Networking and Firewalls

VLANs and Firewalls

Introduction

At Xandr every customer has a private VLAN, or Virtual Local Area Network, in each datacenter where they reserve servers. Your VLAN is a list of sequential IP addresses to be assigned to the instances you launch in the Xandr environment. Your VLAN can consist of 8, 24, 56, ..., (2^N-8) IP addresses; eight addresses in each range are reserved for networking equipment so it can behave as though it was part of your individual VLAN.

IP Addresses

- You can assign specific IP addresses to your equipment by using the optional "`--ip`" parameter for the `manage-instance launch` command. If no specific IP is selected, the next available IP in the range will be automatically assigned. For more information, see manage-instance.
- Instance IPs are static; if the server reboots or the instance goes offline, the IP will remain the same.

ACLs/Firewall

VLANs provide security by segregating each customer's traffic from Xandr and other customers' traffic and also by regulating traffic from the Internet according to a customer-controlled Access Control List (ACL). You can view your current ACLs in the customer portal at https://help.xandr.com.

- By default all inbound traffic from the Internet to your IP block is denied except for ping (ICMP Echo---used to verify that the host is up). With your ACL, you can explicitly permit TCP, UDP, or ANY traffic for particular source and destination IPs and ports.
- You'll set your inital ACL via the customer questionnaire, and you can change it at any time. At the moment, ACL changes must go through Support. Please see How to Set Firewall Rules for more information. Soon there will be an API for ACLs and you will also be able to use the customer portal.
- All traffic within a VLAN is allowed so all instances can freely communicate with each other.
- All outgoing traffic from your VLAN is allowed.
- **By default, all ports/traffic between same-customer VLANs in different datacenters is open. (Note that traffic between LAX1 and NYM1 travels over the Internet and is not encrypted.)**

If you run out of IP addresses in your VLAN

If you outgrow a VLAN, Xandr will assign you a larger one. This can take up to one workday as support staff configures the ACL for the new VLAN. You will then need to migrate instances from the old VLAN to the new one. This can be done without downtime; you will assign each item in your VLAN a second IP address for the duration of the migration. Detailed instructions on VLAN migration will be provided when you make your request to Support.

Note: We assume that customer IP requests are for usable IP addresses; the eight addresses used for network gear have already been accounted for when an IP range is allocated.

Further Information

Network Architecture
How to Set Firewall Rules
Enabled Port Ranges
Direct Connection to 3rd Party Datacenters
Software VPN
VLAN Tagging and Instance Security
manage-vlan CLI tool

Troubleshooting

Connectivity Issues

As always, please create a ticket at https://help.xandr.com if you have any questions or concerns.