Serv-U® Distributed Architecture Guide

Horizontal Scaling and Application Tiering for High Availability, Security, and Performance

Introduction

Serv-U is a high-performance secure file transfer server for Windows and Linux. It supports FTP, FTPS (SSL/TLS), SFTP (SSH), HTTP, and HTTPS connections, and includes optimized interfaces for web browsers and mobile devices (e.g., iPad, iPhone, BlackBerry, Android, and Kindle Fire).

To support stringent redundancy, security, and performance requirements Serv-U supports both multi-tier and high availability architectures. This document describes Serv-U's support for these distributed architectures and their relative advantages and disadvantages.

"No Data in DMZ" for Managed File Transfer

A multi-tier Serv-U / Serv-U Gateway deployment allows you to meet a common managed file transfer requirement: "never store data at rest in a DMZ."

Our Serv-U Gateway safely proxies incoming connections from the Internet to your Serv-U server without opening any connections from the Internet or your DMZ segment into your trusted networked.

High Availability through Horizontal Scaling

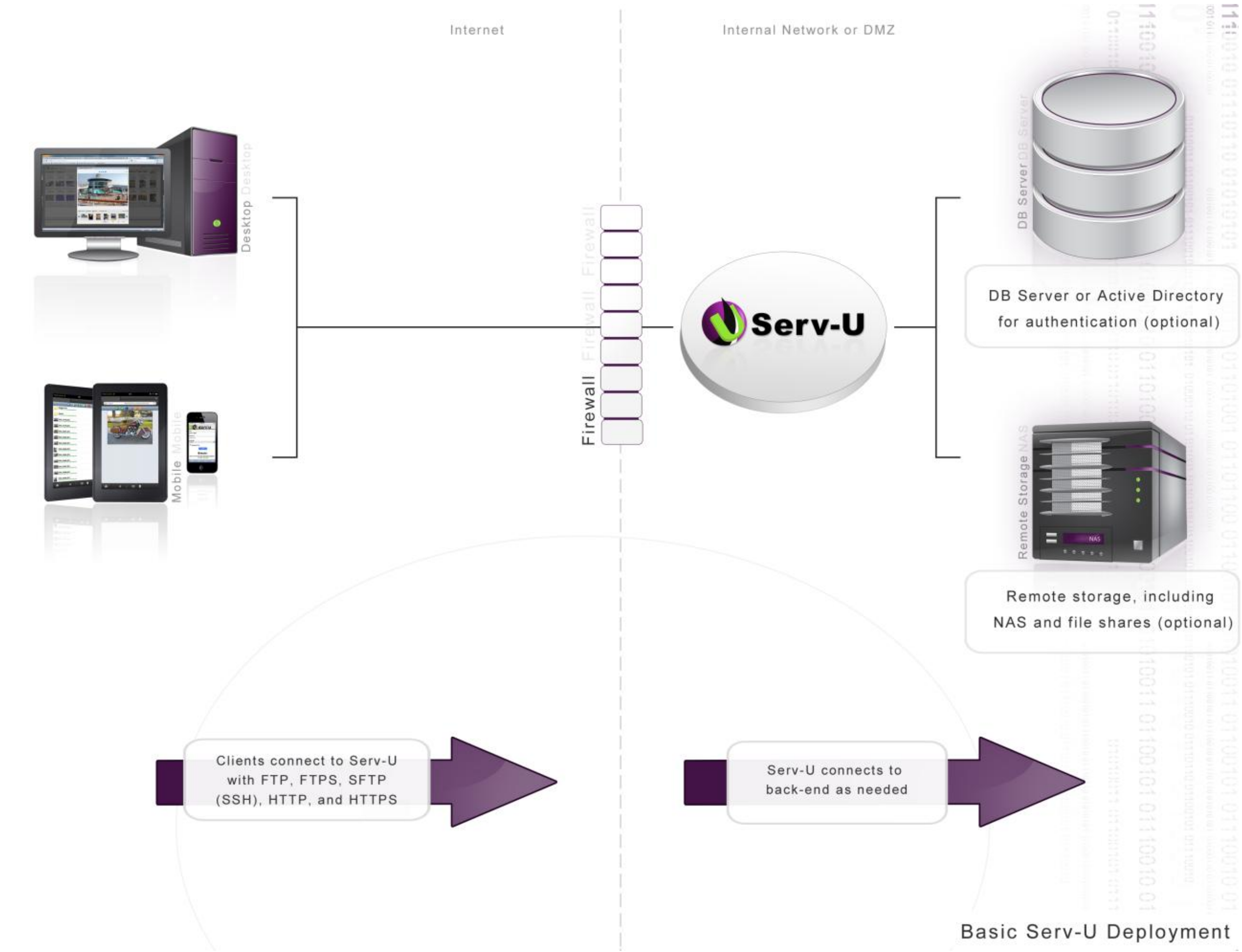
Both our core Serv-U server and our Serv-U Gateway can be deployed in "N+1" configurations to achieve high availability through horizontal scaling. This allows you to avoid single points of failure or scale up to meet your needs.

Table of Contents

Basic Deployment

When Serv-U is deployed as a standalone server it is typically protected from the Internet by a single firewall. It may be connected to remote storage or remote authentication sources.

All editions of Serv-U (Bronze, Silver, Gold and Platinum) may be deployed in this architecture, but only Serv-U Gold and Serv-U Platinum may leverage external authentication sources.


Internet
Internal Network or DMZ
Desktop
Mobile
Firewall
Serv-U
DB Server
DB Server or Active Directory for authentication (optional)
Remote Storage
Remote storage, including NAS and file shares (optional)
Clients connect to Serv-U with FTP, FTPS, SFTP (SSH), HTTP, and HTTPS
Serv-U connects to back-end as needed
Basic Serv-U Deployment

Firewall Configuration:

The primary firewall supports FTP, FTPS (SSL/TLS), SFTP (SSH), HTTP, and/or HTTPS inbound connections from the Internet into Serv-U. This firewall may also be configured to allow outbound connections for support FTP/S active mode data connections, or may be "FTP aware" enough to open FTP data channels dynamically.

Variations:

- If Serv-U accesses remote storage (e.g., NAS or file shares), then Serv-U must be able to make a CIFS (Windows networking) connection to those resources.

- If Serv-U accesses an ODBC-compliant database for remote authentication, then Serv-U must be able to make a database-appropriate connection to that database. For example, SQL Server connections are often made over TCP port 1433.
- If Serv-U accesses Active Directory ("AD") for remote authentication, then your Serv-U server must be part of the AD domain and on the same network segment.

Advantages:

- Easiest configuration to set up. (This configuration is recommended during functional evaluation of Serv-U software.)

Disadvantages:

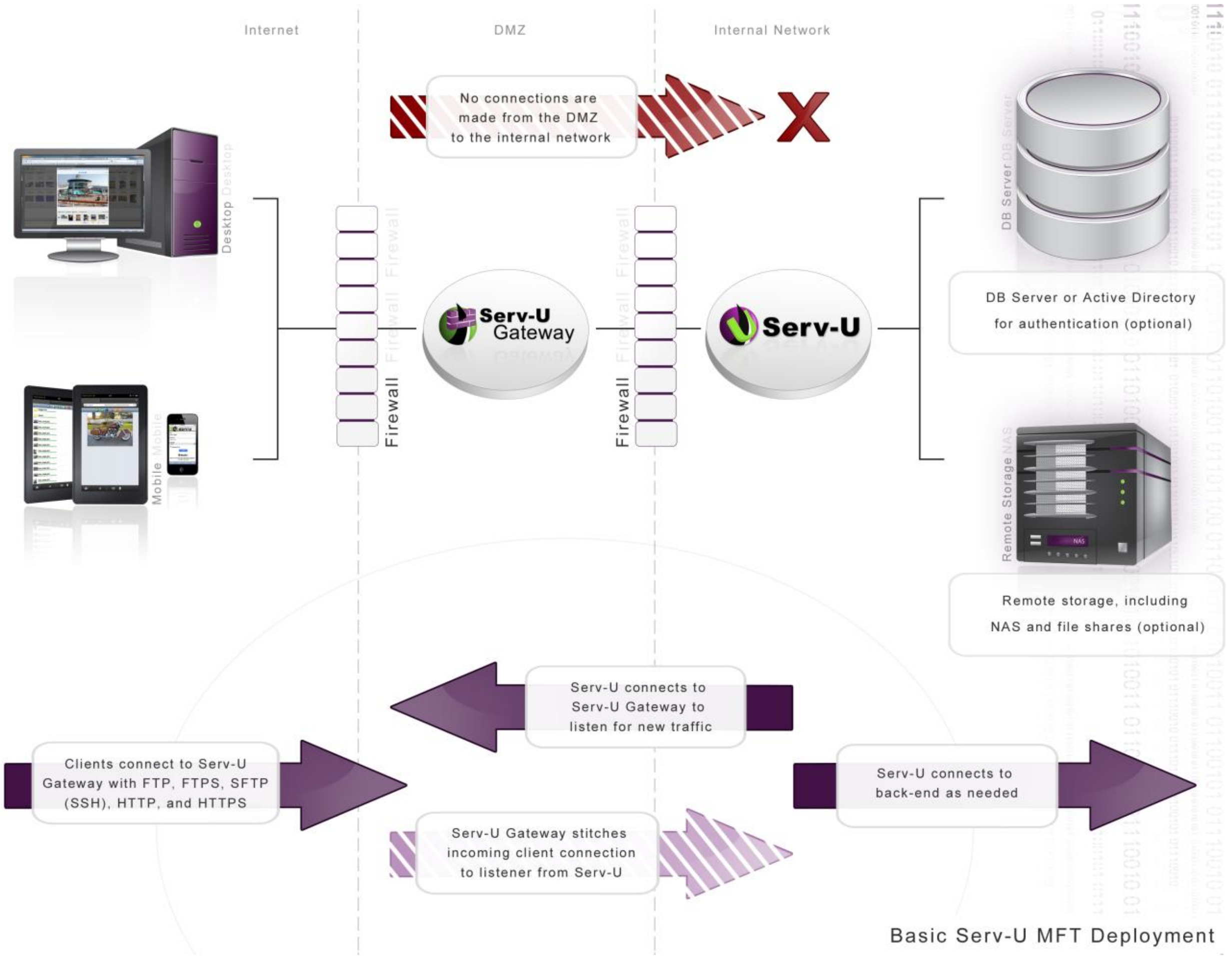
- No active redundancy means the Serv-U server is a single point of failure.
- Direct connections from Serv-U to internal storage, internal databases, or Active Directory domain controllers are not permitted by many security policies.

Basic Multi-Tier (MFT) Deployment

The Serv-U Gateway allows you to deploy Serv-U in a multi-tier architecture that meets or exceeds most managed file transfer ("MFT") security requirements. This architecture allows you to:

- Terminate all incoming transfer connections on a hardened server located in your DMZ segment
- Ensure no data is ever stored in your DMZ segment
- Avoid opening any inbound connections from your DMZ segment to the internal network

Serv-U Silver*, Serv-U Gold, and Serv-U Platinum may all be deployed in this architecture, but Serv-U Gold or Serv-U Platinum should be used if you support SFTP (SSH) or HTTPS transfers or plan to leverage external authentication sources.


Internet
DMZ
Internal Network
No connections are made from the DMZ to the internal network
X
Desktop
Mobile
Firewall
Firewall
Serv-U Gateway
Serv-U
DB Server
DB Server or Active Directory for authentication (optional)
Remote Storage
NAS
Remote storage, including NAS and file shares (optional)
Serv-U connects to Serv-U Gateway to listen for new traffic
Clients connect to Serv-U Gateway with FTP, FTPS, SFTP (SSH), HTTP, and HTTPS
Serv-U connects to back-end as needed
Serv-U Gateway stitches incoming client connection to listener from Serv-U
Basic Serv-U MFT Deployment

** Technically, Serv-U Bronze can also be deployed in this architecture, but Serv-U Bronze does not support any secure protocols.*

Firewall Configuration:

The firewall between the Internet and the DMZ segment supports FTP, FTPS (SSL/TLS), SFTP (SSH), HTTP, and/or HTTPS inbound connections from the Internet into Serv-U. This firewall may also be configured to allow outbound connections for support FTP/S active mode data connections, or may be “FTP aware” enough to open FTP data channels dynamically.

The firewall between the DMZ segment and the internal network only needs to allow outbound connections from Serv-U to Serv-U Gateway over TCP port 1180.

Variations:

- If Serv-U accesses remote storage (e.g., NAS or file shares), then Serv-U must be able to make a CIFS (Windows networking) connection to those resources.
- If Serv-U accesses an ODBC-compliant database for remote authentication, then Serv-U must be able to make a database-appropriate connection to that database. For example, SQL Server connections are often made over TCP port 1433.
- If Serv-U accesses Active Directory (“AD”) for remote authentication, then your Serv-U server must be part of the AD domain and on the same network segment.
- The two firewalls represented in the diagram are really often “two legs” of a single firewall controlling access between multiple segments.
- Serv-U Gateway and Serv-U may be deployed on different operating systems. (e.g., your Internet-facing Serv-U Gateway can be deployed on Linux even if you have deployed your Serv-U server on Windows.)

Advantages:

- Still easy to set up. (Install Serv-U Gateway, define Serv-U Gateway, define Serv-U listeners, test, and go.)
- Completely satisfies MFT requirement that no data at rest exists in the DMZ.
- Satisfies most security policy requirements by ensuring direct connections to internal storage, internal databases, or Active Directory domain controllers are only made between computers on your trusted internal network.
- No CIFS, AD, or DB connections are ever made across a firewall.

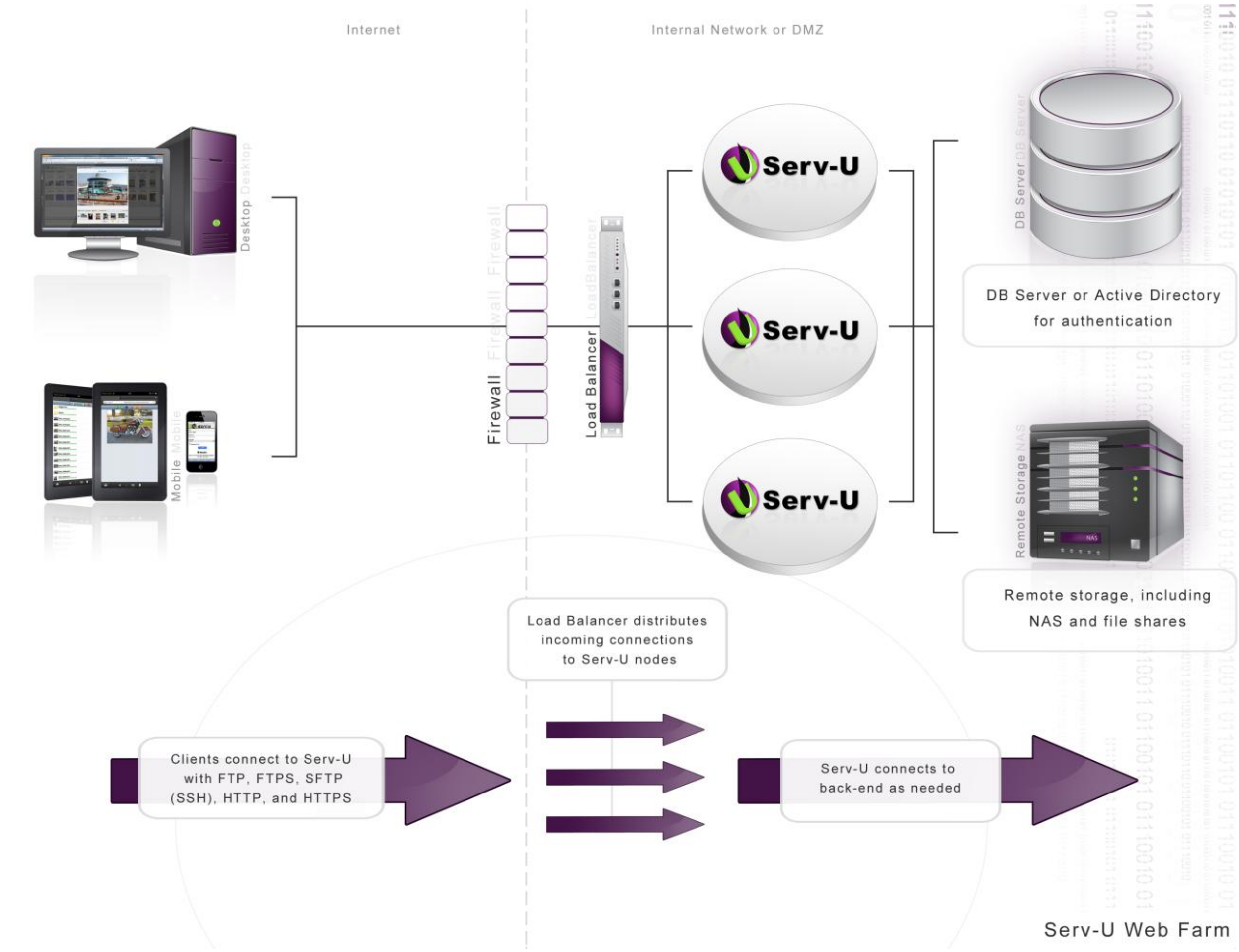
Disadvantages:

- No active redundancy means the Serv-U server and Serv-U Gateway are single points of failure.

Basic High-Availability (N+1) Deployment

Serv-U can be deployed as a web farm of application servers to provide highly available (“HA”) services through horizontal scaling (a.k.a. “N+1”).

Serv-U Gold and Serv-U Platinum are the only Serv-U editions that support HA deployments because Serv-U’s HA configuration requires the use of external authentication sources. Up to five Serv-U servers are currently allowed in this configuration.


Internet
Internal Network or DMZ
Desktop
Mobile
Firewall
Load Balancer
Serv-U
Serv-U
Serv-U
DB Server
DB Server or Active Directory for authentication
Remote Storage
Remote storage, including NAS and file shares
Load Balancer distributes incoming connections to Serv-U nodes
Clients connect to Serv-U with FTP, FTPS, SFTP (SSH), HTTP, and HTTPS
Serv-U connects to back-end as needed
Serv-U Web Farm

Firewall Configuration:

The primary firewall supports FTP, FTPS (SSL/TLS), SFTP (SSH), HTTP, and/or HTTPS inbound connections from the Internet into Serv-U. This firewall may also be configured to allow outbound connections for support FTP/S active mode data connections, or may be “FTP aware” enough to open FTP data channels dynamically.

Load Balancer:

A network load balancer must be used to distribute incoming connections to each Serv-U server.

Load balancers should be configured to preserve original IP addresses if you want to use Serv-U's IP lockout protection. Load balancers should also use "sticky sessions" that lock all incoming connections from a particular IP address to a specific Serv-U server to allow FTP and FTPS connections to work properly.

Remote Storage:

All user home folders, virtual folders and other Serv-U folders must be configured to use remote storage (e.g., NAS or file shares) rather than local hard drives. Serv-U must be able to make a CIFS (Windows networking) connection to those resources.

Remote Authentication:

All Serv-U domains must use remote authentication provided by an ODBC-compliant database or Microsoft Active Directory (AD).

- If Serv-U accesses an ODBC-compliant database for remote authentication, then Serv-U must be able to make a database-appropriate connection to that database. For example, SQL Server connections are often made over TCP port 1433.
- If Serv-U accesses Active Directory ("AD") for remote authentication, then your Serv-U server must be part of the AD domain and on the same network segment.

Variations:

- On Windows Server the built-in Windows Network Load Balancer service may be used instead of a physical load balancer.

Advantages:

- Active redundancy means that your Serv-U application servers are not single points of failure.

Disadvantages:

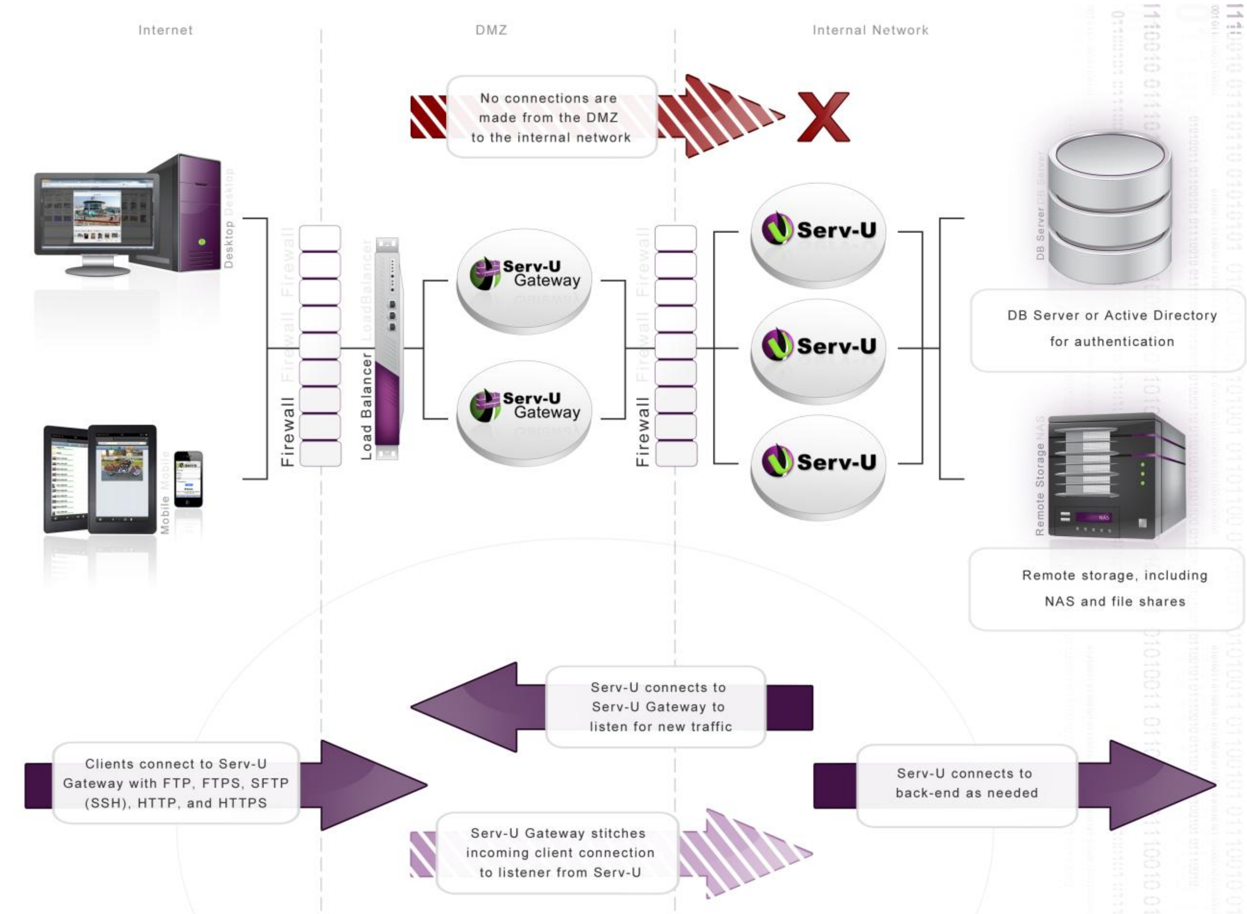
- More difficult to set up than single-node systems. (Must install Serv-U on each application server and point to the same shared resources.)
- Direct connections from Serv-U to internal storage, internal databases, or Active Directory domain controllers are not permitted by many security policies.
- Live user statistics may be unreliable for individual users who sign on to multiple servers simultaneously. (This can be partially mitigated for end user statistics – not group statistics - for end users who sign on from a single IP at a time via "sticky sessions" on your load balancer.)

Highly-Available Multi-Tier (MFT) Deployment

Serv-U can be deployed as a web farm of application servers to provide highly available (“HA”) services through horizontal scaling (a.k.a. “N+1”). It can also be deployed in a multi-tier architecture that meets or exceeds most managed file transfer (“MFT”) security requirements. Together, this sophisticated architecture allows you to:

- terminate all incoming transfer connections on a hardened server located in your DMZ segment
- ensure no data is ever stored in your DMZ segment
- avoid opening any inbound connections from your DMZ segment to the internal network
- avoid single points of failure
- scale up or down to meet actual demand

Serv-U Gold and Serv-U Platinum are the only Serv-U editions that support HA multi-tier deployments because Serv-U’s HA configuration requires the use of external authentication sources. Up to five Serv-U servers and three Serv-U Gateways are currently allowed in this configuration.


Internet
DMZ
Internal Network
No connections are made from the DMZ to the internal network
Desktop
Mobile
Firewall
Load Balancer
Serv-U Gateway
Serv-U Gateway
Firewall
Serv-U
Serv-U
Serv-U
DB Server
DB Server or Active Directory for authentication
Remote Storage NAS
Remote storage, including NAS and file shares
Serv-U connects to Serv-U Gateway to listen for new traffic
Clients connect to Serv-U Gateway with FTP, FTPS, SFTP (SSH), HTTP, and HTTPS
Serv-U connects to back-end as needed
Serv-U Gateway stitches incoming client connection to listener from Serv-U

Serv-U MFT Web Farm w/ Redundant Gateways

Firewall Configuration:

The primary firewall supports FTP, FTPS (SSL/TLS), SFTP (SSH), HTTP, and/or HTTPS inbound connections from the Internet into Serv-U. This firewall may also be configured to allow outbound connections for support FTP/S active mode data connections, or may be "FTP aware" enough to open FTP data channels dynamically.

The firewall between the DMZ segment and the internal network only needs to allow outbound connections from each of the Serv-U servers to each of the Serv-U Gateways over TCP port 1180.

Load Balancer:

A network load balancer must be used to distribute incoming connections to each Serv-U Gateway.

Load balancers should be configured to preserve original IP addresses if you want to use Serv-U's IP lockout protection. Load balancers should also use "sticky sessions" that lock all incoming connections from a particular IP address to a specific Serv-U server to allow FTP and FTPS connections to work properly.

No load balancer is required between the Serv-U Gateway tier and the Serv-U server tier.

Remote Storage:

All user home folders, virtual folders and other Serv-U folders must be configured to use remote storage (e.g., NAS or file shares) rather than local hard drives. Each Serv-U server must be able to make a CIFS (Windows networking) connection to those resources.

Remote Authentication:

All Serv-U domains must use remote authentication provided by an ODBC-compliant database or Microsoft Active Directory (AD).

- If Serv-U accesses an ODBC-compliant database for remote authentication, then each Serv-U server must be able to make a database-appropriate connection to that database. For example, SQL Server connections are often made over TCP port 1433.
- If Serv-U accesses Active Directory ("AD") for remote authentication, then your Serv-U server must be part of the AD domain and on the same network segment.

Variations:

- On Windows Server the built-in Windows Network Load Balancer service may be used instead of a physical load balancer to provide load balancing services to Serv-U Gateway.
- The two firewalls represented in the diagram are sometimes "two legs" of a single firewall controlling access between multiple segments.

- Serv-U Gateway and Serv-U may be deployed on different operating systems. (e.g., your Internet-facing Serv-U Gateway can be deployed on Linux even if you have deployed your Serv-U server on Windows.) However, all Serv-U Gateways should use the same operating system and all Serv-U Servers should use the same operating system whenever possible.

Advantages:

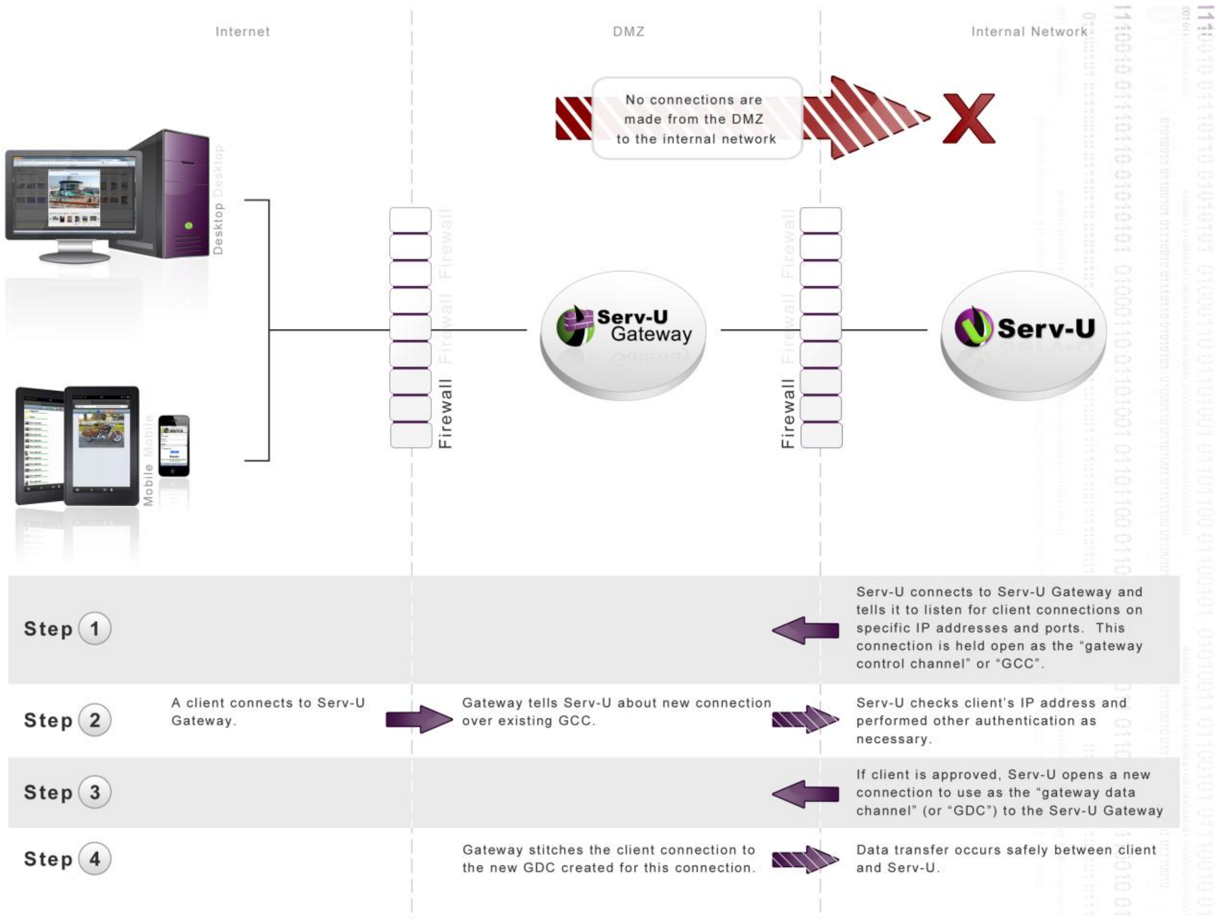
- Active redundancy means that your Serv-U application servers are not single points of failure.
- Completely satisfies MFT requirement that no data at rest exists in the DMZ.
- Satisfies most security policy requirements by ensuring direct connections to internal storage, internal databases, or Active Directory domain controllers are only made between computers on your trusted internal network.
- No CIFS, AD, or DB connections are ever made across a firewall.

Disadvantages:

- More difficult to set up than single-node or single-tier systems. (Must install Serv-U on each application server and point to the same shared resources. Must also configure a load balancer and configure Serv-U Gateways on both Serv-U servers.)
- Live user statistics may be unreliable for individual users who sign on to multiple servers simultaneously. (This can be partially mitigated for end users who sign on from a single IP at a time by using “sticky sessions” on your load balancer.)

Gateway Communication Details

Serv-U Gateway is able to act as a secure “reverse proxy” by avoiding direct connections from the Internet or the DMZ into the internal network. Behind the scenes, all inbound connections are served by Serv-U Gateway by tying them to outbound connections from the internally-based Serv-U server. This allows Serv-U Gateway to perform its duty without ever making an inbound connection from the DMZ segment to the trusted network.



Step 1: Serv-U connects to Serv-U Gateway and tells it to listen for client connections on specific IP addresses and ports. This connection is held open as the “gateway control channel” or “GCC”.

Step 2: A client connects to Serv-U Gateway. Gateway tells Serv-U about new connection over existing GCC. Serv-U checks client’s IP address and performed other authentication as necessary.

Step 3: If client is approved, Serv-U opens a new connection to use as the “gateway data channel” (or “GDC”) to the Serv-U Gateway

Step 4: Gateway stitches the client connection to the new GDC created for this connection. Data transfer occurs safely between client and Serv-U.

Serv-U Gateway Communication - Technical Details

Assumptions:

- The firewall guarding access from the Internet to the DMZ segment is configured to allow standard file transfer services (e.g., FTP/S, SFTP via SSH, HTTPS, etc.) to Serv-U Gateway.
- The firewall guarding access from the DMZ segment to the trusted internal network does not permit any connections from the DMZ to the internal network.
- Serv-U Gateway is powered up and listening for connections in the DMZ segment.
- Serv-U is installed in the trusted internal network.

Communication Walkthrough:

1. When a Serv-U server starts up, it tries to connect to all its configured Serv-U Gateways. As it connects to each one, Serv-U provides specific instructions to each Serv-U Gateway about the protocols, IP addresses, and ports it should use to serve connections from the Internet. The connection Serv-U uses to provide this information is opened and reestablished as necessary so Serv-U Gateway can send messages back to Serv-U. This connection can be thought of as the "gateway control channel" or "GCC."

2. When a file transfer client (e.g., web browser, iPad, or FTP client) opens a connection to Serv-U Gateway, Serv-U Gateway will ask about the connection over the existing GCC. Serv-U performs any necessary IP checks and authentication against its own database or internal resources.

3. If Serv-U approves the incoming connection, Serv-U makes a new outbound connection from Serv-U to the Serv-U Gateway. This second connection can be thought of as the "gateway data channel" or "GDC." If Serv-U denies the incoming connection Serv-U tells Serv-U Gateway to deny the connection via the GCC and Serv-U Gateway terminates the requesting client's connection.

4. Serv-U Gateway stitches the original client connection and the GCD created for the approved connection together. From that point forward data transfer occurs between the client and Serv-U until either side terminates the session.

Security:

- Use of protocols that encrypt data in transit (e.g., FTPS, SFTP over SSH and HTTPS) is supported and encouraged when clients connect to Serv-U Gateway.

- The communication channels between Serv-U and Serv-U Gateway always encrypt all traffic between those two machines, regardless of the protocol the client used to connect. This provides end-to-end secure transport when clients use a secure protocol.

- No data or authentication information is ever stored at rest in the DMZ.

Additional References

The **Serv-U User's Manual** describes how to set up domains, groups, user, and folders to support a Serv-U HA deployment. The following sections are particularly pertinent:

- Mapping home folders and virtual folders to Windows Shares
    - "Virtual Paths" section – "Physical Path" subsection
    - "User Information" section – "Home Directory" subsection
    - "Directory Access Rules" section – "Access as Windows Users" subsection
- Using a common share to handle SSH keys, SSL certificates, server welcome message, FTP message files, event command executables, and log files
    - "User Information" section, "SSH Public Key Path" subsection
    - "Encryption" section, "Configuring SSL for FTPS and HTTPS" subsection
    - "Encryption" section, "SFTP (Secure File Transfer over SSH2)" subsection
    - "FTP Settings" section, "Server Welcome Message" subsection
    - "FTP Settings" section, "Message Files" subsection
    - "Serv-U Events" section, "Execute Command Actions" subsection
    - "Configuring Domain Logs" section, "Log File Path" subsection
- Using external authentication
    - "Domain Settings" to set database-based or Active Directory authentication
    - Serv-U Database Integration Guide for database-based authentication
    - "Serv-U Windows Groups" section for Active Directory authentication

The **Serv-U Database Integration Guide** contains detailed information and instructions to set up an authentication database in support of Serv-U web farms. Supported databases include SQL Server, Oracle Database, MySQL, PostGres, and several other ODBC-compliant relational databases.

The use of **RhinoSoft Premium Support** is recommended for all HA or multi-tier deployments. This level of support was developed for customers who use Serv-U in mission-critical situations and includes:

- Live phone support
- 2-4 hour priority response via email