BROCADE
A Broadcom Company

Smarter technology for all

Lenovo

Security incidents will happen. But your choice of SAN could save the business.

Many security best practices are vulnerable to unintentional mistakes

Today's organizations must use the best security defenses to ensure smooth operations and cyber resiliency across storage environments.

You can protect your data with firewalls, routing tables, VLAN controls, and access lists – but these need to be maintained manually. One error or oversight could leave your storage network exposed, and a compromised host could provide direct access to the next target of attack.

Security likely wasn't the primary reason you chose a Fibre Channel SAN. Yet Fibre Channel can play a valuable role in your enterprise security strategy.

Fibre Channel delivers a strong line of defense

Ethernet-based SANs simply can't come close to matching Fibre Channel's native features in protecting an organization's valuable assets. Fibre Channel fabrics are secure by design, based on controlled access between servers and storage. This prevents attackers from being able to see or infiltrate connected storage devices. This isn't the case for Ethernet-based SANs, making Lenovo Fibre Channel SAN (based on Brocade® technology) the top choice for mission-critical storage.

Lenovo DB Series SAN provides a cyber-resilient network designed with security in mind and implement many security measures that offer the added level of security needed to ensure your operations are protected. The Fabric Operating System (FOS) of the SAN adds additional security enhancements to validate the integrity and security of your Lenovo DB Series hardware and software to further safeguard an organization against vulnerabilities.

Security considerations across Fibre Channel and Ethernet

Shared IP Storage Network

- Host-attached storage/IP storage arrays may be attacked directly
- Firewall configurations require ongoing maintenance to be current
- Any storage that can be addressed via IP is a direct target
- Compromising any host gives a platform for possible direct attack
- iSCSI/HCI/Direct-attached hosts will surrender their storage if breached

Fibre Channel Storage Area Network

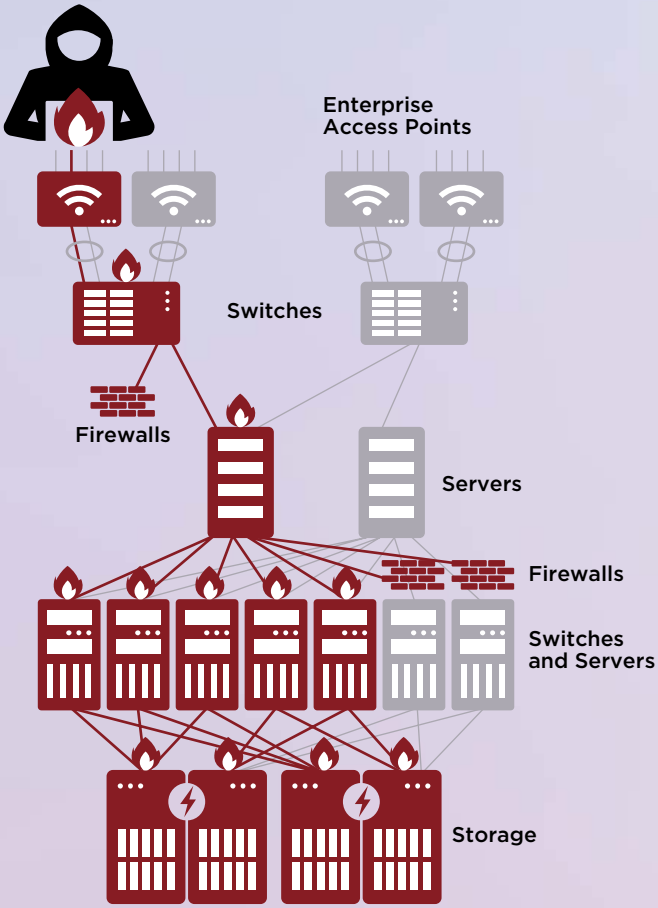
- SAN-attached storage has no direct exposure to IP networks
- All data transfers occur over Fibre Channel Protocol (FCP)
- From a host viewpoint, the network is a data plane, not a control plane
- Fibre Channel requires separate hardware and protocols
- Direct attacks are much more difficult and would require control plane access

Any-to-Any vs. Point-to-Point

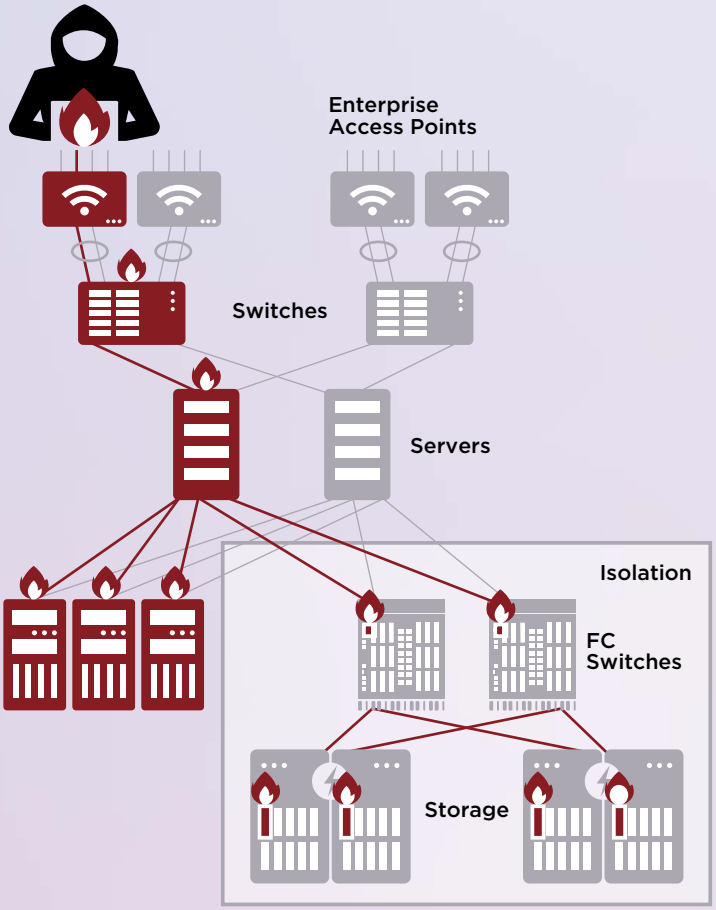
FC networks are based on a 'point-to-point design' where each attached server can see only storage volumes shared to it but not any of the other volumes or attached servers. This makes the FC environment much more secure in the event a server within the network gets compromised. Ethernet is built around an 'any-to-any design' where every attached server sees not only the shared storage but every other attached server as well. This is not the only determinant of security in fabrics, and both Ethernet and FC include other software-driven capabilities (virtual networks, etc.) that help enforce security, but the 'point-to-point nature' of FC does make it inherently more secure.[1]

1 Source – IDC Planning for the Transition to Production-Ready NVMe over Fabrics Deployments in the Enterprise, April 2020.

Any-to-Any Design



Point-to-Point Design



Security Strategies for the SAN

Hear from experts on why native Fibre Channel security outperforms Ethernet

Watch webinar

Safeguard the SAN

Learn how Lenovo Gen 7 takes security further with inherent features that keep your environment protected

Download PDF

Set up a call today

To discuss your specific needs with our data experts

Schedule now