From ‘Firewall at the Edge’ to ‘Security in the Fabric’

India’s small and medium enterprises (SMEs) are entering a new phase of digital transformation. From adopting AI-enabled tools and cloud platforms to expanding e-commerce and remote collaboration, SMEs are increasingly dependent on digital infrastructure to compete and grow.

Aa per available data, India has more than 63 million MSMEs that contribute nearly 30% of the country’s GDP and over 45% of exports. As these businesses adopt digital technologies to improve productivity and reach new markets, their dependence on reliable internet connectivity is growing rapidly.

However, this digital shift is also expanding the security threat surface.

Many SMEs still treat security as an afterthought, something that can be added later in the form of antivirus software, a firewall appliance, or occasional monitoring. But in today’s threat landscape, that model is becoming dangerously outdated.

New cyber threat landscape for SMEs

India has seen a steady rise in cyber incidents across sectors. Cyberattacks are becoming more sophisticated, automated, and targeted. According to Verizon’s DBIR, ransomware attacks in particular have increasingly focused on mid-sized

businesses, accounting for 88% of SMB breaches. These SMBs often lack the security resources of large enterprises but still handle valuable data and critical operations.

For SMEs, these threats often enter through the same pathway that powers their operations: the internet connection.

Every digital activity, right from accessing SaaS applications and ERP systems to video collaboration and cloud platforms, opens a potential entry point for malicious actors. Malware, phishing links, ransomware payloads, and command-and-control traffic can all infiltrate a network through unsecured connectivity.

Firewall at the edge is no longer sufficient

The traditional approach to SME security looks like this: the business purchases an internet connection, gets operations running, and then, perhaps after a scare, perhaps on an IT consultant's recommendation, adds a firewall device at the network edge. Antivirus software is deployed on company machines. A VPN is set up for remote access.

However, these tools are ineffective when deployed in isolation. The problem is the architecture they create: security as a layer added on top of connectivity, rather than integrated into it. Connectivity without embedded security is not a neutral asset. It is a faster way to be breached.

For Indian SMEs accelerating their digital adoption, the attack surface has grown substantially. The perimeter that a traditional edge firewall was designed to defend no longer clearly exists.

From Edge Protection to Security in the Fabric

Modern cybersecurity strategies are increasingly moving toward “security in the fabric”, an approach where security is embedded directly within the network infrastructure rather than added as a separate layer.

In this model, connectivity and security work together as a unified system.

For example, solutions such as ACT Secured Internet Leased Line integrate firewall protection directly into the internet connection itself. This means that security inspection happens at the gateway where internet traffic enters the organisation, blocking malicious content before it reaches internal systems.

A managed firewall sits between the organisation’s internal network, its laptops, servers, and applications, and the internet. All inbound and outbound traffic passes through this security layer, enabling protection against threats such as malware, ransomware and other malicious activity.

This approach also simplifies operations for SMEs. Instead of purchasing and managing complex security hardware independently, businesses can rely on service providers to install, configure, update, and monitor the firewall throughout its lifecycle.

It reduces operational complexity and the burden on internal IT teams.

Securing the distributed workforce

Another key shift in modern network architecture is the move from traditional VPN-based access to more dynamic and intelligent networking frameworks.

Technologies such as SD-WAN (Software-Defined Wide Area Networking) are enabling organisations to connect distributed locations while maintaining centralised control and visibility.

For SMEs with employees working across multiple locations, including smaller cities and emerging digital hubs in Tier-2 and Tier-3 markets, this architecture provides several advantages.

Instead of routing all traffic through a central data centre, SD-WAN can intelligently route traffic across multiple connections while applying consistent security policies across the network. Modern networking approaches emphasize continuous identity verification.

The network does not automatically trust users simply because they are inside the perimeter. Instead, identity, device posture, and application access are validated at multiple points across the network.

This approach aligns with the broader Zero Trust security model, which assumes that threats may exist both outside and inside the network and therefore requires continuous verification.

Another major evolution in security is the integration of AI into threat detection systems. Many modern security devices incorporate AI-driven capabilities that continuously analyse traffic patterns, detect anomalies, and identify emerging threats.

For example, advanced firewall systems can detect unusual behaviour that may indicate malware activity or ransomware propagation and respond automatically to contain the threat.

These capabilities allow organisations to move beyond reactive security, where threats are addressed only after detection, toward proactive defence mechanisms that identify and neutralise threats earlier in the attack lifecycle.

A phased security journey for SMEs

While embedding security into infrastructure is essential, SMEs must also recognise that maturity in the security posture cannot be achieved overnight. Implementing enterprise-grade security architecture can be resource-intensive, particularly for businesses with limited IT staff.

A practical approach is to adopt security in phases:

- Start with secure connectivity by integrating firewall protection into internet infrastructure.
- Adopt managed security services to reduce operational burden.

- Introduce intelligent networking frameworks such as SD-WAN for distributed operations.
- Implement identity-centric security models aligned with Zero Trust principles.
- Provide network segmentation - isolate guest Wi-Fi to prevent their accessing internal systems.
- Opt for role-based access when there are a variety of user categories - for instance, admin staff, students, faculty using the university network for distinct needs.

By taking a phased approach, SMEs can progressively strengthen their security posture while maintaining operational efficiency.

Conclusion

As SMEs continue their digital journey, the role of network infrastructure will evolve beyond simple connectivity.

Networks will become intelligent systems capable of detecting threats, enforcing policies, and adapting dynamically to changing conditions.

In this future, security will not exist as a separate layer applied after deployment. Instead, it will be woven into the very fabric of digital infrastructure.

For India’s rapidly digitising SMEs, this evolution, from “firewall at the edge” to “security in the fabric”, will be essential for building resilient, future-ready businesses.