OARtech Minutes
10/12/11

Introductions

OARnet Network and Technology Updates, Paul Schopis
OMMC - They are working on an agreement with Comnet for services to SOCC. Horizon is working on fiber builds and OneCommunity hosted a workshop for (NTIA). They have also been talking with WVnet about resources.

Consolidated Network Architecture - OH-Tech has been announced by Chancellor Petro and is a consortium of the various Ohio technology service group. All technology services are to be housed at Oarnet. The last group (OhioLink) came in yesterday.
Optical mesh architecture implementation is a full mesh lambda capability to replace the ring architecture. Ring 0,1,4 complete, the next ring they are working on is 2. They are working on another 10G pipe in the Columbus area to all load balance due to changes in contracts and they are continuing to work on peering strategy. MERIT and Oarnet will be working together with Oarnet becoming an I2 connector again.

Shared Infrastructure: They are working on the community cloud service and are developing the different service models. The BOR-CIO committee has asked OARnet to bring up a Virtual Computer Lab (VCL) and the pilot is underway. They have instrumented the stacks in a way to allow objective measurements and they are using both the VCL Open Source and the VMware option. Currently still a pilot and hoping to make it an option shortly.

Are you working with campuses that are already using the VCL concepts? They are hoping that the pilot will help leverage software, licensing, etc... as campuses need it. Oarnet is very interested in how individual campuses feel about their VCL implementations. There are expectation, performance, and licensing issues.

Federated identity - They are trying to get a Federated service in Ohio called "I AM OHIO" and have 5 schools in the pilot. Fischer International is the service provider and they have a lot of background in federated identity. They are working through the integration and working to integrate with schools that already have federated identity and help those that haven't yet. It is shibboleth based, but it is somewhat of a moving target. An immerging standard is using a proxy server to do the exchange. Some shibboleth sites are doing this on the back end.

Client Services, Ann Zimmerman
Tony Capocciama is new client services manager for TJ Sandor's old area. Her contact information istcapocciama@oar.net, 614-292-8592. They are now using ServiceNow for their ticketing system. It is working very well. She showed some summary statistics for the network to show the growth.

They are doing shared gig services with Time Warner, AT&T, and Time Warner Cable. Several campuses have moved to this type of connection. Planned 10G campuses include OU, Kent State, CSCC, Wright State and Bowling Green. They are working on several school collaborations. Several schools are also looking moving to Elan services.

The VMware Renewal Contract has been signed and Oarnet will be adding all the products. Currently the pricing will remain the same with a 2 year contract and a 2 year option. State agencies are using about 50% of the contract with HE and k12 using the other 50%.

I2 initiatives - a new member structure has been suggested and Ohio has volunteered to be a pilot state for the new program. Oarnet has a 10G connection to I2. They are collaborating with WVnet and expect WVnet to become an I2 connector. Member and SEGP rates will remain the same for FY 2012. Bowling Green and Cleveland State have resigned as full I2 members.

Events
VMware workshops - Oct 25th Columbus at Platform Labs.
Miami Valley I2 Consortium Meeting - Oct 26th from 1-3
OARtech Dec 14th at Lakeland
Thanks to Stark State for hosting this meeting. Anyone interesting in hosting in the future let Ann know.

Securing the Virtualized Data Center
Dave Lipowsky, Juniper Networks, Cloud Security Team
dlipowsky@juniper.net

How are you securing your VCL environment? One school is working on issues with anti-virus; they rely on the ASA to protect the switch environment. They tried the Cisco 1000V switch, but found it hard to implement. So they moved away from the virtual switch. Another school is using deep packet inspection.

Gartner says that 60% of virtual servers will be less secure than the physical servers they replace and this would be the case until 2015.

Virtualization Requirements
Secure VMotion/Live-Migration (migration from more secure to less secure hosts), Hypervisor Protection, Regulatory Compliance (you have a mixed compliance scope in the same environment), different customers and the sharing of roles on the same host.

It used to be that you separated by firewalls between zones. But with virtual systems they don't work that way. You have to use virtual switches for VM isolation.

What about IPtables, and puppets? He doesn't see that a lot, but you can use traditional security agents on each vm. It can become a scaling issue.

Approaches:
1. VLANS and physical segmentation; 2. Traditional Security Agents; 3. Purpose Built Virtual Security

The tradeoff between each approach is performance. Number 1 has IOPS cost, 2 uses kernel cycles with a higher cost, and 3 uses the virtual security layer in the hypervisor. Juniper says that #3 has the best performance. It uses the VGW Hypervisor with implementation in the kernel. It allows per-VM policies.

VCenter integration

You see changes to the VM inventory right away and it really doesn't care about association with an IP but cares more about the association with a UUID. A change to the IP doesn't change the security policy. It allows easier changing of nics and working with new VMs.

One school commented that given this integration, you run your vm environment flat. The silos start breaking down.

It is an object oriented policy, but instead of IP it uses UUID vs networks with port information. This would allow you to run your machines with the security in the hypervisor instead of on the vm. PCI compliance now recommends firewalls at the hypervisor level.

The vGW engine can continue to run the security policy even when the control vm is down. You just can't update the policy. Traffic does not actually run through the VM system. For IDS policy the packets are mirrored within the vGW engine. This is all vSphere 4 related info. Performance hit is only 6% from unsecured to secured. You get a much higher hit if you have to run the traffic through the VM. The diagram showed a single ESX host. In the case of a cluster, with Vmotion, in the event of the VM moving to another host, they move the security policy from the vGW engine first then the other pieces. This way you never have a period when the security policy is not working. This scales with large number of virtual machines.

It uses the VMsafe APIs. You can have a default securing policy in place for new VMs. Because it works in the kernel if the control VM is shutdown, it can still vMotion. Assumes that VMs are separate security policies, they do not leak between VM.

VMW Modules - Main (dashboard), Firewall (policy management and logs), Network (traffic flows), IDS, AntiVirus, Introspection (see what is inside the VM), Compliance, Reports. The only ones that require additional cost is the IDS and AntiVirus, the others come in the base license.

Network Visibility - you lose this when you go to a Virtual environment and you may have a need for statistics from within the environment. You can drill down to the VMs for top talkers, connections, and ported to a netflow collector. It uses a browser interface. They don't push the policy through the vcenter. The policy is pushed through their VM. They will push some of the introspection stuff through vcenter.

Firewall - It can setup a global environment (e.g. default policies) as well as grouping machines (dynamic and static) as well as individual virtual machines. You can get down to a vNic on a virtual machine. Default policies can be applied to a new virtual machine no matter the IP you give it since it is using the UUID. There is a quarantine policy that can be applied.

Are there APIs that you can use for dynamic policy changes? Yes. (e.g. a web form that builds the machines and applies a security policy based on the type.)

IDS - It sends selectable traffic flows to internal IDS for deep packet inspection, but recommends that you send the information to external storage.

Antivirus - It can occur on a schedule without requiring endpoint software. Allows reclamation of space and can do on-access scanning. It can do the scanning at a central point and can inspect the network traffic as well.

How does it work if it finds an infection? You can quarantine the machine, or just the file depending on the infection. The file just goes away (in windows to file not found). In the case of network traffic the connection is reset. They are not doing DLP (checking for SSN, identity info, etc) at this point. They are looking to do application intelligence in the future. They leverage Sophos for their signatures. They don't do memory scanning on the VMs.

Introspection - Is an agent-less ability to scan windows and Linux to discover the fixes and installed states. They take a micro-snapshot and then review the snapshot. They can compare a virtual machine from a standard image or template. It can look at what has been installed on the virtual machine. They can leverage dynamic groups by what the virtual system has installed and turned on (smart groups).

Compliance - It looks for versions information and other needs for compliance.

Integration - The SRX has the ability to port in the groups and zones between the SRX series and VM awareness. It is a start for a centralized framework. They are working toward a central policy management for a Juniper network environment.

Contact information for questions:
Dave Lipowsky, dlipowsky@juniper.net

Meeting adjourned at 12:13pm.

--
Teresa Beamer
Networks and Systems Administrator
Information Technology Services
Denison University