# ESTABLISHING NETWORK EQUIPMENT SECURITY

Firewalls and gateway routers are already important components of any organization's network security strategy. But network architects can often overlook the fact that the networking equipment itself can be attacked. Ensuring these devices are resistant to attacks is just as important as conventional security mechanisms that protect PCs and servers.

Attacks carried out on networking equipment can have devastating results:

- Unauthorized devices can gain access to networked data
- Unauthorized code can interfere with safe network operation
- Firmware implants can render network attacks invisible and are unremovable

For improved network security, the Trusted Computing Group (TCG) has developed standards/guidance that specifically addresses the security of networking equipment. The TCG Guidance for Securing Network Equipment is open for review until Sept. 11, 2017.

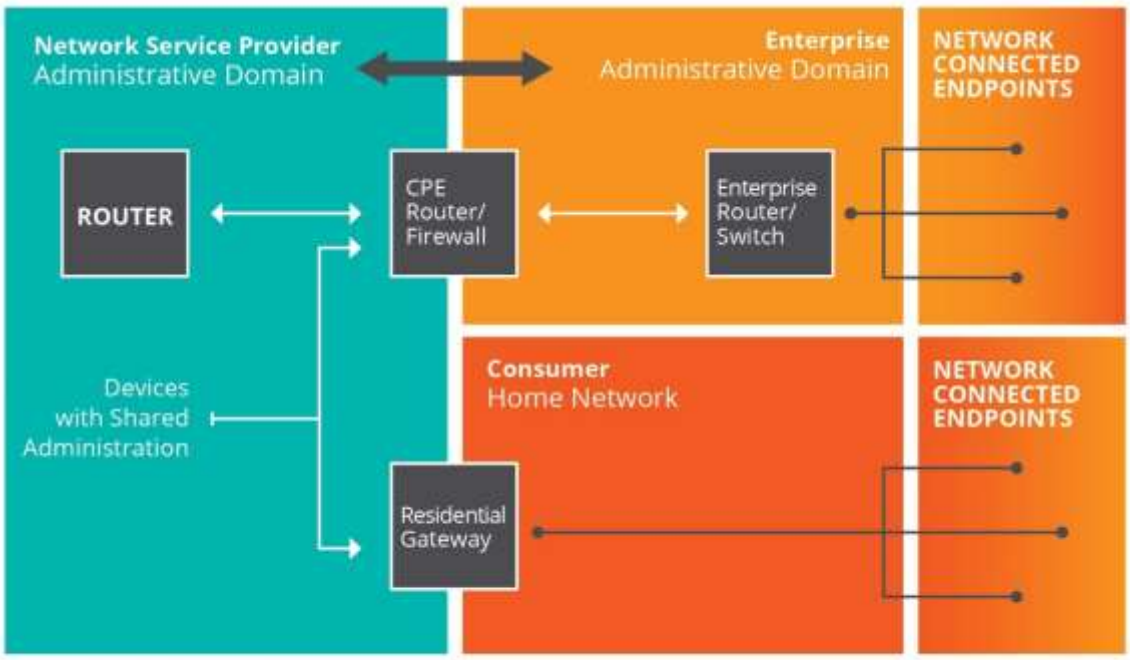


FIGURE 1: SIMPLIFIED NETWORK REFERENCE MODEL

To understand the various system aspects, Figure 1 shows a simplified reference model for network equipment interactions common in communication networks. The interconnections between administrative domains and the protection of end-user equipment are important in securing networking equipment.

To manage access and identity, the customer premise equipment (CPE) or residential gateways are frequently used to bridge between administrative domains, and may require special attention. Since CPE devices are often owned and managed by the service provider, but under the physical control of the Service Providers' customers, TCG's Trusted Platform Module (TPM) can provide important security improvements.

As a hardware-based root of trust, the TPM enables a more reliable approach to security than purely software-based approaches. To address network security, the TPM provides:

- Secure storage of boot state and object hashes
- Secure storage of cryptographic secrets, such as virtual private network (VPN) keys
- Cryptographic-quality Random Number Generator (RNG)

In addition, the TPM includes resistance to physical attack, such as reverse-engineering, allowing network users to keep private keys private.

An important aspect of network security is *identity. Identity* is knowing which device is which, even when situated remotely, might be difficult to protect, and might be either inconvenient or impossible to identify without physical presence. The solution to this problem is a TPM that can be programmed with a unique cryptographic identifier based on the device's serial number, signed by the device supplier.

The IEEE 802.1AR standard, "*Standard for Local and Metropolitan Area Networks: Secure Device Identity*," defines unique per-device identifiers (DevID) that allow establishment of the trustworthiness of devices. Using Public Key Cryptography, the TPM can assert its identity and then prove that it has possession of a difficult-to-steal private key, stored inside the TPM.

In networking equipment, cryptographic device identity has several applications, including:

- Identity for network access
- OEM device identity and counterfeit protection
- Secure autoconfiguration
- Remote device management

Identity for network access can be achieved by using cryptographic device identification, with keys stored in tamper-resistant TPMs.

OEM device identity and counterfeit protection are assured by certificates signed by the manufacturer and with keys rooted in a TPM.

Devices using *autoconfiguration* (also known as zero touch configuration or provisioning) can use a TPM to reliably identify themselves, and communicate through the network, to obtain the configuration information that specifies policy for operational use.

Remote device management can also make use of the TPM for enhanced security.

In addition to establishing identity using IEEE 802.1AR Device Identity certificates, the guidelines address other security-related functions useful in networking:

- A cryptographic random number generator based on physical sources of entropy, contained in the TPM, is critical to the generation of unpredictable keys
- Software attestation/health-check can prove that the device is running an authorized software version, and that it has not been subject to unauthorized modification.

The *TCG Guidance for Securing Network Equipment* covers a variety of other common security-related challenges in networking gear:

- Securing secrets
- Protection of configuration data
- Licensed feature authorization on a network device
- Software inventory
- Inventory of composite devices
- Integrity-protected logs
- Deprovisioning

In addition to these specific items, the TPM can provide many other tools to improve network security.

Although the *TCG Guidance for Securing Network Equipment* is still under review within the TCG, it is currently possible using the TPM and other TCG specifications implemented by several suppliers to:

- Lock down firmware
- Implement a cryptographic Random Number Generator
- Use DevID to identify embedded devices

As the full guidance document is developed and implemented in products from various companies that support TCG standards, network equipment security will improve even further. Vendors interested in learning more are invited to join TCG and participate.

The NetEq work can be seen here, https://trustedcomputinggroup.org/wp-content/uploads/TCG_Guidance_for_Securing_NetEq_1_0r26b_Public-Review.pdf.. For more information about TCG and membership, including participation in work groups, go to http://www.trustedcomputinggroup.org/membership/.