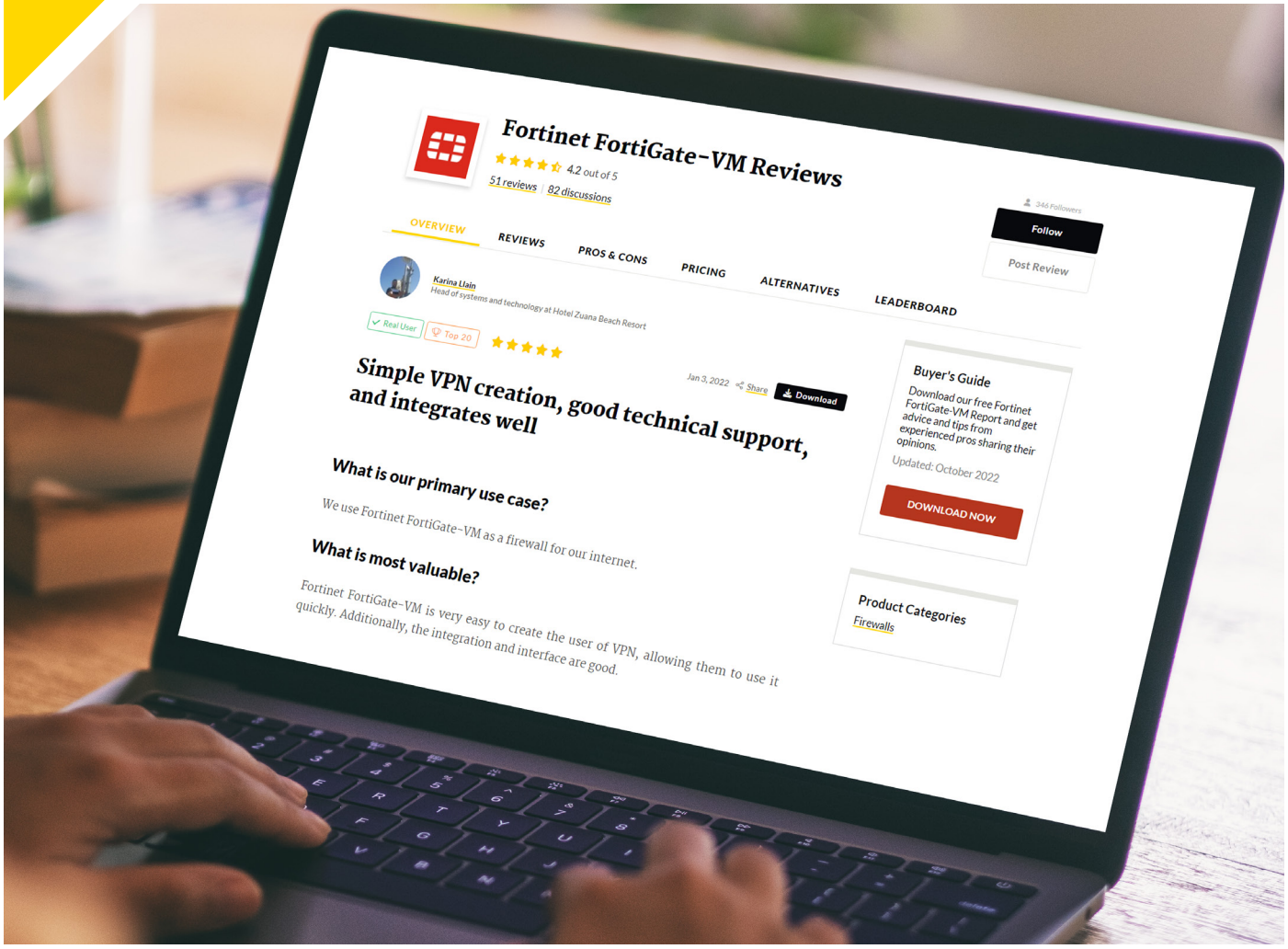
PeerPaper™ Report 2022

Based on Real User Experiences with Fortinet FortiGate-VM

Top 6 Selection Factors for a Next-Generation Firewall (NGFW) for Cloud Environments



PeerSpot

Contents

Page 1. **Introduction**

Page 2. **The Role of the NGFW in the Cloud**

Page 3. **Differentiating Next-Gen Firewall vs. Web Application Firewall**

Page 4. **The Top 6 Selection Criteria for a NGFW for Cloud Environments**

- #1 – Cloud Capabilities, Cloud Integration, and Automation
- #2 – Reliability, Flexibility, and Scalability
- #3 – Security Visibility, Capabilities, and Performance
- #4 – Ease of Use/Single Pane Management
- #5 – Cybersecurity Mesh/Security Fabric
- #6 – Return on Investment (ROI)

Page 13. **Conclusion**

Introduction

Effective cloud security demands solutions, controls, and countermeasures that are created for the cloud. After all, the cloud exposes digital assets to different kinds of risk from those hosted on traditional on-premises infrastructure. The Next Generation Firewall (NGFW) is particularly relevant in defending cloud-based data and applications. An NGFW virtual appliance adds threat intelligence, application awareness, and advanced threat protection, among other features, to cloud security capabilities.

This paper explores the selection factors that prospective NGFW virtual appliance buyers should consider when choosing a solution for cloud environments. It is based on the experiences of real users of the Fortinet FortiGate-VM NGFW, as described on PeerSpot. As they see things, the top six selection criteria include factors like integration, visibility, automation, flexibility and more. The right NGFW virtual appliance for cloud environments will also be scalable, offering strong performance, ease of use and an attractive return on investment (ROI).

The Role of the NGFW in the Cloud

As its name suggests, an NGFW expands on the functionality of the traditional firewall. Rather than just doing stateful inspection of network traffic and blocking traffic based on rules, an NGFW is able to block new kinds of threats, such as application-layer attacks and advanced malware. An NGFW may also offer integrated intrusion prevention, threat intelligence, and application awareness. In the cloud, an NGFW should be able to deliver its functionality across public, private, and hybrid cloud architectures. It needs to offer multi-cloud capabilities, as well, enforcing policies wherever digital assets are deployed.

PeerSpot members' uses of FortiGate bear out this idea. For example:

- An Information Technology Solutions Manager at UBG, a tech services company, uses FortiGate for web filtering and Intrusion Protection (IPS).
- For a Tech Security & Networking Support Lead at a private equity firm, FortiGate's most valuable features are IPS and antivirus.
- A Systems Engineer at a tech services company with more than 500 employees takes advantage of FortiGate's real time threat intelligence delivered by FortiGuard Labs.

Cloud-Native Security

Differentiating Next-Gen Firewall vs. Web Application Firewall

NGFWs tend to get confused with Web Application Firewalls (WAFs). The two technologies are similar and overlap in certain ways, but their core functionalities and purposes are distinct. While they can both be viewed as network functions, NGFWs and WAFs interact with traffic at different places in the network and on the Open Systems Interconnection (OSI) stack. Figure 1 shows where traditional firewalls, NGFWs, and WAFs fit in the OSI stack.

The NGFW operates more on the network level, protecting against unauthorized traffic. The WAF, in contrast, focuses more on applications, e.g., preventing injection attacks and threats that target code level vulnerabilities. In a building analogy, it can be helpful to visualize the NGFW like the lock on the front door, versus the WAF, which is like the lock on each interior room.

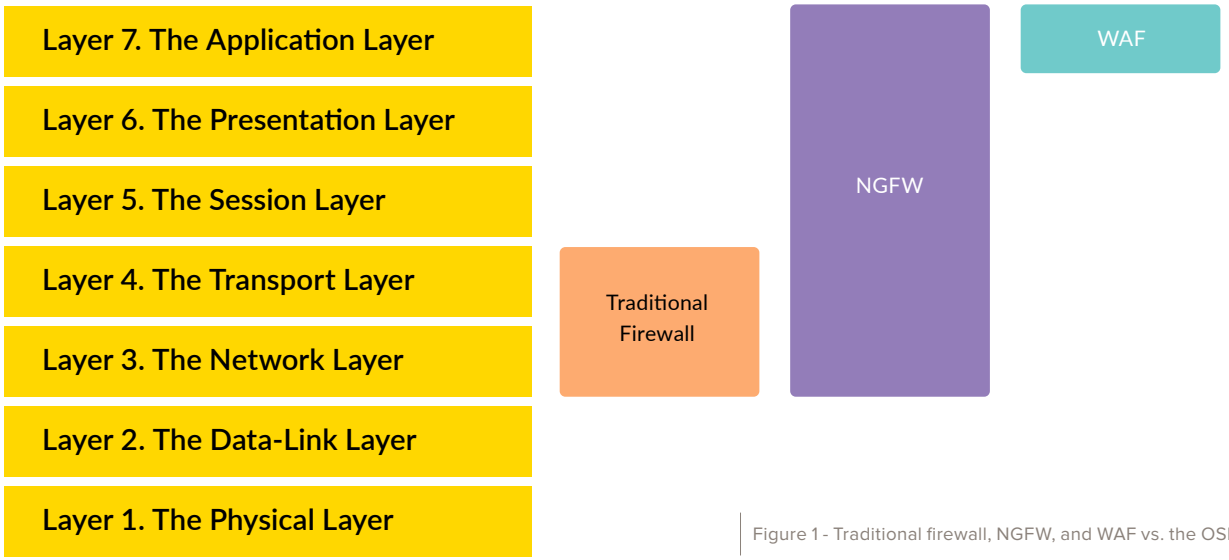


Figure 1 - Traditional firewall, NGFW, and WAF vs. the OSI stack.

The Top 6 Selection Criteria for a NGFW for Cloud Environments

IT professionals have a range of choices when it comes to NGFWs for cloud environments. What makes for a good solution? According to PeerSpot members, an effective NGFW for the cloud is one that combines cloud capabilities with strong cloud-native integration and automation. It's reliable, flexible, and scalable, offering ease of use and unified "single pane of glass" management. Security features must be robust, as well. The solution must also deliver ROI.

#1 – Cloud Capabilities, Cloud Integration, and Automation

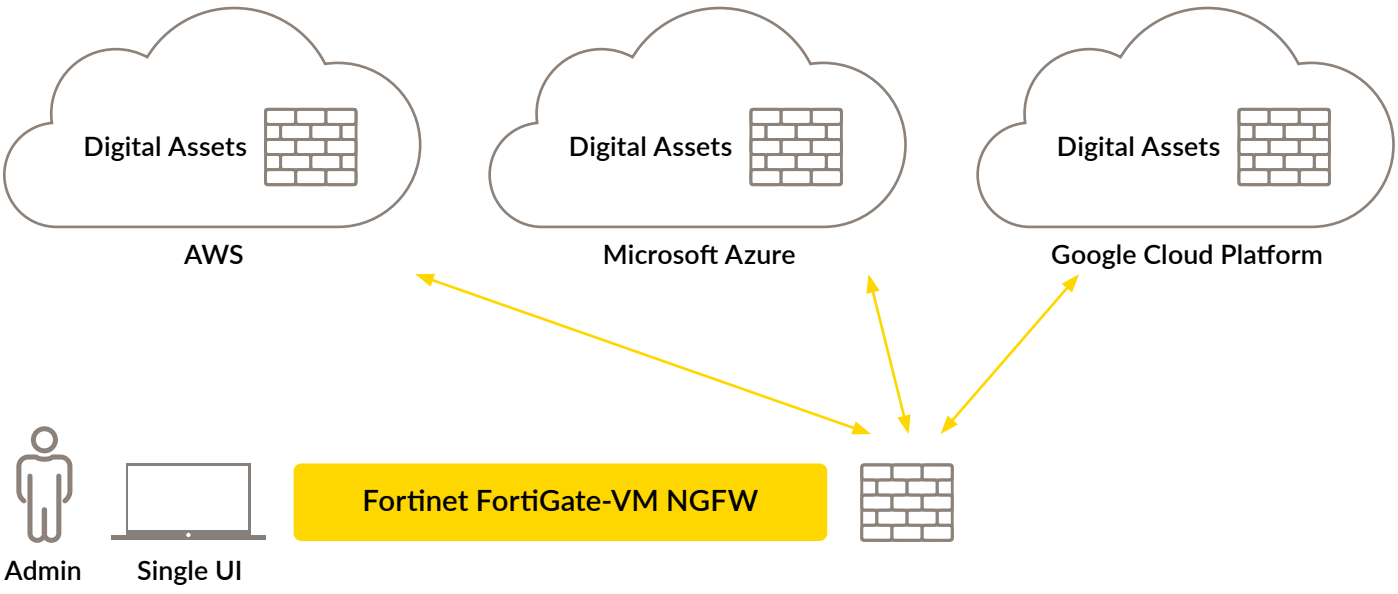
FortiGate users praised the solution for its cloud capabilities and potential to integrate with cloud platforms. A technical support Team Leader at a manufacturing company, for instance, shared, "We have on-premises and cloud deployments. We use the on-premise version for the functionality for our local network, and we use the cloud-based solution to provide the same functionality for our cloud-hosted workspaces."

Visibility Across Multi-Cloud Environments

The Microsoft cloud integration use case was what mattered to an Information Security Manager at a financial services firm with more than 500 employees. His company uses FortiGate-VM to access its clients' networks. He elaborated, saying, "These are generally Azure cloud environments in which we set up resources for clients to use." A Full Support Analyst at Gruppen, a tech services company, also uses the solution as a public cloud for Microsoft Azure.

Regarding automation, another key selection factor for an NGFW virtual appliance, a Team Leader Network & Security at Rogers Capital, a financial services firm, offered a practical example. He said, "Let's say tomorrow we want to upgrade in terms of memory, in terms of processor. If we are VM based we are using files and by default, we have some spec which is set to the VM. If tomorrow we need more capacity for this logging, we can just upgrade it. We take an analyzer like G1 or G5 and we upload the license, and it will upgrade automatically."

Figure 2 - How an NGFW can integrate with multiple cloud platforms.



#2 – Reliability, Flexibility, and Scalability

Users like an NGFW that's reliable, flexible, and scalable. PeerSpot members spoke to the need for these qualities. For example, a Network Engineer at a communications service provider with over 10,000 employees expressed the view that the most valuable features of FortiGate are its user interface, stability, and scalability. A Lead Cybersecurity Analyst at a consultancy with more than 5,000 employees put it this way: "With this solution, clients have the potential to grow in the near future. It's just one of those items that we wanted to make sure they had. It's something that is robust enough to be able to handle growing."

Other notable comments on this subject include:

- "I am impressed by its scalability, given that we are already using it for over 500 users. And, in the future, we plan to increase usage even more." - IT Support Team Leader at a tech services company

- "The solution is very stable. It's reliable and the performance is good. There are no bugs or glitches. It doesn't crash or freeze. The solution is quite scalable. If a company needs to expand the solution, it has the capabilities to do so." - Information Technology Manager and ISMS Auditor at a consultancy

- "It provides greater security and flexibility. Instead of just opening it all up, it allows access to only those people who should have access. The network itself is pretty open, and with FortiGate, we can lock down exactly what they have access to." - IT Engineering Manager at Mission Critical Partners, a tech company

Information Technology Manager and ISMS Auditor at a consultancy with 51-200 employees

"The solution [Fortinet FortiGate-VM] is very stable... There are no bugs or glitches. It doesn't crash or freeze. The solution is quite scalable. If a company needs to expand the solution, it has the capabilities to do so."

Read review »

IT Director at a retailer with 1,001-5,000 employees

"Affordable, easy to set up, and it is a high-performance appliance."

Read review »

#3 – Security Visibility, Capabilities, and Performance

The best NGFWs combine security visibility, a robust feature set and performance. Regarding visibility, an aerospace Sr. Project Consultant praised the solution's monitoring capabilities. He said, "That's something that I love. We are able to closely monitor the usages of individual users and see their usage habits and other items, including the data itself, which gives us quite a bit of visibility."

An IT Director at a retailer with over 1,000 employees described FortiGate as "affordable, easy to set up, and it is a high-performance appliance." He further commented, "Using this product protects our company from attacks that come from outside of our network. At the same time, we get better speed and performance when connecting to the internet." An Information Technology Manager and ISMS Auditor at a consultancy simply stated, "The performance overall is very good."

The tech vendor's Pre-Sales Associate spoke to the importance of security features in an NGFW. He observed, "The most valuable features are locking applications from in and out of my test network and testing malware on different devices. I use malware detection, antivirus, and basic firewall policies to check for different types of security breaches."

"Fortinet provides a great layer of security when it comes to SD-WAN [Software-Defined Wide Area Network] and other security capabilities," said Gruppen's Full Support Analyst. A Senior Network Engineer at a tech services company echoed this sentiment, remarking, "The most valuable features are the SD-WAN and the web filtering applications control."

Mauricio C.
Full support analyst at Gruppen

"Fortinet [FortiGate-VM] provides a great layer of security when it comes to SD-WAN and other security capabilities."

Read review »

Senior Security Engineer at a energy/utilities company with 1,001-5,000 employees

"It's [Fortinet FortiGate-VM] got a clean interface and it's very intuitive. Everything is easy to navigate."

Read review »

#4 – Ease of Use/Single Pane Management

An NGFW needs to be easy to set up and use. Security and network workloads are challenging enough as they are. A solution that adds complexity or takes up administrator time is not viewed in a positive light. PeerSpot users praised FortiGate in this context, with a Network Security Engineer at a government agency with over 1,000 employees describing the solution as cost-effective and "easy to set up."

Ease of setup was a standout characteristic of FortiGate for an IT Manager at Zipper, a tech services company. She said, "It doesn't take a lot of time and offers a quick deployment, so you can start using it almost right away." The government Network Security Engineer also found that "somebody who has a little bit of experience in VMware or with firewalls will be able to do it in no time."

After setup, ease of use is essential, as the Chief Technology Officer at Cornerstone Defense, a tech services company, mentioned. He said, "It's a relatively simple product that is easy to use. It's not overly complex." The consultancy's Information Technology Manager and ISMS Auditor had the same thought. He said, "The solution is easy to use. It's not overly difficult."

For a Senior Security Engineer at an energy/utilities company with over 1,000 employees, ease of use translated into a "single pane of glass" to manage the solution. To achieve this, he used the FortiManager tool. He further commented, "It's got a clean interface and it's very intuitive. Everything is easy to navigate."

Reliable, Flexible, and Scalable

#5 – Cybersecurity Mesh/Security Fabric

The Fortinet Security Fabric is a cybersecurity mesh architecture that is built to encompass broad, integrated, and automation protection across networks, endpoints, and clouds. Users on PeerSpot identified functionality that highlights how FortiGate and the Fortinet Security Fabric enable a high-performing security mesh model.

For instance, a Director at a system integrator shared, "Security Fabric Framework is helping in analyzing sudden and rapid changes in the whole infrastructure, and gives the ability to simplify daily operations (e.g., address objects synchronization between all firewalls in Fabric, estimating overall security rating, single-sign-on for admin access and many more)." A Pre Sales Associate at a tech vendor also acknowledged how the Security Fabric feature allows centralized visibility of all devices and traffic on the network in one place. He said, "This is not typically offered on traditional firewalls."

Chingiz A.
Director at a integrator with 11-50 employees

"Security Fabric Framework is helping in analyzing sudden and rapid changes in the whole infrastructure, and gives the ability to simplify daily operations."

Read review »

Easy to Set Up

What stood out to an Assistant Manager at Ingram Micro was how Fortinet Security Fabric combines many Fortinet products. This allows admins to monitor them from a single vendor. He said, "Fortinet Security Fabric, the log features, and FortiGuard integration are all useful features. Fortinet Cloud also offers data integration with private and public clouds. The configuration isn't too complicated."

A Network Engineer at a small tech services company noted that FortiGate's Security Fabric and Intrusion Protection System and Intrusion Detection System (IPS and IDS) worked together to offer visibility into the whole network. He said, "I was able to see everything that was going on."

A Solutions Architect at a software company with more than 5,000 employees similarly shared that FortiGate "integrates well," adding, "the most valuable features of this solution are the integration within the environment, with centralized reporting." The manufacturing company Team Leader was pleased that FortiGate offered a complete ecosystem with "all kinds of integrations."

A venture capital and private equity firm needed an NGFW virtual appliance that "has a lot of integration with external connectors," according to their Tech Security & Networking Support Lead. He cited the example of Microsoft Teams, which FortiGate can protect from external threats.

#6 – Return on Investment (ROI)

An NGFW virtual appliance represents an investment, so it should ideally show a positive ROI. This does not have to mean a financial ROI, as a Chief of Security and Research at a small tech services company related. He said, "We've seen a decent ROI as it has helped us maintain a good level of security. I'd rate the ROI we've seen at a five out of five." A Network Administrator at Furnmart, a small manufacturing company, believes that their main ROI has been the extra stability on their network. He said, "Since we implemented this solution, we haven't had any major attacks."

Having fewer incidents is an indirect financial metric, in reality. Security events are costly to handle, so a solution that reduces them is earning an ROI. The Owner of Stratus Concept put it in these terms: "The ROI that they were looking for was an improvement in security for the whole company."

Chief of Security and Research
at a tech services company with
1-10 employees

"We've seen a decent ROI as it has helped us maintain a good level of security. I'd rate the ROI we've seen at a five out of five."

Read review »

Conclusion

The right NGFW virtual appliance for the cloud will offer features and embody characteristics that deliver robust security outcomes in the cloud. According to users of the Fortinet FortiGate-VM NGFW, an NGFW virtual appliance should offer visibility into traffic, with an integrated “single pane of glass” admin interface. It should provide automation capabilities and ease of use, coupled with integration with other relevant systems. Performance needs to be good, as well as flexibility, reliability and scalability. There should be an identifiable ROI. As these factors coalesce in an NGFW virtual appliance, users will be able to deploy it to establish a more robust security posture in the cloud.

About PeerSpot

PeerSpot (formerly IT Central Station), is the authority on enterprise technology. As the world's fastest growing review platform designed exclusively for enterprise technology, with over 3.5 million enterprise technology visitors, PeerSpot enables 97 of the Fortune 100 companies in making technology buying decisions. Technology vendors understand the importance of peer reviews and encourage their customers to be part of our community. PeerSpot helps vendors capture and leverage the authentic product feedback in the most comprehensive way, to help buyers when conducting research or making purchase decisions, as well as helping vendors use their voice of customer insights in other educational ways throughout their business.

www.peerspot.com

Fortinet FortiGate Overview

Fortinet FortiGate is #1 ranked solution in best firewalls, SD-WAN tools, and top WAN Edge tools. PeerSpot users give Fortinet FortiGate an average rating of 8.4 out of 10. Fortinet FortiGate is popular among the large enterprise segment, accounting for 50% of users researching this solution on PeerSpot. The top industry researching this solution are professionals from a comms service provider, accounting for 27% of all views.

Learn more about FortiGate-VM at https://www.fortinet.com/products/private-cloud-security/fortigate-virtual-appliances#resources