A MULTILAYERED, DYNAMIC, AND AUTOMATED APPROACH TO SECURING VIRTUALIZED AND CLOUD ENVIRONMENTS

Virtualization and cloud computing have helped organizations of every size achieve significant data center savings in hardware costs, operational expenditures, and energy demands—while achieving meaningful improvements in quality of service and business agility. Yet many organizations don’t realize that using their existing legacy security solutions to address the prevailing threat landscape in virtual environments can expose them to new types of attacks and data loss.

Additionally, as more organizations transition from a mix of physical and virtual data centers to private, public, and hybrid cloud environments, the problem becomes even more evident as gaps in security get even wider. Unfortunately, this undermines the confidence of IT organizations to migrate mission-critical workloads to agile, lower cost cloud environments. And ultimately, this hinders the ability to fully leverage this new computing paradigm and maximize the return on investment in these technologies.

The Challenge
IT and security professionals are continually being asked to deliver the benefits of virtualization and cloud technologies without undermining the security of the organization in the process. Yet to provide security in a cloud environment, it is essential to address the most significant underlying technology of cloud computing—virtualization of workloads or virtual machines (VMs). And at the very heart of the issue is the impact of virtualization on network security.

In the virtual world, virtual machines can be highly dynamic, with frequent add, move, and change operations. This complicates the ability to attach security policies to VM instantiation and track security policies with VM movement so that regulatory requirements and compliance continue to be met. Virtualized computing environments also enable direct communication between virtual machines within a server. But intra-host communications may not be visible to network-based security appliances residing outside a virtual server.

In short, the dynamic and flexible nature of virtualization and cloud computing can easily lead to a loss of visibility and control that were always taken for granted in a physical world. See Figure 1 for a list of common security concerns in the virtualized data center.

Key challenges:
- Lack of visibility into, or control of, traffic between VMs that never touches the physical network
- Undetected and uncontained malware outbreaks or insider attacks in the virtual environment
- Inability to enforce policies that isolate VMs, prevent VM sprawl, or secure features like vMotion
- Virtualization compliance gaps and audit data holes
- Increasing network complexity and administrative burden caused by applying legacy VLAN or firewall technology to the virtual environment, overlay networks, and dynamic resource scheduling

Figure 1. The challenges of virtualized data centers
Juniper Networks Firefly Suite

To protect virtualized environments and avoid the aforementioned security challenges, Juniper Networks has extended the capabilities of our award-winning security products to the virtual world with a next-generation security approach that eases operational challenges by moving beyond conventional security systems to secure virtual assets in highly dynamic environments—without compromising on performance, availability, and management control.

The Juniper Networks® Firefly suite is purpose-built for the virtual environment. It provides a flexible security experience for both enterprises and service providers by delivering a multilayered solution that spans from the network edge for north/south communication to inter-VM packets for east/west communication, thus securing traffic from all directions.

The suite enables network and security administrators to dynamically deploy and scale firewall protection with the breadth and depth required to address the key security challenges unique to the virtual data center.

Features and Benefits

Table 1: Firefly Suite Features and Benefits

<table>
<thead>
<tr>
<th>Secure</th>
<th>Application Agility</th>
<th>Optimized Performance</th>
<th>Rapid Service Rollout</th>
<th>Error-free Deployments</th>
<th>Ready for Innovation</th>
<th>Extensive Visibility</th>
<th>Unified Management</th>
<th>Enhanced Flexibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Targeted Protection</td>
<td>Granular security policy consistent with the risk associated with each application, providing continuous protection for applications in the virtual environment</td>
<td>Performance optimized with firewalls designed to protect communication in specific directions, including a line-rate option in the kernel of the hypervisor or firewalls running in virtual machines</td>
<td>Easily scale out deployments, with zero touch provisioning, bulk provisioning, predefined configuration templates, and automated tasks</td>
<td>Automation tools, workflow-based tasks, and web-based intuitive GUI that ease deployments</td>
<td>Rich set of APIs for easy integration to third-party custom applications and management platforms, supporting Network Functions Virtualization (NFV) and Software Defined Networks (SDN)</td>
<td>Rich information on the virtual environment, including the ability to scan a VM’s content (introspection) or report on the traffic flow</td>
<td>Consistent security policy creation and provisioning for virtual and physical firewalls featuring Juniper Networks Junos® operating system-based security, Network Address Translation (NAT), routing, and VPN connectivity features</td>
<td>Create, attach, and easily change granular security policy that protects communication to the virtual data center and between VMs in the data center</td>
</tr>
<tr>
<td>Automation</td>
<td>Automation tools, workflow-based tasks, and web-based intuitive GUI that ease deployments</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Optimization</td>
<td>Rich set of APIs for easy integration to third-party custom applications and management platforms, supporting Network Functions Virtualization (NFV) and Software Defined Networks (SDN)</td>
<td>Rich information on the virtual environment, including the ability to scan a VM’s content (introspection) or report on the traffic flow</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td>Consistent security policy creation and provisioning for virtual and physical firewalls featuring Juniper Networks Junos® operating system-based security, Network Address Translation (NAT), routing, and VPN connectivity features</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enhanced Flexibility</td>
<td>Create, attach, and easily change granular security policy that protects communication to the virtual data center and between VMs in the data center</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Solution Components

The Firefly suite is a compilation of three innovative security point products that have been brought together into a single comprehensive flexible solution that is designed to keep your VMs secure while addressing the operational challenges posed by the virtual infrastructure.

The Firefly suite includes the following three products: Firefly Host, Firefly Perimeter, and Junos Space Virtual Director (see Figure 2).

Firefly Host

Firefly Host is a comprehensive virtualization security solution that includes integrated stateful inspection firewalling, intrusion detection, compliance monitoring and enforcement, as well as on-access and on-demand antivirus scanning. Key elements of the product include:

- Purpose-built firewall for virtualization designed to protect intra-VM east/west traffic
- Integration into the kernel of the hypervisor
- Synchronization with VMware vCenter
- Introspection and content protection, including anti-malware

Firefly Perimeter

The Firefly Perimeter is a complete firewall in a flexible VM format based on fully tested Junos OS-based Juniper Networks SRX Series Services Gateways code. Key elements of the product include:

- Stateful packet processing and application-layer gateway (ALG) features
- Rich connectivity features based on a powerful Junos OS foundation, including routing, NAT, and VPN
- Granular security between zones, creating boundaries between organizations, lines of business, and applications
Firewall to diversified virtual firewall implementations. With Firefly Perimeter, MSSPs can migrate from the monolithic architecture and design limitations of a physical hardware. Firefly Perimeter enables Managed Security Service Providers (MSSPs) to launch and activate new services more quickly by decoupling security services from customer premises (CPE). Firefly Perimeter for Managed Security Service Providers (MSSPs) can migrate from the public cloud to their private cloud (north/south traffic). Automation allows service providers to easily connect tenants from the kernel, Firefly Host offers easy isolation between tenants sharing the same physical environment. If a service provider wants to prevent an attack on one VM from impacting other tenants sharing the same physical environment. From a management perspective, Junos Space Virtual Director and Junos Space Security Director provide initial setup wizards for provisioning and managing Firefly Perimeter VMs to enforcing context-aware policy.

The Firefly Suite and Private Cloud
IT Administrators who want to provide their internal customers with VM-based services and retain their ability to segment the virtual environment can deploy Firefly Perimeter and Firefly Host in a private cloud by creating clear demarcation zones by campus, line of business, department, user group, or application type. Network and security administrators can leverage Firefly Perimeter’s two key features – zones and policies and configure and deploy security gateways rapidly. From a management perspective, Junos Space Virtual Director and Junos Space Security Director provide initial setup wizards for provisioning and managing Firefly Perimeter VMs to enforcing context-aware policy.

Deployment Models

The Firefly Suite and Public Cloud
Service providers, large and small have one common goal and that is to gain and retain their customer base. To achieve this goal, they must preserve their customer’s trust and to achieve this, service providers must impose a clear demarcation zone between tenants that share the same physical hardware. This is mandatory if a service provider wants to prevent an attack on one VM from impacting other tenants sharing the same physical environment. From the kernel, Firefly Host offers easy isolation between tenants at high speeds (east/west traffic). Firefly Perimeter’s rich routing, VPN, and NAT features, along with its simple provisioning and automation allows service providers to easily connect tenants from the public cloud to their private cloud (north/south traffic). By bundling these advanced products together, the Firefly Suite prevents one tenant from posing a risk to others in terms of data loss, misuse, privacy infringement, or network downtime.

Firefly Perimeter for Managed Security Service Providers (MSSPs)
Firefly Perimeter enables Managed Security Service Providers (MSSPs) to launch and activate new services more quickly by decoupling security services from customer premises (CPE) hardware. With Firefly Perimeter, MSSPs can migrate from the monolithic architecture and design limitations of a physical firewall to diversified virtual firewall implementations. They can decentralize fault domains by deploying Firefly Perimeter VMs instead of dedicating a physical firewall to each tenant/customer or sharing one physical firewall across multiple tenants, reaping better returns on their investment. This reduces capital expenditure while aligning the billing with the actual usage. Additionally, having a firewall in a VM mapped to a single customer allows MSSPs to customize policies and perform maintenance, which only impacts that single customer instead of the traditional approach where numerous customers sharing the same physical firewall are all impacted. Firefly Perimeter enables MSSPs to offer value-added security services such as managed firewall, MPLS, VPN, clean pipe, and secure VM hosting, with a deployment model that lowers time to revenue.

Junos OS Capabilities Out-of-the-Box
Systems integrators and other custom system providers can leverage Firefly Perimeter to provide a firewall offering on x86 appliances. Firefly Perimeter can establish and secure communications via routing, NAT, and VPN technology. The x86 appliances typically host many applications that run in separate VMs. Additionally, these x86 appliances may be built to withstand extreme operating conditions (heat, dirt, etc.) via ruggedized form factors. Such appliances typically include a VPN that provides connectivity to the central office. The variety of management interfaces for Firefly Perimeter enables VMs to be securely initiated via the bootstrap settings and then managed via CLI, DMI/Netconf, Junos Web, or Junos Space Virtual Director—offering the immense flexibility required for different users and use cases.

Enabling a Safe and Secure Journey to the Cloud
At Juniper, we believe that virtualization security goes beyond simply using existing physical security tools to secure virtual data centers. At the same time, allowing security to delay migration to the cloud puts the business at a disadvantage, since it cannot leverage key cloud benefits such as flexibility, new business model enablement, and cost savings.

With Firefly Suite, Juniper offers enterprises and service providers a virtual security solution that enables a safe journey to the cloud. The solution sets offers multilayered security from the network boundary to the smallest inter-VM packets, protecting assets in the cloud from every direction. Whether the business demands a completely outsourced, hosted, or hybrid solution, Juniper Networks Firefly Suite provides virtual security for VMs that is simple and easy to implement, with granular control over physical and virtual assets and automation for operational ease and efficiency.

Next Steps
For more information on how you can securely start your journey to virtualization, please visit www.juniper.net/firefly or contact our sales team.
About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.