riverbed

White Paper

Deploying SteelHead® VCX for Orange FE Workloads

A guide to the preparation and configuration of Riverbed® SteelHead appliances in Orange Flexible Engine.

May 2021

Version 1.0

Table of Contents

1 Preface

Welcome to the Deploying SteelHead VCX for Orange Flexible Engine (FE) Workloads solution guide.

This preface provides an overview of the information provided in this guide and contact information. This preface includes the following sections:

- ✓ About This Guide
- ✓ Target Audience
- ✓ Contacting Riverbed

1.1 About this guide

This guide provides instructions for deploying the Cloud SteelHead CX within Orange FE , peering with another SteelHead, and configuring in-path rules to for optimization. In addition, configuration best practices are provided as well as information on which Orange FE workloads can be optimized.

Use this guide along with the following documents (available in the Riverbed support site):

- ✓ SteelHead User Guide
- ✓ Troubleshooting Riverbed Steelhead WAN Optimizers
- ✓ Steelhead Appliance Deployment Guide — Protocols (Chapter 4, “HTTP Optimization,” and Chapter 11, “SSL Deployments”)
- ✓ SteelHead Deployment Guide

1.2 Target Audience

This guide is written for IT professionals responsible for deploying an optimization solution for Orange FE workloads using the SteelHead VCX virtual appliance. This guide assumes you are familiar with the following items:

- ✓ Networking technology and concepts such as HTTP, SSL, and basic IP routing
- ✓ SteelHead administration console (for details, see the SteelHead User Guide)
- ✓ Orange FE infrastructure services (hosted virtual machines)
- ✓ Orange FE networking and architecture (see: https://docs.prod-cloud-ocb.orange-business.com/en-us/vpc/index.html)

For more details on the SteelHead appliance family, see
https://www.riverbed.com/products/steelhead/application-accelerator.html

1.3 Contacting Riverbed

This section describes how to contact departments within Riverbed.

Internet

You can learn about Riverbed products through the company website: https://www.riverbed.com.

Sales and Marketing

For details see https://www.riverbed.com/how-to-buy/.

Technical Support

If you have problems installing, using, or replacing Riverbed products, contact Riverbed Support or your channel partner who provides support. To contact Riverbed Support, open a trouble ticket by calling 1-888-RVBD-TAC (1-888-782-3822) in the United States and Canada or +1-415-247-7381 outside the United States.

You can also go to : https://support.riverbed.com.

2 Solution Overview

Riverbed SteelHead products are unmatched in the WAN optimization industry. With the release of the Cloud SteelHead VCX in Orange FE, the same technology famous for reducing bandwidth and latency and improving application performance for LAN workloads can be applied to Orange FE workloads.

This chapter includes the following sections:

- ✓ Optimizing Orange FE Workloads
- ✓ Basic Architecture
- ✓ Deployment Overview

2.1 Optimizing Orange FE Workloads

Orange FE cloud includes storage, directory, compute, infrastructure, database, workflow, networking, machine learning, media, and other services. Many companies are moving content, database, and applications such as Microsoft® SharePoint® and custom web applications to Orange FE.

Moving network workloads to cloud services has significant impacts on network architecture and capacity. Companies planning to implement cloud services often already have congested Internet connections or MPLS connections. In addition, network connections to cloud services have more latency than on-premises LANs. As a result, application performance can suffer resulting in lower end-user satisfaction and productivity. Workloads that move large amounts of data take more time due to these new latencies and constrained bandwidth. A SteelHead solution directly addresses each of these problems by significantly increasing the amount of content you can carry on your existing Internet connection while decreasing latency and improving application performance.

A SteelHead can optimize many kinds of traffic including SMB, CIFS, MAPI, HTTP, and HTTPS. SteelHead optimization of HTTP works without any specialized configuration requirements.

As a result, you can optimize FE workloads including (but not limited to): hosted websites and servers, Microsoft® SharePoint®, file and data transfer to FE Storage and FE Site Replication. By adding the proper certificates to the SteelHead CX, HTTPS workloads can also be optimized while still providing end-to-end encryption.

The SteelHead CX series of SteelHeads use the proprietary Riverbed Optimization System (RiOS®) to optimize FE workloads in three ways:

- ✓ Data streamlining (data deduplication)
- ✓ Improved application performance
- ✓ TCP optimizations (transport streamlining)

2.1.1 Data Streamlining (Data Deduplication)

In addition to traditional data reduction techniques like data compression, RiOS also uses a Riverbed proprietary algorithm called Scalable Data Referencing (SDR). RiOS SDR breaks up TCP data streams into unique data chunks that are stored on the hard disks (RiOS data store) of the virtual or physical device running RiOS. Each data chunk is assigned a unique integer label (reference) before it is sent to a peer RiOS device across the WAN. When the same byte sequence occurs in future transmissions from clients or servers, the reference is sent across the WAN instead of the raw data chunk. The peer RiOS device (a SteelHead) uses this reference to find the original data chunk on its RiOS data store and reconstruct the original TCP data stream. This mechanism allows significant bandwidth reduction on second and subsequent downloads or uploads of content. Bandwidth reductions of 90 percent or greater are common in this context.

As SDR identifies content based on the binary content of the data stream, a SteelHead has much better performance than a traditional file cache. If you rename a file and upload it to an optimized target, the bandwidth reduction will be very high when using a SteelHead solution, while a traditional file cache will provide no benefit. Additionally, you will see significant optimization by copying two similar files.

2.1.2 Improved Application Performance

RiOS has built-in optimizations for many applications including HTTP and Microsoft® SharePoint®. These optimizations reduce round trips, which result in a faster user experience. Coupled with data deduplication, end users often experience significantly improved response times.

2.1.3 TCP Optimizations (Transport Streamlining)

Transport streamlining uses a set of standards-based and proprietary techniques to optimize TCP traffic between SteelHead appliances. Without proper tuning, a TCP connection might never be able to fill the available bandwidth between two locations. You must consider the TCP window sizes used during the life span of a connection. If the TCP window size is not large enough, then the sender cannot consume the available bandwidth. You must also consider packet loss due to congestion or link quality. Using SteelHeads to optimize traffic to and from FE, much of the manual analysis, research, and tuning necessary to achieve optimal performance are automated as the SteelHeads quickly negotiate the optimizations needed.
For more details, refer to the Steelhead Deployment Guide.

2.2 Basic Architecture

The SteelHead CX runs as a virtual machine hosted in FE infrastructure services. Figure 1 - shows the most basic setup possible. For optimization of Orange FE workloads, an on-premises SteelHead is peered with the SteelHead instance deployed in Orange FE. The on-premises SteelHead uses a set of rules that identify which network traffic to optimize and what SteelHead to use to achieve that optimization.

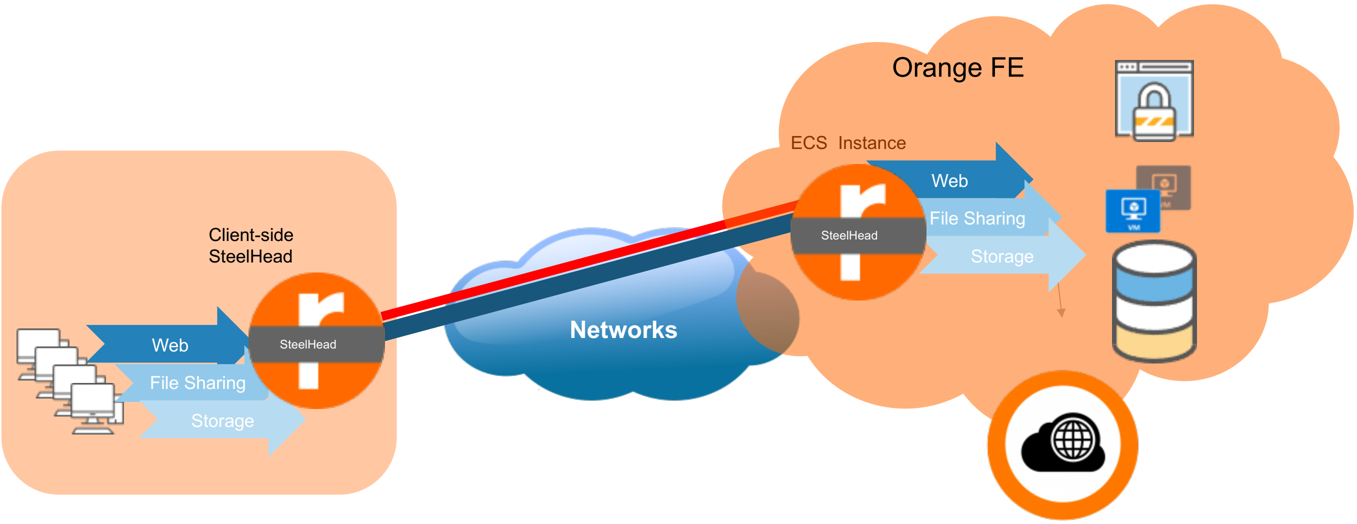


Figure 1 - Basic Architecture

2.3 Deployment Overview

Deployment of a solution to optimize an Orange FE workload with a SteelHead VCX involves several tasks.

- ✓ Deploy the SteelHead VCX to FE
- ✓ Licensing and configuration of the SteelHead VCX
- ✓ Establishing connectivity to and from the your FE SteelHead
- ✓ Configuring an on-premises SteelHead to create an optimized path to FE
- ✓ Configuring Additional Protocoles optimization and SSL if required (see SteelHead Deployment Guide – Protocols for details)

Basic Requirements for Deploying the SteelHead VCX to Orange FE

Items	Description
Orange FE account	The SteelHead VCX runs as a virtual machine in Orange FE. The data and OS disks for the SteelHead virtual machine are hosted in ESM in the FE same region as the SteelHead VCX. You will need login credentials to the FE account where the SteelHead CX can be deployed.
SteelHead CX	The SteelHead CX can be installed from a downloadable package from Riverbed.com/Support or from the Flexible Engine Appliance Catalog
License to activate the SteelHead CX	When you obtain a trial, or purchase the SteelHead CX, You will have the model number and one time activation key in order to deploy and enable optimization for the SteelHead CX.
On-premises SteelHead	The SteelHead CX must be peered with another SteelHead to provide an optimization path.

3 Deploying SteelHead VCX in Orange Flexible Engine

This section describes the process and procedures for deploying the SteelHead CX in FE. It includes the following sections:

- ✓ Prerequisites
- ✓ Deploying the SteelHead VCX from the Orange Flexible Engine Appliance Catalog

3.1 Prerequisites

There are two methods of deploying the SteelHead CX. You can use the SteelHead CX image in the FE Appliance Catalog or you can download the SteelHead CX from support.riverbed.com and deploy manually. This deployment guide uses the Appliance Catalog method.

It will not be possible to use the SteelHead VCX until it is licensed and this requires access to the Riverbed Licence Portal to license the FE SteelHead instance.

Best Practice: While not required, it is highly recommended that you assign static public and private IP addresses for the FE SteelHead instances to ensure the greatest reliability for optimization.

To get access to the outside world, a Public IP address (EIP: Elastic IP) will be statically linked to the Primary interface of the SteelHEad VCX.

3.2 Deploying the FE SteelHead VCX from the FE Appliance Catalog

3.2.1 Security Group creation

A security group needs to be assigned to the SteelHead Primary interface in order to authorize communications from the “on premise” offices to the SteelHead. We require the following ports to be allowed at a minimum on the WAN side:

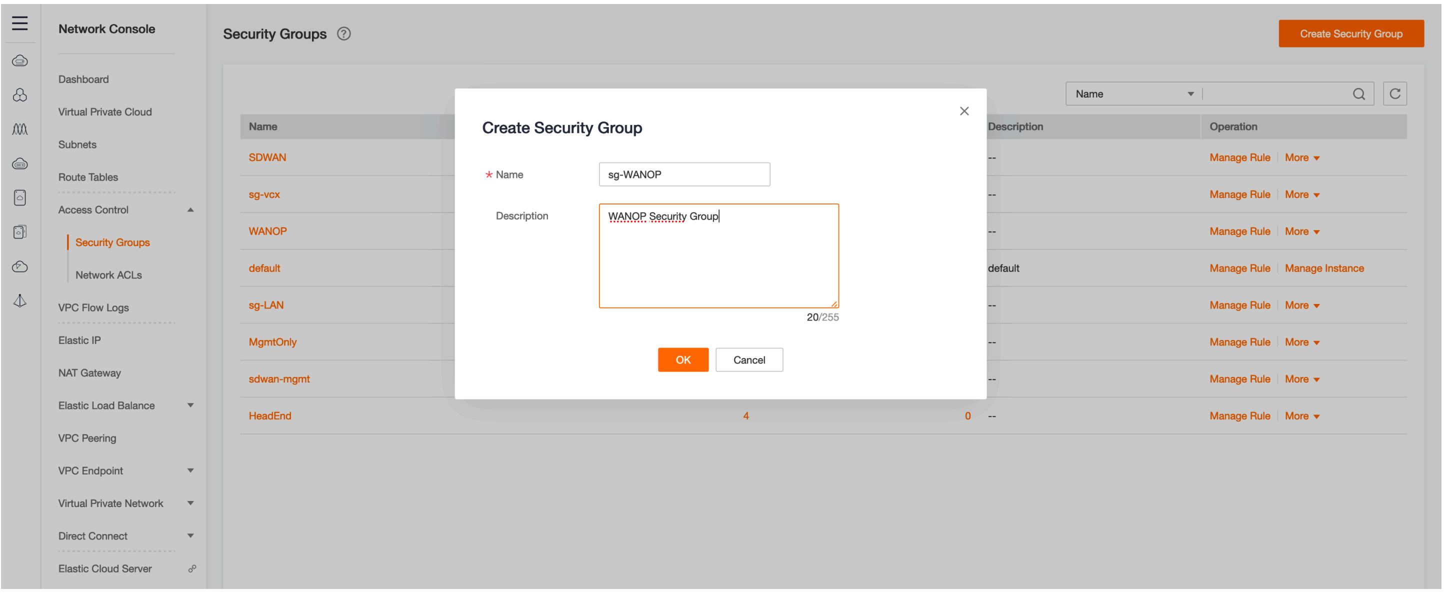
- ✓ TCP/22: for SSH access, required to SteelHead CLI interface
- ✓ TCP/443: for HTTPS GUI, required to access the managent interface of the SteelHead
- ✓ TCP/7800-7810 : for Riverbed SteelHead-to-SteelHead communication

Additional protocols can be add/modified after deployment of security groupe template.

Here are the steps to create the security group:

3.2.1.1 Create Security Group

Navitage to VPC > Access Control > Security Groups



Name			Description	Operation
SDWAN			--	Manage Rule | More
sg-vcx			--	Manage Rule | More
WANOP			--	Manage Rule | More
default			default	Manage Rule | Manage Instance
sg-LAN			--	Manage Rule | More
MgmtOnly			--	Manage Rule | More
sdwan-mgmt			--	Manage Rule | More
HeadEnd	4	0	--	Manage Rule | More

Create Security Group

* Name: sg-WANOP

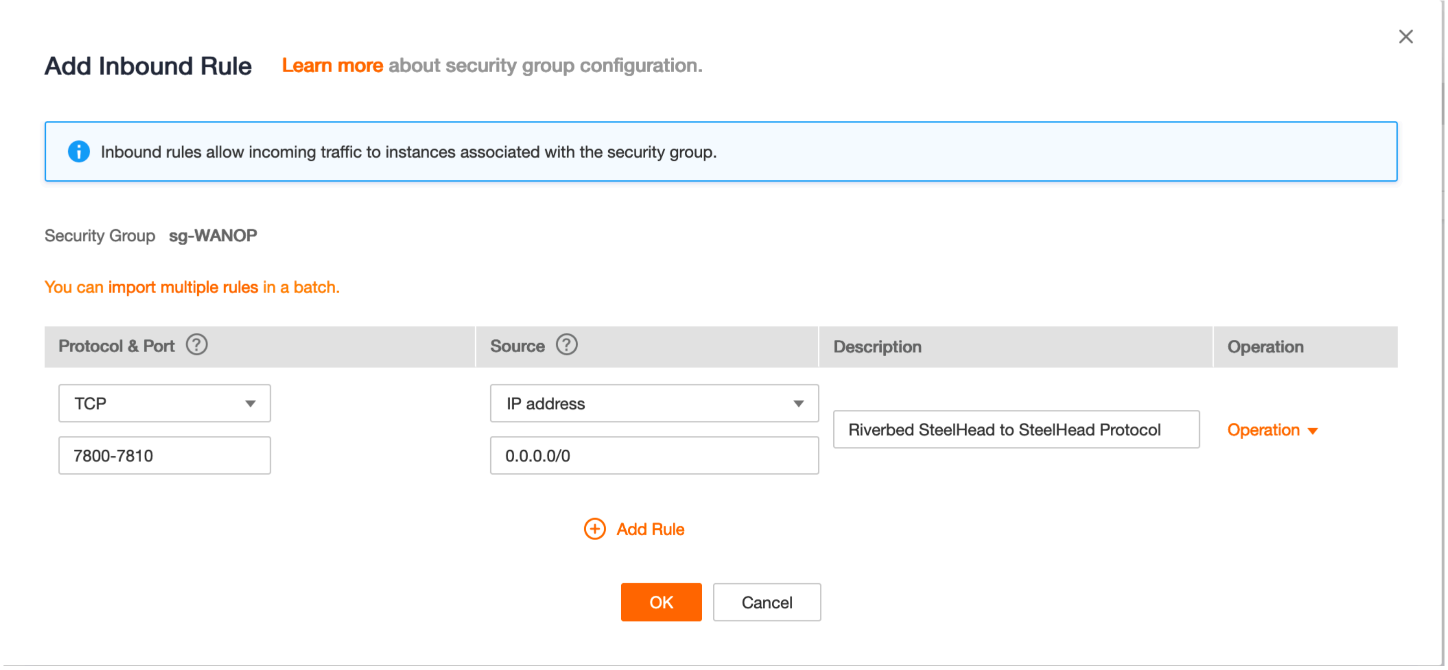
Description: WANOP Security Group

20/255

Figure 2 - Security Group Creation

3.2.1.2 Add required inbound rules

Inbound-Rules -> Add rule



Add Inbound Rule **Learn more** about security group configuration.

Inbound rules allow incoming traffic to instances associated with the security group.

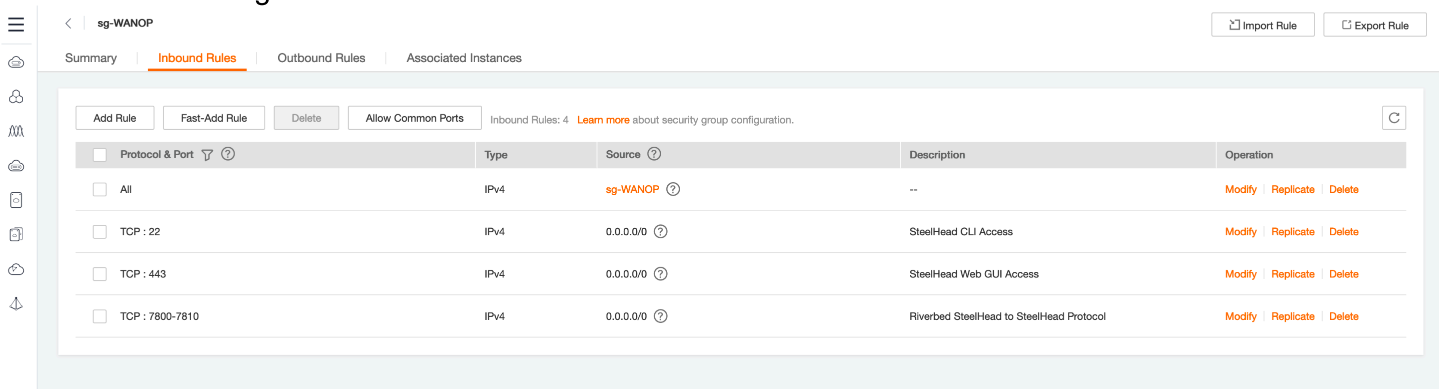
Security Group **sg-WANOP**

You can **import multiple rules** in a batch.

Protocol & Port	Source	Description	Operation
TCP 7800-7810	IP address 0.0.0.0/0	Riverbed SteelHead to SteelHead Protocol	Operation

Figure 3 - Add inbound rule

As a minimum configuration:


sg-WANOP

Import Rule | Export Rule

Summary | Inbound Rules | Outbound Rules | Associated Instances

Add Rule | Fast-Add Rule | Delete | Allow Common Ports

Inbound Rules: 4 Learn more about security group configuration.

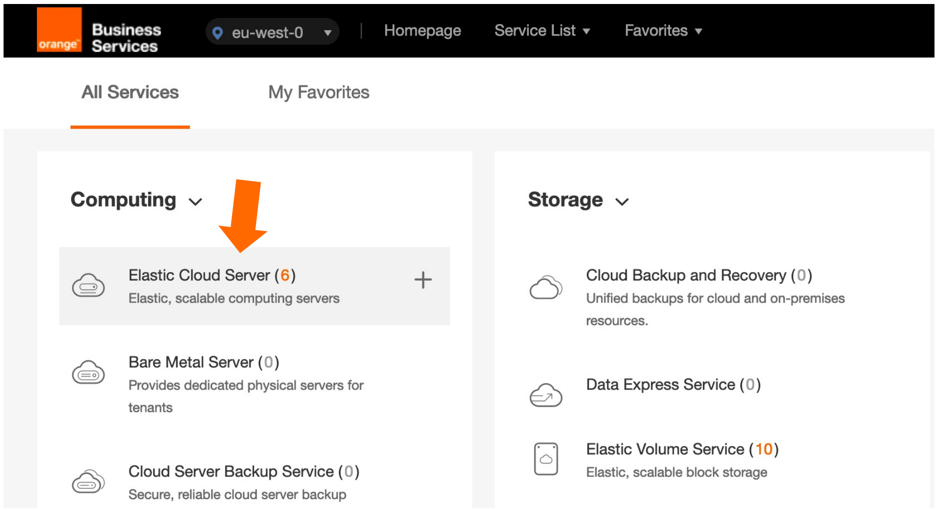
	Protocol & Port	Type	Source	Description	Operation
□	All	IPv4	sg-WANOP	--	Modify | Replicate | Delete
□	TCP : 22	IPv4	0.0.0.0/0	SteelHead CLI Access	Modify | Replicate | Delete
□	TCP : 443	IPv4	0.0.0.0/0	SteelHead Web GUI Access	Modify | Replicate | Delete
□	TCP : 7800-7810	IPv4	0.0.0.0/0	Riverbed SteelHead to SteelHead Protocol	Modify | Replicate | Delete

Figure 4 - Minimum inbound rules for SteelHead

This Security Group will then be associated to the Primary interface of the SteelHead VCX during the Deployment phase.

3.2.2 Deploy Virtual SteelHead VCX appliance in FE

Navigate to the Elastic Cloud Server



Computing

Elastic Cloud Server (6)
Elastic, scalable computing servers

Bare Metal Server (0)
Provides dedicated physical servers for tenants

Cloud Server Backup Service (0)
Secure, reliable cloud server backup

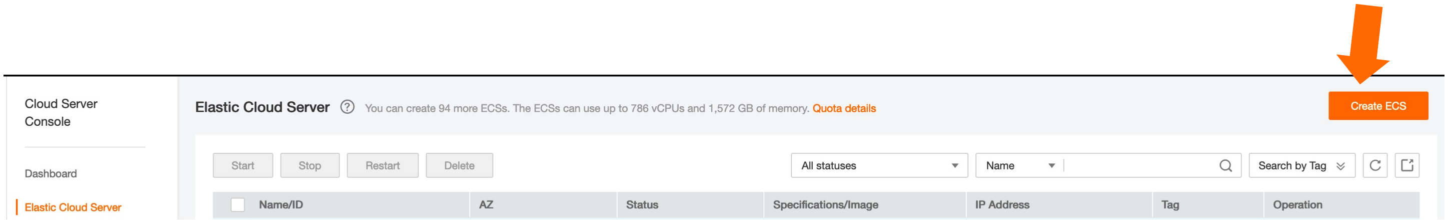
Storage

Cloud Backup and Recovery (0)
Unified backups for cloud and on-premises resources.

Data Express Service (0)

Elastic Volume Service (10)
Elastic, scalable block storage

Create a new ECS



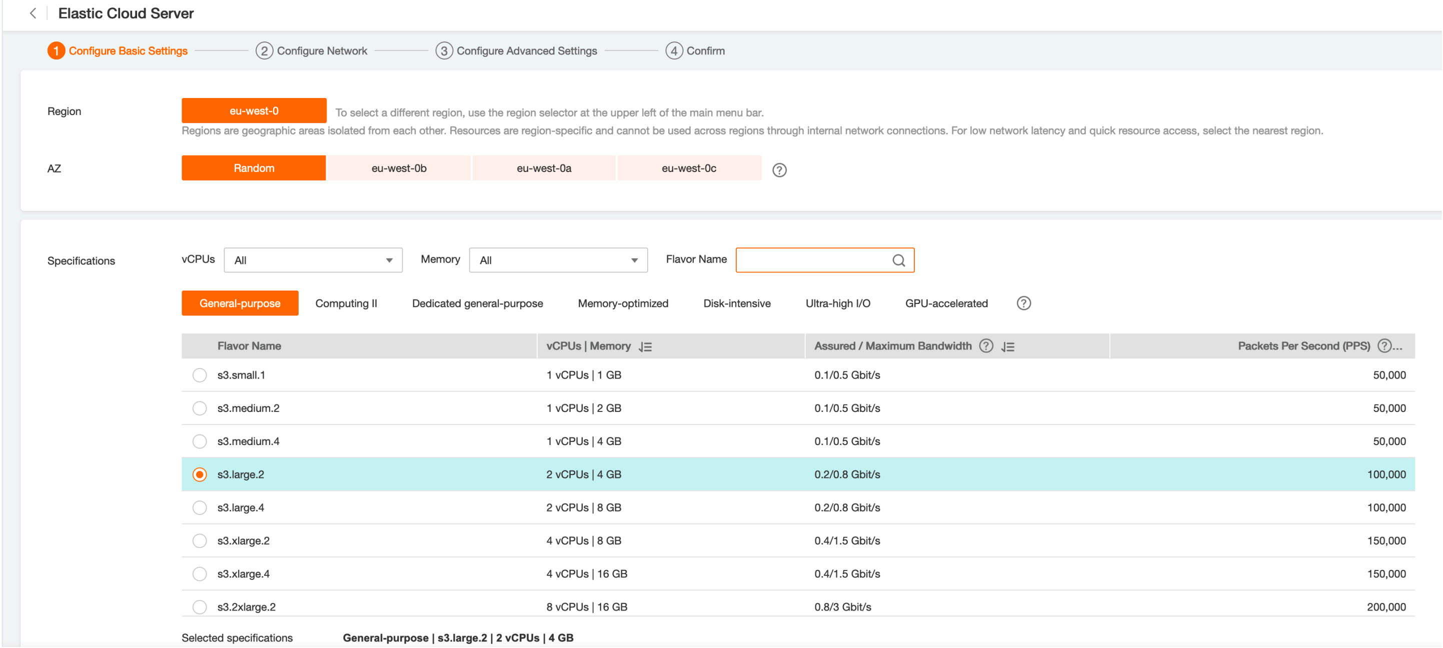
Elastic Cloud Server You can create 94 more ECSs. The ECSs can use up to 786 vCPUs and 1,572 GB of memory. Quota details

□	Name/ID	AZ	Status	Specifications/Image	IP Address	Tag	Operation

Select the Virtual machine properties based on target optimized throuput and tcp connections (Orange FE Cloud SteelHead models and required virtual machine resources.
For example, for a VCX-030 (10 Mbps optimized throughput and 500 tcp connection), a s3.large.2 ECS flavor is required. See Section 6.1 (Appendix A) for the full list of specifications and models available in FE.

Model	vCPU cores	Memory(GB)	MgmtDisk(GB)	SegstoreMax Disk Size(GB)	OptimizedB/W(Mbps)	MaxConnections
VCX-30	2	4	40	100	10	500

Select the Region; the SteelHead must be deployed in same region as the ECS hosting the application to be optimized.



Elastic Cloud Server

1 Configure Basic Settings — 2 Configure Network — 3 Configure Advanced Settings — 4 Confirm

Region: eu-west-0 — To select a different region, use the region selector at the upper left of the main menu bar.

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

AZ: Random | eu-west-0b | eu-west-0a | eu-west-0c

Specifications: vCPUs: All | Memory: All | Flavor Name:

General-purpose | Computing II | Dedicated general-purpose | Memory-optimized | Disk-intensive | Ultra-high I/O | GPU-accelerated

	Flavor Name	vCPUs | Memory	Assured / Maximum Bandwidth	Packets Per Second (PPS)...
○	s3.small.1	1 vCPUs | 1 GB	0.1/0.5 Gbit/s	50,000
○	s3.medium.2	1 vCPUs | 2 GB	0.1/0.5 Gbit/s	50,000
○	s3.medium.4	1 vCPUs | 4 GB	0.1/0.5 Gbit/s	50,000
●	s3.large.2	2 vCPUs | 4 GB	0.2/0.8 Gbit/s	100,000
○	s3.large.4	2 vCPUs | 8 GB	0.2/0.8 Gbit/s	100,000
○	s3.xlarge.2	4 vCPUs | 8 GB	0.4/1.5 Gbit/s	150,000
○	s3.xlarge.4	4 vCPUs | 16 GB	0.4/1.5 Gbit/s	150,000
○	s3.2xlarge.2	8 vCPUs | 16 GB	0.8/3 Gbit/s	200,000

Selected specifications: **General-purpose | s3.large.2 | 2 vCPUs | 4 GB**

From the public image Appliance Catalog, select the last image starting with "Riverbed-SteelHead-*" :

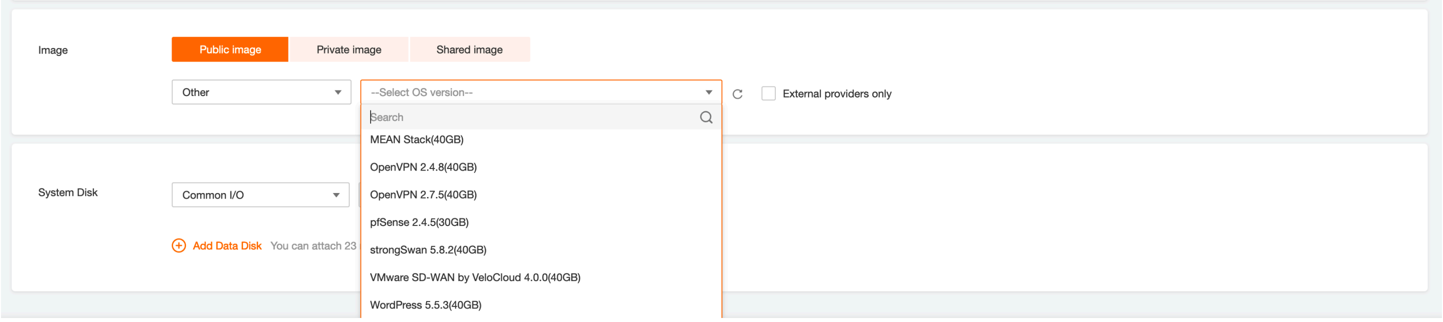


Image: Public image | Private image | Shared image

Other | --Select OS version-- | □ External providers only

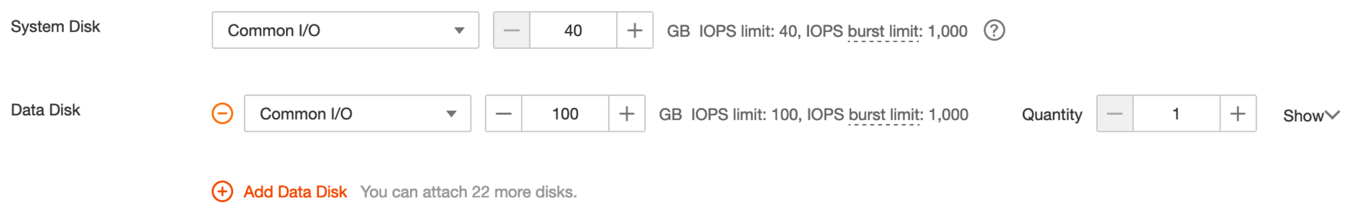
Search

- MEAN Stack(40GB)
- OpenVPN 2.4.8(40GB)
- OpenVPN 2.7.5(40GB)
- pfSense 2.4.5(30GB)
- strongSwan 5.8.2(40GB)
- VMware SD-WAN by VeloCloud 4.0.0(40GB)
- WordPress 5.5.3(40GB)

System Disk: Common I/O

Add Data Disk — You can attach 23

Add the required 2nd disk

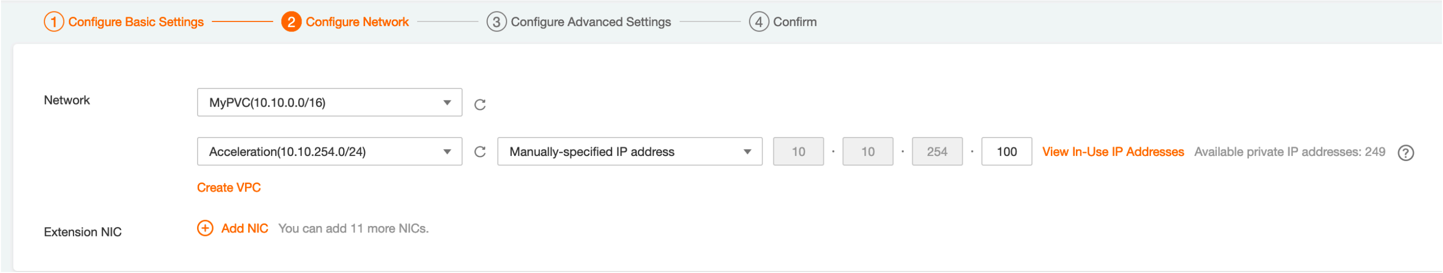


System Disk: Common I/O | 40 | GB IOPS limit: 40, IOPS burst limit: 1,000

Data Disk: Common I/O | 100 | GB IOPS limit: 100, IOPS burst limit: 1,000 | Quantity 1 | Show

Add Data Disk — You can attach 22 more disks.

Assign a subnet and an IP address to the Primary interface



1 Configure Basic Settings — 2 Configure Network — 3 Configure Advanced Settings — 4 Confirm

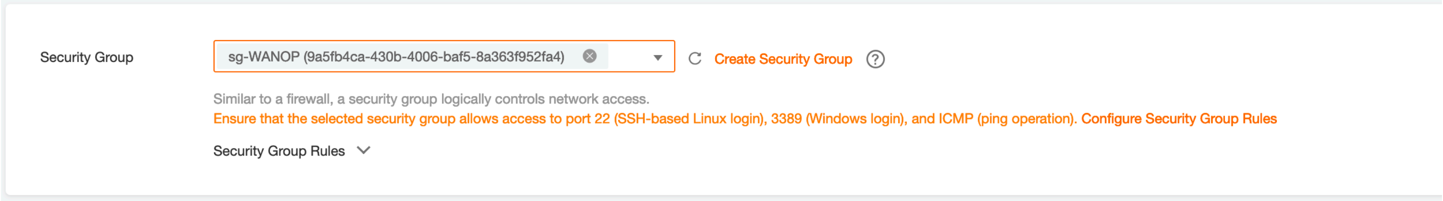
Network: MyPVC(10.10.0.0/16)

Acceleration(10.10.254.0/24) | Manually-specified IP address | 10 . 10 . 254 . 100 | View In-Use IP Addresses | Available private IP addresses: 249

Create VPC

Extension NIC: Add NIC — You can add 11 more NICs.

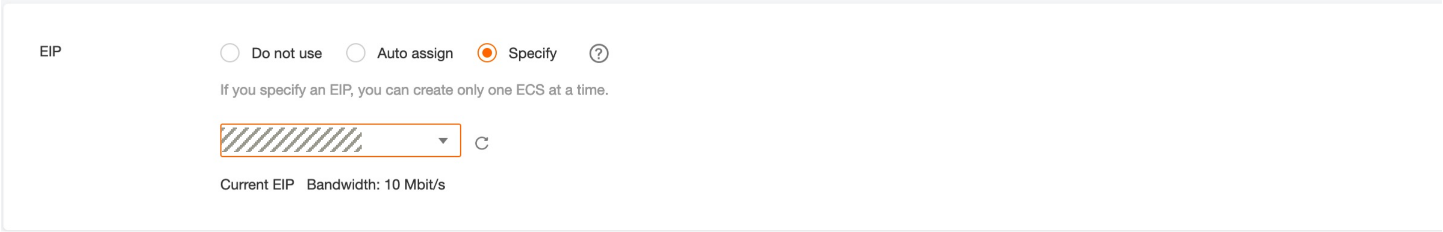
Assign the Security Group you created in the first step



Security Group: sg-WANOP (9a5fb4ca-430b-4006-baf5-8a363f952fa4)

Similar to a firewall, a security group logically controls network access.
Ensure that the selected security group allows access to port 22 (SSH-based Linux login), 3389 (Windows login), and ICMP (ping operation). Configure Security Group Rules

Assign a EIP to be used by remotes branches to connect to the SteelHead



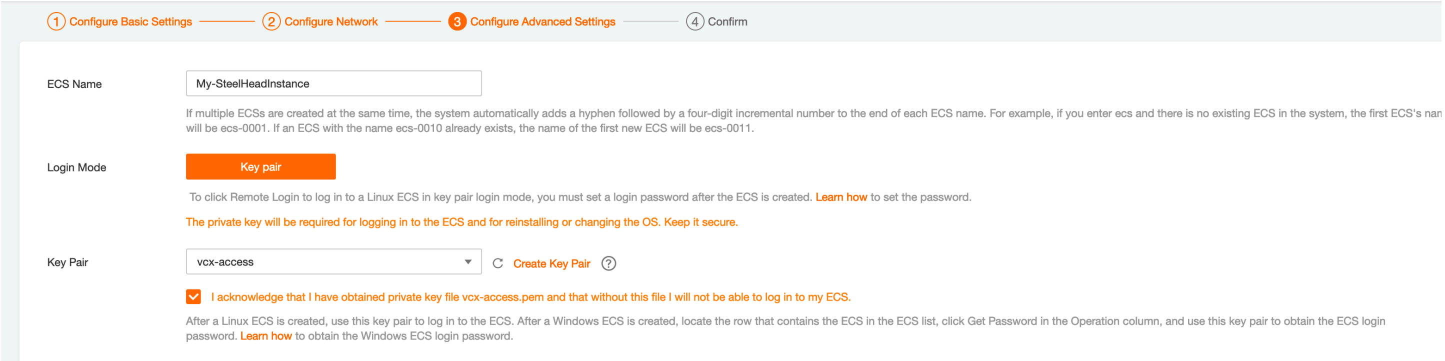
EIP ○ Do not use ○ Auto assign ● Specify

If you specify an EIP, you can create only one ECS at a time.

[redacted]

Current EIP Bandwidth: 10 Mbit/s

Give a name to the SteelHead instance



ECS Name: My-SteelHeadInstance

If multiple ECSs are created at the same time, the system automatically adds a hyphen followed by a four-digit incremental number to the end of each ECS name. For example, if you enter ecs and there is no existing ECS in the system, the first ECS's nan will be ecs-0001. If an ECS with the name ecs-0010 already exists, the name of the first new ECS will be ecs-0011.

Login Mode: Key pair

To click Remote Login to log in to a Linux ECS in key pair login mode, you must set a login password after the ECS is created. Learn how to set the password.

The private key will be required for logging in to the ECS and for reinstalling or changing the OS. Keep it secure.

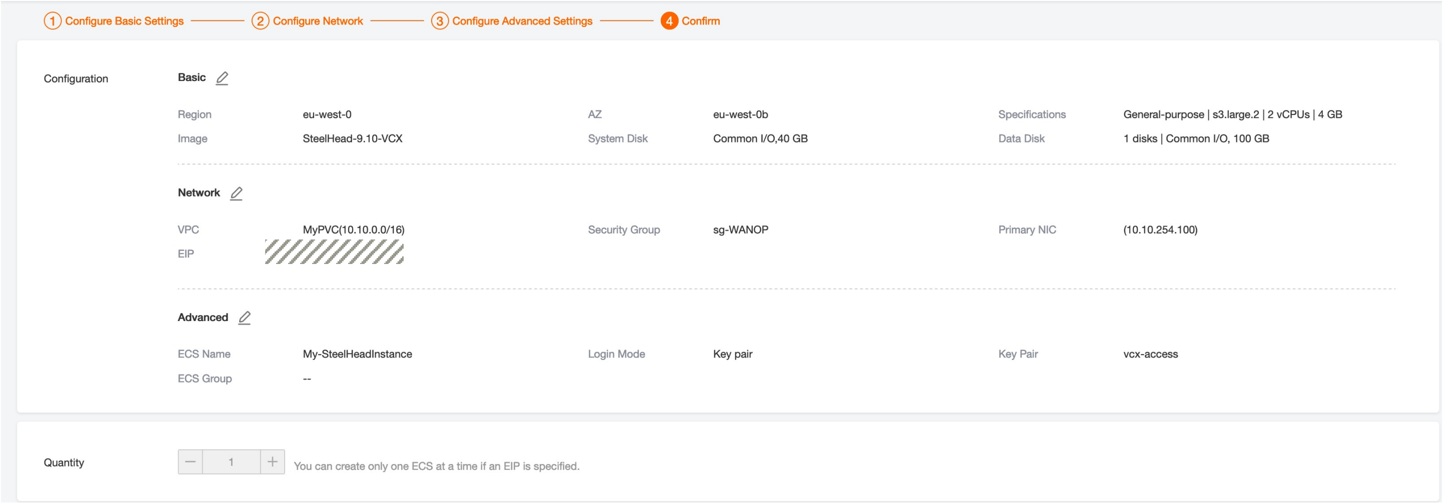
Key Pair: vcx-access

☑ I acknowledge that I have obtained private key file vcx-access.pem and that without this file I will not be able to log in to my ECS.

After a Linux ECS is created, use this key pair to log in to the ECS. After a Windows ECS is created, locate the row that contains the ECS in the ECS list, click Get Password in the Operation column, and use this key pair to obtain the ECS login password. Learn how to obtain the Windows ECS login password.

The SteelHead instance will not use a Key Pair for authentication, Refer to the Installation & Configuration guide for the default credentials.

Check the overall ECS configuration and confirm the creation



Configuration

Basic

Region	eu-west-0	AZ	eu-west-0b	Specifications	General-purpose | s3.large.2 | 2 vCPUs | 4 GB
Image	SteelHead-9.10-VCX	System Disk	Common I/O,40 GB	Data Disk	1 disks | Common I/O, 100 GB

Network

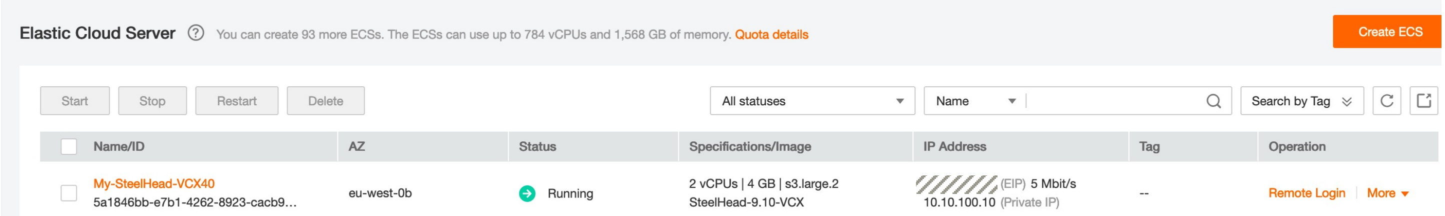
VPC	MyPVC(10.10.0.0/16)	Security Group	sg-WANOP	Primary NIC	(10.10.254.100)
EIP	[redacted]				

Advanced

ECS Name	My-SteelHeadInstance	Login Mode	Key pair	Key Pair	vcx-access
ECS Group	--				

Quantity: 1 You can create only one ECS at a time if an EIP is specified.

Wait until the ECS creation has completed, then connect to the SteelHead Instance GUI.



You can create 93 more ECSs. The ECSs can use up to 784 vCPUs and 1,568 GB of memory. Quota details

□	Name/ID	AZ	Status	Specifications/Image	IP Address	Tag	Operation
□	My-SteelHead-VCX40 5a1846bb-e7b1-4262-8923-cacb9...	eu-west-0b	Running	2 vCPUs | 4 GB | s3.large.2 SteelHead-9.10-VCX	[redacted] (EIP) 5 Mbit/s 10.10.100.10 (Private IP)	--	Remote Login | More

Your SteelHead instance is now ready for Configuration.

3.3 Preliminary Setup Tasks on the SteelHead CX

This section details recommended and required setup tasks when first configuring your SteelHead CX and contains the following sections:

- ✓ Prerequisites
- ✓ Logging in to the SteelHead VCX
- ✓ Changing the Administrative Password
- ✓ Changing the Host Settings
- ✓ Licensing the SteelHead VCX
- ✓ Enabling Server Side Out-of-path Optimization
- ✓ Saving the Configuration and Rebooting the SteelHead VCX

3.3.1 Prerequisites

To complete this section, you will need:

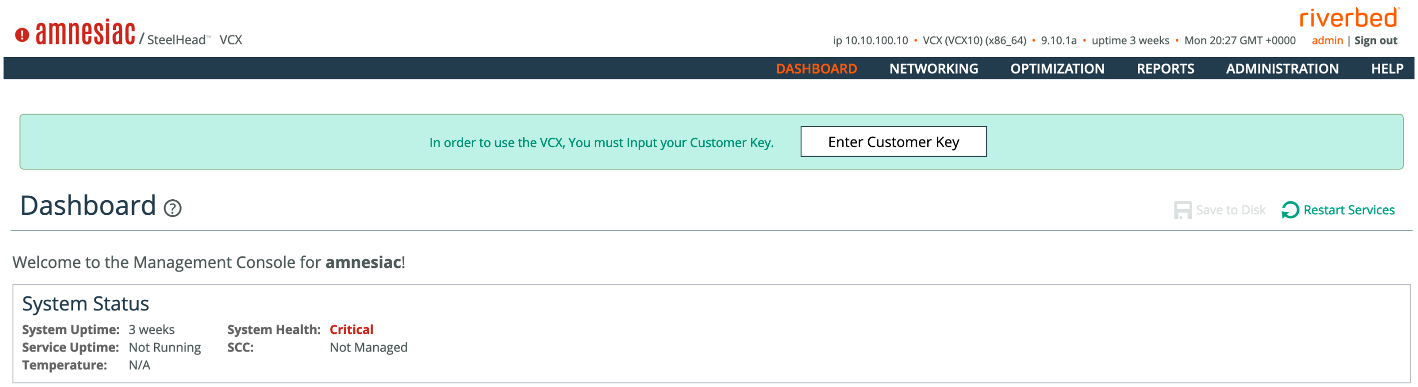
- ✓ Administrative credentials for your Orange FE Console
- ✓ EIP address of the SteelHead VCX
- ✓ IP address of a public DNS server
- ✓ Login credentials to your Riverbed support site
- ✓ An SSH client (such as PuTTY) to connect to the command-line interface (CLI) of the SteelHead VCX

3.3.2 Logging into the SteelHead VCX Web console

Using the EIP linked to the your SteelHead VCX, browse to : https://<EIP>.

Note: You may see a warning message related to the certificate used to secure the administration UI. This message is normal and expected.

Login to the SteelHead CX using the username "admin" and the default SteelHead password.



ip 10.10.100.10 • VCX (VCX10) (x86_64) • 9.10.1a • uptime 3 weeks • Mon 20:27 GMT +0000

In order to use the VCX, You must Input your Customer Key.

Dashboard

Welcome to the Management Console for **amnesiac**!

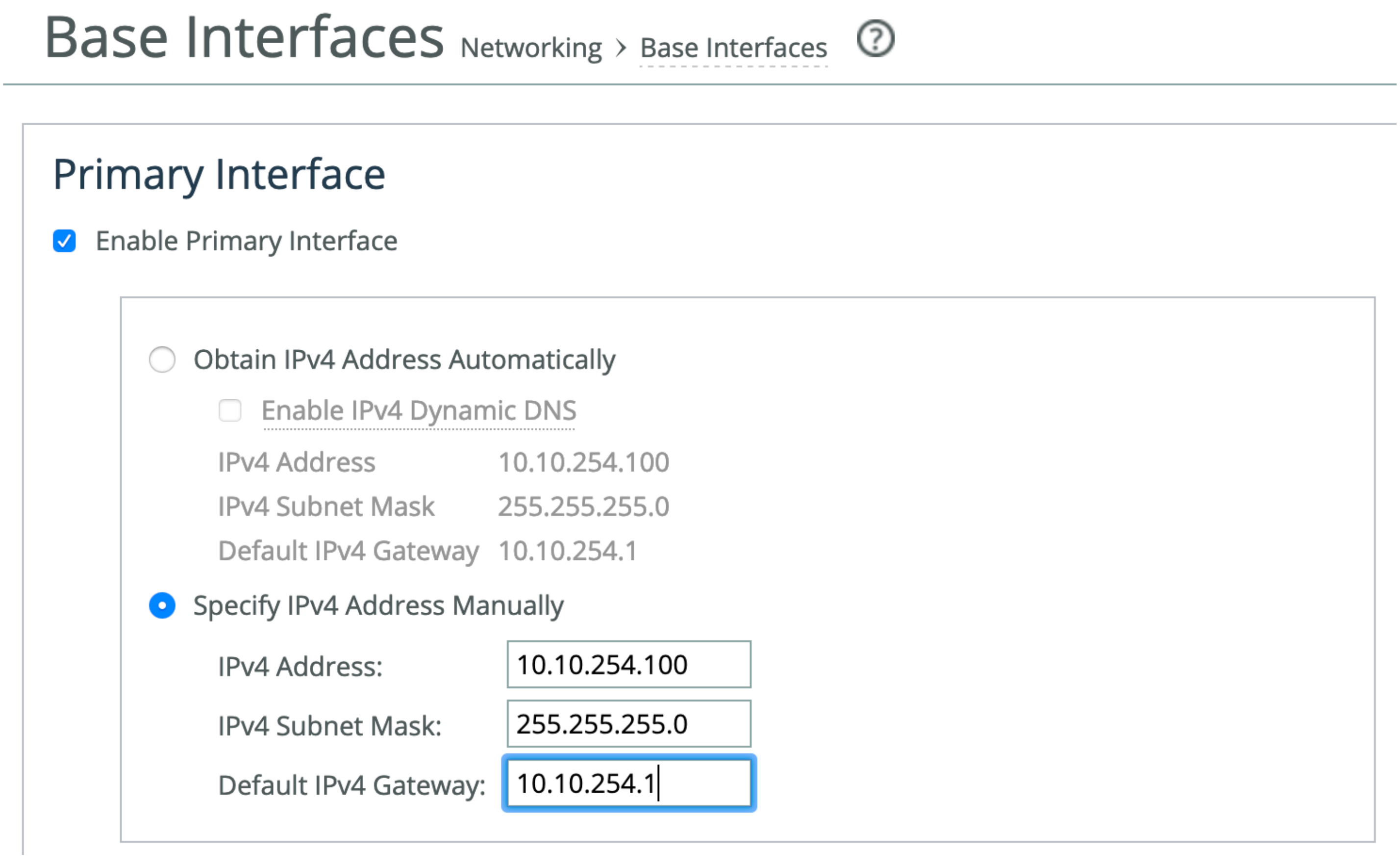
System Status

System Uptime:	3 weeks	**System Health:**	Critical
Service Uptime:	Not Running	**SCC:**	Not Managed
Temperature:	N/A		

Figure 5 - SteelHead VCX RiOS 9.x Home Page

3.3.3 Assign a static IP address to the primary interface

- ✓ Click **Networking** then under **Base Interfaces**.
- ✓ Check "**Specify IPv4 Address Manualy**" for Primary interface
- ✓ Set the IP Address info and Click Apply.



Base Interfaces Networking › Base Interfaces

Primary Interface

☑ Enable Primary Interface

○ Obtain IPv4 Address Automatically

□ Enable IPv4 Dynamic DNS

IPv4 Address	10.10.254.100
IPv4 Subnet Mask	255.255.255.0
Default IPv4 Gateway	10.10.254.1

● Specify IPv4 Address Manually

IPv4 Address:	10.10.254.100
IPv4 Subnet Mask:	255.255.255.0
Default IPv4 Gateway:	10.10.254.1

3.3.4 Change the default "admin " password

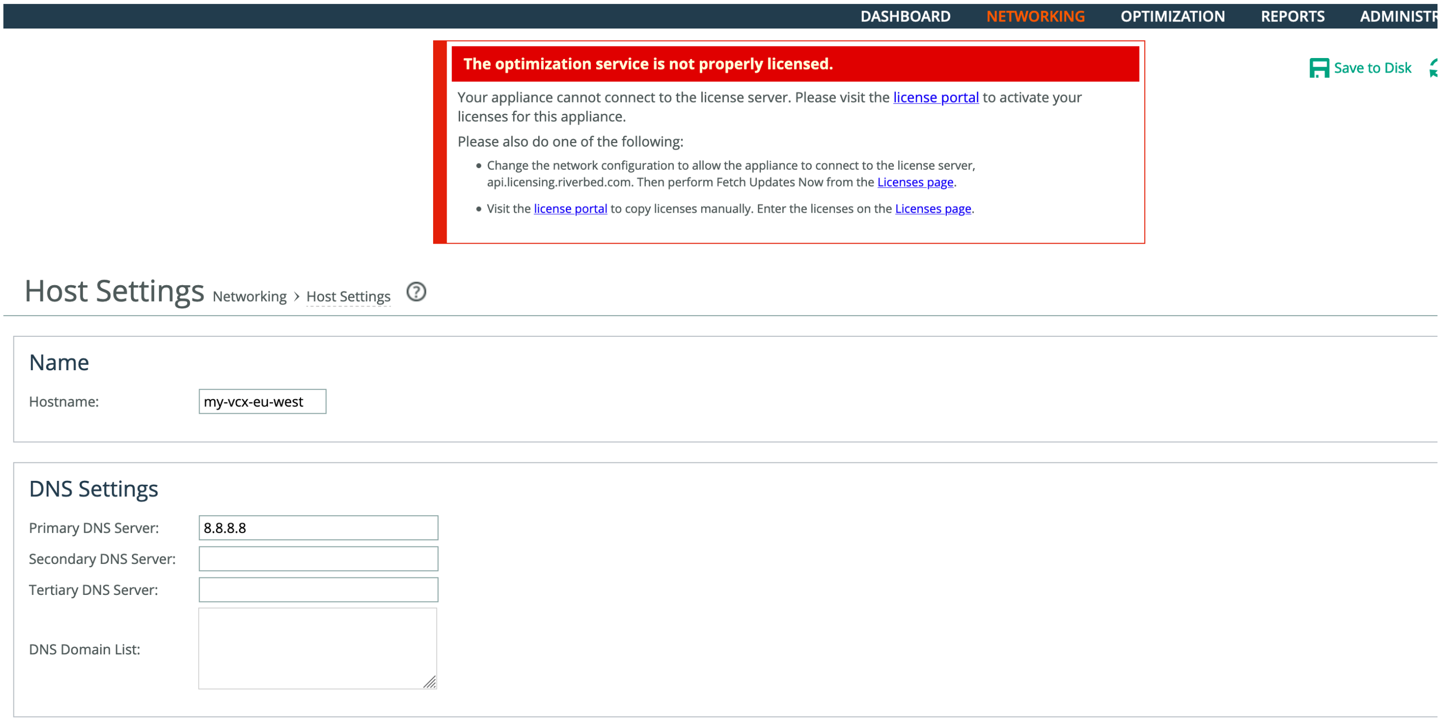
The administrative password cannot be recovered. Ensure you can recall the password you will set. Adding a second administrative account for backup access is strongly advised.

- ✓ Click **ADMINISTRATION** then under **System Settings**, click My **Account**.
- ✓ Set the Password checkbox. Enter a strong password. Click Apply.

3.3.5 Change Host setting

The Host Settings page contains important basic configuration items for the SteelHead CX including the hostname and DNS servers used by the SteelHead VCX when accessing licensing functions.

- ✓ Click **NETWORKING** then click **Host Settings**. You will see a page resembling Figure 6 - .
- ✓ Best Practice: Change the Hostname to a name suited to your business use. Many businesses have multiple SteelHead devices. Having different names assists in general administration and troubleshooting.
- ✓ Required: Add a Primary DNS Server. You must add a valid DNS server available to the SteelHead CX. You can use a private or public DNS server on your virtual network if it can resolve the licensing server for Riverbed.
- ✓ Click Apply.



The optimization service is not properly licensed.

Your appliance cannot connect to the license server. Please visit the license portal to activate your licenses for this appliance.

Please also do one of the following:

- Change the network configuration to allow the appliance to connect to the license server, api.licensing.riverbed.com. Then perform Fetch Updates Now from the Licenses page.
- Visit the license portal to copy licenses manually. Enter the licenses on the Licenses page.

Host Settings Networking › Host Settings

Name

Hostname: my-vcx-eu-west

DNS Settings

Primary DNS Server: 8.8.8.8

Secondary DNS Server:

Tertiary DNS Server:

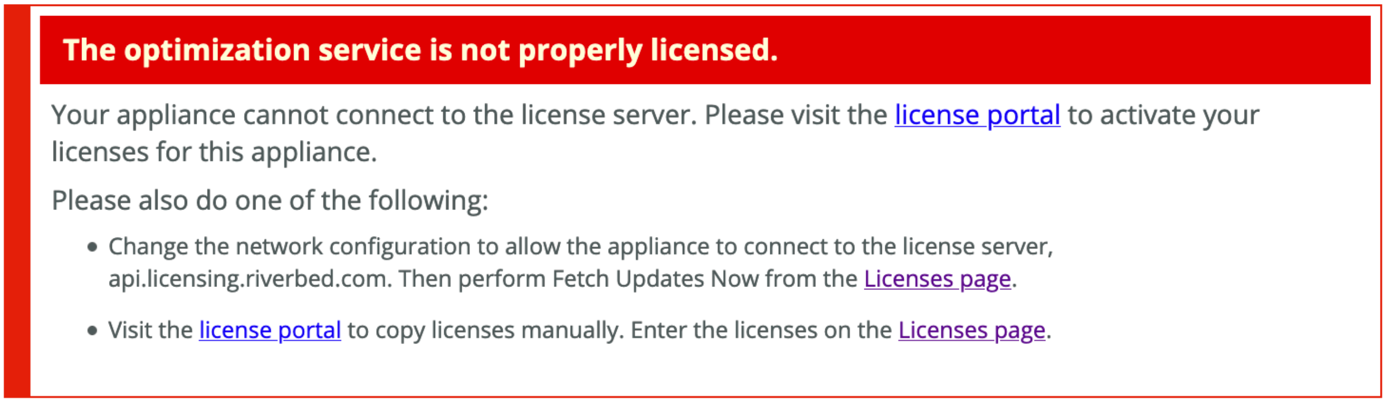
DNS Domain List:

Figure 6 - Configure Host setting page

3.3.6 Licensing the SteelHead instance.

The SteelHead VCX supports both automatic and manual licensing mode, please refer to the SteelHead Installation & Configuration guide for more details on the 2 modes. The automatic mode requires the SteelHead instance to connect to the "Riverbed license portal" (api.licensing.riverbed.com), the following warning message (Figure 7 - indicates a communication issue with the license portal. Please check :

- Check DNS configuration (api.licensing.riverbed.com must be resolved)
- Check the Secuirity Group, outband rules



The optimization service is not properly licensed.

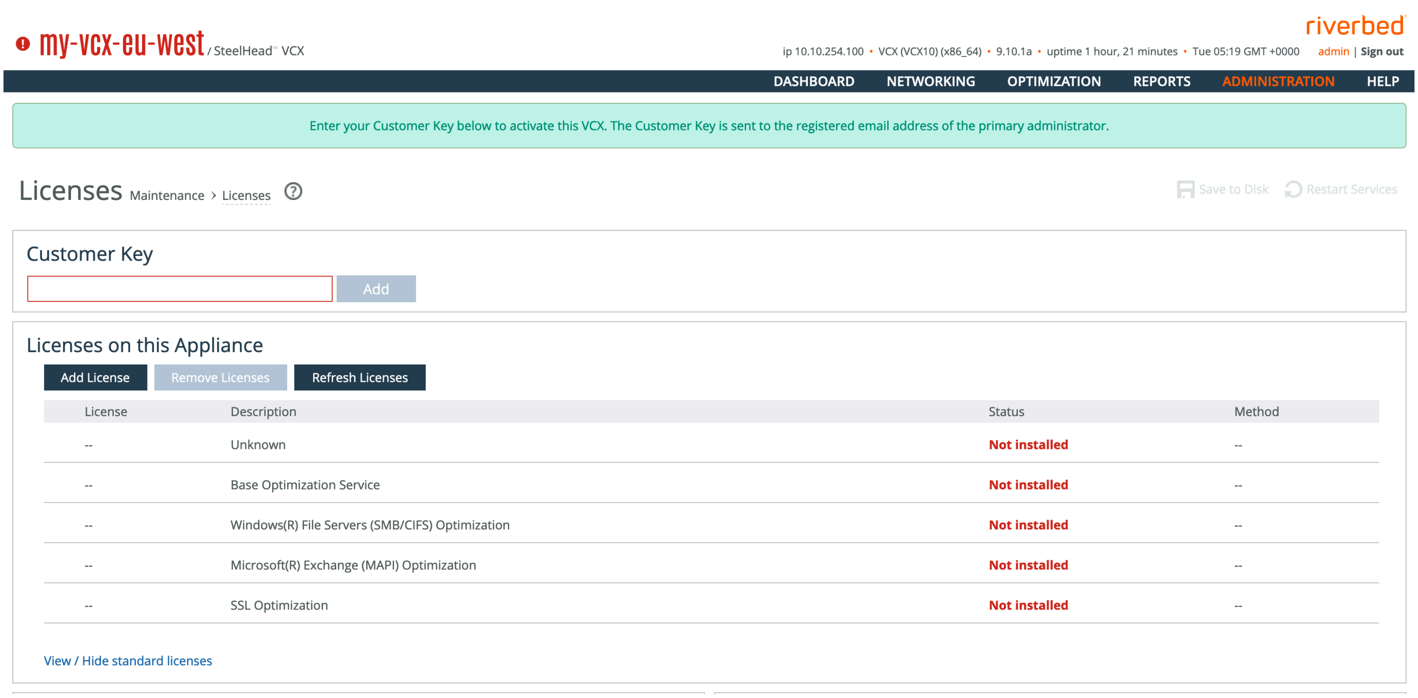
Your appliance cannot connect to the license server. Please visit the license portal to activate your licenses for this appliance.

Please also do one of the following:

- Change the network configuration to allow the appliance to connect to the license server, api.licensing.riverbed.com. Then perform Fetch Updates Now from the Licenses page.
- Visit the license portal to copy licenses manually. Enter the licenses on the Licenses page.

Figure 7 - Licenses Warning

In case communication with the Riverbed License Portal is not allowed, the manual licensing procedure (Challenge & Response) can be used to install a license on the SteelHead.
For the following steps, we consider the "Riverbed Licensing Portal" reachable from the steelhead-VCX appliance(Figure 8 -).



my-vcx-eu-west / SteelHead™ VCX
riverbed
ip 10.10.254.100 • VCX (VCX10) (x86_64) • 9.10.1a • uptime 1 hour, 21 minutes • Tue 05:19 GMT +0000
admin | Sign out
DASHBOARD
NETWORKING
OPTIMIZATION
REPORTS
ADMINISTRATION
HELP

Enter your Customer Key below to activate this VCX. The Customer Key is sent to the registered email address of the primary administrator.

Licenses Maintenance > Licenses

Customer Key

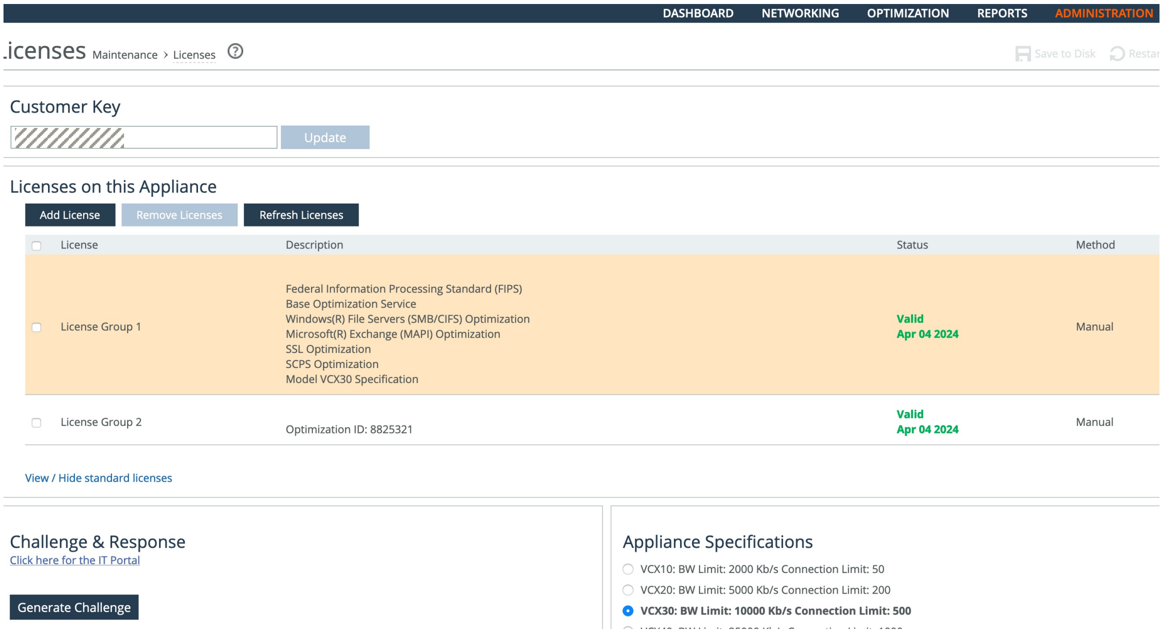
Licenses on this Appliance

License	Description	Status	Method
--	Unknown	Not installed	--
--	Base Optimization Service	Not installed	--
--	Windows(R) File Servers (SMB/CIFS) Optimization	Not installed	--
--	Microsoft(R) Exchange (MAPI) Optimization	Not installed	--
--	SSL Optimization	Not installed	--

View / Hide standard licenses

Figure 8 - Licensing Portal reachable

As soon as a valid Customer Key is configured, the SteelHead will retrieve a licence from the Riverbed License Portal.



Customer Key

Licenses on this Appliance

□	License	Description	Status	Method
□	License Group 1	Federal Information Processing Standard (FIPS) Base Optimization Service Windows(R) File Servers (SMB/CIFS) Optimization Microsoft(R) Exchange (MAPI) Optimization SSL Optimization SCPS Optimization Model VCX30 Specification	**Valid** **Apr 04 2024**	Manual
□	License Group 2	Optimization ID: 8825321	**Valid** **Apr 04 2024**	Manual

View / Hide standard licenses

Challenge & Response

Click here for the IT Portal

Appliance Specifications

○ VCX10: BW Limit: 2000 Kb/s Connection Limit: 50

○ VCX20: BW Limit: 5000 Kb/s Connection Limit: 200

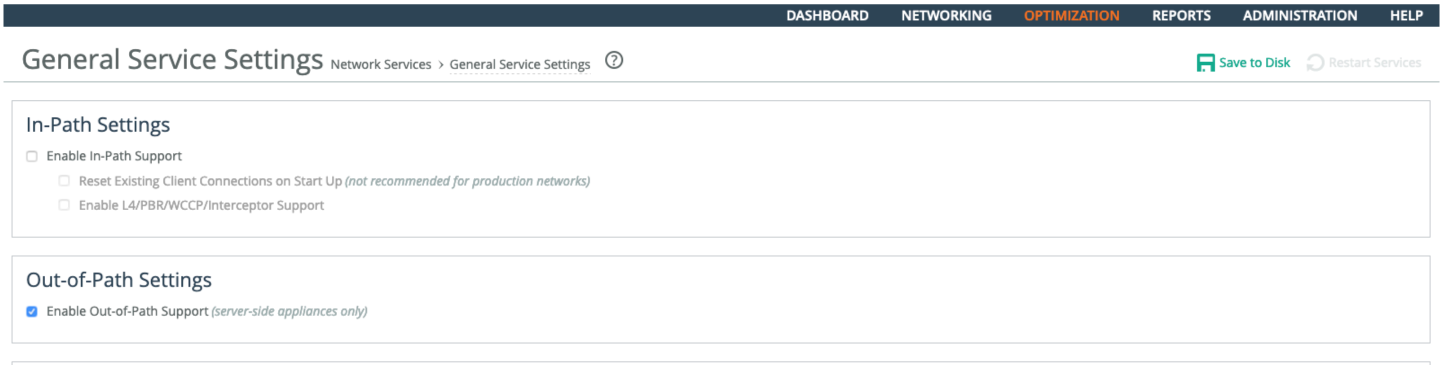
● **VCX30: BW Limit: 10000 Kb/s Connection Limit: 500**

Figure 9 - License status updated

3.3.7 Enable out-of-path optimization

A Physical or Virtual SteelHead can use “in-path” or “out-of-path” (OOP) deployment modes for optimization. Due to networking requirements in Flexible Engine, the SteelHead VCX instance, hosted in Orange FE will support only the OOP deployment mode. To enable this mode, we need to apply the following configuration :

- ✓ Browse to Optimization -> General Service Setting (Figure 10 -)



In-Path Settings

□ Enable In-Path Support

□ Reset Existing Client Connections on Start Up *(not recommended for production networks)*

□ Enable L4/PBR/WCCP/Interceptor Support

Out-of-Path Settings

☑ Enable Out-of-Path Support *(server-side appliances only)*

Figure 10 - Enable OOP support

- ✓ Select the **Enable Out-of-Path** Support check box.
- ✓ Click **Apply**.
- ✓ At the top of the page, click **Save** to save the configuration change.

3.3.8 Additional Settings Using the Command Line Interface

Before the SteelHead VCX is ready for use in Orange FE, you must change the default NAT timeouts. SteelHead appliances can be granularly controlled using command-line instructions documented in the “*Riverbed Command-Line Interface Reference Manual*”.

Log in to the SteelHead VCX using SSH. You can use any SSH client to open a connection to the EIP address for your SteelHead Instance.

Enter the following commands:

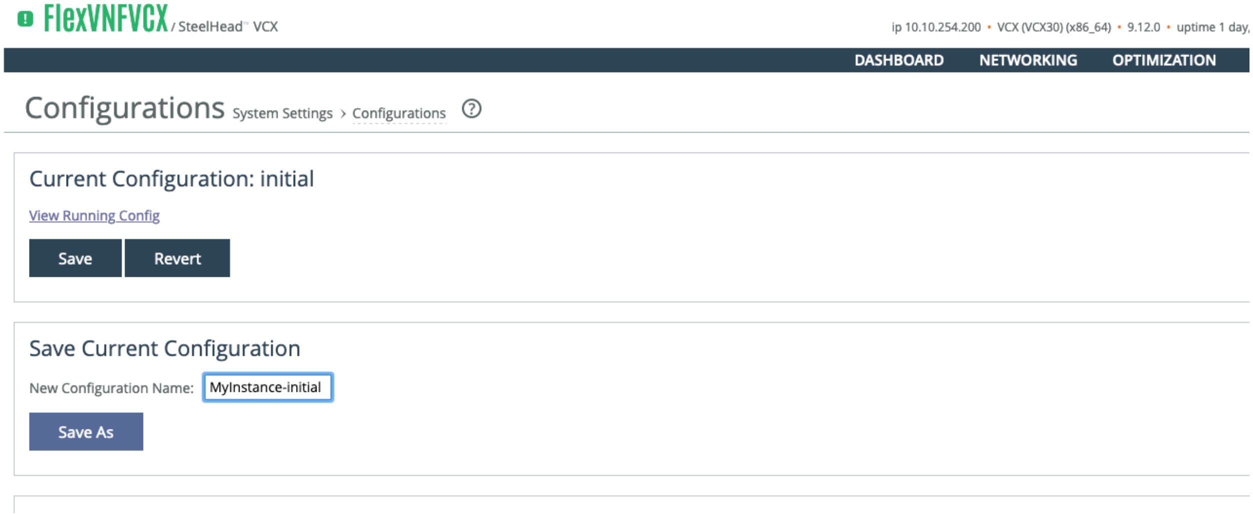
- ✓ fe-sh > enable
- ✓ fe-sh # configure terminal
- ✓ fer-sh (config) # protocol connection addr <EIP> inner-intvl 30 oob-intvl 30
- ✓ fe-sh (config) # write memory

Logout and close your SSH session.

3.3.9 Saving the Configuration and Rebooting the SteelHead VCX

Your SteelHead VCX is now configured. Before proceeding, save the configuration. You can load this configuration anytime you want to start from a known good baseline configuration.

- ✓ To save your configuration, browse to **Administration**> **Configurations** (Figure 11 -)
- ✓ Under “**Save As**”, enter the name for the configuration and click the “**Save As**” button


FlexVNFVCX / SteelHead™ VCX
ip 10.10.254.200 • VCX (VCX30) (x86_64) • 9.12.0 • uptime 1 day,
DASHBOARD
NETWORKING
OPTIMIZATION
Configurations System Settings › Configurations
Current Configuration: initial
View Running Config
Save
Revert
Save Current Configuration
Save As

New Configuration Name: MyInstance-initial

Figure 11 - Configuration Save

You now have a baseline configuration you can revert to should the need arise.

- ➢ To reboot the SteelHead CX, browse to Administration and click Reboot.

After several minutes, the reboot will have completed, you can log back in to the UI and proceed with any other settings or configuration you require.

You are now ready to set up the on-premises SteelHead to peer with the SteelHead instance just deployed in Oranfe Flexible Engine.

4 Configuring On Premises SH and Peering with the FE SH instance

This section describes how to set up an on-premises SteelHead to optimize Orange FE workloads with the SteelHead VCX.
This chapter contains the following sections.

- Prerequisites
- Creating a Fixed-Target In-Path Rule
- Peering

4.1 Prerequisites

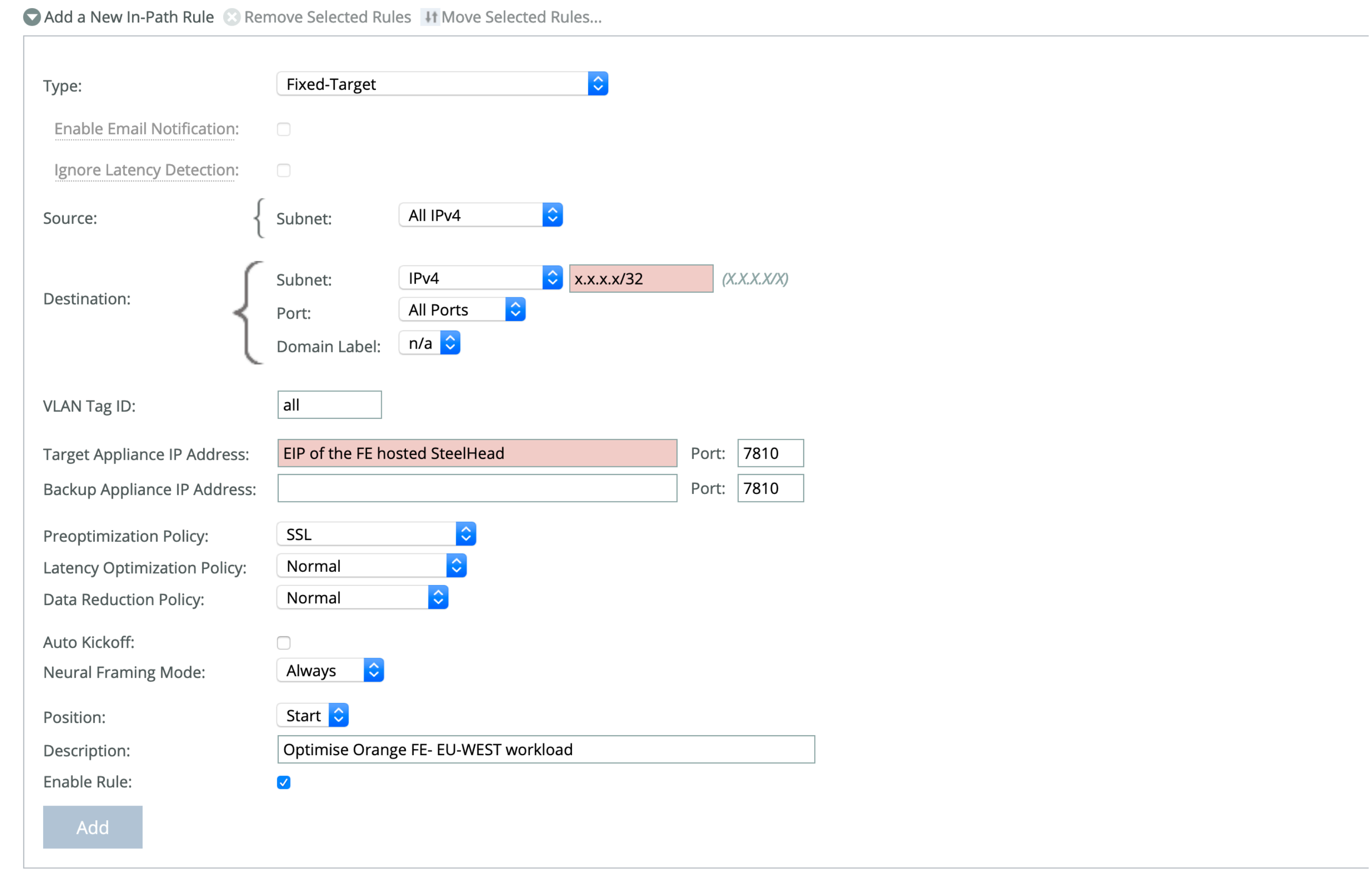
Before performing the tasks in this chapter, you must have:

- Orange FE SteelHead VCX deployed and operational
- EIP of the Orange FE SteelHead VCX
- IP address or subnet of a service you want to optimize (such as an Orange FE hosted SharePoint virtual machine)
- On-premises SteelHead licensed and configured for general optimization

4.2 Creating a Fixed-Target In-Path Rule

One or more in-path rules on the on-premises SteelHead are used to direct traffic to the FE SteelHead VCX. In-path rules allow you to create a set of criteria such as “All traffic from an IP address”, or “All traffic from a subnet on port 443” and take a designated action on matching traffic including the options to optimize, deny, or pass through the traffic. When used with other on premises SteelHeads, the SteelHeads have a built-in mechanism for discovering each other. This is known as an “auto-discover” rule. When setting up peering with a cloud hosted SteelHead, auto-discover cannot be used without special considerations. As a result, you must setup your in-path rules as “fixed-target” rules that let you direct the desired traffic to the EIP address of the Orange FE hosted SteelHead VCX.

- Log in as administrator to the on-premises SteelHead.
- Browse to **Optimization** -> In-Path **Rules**.
- Select the Add a New **In-Path Rule** tab (see Figure 12 **-**).



Type: Fixed-Target

Enable Email Notification: □

Ignore Latency Detection: □

Source: Subnet: All IPv4

Destination: Subnet: IPv4 x.x.x.x/32 (X.X.X.X/X)
Port: All Ports
Domain Label: n/a

VLAN Tag ID: all

Target Appliance IP Address: EIP of the FE hosted SteelHead Port: 7810

Backup Appliance IP Address: Port: 7810

Preoptimization Policy: SSL

Latency Optimization Policy: Normal

Data Reduction Policy: Normal

Auto Kickoff: □

Neural Framing Mode: Always

Position: Start

Description: Optimise Orange FE- EU-WEST workload

Enable Rule: ☑

Figure 12 - Adding an In-Path Rule

◊ Type: Select Fixed-Target.

◊ Source Subnet: All-IP is the default. Replace this with the All-IPv4, a subnet you want to test, or a specific IP address. This entry uses CIDR notation so a specific IP address would be followed by /32 such as 192.168.5.20/32. The Source Subnet entry allows you to easily limit optimization for a proof of concept or restrict optimization to certain groups. For testing purposes, you can specify the IP address of a single computer.

◊ Destination Subnet: The entry is used identify traffic directed to a specific IP or subnet. In practice, you use this entry to specify traffic bound for Cloud Apps. For example, you can designate an IP for a storage account or a subnet for a set of VMs in Orange FE. Instead of IP Address you may use a domain name to slect the traffic to be optimized. Please refer to the **SteelHead User Guide** for more options.

◊ Note: When you specify a Destination Subnet entry, you must change the Source Subnet from All-IP to another entry. Figure 12 - shows a rule that directs All-IPv4 traffic bound for the Destination Subnet to the SteelHead VCX EIP. The SteelHead VCX will forward the traffic to the final destination.

◊ Pre-Optimization-Policy: Set to None for traffic other than SSL. If you plan to optimize SSL related traffic, this setting must be SSL. In addition, you must enable SSL and add the appropriate certificates to the FE hosted SteelHead.

◊ VLAN Tag ID: Specify when you want to only optimize traffic tagged with a specific VALN tag.

◊ Target Appliance IP Address: Enter the EIP the SteelHead VCX hosted in Orange FE. This can be a public or private IP address.

◊ Backup Appliance IP Address: When set, if the Target Appliance is not available, the SteelHead will direct traffic to the Backup Appliance. This may be a second SteelHead VCX hosted in a different Availability Zone

◊ Description: Add a description to simplify administration of in-path rules.

◊

Leave all other settings as the default.

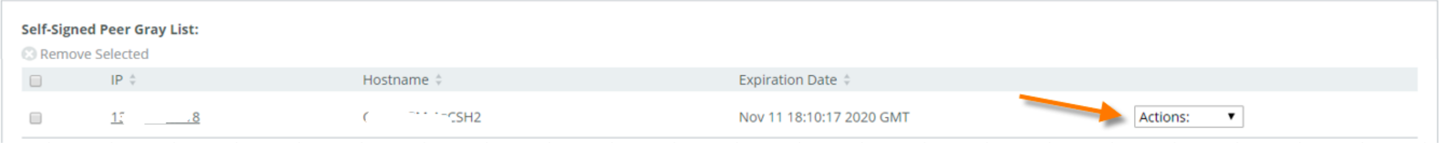
➢ Click Apply.

4.3 Secure Peering

SteelHeads are deployed with self-signed certificates. When one SteelHead attempts to optimize with another, they exchange certficates in order to create a secure connection between them. The first time a SteelHead sees the certificate from another SteelHead, it places the certificate in a "grey list". You can elect to trust the certificate, which enables a secure inner channel to be created.

Optionally, you can create and install your own certificates for this purpose. Refer to the **SteelHead Deployment Guide** for details.

- On both SteelHeads, browse to **Optimization**->**Secure Peering**
- Scroll down to until you **see Self-Signed Peer Gray List**. If the two SteelHeads are communicating, you will see an entry as shown in Figure 13 - .
- Select **Trust** from the **Actions** drop-down.



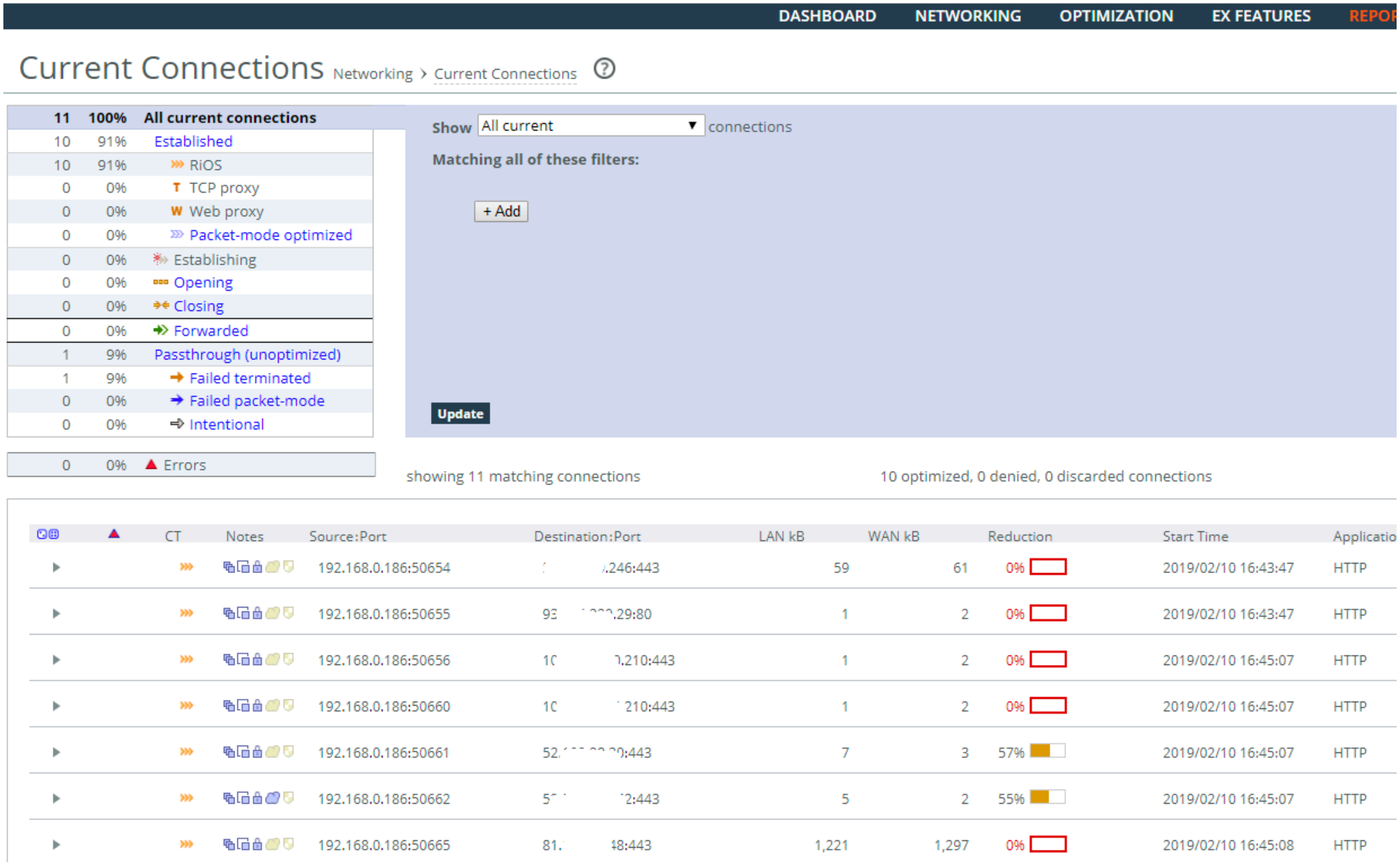
Self-Signed Peer Gray List:

Remove Selected

□	IP	Hostname	Expiration Date	
□	1: 8	(CSH2	Nov 11 18:10:17 2020 GMT	Actions: ▾

Figure 13 - Enabling trust between the SteelHeads

Once you have enabled Trust on both SteelHeads, try https Application . You should see normal optimization occuring, without errors for HTTPS connections. See Figure 14 - for an example report.



Current Connections Networking › Current Connections

11	100%	All current connections
10	91%	Established
10	91%	RiOS
0	0%	TCP proxy
0	0%	Web proxy
0	0%	Packet-mode optimized
0	0%	Establishing
0	0%	Opening
0	0%	Closing
0	0%	Forwarded
1	9%	Passthrough (unoptimized)
1	9%	Failed terminated
0	0%	Failed packet-mode
0	0%	Intentional
0	0%	Errors

Show All current ▾ connections

Matching all of these filters:

+ Add

Update

showing 11 matching connections

10 optimized, 0 denied, 0 discarded connections

		CT	Notes	Source:Port	Destination:Port	LAN kB	WAN kB	Reduction	Start Time	Applicatio
▸		»»		192.168.0.186:50654	.246:443	59	61	0%	2019/02/10 16:43:47	HTTP
▸		»»		192.168.0.186:50655	93 .29:80	1	2	0%	2019/02/10 16:43:47	HTTP
▸		»»		192.168.0.186:50656	1C .210:443	1	2	0%	2019/02/10 16:45:07	HTTP
▸		»»		192.168.0.186:50660	1C 210:443	1	2	0%	2019/02/10 16:45:07	HTTP
▸		»»		192.168.0.186:50661	52. :443	7	3	57%	2019/02/10 16:45:07	HTTP
▸		»»		192.168.0.186:50662	5 2:443	5	2	55%	2019/02/10 16:45:07	HTTP
▸		»»		192.168.0.186:50665	81. 48:443	1,221	1,297	0%	2019/02/10 16:45:08	HTTP

Figure 14 - Current Connections Report Verifies Optimization

5 Expected Optimization

SteelHead optimization of Flexible Engine workloads frequently removes significant traffic from the network while improving performance of applications. The specific amount of bandwidth reduction, latency reduction, and application acceleration depends on the exact use case. Many factors impact results including the characteristics of your network, application performance, distance from your Flexible Engine datacenter, type of traffic, and how frequently you access the same content.

5.1 How to determine if a workload can be optimized

SteelHeads have the ability to optimize many kinds of network traffic including HTTP, HTTPS, MAPI, FTP, RDP, CIFS, SMB and others. Even if the SteelHead does not recognize the application layer protocol, TCP and de-duplication can still provide substantial benefits. Most Cloud workloads utilize HTTPS, so they are good candidates for optimization.

Exceptions include content that is pre-encrypted before it is sent to the cloud. As a result, optimization benefits for this service and others like it are generally not significant. When content is encrypted before it is sent on the network, that resulting content carried on the network cannot effectively be optimized.

Most Cloud workloads benefit from optimization, as they are not pre-encrypted and use standard HTTP or HTTPS/TLS in transit. Before deploying your optimization solution, evaluate your Cloud services to ensure the content is suitable for optimization. Workloads that involve sending the same or similar data over the network are ideal. SMB traffic can be optimized on private networks from cloud to on-premises. You may need to join the SteelHead to the domain in order to decrypt signed SMB. See Optimization in a ***Secure Windows Environment*** located in the “Technical Notes” section of the SteelHead documentation on the Riverbed Support Site. You can also optimize between Orange FE and other Public Cloud Providers, or between Orange FE regions if needed.

5.1.1 Specific Use Cases

5.1.1.1SSL/TLS Optimization

SteelHeads have the ability to optimize encrypted traffic. You will need to install the appropriate certificate(s) on the FE SteelHead in order to optimize SSL/TLS traffic. For specific details about this and other configuration options, refer to the ***SteelHead Deployment Guide – Protocols***.

5.1.1.2SharePoint

Orange FE hosted SharePoint virtual machines are ideal for SteelHead optimization. As you browse web pages, the CSS, images, text, and other content become optimized for other users. Second and subsequent document uploads and downloads are highly optimized. Riverbed published a short study on optimizing SharePoint 2013 using a SteelHead mobile solution, which yields similar results as a SteelHead CX.

5.1.1.3Web Services

Traditionally, SteelHead technology excels at optimizing any Web or FTP server or service. The more users that access the same content, the better efficiency you will see from optimization. Like SharePoint, you will see very high bandwidth reduction on common content. For best results, enable strip compression in the HTTP optimization settings of the client-side SteelHead. You will get the best results when disabling compression on the web server and letting the SteelHeads do compression.

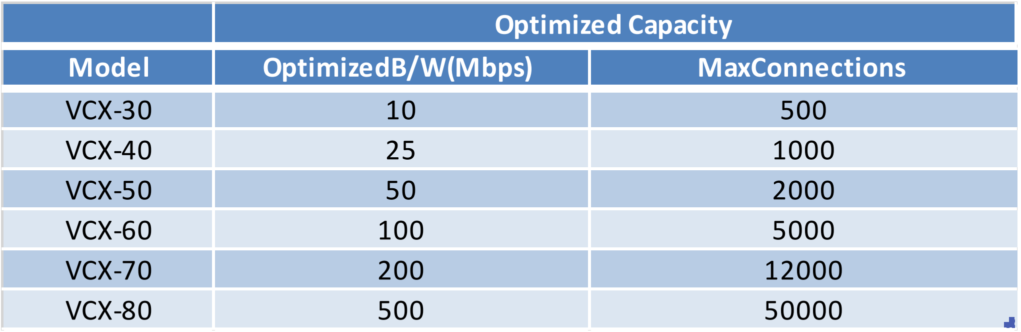
5.1.1.4Storage

As network traffic to Orange FE storage passes through an optimized path, the bits are recorded using Riverbed’s proprietary Scalable Data Reduction technology. When the SteelHeads see the same content, they do not transmit matching data between them. Instead, the data is delivered from the local SteelHead resulting in significant bandwidth reductions and LAN like latencies for data retrieval. This data reduction occurs by matching bit patterns rather than files. For example, if you copy two different virtual machines, ISO files, or other large files into Azure storage that are similar, you can expect to see significant reductions as detailed in Optimization of Large File Transfers Using Riverbed SteelHead Appliances.

6 Appendix A

6.1 Orange FE Cloud SteelHead models and required virtual machine resources.

This section lists available Orange FE Cloud SteelHead models, their supported maximum limits, and the minimum virtual machine resources required for each model.

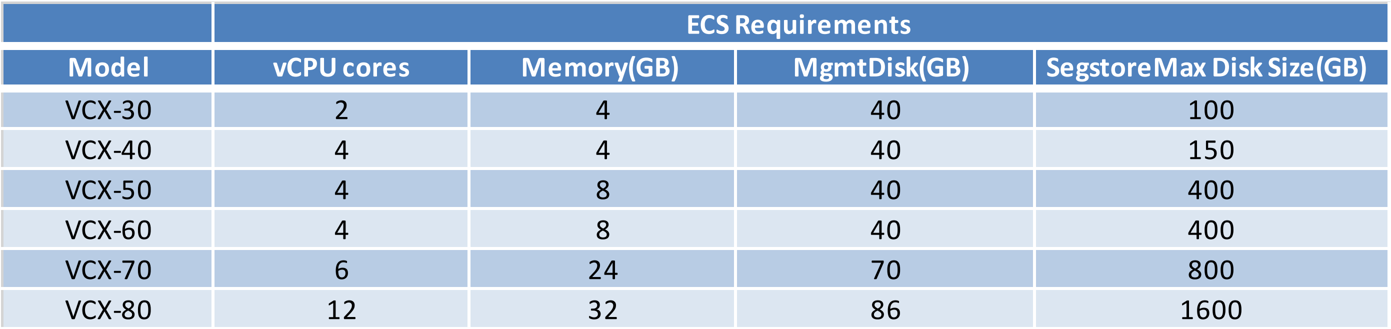


	Optimized Capacity	
Model	OptimizedB/W(Mbps)	MaxConnections
VCX-30	10	500
VCX-40	25	1000
VCX-50	50	2000
VCX-60	100	5000
VCX-70	200	12000
VCX-80	500	50000

Figure 15 - FE SteelHead VCX instance Capacity

Each SteelHead instance requires at least two virtual disks. One disk stores the SteelHead configuration and management resources; the other disk serves as the data store. Hard disk drives (HDD) can be used for most models, but solid state disks (SSD) can provide higher performance.

This table lists SteelHead models and the disk capacities needed for each.



	ECS Requirements			
Model	vCPU cores	Memory(GB)	MgmtDisk(GB)	SegstoreMax Disk Size(GB)
VCX-30	2	4	40	100
VCX-40	4	4	40	150
VCX-50	4	8	40	400
VCX-60	4	8	40	400
VCX-70	6	24	70	800
VCX-80	12	32	86	1600

Figure 16 - VM requirements