

SOLUTION BRIEF

Protect Campus Deployments With Fortinet FortiGate NGFWs

Executive Summary

The new campus deployment model supports growing corporate and educational campuses that need to connect and protect a growing number of buildings using the same network. Campus network security plays a critical role in this process, providing secure access to the internet and applications deployed in the data center and across multiple clouds. When done right, it can effectively protect networks from internal and external threats, including rising ransomware and command-and-control attacks that hide in encrypted flows. This goes well beyond the critical role of preventing attacks from entering the campus by detecting, minimizing, and containing those inevitable breaches that manage to bypass perimeter controls.

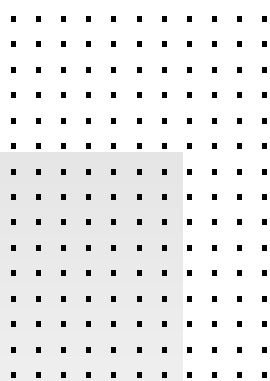
Accelerated convergence of networking and security

Today's networks are highly dynamic. One of the most challenging characteristics of the modern network is the degree of mobility enjoyed by today's workers, whether working remotely or wandering across campus. As the enterprise expands its various edges beyond the campus, it is the user rather than the perimeter that in many ways becomes the core that must be protected—and without impacting user experience. With the proliferation of devices and working-from-anywhere models, the attack surface dramatically increases as it follows the user. Today's campus network security needs to meet users where they are, allowing security to seamlessly follow applications, workflows, and other activities end to end, even when the origin and destination move mid-transaction.

This paradigm shift away from a traditional, fixed-in-place security model requires greater visibility and contextual awareness wherever the user travels, whether throughout the campus network, off-premises, or even off-network. The more you can see, the more you can protect. Broad visibility enables maintaining a strong security posture throughout the network. But enabling proactive protection across today's highly dynamic network environments requires the convergence of networking and security into a single device. Security-Driven Networking is increasingly essential for protecting today's complex networks while maintaining productivity and user experience. And it is a crucial advantage delivered by the Fortinet FortiGate next-generation firewall (NGFW).

Fortinet FortiGate NGFWs enable organizations to build security-driven networks that weave security into the IT architecture. This allows them to secure any edge at any scale—regardless of how dynamic that edge might be, providing more visibility and consistent, coordinated end-to-end policy enforcement to maintain a seamless user experience.

Fortinet FortiGate NGFWs are powered by the world's only security processing units (SPUs), delivering the industry's highest security compute rating for both Layer 4 and Layer 7 advanced security features compared with competing firewalls. In addition to a robust portfolio of advanced and fully integrated security functions, the Fortinet FortiGate NGFW also includes a broad portfolio of cutting-edge FortiOS innovations, like integrated Zero Trust Network Access (ZTNA) and real-time video filtering. These devices have also been enhanced with artificial intelligence/machine learning (AI/ML)-driven FortiGuard services to deliver an intuitive, automated, and easy-to-manage NGFW platform. Because of the high degree of innovation packed into every device, they are better able to manage risks, reduce costs, and streamline operations, allowing customers to scale their business and avoid business disruptions.



Fortinet FortiGate next-generation firewalls (NGFWs) enable organizations to build security-driven networks that weave security into the IT architecture.

Protect, Consolidate, and Automate With Fortinet FortiGate NGFW Solutions

Protect: Managing campus security risks without comprising user experience

Protecting the campus network remains a top priority for IT teams. But so are availability and adaptability. And while the requirement to prevent attacks has not changed, the environments needing to be protected have. Security and networking leaders need complete visibility of their campus deployment, including every device and user, to prevent known and unknown threats. This requires weaving security and networking into a single solution so everything on the network can be seen and addressed. Seeing more—devices, users, applications—provides additional context, which helps drive stronger, more effective policies. But just seeing isn't always enough. The FortiGate firewall is designed to also provide contextual awareness, thereby enabling and maintaining a fortified security posture across the campus network.

As more devices connect to the campus network, the FortiGate firewall can discover and control Internet-of-Things (IoT) devices, operational technology (OT) environments and systems, and a variety of users. It does this through an assured access strategy that leverages things like device posture, operating system, patch status, and more. This enables the delivery of continuous user authentication through its unique ZTNA technology, providing consistent security policy to users as they roam in and out of the campus.

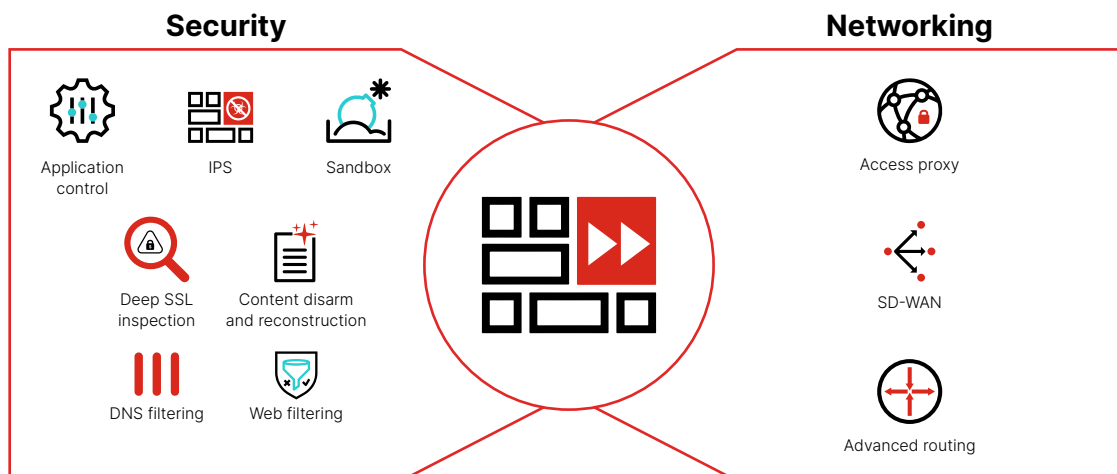
Another unique strategy provided by the Fortinet FortiGate NGFW is its ability to minimize the attack surface with advanced inspection, dynamic network segmentation, and consistent policy application across the entire campus network. It can enforce access policies and limit access to specific resources per user and at the port level. It does this through its integration with the Fortinet network access control (NAC) solution and by leveraging the native integration of the Security Fabric with Fortinet switches and access points for granular access control. And it gathers and responds to informative telemetry through a fabric of interconnected security products to detect and prevent zero-day threats and ransomware in real time, powered by actionable threat intelligence provided by FortiGuard Labs.

Consolidate: Lowering TCO without sacrificing their security posture

Leaders can better protect their campus network with enterprise-grade security when delivered by the industry's fastest and most price-competitive solution. Because the Fortinet FortiGate NGFW is designed to perform processor-intensive functions at network speeds, organizations can confidently consolidate services like intrusion prevention system (IPS), secure sockets layer (SSL) inspection, application protection, web filtering, anti-malware, and more on the FortiGate firewall. These services can all be run simultaneously without compromising throughput or network uptime. This is all enabled by the performance-enhancing innovations provided by FortiGate's advanced security processors.

Driving all of this functionality is FortiOS, which ensures that the entire portfolio of products supporting the Security-Driven Networking vision can be delivered in any environment and form factor. This allows security to be deployed consistently on campus, in the cloud, across the wide-area network (WAN), and even in DevOps containers. By implementing a single security system everywhere across the network, organizations can establish and maintain a superior level of network execution, security, and support all through a single vendor.

Feature Consolidation on Fortinet FortiGate NGFWs



Automate: Simplifying operations through automation provides greater visibility and control

Leaders are under pressure to adapt and scale business efforts across their expanding networks. To do this safely, they need to implement new protective measures to provide comprehensive security. With the Fortinet Fabric Management Center (FMC) controlling all FortiGate firewall deployments, IT leaders can streamline firewall and policy management across the entire campus network and all network edges, providing automatic updates to all the network protective devices from a single console.

Simplify your security posture by utilizing application programming interfaces (APIs) and fabric connectors in concert with your FortiGate firewall to normalize security across multiple clouds and allow users to access applications from wherever they are located, leading to simplified operations with the Fortinet Security Fabric ecosystem.

Advanced Firewall Function Powered by Real-time Threat Intelligence

NGFWs need to filter and inspect network traffic to protect an organization from internal and external threats. Today's NGFWs possess deeper content inspection capabilities to identify and block zero-day attacks, advanced malware, ransomware, and other threats. They also need to provide SSL inspection (including TLS 1.3), application control, intrusion prevention, and complete visibility across the entire attack surface. However, as the threat landscape rapidly expands due to co-location and multi-cloud adoption, and as businesses grow to satisfy escalating customer and user needs, traditional NGFW solutions fall behind because they cannot offer protection at scale. This leads to poor user experience, fragmented visibility, and a weak security posture. Today's NGFWs need to not only block malware but also scale with the network. This also needs to include a pathway for maintaining the flexibility they need to evolve with the threat landscape and keep the network secure as new threats arise and new networking strategies are embraced.

In addition to the industry's only purpose-built security processors and robust FortiOS operating system, Fortinet NGFWs are uniquely suited to remain ahead of today's evolving threat environment through their integration with Fortinet's advanced threat intelligence and research organization, FortiGuard Labs. Comprised of experienced threat hunters, researchers, analysts, engineers, and data scientists—and the world's most advanced AI system designed for threat discovery and analysis—its mission is to provide customers with the industry's best threat intelligence to protect them from today's malicious cyberattacks, through reports, threat updates, coordination with top threat researchers and law enforcement agencies, and daily threat feeds to FortiGate devices deployed around the world. These efforts keep Fortinet security products armed with the best threat identification and protection information available and keep Fortinet customers informed of the latest threats, campaigns, actors, and trends so they can take proactive measures to better secure their environments.

Delivering Advanced Security to Every User, Device, and Edge

A Fortinet FortiGate NGFW delivers comprehensive enterprise visibility and security to protect any user, device, or edge in any location. Fortinet NGFWs also enable the deployment of a Zero Trust Architecture to allow users to securely access the applications and resources they need to do their jobs—from anywhere and at any time—through continuous authentication, effective and dynamic compliance, and adaptable security controls.

Fortinet's industry-leading Security-Driven Networking solutions seamlessly weave security, networking, and essential AI/ML-powered FortiGuard services into a single platform. This integrated approach can better manage today's risks and adapt to today's dynamic network environments to avoid business disruptions, eliminate multiple point-product complexities, and achieve the industry's lowest total cost of ownership (TCOs). Its unique Security-Driven Networking strategy tightly integrates an organization's network infrastructure and security architecture, enabling the network to scale and change without ever compromising security operations or creating exploitable security gaps.

This new next-generation approach is essential for effectively defending today's highly dynamic environments—not only by providing consistent enforcement across today's highly flexible perimeters but by weaving security deeply into the network itself.

Security Designed for the Way You Need To Run Your Business

Today's threat environment is constantly changing. From distributed denial-of-service (DDoS) attacks to ransomware, cyberattacks' frequency, volume, and sophistication show no signs of slowing down. All organizations require security capable of supporting their unique network environments because even a minor disruption to the network infrastructure—even a minute of downtime or a lag in service performance—can cause damage to an organization's reputation, bottom line, or even long-term



viability. And catastrophic cyberattacks, which often begin as seemingly benign intrusions that inadequate network security tools failed to catch, can force organizations to pay crippling fines and even close their doors for good. The challenge is, few traditional NGFW solutions are up to the task.

Fortinet FortiGate NGFWs are designed from the ground up to provide adaptable enterprise-class security to protect any user, any edge, and at any scale across your campus, data center, remote workers, and multi-cloud deployments. As companies expand beyond the data center due to the transition to a hybrid workforce and evolving user expectations, campus deployment becomes equally important as the core user. Security must provide a seamless experience across the variety of applications, networks, and associated functions that the user performs.

For more information, please visit our website at <https://www.fortinet.com/products/next-generation-firewall>.



www.fortinet.com