ARCHITECT'S GUIDE:

Comply to Connect Using TNC Technology

August 2012

Trusted Computing Group
3855 SW 153rd Drive
Beaverton, OR 97006
Tel (503) 619-0562
Fax (503) 644-6708
admin@trustedcomputinggroup.org
www.trustedcomputinggroup.org

Executive Summary and Action Items

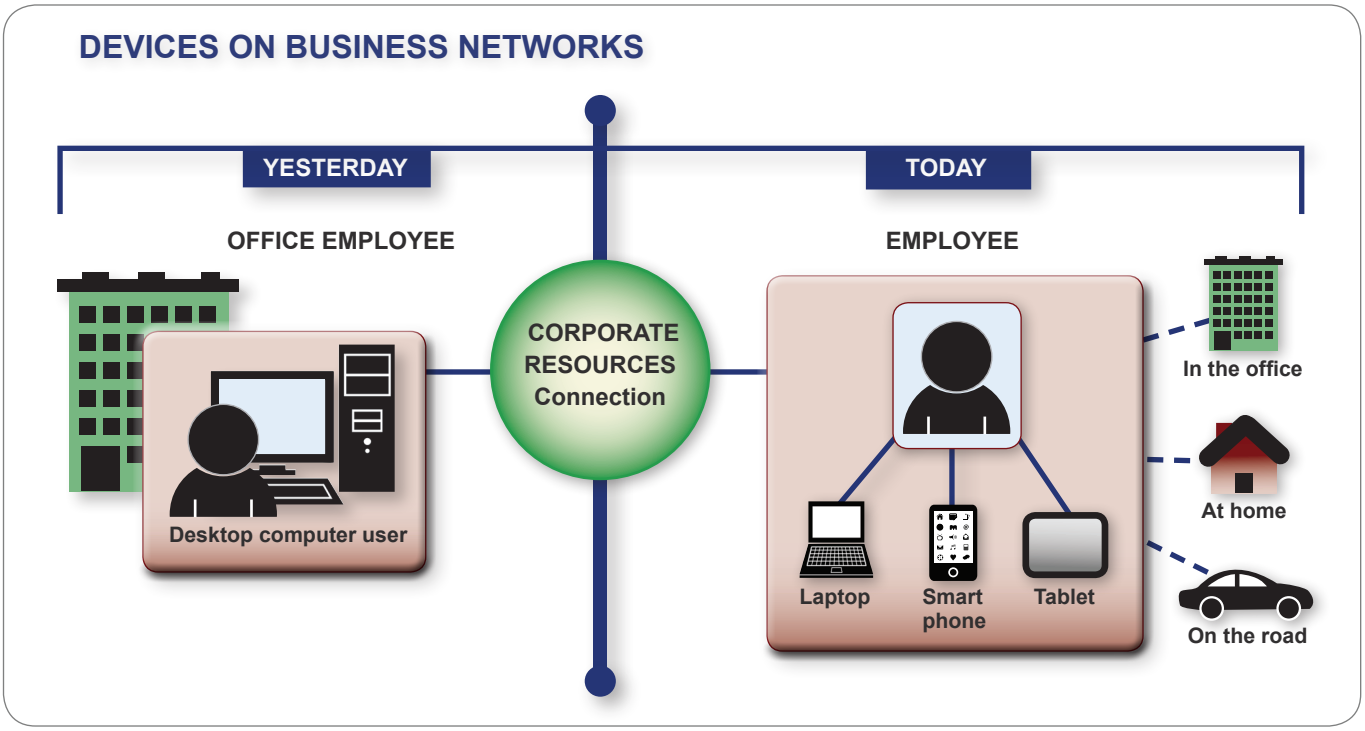
Comply to Connect is a standards-based approach to managing access to corporate networks, both from within and without, on multiple devices as long as the health and state of the devices can be verified.

Just as risk is not a binary (yes or no) concept, neither is compliance. Comply to Connect solutions allow an organization to set policies that define granular access to resources, and enable devices and users to demonstrate ongoing compliance with those policies.

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 solutions for continuous monitoring of device security while enabling mobility and flexibility for users. This Architect's Guide shows security architects how they can design and deploy successful multi-platform Comply to Connect solutions based on the open TNC architecture and standards.

Critical strategies for architects include:

1. **Use a consistent architecture and uniform policy framework** across all devices and access vectors (networks). This enables unified definition of access control policy framework, user authentication, and device compliance checks, rather than for every conceivable access scenario (e.g., mobile user, unmanaged device, managed device).
2. Enable Comply to Connect **policy enforcement** at the edge of the network, **as close to the user as possible**, which helps keep infected machines out of the network and, therefore, away from critical resources. In addition, pushing enforcement out to the endpoints enables better protection when the endpoint user accesses the Internet and helps maintain the endpoint in a secure, non-infected state.



Devices on business networks

- **Conventional devices have left the building:** The traditional desktop computer is no longer the center of the end-user's universe. Employees are using laptops, smart phones, and tablets in the office, at home, and on the road.
- **Unconventional devices are in the building:** Consumer devices on business networks are increasingly proliferating under the "bring your own device" (BYOD) technology approach.

To secure our resources, we must ensure that only healthy, verified devices connect to our networks.

Introduction

Controlling access to sensitive resources is an essential part of information security. Traditionally, access controls have focused on user identity and roles. However, many recent attacks (e.g. Operation Aurora) focus on compromising an authorized user's computer and then using that computer with the user's credentials and privileges to launch further attacks, such as extracting confidential data or infecting other computers.

As cyber security has matured over the years, individual defenses in cyberspace, such as firewalls, antivirus, and automatic updates, have become more commonly available and more commonly used. Keeping anti-virus and anti-spyware software up to date is widely accepted as a critical component of a well-rounded "defense in depth" effort to protect one's computer. Given that these protections are already available, the question is how an organization can ensure that its users and their endpoints are always up to date with the latest security measures.

The **"Comply to Connect"** solution, based on Trusted Computing Group's Trusted Network Connect (TNC) standards, is an ideal way to verify the security of computers both as they connect to the network and then continuously thereafter. Commercial vendors and open source developers have implemented TNC standards to build a rich ecosystem of interoperable products, ideal for deploying Comply to Connect solutions in enterprise networks. Network managers can combine requirements for endpoint integrity checking with other TCG technologies such as TPM (Trusted Platform Module) to write access control rules to protect enterprise resources. The result is a win-win for all involved: the end users are happy that they can get their jobs done with minimum friction, while network and security teams are confident they are keeping enterprise endpoints healthy and up-to-date with the latest security measures.

Solution Overview

Trusted Network Connect, an open architecture and accompanying set of standards for network security, was first released in 2005. Since then, multiple vendors have shipped products and solutions designed accordingly. In order to make standards-based solutions more accessible and to demonstrate interoperability between these solutions, TCG is now developing a set of solution definitions which demonstrate how to apply the TNC architecture and standards to solve common problems in a multi-vendor production environment.

This Architect's Guide gives a basic framework for the Comply to Connect solution, the problems it addresses, the benefits, and the strategic issues related to this solution. Examples of solution process and user experience are included. Related documents will provide technical deployment guidance that enables the solution to be easily deployed in a pilot or production environment.

Comply to Connect ensures that users have clean, healthy devices (endpoints) whenever they access corporate resources, thus protecting against data breaches, improving reliability, and lowering IT costs. The Comply to Connect solution is standards-based and interoperable, enabling a common IT infrastructure and consistent set of policies to protect all types of devices across all types of network connections, which minimizes cost and complexity.

Accounting for newer devices and newer forms of access as well as changing business rules and compliance requirements is an important element of this solution. The Comply to Connect architecture is flexible and adaptive to accommodate these changes over time.

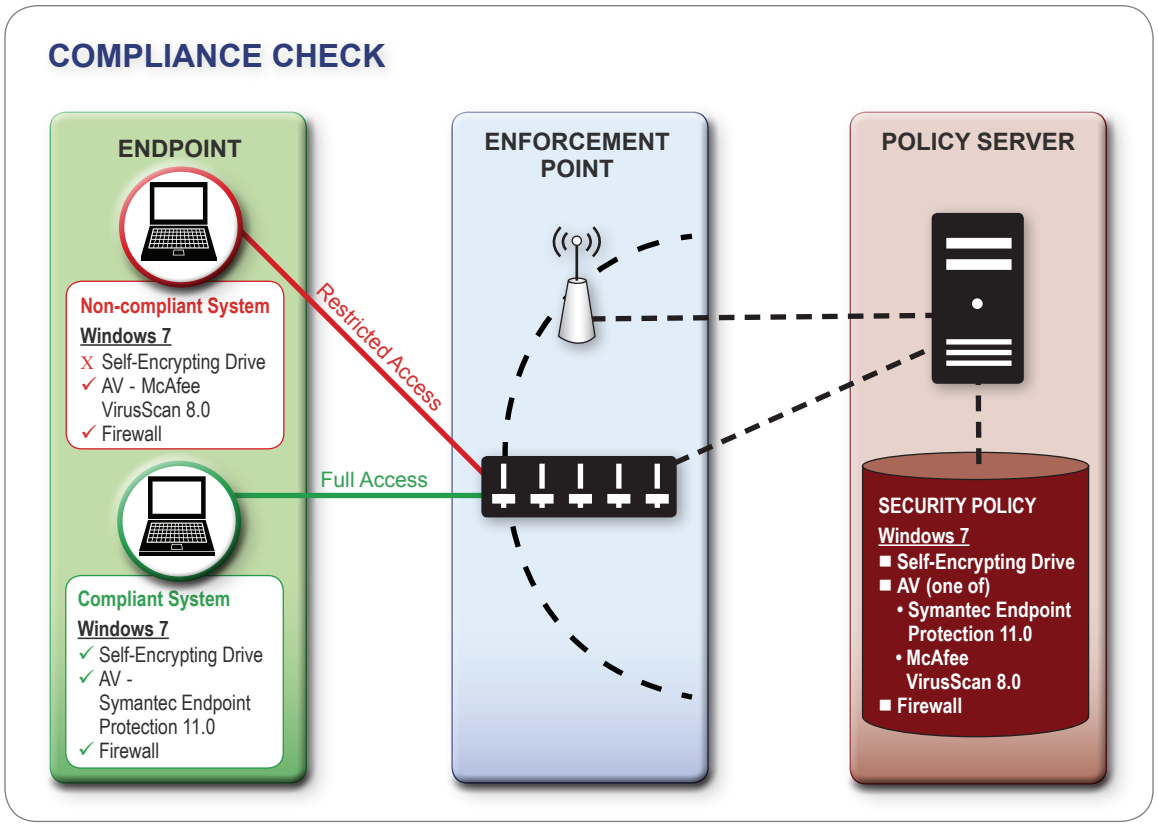
WHAT IS THE HEALTH STATE OF THE DEVICE?

SCENARIOS	AUTHORIZED USER	UNKNOWN USER
Fully compliant device	User has full access as authorized to enterprise network and Internet	User has access to the Internet, no access to enterprise network
Partially compliant device	User has access to remediation resources and limited access to some enterprise resources	Limited or no access to the Internet, no access to enterprise network
Non-compliant device	User has access to remediation resources, no access to enterprise network or Internet	User has no access

Elements of a Unified Solution

Components

- **Endpoint:** Any modern computing device (e.g. desktop, laptop, tablet, smartphone) used to access corporate resources
- **Enforcement Point:** Network access control point and/or an application gauging access to organization resources
- **Policy Server:** A repository of policies (rule sets) and resource access requirements that makes access control decisions based on information from TNC components and other servers (such as a Metadata Access Point (MAP) or Security Token Service (STS) server)



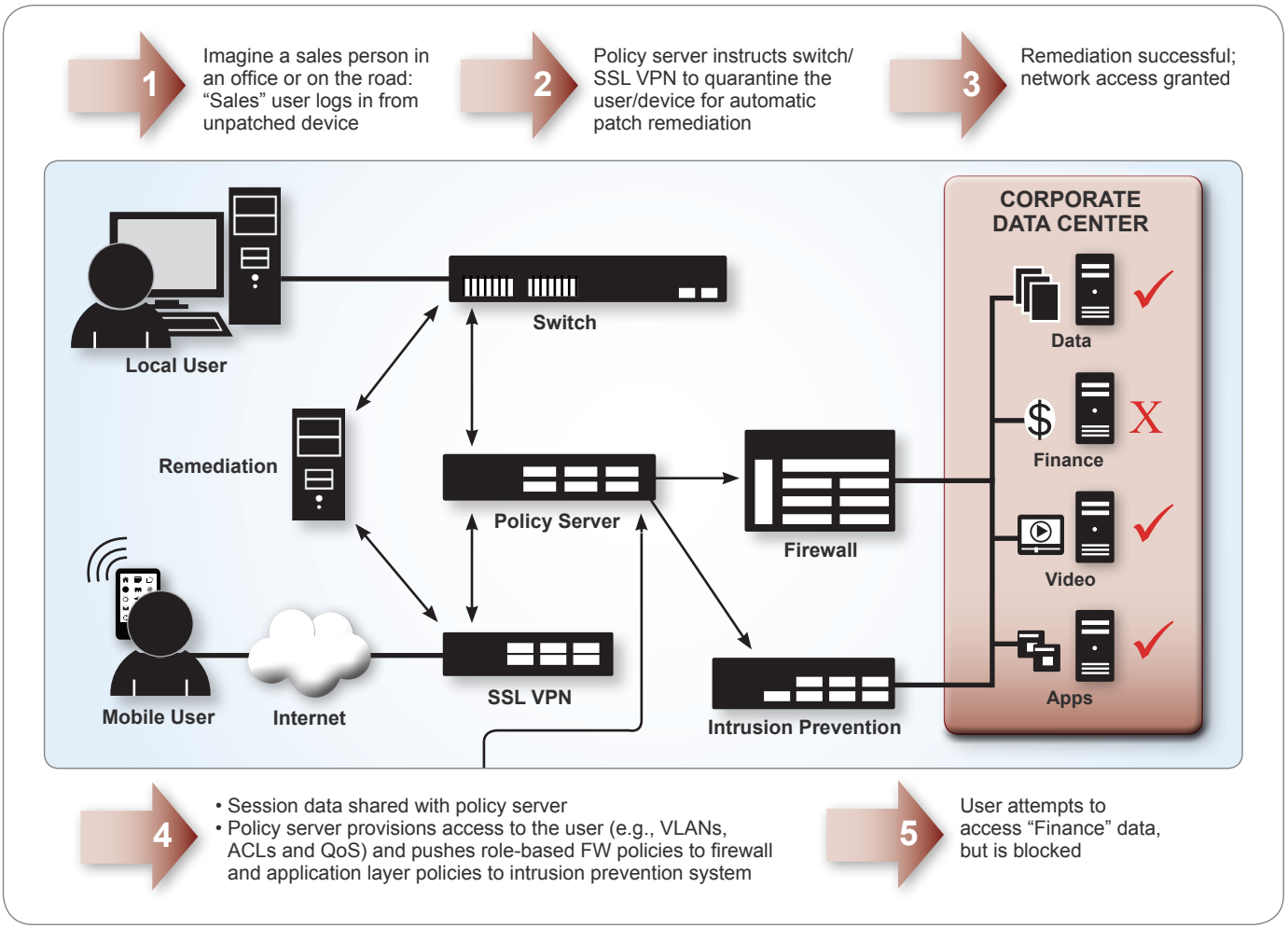
Process

1. An endpoint (user) requests access to a corporate resource
2. An enforcement point queries the endpoint for the required set of attributes for that access
3. The endpoint produces the attributes requested by the enforcement point
4. The enforcement point forwards the attributes from the endpoint to a policy server
5. The policy server compares attributes to applicable policies and makes an access decision
6. The enforcement point receives the decision and allows appropriate access
7. From the user's perspective, he or she gets access to the resources as usual, as long as their endpoint complies with applicable policies

These steps are seamless and in the background in real time. Depending on policy, these device health checks can be configured to run as often as needed.

.

User Experience



Additional Points

Compliance is not just a one-time event. Once a device connects to the network, it may still need to be periodically checked to ensure it has not subsequently gone out of compliance. Comply to Connect continuously checks policy and settings, requiring endpoints on the network to stay compliant and enabling IT to take automated action should endpoints fall out of compliance at any time.

Mobile devices allow anytime/anywhere access to corporate resources. Comply to Connect enables this access in a secure and controlled fashion by extending the trust boundary to the end user and their mobile device wherever they may be. Policy-based Comply to Connect solutions enable different levels of access for various users on a range of devices in multiple locations based on their level of trust. Guests, almost completely untrusted, get minimal access. Trusted users with trusted endpoints (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. Their levels of access are based on the policies established by the organization; the Comply to Connect solution architecture enables flexibility and granularity in enforcing those policies.

A unified approach to mobile security is critical for successful deployment. Using a combination of international and industry standards, Comply to Connect solutions 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" due to inconsistent application of policy, and reduce opportunities for human error.

Benefits and Value Proposition

Fewer data breaches

- When endpoints are up to date on security protection policies, they are better able to protect themselves against malicious actors and botnets targeting valuable data
- Healthier endpoints mean better resistance to attacks by persistent adversaries (protection against endpoint compromise based on known vulnerabilities, social engineering)

More reliable endpoints

- Cleaner, healthier devices
- Beyond security, Comply to Connect can also be used to update software on endpoints, improving reliability and user productivity

Access from anywhere on any device

- Comply to Connect enables uniform policy enforcement regardless of where the endpoint may be, on the intranet or at a hotspot elsewhere
- Uniform Comply to Connect infrastructure and policies can be applied to multiple modes of connectivity — wired to wireless, 802.1X to VPN

Lower costs

- Leveraging best-of-breed equipment from multiple vendors and tying it together with open standards reduces TCO and operational costs as well as complexities caused by proprietary vendor lock-in
- Reduce or eliminate the potential cost of cleanup and disclosure incurred by a security breach resulting from non-compliant endpoints

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 security automation, 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.

Key Strategic Considerations

- A consistent architecture and uniform policy choices across all devices and access vectors (networks) enables unified definition of access control policy framework, user authentication, and device compliance checks, rather than for every conceivable access scenario (e.g., mobile user, unmanaged device, managed device). Within the framework, different policies may apply to different scenarios (see below), but the overall framework remains the same. Enforce policies with re-usable tools, and focus on solutions that handle the entire universe of device security. Minimize special cases.
- Comply to Connect enables policy enforcement at the edge of the network, as close to the user as possible, which helps keep infected machines out of the network and, therefore, away from critical resources. In addition, pushing enforcement out to the endpoints enables better protection when the endpoint user accesses the Internet and helps maintain the endpoint in a secure, non-infected state.
- Flexibility in terms of policies for different types and levels of access (e.g., trusted user, untrusted device, telecommuter, guest) for different types of devices and for different departments (groups of users) within the organization.
- Placing all policy decisions in one logical policy server and connecting that policy server to many enforcement points allows you to gather all the necessary information to have sophisticated decisions and all the enforcement needed to have fine-grained access control.
- Within a consistent architecture and uniform policy framework, there is a need for variation in policies to allow multiple levels of access to resources. Access to some resources (financial data, business strategic plans) may have stronger endpoint security requirements; the policy framework should be able to accommodate these considerations

Call to Action

- Design Comply to Connect solutions customized for your unique environments
- Contact TCG-certified vendors and insist on acquiring standards-based technology solutions
- Deploy solution in pilot first, observe and correct issues, and then deploy into production
- Read more about TNC on the Trusted Computing Group web site: http:www.trustedcomputinggroup.org
- Contact us at admin@trustedcomputinggroup.org

