CloudTechForce

cloudtechforce.com | Managed IT & Cybersecurity

Network Security Assessment Checklist for SMBs

A 40-Point Network Security Checklist to Identify and Close Your Most Critical Vulnerabilities

Prepared by CloudTechForce | 2026 Edition

Section 1

Why Network Security Still Matters in a Cloud World

Cloud adoption has not eliminated network security risks — it has changed them. Most businesses now have a hybrid environment: on-premises devices and servers connecting to cloud applications through a corporate network and over the internet. This hybrid posture creates new attack surfaces that pure cloud-security tools do not address.

Network-level attacks remain a primary initial access vector for ransomware. Verizon's 2025 DBIR found that 22% of breaches involved network-level exploitation — primarily through remote access abuse (RDP, VPN), firewall misconfigurations, and unpatched network devices.

What this checklist covers:

- Perimeter security: firewall configuration, DMZ architecture, internet-facing services
- Internal segmentation: VLANs, east-west traffic controls, critical system isolation
- Remote access: VPN security, RDP controls, zero trust network access
- Wireless security: SSID segmentation, authentication standards, guest network isolation
- Monitoring and logging: network visibility, anomaly detection, log retention

Section 2

Perimeter Security (Points 1–10)

- 1. Next-generation firewall (NGFW) deployed with application-layer inspection
- 2. Firewall rules documented with business justification for each allow rule
- 3. Firewall rules reviewed and recertified at minimum annually
- 4. All internet-facing services inventoried — no forgotten open ports
- 5. Internet-facing services patched within 7 days of critical vulnerability release
- 6. Web Application Firewall (WAF) protecting any internet-accessible web applications
- 7. DMZ architecture separates internet-facing services from internal network
- 8. Outbound traffic filtered — DNS filtering blocks known malicious domains
- 9. IDS/IPS enabled on perimeter firewall — signatures updated automatically
- 10. DDoS protection in place for internet-facing services

Common perimeter failures we see:

The most frequent perimeter issues found in network assessments: RDP (port 3389) exposed directly to the internet, unpatched VPN appliances with known CVEs, firewall rules inherited from years ago with no documentation, and web applications without WAF protection.

Internal Segmentation and Remote Access (Points 11–30)

Internal Network Segmentation (Points 11–20)

- 11. VLANs segment network by function (servers, workstations, printers, IoT, guests)
- 12. Finance, HR, and executive systems on isolated VLAN
- 13. Industrial/OT systems physically or logically separated from corporate IT
- 14. Server-to-server traffic filtered — only required ports allowed between segments
- 15. Workstation-to-workstation communication blocked — prevents ransomware lateral movement
- 16. DNS internally resolved through managed DNS servers — not bypassed
- 17. Network Access Control (NAC) verifies device compliance before granting network access
- 18. Rogue device detection — unauthorized devices identified and blocked
- 19. Network map current and accurate — all segments and connections documented
- 20. Printer and IoT devices on isolated VLAN — never on same segment as sensitive data

Remote Access Security (Points 21–30)

- 21. RDP not exposed directly to internet — accessible only through VPN
- 22. VPN requires MFA for all connections — not just username/password
- 23. VPN appliance firmware current — no known critical CVEs
- 24. VPN split tunneling policy reviewed — security traffic routes through corporate
- 25. Remote access sessions logged with user identity, timestamp, and duration
- 26. Inactive VPN accounts disabled within 24 hours of employee departure
- 27. Third-party remote access (vendors, MSP) uses time-limited, monitored sessions
- 28. Vendor remote access uses separate VPN profile — not same as employee VPN
- 29. Jump server or privileged access workstation required for admin remote access
- 30. Remote access logs reviewed weekly for anomalous patterns

Wireless Security and Network Monitoring (Points 31–40)

Wireless Network Security (Points 31–36)

- 31. WPA3 or WPA2-Enterprise used for corporate wireless — no WEP or open networks
- 32. Corporate SSID uses certificate-based authentication or 802.1X
- 33. Guest wireless on completely separate VLAN with no access to corporate resources
- 34. Wireless access point firmware updated automatically or on quarterly schedule
- 35. Rogue AP detection enabled — unauthorized access points identified
- 36. SSID broadcast for corporate network disabled where possible — hidden SSID

Network Monitoring and Logging (Points 37–40)

- 37. Network flow data (NetFlow, sFlow) collected and retained for 90+ days
- 38. SIEM or log management system aggregates firewall, DNS, and VPN logs
- 39. Alerts configured for high-bandwidth transfers, new outbound connections to uncommon destinations
- 40. Network baseline established — anomalous traffic patterns trigger investigation

CloudTechForce performs network security assessments using this checklist as the framework, supplemented by live network scanning and configuration review. Contact sales@cloudtechforce.com or visit cloudtechforce.com/managed-security-services.

Section 5

Firewall Configuration Best Practices

The firewall is the cornerstone of perimeter defense, but a poorly managed firewall provides false confidence. Most firewall problems stem from accumulated, undocumented rules rather than the device itself.

- Adopt a default-deny posture: block everything, then explicitly permit only what is required
- Document a business justification for every allow rule
- Review and recertify firewall rules at least annually; remove obsolete and overly broad rules
- Use a next-generation firewall with application-layer inspection, not just port/protocol filtering
- Enable and update IDS/IPS signatures automatically
- Filter outbound traffic, not just inbound — block known-malicious destinations and unexpected egress
- Log firewall activity centrally and review it for anomalies
- Keep firewall firmware patched — firewall and VPN appliance CVEs are prime ransomware entry points

The most common dangerous finding in assessments is a firewall ruleset that has grown for years with no documentation — nobody remembers why half the rules exist, and removing them feels risky. Regular recertification prevents this accumulation and shrinks your attack surface.

Network Segmentation in Practice

Segmentation is one of the highest-impact network security controls because it directly limits the lateral movement that turns a single compromised device into an enterprise-wide breach.

A practical segmentation approach:

- Map current traffic flows to understand what actually communicates with what
- Separate by function with VLANs: servers, workstations, printers, IoT, guests, OT
- Isolate high-value systems — domain controllers, finance, HR, backups — into protected segments
- Block workstation-to-workstation communication to stop ransomware spread
- Place IoT and OT devices on isolated segments, never alongside sensitive data
- Apply default-deny between segments; permit only required traffic

Segmentation does not require a forklift upgrade. Start by isolating your most critical assets and your riskiest devices (IoT, guest), then progressively tighten east-west controls. Even basic segmentation dramatically reduces the blast radius of an intrusion.

Securing Remote Access

Remote access is consistently among the top initial-access vectors for ransomware. Exposed RDP and vulnerable VPN appliances are repeatedly exploited.

- Never expose RDP directly to the internet — require VPN or Zero Trust Network Access
- Require MFA on all remote access, not just a username and password
- Keep VPN and firewall appliances patched within days of a critical CVE
- Log all remote sessions with user identity, timestamp, and duration
- Disable remote access accounts immediately when employees leave
- Give vendors time-limited, monitored, separate remote access — never shared employee credentials
- Require a jump server or privileged access workstation for administrative remote access

Consider Zero Trust Network Access:

ZTNA brokers access to specific applications based on identity and device posture, rather than placing a device on the whole network as a VPN does. It shrinks the attack surface, eliminates the exposed VPN appliance, and aligns with modern Zero Trust principles. For many organizations, replacing legacy VPN with ZTNA is the single most valuable remote-access improvement available.

Wireless Network Security

Wireless networks extend your attack surface beyond your walls. Weak wireless security can give an attacker in the parking lot access to your internal network.

- Use WPA3, or at minimum WPA2-Enterprise with 802.1X, for corporate wireless — never WEP or open networks
- Authenticate corporate wireless with certificates or 802.1X, not a shared passphrase
- Place guest wireless on a fully separate VLAN with no access to corporate resources
- Enable rogue access point detection to identify unauthorized devices
- Keep access point firmware current
- Segment IoT devices onto their own wireless network, isolated from sensitive systems

Guest and IoT wireless are frequent weak points. A guest network that can reach internal systems, or smart devices sharing a network with sensitive data, undermines otherwise strong defenses. Strict wireless segmentation closes these gaps.

Section 9

Network Monitoring and Detection

You cannot respond to attacks you cannot see. Network visibility is what turns a silent, weeks-long intrusion into a detected and contained incident.

- Collect network flow data (NetFlow/sFlow) and retain it for 90+ days
- Aggregate firewall, DNS, VPN, and device logs into a SIEM or log management platform
- Establish a baseline of normal traffic so anomalies stand out
- Alert on high-volume transfers, connections to uncommon destinations, and unusual east-west traffic
- Monitor DNS for signs of command-and-control and data exfiltration
- Review remote access logs weekly for anomalous patterns

For most SMBs, a managed detection and response (MDR) service or a co-managed SIEM provides 24/7 monitoring without the cost of building an in-house Security Operations Center. The key is that someone is watching and able to respond — alerts that no one reviews provide no protection.

Section 10

Vulnerability Management and Common Findings

A network assessment is a point-in-time snapshot; vulnerability management is the ongoing practice that keeps the network secure between assessments.

An effective vulnerability management program:

- Scan internal and external assets regularly (at least monthly; weekly for internet-facing)
- Prioritize remediation by exploitability and asset criticality, not just CVSS score
- Patch internet-facing critical vulnerabilities within days
- Track remediation to closure and measure mean time to remediate
- Re-scan to verify fixes actually closed the vulnerability

The most common findings we see:

- RDP exposed directly to the internet
- Unpatched VPN and firewall appliances with known CVEs
- Undocumented firewall rules accumulated over years
- Flat networks with no segmentation, enabling free lateral movement
- Default or weak credentials on network devices
- Guest or IoT devices with access to internal resources

These findings recur because they are easy to introduce and easy to overlook. Combining periodic assessment with continuous vulnerability management catches them before an attacker does.

About CloudTechForce

CloudTechForce is a managed IT services provider serving businesses across North America and globally since 2016. We deliver 24/7 IT monitoring, cybersecurity, cloud management, Microsoft 365 administration, compliance support, and virtual CIO advisory — all at a predictable monthly cost.

Our certified team includes Microsoft and AWS professionals with deep expertise in regulated industries including healthcare, defense contracting, financial services, and SaaS.

Get in Touch

- Website: cloudtechforce.com
- Email: sales@cloudtechforce.com
- Free Assessment: cloudtechforce.com/free-assessment