Securing your network with Riverbed SteelConnect and Zscaler

The combination of Riverbed’s SD-WAN solution SteelConnect, with Zscaler’s cloud security platform provides a secure, scalable, and agile network architecture that simplifies branch operations—empowering IT to react quickly to evolving business needs while ensuring stringent security postures across the enterprise.

Riverbed SteelConnect is a revolutionary SD-WAN solution that provides an intelligent and intuitive approach to designing, deploying, and managing distributed networks for today’s cloud-centric world. The Zscaler Cloud Security Platform delivers superior security without the cost and complexity of on-premises security appliances. Zscaler provides security as a cloud service, with Cloud Sandboxing, Cloud Firewall, Data Loss Prevention (DLP), and more.

The native integration of Zscaler with SteelConnect provides significant benefits:

- **Easy configuration** - Organizations with mobile users and numerous branch offices can use Zscaler instead of deploying an advanced firewall at each branch office. SteelConnect reduces the complexity of connecting to the cloud security service to a few simple clicks. A SteelConnect gateway automatically connects with a Zscaler Enforcement Node (ZEN), creating a secure IPsec VPN tunnel between the Zscaler cloud and the SteelConnect gateways at sites.

- **Flexibility** - After establishing a secure IPsec tunnel between the Zscaler cloud and SteelConnect gateways, you have the flexibility to configure Zscaler as an internet breakout preference at the organization, site, or zone level or as a breakout preference in traffic rules.

- **Robustness** - If the primary IPsec VPN tunnel or an intermediate connection goes down, all traffic is rerouted through the backup IPsec tunnel to a secondary ZEN in approximately 60 seconds.

- **Visibility** - The SCM troubleshooting page provides visibility into tunnel status.

- **Automatic tunnel optimization** - SteelConnect automatically optimizes tunnel latency by choosing the best ZEN for each site.

This document lists steps on how to configure Riverbed SteelConnect Manager (SCM) and Zscaler to connect a SteelConnect gateway with its closest ZEN via a secure IPSec VPN tunnel.
Figure 1. IPSec tunnel between a SteelConnect gateway at a branch site and the Zscaler cloud

**Before you Begin**

Before configuring Zscaler, make sure you:

- Have a Riverbed SteelConnect Manager (SCM) subscription running version 2.9 or later.
- Have a Zscaler Security as a Service platform subscription. The SteelConnect integration with Zscaler supports Zscaler Internet Access (ZIA).
- Plan the level at which to configure internet break out. For example, you might want to fall back to direct breakout if Zscaler is unavailable, or you might want to break traffic out at the organization or site level using a traffic rule.
- Decide in which order the breakout should occur: Zscaler, Zscaler and then internet, or internet and then Zscaler. Are there sites that require special routing such as guest zones? Do you need to break out the data center sites directly?

**Configuring SCM**

SteelConnect automatically routes traffic destined for the internet to the nearest ZEN for minimum latency, and it enforces traffic policies configured on Zscaler. Here are some key Zscaler components:

- Each customer account is associated with one Zscaler cloud.
- Each cloud consists of ZENs in various geographic regions.
- ZENs act as proxy servers that do traffic analysis and filtering.

Automatic ZEN assignment is the default, recommended method; however, you can manually choose a primary ZEN and a secondary ZEN for each site. For example, you might need to select ZENs located in a country for certain geographic requirements and regulations, or for users who need to see localized content.

**Selecting a cloud:**

The first step is to select an active cloud. To select a cloud:

1. On SCM, under Network Design, Zscaler, select a cloud from the drop-down Active Cloud menu.
By default, SteelConnect performs automatic ZEN selection. After you select a cloud:

- SteelConnect automatically enables Zcaler and sends the list of available ZENs to all gateways.
- The ZENs belonging to the selected cloud appear.
- SteelConnect creates a Zcaler WAN for the organization.
- The gateway measures latency to all the ZENs. SteelConnect selects the two ZENs with the lowest latency.
- SteelConnect pairs the ZENs with the sites in the organization.
- Each gateway establishes IPsec VPN tunnels to its primary and secondary ZENs through an internet connection to the assigned ZEN pairs for the sites. Automatic ZEN selection and tunnel creation finish in approximately two minutes.
- If the primary IPsec VPN tunnel or an intermediate connection goes down, all traffic is rerouted through the backup IPsec tunnel to the secondary ZEN in approximately 60 seconds. It can take up to 120 seconds.
Figure 3. ZEN selection

Viewing the ZEN selections

You can view the ZEN selection pairings of your IPsec VPN tunnels in SCM. To view the ZEN selection pairings for the site:

1. In SCM, choose Network Design > Zcaler.
2. Click the site.

Setting the ZENs manually

Automatic ZEN assignment is the default and the recommended method; however, you can manually choose a primary ZEN and a secondary ZEN for each site.

You can use any ZEN in the same cloud. All ZENs in a cloud share the same configuration. For some ZENs, a regional surcharge may apply. SteelConnect doesn’t support ZENs with a regional surcharge. To manually set the ZENs for the site:

1. Choose Network Design > Sites.
2. Select a site. Click on the Zcaler tab.
4. Click the search selector and select a primary and secondary ZEN.

5. Click Submit.

SCM shows all VPN configuration details under ZEN status as soon as the system creates the third-party VPN connection. The status also reports any tunnel latency.

You can disable Zscaler on a per-site basis. To enable or disable a ZEN from the active cloud, next to the ZEN, click On or Off.

**Configuring Zscaler**

**White listing the VPN credential domain**

The next step is to ask Zscaler support to white list your VPN credential domain for successful authentication. After your credentials are white listed, you need to add the credentials to the Zscaler admin portal and then link the credentials to a location.

To white list the VPN credential domain

1. In SCM, choose Network Design > Zscaler.
2. Click Download Config.

A dialog displays your VPN credential domain.

![Image](image-url)

**Figure 4. Download Zscaler configuration**

You’ll need this VPN credential domain for the Zscaler support representative. The next step is to ask Zscaler support to white list the credential. Don’t click Download yet. You’ll do that in Step 6.

3. In Zscaler, click the Question mark icon at the top of the Zscaler admin portal.

![Image](image-url)

**Figure 5. Question mark icon**

4. Click Submit a ticket.
5. Ask Zscaler support to white list the VPN domain credential for the organization. You only need to add the domain once for the organization. It typically takes about five minutes to receive a response from Zscaler support.

6. After receiving a response from Zscaler support, return to the SCM Zscaler Configuration dialog and click Download. The configuration file downloads.

**To add the VPN credentials to the admin portal**

1. In Zscaler, choose Administration > Resources > VPN Credentials.
2. Click **Import**.
3. Click **Apply Changes** to store the changes locally.

After adding the VPN credentials to the Zscaler admin portal, the next step is to link the credentials to a location. Linking the VPN credentials to a location is required. Zscaler ignores VPN credentials that are not linked to a location.

You can link multiple credentials to one location to speed up configuration of multiple sites.

**To link the VPN credentials to a location**

1. Choose Administration > VPN Credentials > Locations.
2. Click **Add**.
3. Enter the name, state/province, country, and time zone for the branch office location.
4. Click the down arrow beside VPN Credentials and select the credentials you created to associate with this branch location.
5. Click **Save** to store the changes locally.
6. Click **Activate changes**.

This action pushes the configuration changes to the Central Authority (CA) immediately. The CA serves as the central repository for policies and configuration settings. The ZENs retrieve the policies from the CA and apply them to your organization's internet traffic. Because all policies are centrally stored on the CA, the latest policies are always applied, no matter which ZEN your users connect to.

**Setting Traffic Path Rules**

The final step is to steer traffic through Zscaler using internet breakout preferences and/or traffic rules. When Zscaler is enabled, SCM creates a Zscaler WAN. You can configure the Zscaler WAN as the default internet breakout (as the organization's default, as the site's default, or for specific zones) under Organization > Networking Defaults > Internet Breakout Preference.
Zscaler can also be used as a breakout preference for particular sites, VLANs, user groups, individual users, or select applications using Traffic Path Rules. Traffic rules determine which traffic is sent to the internet breakout or other VPNs. For example, you could send all trusted SaaS application or Voice over IP (VoIP) traffic direct-to-net and all other Internet traffic to the Zscaler WAN for additional scrubbing. As a secondary preference, you can also choose to backhaul traffic to the data center via the MPLS link if available.
Viewing Zscaler tunnels

Lastly, you can check the status of Zscaler tunnels in SCM. To view Zscaler tunnels:

1. Choose Visibility > Troubleshooting.
2. Select a site. The Tunnels tab shows the tunnel status for each site.

![Zscaler tunnel status](image)

**Figure 8. Zscaler tunnel status**

To verify your traffic is going through a Zscaler node, open a web browser on a client and visit: ip.zscaler.com

You should see a message confirming that the client is going out to the Internet via a Zscaler node as shown below:

![Confirmation from ip.zscaler.com](image)

**Figure 9. Confirmation from ip.zscaler.com that traffic to the Internet goes through the Zscaler node**

**Conclusion**

Riverbed and Zscaler make it easy to migrate from a hub-and-spoke, datacenter-focused security infrastructure to a software-defined, Internet-only branch architecture based on secure, local Internet breakouts. Riverbed SteelConnect’s native integration with Zscaler enables enterprises to send traffic direct-to-net securely to provide better end-user experience, business agility and lower costs. The combination of Riverbed SteelConnect and Zscaler delivers an entirely cloud-controlled solution that eliminates management complexity and cost and the compromises that often exist between security and business goals of and enterprise for performance and agility and scalability.
About Zscaler
Zscaler enables the world’s leading organizations to securely transform their networks and applications for a mobile and cloud-first world. Its flagship services, Zscaler Internet Access and Zscaler Private Access, create fast, secure connections between users and applications, regardless of device, location, or network. Zscaler services are 100% cloud delivered and offer the simplicity, enhanced security, and improved user experience that traditional appliances or hybrid solutions are unable to match. Used in more than 185 countries, Zscaler operates a massive, global cloud security platform that protects thousands of enterprises and government agencies from cyberattacks and data loss. Learn more at zscaler.com.

About Riverbed
Riverbed, at more than $1 billion in annual revenue, is the leader in application performance infrastructure, delivering the most complete platform for the hybrid enterprise to ensure applications perform as expected, data is always available when needed, and performance issues can be proactively detected and resolved before impacting business performance. Riverbed enables hybrid enterprises to transform application performance into a competitive advantage by maximizing employee productivity and leveraging IT to create new forms of operational agility. Riverbed’s 27,000+ customers include 97% of the Fortune 100 and 98% of the Forbes Global 100. Learn more at Riverbed.com.