FUJITSU

FUJITSU Storage ETERNUS DX series and ETERNUS AF series
ETERNUS SF AdvancedCopy Manager
Guide for Secure File Transfers Using the Storage Function

Using the ETERNUS DX series or the ETERNUS AF series in combination with ETERNUS SF AdvancedCopy Manager provides an easy way to transfer files between systems that are not network-connected.

Table of Contents

Preface

Attacks that exploit system vulnerabilities, including the leaking of personal information handled by companies, falsification, or damage to systems by viruses, have become a major problem in recent years, having resulted in large compensation payouts and reputational damage to companies. To protect their data and systems, companies need to adopt better security measures.

One such security measure is a combination of network isolation, virus protection, file sanitization, and measures to protect the intranet against unauthorized access and information leaks. Using the ETERNUS DX series or the ETERNUS AF series with ETERNUS SF AdvancedCopy Manager provides secure file transfers between the intranet and internet-connected networks without the use of a LAN. This reduces the risk of intrusions into the intranet or information leaking out from the intranet.

This document describes how the ETERNUS DX series or the ETERNUS AF series is used with ETERNUS SF AdvancedCopy Manager to transfer files, and compares this method with other file transfer methods. It also describes the system configuration for file transfers using ETERNUS SF AdvancedCopy Manager with the ETERNUS DX series or the ETERNUS AF series.

Prerequisites

The product lineup and product information stated in this document are current as of April 2017.

Target Readers

This document is intended for readers who are considering security measures for new systems or for readers who are considering improvements to the security of existing systems.

Abbreviations

This document uses the following abbreviations.

- FUJITSU Storage ETERNUS DX series/AF series	ETERNUS DX/AF
- ETERNUS SF AdvancedCopy Manager Copy Control Module	ETERNUS SF AdvancedCopy Manager CCM

1. What is a Secure File Transfer?

One approach that is attracting attention for protecting intranets from the risks of targeted attacks and information leaks is to prevent direct internet access by isolating the intranet from networks able to connect to the internet. Generally, when an intranet is isolated, the remote desktop function is used to provide internet access by connecting intranet user terminals to an internet-connected virtual terminal.

There are times when user terminals may have to exchange files with web sites or cloud-based systems. When such files are received, the file is downloaded from the internet using the virtual terminal and is then transferred to the intranet. When a file is sent to the internet, it is first transferred to the internet-connected network and then uploaded to the internet site.

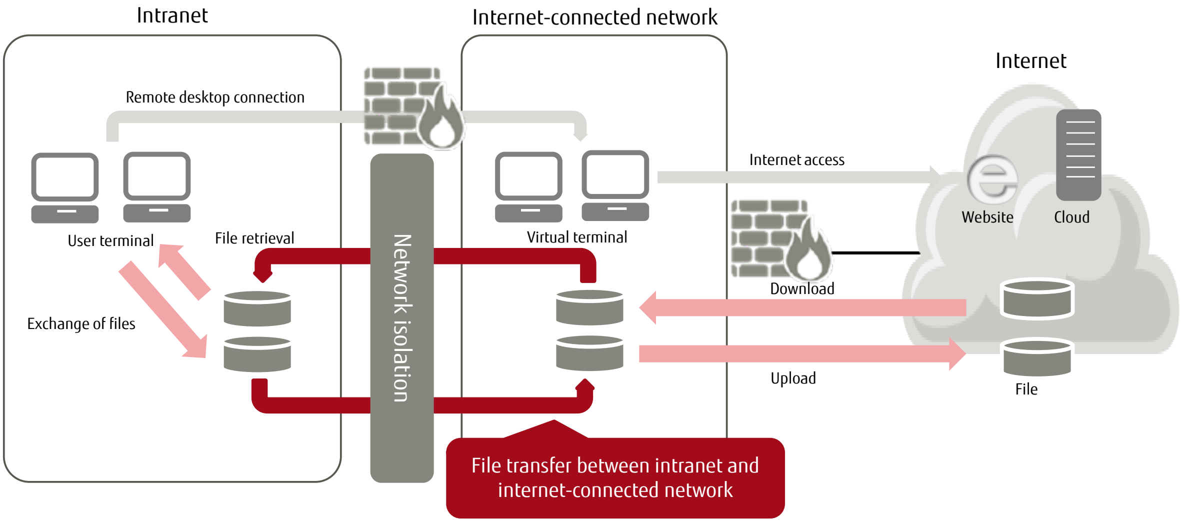


Figure-1 File transfer between the intranet and the internet-connected network

To protect the intranet, measures need to be taken to prevent information leaks or other unauthorized access via the file transfer pathway. This document describes how to transfer files securely between the intranet and internet-connected networks.

2. Comparison of File Transfer Methods

Along with transfer via a LAN or removable storage, files can also be transferred between an intranet and internet-connected network via the storage system. This section compares the following three methods in terms of security, cost, and convenience.

(1) File transfer via LAN
The intranet and internet-connected network are linked via a LAN and a communication protocol is used to transfer files.

(2) File transfer via removable storage
There is no link between the intranet and internet-connected network and instead a removable storage medium is used to transfer files. Example media include USB memory and magnetic tape.

(3) File transfer via storage system
A storage system is attached to both the intranet and internet-connected network and its copy function is used to transfer files between the two environments. This can be done using NAS or by using a SAN to link servers and storage (link file servers to block storage systems such as the ETERNUS DX/AF).

2.1. File Transfer via LAN

This involves linking the intranet and internet via a LAN and using a communication protocol to transfer files via file transfer servers or other file sharing servers. Various file transfer software or other file sharing software can be installed in both the source and destination systems as required. Because these software products communicate with each other at the application level, they can deliver an extensive array of functions such as notification, approval workflow, user authentication, delivery confirmation, and logging in addition to realtime interoperation at the level of individual files.

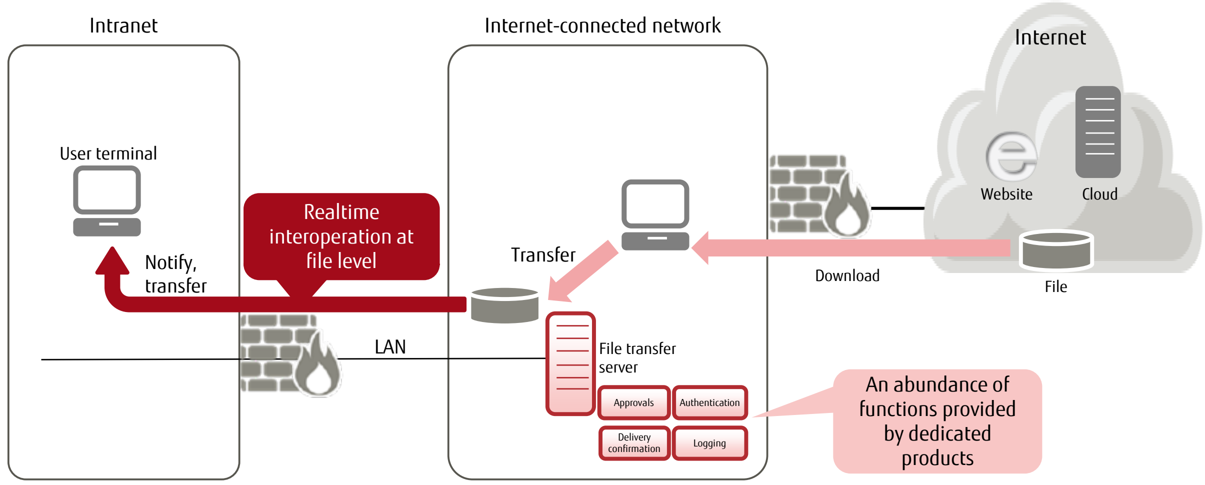


Figure-2 File transfer via LAN

Use of a firewall for access control between the intranet and internet-connected network is essential when a LAN is used to transfer files. Because firewalls require open ports for communication, there is a risk that these open ports will be used for intrusions into the intranet or for leaking information out from the intranet.

When files are transferred via a LAN, the same method can be adopted when transferring files from the intranet to the internet.

2.2. File Transfer via Removable Storage

This means using removable media such as USB memory, CD, DVD, or magnetic tape to transfer files. This is the cheapest way to transfer files between systems that have no network connection to each other. Unfortunately, it is not very convenient because of the time it takes to store data in and retrieve data from the storage media as well as the need to physically carry the media. Moreover, being a manual process, there is a risk of theft or loss.

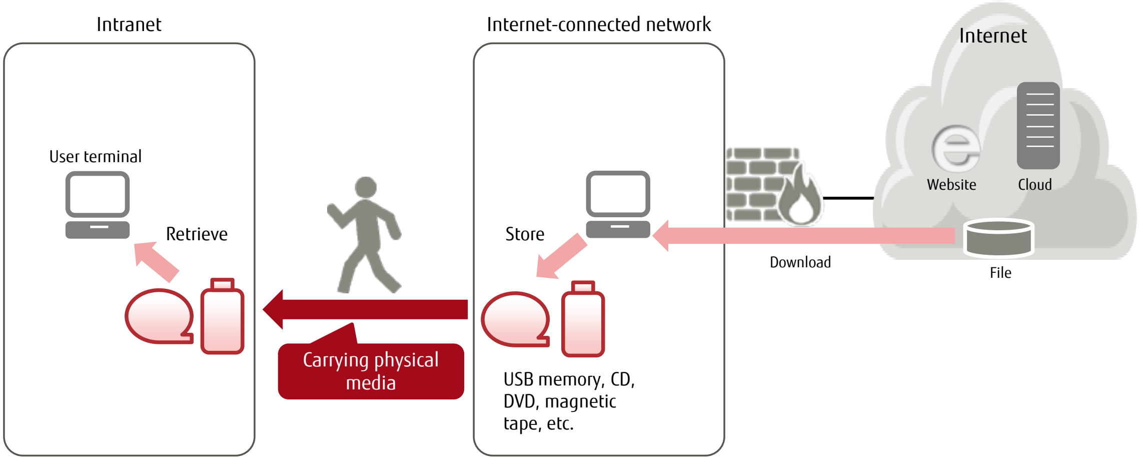


Figure-3 File transfer via removable storage

2.3. File Transfer via Storage System

This means having a storage system that is attached to both the intranet and internet-connected network, and using its volume copy function to transfer between the two environments. This has the same convenience as using a single file sharing server. Because the intranet is fully isolated from the internet-connected network, there is no need to use a firewall for access control of the file transfer pathway. This method can be done using either NAS or a SAN.

2.3.1. File Transfer via NAS

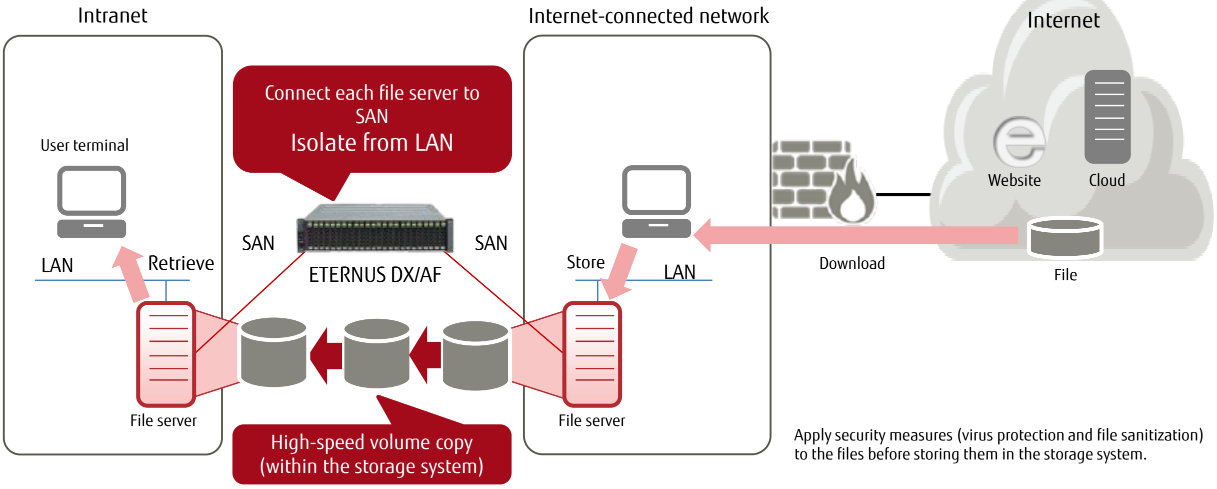
This involves configuring a single NAS device to have separate environments and storage volumes that are accessible to the internet-connected network and intranet respectively, such that files can be transferred by copying these volumes in their entirety. While there is no risk of information being leaked via the transfer pathway (because the LAN between the intranet and the internet-connected network is isolated by the NAS device, and because the data in a volume is copied one-way), further consideration is needed to prevent unauthorized access because the terminals and the NAS device are still connected via the LAN.

2.3.2. File Transfer via SAN

This involves configuring a SAN by connecting two file servers (one for each environment) to a single ETERNUS DX/AF, and providing each file server with a file storage volume and a buffer volume to use for file transfers. It transfers files at the volume level by using the storage system functions to perform copies from one volume to another at high speed (within the storage system). Because the data in a volume is copied one-way via the buffer volume, the existence of the intranet volumes is not visible to the internet-connected network.

Moreover, using a SAN means that the respective LANs and the ETERNUS DX/AF are isolated, thereby preventing access to the storage system from the terminals. If the SAN also includes other servers and storage, host affinity can be used to prevent access to the volumes from the other servers.

Using the ETERNUS DX/AF together with file servers to implement file transfers provides the best protection against unauthorized access from the network.



Apply security measures (virus protection and file sanitization) to the files before storing them in the storage system.

Figure-4 File transfer using the ETERNUS DX/AF together with file servers

Using the ETERNUS DX/AF together with file servers also provides flexibility in file server use because it does not restrict the choice of which software they can run. For example, users can choose whichever product they want for virus protection or sanitizing incoming files, depending on their security requirements.

When files are transferred via a SAN, the same method can be adopted when transferring files from the intranet to the internet.
If files need to be retrieved from the intranet, a file checker should be used as protection against information leakage.

2.4. Comparison of Different Methods

The table below compares the different file transfer methods.

Category	LAN	Removable media	NAS	SAN
Security	Fair The risk of unauthorized access or information leak via communication ports remains because both environments are part of the same physical network.	Fair The risk of information leak or theft remains because files are transferred manually.	Good File transfers are one-way. Although the networks are isolated from each other by the NAS device, the risk of unauthorized access to the NAS device remains.	Best File transfers are one-way. The destination volumes are hidden by the buffer volumes. This option has the lowest risk of unauthorized access because the networks are isolated from each other by the SAN.
Installation cost	Good Easy to install products selected for the functions they provide. While use of a LAN means networking costs are low, a firewall must be configured.	Best Removable media are cheap, making this the lowest cost option.	Fair Incurs the cost of installing a NAS device.	Fair Incurs the cost of installing the ETERNUS DX/AF as well as file servers.
Operating cost	Good In addition to managing the file transfer software, user administration and firewall maintenance are required.	Fair Numerous costs associated with human involvement in transferring files and managing removable media.	Best A NAS device requires administration. No network product maintenance is required.	Best The ETERNUS DX/AF and file servers require administration. No network product maintenance is required.
User convenience	Best Realtime interoperation at the level of individual files. File transfer software and file sharing software can provide functions as required for individual users and files, such as arrival notification, delivery confirmation, and approvals workflow.	Fair Saving to media, physical transfer, and retrieval all take time.	Good Files are transferred at the volume level. While it provides the same level of convenience as a file sharing server, notifications and copy functions that are linked with file storing are not available.	Good Files are transferred at the volume level. While it provides the same level of convenience as a file sharing server, notifications and copy functions that are linked with file storing are not available.

Table-1 Comparison of different file transfer methods

Although using a SAN costs more than using a LAN, it minimizes the risk of unauthorized access or information leaks via the network, and provides same level of user convenience as a file sharing server. It is suitable for systems that place a high priority on intranet security.

3. File Transfers Using the ETERNUS DX/AF

This chapter describes the configuration when the ETERNUS DX/AF is used together with file servers and ETERNUS SF AdvancedCopy Manager CCM for file transfers via a SAN, and how files are transferred using the copy function of ETERNUS SF AdvancedCopy Manager CCM.

3.1. Configuration

The following sections describe the hardware, network, and software configurations for the ETERNUS DX/AF and the file servers, and the volume configuration used for the file transfers.

3.1.1. Hardware and Network Configuration

This assumes a single ETERNUS DX/AF and two PRIMERGY file servers. The file servers are connected to the intranet and internet-connected network respectively, and the storage system is located either between the two networks or in the intranet.

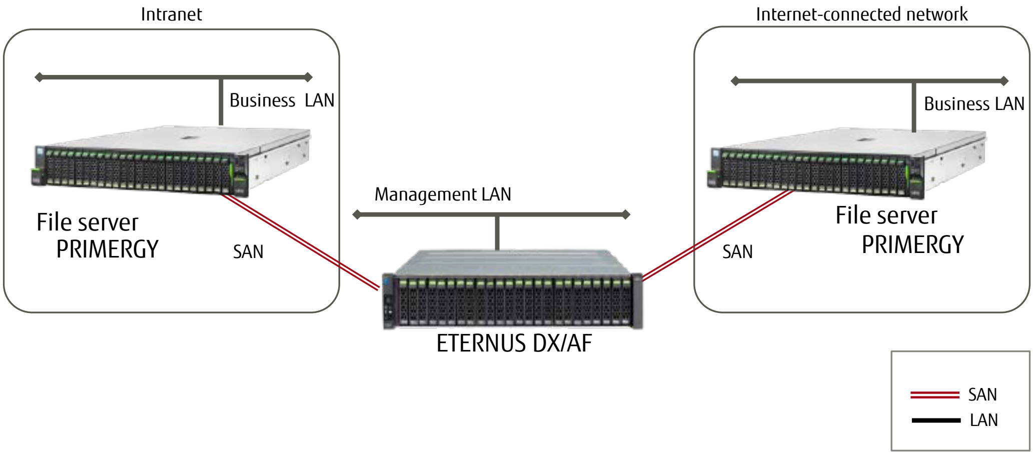


Figure-5 Hardware and network configuration

The SAN that links the file servers and the storage system uses FC or iSCSI. Each file server is connected to its associated business LAN. The ETERNUS DX/AF is connected to a management LAN for storage administration and monitoring. This management LAN can be either a dedicated LAN or the intranet.

3.1.2. Software Configuration

The file servers run on either the Windows Server or Linux OS. ETERNUS SF AdvancedCopy Manager CCM is installed on the intranet file server, and volume copying is controlled from the intranet side. ETERNUS SF AdvancedCopy Manager CCM is a backup tool provided by ETERNUS SF AdvancedCopy Manager. This tool uses the Advanced Copy function of the SAN-connected ETERNUS DX/AF. The figure below shows a software implementation.

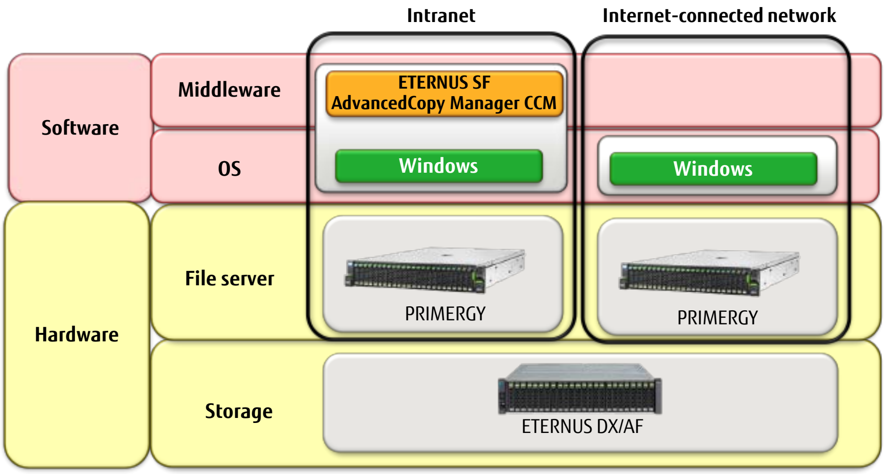


Figure-6 Software implementation

The following license is required to use the Advanced Copy function with ETERNUS SF AdvancedCopy Manager CCM.

- ETERNUS SF AdvancedCopy Manager V16 Local Copy License

3.1.3. Volume Configuration

Files are transferred using three logical volumes of equal size (source volume, buffer volume, and destination volume). In addition to the file transfer volumes, a volume is also required for ETERNUS SF AdvancedCopy Manager CCM to issue the copy instruction. Allocate the volumes in the ETERNUS DX/AF as a Standard Volume or Thin Provisioning Volume (TPV).

Register the volumes in the affinity groups for their respective servers to prohibit access from other servers. Connect the source volume to the internet-connected file server and connect the destination and CCM volumes to the intranet file server. Do not connect the buffer volume to either server.

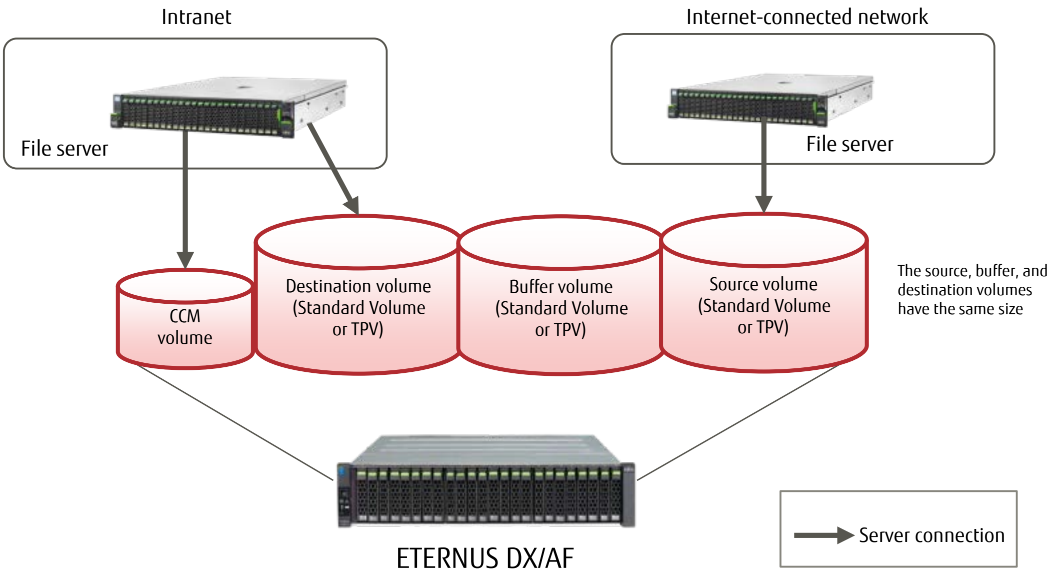

Intranet
File server
Internet-connected network
File server
CCM volume
Destination volume (Standard Volume or TPV)
Buffer volume (Standard Volume or TPV)
Source volume (Standard Volume or TPV)
The source, buffer, and destination volumes have the same size
ETERNUS DX/AF
Server connection

Figure-7 Volume configuration

3.2. File Transfer Using ETERNUS SF AdvancedCopy Manager CCM

For file transfers, ETERNUS SF AdvancedCopy Manager CCM combines different types of logical volume copies with the Advanced Copy function of the ETERNUS DX/AF. First a synchronous high-speed equivalent copy (EC) is executed from the source volume to the buffer volume. Then, a differential copy is executed from the buffer volume to the destination volume by using the high-speed snapshot copy (QuickOPC).

Because a logical volume copy transfers the entire file system, the destination volume ends up with the same directory structure as the source volume. In the same way as when using a single file server, the intranet computer can retrieve the file from the directory in which it was saved on the internet-connected network.

The figure below shows a schematic of how ETERNUS SF AdvancedCopy Manager CCM is used to transfer a file from the internet to an intranet.

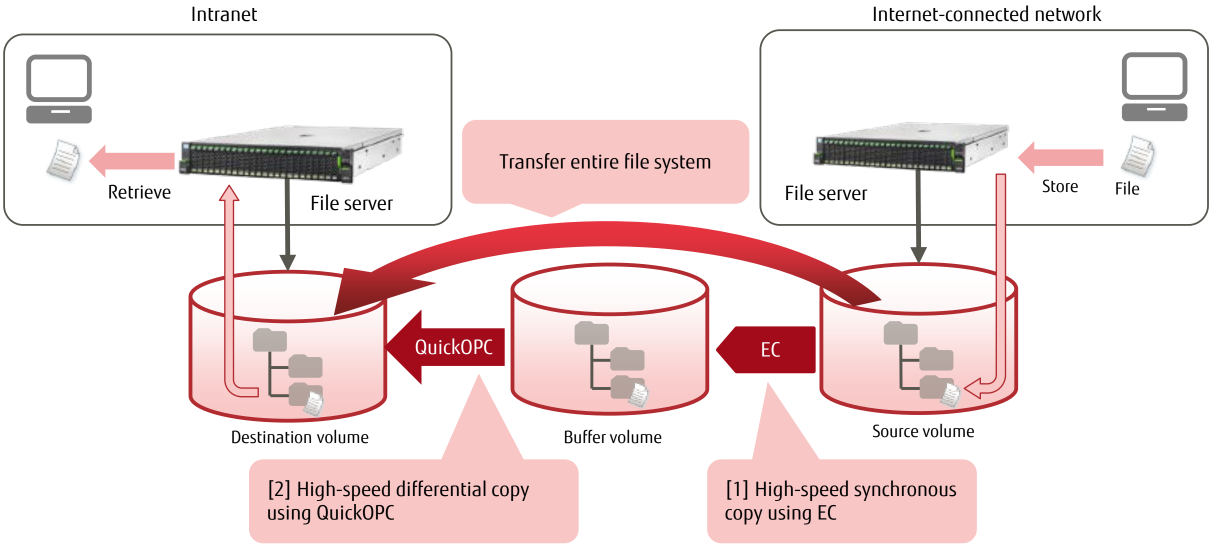

Intranet
Internet-connected network
Retrieve
File server
Transfer entire file system
File server
Store
File
QuickOPC
EC
Destination volume
Buffer volume
Source volume
[2] High-speed differential copy using QuickOPC
[1] High-speed synchronous copy using EC

Figure-8 File transfer using ETERNUS SF AdvancedCopy Manager CCM

Once the synchronous high-speed equivalent copy (EC) has been used to transfer the entire source volume, the source and buffer volumes maintain an equivalent state. With this equivalency having been established, the EC is then suspended to allow the high-speed snapshot copy (QuickOPC) to copy data from the buffer volume to the destination volume.

When the QuickOPC is complete, EC resumes to restore consistency between the source and buffer volumes.

By combining the synchronous high-speed equivalent copy (EC) and high-speed snapshot copy (QuickOPC), the time taken for copying is reduced and data can be coordinated at a specific time. Moreover, in the event of data in the source volume being lost, the volume can be restored in its entirety from the destination volume.

Because QuickOPC overwrites the entire file system of the destination volume, the intranet file server must temporarily unmount the drive to which the volume is assigned before QuickOPC is started and then remounted after completion.

The same procedure is used to transfer files from the intranet to the internet, but diffident volumes are used.

4. Summary

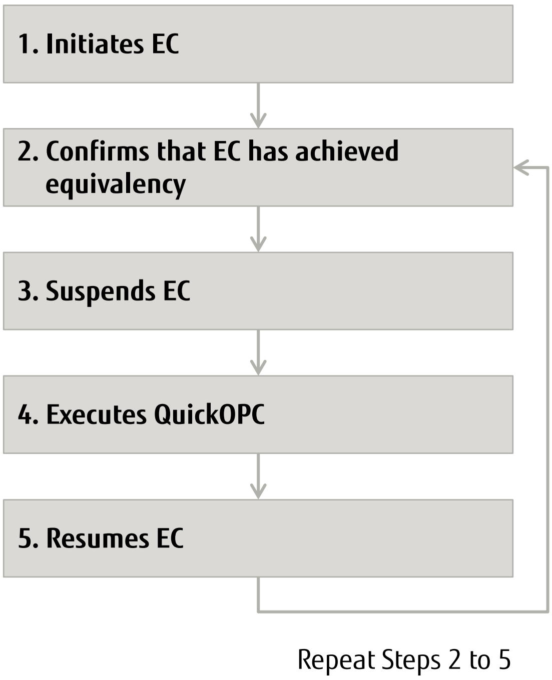
Use of the ETERNUS DX/AF with ETERNUS SF AdvancedCopy Manager enables secure file transfers between an internet-connected network and an intranet.

By fully isolating the intranet from internet-connected networks, the intranet is protected from the threat of unauthorized access or information leaks via file transfer pathways. The use of a SAN for storage access prevents unauthorized access via the LAN.

The ETERNUS DX/AF is ideal for secure file transfers between internet-connected networks and an intranet.

Appendix Operation Flowchart

The flowchart below shows how ETERNUS SF AdvancedCopy Manager CCM transfers files.



EC is started by a CCM command. Copying starts from the source volume to the buffer volume.

An equivalent state between the source volume and the buffer volume is confirmed by a CCM command.

EC is suspended by a CCM command to prevent further changes to the buffer volume.

QuickOPC is executed by a CCM command to perform a differential* copy from the buffer volume to the destination volume.
The destination volume is unmounted before QuickOPC is started and then remounted after completion.

EC is resumed by a CCM command.

* For the second and subsequent copies. A full copy is only performed for the initial copy.

Figure-9 Operation flowchart for ETERNUS SF AdvancedCopy Manager CCM

The sequence of operations shown in Figure-9 can be automated using a script. Files written to the source volume after Step 3 (Suspends EC) are available in the destination volume after Step 4 (Executes QuickOPC) of the next iteration.

Contact
FUJITSU Limited
Website: http://www.fujitsu.com/eternus/

■Disclaimer
FUJITSU Limited is not responsible indemnity that might be caused by the contents in this documentation or any damage related to contents in this documentation.