Serv-U® Distributed Architecture Guide

Horizontale Skalierung und mehrstufiges Setup für Hohe Verfügbarkeit, Sicherheit und Performance

Einleitung

Serv-U ist ein höchst-performanter und sicherer Server für Dateitransfers in Windows und Linux Umgebungen. Es unterstützt FTP, FTPS (SSL/TLS), SFTP (SSH), HTTP und HTTPS Verbindungen und bietet zudem optimierte Benutzerschnittstellen für Webbrowser sowie für mobile Geräte wie iPad, iPhone, BlackBerry, Android und Kindle Fire.

Um hohe Redundanz, Sicherheit und Performance zu bieten, unterstützt Serv-U sowohl mehrstufige als auch hoch-verfügbare Konfigurationsvarianten. Dieses Dokument beschreibt, wie Serv-U diese beiden Architekturen unterstützt und zeigt Ihnen die Vor- und Nachteile dazu auf.

"Keine Daten in der DMZ" bei Managed-File-Transfer

Eine mehrstufige Serv-U / Serv-U Gateway Installation ermöglicht es Ihnen, eine der wichtigsten Regeln bei Managed-File-Transfer zu erfüllen: „Speichere niemals Daten in der DMZ".

Unser Serv-U Gateway leitet eingehende Verbindungen aus dem Internet auf sichere Art und Weise zu ihrem Serv-U Server weiter, ohne Verbindungen aus dem Internet oder ihrer DMZ in ihr vertrauenswürdiges Netzwerk öffnen zu müssen.

Hohe Verfügbarkeit durch horizontale Skalierung

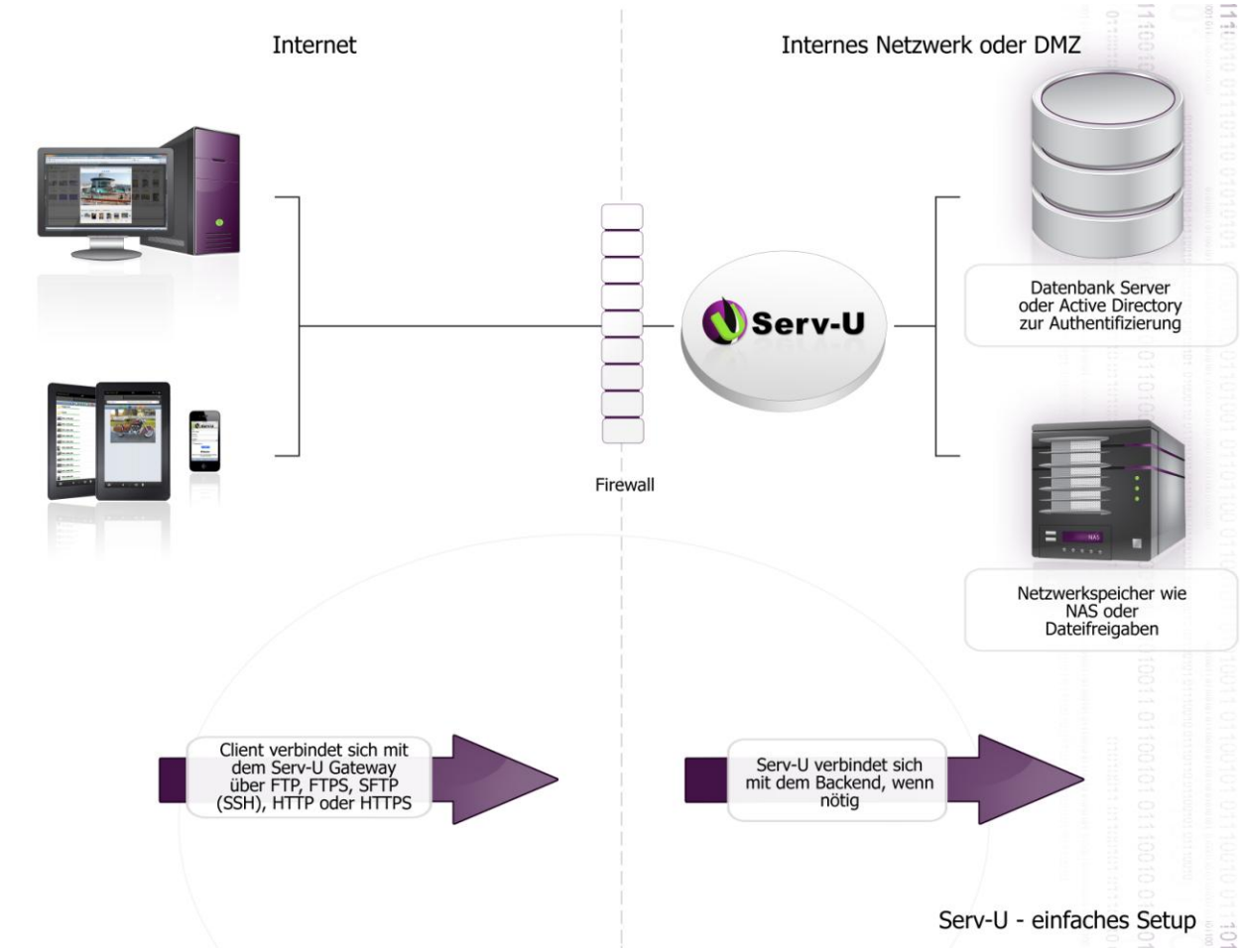
Sowohl der eigentliche Serv-U Server als auch unser Serv-U Gateway können in einer „N+1" Konfiguration eine hohe Verfügbarkeit durch eine horizontale Skalierung bereitstellen. Das ermöglicht Ihnen einen Ausbau um ihre Bedürfnisse zu erfüllen und reduziert Ausfallrisiken, durch die Vermeidung einzelner system-kritischer Komponenten.

Inhaltsverzeichnis

Standard Installation

Wird Serv-U als Einzelserver installiert, wird er im Allgemeinen über eine Firewall von Zugriffen aus dem Internet geschützt. Serv-U selbst greift beispielsweise auf Netzwerkspeicher oder externe Authentifizierungsquellen zu.

Alle Serv-U Editionen (Bronze, Silver, Gold und Platinum) können in so einem Umfeld installiert werden, aber nur Serv-U Gold und Serv-U Platinum bieten die Möglichkeit, auf externe Authentifizierungsquellen zurückzugreifen.



Firewall Konfiguration

Die Standardfirewall ermöglicht FTP, FTPS (SSL/TLS), SFTP (SSH), HTTP und/oder HTTPS Verbindungen aus dem Internet zu ihrem Serv-U Server. Die Firewall sollte auch für ausgehende Verbindungen für FTP/S Aktiv-Mode Daten Transfers konfiguriert sein oder aber FTP Datenverbindungen dynamisch öffnen können.

Möglichkeiten

- Greift Serv-U auf einen externen Speicher wie NAS oder Dateifreigaben zu, dann muss es Serv-U möglich sein, CIFS (Windowsnetzwerk) Verbindungen zu diesen Ressourcen zu öffnen.
- Verwendet Serv-U eine ODBC-konforme Datenbank für die Authentifizierung, dann muss es Serv-U ermöglicht werden, eine Datenbankverbindung aufzubauen. SQL Server Verbindungen werden oft über TCP Anschluss 1433 abgewickelt.
- Wenn Serv-U ein Active Directory („AD") für die Authentifizierung verwendet, muss der Serv-U Server Teil dieser AD Domäne und im gleichen Netzwerksegment sein.

Vorteile

- Einfachste Möglichkeit der Installation (Diese Konfiguration wird zum Testen von Serv-U empfohlen)

Nachteile

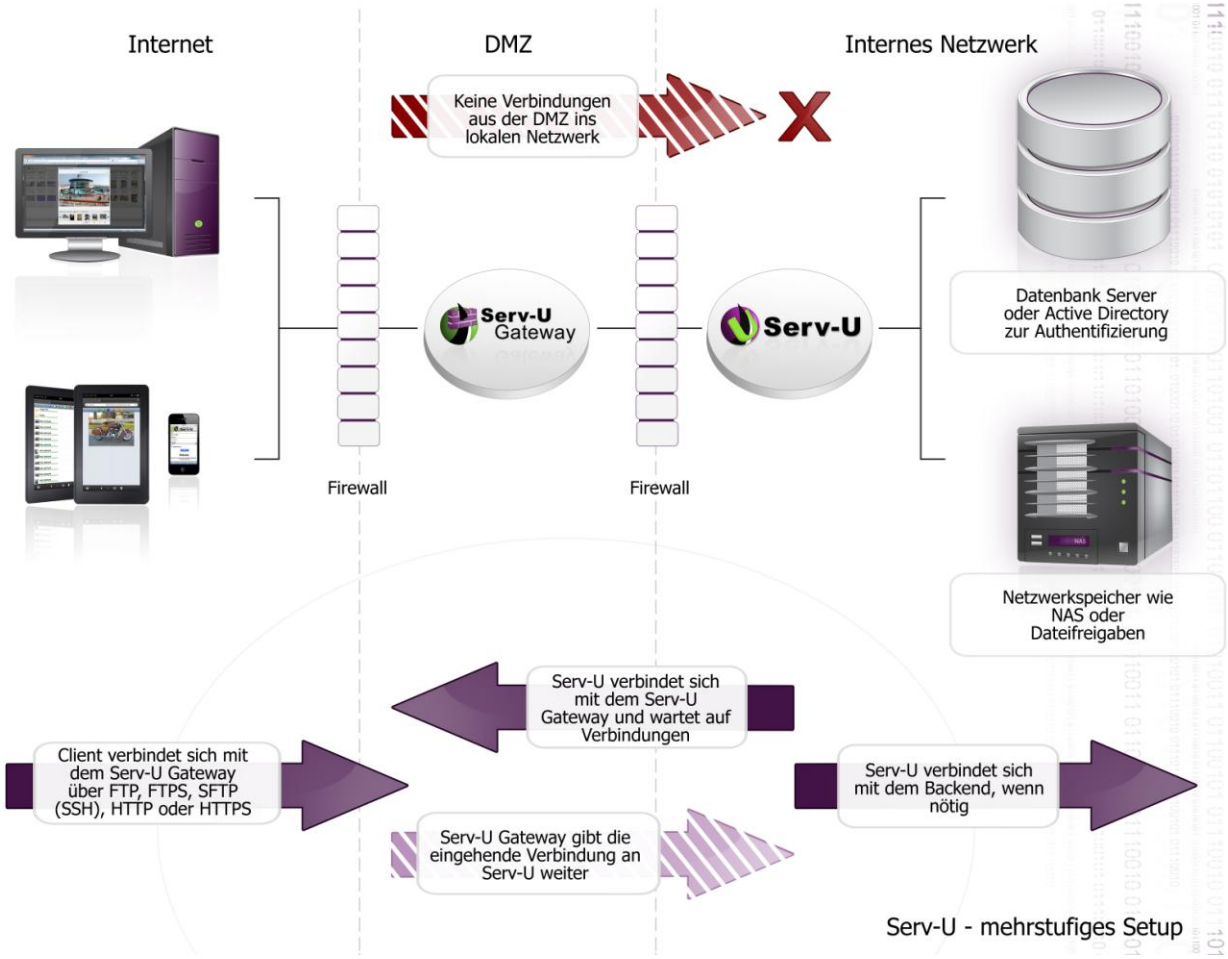
- Keinerlei Redundanzen eingebaut, Serv-U Server ist ein „Single Point of failure" und somit systemkritisch
- Direkte Verbindungen von Serv-U zum lokalen Speichermedien, internen Datenbanken, Active Directory Domain Controller sind möglicherweise aufgrund verschiedener Sicherheitsrichtlinien nicht erlaubt.

Elementare mehrstufige (MFT) Konfiguration

Das Serv-U Gateway ermöglicht es Ihnen, Serv-U in einer mehrstufigen Konfiguration zu betreiben. Damit erfüllen sie die meisten Sicherheitserfordernisse für Managed-File-Transfers („MFT“) mehr als ausreichend. Dieses Setup ermöglicht es Ihnen,

- Dass alle eingehenden Transfers auf einem Server in ihrer DMZ terminieren
- keine Daten jemals in der DMZ gespeichert werden
- eingehende Verbindungen von ihrer DMZ in ihr lokales Netzwerk vermieden werden

Serv-U Silver, Serv-U Gold und Serv-U Platinum können in einem solchen Setup verwendet werden. Serv-U Gold oder Serv-U Platinum sind notwendig, wenn sie SFTP (SSH) oder HTTPS Transfers anbieten oder auf externe Authentifizierungsquellen zurückgreifen möchten.



Firewall Konfiguration:

Die Firewall zwischen dem Internet und ihrer DMZ sollte eingehende FTP, FTPS (SSL/TLS), SFTP (SSH), HTTP und/oder HTTPS Verbindungen aus dem Internet zu Serv-U erlauben. Die Firewall sollte auch für ausgehende Verbindungen konfiguriert werden, um FTP/S Aktiv-Mode Daten Transfers zu erlauben oder aber FTP Datenverbindungen dynamisch öffnen können.

Die Firewall zwischen der DMZ und dem internen Netzwerk muss eigentlich nur ausgehende Verbindungen von Serv-U zum Serv-U Gateway über TCP Anschluss 1180 (frei konfigurierbar) erlauben.

Optionen

- Greift Serv-U auf einen externen Speicher wie NAS oder Dateifreigaben zu, dann muss es Serv-U möglich sein, CIFS (Windowsnetzwerk) Verbindungen zu diesen Ressourcen zu öffnen.
- Verwendet Serv-U eine ODBC-konforme Datenbank für die Authentifizierung, dann muss es Serv-U ermöglicht werden, eine Datenbankverbindung aufzubauen. SQL Server Verbindungen werden oft über TCP Anschluss 1433 abgewickelt.
- Wenn Serv-U ein Active Directory („AD") für die Authentifizierung verwendet, muss der Serv-U Server Teil dieser AD Domäne und im gleichen Netzwerksegment sein.
- Die zwei in den Graphiken dargestellten Firewalls können auch zwei Seiten der gleichen einzelnen Firewall sein, die den Zugriff zu den unterschiedlichen Netzwerkbereichen regelt.
- Serv-U Gateway und Serv-U können auf unterschiedlichen Betriebssystemen installiert werden. (Das Serv-U Gateway könnte beispielsweise in einer Linuxumgebung installiert werden, während der oder die Serv-U Server in einer Windowsumgebung laufen.)

Vorteile

- Nach wie vor einfach einzurichten: Serv-U Gateway installieren, Serv-U Gateway festlegen und die Ports definieren
- Erfüllt die Erfordernisse der MFT komplett, keine Daten werden in der DMZ gespeichert.
- Erfüllt auch die meisten Sicherheitseinstellungen, da direkte Verbindungen zu den internen Speicherorten, den internen Datenbanken oder Active Directory Domain Controller nur über Rechner, die sich im vertrauenswürdigen internen Netz befinden, stattfinden.
- Keine CIFS, Active Directory oder Datenbankverbindungen über die Firewall hinaus

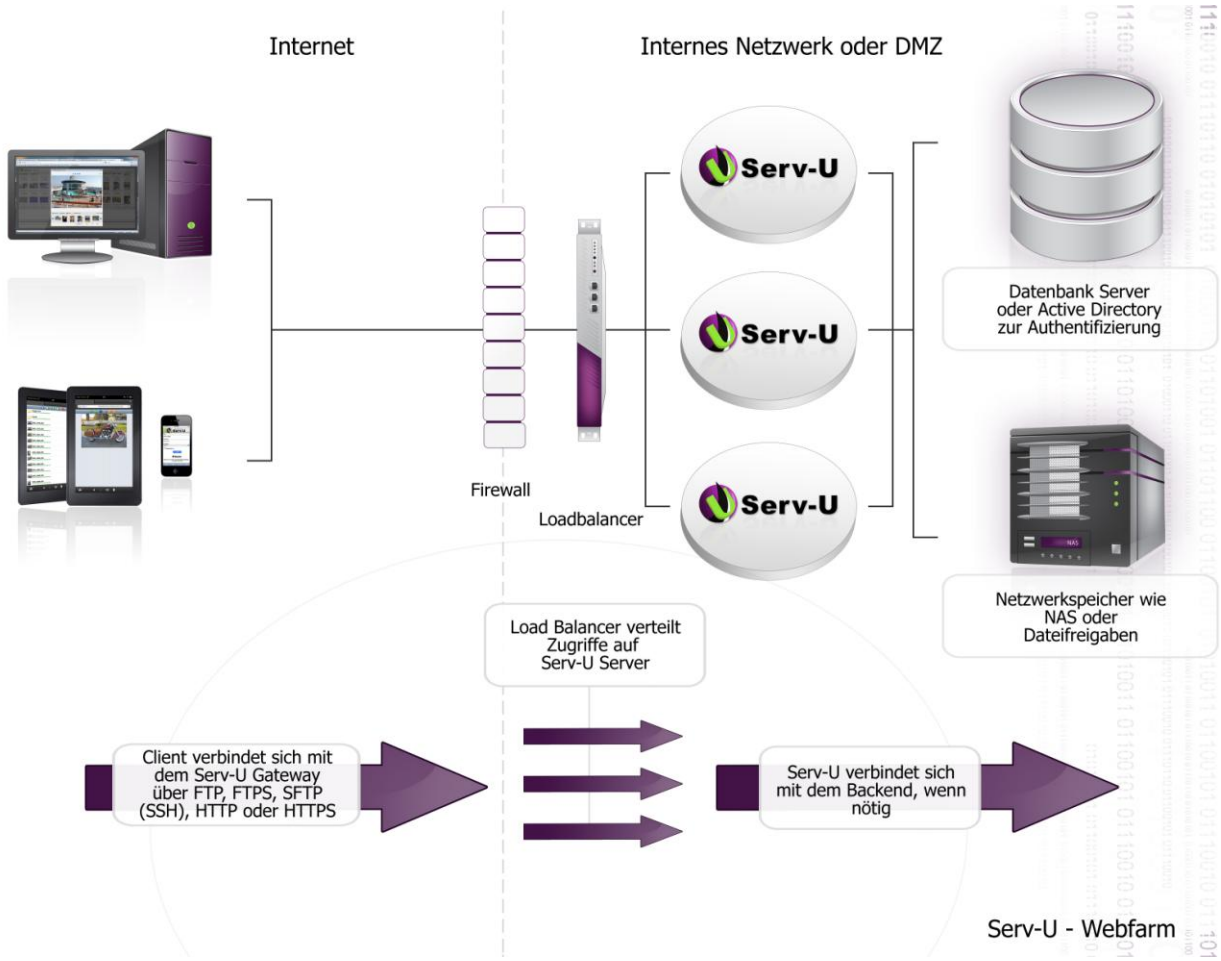
Nachteile

- Noch keine redundanten Systeme, Serv-U Server und Serv-U Gateway sind die „Single Points of Failure".

Konfiguration mit hoher Verfügbarkeit (N+1)

Serv-U kann auch als Serverfarm betrieben werden und wird somit zu einem Dienst mit hoher Verfügbarkeit (highly available, „HA“) durch horizontale Skalierung (N+1).

Serv-U Gold und Serv-U Platinum sind die beiden Serv-U Editionen, die eine Konfiguration mit hoher Verfügbarkeit ermöglichen, da beide eine Authentifizierung der Benutzer von externen Quellen unterstützen. Derzeit ist es möglich, bis zu 5 Serv-U Server so parallel zu betreiben.



Firewall Konfiguration

Die Firewall zwischen dem Internet und ihrer DMZ sollte eingehende FTP, FTPS (SSL/TLS), SFTP (SSH), HTTP und/oder HTTPS Verbindungen aus dem Internet zu Serv-U erlauben. Die Firewall sollte auch für ausgehende Verbindungen konfiguriert werden, um FTP/S Aktiv-Mode Daten Transfers zu erlauben oder aber FTP Datenverbindungen dynamisch öffnen können.

Load Balancer

Ein Netzwerk Loadbalancer muss für die Verteilung der eingehenden Verbindungen auf die Serv-U Server verwendet werden.

Dieser sollte so konfiguriert werden, dass er die ursprüngliche IP Adresse erhält, wenn sie in Serv-U auch IP Blocks verwenden möchten. Der Loadbalancer soll weiters „sticky session“ unterstützen, damit alle Verbindungen von einer bestimmten IP Adresse immer zum selben Serv-U Server weitergeleitet werden und so FTP und FTPS Verbindungen richtig funktionieren.

Netzwerkspeicher

Die Stammverzeichnisse aller Benutzer, die virtuellen Pfad und andere Serv-U Verzeichnisse müssen so konfiguriert sein, dass sie Netzwerkspeicherplätze (zB NAS, Dateifreigaben) verwenden. Es sollten dazu keine lokalen Laufwerke verwendet werden. Serv-U muss es möglich sein, CIFS (Windows Netzwerk) Verbindungen zu diesen Ressourcen herzustellen.

Externe Authentifizierungsquellen

Alle Serv-U Domains müssen auf externe Authentifizierungsquellen, wie eine ODBC-konforme Datenbanken oder aber ein Microsoft Active Diretory (AD), zugreifen können.

- Greift Serv-U auf eine ODBC-konforme Datenbank zu Authentifizierungszwecke zu, muss es Serv-U möglich sein, die nötige Verbindung dafür zur Datenbank aufzubauen. Verbindungen zu einem SQL Server werden in der Regel über den TCP Anschluss 1433 getätigt.

- Verwendet Serv-U das Active Directory (“AD”) zur Authentifizierung, muss der Serv-U Server Teil der AD Domain sein und sich im selben Netzwerkbereich befinden.

Optionen

- Der auf einem Windows Server mitgelieferte Windows Network Load Balancer Dienst kann anstelle eines physischen Loadbalancers verwendet werden, um die Dienste des Serv-U Gateway zu verteilen.

Vorteile

- Aktive Redundanzen bedeuten, dass ihre Serv-U Server keine Single-Points-of Failure und somit auch nicht mehr systemkritisch sind.

Nachteile

- Weitaus schwierigeres Setup als bei Einzelinstallationen. Serv-U muss auf jedem Programmserver installiert werden und die gleichen Ressourcen wie die anderen verwenden können.

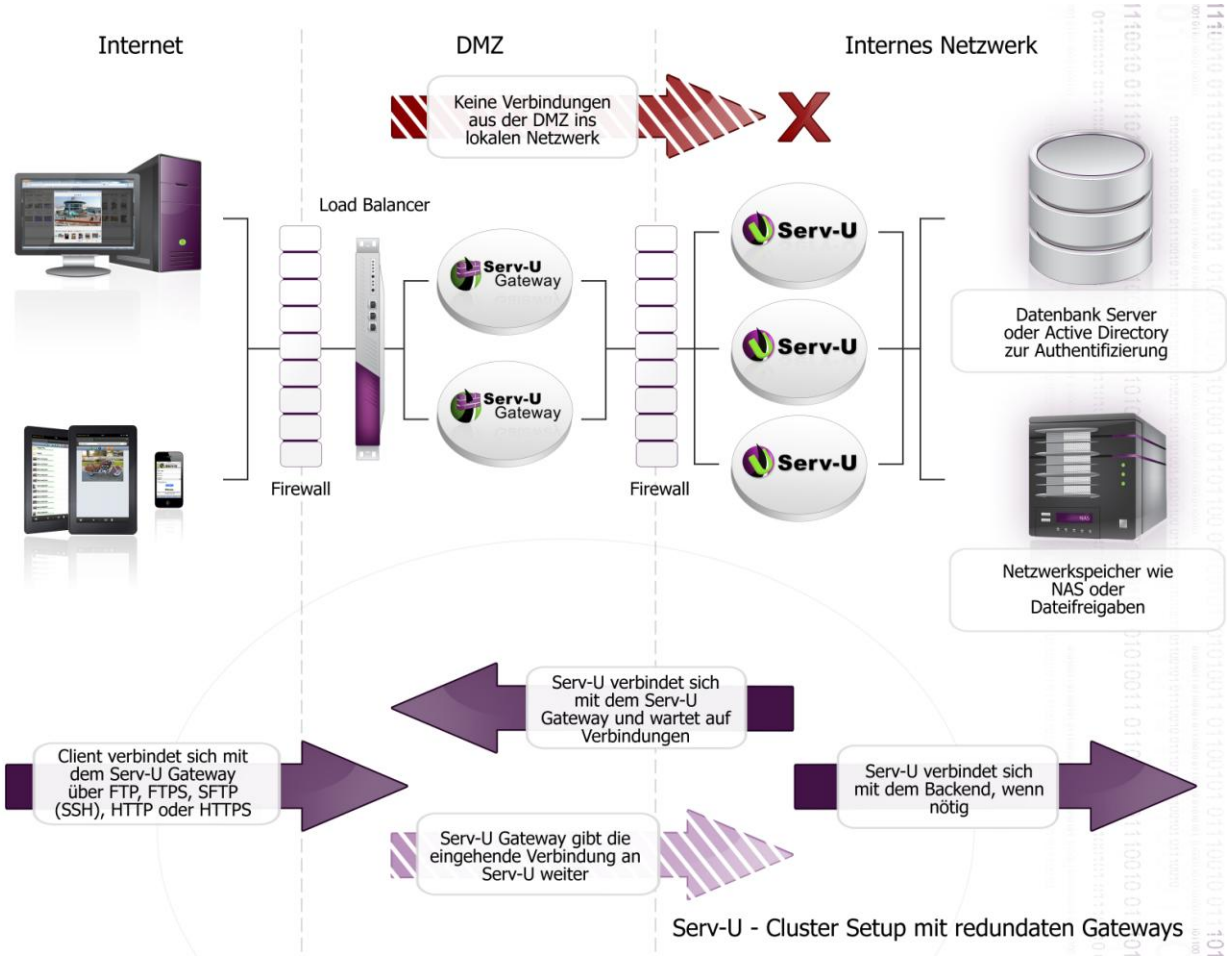
- Direkte Verbindungen von Serv-U zum internen Speicher, zu internen Datenbanken oder dem Active Directory sind mitunter nicht überall aufgrund von Sicherheitsregeln erlaubt.
- Aktuelle Benutzer Statistiken für einzelne Benutzer, die sich auf unterschiedlichen Servern gleichzeitig anmelden könnten, sind nicht sehr aussagekräftig. (Das Problem kann zwar bei Endbenutzerstatistiken und bei Benutzern, die sich von einer einzelnen IP aus anmelden, durch die „sticky session“ am Loadbalancer gemildert werden, bleibt aber bei Gruppenstatistiken leider bestehen.)

Mehrstufige, hochverfügbare Konfiguration

Serv-U kann nun als Serverfarm auf mehreren Applikationsserver installiert werden, um hier durch eine horizontale Skalierung (N+1) eine hohe Verfügbarkeit („HA“ … high availability) zu ermöglichen. Es kann auch durch sein mehrstufiges Setup alle (und sogar darüber hinaus) wichtigen Sicherheitserfordernisse für Managed-File-Transfers (MFT) erfüllen. Beides gemeinsam nun ermöglicht eine ausgeklügelte hochverfügbare und sichere Installation, bei der

- alle eingehenden Verbindungen auf einem Server in ihrer DMZ enden
- keinerlei Daten in der DMZ gespeichert werden
- keine eingehenden Verbindungen aus der DMZ in ihr internes Netz aufgebaut werden
- es keine systemkritische Komponente (Single Point of Failure) gibt
- je nach Bedarf skaliert werden kann

Serv-U Gold und Serv-U Plantium sind die beiden einzigen Serv-U Editionen, die ein hochverfügbares, mehrstufiges Setup ermöglichen, da dies die einzigen Editionen sind, die auf externe Authentifizierungsquellen zugreifen können. Bis zu fünf Serv-U Server und drei Serv-U Gateways sind derzeit in einer solchen Konfiguration maximal möglich.



Firewall Konfiguration

Die Firewall zwischen dem Internet und ihrer DMZ sollte eingehende FTP, FTPS (SSL/TLS), SFTP (SSH), HTTP und/oder HTTPS Verbindungen aus dem Internet zu Serv-U erlauben. Die Firewall sollte auch für ausgehende Verbindungen konfiguriert werden, um FTP/S Aktiv-Mode Daten Transfers zu erlauben oder aber FTP Datenverbindungen dynamisch öffnen können.

Die Firewall zwischen der DMZ Und dem internen Netzwerk muss eigentlich nur ausgehende Verbindungen von Serv-U zum Serv-U Gateway über TCP Anschluss 1180 (frei konfigurierbar) erlauben.

Load Balancer

Ein Netzwerk Loadbalancer muss für die Verteilung der eingehenden Verbindungen auf die Serv-U Server verwendet werden.

Dieser sollte so konfiguriert werden, dass er die ursprüngliche IP Adresse erhält, wenn sie in ServU auch IP Blocks verwenden möchten. Der Loadbalancer soll weiters „sticky session“ unterstützen, damit alle Verbindungen von einer bestimmten IP Adresse immer zum selben Serv-U Server weitergeleitet werden und so FTP und FTPS Verbindungen richtig funktionieren.

Zwischen den Serv-U Gateway und den Serv-U Server Installationen ist kein Load-Balancer notwendig.

Netzwerkspeicher

Die Stammverzeichnisse aller Benutzer, die virtuellen Pfade und andere Serv-U Verzeichnisse müssen so konfiguriert sein, dass sie Netzwerkspeicherplätze (zB NAS, Dateifreigaben) verwenden. Es sollten dazu hier keine lokalen Laufwerke verwendet werden. Serv-U muss es möglich sein, CIFS (Windows Netzwerk) Verbindungen zu diesen Ressourcen herzustellen.

Externe Authentifizierungsquellen

Alle Serv-U Domains müssen auf externe Authentifizierungsquellen, wie eine ODBC-konforme Datenbanken oder aber ein Microsoft Active Diretory (AD), zugreifen können.

- Greift Serv-U auf eine ODBC-konforme Datenbank zu Authentifizierungszwecke zu, muss es Serv-U möglich sein, die dafür nötige Verbindung zur Datenbank aufzubauen. Verbindungen zu einem SQL Server werden in der Regel über den TCP Anschluss 1433 getätigt.

- Verwendet Serv-U das Active Directory (“AD”) zur Authentifizierung, muss der Serv-U Server Teil der AD Domain sein und sich im selben Netzwerkbereich befinden.

Möglichkeiten

- Der auf einem Windows Server mitgelieferte Windows Network Load Balancer Dienst kann anstelle eines physischen Loadbalancers verwendet werden, um die Dienste des Serv-U Gateway zu verteilen.

- Die zwei in den Graphiken dargestellten Firewalls können auch zwei Seiten der gleichen einzelnen Firewall sein, die den Zugriff zu den unterschiedlichen Netzwerkbereichen regelt.

- Serv-U Gateway und Serv-U können auf unterschiedlichen Betriebssystemen installiert werden. (Das Serv-U Gateway könnte beispielsweise in einer Linuxumgebung installiert werden, während der oder die Serv-U Server in einer Windowsumgebung laufen). Es sollten allerdings alle Serv-U Gateways auf dem gleichen Betriebssystem installiert sein, ebenso wie alle Serv-U Server das gleiche Betriebssystem als Grundlage verwenden – sofern dies möglich ist.

Vorteile

- Aktive Redundanzen bedeuten, dass ihre Serv-U Server keine Single-Points-of Failure und somit system kritisch sind.

- Erfüllt die Erfordernisse der MFT zur Gänze, keine Daten werden in der DMZ gespeichert.

- Geht mit den meisten Sicherheitsanforderungen konform, die sicherstellen, dass direkte Verbindungen zu Netzwerkspeicher, internen Datenbanken oder zum Active Directory nur

zwischen Computer stattfinden, die sich innerhalb des vertrauenswürdigen internen Netzwerks befinden.

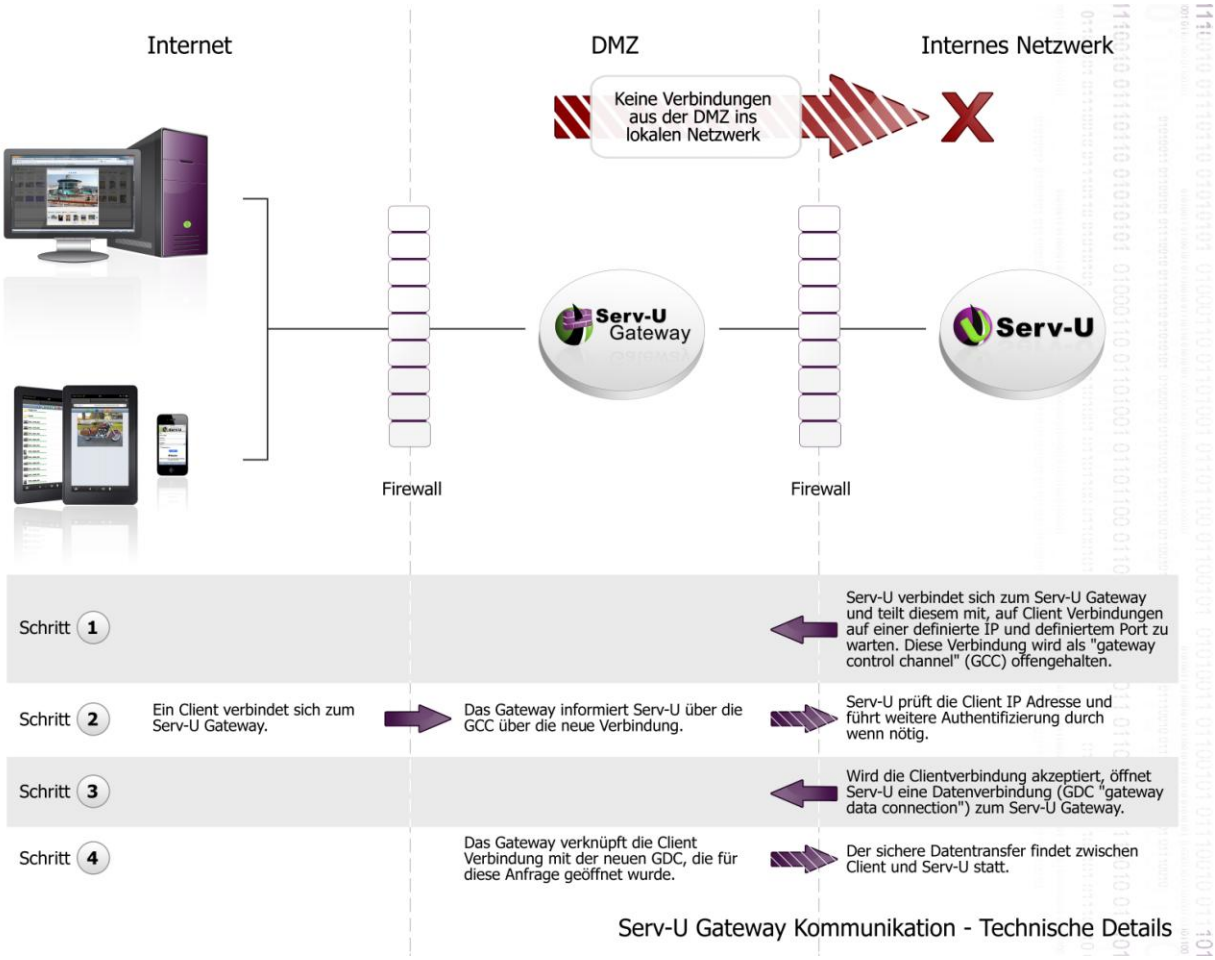
- Keine CIFS, AD oder DB Verbindungen über die Firewall hinweg sind nötig.

Nachteile

- Weitaus schwierigeres Setup als bei Einzel- oder einstufigen Installationen. Serv-U muss auf jedem Programmserver installiert werden und die gleichen Ressourcen wie die anderen verwenden.
- Aktuelle Benutzer Statistiken für einzelne Benutzer, die sich auf unterschiedlichen Servern gleichzeitig anmelden könnten, sind nicht sehr aussagekräftig. (Das Problem kann zwar bei Endbenutzerstatistiken und bei Benutzern, die sich von einer einzelnen IP aus anmelden, durch die „sticky session“ am Loadbalancer gemildert werden, bleibt aber bei Gruppenstatistiken leider bestehen.)

Details zur Kommunikation mit dem Gateway

Dieser Abschnitt beschreibt, wie es dem Serv-U Gateway möglich ist, als sicherer „Reverse Proxy“ zu arbeiten. Alle eingehenden Verbindungen werden vom Serv-U Gateway bedient, indem sie den ausgehenden Verbindungen der internen Serv-U Server zugewiesen werden. Damit ist es für das Serv-U Gateway nicht nötig, Verbindungen aus der DMZ ins vertrauenswürdige Netzwerk zu öffnen, um seine Funktion zu erledigen.



Annahmen

- Die Firewall, welche die DMZ vor Zugriff aus dem Internet schützt, ist so konfiguriert, dass sie die Standard Dienste des Dateitransfers (etwa FTP/S, HTTP/S, etc) an das Serv-U Gateway weitergibt.
- Die Firewall, welche den Zugriff aus der DMZ ins interne, vetrauenswürdige Netzwerk schützt, erlaubt keine Verbindungen in diese Richtung
- Das Serv-U Gateway wird aktiviert und es wartet auf Verbindungen in die DMZ.
- Serv-U ist im geschützten internen Netzwerk installiert.

Kommunikationswege

1. Startet der Serv-U Server, versucht er sich mit allen Serv-U Gateways zu verbinden, die für ihn konfiguriert wurden. Einmal mit einem Serv-U Gateway verbunden, gibt Serv-U dem Gatway Informationen über Protokolle, IP Adresse und Anschlüsse, die es für die Verbindungen aus dem Internet verwenden soll, weiter. Die Verbindung, die Serv-U für diese Informationen verwendet, wird immer offengehalten (und gegebenenfalls neu aufgebaut). So kann das Serv-U Gateway Informationen zu Serv-U zurücksenden. Diese Verbindung wird als „gateway control channel“ oder „GCC“ bezeichnet.

2. Öffnet ein Dateitransferclient (zB Browser, iPad, FTP Client) eine Verbindung zum Serv-U Gateway, holt das Serv-U Gateway über den bestehenden GCC Informationen ein. Serv-U erledigt die nötigen IP Adressprüfungen sowie die Benutzeranmeldung über die eigene Datenbank oder externe Ressourcen.

3. Wird die Verbindung von Serv-U für in Ordnung befunden, öffnet Serv-U eine ausgehende Verbindung zum Serv-U Gateway. Diese zweite Verbindung kann als „gateway data channel“ oder „GDC“ bezeichnet werden. Erlaubt Serv-U die Verbindung nicht, gibt es diese Information über das GCC an das Serv-U Gateway weiter und das Serv-U Gateway seinerseits beendet die Verbindung des Anfragenden.

4. Das Serv-U Gateway verbindet die ursprüngliche Client-Verbindung und die GCD, die für die erfolgreiche Authentifizierung eingerichtet wurde. Der Datentransfer passiert ab jetzt zwischen Client und Serv-U, bis eine der beiden Seite die Sitzung beendet.