



Pulse Secure Virtual Traffic Manager: Appliance Image Installation and Getting Started Guide

Supporting Pulse Secure Virtual Traffic Manager 19.1

Product Release	19.1
Published	29 April, 2019
Document Version	1.0

Pulse Secure, LLC
2700 Zanker Road,
Suite 200 San Jose
CA 95134

www.pulsesecure.net

© 2019 by Pulse Secure, LLC. All rights reserved.

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Pulse Secure Virtual Traffic Manager: Appliance Image Installation and Getting Started Guide

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at <http://www.pulsesecure.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Contents

.....	PREFACE	1
DOCUMENT CONVENTIONS		1
TEXT FORMATTING CONVENTIONS.....		1
COMMAND SYNTAX CONVENTIONS.....		1
NOTES AND WARNINGS.....		2
REQUESTING TECHNICAL SUPPORT		2
SELF-HELP ONLINE TOOLS AND RESOURCES.....		2
OPENING A CASE WITH PSGSC		3
OVERVIEW		5
ABOUT THIS GUIDE.....		5
INTRODUCING THE TRAFFIC MANAGER.....		5
PRODUCT VARIANTS		6
GETTING STARTED.....		7
NETWORK ARCHITECTURE		7
PREREQUISITES.....		7
NETWORK CONFIGURATIONS.....		9
SCENARIO 1: SIMPLE NETWORK		9
SCENARIO 2: PUBLIC/PRIVATE NETWORKS.....		10
SCENARIO 3: MULTIPLE TRAFFIC MANAGERS.....		11
MANAGEMENT NETWORK.....		12
INSTALLING THE TRAFFIC MANAGER APPLIANCE IMAGE.....		15
BEFORE YOU BEGIN.....		15
CREATING AN INSTALLATION DISK OR USB FLASH DRIVE		15
CREATING A BOOT-ABLE TRAFFIC MANAGER CD-ROM OR DVD-ROM.....		15
CREATING A BOOT-ABLE TRAFFIC MANAGER USB FLASH DRIVE		16
INSTALLING THE TRAFFIC MANAGER FROM A DISK OR USB FLASH DRIVE.....		18
INSTALLING THROUGH A PXE BOOT ENVIRONMENT.....		19
CONFIGURING THE TRAFFIC MANAGER APPLIANCE		21
CHECKING THE INITIAL IP ADDRESS.....		21
CONNECTING TO THE ADMIN UI		22
RUNNING THE INITIAL CONFIGURATION WIZARD		23
ACCEPT THE TERMS AND CONDITIONS OF SALE		23
CONFIGURING NETWORKING.....		24

DNS SETTINGS	27
HOSTNAME RESOLUTION	27
TIMEZONE SETTINGS	28
ADMIN PASSWORD.....	29
IPMI SETTINGS	29
LICENSE KEY.....	30
SUMMARY.....	30
CONFIGURING THE APPLIANCE FROM THE COMMAND LINE	32
PERFORMING AN UNATTENDED CONFIGURATION.....	37
THE COMMUNITY EDITION.....	37
NTP SETTINGS	38
IPMI MANAGEMENT	38
UPGRADING YOUR TRAFFIC MANAGER.....	39
BEFORE YOU START	39
PERFORMING AN UPGRADE	40
REVERTING TO AN EARLIER VERSION	41
CHANGING YOUR TRAFFIC MANAGER VERSION MANUALLY	43
MONITORING YOUR HARDWARE.....	43
NETWORK INTERFACES.....	43
APPLIANCE HARDWARE STATUS REPORTING	45
USEFUL SYSTEM INFORMATION	46
SSH.....	46
FREEING UP DISK SPACE	46
CHANGING THE TRAFFIC MANAGER NAME	46
RESETTING TO FACTORY DEFAULTS	47
RESETTING THE ADMIN PASSWORD	47
BASIC CONFIGURATION INFORMATION.....	49
VIRTUAL SERVERS, POOLS, AND RULES.....	49
MANAGING YOUR FIRST SERVICE.....	50
CREATING A TRAFFIC MANAGER CLUSTER	51
OPEN SOURCE SOFTWARE NOTICE	55

Preface

- [Document conventions](#) 1
- [Requesting Technical Support](#) 2

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Pulse Secure technical documentation.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used in the flow of the text to highlight specific words or phrases.

Format	Description
bold text	Identifies command names
	Identifies keywords and operands
	Identifies the names of user-manipulated GUI elements
	Identifies text to enter at the GUI
<i>italic text</i>	Identifies emphasis
	Identifies variables
	Identifies document titles
Courier Font	Identifies command output
	Identifies command syntax examples

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
<i>italic text</i>	Identifies a variable.
[]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.

Convention	Description
{ x y z }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x y	A vertical bar separates mutually exclusive elements.
< >	Non-printing characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, member[member...].
\	Indicates a “soft” line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Notes and Warnings

Note, Attention, and Caution statements might be used in this document.

Note: A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION

An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

CAUTION

A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

Requesting Technical Support

Technical product support is available through the Pulse Secure Global Support Center (PSGSC). If you have a support contract, file a ticket with PSGSC.

- Product warranties—For product warranty information, visit <https://support.pulsesecure.net/product-service-policies/>

Self-Help Online Tools and Resources

For quick and easy problem resolution, Pulse Secure provides an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://support.pulsesecure.net>
- Search for known bugs: <https://support.pulsesecure.net>
- Find product documentation: <https://www.pulsesecure.net/techpubs>
- Download the latest versions of software and review release notes: <https://support.pulsesecure.net>
- Open a case online in the CSC Case Management tool: <https://support.pulsesecure.net>

- To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://support.pulsesecure.net>

For important product notices, technical articles, and to ask advice:

- Search the Pulse Secure Knowledge Center for technical bulletins and security advisories: <https://kb.pulsesecure.net>
- Ask questions and find solutions at the Pulse Community online forum: <https://community.pulsesecure.net>

Opening a Case with PSGSC

You can open a case with PSGSC on the Web or by telephone.

- • Use the Case Management tool in the PSGSC at <https://support.pulsesecure.net>.
- • Call 1-844 751 7629 (Toll Free, US).

For international or direct-dial options in countries without toll-free numbers, see <https://support.pulsesecure.net/support/support-contacts/>

Overview

This chapter provides an overview of Pulse Secure Virtual Traffic Manager (the Traffic Manager). This chapter contains the following sections:

- [About This Guide](#) 5
- [Introducing the Traffic Manager](#) 5
- [Product Variants](#) 6

About This Guide

The *Pulse Secure Virtual Traffic Manager: Appliance Image Installation and Getting Started Guide* describes the appliance image variant of the Traffic Manager.

Read this guide for an introduction to the functionality available in the Traffic Manager appliance image variant, and for instructions on how to install and configure the Traffic Manager on supported hardware appliances.

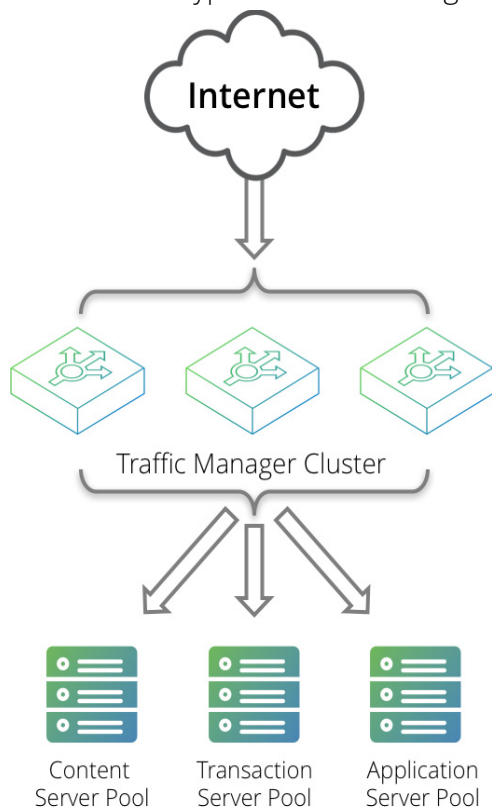
For a detailed description of the Traffic Manager and it's full feature set, see the *Pulse Secure Virtual Traffic Manager: User's Guide*.

Introducing the Traffic Manager

The Traffic Manager product family provides high-availability, application-centric traffic management and load balancing solutions in a range of software, hardware-ready, virtual appliance, and cloud-compute product variants. They provide control, intelligence, security and resilience for all your application traffic.

The Traffic Manager is intended for organizations hosting valuable business-critical services, such as TCP-based and UDP-based services like HTTP (web) and media delivery, and XML-based services such as Web Services.

FIGURE 1 A Typical Cluster Configuration



Product Variants

The Traffic Manager product line is available in a variety of forms on different platforms:

- As software, with versions for supported Linux and UNIX operating systems (including support for virtual machine instances running on Amazon's Elastic Compute Cloud (EC2) platform).
- As a virtual appliance, with versions for VMware vSphere, Citrix XenServer, Microsoft Hyper-V, and QEMU/KVM.
- As a cloud computing platform machine image, with versions for Amazon's Elastic Compute Cloud (EC2), Rackspace, Microsoft Azure, and Google Compute Engine (GCE). Pulse Secure additionally supports installing the Traffic Manager software variant on supported Linux and UNIX virtual machine instances running on EC2 and GCE.
- As an appliance disk image, suitable for deployment on approved server hardware platforms.

Pulse Secure provides a separate edition of this guide for each of the above product variants.

The release notes included with your product variant contain a full list of the supported platforms and versions.

Getting Started

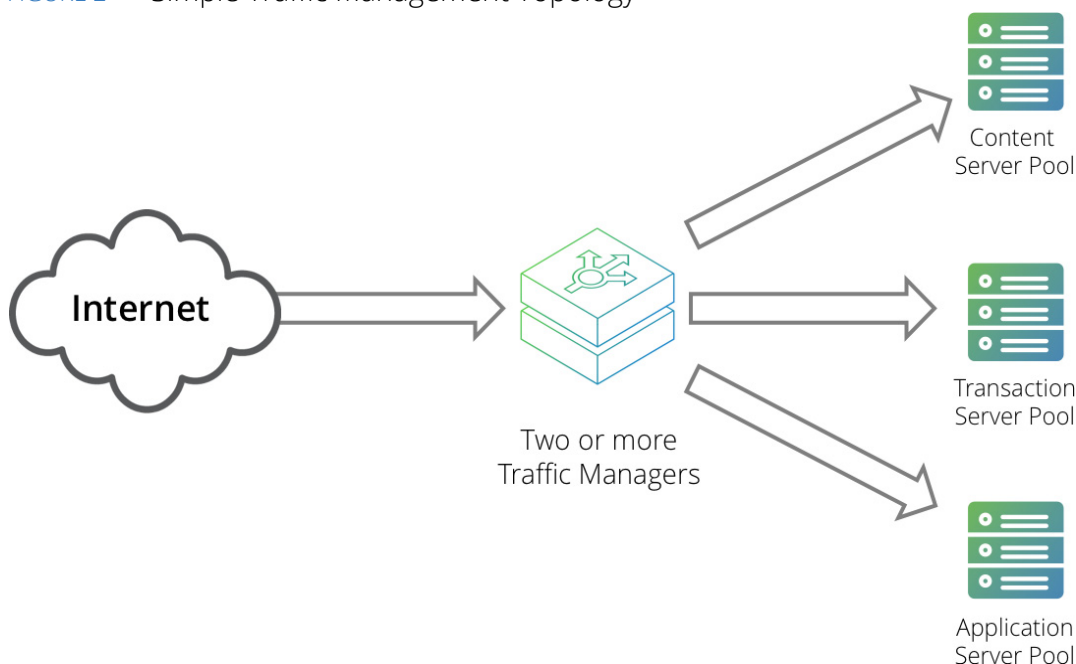
This chapter contains information about getting started using the Traffic Manager. This chapter contains the following sections:

- **Network Architecture** 7
- **Prerequisites** 7
- **Network Configurations** 9
- **Management Network** 12

Network Architecture

The Traffic Manager is positioned between the Internet and your back-end servers, acting as a reverse proxy. It can be used in conjunction with a standalone firewall if desired. Traffic received from the Internet is passed on to the most appropriate back-end server to respond to the request.

FIGURE 2 Simple Traffic Management Topology



You can install two or more Traffic Managers in a clustered configuration to provide full fault-tolerance for individual software failures. A typical configuration contains at least two Traffic Managers, and at least two servers hosting the load-balanced application.

Prerequisites

Pulse Secure supports use of the Traffic Manager software on approved hardware server appliances. To view the current reference hardware specifications, see the Pulse Community Web site (<http://kb.pulsesecure.net>).

To install the Traffic Manager on your server appliance, first create a suitable installation medium containing the necessary files. Pulse Secure supports use of a CD-ROM/DVD-ROM or USB memory drive for this purpose.

Pulse Secure additionally supports deployment of the Traffic Manager through a Preboot Execution Environment (PXE). For further information on PXE and compatibility with your server appliance, refer to your hardware supplier.

Before you begin the installation of the Traffic Manager appliance image, make sure you have the version appropriate to your deployment type, and suitable license keys for each Traffic Manager instance you want to install.

To configure the Traffic Manager software, make sure that you have the following information:

- Hostnames for each of the virtual appliance instances that you are creating.
- IP addresses for each of the interfaces that you intend to use on each virtual appliance.
- Subnet masks for each of the IP addresses you are using.
- The domain name to which your appliances belong (optional)
- The IP address for the default gateway.
- The IP address for each name server that the virtual appliance uses to resolve your internal network addresses (optional).
- The DNS search path (the "local part" of your machine hostnames) (optional). This item is commonly the same as the domain name.
- An Admin password for the Admin UI.

You administer all Traffic Manager variants through a Web-enabled user interface. The Traffic Manager supports the following browsers for this purpose:

- Internet Explorer: v.11 or newer
- Microsoft Edge: latest version
- Mozilla Firefox: latest version
- Apple Safari: latest version
- Google Chrome: latest version

Pulse Secure does not warrant the use of browser versions older than those listed here due to potential discontinuation of security updates by the vendor.

Pulse Secure recommends using one or more test servers (for example, Web servers) to which you can direct traffic.

Note: References to \$ZEUSHOME throughout this guide refer to the Traffic Manager software installation directory at /opt/zeus.

Network Configurations

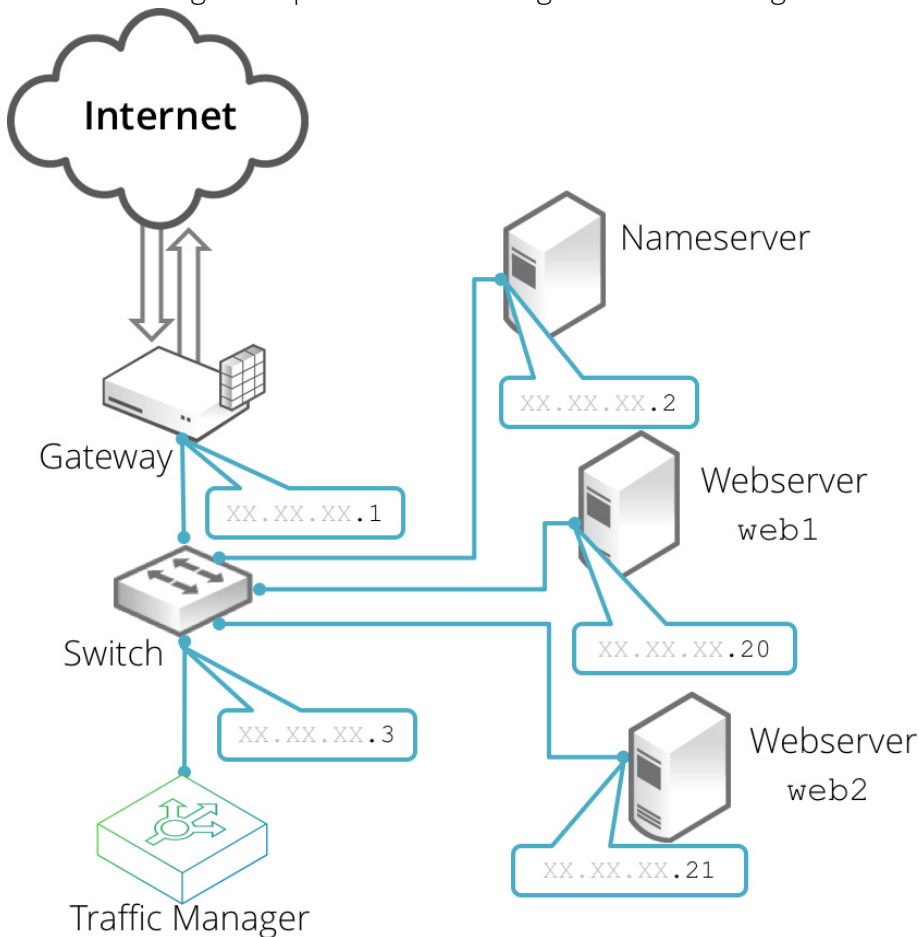
This section provides a number of scenarios showing how you can deploy the Traffic Manager into your network.

Scenario 1: Simple Network

This scenario demonstrates how you can place a single Traffic Manager into an existing network to handle traffic for a Web site. All IP addresses run on a publicly addressable network (represented by xx.xx.xx in the diagram, with a netmask of 255.255.255.0).

Without the Traffic Manager, clients connecting to the Web site are directed, through the gateway, to one of the Web servers hosting the site (for example, "web1" on the IP address xx.xx.xx.20).

FIGURE 3 Single setup of a Traffic Manager into an existing network



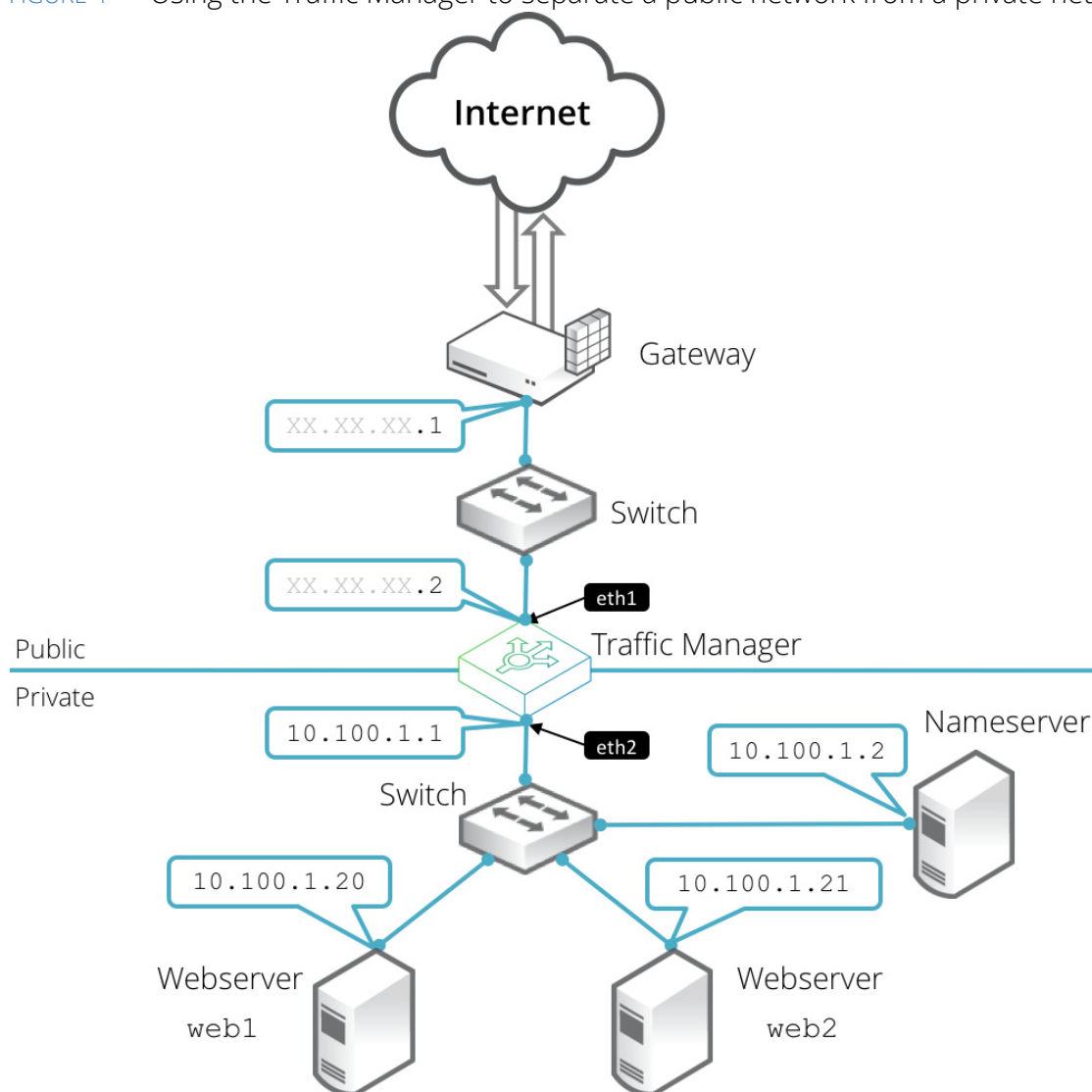
By installing a Traffic Manager, configured to receive traffic over a single network port and IP address xx.xx.xx.3, you can alter your DNS record to instead direct clients to xx.xx.xx.3. In this way, the Traffic Manager receives the Web page requests and responds with content from one of the available Web servers.

Scenario 2: Public/Private Networks

This scenario splits your network infrastructure into separate public and private networks. This offers greater security as the private network hides the internal back-end services from the outside world. Access is only permitted through the Traffic Manager. Using more network interfaces also gives higher performance as there is greater bandwidth capacity.

The diagram shows how you can configure the network gateway and the Traffic Manager's front-end (eth1) interface with publicly routable IP addresses (the xx.xx.xx network, netmask 255.255.255.0). You then configure the Traffic Manager's back-end interface (eth2) on the internal network (10.100.xx.xx, netmask 255.255.0.0).

FIGURE 4 Using the Traffic Manager to separate a public network from a private network

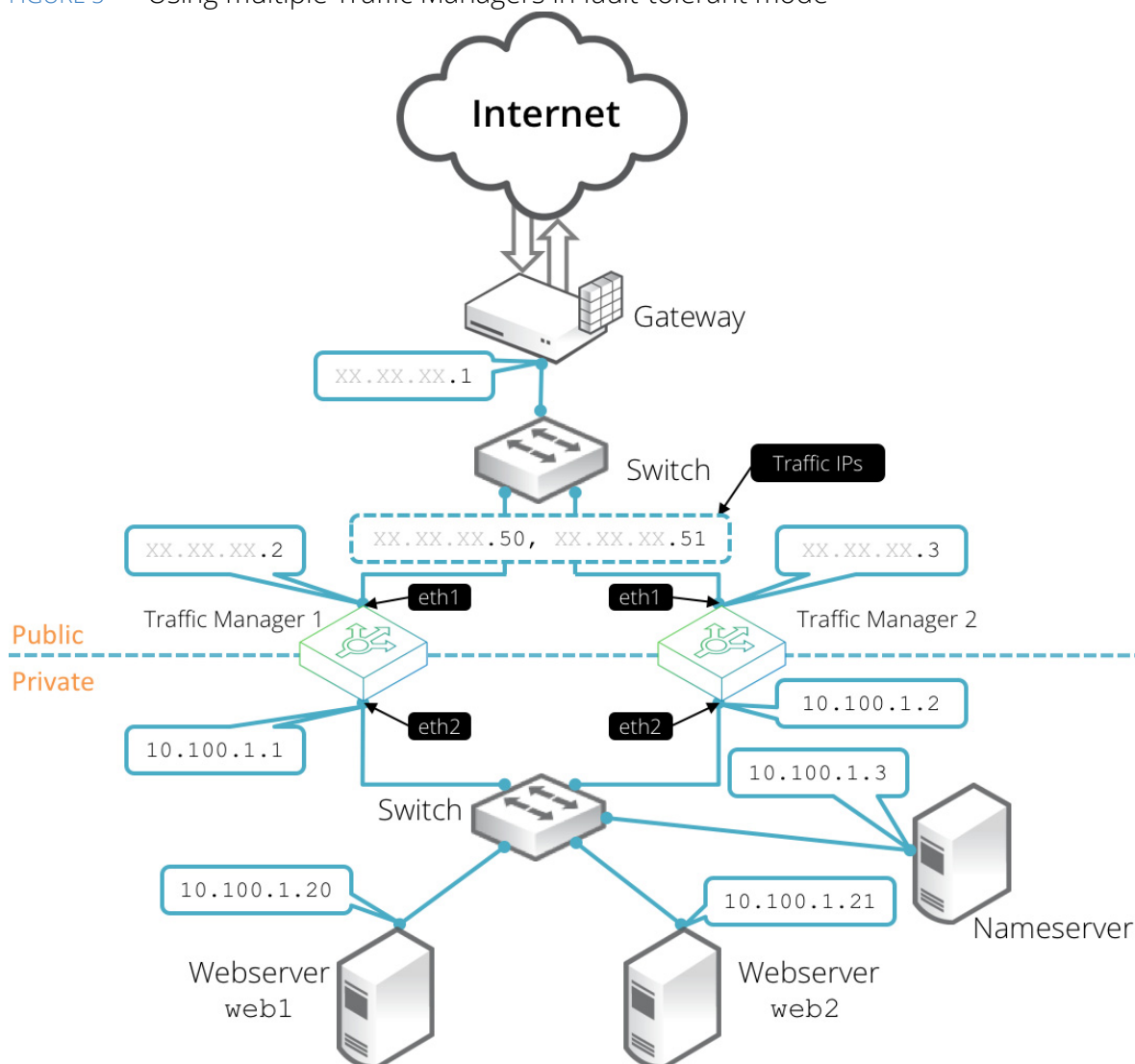


Scenario 3: Multiple Traffic Managers

This scenario deploys two Traffic Managers in a public/private network. The Traffic Managers make use of Traffic IP Addresses to provide a fault tolerant service. Traffic IP addresses are additional IP addresses that are distributed across the front-end network interfaces. If one Traffic Manager becomes uncontactable, the other Traffic Manager is able to adopt the Traffic IP address and continue handling requests.

You define and manage your Traffic IP addresses through the Traffic Manager's Web-based Admin UI, and you set them up after the initial low-level networking is complete. For more information, see the *Pulse Secure Virtual Traffic Manager: User's Guide*.

FIGURE 5 Using multiple Traffic Managers in fault-tolerant mode



Management Network

By default, the Traffic Manager accepts management traffic on all of its network interfaces. All management traffic is encrypted or secured.

Management traffic includes the following types:

- Access to the Web-based administration interface (also known as the Admin UI).
- Connections through the SOAP-based Control API, the REST API, and Command-Line Interface (CLI).
- Internal health and state sharing traffic.

You typically use a network firewall to prevent external clients from attempting to access any of the management interfaces.

For heightened security, the Traffic Manager enables you to nominate a particular network interface for management traffic. This interface can reside on a secure internal management network.

Installing the Traffic Manager Appliance Image

This chapter describes how to install the Traffic Manager appliance image on an approved server hardware platform.

It contains the following sections:

- [Before you Begin](#) 15
- [Creating an Installation Disk or USB Flash Drive](#) 15
- [Installing the Traffic Manager From a Disk or USB Flash Drive](#) 18
- [Installing Through a PXE Boot Environment](#) 19

Before you Begin

Pulse Secure provides a Traffic Manager appliance disk image conforming to the ISO standard format, with supporting files supplied in a pair of ZIP archives:

- `ZeusTM_<Version>_Appliance-x86_64.zip`: Contains files for creating boot-able CD-ROMs, DVD-ROMs, and USB flash drives.
- `ZeusTM_<Version>_Appliance-x86_64-PXE.zip`: Contains files for deploying the Traffic Manager through a configured PXE environment.

Note: Throughout this chapter, substitute the string `<Version>` in file names with the release number for the Traffic Manager you are installing. For example, `ZeusTM_19.1_Appliance-x86_64.zip`.

ATTENTION

Before you begin installation, make sure your appliance RAID controller (if applicable) is properly configured and your system BIOS is set to boot in legacy mode.

Creating an Installation Disk or USB Flash Drive

This section describes the process of creating a boot-able Traffic Manager appliance installation CD-ROM, DVD-ROM, or USB flash drive.

Creating a boot-able Traffic Manager CD-ROM or DVD-ROM

1. Unpack the Traffic Manager ZIP archive to your workstation.
2. Locate the Traffic Manager .iso disk image file (`ZeusTM_<Version>_Appliance-x86_64.iso`) from within the unpacked file set.
3. Insert a blank CD-ROM or DVD-ROM.

4. Use a suitable CD/DVD writing program to create a boot-able disk from the Traffic Manager .iso disk image file.

Creating a boot-able Traffic Manager USB flash drive

For USB flash drives, use the instructions that correspond to your workstation operating system - Linux/UNIX, Windows, or Macintosh.

CAUTION

The procedures described in this section completely erase the contents of your USB flash drive. Make sure you have a backup of any important data before you begin.

In all cases, perform the following initial steps:

1. Before you start, make sure your USB flash drive is compatible with the Traffic Manager appliance files. For preparation advice and instructions covering a variety of flash drive types, search the Pulse Community website at <http://kb.pulsesecure.net>.
2. Unpack the Traffic Manager ZIP archive to your workstation.
3. Plug your USB drive into the workstation.

Next, use one of the procedures that follows to complete the process.

To create a boot-able Traffic Manager USB flash drive on a Linux/UNIX-based workstation

1. Locate the USB drive device directory within your filesystem. To list all mounted filesystems and drives, use the `dƒ` command in a console or terminal program. A device directory of `"/dev/sdb"` is typical.

CAUTION

Make sure you have identified the correct device directory. The following steps overwrite everything on this device, and your workstation might become unusable if you select the wrong one.

2. If your USB drive has auto-mounted, type `umount <device_directory>` to unmount it.
3. Navigate to the directory containing your unpacked Traffic Manager archive.
4. Type `zcat USB-boot.img.amd64.gz > <device_directory>` to perform a raw copy of the boot files to the USB drive.
5. Type `mount <device_directory> /mnt` to re-mount the USB drive using `"/mnt"` as the mount point.
6. Type `cp ZeusTM_<Version>_Appliance-x86_64.iso /mnt` to copy the Traffic Manager appliance .iso file onto the USB drive.
7. Do not continue until you are satisfied that the file copy process has completed. For example, if your USB drive has a flashing light to indicate when data is being written to it, wait until this indicates completion.
8. Type `umount <device_directory>` to unmount the USB drive.
9. Type `sync` to force completion of any pending disk writes.

10. Remove your USB drive.

To create a boot-able Traffic Manager USB flash drive on a Windows-based workstation

1. Download the free "Win32DiskImager" tool (<https://sourceforge.net/projects/win32diskimager>).
2. Locate and unzip `USB-boot.img.amd64.gz`.
3. Rename the unzipped file to `USB-boot.img`.
4. Start Win32DiskImager and perform the following actions:
 - a. Set Image file to "USB-boot.img".
 - b. Set Device to your USB drive.
 - c. Click "Write".
 - d. After the image has completed writing, exit the application.
5. Locate and copy `ZeusTM_<Version>_Appliance-x86_64.iso` to the root of the USB drive.
6. Eject and remove the USB drive.

To create a boot-able Traffic Manager USB flash drive on a Macintosh-based workstation

1. Open a Terminal window.
2. Change directory to the location of the unzipped Traffic Manager archive.
3. Run the command `diskutil list` to get the current list of devices and thus to determine the device node assigned to your USB drive (for example, `/dev/disk2`).
4. Run the command `diskutil unmountDisk /dev/diskN` (where `diskN` is replaced with the device identifier from the previous command).
5. Run the command `sudo -s`.
6. Run the command `gunzip -c USB-boot.img.amd64.gz > /dev/rdiskN` to write the extracted contents of the boot image tarball to the USB drive (note the use of `/dev/rdiskN` instead of `/dev/diskN` - in most cases this improves the speed of data transfer).

Note: `gunzip -c` is equivalent to `zcat`. See the respective manpages for more details.

7. Run the command `sync` to force completion of any pending disk writes.
8. Run the command `exit` to exit the superuser shell.
9. Run the command `diskutil eject /dev/diskN` to unmount the USB drive from your filesystem.
10. Close the terminal window.
11. Remove the USB drive, then reinsert it.

12. Copy the disk image file `ZeusTM_<version>_Appliance-x86_64.iso` to the USB drive.
13. After the copy process has completed, eject and remove the USB drive.

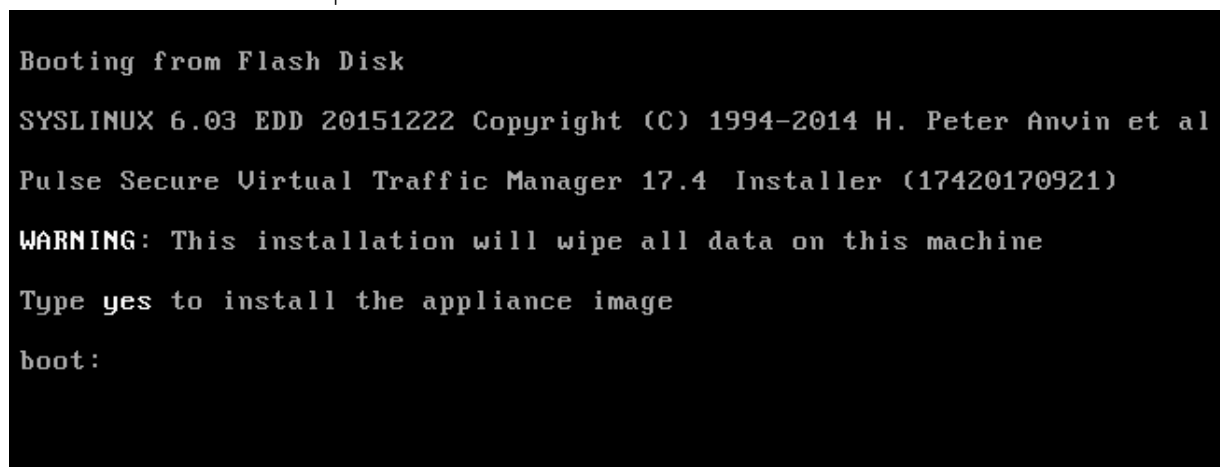
Installing the Traffic Manager From a Disk or USB Flash Drive

Note: This section applies only to installation from a physical medium such as a CD-ROM, DVD-ROM, or USB flash drive. To install the Traffic Manager through a PXE boot environment, see instead [“Installing Through a PXE Boot Environment” on page 19](#).

To install the Traffic Manager software on your appliance, insert the CD-ROM, DVD-ROM, or USB flash drive prepared earlier, and then power on the appliance.

Connect to the appliance console, and wait until the Traffic Manager installer screen appears:

FIGURE 6 The installer splash screen



```
Booting from Flash Disk
SYSLINUX 6.03 EDD 20151222 Copyright (C) 1994-2014 H. Peter Anvin et al
Pulse Secure Virtual Traffic Manager 17.4 Installer (17420170921)
WARNING: This installation will wipe all data on this machine
Type yes to install the appliance image
boot:
```

To continue installing the Traffic Manager, type “yes” at the prompt and press Return.

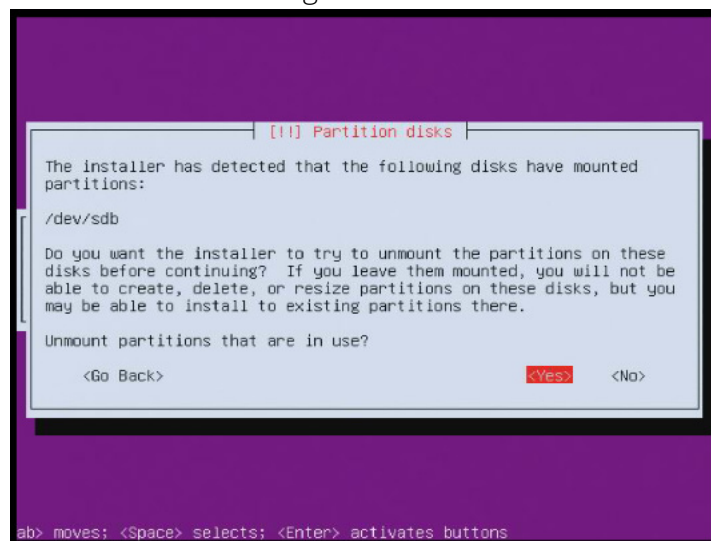
CAUTION

Be aware that this process completely wipes all data from the hard disk in your appliance.

The installer then proceeds to set up the Traffic Manager software on your appliance.

After a short period of time, the installer requests your confirmation to unmount the source drive before it can complete the installation process:

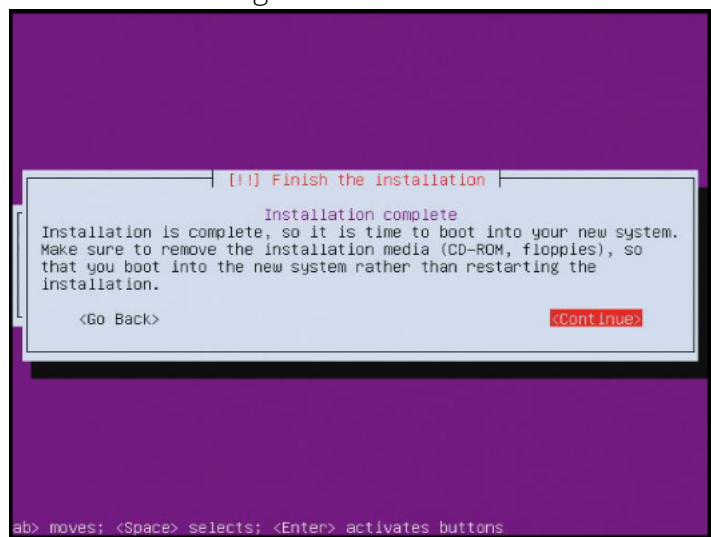
FIGURE 7 Unmounting the installation drive



Select **Yes** and press Return to unmount the installation drive from the system.

Make sure you remove the installation CD-ROM, DVD-ROM, or USB flash drive before continuing.

FIGURE 8 Finishing the installation



To complete the installation and shut down the appliance, select **Continue** and press Return. Your Traffic Manager is now ready for initial configuration.

Installing Through a PXE Boot Environment

Note: This section applies only to installation through PXE. To install the Traffic Manager from a physical medium such as CD-ROM, DVD-ROM, or USB flash drive, see instead [“Installing the Traffic Manager From a Disk or USB Flash Drive” on page 18](#).

This section describes a typical process for setting up a PXE environment with the Traffic Manager installation files.

The minimum required Traffic Manager files for a PXE installation are the following:

- `vmlinux`: The kernel file
- `initrd.gz`: Contains the Traffic Manager ISO image file
- `pxelinux.cfg`: A PXE configuration file

To configure a PXE environment with the Traffic Manager installation files

1. Ensure you have a properly configured PXE environment, with DHCP records pointing to a working TFTP server.
2. Copy `vmlinux` and `initrd.gz` into `<TFTP_path>` on the TFTP server.
3. Copy `pxelinux.cfg` into the directory `<TFTP_path>/pxelinux.cfg/` on the TFTP server.
4. Identify the MAC address of the network interface on the appliance you want PXE to use for installing the Traffic Manager. This interface must be contactable from the TFTP server.
5. Using the format "01-`<appliance_mac_address>`", create a symbolic link in the directory `<TFTP_path>/pxelinux.cfg/` pointing to `<TFTP_path>/pxelinux.cfg/pxelinux.cfg`. For example, the link name might be "01-b6-39-b9-f6-91-2b".
6. Reboot your appliance and check its console output to make sure it is able to load `vmlinux` and `initrd.gz` through PXE.
7. The appliance shuts down after the installer has finished.

CAUTION

To avoid PXE attempting to re-install the Traffic Manager appliance software after the initial installation, you must remove the symbolic link containing the identifying appliance MAC address. Failure to remove this link results in the installer being run multiple times.

Configuring the Traffic Manager Appliance

This chapter describes how to configure a newly installed Traffic Manager appliance. It assumes you have already performed the installation procedure described earlier in this guide.

This chapter also documents further configuration tasks such as reconfiguring, uninstalling, and upgrading the appliance.

It contains the following sections:

• Checking the Initial IP Address	21
• Connecting to the Admin UI	22
• Running the Initial Configuration Wizard	23
• Configuring the Appliance From the Command Line	32
• The Community Edition	37
• NTP Settings	38
• IPMI Management	38
• Upgrading Your Traffic Manager	39
• Monitoring your Hardware	43
• Useful System Information	46

Checking the Initial IP Address

Before you switch on your Traffic Manager appliance, attach your required network connections. To obtain details of the available network ports and their configuration, consult your hardware specifications.

When you first switch on the Traffic Manager appliance after installation, it attempts to obtain initial IPv4 addresses on all connected interfaces using DHCP. The first assigned address is displayed in the appliance console, although you can use any of the assigned IP addresses to initially access the Traffic Manager appliance administrative interface (also known as the Admin UI).

ATTENTION

For appliances with a large number of network interfaces, the process of starting the appliance for the first time can take several minutes while the Traffic Manager attempts to obtain initial IP addresses for each interface. Do not switch off or reboot your appliance during this process.

The Traffic Manager provides the opportunity to configure all connected and unconnected network interfaces to your requirements during initial configuration.

Connect to the appliance console to view the current primary management IP address (shown in the URL for “Administration Interface”).

FIGURE 9 The Traffic Manager appliance console

```
Pulse Secure Virtual Traffic Manager, version 17.4 (patchlevel 17420170921)

Welcome to Pulse Secure Virtual Traffic Manager.

The appliance has now booted. To manage, please use a web browser
to access this URL:

Administration interface: https://10.62.165.97:9090/
Username: admin
SSL(SHA-1) fingerprint: B6:35:68:29:76:56:15:C0:FF:76
69:89:DA:30:7A:DB:02:60:2A:89

SSH(RSA) fingerprint: BF:A7:A6:0F:17:8A:0D:15
FE:BA:00:A0:99:5D:05:BC

SSH(ECDSA) fingerprint: E3:8E:AF:CA:F0:D0:04:01
3B:97:07:CB:25:1F:CB:1A

Support can be obtained from your reseller, or online assistance
is available at https://forums.pulsesecure.net/
```

If the Traffic Manager receives no response to its DHCP requests, the appliance configures itself with the static IP address 192.168.1.101 (on the 192.168.1.0/24 network).

If the appliance could not obtain an address using DHCP and the default 192.168.1.101 address is not appropriate for your network, you can manually set the initial management IP address from the appliance console.

To set the initial IP address from the console

1. Type Alt+F2 to switch to the alternative console display "tty2".
2. Log in as "admin" with the default password of "admin".
3. Run the following command:

```
z-set-initial-address
```

4. Type an IP address and netmask at the prompt.
5. Once the command terminates, type logout to log out of the console.
6. Switch back to "tty1" by typing Alt+F1.
7. Observe that the IP address in the URL for "Administration Interface" has changed to your new IP address.

Connecting to the Admin UI

To connect to the Traffic Manager Admin UI, type the URL displayed on the appliance console into your Web browser.

By default, this URL is "https://<appliance_IP>:9090/", where <appliance_IP> is either:

- The IP address obtained using DHCP
- The IP address specified with the z-set-initial-address command (if used).
- 192.168.1.101

Note: Before you can connect to the Admin UI, your Web browser might report problems with the SSL certificate (either that it cannot trust it, or that the hostname in the certificate does not match the hostname in the URL). These problems can safely be ignored: the certificate is a self-signed certificate, and the hostname in the certificate might not match the URL you have used to access it, particularly if you have used the appliance's IP address in the URL.

Access to the Admin UI is authenticated with a dedicated SSL certificate. The SHA-1 fingerprint of the SSL certificate is displayed on the appliance console. The SHA-1 fingerprint is useful for the following purposes:

- To verify the SSL certificate when connecting with a Web browser for the first time.
- To verify the authenticity of Traffic Manager identities when joining a cluster.

Note: When you set up a new Traffic Manager, Pulse Secure recommends noting the SHA-1 fingerprint. You can also display the fingerprint from the appliance console command line using the following command:

```
$ZEUSHOME/admin/bin/cert -f fingerprint -in $ZEUSHOME/admin/etc/admin.public
```

Running the Initial Configuration Wizard

Before you begin this procedure, make sure you have met all the requirements listed in [“Prerequisites” on page 7](#). Pulse Secure recommends that you read this section fully before continuing.

A newly installed Traffic Manager appliance requires some basic information in order to function. The Traffic Manager gathers this information over a series of steps that form the Initial Configuration wizard.

Type the URL of the Admin UI into your Web browser to view the first step of the wizard:

FIGURE 10 Step 1 of the initial configuration wizard

Initial configuration, step 1 of 9

1. Welcome to your Pulse Secure Virtual Traffic Manager

The following pages will guide you through the process of setting up your Pulse Secure Virtual Traffic Manager Appliance for basic operation. This should only take a few minutes. Some initial networking settings will be required - please contact your support provider if you need any help.

◀ Back Next ▶

Click **Next** to begin the initial configuration of your appliance.

Accept the Terms and Conditions of Sale

Read and accept the Pulse Secure Terms and Conditions of Sale, available from the URL shown:

FIGURE 11 Accept the terms and conditions of sale

Initial configuration, step 2 of 9

2. Pulse Secure Terms and Conditions of Sale

Use of this software is subject to the Pulse Secure Terms and Conditions of Sale.
Please review these terms, published at <https://www.pulsesecure.net/support/eula> before proceeding.

☐ I accept the license agreement

◀ Back Next ▶

Read the agreement fully. If you agree to its terms, click **I accept the license agreement** and then click **Next** to continue. You cannot proceed with the wizard, and thus use the software, if you do not accept the license agreement.

Configuring Networking

Use this page to set your appliance basic network configuration. A summary of the network settings to be applied to your appliance is given at the end of the wizard.

FIGURE 12 Key networking settings when configuring the appliance
Initial configuration, step 3 of 9

3. Networking

Please provide the basic network configuration for this appliance. The configuration may be changed at a later date using the user interface.

The hostname that this appliance will be known by. This can be provided as 'hostname' or 'hostname.domainname'. If the machine is currently assigned a hostname, you can continue to use that. If a hostname is assigned via DHCP, please configure at least one interface to use DHCP.

Hostname:

Each network interface can be configured to either use DHCP or static configuration. Please enter a valid IPv4 address and netmask for at least one network card if all the cards are in static mode. If you want to use an IP address assigned via DHCP as static IP address, please make sure that the DHCP server will not reassign this IP address to any other machine in the network while this machine is in use.

IPv6 addresses can be configured on the *System > Networking* page.

Interface	Mode	IP address	Netmask	Management IP address
enp1s0f0 (unplugged)	<input checked="" type="radio"/> static <input type="radio"/> dhcp	<input type="text"/>	<input type="text"/>	<input type="radio"/>
enp1s0f1 (unplugged)	<input checked="" type="radio"/> static <input type="radio"/> dhcp	<input type="text"/>	<input type="text"/>	<input type="radio"/>
enp4s0f0 (unplugged)	<input checked="" type="radio"/> static <input type="radio"/> dhcp	<input type="text"/>	<input type="text"/>	<input type="radio"/>
enp4s0f1 (unplugged)	<input checked="" type="radio"/> static <input type="radio"/> dhcp	<input type="text"/>	<input type="text"/>	<input type="radio"/>
enp7s0f0	<input checked="" type="radio"/> static <input type="radio"/> dhcp	10.62.142.27	18	<input type="radio"/>
enp7s0f1	<input checked="" type="radio"/> static <input type="radio"/> dhcp	10.62.134.51	18	<input type="radio"/>

The appliance can be configured to only allow management on one specific IP address. This restricts all admin server access, SOAP management, REST API access and other control information to this IP address. This setup is useful if you want to completely separate your public and private networks. If you wish to do this, tick the box below and select an IP address using the Management IP address option buttons above.

☐ Use a single Management IP address

To use trunking, give interfaces the same IP address. All interfaces in a trunk must be connected to the same switch and the switch must have IEEE 802.3ad support enabled.

Note: Unplugged interfaces should not be assigned IP addresses on the management network.

The gateway IP address for this appliance.

Gateway:

◀ Back Next ▶

Configure the following settings:

Setting	Description
Hostname	The hostname of the appliance, in either the simple form or fully qualified form (for example, "vtm1" or "vtm1.mgmt.site.com"). If you intend to create a cluster of Traffic Manager appliances and you are using DNS servers for name resolution, it is important that the name you choose is resolvable from your name servers. Name resolution issues are flagged up later in the wizard.
Mode	<p>The mode of the network interface. Choose one of the following options:</p> <ul style="list-style-type: none"> static: manually configure the IP address and netmask for the interface. dhcp: use DHCP to automatically obtain network settings for the interface. <p>If you intend to use DHCP with your Traffic Manager deployment, Pulse Secure recommends that your network infrastructure is configured with long-life IP reservations for each interface in your system. IP address renewal after lease expiry can cause service interruption and communication issues in your Traffic Manager cluster.</p> <p>If you select DHCP for at least one of your interfaces, the Traffic Manager attempts to automatically obtain a default gateway, name server, and search domain from the DHCP service. If successful, the Traffic Manager uses these settings in place of any values entered during the wizard.</p>

Setting	Description
IP address	The IP address in dotted quad notation (for example, 192.168.1.101) for each interface.
Netmask	The netmask for the associated IP address (for example, 255.255.0.0) for each interface.
Use a single Management IP	<p>Click to restrict management traffic to a single network interface. Then click the Management IP radio button next to the interface you want to use.</p> <p>Management traffic includes access to the Traffic Manager Admin UI, external API access, and internal communications within a Traffic Manager cluster. This address normally resides on a private or dedicated management network.</p> <p>Note: Pulse Secure recommends only choosing to use a management address if you have a dedicated, reliable management network. Each management address is a single point of failure for an entire Traffic Manager cluster. All of your management addresses must always be available.</p> <p>To later modify the management IP address, use the System > Traffic Managers page of the Admin UI. Note that a software restart is required for this procedure.</p>
Gateway	<p>The IP address of the default gateway. This IP address is also used for network connectivity tests by your Traffic Manager appliance, and the gateway machine should respond to "ping" requests for this purpose. If it does not, you must configure your appliance with an additional machine to ping instead. To set a different address to ping, use the Admin UI after your Traffic Manager has been configured.</p> <p>Note: A DHCP service configured to provide a gateway IP address takes precedence over the value manually specified here.</p>

To modify the network settings of a fully configured Traffic Manager, use the **System > Networking** page in the Admin UI. For further details, see the "Configuring System Level Settings" chapter of the *Pulse Secure Virtual Traffic Manager: User's Guide*.

CAUTION

Configuring IP addresses on unplugged interfaces is not recommended. Routing problems could occur if the IP address is located on the same subnet as an IP address on a connected interface. If the IP is on the same subnet as the management port, your appliance might become unreachable.

For optimum performance, Pulse Secure recommends that you use separate interfaces for front and back end traffic. In other words, for traffic between remote clients and the Traffic Manager, and for traffic between the Traffic Manager and the servers that it is load balancing.

You might find the "Network Layouts" chapter of the *Pulse Secure Virtual Traffic Manager: User's Guide* helpful in planning your network. Additionally, the Pulse Community Web site (<http://kb.pulsesecure.net>) contains several articles about configuring your Traffic Manager.

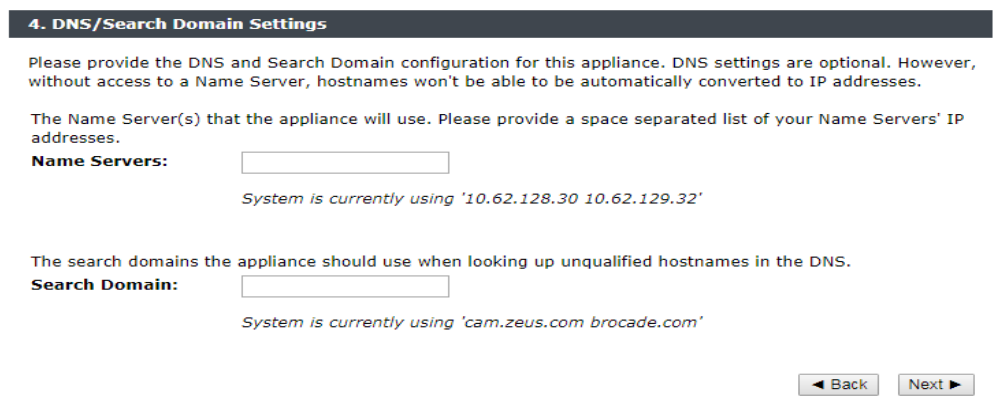
DNS Settings

Use this page to configure the IP addresses of the name servers to use for DNS resolution and the DNS search domains. In each case, enter a single value or space-separated list of values. These settings are optional, but if you configure one or more name servers, you can use your servers' hostnames rather than IP addresses. This can make subsequent configuration tasks easier.

Note: If you selected DHCP for at least one of your network interfaces, the Traffic Manager attempts to automatically obtain a default gateway, name server, and search domain from the DHCP service. If successful, the Traffic Manager uses these settings in place of any values entered during the wizard.

FIGURE 13 Entering Name Servers and the default Search Domains

Initial configuration, step 4 of 9



The screenshot shows a web-based configuration interface for DNS settings. At the top, a dark header bar contains the text "4. DNS/Search Domain Settings". Below this, a paragraph explains that DNS settings are optional but necessary for hostname resolution without a name server. The interface then prompts the user to enter name servers, showing a text input field and a hint that the system is currently using "10.62.128.30 10.62.129.32". Next, it prompts for search domains, showing another text input field and a hint that the system is currently using "cam.zeus.com brocade.com". At the bottom right, there are "Back" and "Next" navigation buttons.

4. DNS/Search Domain Settings

Please provide the DNS and Search Domain configuration for this appliance. DNS settings are optional. However, without access to a Name Server, hostnames won't be able to be automatically converted to IP addresses.

The Name Server(s) that the appliance will use. Please provide a space separated list of your Name Servers' IP addresses.

Name Servers:

System is currently using '10.62.128.30 10.62.129.32'

The search domains the appliance should use when looking up unqualified hostnames in the DNS.

Search Domain:

System is currently using 'cam.zeus.com brocade.com'

[< Back](#) [Next >](#)

The Traffic Manager works correctly without access to external name servers, however you then have to use IP addresses instead of hostnames when setting up pools of servers, or manually enter the hostname to IP mappings, which can be done from the Admin UI (in the "DNS" section of the **System > Networking** page) once you have completed the initial configuration wizard.

Hostname Resolution

The Traffic Manager attempts to resolve your chosen hostname to an IP address using the Name Servers specified (or obtained through DHCP). Where the hostname cannot be resolved, the wizard suggests using one of the IP addresses assigned to your network interfaces instead to identify this Traffic Manager to other cluster members:

FIGURE 14 Configuring the resolvable name

Initial configuration, step 4 of 9

4. DNS/Search Domain Settings

Please provide the DNS and Search Domain configuration for this appliance. DNS settings are optional. However, without access to a Name Server, hostnames won't be able to be automatically converted to IP addresses.

The Name Server(s) that the appliance will use. Please provide a space separated list of your Name Servers' IP addresses.

Name Servers:

The search domains the appliance should use when looking up unqualified hostnames in the DNS.

Search Domain:

'vtm-01' cannot be resolved using '10.62.128.30, 10.62.129.32'. The traffic manager will not work properly if it is identified by a name that is not resolvable. You can choose to identify this traffic manager with an IP address to fix the problem. If you wish to do this, select an IP address from the list below. Please tick the box before continuing.

Select IP Address

Ignore Warning ☐ I understand the traffic manager may not function as expected if I do not use either a resolved hostname/IP address pair or select a specific IP address to use

Select the desired IP address from the drop-down list, or select "None" to force the wizard to set the Traffic Manager name to be the unresolvable hostname. However, you can experience connectivity issues until the hostname successfully resolves to an IP address within your DNS. Read and confirm your acknowledgement of the Ignore Warning message by clicking the checkbox provided.

To change the identifying IP address after the wizard has completed, use the "Replace Traffic Manager Name" section on the **System > Traffic Managers** page of the Admin UI.

Timezone Settings

Use this page to set the time zone for the appliance. This ensures that any logs and diagnostic messages generated by the Traffic Manager have the correct timestamps:

FIGURE 15 Configuring the date and time

Initial configuration, step 5 of 9

5. Date and Time Settings

Please specify the time settings for this appliance.

Time Zone:

Date:

Time: : :

After initial configuration is complete, you can additionally configure your appliance to synchronize with a collection of Network Time Protocol (NTP) servers. For further details, see the *Pulse Secure Virtual Traffic Manager: User's Guide*.

Admin Password

Use this page to set the password for the admin user. This is the master password that is used when configuring the appliance through a Web browser, or when you log in to the Traffic Manager command line using SSH (with the username "admin"):

FIGURE 16 Entering the Admin password

Initial configuration, step 6 of 9

6. Security

A master 'admin' user is created that you can use to log in to the Administration Server and SSH console. Please choose a password for this user.

Enter Password:

Confirm Password:

Pulse Secure vTM Appliances come with a tool pre-installed to help prevent brute-force SSH attacks. This will block remote hosts that have made multiple failed connection attempts for a set time. The specific parameters, including the time spent blocked and the number of permissible failed attempts, can be configured on the Security page when you have completed the initial configuration.

Would you like to enable this tool now?

☐ Enable SSH Intrusion Prevention

[< Back](#) [Next >](#)

The Traffic Manager also contains the option to enable SSH Intrusion Detection to help prevent brute-force SSH attacks on your appliance. Pulse Secure strongly recommends you enable this option.

IPMI Settings

Use this page to optionally configure the IPMI settings for this appliance. Choose whether to disable LAN access to the IPMI module, or whether to set the IPMI user account to the Traffic Manager admin username and password defined in this wizard.

FIGURE 17 Configuring IPMI settings

Initial configuration, step 7 of 9

7. IPMI settings

You can modify the IPMI configuration for this appliance, or leave these settings blank to use the current IPMI configuration.

You may choose to disable IPMI LAN access entirely.

☐ Disable IPMI LAN access

You may create an IPMI 'admin' user to access IPMI remotely using the IPMI LAN channel. The IPMI 'admin' user will be configured with the same password as the traffic manager 'admin' user.

☐ Create an IPMI admin user

[< Back](#) [Next >](#)

Note that if you disable IPMI LAN access, you cannot then set the IPMI user.

License Key

The Traffic Manager requires a license key to operate fully. The feature set and bandwidth limits are determined by the license applied, the details of which can be seen on the **System > Licenses** page of the Admin UI after the Initial Configuration Wizard has completed.

Choose either to upload the license key now, or to upload it later once you have completed the wizard.

FIGURE 18 Uploading a license key file to the Traffic Manager

Initial configuration, step 8 of 9

8. License Key

To use the traffic manager, you will need a valid license key. You have the following licensing options:

- ☒ Upload a license key for this traffic manager
- ☐ Register for flexible licensing using **Services Director**. This option is available for KVM, VMware and EC2 platforms only
- ☐ Skip licensing for now (traffic manager will run as the **Community Edition** until licensing is configured)

Upload a new license key:

Key file: No file chosen

If you need to obtain a license key, please visit the **Pulse Secure vTM website**

This page includes the option to skip uploading a license key and instead run the Traffic Manager software as the Community Edition. For further information, see [“The Community Edition” on page 37](#).

For information about paid licensing, contact Pulse Secure Technical Support.

Summary

Before your settings are applied to the appliance, the initial configuration wizard displays a summary of the settings you have configured.

FIGURE 19 Configuration summary

Initial configuration, step 9 of 9

9. Summary

You have specified the following network settings:

enp7s0f0:	10.62.142.27 (netmask 18)
enp7s0f1:	10.62.134.51 (netmask 18)
Gateway:	10.62.128.1
Hostname:	vtm-01
DNS Servers:	10.62.128.30 10.62.129.32
Search Domain:	cam.zeus.com

Your date and time settings are:

Date:	4 October 2017
Time:	03:55:43
Time Zone:	America/Los_Angeles

Additional settings:

SSH Intrusion Protection:	Enabled
----------------------------------	---------

IPMI settings:

Disable IPMI:	Keep current configuration
Create IPMI admin user:	Yes

License key: No license key provided

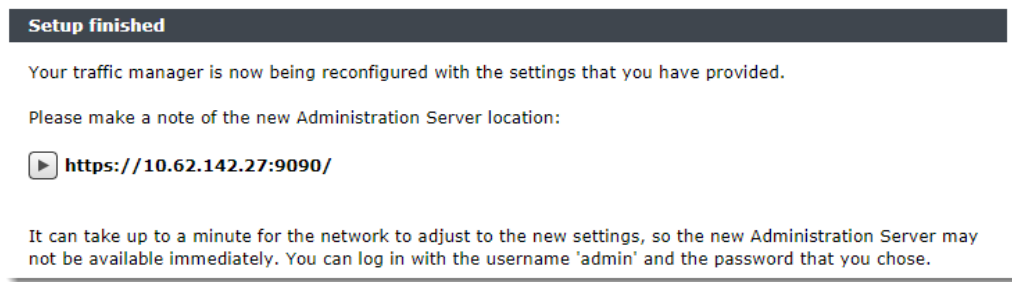
To store these settings, press 'Finish'. To change your settings, press 'Back'.

◀ Back Finish

Review these settings, and in particular the specified network settings, since your appliance might become uncontactable if any of the settings are incorrect. Use the **Back** button to go back through the wizard to make any changes.

To apply your settings, click **Finish**.

FIGURE 20 Configuration is complete

Initial configuration, finished

The Admin UI presents a page with a link to the new URL of the Admin UI. Pulse Secure recommends waiting a short period (typically 10 – 30 seconds) before clicking the link, to allow the appliance time to reconfigure its network interfaces. You might also need to reconfigure your computer's network settings so that it can send packets to the IP address of the appliance management interface.

Click the link to view the login page of the Admin UI. Log in using the username "admin" and the password you chose during the wizard.

Note: If you close the Web page before clicking the link, you can view the Admin UI URL from the appliance console.

Configuring the Appliance From the Command Line

The Traffic Manager supports performing initial configuration through the command line, as an alternative to using the Web-based Initial Configuration Wizard.

To use the Initial Configuration Wizard, see [“Running the Initial Configuration Wizard” on page 23](#).

To start the configuration program, login to the appliance console and type the following command at the prompt:

```
z-initial-config
```

Follow the on-screen instructions to proceed.

```
Pulse Secure Virtual Traffic Manager Installation Program
Copyright (C) 2019, Pulse Secure, LLC. All rights reserved.
```

```
Welcome to your Pulse Secure Virtual Traffic Manager Appliance
```

```
This application will guide you through the process of setting up
your Pulse Secure Virtual Traffic Manager Appliance for basic operation.
This should only take a few minutes. Some initial networking settings
will be required - please contact your support provider if you need any help.
```

```
Press return to continue.
```

```
Press RETURN to start configuring the appliance.
```

 Use of this software is subject to the Pulse Secure Terms and Conditions of Sale.

Please review these terms, published at
<http://http://www.pulsesecure.net/support/eula/> before proceeding.

 Enter 'accept' to accept this license, or press return to abort:

Read and accept the Pulse Secure Terms and Conditions of Sale, available from the URL indicated. If you agree to its terms, type "accept" at the prompt to continue. You cannot proceed with the configuration program, and thus use the software, if you do not accept the terms of the agreement.

Enter the license key file name, or leave blank for the Community Edition.
 Enter 'help' for more information.

License key file:

The Traffic Manager requires a license key to operate fully. The feature set and bandwidth limits are determined by the license applied, the details of which can be seen on the **System > Licenses** page of the Admin UI after you have finished configuring your instance.

Choose either to install the license key now, or to upload it later from the Admin UI. If you choose to leave this entry blank, the system defaults to running as the Community Edition. For further information, see ["The Community Edition" on page 37](#).

For information about paid licensing, contact Pulse Secure Technical Support.

Please provide the basic network configuration for this appliance.
 The configuration may be changed at a later date
 using the administration server.

Please provide the hostname that this appliance will be known by.
 This can be provided as 'hostname' or 'hostname.domainname'.

Hostname:

Type the desired hostname for the appliance, in either the simple form or fully qualified form (for example, "vtm1" or "vtm1.mgmt.site.com"). If you intend to create a cluster of Traffic Manager appliances and you are using DNS servers for name resolution, it is important that the name you choose here is resolvable from your name servers. If you are unable to specify a resolvable hostname, type a suitable text name here and use the IP address identification option offered later in the configuration program.

To use trunking, give interfaces the same IP address.
 All interfaces in a trunk must be connected to the same switch and
 the switch must have IEEE 802.3ad support enabled.

Enter space separated list of interfaces you would like to configure.

Available options: eth0 eth1 eth2 eth3 eth4 eth5. At least one network interface must be selected.

Interfaces:

Type the interface name you want to configure from the list given. For example, "eth0 eth1 eth2 eth3".

Would you like to enable DHCP on eth0? Y/N [N]: y

Would you like to enable DHCP on eth1? Y/N [N]: y

Would you like to enable DHCP on eth2? Y/N [N]: y

Would you like to enable DHCP on eth3? Y/N [N]: n

For each interface, type "Y" to enable DHCP. The Traffic Manager then attempts to obtain address details from the DHCP service in your network. Type "N" to instead specify an IP address and netmask manually.

Enter eth3 IPv4 address or 'use_current' to use currently configured IP which is none.
IP:

Type the IP address for the selected interface in dotted quad notation. For example, "192.168.1.101".

Enter eth3 netmask or 'use_current' to use currently configured netmask which is none.
Netmask:

Type the netmask for the associated IP address. For example, "16" or "255.255.0.0".

The gateway IP address for this appliance:

Type the IP address of the default gateway. This IP address is also used for network connectivity tests by your Traffic Manager, and the gateway machine should respond to "ping" requests for this purpose. If it does not, you must configure your Traffic Manager with an additional machine to ping instead. To set a different address to ping, use the Admin UI after your Traffic Manager has been configured.

Note: If you selected DHCP for at least one of your network interfaces, the Traffic Manager attempts to automatically obtain a default gateway, as well as name servers and a search domain, from the DHCP service. If successful, the Traffic Manager uses these settings in place of any values entered during this step.

Optional: choose management IP, or press return to skip.

Available options: 192.168.1.101

Enter 'help' for more information.

Management IP [none]:

Type the IP address of the interface you want to use as the management IP address, based on the list of IP addresses you configured earlier. Management traffic includes access to the Traffic Manager Admin UI, external API access, and internal communications within a Traffic Manager cluster. This address normally resides on a private or dedicated management network.

CAUTION

Pulse Secure recommends only choosing to use a management address if you have a dedicated, reliable management network. Each management address is a single point of failure for an entire Traffic Manager cluster. All of your management addresses must always be available.

Please provide the DNS and Search Domain configuration for this appliance. DNS settings are optional. However, without access to a Name Server, hostnames won't be able to be automatically converted to IP addresses.

Optional: the Name Server(s) that the appliance will use. Please provide a space separated list of your Name Servers' IP addresses or 'use_current' to use system settings. Currently system is configured to use: '192.168.1.127 192.168.1.128'.

Nameservers:

Type the IP addresses of the external name servers the appliance should use for DNS resolution.

The Traffic Manager works correctly without access to external name servers, however you then have to use IP addresses instead of hostnames when setting up pools of servers. Alternatively, you can manually enter hostname-to-IP address mappings in the Admin UI (in the "DNS" section of the **System > Networking** page) after you have completed the configuration program.

Optional: the default domain name used when looking up unqualified hostnames in the DNS. Please provide a space separated list of search domains.

Search domains:

Type the default search domains the appliance should use when looking up unqualified hostnames.

Optional: do you want to replace the traffic manager name with an IP address? You might want to identify this traffic manager instance using its IP address if its hostname is not resolvable.

Available options: 192.168.1.101.

Enter the value of nameip parameter, or press return to skip,

nameip [none]:

If your designated appliance hostname is not resolvable, you must use the IP address of a configured network interface as the appliance identifier. Type the desired IP address from list of available addresses, or type "None" (the default value) to force the wizard to set the Traffic Manager name to be the unresolvable hostname. Be aware that you might experience connectivity issues until the hostname successfully resolves to an IP address within your DNS.

To change the identifying IP address after you have completed the configuration program, use the "Replace Traffic Manager Name" section on the **System > Traffic Managers** page of the Admin UI.

Please specify the time zone of this appliance, or enter 'help' for the list of available time zones.

Timezone:

Type the time zone you want this appliance to use, or type “help” to first display a list of available time zones.

A master 'admin' user is created that you can use to log in to the Administration Server and SSH console.
Please choose a password for this user:
Re-enter:

Type (and confirm) a password for the Traffic Manager “admin” user. This is the master password that is used when configuring the appliance through a Web browser, or when you log in to the Traffic Manager command line using SSH (with the username “admin”).

Do you want to enable SSH intrusion detection?
Enter 'help' for more information:

Enable SSH intrusion detection? Y/N [N]:

The Traffic Manager also contains the option to enable SSH Intrusion Detection to help prevent brute-force SSH attacks on your appliance. Pulse Secure strongly recommends you enable this option.

Do you want to enable REST API access to the appliance?

Enable REST API? Y/N [N]:

The Traffic Manager provides an industry-standard REST API. Type “Y” to enable or “N” to disable the REST API. For further information, see the *Pulse Secure Virtual Traffic Manager: REST API Guide*.

Do you want to disable IPMI LAN access? Y/N [N]:

Your appliance hardware might come supplied with an Intelligent Platform Management Interface (IPMI) card. Type “Y” if you want to disable LAN access to the IPMI module for increased security.

You may create an IPMI admin user to access IPMI remotely using IPMI LAN channel.

Do you want to create an IPMI admin user? Y/N [N]:

If you choose to retain IPMI LAN access, type “Y” here to set the IPMI administration user credentials to match the Traffic Manager admin user configured earlier.

You have specified the following settings:

No license file:	the traffic manager will run as the Community Edition
Hostname:	vtm-01
DHCP enabled on:	eth0 eth1 eth2
eth3 IP address:	192.168.1.101
eth3 netmask:	16
Gateway:	192.168.1.1


```
Management IP:                (none)
Nameservers:                  192.168.1.30
DNS search domains :          cam.zeus.com
Traffic Manager Name IP:      (none)
Timezone:                     Europe/London
SSH protection enabled:        Yes
REST enabled:                  No
Disable IPMI:                  No
Create IPMI admin user:        Yes
```

You may be logged out when the network configuration changes.

Proceed with configuration? Y/N:

Before you finish, check through the summary to confirm your intended settings. To configure your appliance with these settings, type "Y" at the prompt.

If your configuration is successful, the following message is displayed:

```
Initial configuration completed successfully.
```

Performing an Unattended Configuration

The Traffic Manager provides the ability to automate `z-initial-config` using a *replay file* containing pre-determined responses to the questions asked during the configuration process. To perform an unattended configuration, type the following command at the prompt:

```
z-initial-config --replay-from=<replay filename>
```

To create a suitable replay file, capture your responses using the following command:

```
z-initial-config --record-to=<replay filename>
```

The Community Edition

If your license key expires (or if you actively select it the first time you log in), the Traffic Manager operates in a default state known as the Community Edition. In this state, the Traffic Manager operates normally and with full functionality, but with a bandwidth limit of 10Mb/second and cluster size limit of 4. The Community Edition is designed as a free, production-ready, variant of the Traffic Manager useful for system administrators and application developers wanting to try out advanced vADC (virtual Application Delivery Controller) capabilities in a production environment.

To upgrade the Traffic Manager from the Community Edition to incorporate a full license key, use the **System > Licenses** page of the Admin UI.

Where the Traffic Manager is operating inside a cluster, you must ensure that the proposed license key update is compatible with other fully licensed cluster instances to avoid unintended functionality impairment. Pulse Secure strongly recommends that you seek advice from your support provider before updating license keys in a mixed cluster of Community Edition and fully-licensed Traffic Managers.

NTP Settings

Pulse Secure recommends configuring your Traffic Manager appliance to use the Network Time Protocol (NTP) to synchronize its clock. To do this, visit the **System > Time** page of the Admin UI and set your NTP servers accordingly. By default, the appliance attempts to use the public NTP servers referenced by "pool.ntp.org".

FIGURE 21 Setting NTP servers



▼ NTP Settings

NTP Server	Remove
0.zeus.pool.ntp.org	<input type="checkbox"/>
1.zeus.pool.ntp.org	<input type="checkbox"/>
2.zeus.pool.ntp.org	<input type="checkbox"/>
3.zeus.pool.ntp.org	<input type="checkbox"/>

Add server:

Note: If, for any reason, the time on your appliance differs from the correct time by more than a few minutes, the NTP daemon is not able to adjust the time automatically. To correct the time difference in this case, click **Sync Time Now** on the **System > Time** page.

Traffic Manager appliances also run a local NTP server that listens for NTP (time) requests on all interfaces. You can optionally use the Traffic Manager as a local time source for other servers on your network.

Unexpected time jumps by more than one second trigger a warning message in the Event Log and an SNMP Trap (where configured). Synchronize the time of your appliance if such messages appear.

IPMI Management

Your hardware appliance might contain an Intelligent Platform Management Interface (IPMI) card. IPMI is a remote monitoring and power management interface installed into the appliance that enables remote management, console access, and hardware monitoring functions separate to the Traffic Manager's own administration interfaces.

IPMI is vendor dependent and as such the layout, style, and access mechanism can vary. IPMI is typically accessed through a dedicated Ethernet port in the appliance which, once connected to your network, serves a Web enabled user interface. To gain access to this user interface, type the DHCP-provided IP address into your Web browser (typically over port 80). Use the default credentials provided by your appliance vendor to login to the IPMI user interface.

By default, IPMI is enabled. Use the Traffic Manager initial configuration wizard to disable access to the IPMI Web interface, or to set the IPMI credentials to match the Traffic Manager admin user.

Upgrading Your Traffic Manager

This section contains details of how to upgrade and, if necessary, revert your Traffic Manager appliance version.

Before You Start

These instructions describe the upgrade and reversion functionality available in version 19.1. For upgrades from an earlier release, use the Upgrading instructions in the *Pulse Secure Virtual Traffic Manager: Installation and Getting Started Guide* applicable to the former version. Functionality described here might not be present in earlier releases.

CAUTION

If you are upgrading your Traffic Manager appliance from a version earlier than 9.9, before you can upgrade to the latest release you must first install version 17.2 and import your configuration into it. From there, you can upgrade a further time to any newer supported version. This is due to underlying operating system changes introduced in version 17.2 that affect the upgrade path for older Traffic Manager releases. For information on creating and importing configuration backups, see the *Pulse Secure Virtual Traffic Manager: User's Guide*.

Before you start, make sure you have enough system resources to perform the upgrade:

- **Available memory:** The Traffic Manager requires a minimum of 2GB of RAM to function normally. If the Traffic Manager in question currently has less memory, assign more to the virtual machine before proceeding.
- **Free disk space:** For an upgrade to succeed, a minimum of 700MB must be free on the / (root) partition, and at least 600MB must be free on the /logs partition. To confirm the available free disk space, use the **System > Traffic Managers** page of the Admin UI.

Note: Pulse Secure recommends you backup your configuration as a precaution before upgrading a Traffic Manager. Use the **System > Backup** page to create a snapshot of your current configuration that you can restore later if necessary.

For further information on upgrading and space requirements, see the Pulse Community Web site:

<http://kb.pulsesecure.net>

Upgrading a Cluster of Traffic Managers

Note: This section is applicable to upgrades from version 17.4 and later only.

An upgrade initiated on one cluster member can optionally be rolled out to all other cluster members automatically.

To initiate an upgrade, you must first obtain the software package specific to your appliance platform. For clusters containing two or more Traffic Managers, one of the following scenarios must apply:

- Where a cluster contains Traffic Managers of only one variant (for example, hardware appliances), the uploaded software package is applicable to all Traffic Managers in the cluster. Hence, an upgrade initiated on one Traffic Manager can upgrade all other Traffic Managers in the cluster without further user intervention.

- Where a cluster contains Traffic Managers spanning multiple platforms (for example, a mixed cluster of software instances and appliances), a single uploaded software package applies only to a subset of your cluster. To upgrade all the Traffic Managers in your cluster, obtain software upgrade packages that cover all product variants used. Then, execute an upgrade for each product variant in turn from any cluster member (regardless of that cluster member's host platform).

In the event an upgrade fails on any Traffic Manager in the cluster, the default behavior is to roll-back the upgrade in progress and leave your entire cluster on the previous working software version.

Note: Command line upgrades contain an additional option to not automatically roll-back *all* Traffic Managers in the event of an upgrade failure. You can instead instruct the cluster members which upgraded successfully to remain using the new version, and to only roll-back the Traffic Managers that failed. However, you must not make any configuration changes while your cluster is in a mixed-version state.

Performing an Upgrade

Traffic Manager version upgrades involve installation of a new operating system image and a full system restart. To achieve this, the Traffic Manager maintains a secondary disk partition into which the new system image is installed. The Traffic Manager then applies a copy of the configuration from the previous version to the new version, marks the partition as primary, and restarts the appliance.

The previous partition is not deleted, but instead marked as dormant. This dual-partition mechanism facilitates a roll-back capability, should you need to revert to the previous version (see [“Reverting to an Earlier Version” on page 41](#)).

Note: Traffic Manager releases earlier than 18.2 install maintenance releases inside the same partition as the parent release. For example, 17.2r1 and 17.2r2 are installed into the same partition holding feature release 17.2. From version 18.2 onwards, all Traffic Manager upgrades are treated equally, regardless of the type of change being attempted. In other words, each new feature release or maintenance release is installed to the alternate partition.

Only one previous version can be maintained on the appliance in addition to the current version. If you have previously upgraded to a new version, upgrading a further time overwrites the oldest version held. Take note that this operation is permanent – the overwritten version cannot be retrieved after the upgrade is applied.

Before you begin, obtain the relevant Traffic Manager appliance installation package. Packages are named according to the following convention:

```
ZeusTM_<version>_Appliance-Upgrade-x86_64.tgz
```

Perform the upgrade through the Admin UI or from the appliance console command line.

To upgrade using the Admin UI

1. Log in to the Admin UI, and click **System > Traffic Managers > Upgrade...**
2. Follow the instructions to upload and apply the upgrade package. Where you are upgrading a cluster of Traffic Managers, select which of your other cluster members should receive the upgrade package (subject to the platform rules in [“Upgrading a Cluster of Traffic Managers” on page 39](#)).

To upgrade using the command line

1. Copy the upgrade package to the appliance using the Linux scp command, or Windows based pscp (<http://www.chiark.greenend.org.uk/~sgtatham/putty/>) or WinSCP (<http://winscp.net/eng/index.php>).

CAUTION

Pulse Secure recommends the package is copied to the /logs partition to avoid any disk space issues during the upgrade process.

2. Connect to the appliance command line.
3. To upgrade the current Traffic Manager only, run the command:

```
ZEUSHOME/zxtm/bin/upgrade <package_filename> [<args>]
```

To upgrade a cluster of Traffic Managers, run the command:

```
ZEUSHOME/zxtm/bin/upgrade-cluster --package <package_filename> --mode <mode> [<args>]
```

To see the full list of optional arguments available for each command, add the `--help` argument.

For `upgrade-cluster`, `<mode>` is either "info" (just report on the potential upgrade) or "install" (perform the upgrade). Additionally, upgraded cluster members reboot automatically into the new software version by default. To override this behavior, use the option `--no-restart`.

4. Follow the instructions provided. The upgrade program then copies your configuration data to the new version, but a reboot is required before you can start to use it.

Note: Subsequent configuration changes in the original version are not migrated to the new version.

5. Reboot the appliance when convenient from the Admin UI or command line (type "reboot").

Reverting to an Earlier Version

The upgrade process preserves the previous Traffic Manager version in a separate disk partition to facilitate a reversion capability. To revert to the previous version, use the *Switch Versions* feature in the Admin UI or the *rollback* program from the command line.

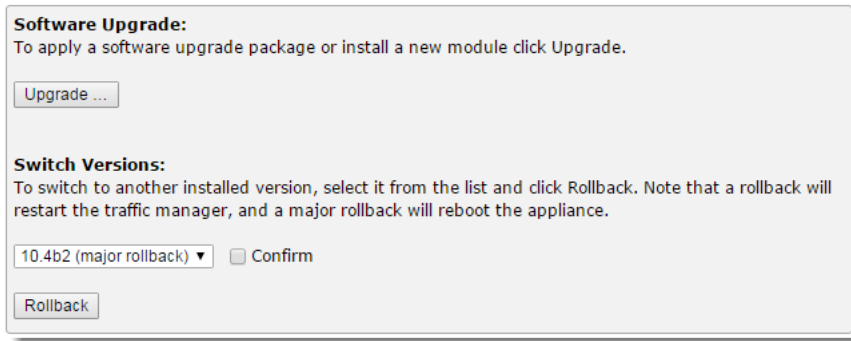
Note: This procedure does not retain any configuration you have made since upgrading to the current version. It is strictly a roll-back procedure that reinstates the selected software version and reinstates the previous configuration settings. Therefore, Pulse Secure strongly recommends that you make a backup copy of your configuration before reverting your appliance.

To revert the Traffic Manager to a previous version using the Admin UI

Note: Traffic Manager versions earlier than 10.4 do not contain a switch feature in the Admin UI. If you roll back to a version earlier than 10.4 and then want to switch again to a different revision, or even to return to the newest software version, you must use the command line "rollback" program until you reach version 10.4 or later.

1. Login to the Admin UI of the Traffic Manager you want to revert.
2. Click **System > Traffic Managers** and locate the “Switch Versions” section:

FIGURE 22 Switching Traffic Manager versions



Note: The Switch Versions section is hidden if there are no applicable versions to revert to.

3. Select a Traffic Manager version to use from the drop-down list.
4. Tick **Confirm** and then click **Rollback** to start the roll back process.

To revert the Traffic Manager to a previous version using the command line

1. Connect to the appliance command line.
2. Ensure you are the root user.
3. Run the command:

```
$ZEUSHOME/zxtm/bin/rollback
```

This starts the rollback program:

```
Rollback
Copyright (C) 2019, Pulse Secure, LLC. All rights reserved.
```

This program allows you to roll back to a previously installed version of the software. Please note that the older version will not gain any of the configuration changes made since upgrading.

Do you want to continue? Y/N [N]:

4. Type **Y** and press Enter to continue. The program lists all versions of the Traffic Manager it can restore:

```
Which version of the Traffic Manager would you like to use?
```

- ```
1) 18.2
2) 18.3 (current version)
```

```
Select a version [2]
```

5. Select the version you want to restore, and press Enter.
6. The Traffic Manager stops the current version and restarts itself with the selected version.

If you need to cancel this process and return to the latest version, repeat the rollback procedure and select the newer version to restore. You do not need to reinstall the latest version of the Traffic Manager to achieve this. The change in version is applied permanently; subsequent appliance reboots continue to use the version you select from the rollback program.

**Note:** For rollbacks to 18.1 or earlier, be aware that if you subsequently decide to roll forward again to version 18.2 or later, the Admin UI “Switch Versions” feature is not supported. Use only the command line rollback program for this purpose.

## Changing Your Traffic Manager Version Manually

If the rollback program is unable to complete a version change, you can perform the operation manually by editing the Traffic Manager “boot menu” from the command line.

**Note:** Due to boot menu updates implemented in version 18.2, this process applies only if you want to switch between Traffic Manager versions from 18.2 onwards. For version changes between version 18.2 (or later) and version 18.1 (or earlier), use only the rollback program. For more information, contact Pulse Secure Technical Support.

To complete a manual version change, perform the following steps:

1. Ensure you have access to the appliance console.
2. Reboot the appliance from the **System > Traffic Managers** page of the Admin UI, or from the console (use the command “reboot”).
3. During the reboot process, press Escape when you see the 5-second countdown on the console.
4. Select the required version from the list provided.

## Monitoring your Hardware

Your Traffic Manager appliance reports its condition through the Admin UI, with warnings and errors reported in the Event Log and Diagnose sections in common with other product variants. To monitor the Traffic Manager’s hardware status, you can additionally use the following appliance-specific Admin UI features.

### Network Interfaces

To view details of the configured network interfaces on your appliance, click **System > Networking > Interfaces**.

**FIGURE 23** Network interfaces configured on this appliance

This section allows you to configure the network settings for this appliance.

| ▼ Interfaces                                                       |       |                                                |                   |              |             |        |              |                                                              |
|--------------------------------------------------------------------|-------|------------------------------------------------|-------------------|--------------|-------------|--------|--------------|--------------------------------------------------------------|
| Link information, eg. speed, type, etc might not show immediately. |       |                                                |                   |              |             |        |              |                                                              |
| Card                                                               | Port  | IP                                             | MAC               | Status       | Speed(Mbps) | Duplex | Type         | Error                                                        |
| First<br>[10G]<br>{01:00}                                          | eth0  | 10.62.142.26/18<br>fe80::1618:77ff:fe29:442b64 | 14:18:77:29:44:2F | running      | 1000        | Full   | Twisted Pair |                                                              |
|                                                                    | eth1  | 10.63.167.60/18                                | 14:18:77:29:44:31 | disconnected | -           | -      | Twisted Pair | No network cable detected on eth1. Please check your cabling |
|                                                                    | eth2  | -                                              | -                 | no IP        | -           | -      | -            |                                                              |
|                                                                    | eth3  | -                                              | -                 | no IP        | -           | -      | -            |                                                              |
| Second<br>[10G]<br>{03:00}                                         | eth4  | 10.63.167.52/18<br>fe80::a236:9fff:fe7f:72fc64 | A0:36:9F:7F:72:FC | running      | 1000        | Full   | Twisted Pair |                                                              |
|                                                                    | eth5  | 10.63.167.58/18                                | A0:36:9F:7F:72:FE | down         | -           | -      | -            |                                                              |
| Third<br>[10G]<br>{04:00}                                          | eth6  | -                                              | -                 | no IP        | -           | -      | -            |                                                              |
|                                                                    | eth7  | -                                              | -                 | no IP        | -           | -      | -            |                                                              |
| Fourth<br>[10G]<br>{05:00}                                         | eth8  | -                                              | -                 | no IP        | -           | -      | -            |                                                              |
|                                                                    | eth9  | -                                              | -                 | no IP        | -           | -      | -            |                                                              |
| Last<br>[10G]<br>{82:00}                                           | eth10 | -                                              | -                 | no IP        | -           | -      | -            |                                                              |
|                                                                    | eth11 | -                                              | -                 | no IP        | -           | -      | -            |                                                              |

| ▼ Card Labels           |                                     |
|-------------------------|-------------------------------------|
| Network card labelling. |                                     |
| Card PCI ID             | Label                               |
| 01:00                   | <input type="text" value="First"/>  |
| 03:00                   | <input type="text" value="Second"/> |
| 04:00                   | <input type="text" value="Third"/>  |
| 05:00                   | <input type="text" value="Fourth"/> |
| 82:00                   | <input type="text" value="Last"/>   |

The table shows each network card attached to the appliance, with each network port on the card shown individually. The card is identified by its PCI ID and bandwidth class.

For each network port, the following parameters are shown:

- **IP:** The IP address assigned to this port.
- **MAC:** The hardware MAC address belonging to this port.
- **Status:** A short descriptive status for this port: "running", "down", "disconnected", and "no IP".
- **Speed:** The speed, in Mbps, this connection is operating at.
- **Duplex:** The duplex setting for this connection, either "Full" or "Half".
- **Type:** The physical medium for this connection.
- **Error:** Any current error state information.

To aid identification of network cards, the Traffic Manager provides the ability to label individual cards with a suitable name. Use the Card Labels section to assign names to your cards based on the PCI ID.



## Appliance Hardware Status Reporting

The Traffic Manager is capable of displaying the hardware status reported by an appliance IPMI management interface. To observe a basic health indicator for each appliance in your cluster, click **System > Traffic Managers**. Observe the “Hardware Status” indicator against each Traffic Manager, as shown here:

FIGURE 24 Traffic Manager appliance health indicator

Hardware Status 

To view the full IPMI output for the current Traffic Manager appliance, click **Diagnose > Hardware**.

FIGURE 25 Your appliance hardware status report

**Hardware Status**

The hardware health status of traffic manager 'leela'

The health status of this appliance.

IPMI readings

| Type | Entity       | Item                  | Reading              | Text |
|------|--------------|-----------------------|----------------------|------|
| AMP  | Power Supply | [10.1] Current 1      | 0.400 (+/- 0) Amps   | OK   |
|      | Power Supply | [10.2] Current 2      | 0.200 (+/- 0) Amps   | OK   |
|      | System Board | [7.1] Pwr Consumption | 112 (+/- 0) Watts    | OK   |
| FAN  | System Board | [7.1] Fan Redundancy  | 0h                   | OK   |
|      | System Board | [7.1] Fan1            | 3960 (+/- 120) RPM   | OK   |
|      | System Board | [7.1] Fan2            | 3960 (+/- 120) RPM   | OK   |
|      | System Board | [7.1] Fan3            | 3960 (+/- 120) RPM   | OK   |
|      | System Board | [7.1] Fan4            | 3840 (+/- 120) RPM   | OK   |
|      | System Board | [7.1] Fan5            | 3960 (+/- 120) RPM   | OK   |
|      | System Board | [7.1] Fan6            | 3960 (+/- 120) RPM   | OK   |
| PSU  | System Board | [7.1] PS Redundancy   | 0h                   | OK   |
| TEMP | Processor    | [3.1] Temp            | 43 (+/- 1) degrees C | OK   |
|      | Processor    | [3.2] Temp            | 44 (+/- 1) degrees C | OK   |
|      | System Board | [7.1] Exhaust Temp    | 32 (+/- 1) degrees C | OK   |
|      | System Board | [7.1] Inlet Temp      | 25 (+/- 1) degrees C | OK   |
| VCC  | Power Supply | [10.1] Voltage 1      | 238 (+/- 0) Volts    | OK   |
|      | Power Supply | [10.2] Voltage 2      | 238 (+/- 0) Volts    | OK   |
|      | Processor    | [3.1] FVR PG          | 0h                   | OK   |
|      | Processor    | [3.1] M01 VDDQ PG     | 0h                   | OK   |
|      | Processor    | [3.1] M01 VPP PG      | 0h                   | OK   |
|      | Processor    | [3.1] M01 VTT PG      | 0h                   | OK   |
|      | Processor    | [3.1] M23 VDDQ PG     | 0h                   | OK   |

The Hardware Status page provides a list of hardware devices present in the appliance. Each device section contains a list of parameters along with the current reading and overall health state of that parameter.

Hardware status events and alarms are reported and logged in the Traffic Manager event log, with a visual indication of serious errors shown in the Admin UI.

This information is also present in a Technical Support Report (TSR).

## Useful System Information

### SSH

You normally administer the appliance through the Web-based Admin UI. However, you can also access the Traffic Manager through the console (command line) to access files stored on the system. To do this, either connect directly to the appliance (type ALT+F2 to access a login prompt), or use an SSH client to log in to the appliance remotely.

### Freeing Up Disk Space

Over time, your appliance can run low on disk space. For example, your system logs can become large if you have configured your Traffic Manager to produce detailed request log information.

The Traffic Manager warns you if disk space is running low through the **Event Log** and **Diagnose > Cluster Diagnosis** page. You can also view disk space usage at any time through the **System > Traffic Managers** page.

To free up disk space, click **Free up some disk space** from the Wizards: drop-down menu in the main tool bar. You can also run the wizard from the "Free Disk Space" link on the **System > Traffic Managers** page at any time, and from the **Diagnose > Cluster Diagnosis** page when a low disk space warning appears.

#### CAUTION

This operation is irreversible. Make sure you have created a backup of any files you need to keep before running the wizard. Note also that any "Technical Support Reports" you create afterwards contain only those logs generated since the wizard was run.

### Changing the Traffic Manager Name

Each Traffic Manager in your cluster uses a DNS resolvable hostname with which it can be identified and contacted by each other cluster member. If you are unable to use a resolvable name, you can instead use a contactable IP address. You set the hostname or IP address during the initial configuration of your Traffic Manager. See ["Running the Initial Configuration Wizard" on page 23](#).

To change the designated Traffic Manager hostname after you have completed the initial configuration, or to instead switch to using an IP address, run the Pulse Secure Configuration Program from the appliance console:

```
$ZEUSHOME/zxtm/configure
```

This program displays the following options:

```
Pulse Secure Configuration Program
Copyright (C) 2019, Pulse Secure, LLC. All rights reserved.
```

```
This program will perform the initial configuration of the
Traffic Manager.
```

```
Initial configuration has already been performed on this Traffic Manager installation.
```

1. Quit (default)
2. Perform the post-install configuration again

- 3. Clear all configuration
- H. Help

Choose option [1]:

Select **Perform the post-install configuration again** and then choose which action you want to perform from the further options provided:

Each traffic manager in your cluster must have a unique name, resolvable by each member of the cluster.

This traffic manager is currently called 'vtm1.example.com'.  
Would you like to

- 1. Keep the current traffic manager name (default)
- 2. Specify a new resolvable hostname
- 3. Use an IP address instead of a hostname

Choose option [1]:

You can also switch to using an IP address from the Replace Traffic Manager Name section on the **System > Traffic Managers** page of the Admin UI. You cannot, however, switch back to using a resolvable name from this page. Instead, rerun `$ZEUSHOME/zxtm/configure` as previously described.

## Resetting to Factory Defaults

If you would like to completely reset the appliance back to its unconfigured state, use the following command. Be aware that this command completely erases your existing configuration, including the network configuration and any additional software modules you might have installed (such as the Pulse Secure Virtual Web Application Firewall).

```
z-reset-to-factory-defaults
```

After the appliance has been reset, reconfigure the appliance using the instructions in [“Running the Initial Configuration Wizard” on page 23](#) or [“Configuring the Appliance From the Command Line” on page 32](#).

## Resetting the Admin Password

If you forget the admin user password, you can reset it from the appliance console.

### To reset the admin user password

- 1. Connect to the appliance console.
- 2. Reboot the appliance, “forcefully” if required.
- 3. During startup, press Escape when you see the 5-second countdown
- 4. Choose *Recovery mode* from the boot menu and press Enter.
- 5. At the prompt, enter the following command:

```
z-reset-password
```

- 6. Follow the instructions to change the password (enter a new admin password twice as directed).

7. Type the following command to reboot the appliance:

```
reboot
```

8. After the appliance reboots, log in to the Admin UI using the username “admin” and your new admin password.

**Note:** If your appliance is a member of a cluster, the Diagnose page of the Admin UI might report a configuration conflict. Use this page to push the new admin password to the other Traffic Managers in the cluster.

# Basic Configuration Information

The Traffic Manager receives traffic from the Internet, makes decisions based on the traffic source, destination and content, and chooses a group of back-end servers to handle the traffic. Traffic is balanced across this group according to the network resources.

In a traffic management system, you configure a virtual server object to manage connections from remote clients, and configure a pool object to manage connections to your local servers.

Once you have installed and configured your Traffic Manager system on the network, you can access the Admin UI to set up a pool and a virtual server.

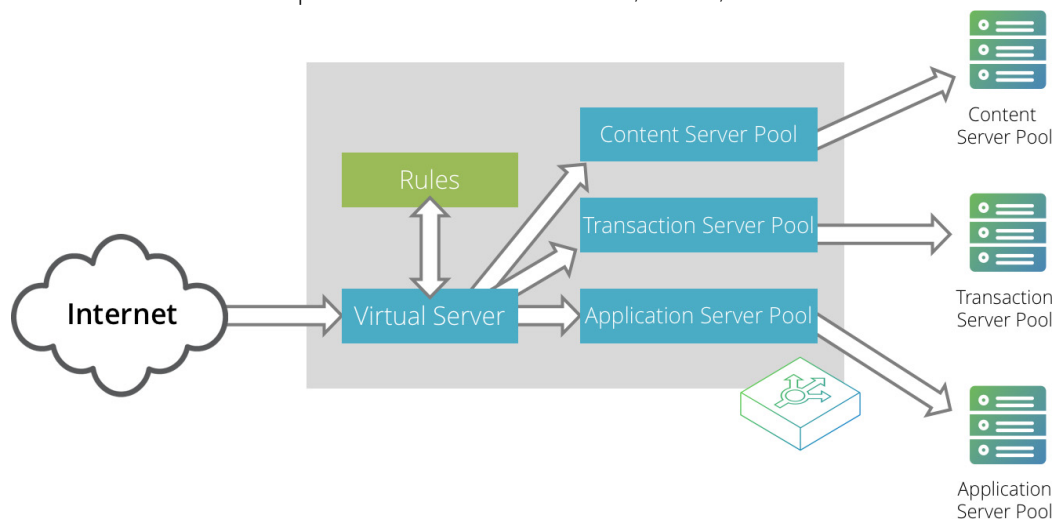
This chapter describes the basic Traffic Manager configuration and contains the following sections:

- [Virtual Servers, Pools, and Rules](#) ..... 49
- [Managing Your First Service](#) ..... 50
- [Creating a Traffic Manager Cluster](#) ..... 51

## Virtual Servers, Pools, and Rules

The following figure illustrates the relationship between virtual servers, rules, and pools.

FIGURE 26 Relationship Between Virtual Servers, Rules, and Pools



A pool is a collection of nodes. Each node corresponds to a back-end server and port, such as `server1.mysite.com:80`. You can set up several pools with nodes in common.

A virtual server listens for and processes incoming network traffic, and typically handles all of the traffic for a certain protocol (for example, HTTP or FTP). In contrast, a virtual server in a Web server typically serves only one website. The Traffic Manager sends traffic to a default pool, although the virtual server first runs through any rules that you have associated with it. Each of these might select a different pool to use depending on the conditions satisfied within the rule. Traffic is balanced across the nodes in the selected pool.

A request rule can do much more than just select a pool. It can read an entire request, inspect and rewrite it, and control how the other traffic management features on the Traffic Manager are used to process that particular request. It can select the pool based on the contents of the request.

Response rules process responses. They can inspect and rewrite responses, control how the response is processed, or even instruct the Traffic Manager to try the request again against a different pool or node.

## Managing Your First Service

### To manage your first service

1. Browse to the Admin UI and log in with the username “admin” and your password.
2. The Admin UI home page shows that you have not yet created any pools or virtual servers. From the Wizards drop-down menu, choose Manage a New Service to begin using the wizard.
3. Specify a name that identifies the virtual server, and choose a protocol and port (for example, HTTP and default port 80).
4. Click **Next** to continue.
5. Create a list of backend nodes, which form the default pool for the virtual server.

The nodes are identified by hostname and port. You can modify these later from the **Pools > Edit** page. Make sure that you can serve content directly from the hostname/port combinations you specify here.

6. Click **Next** to display the setting summary page.
7. Review the settings that you have chosen. Click **Back** to make changes or click Finish to set up the service.
8. Test your Traffic Manager setup by browsing to it, using the port you set up for your new service. Use one of the following paths:

```
http://<machine_name>:<port>
```

or

```
http://<ip_address>:<port>
```

9. (Optional) You can observe the traffic handled by the Traffic Manager to verify that the traffic was processed and routed correctly. To do so, click Activity in the Admin UI and select the Connections tab. This page lists connections that the Traffic Manager has recently managed. If the list is empty, reload pages from the Website that the Traffic Manager is managing and check that the connections list is modified accordingly.

You can also use the Current Activity graph to watch the activity of the Traffic Manager in real-time.

## Creating a Traffic Manager Cluster

If you are configuring two or more Traffic Managers in a cluster, first perform the initial configuration process for each instance. Then, before making any other changes, join the instances together to form a cluster using one of the following procedures:

- If you are creating a new Traffic Manager cluster, choose one Traffic Manager as the first cluster member. Log in to the Admin UI on each of the other instances, and use the Join a cluster wizard to join each of these with the first Traffic Manager.
- If you want to join an existing Traffic Manager cluster, log in to the Admin UI on each of the new instances and use the Join a cluster wizard to join each of these to the existing cluster.

**Note:** In a Traffic Manager cluster, all systems are considered equal. You can access the Admin UI on any of the Traffic Managers. Any configuration changes you make are automatically replicated across the cluster. All Traffic Managers function together to provide fault tolerance and simplified management.

### To join a cluster

1. Log in to the Admin UI on one of your Traffic Managers and select Join a cluster from the Wizards drop down box manu in the tool bar.
2. Step 1 of the Join a cluster wizard requires you to choose whether to scan for existing clusters or manually specify the cluster details.

**FIGURE 27** Getting Started with the cluster joining wizard

#### Cluster Joining wizard, step 1 of 5

**1. Getting Started**

This wizard joins your current traffic manager to an existing cluster so that it can share the cluster's configuration and traffic.

Joining a new cluster will remove this traffic manager from its current cluster.

Would you like to select an existing cluster from a list of available clusters on your network, or enter the Administration Server address and port of a specific traffic manager to join?

☒ Select existing cluster

☐ Manually specify host/port

Cancel < Back Next >

To instruct the Traffic Manager to automatically scan the network for contactable Traffic Managers, click "Select existing cluster". Alternatively, to enter a specific hostname and port you want to join, click "Manually specify host/port".

3. Click **Next** to continue.
4. Step 2 reflects the choice you make in step 1. If you clicked "Select existing cluster", the Traffic Manager presents a list of discovered Traffic Manager instances and clusters.

**FIGURE 28** Select an existing Traffic Manager cluster to join  
**Cluster Joining wizard, step 2 of 5**

**2. Cluster selection**

Please select the cluster you wish to join:

- ☐ Cluster 1: aknox-02.cam.zeus.com:9092
- ☐ Cluster 2: apritchard-12.cam.zeus.com:9090
- ☐ Cluster 3: coeus.cam.zeus.com:9090
- ☐ Cluster 4: fry:9090
- ☐ Cluster 5: rkistruck-2b:9090 rkistruck-2d.cam.zeus.com:9090
- ☐ Cluster 6: jmoore-01:9090
- ☐ Cluster 7: jsteele-00.cam.zeus.com:9090 jsteele-04.cam.zeus.com:9090

Cancel < Back Next >

If you clicked "Manually specify host/port", enter your hostname and port number in the boxes provided.

5. Click **Next** to continue.
6. To connect to the specified instance or cluster, first verify the identity of the Traffic Managers within the cluster, and provide the administration credentials used by the cluster.

**FIGURE 29** Authenticating the Cluster

**3. Authentication**

The admin server you are clustering with is using an SSL certificate with the following SHA-1 fingerprint:

10.62.165.97:9090 ☒ B6:35:68:29:76:56:15:C0:FF:76:69:89:DA:30:7A:DB:02:60:2A:89  
 ► Unfold to view full certificate details ...

Please check the box beside the fingerprint above to indicate that you have verified it or that you trust the network between it and this system.

If you do not already have this fingerprint on record you can get it by logging into the target admin server and visiting the **System > Security** page. (Refer to the product documentation for further information on cluster security.)

Enter the username and password of a user in the target cluster with permission to add and remove traffic managers.

Username: admin

Password: .....

Cancel < Back Next >

Check the displayed SHA-1 fingerprint against the fingerprint shown in the target Traffic Manager's Admin UI, in **System > Security**.

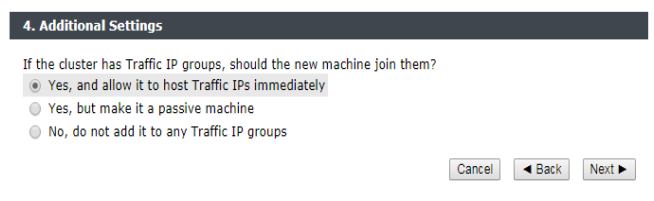
Tick the checkbox next to each Traffic Manager hostname to confirm you trust its identity, and then enter the cluster admin username and password. Click Next to continue.

7. If the cluster already has one or more Traffic IP groups configured, you can elect to add the new Traffic Manager to these Traffic IP groups so that it starts handling traffic immediately.



**FIGURE 30** Assigning Traffic IP Group Membership

Cluster Joining wizard, step 4 of 5



**4. Additional Settings**

If the cluster has Traffic IP groups, should the new machine join them?

☒ Yes, and allow it to host Traffic IPs immediately

☐ Yes, but make it a passive machine

☐ No, do not add it to any Traffic IP groups

Cancel Back Next

To add the Traffic Manager to existing Traffic IP groups, click "Yes, and allow it to host Traffic IPs immediately". However, this can result in a number of connections being dropped at the instant the new Traffic Manager is added to the Traffic IP group, because allocations of traffic need to be transferred to the new Traffic Manager.

To avoid this situation, click "Yes, but make it a passive machine" to add the new Traffic Manager as a "passive" member of the Traffic IP group. This way, it does not accept any traffic until another member of the group fails.

To leave the new Traffic Manager out of all existing Traffic IP groups, click "No, do not add it to any Traffic IP groups".

Click Next to continue.

8. Check your settings in the summary step and then click Finish to join the cluster.

Provided the other Traffic Manager instances can be contacted, the Traffic Manager software reconfigures itself and presents a new home page showing all connected Traffic Manager instances in the Traffic Managers list.

To add further Traffic Managers to the cluster, run the Join a cluster wizard on the Admin UI of each Traffic Manager instance you want to add.

**Note:** When you join a Traffic Manager to an existing cluster, it takes on the entire configuration that the cluster is using, including the administration password you specify during the wizard.

Clusters consisting of Traffic Managers on different platforms is possible, although you might find that product capabilities present on one of your cluster members are not present on others. For example, Networking and Time settings are configurable only for certain Traffic Manager variants.



# Open Source Software Notice

---

This product includes software originating from third parties that are subject to one or more of the following:

- The GNU Library/Lesser General Public License (LGPL)
- The GNU General Public License (GPL)
- The Berkeley Software Distribution (BSD) License
- The OSI Artistic License
- Various GPL/BSD-like Distribution Licenses

All applicable third party software packages and accompanying licenses are listed in the *Pulse Secure Virtual Traffic Manager: User's Guide* and in the *Pulse Secure Virtual Traffic Manager: Appliance License Acknowledgements*, available from the Traffic Manager product pages on the Pulse Secure Web site.

Pulse Secure, LLC offers to provide a complete copy of the source code for the software under said licenses on a CD-ROM, for a charge covering the cost of performing such distribution, such as the cost of media, shipping, and handling, upon written request to Pulse Secure, LLC at the following address:

Source Code Requests VTM-APPLIANCE (GPL)

Pulse Secure, LLC

The Jeffreys Building

Cowley Road

Cambridge

CB4 0DS

United Kingdom

This offer is valid for a period of three (3) years from the date of the distribution of this product by Pulse Secure, LLC. Please refer to the exact terms of the appropriate license regarding your rights.

