Load Balancing Microsoft Always On VPN

Version 1.2.0
Table of Contents

1. About this Guide ................................................. 3
2. Loadbalancer.org Appliances Supported ................................................. 3
3. Loadbalancer.org Software Versions Supported ................................................. 3
4. Microsoft Windows Versions Supported ................................................. 3
5. Microsoft Always On VPN ................................................. 3
   Introduction ........................................................................... 3
   Always On VPN Components ................................................. 3
   How it Works ......................................................................... 4
6. Always On VPN Prerequisites ................................................. 4
7. Load Balancing Always On VPN ................................................. 5
   Basic Concepts .................................................................. 5
   Load Balancer Deployment ................................................. 5
   Load Balancer Deployment Methods ................................................. 5
   Load Balanced Ports & Services ................................................. 6
   Persistence (Server Affinity) ................................................. 6
   Server Health Checking ......................................................... 6
   SSL Offloading .................................................................. 6
8. Loadbalancer.org Appliance – the Basics ................................................. 6
   Virtual Appliance ......................................................... 6
   Initial Network Configuration ................................................. 7
   Accessing the WebUI ......................................................... 7
   Main Menu Options .......................................................... 8
   HA Clustered Pair Configuration ................................................. 9
9. Configuration for Always On VPN ................................................. 9
   Step 1 – Appliance Configuration ................................................. 9
      IKEv2 Virtual Service Configuration ................................................. 9
      SSTP Virtual Service Configuration ................................................. 10
      NPS Virtual Service Configuration ................................................. 12
   Step 2 – Always On VPN Server Configuration ................................................. 13
      NPS Server Configuration ......................................................... 13
      Solving the ARP Problem For the VPN Servers ................................................. 14
10. Testing & Verification ......................................................................... 19
   Using the System Overview ......................................................... 19
11. Technical Support ........................................................................... 20
12. Further Documentation ....................................................................... 20
13. Conclusion ......................................................................................... 20
14. Appendix ......................................................................................... 21
   Configuring HA - Adding a Secondary Appliance ................................................. 21
   Useful Microsoft Resources & References ................................................. 23
15. Document Revision History ......................................................... 24
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 supported in all cloud platforms due to platform specific limitations. Please check with Loadbalancer.org support for details.

3. Loadbalancer.org Software Versions Supported

- V8.4.1 and later

Note

The screenshots used throughout this document aim to track the latest Loadbalancer.org software version. If using an older software version, note that the screenshots presented here may not match the WebUI exactly.

4. Microsoft Windows Versions Supported

- Windows 2016 and later

5. Microsoft Always On VPN

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.

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”.

**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.

**6. 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.

7. 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.

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.

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.

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 additional 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>
</table>

| Note | For more information on the ARP Problem, please refer to DR Mode Considerations. |

### 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>

### 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.

### 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.

### SSL Offloading

To provide scalability and effective load sharing we recommend that SSL is terminated on the VPN servers rather than on the load balancer.

### 8. Loadbalancer.org Appliance – the Basics

#### 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](#).
Note: 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.

Note: Please refer to The Virtual Appliance - Hypervisor Deployment and the ReadMe.txt text file included in the VA download for more detailed information on deploying the VA using various Hypervisors.

Note: For the VA, 4 NICs are included but only eth0 is connected by default at power up. If the other NICs are required, these should be connected using the network configuration screen within the Hypervisor.

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

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

Accessing the WebUI
The WebUI is accessed using a web browser. By default, user authentication is based on local Apache .htaccess files. User administration tasks such as adding users and changing passwords can be performed using the WebUI menu option: Maintenance > Passwords.

Note: A number of compatibility issues have been found with various versions of Internet Explorer and Edge. The WebUI has been tested and verified using both Chrome & Firefox.

Note: If required, users can also be authenticated against LDAP, LDAPS, Active Directory or Radius. For more information please refer to External Authentication.

1. Using a browser, access the WebUI using the following URL:


2. Log in to the WebUI:

   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. If you click **Accept** the Layer 7 Virtual Service configuration wizard will start. If you want to configure the appliance manually, simple click **Dismiss**.

**Main Menu Options**

- **System Overview** - Displays a graphical summary of all VIPs, RIPv 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 & RIPv
- **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
9. 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.

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:

   - Label: IKEv2_VIP
   - IP Address: 192.168.0.242
   - Ports: 500,4500
   - Protocol: UDP
   - Forwarding Method: Direct Routing

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:

<table>
<thead>
<tr>
<th>Label</th>
<th>VPNSVR1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.0.43</td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
<tr>
<td>Minimum Connections</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Connections</td>
<td>0</td>
</tr>
</tbody>
</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. 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:
3. Enter an appropriate name (Label) for the Virtual Service, e.g. SSTP_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 443.
6. Set the Protocol to TCP Mode.
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 the Health Checks section set the Check Type to Negotiate.
12. Set the Check Port to 443.
13. Set the Protocol to HTTPS.
14. Set the Request to send to /sra_{BA195980-CD49-458b-9E23-C84EE0ADCD75}/.
15. 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:
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:

<table>
<thead>
<tr>
<th>Virtual Service</th>
<th>NPS_VIP</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.168.0.242</td>
</tr>
<tr>
<td>Ports</td>
<td>1812,1813</td>
</tr>
<tr>
<td>Protocol</td>
<td>UDP</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Label</th>
<th>NPS_SVR1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real Server IP Address</td>
<td>192.168.1.43</td>
</tr>
<tr>
<td>Real Server Port</td>
<td></td>
</tr>
<tr>
<td>Weight</td>
<td>100</td>
</tr>
<tr>
<td>Minimum Connections</td>
<td>0</td>
</tr>
<tr>
<td>Maximum Connections</td>
<td>0</td>
</tr>
</tbody>
</table>

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.

**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, 2016 & 2019**

Windows Server 2012 and later support Direct Routing (DR) mode through the use of the Microsoft Loopback Adapter. The IP address allocated to the Loopback Adapter must be the same as the Virtual Service (VIP) address. If the Real Server is included in multiple DR mode VIPs, additional IP addresses can be added to the Loopback Adapter that correspond to each VIP. In addition, steps must be taken to set the strong/weak host behavior which is used to either block or allow interfaces to receive packets destined for a different interface on the same server.

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

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

2. When 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.
4. Uncheck all items except Internet Protocol Version 4 (TCP/IPv4) and Internet Protocol Version 6 (TCP/IPv6) as shown below:
Note
Leaving both checked ensures that both IPv4 and IPv6 are supported. Select one if preferred.

5. If configuring IPv4 addresses select Internet Protocol Version (TCP/IPv4), click Properties and configure the IP address to be the same as the Virtual Service (VIP) with a subnet mask of 255.255.255.255, e.g., 192.168.2.20/255.255.255.255 as shown below:

6. If configuring IPv6 addresses select Internet Protocol Version (TCP/IPV6), 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:

7. Click **OK** on TCP/IP Properties, then click **Close** on Ethernet Properties to save and apply the new settings.

**Note**

For Windows 2012/2016/2019, it’s not necessary to modify the interface metric on the advanced tab and should be left set to Automatic.

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

To configure the correct strong/weak host behavior for Windows 2012/2016/2019, the following commands must be run on each Real Server:

**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 these commands to work, the LAN connection NIC must be named "net" and the loopback NIC must be named "loopback" as shown below. If you prefer to leave your current NIC names, then the commands above must be modified accordingly. For example, if your network adapters are named "LAN" and "LOOPBACK", the commands required would be:

```
netsh interface ipv4 set interface "LAN" weakhostreceive=enabled
netsh interface ipv4 set interface "LOOPBACK" weakhostreceive=enabled
netsh interface ipv4 set interface "LOOPBACK" weakhostsend=enabled
```

**For IPv6 addresses:**
For these commands to work, the LAN connection NIC must be named "net" and the loopback NIC must be named "loopback" as shown below. If you prefer to leave your current NIC names, then the commands above must be modified accordingly. For example, if your network adapters are named "LAN" and "LOOPBACK", the commands required would be:

```
netsh interface ipv6 set interface "LAN" 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
```

Note The names for the NICs are case sensitive, so make sure that the name used for the interface and the name used in the commands match exactly.

* Start PowerShell or use a command window to run the appropriate netsh commands as shown in the example below:

```
Set-NetIpInterface -InterfaceAlias loopback -WeakHostReceive enabled -WeakHostSend enabled -DadTransmits 0
```

Note This shows an IPv6 example, use the IPv4 commands if you’re using IPv4 addresses.

Repeat steps 1 - 3 on all remaining Windows 2012/2016/2019 Real Server(s).

If preferred you can also use the following PowerShell Cmdlets:

The following example configures both IPv4 and IPv6 at the same time:

```
Set-NetIpInterface -InterfaceAlias loopback -WeakHostReceive enabled -WeakHostSend enabled -DadTransmits 0
```
Set-NetIpInterface -InterfaceAlias net -WeakHostReceive enabled

To configure just IPv4:

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

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

To configure just IPv6:

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

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

10. Testing & Verification

Note For additional general guidance please also refer to Testing Load Balanced Services.

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

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:

11. 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.

12. Further Documentation


13. Conclusion

Loadbalancer.org appliances provide a very cost effective and flexible solution for highly available load balanced Always On VPN Server environments.
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 should be configured first, then the Secondary should be added. Once the Primary and Secondary are paired, all load balanced services configured on the Primary are automatically replicated to the Secondary over the network using SSH/SCP.

**Note**

For Enterprise Azure, the HA pair should be configured first. In Azure, when creating a VIP using an HA pair, 2 private IPs must be specified – one for the VIP when it’s active on the Primary and one for the VIP when it’s active on the Secondary. Configuring the HA pair first, enables both IPs to be specified when the VIP is created.

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.

**Note**

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</td>
<td>All network settings including IP address(es), bonding configuration and VLANs</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Routing</td>
<td>Routing configuration including default gateways and static routes</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>System Date &amp; time</td>
<td>All time and date related settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Physical – Advanced</td>
<td>Various settings including Internet Proxy, Management Gateway, Firewall</td>
</tr>
<tr>
<td></td>
<td>Configuration</td>
<td>connection tracking table size, NIC offloading, SMTP relay, logging</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Security</td>
<td>Appliance security settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>SNMP Configuration</td>
<td>Appliance SNMP settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>Graphing</td>
<td>Appliance graphing settings</td>
</tr>
<tr>
<td>Local Configuration</td>
<td>License Key</td>
<td>Appliance licensing</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Software Updates</td>
<td>Appliance software update management</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Firewall Script</td>
<td>Appliance firewall (iptables) configuration</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Firewall Lockdown</td>
<td>Appliance management lockdown settings</td>
</tr>
</tbody>
</table>

To add a Secondary node - i.e. create a highly available clustered pair:
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 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 blue 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.

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
<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>
</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.