VLAN Tagging and Instance Security

VLAN Tagging and Instance Security

Q: What prevents one customer from intruding on another customer's instance? (Jumping between VLANs, IP spoofing, DoS attacks).

A: In short, this is prohibited by the Xen hypervisor on the base OS (Dom0).

The more detailed answer is that Dom0 creates a bridge from a physical interface on the base box to the instance and controls where traffic coming from that virtual NIC goes. Security is achieved because the bridge works like this: Base Box VLAN sub interface <--> instance eth0.

Example:

1) The interface `peth0.2999` is the physical eth0 using vl2999 tagging.
2) The bridge `xenbrVLAN2999` is attaching `vif4.0` with `peth0.2999` which means that any traffic coming into interface `vif4.0` is leaving out the physical interface tagged on vl2999, and conversely any traffic coming into the physical interface with vl2999 tagging will be sent to `vif4.0`.
3) Xen then presents `vif4.0` to the instance as `eth0`.
4) The result is that the instance ethernet interface is successfully confined to VLAN2999.

If the customer created an interface `eth0.2000` in attempt to sneak into our management VLAN, they would be sending tagged frames to `vif4.0`, which would then be sent to the switch with vl2999 tagging. The Ethernet switch would only see the vl2999 tag and place that traffic into VLAN2999, and the vl2000 tag would have no impact.

But let's say you're not trying to sneak into another VLAN, you're simply trying to spoof an IP. Obviously, the return traffic would never get to you.

And let's say you're trying to do some damage / DDoS etc. To protect against that we have strict anti-spoof inbound ACLs (see **Example** below) that only allow traffic on a VLAN from its allocated IP range.

Example:

interface VLAN2999
ip address 8.19.30.114 255.255.255.240
ip access-group LAX1-VLAN2999-IN in
ip access-list extended LAX1-VLAN2999-IN

```
remark - allow traffic from LAX1:VLAN2999
permit ip 8.19.30.112 0.0.0.15 any
...
remark - ! deny and log all else
deny ip any any log
```

The result is that if a customer tried to send traffic from an IP that is not theirs, they will fail and the attempt will be logged.

Finally, in the case of a customer instance migrating from one VLAN to another, a new bridge is configured on the Dom0 hypervisor, attached to a new `vif`, and presented as "eth1" to the instance.