# The Top 5 Challenges of Firewall Management

Overcome the obstacles and learn how to protect your growing network

Sponsored by

Megaport

Mighty Guides

# Table of Contents



Mighty Guides

# Meet Our Experts

Firewall management can be extremely challenging due to constantly evolving cyber threats, the multitude of vendors, the surge in remote working, and more. We've interviewed four experts on how they address these difficulties to ensure consistent security and real-time threat response to their growing networks.

We hope you enjoy their insights!


**David Rogelberg**
Publisher,
Mighty Guides Inc.
david@mightyguides.com
+1 (516) 788-7886


Mighty Guides

**Graham Todd**
Manager, Security Engineering,
International Law Firm

**Anand Sengar**
Technical Architect,
Tata Consultancy Services

**Richard Holguín**
Network Consultant,
Best Path

**Paul McGuinness**
Head of Solutions, EMEA,
Megaport

# Introduction

As networks become increasingly complex and cyber threats continue to evolve, firewall management has become more critical than ever for organizations of all sizes. However, managing them can be a complex and challenging task for IT and security teams. Companies may have multiple firewall vendors, each with their own configuration and rules, making it difficult to ensure consistent security across the organization. Meanwhile, firewalls can generate a large amount of data, and it can be difficult for security teams to identify and respond to threats in real time.

In this guide, we'll discuss the top five challenges of firewall management that organizations face today. These challenges include managing the firewall lifecycle, protecting remote workforces, creating strong network segmentation, securing multicloud infrastructure, and establishing firewalls in multiple locations. Each of these challenges can have a significant impact on an organization's security posture, making it essential to address them effectively.

We will explore each of these challenges in detail, highlighting the risks they pose and the solutions available to overcome them. We'll also share how organizations can optimize their firewall management processes to enhance their security posture and reduce the risk of cyberattacks.



Mighty Guides

**Mighty Guides make you stronger.**

**Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.**

**Reading a Mighty Guide is kind of like having your own team of experts. These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you.**

# Foreword

We're delighted to sponsor this Mighty Guides ebook, which is a valuable addition to the debate about firewall management, featuring the insights and experiences of real users across different industries. Their contribution offers first-hand knowledge about the challenges companies face when implementing firewalls and the factors that need to be considered to overcome them.

The observations and recommendations made in this ebook support Megaport's belief that implementing a virtual firewall offers the most secure, flexible, and cost-effective approach to mitigating risks and delivering network security. At a time when cyberattacks are becoming more frequent and advanced than ever before, it is critical that companies review their security strategies and the firewall(s) they have in place.

Our Megaport Virtual Edge (MVE) solution enables users to deploy a Firewall as a Service (FWaaS) to suit their specific needs, safeguarding enterprises from both internal and external threats. The benefits are clear: manageable OpEx in place of costly upfront CapEx, no hardware maintenance or upgrades needed, no deployment delays, and better security that's easier to utilize. Just as cloud adoption began in certain industries and spread widely, virtual firewalls first earned a following among early adopters and are now growing in popularity across a broad cross-section of industries.

We hope you find this ebook valuable in your discussions about your organization's approach to network security. If you need further guidance, check out www.megaport.com.

Megaport

**Megaport is a leading provider of Network as a Service (NaaS) solutions. The company's global Software Defined Network (SDN) helps businesses rapidly connect their network to services via an easy-to-use portal or our open API. Megaport offers agile networking capabilities that reduce operating costs and increase speed to market compared to traditional networking solutions. Megaport partners with the world's top cloud service providers, including AWS, Microsoft Azure, and Google Cloud, as well as the largest data center operators, systems integrators, and managed service providers in the world.**

Megaport

# Transform Networking at the Edge

Modernize private connectivity with Megaport Virtual Edge (MVE), our on-demand Network Function Virtualization (NFV) service. Deploy SD-WAN gateways, virtual routers, and virtual firewalls in minutes.

**Find out more at megaport.com/mve**

Spin up edge networking in minutes.

Reduce cloud egress costs.

Improve network performance and security.

Deploy immediately avoiding hardware shortages and project delays.

Reduce data center footprint by transforming your network into virtual connectivity hubs.

Pay for what you need when you need it, with no lock-in contracts.

Bring private networking closer to the edge with API-level integration between Megaport Virtual Edge and leading industry providers.

aruba NETWORKS · cisco · FORTINET · paloalto NETWORKS · VERSA NETWORKS · vmware

Chapter 1

# MANAGING THE FIREWALL LIFECYCLE

Deploying a firewall is a complex task, and creating a policy that satisfies the requirements of different departments can be challenging. What's more, when a server gets decommissioned, the firewall team is often left in the dark. Without finding a way for the firewall rules to be updated at the same time, the business can be left with significant technical debt.

"Having a good way to define your firewall policies, manage them long-term, and integrate them with business processes is absolutely key," said Paul McGuinness, Head of Solutions Europe at Megaport.

A big part of this is also using the right language to define firewall requirements and policies amongst different teams.

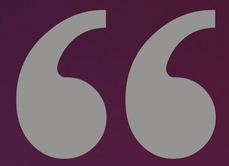
"Bridging the gap between business and technical language is essential; you need someone who can convert business requirements into technical language," explained Anand Sengar, Technical Architect at Tata Consultancy Services.

When looking for a firewall provider, it can be tempting to use a single company that offers the next-generation firewall (NGFW) with all sorts of plugins. However, while there are financial benefits to using one vendor for multiple products, this needs to be balanced against the size of the business, the budget, and the risk appetite. Ideally, it's advisable to have some kind of

***Having a good way to define your firewall policies, manage them long-term, and integrate them with business processes is absolutely key."***

**Paul McGuinness**

Head of Solutions, EMEA, Megaport



***Bridging the gap between business and technical language is essential; you need someone who can convert business requirements into technical language.”***

**Anand Sengar**

Technical Architect, Tata Consultancy Services

> ***Security is a matter of building layers, layers, and more layers; there's no one solution that can do all of that."***

**Richard Holguín**

Network Consultant, Best Path

dual vendor strategy. It's all about building not only defense in depth with technology but with vendors too.

"Security is a matter of building layers, layers, and more layers; there is no one solution that can do all of that," agreed Richard Holguín, Network Consultant at BestPath and LSEG.

Another important consideration is the application layer, as this is where many of today's cyber threats originate.

"The application layer needs to be analyzed to ensure that users aren't piggybacking on a port or service that they shouldn't be," explained Graham Todd, CISSP, Manager of Security Engineering.

Organizations also need to decide whether they're going to do things like SSL decryption and whether the hardware they have is sturdy enough to act as the front end.

"Every security decision involves a balance between speed and risk," noted Todd.

***The application layer needs to be analyzed to ensure that users aren't piggybacking on a port or service that they shouldn't be."***

**Graham Todd**

Manager, Security Engineering, International Law Firm

***Every security decision involves striking the right balance between speed and risk.”***

**Graham Todd**

Manager, Security Engineering, International Law Firm

# Key Points

- Deploying a firewall is a complex task; it can be incredibly challenging to unify and define policy in the long term.
- When looking for a firewall provider, automation should be a fundamental consideration.
- It's advisable to have some kind of diversity and to build defense in depth with vendors as well as technology.

Chapter 2

# PROTECTING REMOTE WORKFORCES

With more people working from home than ever, protecting remote workforces is a fundamental aspect of firewall management. Having a firewall vendor who has templates to help onboard new remote users is key. Meanwhile, deploying firewalls in the cloud enables businesses to spin up quick solutions and minimize downtime.

“It’s a matter of having an endpoint solution that is linked to the firewalls and then having the latest release of patches or updates; you then have the ability to decide whether you need to extend that protection,” mentioned Sengar.

However, it all comes down to responding to how the business and its workforce function.

***Security starts with an endpoint solution focused on firewalls and having the latest patches or updates; you can then decide whether you need to extend that protection.”***

**Anand Sengar**

Technical Architect, Tata Consultancy Services

> ***While most people now have the work-from-anywhere mindset, businesses need to question whether this really means anywhere.”***

**Graham Todd**

Manager, Security Engineering, International Law Firm

“While most people now have the work-from-anywhere mindset, businesses need to question whether this really means anywhere,” explained Todd.

Every business has a different risk tolerance, and there might still need to be certain restrictions in place and conditional access. While many companies are making the move to the cloud and reducing the size of their data centers, networking equipment is the last piece of the puzzle.

“With virtual firewalling, businesses can virtualise that as well,” noted Todd.

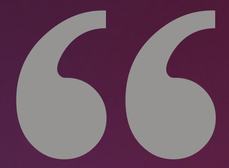
Instead of deploying firewalls, buying licenses, and putting them in hardware or the cloud, virtual firewall providers can host the hardware and the networking.

“Businesses just bring the licenses,” confirmed McGuinness.

What’s more, with the various data laws out there, such as GDPR, having the ability to spin up firewalls to control particular areas is a much more manageable solution.

Another important aspect in relation to remote working is ensuring that firewalls don’t negatively impact user experience. It’s important for the architecture team to investigate every aspect individually, including Infrastructure as a Service (IaaS) and Software as a Service (SaaS).

“Long distance communications to get to a data center and then share a connection to the cloud leads to a poor user experience,” explained McGuinness.



***With virtual firewalling, businesses can virtualize that as well.”***

**Graham Todd**

Manager, Security Engineering, International Law Firm

*Long-distance communications to get to a data center and then share a connection to the cloud leads to a poor user experience.”*

**Paul McGuinness**

Head of Solutions, EMEA, Megaport

# Key Points

- With the rise in remote working, ensuring all users are protected has become a fundamental aspect of firewall management.
- With a virtual firewall solution, businesses essentially pay for what they use; the solution is easy to spin up and offers the resilience that hardware doesn't.
- It's important that architecture teams investigate every aspect of their firewall solution to ensure it doesn't negatively impact user experience.

Chapter 3

# CREATING STRONG NETWORK SEGMENTATION

Network segmentation is an essential practice for businesses that want to improve their security posture, meet compliance requirements, optimize their resources, and improve their overall network performance. However, integrating different technologies and systems can create interoperability issues. Meanwhile, improperly implemented network segmentation can create new security risks and vulnerabilities.

“Grouping within network segmentation helps avoid the issues of individual user rules, but this comes down to good data analytics to create the right policies,” explained Todd.

It’s vital for businesses to create a governance path, have an awareness of what they’re doing in the cloud, and plan appropriately. It’s not just about networking, it covers all aspects of security and impacts costs.

“Technically you can achieve anything, but you need to have governance in place to control costs,” noted Sengar.

Software-defined networking (SDN) solutions can help businesses manage the

> ***Grouping within network segmentation helps avoid the issues of individual user rules, but this comes down to using good data analytics to create the right policies.”***

**Graham Todd**

Manager, Security Engineering, International Law Firm

> ***Technically, you can achieve anything, but you need to have governance in place to control costs.”***

**Anand Sengar**

Technical Architect, Tata Consultancy Services

complexities of network segmentation by providing real-time traffic monitoring and management.

“It’s just like having a cloud network that’s under your control,” explained McGuinness.

Meanwhile, by taking advantage of Virtual Cross Connect (VXC) services, businesses are able to connect to multiple cloud providers and data centers in a secure and scalable manner; create private connections between their various cloud environments, data centers, and other networks; and ensure that sensitive data and applications are not exposed to the public internet.

***Software-defined networking is just like having a cloud network that's under your control."***

**Paul McGuinness**

Head of Solutions, EMEA, Megaport

# Key Points

- Network segmentation is an essential practice for businesses that want to improve their security posture and improve their overall network performance.
- It's vital for businesses to create a governance path, have an awareness of what they're doing in the cloud, and plan appropriately.
- SDN solutions can help businesses manage the complexities of network segmentation by providing real-time traffic monitoring and management.

Chapter 4

# SECURING MULTICLOUD INFRASTRUCTURE

When businesses move to a multicloud infrastructure, they need to review and adapt their internal security controls to ensure that they can effectively manage the new security risks.

“Some clouds have restrictions that don’t allow you to put as many measures in place as you’d like to,” explained Holguín.

Managing new security risks may involve implementing new controls or adopting new security strategies and best practices to protect their cloud infrastructure and data.

“Shadow IT is a massive problem in the cloud that opens up all sorts of concerns in relation to data loss prevention,” explained Todd.

“We’ve moved from a centralized to a decentralized environment, not only in terms of the workforce, but with IoT devices working and sending data to the cloud; it’s yet another environment that needs to be secured,” added Holguín.

To manage the risk, businesses need to look at data labeling and what controls are in place. However, businesses should consider the needs of different

> ***“Some clouds have restrictions that don’t allow you to put as many measures in place as you’d like to.”***

**Richard Holguín**

Network Consultant, Best Path

> ***Shadow IT is a massive problem in the cloud that opens up all sorts of concerns related to data loss prevention.”***

**Graham Todd**

Manager, Security Engineering, International Law Firm

applications; this requires a dynamic, rule-based, multicloud security policy that is tailored to the importance of each application to the business, rather than being based solely on the underlying infrastructure. New technologies such as SD-WAN, SASE, and Security Services Edge (SSE) can help by providing a centralized controller with comprehensive visibility.

When it comes to issues with working across and integrating AWS, Azure, and on-premises data centers, a lot can come down to legislation and regulation.

“The lack of knowledge about connectivity and private connectivity and how it works still surprises me,” exclaimed McGuinness.

To manage the issue, smaller businesses may need to either buy in professional service consultancy or use a managed security services provider (MSSP).

“Most smaller organizations won’t be able to afford to have in-house engineers that are experts in all areas of multicloud maintenance,” stated Todd.

MSSPs can provide expertise, tools, and resources to help businesses manage their cloud infrastructure effectively and efficiently.

***We’ve moved from a centralized to a decentralized environment, not only in terms of the workforce but with IoT devices working and sending data to the cloud. It’s yet another environment that needs to be secured.”***

**Richard Holguín**

Network Consultant, Best Path

***Most smaller organizations won't be able to afford in-house engineers who are experts in all areas of multicloud maintenance."***

**Graham Todd**

Manager, Security Engineering, International Law Firm

# Key Points

- When moving to a multicloud infrastructure, organizations need to review and adapt their internal security controls to account for new risks.
- Businesses should consider the needs of different applications and create a dynamic, rule-based, multicloud security policy.

Chapter 5

# ESTABLISHING FIREWALLS IN MULTIPLE LOCATIONS

Implementing firewalls to cover offices in multiple locations, regions, or countries can be a complex task. Before implementing firewalls, it's important that organizations establish a security policy that outlines what needs to be protected, who should have access, and what types of traffic should be allowed or blocked. Adopting a zero-trust security model is fundamental; all traffic should be treated as untrusted and be inspected before being allowed access. Meanwhile, automation and orchestration tools can help reduce the IT workload and ensure consistent security policies are implemented across all locations.

Software-defined networking solutions can allow businesses to connect their data centers to cloud providers and leverage cloud resources rather than building privately-owned data centers in multiple countries. This can reduce the cost of building and maintaining physical data centers while providing greater flexibility and scalability.

"However, establishing multiple firewalls and managing costs requires templates and good back-end data," explained Todd.

If the CMBD (Configuration Management Database) is up to date, it makes a considerable difference, and rollouts will run much more smoothly.

The other huge consideration is compliance with regulatory requirements, such as GDPR. As regulations continue to evolve, different regions and states may have their own competing data rules, and firewalls will need to be able to manage all of that. According to Todd, the industry as a whole needs to tackle the issue of regulation, how businesses stay compliant yet still function and continue to operate securely across different regulatory boundaries.

***Establishing multiple firewalls and managing costs requires templates and good back-end data.”***

**Graham Todd**

Manager, Security Engineering, International Law Firm

# Key Points

- Adopting a zero-trust security model, using automation tools, and working with a trusted provider can all help when establishing firewalls in multiple locations.
- SDN solutions can help businesses leverage cloud resources, but identity access management and good back-end data are fundamental to achieving this.
- Regulations are going to be a growing challenge when it comes to establishing firewalls across multiple locations.

# The Future of Firewall Management

Effective firewall management is crucial for organizations to navigate the complex and evolving cybersecurity landscape. By embracing comprehensive solutions, organizations can optimize their firewall management processes, enhance their security posture, and mitigate the risks of cyberattacks.

As the cybersecurity landscape evolves, organizations must remain vigilant and adaptive in their approach to firewall management. The future of firewalls lies in their ability to provide advanced threat intelligence, automation, and seamless integration with other security solutions to create a comprehensive defense strategy.

# Learn More About Our Experts

### Graham Todd

**Manager, Security Engineering, International Law Firm**

Graham is a CISSP certified cybersecurity expert with over 20 years' experience. Having cut his teeth in firewalls at a start-up MSSP in Edinburgh, Graham moved to Belfast and into the network architecture space before going on to spend a decade at one of America's largest insurance companies managing multiple security teams. He now leads a team of security experts protecting a global law firm.

### Anand Sengar

**Technical Architect, Tata Consultancy Services**

Anand has 15 years of dynamic and technology-oriented professional experience in network security, cloud security, cyber security, and project management. With a proven ability to implement best practices, set up security solutions, and develop holistic security programs, Anand helps businesses select the right set of solutions and implement those solutions properly.

### Richard Holguín

**Network Consultant, Best Path**

With 17 years of IT expertise, Richard specializes in providing next-gen networking and security solutions. He brings extensive experience in optimizing enterprise networks; migrating, deploying, and configuring firewalls; and implementing automation strategies to reduce OpEx and drive operational efficiencies. Richard is dedicated to helping customers with their IT challenges, enabling them to focus on what they do best—running their business.

### Paul McGuinness

**Head of Solutions, EMEA, Megaport**

Paul has held senior positions at several global telecommunications vendors, including solution consulting on Cisco's communications API portfolio. Paul now leads a team of Solutions Architects who work with customers on designing and implementing their networks. He also leads market education on global Network as a Service (NaaS) private connectivity solutions across industry verticals, including Virtual Connectivity hubs, SD-WAN, Virtual Firewalling, and Virtual Routing solutions.