

FEATURE BRIEF: SSL Acceleration

A breakthrough in both speed and security, Riverbed's new SSL acceleration gives true data streamlining, transport streamlining, and application streamlining for SSL-encrypted traffic. Unlike any competitive system, Steelheads use a simple, sound, proven trust model like an SSL offload device – but deliver performance far beyond what any SSL offload system can provide

Securing the End-to-end Network Path: Riverbed's New Feature Extends Capabilities for Secure Application Acceleration

Riverbed Steelhead appliances have provided award-winning performance for more than 1700 customers since they were first delivered in May 2004. With the release of RiOS 4.0, Riverbed offers a new, powerful, patent-pending feature: acceleration of SSL traffic. With the latest version of Riverbed's award-winning software, Steelhead appliances can now accelerate data transfers that are encrypted using SSL. Steelhead appliances can do so by applying all of the same optimizations they apply to unencrypted traffic. Remarkably, Steelheads accomplish this while maintaining end-to-end security and maintaining the trust model that enterprises require. This ground-breaking approach is the first by any vendor that can really allow organizations to have the best of both worlds: end-to-end secure traffic that is accelerated to LAN-like performance over the WAN.

THE SECURITY VS. ACCELERATION TRADEOFF

As data security has become a more important concern for organizations, they have looked for ways to lock down their data and ensure its safety. Some have consolidated servers to fewer locations. Others have invested more in data center replication and security. Many of these same companies are adopting policies that mandate migration to SSL transports to ensure that data in flight is always protected.

Organizations enjoy the security that SSL provides – and many would like to adopt SSL for even more of their applications – but there has been a difficult tradeoff to make. Until now, organizations could do very little to truly accelerate the performance of these encrypted applications while still maintaining the security of the data.

Straightforward solutions to symmetric secure traffic acceleration (that is, a solution where one appliance is in the data center and then an additional appliance is in the branch office) often look good at first glance, but turn out to be unusable in practice. These approaches generally introduce security issues, use inferior acceleration techniques, or both. The security issues arise in the area that goes by the name of "key management:" the weak link in an encryption system like SSL is typically protecting the private key information.

All the valuable privacy properties of SSL actually depend on the "private" key of a private/public key pair actually being kept private. In theory, it's easy to keep a key private; but in practical use in data communication systems, you have to find ways of storing that private key on a machine. The more times you have to handle a key, and the more places you have to store the key, the higher the risk of an inadvertent disclosure of the key.

Unfortunately, such a single disclosure, exploited by an attacker, completely destroys the security of all communication that was previously protected by that key. So it makes no difference if a private key was successfully handled 500 times in configuring 500 different sites without disclosing the key; a disclosure at the 501st site undoes all the work and means that all communication across the enterprise using that key is now insecure.

This challenge of key management explains why it's not sensible to make a symmetric acceleration device support SSL by simply putting the origin server's private key information onto every device. Such a configuration would allow apparent protection of traffic, because every device would have the key information necessary to decrypt and examine the interactions between client and server, and to continue to follow those interactions even as new session keys were negotiated. But the actual security of such a system would be quite low. Especially in organizations with a large number of branches, there would be a correspondingly large increase in the chance of exposure of the private key of each server whose traffic should be optimized.

For most organizations, an acceleration approach that scatters private keys throughout branches is not a reasonable trade-off: even if performance is substantially improved, the associated risks are too high. Instead, many have settled for only using an SSL-offload device or application front-end (AFE). Such systems are used in front of SSL-enabled web



WAN Optimization – Riverbed RiOS 3.0



FEATURE BRIEF: SSL Acceleration

RIVERBED AND SECURE ACCELERATION

Strictly speaking, SSL acceleration is not Riverbed's first feature to support secure acceleration.

Because Steelheads use ordinary TCP for communication, even the earliest models supported secure acceleration by using the customer's existing VPN infrastructure – with no configuration or tunnel setup required. Later improvements added Steelhead-based IPSec authentication and encryption to further protect optimized traffic across the WAN. The net result was a system that was powerful in its capabilities for speeding up performance and protecting traffic across the WAN.

However, there was still a gap: the one area that Steelheads couldn't help was network traffic that needed to be protected on the LAN. Enterprise applications dealing with sensitive data typically use SSL to protect the data traveling between client and server. The SSL encryption hides the data from spies or attackers, but also means that Steelheads are unable to examine the traffic to optimize it. So until recently, network architects have faced an unappealing tradeoff between security on the LAN and acceleration: SSL-encrypted traffic could be protected but slow, while unencrypted traffic could be accelerated but unprotected. With SSL acceleration, Riverbed eliminates this tradeoff.

servers. They offload some of the CPU costs of SSL from the server, and some also provide forms of filtering or caching, or rudimentary compression schemes supported by web browsers. But such "acceleration" is primarily a technique for allowing the server to serve more. While it can be valuable for scaling up servers; it doesn't address bandwidth issues, latency, or protocol chattiness with anything approaching the effectiveness of a double-ended accelerator system. These double-ended approaches are what enterprises have come to expect from a true acceleration solution. While a single-ended offload device is often better than nothing, any such system falls far short of what is desirable for SSL acceleration: accelerating SSL with the same impressive capabilities that are already deployed in hundreds of customer networks to accelerate unencrypted TCP traffic.

THE RIVERBED ADVANTAGE: BOTH SECURITY AND ACCELERATION

Riverbed's new SSL acceleration architecture allows Steelhead appliances to apply the optimizations that they can currently apply to ordinary unencrypted TCP traffic. In contrast to only using SSL-offload devices, Riverbed has the power that comes from using an appliance on both sides of the WAN: not mere caching or SSL offload, but true data streamlining, transport streamlining, and application streamlining capabilities that can deliver from 5 to 50 times, and sometimes up to 100 times faster application performance – even for SSL-encrypted applications.

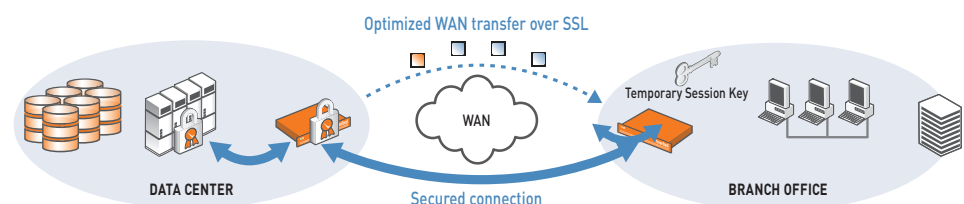
In contrast to other competitive systems that claim SSL acceleration but have unworkable approaches to key management, Riverbed combines powerful symmetric acceleration with a trust model roughly analogous to an SSL offload device. Private keys need only be configured on the server side of connections (typically appliances in a data center) and branch appliances never hold private key information – not even in memory! In contrast to still other competitive systems, Riverbed does not require the subversion of all SSL traffic through faked certificates, nor the deployment of a private Certificate Authority (CA), nor the installation of new root certificates on clients. Instead, Riverbed works within your existing certificate and key infrastructure – whether you use certificates from a private CA, a public CA, or even self-signing.

HOW IT WORKS

Riverbed's approach starts with Steelheads that have a configured trust relationship, so they can exchange information securely over an SSL connection. As with all previous versions of RiOS, each client uses unchanged server addresses and each server uses unchanged client addresses; no application changes or explicit proxy configuration is required. What is new is that Riverbed splits up the SSL "handshake," the sequence of message exchanges at the start of an SSL connection.

In an ordinary SSL handshake, the client and server first establish identity using public-key cryptography, then negotiate a symmetric "session" key to be used for data transfer. When using Riverbed's SSL acceleration, the initial SSL message exchanges take place between the client and the server-side Steelhead appliance. Then the server-side Steelhead sets up a connection to the server, to ensure that the service requested by the client is available. In the last part of the handshake sequence, a Steelhead-to-Steelhead process ensures that both appliances (client-side and server-side) know the session key.

The net effect is that the client's SSL connection logically terminates at the server but physically terminates at the client-side Steelhead – just as is true for logical vs. physical unencrypted TCP connections. And just as the Steelhead-to-Steelhead TCP connection over the WAN may use a better TCP implementation than the ones used by client or server, the Steelhead-to-Steelhead connection may be configured to use better ciphers and protocols than the client and server would normally use.



FEATURE BRIEF: SSL Acceleration

SSL: THE KEY INFORMATION

SSL depends on both public-key cryptography and symmetric-key cryptography.

Public-key cryptography uses two different keys: one is made widely available (public) while the other is kept secret (private). Public-key cryptography makes it possible for one user to receive private messages from an unlimited number of other users, or to publish a signed message that is verifiable as authentic for an unlimited number of users.

In contrast, symmetric-key cryptography uses a single key, and that shared key must be kept private by the communicating parties: as soon as any third party knows the shared key, that third party can read any message or fake any message from either party, so both privacy and authentication are lost.

It is much easier to manage keys well in a public-key system, but the computation required to do public-key cryptography is expensive – too expensive to use for large amounts of data over long periods of time.

SSL strikes a great compromise: public-key cryptography is used to negotiate a short-lived symmetric key. This means that efficient symmetric-key cryptography can be used for data transfer, while easy-to-manage public keys can be used for establishing identity – ensuring that the communicating parties really are who they claim to be.

FLEXIBLE CONTROL

As with other Riverbed optimizations, the choice of SSL optimization with SDR and/or LZ can be made based on any combination of

- source address & subnet;
- source port;
- destination address & subnet;
- destination port; and/or
- VLAN number

DESIGNED FOR REAL-WORLD DEPLOYMENT

Riverbed has worked with large enterprise design partners to ensure that SSL acceleration delivers real benefits in real-world deployments:

- Cryptographic information is kept in a separate, encrypted store on the disk.
- Built-in support for popular Certificate Authorities (CAs) such as Verisign, Thawte, Entrust, and GlobalSign. In addition, Steelhead appliances allow the installation of other commercial or privately-operated CAs.
- Import of existing server certificates and keys in PEM, PKCS12, or DER formats. Steelhead appliances also support the generation of new keys and self-signed certificates.
- Separate control of cipher suites for client connections, server connections, and peer connections.
- Server configurations (including keys and certificates) can be bulk-exported from or bulk-imported to the server-side Steelhead appliance.
- New Central Management Console (CMC) features streamline setup of Steelhead trust relationships.

BREADTH AND FLEXIBILITY

Just as SSL is a general-purpose layer that can secure a variety of application protocols, Riverbed's SSL acceleration is designed as an application-independent foundation. Although the most common use of SSL acceleration is for HTTPS, all of the Steelhead appliance's Data Streamlining and Application Streamlining mechanisms can be used on any SSL traffic that is "unlocked" for optimization.

Riverbed has also designed this patent-pending approach with the ability to enable IT administrators to choose the appropriate level of security for their organization. RiOS supports the use of SSL interception with disk-based Data Streamlining (Riverbed's patented Scalable Data Referencing, SDR) or diskless Data Streamlining (conventional LZ compression). Together with Riverbed's previous ability to optimize ordinary TCP or bypass SSL traffic entirely, Riverbed offers a full spectrum of combinations of security and performance:



ENABLING AN EVEN TIGHTER SECURITY MODEL FOR TODAY'S ENTERPRISES

This powerful form of SSL acceleration now gives enterprises new, better choices in the security vs. acceleration tradeoff. With Riverbed's approach to end-to-end secure traffic acceleration, enterprises may choose to migrate more of their applications to SSL-encrypted protocols to give them the data security they are looking for. With Riverbed, they can be assured that their distributed workforce can still access the information they need at LAN-like speeds, no matter where in the world their office is located.

While other vendors may claim some similar-sounding features, only Riverbed Steelhead appliances combine this exclusive approach to secure traffic acceleration with the widest set of application-specific optimizations, the largest deployments, the easiest installation, the broadest choice of models, and the most powerful collection of high-availability features. With this combination of market-leading functionality, Riverbed is truly enabling IT infrastructure to meet the needs of today's changing environment.

Riverbed Technology, Inc.
199 Fremont Street
San Francisco, CA 94105
Tel: +1 415 247 8800
Fax: +1 415 247 8801
www.riverbed.com

Riverbed Technology Ltd.
1, The Courtyard, Eastern Road
Bracknell
Berkshire RG12 2XB
United Kingdom
Tel: +44 1344 354 910

Riverbed Technology Pte. Ltd.
350 Orchard Road #21-01/03
Shaw House
Singapore 238868
Tel: +65 68328082

Riverbed Technology K.K.
Shiba-Koen Plaza Building 9F
3-6-9, Shiba, Minato-ku
Tokyo, Japan 105-0014
Tel: +81 3 5419 1990