FIREFLY PERIMETER

Product Overview

Network vulnerabilities are just as applicable in a virtualized data center as a traditional one. The virtual infrastructure also introduces new elements that require additional security considerations over and above those required to secure the physical data center. These new challenges demand solutions that integrate seamlessly into virtualized and cloud environments and can provide real-time security for virtual assets.

Firefly Perimeter addresses these aforementioned challenges by extending the capabilities of Juniper Network's award-winning security products to the virtual world, empowering administrators to dynamically deploy and scale firewall protection without compromising on performance, availability and control.

Product Description

Juniper Networks® Firefly Perimeter goes beyond traditional security appliances with a new virtual firewall that is delivered in a virtual machine (VM) form factor and based on Juniper's Junos® operating system and SRX Series Services Gateway. Firefly Perimeter delivers scalable, available, and granular security with segmentation capabilities that create clear demarcation between departments, lines of business, user groups and application types as well as rich connectivity features like Network Address Translation (NAT), routing and VPN.

Firefly Perimeter operates deep within the virtualized fabric, offering layers of defense and secure connectivity with multilevel policy controls that safeguard dynamic changes in workloads, traffic and content allowing enterprises and services providers alike to deliver IT services to their internal and external customers securely and efficiently.

Features and Benefits

Firefly Perimeter is designed to provide firewall protection and apply policies at the VM level. Firefly Perimeter features include:

- Complete firewall with stateful packet processing and application-layer gateway (ALG) features in a flexible virtual machine format
- Rich connectivity features with extensive routing capabilities, NAT, and VPN, based on a powerful Junos OS foundation
- Industry-leading management that leverages Juniper Networks Junos Space Security Director for both physical and virtual firewall configuration, and Junos Space Virtual Director for deployment and monitoring. Junos Space also provides a rich set of APIs, supporting custom integrations with third-party management platforms.

Easy Configuration

Firefly Perimeter uses two features—zones and policies. The default configuration contains, at a minimum, a "trust" and an "untrust" zone. The trust zone is used for configuration and attaching the internal network to Firefly Perimeter. The untrust zone is commonly used for the untrusted network. To simplify installation and make configuration easier, a default policy is in place that allows traffic originating from the trust zone to flow to the untrust zone. This policy blocks all traffic originating from the untrust zone to the trust zone. A traditional router forwards all traffic without regard to a firewall (session awareness) or policy (origination and destination of a session). Furthermore, because of the virtual nature of Firefly Perimeter, customers can leverage snapshots, cloning, and related technology to streamline maintenance and operational tasks.

High Availability (HA)

Firefly Perimeter provides mission-critical reliability, supporting chassis clustering for both active/active as well as active/passive modes. This support provides full stateful failover for any connections being processed. In addition, it is possible for the cluster members to span hypervisors. When Firefly Perimeter VMs are configured in a cluster, the VM synchronizes connection/session state and flow information, IPsec security associations, NAT traffic, address book information, configuration changes, and more. As a result, not only is the session preserved during failover but security is kept intact. In an unstable network, Firefly Perimeter also mitigates link flapping. Figure 1 shows the HA deployment model.

Note: HA is currently only supported on the VMware platform.

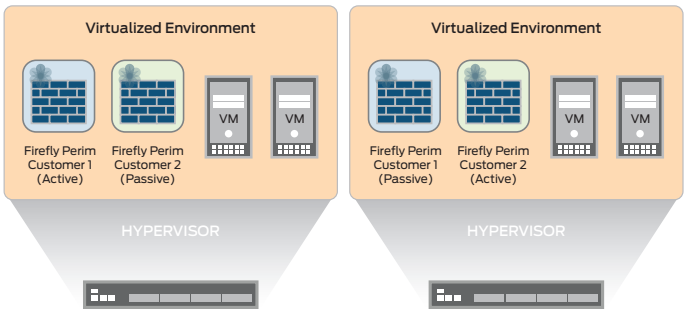

Figure 1: Chassis clustering, with the ability to span hypervisors

Performance

Traditionally, customers have needed to make a trade-off between scalability and performance. The Firefly Perimeter solution is optimized to leverage multiple virtual CPUs to maximize packet processing and overall throughput in the virtual environment. Each Firefly Perimeter VM also has multiple virtual network interface cards (vNICs), which can be connected to various virtual networks to simultaneously protect multiple zones of similar VMs. Operating from within the virtual fabric, Juniper Networks Firefly Perimeter provides the best of both worlds—strong security with the performance needed in a virtual environment.

Security policies determine if a session can originate in one zone and traverse to another zone. Firefly Perimeter receives packets and keeps track of every session, of every application, and of every user. As a VM moves within a cloud environment, it will still send its packets to Firefly Perimeter for processing and therefore will always be communicating in a secure mode.

In order to optimize the throughput and latency of the combined router and firewall, Junos OS implements session-based forwarding, an innovation that combines the session state information of a traditional firewall and the next-hop forwarding of a classic router into a single operation. With Junos OS, a session that is permitted by the forwarding policy is added to the forwarding table along with a pointer to the next-hop route. Established sessions have a single table lookup to verify that the session has been permitted and to find the next hop. This efficient algorithm improves throughput and lowers latency for session traffic when compared with a classic router that performs multiple table lookups to verify session information and then to find a next-hop route.

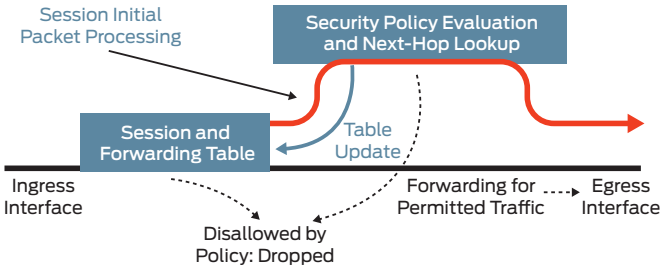

Figure 2: Session-based forwarding algorithm

Figure 2 shows the session-based forwarding algorithm. When a new session is established, the session-based architecture within Junos OS verifies that the session is allowed by the forwarding policies. If the session is allowed, Junos OS will look up the next-hop route in the routing table. It then inserts the session and the next-hop route into the session and forwarding table and forwards the packet. Subsequent packets for the established session require a single table lookup in the session and forwarding table, and are forwarded to the egress interface.

Intelligent Management with Consistent Security Policy Across Physical and Virtual Networks

Handling multiple Firefly VMs across different hypervisor hosts and tenants requires a seamless way to centrally manage the VM from provisioning to decommissioning. Workloads must be secured in a consistent manner, and the policies that apply to physical workloads must also apply to virtual workloads, regardless of where they reside.

Junos Space Virtual Director is a smart, comprehensive, and automated VM management application. Administrators can automate the provisioning and resource allocation for Firefly Perimeter VMs, easily scaling them to meet dynamic demand. Firefly Perimeter with Virtual Director also provides insight into the traffic, capacity utilization, and health of the security layer.

Junos Space Security Director offers administrators a simple way to create a series of security policies that will control the traffic from within and in between zones for both physical and virtual firewalls. At the broadest level, all types of traffic can be allowed from any source in security zones to any destination in all other zones without any restrictions. At the narrowest level, policies can be created to allow only one kind of traffic between a specified system in one zone and another specified system in another zone during a scheduled time period.

Firefly Perimeter also includes wizards for firewall, IPsec VPN, NAT, and initial setup to simplify configurations out-of-the-box. Policy-based VPNs support more complex security architectures that require dynamic addressing and split tunneling.

Junos Space and the applications which run on it each provide a rich set of APIs for easy integration to third-party custom applications and management platforms, supporting SDN and Network Functions Virtualization (NFV).

Juniper offers firewall services in both physical and virtualized deployments providing deployment choices which best suits your particular use case.

Specifications

The following table highlights high-level specifications. Please see the product documentation for a complete list.

Protocols	IP Address Management	Security	SLA, Measurement, and Monitoring	Hypervisors
• IPv4, IPv6, MPLS, ISO Connectionless Network Service (CLNS) • Static routes • RIPv2 +v1 • OSPF/OSPFv3 • BGP • IS-IS • Multicast (Internet Group Management Protocol, PIM, Session Description Protocol) • MPLS • VPLS	• Static • Dynamic Host Configuration Protocol (DHCP) • Internal DHCP server, DHCP relay • Address Translation • Source NAT with Port Address Translation (PAT) • Static NAT • Destination NAT with PAT • Persistent NAT, NAT64 • Encapsulations • Ethernet • 802.1q VLAN support	• Firewall • Firewall, zones, screens, policies • Stateful firewall, stateless filters • Network attack detection • Screens denial of service (DoS) and DDoS protection (anomaly-based) • Replay attack prevention; anti-replay • Unified access control (UAC) • TCP reassembly for fragmented packet protection • Brute force attack mitigation • SYN cookie protection • Zone-based IP spoofing • Malformed packet protection • VPN • Tunnels (generic routing encapsulation, IP-IP) • IPsec, Data Encryption Standard (DES) (56-bit), triple Data Encryption Standard (3DES) (168-bit), Advanced Encryption Standard (AES) (128-bit+) encryption • Message Digest 5 (MD5), SHA-1, SHA-128, SHA-256 authentication • IPv6	• Real-time performance monitoring (RPM) • Sessions, packets, and bandwidth usage • IP monitoring • Logging • System logging • Traceroute • Extensive control and data plane structured and unstructured system log administration • Junos Space Security Director support • Juniper Networks Secure Analytics • Juniper Networks Advanced Insight Solutions support • External administrator database (RADIUS, LDAP, SecureID) • Auto-configuration • Configuration rollback • Rescue configuration with button • Commit confirm for changes • Auto-record for diagnostics • Software upgrades • Junos Web • CLI	Firefly Perimeter supports VMware vSphere 5.0 and 5.1 and KVM CentOS 6.3.

Table 1: Firefly Perimeter Scale and Performance

Scale (VMware ad KVM)	
vRAM Required/Instance	2 GB
vCPUs Required/Instance	2
Max vNICs/Instance	10
Max Zones	128
Max Address Books	128
Max Policies	10240
Max Policies with Count	1024
Max Applications/Policy	128
Max Addresses/Policy	1024
Max Addresses/Address-set	1024
Max Firewall Sessions	256k
Max PAT Sessions (Source NAT with PAT	256k
MAC/ARP Table Size	8k
Max VLANs	4k
Max OSPF Routes	160k
Max VRs Supported	5

Performance	VMware	KVM
Firewall (UDP 1514B pkts)	4.9 Gbps (400 kpps)	1.1 Gbps (85 kpps)
Firewall (IMIX)	1.2 Gbps	242 Mbps
Firewall Ramp Rate (TCP)	26K CPS	9K CPS
Firewall Latency (512B UDP)	105 MicroSec	482 MicroSec
Firewall IPv6 (UDP 512B pkts)	1.7 Gbps	383 Mbps
NAT (UDP 1514B pkts)	4.4 Gbps	1 Gbps
NAT (IMIX)	1.1 Gbps	240 Mbps
NAT Ramp Rate (TCP)	20K CPS	8K CPS
IPsec (3DES+SHA1, 1514B)	295 Mbps	241 Mbps
IPsec (3DES+SHA1, IMIX)	66 Mbps	33 Mbps
IPsec (3DES+SHA1, 64B)	78 kpps	23 kpps
IKE Rate (3DES+SHA1, V1 or 2)	2000 Tunnels (83 Tunnels/sec)	2000 Tunnels (48 Tunnels/sec)

Juniper Networks Service and Support

Juniper Networks is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit **www.juniper.net/us/en/products-services**.

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**.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at +1-866-298-6428 or authorized reseller.

1000489-002-EN Jan 2014 Printed on recycled paper