

# AFFILIATED COMPUTER SERVICES (ACS), A XEROX COMPANY

## Summary

**Company:** Affiliated Computer Services (ACS), A Xerox Company

**Industry:** Cloud Services Provider

**Challenges:** Creating a secure, multi-tenant virtual environment while limiting the number of VLANs required

**Selection Criteria:** Juniper Networks vGW met ACS' must-have requirements for a cloud security vendor: VMsafe-certified, ease of installation, ease of security policy configuration, logging and reporting comprehensiveness, and the availability of integrated virtual intrusion detection (IDS).

**Solution:**

- Juniper Networks vGW Virtual Gateway, Security Design for vGW

**Results:**

- Gained complete visibility into all VM traffic in a multi-tenant environment, including network utilization reporting and virtual IDS
- Diminished VM administration complexity with automated policies
- Gained ability to offer customer significant savings in time and money
- Alleviated concerns of customers regarding security in a multi-tenant virtualized environment

Affiliated Computer Services (ACS) is part of Xerox's \$22 billion global enterprise with 130,000 employees, serving clients in 160 countries. ACS brings innovative offerings to clients in the communications, education, financial services, government, healthcare, manufacturing, retail, and travel and transportation sectors.

New to the company's portfolio of services is the ACS Enterprise Cloud. This Infrastructure as a Service (IaaS) offering enables enterprises to access cloud capabilities through an on-demand model to support the rapid deployment of standardized business applications. In addition to providing flexibility, the ACS Enterprise Cloud promises to meet the enterprise-class security, reliability, and compliance requirements of its clients.

## Challenge

ACS customers include brand-name companies across diverse industries—including manufacturing, healthcare, financial services, retail, entertainment, and more. While the types of workloads from these clients span the gamut in terms of criticality, all workloads must still receive the resources they need to meet availability and performance required. Moreover, clients need sufficient autonomy over the administration of virtualized machines (VMs) and applications, as well as centralized and consistent enforcement of resource segmentation and security policies. "ACS clearly understood that the key barrier for enterprises to adopt cloud services is security all the way down to the VM level," says Nagesh Kunamneni, VP and CTO for ACS, A Xerox Company. "We committed ourselves to providing the highest levels of security in our Enterprise Cloud Services."

As a senior architect for the ACS Cloud Services team, Jason Bain had to determine how best to equip the ACS private cloud infrastructure for granular customer resource isolation, protection, and continuous monitoring. Bain handles the underlying network connectivity between ACS clients and the Internet; the dedicated client environments across the WAN; and the overall security of the environment. In this customer-facing role, he is heavily involved from a technical and relationship-building perspective to answer questions and guide clients through the process of transitioning to the multi-tenant private cloud.

"We knew we had to have a secure offering that included proper isolation of customers' virtual machines and was simple to use," says Bain. "We had to focus on ways to offer virtual security in a way that was both granular and scalable at the same time, so we looked for guidance within the VMware VMsafe program and found our way to Juniper Networks."



## Selection Criteria

The choice to go with Juniper Networks® vGW Virtual Gateway for hypervisor-based virtual firewall security evolved as ACS defined its must-have requirements of a cloud security vendor. ACS was looking for a solution that was certified to the VMsafe API. Of equal importance, though, were the ease of installation, ease of security policy configuration, logging and reporting comprehensiveness, and the availability of integrated virtual intrusion detection service (IDS). Says Bain, “Not only was I sold on Juniper Networks vGW due to the ease of installation of the product—it was so simple to download and activate—but the way vGW defines policy just made sense to me. There’s a quick and easy way to see from the global level down to VM groups and then down to individual VMs. While evaluating competing products to vGW, we not only found buggy installation and stability issues, but also quite cumbersome policy creation.”

**“Security and trust are key to adoption of cloud services by enterprises. With Juniper Networks as a base component of ‘enterprise cloud’ reference architecture, ACS delivers isolation of virtual machines, providing differentiated security and trust to enterprises.”**

Nagesh Kunamneni, vice president and CTO, IT Outsourcing, ACS, A Xerox Company

## Solution

ACS selected the Juniper Networks vGW Virtual Gateway, VM introspection, security automation, and compliance assessment; as well as Security Design for vGW for centralized management and reporting.

### The ACS Private Cloud Architecture

ACS has decided to base its private cloud on virtualization technology from VMware and storage/system management from EMC, while giving its clients the additional benefits and protections of the Juniper Networks vGW Virtual Gateway security component for per-VM visibility, security, and isolation.

In addition to simplified client access to services and increasing flexibility in IT consumption, ACS solutions deliver enhanced cloud security in the forms of SIEM, IDS, privileged user management, physical VLAN segregation, and, now, VM isolation using Juniper Networks vGW.

“Cloud services providers like ACS are leading the industry by putting in place reference architectures for secure IaaS offerings. ACS customers are not only getting VMs that are assured to be appropriately configured, isolated, and protected, they are also able to self-provision additional resources without fear of mis-configuration. Juniper Networks and ACS have automated continuous VM security to ensure safe computing in the ACS cloud,” says Bain.

Currently, ACS Enterprise Cloud has three cloud operational nodes—in Dallas, Texas; Pittsburgh, Pennsylvania; and Kuala Lumpur, Malaysia—that are connected over high-speed networks to provide resilient services and that have grown to run more than 1,000 VMs in production in less than a year’s time. ACS’ growth strategy includes plans for another U.S.-based node in 2012, as well as further expansion into the Pacific Northwest, Europe, and Asia.

“Initially, we’re targeting areas of the country where our current clients have their data centers. Our aim is to allow clients to transition all the enterprise IT services into cloud services in a seamless way,” says Bain. “Things happen much more quickly in the cloud. Customers can spin VMs up and down at their leisure, as well as buy monthly versus yearly contracts.”

### Multi-Tenant Security

Today, ACS has a hybrid model of physical firewalls and the hypervisor-based Juniper Networks virtual firewalls to give the company—and its clients—complete security in a multi-tenant environment. Part of Bain’s job is to build the backend connectivity into the cloud node so as to make it an extension of current client networks. Clients might virtualize portions of their data centers at their premises and also use the ACS Enterprise Cloud for some of their workloads. ACS ensures that customers have a seamless communications path between their premised virtualized resources and their ACS-hosted ones. In this way, they have the utmost flexibility to take advantage of the ACS Enterprise Cloud offerings based on demand.

“Security for our various clients runs the gamut. Some clients leave the choices entirely up to us, while others are very specific,” says Bain. “Generally, ACS has created a baseline of the ports that are allowed outbound and inbound. Nothing is allowed inbound until it is requested. For example, they [clients] can request a new public IP to host a website through our portal. We’ll enable that and work with our clients to identify the exact ports that need to be open. We’re using vGW to enable tiered applications in the client’s dedicated VLAN. A client can run Web, application, and database servers all in a single VLAN since all packets flowing through the hypervisor and VMsafe API are inspected by vGW. This enables us to build ‘virtual DMZs’ or trust zones per client, whereby we only allow the ports between zones that are required and documented for application functionality. Once the zones and rules are created, a client can provision new VMs directly into those zones via our automated provisioning platform.”

"In designing the model, one of the issues we had to address was VLAN sprawl. Consider this example. If 30 clients require three virtualized environments each (for example, production, DMZ, and QA), then using VLANs to provide the isolation would mean 30 times 3 or 90 VLANs to manage," Bain continues. "With Juniper's solutions, we're able to give each customer a VLAN and guarantee highly granular isolation of their environments within the VM host. That means 30 rather than 90 VLANs to maintain. In fact, we can use Juniper Networks firewalling to isolate customers from one another, so eventually, we'd like to remove the physical firewalls—except at the network boundaries—and strictly rely on the Juniper Networks hypervisor firewall solution for client-to-client security."

### VM Availability Gets a Boost

Currently, ACS offers its clients SLAs that have three nines to four nines (99.9% and 99.99%) of availability per individual VM workload. Juniper Networks software helps ACS meet its VM availability assurance levels by providing visibility into all VM traffic and enabling ACS to track VMs as they are created, migrated, cloned, or decommissioned. vGW maintains detailed information about each VM it monitors—including applications and services, OS version, patch levels, protocols, bandwidth use, memory consumption, and more. ACS uses the information to create policies, which maintain the optimal security state of the VM and ensure that it is accepting and forwarding traffic in a business-warranted way.

### Automated Security for Virtual Workloads

Since launching the ACS Enterprise Cloud, Bain has seen some interesting and unexpected requests.

"Going into our pilot phase, we expected that many client workloads would be used mainly for testing and development purposes, but we've been very pleasantly surprised," says Bain. "For instance, we have one large client of business processing outsourcing services—kind of a service provider within a service provider model—who is putting all production workloads into our cloud. Their business is medical claims processing and they have Internet-facing applications. They need to connect to medical claims providers throughout the country and rely on the ease of use and security we provide."

The ACS Enterprise Cloud Services team has been particularly excited about vGW Smart Groups and Auto Secure—so much so that these security automation features are now part of ACS' baseline offering. ACS does this based on VMware port groups. As an example, ACS can assign a client three port groups (e.g., ClientXWeb, ClientXApp, and ClientXDB). These port groups map to Smart Groups such that any new VM spun up on them is automatically assigned to the proper security zone and inherits the security policy defined by that zone. Essentially, Smart Groups diminish VM administration complexity, as well as VM sprawl.

"We initially thought that it would be a major effort to secure every single VM so we would use customer feedback to do this on an as-required basis. But now, with vGW, I see that changing," says Bain. "Now we can secure the templates. So every time we spin up a VM, we don't have to manually work with the client to secure it—after the fact. Instead, vGW will automatically apply the policy the customer wants."

Going forward, ACS plans to automate vGW Smart Groups into its cloud services portal so clients/operational support groups can self-serve, for instance, "New Web DMZ VM" on a drop-down list and have that VM automatically flow through and into the correct security zone. And if for some reason a customer accidentally brings up a VM with a "bad" security posture, it is automatically quarantined and an alert is generated to the clients/support groups and to ACS to take care of the issue.

"The best part is that there is no coding necessary to define these policies," adds Bain. "It's simply a matter of pointing to the condition you want and clicking to select and enforce it."

### Virtualization and Security Group Collaboration Enablement

ACS recognized that the effort to build its private cloud would be multi-disciplinary both at implementation and for ongoing management and scale. This is particularly true for the VM administration and security groups, who must constantly coordinate their efforts so that security does not impede business flow, but rather enables it. Collaboration is also critical for cloud services providers who must also consult with clients when it comes to security policy definition and reporting.

"Juniper software brokers the communication between networking, VM administration, and security, enabling our cross-functional cloud services team to be highly productive," says Kunamneni. "Leveraging the single view into the cloud, each individual can contribute his unique skill sets to optimize the VM connectivity, security, and maintenance. This kind of collaboration helps us deliver the most secure multi-tenant private-cloud environment possible to our customers."

### Results

For ACS, Juniper Networks vGW is key to selling multi-tier enterprise application support. ACS clients appreciate the ability to maintain the three-tiered security architecture that's required by enterprise applications to minimize any risk from public- and non-public-facing workloads that co-exist in the same VLAN and cloud.

Moreover, thanks to the enhanced visibility that vGW provides, the ACS Cloud Services team is saving countless hours assisting application owners and server admins with troubleshooting application traffic flows. And the vGW compliance reporting functionality has enabled the team to guarantee the integrity of client VMs, as well as mitigate the risk of rogue VMs or malicious behavior within the virtual network.

## Next Steps and Lessons Learned

According to Bain, Juniper Networks vGW has more than proven its worth and ACS is confidently selling the solution to its enterprise clients running either their own private clouds or traditional VMware environments. Upcoming plans for the company include further automation of client onboarding via the API, as well as self-service firewall administration through the ACS cloud portal in lieu of the current managed service method support.

## For More Information

To find out more about Juniper Networks products and solutions, visit [www.juniper.net](http://www.juniper.net).

## 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](http://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](http://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 2011 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. 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.