FortiADC - VMware Horizon Deployment Guide

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

November 20, 2020
FortiADC VMware Horizon Deployment Guide

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-11-20	FortiADC 6.1.2 VMware Horizion Deployment Guide initial release

Overview

VMware Horizon is a centralized desktop virtualization solution that enables organizations to deliver virtualized desktop services and applications to end users from centralized VMware vSphere servers. Horizon has advantages for both end users and IT administrators.

About Core Horizon Components

VMware Horizon Client

VMware Horizon® Client for Windows, Windows 10 UWP, macOS, iOS, Linux, or Android is installed on every endpoint. This enables your end users to access their virtual desktops and published applications from a variety of devices such as smartphones, zero clients, thin clients, PCs, laptops, and tablets.

VMware Unified Access Gateway (UAG)

VMware Unified Access Gateway (formerly called VMware Access Point) provides a secure gateway that allows users to access their desktops and applications from outside a corporate firewall. Use UAG for secure external access to internal Horizon desktops and applications. UAG appliances typically reside in a demilitarized zone (DMZ) and act as a proxy host for connections inside your trusted corporate network. The UAG is optional. The Horizon View can work well without this component.

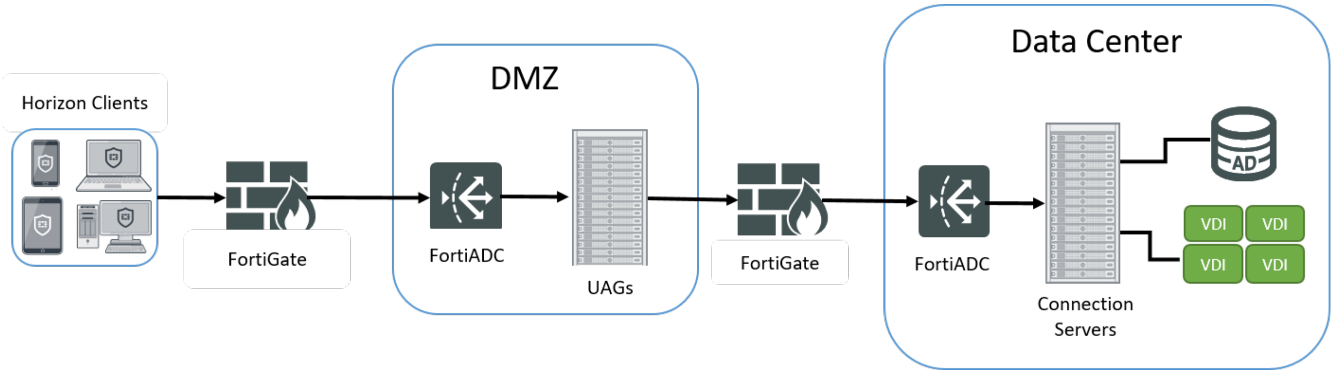
Horizon Connection Server (CS)

The Horizon Connection Server brokers client connections by authenticating users and directing incoming user desktop and application requests. Users connect to a Connection Server to access their virtual desktops and native, virtual, or RDSH-based applications.

About Load balancing for Horizon

The FortiADC D-series family of application delivery controllers (ADC) optimizes the availability, user experience, performance and scalability of enterprise application delivery. FortiADC is like an advanced server load balancer. FortiADC routes traffic to available destination servers based on health checks and loadbalancing algorithms; full-featured FortiADC also improve application performance by assuming some of the server task load. After you have deployed FortiADC, traffic is routed to the ADC virtual server instead of the destination real servers. For Horizon environments, you can load balance for the UAGs or CSs. The simple architecture is listed as Figure 1. This file is focusing on the FortiADC configuration for UAGs and CSs in Horizon View.

Figure 1: Horizon Architecture Overview



Horizon Protocols

When a Horizon Client user connects to a Horizon environment, several different protocols are used. The first connection is always the primary XML-API protocol over HTTPS. Following successful authentication, one or more secondary protocols are also made.

Primary Horizon Protocol

The user enters a hostname at the Horizon Client and this starts the primary Horizon protocol. This is a control protocol for authentication, authorization and session management. It uses XML structured messages over HTTPS (HTTP over SSL). This protocol is sometimes known as the Horizon XML-API control protocol. In a load balanced environment as shown above in Figure 1, the load balancer will route this connection to one of the UAGs or CSs. The load balancer will usually select the appliance based first on availability, and then out of the available appliances will route traffic based on the different load-balancing algorithm. This has the effect of evenly distributing the traffic from different clients across the available set of UAGs or CSes.

Secondary Horizon Protocols

After the Horizon Client has established secure communication to one of the UAGs or CSes, the user authenticates. If this authentication attempt is successful, then one or more secondary connections are made from the Horizon client. These secondary connections can include:

- HTTPS Tunnel used for encapsulating TCP protocols such as RDP, MMR/CDR and the client framework channel. (TCP 443).
- Blast Extreme display protocol (TCP 443 and UDP 8443). Note that UDP is optional with Blast.
- PCoIP display protocol (TCP 4172 and UDP 4172).

These secondary Horizon protocols must be routed to the same UAG or CS to which the primary Horizon protocol was routed. The reason for this is so that UAG or CS can authorize the secondary protocols based on the authenticated user session. An important security capability of UAG or CS is that it will only forward traffic into the corporate datacenter if the traffic is on behalf of an authenticated user. If the secondary protocols were to be misrouted to a different UAG or CS to the primary protocol one, they would not be authorized and would therefore be dropped in the DMZ and the connection would fail. Misrouting the secondary protocols is a common problem if the Load Balancer is not configured correctly.

Prerequisites

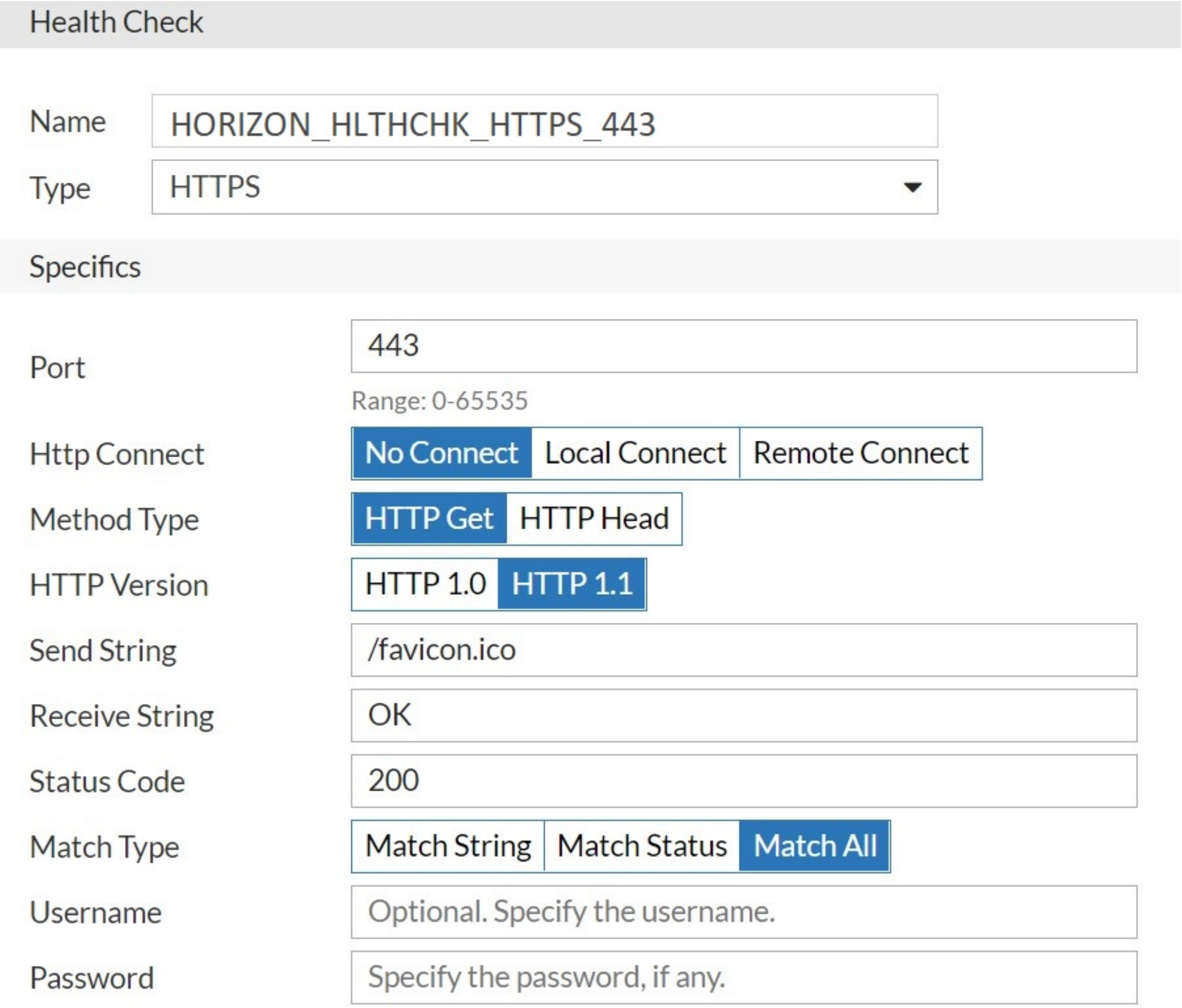
To configure FortiADC for VMware Horizon deployments, ensure the following prerequisites are met:

- The Horizon environment is up and running
- The FortiADC is deployed in your environment
- You must have Read-Write permission for Horizon and FortiADC settings.
- In this Guide, all the configurations used are for Horizon 7 and FortiADC v5.4.1.

Health Check

FortiADC uses health checks to poll the members of the real server pool (UAGs or CSs) to test whether an application is available. You can also configure additional health checks to poll related servers (UAGs or CSs), and you can include results for both in the health check rule. The primary Horizon protocol uses HTTPS with port 443, so you can create Health Check with type HTTPS and port 443.

1. Go to **Shared Resources > Health Check** and click the **Create New** button.
2. Fill in the name, select **Type to HTTPS**, set port to **443**, and set the Method Type to **HTTP Get**.



Health Check

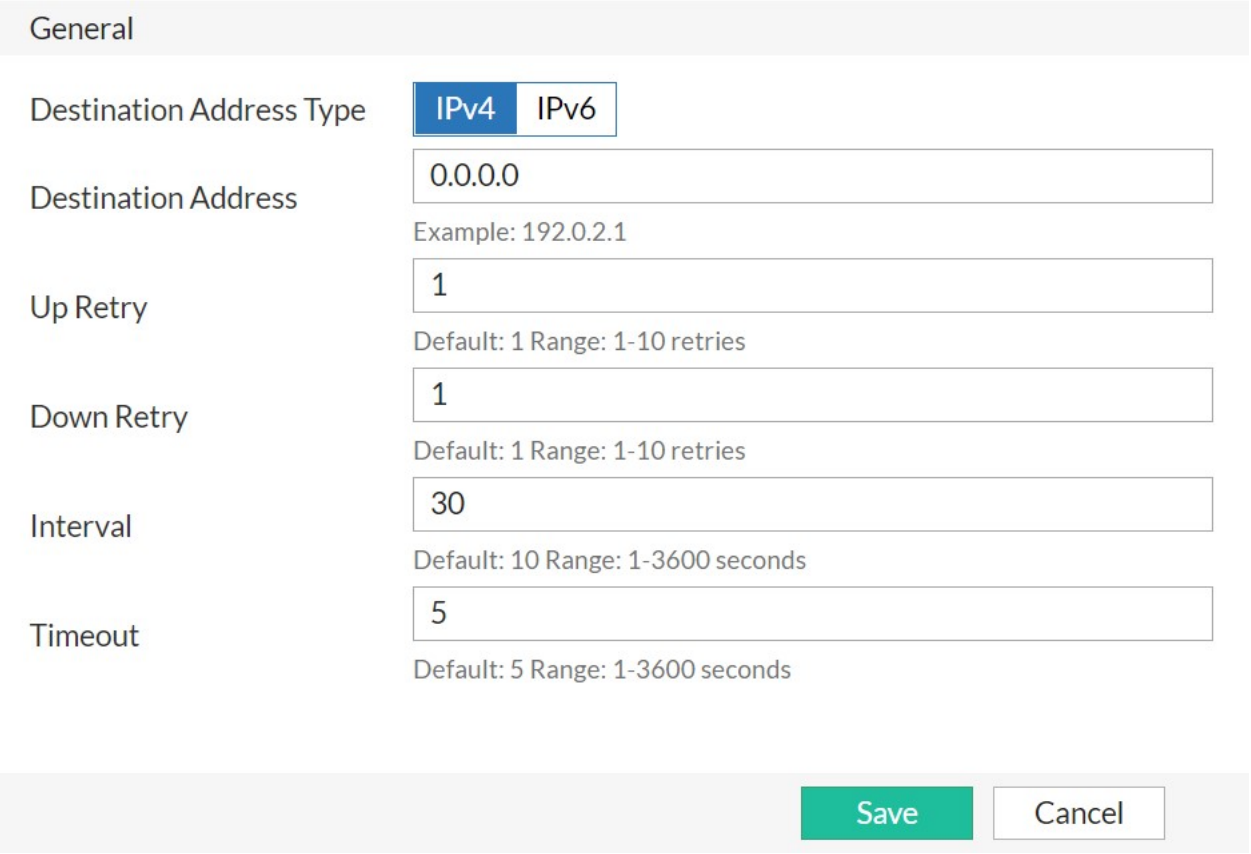
Name	HORIZON_HLTHCHK_HTTPS_443
Type	HTTPS

Specifics

Port	443 Range: 0-65535
Http Connect	[✓ No Connect] Local Connect Remote Connect
Method Type	[✓ HTTP Get] HTTP Head
HTTP Version	HTTP 1.0 [✓ HTTP 1.1]
Send String	/favicon.ico
Receive String	OK
Status Code	200
Match Type	Match String Match Status [✓ Match All]
Username	Optional. Specify the username.
Password	Specify the password, if any.

3. Set the Send String to **/favicon.ico**, set the Receive String to **OK**, set the Status Code to 200, change the Match Type to **Match All**.
4. Enable all the SSL Ciphers by checking all the boxes.

5. Set Interval to **30** and keep other fields to the default values.



General

Destination Address Type: IPv4 (selected) | IPv6

Destination Address: 0.0.0.0
Example: 192.0.2.1

Up Retry: 1
Default: 1 Range: 1-10 retries

Down Retry: 1
Default: 1 Range: 1-10 retries

Interval: 30
Default: 10 Range: 1-3600 seconds

Timeout: 5
Default: 5 Range: 1-3600 seconds

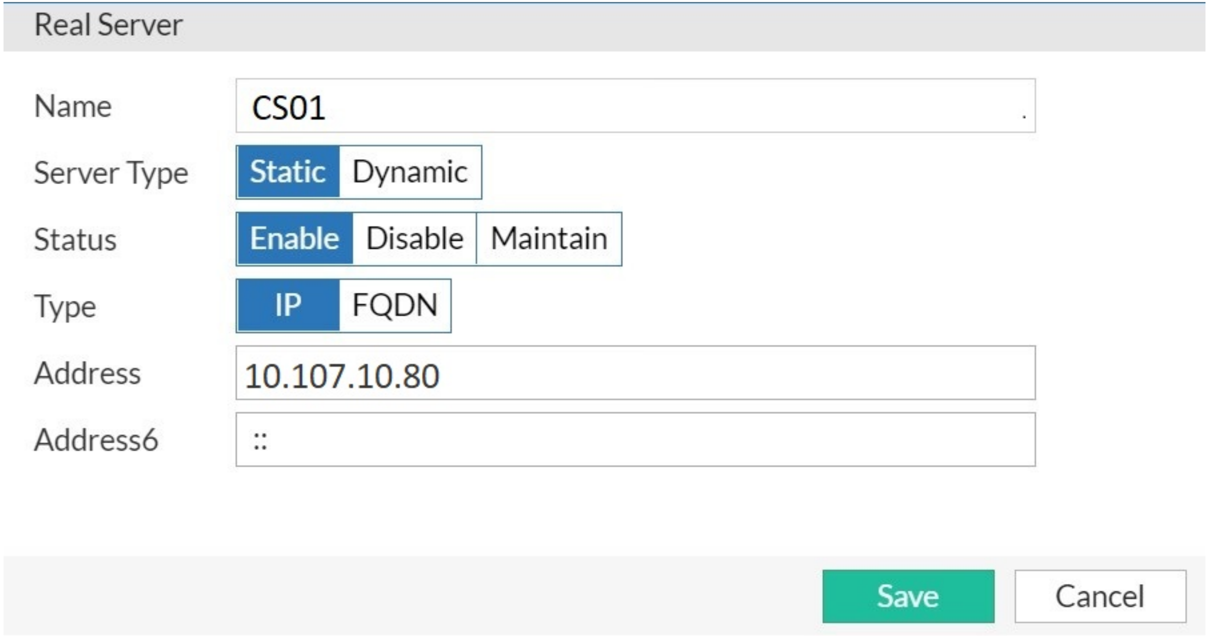
CLI Example:

```
config system health-check
   edit "HORIZON_HLTHCK_HTTPS_443"
      set type https
      set port 443
      set method-type http_get
      set send-string /favicon.ico
      set receive-string OK
      set match-type match_all
      set ssl-ciphers ECDHE-ECDSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-SHA384 ECDHEECDSA-
            AES256-SHA ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-SHA256ECDHE-ECDSA-
            AES128-SHA ECDHE-ECDSA-DES-CBC3-SHA ECDHE-ECDSA-RC4-SHA ECDHERSA-AES256-GCM-
            SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-SHA DHE-RSAAES256-GCM-SHA384 DHE-
            RSA-AES256-SHA256 DHE-RSA-AES256-SHA AES256-GCM-SHA384AES256-SHA256 AES256-SHA
            ECDHE-RSA-AES128-GCM-SHA256 ECDHE-RSA-AES128-SHA256ECDHE-RSA-AES128-SHA DHE-RSA-
            AES128-GCM-SHA256 DHE-RSA-AES128-SHA256 DHE-RSAAES128-SHA AES128-GCM-SHA256
            AES128-SHA256 AES128-SHA ECDHE-RSA-RC4-SHA RC4-SHA RC4-MD5 ECDHE-RSA-DES-CBC3-SHA
            EDH-RSA-DES-CBC3-SHA DES-CBC3-SHA eNULL
      set local-cert Factory
   next
end
```

Real Server

Real servers are physical servers that are used to form real server pools. In this guide, the UAGs or CSs are real servers that are load balanced by FortiADC.

1. Go to **Server Load Balance > Real Server Pool > Real Server**, click the **Create New** button.
2. Fill in the name and address.
3. Repeat the above steps to create other real servers.



Real Server

Name: CS01

Server Type: Static Dynamic (Static selected)

Status: Enable Disable Maintain (Enable selected)

Type: IP FQDN (IP selected)

Address: 10.107.10.80

Address6: ::

CLI Example:

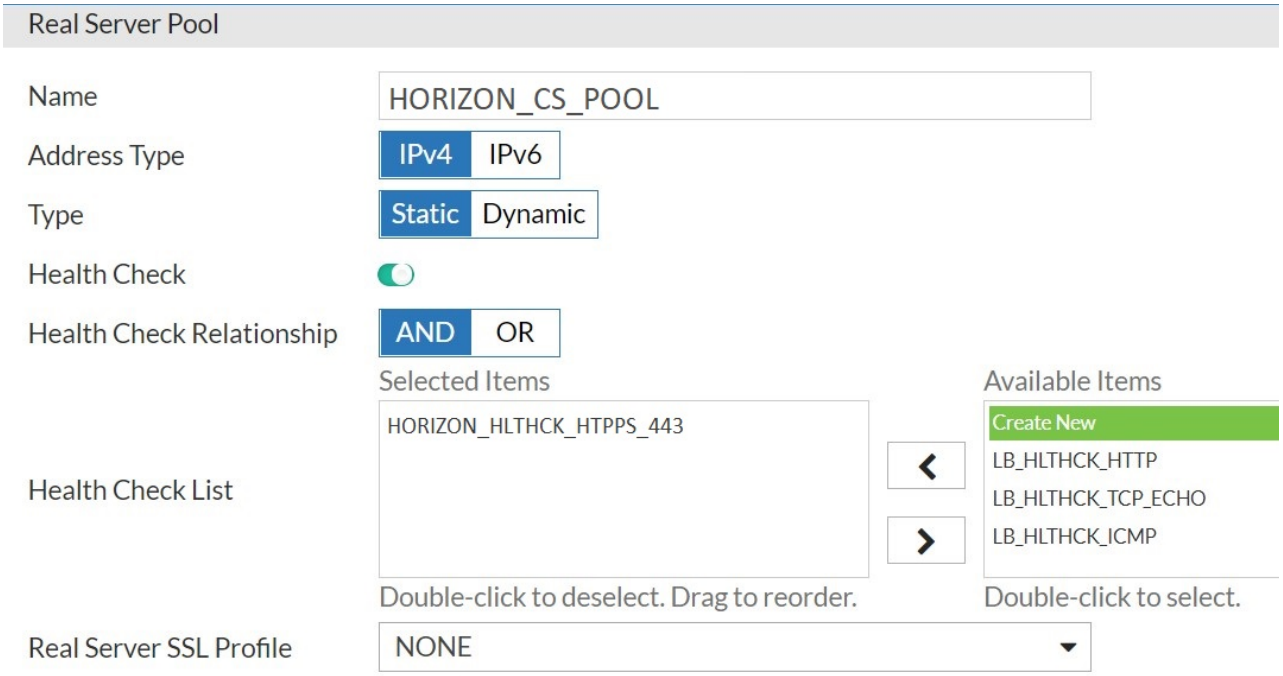
```
config load-balance real-server
   edit "CS01"
      set ip 10.107.10.80
   next
   edit "CS02"
      set ip 10.107.10.81
   next
end
```

Real Server Pool

Real server pools are groups of real servers that host the applications that you load balance.

1. Go to **Server Load Balance > Real Server Pool > Real Server Pool**, click the **Create New** button.

2. Fill the Name, enable the Health Check and select the Horizon health check created above. Then click the **Save** button.

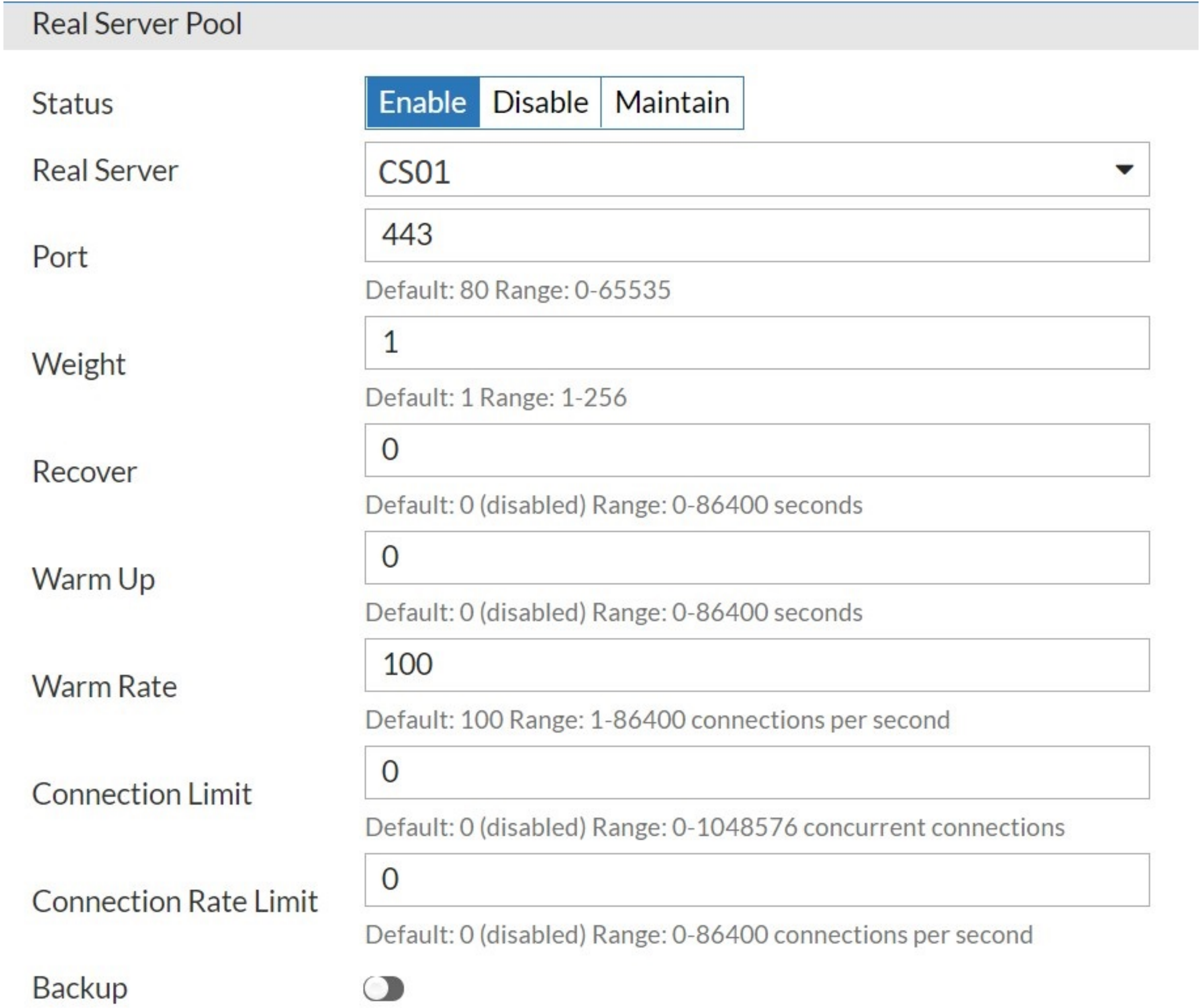


Real Server Pool

Name	HORIZON_CS_POOL
Address Type	IPv4 IPv6
Type	Static Dynamic
Health Check	●
Health Check Relationship	AND OR
Health Check List	Selected Items: HORIZON_HLTHCK_HTPPS_443 Available Items: Create New, LB_HLTHCK_HTTP, LB_HLTHCK_TCP_ECHO, LB_HLTHCK_ICMP
Real Server SSL Profile	NONE

3. Find the saved real server pool and edit it.
4. Click the **Create New** button to create the member of the real server pool.

5. Select the Real Server and set the Port to **443**. The system uses Port 0 as a “wildcard” port. When configured to use Port 0, the system uses the destination port from the client request.



Real Server Pool

Status: [✓ Enable] Disable Maintain

Real Server: CS01

Port: 443
Default: 80 Range: 0-65535

Weight: 1
Default: 1 Range: 1-256

Recover: 0
Default: 0 (disabled) Range: 0-86400 seconds

Warm Up: 0
Default: 0 (disabled) Range: 0-86400 seconds

Warm Rate: 100
Default: 100 Range: 1-86400 connections per second

Connection Limit: 0
Default: 0 (disabled) Range: 0-1048576 concurrent connections

Connection Rate Limit: 0
Default: 0 (disabled) Range: 0-86400 connections per second

Backup: ○

6. Add other real servers.

CLI Example:

```
config load-balance pool
   edit "HORIZON_CS_POOL"
      set health-check-ctrl enable
      set health-check-list HORIZON_HLTHCK_HTTPS_443
      set real-server-ssl-profile NONE
      config pool_member
         edit 1
            set pool_member_service_port 0
            set pool_member_cookie rs1
            set real-server CS01
         next
         edit 2
            set pool_member_service_port 0
            set pool_member_cookie rs1
            set real-server CS02
         next
      end
   next
end
```

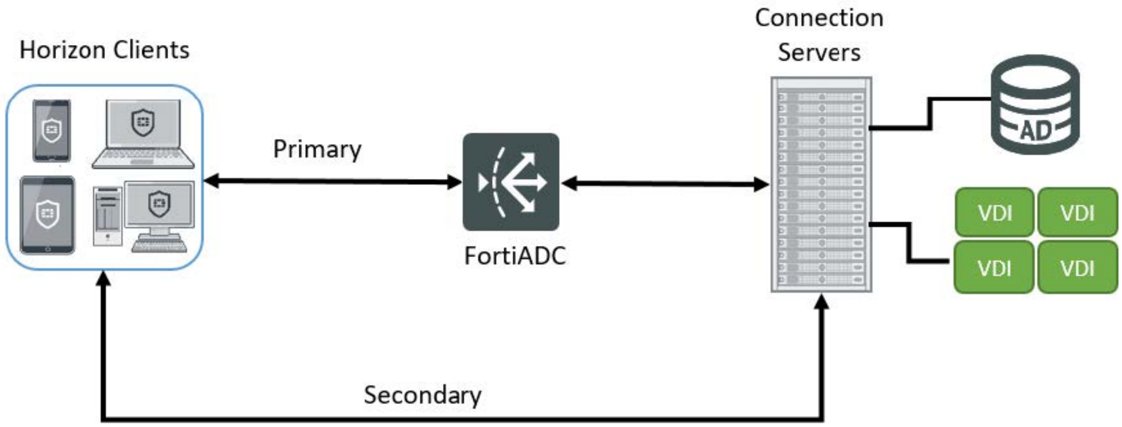
Load Balancing for Connection Servers

There are two types of Horizon Clients: one is the internal type which is in the internal network and can be trusted; the other is the external type as shown in Figure 2, and requires more security consideration.

Internal Clients

For this type clients, you don’t need to load balancing all the protocol packets for the CSs. You can only load balancing the primary protocol packets, then the following secondary protocol packets can be sent to the CS directly, and not pass through FortiADC.

Figure 2: Load Balancing Internal CS

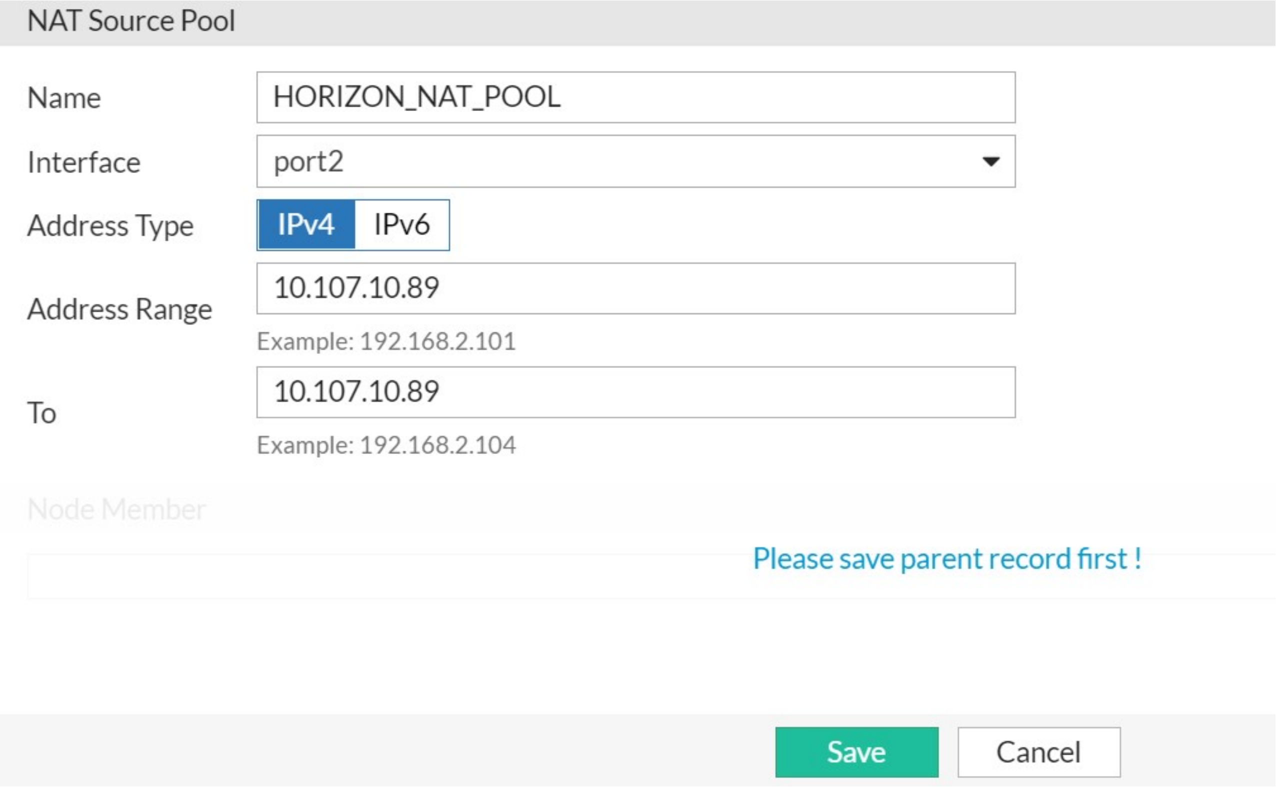


The FortiADC supports multiple Packet Forwarding Method. In this case, you can use the Full NAT select which will rewrite both the source and destination IP addresses. You would first need to create the NAT Source Pool

NAT Source Pool

1. Go to **Server Load Balance > Virtual Server > NAT Source Pool**, click the **Create New** button.

2. Fill in the Name, select the Interface to receive responses from the backend server and set the Address Range. Then click the **Save** button.



NAT Source Pool

Name: HORIZON_NAT_POOL

Interface: port2

Address Type: IPv4 (selected) | IPv6

Address Range: 10.107.10.89

Example: 192.168.2.101

To: 10.107.10.89

Example: 192.168.2.104

Node Member

Please save parent record first !

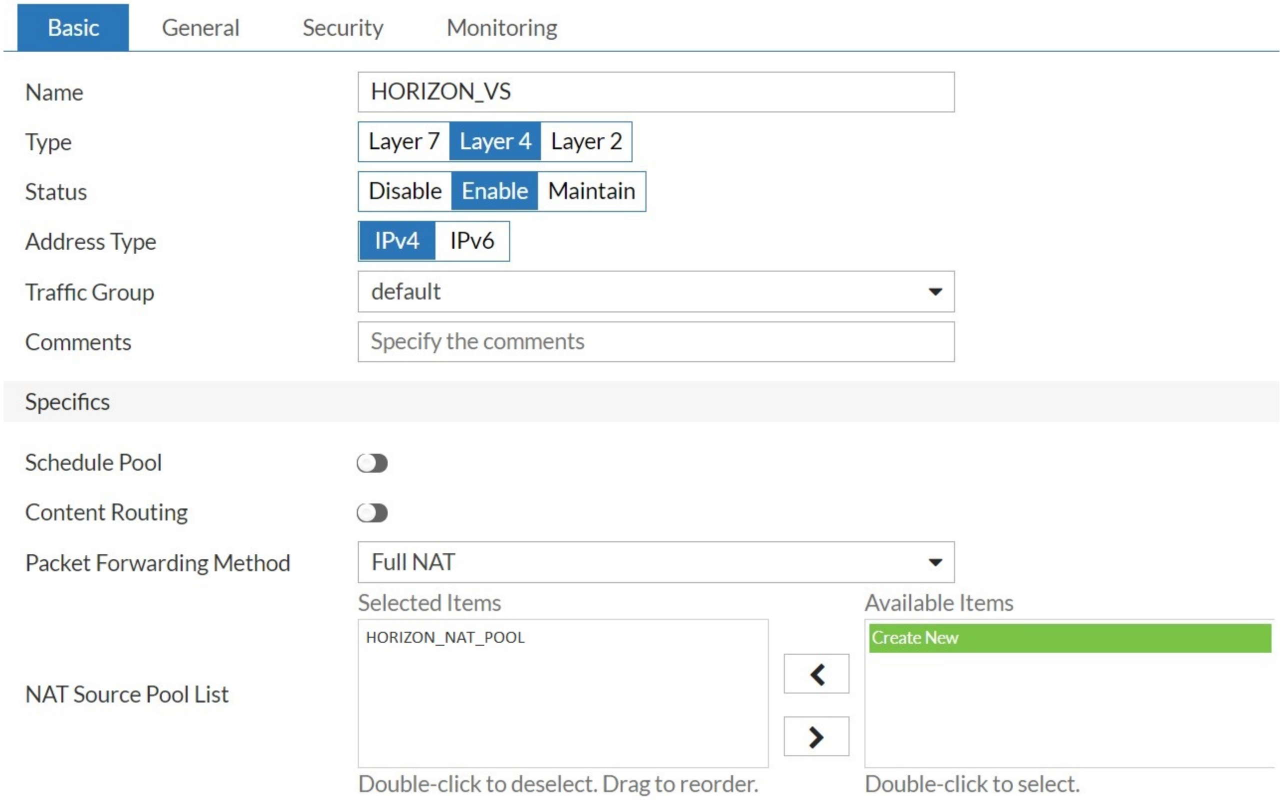
CLI Example:

```
config load-balance ippool
   edit "HORIZION_NAT_POOL"
      set interface port2
      set ip-min 10.107.10.89
      set ip-max 10.107.10.89
      config node-member
      end
   next
end
```

Virtual Server using TCP profile

1. Go to **Server Load Balance > Virtual Server > Virtual Server**, click the **Create New -> Advanced Mode** button.

2. In the Basic settings, fill the Name, select the Full NAT of Packet Forwarding Method and select the NAT Source Pool created above.



Basic | General | Security | Monitoring

Name	HORIZON_VS
Type	Layer 7 [✓ Layer 4] Layer 2
Status	Disable [✓ Enable] Maintain
Address Type	[✓ IPv4] IPv6
Traffic Group	default
Comments	Specify the comments

Specifics

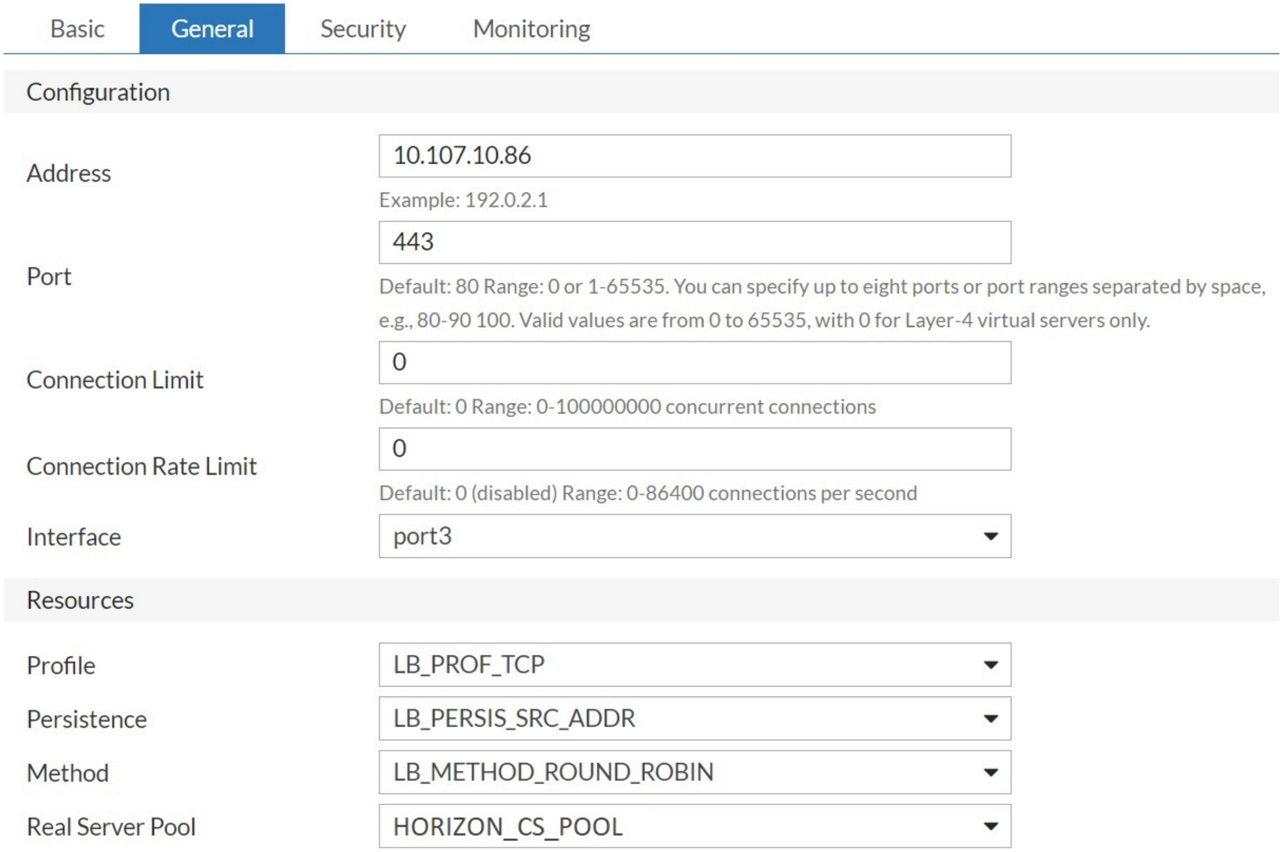
Schedule Pool	○
Content Routing	○
Packet Forwarding Method	Full NAT
NAT Source Pool List	Selected Items: HORIZON_NAT_POOL Available Items: Create New

Double-click to deselect. Drag to reorder.

Double-click to select.

3. In General settings, set the virtual server Address and Port, and select the Interface in which the virtual server will work. Use the default profile LB_PROF_TCP, you can select one Method which means differentload balancing methods. For keeping the primary protocol packets from one client to the same CS, you should select one Persistence. Select the Real Server Pool created above.

4. Keep other fields to the default values or you can change them as you need.



Configuration

Address: 10.107.10.86
Example: 192.0.2.1

Port: 443
Default: 80 Range: 0 or 1-65535. You can specify up to eight ports or port ranges separated by space, e.g., 80-90 100. Valid values are from 0 to 65535, with 0 for Layer-4 virtual servers only.

Connection Limit: 0
Default: 0 Range: 0-100000000 concurrent connections

Connection Rate Limit: 0
Default: 0 (disabled) Range: 0-86400 connections per second

Interface: port3

Resources

Profile: LB_PROF_TCP

Persistence: LB_PERSIS_SRC_ADDR

Method: LB_METHOD_ROUND_ROBIN

Real Server Pool: HORIZON_CS_POOL

Now the virtual server has been created, and in your Horizon Client, you can add the CS with virtual server IP address. The FortiADC will load balance the primary Horizon protocol packets to the available CSs what the Health Check will do periodically. After authenticating user successfully, the Horizon Client will send the secondary Horizon protocol packets to the CS (selected by FortiADC) directly and not pass through FortiADC.

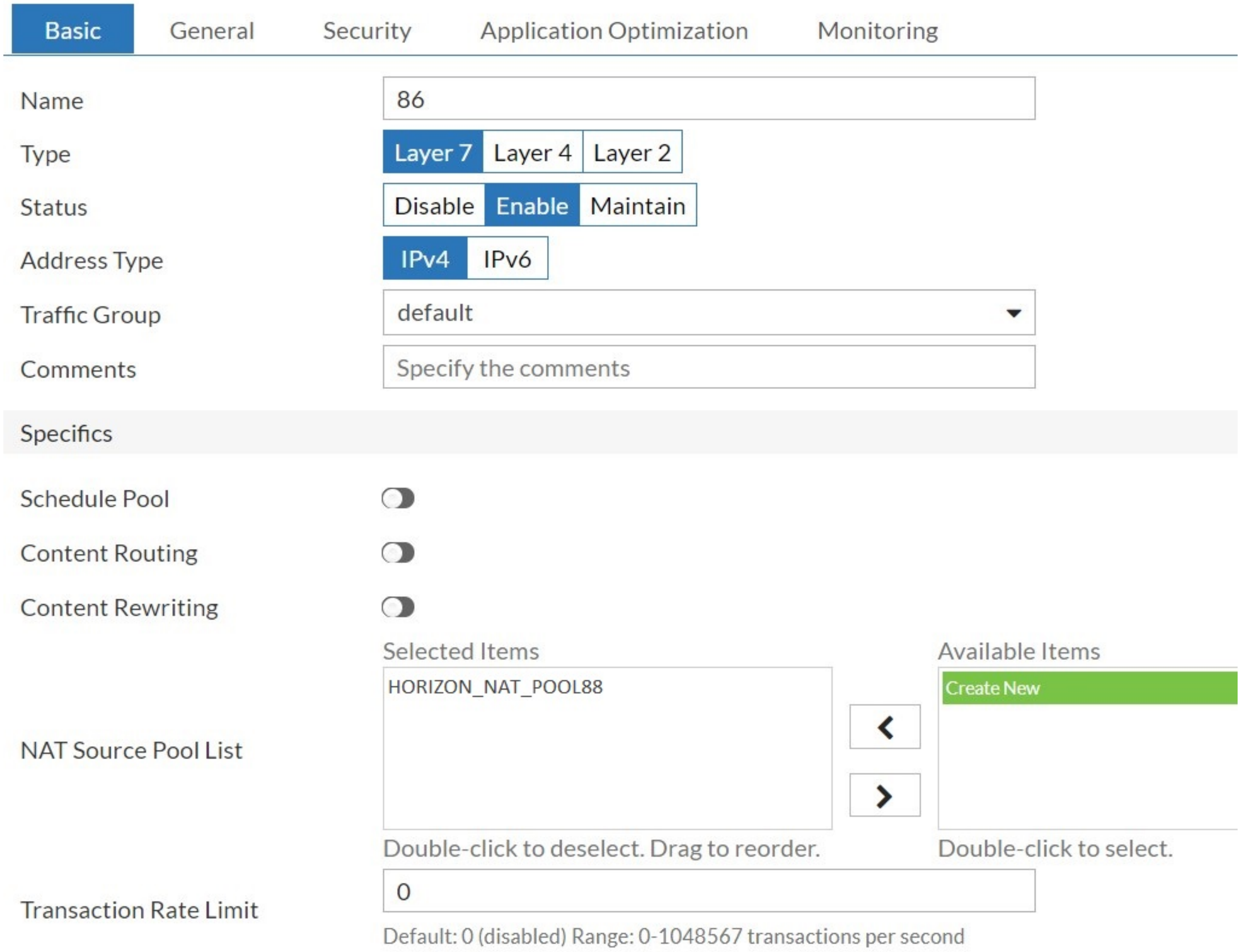
CLI Example:

```
config load-balance virtual-server
   edit "HORIZON_TCP_VS"
      set packet-forwarding-method FullNAT
      set interface port3
      set ip 10.107.10.86
      set port 443
      set load-balance-profile LB_PROF_TCP
      set load-balance-persistence LB_PERSIS_SRC_ADDR
      set load-balance-method LB_METHOD_ROUND_ROBIN
      set load-balance-pool HORIZON_CS_POOL
      set ippool-list HORIZION_NAT_POOL
      set traffic-group default
   next
end
```

Virtual Server using HTTPS profile

Users can also use L7 HTTPS Virtual server to load-balance Connection Servers.

1. Go to **Server Load Balance > Virtual Server > Virtual Server**, click the **Create New > Advanced Mode** button.
2. In the Basic settings, fill the Name, select the Type Layer 7. If need to use SNAT please set ippool.



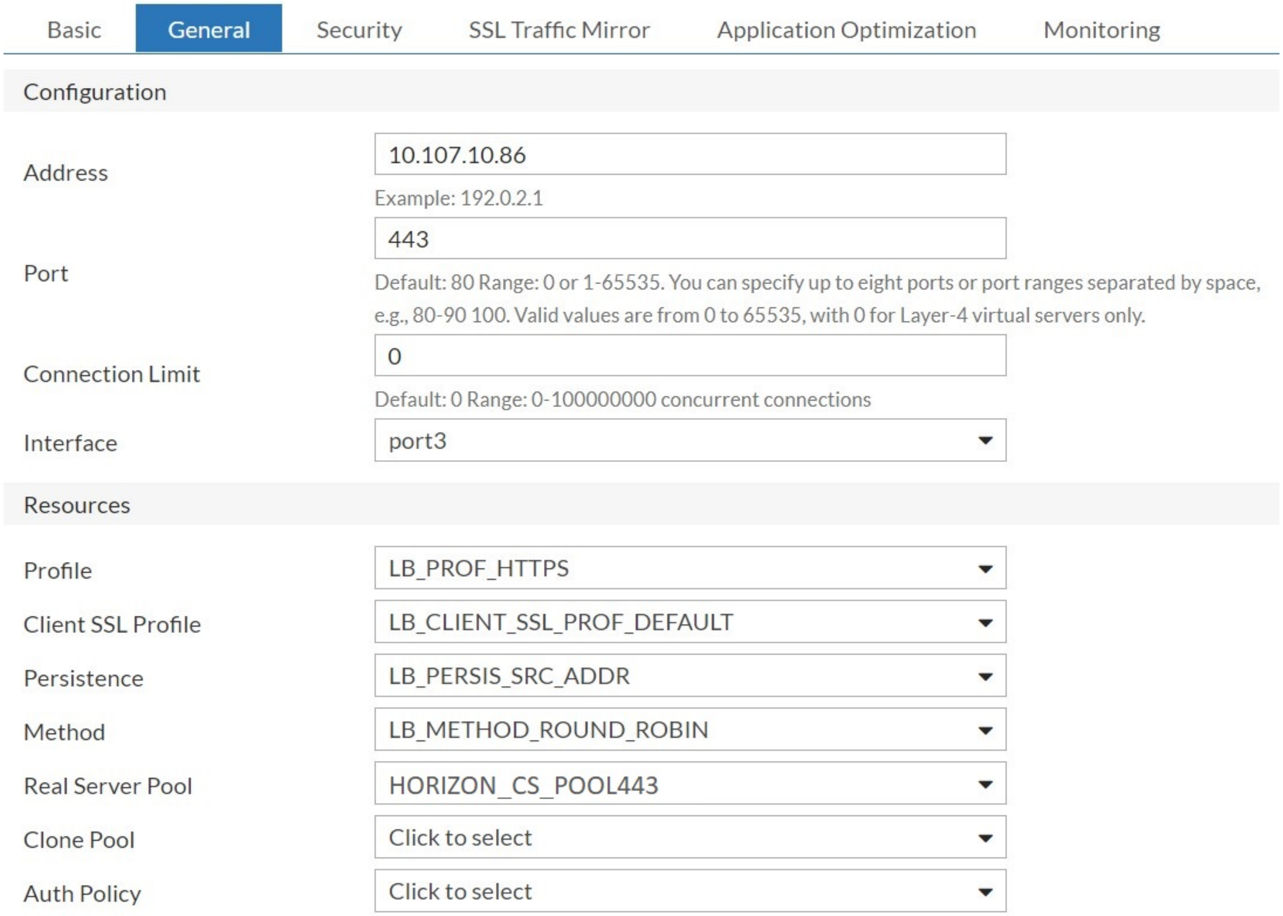
Name	86
Type	[✓ Layer 7] Layer 4 Layer 2
Status	Disable [✓ Enable] Maintain
Address Type	[✓ IPv4] IPv6
Traffic Group	default
Comments	Specify the comments

Specifics

Schedule Pool	○
Content Routing	○
Content Rewriting	○
NAT Source Pool List	Selected Items: HORIZON_NAT_POOL88 Double-click to deselect. Drag to reorder. Available Items: Create New Double-click to select.
Transaction Rate Limit	0 Default: 0 (disabled) Range: 0-1048567 transactions per second

3. In General settings, set the virtual server Address and Port, and select the Interface in which the virtual server will work. Use profile LB_PROF_HTTPS and set Client SSL Profile. You can select one Method for different load balancing methods. For keeping the primary protocol packets from one client to the same CS, you should select one Persistence. Select the Real Server Pool created for Connection server HTTPS service.

4. Keep other fields to the default values or you can change as you need.



Configuration

Address: 10.107.10.86

Example: 192.0.2.1

Port: 443

Default: 80 Range: 0 or 1-65535. You can specify up to eight ports or port ranges separated by space, e.g., 80-90 100. Valid values are from 0 to 65535, with 0 for Layer-4 virtual servers only.

Connection Limit: 0

Default: 0 Range: 0-100000000 concurrent connections

Interface: port3

Resources

Profile: LB_PROF_HTTPS

Client SSL Profile: LB_CLIENT_SSL_PROF_DEFAULT

Persistence: LB_PERSIS_SRC_ADDR

Method: LB_METHOD_ROUND_ROBIN

Real Server Pool: HORIZON_CS_POOL443

Clone Pool: Click to select

Auth Policy: Click to select

Now the virtual server has been created, and in your Horizon Client, you can add the CS with virtual server IP address. The FortiADC will load balance the primary Horizon protocol packets to the available CSes what the Health Check will do periodically. After authenticating user successfully, the Horizon Client will send the secondary Horizon protocol packets to the CS (selected by FortiADC) directly and not pass through FortiADC.

CLI Example:

ippool (optional)

```
config load-balance ippool
   edit "HORIZION_NAT_POOL88"
      set interface port2
      set ip-min 10.107.10.88
      set ip-max 10.107.10.88
      config node-member
      end
   next
end
```

pool

```
config load-balance pool
   edit "HORIZON_CS_POOL443"
```

```
        set real-server-ssl-profile LB_RS_SSL_PROF_DEFAULT
        config pool_member
          edit 1
            set pool_member_service_port 443
            set pool_member_cookie rs1
            set real-server CS01
          next
          edit 2
            set pool_member_service_port 443
            set pool_member_cookie rs1
            set real-server CS02
          next
        end
    next
end
```

virtual server

```
config load-balance virtual-server
    edit "86"
        set type l7-load-balance
        set interface port3
        set ip 10.107.10.86
        set port 443
        set load-balance-profile LB_PROF_HTTPS
        set client-ssl-profile LB_CLIENT_SSL_PROF_DEFAULT
        set load-balance-persistence LB_PERSIS_SRC_ADDR
        set load-balance-method LB_METHOD_ROUND_ROBIN
        set load-balance-pool HORIZON_CS_POOL443
        set ippool-list HORIZION_NAT_POOL88
        set traffic-group default
    next
end
```

External Clients

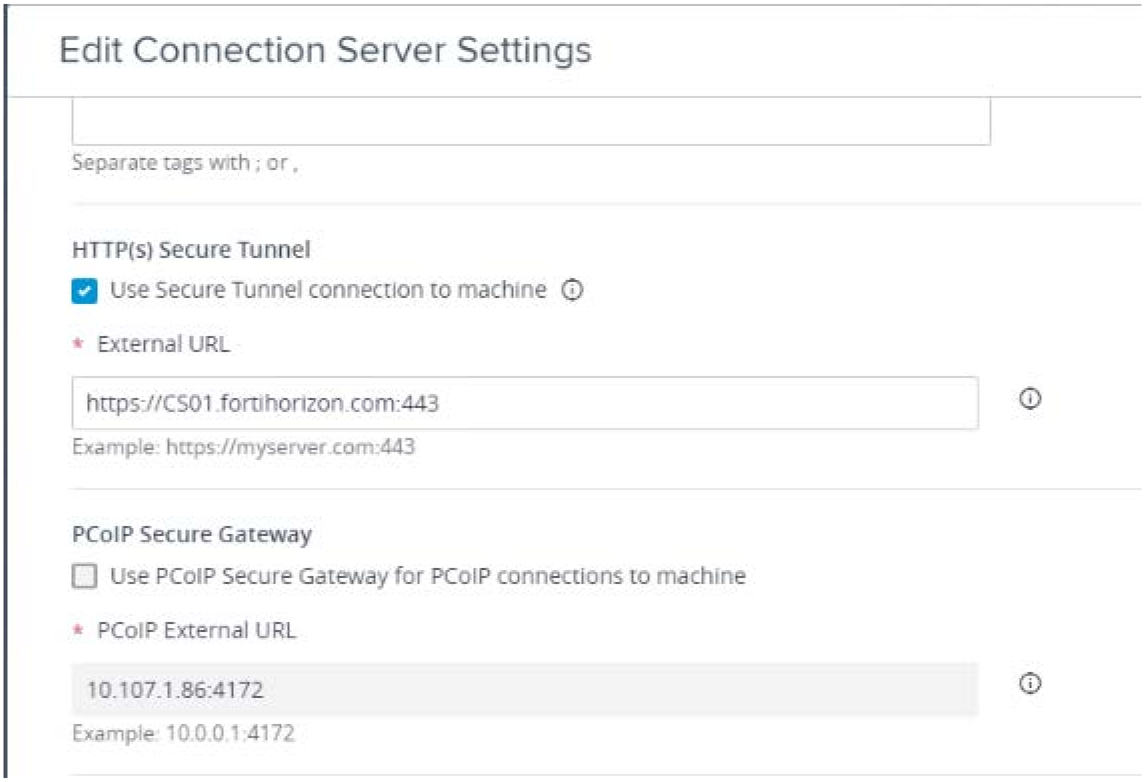
For this type of client, all the Horizon protocol packets should pass through the FortiADC. There are three different session affinity methods:

Method 1: Source IP Affinity

This is the simplest configuration as it uses standard port numbers and a single load balanced VIP. It relies on the FortiADC to route secondary protocols to the same CS appliance as was selected for the primary Horizon protocol. It can do this on the basis of repeat connections coming from the same Horizon client IP address.

In this example, the IP address of virtual server is 10.107.1.86 (cs.fortihorizon.com). And you should change the configurations of all the CS's as shown in the below table.

CS Appliance	Configuration Item	Value
CS01	tunnelExternalURL	https://cs.fortihorizon.com:443
	blastExternalURL	https://cs.fortihorizon.com:8443
	pcoipExternalURL	10.107.1.86:4172
CS02	tunnelExternalURL	https://cs.fortihorizon.com:443
	blastExternalURL	https://cs.fortihorizon.com:8443
	pcoipExternalURL	10.107.1.86:4172



Edit Connection Server Settings

Separate tags with ; or ,

HTTP(s) Secure Tunnel

☑ Use Secure Tunnel connection to machine

* External URL

https://CS01.fortihorizon.com:443

Example: https://myserver.com:443

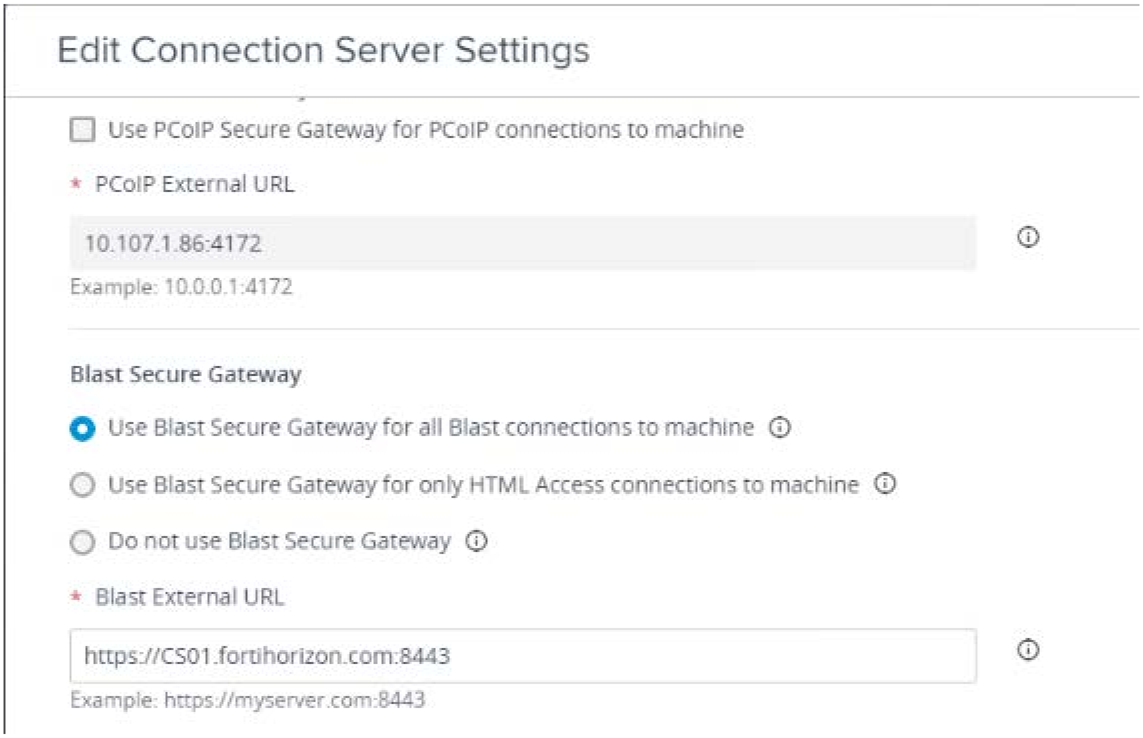
PCoIP Secure Gateway

□ Use PCoIP Secure Gateway for PCoIP connections to machine

* PCoIP External URL

10.107.1.86:4172

Example: 10.0.0.1:4172



Edit Connection Server Settings

☐ Use PCoIP Secure Gateway for PCoIP connections to machine

* PCoIP External URL

10.107.1.86:4172

Example: 10.0.0.1:4172

Blast Secure Gateway

● Use Blast Secure Gateway for all Blast connections to machine

○ Use Blast Secure Gateway for only HTML Access connections to machine

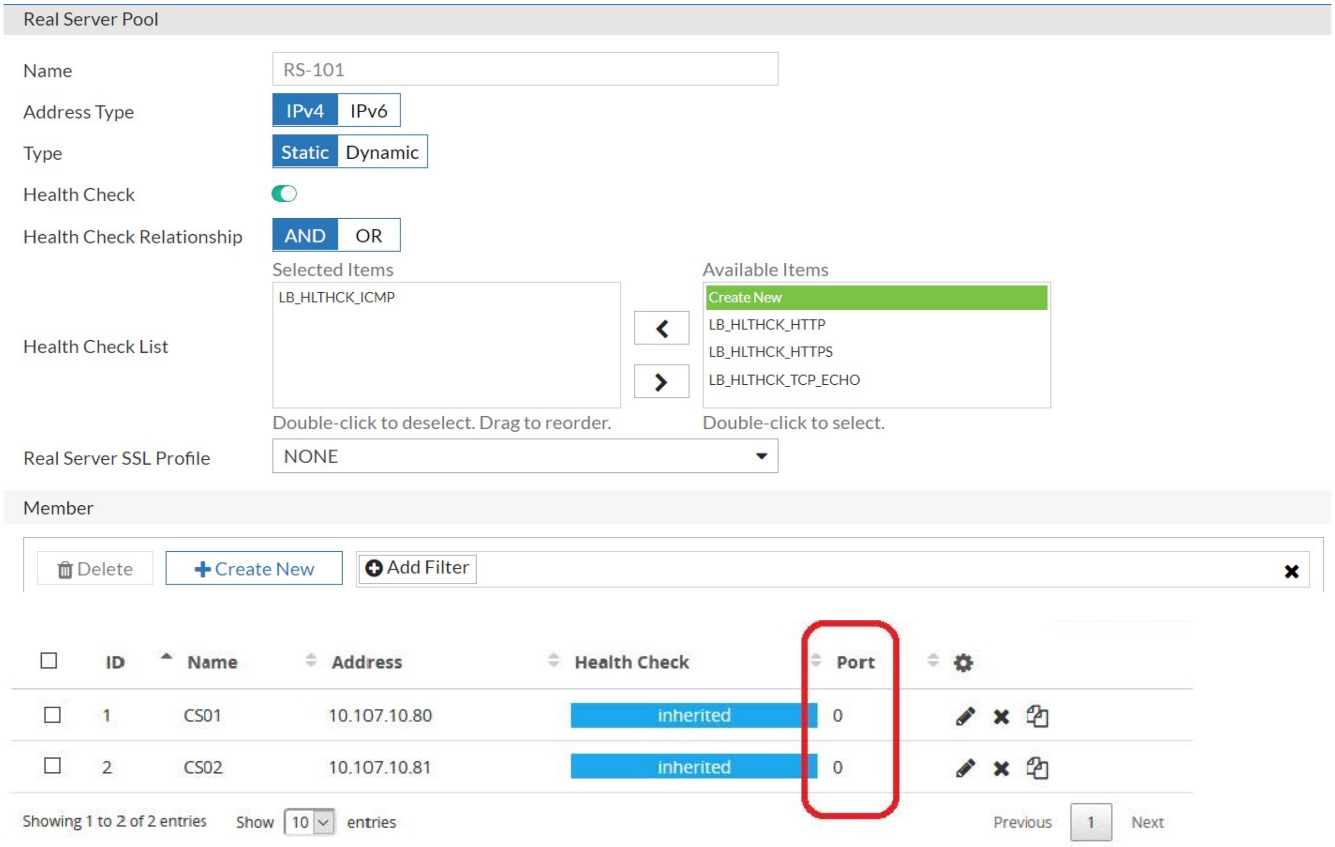
○ Do not use Blast Secure Gateway

* Blast External URL

https://CS01.fortihorizon.com:8443

Example: https://myserver.com:8443

You need to create two virtual-server with same VIP, different ports and different profiles. And you should change the Port to 0 for the members of Real Server Pool.



Real Server Pool

Name	RS-101
Address Type	[✓ IPv4] IPv6
Type	[✓ Static] Dynamic
Health Check	On
Health Check Relationship	[✓ AND] OR
Health Check List	Selected Items: LB_HLTHCK_ICMP Double-click to deselect. Drag to reorder. Available Items: Create New, LB_HLTHCK_HTTP, LB_HLTHCK_HTTPS, LB_HLTHCK_TCP_ECHO Double-click to select.
Real Server SSL Profile	NONE

Member

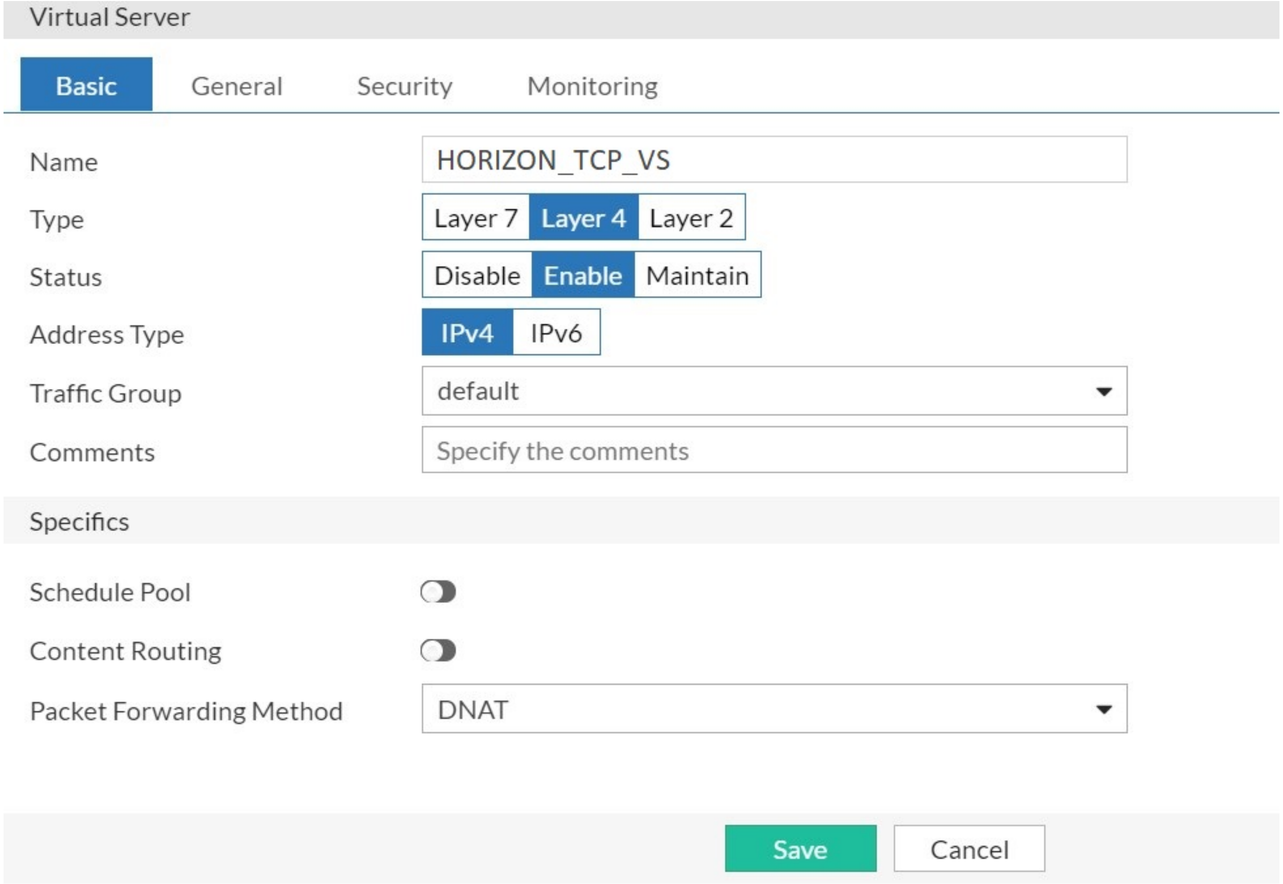
☐	ID	Name	Address	Health Check	Port	
☐	1	CS01	10.107.10.80	inherited	0	
☐	2	CS02	10.107.10.81	inherited	0	

Showing 1 to 2 of 2 entries Show 10 entries

For the external clients, you can use the DNAT Packet Forwarding Method not same as the internal clients. It will replace the destination IP address with the IP address of the backend CS selected by the FortiADC, so you need add the FortiADC interface IP as the gateway in all the used CSes, this will guarantee the response packets will route to FortiADC. According the Horizon protocols and ports, you need to create one TCP and one UDP virtual servers.

TCP Virtual Server

1. Go to **Server Load Balance > Virtual Server > Virtual Server**, click the **Create New > Advanced Mode** button.
2. In the Basic settings, fill the Name, use the default Packet Forwarding Method DNAT.


Virtual Server

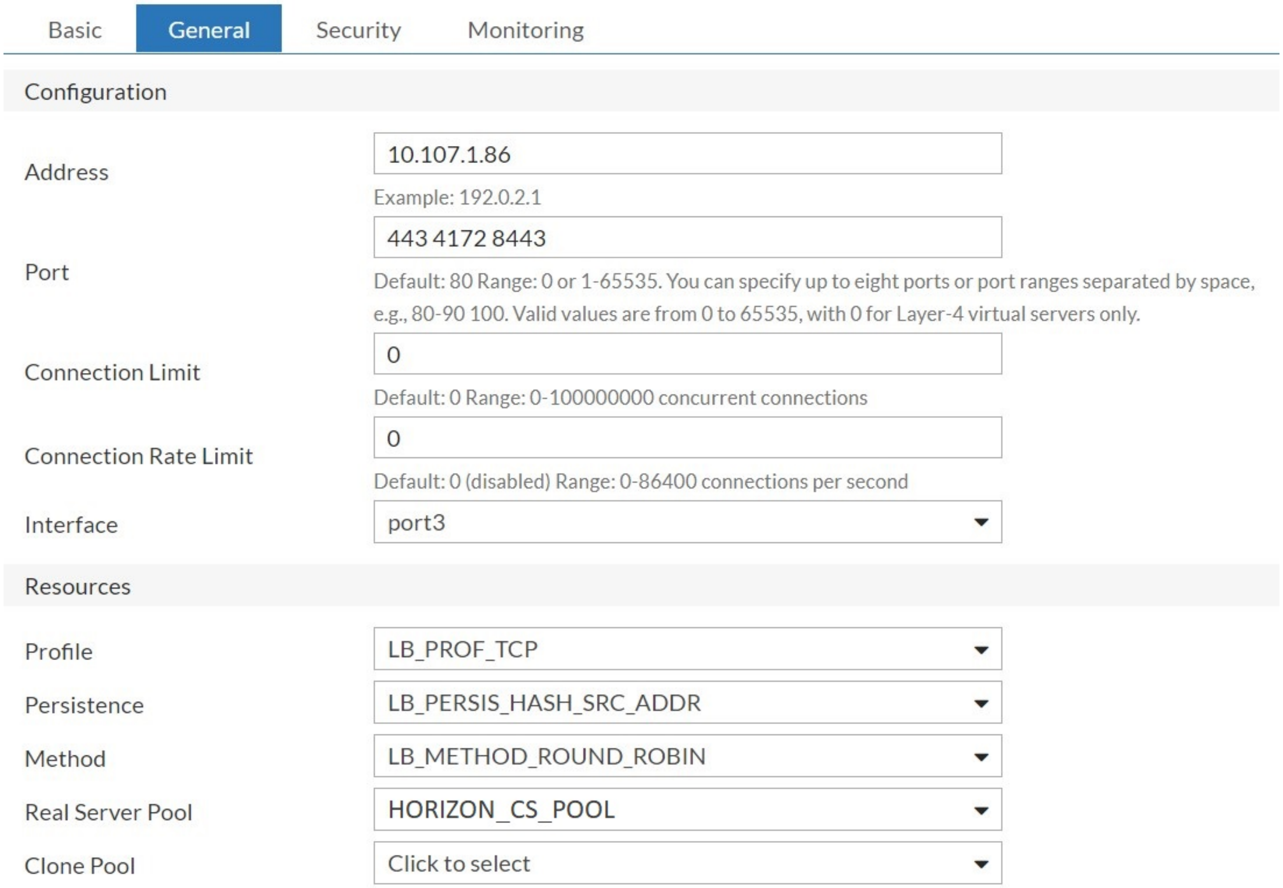
Name	HORIZON_TCP_VS
Type	Layer 7 [✓ Layer 4] Layer 2
Status	Disable [✓ Enable] Maintain
Address Type	[✓ IPv4] IPv6
Traffic Group	default
Comments	Specify the comments

Specifics

Schedule Pool	○
Content Routing	○
Packet Forwarding Method	DNAT

3. In General settings, set the virtual server Address and Port (443 4172 8443), and select the Interface in which the virtual server will work. Use the default profile LB_PROF_TCP. For keeping the primary and secondary protocol packets from one client to the same CS, you should select Persistence with LB_PERSIS_HASH_SRC_ADDR. Select the Real Server Pool created before.

4. Keep other fields to the default values or you can change them as you need.



Configuration

Address: 10.107.1.86
Example: 192.0.2.1

Port: 443 4172 8443
Default: 80 Range: 0 or 1-65535. You can specify up to eight ports or port ranges separated by space, e.g., 80-90 100. Valid values are from 0 to 65535, with 0 for Layer-4 virtual servers only.

Connection Limit: 0
Default: 0 Range: 0-100000000 concurrent connections

Connection Rate Limit: 0
Default: 0 (disabled) Range: 0-86400 connections per second

Interface: port3

Resources

Profile: LB_PROF_TCP

Persistence: LB_PERSIS_HASH_SRC_ADDR

Method: LB_METHOD_ROUND_ROBIN

Real Server Pool: HORIZON_CS_POOL

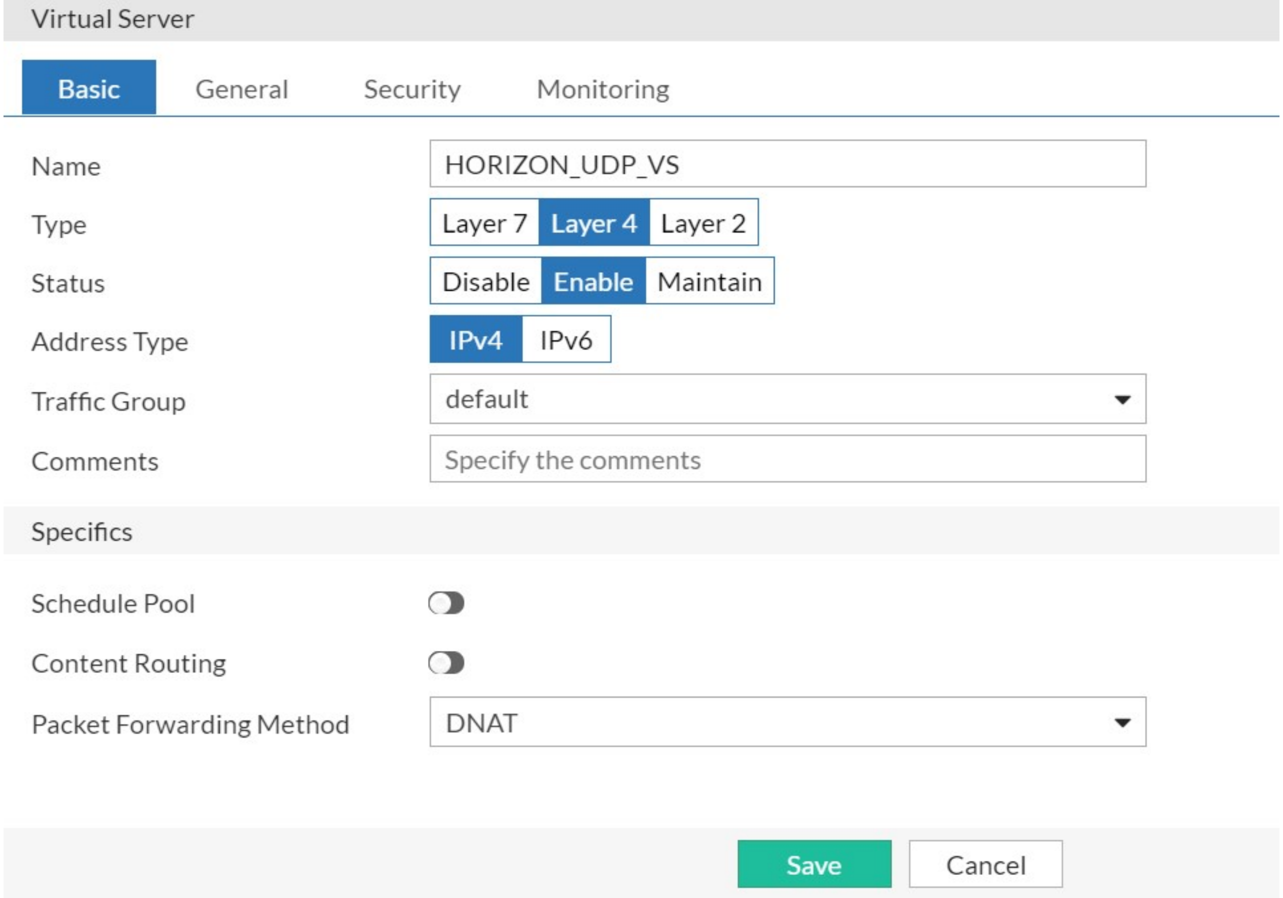
Clone Pool: Click to select

TCP virtual server CLI configuration

```
config load-balance virtual-server
   edit "HORIZON_TCP_VS"
      set interface port3
      set ip 10.107.1.86
      set port 443 4172 8443
      set load-balance-profile LB_PROF_TCP
      set load-balance-persistence LB_PERSIS_SRC_ADDR
      set load-balance-method LB_METHOD_ROUND_ROBIN
      set load-balance-pool HORIZON_CS_POOL
      set traffic-group default
   next
end
```

UDP Virtual Server

1. Go to **Server Load Balance > Virtual Server > Virtual Server**, click the **Create New > Advanced Mode** button.
2. In the Basic settings, fill the Name, use the default Packet Forwarding Method DNAT.



Virtual Server

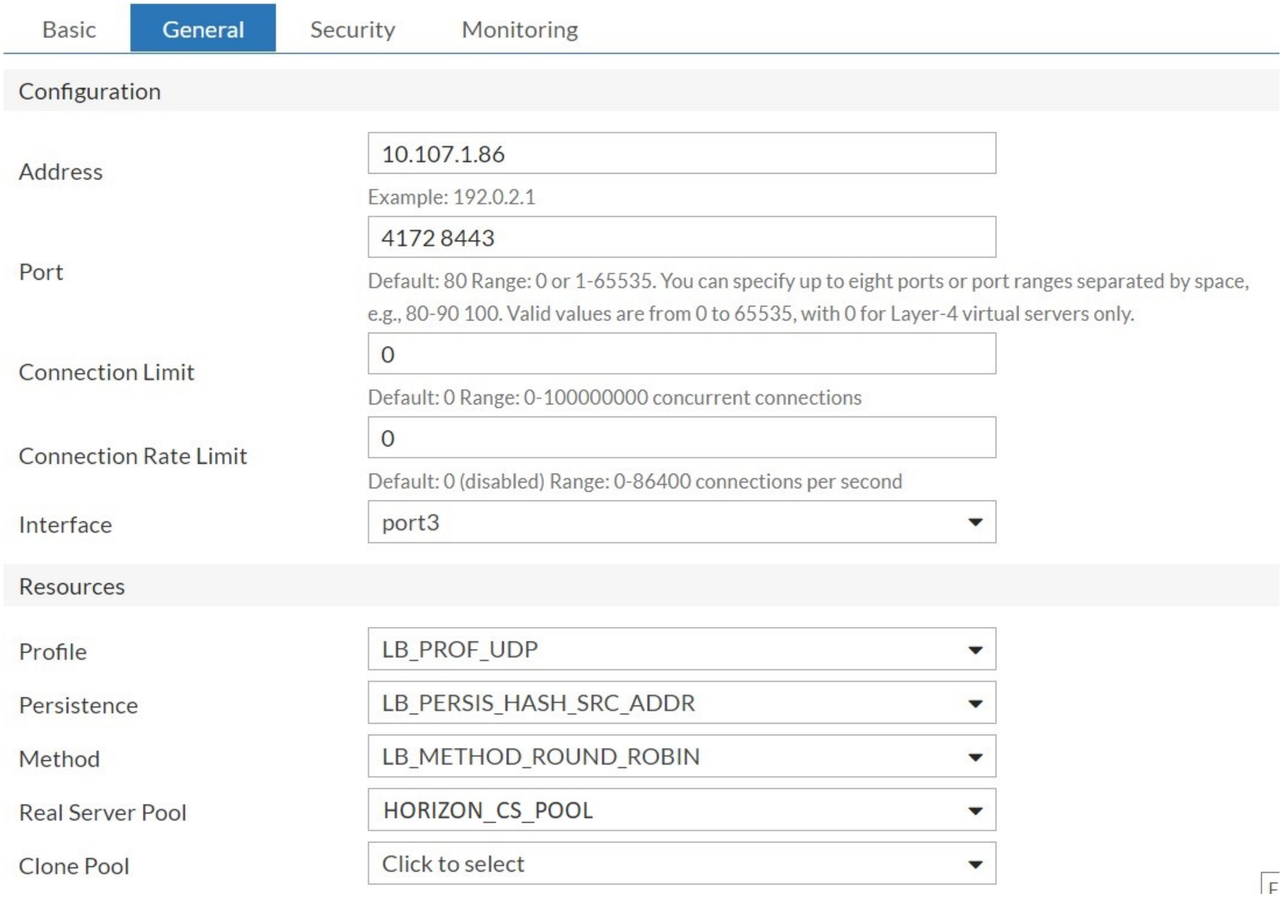
Name	HORIZON_UDP_VS
Type	Layer 7 [✓ Layer 4] Layer 2
Status	Disable [✓ Enable] Maintain
Address Type	[✓ IPv4] IPv6
Traffic Group	default
Comments	Specify the comments

Specifics

Schedule Pool	○
Content Routing	○
Packet Forwarding Method	DNAT

3. In General settings, set the virtual server Address (same as the TCP VIP) and Port (4172 8443), and select the Interface (same as TCP VS) in which the virtual server will work. Select the profile LB_PROF_UDP. For keeping the primary and secondary protocol packets from one client to the same CS, you should select Persistence with LB_ PERSIS_HASH_SRC_ADDR. Select the Real Server Pool created before.

4. Keep other fields to the default values or you can change them as you need.



Configuration

Address: 10.107.1.86
Example: 192.0.2.1

Port: 4172 8443
Default: 80 Range: 0 or 1-65535. You can specify up to eight ports or port ranges separated by space, e.g., 80-90 100. Valid values are from 0 to 65535, with 0 for Layer-4 virtual servers only.

Connection Limit: 0
Default: 0 Range: 0-100000000 concurrent connections

Connection Rate Limit: 0
Default: 0 (disabled) Range: 0-86400 connections per second

Interface: port3

Resources

Profile: LB_PROF_UDP

Persistence: LB_PERSIS_HASH_SRC_ADDR

Method: LB_METHOD_ROUND_ROBIN

Real Server Pool: HORIZON_CS_POOL

Clone Pool: Click to select

Unfortunately, this method doesn't work in all situations. For example, with certain Network Service Providers or NAT devices, the source IP address is not available for this affinity configuration. If source IP affinity can't be used in your environment, then one of the other two methods should be used as they don't rely on source IP affinity.

UDP virtual server CLI configuration

```
config load-balance virtual-server
   edit "HORIZON_UDP_VS"
      set interface port5
      set ip 10.107.1.86
      set port 4172
      set load-balance-profile LB_PROF_UDP
      set load-balance-persistence LB_PERSIS_HASH_SRC_ADDR
      set load-balance-method LB_METHOD_ROUND_ROBIN
      set load-balance-pool CS1_4172
      set traffic-group default
   next
end
```

Method 2: Multiple port number groups

Multiple port group affinity does not rely on source IP address for affinity. Instead the FortiADC is configured to route the secondary Horizon protocols based on unique port numbers assigned to each CS appliance. The primary Horizon protocol on HTTPS port 443 is load balanced to allocate the session to a specific CS appliance based on health check and load balance algorithms. The secondary connections would then be routed to the correct CS appliance based on the following FortiADC configuration table. In this method, you can select any Persistence as you need.

VIP:Port	P/S	Profile	Name	Real Servers
10.107.1.86:443	Primary	LB_PROFILE_TCP	HORIZON_VS	10.107.10.80:443 10.107.10.81:443
10.107.1.86:10443	Secondary	LB_PROFILE_TCP	CS01_HTTPS	10.107.10.80:443
10.107.1.86:10143	Secondary	LB_PROFILE_TCP	CS01_BLAST	10.107.10.80:8443
10.107.1.86:10143	Secondary	LB_PROFILE_UDP	CS01_BLAST_UDP	10.107.10.80:8443
10.107.1.86:10172	Secondary	LB_PROFILE_TCP	CS01_PCOIP	10.107.10.80:4172
10.107.1.86:10172	Secondary	LB_PROFILE_UDP	CS01_PCOIP_UDP	10.107.10.80:4172
10.107.1.86:11443	Secondary	LB_PROFILE_TCP	CS02_HTTPS	10.107.10.81:443
10.107.1.86:10243	Secondary	LB_PROFILE_TCP	CS02_BLAST	10.107.10.81:8443
10.107.1.86:10243	Secondary	LB_PROFILE_UDP	CS02_BLAST_UDP	10.107.10.81:8443
10.107.1.86:10272	Secondary	LB_PROFILE_TCP	CS02_PCOIP	10.107.10.81:4172
10.107.1.86:10272	Secondary	LB_PROFILE_UDP	CS02_PCOIP_UDP	10.107.10.81:4172

CS Configuration for External URLs for this configuration would be as shown in this table.

CS Appliance	Configuration Item	Value
CS01	tunnelExternalURL	https://cs.fortihorizon.com:10443
	blastExternalURL	https://cs.fortihorizon.com:10143
	pcoipExternalURL	10.107.1.86:10172
CS02	tunnelExternalURL	https://cs.fortihorizon.com:11443
	blastExternalURL	https://cs.fortihorizon.com:10243
	pcoipExternalURL	10.107.1.86:10272

```
config load-balance virtual-server
   edit "CS01_HTTPS"
      set interface port5
      set ip 10.107.1.86
      set port 10443
      set load-balance-profile LB_PROF_TCP
      set load-balance-method LB_METHOD_ROUND_ROBIN
      set load-balance-pool CS1_443
      set traffic-group default
   next
```

```
end

config load-balance virtual-server
   edit "CS01_BLAST_UDP"
      set interface port5
      set ip 10.107.1.86
      set port 10143
      set load-balance-profile LB_PROF_UDP
      set load-balance-persistence LB_PERSIS_SRC_ADDR
      set load-balance-method LB_METHOD_ROUND_ROBIN
      set load-balance-pool CS1_8443
      set traffic-group default
   next
end

config load-balance virtual-server
   edit "CS01_PCOIP"
      set interface port5
      set ip 10.107.1.86
      set port 10172
      set load-balance-profile LB_PROF_TCP
      set load-balance-persistence LB_PERSIS_SRC_ADDR
      set load-balance-method LB_METHOD_ROUND_ROBIN
      set load-balance-pool CS1_4172
      set traffic-group default
   next
end

config load-balance virtual-server
   edit "CS01_PCOIP_UDP"
      set interface port5
      set ip 10.107.1.86
      set port 10172
      set load-balance-profile LB_PROF_UDP
      set load-balance-persistence LB_PERSIS_SRC_ADDR
      set load-balance-method LB_METHOD_ROUND_ROBIN
      set load-balance-pool CS1_4172
      set traffic-group default
   next
end

config load-balance virtual-server
   edit "CS01_BLAST"
      set interface port5
      set ip 10.107.1.86
      set port 10143
      set load-balance-profile LB_PROF_TCP
      set load-balance-method LB_METHOD_ROUND_ROBIN
      set load-balance-pool CS1_8443
      set traffic-group default
   next
end
```

Method 3: Multiple VIPs

This method is similar to the multiple port groups method except instead of dedicating port number to each CS appliance it dedicates an individual VIP to each appliance in addition to the primary load balanced VIP. If you have 2 CS appliances then you would set up 3 VIPs. The primary Horizon protocol on HTTPS port 443 is load balanced to allocate the session to a specific CS appliance based on health check and load balance algorithms. The secondary connections would then be routed to the correct CS appliance based on the following FortiADC configuration table. In this method, you can select any **Persistence** as you need.

VIP:Port	P/S	Profile	Name	Real Servers
10.107.1.86:443	Primary	LB_PROFILE_TCP Or LB_PROFILE_ HTTPS	HORIZON_VS	10.107.10.80:443 10.107.10.81:443
10.107.1.87:443, 4172, 8443	Secondary	LB_PROFILE_TCP	CS01_VS_TCP	10.107.10.80:0
10.107.1.87:4172, 8443	Secondary	LB_PROFILE_UDP	CS01_VS_UDP	10.107.10.80:0
10.107.1.88:443, 4172, 8443	Secondary	LB_PROFILE_TCP	CS02_VS_TCP	10.107.10.81:0
10.107.1.88:4172, 8443	Secondary	LB_PROFILE_UDP	CS02_VS_UDP	10.107.10.81:0

In this example, the FQDN https:// cs1.fortihorizon.com resolves to 10.107.1.87 and https://cs2.fortihorizon.com resolves to 10.107.1.88.

CS Appliance	Configuration Item	Value
CS01	tunnelExternalURL	https://cs1.fortihorizon.com:443
	blastExternalURL	https://cs1.fortihorizon.com:8443
	pcoipExternalURL	10.107.1.87:4172
CS02	tunnelExternalURL	https://cs2.fortihorizon.com:443
	blastExternalURL	https://cs2.fortihorizon.com:8443
	pcoipExternalURL	10.107.1.88:4172

```
config load-balance virtual-server
   edit "CS87_TCP"
      set interface port5
      set ip 10.107.1.87
      set port 443 4172 8443
      set load-balance-profile LB_PROF_TCP
      set load-balance-method LB_METHOD_ROUND_ROBIN
      set load-balance-pool CS1_PORT_0
      set traffic-group default
   next
end
```

```
config load-balance virtual-server
   edit "CS87_UDP"
      set interface port5
      set ip 10.107.1.87
      set port 4172 8443
      set load-balance-profile LB_PROF_UDP
      set load-balance-method LB_METHOD_ROUND_ROBIN
      set load-balance-pool CS1_PORT_0
      set traffic-group default
   next
end

config load-balance virtual-server
   edit "CS88_TCP"
      set interface port5
      set ip 10.107.1.88
      set port 443 4172 8443
      set load-balance-profile LB_PROF_TCP
      set load-balance-method LB_METHOD_ROUND_ROBIN
      set load-balance-pool CS2_PORT_0
      set traffic-group default
   next
end

config load-balance virtual-server
   edit "CS88_UDP"
      set interface port5
      set ip 10.107.1.88
      set port 4172 8443
      set load-balance-profile LB_PROF_UDP
      set load-balance-method LB_METHOD_ROUND_ROBIN
      set load-balance-pool CS2_PORT_0
      set traffic-group default
   next
end
```

Load Balancing for Unified Access Gateway (UAG)

Load Balancing for UAG is the same as "Load Balancing for Connection Servers" with "External Clients". Please refer to External Clients on page 21

HTML Access

With the release of Horizon 7, another method for accessing your desktop from Horizon Workspace is by using an HTML5 compatible browser. From your Horizon Workspace, you can now allow a user to access their desktop either from a compatible browser or View Client. In order to provide browser access, you should enable the HTML Access in the CS configuration firstly. If you have deployed the FortiADC before your CSes, you need do the below configuration that must be done on each Connection Server to allow FortiADC configurations to work correctly: https://kb.vmware.com/s/article/2144768

References

https://techzone.vmware.com/quick-start-tutorial-series-vmware-horizon-7

https://communities.vmware.com/docs/DOC-32792

https://docs.fortinet.com/document/fortiadc/5.4.1/handbook/105358/introduction

https://www.vmware.com/pdf/horizon-view/horizon-view-html-access-document.pdf

https://kb.vmware.com/s/article/2144768