RCMOS – Revista Científica Multidisciplinar O Saber | ISSN 2675-9128 | São Paulo, SP

Year VII, Vol. 2, 2026 | Submitted: October 1, 2026 | Accepted: October 3, 2026 | Published: October 6, 2026

Connectivity Architectures for SMEs: Network Segmentation, VPNs, Virtualization, and Operational Availability

Guilherme Gallo Zazeri

Information Technology professional, consultant, and entrepreneur specializing in infrastructure, connectivity, and technology solutions, with more than 25 years of professional experience.

Abstract

Corporate networks in small and medium-sized enterprises now support access to local and cloud applications, remote work, IP telephony, virtualized services, and communication between locations. This article examines architectural principles for secure and available connectivity, addressing segmentation, firewalls, wireless networks, VPNs, link redundancy, virtualization, and documentation. The study uses a structured narrative review of established networking textbooks, NIST publications, and data from the Verizon Data Breach Investigations Report. Findings indicate that performance and security should not be treated as competing objectives: coherent architecture reduces exposure, limits failure propagation, improves troubleshooting, and creates conditions for recovery. For SMEs, standardization and operational simplicity are particularly relevant because unnecessarily complex environments can increase costs and dependence on specialists.

Keywords: corporate networks; connectivity; VPN; firewall; virtualization; small and medium-sized enterprises; availability.

1. Introduction

Corporate networks no longer connect only computers within an office. Today, they integrate cloud applications, virtualized servers, IP telephony, wireless devices, branch offices, and remote professionals. Tanenbaum and Wetherall (2021) show that network communication is built upon interdependent layers and protocols, making architectural design decisive for performance and reliability.

The expansion of connectivity also increases the attack surface. The Verizon DBIR 2025 found that, among the small organizations covered in the report, System Intrusion, Social Engineering, and Basic Web Application Attacks jointly accounted for 96% of breaches. This finding demonstrates that networks and access cannot be managed solely from the standpoint of availability.

This article analyzes six dimensions of connectivity architecture for SMEs: design and segmentation, firewalls, VPNs, redundancy, virtualization, and documentation. The discussion seeks to show how established technical principles can be applied without assuming structures equivalent to those of large corporations.

Open Access | Creative Commons Attribution: reuse permitted with proper attribution.

2. Methodology

The research adopts a structured narrative review, bringing together literature on computer networks, perimeter security, remote access, virtualization, and risk management.

Tanenbaum and Wetherall (2021), Kurose and Ross (2021), and Stallings (2016) were used as conceptual foundations for architecture, protocols, performance, and modern networks.

Security recommendations were compared against NIST SP 800-41 Rev. 1, NIST SP 800-46 Rev. 2, NIST CSF 2.0, and the NIST guide for small businesses.

The Verizon DBIR 2025 was incorporated as an empirical source on breach patterns, with specific attention to the report's small-organization segment.

The analysis does not evaluate commercial brands. Firewall, Wi-Fi, hypervisor, and tunneling technologies are discussed according to their architectural functions to preserve neutrality and applicability.

The findings were organized into six areas. Each area considers availability, security, maintainability, and suitability for organizational size.

3.1 Network Design and Logical Segmentation

Tanenbaum and Wetherall (2021) explain that networks consist of interconnected systems whose organization influences performance and reliability. In companies, design must reflect distinct functions, such as users, servers, telephony, guests, and specialized devices.

Logical segmentation makes it possible to separate groups of assets and control communication among them. Instead of a flat network, in which all devices share broad reachability, segments reduce the propagation of failures and limit unnecessary communication paths.

Kurose and Ross (2021) emphasize the importance of forwarding and the policies that determine how flows traverse the network. In corporate settings, these decisions should be documented and linked to actual communication needs.

Segmentation does not mean creating unlimited complexity. Each additional division increases the need for rules, testing, and troubleshooting. For SMEs, balancing isolation and administrative effort is part of the design.

Wireless networks must also be integrated into the architecture. Separating corporate access from guest access, for example, prevents convenient connectivity from unnecessarily exposing internal resources.

A well-segmented architecture establishes a foundation for firewall policies, monitoring, and response. Network design begins to express business rules rather than merely the physical arrangement of equipment.

3.2 Firewalls and Traffic Control Policies

Firewalls serve as policy enforcement points between networks or different trust zones. Scarfone and Hoffman (2009), in NIST SP 800-41 Rev. 1, treat firewall policy as an essential

Open Access | Creative Commons Attribution: reuse permitted with proper attribution.

part of planning and administering these controls.

Effectiveness depends on the quality of the rules. Permissions accumulated over the years can create exceptions whose original purpose no longer exists. Periodic reviews help remove obsolete rules and reduce exposure.

The principle of allowing only what is necessary is particularly useful. Published services, open ports, and administrative access should correspond to an identified need, with defined sources and destinations.

Firewall logs provide evidence for troubleshooting and investigation, but their volume requires selection criteria. Relevant events need to be retained and analyzed in a manner consistent with risk and team capacity.

Firewalls also perform connectivity functions such as NAT, VPN, and failover. This concentration makes configuration documentation and device backups part of operational continuity.

Therefore, a firewall should not be regarded as a device that automatically makes a network secure. Its value depends on architecture, rules, maintenance, and monitoring.

3.3 VPNs and Connectivity Between Locations and Remote Professionals

Remote access and interconnection between locations require channels that protect data in transit and control who can reach internal resources. Souppaya and Scarfone (2016), in NIST SP 800-46 Rev. 2, discuss telework and remote-access security as a combination of technologies, policies, and management.

VPNs can establish tunnels between sites or connect individual users. The choice depends on topology, application, performance, and authentication model.

Tunnel encryption protects traffic but does not, by itself, resolve endpoint risk. A compromised device with authorized access can carry threats into the network.

For this reason, remote-access design should apply privileges appropriate to each role. Not every remote user needs access to all segments or services.

Availability must also be considered. Dependence on a single link, device, or authentication service can turn remote access into a point of interruption.

VPNs are therefore components of a broader architecture. Security depends on combining identity, segmentation, updates, monitoring, and access rules.

Figure 1. Three Leading Breach Patterns in Small Organizations

Open Access | Creative Commons Attribution: reuse permitted with proper attribution.

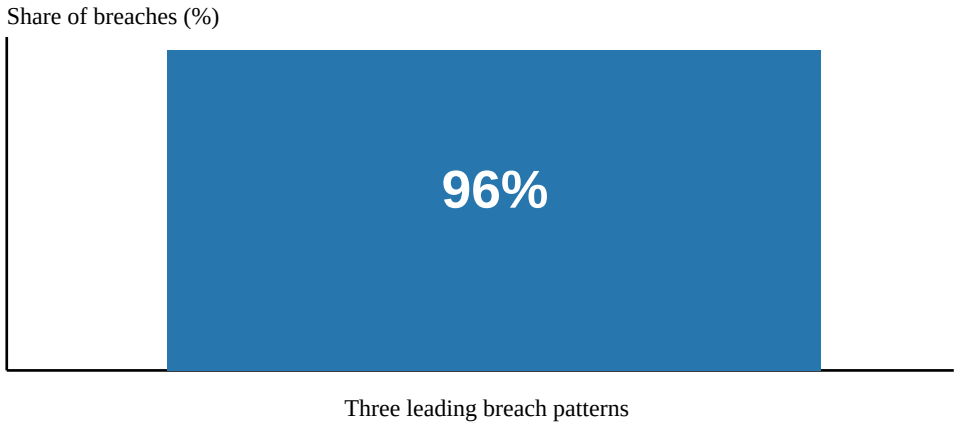


Figure 1. Combined share of the three leading breach patterns in small organizations: System Intrusion, Social Engineering, and Basic Web Application Attacks. Source: Author's own illustration based on Verizon (2025).

3.4 Link Redundancy and Connectivity Continuity

External connectivity has become a critical dependency for companies using SaaS, cloud email, IP telephony, and remote work. An internet outage can interrupt multiple services simultaneously.

Link redundancy reduces this dependence when providers, routes, and equipment are planned to avoid a single point of failure. Having two contracts, however, does not guarantee physical or logical independence.

Load balancing and failover have different objectives. The former distributes traffic; the latter seeks to maintain service when a path stops functioning. The architecture should clearly define the expected behavior.

Testing is necessary because automatic switchover can fail due to DNS, sessions, routing, or dependence on a public IP address. Availability needs to be assessed from the application's perspective.

IP telephony illustrates this challenge. Even if the PBX remains operational, loss of connectivity to external trunks can prevent calls. Kurose and Ross (2021) show how real-time applications are sensitive to delay, loss, and network availability.

Effective redundancy therefore depends on diversity, configuration, testing, and monitoring. Duplicating components without validating the complete path may create only the appearance of resilience.

3.5 Virtualization and Server Consolidation

Virtualization separates the logical execution of systems from the underlying physical hardware. Stallings (2016) relates virtualization to the evolution of modern infrastructures, in which computing resources can be abstracted and managed with greater flexibility.

For SMEs, consolidating workloads can reduce the number of devices and simplify provisioning. Virtual machines can be copied, migrated, and organized differently from

Open Access | Creative Commons Attribution: reuse permitted with proper attribution.

exclusively physical servers.

Consolidation also concentrates risk. When multiple services depend on the same host, a physical failure can affect several functions. Capacity, storage, power, and recovery strategy must keep pace with workload density.

Virtualization does not replace backup. Snapshots can support maintenance or short-term rollback, but should not automatically be confused with an independent protection and retention strategy.

Environment standardization facilitates support. Templates, naming conventions, documentation, and allocation criteria make changes more predictable and reduce improvised configurations.

Thus, virtualization creates value when it integrates capacity, continuity, and governance. The objective is not to maximize the number of virtual machines per host, but to obtain an infrastructure that can be managed and recovered.

3.6 Monitoring, Documentation, and Operational Troubleshooting

Complex networks produce signals from routers, firewalls, access points, servers, and applications. Monitoring converts some of these signals into operational information, allowing outages, saturation, and anomalous behavior to be recognized.

Tanenbaum and Wetherall (2021) show that network problems can arise at different layers. Efficient troubleshooting requires distinguishing physical failures, addressing, routing, name resolution, transport, and applications.

Documentation reduces the time needed for this investigation. Diagrams, inventories, addressing schemes, essential rules, and dependencies help reconstruct the traffic path.

The Verizon DBIR 2025 reinforces the importance of maintaining visibility over the environment. In its small-organization segment, three patterns—System Intrusion, Social Engineering, and Basic Web Application Attacks—accounted for 96% of breaches.

This figure does not mean that every incident is caused by network architecture. It does demonstrate, however, that connectivity, systems, and identity operate in a context in which exposure and access must be continuously observed.

Monitoring and documentation complete the architectural cycle. A well-designed network that cannot be observed or understood by its administrators loses an important part of its ability to remain available and secure.

3.7 IP Telephony, Quality of Service, and Communications Convergence

The convergence of voice and data has changed the role of the corporate network. IP telephony systems share infrastructure with applications, internet access, and internal services, meaning that connectivity degradation can simultaneously affect communication and business systems.

Open Access | Creative Commons Attribution: reuse permitted with proper attribution.

Kurose and Ross (2021) explain that real-time applications have specific requirements regarding delay, delay variation, and packet loss.

In a network without prioritization criteria, high-volume traffic can compete for resources with voice calls. Users immediately perceive the effects: delays, interruptions, and reduced intelligibility. Quality-of-service management seeks to address this difference in sensitivity without assuming that every application requires the same network behavior.

Stallings (2016) connects Quality of Service and Quality of Experience to the evolution of modern networks. In corporate environments, this means technical metrics must be interpreted according to their impact on activities: a connection may be available and still provide an inadequate experience for voice or videoconferencing.

IP telephony also increases the importance of segmentation. Logically separating voice devices and flows can facilitate policy enforcement, troubleshooting, and broadcast control. The decision, however, must remain compatible with the team’s administrative capacity.

Another aspect is external dependency. SIP trunks, DNS, internet connectivity, and power can all form part of the telephony operating chain. Redundancy must account for these relationships; keeping the PBX running does not resolve an outage if the external route required for calls remains unreachable.

Documentation becomes particularly relevant in environments with large numbers of extensions. Numbering, groups, routes, inbound and outbound rules, and carrier dependencies must be recorded so that changes and incidents can be handled predictably.

Convergence also changes troubleshooting. Problems perceived as telephony failures may originate in packet loss, saturation, DNS, routing, firewalls, or endpoint configuration. Tanenbaum, Feamster, and Wetherall (2021) show why layered analysis remains useful even in modern architectures.

Thus, IP telephony should not be managed as an isolated system. It forms part of the connectivity architecture and must share the same principles of availability, segmentation, monitoring, documentation, and recovery applied to the rest of the infrastructure.

3.8 Architectural Standardization and Scalability in Distributed Environments

Companies that expand through new locations, remote work, or adoption of cloud services face an additional problem: configurations created case by case tend to produce environments that are difficult to maintain. Standardization reduces unnecessary variation and creates reference points for deployment and troubleshooting.

Standardization does not mean making all locations identical. It means establishing repeatable principles for addressing, segmentation, remote access, naming, logging, updates, and configuration backups. Kurose and Ross (2021) show that predictable network behavior depends on clear forwarding and communication rules.

Templates and checklists can reduce omissions during new deployments. In distributed networks, consistently repeating criteria also facilitates comparing performance across locations and identifying deviations.

Open Access | Creative Commons Attribution: reuse permitted with proper attribution.

NIST CSF 2.0 (PASCOE; QUINN; SCARFONE, 2024) emphasizes that security outcomes should be understood, prioritized, and communicated. A standardized architecture facilitates this process because controls can be associated with known patterns rather than rebuilding the environment for each assessment.

Scalability includes human operational capacity. A solution that requires manual intervention for every new user, tunnel, or location may work at a small scale and become unsustainable as the organization grows. Automation and standardization should also be assessed for this effect.

Standardized documentation further reduces dependence on the professional who performed the original deployment. When topology, rules, and essential parameters follow a common model, other team members can understand the environment at a lower transition cost.

Finally, standardization creates a safer foundation for innovation. New technologies can be assessed against a known architecture, allowing benefits and risks to be compared without introducing simultaneous changes at every layer.

Scaling connectivity, therefore, is not merely a matter of adding equipment and links. It means preserving understandability, security, and maintainability as the network grows larger and more distributed.

Conclusion

An SME’s connectivity supports services that were previously independent and must therefore be treated as critical architecture. Segmentation helps organize flows and limit exposure, provided that complexity remains manageable. Firewalls are policy enforcement mechanisms; their effectiveness depends on rule quality and maintenance, not merely on the presence of the equipment. VPNs increase mobility and integration between locations, but must be combined with identity, privileges, and device security. Link redundancy must be tested along the complete application path. Two circuits do not constitute continuity if they share hidden dependencies. Virtualization provides flexibility and consolidation while requiring attention to workload concentration, capacity, and recovery.

Monitoring and documentation make the architecture observable and reduce troubleshooting time, while also decreasing dependence on individual knowledge. The conclusion is that resilient networks for SMEs are built through a combination of simplicity, segmentation, access controls, proportionate redundancy, and disciplined operations. Technical design creates value when it remains understandable, testable, and sustainable over time.

References

TANENBAUM, Andrew S.; FEAMSTER, Nick; WETHERALL, David J. Computer Networks. 6th ed. Harlow: Pearson, 2021.

KUROSE, James F.; ROSS, Keith W. Computer Networking: A Top-Down Approach. 8th ed. Hoboken: Pearson, 2021.

STALLINGS, William. Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. Boston: Addison-Wesley, 2016.

Open Access | Creative Commons Attribution: reuse permitted with proper attribution.

PASCOE, Cherilyn; QUINN, Stephen; SCARFONE, Karen. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. Gaithersburg: National Institute of Standards and Technology, 2024.

ELIOT, Daniel. NIST Cybersecurity Framework 2.0: Small Business Quick-Start Guide. NIST SP 1300. Gaithersburg: National Institute of Standards and Technology, 2024.

VERIZON. 2025 Data Breach Investigations Report. Basking Ridge, 2025.

SCARFONE, Karen; HOFFMAN, Paul. Guidelines on Firewalls and Firewall Policy. NIST SP 800-41 Rev. 1. Gaithersburg: National Institute of Standards and Technology, 2009.

SOUPPAYA, Murugiah; SCARFONE, Karen. Guide to Enterprise Telework, Remote Access, and Bring Your Own Device Security. NIST SP 800-46 Rev. 2. Gaithersburg: National Institute of Standards and Technology, 2016.

Open Access | Creative Commons Attribution: reuse permitted with proper attribution.