Altor VF

ALTOR NETWORKS

Key Benefits

- Enables granular control of all virtual network traffic, including inter-VM communication
- Enforces security policy for individual VMs
- Secures VMotion live migrations, with continuous connectivity
- Stops the mixing of VM trust levels (e.g., production, QA)
- Mitigates risk of inter-VM infection
- Prevents new or rogue VMs from opening security holes
- Extends intrusion detection to the virtual network with little extra cost
- Boosts VM troubleshooting effectiveness
- Automated installation and integration with the virtual environment

Enforcing Security Policies in the Virtual Environment

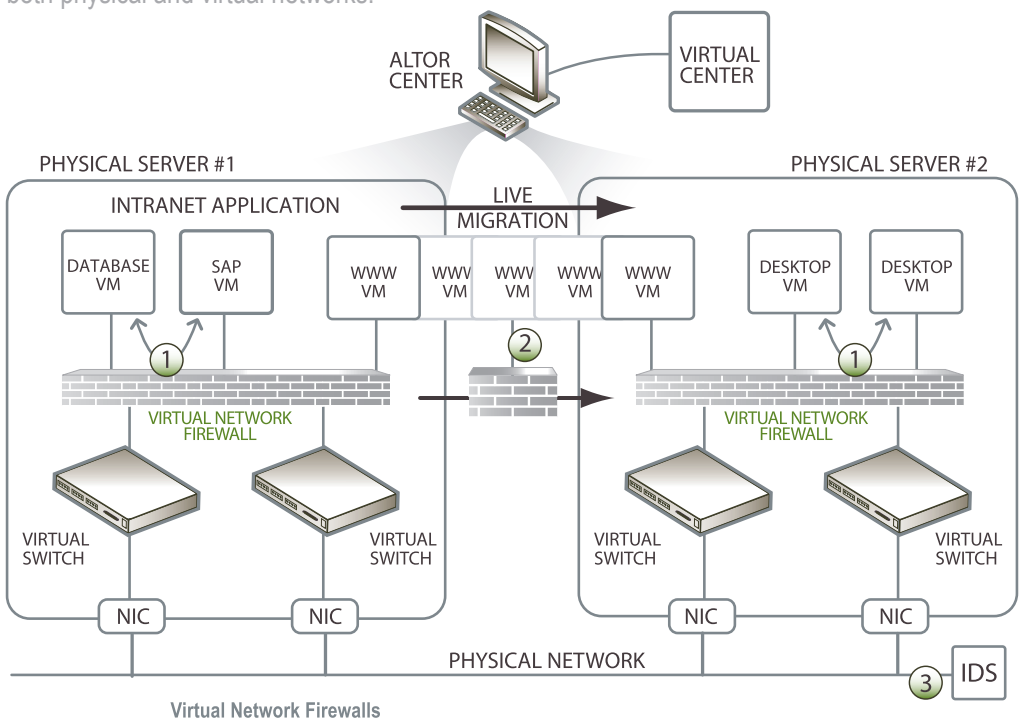
Server and desktop virtualization is revolutionizing the data center, delivering major capacity utilization and productivity improvement. It is also dramatically changing the enterprise network by adding a rapidly growing "virtual network" of virtual machines (VMs) connected to each other and the physical world through virtual switches. Yet even basic security practices - including monitoring network activity, inspecting and filtering traffic, and maintaining strictly separate security domains - are often absent in the virtual environment. Inter-VM communication in particular is a blind spot. This traffic never touches the physical network, making it invisible to physical network monitoring tools and unprotected by physical network security.

The risks of an invisible, uncontrolled network with no enforceable security policies are sobering. Among them is the potential for privilege escalation when VM workloads with different trust levels, such as Production and QA systems, reside on the same physical server. This risk is amplified when the VMs move from host to host via VMotion and DRS.

The Altor Networks Solution

Altor Networks VF is purpose built to meet the unique security challenges of the virtual environment. Administrators can now control the virtual network by enforcing a rule-based policy for each VM. Because Altor VF was designed with virtualization features in mind, it synchronizes automatically with VMware VirtualCenter and secures VMotion.

VF is the only product that solves the problems of blind spots, uncontrollable inter-VM traffic, unprotected migration of VMs, and erroneous mixing of VM trust levels. Enterprises can now achieve the full ROI of virtualization while maintaining security and regulatory compliance across both physical and virtual networks.



Virtual Network Firewalls

1. secure inter-VM communication, stopping infections,
2. secure VMotion by "attaching" an enforceable policy to the migrating VM, and
3. enable virtual network intrusion detection by mirroring traffic to a physical IDS/IPS

Product Details

Enforceable Policy per VM

Admin can enforce stateful firewall policies for individual VMs, logical groups of VMs, or all VMs. Global, group and single VM rules ensure easy creation of policies with tight security, while enabling enterprises to take full advantage of virtualization benefits.

Secure VMotion

Firewall protection is continuous as VMs move from host to host using VMotion. Unlike legacy firewalls, Altor VF keeps the “live” in live migration by maintaining open connections and security throughout the event.

Physical IDS/IPS Integration

Altor VF can send some or all inter-VM traffic out the physical security devices, such as IDS/IPS sensors. By mirroring traffic based on firewall rules, it brings intrusion detection to virtual environments by leveraging existing physical ISC capabilities, with no performance degradation to the virtual environment.

Default Policy for New VMs

When a new VM is created, Altor VF assigns it administrator-defined default policy. Allowing only admin and DNS protocols, for example, mitigates the risks of misconfigured or “rogue” VMs with vulnerable or infected workloads.

Automated Deployment & Integration

The Altor VF appliance automatically installs itself and discovers all guest VMs through integration with VirtualCenter. Unlike VLANs used to isolate VMs, the Altor solution is easy to maintain and readily scales as virtualization use grows and new VMs are added to the environment.

Intuitive Central Management

The web-based central management console displays real-time views of each VM's operating and security status at a glance. A simple, familiar interface for defining rules and managing policies supports role-=based administration, enabling separation of duties.

Logging, Reporting and Alerts

Syslog output gives security event management systems insight into virtual network activity. Admins can print reports of historical VM traffic data and configure SNMP traps to alert them to selected events.

Architected for Multiple Platforms

Altor Networks’ multi-platform architecture is designed to secure all leading virtualization platforms (i.e., Microsoft Hyper-V, Xen) and support their newest technologies, such as VMsafe from VMware. Enterprises retain the freedom to choose whatever virtualization technologies meet their needs, today and in the future.

System Requirements

Altor Agent

Operating System	Altor Virtual Appliance
Memory	512MB
Disk Space	1GB
Virtual Infrastructure	VMware Infrastructure 3
	VMware ESX Server 3.x.x

Altor Center

Operating System	Altor Virtual Appliance
Memory	512MB
Disk Space	10GB (2GB OS + 8GB Database)
Virtual Infrastructure	VMware Infrastructure 3
	VMware ESX Server 3.x.x
	VirtualCenter 2.x.x

Contact

Altor Networks, Inc.
350 Bridge Parkway, Suite 6
Redwood City, CA 94065

Altornetworks.com

© 2008, Altor Networks, Inc. All rights reserved. Virtual Network Security Analyzer is a trademark of Altor Networks, Inc. All other company, brand and product names may be trademarks or registered trademarks of their respective holders.

ALTOR
NETWORKS