Protecting the human point.

Solution Brief

FORCEPOINT Microsegmentation with Forcepoint NGFW in VMware NSX

The accelerating adoption of virtualization is driving a real need for balancing rapid provisioning of granular security services and the dynamic updating of security policies on deployed virtual firewalls. The integration of Forcepoint NGFW and VMware NSX manager enables the automated rollout of strong security for both north-south and east-west traffic, providing full visibility and consistent enforcement throughout the enterprise.

Challenges with Virtualized Environment

Even though data centers are traditionally protected by strong perimeter defenses (Figure 1), sophisticated threats and exploits still manage to get through. Once inside the data center, these attacks target critical systems, often taking advantage of weak internal security controls to spread throughout various servers and databases.

Internal east-west communication among servers is growing rapidly, due to data and applications being combined in innovative ways by service-oriented architectures. Visibility into cyber behaviors and inspection of data traffic has become crucial to detecting malicious intrusions into the data center and shutting down attacks before they can spread laterally and compromise operations. Simplistic partitioning of networks within data centers is no longer feasible—digital transformation requires sharing information across many different systems. This sharing must dynamically controlled and secured.

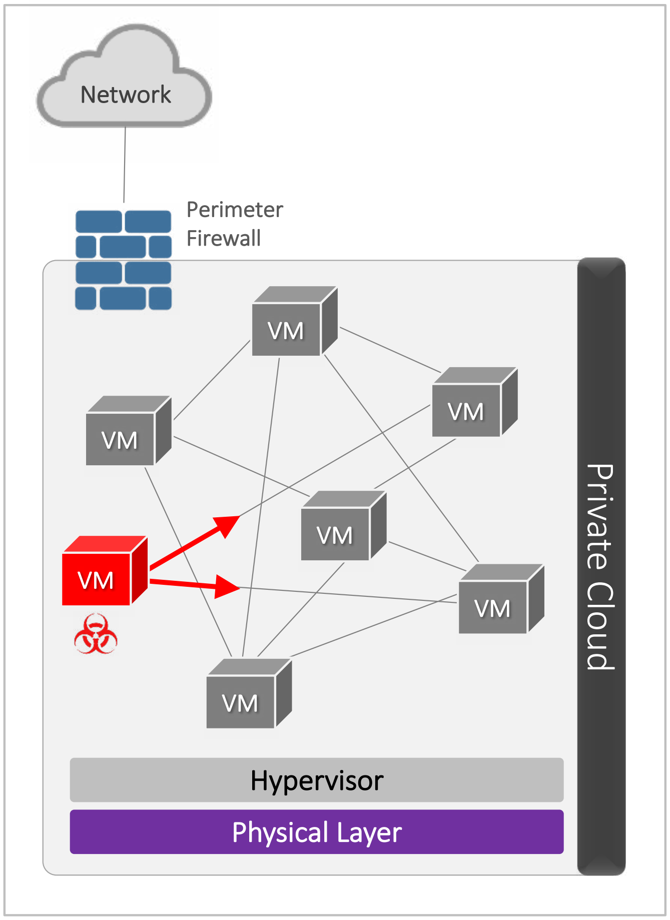

Figure 1.

To be effective, east-west security solutions need to:

- **Automate the provisioning of new servers or services into the data center.**
- **Apply granular security controls to individual components.**
- **Minimize traffic disruption when virtual machines migrate to different hosts.**
- **Provide visibility across network components, even as they change over time.**

Microsegmentation in Data Centers

To prevent attacks from spreading from one server to another, organizations are using firewalls to control network traffic within the data center. Figure 2 shows a common approach in which web servers, application servers and database servers are isolated to prevent a compromise in one part of the system from opening the door to attacks on other parts. Microsegmentation enables appropriate communications and data to be sent between systems while blocking any unexpected traffic. It is a zero-trust approach that provides granular protection for each segment in the datacenter down to the individual workload level.

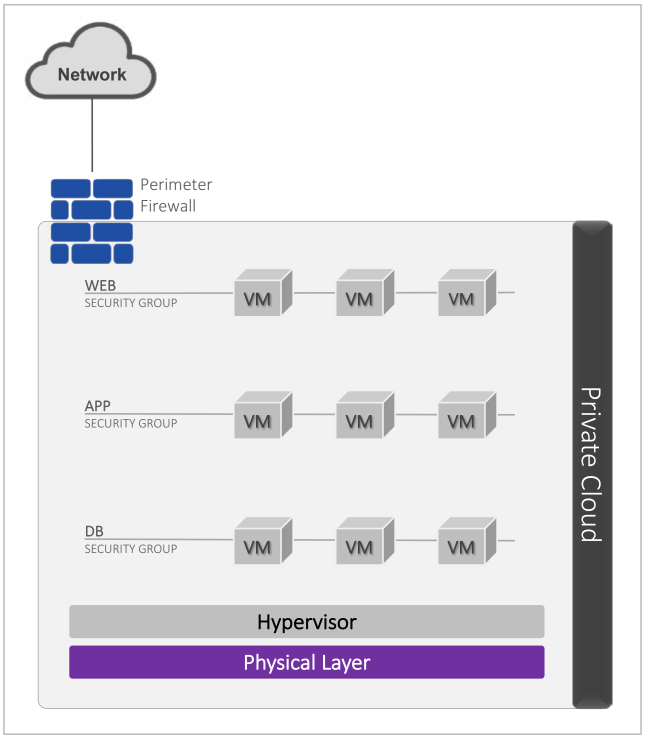

Figure 2

Deploying Forcepoint NGFW in VMware NSX using Intel Security Controller

By applying appropriate firewall rules to each security group, Forcepoint NGFW provides microsegmentation and deep packet inspection of east-west traffic managed by NSX. It goes beyond the basic network isolation provided within NSX, providing deep packet inspection and application-level control for traffic among the different workloads. Virtualized Forcepoint NGFW instances have all of the same inspection capabilities of physical firewall appliances—and can even share the same security policies—providing consistent visibility and enforcement throughout the enterprise. This combines both distributed firewall and next generation IPS capabilities into the heart of the virtualized platform in a way that scales seamlessly with the rest of the environment.

Forcepoint NGFW uses Intel Security Controller software to orchestrate the fast provisioning and scalability of security services and to dynamically update security policies on the virtual firewalls. ISC essentially acts as a broker for policy information between VMware NSX and Forcepoint Security Management Center, immediately synchronizing policy updates with NSX as service profiles within the NSX service composer.

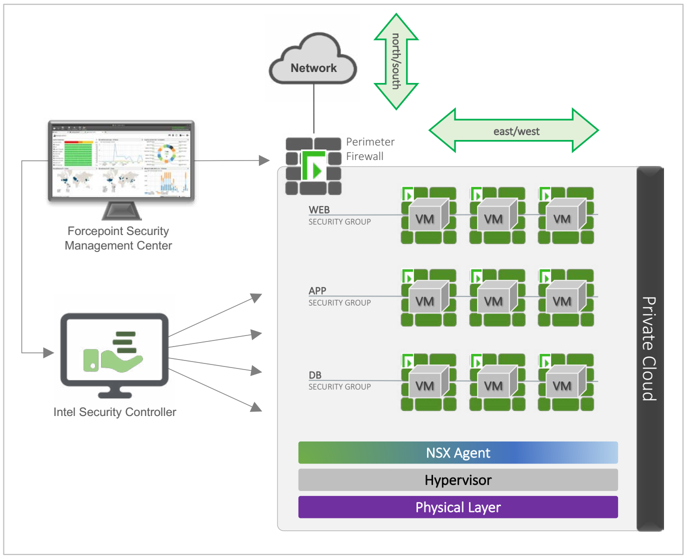

Figure 3

High Security with High Efficiency

The combination of Forcepoint NGFW and Intel Security Controller enables strong security to be deployed quickly throughout workloads in VMware NSX. Forcepoint's rich security policies, along with automated orchestration, enable comprehensive protection to be implemented at scale with the click of a button. Forcepoint NGFW enables organizations to deploy new services quickly and safely, reducing the risk of breaches while dramatically reducing the time spent by admins and IT personnel.

CONTACT
www.forcepoint.com/contact

[SOLUTIONBRIEF_NGFW-VMWARE_EN] 700005.071817