Internet SCSI (iSCSI) carries SCSI commands between host systems (initiators) and storage systems (targets) by defining the encapsulation of SCSI packets in TCP and routing them through IP—allowing block-level storage data to be transported seamlessly over IP networks. With Gigabit Ethernet already widespread and 10 Gigabit Ethernet becoming available, IP-based storage has become increasingly viable in enterprise data centers.

Appropriately configured iSCSI networks can provide security comparable to or better than Fibre Channel, particularly when a separate Ethernet network is used for iSCSI traffic. Because iSCSI runs over TCP/IP, all of the security options for standard network traffic are also available for iSCSI. However, administrators should take specific steps when sharing a single physical network to help ensure the separation and security of iSCSI traffic. Key methods include deploying security negotiation and authentication processes and implementing IP security (IPsec), Internet Storage Name Service (iSNS), and virtual LANs (VLANs).

**SECURITY NEGOTIATION AND AUTHENTICATION**

The interaction between initiators and targets begins with the iSCSI login process, which establishes the iSCSI connection, sets the protocol parameters, and authenticates initiators and targets with each other. During the initial phase of security negotiation, initiators and targets negotiate the security parameters using text keys. The AuthMethod text key passed by the initiator contains a list of authentication methods in order of preference. The available authentication methods are Kerberos V5 (KRB5), Simple Public-Key Generic Security Services Application Programming Interface (GSS-API) Mechanism (SPKM1), Simple Public-Key GSS-API Mechanism 2 (SPKM2), Secure Remote Password (SRP), Challenge Handshake Authentication Protocol (CHAP), and no authentication. The target must reply with the first option in the list it supports and is allowed to use. The initiator and target must implement CHAP, but the other authentication methods are optional. After the authentication process is complete, the initiator and target move on to the optional login operational negotiation phase or the iSCSI full feature phase.

CHAP, the only required authentication method, defines a methodology for authenticating initiators and targets. It is a form of in-band negotiation that provides end-to-end trust between initiator and target, and periodically verifies peer identity using a three-way handshake. This handshake is performed when...
the link is initially established, and may be subsequently repeated at different times. The authentication method depends on a key known only to the authenticator and the peer, which is not sent over the link. Unidirectional authentication enables the target to validate the initiator. Bidirectional authentication adds an additional level of security by providing a means for the initiator to authenticate the target.

Figure 1 illustrates the CHAP unidirectional authentication process. After the initial authentication has succeeded, the target sends a new challenge to the initiator at random intervals and repeats this process to verify the authentication. If the authentication fails, the target rejects the login attempt.

Each initiator should use a single unique CHAP authentication key: administrators should not use the same key for multiple initiators, and should not configure initiators to use multiple keys. In addition, initiators should not reuse CHAP challenges sent by targets for the other direction of a bidirectional authentication.

The other available authentication methods are more advanced than CHAP. Kerberos enables authentication through a trusted third-party service. SPKM1 and SPKM2 use public keys rather than symmetric keys. SRP is well suited for negotiating secure connections with user-supplied passwords, helping eliminate security problems traditionally associated with reusable passwords.

IPSEC
Because iSCSI uses TCP/IP, administrators can help secure iSCSI traffic by using cryptography at the IP layer. IPsec, a set of security extensions developed by the IETF, provides privacy and authentication services at the IP layer by enabling a system to select the required security protocols, determining the algorithms to use for the services, and putting in place the cryptographic keys required for these services. To help protect the contents of IP datagrams, IPsec uses encryption algorithms to transform the data.

IPsec comprises two primary transformation protocols: Authentication Header (AH) and Encapsulating Security Payload (ESP). AH helps provide connectionless integrity, data origin authentication, and an optional anti-replay service. ESP helps provide confidentiality (encryption) in addition to the AH services. Each protocol supports two modes: transport mode and tunnel mode. In transport mode, they help provide protection primarily for upper-layer protocols; in tunnel mode, they are applied to tunneled IP packets. IPsec-compliant iSCSI security implementations may or may not support ESP in transport mode, but must support it in tunnel mode.

IPsec uses multiple security protocols, a few of which must be supported by IPsec-compliant iSCSI implementations. A keyed-hash message authentication code with Secure Hash Algorithm (SHA-1) must be supported to help verify data integrity and authentication. Triple Data Encryption Standard (3DES) with cipher block chaining (CBC) is required. MD5 is also required, although it is not used for iSCSI.

Figure 2 illustrates the IPsec and IKE security process. Step 2 (IKE phase 1) involves negotiating authentication and the hash and encryption algorithms, generating shared keys, and authenticating the initiator and target. Step 3 (IKE phase 2) occurs while the systems are protected by the IKE SA set up in the previous step; two unidirectional IPsec SAs are generated for the security protocol (AH or ESP) and cryptographic algorithms identified during negotiation.

IPsec may not be supported by all iSCSI storage systems, and because significant resources are required for processing IPsec traffic, many solutions may not be cost-effective and may reduce performance for iSCSI traffic.

INTERNET STORAGE NAME SERVICE
iSNS facilitates automated discovery, management, and configuration of iSCSI devices on TCP/IP networks. It provides
intelligent storage services comparable to those found in Fibre Channel–based SANs by using discovery domains. Its discovery domain service enables administrators to partition storage nodes into manageable groupings for administrative and login control purposes. Administrators can limit login processes for each initiator to an appropriate subset of targets registered in iSNS, which can help limit the time that servers spend initializing login relationships as SANs grow.

iSCSI-based servers and storage act as iNS clients, communicating with the iSNS server using iSNS Protocol (iSNP). Storage controllers send storage array profiles to the iSNS server. Storage clients can discover accessible storage controllers through the iNS server.

Administrators can place the systems that should be accessible to each other in a single discovery domain. Each system may be part of multiple discovery domains. If administrators have placed one or more network portals of a system into a discovery domain, then queries to that domain report only portals that have been explicitly placed there. Administrators can manage discovery domains offline through a separate management workstation using iSNP or Simple Network Management Protocol (SNMP). Figure 3 illustrates an example environment using iSNS zoning.

iSNS also supports discovery domain sets. Valid and active discovery domains belong to at least one active discovery domain set; domains that do not belong to an activated set are not enabled. Analogous to zone sets in Fibre Channel-based SANs, discovery domain sets can be used to quickly reconfigure an iSCSI-based SAN for different application requirements.

VIRTUAL LANS

VLANS divide physical networks into separate virtual networks, which helps reduce broadcast traffic to individual nodes. Administrators can also use VLANS to segregate networks to help increase security. By deploying an iSCSI network on a separate VLAN, traffic between the iSCSI network and outside networks can take place only through a router or Layer 3 switch. This configuration helps minimize the risk of unauthorized access to iSCSI storage from the outside network. To help further increase security, administrators can also deploy multiple portals for a single storage array on separate VLANS.

Figure 4 illustrates an example environment in which one port of an iSCSI array has been placed on VLAN 2 with two servers. VLAN 3 includes the other port of the storage array and a third server. Administrators can use the management station for out-of-band array configuration. Segregating the devices and network portals into distinct VLANS in this way helps increase security.

SECURE iSCSI NETWORKS

Using the methods described in this article can help administrators secure iSCSI networks in enterprise environments. Administrators should keep in mind that all of these methods may not be supported on all iSCSI storage arrays; when planning an iSCSI network, they should evaluate the available methods and choose the appropriate ones based on their security requirements. Doing so can help administrators deploy iSCSI over many different types of IP networks while providing an appropriate level of security.

Surendra Bhat is a Product Group test engineer senior analyst in the Enterprise Server Test Group at the Dell India R&D Center. His interests include networking and storage technologies, and he has a bachelor’s degree in Electronics Engineering from the University of Mumbai.
Lokesh Singh is a Product Group test engineer analyst in the Sustaining Business organization at the Dell India R&D Center. His interests include networking and storage technologies, and he has a B.E. in computer science from Kumaun University.

Santosh Bhadri is a Product Group engineer senior analyst in the Sustaining Business organization at the Dell India R&D Center. His interests include computer architecture and storage technologies, and he has a bachelor’s degree in Electronics and Communication from B.M.S. College of Engineering.