Virtual Networks aren't Visible Networks

Virtualization technologies from leading industry vendors like VMware, Microsoft, Citrix, Oracle, Sun, and RedHat are enabling enterprises to consolidate applications on separate physical servers into one physical server as virtual machines (VMs). While the benefits – including maximizing hardware utilization, reducing costs and fast backup and disaster recovery – are apparent and appreciated, enterprises are losing visibility and control into the "last mile" of the network.

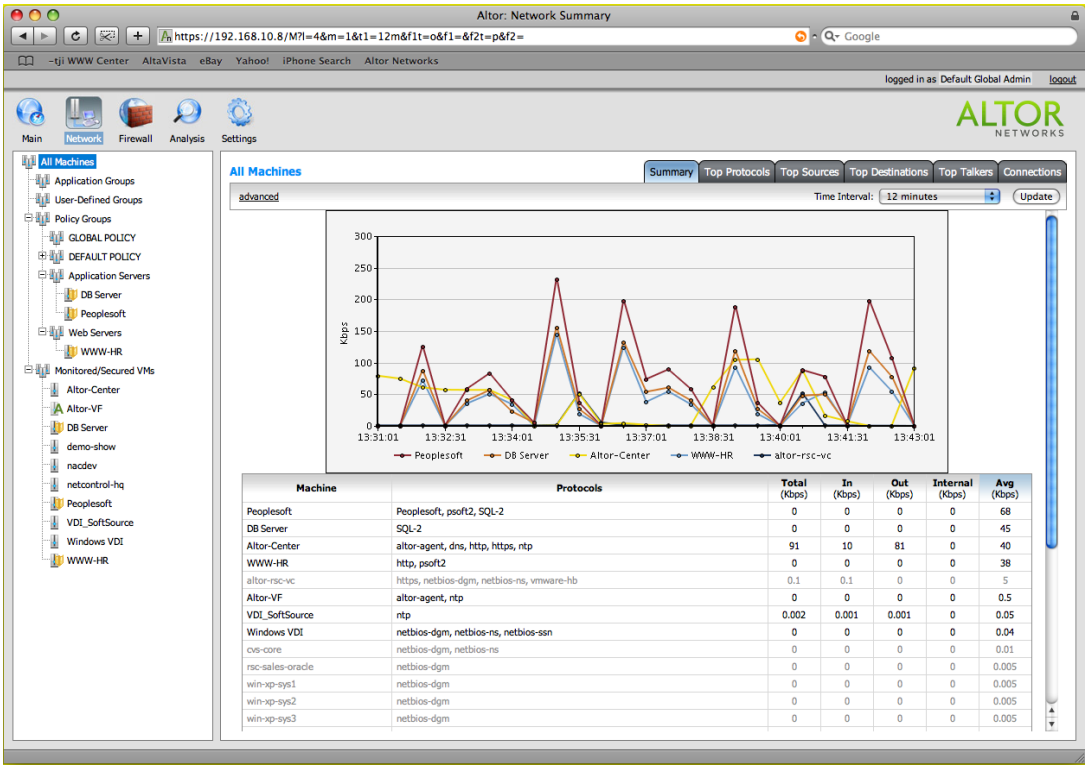
VMs are connected to each other and rest of the world via virtual switches embedded in the virtualization platforms like VMware ESX Server and Microsoft Hyper-V. Inter-VM communication on this "virtual network" in particular is a blind spot since it never touches the physical network. The risks of an invisible, uncontrolled network are wide ranging – from undetected malware outbreak to difficulty identifying network and resource bottlenecks.

Enterprises need visibility into the activity of users, applications, and systems of both their physical and virtual networks to ensure security and operational efficiency.

Mazu Networks and Altor Networks add Security and Visibility to Virtual Networks

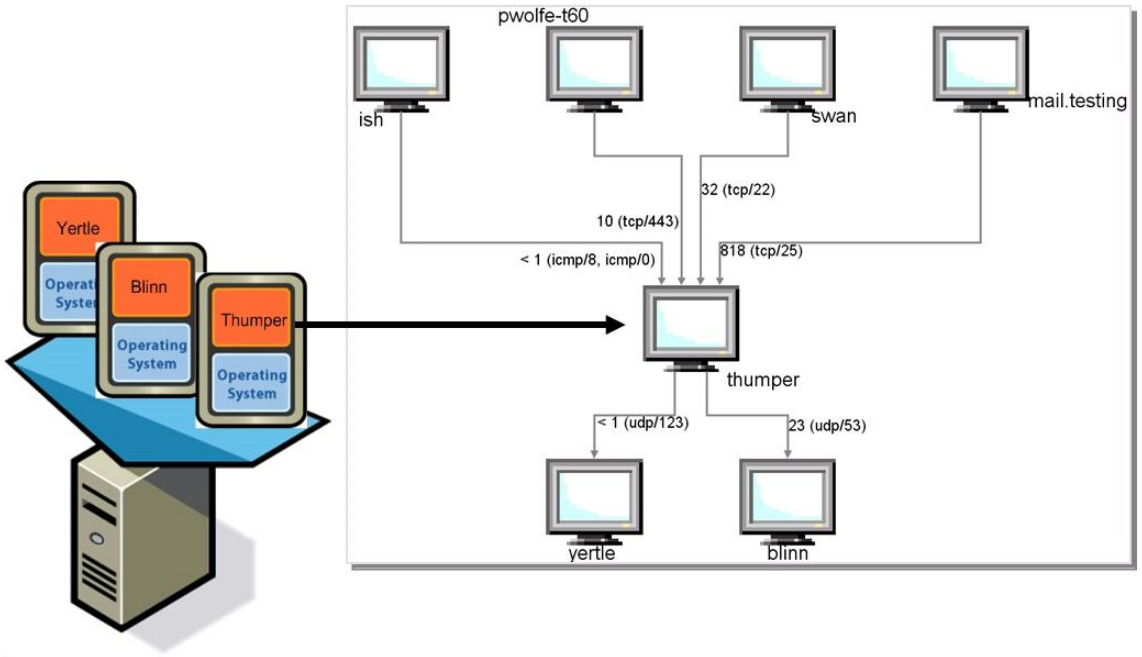
Mazu Networks and Altor Networks have partnered to deliver a solution that provides comprehensive visibility of the entire enterprise, including the virtualized data center. The combined solution integrates Altor VF virtual appliance for VMware ESX and Mazu Profiler.

Altor VF is a software security appliance that runs in a virtualized environment and enforces security policy on a per-virtual-machine (VM) basis. Unlike existing firewalls designed for physical networks, the Altor VF virtual firewall can secure Live Migration, a technology designed to trigger automatic movement of VMs across physical servers but capable of inadvertently moving an application to a less trusted network. The Altor VF was purpose-built for the virtual environment enabling tighter security policy and greater ease of use than existing virtual firewalls adapted from their physical firewall counterparts.



Altor VF monitors and controls all the traffic that traverses the virtual switch. It exports detailed connection statistics via NetFlow even when the VM migrates between physical servers.

Mazu Profiler provides a new way of managing application performance and security by analyzing the interactions of users with the applications, systems, and network devices that comprise the application delivery infrastructure. Mazu Profiler delivers the critical data customers need to quickly resolve problems that affect service — such as unauthorized usage, availability and performance issues, and security threats — as well as to inform consolidation, virtualization and optimization initiatives. Mazu Profiler collects network flow data and enhances it with application and user identification, behavioral analytics, and network performance metrics. Because you can create groupings based on logical business categories, Mazu Profiler presents a complex infrastructure in a business context. Pre-defined and customizable behavioral analytics enable users to identify performance, availability, and security issues before they disrupt business services. Complete and accurate usage and dependency data provide the key inputs for making the right optimization and change management decisions. Mazu Profiler also provides an extensive set of integrations, which enable it to interoperate intelligently with other systems to increase their value and improve your workflow. Mazu Profiler's passive, agent-less deployment allows fast implementation.



Mazu Profiler can map dependencies within the virtualized environment using the VM-to-VM communication data provided from Altor. In this example, you can see that Thumper depends on guest systems Yertle and Blinn to serve it's clients ish, pwolfe-t60, swan, and mail.testing.

A Comprehensive Approach for Visibility

As companies move to virtualization, they give up the security and visibility of traditional networks that is provided by solutions like Mazu Profiler because the network access layer disappears into the virtual server. By providing NetFlow statistics from within the virtual servers, the Altor VF returns to the Mazu Profiler the ability to analyze the network for application performance and security. Together, the two solutions enable customers to secure and manage their virtualized environments in the way they are accustomed to securing and managing their physical servers. With this powerful integration, you get:

- **Consistent NetFlow analysis –** The solution delivers consistent and accurate information, even as VMs migrate across the data center
- **Visibility into the virtual network –** The solution provides the visibility you need to ensure end-to-end application performance and security
- **Fast deployment –** Mazu Profiler and Altor VF have been integrated to make configuration quick and easy

About Mazu Networks

Mazu Networks offers solutions that enable IT organizations to manage, secure, and optimize the availability and performance of business services. Based on Network Behavior Analysis (NBA), Mazu Profiler provides a new way of looking at the IT infrastructure by analyzing network traffic to provide valuable information about the interactions of and dependencies between users, applications, and systems. This enables enterprise IT organizations to ensure optimal performance and availability, enhanced protection and support for regulatory compliance, and informed decision making for IT initiatives. Only Mazu Profiler offers behavioral analytics, user identification and application fingerprinting, role-based presentation using common data, and intelligent operation with other systems in the infrastructure. With Mazu Profiler, hundreds of customers are able to ensure the availability, performance, and security of business services as well as to reduce costs and satisfy regulatory requirements. For more information, please visit www.mazunetworks.com.

About Altor Networks

Altor Networks is pioneering a new class of virtual security solutions to secure production-oriented virtualized data centers. The company's initial product line includes the industry's first-ever purpose-built virtual firewall, a software security appliance that runs in a virtualized environment and enforces security policy on a per virtual machine basis. Data center administrators can now pinpoint a broad range of virtual network security compromises and easily create roles-based security policies. For the first time, security policies can be continuously enforced on individual virtual machines, even as they move throughout the virtualized data center. Founded by security and networking experts from Check Point Software, Cisco and Oracle, Altor Networks is funded by Accel Partners and Foundation Capital and is headquartered in Redwood City, California. For more information, visit www.altornetworks.com.