

McAfee Web Gateway for Riverbed

Web 2.0 security combined with WAN optimization

McAfee Web Gateway for Riverbed Features

Security

- Proactive anti-malware protection
- McAfee anti-virus with cloud-based file reputation
- Advanced web filtering with web reputation and geo-location
- Deep content inspection, including SSL traffic

Control

- Inbound/outbound filtering
- Granular application control
- Powerful policy engine
- Prevent data loss
- Extensive reporting/auditing

Performance

- Robust proxy/cache
- Enterprise scalability
- Manage multiple web security components

As workers become increasingly distributed, IT infrastructure is rapidly consolidating. The accelerated adoption of virtualization technologies has now made cloud computing a viable and increasingly compelling option for many enterprises (public, private, hybrid). Along with this trend towards the “virtual data center,” it’s no longer practical or affordable to simply backhaul all branch office traffic back to a central data center via dedicated WAN circuits and leased lines. Branch offices are rapidly adopting lower-cost, reliable direct Internet connections to access their data center and cloud-based services. The challenge then becomes ensuring that this new distributed network architecture delivers the same or an even greater level of availability, performance, and security as before.

To solve these challenges, McAfee and Riverbed have partnered to deliver industry-leading WAN optimization and branch office web security on a single device: the Riverbed Steelhead Appliance. The solution takes advantage of advanced technologies offered by both companies—from the McAfee® Web Gateway appliance and Riverbed WAN optimization products. McAfee Web Gateway runs on the Riverbed Services Platform (RSP), which is a virtualized, extensible data services platform that allows customers to deploy edge services that formerly required dedicated servers as virtual appliances. Customers can deploy the McAfee Web Gateway for Riverbed software directly on Riverbed Steelhead Appliances to further minimize the hardware infrastructure footprint at the branch office, reducing operational overhead.

The Web 2.0 Paradox

Organizations can do more over the web today than ever before. Often referred to as Web 2.0, today’s web offers a dynamic, real-time user experience. Static information has given way to social networking sites, blogs, wikis, RSS feeds, interactive applications, and user-generated content. Enterprises are taking advantage of these innovative capabilities to do business in more efficient, collaborative ways. As Web 2.0 application use and sophistication increases, so too does the need for flexible access coupled with Web 2.0-ready security because even seemingly “safe” sites can be targeted for malware distribution. And, as organizations consolidate their IT infrastructure and move data farther from users, the response time of business-critical applications can be negatively impacted.



Figure 1. Comprehensive Web 2.0 security in a single package.

McAfee Web Gateway for Riverbed Steelhead System Requirements

- Steelhead 1050 and 2050 appliances
- Riverbed Optimization System (RiOS) version 6.0 or later
- RSP version 6.0 or later, installed and licensed
- Available RSP slot
- 35 GB of free disk space
- 2 GB of free memory
- Supports up to 500 users in explicit proxy mode

Complete Inbound and Outbound Protection

McAfee Web Gateway delivers comprehensive security for all aspects of Web 2.0 traffic. For user-initiated web requests, McAfee Web Gateway first enforces an organization’s Internet use policy. For all allowed traffic, it uses local and global techniques to analyze the nature and intent of all content and active code entering the network via the requested web pages, providing immediate protection against malware and other hidden threats. And, unlike basic packet inspection techniques, McAfee Web Gateway can even examine SSL traffic to provide in-depth protection against malicious code that has been disguised through encryption.

To secure outbound traffic, McAfee Web Gateway scans user-generated content on all key web protocols—including HTTP, HTTPS, and FTP—and protects against loss of confidential information and other threats leaking from the organization through social media, blogs, and other avenues. McAfee Web Gateway also safeguards against unauthorized data leaving the organization through “bot-infected” machines attempting to phone home or transmit sensitive data.

McAfee Global Threat Intelligence™ powers McAfee Web Gateway and its web reputation technology. This technology creates a profile

of all Internet entities based on hundreds of attributes gathered from the massive, global data collection capabilities of McAfee Labs™. It then assigns a reputation score based on the security risk posed, enabling administrators to apply very granular rules about what to permit or deny. McAfee Web Gateway offers expanded cloud-based reputation capabilities that now include geo-location, enabling geographic visibility and policy management based on the web traffic’s originating country.

Key Advantages

- Reducing total cost of ownership:
 - » Branch office box consolidation to deliver lower capital and operating expenditures
- Reducing WAN costs with secure deployment flexibility:
 - » Use low-cost Internet connections with split tunneling deployments
 - » Secure both corporate-bound and Internet-bound applications
- Improving security posture:
 - » Predictive, proactive, real-time protection blocks malware
 - » Fine-grained control and advanced security combine to enable safe, productive Web 2.0 access

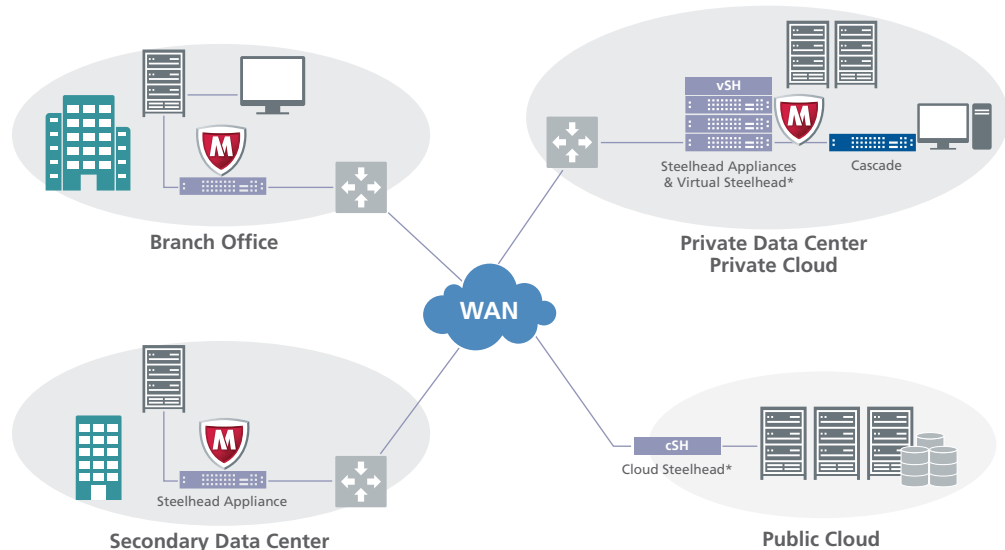


Figure 2. Sample deployment of McAfee Web Gateway for Riverbed.

