Load Balancing Microsoft Always On VPN
Version 1.3.0
Table of Contents

1. About this Guide .......................................................... 3
2. Loadbalancer.org Appliances Supported .......................... 3
3. Software Versions Supported ........................................ 3
   3.1. Loadbalancer.org Appliance .................................... 3
   3.2. Microsoft Windows .............................................. 3
4. Microsoft Always On VPN ........................................... 3
   4.1. Introduction ...................................................... 3
   4.2. Always On VPN Components .................................. 3
   4.3. How it Works .................................................... 4
5. Always On VPN Prerequisites ....................................... 4
6. Load Balancing Always On VPN ................................... 5
   6.1. Basic Concepts .................................................. 5
   6.2. Load Balancer Deployment .................................... 5
   6.3. Load Balancer Deployment Methods ......................... 6
   6.4. Load Balanced Ports & Services .............................. 6
   6.5. Persistence (Server Affinity) ................................. 6
   6.6. Server Health Checking ....................................... 6
   6.7. SSL Offloading .................................................. 6
7. Loadbalancer.org Appliance – the Basics ....................... 7
   7.1. Virtual Appliance ............................................... 7
   7.2. Initial Network Configuration ................................ 7
   7.3. Accessing the Appliance WebUI ............................... 7
      Main Menu Options ............................................... 9
   7.4. Appliance Software Update ................................... 9
      Determining the Current Software Version .................. 9
      Checking for Updates using Online Update .................. 9
      Using Offline Update ........................................... 10
   7.5. Ports Used by the Appliance ................................ 10
   7.6. HA Clustered Pair Configuration ............................ 11
8. Configuration for Always On VPN .................................. 11
   8.1. Step 1 – Appliance Configuration ............................ 11
      IKEv2 Virtual Service Configuration ......................... 11
      SSTP Virtual Service Configuration ........................... 13
      NPS Virtual Service Configuration ........................... 14
   8.2. Step 2 – Always On VPN Server Configuration ............ 16
      NPS Server Configuration ...................................... 16
      Solving the ARP Problem For the VPN Servers .............. 16
9. Testing & Verification .................................................. 22
   9.1. Using the System Overview ................................... 22
10. Technical Support ...................................................... 23
11. Further Documentation .............................................. 23
12. Appendix .................................................................. 24
   12.1. Configuring HA - Adding a Secondary Appliance ...... 24
      Non-Replicated Settings ......................................... 24
      Configuring the HA Clustered Pair ......................... 25
   12.2. Useful Microsoft Resources & References ................. 26
13. Document Revision History ......................................... 27
1. About this Guide

This guide details the steps required to configure a load balanced Microsoft Always On VPN environment utilizing Loadbalancer.org appliances. It covers the configuration of the load balancers and also any Microsoft Always On VPN configuration changes that are required to enable load balancing.

For more information about initial appliance deployment, network configuration and using the Web User Interface (WebUI), please also refer to the Administration Manual.

2. Loadbalancer.org Appliances Supported

All our products can be used with Always On VPN. For full specifications of available models please refer to: https://www.loadbalancer.org/products

Some features may not be available or fully supported in all cloud platforms due to platform specific limitations. For more details, please refer to the "Main Differences to our Standard (Non-Cloud) Product" section in the appropriate cloud platform Quick Start Guide or check with Loadbalancer.org support.

3. Software Versions Supported

3.1. Loadbalancer.org Appliance
- V8.9.1 and later

Note

The screenshots used throughout this document aim to track the latest Loadbalancer.org software version. If you’re using an older version, or the very latest, the screenshots presented here may not match your WebUI exactly.

3.2. Microsoft Windows
- Windows 2016 and later

4. Microsoft Always On VPN

4.1. Introduction

Always On VPN provides a single, cohesive solution for remote access and supports domain-joined, non domain-joined (workgroup), or Azure AD–joined devices, even personally owned devices. With Always On VPN, the connection type does not have to be exclusively user or device but can be a combination of both. For example, you could enable device authentication for remote device management and then enable user authentication for connectivity to internal company sites and services.

4.2. Always On VPN Components

Always On VPN is part of the Remote Access server role. The table below details the key components that must be available for Always On VPN to work.
These are the components that are made highly available using the load balancer:

<table>
<thead>
<tr>
<th>Component</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing and Remote Access Servers (RRAS)</td>
<td>An Always On VPN deployment may require more than one RRAS server to provide redundancy or to increase capacity to service more VPN connections than a single server is capable of</td>
</tr>
<tr>
<td>Network Policy Servers (NPS)</td>
<td>To authenticate VPN connections, VPN servers are configured to forward authentication requests to an NPS server. Having more than one NPS server eliminates this single point of failure and may be required to support authentication for large scale deployments</td>
</tr>
<tr>
<td>Multisite redundancy</td>
<td>Unlike DirectAccess, Always On VPN has no concept of “multisite” configuration. To provide geographic redundancy multiple VPN servers can be configured in various locations using a single, common public hostname. VPN client connections can then be routed to the most preferred location using the GSLB feature on the load balancer.</td>
</tr>
</tbody>
</table>

**Note**
For more information about GSLB, please refer to the Administration Manual and search for "Global Server Load Balancing".

### 4.3. How it Works

Using public DNS servers, the Windows 10 VPN client performs a name resolution query for the IP address of the VPN gateway.

Using the IP address returned by DNS, the VPN client sends a connection request to the VPN gateway.

The VPN gateway is also configured as a Remote Authentication Dial-In User Service (RADIUS) Client; the VPN RADIUS Client sends the connection request to the organization/corporate NPS server for connection request processing.

The NPS server processes the connection request, including performing authorization and authentication, and determines whether to allow or deny the connection request.

The NPS server forwards an Access-Accept or Access-Deny response to the VPN gateway.

The connection is initiated or terminated based on the response that the VPN server received from the NPS server.

### 5. Always On VPN Prerequisites

Several prerequisites must be in place before proceeding with this documentation. As such, it is assumed that the load balancer has been configured and that network connectivity to all networks has been validated. In addition, the following prerequisites must be in place before continuing:

- A public hostname for the VPN server which resolves to the IP address assigned to the VPN virtual service (or edge firewall if the load balancer is in a perimeter or DMZ network).
• An SSL certificate with a subject name that matches the VPN server’s public hostname.

• Each VPN server must be configured to assign unique IP addresses to its clients. Using DHCP for VPN client address assignment when there is more than one VPN server in a cluster is not supported.

• An internal hostname for the NPS cluster which resolves to the IP address assigned to the NPS virtual service.

6. Load Balancing Always On VPN

Note
It’s highly recommended that you have a working Always On VPN environment first before implementing the load balancer.

6.1. Basic Concepts

To provide resilience and high availability for your Always On VPN infrastructure, multiple Always On VPN servers should be deployed with a load balancer. This helps ensure that users can always connect to the corporate network by constantly checking the health of the Always On VPN servers and only forwarding connections to functional servers.

6.2. Load Balancer Deployment

The following diagram shows a typical load balanced Always On VPN deployment.

Note
Load balancers can be deployed as single units or as a clustered pair. Loadbalancer.org recommends deploying a clustered pair for HA and resilience.
6.3. Load Balancer Deployment Methods

For IKEv2, the load balancing method used must be transparent. This means that the client’s source IP address is retained through to the Real Servers. Transparency is required for IKEv2 because Windows limits the number of IPSec Security Associations (SAs) coming from a single IP address. If a non-transparent method was used, the source IP address for all traffic reaching the IKEv2 servers would either be the VIP address or the load balancer’s own address, depending on the specific configuration.

Both layer 4 DR mode and layer 4 NAT mode are transparent and either can be used for IKEv2. When using DR mode, the “ARP problem” must be solved on all VPN Servers. For NAT mode, the default gateway for each VPN Server must be the load balancer.

For SSTP and NPS transparency is not required, although the load balancing method selected must support UDP. Therefore, whilst DR mode or NAT mode can be used, layer 4 SNAT mode is a simpler option since it requires no mode-specific configuration changes to the Real Servers.

In this guide layer 4 DR mode is used for IKEv2 and layer 4 SNAT mode is used for SSTP and NPS.

<table>
<thead>
<tr>
<th>Note</th>
<th>For more information on the various load balancing methods supported, please refer to Supported Load Balancing Methods.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Note</td>
<td>For more information on the ARP Problem, please refer to DR Mode Considerations.</td>
</tr>
</tbody>
</table>

6.4. Load Balanced Ports & Services

The following ports/protocols must be load balanced:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP/HTTPS</td>
<td>All Always On VPN client to server SSTP communication</td>
</tr>
<tr>
<td>500, 4500</td>
<td>UDP/IKEv2</td>
<td>IKEv2 communication</td>
</tr>
<tr>
<td>1812,1813</td>
<td>UDP</td>
<td>Network policy server communication</td>
</tr>
</tbody>
</table>

6.5. Persistence (Server Affinity)

Source IP address persistence is used for the Always On VPN servers. This ensures that a particular client will connect to the same Always On VPN server for the duration of the session and the Always On VPN server will connect to the same Network Policy server.

6.6. Server Health Checking

The load balancer performs regular checks to verify the health of each server / service. For the IKEv2 and NPS services an ICMP ping check is used, for SSTP a HTTPS negotiate check is used.

6.7. SSL Offloading

To provide scalability and effective load sharing we recommend that SSL is terminated on the VPN servers rather
7. Loadbalancer.org Appliance – the Basics

7.1. Virtual Appliance
A fully featured, fully supported 30 day trial is available if you are conducting a PoC (Proof of Concept) deployment. The VA is currently available for VMware, Virtual Box, Hyper-V, KVM, XEN and Nutanix AHV and has been optimized for each Hypervisor. By default, the VA is allocated 2 vCPUs, 4GB of RAM and has a 20GB virtual disk. The Virtual Appliance can be downloaded [here](#).

The same download is used for the licensed product, the only difference is that a license key file (supplied by our sales team when the product is purchased) must be applied using the appliance’s WebUI.

Please refer to Virtual Appliance Installation and the ReadMe.txt text file included in the VA download for additional information on deploying the VA using the various Hypervisors.

The VA has 4 network adapters. For VMware only the first adapter (eth0) is connected by default. For HyperV, KVM, XEN and Nutanix AHV all adapters are disconnected by default. Use the network configuration screen within the Hypervisor to connect the required adapters.

7.2. Initial Network Configuration
After boot up, follow the instructions on the appliance console to configure the management IP address, subnet mask, default gateway, DNS servers and other network and administrative settings.

Be sure to set a secure password for the load balancer, when prompted during the setup routine.

7.3. Accessing the Appliance WebUI
The WebUI is accessed using a web browser. By default, users are authenticated using Apache authentication. Users can also be authenticated against LDAP, LDAPS, Active Directory or Radius - for more information, please refer to External Authentication.

There are certain differences when accessing the WebUI for the cloud appliances. For details, please refer to the relevant Quick Start / Configuration Guide.

Using a browser, navigate to the following URL:


You’ll receive a warning about the WebUI’s SSL certificate. This is due to the default self signed certificate that is used. If preferred, you can upload your own certificate - for more information, please refer to Appliance Security Features.
2. Log in to the WebUI using the following credentials:

**Username:** loadbalancer  
**Password:** <configured-during-network-setup-wizard>

**Note** To change the password, use the WebUI menu option: *Maintenance > Passwords.*

Once logged in, the WebUI will be displayed as shown below:

3. You’ll be asked if you want to run the Setup Wizard which can be used to configure layer 7 services. Click **Dismiss** if you’re following a guide or want to configure the appliance manually or click **Accept** to start the
Main Menu Options

System Overview - Displays a graphical summary of all VIPs, RIPs and key appliance statistics
Local Configuration - Configure local host settings such as IP address, DNS, system time etc.
Cluster Configuration - Configure load balanced services such as VIPs & RIPs
Maintenance - Perform maintenance tasks such as service restarts and taking backups
View Configuration - Display the saved appliance configuration settings
Reports - View various appliance reports & graphs
Logs - View various appliance logs
Support - Create a support download, contact the support team & access useful links
Live Chat - Start a live chat session with one of our Support Engineers

7.4. Appliance Software Update

To ensure that the appliance(s) are running the latest software version, we recommend a software update check is performed.

Determining the Current Software Version

The software version is displayed at the bottom of the WebUI as shown in the example below:

Copyright © Loadbalancer.org Inc. 2002 – 2024
ENTERPRISE VA Max - v8.11.1

Checking for Updates using Online Update

Note: By default, the appliance periodically contacts the Loadbalancer.org update server and checks for updates. An update check can also be manually triggered as detailed below.

1. Using the WebUI, navigate to: Maintenance > Software Update.
2. Select Online Update.
3. If the latest version is already installed, a message similar to the following will be displayed:

Information: Version v8.11.1 is the current release. No updates are available

4. If an update is available, you'll be presented with a list of new features, improvements, bug fixes and security related updates.
5. Click Online Update to start the update process.

Note: Do not navigate away whilst the update is ongoing, this may cause the update to fail.
6. Once complete (the update can take several minutes depending on download speed and upgrade version) the following message will be displayed:

![Information: Update completed successfully.]

7. If services need to be reloaded/restarted or the appliance needs a full restart, you’ll be prompted accordingly.

**Using Offline Update**

If the load balancer does not have access to the Internet, offline update can be used.

---

### Note

Please contact support@loadbalancer.org to check if an update is available and obtain the latest offline update files.

---

To perform an offline update:

1. Using the WebUI, navigate to: *Maintenance > Software Update*.
2. Select *Offline Update*.
3. The following screen will be displayed:

![Software Update]

**Offline Update**

The following steps will lead you through offline update:

1. Contact loadbalancer.org support to obtain the offline update archive and checksum.
2. Save the archive and checksum to your local machine.
3. Select the archive and checksum files in the upload form below.
4. Click *Upload and Install* to begin the update process.

4. Select the **Archive** and **Checksum** files.
5. Click **Upload and Install**.
6. If services need to be reloaded/restarted or the appliance needs a full restart, you’ll be prompted accordingly.

### 7.5. Ports Used by the Appliance

By default, the appliance uses the following TCP & UDP ports:
### Protocol Port Purpose

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Port</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>22 *</td>
<td>SSH</td>
</tr>
<tr>
<td>TCP &amp; UDP</td>
<td>53 *</td>
<td>DNS / GSLB</td>
</tr>
<tr>
<td>TCP &amp; UDP</td>
<td>123</td>
<td>NTP</td>
</tr>
<tr>
<td>TCP &amp; UDP</td>
<td>161 *</td>
<td>SNMP</td>
</tr>
<tr>
<td>UDP</td>
<td>6694</td>
<td>Heartbeat between Primary &amp; Secondary appliances in HA mode</td>
</tr>
<tr>
<td>TCP</td>
<td>7778</td>
<td>HAProxy persistence table replication</td>
</tr>
<tr>
<td>TCP</td>
<td>9000 *</td>
<td>Gateway service (Centralized/Portal Management)</td>
</tr>
<tr>
<td>TCP</td>
<td>9080 *</td>
<td>WebUI - HTTP (disabled by default)</td>
</tr>
<tr>
<td>TCP</td>
<td>9081 *</td>
<td>Nginx fallback page</td>
</tr>
<tr>
<td>TCP</td>
<td>9443 *</td>
<td>WebUI - HTTPS</td>
</tr>
<tr>
<td>TCP</td>
<td>25565 *</td>
<td>Shuttle service (Centralized/Portal Management)</td>
</tr>
</tbody>
</table>

**Note**: The ports used for SSH, GSLB, SNMP, the WebUI, the fallback page, the gateway service and the shuttle service can be changed if required. For more information, please refer to Service Socket Addresses.

### 7.6. HA Clustered Pair Configuration

Loadbalancer.org recommend that load balancer appliances are deployed in pairs for high availability. In this guide a single unit is deployed first, adding a secondary unit is covered in Configuring HA - Adding a Secondary Appliance.

### 8. Configuration for Always On VPN

This is completed in 2 steps; step 1 covers the appliance configuration, step 2 covers the configuration changes required to the Always On VPN servers to enable load balancing.

#### 8.1. Step 1 – Appliance Configuration

3 Virtual Services (VIPs) are required for Always On VPN. These are for IKEv2, SSTP and NPS. The following sections cover the configuration of each VIP.

**IKEv2 Virtual Service Configuration**

Setting up the Virtual Service (VIP)

1. Using the WebUI, navigate to: Cluster Configuration > Layer 4 – Virtual Services and click Add a New Virtual Service.
2. Enter the following details:
3. Enter an appropriate name (Label) for the Virtual Service, e.g. IKEv2_VIP.

4. Set the Virtual Service IP address field to the required IP address, e.g. 192.168.0.242.

5. Set the Virtual Service Ports field to 500,4500.

6. Set the Protocol to UDP.

7. Set the Forwarding Method to Direct Routing.

8. Click Update.

9. Now click Modify next to the newly created Virtual Service.

10. Verify that the Persistence Timeout is set to 300.

11. Under Health Checks ensure that Check Type is set to ping server.

12. Click Update.

Configuring the Associated Real Servers (RIPs)

1. Using the WebUI, navigate to: Cluster Configuration > Layer 4 – Real Servers and click Add a new Real Server next to the newly created Virtual Service.

2. Enter the following details:
3. Enter an appropriate name (Label) for the first VPN server, e.g. **VPNSVR1**.

4. Change the *Real Server IP Address* field to the required IP address, e.g. **192.168.0.43**.

5. Click **Update**.

6. Now repeat the above steps to add your remaining VPN server(s).

**SSTP Virtual Service Configuration**

**Setting up the Virtual Service (VIP)**

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 – Virtual Services* and click **Add a New Virtual Service**.

2. Enter the following details:

   - Enter an appropriate name (Label) for the Virtual Service, e.g. **SSTP_VIP**.
   - Set the *Virtual Service IP address* field to the required IP address, e.g. **192.168.0.242**.
   - Set the *Virtual Service Ports* field to **443**.
   - Set the *Protocol* to **TCP Mode**.
   - Set the *Forwarding Method* to **SNAT**.
   - Click **Update**.
   - Now click **Modify** next to the newly created Virtual Service.
   - Verify that the *Persistence Timeout* is set to **300**.
   - Under the *Health Checks* section set the *Check Type* to **Negotiate**.
   - Set the *Check Port* to **443**.
   - Set the *Protocol* to **HTTPS**.
   - Set the *Request to send* to `/sra_{BA195980-CD49-458b-9E23-C84EE0ADCD75}/`.
   - Set the *Response expected* to **401**.
16. Click **Update**.

### Configuring the Associated Real Servers (RIPs)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 – Real Servers* and click **Add a new Real Server** next to the newly created Virtual Service.

2. Enter the following details:

![Real Server Configuration Table]

3. Enter an appropriate name (Label) for the first VPN server, e.g. **VPNSVR1**.

4. Change the **Real Server IP Address** field to the required IP address, e.g. **192.168.0.43**.

5. Set the **Real Server Port** field to **443**.

6. Click **Update**.

7. Now repeat the above steps to add your remaining VPN server(s).

### NPS Virtual Service Configuration

#### Setting up the Virtual Service (VIP)

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 – Virtual Services* and click **Add a New Virtual Service**.

2. Enter the following details:
3. Enter an appropriate name (Label) for the Virtual Service, e.g. NPS_VIP.

4. Set the **Virtual Service IP address** field to the required IP address, e.g. 192.168.0.242.

5. Set the **Virtual Service Ports** field to 1812,1813.

6. Set the **Protocol** to UDP.

7. Set the **Forwarding Method** to SNAT.

8. Click **Update**.

9. Now click **Modify** next to the newly created Virtual Service.

10. Verify that the **Persistence Timeout** is set to 300.

11. Under **Health Checks** ensure that **Check Type** is set to ping server.

12. Click **Update**.

**Configuring the Associated Real Servers (RIPs)**

1. Using the WebUI, navigate to: *Cluster Configuration > Layer 4 – Real Servers* and click **Add a new Real Server** next to the newly created Virtual Service.

2. Enter the following details:
3. Enter an appropriate name (Label) for the first Network Policy Server, e.g. **NPS_SVR1**.

4. Change the **Real Server IP Address** field to the required IP address, e.g. **192.168.1.43**.

5. Leave **Real Server Port** blank.

6. Click **Update**.

7. Now repeat the above steps to add your remaining NPS server(s).

---

**Note**

The certificate installed on the NPS server must be configured to use the cluster Fully Qualified Domain Name (FQDN) as the subject name on the certificate, with the Subject Alternative Name fields including the FQDNs of both the cluster and server names.

---

### 8.2. Step 2 – Always On VPN Server Configuration

#### NPS Server Configuration

The source IP address of the RADIUS authentication and accounting requests is the Virtual IP Address (VIP) assigned to the virtual service. A RADIUS client must be configured in NPS to allow authentication and accounting requests to be processed. Open the NPS management console and perform the following steps:

1. Expand **RADIUS Clients and Servers**.

2. Right-click **RADIUS Clients** and select **New**.

3. Enter a friendly name for the new RADIUS client.

4. Enter the IP address of the NPS Virtual Service in the **Address (IP or DNS)** field.

5. Enter and confirm the shared secret used between the NPS and VPN servers.

6. Click **OK**.

7. Repeat the above steps on all other NPS servers in the cluster.

#### Solving the ARP Problem For the VPN Servers

When using Layer 4 DR mode, the ARP problem must be solved. This involves configuring each Real Server to be able to receive traffic destined for the VIP, and ensuring that each Real Server does not respond to ARP requests.
for the VIP address – only the load balancer should do this.

The steps below are for Windows 2012 and later and must be completed on each VPN server.

**Windows Server 2012 & Later**

Windows Server 2012 and later support Direct Routing (DR) mode through the use of the Microsoft Loopback Adapter that must be installed and configured on each load balanced (Real) Server. The IP address configured on the Loopback Adapter must be the same as the Virtual Service (VIP) address. This enables the server to receive packets that have their destination set as the VIP address. If a Real Server is included in multiple DR mode VIPs, an IP address for each VIP must be added to the Loopback Adapter.

In addition, the strong/weak host behavior must be configured on each Real Server. The weak host model allows packets with any IP to be sent or received via an interface. The strong host model only allows packets with an IP belonging to the interface to be sent or received.

**Important** The following 3 steps must be completed on all Real Servers associated with the VIP.

**Step 1 of 3: Install the Microsoft Loopback Adapter**

1. Click **Start**, then run **hdwwiz** to start the Hardware Installation Wizard.

2. Once the Wizard has started, click **Next**.

3. Select **Install the hardware that I manually select from a list (Advanced)**, click **Next**.

4. Select **Network adapters**, click **Next**.

5. Select **Microsoft & Microsoft KM-Test Loopback Adapter**, click **Next**.

6. Click **Next** to start the installation, when complete click **Finish**.
Step 2 of 3: Configure the Loopback Adapter

1. Open Control Panel and click **Network and Sharing Center**.

2. Click **Change adapter settings**.

3. Right-click the new Loopback Adapter and select **Properties**.

**Note** You can configure IPv4 or IPv6 addresses or both depending on your requirements.

**IPv4 Addresses**

1. Uncheck all items except **Internet Protocol Version 4 (TCP/IPv4)** as shown below:

2. Ensure that **Internet Protocol Version (TCP/IPv4)** is selected, click **Properties** and configure the IP address to be the same as the Virtual Service address (VIP) with a subnet mask of **255.255.255.255**, e.g. **192.168.2.20/255.255.255.255** as shown below:
192.168.2.20 is an example, make sure you specify the correct VIP address.

If a Real Server is included in multiple DR mode VIPs, an IP address for each VIP must be added to the Loopback Adapter.

3. Click OK then click Close to save and apply the new settings.

IPv6 Addresses

1. Uncheck all items except Internet Protocol Version 6 (TCP/IPv6) as shown below:
2. Ensure that Internet Protocol Version (TCP/IPv6) is selected, click Properties and configure the IP address to be the same as the Virtual Service (VIP) and set the Subnet Prefix Length to be the same as your network setting, e.g. 2001:470:1f09:e72::15/64 as shown below:

![Internet Protocol Version 6 (TCP/IPv6) Properties](image)

**Note** 2001:470:1f09:e72::15/64 is an example, make sure you specify the correct VIP address.

**Note** If a Real Server is included in multiple DR mode VIPs, an IP address for each VIP must be
3. Click **OK** then click **Close** to save and apply the new settings.

**Step 3 of 3: Configure the strong/weak host behavior**

The strong/weak host behavior can be configured using either of the following 2 methods:

- Option 1 - Using network shell (netsh) commands
- Option 2 - Using PowerShell cmdlets

The commands in this section assume that the LAN Adapter is named "**net**" and the Loopback Adapter is named "**loopback**" as shown in the example below:

---

**Option 1 - Using Network Shell (netsh) Commands**

To configure the correct strong/weak host behavior run the following commands:

For IPv4 addresses:

```
netsh interface ipv4 set interface "net" weakhostreceive=enabled
netsh interface ipv4 set interface "loopback" weakhostreceive=enabled
netsh interface ipv4 set interface "loopback" weakhostsend=enabled
```

For IPv6 addresses:

```
netsh interface ipv6 set interface "net" weakhostreceive=enabled
netsh interface ipv6 set interface "loopback" weakhostreceive=enabled
netsh interface ipv6 set interface "loopback" weakhostsend=enabled
netsh interface ipv6 set interface "loopback" dadtransmits=0
```

---

**Option 2 - Using PowerShell Cmdlets**

For IPv4 addresses:
Set-NetIpInterface -InterfaceAlias loopback -WeakHostReceive enabled -WeakHostSend enabled -DadTransmits 0 -AddressFamily IPv4

Set-NetIpInterface -InterfaceAlias net -WeakHostReceive enabled -AddressFamily IPv4

For IPv6 Addresses:

Set-NetIpInterface -InterfaceAlias loopback -WeakHostReceive enabled -WeakHostSend enabled -DadTransmits 0 -AddressFamily IPv6

Set-NetIpInterface -InterfaceAlias net -WeakHostReceive enabled -AddressFamily IPv6

9. Testing & Verification

For additional guidance on diagnosing and resolving any issues you may have, please also refer to Diagnostics & Troubleshooting.

Make sure that the firewall on the clients and servers is enabled. This is a requirement for Always On VPN to work successfully.

9.1. Using the System Overview

Verify that all VIPs & associated RIPS are reported as up (green) as shown below:
If certain servers are down, i.e. failing their health check, they will be highlighted red as shown below:

10. Technical Support

If you have any questions regarding the appliance or would like assistance designing your deployment, please don’t hesitate to contact our support team: support@loadbalancer.org.

11. Further Documentation

For additional information, please refer to the Administration Manual.
12. Appendix

12.1. Configuring HA - Adding a Secondary Appliance

Our recommended configuration is to use a clustered HA pair of load balancers to provide a highly available and resilient load balancing solution. We recommend that the Primary appliance is fully configured first, then the Secondary appliance can be added to create an HA pair. Once the HA pair is configured, load balanced services must be configured and modified on the Primary appliance. The Secondary appliance will be automatically kept in sync.

For Enterprise Azure, the HA pair should be configured first. For more information, please refer to the Azure Quick Start/Configuration Guide available in the documentation library.

The clustered HA pair uses Heartbeat to determine the state of the other appliance. Should the active device (normally the Primary) suffer a failure, the passive device (normally the Secondary) will take over.

Non-Replicated Settings

A number of settings are not replicated as part of the Primary/Secondary pairing process and therefore must be manually configured on the Secondary appliance. These are listed by WebUI menu option in the table below:

<table>
<thead>
<tr>
<th>WebUI Main Menu Option</th>
<th>Sub Menu Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local Configuration</td>
<td>Hostname &amp; DNS</td>
<td>Hostname and DNS settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Network Interface Configuration</td>
<td>Interface IP addresses, bonding configuration and VLANs</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Routing</td>
<td>Default gateways and static routes</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>System Date &amp; time</td>
<td>Time and date related settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Physical – Advanced Configuration</td>
<td>Various appliance settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Portal Management</td>
<td>Portal management settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Security</td>
<td>Security settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>SNMP Configuration</td>
<td>SNMP settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Graphing</td>
<td>Graphing settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>License Key</td>
<td>Appliance licensing</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Backup &amp; Restore</td>
<td>Local XML backups</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Software Updates</td>
<td>Appliance software updates</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Fallback Page</td>
<td>Fallback page configuration</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Firewall Script</td>
<td>Firewall (iptables) configuration</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Firewall Lockdown Wizard</td>
<td>Appliance management lockdown settings</td>
</tr>
</tbody>
</table>
Make sure that where any of the above have been configured on the Primary appliance, they’re also configured on the Secondary.

### Configuring the HA Clustered Pair

#### Note
If you have already run the firewall lockdown wizard on either appliance, you’ll need to ensure that it is temporarily disabled on both appliances whilst performing the pairing process.

1. Deploy a second appliance that will be the Secondary and configure initial network settings.
2. Using the WebUI on the Primary appliance, navigate to: **Cluster Configuration > High-Availability Configuration.**

![Create a Clustered Pair](image)

3. Specify the IP address and the `loadbalancer` user’s password for the Secondary (peer) appliance as shown in the example above.
4. Click **Add new node.**
5. The pairing process now commences as shown below:

![Create a Clustered Pair](image)

6. Once complete, the following will be displayed on the Primary appliance:
7. To finalize the configuration, restart heartbeat and any other services as prompted in the "Commit changes" message box at the top of the screen.

**Note**
Clicking the Restart Heartbeat button on the Primary appliance will also automatically restart heartbeat on the Secondary appliance.

**Note**
For more details on configuring HA with 2 appliances, please refer to Appliance Clustering for HA.

**Note**
For details on testing and verifying HA, please refer to Clustered Pair Diagnostics.

### 12.2. Useful Microsoft Resources & References

**Microsoft Windows 10 Always On VPN:**

https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/always-on-vpn/

**Microsoft Windows 10 Always On VPN Deployment Guide:**

https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/always-on-vpn/deploy/always-on-vpn-deploy

**Troubleshooting Always On VPN:**

https://docs.microsoft.com/en-us/windows-server/remote/remote-access/vpn/always-on-vpn/deploy/always-on-vpn-deploy-troubleshooting
# 13. Document Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Change</th>
<th>Reason for Change</th>
<th>Changed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0.0</td>
<td>27 March 2020</td>
<td>Initial creation</td>
<td></td>
<td>IBG</td>
</tr>
<tr>
<td>1.0.1</td>
<td>3 September 2020</td>
<td>New title page</td>
<td>Branding update</td>
<td>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Updated Canadian contact details</td>
<td>Change to Canadian contact details</td>
<td></td>
</tr>
<tr>
<td>1.0.2</td>
<td>24 September 2020</td>
<td>Health check update</td>
<td></td>
<td>IBG</td>
</tr>
<tr>
<td>1.1.0</td>
<td>11th August 2021</td>
<td>Changed the health check for the IKEv2 VIP to an ICMP ping check</td>
<td>Incorrectly specified a Radius check</td>
<td>RJC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Changed the persistence timeout to 300 seconds (5mins) for all VIPs</td>
<td>Previous setting was unnecessarily high</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Changed load balancing method for the IKEv2 VIP from SNAT mode to DR mode</td>
<td>IKEv2 client connections must be transparent</td>
<td></td>
</tr>
<tr>
<td>1.2.0</td>
<td>1 January 2022</td>
<td>Converted the document to AsciiDoc</td>
<td>Move to new documentation system</td>
<td>AH, RJC, ZAC</td>
</tr>
<tr>
<td>1.2.1</td>
<td>5 January 2023</td>
<td>Combined software version information into one section</td>
<td>Housekeeping across all documentation</td>
<td>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added one level of section numbering</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added software update instructions</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Added table of ports used by the appliance</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reworded ‘Further Documentation’ section</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2.2</td>
<td>2 February 2023</td>
<td>Updated screenshots</td>
<td>Branding update</td>
<td>AH</td>
</tr>
<tr>
<td>1.2.3</td>
<td>7 March 2023</td>
<td>Removed conclusion section</td>
<td>Updates across all documentation</td>
<td>AH</td>
</tr>
<tr>
<td>1.3.0</td>
<td>24 March 2023</td>
<td>New document theme</td>
<td>Branding update</td>
<td>AH</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Modified diagram colours</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
About Loadbalancer.org

Loadbalancer.org’s mission is to ensure that its clients’ businesses are never interrupted. The load balancer experts ask the right questions to get to the heart of what matters, bringing a depth of understanding to each deployment. Experience enables Loadbalancer.org engineers to design less complex, unbreakable solutions - and to provide exceptional personalized support.