riverbed

SOLUTION BRIEF

Monitoring Remote Work and SSE Environments

The addition of Riverbed® Aternity endpoint data to Riverbed® IQ Unified Observability enables networking teams to monitor two new environments: Remote work and Secure Service Edge (SSE).

NetOps Responsible for Access and Performance Issues

When employees work in a traditional office environment, the network team is responsible for application access and delivery. The network team identifies issues where employees cannot access applications, or application performance is degraded due to network performance problems.

In remote work environments, the responsibility of identifying and troubleshooting access and performance issues still resides with the network team, but there are growing blind spots to accomplishing this task: remote workers transit non-enterprise infrastructure that is opaque to network teams.

Early remote environments relied on Virtual Private Networks (VPNs) to connect remote workers to the enterprise architecture. Today, it is evolving to a Secure Service Edge (SSE) approach that secures service access to users wherever they are located. The evolution to SSE provides a complete solution for securely connecting workers in cloud and multi-site environments, but the resulting secure network perimeter is tunneled and therefore less transparent to network team for performance monitoring.

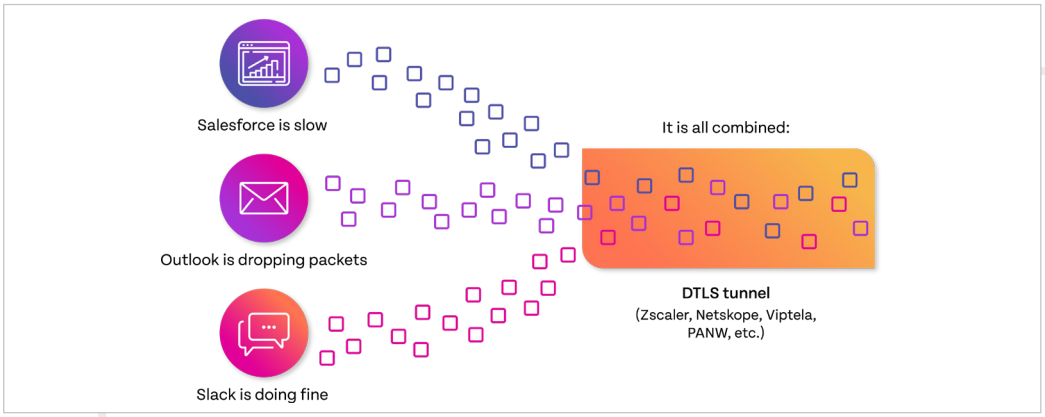

Figure 1: The problem with monitoring tunnels is that once the data reaches the tunnel it gets combined with all the other traffic and NetOps loses most of their traditional visibility.

Environmental Challenges

In modern remote work environments, it's common to have three different routing options for traffic: direct to internet, corporate VPN, and a Cloud Access Security Broker (CASB) with tunneled traffic. There are often routing rules in place where business applications use one route (such as the CASB) and other applications go direct to internet. The routing or tunnel used can have a significant impact on application performance / end user experience.

Below is more detail on the common methods used to support remote workers:

CASBs

Although widely adopted, SSE/CASBs create a bottleneck for performance visibility while optimizing for security. SSE/CASBs are often implemented by the security team, and it makes it more difficult for NetOps to troubleshoot as tunnels reduce visibility and add complexity. In a few ad hoc tests, CASB bandwidth can be as low as 3Mbps and there is added security scanning time as an additional slowdown.

Multiple Gateways and VPNs

There are often multiple gateways being used by each type of CASB. For example, users in the northeast United States may have CASB traffic tunneled to gateway X, while users in central US are connecting to gateway Y. If only one gateway is causing problems, it's difficult to determine which is causing the issue. This also applies to corporate VPNs; it's often difficult to determine which VPN is problematic.

Virtual Desktops

When using virtual desktops, remote user traffic may have an additional routing step of first going to a hosted virtual desktop app, which can be hosted in a SaaS environment or the data center. The data is then routed to the specific application that the user is trying to access. This routing adds more complexity and more possible points of failure to investigate.

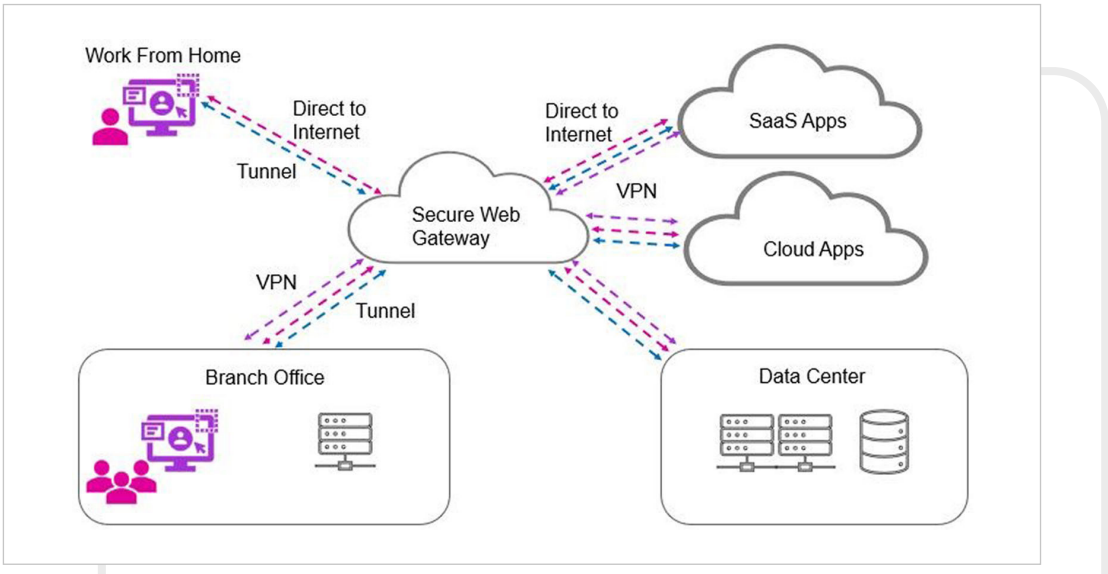

Figure 2: In today's modern IT environments, it's common to have three different routing options: direct to internet, VPN, and CASB with tunneled traffic, which has a significant impact on what NetOps teams can monitor.

Remote Work

In a remote work environment, there may be users in a general geographic area that are having issues due to an ISP or CASB gateway. It's not easy to identify the specific site or location having the problem.

Additionally, remote workers are responsible for their home network. Variables such as poor WIFI, ISP outage, or congestion on the home network are an additional challenge when trying to identify root cause.

Riverbed IQ Solution

Riverbed IQ leverages network performance and end user experience metrics plus advanced logic to provide much needed visibility into hybrid work and SSE visibility. This visibility helps network teams monitor and troubleshoot network-related access and performance issues. When application performance issues occur, Riverbed IQ surfaces network indicators, include valuable context about the scope, severity, and possible cause of the problem.

Aternity metrics are measured at the end user device and can be run through the Riverbed IQ analytics pipeline and correlated to detect anomalies and surface issues affecting the performance of SSE or remote work environments. These metrics include:

- **Application-level metrics:** native and derived high-level metrics associated with application performance from the user perspective.
- **Activity-level metrics:** very detailed metrics associated with the "activities" that comprise an application, such as download a Salesforce report. Activity-level metrics offer excellent visibility into issues affecting a specific activity or part of an application.

Riverbed IQ currently leverages Aternity application-level and activity-level metrics to equip NetOps teams with the observability they need to peer into remote work or SSE-generated blind-spots. When application performance issues occur, Riverbed IQ surfaces any suspect remote work or SSE/CASB indicators and includes valuable context about the scope, severity, and what is causing the problem.

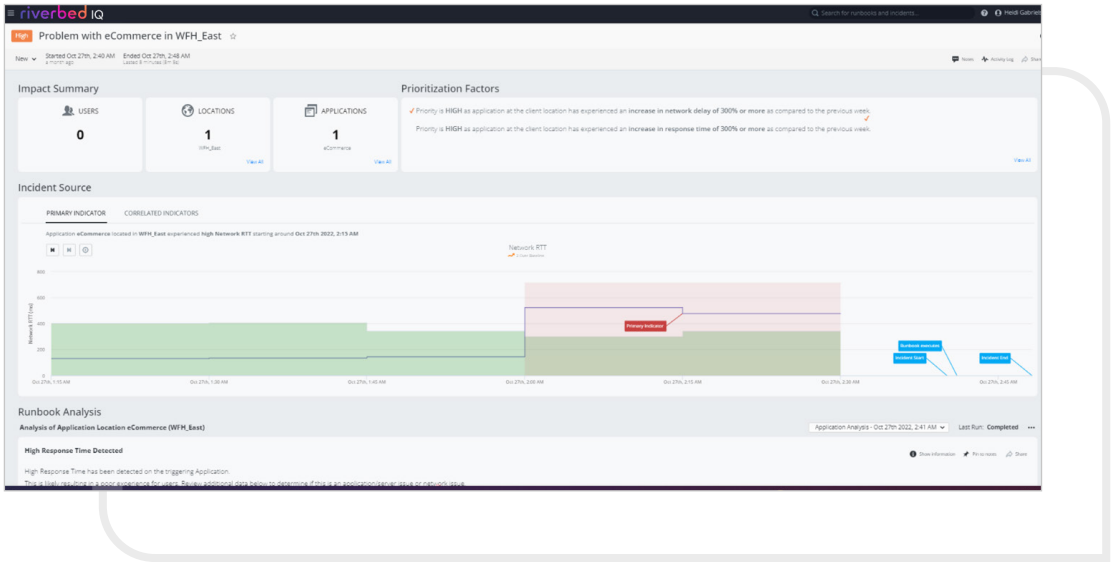

Figure 3: In this screenshot, Riverbed IQ has alerted on a problem with the ecommerce app from a remote location. It alerted because network delay and response time have both increased by more than 300%.

Key Measurements

The key measurements that Riverbed IQ uses to identify remote work or SSE issues include where the problems are occurring, the user impact and severity:

- Which applications are having network performance issues?
- How severe is the impact?
- How many users are impacted?
- Which locations are impacted?
- How are the impacted users accessing the application? (CASB, VPN, Direct to internet?)
- Is the issue caused by a specific ISP?
- Is the VPN the issue?

Example Incident: ISP Problem

This example incident shows how Level 1-2 network troubleshooters can use Riverbed IQ to determine root cause of the problem. In this case, it's a remote work incident with a poorly performing ISP.

Which application are having issues?	Salesforce, Microsoft 365, +10 others
How severe is the impact?	Network wait times are 3x longer than normal
How many users are impacted?	75
What locations are impacted?	Northeast United States
How are the impacted users accessing the application? (CASB, VPN, direct to internet)	CASB and Direct to Internet
Is the CASB or VPN causing problem?	Network wait times for direct to internet applications are also slower than normal
Is a specific gateway creating the issue?	No correlation to a specific gateway
Is an ISP causing the problem?	All 75 users are connecting through Comcast

Summary

Providing IT teams with the visibility to troubleshoot remote and SSE-based problems is difficult. Many organizations resort to synthetic testing, but this does not provide root cause analysis for SSE environments.

Riverbed IQ delivers the observability that network teams need to diagnose and resolve remote work and SSE visibility problems by integrating and correlating endpoint data from Riverbed Aternity End User Experience Monitoring. NetOps teams can now determine where the problem resides, how severe it is, and how many users are impacted. Armed with this information, they can now identify previously difficult-to-diagnose issues in remote work and SSE environments.

Learn More

For more info on the Riverbed IQ service, go to riverbed.com/IQ.
If you're curious about Riverbed Aternity, click here.