Service-defined Firewall for Virtual Desktops

Micro-segment VDI environments to isolate desktops and block the lateral movement of threats

AT A GLANCE

Virtual desktops help consolidate end-user applications and data into well-managed data centers—thus lowering costs and improving data protection. However, they expose data center infrastructure to end-user security violations. VMware enables easy micro-segmentation for virtual desktops, thereby isolating end users from data center infrastructure.

KEY HIGHLIGHTS

- **Uniform security infrastructure:** Use a single firewalling infrastructure for the entire data center, including security zones, applications, and the virtual desktop infrastructure (VDI).
- **Compact policies:** Define compact security policies using intuitive constructs such as user-id, application-id, and security tags.
- **Restricted lateral movement:** Isolate virtual desktops from the VDI back end and the rest of the data center infrastructure, thereby restricting the lateral movement of threats.

Virtual desktops offer simplicity, savings, yet introduce threats

VMware Horizon enables centralized hosting of users' desktop sessions using either Remote Desktop Session Host (RDSH) or virtual desktop pools. The consolidation of end users' applications and data reduces infrastructure costs and improves manageability and data protection. However, since users' desktops are occasionally breached, their proximity to sensitive data center infrastructure presents a new threat. An attacker might take over a user desktop and use it to infiltrate nearby servers. Security teams must isolate virtual desktops and block lateral attacks.

Solution: Service-defined Firewall for virtual desktops

The VMware NSX Service-defined Firewall protects East-West network traffic across multi-cloud environments with stateful layer 2–layer 7 distributed firewalling. The Service-defined Firewall supports fine-grained segmentation of the data center network, down to the individual workload, and includes user identification and application identification. Using the Service-defined Firewall, admins can isolate virtual desktop zones from other data center infrastructure, inspect the traffic between the zones, and block potential lateral movement.

Typically, users have different access rights to applications and resources based on their role (e.g., only the finance group can access financial systems). However, virtual desktop sessions share IP addresses between users, complicating enforcement of proper access rights using just IP addresses. The Service-defined Firewall's identity-based firewalling capability seamlessly integrates with Active Directory. Thus, admins can use the Service-defined Firewall to control user access to resources based on their Active Directory groups and identity.

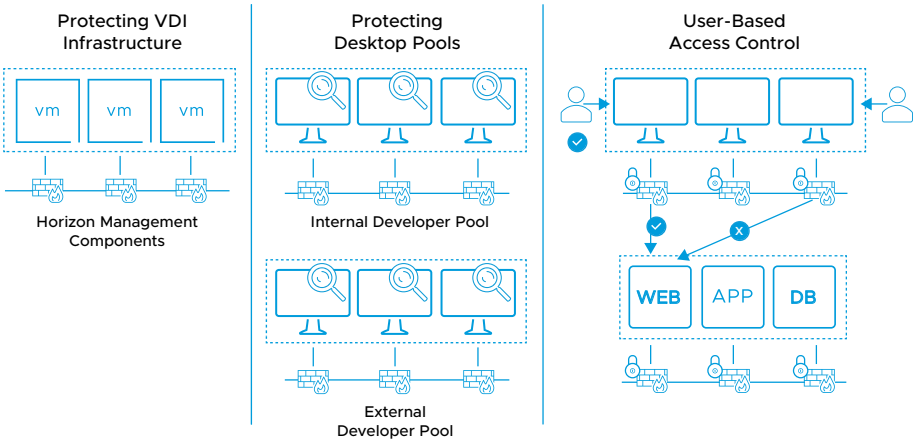

FIGURE 1: Service-defined Firewall Protects VDI, Virtual Desktops and Applications

USE CASES (See Figure 1)

Protecting VDI Infrastructure: Leverage the distributed architecture of the Service-defined Firewall to protect the VDI infrastructure itself, including the Horizon management components.

Isolating desktop pools: Isolate vulnerable user desktops from the rest of the data center infrastructure, via the network segmentation capabilities of the Service-defined Firewall.

User-based access control: Define security policies based on users' identity and Active Directory group membership. Use the Service-defined Firewall to inspect and enforce user access control rights to designated applications and data center resources.

Agentless anti-virus: Easily insert anti-virus inspection into every virtual desktop, without the overhead of licensing or deploying agents on the desktop.

LEARN MORE

Check out these resources to learn more about how to protect your virtual desktops. Reach out to your VMware Sales Representative for further details.

VMware Horizon

NSX Data Center

NSX Service-defined Firewall

Independent Solution Test

Key capabilities

Distributed Micro-segmentation
The Service-defined Firewall utilizes the VMware NSX virtual network to isolate and segment resources regardless of the underlying physical network. Its distributed architecture supports stateful network traffic inspection and policy enforcement on a per-workload granularity.

User-Based Policies
Through its integration with Active Directory (AD), the Service-defined Firewall enables user-specific security policies. User access to critical data center resources is governed by their AD group membership and access rights.

Compact Object-Based Model
Security policies are based on a high-level object model, using attributes such as OS type, VM names, and Active Directory entries. This model eliminates dependencies on ephemeral IP addresses and low-level traffic attributes while enabling isolation of virtual desktops with just a few policies.

Centralized Control
Security policies are defined centrally and distributed throughout the network. A central control plane ensures consistency across virtual desktops and a hybrid network composed of VMs, containers, bare-metal machines, and cloud services.

VMware Horizon + Service-defined Firewall = Secure virtual desktops

VMware Horizon is a comprehensive solution for desktop virtualization. The Service-defined Firewall adds a security layer to desktop virtualization, protecting critical data center resources from lateral attacks initiated via users' desktops. Combined, VMware Horizon and Service-defined Firewall provide operational benefits inherent to desktop virtualization while mitigating its security challenges.

Independently tested

Coalfire, a leading cybersecurity advisory firm, has independently tested the Service-defined Firewall capabilities for protecting virtual desktops. The tests conducted at the Coalfire Labs illustrated how cyber-attacks launched through virtual desktops can be averted by the Service-defined Firewall.

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com Copyright © 2020 VMware, Inc.
All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: vmw-so-firewall-for-virtual-desktops-uslet_v9 3/20