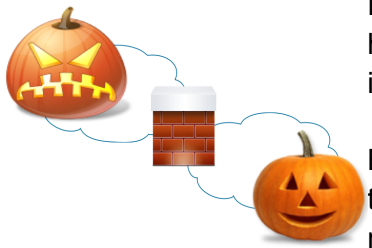
Marathon Networks

Protect and Survive

Convert a flat network to a highly segregated network without resegmentation

Firewalls through time

Firewalls are tried and true technology to protect IT resource.



Firewalls are usually deployed with two interfaces. One is the hostile outside world, and the other is the warm and secure internal network.

But two interfaces are not enough. It was soon discovered that to provide a proper protection to IT assets, more interfaces are needed, be it logical or physical.

Also, firewalls were initially installed on the perimeter of the network, facing the internet. But today, due to security threats and regulation, there is an increasing demand for internal firewalls to protect servers from within.

Planning for a new firewall, or expanding an existing firewall is not easy.

Evil Segments

When planning for a new firewall or expanding an existing one, we face two major questions:

- How many firewall interfaces do we need now, and how many will we need in the future?
- How to migrate from our existing, somewhat flat, network to a segmented network?

Multi Interface Large Firewall

How many firewall interfaces do we need? The clean room answer is one interface per server, were all servers are isolated from each other. In reality the answer is somewhere in between the clean room with endless number of interface and the flat network with two interfaces only.

Also, firewall interfaces are not for free. Some vendors charge licenses fees, and managing many interfaces, on any firewall, is not a pretty sight.

Next comes the IP addressing issue. Do we plan to use the easy but overly underutilized /24 segments? Do we plan to use non /24 segments, such as /29. Any non /24 can make the server team grow white hair while figuring out what is the address of the default gateway, and whether two servers are in the same segment or not.

And what about VDI? Should we protect the hundreds or thousands virtual desktops running in the data center from directly infecting each other with malware and infections? Do we need to segment them? If so, how do we segment desktops?

After Thought Migration

Now that we have decided how many firewall interface we need and how to allocate their IP addresses, we now need to move the existing hundreds or thousands of servers to their new locations.

From the servers prospective, moving a server to a new firewall interface is just about changing its IP address. Easy, right?

In reality, even when using DNS, changing a server's IP address is not an easy task. The IP address might be embedded in various places, and for each server, those places need to be found and dealt with. And most importantly, who is in charge of the IP address change? And what about the labor intensive operation of actually changing IP address in hundreds or thousands of server?

Firewall Segmentation Light

Wouldn't it be great if we could install a new firewall, or expand an existing one, without changing a single IP address? Are there magical unicorns?

There is a technology, which is implemented on all major vendor's switches, that can make this magic true. It is called Private VLANs

Private VLANs

With Private VLANs, you can take an existing segment and divide it to secondary segments. Each secondary segment it isolated.

With Private VLANs, even though hosts are on the same subnet, they can't reach each other without going through the firewall.

It is like taking a whole VLAN and dividing it into tiny little VLANs without changing anything at the server's or the firewall's interfaces.

With Private VLANs, there is no need to change a single IP address or a default gateway. There is no need to do complex IP addressing plan or work with crazy /29.

Cisco, Juniper, HP, Brocade, Force 10, Arista all support Private VLANs and so are VMWare's ESX and Microsoft's Hyper-V.

If Private VLANs are so wonderful, why aren't they common? Other than that Private VLANs are somewhat a new technology (about 5 years old), the answer is that Private VLANs are a bit harder to implement and operate.

Marathon Networks PVTD

Coming to the rescue of Private VLANs is Marathon Networks PVTD (Private VLAN Tool Daemon), which is a network appliance that helps with Private VLANs implementations and operations.

Marathon Networks PVTD saves you endless hours when deploying services in Private VLANs networks and also enables fast troubleshooting for Private VLANs.

With PVTD, time consuming complex work becomes no work at all.

PVTD is an enabler for network wide Private VLANs deployment. PVTD and Private VLANs can help you to smoothly transform your network from a flat insecure to a secure segregated network.

To find more information about Private VLANs and PVTD, please visit:
http://marathon-networks.com

Marathon Networks