Security

Security

Private VLANs

Our network is configured for 802.1q tagging, which creates separate logical networks for each client.

When a bare metal AppNexus server is imaged, it runs a vanilla Linux environment. On top of this, we run a hypervisor application (currently Xen) which allows virtual machines to run on the box. All file, memory, and network requests run through the hypervisor before accessing the physical hardware. This allows us to enforce security rules on the underlying virtual machines. When an instance is launched on a physical server, all network traffic from that instance is forced to run through the appropriate VLAN. The instance itself simply sees a normal Ethernet interface.

Firewalls

Instances sharing a VLAN can communicate openly with each other. Each customer's VLAN is completely blocked off from both the outside world and other customer VLANs. Customers who wish to work together within the cloud must set firewall/ACL rules explicitly allowing traffic. Although AppNexus recommends that external traffic is routed through an F5 load-balancing pool for improved DDOS and Flood protection, customers may open up specific ports and IP addresses on the firewall.

Dedicated Servers

Each server in the AppNexus environment is dedicated to a single customer. This further isolates customer data from potential security holes in the underlying virtualization layer, and guarantees that there will be no contention for CPU, disk, and memory. Access to the host operating system is severely restricted to a limited number of trusted users. All access is logged and monitored, and access outside of specified maintenance windows triggers security alerts.

Secure Datacenters

AppNexus colocation facilities must have top-tier physical security, including 24/7 guards, security cameras, and biometric authentication. Only AppNexus personnel and vendors have access to our physical cages. For an example of physical security at one of our facilities, see http://www.equinix.com/locations/tours/security/.

Point-to-point Connections

To prevent sensitive data traveling over the public internet, AppNexus customers can provision a point-to-point connection from existing datacenters or office facilities to AppNexus.

Secure API Access

Access to the API is highly restricted. In addition to using secure SSL connections, API requests that do not originate from a customer's VLAN are immediately rejected. This means that to manipulate a customer's environment an individual must have access to that environment first. Customer bootstrapping (launching their first instances) is done entirely password-less; to gain access customers must first send us a public key. This way there is no risk of passwords being sniffed, and access to the environment is entirely in the customer's control.

Further Reading

- Security Recommendations