

SECURING VIRTUAL SERVER ENVIRONMENTS WITH JUNIPER NETWORKS AND ALTOR NETWORKS

Challenge

In a traditional data center, applications and application components run on distinct machines that are segregated by firewalls into trust zones. In a virtualized environment, applications may be running in VMs on the same host, beyond the visibility and control of traditional firewalls.

Solution

Altor Networks' VF, which combines a stateful virtual firewall with a virtual intrusion detection service (IDS), integrates with Juniper Networks security products to deliver a comprehensive data center security solution.

Benefits

With the Juniper-Altor solution, customers benefit from streamlined security management, including a centralized view of security information and consistent policy enforcement across both physical and virtual infrastructures. Meeting compliance requirements is greatly simplified.

As enterprises expand their use of virtual server technology, IT managers have become aware that virtual systems pose unique security challenges. Understanding these challenges is key to extending the existing data center security infrastructure with new tools that encompass virtualized systems.

Through its partnership with Altor Networks, Juniper Networks makes it easy for customers to incorporate virtual servers seamlessly into their security architecture. Juniper has integrated Altor's virtual firewall (VF) technology into the Juniper security portfolio, including Juniper Networks® Network and Security Manager, a unified security policy manager, and Juniper Networks STRM Series Security Threat Response Managers, giving customers visibility into and granular control over virtual machine (VM) traffic.

As a result, administrators can apply security policies consistently across both physical and virtual networks, as well as collect application access data for comprehensive compliance reporting. Combining Altor's virtual firewall technology with Juniper's industry leading security products enables customers to fully secure their virtual server environments and maximize the benefits of server virtualization.

The Challenge

Virtualization changes the way physical devices operate and are managed in the data center, which has significant security implications. For example, virtualized environments create a new access layer, the virtual switch network. Typically, each physical server hosts a virtual switch that supports communication between virtual machines on the same host. The virtual network can grow rapidly as new VMs are created, resulting in complex networking flows and VLAN management.

IT administrators lose visibility into and control over some traffic, since communication between colocated VMs is handled by the host's virtual switch and never leaves the host. In a traditional data center environment, applications and application components (such as databases and Web interfaces) run on distinct machines that are segregated by firewalls into zones of trust. In a virtualized environment, these applications may be running in VMs on the same host, so are able to communicate without accessing the physical network. Consequently, they are beyond the visibility and control of traditional firewalls.

Security is further complicated by VM live migration technologies, such as VMware VMotion and DRS. While these technologies ensure that host resources are maximized, allowing virtual machines to be created, moved, and decommissioned as application loads change, they essentially break zones of trust. For example, traffic isolation mechanisms such as VLANs can be circumvented when a VM is migrated to a host on a VLAN that is different from the original host. Likewise, as VMs move, a server may end up hosting VMs with different trust levels, potentially resulting in privilege escalation for some users.

Further complicating security is the fact that virtual server environments are typically managed by server administration staff, not network or security professionals. Because they lack the training needed to manage and secure virtual networks, server administrators can inadvertently introduce vulnerabilities.

Security Challenges of Server Virtualization

Server virtualization can deliver a substantial return on investment, enabling enterprises to cut their server count as much as ten-fold and reduce the space, air conditioning, and electricity needed in the data center. But enterprises can't afford to achieve these operational savings at the expense of security. They need a comprehensive security solution that enables them to:

- **Gain visibility into VM application behavior and traffic flows:** Enterprises need real-time visibility into the applications running on each VM, as well as the ability to analyze application traffic volumes and bottlenecks, and the ability to profile application types and VM functions.
- **Prevent propagation of worms and trojans:** Enterprises need the ability to block worms and other malicious traffic from propagating across VMs within a virtual server or across virtual servers as VMs migrate. They also need the ability to block traffic that doesn't fit a VM's expected traffic profile.
- **Ensure compliance reporting:** To meet regulatory requirements, enterprises need the ability to report all access attempts into VM-based applications, to collect and report historical application usage, and to generate unified compliance reports that encompass both the physical and virtual environments.
- **Micro-segment zones of trust:** Large enterprises as well as cloud providers need the ability to segment traffic in the virtualized data center without exceeding the maximum number of VLANs. For example, a large enterprise may need to isolate traffic from different groups of users on the same departmental VLAN to prevent unauthorized access to sensitive project information. Similarly, a cloud provider, which can easily have up to 10,000 customers, needs a way to create zones of trust within VLANs that are shared by two or more customers.

In addition to the capability to micro-segment zones of trust, organizations need the ability to define and enforce granular security policies within zones of trust. For example, an enterprise may place all Web servers within the same zone of trust, but disallow communication between the servers to prevent worms or other malware from easily propagating between servers. In a virtualized environment, each VM can potentially represent a zone of trust. Consequently, enterprises need a way to restrict communication between VMs in different zones of trust, and potentially between VMs within the same zone of trust.

The Juniper Networks-Altor Networks Solution

Although virtual server environments present new security challenges, they don't change the traditional model for security. Rather, they require innovative, high-performance solutions that integrate with established security infrastructures. Altor's VF, which combines a stateful virtual firewall with a virtual intrusion detection service (IDS), integrates with Juniper Networks security products to deliver a comprehensive data center security solution. Altor's VF complements physical infrastructure security by providing visibility and control over VM traffic, enforcing policies at the VM level, securing live migration, and preventing inter-VM malware propagation.

A hypervisor-neutral solution, Altor's VF inspects all traffic to and from each VM to eliminate blind spots, and enforces policies at the global, group, and per-VM level. With the Altor VF, enterprises can granularly define security policies within zones of trust and precisely control whether VMs within the same zone of trust can communicate, ensuring isolation between and within trust levels, and allowing for precise micro-segmentation.

For example, IT has the flexibility to define a policy to prevent any traffic from traversing between VMs in the same VLAN, or to allow only certain types of traffic to pass between VMs. Not only does the Altor VF allow for more granular traffic isolation than is possible with VLANs, it also applies default policies to every new VM, which mitigates the risks associated with VM sprawl.

The Altor VF can be installed as a virtual appliance on hosts, or in a VMware environment, it can be installed as a VMsafe module within the hypervisor, delivering 10 times the performance of non-VMsafe virtual firewalls. In addition, by operating as a kernel module rather than a guest VM, the Altor VF can defend itself and the hypervisor against VM-layer attacks.

Juniper's integration of Altor's management server and reporting module with Network and Security Manager and STRM Series Security Threat Response Managers gives customers unified management of the physical and virtual infrastructure within the data center. For example, customers can use NSM to define one set of security policies that are enforced by both the Altor VF and Juniper Networks SRX Series Services Gateways, a multiservice platform that delivers firewall, IPsec VPN, intrusion prevention system (IPS), denial of service (DoS) protection, Network Address Translation (NAT), routing, and quality of service (QoS).

In addition, Juniper imports analyzer output and logs from the Altor VF into the STRM Series, an appliance that provides converged network and security management, including log, compliance, and threat management, for Juniper and multivendor environments. Through this integration, customers get consolidated application usage information and compliance reporting, centralized log/event management, and network-wide threat detection across both the physical and virtual infrastructure. Altor VF also supports rule-based mirroring of virtual network traffic to external devices, so that enterprises can easily leverage SRX Series devices for policy enforcement.

Features and Benefits

With the Juniper-Altor solution, customers benefit from streamlined security management, including a centralized view of security information and consistent policy enforcement across physical and virtual infrastructure. Meeting compliance requirements is greatly simplified.

Consider an environment where multitier applications are deployed across virtual and physical servers, compliance dictates that access controls be in place for all components of the application, and that all instances of network and application access be auditable. In this case, the SRX Series secures access across domains of trust and provides logs to the STRM Series. Altor provides audit information in “blind spots,” such as inter-VM communication on the same virtualized host, and passes it to STRM Series devices, which consolidate all firewall access logs and traffic flow data for complete compliance reporting.

Similarly, the Juniper-Altor solution significantly mitigates malware infections such as Conficker in the virtualized data center. Unpatched Windows servers and VMs are a common problem in the virtualized data center, making it possible for a worm to penetrate one VM and propagate undetected over the virtual network, or be spread via VMotion as infected VMs move to other servers.

In this scenario, the Altor firewall detects and blocks malware in the virtual environment, while the SRX Series detects and blocks it in the physical environment. IT’s ability to micro-segment the network by creating zones of trust down to the individual VM level, as needed, ensures that malicious traffic is unable to spread.

Extending the Data Center Security Architecture

The Juniper-Altor solution enables enterprises to easily extend their existing data center security architecture to encompass virtual servers. For example, traditional firewalls continue to play a key role in securing communication between devices and zones of trust. Whether traffic originates from a physical device or a VM, all communication between security zones should be forwarded through the SRX Series data center firewall. For its part, the Altor VF is ideally positioned to enforce security policies on intra-zone communication between VMs on the same virtual server.

Likewise, physical servers and virtual machines in the same security zone should be placed on a shared VLAN, and VMs in the same security zone should also reside on the same virtual server cluster. These configurations allow for isolation between zones of trust, with inter-zone communication controlled by the SRX Series. Communication within a security zone should be controlled via intra-zone policies, which can easily be defined within NSM. These policies are enforced by the SRX Series when communication occurs between physical devices, virtual server clusters, or VMs that reside on separate servers, while the Altor VF enforces policy controls on VMs running on the same host.

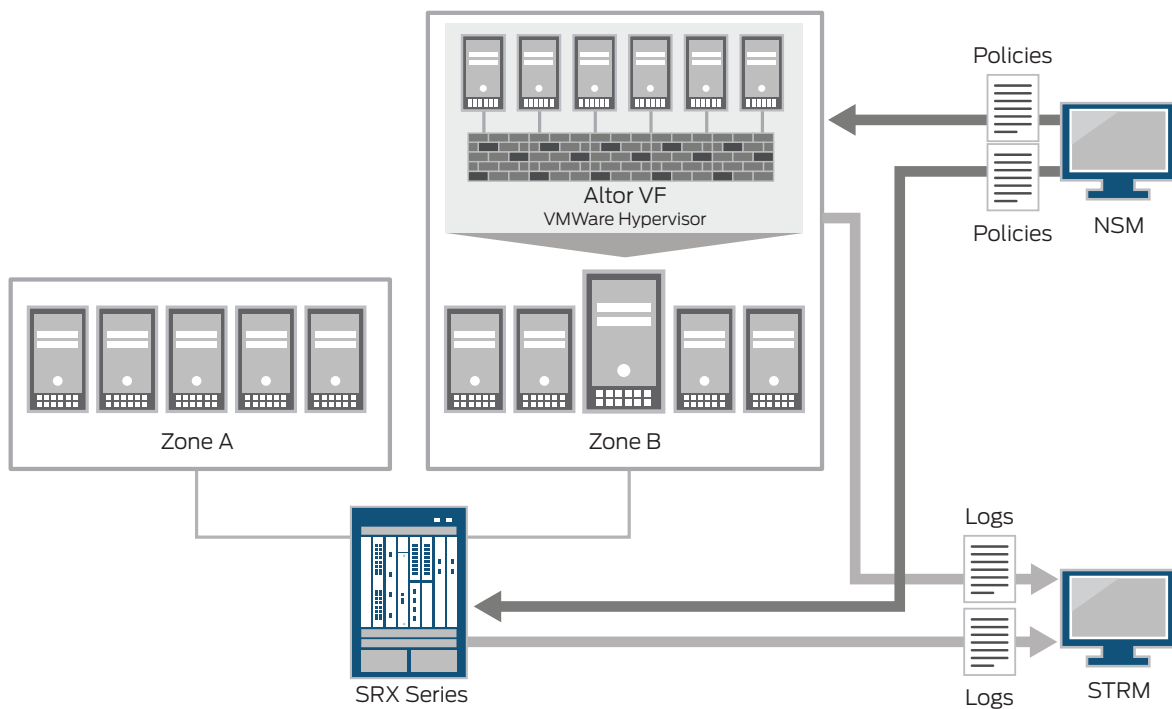


Figure 1. The Altor VF virtual firewall integrates with Juniper Networks NSM and STRM Series for streamlined policy management across the virtual and physical infrastructure.

Solution Components

Juniper-Altor solution components include:

- Altor VF
- Juniper Networks Network and Security Manager
- Juniper Networks SRX Series Services Gateways
- Juniper Networks STRM Series Security Threat Response Managers

Summary—Juniper-Altor Solution Secures Data Center Virtual Server Environments

With the Juniper-Altor solution, enterprises can evolve their data center security architecture to be “cloud ready,” ensuring that security policies are consistently applied to virtual networks and machines as well as to the physical infrastructures that support them. The ability for IT administrators to centrally define policies within Network and Security Manager and correlate event and compliance information through the STRM Series greatly streamlines management of the virtual server security environment. As a result, enterprises can reap the full benefits of server virtualization.

Next Steps

To test drive the Altor VF, please visit www.altornetworks.com or send an email to juniper@altor.com.

About Altor Networks

Altor Networks is a leading innovator and provider of virtual and cloud security. The company's flagship product was the industry's first purpose-built virtual firewall. Now in its third release, the Altor VF includes integrated intrusion detection, VMotion and vCenter support as well as VMware VMsafe API certification. Altor helps data center administrators control and segment access to their virtual machines with the enforcement of customizable and centrally managed security policies.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. 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 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

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

Copyright 2009 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. Junos is a trademark of Juniper Networks, Inc. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.