iSCSI Security Overview

Otakar Likar, Chris Odhner | Network Appliance | March 2005 | TR 3338

TECHNICAL
REPORT

Network Appliance, a pioneer and industry leader in data storage technology, helps organizations understand and meet complex technical challenges with advanced storage solutions and global data management strategies.

Network Appliance Inc.

Table of Contents

Introduction

iSCSI Security Model

Product Overview

Security on Filer

Security on Network

Security on Host

Conclusion

Introduction

iSCSI is defined as Internet Small Computer System Interface, an IP-based storage networking protocol developed by the Internet Engineering Task Force (IETF) to link data storage facilities. By carrying SCSI commands over standard IP networks, iSCSI facilitates data transfers over LANs, WANs, and intranets and manages storage over almost any distance. Because iSCSI is transmitted over standard Ethernet connections using TCP/IP, many benefits are easily realized. You should realize the following benefits whether you choose to implement iSCSI over a dedicated Ethernet network or run it over your existing Ethernet infrastructure. Almost every IT staff is familiar with Ethernet networks, TCP/IP, and related technologies, such as switches, VLANs, DNS, and DHCP. This translates into little or no new network/fabric knowledge or training requirements. If you choose to implement a dedicated Ethernet network for your iSCSI solution, you will realize performance potentially comparable to Fibre Channel.

During an iSCSI session when an end user or application on the host sends a request, the host operating system generates the appropriate SCSI commands and data request, which then go through encapsulation into an IP packet and, if necessary, encryption procedures. A packet header is added before the resulting IP packets are transmitted over an Ethernet connection to the target filer. When a packet is received, it is decrypted (if it was encrypted before transmission) and disassembled, separating the SCSI commands and request. The SCSI commands are sent on to the SCSI controller and from there to the SCSI storage device. Because iSCSI is bidirectional, the protocol is also used to return data in response to the request.

An administrator allocates data storage by creating and configuring LUNs on the filer and mapping them to one or more host initiators. Usually each host has exclusive access to a LUN at any given time.

This paper discusses iSCSI security and helps you achieve the security level appropriate to your implementation. It covers the following iSCSI security topics: NetApp Data ONTAP™ iSCSI security features, security built into the iSCSI protocol, TCP/IP-based security that can be used in an iSCSI implementation, and Ethernet topology security considerations.

This paper is intended for storage or security administrators and assumes some familiarity with Data ONTAP and IP networking technology.

iSCSI Security Model

Since iSCSI provides block-level access to storage, it is accessed by the host operating system as if it were a directly attached (local) storage device; this means that in most cases the root or administrator user on the host OS is used to configure and initiate access. An iSCSI storage device (also known as an iSCSI target) has no way of knowing which user on the host system is requesting access to the storage; thus all user-level authentication and authorization for access to data within the LUN must be delegated to the host operating system. This is the same overall security model used by direct-attached or Fibre Channel SAN-attached storage.

The following iSCSI security methods can be configured on a filer. In some cases the iSCSI initiator may also have to be configured with security information.

1. LUN masking: Each LUN may have access to it restricted to a specified group of iSCSI initiators; Network Appliance refers to these initiator groups on the filer as *igroups*. LUN masking and igroups will be discussed in detail later in this paper.
2. Initiators and filers may be required to authenticate when establishing an iSCSI session using the Challenge Handshake Authentication Protocol (CHAP). CHAP and how it is implemented in the NetApp environment will be discussed in detail later in this paper.
3. IPSec may be used to encrypt authentication and data packets on the network.

It is advisable to configure a network topology that minimizes risk of unauthorized access to or modification of data as it traverses the network; one can accomplish this by use of direct cabling, switched network environments, virtual LANs (VLANs), and dedicated storage network interfaces when appropriate.

Finally, hosts that access iSCSI storage resources should be carefully configured, secured, and monitored for unauthorized access. If an attacker compromises an authorized iSCSI host system, there is nothing that the filer (or indeed, any storage system) can do to distinguish the attacker from an authorized user.

Product Overview

The NetApp iSCSI solution consists of

Network Appliance storage systems with iSCSI support*

Data ONTAP 6.4.5 or later

A host operating system supported* by NetApp with iSCSI, including Microsoft Windows 2000, Windows Server 2003, Linux , Solaris™, AIX, and Novell NetWare

An iSCSI initiator supported* by NetApp (software initiator with standard network interface card [NIC]), software initiator with TCP/IP offload engine (TOE) adapter card, or iSCSI host bus adapter (HBA) in the host system(s)

* Read the NetApp iSCSI initiator Support Matrix for up-to-date information about supported NetApp storage systems, initiators, and host operating systems:

http://now.netapp.com/NOW/knowledge/docs/san/fcp_iscsi_config.

NetApp iSCSI network implementation:

Application hosts are iSCSI initiators

Filers are iSCSI targets with storage devices

Two configurations are currently supported:

- Direct: single filer or cluster directly attached to one or more hosts
- Switched: single filer or cluster connected to one or more hosts through TCP/IP switched network

Security on Filer

There are two levels of security on filer; mandatory steps and recommended steps:

Mandatory steps:

1. License iSCSI on the filer.
   - `license add <iscsi license code>`
2. Start iSCSI on the filer.
   - `iscsi start`
3. Create igroup.

   Each iSCSI entity has an iSCSI node name. This is a logical name that is not directly linked to an IP address. Only targets and initiators are iSCSI entities. Switches, routers, and ports are TCP/IP devices only and do not have iSCSI node names. An initiator group, or igroup, is simply a group of node names used for access control.

   In most cases, igroups are used to apply consistent access controls to multiple iSCSI interfaces on the same host; thus each igroup typically is associated with a single host. Using igroups for other purposes is also possible. For example, a failover cluster of application servers might require the same iSCSI access for each node in the cluster.

   An iSCSI node name has the following format:

   ```
   iqn.yyyy-mm.backward_naming_authority:
   unique_device_name
   ```

`backward_naming_authority` is the reverse domain name of the entity responsible for naming this device. An example of reverse domain name is `com.netapp.`

`yyyy-mm` is the year and month in which the naming authority acquired the domain name.

`Unique_device_name` is a free-format unique name for the device assigned by the naming authority.

- `igroup create –i –t windows igroup-name [node-name]`

  Example: `igroup create –i –t windows my-igroup iqn.1992-08.com.netapp:my-host`

4. Create LUN.

- `lun create –s size –t windows lun_name`

When the LUN is first created, it is inaccessible by iSCSI clients because it is not yet mapped to an initiator group.

5. Map LUN to igroup.

- `lun map lun_name igroup_name [lun_ID]`

This step associates the target LUN with the igroup. All initiators listed in a particular igroup that is mapped to a particular LUN now have access to that LUN (provided all other security procedures are successfully met). This initiator → igroup → LUN combination is known as LUN masking. In simple terms, if an initiator is not listed in an igroup that is mapped to a LUN, that initiator is “masked out” and will not be able to access that LUN. In most cases each LUN will be mapped to a single igroup, but each igroup may be mapped to several LUNs.

Recommended steps:

The following recommended steps can be used to provide additional security.

1. On the filer disable the iSCSI *iswt* driver on network interfaces that you do not plan to operate in iSCSI mode.

- `iswt interface disable [-f ] {-a / <interface>…}`

  The iSCSI `iswt` driver is disabled for specified interfaces or all interfaces if `–a` is specified.

The process of disabling an interface requires termination of any iSCSI sessions currently using that interface. If outstanding iSCSI sessions exist on an interface to be disabled, the command displays a message to notify the administrator and prompt for confirmation prior to proceeding with the disable. The `-f` option forces termination of any outstanding sessions without prompting for confirmation.

- `iswt interface enable {-a / <interface>…}`

  The iSCSI `iswt` driver is enabled for a specified interface or for all interfaces if `-a` is specified.

The Data ONTAP `iswt` driver is a software-only target implementation of the iSCSI protocol, which allows the filer to be accessed as an iSCSI target device over the filer's standard network interfaces. The `iswt` driver allows the filer to be accessed as an iSCSI target device over the filer's standard network interfaces. The `iswt` interface command allows the administrator to control which network interfaces may be used for iSCSI connectivity. For example, an administrator may wish to configure a filer to support iSCSI access only through the filer's Gigabit Ethernet interfaces.

When the iSCSI service is enabled and the `iswt` adapter is online via the iSCSI command, the `iswt` driver supports iSCSI access over those network interfaces enabled for its use via the `iswt` interface command, but not over disabled interfaces. When the iSCSI service is stopped or the `iswt` adapter is offline, the `iswt` driver does not allow iSCSI access over any interface, regardless of its enable/disable state.

Once disabled, the `iswt` driver rejects subsequent attempts to establish new iSCSI sessions over that interface.

In a cluster configuration `iswt` driver supports two separate logical "adapters," `iswta` and `iswtb`. The `iswta` logical adapter is dedicated to local host traffic, and supports iSCSI sessions over all of the filer's local host standard network interfaces. The `iswtb` adapter is dedicated to partner host traffic, and is online only when the filer is operating in takeover mode.

- `iswt session show [-v] <adapter> [<session_num>]`

Show status of one session or for all connections associated with a specified `adapter` if no `session number` is specified. If the `-v` option is specified, the output is verbose.

2. On the filer, change the default security (authentication) method to `deny`.

When an initiator and target attempt to establish an iSCSI session, during the initial link establishment phase, the initiator sends a login request to the filer. The filer permits or denies the login request according to one of the following security methods:

- `none` The filer does not require authentication for the initiator to establish a session. Even though a session can be established, LUN masking still applies. If the initiator is not listed in any igroups, it cannot access any LUNS on the filer. If the initiator belongs to an igroup, but a LUN is not mapped to that igroup, the initiator cannot access a LUN even though the initiator is listed in an igroup. If the initiator is in one or more igroups on the filer, it can access only the LUNs mapped to the igroups in which it belongs.

- `deny` The initiator is denied access to the filer. No session will be established between the initiator and the filer regardless of igroup membership.
- `CHAP` When this security method is configured CHAP is used when establishing a session between the filer and initiator. It provides encrypted authentication protection. There are two CHAP configurations available. Option one is known as one-way CHAP authentication, where the filer requests CHAP authentication from the initiator only. Option two is known as bidirectional (mutual) CHAP authentication, because the filer requests CHAP authentication from the initiator, and the initiator requests CHAP authentication from the filer.

You can define a list of initiators and their security methods. You can also define a default security method for initiators that are not on this list. If you do not specify a list of initiators and security methods, the default security method is `none`—any initiator can access the filer without CHAP authentication.

To ensure that only authorized initiators access resources on the filer, first change the default security method to `deny.` All initiators in the list of initiators are not affected by this command. They will behave based on their individual security method setting which is set on a per initiator basis. All initiators *not* in the list of initiators will be unable to establish a session with the filer as a result of the default security method being set to `deny.`

- `iscsi security default –s deny`

After setting the default security method to `deny,` individual initiators can have their security methods set to either `none` or `CHAP.`

To allow an initiator to establish a session without authentication, specify the `none` security method.

- `iscsi security add –i` *`initiator`* `–s none`

For additional security specify the `CHAP` security method for an initiator. The CHAP security method requires additional credentials: a username and a password (secret) in the case of one-way CHAP.

- `iscsi security add –i` *`initiator`* `–s CHAP –p` *`password`* `–n` *`name`*

`initiator` is the iSCSI node name.

`password/secret` is the inbound password

`inname` is the inbound CHAP username.

In the case of bidirectional (mutual) CHAP both inbound and outbound usernames and passwords must be specified. The inbound and outbound CHAP passwords must be different.

- `iscsi security add –i` *`initiator`* `–s CHAP –p` *`inpassword`* `–n` *`inname`* `–o` *`outpassword`* `–n` *`outname`*

  `initiator` is the iSCSI node name.

  `inpassword/secret` is the inbound password from the initiator.

  `inname` is the inbound CHAP username from the initiator.

  `outpassword/secret` is the outbound password to the initiator.

  `outname` is the outbound CHAP username to the initiator.

While it is possible to use the same username and password for each initiator, the best security is provided if each initiator uses a different username and password. One exception to this rule is that initiators within the same igroup (especially those on a single host) should often share a username and password.

Username and password rules for Data ONTAP:

`username` supports a case-sensitive username from 1 to 128 characters in length. The value cannot be `NULL`.

`password/secret` supports a case-sensitive password/secret from 1 to 512 characters in length. The password/secret can be in ASCII format or in hexadecimal format prefixed with `0x` or `0X`. The value cannot be *`NULL`*.

Data ONTAP includes a command you can use to generate random iSCSI passwords for use with CHAP authentication:

- `iscsi security generate`

This command will automatically generate a 128-bit random CHAP password/secret in hexadecimal format (beginning with `0x`) that you can cut and paste to use in the `iscsi security add` command. ASCII passwords can not be generated with this command.

Example: `0x8d5bda24e198b07b381b050721fd3d60`

When assigning CHAP passwords to initiators, it is important to record the passwords for use when configuring the iSCSI host systems. The username and password used on the filer must match those used on the host initiator(s). Also note that each initiator vendor may have different rules about usernames and passwords.

Security on Network

When deploying storage network technology, it is common to create a private network dedicated exclusively to storage traffic. This has performance benefits as well as security benefits. When using a FCP infrastructure, this is the default configuration because FCP networks are not suitable for nonstorage network traffic. Even when using file access protocols such as NFS or CIFS, which operate over IP, it is common to create an IP storage area network (IP SAN) to segregate the storage traffic from the “normal” IP traffic.

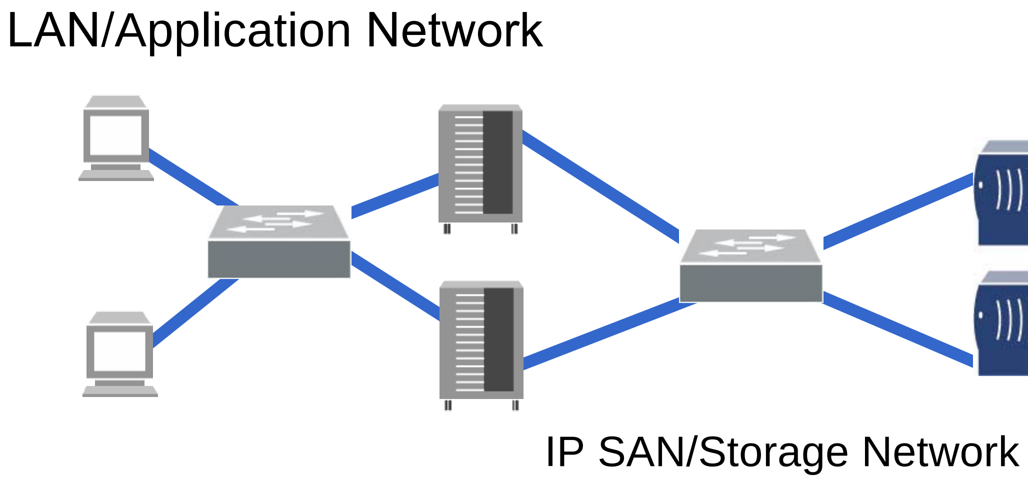

Figure 1) iSCSI IP SAN architecture.

Figure 1 shows the most common architecture for iSCSI deployments, which uses a dedicated storage network for iSCSI traffic, shared among multiple application servers and storage systems. This architecture provides good performance and security at a reasonable cost. An attacker cannot compromise the storage systems in this architecture without first gaining control of one of the application server hosts.

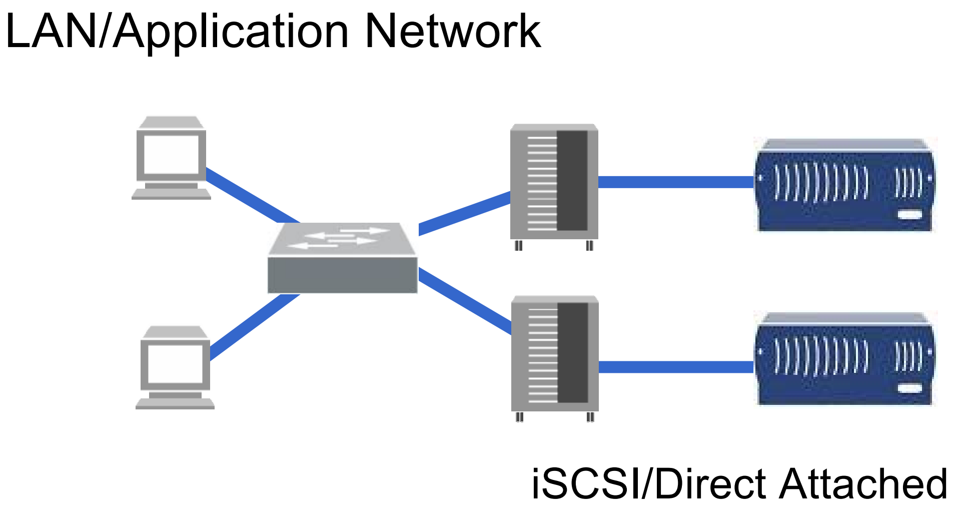

Figure 2) iSCSI direct-attached architecture.

Figure 2 illustrates another option with application server hosts directly connected to storage systems without a shared switch. This architecture provides equivalent performance to the IP SAN architecture, but may improve security if you are concerned about application servers communicating with each other over the back-end storage network. This effectively reduces the security problem to the same set of threats as in a direct-attached storage scenario, and it is the best option when you have multiple application servers in different security zones that need to share a physical storage device but should not have access to each other’s data. The increased security of this solution comes at the cost of installing and managing additional network interfaces.

Security on Host

During the configuration of HBA cards, the IP addresses of target filers are added. This step restricts the target filers that are visible to the host. One or more target filers can be associated with each HBA card. Once filer target IP addresses are added to HBA card, the status of the available targets can be checked by double-clicking the adapter IP address.

Conclusion

iSCSI can provide significant benefits by providing networked block-based storage over standard IP infrastructures, reducing the cost and complexity of SAN deployments. However, it is important to enforce access restrictions on storage resources. Both the iSCSI protocol and the NetApp implementation provide security mechanisms that can protect iSCSI data from unauthorized access and modification. With correct configuration, one can provide the benefits of an iSCSI SAN without compromising on security.

NetApp®

Network Appliance, Inc.
495 East Java Drive
Sunnyvale, CA 94089
www.netapp.com