

# Virtual Server Reverse Proxy

## What will be done

- Using a FortiGate to act as a Reverse Proxy, forwarding `domain.tld` to `ip:port`

## Prerequisites

- Static IP
- Port 443 (TCP) for HTTPS open

In this Example, Forgejo will be used as Application

## 1. Creating a Virtual Server

1. Go to Policy & Objects - Virtual Servers and Click Create New
2. Set a Name

### 1.2 Network Configuration

1. Set *Type* to **HTTPS**
2. Set *Interface* to your WAN Interface
3. Set *Virtual server IP* to your Public IP (or TN IP if behind a NAT Router)
4. Set *Virtual server port* to `443`
5. Set *Load balancing method* to **HTTP Host**
6. Set *Persistence* to **HTTP Cookie**
7. Enable *Preserve client IP*

Network	
Type	HTTPS
Interface	FB WAN (wan1)
Virtual server IP	172.16.1.200
Virtual server port	443
Load balancing method	HTTP Host
Persistence	<input checked="" type="radio"/> None <input type="radio"/> HTTP Cookie <input type="radio"/> SSL Session ID
Health check	+
HTTP multiplexing	<input type="checkbox"/>
Preserve client IP	<input checked="" type="checkbox"/>

You can add Health Checks for this Virtual Server here

## 1.3 SSL Offloading

As the FortiGate will be acting as Reverse Proxy in this Situation, SSL Encryption needs to be done at the Firewall. Select/Upload your SSL Certificate here and Set *Mode* to **Full**

SSL Offloading	
Mode	<input type="radio"/> Client <-> FortiGate <input checked="" type="radio"/> Full
Certificate	FortiGate Web

## 1.4 Real Servers

For each public Domain, create a Real Server here

Example: git.domain.tld

1. Click *Create New*
2. Set *IPv4 Address* to your internal Server IP Address
3. Set *Port* to your internal Server Port
4. Set *Max connections* to  for unlimited Connections or set a fixed limit
5. Set *HTTP host* to your public Domain
6. Set *Mode* to **Active**

## Edit Real Server

Type	IP
IPv4 address	<input type="text" value="10.0.0.14"/>
Port	<input type="text" value="443"/>
Max connections	<input type="text" value="0"/>
HTTP host	<input type="text" value="git.domain.tld"/>
Mode	<input checked="" type="radio"/> Active <input type="radio"/> Standby <input type="radio"/> Disable

OK

Cancel


## 2. Creating Firewall Policy


We need a Proxy-based Policy that allows WAN Access to the created Virtual Server


If you can't select your Virtual Server here, switch to *Proxy-based* Inspection Mode first.

ID 16


Name **i** Allow-WAN-to-VS-REVERSEPROXY

Incoming Interface  FB WAN (wan1) **x**  
+


Outgoing Interface  LAN (internal) **x**  
+


Source  all **x**  
+

Negate Source

Destination  VS-REVERSEPROXY **x**  
+

Negate Destination

Schedule  always ▾

Service  HTTPS **x**  
+

Action  ACCEPT  DENY  IPsec

Inspection Mode  Flow-based  Proxy-based


Proxy HTTP(S) traffic **i**

#### Firewall/Network Options

NAT

IP Pool Configuration  Use Outgoing Interface Address  Use Dynamic IP Pool

Preserve Source Port

Protocol Options  PROT default ▾ 

## 3. Application Configuration

Your Application needs to be able to accept Traffic to Port 80 with the specific Public Domain. As the FortiGate will handle SSL Encryption, you need to make sure your Application accepts plain HTTP without HTTP-to-HTTPS-Redirection

Revision #4

Created 11 September 2025 14:10:51 by Oliver Karger

Updated 12 September 2025 09:34:23 by Oliver Karger