451 Research® | PATHFINDER REPORT

Firewall Strategies Must Evolve with Application Strategies

COMMISSIONED BY

vmware®

MARCH 2019

About this paper

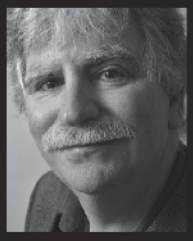
A Pathfinder paper navigates decision-makers through the issues surrounding a specific technology or business case, explores the business value of adoption, and recommends the range of considerations and concrete next steps in the decision-making process.

ABOUT THE AUTHOR

ERIC HANSELMAN

CHIEF ANALYST

Eric Hanselman is the Chief Analyst at 451 Research. He has an extensive, hands-on understanding of a broad range of IT subject areas, having direct experience in the areas of networks, virtualization, security and semiconductors. He coordinates industry analysis across the broad portfolio of 451 Research disciplines.



MIKE FRATTO

SENIOR ANALYST, APPLIED INFRASTRUCTURE AND DEV OPS

Mike Fratto is a senior analyst on 451 Research's Applied Infrastructure and DevOps team covering enterprise networking. He has extensive experience reviewing and writing about enterprise remote access, security and network infrastructure products, as well as consulting with enterprise IT, equipment and software vendors, and service providers.

Introduction

A network firewall is an integral component of any company's security strategy. These devices are designed to segment traffic across different parts of the business and are traditionally placed at boundaries to regulate traffic between clients in one zone and servers in one or more other zones.

Perimeter firewalls are well suited for the larger border, protecting the interior of the network from unknown hosts that sit outside. These firewalls inspect traffic coming in and out of the network. Access is granted to specific services protected by the firewall that are available to the outside world, and potentially, there is filtering to outbound traffic destinations. These are typically statically defined, and the access rules don't change significantly over time.

For internal traffic, however, new requirements have emerged. Internal networks are not flat, so organizations need ways to efficiently segment applications, users and zones within the perimeter. This is complicated by the fact that applications have become more dynamic and distributed. Modern application development, which uses cloud-based services, containers and microservices, necessitates fine-grained policy and control. Because of this, IT needs to rethink the fundamental capabilities and deployment models of network firewalls and consider what features and functions they need for each job.

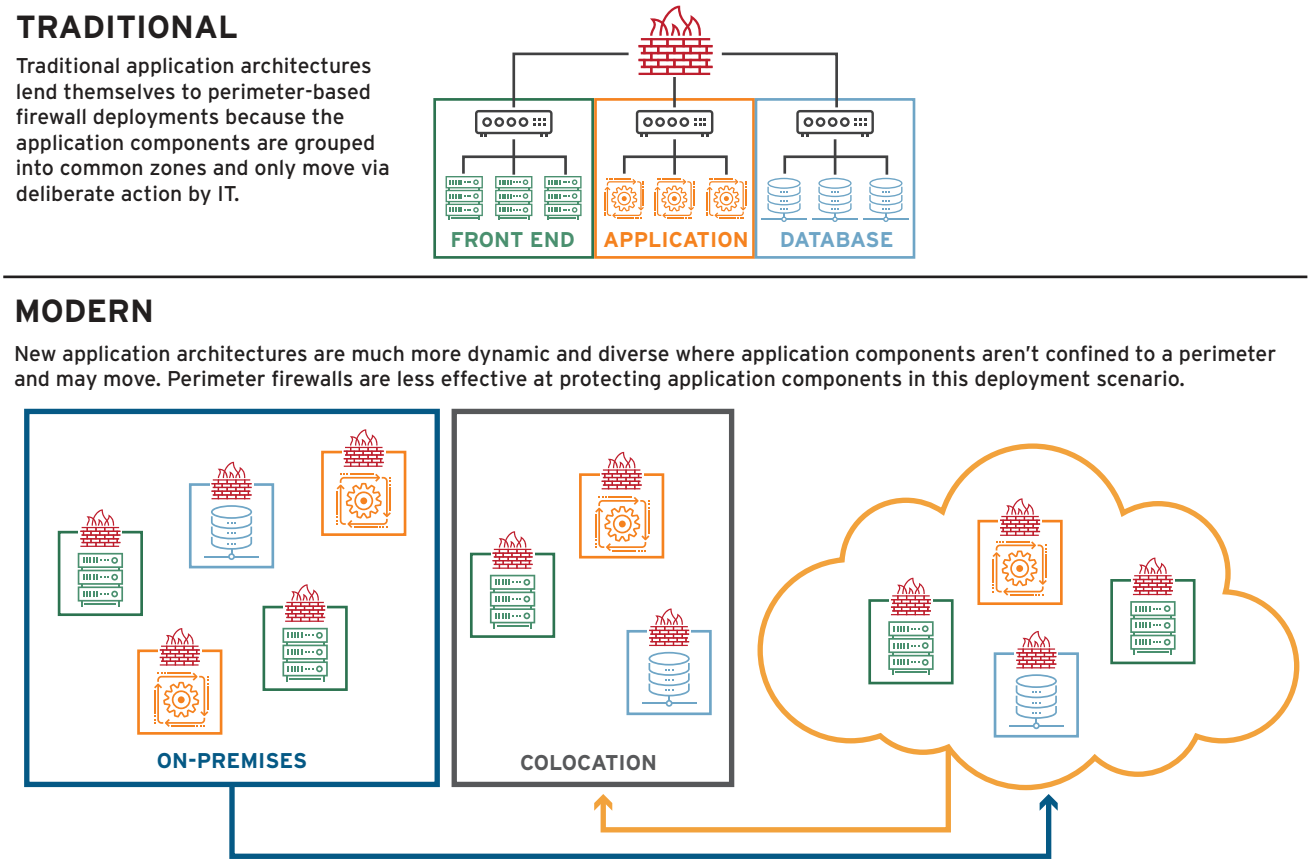
Why You Need to Expand Your Thinking About How a Firewall Functions

Multi-and hybrid cloud strategies are particularly impacted because cloud services offer varying security capabilities, meaning that a consistent set of policies can't be applied across multiple services. Cloud providers offer varying sets of controls to enforce access protections. It can be difficult to ensure consistent protection and policy enforcement when these controls don't align. Errors in control can lead to gaps that attackers can exploit.

Traditional applications are deployed on servers – or these days, on a VM on a hypervisor – and spend their entire lifecycle at that one spot. Dynamic events such as scaling up or scaling out or moving to a new location are often deliberate events driven by a change-control process. Application tiers can be moved into network zones protected by an internal firewall – firewalls normally found on the perimeter but are deployed within the enterprise network, isolating workloads from each other – usually with other servers of a similar nature. This structure works well when the applications don't move, and the zones can be predefined (see Figure 1).

Figure 1: Different Application Architectures Require Different Firewall Functions

Source: 451 Research

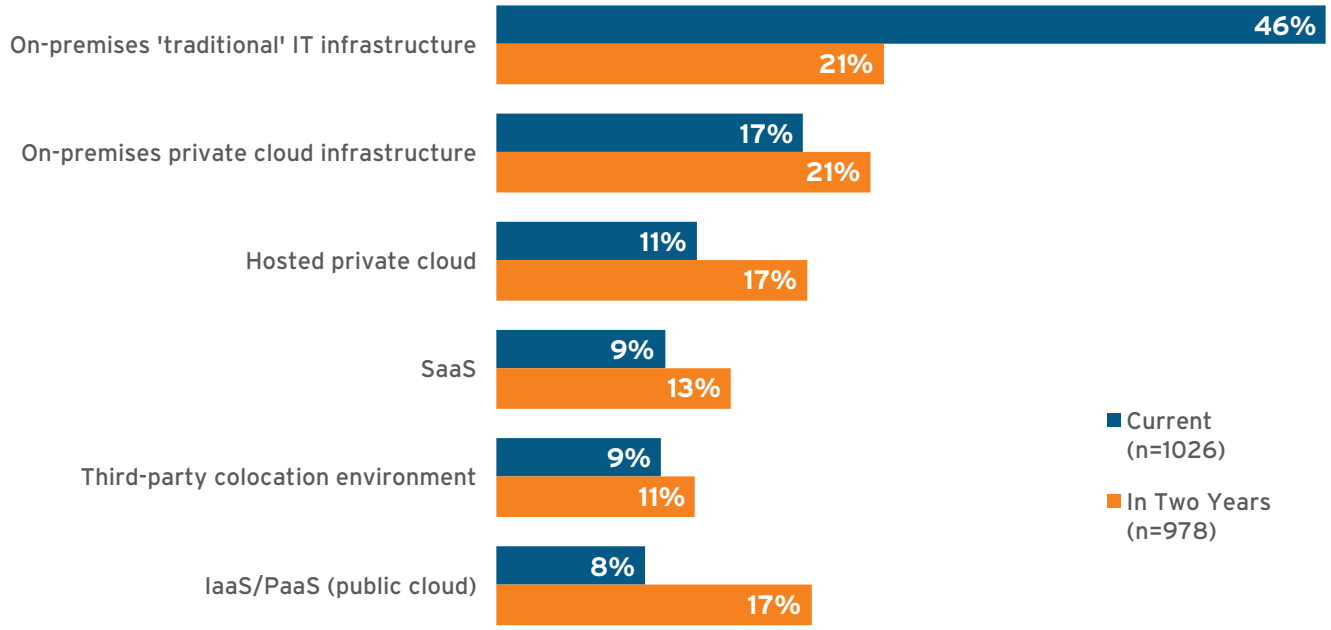


Modern enterprises expect to be able to deploy and interact with a range of providers, extending from datacenters to cloud, colocation, or to partner environments. Figure 2 illustrates the speed with which respondents to the 451 Research Voice of the Enterprise: Digital Pulse study reported that they want to move workloads to new locations as they adapt and grow their businesses. This movement demands more flexibility in the way security protections are applied.

Figure 2: The Movement to Multiple Locations is Real

Source: 451 Research's Voice of the Enterprise: Digital Pulse, Q3 2018

Q. Thinking about all of your organization's workloads/applications, where are the majority of these currently deployed? Where will the majority be deployed two years from now?



The changes in how applications are deployed are driving the requirement to change how security is deployed along with them. Retrofitting security products designed for traditional application deployments won't fit well with modern application architectures and processes. These differences are significant for ongoing operations over the application lifecycle.

Modern applications are designed to change – often rapidly – over time with the expectation that those changes will be automated. For example, a scale-up event triggered by an increase in requests initiates the deployment of new servers – and the associated networking and storage access – across one or more tiers to handle the new load and then scales back down when demand subsides. Containers were built for this model where hundreds or thousands of new instances can be created and destroyed throughout the day. Complicating matters, container environments were created with the assumption that the networks in the application would be dedicated to a single application pod and isolated from all else, and technologies such as service meshes were created to handle service identification and location within the pod; however, applications need to reach outside the pod and are thus exposed to the outside network.

Internal Firewall Requirements for Today's Applications

With all of this in mind, below is a list of key functions and capabilities that firewalls need to provide to protect data and applications in the internal network:

- **Full application context:** An understanding of application and workload attributes that extends beyond observable network characteristics into application topology and the state of the workload.
- **Dynamic rule capabilities:** The ability to build policy from a repository of abstractions that can be dynamically updated to reflect changes in the definition of policy elements.
- **Application-specific controls:** The ability to define controls that leverage identity and application permissions that extend through users and devices.
- **Distributed policy knowledge:** Policy information must be able to extend to the full range of execution venues where any of the application components can be distributed.
- **Workflow integration:** The ability to build firewall controls into the application production workflow with minimum impact on the application development process.
- **Run anywhere:** The bane of IT is inconsistent technology. Modern application deployments are potentially distributed on-premises, in a colocation datacenter, or in one or more cloud services, so using the same product ensures that a consistent set of capabilities and security policies are enforced and removes the need for IT to close gaps that may arise in using different products in different environments.
- **Fully automated:** Application deployment models are expanding to include more than the application components and services. Application deployment now often includes products and capabilities that support the application, including the firewall and its policy throughout the entire application lifecycle – test and development, deployment and retirement. The firewall component should be fully defined by application developers in the deployment workflow and pushed out to all environments where the application will run.
- **Application independence:** Host-based inspection and access control of processes can limit the actions that malicious software/actors can take, but the controls should also be independent of the application code and services. Utilizing in-network controls ensures that a compromised host or process will still have its security controls in place despite the compromise, and new access controls such as cutting off network access can be applied at a surgical level. In-host and in-network controls have complementary strengths and weaknesses, so it's important to have both types.
- **Business policy:** The access-control policy should be expressed in a natural manner that embodies the intent of the policy, which is then applied in the appropriate location – in-network or in-host – as required and as best suits the outcome. Natural language reporting also helps during internal and external audits to express the intended outcome, which can then be compared to the implemented policy controls.

As we show in Figure 3, yesterday's applications were predictable, and changes were made with deliberate steps. Today's applications are dynamic, interconnected and distributed. These stark differences are driving the requirements for secruity controls that match.

Figure 3: Features of Traditional vs. Modern Applications

Source: 451 Research

TRADITIONAL APPLICATIONS	MODERN APPLICATIONS
Monolithic – dedicated servers of code	**Composable** – components and microservices
Scale-up – one way to scale	**Scale-Up/Down/In/Out** – versatile scaling options
Static – clearly defined Dev-Test-Run	**Dynamic** – CI/CD and workload movement
Centralized – centralized RDBMS and storage	**Distributed** – use of distributed services
On-Premises – applications in a datacenter	**Anywhere** – datacenter, colo, cloud, edge
Predicted – size and scope predetermined	**Demand** – size and scope determined live
Physical – one application per server	**Virtual** – applications in servers, containers, cloud

Proof Points

One of the most significant motivations for overhauling network-based controls is the dramatic change in the nature of attacks being launched at enterprise environments. What were previously attacks directed at targets of interest have morphed into exploitation of trusted relationships. This means that protections must change focus from detecting and thwarting outsiders to managing internal connections that have been hijacked.

Target Breach of 2013

Examples of the risks that these newer attack techniques pose are easy to find. One of the best known is the Target breach of 2013. Attackers compromised the credentials of an HVAC contractor for large retailer Target Corporation and used the credentials to gain access to internal systems. The attackers then moved laterally to the point-of-sale (PoS) systems and installed malware that harvested credit card information. If there had been more significant internal controls in place to block that lateral movement, the outcome of the attack might have been different. Access to the PoS systems should have been managed through access controls, which would allow only application and management components of the environment to connect to the PoS terminals. However, allowing all connections to flow within the environment without the perspective of the expected connection types could have been enough to lead to disaster.

TechTalk and Three UK Breaches

To be effective, internal network controls must include sufficient context. In the case of the Target breach, it appears that fairly coarse isolation could have helped. However, a pair of telecommunications breaches in the UK speak to the need for much richer capabilities. Breaches at TalkTalk and Three UK also depended on compromised trust, but they proceeded in different directions. In the TalkTalk breach, a vulnerable web app was used to access customer data. While the web app should have been

able to connect to the database containing the data, the types of connections that it established to manipulate the configuration should have been blocked. A set of compromised credentials started the Three UK attack, but the locations of the systems from which they were used should have been an indication that the activities they pursued weren't legitimate. If there had been isolating protections that restricted the locations that were allowed, the attack chain could have been broken.

For too long, system architectures have used zone-based controls with the expectation that communications could be allowed within a protected zone. In many cases, that was expedient because getting detailed information about the workloads that made up the application was too difficult. The next generation of attacks is actively abusing that trust, however. Protections with greater context and resulting control granularity are required to stop these threats. The more detailed context that's available to internal network protections can address this.

Conclusion

Organizations need to transition to a new way of addressing network security controls to ensure that they've got both the mechanisms and the flexibility to protect modern application infrastructure from today's threats. For an approach to be effective, it's got to be able to carry the context that the environment generates into the policy process so that it can automate necessary changes as workloads are deployed and moved. Network security needs the ability to span existing environments and their links to cloud and edge while providing control abstractions that can extend policy imperatives to where they're needed. It also needs to be able to adapt to changes rapidly, to move beyond the 'change window' thinking that has limited more powerful controls. The means to do all this are available today. An enlightened viewpoint is required to raise the security protection posture and enable the flexibility that modern applications demand.

An effective defense requires:

1. **Know your apps.** Audit, catalog, and understand the application development process in your organization so you can better apply security at the front end.
2. **Enhance your existing protection**. Evaluate your needs for policy controls for applications for internal network traffic. Align your existing perimeter firewall to the external boundary and start looking at solutions for internal protection.
3. **Build for the cloud.** Ensure your solution is flexible enough to map to the evolution of your IT model: on-premises, multi-cloud hybrid-cloud, public cloud, and containers.

Learn more by visiting: *http://www.vmware.com/security*

vmware®

About 451 Research

451 Research is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, we provide essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to over 1,000 client organizations in North America, Europe and around the world. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

NEW YORK
1411 Broadway
New York, NY 10018
+1 212 505 3030

SAN FRANCISCO
140 Geary Street
San Francisco, CA 94108
+1 415 989 1555

LONDON
Paxton House
30, Artillery Lane
London, E1 7LS, UK
+44 (0) 203 929 5700

BOSTON
75-101 Federal Street
Boston, MA 02110
+1 617 598 7200

451 Research®