

# HOW XSIGO VIRTUAL I/O ENSURES SECURITY AND DATA ISOLATION



## The industry's only solution to provide fully isolated Ethernet and Fibre Channel networks within a shared fabric

### OVERVIEW

Network isolation is a critical part of any data center design. To control data access and maintain security, best practices often dictate that different data types or network functions remain on physically separate networks. This need for isolation raises important questions when consolidating I/O. When you converge multiple network and storage connections to a single server cable, what isolation is provided for those connections?

Xsigo virtual I/O was designed to address exactly this challenge. It provides the isolation of physically separate connections, while also delivering the flexibility and agility of software-controlled connections.

### HOW XSIGO VIRTUAL I/O PROVIDES ISOLATION

Xsigo virtual I/O replaces a server's multiple Ethernet and Fibre Channel cables with a single link (or two for redundancy) that connects the server to the Xsigo I/O Director. The I/O Director provides the uplinks to the core networks. Within the servers, virtual NICs

and virtual HBAs replace the traditional I/O cards. These virtual devices "look" just like traditional physical I/O cards (just as a virtual machine "looks" like a physical server).

Isolation is achieved with resource mapping. Each virtual NIC and HBA is mapped exclusively to a specific port on the I/O Director. Data from that virtual resource is not accessible at any other port. It is the same as if a physical cable was extended from the vNIC or vHBA to the port on I/O Director. (Note that data can be made accessible from one virtual NIC to another those vNICs are mapped to the same physical port and are on the same VLAN.)

The I/O Director provides the same isolation as a physical link, but with far more flexibility. All mappings are established in software and can be changed at any time, without downtime.

This isolation does not rely on VLANs. While Xsigo's Ethernet links do support VLANs, that functionality is not used to enforce isolation at the I/O Director level.

### QUICK BENEFITS

- Converges multiple Ethernet and Fibre Channel connections to a single server link
- Provides the same link isolation as physically separate connections
- Up to 64 isolated connections per virtual link
- Dynamically connects isolated networks to servers
- Ensures predictable application performance with QoS controls per virtual connection
- Supports VLANs (but does not rely on them for isolation)
- Industry's only solution to provide fully isolated Ethernet and Fibre Channel networks within a shared fabric

### HOW VIRTUAL I/O ISOLATION WORKS

To ensure isolation between virtual I/O resources, each vNIC and vHBA has its own dedicated communication channel between the server and the I/O module within the I/O Director. Data belonging to a virtual I/O device is forwarded by the I/O fabric only between the relevant server and the relevant I/O module. Data cannot move from one I/O module to another, and cannot move from one vNIC or vHBA to another (again, unless those two resources are connected to the same physical I/O port and are on the same VLAN.)

### QOS ENSURES APPLICATION PERFORMANCE

QoS controls let you configure bandwidth capability per virtual link to ensure predictable application performance. QoS is hardware-enforced at the I/O Director level, so it does not consume server processor resources.

### OPENS NEW ARCHITECTURE OPTIONS

Xsigo's isolation opens up new architectural options. You can, for example, configure a DMZ network and a production network within a single Xsigo fabric and then connect those networks to servers and VMs as needed. To isolate those networks with an external firewall, simply connect the two sides of the firewall to separate ports on the I/O Director and map the respective networks to those ports.

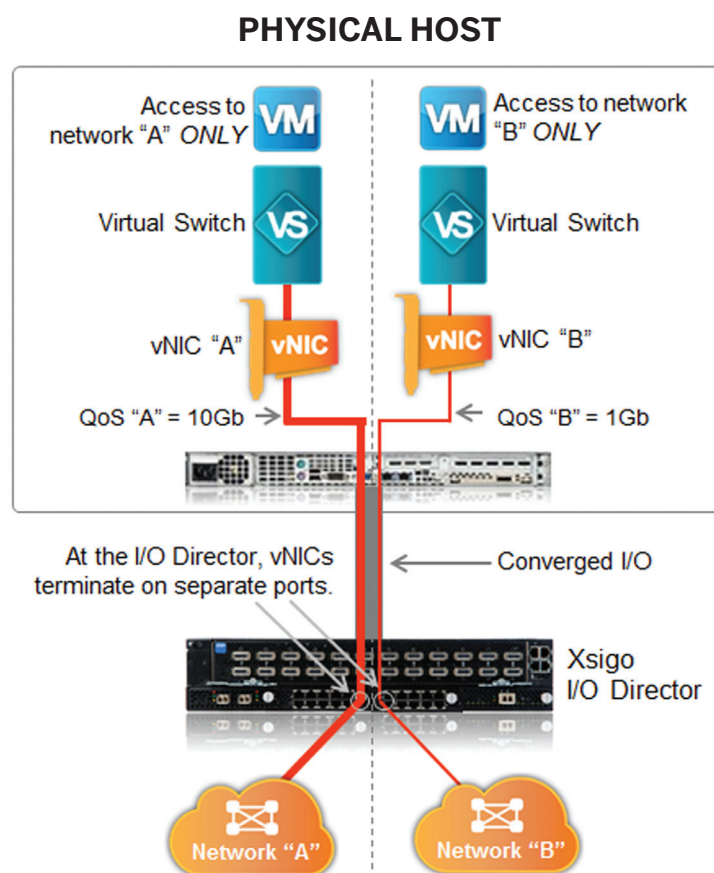
Alternately, you could configure the firewall as a software-based appliance on a server and deploy separate virtual NICs on either side of that device to maintain complete isolation.

No other infrastructure solution gives you the equivalent of physically separate networks within a single shared fabric.

### ENHANCES SERVER VIRTUALIZATION

These capabilities are particularly useful with virtualized servers. For example, it is sometimes undesirable to put multiple virtual machines on the same virtual switch. With traditional I/O, this security issue can be difficult to avoid since it is typically not feasible to dedicate a physical NIC per virtual machine. Xsigo eliminates this restriction. It is a simple matter to dedicate virtual NICs when needed, thus relieving the need to share virtual switches.

Xsigo provides network isolation without the need for VLANs or separate physical NICs and switches, greatly simplifying the infrastructure and making it both secure and dynamic.



Connect to physically separate networks simply by mapping virtual NICs to different ports on the I/O Director. The two connections will remain fully isolated within the converged I/O link. Quality of Service controls let you ensure predictable application performance.