SOLUTION BRIEF

Secure Remote Connectivity with FortiGate NGFW

Executive Summary

After the rapid shift to hybrid work, many organizations now rely on virtual private networks (VPNs) so their employees can remotely access corporate resources. Virtual private networks were developed to protect sensitive company data by establishing a secure connection to the corporate network. However, VPN does not provide many essential security functions that today's businesses require. Sixty-two percent of organizations have experienced a security breach that they can attribute to their remote workforce.[1] This includes criminals breaching a home network and hijacking the VPN connection to access the corporate network. The truth is that VPN's legacy, perimeter-based approach is simply inadequate for today's dynamic network edges and evolving cyber landscape.

The average total cost of a data breach was nearly $1 million greater when remote work was a factor in causing the data breach.[2]

Zero-trust network access (ZTNA) is a better approach. It offers controlled remote access to applications that is easier and faster to initiate than VPN, combined with a granular set of security protections, such as per-user authentication, connection monitoring, and encrypted traffic inspection. However, ZTNA solutions can be challenging to deploy as they require interconnecting technologies not designed to work together. FortiGate Next-Generation Firewalls (NGFWs) resolve this issue by being the only network firewall to deliver unified networking and security across all attack surfaces, including built-in ZTNA. FortiGate NGFWs simplify secure connectivity and provide seamless access to applications wherever a user or application may be located.

FortiGate NGFWs also provide a wide range of additional advanced security, including the ability to be deployed as part of a hybrid mesh firewall (HMF) architecture, built-in SD-WAN, dynamic network segmentation, and converged networking and security functionality. When deployed as part of a cybersecurity mesh architecture, FortiGate also provides single-pane-of-glass management, making security visibility and policy orchestration less complex and more flexible across all network edges.

VPN: Not Enough for Secure Remote Access

A VPN is designed to extend the corporate network by providing encrypted connections over an internet connection. This enables everyone working remotely to securely log in to the shared company network while protecting a user's identity when using public Wi-Fi. But, while VPN may provide fast and secure connections, once an attacker has gained access to it by breaching the end-user device or local network, they also gain access to the entire network, putting the whole organization at risk. And a VPN cannot protect users from insecure HTTP connections, tracking cookies, and blocking malware due to its lack of security features.

Virtual private networks also have usability challenges. Connections are often complicated, initiating calls to help desk services. The encryption process and unreliable internet connections can reduce application performance and cause latency in critical business applications, such as videoconferencing. This can result in reduced employee productivity and poor user experience.

Organizations need a more secure and effective connection process to protect their networks, applications, devices, and users, regardless of location.

FortiGate NGFW: Redefining Security Rules at Every Edge

Given the rising rate of security outbreaks and the demands of today's hybrid work model, organizations recognize the need to enhance their remote access solutions with more comprehensive security. FortiGate NGFWs provide organizations of any size with enterprise-grade protection against ever-evolving cyberattacks across all edges—from corporate networks and data centers to cloud applications to remote users—combined with advanced application connection and authentication services.

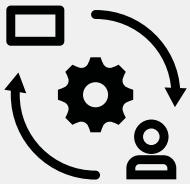
Zero-trust remote access

Fortinet includes encrypted VPN and ZTNA capabilities in our FortiGate NGFW devices and FortiClient agents without an additional license. FortiGate is the only network firewall with built-in ZTNA, offering advanced secure remote connectivity for application access. Our unique Universal ZTNA approach makes it easy for IT teams to extend a zero-trust model beyond their corporate networks, covering users whether they are remote or on-premises. This gives organizations the flexibility they need to control access to applications that is easier and faster to initiate while providing a more granular set of security protections than traditional VPNs.

Consistent protection across networks, devices, and users

FortiGate NGFWs enable IT to effectively combat advanced cyber threats and avoid business disruptions through artificial intelligence (AI)-powered security protection, including IPS, antivirus, DNS and URL filtering, application control, and more. And these robust solutions extend beyond the network to FortiClient endpoint agents, ensuring unified security for every edge while providing users with comprehensive protection and secure connections regardless of location.

57% of cyberattacks occurred while using a VPN, accounting for $6.9 billion in losses.[3]



By 2025 at least 70% of new remote access deployments will rely on ZTNA rather than VPN services.[4]

High-performance, secure network

FortiGate appliances use purpose-built ASICs to accelerate network functions and security services. This reduces CPU usage by taking advantage of custom-designed hardware acceleration. And for virtual and cloud-based instances, Fortinet has optimized its software for general-purpose and cloud processors.

Centralized control and access verification

FortiGate helps organizations simplify management by enforcing the same zero-trust access policy whether users are on or off the network. FortiGate and FortiClient work together seamlessly to provide ongoing verification, allowing users to securely access the applications and resources they need to do their jobs through continuous authentication, effective and dynamic compliance, and adaptable security controls.

Unified management and visibility

Critical components of Fortinet's Hybrid Mesh Firewall solution include comprehensive visibility, consistent policy enforcement, and unified management that extends to all edges. This unified security platform approach enables coordinated protection across enterprise IT, including corporate sites, branches, data centers, public and private clouds, and remote workers. Whether you have all on-premises firewalls, all cloud firewalls, or a mix of both, Fortinet helps you simplify operations, reduce complexity, and enable broad automation to increase operational efficiency while securing every user and resource everywhere.

FortiGate Benefits

Today's users must connect to any resource from any location using any device. FortiGate NGFWs are designed to support today's hybrid environment by providing comprehensive protection and cost-effective remote access to optimize employee productivity and business efficiency.

FortiGate NGFWs deliver several benefits for organizations when managing secure connections for remote users:

- **Enhanced security to reduce data breaches:** With its integrated ZTNA capabilities, a FortiGate NGFW acts as a ZTNA gateway to automatically inspect all traffic and block suspicious activities to prevent hackers from entering the network. Its cost-effective protection enables the seamless deployment of ZTNA without additional cost.
- **Simplified access control:** Unlike a traditional VPN, FortiGate has built-in ZTNA capabilities that allow IT to establish granular access policies with individual application-level controls for both on-premises and remote users.
- **Simplified network management:** FortiGate eliminates different access controls for on-premises and cloud applications for network-based and remote users. IT teams can have consistent policies and comprehensive visibility to control user access to applications regardless of where the users are located, or applications are deployed.
- **Easy transition from VPN to ZTNA:** Fortinet delivers VPN and ZTNA capabilities using the same combination of FortiGate NGFW and FortiClient agents. This allows organizations to operate a mixed VPN and ZTNA approach and easily transition to ZTNA-based access to applications at whatever pace suits them.
- **Consistent user experience:** FortiGate NGFWs deliver consistent levels of security for application access, regardless of user or application location. Users can be granted access to applications without establishing a separate VPN connection or knowing where the application is located.

Conclusion

Individual and corporate data must be consistently protected end to end as it moves across applications, devices, and geographical boundaries. This requires security to seamlessly extend to the farthest reaches of the network. It must also be found at every point of data interaction to ensure data privacy, confidentiality, and origin authentication.

FortiGate NGFWs are designed to provide adaptable enterprise-class protection to safeguard any user, any edge, and at any scale. With its fully integrated Universal ZTNA functionality, FortiGate helps organizations gain visibility into and control what's connected to a network to ensure secure access from anywhere to everywhere.

[1] Fortinet, 2023 Work-from-Anywhere Global Study Report, March 7, 2023.

[2] IBM, Cost of a Data Breach Report 2022, July 2022.

[3] Forbes Advisor, VPN Statistics And Trends In 2023, February 9, 2023.

[4] Gartner, Gartner Identifies Three Factors Influencing Growth in Security Spending, October 13, 2022.

June 17, 2023 8:19 AM
2173797-0-0-EN