VMware Service-Defined Firewall

Shrink the application attack surface with a new approach to firewalling

Introduction

With digital transformation, business applications are changing rapidly from a traditional framework to a distributed architecture. Applications now consist of many distinct services running on heterogeneous workloads that are networked together, increasing both complexity and the size of the applications' attack surface. For many organizations like yours, it's increasingly difficult to keep attackers out of the internal network perimeter.

As a result, one of the biggest challenges you face in keeping your organization secure is to shrink your applications' attack surface and prevent the lateral movement of threats within the network perimeter. The **VMware Service-Defined Firewall** is designed specifically to mitigate threats inside a data center or cloud network. The Service-Defined Firewall establishes a verified understanding of known good application behavior. From this, it generates adaptive security policies to shrink the application attack surface consistently across on-premises and multi-cloud environments.

VULNERABLE CORPORATE INFORMATION SYSTEMS

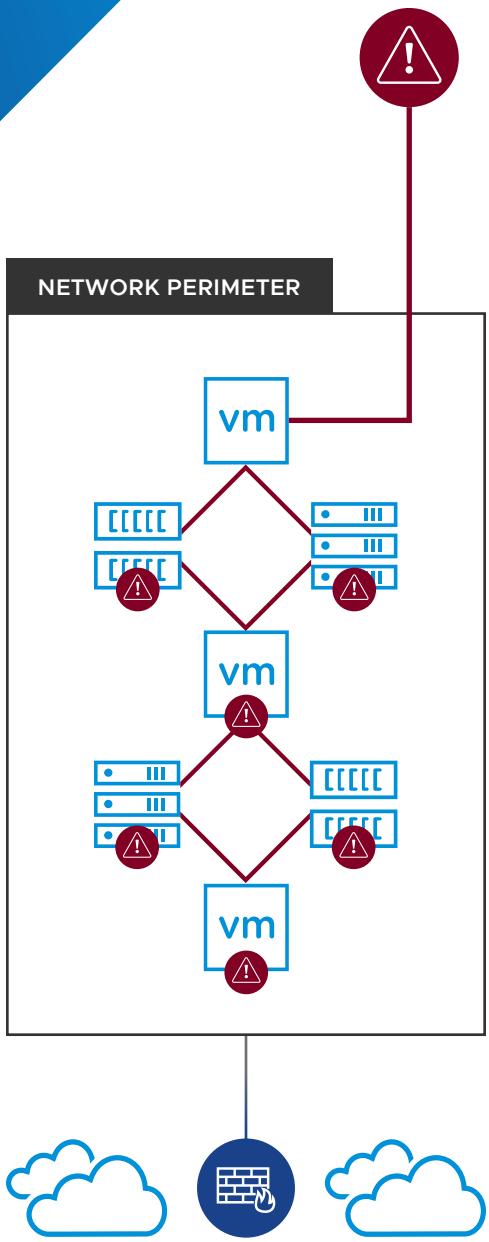
59% of attacks involve attempted lateral movement, according to a recent report.[1]

Addressing Key Issues in Application Security

New application architectures are modernized and distributed across both private and public clouds. Modern network teams are struggling to find ways to ensure comprehensive security and automation for an application-driven network.

Increased Attack Surface – Applications are now comprised of a complex set of distributed services (and increasingly, microservices) running across private and public clouds as well as in VMs, containers, and on bare-metal hosts. They are no longer a simple monolithic stack on a single server (or a few servers) that can be easily secured. This explosion of services on the network has significantly increased the attack surface of an organization.

[1]Source: "Quarterly Incident ResponseThreat Report," July 2018, Carbon Black



Rapid Application Change – Application developers are continually making changes to applications and deploying new services, which in turn require changes to security policies. This creates a reactive dynamic between developer and security operations teams, which can create vulnerabilities.

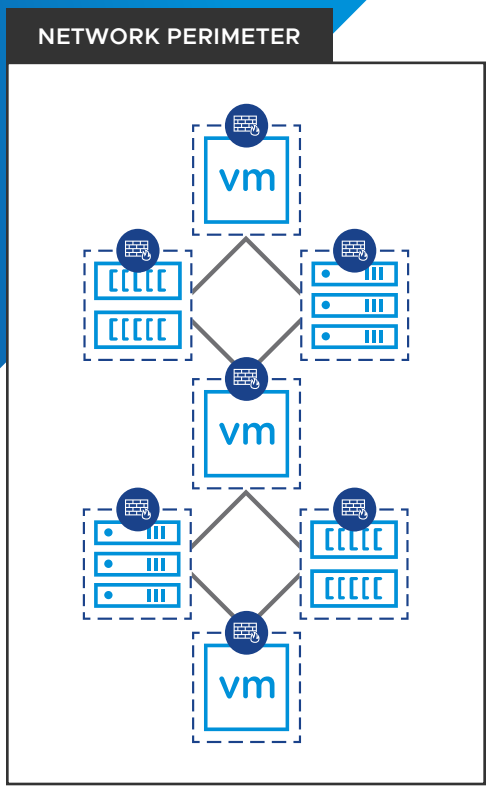
Thinking Beyond the Perimeter Firewall to Improve Security

In order to shrink their attack surface and limit lateral movement of attackers within the environment, many organizations have tried to segment their network with traditional perimeter firewalls deployed inside the network perimeter. While perimeter firewalls excel at filtering traffic coming into the network from external sources, there are a few reasons why their capabilities are ill-suited to reducing the attack surface of the internal network.

First, perimeter firewalls typically filter traffic from unknown hosts and are, therefore, limited to network-centric techniques of determining safe traffic from malicious traffic, such as Layer 7 packet inspection. In order to filter east-west traffic within the network perimeter, it's important to have a deep contextual understanding of the traffic. With an understanding of which application is generating the traffic, where it is originating, and where it is expected to terminate, it is much easier to determine good from bad network activity. Perimeter firewalls lack a comprehensive understanding of application topology, including insight into the hosts that comprise applications and their intended—or known good—behavior.

Second, perimeter firewalls rely primarily on port blocking to control the traffic that they filter. Lateral movement attacks often leverage trusted communication paths to propagate throughout the environment, a technique that port blocking is ineffective against.

And finally, perimeter firewalls are designed to intentionally create choke points for traffic to pass through at the edge of the network so that it can be filtered. Using perimeter firewalls to filter internal network traffic requires that either the traffic be hair-pinned through those choke points or that a firewall is placed in front of every host. The former option creates serious network performance challenges, while the latter option is both operationally infeasible and cost prohibitive.



In order to adequately protect applications and their services, a new approach to firewalling is required. This new type of firewall must be able to understand and control application services at a deep level in order to operationalize strategies like micro-segmentation and reduce the attack surface of an environment.

A New Approach to Firewalling: The VMware Service Defined Firewall

The Service-Defined Firewall takes a very different approach from a perimeter firewall. It is designed to establish a verified understanding of known good application behavior and generate adaptive security policies to shrink the application attack surface consistently across large, distributed environments.

The Service-Defined Firewall accomplishes this with the following capabilities:

Deep Application Visibility and Control – Application visibility and control must extend beyond pure network-centric approaches, such as L7 packet inspection. The Service-Defined Firewall has deep visibility into application services and their behavior, including topology, to understand and control the originating processes that generate network communications. This level of visibility and control is made possible by the fact that the Service-Defined Firewall is built directly into the vSphere hypervisor, making it an intrinsic part of the application infrastructure. This built-in position also alleviates the need for additional agents.

App Verification Cloud - The App Verification Cloud combines artificial intelligence with human intelligence and applies both to the problem of building and verifying a model of known good application behaviour. By analysing known good application behaviour across VMware's massive footprint, the App Verification Cloud can quickly help customers profile their own applications' behaviour and create the best policies for enforcement.

Automated & Adaptive Policies – The Service-Defined Firewall is capable of intelligently configuring and adapting security policies based on changes in application services, which helps keep up with rapid application change.

VULNERABLE MANAGEMENT TODAY

67% of organizations lack full confidence that they can avoid a data breach.[2]

[2]Source: "Gaps in Resources, Risk and Visibility Weaken Cybersecurity Posture," February 2019, Balbix, INC.

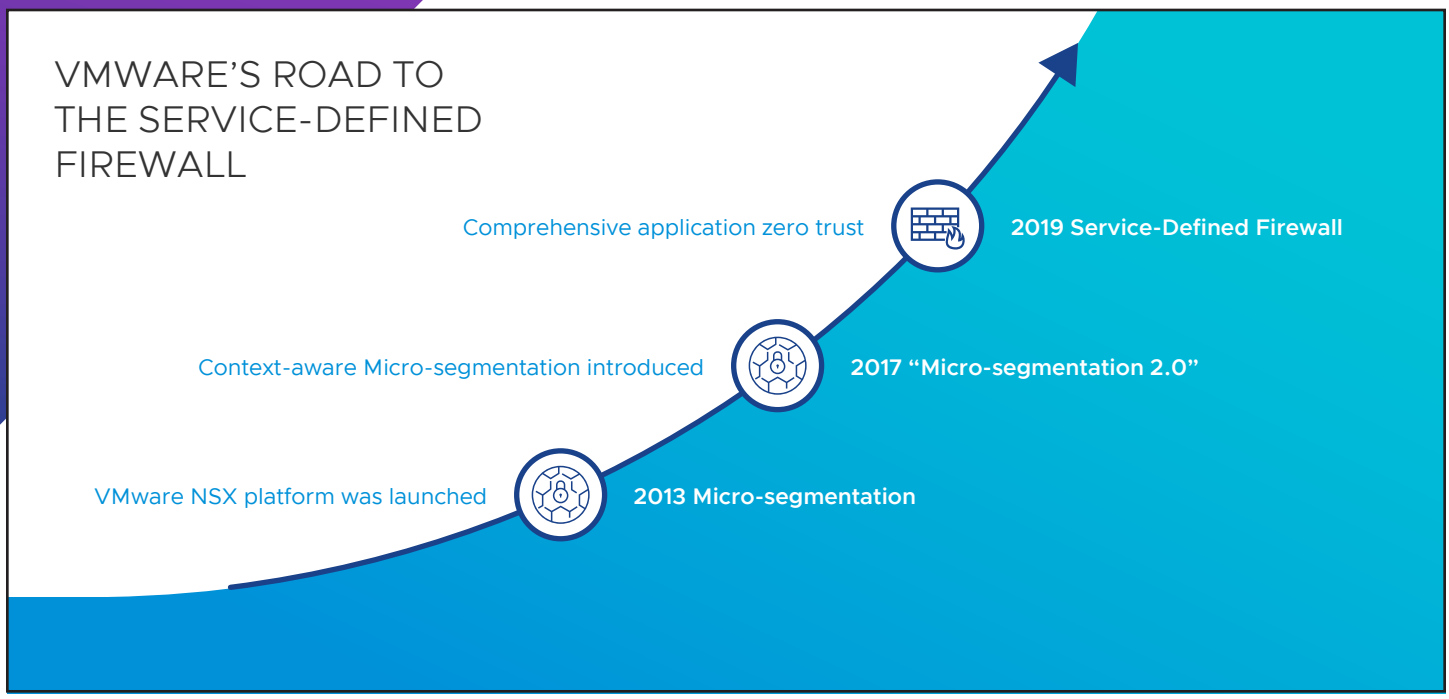
Distributed in Software – In order to deliver ubiquitous protection, the Service-Defined Firewall is deployed consistently wherever application services may be running, across multi-cloud and heterogeneous environments that include VMs, containers, and bare-metal servers. This is achieved through a distributed architecture delivered entirely in software.

Achieving a Milestone in Attack Surface Reduction

VMware has worked for a long time to build and deliver a Service-Defined Firewall solution for organizations like yours. Micro-segmentation was the first step toward shrinking the application attack surface and mitigating the lateral movement of threats inside the network perimeter. However, micro-segmentation was originally focused on relatively crude network segmentation at Layer 4. As applications have continued to become more complex, a deeper level of application visibility and control is required that takes into account the workloads and services that comprise applications.

SECURITY BOOST WITH AI

60% of respondents found that AI-based technologies provided deeper security than humans alone.[3]



[3]Source: "The Value of Artificial Intelligence in Cybersecurity," July 2018, Ponemon Institute LLC.

The Service-Defined Firewall not only enables micro-segmentation at Layer 7, but introduces additional capabilities to control the services that generate network traffic to begin with. The Service-Defined Firewall also supports adaptive policies that are capable of changing with applications as they change over time, something that was difficult to operationalize with pure micro-segmentation products. VMware delivers its comprehensive solution for Service-Defined Firewall capabilities through a combination of VMware NSX and VMware AppDefense.

Summary

Solving the problem of how to mitigate lateral movement requires a different set of capabilities that go beyond those required for protecting your organization's perimeter. VMware's Service-Defined Firewall is the right tool for the right job.

The VMware Service-Defined Firewall leverages its intrinsic position within the hypervisor to obtain unparalleled visibility and control over known good application behavior, without the need for more agents. The App Verification Cloud combines machine learning with human intelligence to verify that known good application behavior is as expected to expedite the creation of security policies. Finally, the Service-Defined Firewall is delivered entirely in software—ensuring that protection for your organization is extended consistently across heterogeneous infrastructure to help ease policy management.

Learn More:

VMware Service-Defined Firewall

VMware NSX Data Center

VMware AppDefense