Executive Summary

As FC technology evolves into a new generation of 8Gbps products, it is imperative that a scalable architecture be deployed to meet a full spectrum of concerns beyond cost, performance, and backwards compatibility. The modern data center is faced with ever growing demands in the areas of virtualization; power consumption; Reliability, Availability, and Serviceability (RAS); security; and manageability.

Key Findings

- **Enhanced Authentication**: QLogic 8Gb Host Bus Adapters (HBAs) offer support for Fibre Channel-Security Protocol (FC-SP) and Diffie Hellman-Challenge Handshake Authentication Protocol (DH-CHAP) security mechanisms that can be utilized to authenticate all in-band communication requests. This feature, along with the existing user authentication solutions in SANsurfer® FC HBA Manager, provides an authentication solution for HBA requests that are both in-band and out-of-band.

- **Comprehensive Access Control**: QLogic’s port-level virtualization and N_Port ID Virtualization (NPIV) implementation offers a comprehensive access control solution for virtualized FC SAN environments. QLogic’s NPIV features are extended through SANsurfer FC HBA Manager and other popular virtualization management solutions such as the Microsoft® System Center Virtual Machine Manager and the VMware® VirtualCenter and Virtual Infrastructure Client.

- **Complete Data Integrity**: QLogic’s 8Gb HBAs offer an end-to-end data integrity solution by supporting FC Cyclic Redundancy Check (CRC) and T10-CRC mechanisms. This feature enhances the data reliability of enterprise class FC SANs by minimizing data loss situations.
Executive Summary (Continued)

QLogic’s 8Gb HBAs address the growing need for SAN security by incorporating comprehensive authentication, authorization, access control, and data confidentiality solutions in its FC HBA drivers and management solutions, SANsurfer FC HBA Manager (GUI-based), and SANsurfer FC HBA Command Line Interface (CLI).

This white paper explores QLogic’s 8Gb HBA security features, one of the key pillars of QLogic’s next generation of Fibre Channel products that are optimized to meet the business needs of the modern data center.

Introduction

Over the years, FC SANs have become the backbone for serving information needs of enterprise data centers. SANs have been traditionally considered physically secure due to their closed and physically isolated location in data centers. While physical network isolation offers the critical security, breaches through unauthorized hosts or users could still pose potential security risks.

Adoption of server virtualization technologies, increasing number of physical or virtual servers in data centers, data center growth through mergers and acquisitions have resulted in increased security concerns. Accordingly, security has remained the top budget priority over the last five or six years, with 60 percent of companies placing it as the highest priority in a recent International Data Corporation™ (IDC) survey. The industry drivers for security are listed in the following table.

<table>
<thead>
<tr>
<th>IT Challenges</th>
<th>Regulatory Compliance</th>
<th>Business Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consolidation</td>
<td>Industry (SOX, HIPAA)</td>
<td>Insiders</td>
</tr>
<tr>
<td>Off-Site Replication</td>
<td>National (SB 1386)</td>
<td>Lost Tapes</td>
</tr>
<tr>
<td>Outsourcing</td>
<td>Local</td>
<td>Data Breaches</td>
</tr>
</tbody>
</table>

IT challenges such as offsite replication and geographically separated development centers have introduced new potential breach points to access company confidential information. New regulatory compliance laws are stringent and require companies to store large amounts of historical information for audit purposes. Many businesses have been affected, because lapses such as insiders leaking information and lost tapes have led to the compromise of confidential information. According to Infostor, 36 percent of the security breaches have cost corporations over a million dollars to recover from the attack.

In addition, information explosion and server proliferation have caused new challenges for data centers driving security threats to critical levels. Organizations are adding data storage at a rate of 80 percent per year, according to IDC. This data explosion has been fueled in part by powerful database applications, deployed by organizations to capture and manage information. With regulations like Sarbanes-Oxley, Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), and California Security Breach Information Act (SB-1386), companies are facing increasing pressure to retain this information for longer periods of time, while also ensuring its privacy. Proliferation of devices means businesses face tough decisions on how to store and secure data and comply with regulations. The cost of security breaches coupled with emerging business practices and regulatory compliance creates a new set of challenges that enterprise data centers have to address. Downtime for company’s media servers could mean thousands, if not millions, of lost page views.

QLogic’s new 8Gb FC HBAs deliver not only faster access to the data, but also offer the highest levels of data integrity to enterprise data. With its 8Gbps solution, QLogic has extended its leadership in enterprise security features offered in FC HBA solutions by incorporating innovative designs across hardware, firmware, and software components. The following sections describe the specific building blocks in QLogic’s 8Gb FC HBA security solution that help data center administrators align the IT infrastructure with the business goals of their organizations.

Authentication

Authentication is the process of attempting to verify the digital identity of the sender or initiator of a communication. In other words, it is the process of determining whether someone is in fact who they claim to be. Authentication techniques make sure that only valid users have access to protected resources.
In private and public computer networks (including the Internet), authentication is commonly done through the use of logon passwords.

From an FC SAN perspective, an authentication solution is delivered through FC-SP technology. FC-SP is a security framework (defined by the T11 standards group) that includes protocols to enhance FC security in several areas, including authentication of FC devices, cryptographically secure key exchange, and cryptographically secure communication between FC devices. FC-SP is focused on protecting data in transit throughout the FC network. DH-CHAP is a secure key-exchange authentication protocol that supports both switch-to-switch and host-to-switch authentication.

DH-CHAP is a secret based authentication and key management protocol that uses the CHAP algorithm (see RFC 1994) augmented with an optional Diffie-Hellman algorithm (see RFC 2631). DH-CHAP provides bidirectional authentication and may provide unidirectional authentication between an Authentication Initiator and an Authentication Responder. In order to authenticate with the DH-CHAP protocol, each entity, identified by a unique Name, is provided with a secret. Two entities may impersonate one another if they have the same secret; therefore, when the assigned secrets for each entity are identical, there is security vulnerability.

QLogic’s 8Gb FC HBAs offer support for FC-SP authentication using DH-CHAP protocol. In addition, QLogic has provided proof of concept software solutions to expose these features to the end users. QLogic is currently working with ecosystem partners to enable these features as part of drivers and management solutions for all leading operating systems. Using DH-CHAP capabilities through SANsurfer FC HBA Manager, data center managers can enforce authentication between hosts and switches connected to a FC SAN.

Access Control

Many organizations still rely on age old “trust based” access control mechanisms to safeguard protected information. This has fueled the rise of security breaches that cost corporations millions of dollars. Enterprise class data centers need protection mechanisms to ensure that company confidential information and other important resources are safeguarded from malicious users and involuntary mistakes by data center administrators. Access control refers to the mechanisms and policies that restrict access to computer resources. Access control is the process of enforcing the rights of individuals or application programs to obtain data from, or place data into, a storage device.

Access control in an FC SAN environment is accomplished through a technology called zoning. Zoning provides the ability for users to specify groups of devices that are supposed to talk to each other. Zoning is primarily used to protect FC SAN environments from spoofing attacks. Spoofing attacks are situations where a malicious system successfully presents itself as a legitimate system and gains access to a protected resource. Zoning can be accomplished either through hardware or software depending on which it is termed: “hard zoning” or “soft zoning”.

Traditional FC SAN environments require systems administrators to use a physical HBA World Wide Port Name (WWPN) for defining fabric zones, masking storage Logical Unit Number (LUNs), and migrating Virtual Machines (VMs). This approach does not work well in virtualized environments, as it forces system administrators to reconfigure FC SAN network settings (zoning, masking, and binding) when a VM is migrated from one physical server to another. In addition, storage administrators typically define one zone where all disks are exposed to every server to support the migration of VMs to new servers. This design creates access control concerns for disks with sensitive information, and requires the reconfiguration of the network if more than one zone is defined. QLogic’s pioneering efforts in HBA Virtualization technologies (NPIV and Virtual Fabrics) help address the above mentioned risks.
It is a common practice to place servers in different zones when they need exclusive access to two different LUNs. In a virtualized FC SAN environment, such a solution does not guarantee complete access control since there can be multiple virtual machines associated with a single physical server. HBA virtualization technologies are needed to provide access control in a virtualized FC SAN environment. QLogic 8Gb FC HBAs provide a complete HBA virtualization solution through NPIV.

QLogic’s 8Gbps NPIV implementation virtualizes the physical HBA port configured in a point-to-point FC SAN topology and allows a single physical FC HBA port to function as multiple logical ports, each with its own identity. Virtual HBA ports allow storage administrators to bind VMs to storage and define multiple zones using the virtual port parameters, creating a more manageable and more secure virtualized environment. Using QLogic’s NPIV implementation, virtual machines can be restricted from accessing LUNs even though the underlying physical servers have access to the same LUNs. Data center managers no longer need to reconfigure zoning and LUN masking settings after a VM migration. NPIV technology also eliminates the necessity to expose all LUNs to all physical servers to plan for a VM migration.

**Data Integrity**

Reliable access to data is a prerequisite for most computer systems and applications. There are several factors that cause unexpected or unauthorized modifications to stored data. Data can get corrupted due to hardware or software malfunctions. Disk errors are common today, and current storage software is typically not designed to handle a large class of these errors. A minor integrity violation, when not detected by the higher level software on time, could cause further loss of data. Data Integrity is a term that refers to a condition in which data is identically maintained during operations such as transfer, operation, and retrieval. In simple terms, data integrity is the assurance that data is consistent and correct.

Data integrity can be guaranteed in several ways. These data integrity solutions can be classified into four main categories:

- **Avoidance**: Some systems provide a certain level of integrity guarantee for the data they store, so as to avoid explicit integrity checking mechanisms. These systems come with an advantage in that they do not incur additional overheads for integrity verification.

- **Detection**: Most of the storage integrity assurance techniques that exist today perform detection of integrity violations, but do not help recover from the violation.

- **Correction**: When an integrity violation is detected by some means, some methods can be used to recover data from the damage.

- **Detection & Correction**: Ensuring data integrity is extremely crucial to meet important Service-Level Agreement (SLAs) and Quality of Service (QoS) service offerings. The FC protocol offers Cyclic Redundancy Check (CRC) to detect data integrity issues at a frame level.

FC protocol has a built-in frame level data integrity solution at the FC-2 layer to protect against data mismatch situations. An FC-2 frame is composed of a Start of Frame (SOF) delimiter, frame content, and an End of Frame (EOF) delimiter. The frame content is composed of zero or more Extended Headers, a Frame Header, Data Field, and CRC. The Fibre Channel Cyclic Redundancy Check (FC-CRC) — a four byte field that immediately follows the Data Field — verifies the data integrity and validity of the FC frame. QLogic 8Gb FC HBAs comply with the requirements of the FC protocol and offer comprehensive support for FC-CRC implementation.

Enterprise class data centers depend heavily on the FC-CRC to safeguard against data loss and data mismatch situations. During a write operation, the FC-CRC field is appended to the FC data field that is generated on the initiator side. This FC frame is then sent to the front-end of the storage system, which strips the FC-CRC out of the FC frame and performs the check. The data field is removed and sent to the storage back-end if it is not corrupted or modified. The data field is then stored in the form of blocks on disks in the storage back-end. Though FC-CRC provides data integrity services for FC, it has some limitations:

- The FC-CRC field is generated at the initiator and verified at the target; it is not persistently stored.

- FC-CRC does not offer an end-to-end solution.
The consequence of FC-CrC design and implementation is that the data remains unprotected when being transferred from the storage system front-end to the storage system back-end. Data integrity issues during transfer between the storage front-end and the storage back-end will go undetected.

The INCITS T11 committee, which comprises industry leaders including QLogic, has designed a specification called the T10-CrC that addresses the existing data integrity gaps in the FC SAN environments. The combination of FC-CrC and T10-CrC deliver a true end-to-end data integrity solution for physical and virtual FC SANs.

T10-CrC provides end-to-end data protection through an eight-byte Data Integrity Field (DIF). DIF consists of a two-byte Guard (CrC), a two-byte Application Tag (meta-data), and a four-byte Reference Tag (meta-data for LBA). The DIF is appended at the end of data blocks. The CrC is stored (persistently) just like data.

QLogic's 8Gb HBAs have built-in support for both FC-CrC and T10-CrC technologies. In enterprise class FC SAN environments that utilize QLogic 8Gb HBAs, every block of data generated on the initiator side is appended with eight-bytes of T10-CrC. Multiple blocks of data are then combined to form the Data Field of the FC frame. This Data Field is then appended with the FC-CrC field. The FC frame is then sent to the storage front-end, where the FC-CrC check is performed by stripping off the FC-CrC field. If the FC-CrC check returns no error, the Data Field is then sent to the storage back-end, where the T10-CrC check is performed on the individual blocks of data. The individual blocks of data along with their T10-CrC fields are stored in the storage back-end.
Summary and Conclusion

The modern data center faces security challenges due to device proliferation, disruptive technologies such as virtualization, and new regulatory compliance laws. It is imperative to safeguard the storage infrastructure that feeds the needs of the day-to-day business demands. QLogic 8Gb FC HBAs incorporate several security features designed to protect FC SAN environments from security breaches. These features include the following:

- In addition to offering a complete user management solution, QLogic’s 8Gb HBAs support FC-SP and DH-CHAP security mechanisms, thus offering a complete authentication solution for both in-band and out-of-band requests.
- QLogic’s 8Gb HBAs offer a comprehensive HBA virtualization solution through NPIV. QLogic’s NPIV implementation offers an access control solution for virtualized FC SAN environments.
- QLogic’s 8Gb HBAs provide support for both FC-CrC and T10-RC, offering best-of-breed data integrity solution for both physical and virtualized FC SAN environments.

<table>
<thead>
<tr>
<th>Challenges</th>
<th>Solution</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>FC-SP, DH-CHAP</td>
<td>Prevents user impersonation attacks. Ensures enhanced security in SANs.</td>
</tr>
<tr>
<td>Access Control</td>
<td>NPIV</td>
<td>Enhanced access control for virtualized SANs</td>
</tr>
<tr>
<td>Data Integrity</td>
<td>T10-CRC, FC-CrC</td>
<td>Enhanced data reliability</td>
</tr>
</tbody>
</table>
Dell has tested and certified the QLE2560 QLogic Series HBA with Dell™ PowerEdge™ R805, R905, R900, 1900, 1950, 2900, 2950, 2970 servers and storage systems. Dell specifically disclaims knowledge of the accuracy, completeness or substantiation for all statements and claims made in this document regarding the properties, capabilities, speeds or qualifications of the QLogic 2500 Series adapters.

Disclaimer
Reasonable efforts have been made to ensure the validity and accuracy of these performance tests. QLogic Corporation is not liable for any error in this published white paper or the results thereof. Variation in results may be a result of change in configuration or in the environment. QLogic specifically disclaims any warranty, expressed or implied, relating to the test results and their accuracy, analysis, completeness or quality.