**Report: Secure Network Deployment Using NIST SP 1800-34**

**1. Introduction**

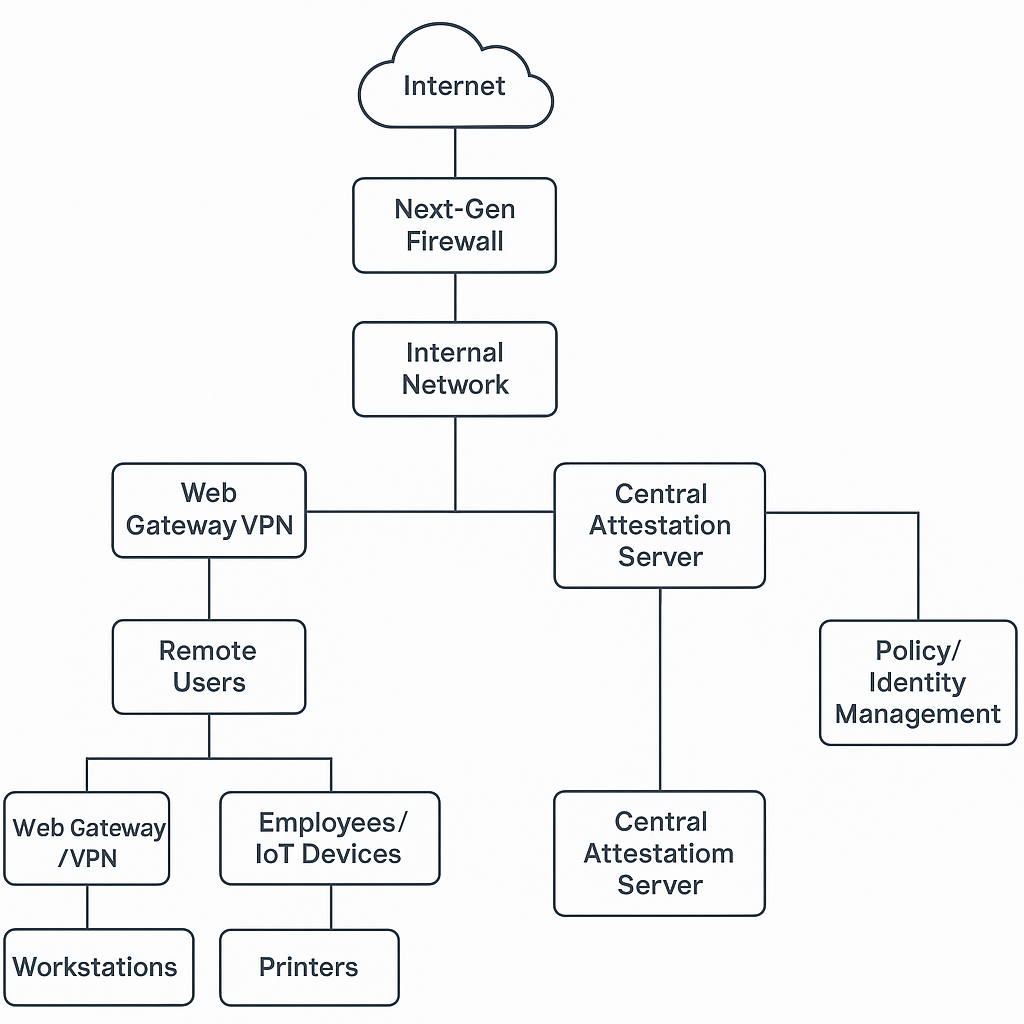
In an era of increasingly sophisticated cyber threats and rising concerns around device tampering, establishing a secure and trustworthy network environment is paramount. This report outlines the deployment of a computer network that incorporates the integrity validation framework described in *NIST SP 1800-34: Validating the Integrity of Computing Devices*. The approach prioritizes endpoint trust, secure boot mechanisms, remote attestation, and integration into a zero trust architecture (ZTA), ensuring that only verified, uncompromised devices are allowed to operate on the network.

**2. Objectives**

* Ensure all devices on the network boot into a trusted state.
* Prevent compromised or misconfigured systems from connecting to core services.
* Provide centralized visibility into device health and trust status.
* Enable automatic enforcement of policies based on hardware and firmware integrity.
* Support a zero trust model where trust is established through continuous validation.

**3. Network Design Overview**

**3.1 Logical Network Layout**



**4. Secure Network Setup Using NIST SP 1800-34**

**4.1 Device Hardware Baseline**

* All endpoints (desktops, laptops, servers) are equipped with **Trusted Platform Modules (TPM 2.0)**.
* BIOS and firmware support **Secure Boot** and **Measured Boot**.
* Network devices such as routers and switches also support secure firmware verification (when applicable).

**4.2 System Image and Software Validation**

* Device images are built from a **golden, validated baseline**.
* Before provisioning, each device goes through integrity checks to compare with a secure hash inventory stored centrally.
* Boot process is verified using TPM measurements (Platform Configuration Registers or PCRs).

**4.3 Remote Attestation Infrastructure**

* A **Remote Attestation Server (RAS)** is deployed within the internal network.
* Devices report their boot measurements to the RAS on startup.
* The RAS compares reported hashes with expected values and assigns a trust status (e.g., "trusted", "warning", "quarantined").

**4.4 Network Access Control Integration**

* The RAS communicates with a **Network Access Control (NAC)** platform such as Cisco ISE or Microsoft Intune.
* Devices that pass attestation are granted full access.
* Untrusted or unknown devices are segmented into a **remediation VLAN** or denied access entirely.

**5. Key Components and Tools**

| **Component** | **Role** |
| --- | --- |
| **TPM 2.0** | Secure hardware root of trust |
| **Secure Boot** | Ensures only signed code runs during boot |
| **Measured Boot** | Records hashes of loaded components |
| **Remote Attestation Server** | Verifies boot integrity remotely |
| **Integrity Measurement Verifier (IMV)** | Compares measurements against policy |
| **Network Access Control (NAC)** | Enforces access based on device trust |

**6. Implementation Steps**

1. **Prepare Device Hardware**  
   Ensure all devices have TPMs and firmware that supports measured boot.
2. **Build Golden Image**  
   Create a secure, hardened OS image. Hash the boot loader, OS kernel, and key applications.
3. **Deploy Attestation Infrastructure**  
   Set up the Remote Attestation Server with expected measurements and a secure database.
4. **Integrate with NAC & Identity Provider**  
   Connect the RAS with your NAC system and enforce policies based on trust posture.
5. **Monitor and Enforce**  
   Continuously monitor device posture and revoke or reduce access when integrity is compromised.
6. **Train Staff and Monitor Logs**  
   Provide staff with awareness training, and continuously analyze attestation and access logs.

**7. Benefits of This Architecture**

* **Trustworthy Devices**: Only validated systems can join the network.
* **Proactive Security**: Attacks or tampering at the firmware level are caught before a device boots.
* **Visibility**: Admins gain real-time insight into the health and posture of every device.
* **Compliance Ready**: Aligns with ZTA guidance and frameworks like NIST 800-207 and 800-53.

**8. Challenges and Mitigations**

| **Challenge** | **Mitigation** |
| --- | --- |
| Legacy hardware lacking TPMs | Segment legacy systems and plan phased upgrades |
| Complexity of initial rollout | Use pilot groups and test environments |
| Integration with existing tools | Use standards like DICE, IETF RATS, and TCG for interoperability |

**9. Conclusion**

Building a computer network using the guidance in NIST SP 1800-34 empowers organizations to trust the devices operating within their infrastructure. By enforcing strict validation at boot time and integrating remote attestation into access policies, organizations can significantly reduce risk from compromised devices, firmware-level malware, and supply chain attacks. This approach not only supports zero trust principles but also future-proofs infrastructure against evolving threats.