SYRACUSE UNIVERSITY

Summary

Company: Syracuse University

Industry: Education

Challenge: Applying highly granular access controls per virtual machine in order to isolate resources by unit or college

Solutions:

- Juniper Networks Firefly Host*
- Security Design for Firefly Host

Results:

- Access control that is enforced by application, protocol, VM, VM group, and global level
- VMware VMsafe certification
- Implementation that has fault tolerance and high availability
- Compliance with access control enforcement and malware suppression in a highly dynamic mixed-VM-use environment

Founded in 1870 as a private coeducational institution offering programs in the physical sciences and modern languages, Syracuse University (www.syr.edu) now spans 13 academic units and 25 centers and institutes. The university's 16,000-plus undergraduate and graduate students have access to a broad array of networked computing services, including 30 labs, more than 1000 PCs, specialized software, and more than 200 classrooms equipped with the latest multimedia technologies. And campus-wide e-services facilitate the ordering of books, meals, courseware, and communication. Located in the geographic center of New York State, and with a rich history of academic excellence and innovation, Syracuse University (SU) is a destination spot for technology conferences and seminars jointly conducted with academic and corporate partners.

Challenge

SU's information network is as dynamic and sophisticated as any in the U.S. The Information Technology and Services (ITS) department has as part of its charter ensuring that all of the academic units, colleges, and institutes—known collectively as "the units"—have the resources they need to undertake projects and provide the highly specialized training that each of them administers. This is accomplished through various groups, which include core infrastructure and security. This means that in addition to the centralized, campus-wide services—such as email, retail, food, Blackboard, survey, and other enterprise applications—each of the units might require customized servers and databases for file sharing, software license administration, Web micro sites, and high-performance applications. The needs of each of the schools, colleges, and administrative units can vary greatly depending on the discipline as well as the student population density for that semester. The challenge is to provide each unit with the resources that it needs as it requires them, allowing for sufficient autonomy over the administration of those servers and applications while at the same time ensuring that the enforcement of resource segmentation and security policies is centralized and consistent. Furthermore, the entire process has to be cost effective relative to the administrative burden that campus-wide needs place on ITS.

Selection Criteria

To address the challenges of on-demand and cost-network scalability, SU turned to virtualization of its entire infrastructure for the campus-wide services as well as the "per-unit" computing resources. By opting for a virtualized server pool to service all of the academic units, SU ITS has essentially built a private cloud whose successful implementation is predicated on adequate inter-unit segmentation and access control. At first, SU ITS staff tried to accomplish this by using legacy physical firewalls. However, upon learning about VMware VMsafe API, the team switched its priority to having purpose-built certified security in the hypervisor for its virtual network security plan.

Solution

SU ITS staff chose the Juniper Networks® Firefly Host* with integrated intrusion detection service (IDS) capabilities as well as the Juniper Networks center for centralized management and the optional reporting module.

> "Juniper Networks lets us build a bubble around the VMs of each one of the units or colleges. This is a whole new and more efficient way of securing our virtualized environment. We don't have to design around the limitations of our physical firewalls."
>
> Joshua B. Slade, IT analyst,
> Syracuse University, Core Infrastructure Services

Academic Unit Segmentation

To enable academic units to provision new VMs as they need them, the SU ITS expert staff realized that security and access control would have to be provisioned at the VM level as opposed to the subnet level. In this way, the applications and traffic of each of the schools and colleges could be isolated from one another. This would enable resource provisioning and performance that is commensurate with the need of the unit while reducing the risks from cross-pollinating traffic. Attempts to do this using physical network firewalls and VLAN isolation resulted in a rigid and somewhat complex network architecture that was "messy" to manage. The requirement was for granular access control that could be applied by school or college as well as by application and virtual machine, creating essentially a "security bubble" around the virtualized resources of each unit. Juniper Networks gave SU exactly that solution and the means to manage those access policies in a centralized way that is highly coordinated with the virtualized network's management system or VMware vCenter. Because Juniper's management system is in constant communication with vCenter, new VMs are quickly detected and security policy is immediately applied to them. This gives the units autonomy in provisioning compute power, but retains the centralized control that SU ITS needs to maintain a good security posture for all VMs on campus.

High Availability

Academic environments are very deadline driven, so network availability is key to keeping students, faculty, and research moving according to schedule and plan. This means that all parts of the SU network must be highly fault tolerant, including the virtualized network serving the specific needs of the units. When evaluating virtual network and cloud security solutions, SU ITS staff understood that highly available virtualized access control and policy administration were capabilities uniquely offered by Juniper Networks. This highlighted Juniper as a leading provider of enterprise-grade virtual security and made the selection of the Juniper solution a likely ultimate choice for securing SU's private cloud.

VMware VMsafe API Certification

SU ITS staff had been aware of trends in virtualization security for quite some time and had been monitoring virtualization operating system and security vendor progress in this area. The availability of the VMsafe API and certification program from VMware in late summer of 2009 signaled the right time for SU to transition from legacy to purpose-built security for the virtualized network. VMware VMsafe certification gives SU the assurance that Juniper's security solution has been certified under rigorous testing to be seamlessly operational in the hypervisor. It further gives Juniper the ability to deliver sophisticated protection that extends to VMs in motion (that is, live migration) as well as to the hypervisor itself. Further, it makes Juniper Networks the singular option for an extremely fast-performing access control solution for the virtual network.

Interoperability with Juniper Security Solutions

A key requirement for SU ITS was the ability to apply security policies consistently across both physical and virtual networks. SU's information technology specialists also had a need to collect and aggregate information about access activity across the two types of devices. With Juniper Networks it's easy for customers to incorporate virtual servers seamlessly into their security architecture because virtual firewall technology is part of a comprehensive security portfolio—including Network and Security Manager, a unified security policy manager, and Juniper Networks STRM Series Security Threat Response Managers—giving end users of those technologies the visibility into and granular control over VM traffic. Combining Juniper's virtual firewall technology with its portfolio of industry-leading security products enables secure virtual server environments and optimization of the benefits of server virtualization.

Malware Suppression—Integrated IDS

Academic environments can be hotbeds for malware introduction and propagation. For this reason, it was important to provision the virtualization security regimen with capabilities for detecting and alerting on the presence of this type of unwanted traffic in the virtualized server environment. The Juniper Networks virtualization security solution includes IDS functionality as well as signature updating capabilities and mitigation guidance as part of its core offering. Further, for those organizations that have standardized on IDS technology from a third party, Juniper offers support and integration with those solutions as well.

For More Information

To find out more about Juniper Networks products and solutions, please visit **www.juniper.net**.

*Formerly vGW Virtual Gateway

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.

3520391-002-EN Feb 2011

Printed on recycled paper