that can grow as needed.

### ELEMENTS OF A UNIFIED SOLUTION

1. USER AUTHENTICATION AND DEVICE COMPLIANCE CHECKS
2. POLICY EVALUATION
3. ACCESS CONTROL ENFORCEMENT
4. DATA ORCHESTRATION

## THE BIG PICTURE OF MOBILE SECURITY

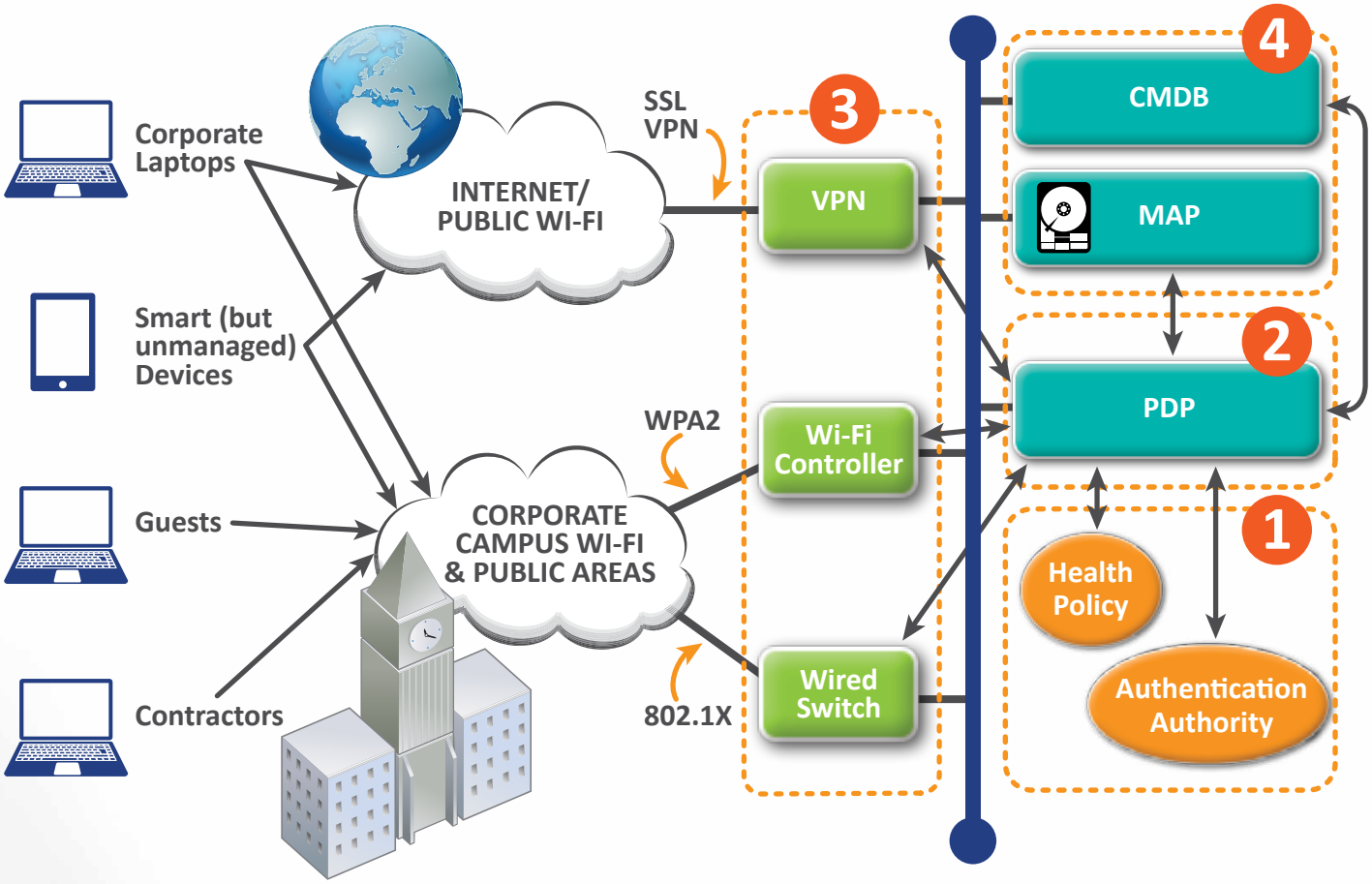


*Figure 2: The Big Picture of mobile security.*

1. **User authentication and device compliance checks** are the first elements needed. Enterprises have long embraced centralized authentication and authorization systems, so integrating these into portable device 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 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 be tuned to reflect the type of platform (e.g., device type or operating system), the role of the user (e.g., contractor or regular staff), and whether the platform is managed or unmanaged.

2. **Access control enforcement** in portable device 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 (PEP) 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 portable device 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 portable device users compromising 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.

 

3. Moving **policy evaluation** into Policy Decision Points (PDP) separate from the enforcement points provides scalability and consistency in portable device solutions and handles the network/security boundary best. Tightly connected decision and enforcement capabilities limit the flexibility enterprises have in their selection of products. By separating these functions into separate devices connected by standard interfaces, enterprises have the power to mix and match products based on their needs. 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 portable devices can be assessed for unauthorized activity and cause further access restrictions due to policy-based enforcement. By having a separate PDP that uses standardized interfaces, input sensors that monitor this sort of behavior can feed into decisions. This allows more sophisticated policies and policy evaluations than possible at any single sensor or enforcement point.

4. **Data Orchestration** in enterprise systems helps ensure that the information collected about endpoints during compliance checks is made available to the tools and processes that can use it. For example, this improves the power and efficiency of the enforcement mechanisms – all tools, including those making enforcement decisions, are working off the same information and thus share the same view of managed devices. This also means that tools can make correlations that might not otherwise be possible. Moreover, at enterprise scales, orchestration may be the only way the necessary volume of data can be effectively collected and managed.

   The Metadata Access Point (MAP) can manage and disseminate collected information about enterprise assets and states in real time, creating a common reference for the current state of connected devices. In addition, long term storage of collected information is supported by the use of a Configuration Management Database (CMDB). This long-term storage supports trending analytics and other evaluations that require more than a single snapshot in time. Between the MAP and CMDB, security tools have access to what they need to know about the state of endpoints and the enterprise.

## ON CAMPUS: INCREASING TRUST BRINGS INCREASING ACCESS

In the on-campus wireless environment, the best approach for portable device 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 public resources. Trusted users with fully trusted device would be on the other extreme, given the same access as one would expect sitting down at a corporate computer 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.

 

## ON-CAMPUS VIA WI-FI OR DIRECT CONNECTIONS

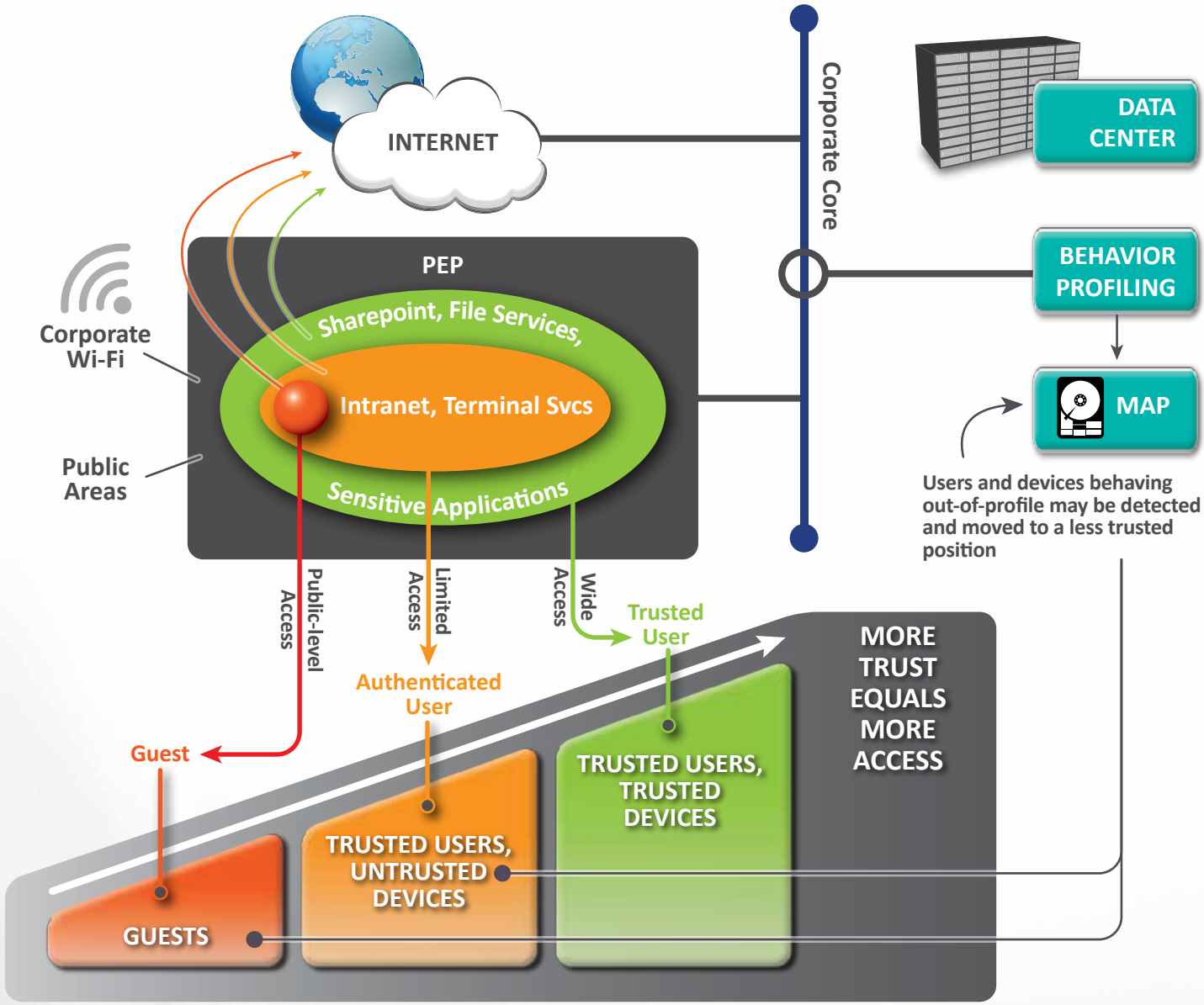


*Figure 3: On-campus via Wi-Fi or direct connections*

## A STARTING POINT: THREE TYPES OF ACCESS

The example architecture for portable device security in a campus wireless environment ***(Figure 3)*** shows an easy-to-deploy, but very powerful, configuration. This architectural diagram has been simplified to focus on the critical piece, the PEP, and the escalating trust model. Other components, such as the PDP, are visible in the "big picture" view ***(Figure 2)***.

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

Of course, one could have fewer or more access types and different types of access as fits the needs of one's 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 more constrained access than other 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.

Using a combination of TNC-compliant PEP devices with TNC-compliant endpoint security assessment clients, this type of portable device 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, all while getting the access they need.

## WHAT ARE TRUSTED NETWORK COMMUNICATIONS?

TCG's 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. In 2008, TNC was shared with the Internet Engineering Task Force (IETF), who codified TNC as their Network Endpoint Assessment (NEA) architecture. (RFC 5209) NEA and TNC are interoperable and adoption as an IETF standard extends the awareness of TNC-compatible capabilities.

## USER + DEVICE = ACCESS

| USER AUTHENTICATION | DEVICE TRUST | ACCESS GRANTED |
|---|---|---|
| AUTHENTICATED | TRUSTED | "Corporate Laptop"<br>Full access to corporate networks |
| AUTHENTICATED | UNTRUSTED | "Smartphone"<br>Moderate access to corporate networks: Intranet, email, etc. |
| UNAUTHENTICATED | UNTRUSTED | "Guest" access 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. Because their device is not trusted, the PDP assigns a limited set of access controls to the PEP. The user gets a lower level of access, such as the basic services as expected 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 PEP or move the misbehaving device completely off the corporate network. Such misbehavior can be detected through ongoing monitoring of the device, the results of which are stored in the MAP and CMDB where other security analytic tools can use them.

Contractors and consultants are another common category. In this case, the user may have a fully-trusted device, but more limited access to enterprise services—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.

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. All this collected information is stored in the MAP and CMDB where, augmented by information from other network monitoring tools, it is used by other security analytic tools to monitor for suspicious behavior or other changes that could lead to a need to modify the granted access.

## OFF CAMPUS: ENHANCED VPN TUNNELS DIFFERENTIATE DEVICES

A unified portable device security solution uses the same TNC-compatible client, PEPs, PDP, MAP, and CMDB. 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.

 

## OFF-CAMPUS VIA ENHANCED VPN TUNNELS

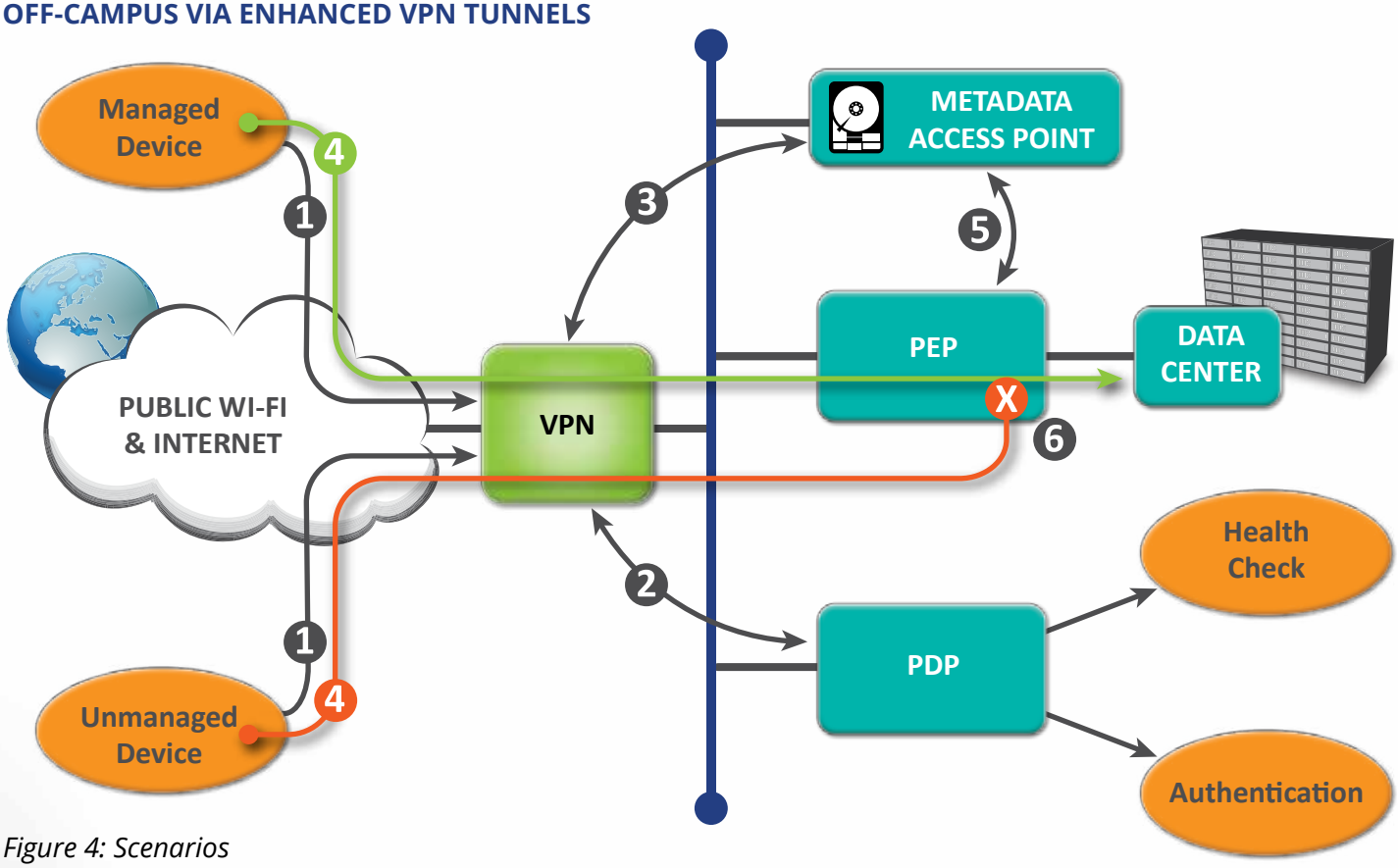


*Figure 4: Scenarios*

## WALKING THROUGH SCENARIOS

***Figure 4*** traces connections both from trusted devices (such as corporate laptops and smart phones) and untrusted devices (such as personal devices) as they connect to the corporate network through a VPN concentrator.

**(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 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 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 PEP.

**(5).** TNC PEP contacts the 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.

 