

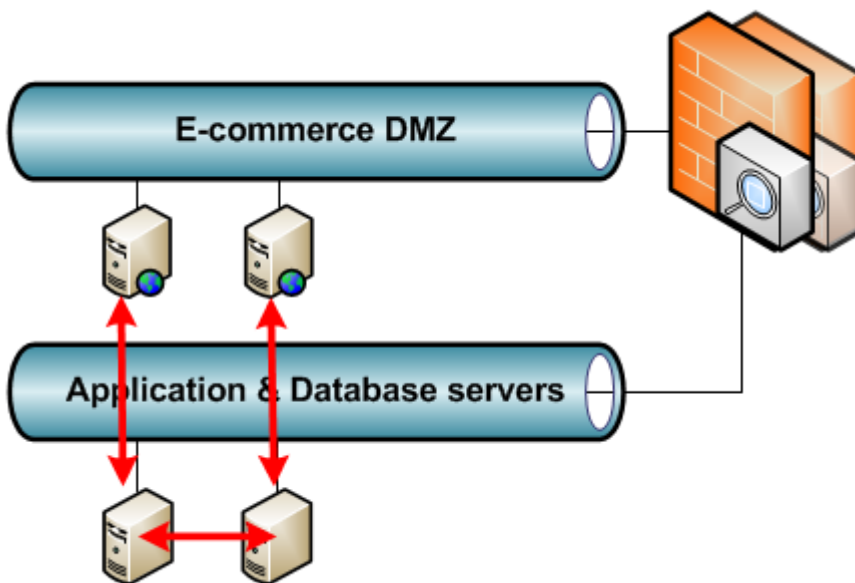
PRIVATE VLANS: WHERE TO DEPLOY THEM.

Part of the problem is covered in the article about deployment over multiple switches: you can't connect a trunked device such as a firewall to it. Although the Nexus 7000 provides a solution, that doesn't make it much easier (or cheaper).

Another important reason is that few are willing to take the risk to deploy a VLAN where hosts cannot communicate with each other, as this is usually the reason hosts are put in the same VLAN in the first place. There's the hesitation because it would introduce complexity or limit scalability, as new servers later on may need to communicate in the same subnet after all.

So where would it be beneficial and with low risk to use a Private VLAN? Actually quite a few places.

E-commerce

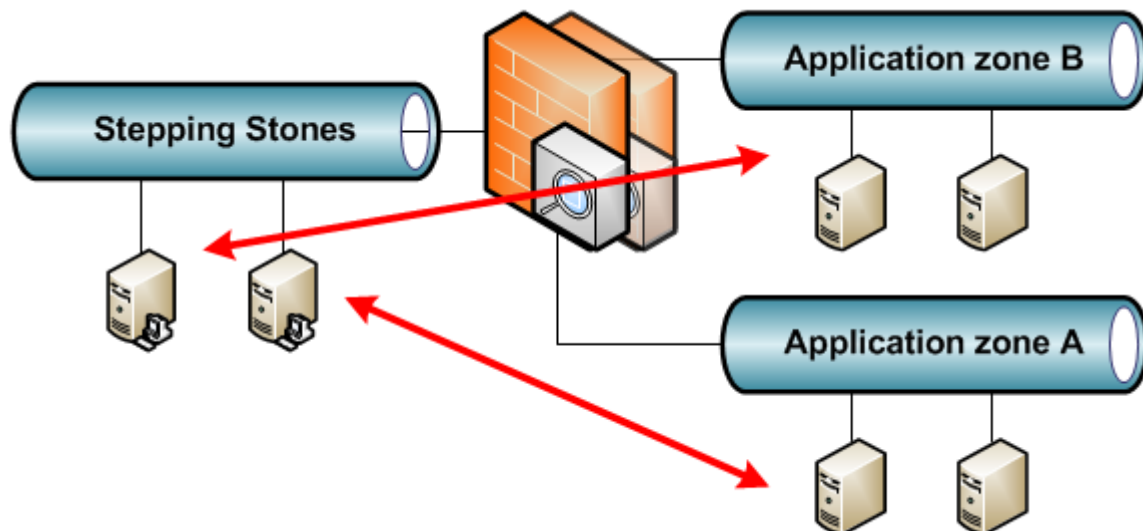


Say you have an internet-facing business with e-commerce websites where anyone can log in, create an account, or do a purchase. A compromised e-commerce server in the DMZ means immediate access to the entire DMZ VLAN. This VLAN has the highest chance of being compromised from the internet, yet the servers in it rarely need to speak with each other. In fact,

if properly designed, they will all connect to backend application and/or database servers that on their turn communicate with each other. This way the e-commerce data is synchronised without the DMZ servers requiring a connection to each other.

Stepping

Stones

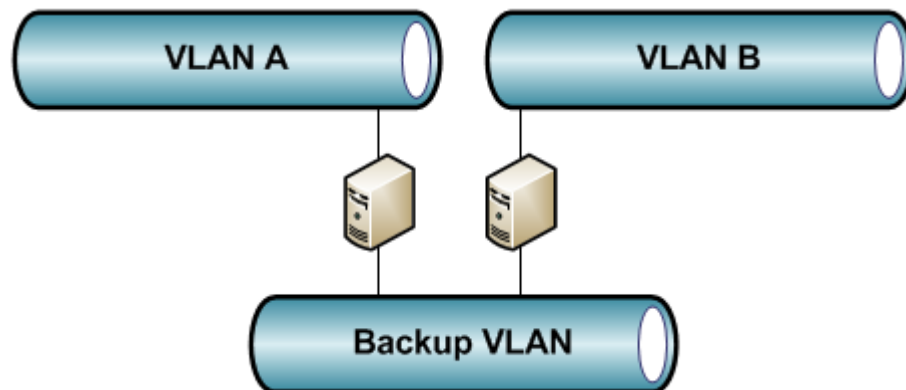


Some environments have a VLAN with Stepping Stone servers where users can log on to with pre-installed tools to access confidential resources. Access from one Stepping Stone server to another is not needed here. Sometimes it's even not desired as there may be a Stepping Stone per application, environment or third-party.

Out-of-Band

A modern rackserver has an out-of-band port to a dedicated chip in the server that can power off and on the server, and even install the OS remotely. For example, HP iLO. Typical here is that the out-of-band port never initiates connections but only receives connections for management, usually though the default gateway. This makes for a good Private VLAN deployment without issues.

Backup



Similar to out-of-band, some environments use a dedicated network card on all servers for backup. This introduces a security issue as it's possible for two servers in different VLANs to communicate without a firewall in between. Again a Private VLAN can counter this. Somewhat unusual in the design is that it's best to put the servers taking the backup in the promiscuous VLAN, so they can communicate with all servers and the backup VLAN default gateway, and put the default gateway in an isolated VLAN, preventing any other server from using it.

Campus – Wired guests

Similar to the Stepping Stones: guests can access the network through a firewall (the default gateway) but don't need to access each others computers.

Campus – Wireless APs

In a WLAN deployment with a central controller (WLC), all the Lightweight APs do is connect to the controller using the subnet default gateway. Any other services such as DHCP and DNS will be through this default gateway as well.

Campus – Utilities

Utilities such as printers, camera's, badge readers,... will likely only need the default gateway and not each other.

Where not to use PVLANS

This should give some nice examples already. But for last, a couple of places where not to use Private VLANs:

- ♦ Routing VLANs: unless you want to troubleshoot neighborships not coming up.
- ♦ VLANs with any kind of cluster in it: still doable with community VLANs for the cluster synchronisation, but usually better off in their own VLAN.

- ◆ User VLANs, VOIP VLANs and the like: VOIP and videoconferencing may set up point-to-point streams.
- ◆ Database server VLANs: not really clusters but they will often require access to each other.

Source : <http://reggle.wordpress.com/2014/01/14/private-vlans-where-to-deploy-them/>