



IPsec Tunneling

Feature Description

UPDATED: 30 July 2023

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

These materials and all Progress® software products are copyrighted and all rights are reserved by Progress Software Corporation. The information in these materials is subject to change without notice, and Progress Software Corporation assumes no responsibility for any errors that may appear therein. The references in these materials to specific platforms supported are subject to change.

#1 Load Balancer in Price/Performance, 360 Central, 360 Vision, Chef, Chef (and design), Chef Habitat, Chef Infra, Code Can (and design), Compliance at Velocity, Corticon, Corticon.js, DataDirect (and design), DataDirect Cloud, DataDirect Connect, DataDirect Connect64, DataDirect XML Converters, DataDirect XQuery, DataRPM, Defrag This, Deliver More Than Expected, DevReach (and design), Driving Network Visibility, Flowmon, Inspec, Ipswitch, iMacros, K (stylized), Kemp, Kemp (and design), Kendo UI, Kinvey, LoadMaster, MessageWay, MOVEit, NativeChat, OpenEdge, Powered by Chef, Powered by Progress, Progress, Progress Software Developers Network, SequeLink, Sitefinity (and Design), Sitefinity, Sitefinity (and design), Sitefinity Insight, SpeedScript, Stylized Design (Arrow/3D Box logo), Stylized Design (C Chef logo), Stylized Design of Samurai, TeamPulse, Telerik, Telerik (and design), Test Studio, WebSpeed, WhatsConfigured, WhatsConnected, WhatsUp, and WS_FTP are registered trademarks of Progress Software Corporation or one of its affiliates or subsidiaries in the U.S. and/or other countries.

Analytics360, AppServer, BusinessEdge, Chef Automate, Chef Compliance, Chef Desktop, Chef Workstation, Corticon Rules, Data Access, DataDirect Autonomous REST Connector, DataDirect Spy, DevCraft, Fiddler, Fiddler Classic, Fiddler Everywhere, Fiddler Jam, FiddlerCap, FiddlerCore, FiddlerScript, Hybrid Data Pipeline, iMail, InstaRelinker, JustAssembly, JustDecompile, JustMock, KendoReact, OpenAccess, PASOE, Pro2, ProDataSet, Progress Results, Progress Software, ProVision, PSE Pro, Push Jobs, SafeSpaceVR, Sitefinity Cloud, Sitefinity CMS, Sitefinity Digital Experience Cloud, Sitefinity Feather, Sitefinity Thunder, SmartBrowser, SmartComponent, SmartDataBrowser, SmartDataObjects, SmartDataView, SmartDialog, SmartFolder, SmartFrame, SmartObjects, SmartPanel, SmartQuery, SmartViewer, SmartWindow, Supermarket, SupportLink, Unite UX, and WebClient are trademarks or service marks of Progress Software Corporation and/or its subsidiaries or affiliates in the U.S. and other countries. Java is a registered trademark of Oracle and/or its affiliates. Any other marks contained herein may be trademarks of their respective owners.

Please refer to the NOTICE.txt or Release Notes – Third-Party Acknowledgements file applicable to a particular Progress product/hosted service offering release for any related required third-party acknowledgements.

Table of Contents

| | |
|---|-----------|
| 1 Introduction | 5 |
| 1.1 Document Purpose | 6 |
| 1.2 Intended Audience | 6 |
| 1.3 Prerequisites | 6 |
| 1.4 Limitations | 6 |
| 1.4.1 Limitations Relating to the Cloud Platform Used | 6 |
| 1.4.2 LoadMaster Clustering | 7 |
| 2 Site-To-Site Tunneling | 8 |
| 2.1 Configure the Cloud Platform | 9 |
| 2.1.1 Configure Microsoft Azure | 9 |
| 2.1.2 Configure AWS | 12 |
| 2.2 Configure the LoadMaster | 14 |
| 2.2.1 Virtual Service Configuration | 16 |
| 2.2.1.1 Enable Non-Local Real Servers | 16 |
| 2.2.1.2 Disable Transparency | 17 |
| 2.2.1.3 Allow Remote Addresses | 18 |
| 2.3 Configure the LoadMaster using Route Based VPN | 19 |
| 2.3.1 View/Modify VPN Connection | 21 |
| 2.4 Configuring IPsec Tunneling in a HA Setup | 22 |
| 2.5 Delete the Connection | 23 |
| 3 IPsec Debug Options | 24 |

| | |
|--------------------------------|-----------|
| References | 27 |
| Last Updated Date | 28 |

1 Introduction

Internet Protocol Security (IPsec) is designed and used to provide secure connections between nodes and networks throughout the internet. IPsec has become the standard for most of the IP Virtual Private Network (VPN) technology.

This document covers the policy-based VPN functionality that is available in the latest LoadMaster Long Term Support (LTS) release. As of LoadMaster firmware version 7.2.53, support was added for route-based VPNs.

IPsec can operate in a point-to-point (aka host-to-host) configuration or in a site-to-site (aka network-to-network) configuration. An IPsec implementation operates in a host, as a Security Gateway (SG), or as an independent device, affording protection to IP traffic for both IPv4 and IPv6. (A security gateway is an intermediate system implementing IPsec, for example a firewall, router or gateway which has been IPsec-enabled.)

A suite of protocols are utilized to implement IPsec. These include Authentication Header (AH) and Encapsulating Security Payload (ESP). Handshaking and exchanging session keys is implemented using the Internet Key Exchange (IKE) protocol.

IPsec also has several Hashed Message Authentication Codes (HMAC) from which to choose, each giving different levels of protection for attacks such as man-in-the-middle, packet replay (anti-replay), and data integrity attacks.

There are many benefits of using IPsec. These include, but are not limited to:

- Secure connectivity provided across distributed enterprises
- Bandwidth benefits over traditionally expensive Wide Area Network (WAN) infrastructure
- Cost benefits over traditionally expensive WAN infrastructure
- Security - IPsec VPNs inherently provide a high degree of data security
- Flexibility - IPsec VPNs can be established and be available using the internet
- Resilience and High Availability (HA) for critical and sensitive applications available over the internet

1.1 Document Purpose

The purpose of this document is to explain how to set up and configure IPsec tunneling on the Kemp LoadMaster.

1.2 Intended Audience

This document is intended to be used by anyone who is interested in setting up IPsec tunneling on the LoadMaster.

1.3 Prerequisites

If needed, please obtain an externally-facing IPv4 address for the VPN device. This IP address may be required for a site-to-site configuration. Please refer to the **Limitations** section below to find out what is supported for what platforms in relation to using a public IP address.

The VPN device will either be a LoadMaster or a Network Address Translation (NAT)/firewall device.

The externally-facing public IPv4 address will either be the externally accessible public IP address which is directly available on the LoadMaster or a public IP address on a NAT/firewall device which will be NATed from the LoadMaster's internal IP address.

1.4 Limitations

1.4.1 Limitations Relating to the Cloud Platform Used

Microsoft Azure and Amazon Web Services (AWS) are currently the only supported platforms that VPN tunneling on the LoadMaster works with. There are some limitations depending on the cloud platform being used. These limitations are outlined in the table below.

| Architecture | Connection | Azure | AWS |
|-----------------------------|------------|-------------|-------------|
| Perfect Forward Secrecy | | Unsupported | Supported |
| No Perfect Forward Secrecy | | Supported | Unsupported |
| LoadMaster behind a Gateway | | Supported | Unsupported |

| Architecture | Connection | Azure | AWS |
|-------------------------------------|-----------------|-------------|-------------|
| LoadMaster with a public IP address | Private subnets | Unsupported | Unsupported |
| | Public subnets | Unsupported | Supported |

As indicated by the table above, only a public interface tunnel is supported on AWS. This is because Network Address Translation Traversal (NAT-T) is not supported on AWS.

In Azure - multiple remote and private subnets are supported. So, it is possible to have multiple IPsec connections between Azure and the LoadMaster - each connection can connect a certain LoadMaster's private subnet with a certain Azure subnet. It is also possible to connect to multiple tunnels within the one connection.

1.4.2 LoadMaster Clustering

IPsec tunneling is not enabled or supported on a system which is configured for LoadMaster clustering.

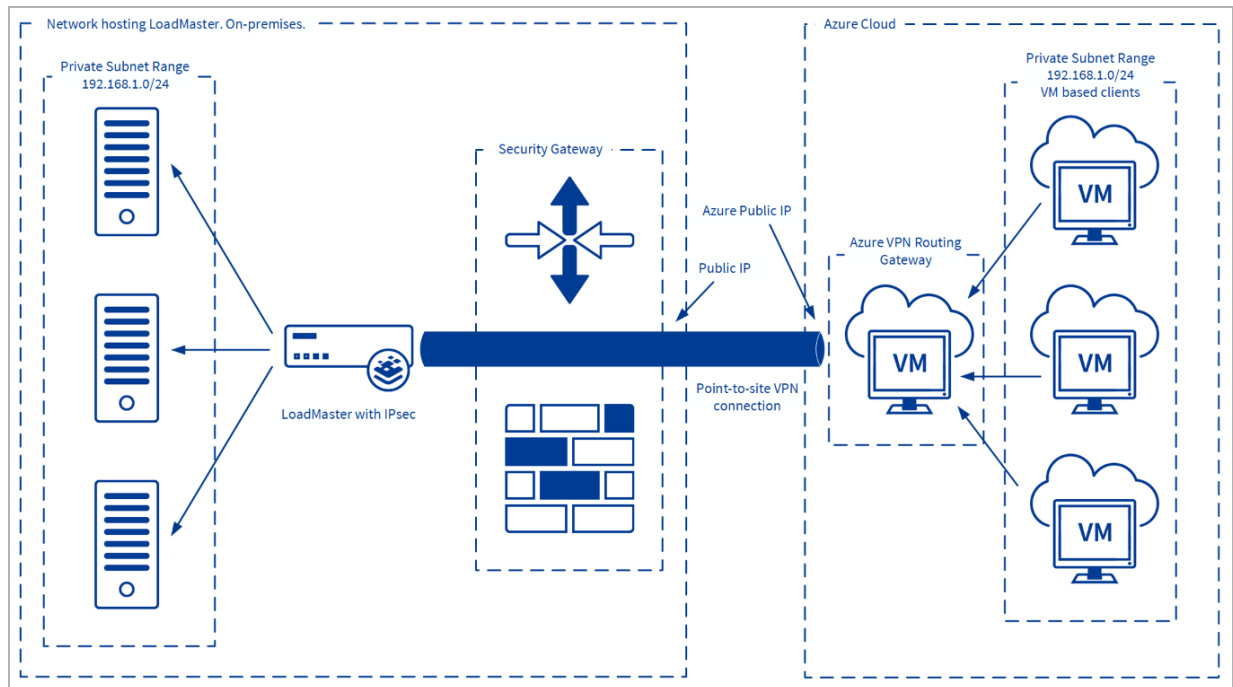
2 Site-To-Site Tunneling

IPsec is most widely used in the context of configuring a secure connection between an entire network (such as a Local Area Network (LAN)) and a remote network using a site-to-site (network-to-network) connection. This document focuses on the setting up and configuring site-to-site tunneling. However, point-to-site and host-to-host (point-to-point) will also work. Please consult the third party documentation or contact Kemp Support for further assistance.

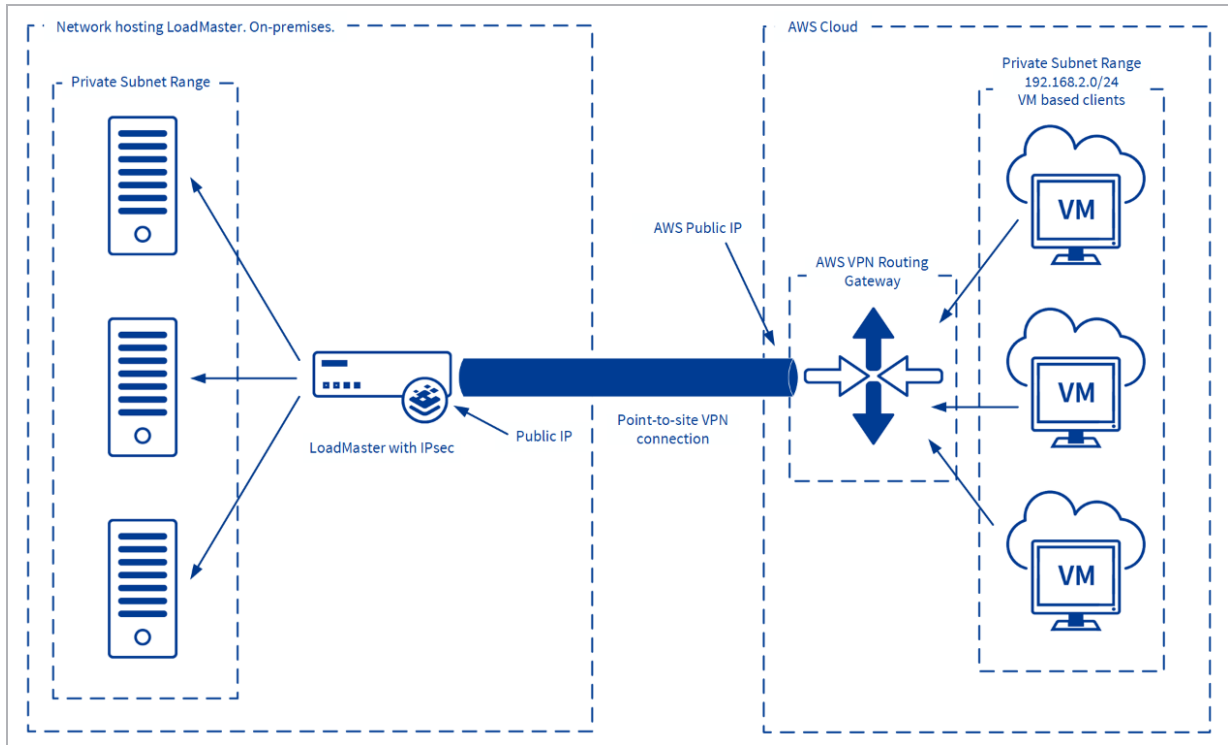
A site-to-site connection requires the setup of IPsec routers/gateways on each side of the connecting networks to transparently process and route information from one node on a LAN to a node on a remote LAN. For example, hosts on the 192.168.1.0/24 IP range can communicate with hosts on the 192.168.2.0/24 IP range.

These LANs use IPsec routers to authenticate and initiate a connection using a secure tunnel through the internet. The process of communicating from one node in the 192.168.1.0/24 IP range to another in the 192.168.2.0/24 range is completely transparent to the nodes as the processing, encryption/decryption and routing of the IPsec packets are completely handled by the IPsec routers.

The following diagram outlines a potential deployment scenario in Microsoft Azure.



The following diagram outlines a potential deployment scenario in AWS. In this case, the firewall and Public IP address are on the LoadMaster and the LoadMaster acts as the security gateway.



2.1 Configure the Cloud Platform

IPsec tunnelling using the LoadMaster is currently supported on these cloud platforms:

- Microsoft Azure
- Amazon Web Services (AWS)

Steps on how to set up a VPN connection on each of these cloud platforms are provided in the sections below.

These steps are correct at the time of writing this document. These steps may change without our knowledge. Please consult the relevant third party cloud platform documentation for the latest steps.

2.1.1 Configure Microsoft Azure

There are two options for creating and configuring a virtual network:

- Configure the network manually by using a network configuration file
- Use the wizard in the Azure Management Portal

It is recommended to use the wizard the first time a virtual network is created. The wizard creates a network configuration file (.xml file) for the virtual network. After creating the first virtual network using the Management Portal, the network configuration file can be exported and used as a template to create additional virtual networks.

Follow the steps below to configure a site-to-site VPN in the Azure Management Portal:

These steps are correct at the time of writing this document.
These steps may change without our knowledge. Please
consult the Microsoft documentation for the latest steps.

1. Log in to the Azure Management portal.
2. Click **New**.
3. Click **Network Services** and then click **Virtual Network**.
4. Click **Custom Create**.
5. Enter the **Name** of the virtual network, for example **EastUSVNet**.

This network name will be used when deploying the Virtual Machines and Platform as a Service (PaaS) instances so it is recommended to not enter a complicated name here.

6. Specify the **Location**.

The location is directly related to the physical location (region) where the resources (Virtual Machines) will reside. For example, if the Virtual Machines that will be deployed to this network will be physically located in East US, select that location. The region associated with the virtual network cannot be changed after it is created.

7. On the **DNS Servers and VPN Connectivity** page, enter the following information and then click the **Next** arrow:

- a) **DNS Servers:** Enter the DNS server name and IP address, or select a previously registered DNS server from the drop-down menu.

This setting does not create a DNS server. It allows the specification of the DNS servers to be used for name resolution for this virtual network.

b) Configure Site-To-Site VPN: Select the check box called Configure a site-to-site VPN.

c) **Local Network:** A local network represents the physical on-premises location. Select a local network that has previously been created, or create a new local network.

If an existing local network was selected, go to the **Local Networks** configuration page and ensure that the VPN Device IP address (public-facing IPv4 address for the VPN device) is accurate for this local network.

8. If an existing local network was selected, skip this step. If creating a new local network, the **Site-To-Site Connectivity** page will appear. Enter the following information and then click the **Next** arrow:

a) **Name:** The name of the local (on-premises) network site.

b) **VPN Device IP Address:** This is the public-facing IPv4 address of the on-premises VPN device used to connect to Azure.

c) **Address Space:** Specify the address range(s) (including starting IP and CIDR) to be sent through the virtual network gateway to the local on-premises location. If a destination IP address falls between the ranges specified here, it will be routed through the virtual network gateway.

d) **Add address space:** If there are multiple address ranges to be sent through the virtual network gateway, this is where each additional address range is specified. Ranges can be added or removed later as needed, on the **Local Network** page.

9. On the **Virtual Network Address Spaces** page, specify the address range to be used for the virtual network. Enter the following information, and then click the checkmark to configure the network:

These are the Dynamic IP addresses (DIPS) that will be assigned to the Virtual Machines and other role instances that are deployed to this virtual network. There are a few rules regarding the virtual network address space - please refer to the [Microsoft - Virtual Network Address Spaces page](#) for more

information. It is particularly important to select a range that does not overlap with any of the ranges that are in use for the on-premises network. A range of IP addresses might need to be carved out from the on-premises network address space to be used for the virtual network.

- a) **Address Space:** Include the starting IP address and the address count.

Verify that the address spaces specified do not overlap with any of the address spaces on the on-premises network.

- b) **Add subnet:** Include the starting IP address and address count.

Additional subnets are not required, but a separate subnet may be needed for Virtual Machines that will have static DIPS. Or the Virtual Machines might need to be in a subnet that is separate from the other role instances.

- c) **Add gateway subnet:** Click to add the gateway subnet. The gateway subnet is used only for the virtual network gateway and is required for this configuration.

10. Click the checkmark on the bottom of the page and the virtual network will begin to create. When it completes, **Created** will be shown under **Status** on the **Networks** page in the Azure Management Portal.

11. Next, configure the virtual network gateway to create a secure site-to-site connection. Refer to [Microsoft - Configure a Virtual Network Gateway in the Management Portal](#) for instructions on how to do this.

12. When you get to the **Configure your VPN Device** section, refer to the section below for instructions on how to configure the LoadMaster.

2.1.2 Configure AWS

Follow the steps below to set up a VPN connection on the AWS platform:

1. Log in to the AWS console.
2. Click **VPC**.
3. Click **Virtual Private Gateways**.
4. Click **Create Virtual Private Gateway**.

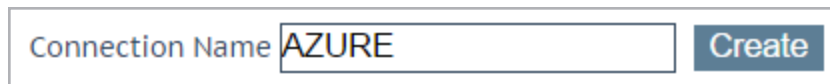
5. Enter a **Name tag**.
6. Click the **Yes, Create** button.
7. Select the Virtual Private Gateway that was just created and click the **Attach to VPC** button.
8. Select the relevant Virtual Private Cloud (VPC) from the list.
9. Click **Yes, Attach**.
10. Click **Customer Gateways** in the menu.
11. Click the **Create Customer Gateway** button.
12. Enter a recognizable **Name tag** for the LoadMaster.
13. Enter the **IP address** of the LoadMaster.
14. Click the **Yes, Create** button.
15. Click **VPN Connections** in the menu.
16. Click **Create VPN Connection**.
17. Enter a recognizable **Name tag** for the VPN connection.
18. In the **Virtual Private Gateway** drop-down list, select the Virtual Private Gateway which was created earlier.
19. Select **Static** in the **Routing Options** section.
20. Enter the LoadMaster-side network IP address followed by the CIDR in the **Static IP Prefixes** field.
21. Click the **Yes, Create** button.
22. Wait for the VPN status to become available.
23. Click **Download Configuration**.
24. Select **Generic** as the **Vendor**.
25. Select **Generic** as the **Platform**.
26. Select **Vendor Agnostic** as the **Software**.
27. Click the **Yes, Download** button.
28. Save the text file.

The text file contains the Pre-Shared Key which will be needed when configuring the LoadMaster side.

2.2 Configure the LoadMaster

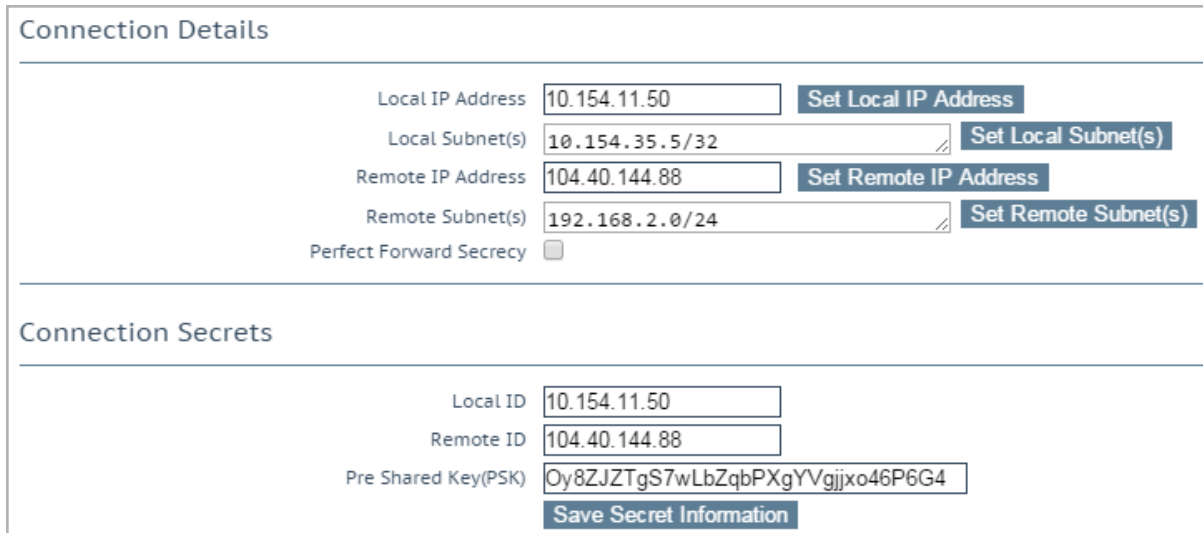
A connection end point must be added in the LoadMaster for tunneling to work. Follow the steps below to configure the LoadMaster settings:

1. In the main menu of the LoadMaster Web User Interface (WUI), go to **System Configuration > Route Management > VPN Management**.



Connection Name

2. Enter a unique and recognizable **Connection Name** and click **Create**.



Connection Details

| | | |
|-------------------------|---|--|
| Local IP Address | <input type="text" value="10.154.11.50"/> | <input type="button" value="Set Local IP Address"/> |
| Local Subnet(s) | <input type="text" value="10.154.35.5/32"/> | <input type="button" value="Set Local Subnet(s)"/> |
| Remote IP Address | <input type="text" value="104.40.144.88"/> | <input type="button" value="Set Remote IP Address"/> |
| Remote Subnet(s) | <input type="text" value="192.168.2.0/24"/> | <input type="button" value="Set Remote Subnet(s)"/> |
| Perfect Forward Secrecy | <input type="checkbox"/> | |

Connection Secrets

| | |
|--|--|
| Local ID | <input type="text" value="10.154.11.50"/> |
| Remote ID | <input type="text" value="104.40.144.88"/> |
| Pre Shared Key(PSK) | <input type="text" value="Oy8ZJTgS7wLbZqbPXgYVgjjxo46P6G4"/> |
| <input type="button" value="Save Secret Information"/> | |

3. Enter the IP address for the local side of the connection in the **Local IP Address** text box and click **Set Local IP Address**.

In non-HA mode, the **Local IP Address** should be the LoadMaster IP address, that is, the IP address of the default gateway interface.

In HA-mode, the **Local IP Address** should be the shared IP address. This will be automatically populated if HA has already

been configured. For more information on setting up tunneling in a HA configuration, refer to the next section.

4. When the **Local IP Address** is set, the **Local Subnet Address** will be automatically populated. Review the **Local Subnet Address** and update it if needed. Ensure to click **Set Local Subnet Address** to apply the setting, whether the address has been changed or not. Multiple local subnets can be specified using a comma-separated list. Up to 10 IP addresses can be specified.

5. The local IP can be the only participant if applicable, given the /32 CIDR. Enter the IP address of the remote side of the connection in the **Remote IP Address** text box and click **Set Remote IP Address**.

In the context of an Azure endpoint, this IP address is expected to be the public-facing IP address for the VPN Gateway device. For instructions on how to get this IP address, refer to [Microsoft - Configure a Virtual Network Gateway in the Management Portal](#).

6. Enter the **Remote Subnet Address** and click **Set Remote Subnet Address**. Multiple remote subnets can be specified using a comma-separated list. Up to 10 IP addresses can be specified.

7. Either enable or disable **Perfect Forward Secrecy**.

The cloud platform being used will determine what the **Perfect Forward Secrecy** option should be set to. **Perfect Forward Secrecy** is needed for some platforms but is unsupported on others. To find out what will work with your cloud platform, refer to the **Prerequisites** section.

8. By default, the **Local ID** text box is populated with the **Local IP Address** when the **Set Local IP Address** button is clicked. Review and update this address, if needed.

This may be the local IP address.

If the LoadMaster is in HA mode, the **Local ID** field will be automatically set to **%any**. This value cannot be updated when the LoadMaster is in HA mode.

9. Enter identification for the remote side of the connection.

This may be the remote IP address.

10. Enter the pre-shared key string in the **Pre-Shared Key (PSK)** text box.

This is the **Shared key** which is generated and managed on the Azure side, as outlined in [Microsoft - Configure a Virtual Network Gateway in the Management Portal](#). It must be taken from Azure and entered in the **Pre-Shared Key (PSK)** text box in the LoadMaster WUI.

If you are upgrading the LoadMaster firmware from a version older than 7.2.41 to version 7.2.41 or above, Kemp recommends re-entering the PSK to encrypt it.

11. Click **Save Secret Information** to generate and save the connection identification and secret information.

12. Go back to the **VPN Management** screen.

2.2.1 Virtual Service Configuration

Refer to the sections below for information on how to configure certain Virtual Service options.

The **Subnet Originating Requests** (SOR) option is not relevant in the context of IPsec virtual Real Server resources.

2.2.1.1 Enable Non-Local Real Servers

Real Servers that are cloud-based must be specified/configured as non-local for the Virtual Services that require remote resources. The **Enable Non-Local Real Servers** option must be enabled globally in order for IPsec tunneling to work.

To enable non-local Real Servers globally, follow the steps below in the LoadMaster WUI:

1. In the main menu, go to **System Configuration > Miscellaneous Options > Network Options**.

| | |
|---|--|
| Enable Server NAT | <input type="checkbox"/> |
| Connection Timeout (secs) | <input type="text" value="660"/> Set Time (Valid values:0, 60-86400) |
| Enable Non-Local Real Servers | <input checked="" type="checkbox"/> |
| Enable Alternate GW support | <input checked="" type="checkbox"/> |
| Enable TCP Timestamps | <input type="checkbox"/> |
| Enable TCP Keepalives | <input checked="" type="checkbox"/> |
| Enable Reset on Close | <input type="checkbox"/> |
| Subnet Originating Requests | <input type="checkbox"/> |
| Enforce Strict IP Routing | <input type="checkbox"/> |
| Handle non HTTP Uploads | <input type="checkbox"/> |
| Enable Connection Timeout Diagnostics | <input type="checkbox"/> |
| Legacy TCP Timewait handling | <input type="checkbox"/> |
| Enable SSL Renegotiation | <input checked="" type="checkbox"/> |
| Force Real Server Certificate Checking | <input type="checkbox"/> |
| Disable Master Secret Handling | <input type="checkbox"/> |
| Size of SSL Diffie-Hellman Key Exchange | <input type="text" value="2048 Bits"/> |
| Log SSL errors | <input type="text" value="Fatal errors only"/> |
| OpenSSL Version | <input type="text" value="Use current SSL library + TLS 1.3"/> |
| Use Default Route Only | <input type="checkbox"/> |
| HTTP(S) Proxy | <input type="text"/> Set HTTP(S) Proxy |

2. Select the Enable Non-Local Real Servers check box.

2.2.1.2 Disable Transparency

Due to the use of non-local Real Servers, the **Transparency** option must be disabled in the relevant Virtual Services. To disable transparency, follow the steps below:

1. In the main menu, go to Virtual Services > View/Modify Services.

| Add New | | | | | | | | |
|-------------------------|------|----------|-------|-----------------------|-------------|--------|----------------------------|---|
| Virtual IP Address | Prot | Name | Layer | Certificate Installed | Scheduler | Status | Real Servers | Operation |
| 10.0.35.6:80 | tcp | TestHttp | L7 | | round robin | Up | 192.168.2.4 | Modify Delete |
| 10.0.35.7:22 | tcp | TestSSH | L7 | | round robin | Up | 192.168.2.4 192.168.2.5 | Modify Delete |

2. Click **Modify** on the relevant Virtual Service.
3. Expand the **Standard Options** section.

▼ Standard Options

Force L7 ☒

Transparency ☐

Subnet Originating Requests ☐

Extra Ports Set Extra Ports

Persistence Options Mode:

None ▼

Scheduling Method

round robin ▼

Idle Connection Timeout (Default 660) Set Idle Timeout

Quality of Service

Normal-Service ▼

- Remove the tick from the **Transparency** text box.

2.2.1.3 Allow Remote Addresses

When adding a Real Server, ensure the **Allow Remote Addresses** option is enabled.

This option will only be visible when adding a Real Server if **Enable Non-Local Real Servers** has been enabled and **Transparency** has been disabled on the relevant Virtual Service. For instructions on how to configure these options, refer to the **Enable Non-Local Real Servers** and **Disable Transparency** sections.

To do this, follow the steps below in the LoadMaster WUI:

- In the main menu, go to **Virtual Services > View/Modify Services**.

| <button>Add New</button> | | | | | | | | | |
|--------------------------|------|----------|-------|-----------------------|-------------|--------|----------------------------|-------------------------|-------------------------|
| Virtual IP Address | Prot | Name | Layer | Certificate Installed | Scheduler | Status | Real Servers | Operation | |
| 10.0.35.6:80 | tcp | TestHttp | L7 | | round robin | Up | 192.168.2.4 | <button>Modify</button> | <button>Delete</button> |
| 10.0.35.7:22 | tcp | TestSSH | L7 | | round robin | Up | 192.168.2.4 192.168.2.5 | <button>Modify</button> | <button>Delete</button> |

- Click **Modify** on the relevant Virtual Service.
- Expand the **Real Servers** section.
- Click **Add New**.

Please Specify the Parameters for the Real Server

| | |
|------------------------|-------------------------------------|
| Allow Remote Addresses | <input checked="" type="checkbox"/> |
| Real Server Address | <input type="text"/> |
| Port | <input type="text" value="80"/> |
| Forwarding method | <input type="text" value="nat"/> |
| Weight | <input type="text" value="1000"/> |
| Connection Limit | <input type="text"/> |

5. Enable the **Allow Remote Addresses** option.

6. Fill out the other details as needed.

Kemp recommends using static IP addresses for the Real Servers on the Azure side.

7. Click **Add This Real Server**.

2.3 Configure the LoadMaster using Route Based VPN

Prior to LoadMaster firmware version 7.2.53, the LoadMaster only supported policy-based Virtual Private Networks (VPNs). As of LoadMaster version 7.2.53, route-based VPN support has been introduced. The route-based VPN functionality is available as an add-on pack which you can download from the [Kemp Support Site](#). When you have the add-on file, install it in **System Configuration > System Administration > Update Software**. Reboot the LoadMaster after installing the add-on to activate it (**System Configuration > System Administration > System Reboot**).

The route-based VPN add-on is only supported in firmware version 7.2.53 and above.

After installing the add-on and rebooting the LoadMaster, a new main menu option becomes available: **System Configuration > Network Setup > Route Based VPN**. Specify a unique name to identify the connection and click **Create**.

After configuring the details of the VPN connection, you can also see the **Connection Debug** options:

- Stop and start the IPsec daemon on the LoadMaster.
- Display the connection status.
- Display routes.
- Show logs.

Connection Endpoints Configuration

Refresh

| Connection Name | Status | Local Subnet(s) | Remote Subnet(s) | Operation |
|-----------------|--------|-----------------|------------------|--------------------|
| test | ● Down | | | View/Modify Delete |

Connection Debug

Stop IPsec Daemon

Stop IPsec Daemon

Show IPsec Status

IPsec Status

Show Routes

Routes

Show Logs

Logs

Create a new connection

Connection Name

Create

Connection Name

Specify a unique name to identify the connection.

Create

Create a uniquely identifiable connection with the specified name.

View/Modify

View or modify the configuration parameters for this connection.

Delete

Delete this connection.

Ensure the **Connection Name** is the same as the connection name in the **ipsec.conf** file you will be uploading.

The **Connection Name** must be at least three and at most 20 characters in length. Valid characters are **a-z, A-Z, 0-9, _**, and **-**.

After creating the connection initially, you must upload the connection configuration, route configuration, and secrets files based on the strongSwan standard format.

Ensure to set the left IP address in the ipsec.conf file to your LoadMaster IP address (eth0).

Once the files have been uploaded and validated, the **Connection Details** are shown in the fields on the **View/Modify** VPN Connection screen.

2.3.1 View/Modify VPN Connection

| Connection Details | | |
|---------------------------------------|---|---|
| Local IP Address | <input type="text" value="10.35.30.109"/> | |
| Local Subnet(s) | <input type="text" value="0.0.0.0/0"/> | |
| Remote IP Address | <input type="text" value="10.35.44.42"/> | |
| Remote Subnet(s) | <input type="text" value="0.0.0.0/0"/> | |
| Connection Config file | <input type="button" value="Choose File"/> No file chosen | <input type="button" value="Update Config"/> |
| Route Config file | <input type="button" value="Choose File"/> No file chosen | <input type="button" value="Update Route"/> |
| Connection Secrets | | |
| Secrets file | <input type="button" value="Choose File"/> No file chosen | <input type="button" value="Update Secrets"/> |
| Connection Debug | | |
| Start Connection | <input type="button" value="Start Connection"/> | |
| Show IPsec Status | <input type="button" value="IPSec Status"/> | |
| Show Logs | <input type="button" value="Logs"/> | |
| <input type="button" value="←-Back"/> | | |

Local IP Address

Display the IP address for the local side of the connection.

In non-HA mode, the **Local IP Address** should be the LoadMaster IP address, that is, the IP address of the default gateway interface.

In HA-mode, the **Local IP Address** should be the shared IP address. This will be automatically populated if HA has already been configured. For more information on setting up tunneling in a HA configuration, refer to the next section.

Local Subnet(s)

Display the **Local Subnet(s)** for the local side of the connection.

Remote IP Address

Display the IP address for the remote side of the connection. In the context of an Azure endpoint, this IP address is expected to be the public-facing IP address for the Virtual Private Network (VPN) Gateway device.

Remote Subnet(s)

Display the subnet for the remote side of the connection.

Connection Config file

Click the **Choose File**, browse to and select the file and click **Update Config**.

Route Config file

Click the **Choose File**, browse to and select the file and click **Update Route**.

Secrets file

Click the **Choose File**, browse to and select the file and click **Update Secrets**.

Show IPsec Status

You can display the connection status by clicking **IPSec Status**.

Show Logs

You can display the connection logs by clicking **Logs**.

2.4 Configuring IPsec Tunneling in a HA Setup

When configuring IPsec tunneling in a HA setup, ideally HA should be configured first. For instructions on how to configure HA, refer to the [High Availability \(HA\), Feature Description](#).

When HA is configured - to set up tunneling, follow the steps in the **Configure the Cloud Platform** and **Configure the LoadMaster** sections above. Ensure to configure IPsec tunneling on the master HA unit. If HA is configured, the **Local IP Address** will be automatically populated with the HA shared IP address. Also, the **Local ID** field will be automatically set to **%any**. This value cannot be updated when the LoadMaster is in HA mode.

If the HA shared IP address is changed after the VPN tunnel connection has been established, the tunnel connection will break. Please ensure to update the **Local IP Address** if the shared IP address changes.

2.5 Delete the Connection

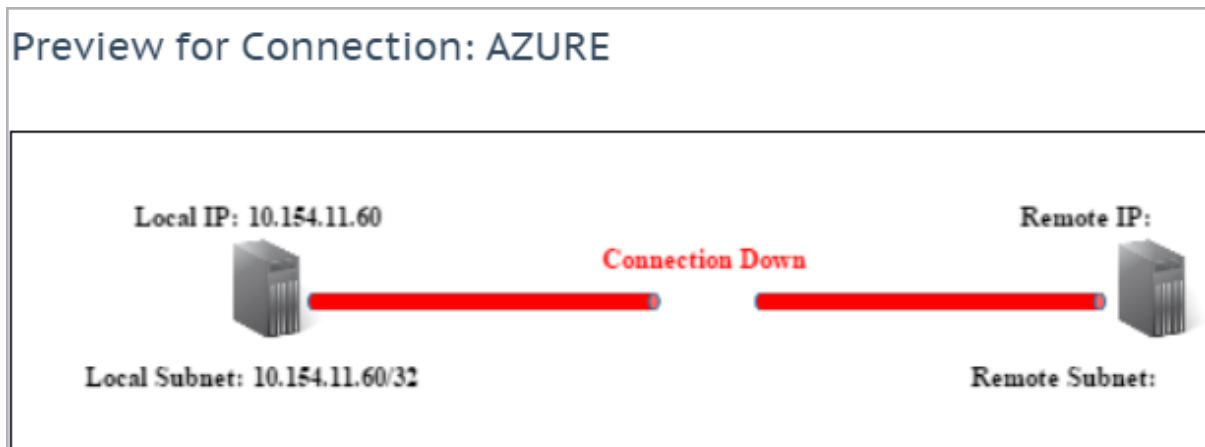
| Status | Operation |
|--------|------------------------------|
| Down | <div>View/ModifyDelete</div> |
| Down | <div>View/ModifyDelete</div> |
| Up | <div>View/ModifyDelete</div> |
| Up | <div>View/ModifyDelete</div> |

To delete a VPN connection, go to **System Configuration > Route Management > VPN Management** and click **Delete**. Then, click **OK** to the warning.

All associated configuration will be permanently deleted.

A connection can be deleted at any time, even if it is running.

3 IPsec Debug Options



If the connection is down, the diagram on the **VPN Management** page will say **Connection Down** and the tunnel will be red.

| | |
|-------------------------------|------------------------------------|
| Boot.msg File | View |
| Warning Message File | View |
| System Message File | View |
| Nameserver Log File | View |
| Nameserver Statistics | View |
| IPsec IKE Log | View |
| WAF Event Log | View |
| Audit LogFile | View |
| <hr/> | |
| Reset Logs | Reset |
| Save all System Log Files | Download Log Files |
| <hr/> | |
| Debug Options | |

To view the IPsec IKE Log, go to **Logging Options > System Log Files** and click **View** next to **IPsec IKE Log**.

Debug Options

Disable All Transparency

Disable Transparency

Enable L7 Debug Traces

Enable Traces

Enable Extended L7 Debug

Enable Extended Debug

Enable IRQ Pinning

Enable IRQ Pinning

Perform an l7adm

l7adm

Enable WAF Debug Logging

Enable Logging

Enable IRQ Balance

Enable IRQ Balance

Enable TSO

Enable TSO

Enable TCP SACK

Enable TCP SACK

Enable Layer 4 IPv6 Forwarding

☒

Disable CLI VS Management

Disable CLI VS Management

Enable Bind Debug Traces

Enable Bind Traces

Perform a PS

ps

Perform Top

top

Iterations

10

Interval

1

sec

☐ Show Threads

☐ Sort by Memory usage

Include Top in Backups

☐

Display Meminfo

Meminfo

Display Slabinfo

Slabinfo

Perform an Ifconfig

Ifconfig

Perform a Netstat

Netstat

Include Netstat in Backups

☒

Reset Statistic Counters

Reset Statistics

Flush OCSPD Cache

Flush Cache

Enable SSOMGR Debug Traces

Enable Traces

Flush SSO Authentication Cache

Flush SSO Cache

Linear SSO Logfiles

☐

Start IPsec IKE Daemon

Start IPsec IKE Daemon

Perform an IPsec Status

IPsec Status

Enable IKE Debug Level Logs

Enable Logs

Netconsole Host

Interface

eth0

Set Netconsole Host

Ping Host

Interface

eth0

Ping

Ping6 Host

Interface

Automatic

Ping6

Traceroute Host

Traceroute

Kill LoadMaster (395722)

Kill LoadMaster

Enable DHCPv6 Client

☐

There are debug options that can help when troubleshooting problems with IPsec tunneling. To see these options, go to **System Configuration > Logging Options > System Log Files > Debug Options** in the main menu of the LoadMaster WUI.

Stop IPsec IKE Daemon

Stop the IPsec IKE daemon on the LoadMaster.

If this button is clicked, the connection for all tunnels will go down.

Perform an IPsec Status

Display the raw IPsec status output.

```
000 stats db_ops: {curr_cnt, total_cnt, maxsz}:context={0,124,64} trans={0,124,648} attrs={0,124,432}
000
000 "AZURE": 10.0.35.0/24===10.0.35.5<10.0.35.5>...104.40.144.88<104.40.144.88>===192.168.2.0/24; erouted; eroute owner: #139
000 "AZURE": myip=unset; hisip=unset;
000 "AZURE": ike_life: 28800s; ipsec_life: 3600s; rekey_margin: 540s; rekey_fuzz: 100%; keyingtries: 0
000 "AZURE": policy: PSK+ENCRYPT+TUNNEL+IKEv2ALLOW+SAREFTRACK+IKOD+rKOD; prio: 24,24; interface: eth0;
000 "AZURE": dpd: action:restart; delay:30; timeout:120;
000 "AZURE": newest ISAKMP SA: #138; newest IPsec SA: #139;
000 "AZURE": IKE algorithms wanted: AES_CBC(7)_128-SHA1(2)_000-MODP1024(2); flags=-strict
000 "AZURE": IKE algorithms found: AES_CBC(7)_128-SHA1(2)_160-MODP1024(2)
000 "AZURE": IKE algorithm newest: AES_CBC_128-SHA1-MODP1024
000 "AZURE": ESP algorithms wanted: AES(12)_128-SHA1(2)_000; flags=-strict
000 "AZURE": ESP algorithms loaded: AES(12)_128-SHA1(2)_160
000 "AZURE": ESP algorithm newest: AES_128-HMAC_SHA1; pfsgroup=<N/A>
000
000 #139: "AZURE":4500 STATE_QUICK_I2 (sent QI2, IPsec SA established); EVENT_SA_REPLACE in 2504s; newest IPSEC; eroute owner; isakmp#138; idle; import:local rekey
000 #139: "AZURE" esp.226a22e2@104.40.144.88 esp_fa4b443@10.0.35.5 tun.0@104.40.144.88 tun.0@10.0.35.5 ref=0 refhim=4294901761
000 #138: "AZURE":4500 STATE_MAIN_I4 (ISAKMP SA established); EVENT_SA_REPLACE in 27463s; newest ISAKMP; nodpd; idle; import:local rekey
000
```

Connection information for each tunnel in the output is prefixed with “<ConnectionName>” (for example **AZURE** in the screenshot above).

Enable IKE Debug Level Logs

Control the IPsec IKE log level. When this option is enabled, additional logs will be shown in the **IPsec IKE Log** and the **IPsec Status**.

This debug option can be useful when setting up the connection initially. However, please use extreme caution if enabling this option - enabling this option will restart the daemon which will drop any connections and reestablish them.

Ping Host

Try to ping the remote IP address to check if the connection is working.

References

Some useful links containing further information are provided below:

High Availability (HA), Feature Description

<http://kemptechnologies.com/documentation/>

Microsoft - Virtual Network Address Spaces page

<http://msdn.microsoft.com/en-us/library/azure/09926218-92ab-4f43-aa99-83ab4d355555> - **Virtual Network Address Spaces page section**

Microsoft - Configure a Virtual Network Gateway in the Management Portal

<http://msdn.microsoft.com/en-us/library/azure/jj156210.aspx>

Last Updated Date

This document was last updated on 30 July 2023.