riverbed

SteelHead Path Selection to Zscaler with RiOS 9.0

Solution Guide

February 2015

Riverbed Technical Marketing

Contents

Preface

Welcome to the *SteelHead Path Selection to Zscaler with RiOS 9.0 Solution Guide.* Read this preface for an overview of the information provided in this guide and the documentation conventions used throughout, hardware and software dependencies, additional reading, and contact information. This preface includes the following sections:

About This Guide

The *SteelHead Path Selection to Zscaler with RiOS 9.0: Solution Guide* describes how to configure the SteelHead path selection to direct internet traffic to Zscaler Secure Web Gateway. Path selection chooses a predefined WAN gateway for certain traffic flows in real time, based on availability. You define a path by specifying a WAN egress point and providing a direction for the egressing packets to take. This granular path manipulation enables you to better use and more accurately control traffic flow across multiple WAN circuits.

This guide includes information relevant to the following products:

- Riverbed Steelhead EX appliance (Steelhead EX
- Riverbed Steelhead appliance (Steelhead appliance)

This guide is intended to be used together with the following documentation:

- *Steelhead Appliance Management Console User's Guide* (xx60)
- *Riverbed Command-Line Interface Reference Manual*

Note: This guide is specific to SteelHead running RiOS 9.0 and later. For RiOS 8.6 specific configuration please see the *SteelHead Path Selection to Zscaler with RiOS 8.6: Solution Guide*.

Audience

This guide is written for security and network administrators familiar with administering and managing switches, routers, firewalls, and SteelHead.

Document Conventions

This guide uses the following standard set of typographical conventions.

Convention	Meaning
italics	Within text, new terms, emphasized words, and REST API URIs appear in *italic* typeface.
boldface	Within text, CLI commands, CLI parameters, and REST API properties appear in **bold** typeface.

Courier	Code examples appears in Courier font:
	`amnesiac > enable`
	`amnesiac # configure terminal`

< >	Values that you specify appear in angle brackets: **interface <ipaddress>**
[ ]	Optional keywords or variables appear in brackets: **ntp peer <addr> [version <number>]**
{ }	Required keywords or variables appear in braces: **{delete <filename>}**
|	The pipe symbol represents a choice to select one keyword or variable to the left or right of the symbol. The keyword or variable can be either optional or required: **{delete <filename> | upload <filename>}**

Accessing Documentation and the Support Knowledge Base

For a complete list and the most current version of Riverbed documentation, visit the Riverbed Support Web site located at https://support.riverbed.com.

The Riverbed Knowledge Base is a database of known issues, how-to documents, system requirements, and common error messages. You can browse titles or search for keywords and strings.

To access the Riverbed Knowledge Base, log in to the Riverbed Support site located at

https://support.riverbed.com.

Contacting Riverbed

This section describes how to contact departments within Riverbed.

Internet

You can learn about Riverbed products at http://www.riverbed.com.

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.

Professional Services

Riverbed has a staff of professionals who can help you with installation, provisioning, network redesign, project management, custom designs, consolidation project design, and custom coded solutions. To contact Riverbed Professional Services, email proserve@riverbed.com or go to http://www.riverbed.com/services-training/Services-Training.html.

Documentation

The Riverbed Technical Marketing team continually strives to improve the quality and usability of Riverbed documentation. Riverbed appreciates any suggestions you might have about its online documentation or printed materials. Send documentation comments to tech-mktg@riverbed.com.

Chapter 1 Overview

Enterprises are increasingly using DSL or Cable internet connections at Remote and Branch Offices. These *direct to net* connections can be the primary source of connectivity at the branch or can supplement existing MPLS connections to make a hybrid network. Going direct to net at the branch provides a number of benefits:

- **Cost.** DSL/Cable internet connections are cheap compared to MPLS
- **Redundancy**. Cheap direct to net connections can be doubled up or used to supplement MPLS links to eliminate the single point of failure
- **Performance**. Internet traffic does not to be *backhauled* to the data center, saving bandwidth on the MPLS link and reducing overall latency

Going direct to net, however, bring up new security concerns. With a single MPLS link and a backhaul to the datacenter, internet access is centralized and a single secure web gateway (SWG) is enough to defend again internet-borne threats. With multiple points of entry into the corporate network, defending against threats becomes more complicated.

Deploying a secure web gateway at each branch office is possible but not ideal solution, it requires additional infrastructure to manage and maintain at each location. Zscaler and Riverbed offer a different approach to securing the branch using cloud based web security and path selection.

With Zscaler, there are no appliances that need to be deployed and maintained at branch offices. Zscaler is a cloud based secure web gateway built to protect users at the branch and mitigate business risk while reaping the benefits of mobility and public and private cloud computing.

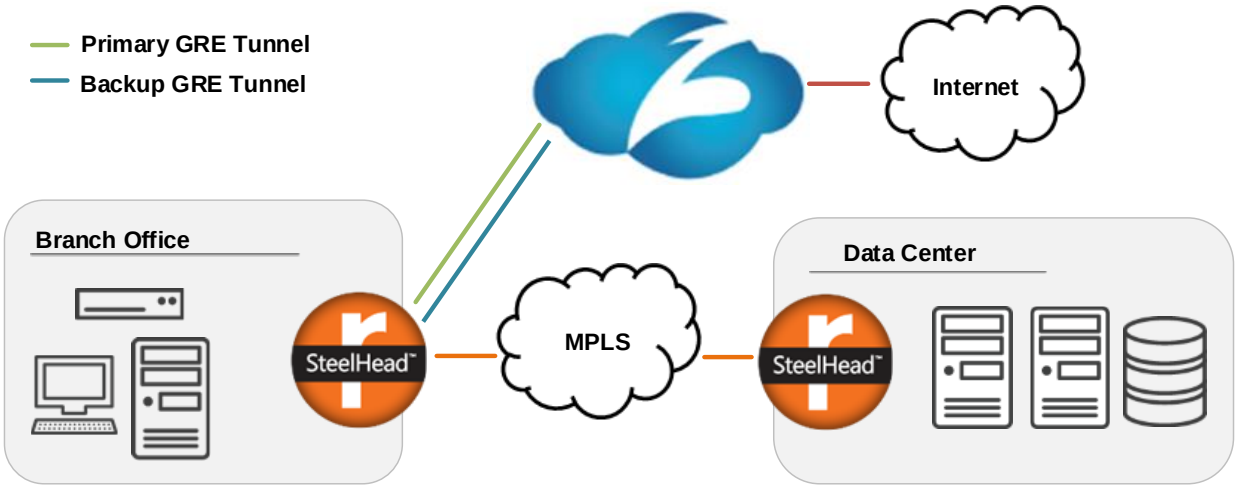
The SteelHead is able to GRE encapsulate and redirect traffic to Zscaler. GRE enables Layer 2 connectivity over a layer 3 network. The solution guide provides detailed steps on configuring the SteelHead to GRE encapsulate traffic to Zscaler.

This chapter includes the following sections:

System Architecture and Components

This section describes the system components and their roles.

Figure 1-1. Zscaler Deployment with SteelHead



The branch office in Figure 1-1 has an MPLS link as well as a direct internet link. Using path selection, the SteelHead in the branch office will GRE encapsulate and redirect all public web traffic to Zscaler.

Requirements

Requirement	Notes
Riverbed SteelHead with RiOS version 9.0 or later	GRE encapsulation with SteelHead was introduced in RiOS 8.6. This guide is specific to RiOS 9.0.
Zscaler Security as a Service platform	A subscription to Zscaler Security as a Service platform is required

Chapter 2 Deploying SteelHead Path Selection with Zscaler

This chapter describes the process and procedures for deploying SteelHead Path Selection with Zscaler at the branch office. It includes the following sections:

Prerequisites

Before you configure SteelHead Path Selection with Zscaler, ensure that the following steps have been completed:

- IP addresses for the primary and backup GRE tunnel to Zscaler. For the SteelHead in the branch office these will be the remote tunnel endpoints. This information is provided by Zscaler.
- The firewall or edge device in the branch must perform Static NAT for the SteelHead inpath IP address for the GRE tunnel to come up. GRE tunnels do not support NAT-T.
- The public facing IP Address must be provided to Zscaler.
- The inpath interface must be configured and enabled following the steps in the *Steelhead Installation and Configuration Guide*.

Note: SteelHead does not support internal, private IP addresses for the GRE tunnels. Therefore, Zscaler does not need to provide VIPs (virtual IP addresses) for use as the source and destination addresses inside the tunnel.

The SteelHead Path Selection with Zscaler Deployment Process

This section provides a broad outline of the process for deploying SteelHead Path Selection with Zscaler. The steps are listed in approximate order; dependencies are listed when required.

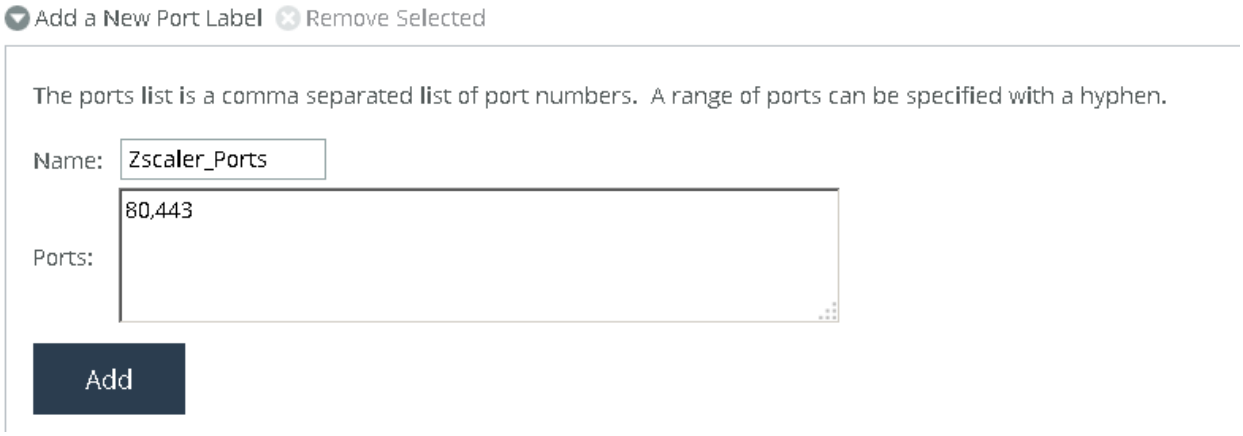
The steps are as follows:

Create Port Labels

This section describes how to create port labels for ports 80 and 443. The port label will be used later to define Zscaler as a custom application.

1. In the SteelHead Management Console go to **Networking -> App Definitions -> Port Labels**
2. Click on **Add a New Port Label**
3. Give the label a name, for example **Zscaler_Ports**
4. Enter **80, 443** in the **Ports** field.
5. Click **Add** to add the label and Save to save it

Figure 2-1 Port Label for Zscaler traffic

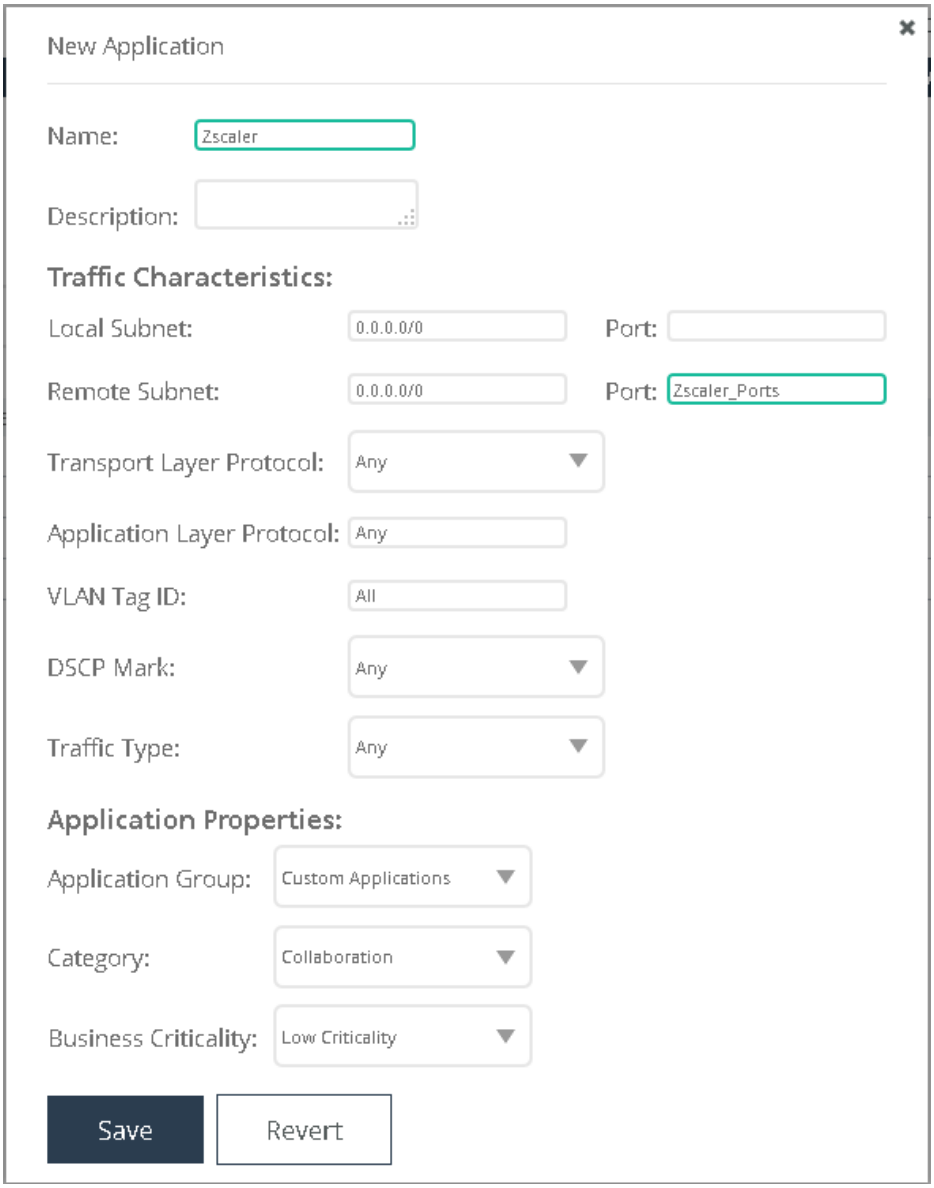


Create a Custom Application

This section describes how to create a custom application. The custom application will match all traffic destined for ports 80 and 443 using the label created in the previous section. The custom application will be used later to direct traffic via a GRE tunnel to Zscaler

1. In the SteelHead Management Console go to **Networking -> App Definitions -> Application**
2. Click on **Add**
3. Fill in the **Name** of the application (Zscaler in this example)
4. Fill in the **Remote Subnet Port** with the port label created in the previous step (*Zscaler_Ports* in this example)
5. Click **Save** to save the changes

Figure 2-2 Custom Application for Zscaler traffic

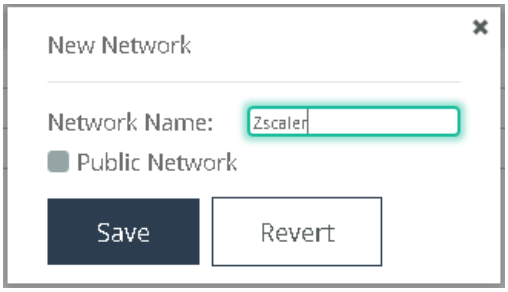


Create Zscaler Network

This section describes how to update the SteelHead topology to create a new network for Zscaler. This network will be used in subsequent steps.

1. In the SteelHead Management Console go to **Networking -> Topology -> Sites & Networks**
2. Under **Neworks** click on **Add a Network**
3. Under **Network Name** fill in *Zscaler*
4. Click **Save** to save the changes

Figure 2-3 Create a new network for Zscaler traffic

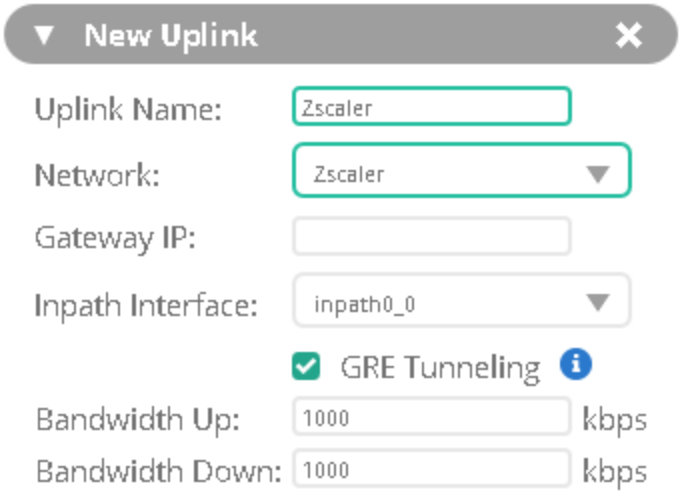


Add Zscaler Uplink to Local Site

This section describes how to add the Zscaler uplink to the *Local site*. This section uses the *Zscaler* network crated in the previous step.

1. In the SteelHead Management Console go to **Networking -> Topology -> Sites & Networks**
2. Under **Sites** click on **Edit** next to **Local (Local)**
3. In the **Edit a Site** menu click on **Add New Uplink** under **Uplinks**
4. Set the **Uplink Name** to *Zscaler*
5. In the **Network** drop down menu select **Zscaler**
6. Fill in the IP Address of your Internet Gateway in the Gateway IP field
7. Check the **GRE Tunneling** checkbox
8. Click **Save** to save the changes

Figure 2-4 Create a new uplink for Zscaler traffic

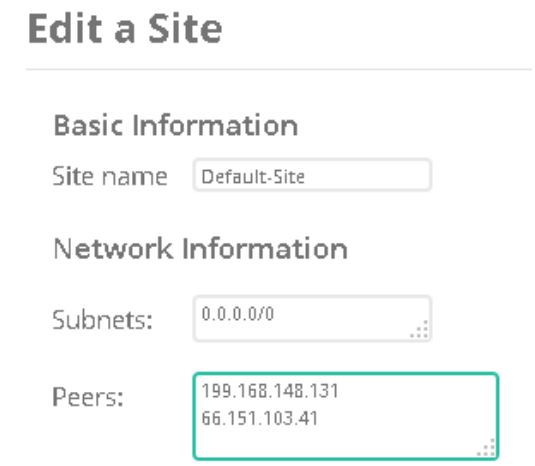

New Uplink
Uplink Name:
Zscaler
Network:
Zscaler
Gateway IP:
Inpath Interface:
inpath0_0
GRE Tunneling
Bandwidth Up:
1000
kbps
Bandwidth Down:
1000
kbps

Add GRE Tunnel Endpoints

This section describes how to add in the IP addresses for the GRE tunnel endpoints on the Zscaler side. These IPs will be provided by Zscaler.

1. In the SteelHead Management Console go to **Networking -> Topology -> Sites & Networks**
2. Under **Sites** click on **Edit** next to **Default-Site**
3. Under **Peers** fill in both the primary and backup GRE endpoints to Zscaler. The first address in the list will be the primary
4. Click on **Add New Uplink**
5. Set the **Uplink Name** to *Zscaler*
6. In the **Network** drop-down select **Zscaler**
7. Click **Save** to save the changes

Figure 2-5 Add GRE tunnel endpoints and new Zscaler uplink

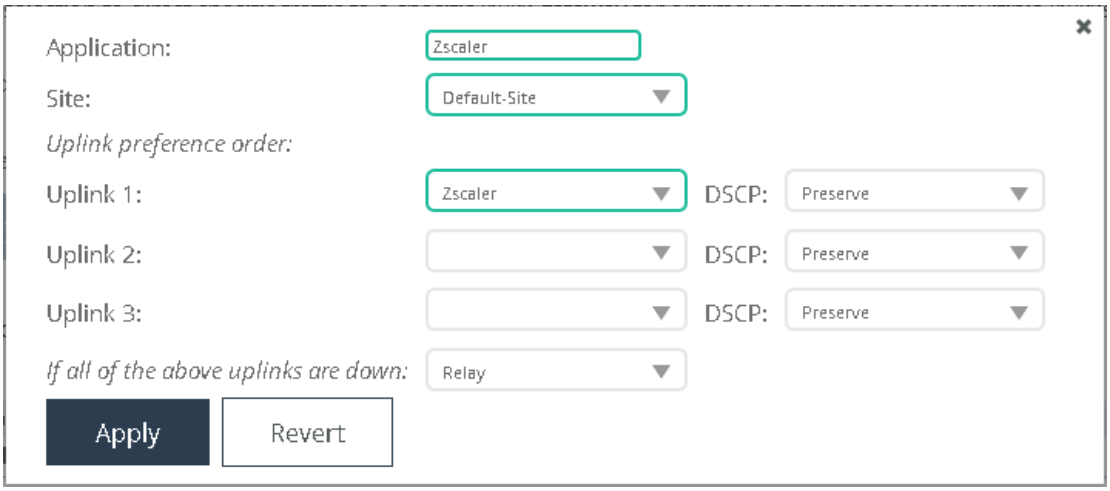


Configure Path Selection Settings

This section combines all the components configured in previous sections. This describes how to configure the SteelHead to GRE encapsulate all traffic on ports 80 and 443 to Zscaler.

1. In the SteelHead Management Console go to **Networking -> Network Services -> Path Selection**
2. Make sure the **Enable Path Selection** checkbox is checked. Click **Apply** to save changes if path selection was not enabled
3. Under **Path Selection Rules** click on **Add**
4. Set **Application** to *Zscaler*
5. Set **Site** to *Default-Site*
6. Set **Uplink 1** to *Zscaler*
7. Click on **Apply** to save the changes

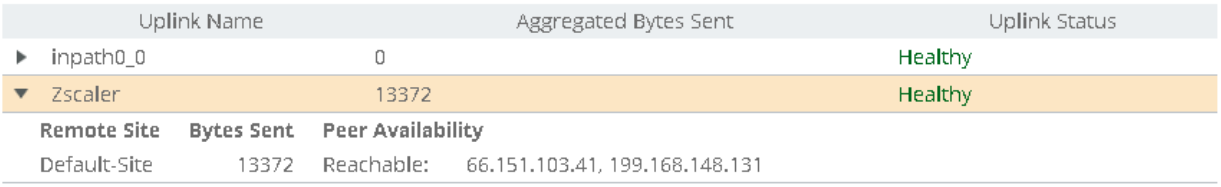
Figure 2-6 Add GRE tunnel endpoints and new Zscaler uplink



Verify GRE Tunnels to Zscaler are up

This section describes how to verify the GRE tunnels to Zscaler are up. In the SteelHead Management Console go to **Features -> Path Selection,** scroll down and expand the **Zscaler** uplink. The **Uplink Status** should be healthy and both peers should be **Reachable.**

Figure 2-7 Verify GRE tunnels to Zscaler are up



Verify GRE Encapsulation to Zscaler

GRE encapsulation to Zscaler can be verified using the *Zscaler Cloud Portal*. This section covers the steps to verify GRE encapsulation to Zscaler.

1. In the Zscaler Cloud Portal go to **Analytics -> Web Insights**
2. Under **Select Chart Type** click on **Logs**
3. Under **Choose a Timeframe** select **Last 5 Minutes**
4. From a client PC go to a website such as http://www.riverbed.com
5. In the Zscaler Cloud Portal click on **Apply Filters.** The website visited should show up in the list as in Figure 2-5 below

Figure 2-8 Zscaler log showing traffic passing through Zscaler

No.	Time	URL	Policy Action
1	Wednesday, July 16, 2014 10:26:46 AM	www.riverbed.com/	Allowed
2	Wednesday, July 16, 2014 10:26:47 AM	www.riverbed.com/includes/earnings.css?clear=4	Allowed
3	Wednesday, July 16, 2014 10:26:47 AM	www.riverbed.com/includes/riverbed-us.css?clear=5	Allowed
4	Wednesday, July 16, 2014 10:26:47 AM	www.riverbed.com/includes/riverbed.css?clear=460	Allowed
5	Wednesday, July 16, 2014 10:26:47 AM	www.riverbed.com/includes/riverbed_fonts.css	Allowed
6	Wednesday, July 16, 2014 10:26:47 AM	www.riverbed.com/includes/jquery.datepick.css	Allowed
7	Wednesday, July 16, 2014 10:26:47 AM	www.riverbed.com/includes/jquery.1.8.2.js	Allowed
8	Wednesday, July 16, 2014 10:26:47 AM	www.riverbed.com/includes/modernizr.foundation.js	Allowed
9	Wednesday, July 16, 2014 10:26:47 AM	www.riverbed.com/includes/jquery.flexslider-min.js?clear=Wed Jul 1...	Allowed
10	Wednesday, July 16, 2014 10:26:47 AM	www.riverbed.com/includes/jquery.blockui.js	Allowed
11	Wednesday, July 16, 2014 10:26:47 AM	www.riverbed.com/includes/validation.js?clear=Wed Jul 16 10:26:46 ...	Allowed
12	Wednesday, July 16, 2014 10:26:47 AM	www.riverbed.com/includes/foundation.js?clear=Wed Jul 16 10:26:46...	Allowed
13	Wednesday, July 16, 2014 10:26:47 AM	www.riverbed.com/includes/foundation.css	Allowed
14	Wednesday, July 16, 2014 10:26:48 AM	www.riverbed.com/includes/cookies.js	Allowed
15	Wednesday, July 16, 2014 10:26:48 AM	www.riverbed.com/includes/jquery.ba-bbq.js?clear=1	Allowed
16	Wednesday, July 16, 2014 10:26:48 AM	www.riverbed.com/includes/embed.js	Allowed

Appendix A Additional Resources

This appendix describes resources that supplement the information in this guide. It includes the following resources:

- SteelHead Management Console User's Guide
- SteelHead Appliance Deployment Guide
- RiOS Technical Overview
- SteelHead Installation and Configuration Guide

SteelHead Management Console User's Guide

The *SteelHead Management Console User's Guide* describes how to configure and monitor SteelHead using the Management Console. It is available at https://support.riverbed.com/content/support/software/steelhead/appliance.html

SteelHead Appliance Deployment Guide

The *SteelHead Appliance Deployment Guide* describes why and how to configure the SteelHead appliance in complex in-path and out-of-path deployments such as failover, multiple routing points, static clusters, connection forwarding, WCCP, Layer-4, PBR, and PFS. It is available at: https://support.riverbed.com/content/support/software/steelhead/appliance.html

RiOS Technical Overview

The Riverbed Optimization System (RiOS) is the software that powers Riverbed's unique award-winning line of SteelHead application acceleration appliances. RiOS is based on patented technologies that solve a range of problems affecting wide area networks (WANs) and application performance. The RiOS Technical Overview discusses how the SteelHead is able to improve application performance. It is available at https://splash.riverbed.com/docs/DOC-1198

SteelHead Installation and Configuration Guide

The Steelhead Appliance Installation and Configuration Guide describes how to install and configure the Steelhead appliance. It also describes the status lights and specifications for the system. It is available at: https://support.riverbed.com/content/support/software/steelhead/appliance.html