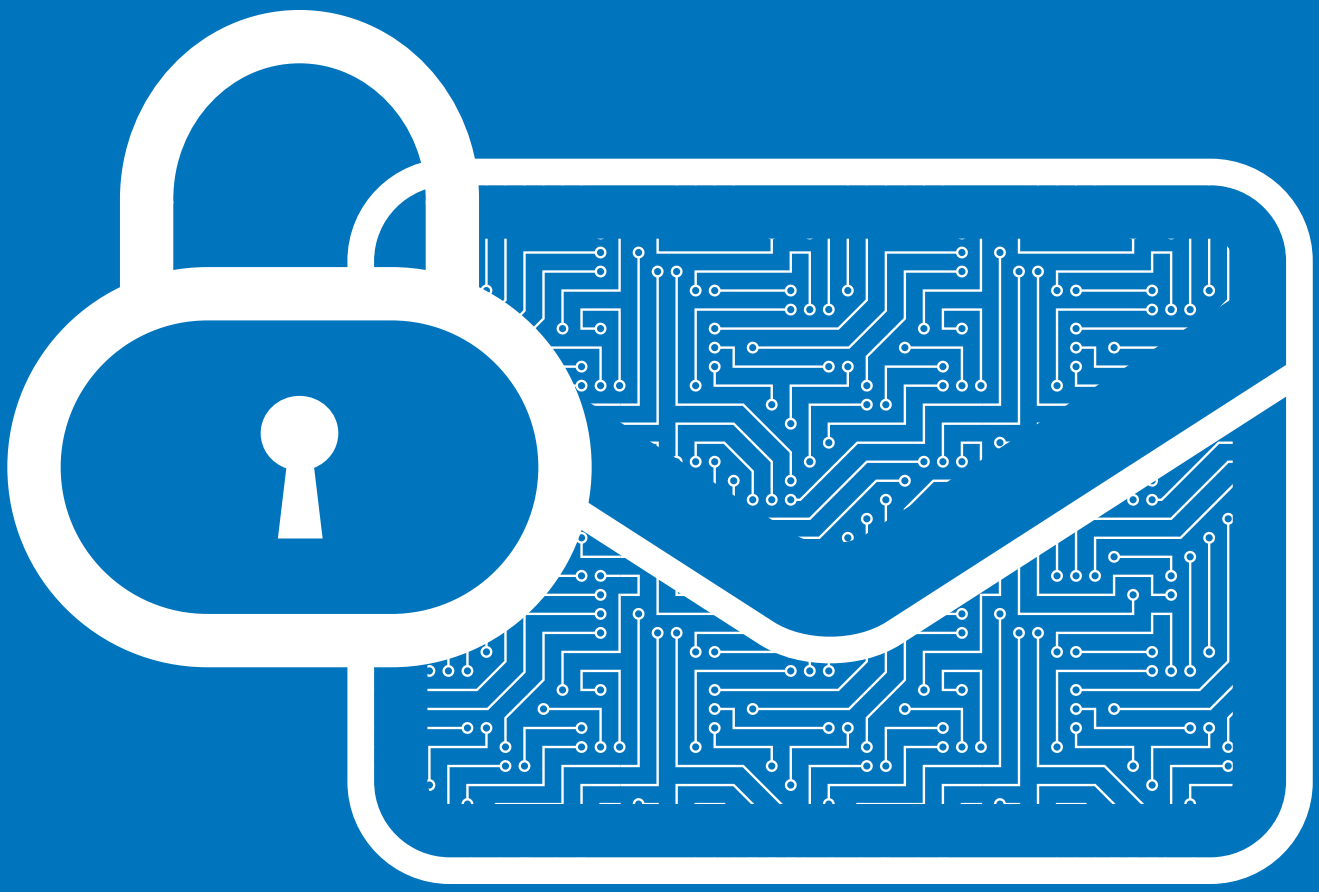
PeerPaper™ Report 2021

What to Consider When Choosing a Next-Generation Firewall (NGFW)

Based on real user reviews of Fortinet FortiGate



IT Central Station
Unbiased reviews from the tech community

ABSTRACT

The prevalence of remote work, cloud computing and the challenges of dealing with branch offices have rendered the traditional perimeter-based security model obsolete. As users gain access to systems and data from virtually any device and any location, the traditional firewall is less and less effective. Nor is the data center still the core of a digital organization. The Next-Generation Firewall (NGFW) provides a solution by adding device filtering, edge security and SD-WAN to protect users and data. This paper explores key selection factors for an NGFW, based on real user experiences with the Fortinet FortiGate NGFW on IT Central Station.

CONTENTS

INTRODUCTION

The increase in remote work, a necessity during the pandemic but now becoming the norm in many companies, has challenged notions of traditional perimeter-based security on many levels. The standard firewall will no longer suffice as users access systems and data from virtually any device and any location. The data center is no longer the core. Indeed, some of the data they seek is not even located behind the firewall at all. It's in the cloud or Software-as-a-Service (SaaS) applications. Network edges are expanding, not just to accommodate remote workers, but also to support branch offices, remote campuses and the like.

While the data center is still vital to host business critical applications and data that can't be moved to the cloud for intellectual property and compliance reasons, hybrid deployments are becoming more prevalent as people and digital assets spread out geographically. However, as the network edges expand, so does the attack surface. This reality necessitates a stronger security posture to protect employees and data. The Next-Generation Firewall (NGFW) offers a solution. It adds functionality like content security, web filtering, edge security and Software-Defined Wide Area Network (SD-WAN) to defend users and digital assets alike in this new era of security. As part of the Secure Access Service Edge (SASE), the NGFW either natively integrates or works with Zero Trust Network Access (ZTNA) to secure the workforce transition without compromising user experience.

The rapid pace of change and evolution of security models can make it challenging to identify the right NGFW solution. This paper looks at key considerations in choosing an NGFW. Based on real user experiences with the Fortinet FortiGate NGFW, also known as Network Firewall, it discusses factors like segmentation, performance, visibility and more to guide potential NGFW buyers to select a solution that will meet their needs.

The Context: Safely Connecting Remote Workers

The changes in the security landscape that have led to the creation of the NGFW predate the current move to widespread remote work. However, the last year and a half has seen a substantial and likely permanent shift in the way employees interact with their companies. People can be anywhere on any device. Figure 1 shows how things have changed, with the legacy architecture at the core now having to connect with remote users, branch offices, cloud assets and SaaS.

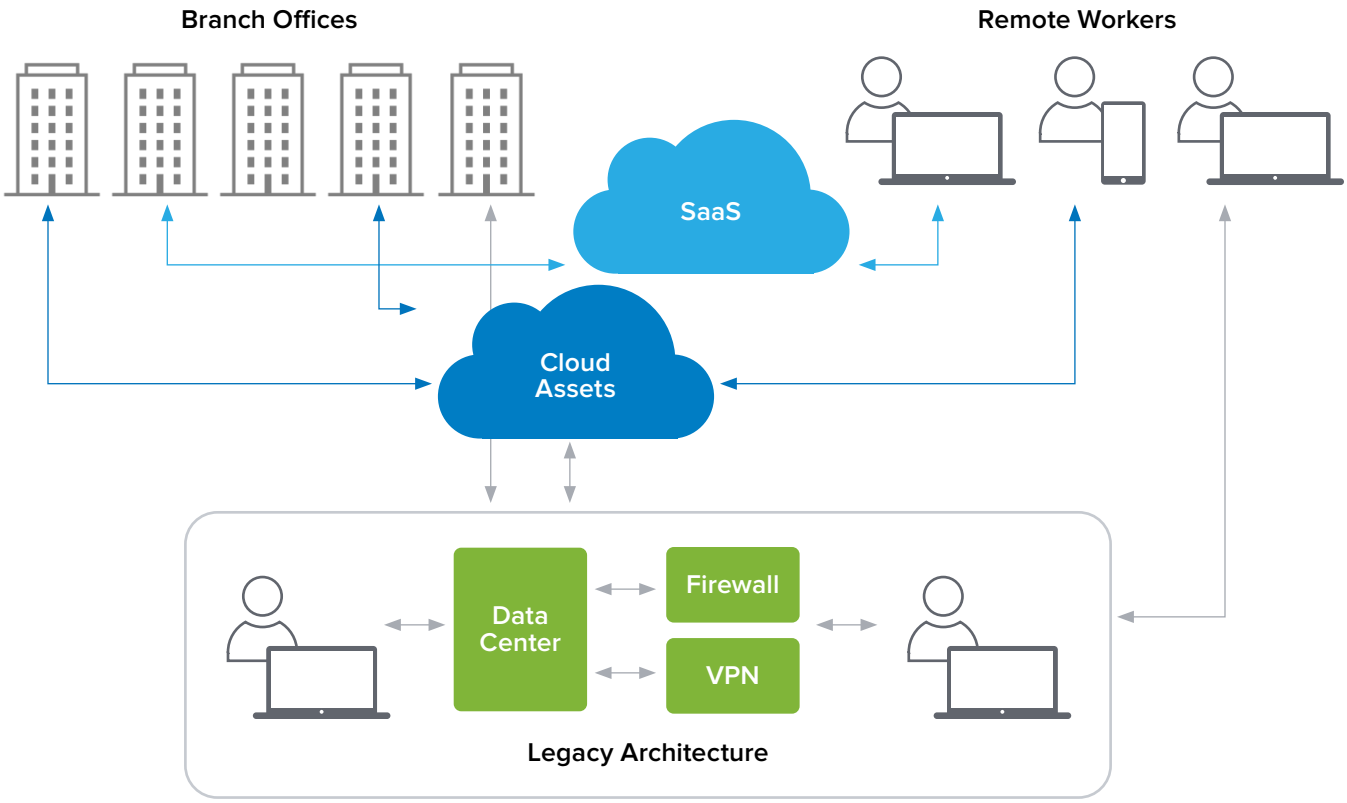


Figure 1
The new network reality: Remote users, branch offices and cloud computing complicate secure connectivity.

Security professionals and network managers are adapting in response. For example, according to a Sr. Network Engineer at a pharma/biotech company with more than 5,000 employees, "With the COVID pandemic, the VPN has become the most valuable feature. With the majority of traffic connecting from remote locations, the VPN provides stability and reliability."

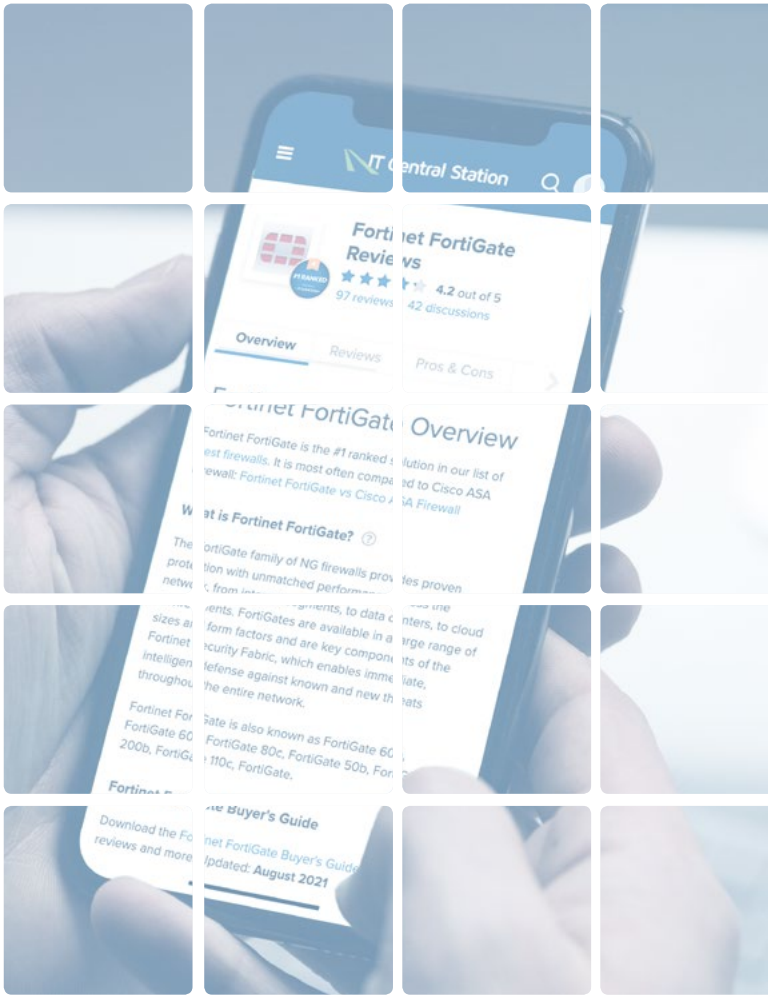
Recent events have also highlighted the importance of allowing IT staff to work remotely. In this context, the Owner of Tech Exchange, a small consultancy, uses FortiGate firewalls because he finds it makes remote access simple.

He also values how the included client works with MacOS Windows and IOS devices. An IT Infrastructure Specialist at a government agency with over 1,000 employees also commented, "It has provided us the ability to work remotely during the pandemic. It opens a secure connection to the office for an employee working remotely from home."

> **"It opens a secure connection to the office for an employee working remotely from home.**

NGFW Use Cases

IT Central Station members are putting NGFW solutions to work in the data center and across campuses, among many use cases. An IT Infrastructure Engineer at Communication Progress, a tech services company, deploys his NGFW to protect clients' internal networks with data center firewalls and internal segmentation. For a Senior Network Architect at Combat Networks, a small communications service provider, his clients' main use case for Fortinet FortiGate is the firewall on the outside perimeter to the internet. Some of his clients have started using FortiGate for SD-WAN as well.



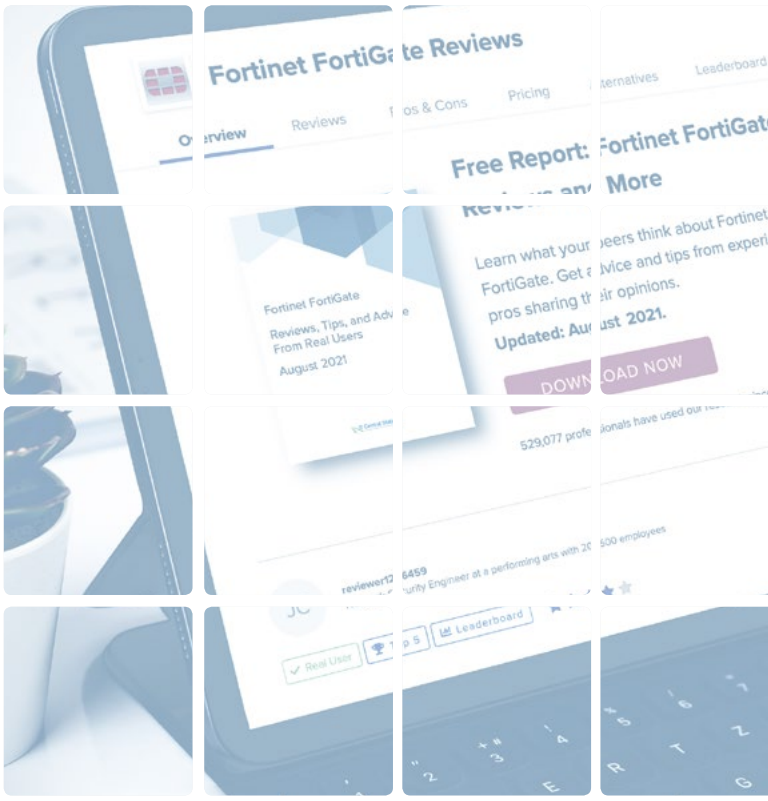
"We use the FortiGate firewall for our centralized management services," said a Deputy Manager Of Information Technology at Nitco Limited, a construction company with over 1,000 employees. He added, "We have SAP and there are multiple work-from-home users that connect using the VPN to access it. Also, we have some applications that are hosted on the server and we have assigned a public IP through the firewall for them."

Providing endpoint security for small offices is the NGFW use case pursued by the President of Sovereign Managed Services, an IT service provider. Their goal is to provide intrusion protection for small offices that need HIPAA compliance. For an IT & PPN Coordinator at a manufacturing company with 45 branches, FortiGate 200 series models in their data centers have centralized connectivity between the different branches and the data centers. A financial services firm with branches in the UK, Brazil and Singapore use their NGFW for its Unified Threat Management (UTM), along with access to a VPN.

Selection Factors

What makes for a good NGFW solution? Many factors affect the suitability of an NGFW for a given organization. At a high level, it must advance the cause of robust security, as a System Administrator at a small media company related. He said, “There have been a number of high-profile security issues in our industry. This [Fortinet FortiGate NGFW] has brought us to a higher standard of security, which our clients are very keen on these days.”

A Director at a small system integrator similarly found that his NGFW led to better security posture, with safe web surfing, less spam and viruses in incoming email messages as well as very granular AppControl. His NGFW also blocked vulnerability exploitation attempts and detected traffic anomalies in order to prevent Denial of Service (DoS) attacks. Other NGFW selection factors include qualities like reliability, flexibility and scalability, coupled with threat management and edge security capabilities.



Reliability, Flexibility and Scalability

An NGFW must be flexible and scalable. It also has to be reliable. These are characteristics that do not always coexist in the same product. The Owner of Tech Exchange found, however, that FortiGate firewalls are very reliable. He claimed, “in the past 15 years I believe only 2 devices in 100 have failed. The failures were due to harsh environments (dust and water will ruin any electronic device).”

He added, “I would highly recommend the stability / reliability of FortiGate. Once installed it

will do its job efficiently and effectively for several years. At the end of the day, the solution is very flexible, and if the client has special business partners that want a special type of nailed up VPN or special configuration for the clients, it offers that."

> **The virtual machine (VM) version of FortiGate with the hardware appliances is widely scalable.**

"Overall stability of the solution is good," explained the pharma Sr. Network Engineer. He then added, "I am totally dependent on this device." A Service Delivery Engineer at a tech services company felt that the virtual machine (VM) version of FortiGate with the hardware appliances is widely scalable. He elaborated, saying, "It can handle small businesses to large scale enterprises. In terms of mode of deployment, you have VM, hardware appliance, and cloud. There is cloud management as well that is scalable. It can suit a number of deployment scenarios."

Threat Protection

An NGFW will ideally help with threat management while it detects and blocks threats. In the case of Fortinet, FortiGuard Labs provides threat intelligence for the company's portfolio of security products, including FortiGate. Users commented on this capability, with a Technical Account Manager at DSM Technology Consultants, a small healthcare company, remarking, "The next-gen features, the unified threat management capabilities are something that just about everybody is interested in at this point." A Manager of IT at Mosambee, a small software company, said that his company uses FortiGate Sandbox to detect zero-day vulnerabilities, such as anomalies or malware, that are unknown and have not yet been discovered.

Edge Security Capabilities

As corporate campuses and branch offices proliferate and users are increasingly outside the data center, the edge becomes a critical attack surface. An NGFW needs to provide edge protection. As an IT Operations Director at a tech services company put it, "We primarily use the solution for edge protection as well as the VPN and SD-WAN." Figure 2 depicts how the edge is becoming the primary point of connection for all users, even those who are located on site.

> **Fundamentally, its primary purpose is security at the edge of the network.**

A Solutions Engineer/Consultant at a small tech services company similarly noted, "Fundamentally, its primary purpose is security at the edge of the network." He has clients who use the SD-WAN feature for multi-location setups. Other clients employ IPSec [IP Security] tunnels. The Senior Information Security Consultant at Alkhorayef valued the fact that FortiGate NGFW delivers "a security-driven networking WAN edge transformation in a unified offering."

SD-WAN

FortiGate firewalls enable the creation of an SD-WAN, which the Senior Information Security Consultant at Alkhorayef has implemented in 15 locations. He said it is "working extremely well." A Technical Services Manager at ProComm

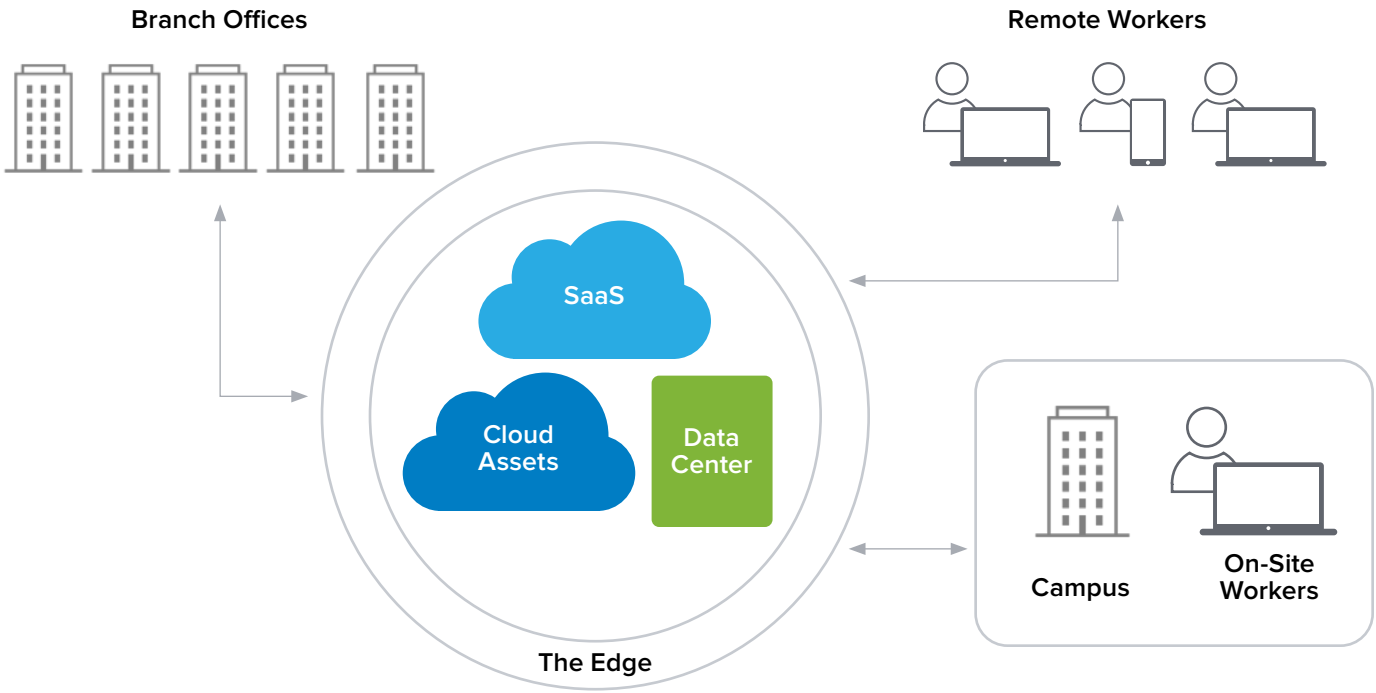


Figure 2
The edge as the primary point of connection for all users and devices.

Technologies, a small tech services company, concurred, saying, "The SD-WAN feature is the most valuable. This feature evolved from link load balancing. It has helped us in terms of our uptime and privatizing applications whenever we experience an outage. The SD-WAN feature has been a plus for us."

Web Filtering and Anti-Virus

An NGFW serves as a filter on malicious content. A Senior Scientist at ATS, Inc., a small consultancy, spoke to this requirement when he said, "This solution allows solid VPN service for access from the field, and the anti-virus/anti-malware detection works well." The Owner of Computech Associates, a small tech services company, made a comparable remark, indicating, "The web filtering facility and application control are the most valuable features from the point of view of our clients."

Other notable comments about filtering and anti-virus included:

- "Customers are more inclined towards FortiGate because of application control, web filtering, and anti-spam features." - CEO at Acme Technologies, a small software company
- "The solution has very good threat and content filtering switches." - Director at a small tech services company
- "We use the filtering feature the most. It has filtering and inbuilt securities. We can create customized rules to define which users can access a particular type of site. We can create

policies inside the firewall." - Deputy General Manager Information Technology at a media company with over 200 employees

- "The solution has built-in features for web filtering that are great. It categorizes it nicely for you." - Network Security Engineer at a performing arts company with over 200 employees

Segmentation

Network segmentation is now a "must have" attribute to build defense-in-depth for digital assets. Segmentation reduces the attack surface, making it harder to attackers to move laterally across networks. It is a core principle of ZTNA. The NGFW supports segmentation, as the Manager of IT at Sfn explained. He said, "We are using network segmentation. Based on the segmentation, there are policies. Based on the policies, the traffic to the critical components is monitored and goes through the IDS/IPS antivirus profile."

The Chief Information Officer at an analyst firm with over 10,000 employees also uses FortiGate for network zone segmentation. A Sales Engineer at a tech services company with over 200 employees - shared, "We primarily use the solution just for internal segmentation and connection of some ranges using IPSec."

Cloud Capabilities

Cloud functionality is an essential factor to consider when selecting an NGFW. FortiGate users acknowledged the importance of NGFW cloud functionality, with the tech services Sales Engineer, for example, saying, "The solution's most valuable aspect is the IPS for potential mitigation from the cloud inside our network." The Solutions Engineer/Consultant echoed this sentiment. He said, "One of the nice things about FortiGate is that it can be deployed on the cloud or on-premises. You can actually do both. That's the biggest reason why I stick with this solution as opposed to something like Cisco Meraki."

> **"One of the nice things about FortiGate is that it can be deployed on the cloud or on-premises.**

Integration

IT Central Station members discussed how an NGFW has to integrate with multiple systems. The Service Delivery Engineer observed, "The solution integrates well. It provides a full end-to-end security suite." For the IT Infrastructure Engineer at Communication Progress, FortiGate's SD-WAN, security fabric integration, two-factor authentication, ADVPN, dynamic routing, single pane of glass managements "are great features." A Solution Architect at Brillbean Ventures Pvt Ltd, a small marketing services firm, likewise related, "This solution made it easier to connect all of the branches together via an IPsec VPN and remote users with SSL VPN."

> **"The solution integrates well. It provides a full end-to-end security suite.**

Visibility

Visibility is one of the most important elements of an effective NGFW solution. As security professionals know, the more you see, the more you can protect. The Solution Architect at Brillbean Ventures has found this to be the case with FortiGate. In his experience, FortiGate provides comprehensive visibility and advanced

layer 7 security, including threat protection, intrusion prevention, web filtering, and application control. He added, "The solution provides a high-performance inspection of clear-text and encrypted traffic."

Performance

NGFWs must maintain high performance with limited impact to the network uptime. They should not impede network performance if at all possible. "The firewall throughput is very good," said a Solution Architect at a tech services company. He then shared, "Most of the customers in this region use FortiGate for their data center firewalls, and the main reason is because of its high throughput." The Senior Network Architect at Combat Networks discussed how FortiGate's specific chip sets serve to accelerate different features in the product. The result was improved NGFW performance.

Analytics and Reporting

Several FortiGate users on IT Central Station alluded to the significance of analytics and reporting features in an NGFW solution. A Director at a small consultancy, for instance, felt that good reporting was one of the solution's key features. He said, "You can receive many details from the connection, for example, clients and website information. Additionally, you can determine if an action has taken place such as virus scan information."

> **It can give you a better understanding of what is going on in your network.**

Regarding the FortiAnalyzer, the NGFW's analytics tool, the Director at the small system integrator observed, "It can give you a better understanding of what is going on in your network. When FortiGate sends logs to FortiAnalyzer, FortiAnalyzer inserts received log data into the database. Predefined and customizable data queries, charts and reports can significantly help you by visualizing problem points, so you can thoroughly investigate security events and traffic behavior anomalies."

Ease of Use/Single Pane Management

Firewall administrators appreciate solutions that are easy to set up and use. The Fortinet Management Center provides this capability, with users like a Sr. Corporate Marketing Executive at Amity Infosoft Pvt. Ltd., a tech services company, rating the solution's "single pane of glass management" as one its most valuable features, along with its easy graphical user interface (GUI) for monitors.

> **FortiOS has a very good, intuitive GUI.. easy to use and flexible... it gives you a simpler way to operate."**

A Sales Engineer/Technical Support Engineer at a small tech services company also valued how the SD-WAN's functionality puts all its security features in one device. He said, "We can manage from one single console SD-WAN and the security policy. You don't need to buy two separate devices for two functionalities. Single pane of glass, easy policy management."

The Solutions Engineer/Consultant also liked the single pane of management, saying, "I can deploy their line of firewalls in conjunction with their switching and access points, and I can manage

the entire network from one interface. I don't have to log into one interface for the firewall, another one for the access points, and another one for the switches."

For a Lead Architect at a small software company the NGFW features were "relatively easy to implement," while the IT Infrastructure Engineer at Communication Progress also related that Fortinet "is easy to implement." In contrast, he said, "Cisco and Check Point are a little bit more difficult in that aspect."

"FortiOS has a very good, intuitive GUI," said a Network Engineer at Concentus, a small tech company. A General Manager at a real estate/ law firm with more than 500 employees felt the same way, finding the solution "easy to use and flexible." The Director at the small system integrator put it this way: "When you have such management plane consolidation it gives you a simpler way to operate."

Total Cost of Ownership (TCO) and Return on Investment (ROI)

Cost is always a selection factor for NGFW, as it is for any IT or security solution. Experienced users understand that pure costs are not the only factor, that return on investment (ROI) may matter more. However, saving money is seldomly discouraged. An IT Manager at Riphah, a university with over 1,000 employees, found FortiGate reasonably priced compared to competing solutions like Sophos. The Senior Network Architect at Combat Networks simply stated, "Fortinet FortiGate's pricing is pretty hard to beat."

> **"Excellent ROI. Since implementing, the total cost of ownership (TCO) has been lowered...**

"Excellent ROI," is how the Sr. Corporate Marketing Executive at Amity Infosoft characterized his experience with FortiGate, due to virus spambot intrusion free network. The Senior Information Security Consultant at Alkhorayef commented, "Since implementing, the total cost of ownership (TCO) has been lowered and the day-to-day security operations have been simplified through our FortiOps services." The Senior Information Security Consultant at Alkhorayef similarly related that Fortinet Secure SD-WAN delivered the lowest total cost of ownership (TCO) per Mbps among all other vendors.

CONCLUSION

Everyone's definition of the right NGFW solution will be different, based on myriad unique organizational requirements. IT Central Station members who use Fortinet FortiGate feel, in general, that reliability, flexibility and scalability are among the prime selection factors for an NGFW, as are threat protection, edge security capabilities, SD-WAN and web and content filtering. Segmentation is essential to success and prevent lateral spread. So are cloud capabilities and broad integration. An NGFW should enable high visibility while delivering ease of use and strong performance. When an NGFW solution can meet these criteria, it is able to fulfil the new, challenging mission of the firewall in a perimeterless world.

ABOUT IT CENTRAL STATION

User reviews, candid discussions, and more for enterprise technology professionals.

The Internet has completely changed the way we make buying decisions. We now use ratings and review sites to see what other real users think before we buy electronics, book a hotel, visit a doctor or choose a restaurant. But in the world of enterprise technology, most of the information online and in your inbox comes from vendors. What you really want is objective information from other users. IT Central Station provides technology professionals with a community platform to share information about enterprise solutions.

IT Central Station is committed to offering user-contributed information that is valuable, objective, and relevant. We validate all reviewers with a triple authentication process, and protect your privacy by providing an environment where you can post anonymously and freely express your views. As a result, the community becomes a valuable resource, ensuring you get access to the right information and connect to the right people, whenever you need it.

www.itcentralstation.com

IT Central Station does not endorse or recommend any products or services. The views and opinions of reviewers quoted in this document, IT Central Station websites, and IT Central Station materials do not reflect the opinions of IT Central Station.

ABOUT FORTINET

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network—today and into the future. Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud, or mobile environments. Fortinet ranks number one in the most security appliances shipped worldwide and more than 500,000 customers trust Fortinet to protect their businesses.

Fortinet is the only security leader to develop and build custom security processing unit (SPU) technology to offer the best performance and cost value in the industry with a Security Compute Rating that ranges between 3 to 47x the performance of other software approaches. Each day Fortinet FortiGuard Labs uses one of the most effective and proven artificial intelligence (AI) and machine learning (ML) systems in the industry to process and analyze more than 100 billion events daily, sending actionable real-time threat intelligence to customers. The combination of FortiOS, purpose-built SPU technology, and AI-powered threat intelligence showcases the Fortinet commitment to cybersecurity innovation and excellence.

The Fortinet flagship enterprise firewall platform, FortiGate, is available in a wide range of sizes and form factors to fit any environment and provides a broad array of next-generation security and networking functions. The Fortinet market position and solution effectiveness have been widely validated by industry analysts, independent testing labs, business organizations, and media outlets worldwide. Fortinet is proud to count the majority of Fortune 500 companies among its satisfied customers.