SECURING STORAGE AREA NETWORKS WITH ISCSI

PROTECTING NETWORKED STORAGE WITH ISCSI

Already, iSCSI has established its value as a consolidated storage solution that leverages existing skills and infrastructure — while delivering high performance and platform interoperability. However, if iSCSI is to realize its potential as the standard for networked storage, businesses must be assured that their data will be secure. In an iSCSI SAN, traditional SCSI direct cabling is replaced by device connections to an IP network infrastructure. Based on SCSI and Ethernet, the iSCSI protocol enables block-level data to be transported between an iSCSI initiator running on a server and an iSCSI target on a storage device. An iSCSI SAN provides a number of built-in features that together can deliver some of the most comprehensive security currently available in SAN technology — whether you are transferring data within a LAN or across the Internet.

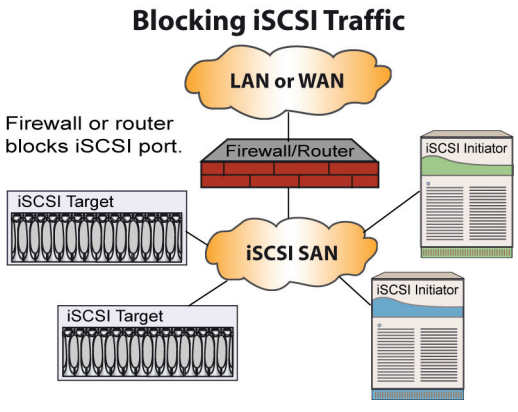
iSCSI SANs typically provide a number of built-in features that together can deliver some of the most comprehensive security currently available in SAN technology—whether you are transferring data within a LAN or across the Internet.

ISOLATING AN ISCSI SAN

An iSCSI SAN uses Gigabit Ethernet, a switched network with a point-to-point architecture that is designed to make it nearly impossible to “snoop” or “hijack” packets unless you have physical access to the network or administrative access to the switches. To isolate or partition an iSCSI SAN from a LAN or WAN, you can block the standard iSCSI port 3260 on a router or firewall, while keeping other ports available for management purposes. Firewall and router security rules may be tightened as needed.

SECURING DATA ACROSS THE INTERNET

When an iSCSI SAN must be accessed from a WAN, the Internet, or other publicly accessible network, additional security mechanisms are needed to protect packets across potentially insecure network links. A Virtual Private Network (VPN) can be used to safeguard data across a public network. IPsec is one of the most widely used security protocols for VPNs. The IPsec protocol provides a secure path between an iSCSI initiator and target by authenticating the devices and encrypting data that travels over the path. In a VPN, each iSCSI SAN is connected to a VPN gateway.



When data is transferred between two SANs, the VPN gateways first use IPsec to authenticate each other. Then, data is encrypted and sent across a "tunnel" to the receiving gateway, which decrypts the data and delivers it to its final destination. The virtual path between VPN gateways prevents "snooping" and "hijacking." To applications, the path appears to be a point-to-point connection. IPsec can be implemented in hardware or software, including iSCSI devices. However, there are performance and administration issues to consider when determining which IPsec delivery mechanism is best for a particular environment.

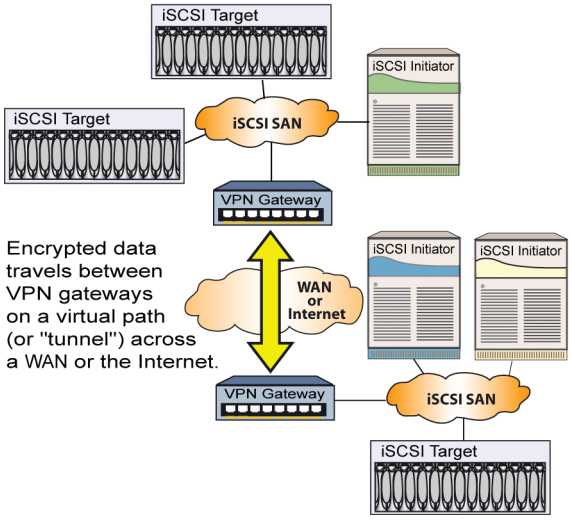
ISCSI AUTHENTICATION COMPLETES THE TASK

While firewalls and IPsec protect packets at the IP level, iSCSI provides a request and response login procedure to help ensure that only trusted iSCSI initiators can access the storage behind a particular target. When an iSCSI initiator connects to a target, the login procedure authenticates both the initiator and the target and sets iSCSI and security protocols for the session. SCSI commands can be sent only after the login completes. iSCSI supports login using Challenge Handshake Authentication Protocol (CHAP). Some iSCSI SAN solutions can further restrict iSCSI target access to specific initiators or IP addresses.

A COMPREHENSIVE SOLUTION FOR SECURE STORAGE

An iSCSI SAN delivers some of the most comprehensive security currently available. By physically limiting access to iSCSI SAN devices and isolating SANs from public networks, data can be protected across all network paths. The added security of iSCSI login authentication between initiator and target helps assure businesses that data is accessible only to authorized individuals.

Using a VPN to Securely Transfer Data



While firewalls and IPsec protect packets at the IP level, iSCSI uses a login procedure to help ensure that only trusted iSCSI initiators can access the storage behind a particular target.