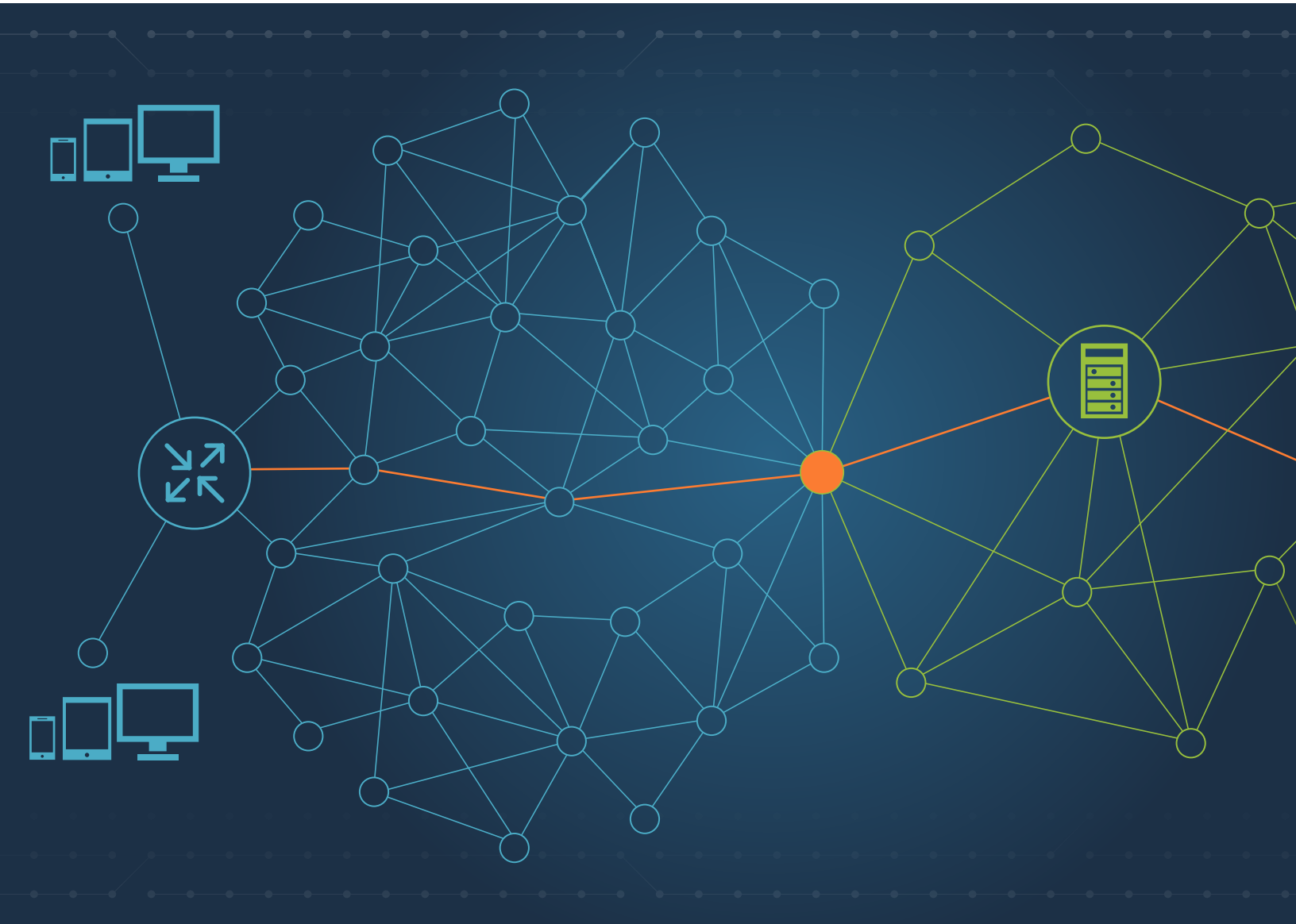
ThousandEyes

Monitoring Cloud-Based Secure Web Gateways Using ThousandEyes

White Paper



Cloud Security Services Bring Operational Blind Spots

Enterprise WAN architectures have seen a seismic shift in the last few years. Enterprises are increasingly adopting direct Internet access (DIA) from branch offices as they migrate to SaaS applications (like Office 365 and Salesforce) and build more of their enterprise applications on IaaS and PaaS platforms (such as Azure, AWS and GCP). Branch DIA allows better end-user experience and performance for these cloud-hosted applications and avoids costly backhauling of web traffic over MPLS backbones to centralized Internet breakouts.

This trend has led to a transition away from centralized firewalls to cloud-based Secure Web Gateway (SWG) providers for providing essential security functionality. These security solutions allow the benefits of local Internet breakout at the branch site, and provide security services (such as URL filtering, advanced threat defense, and antivirus protection technologies) to defend corporate users from Internet-borne threats and enforce Internet policy compliance.

However, this deployment model creates significant blind spots for IT and network administrators. Network paths are now much longer and more complex and include segments (Internet, security and cloud providers) entirely out of the control of IT. Legacy network monitoring tools are no longer suitable for this Internet-centric environment because they primarily collect passive data from on-premises infrastructure, which makes up an increasingly smaller component of enterprise operations. Ultimately, preparing for DIA cloud access, including necessary operational monitoring, reporting and fault isolation, requires visibility beyond the four walls of the data center and branch offices.

Security as a Service Architecture

Cloud-native SWG services are built as highly scalable multi-tenant platforms by functionally distributing components of a standard SWG to create a global network that acts as a single virtual proxy.

Cloud security providers typically offer multiple access options, but in a typical deployment, enterprises will send user traffic from the branch office location to the closest cloud security data center or node via a GRE tunnel from their on-premises Internet router or firewall. User traffic is then inspected at the provider's node by an inline proxy that enforces security policies such as advanced threat defense, malware protection and application control, with user-level granularity. The node then sends the user traffic over the Internet to the SaaS provider. The traffic path is illustrated in Figure 1.

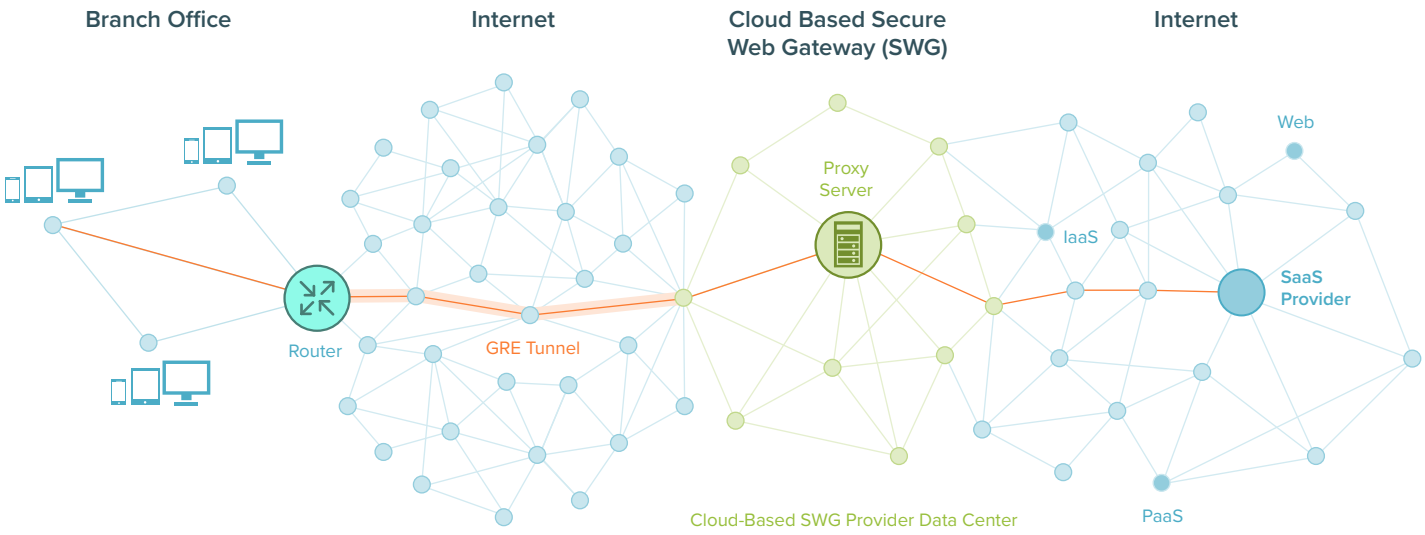


Figure 1

Monitoring User Experience with ThousandEyes

In a cloud SWG deployment, the end user experience for accessing cloud-hosted applications depends on the performance and availability of multiple providers:

1. The local ISP providing connectivity at the branch site. For global enterprises this might be multiple providers covering different regions or countries.
2. Transit ISPs on the path to the cloud security provider
3. Cloud security provider
4. Transit ISPs on the path from the security provider to SaaS and IaaS providers
5. SaaS, IaaS providers

ThousandEyes offers a network intelligence solution that actively probes the network, a unique monitoring technique to provide a complete hop-by-hop picture of performance between a client and a server and the intermediate SWG provider at work in that data path. ThousandEyes performance and availability monitoring capabilities help IT and network teams to troubleshoot issues quickly and make these deployments successful.

ThousandEyes Enterprise Agents deploy at branch offices and run active tests across the whole path of traffic as it exits the enterprise, transits ISPs, proceeds through cloud-based SWGs, and transits further ISPs to SaaS services, as shown from left to right in Figure 2. Tests run at regular intervals to collect application and network layer metrics like server response time, network latency, browser render time, redirect time, resource loading times, and DNS lookup delay.

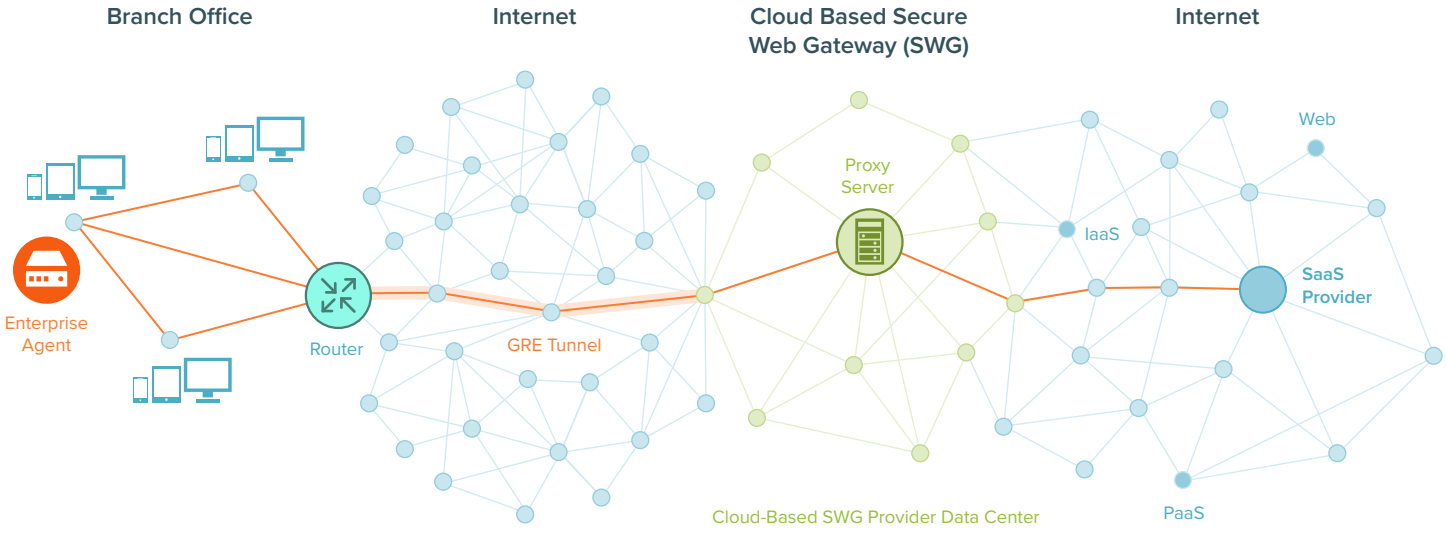


Figure 2

Let's say it's 8:00 am in the morning, and your IT support team starts receiving calls from their users complaining of slow access to one of their cloud apps, in this case, Salesforce. Since ThousandEyes active monitoring tests can run at up to one-minute intervals, in parallel your team will receive automated alerts from the ThousandEyes platform showing error conditions such as high page load time and HTTP server errors.

You can log into the ThousandEyes platform and access detailed information about the end-user experience for accessing Salesforce. Looking at the Page Load view shown in Figure 3, you can see a spike in the page load time from a real-world monitoring test. Under normal operations, the Salesforce login page takes around 1 second to load, but at the time of the test, it is taking almost 10 seconds.

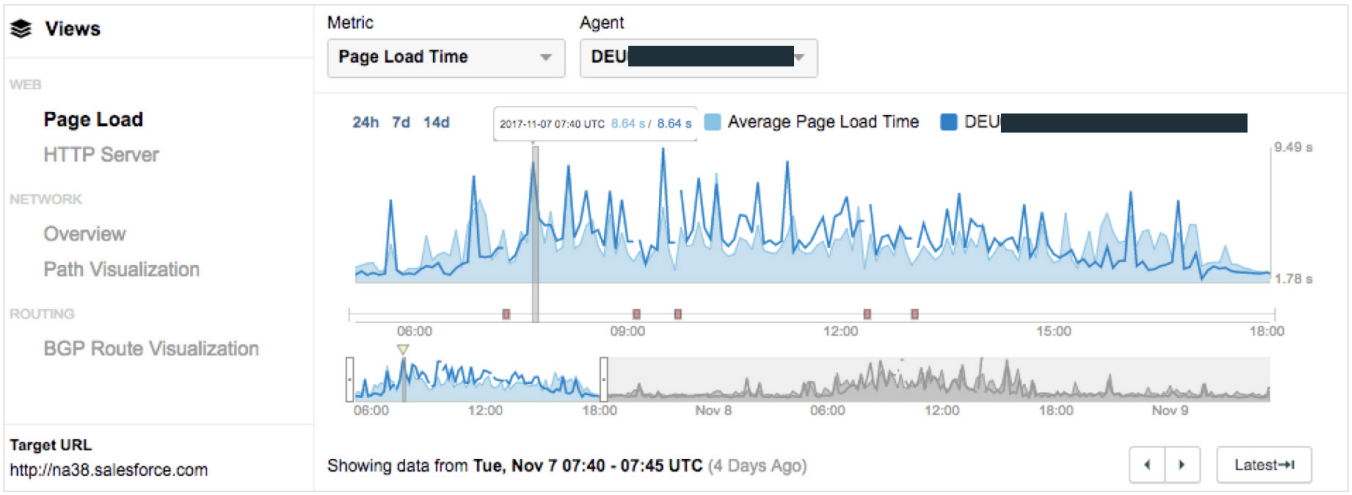


Figure 3

You can jump into the HTTP Server view, and see a high number of HTTP (connect, SSL and receive) errors and a spike in HTTP Server response time. ThousandEyes provides details of the exact errors as shown in the red boxes in Figure 4.

These observations are symptomatic of network layer issues like high packet loss and congestion, so to get further insight you can start examining and troubleshooting the network layer.

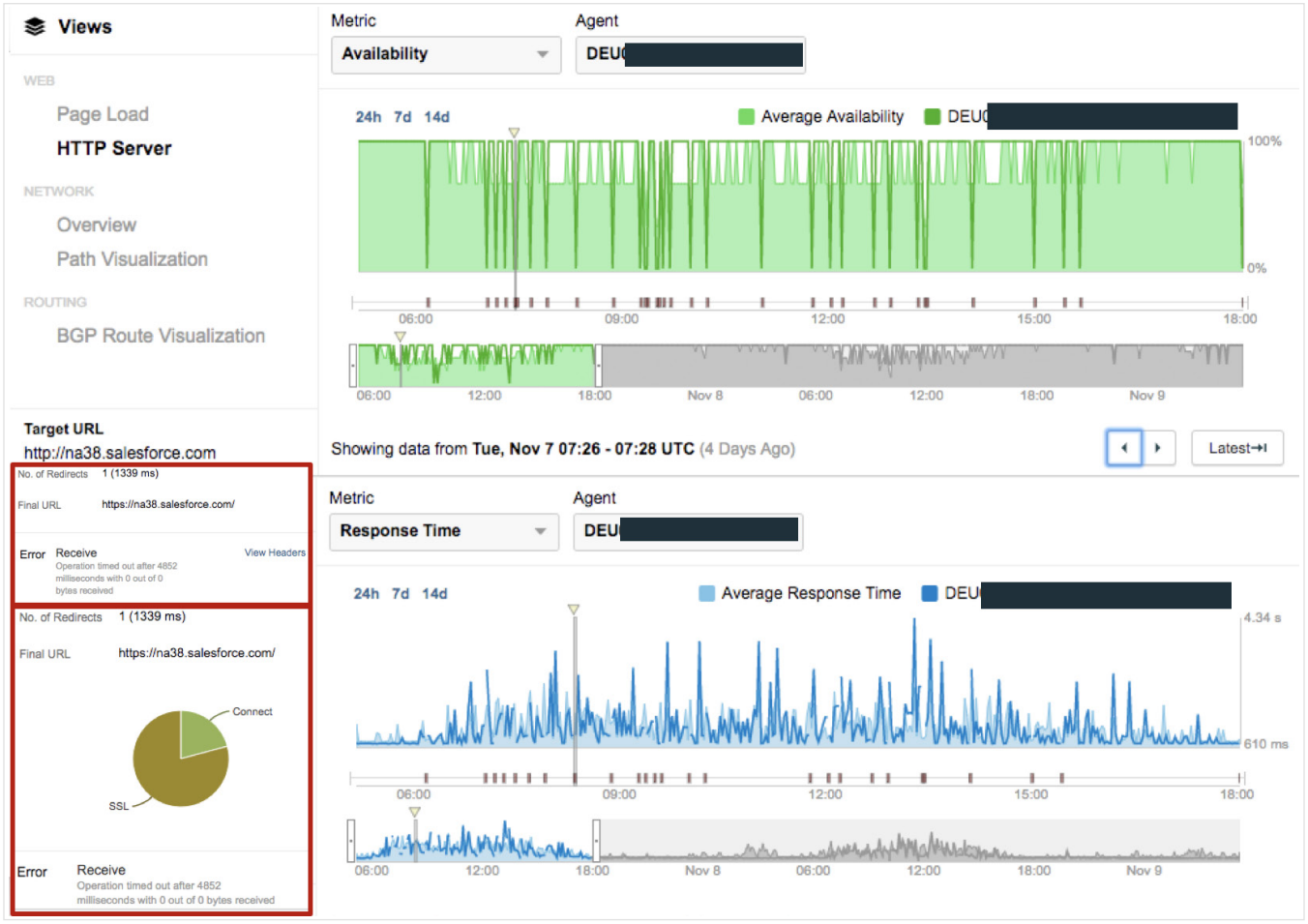


Figure 4

Network Path Monitoring with ThousandEyes

In cloud SWG deployments, ThousandEyes recommends monitoring three important network segments with separate tests to create full visibility, as illustrated in Figure 5. Each test collects per-hop metrics such as latency, packet loss MTU, and QoS markings.

1. Connectivity from the branch to the security proxy GRE tunnel virtual IP (VIP), as shown by the **- - blue dashed line - -**
2. Connectivity from the branch to the specific cloud security proxy server inside the GRE tunnel, as shown by the **— black line —**
3. Upstream connectivity from the security proxy site to the SaaS or IaaS provider, as shown by the **— orange line —** portraying an end-to-end test from the Enterprise Agent to Salesforce.com.

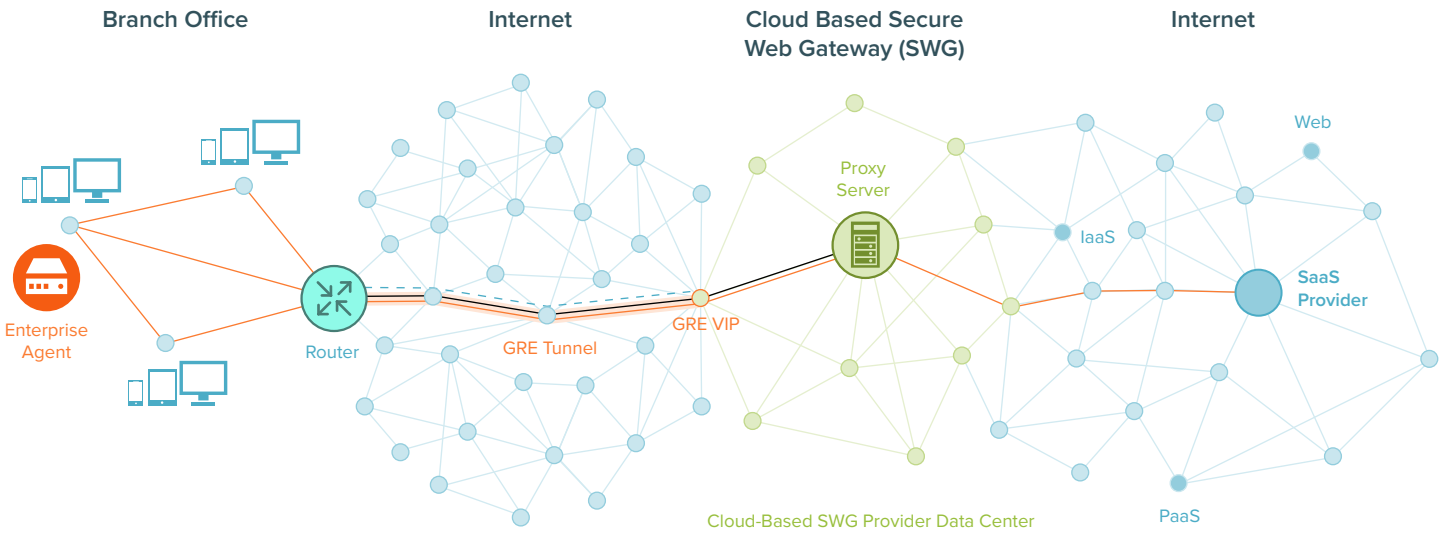


Figure 5

By collecting data about each of these network segments, ThousandEyes helps to very quickly identify the root cause of issues and fix them.

Monitoring Connectivity from Branch to Cloud Proxy VIP

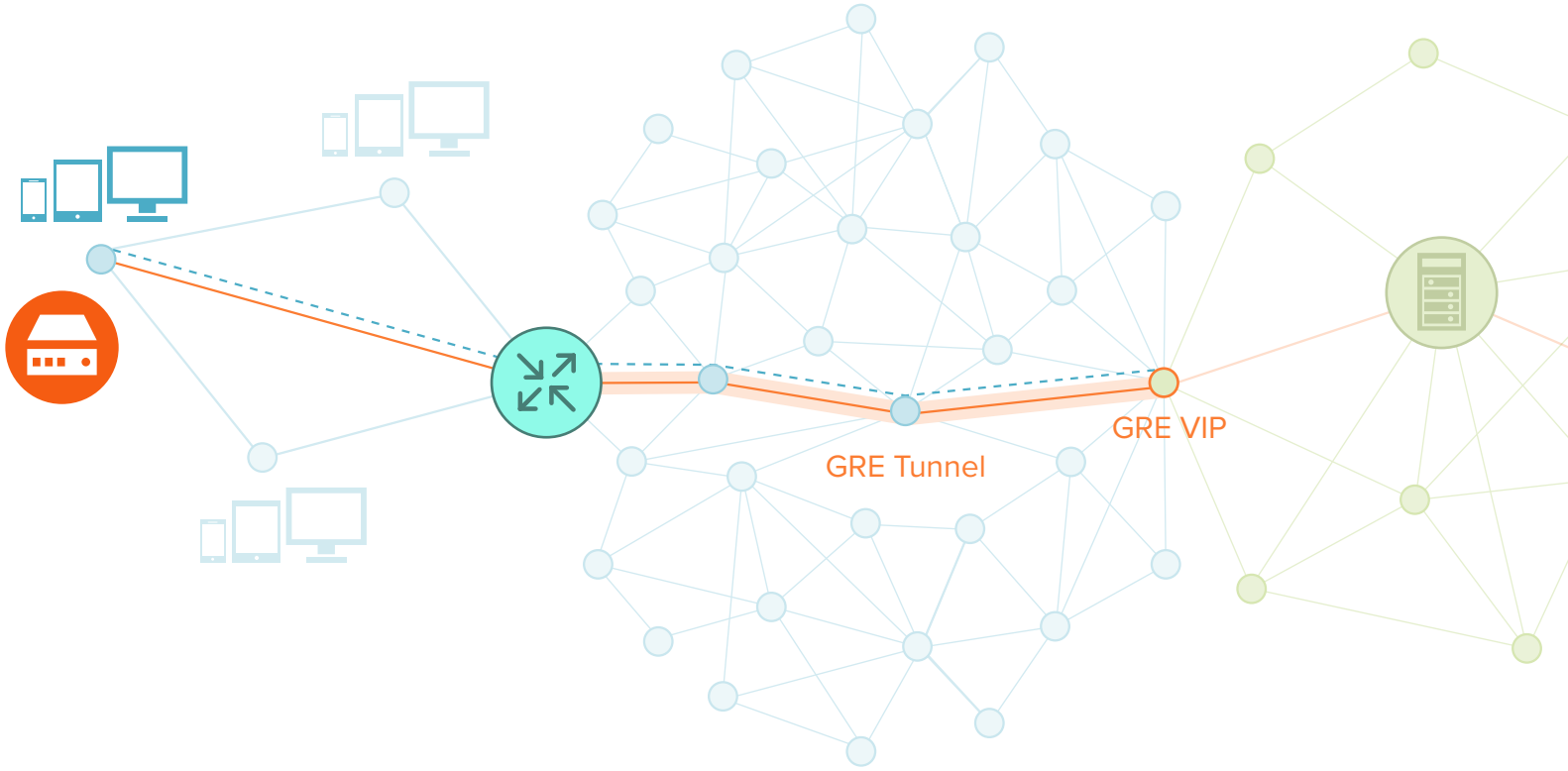
To get the best secure proxy performance, typically you will be sending your traffic via a GRE tunnel to the provider's "closest" or most optimal node. To test the health of the underlying Internet connectivity from the branch location to the provider node, we recommend setting up a network layer test to the GRE Virtual IP (VIP) address as published by the SWG provider, to provide the perspective of the GRE tunnel path through the Internet.

Using the data collected from ThousandEyes, you can quickly identify the specific hops and organizations responsible for the nodes as well as compare it to the network behavior during healthy operations by going back using the timeline feature.

Reprising the troubleshooting sequence we started above, Figure 6 (on the following page) shows that starting at 7:48 am CEST, there is high packet loss to the cloud SWG's Frankfurt GRE VIP address from the branch office. You can dive deeper and also see the specific nodes where the packet loss is happening. You can also see the full path of how branch locations connect to the VIP—in this case, for Zscaler's Frankfurt "ZEN" node (165.225.72.32).

The test monitors the health of the path from your Internet router to the proxy. ThousandEyes allows you to monitor:

- Latency, jitter and packet loss from the branch office to the VIP
- Per-hop latency and packet loss of each of the layer 3 nodes in the network path



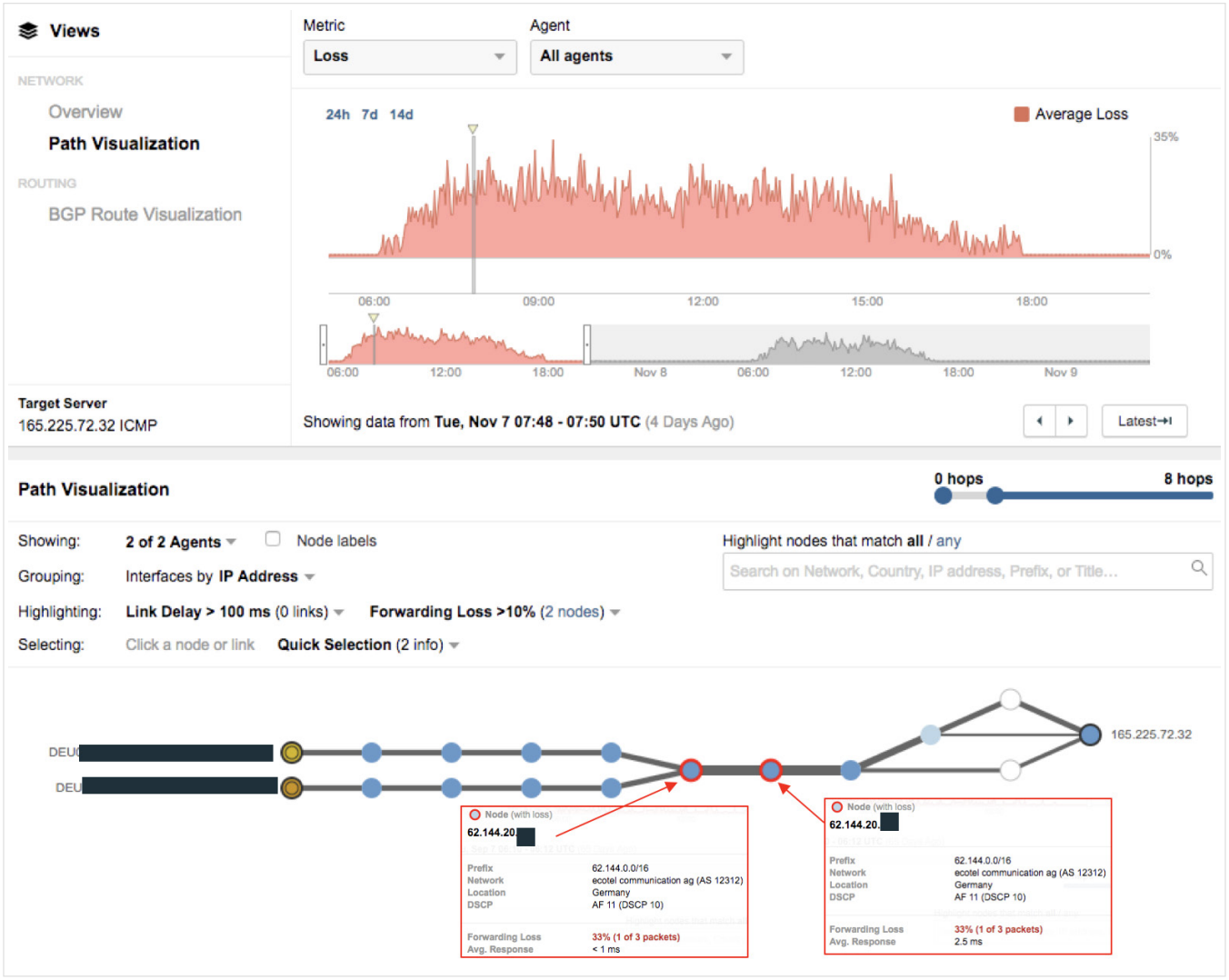


Figure 6

This confirms initial findings that the reported access issues with Salesforce are due to network issues. Furthermore, ThousandEyes provides the exact root cause of the issue: network loss and congestion inside the upstream ISP- Ecotel Communications (AS 12312). The specific routers in their network that are experiencing packet loss are also identified.

Monitoring Connectivity from Branch to Proxy Server

In addition to monitoring the tunnel VIP, it is important to monitor the performance and availability of the proxy server to ensure that users can connect securely. This specific branch office uses the proxy IP address for the Zscaler Frankfurt ZEN (165.225.72.40). Figure 7 shows a spike in packet loss that correlates with the loss we observed above for the Zscaler ZEN Frankfurt GRE VIP.

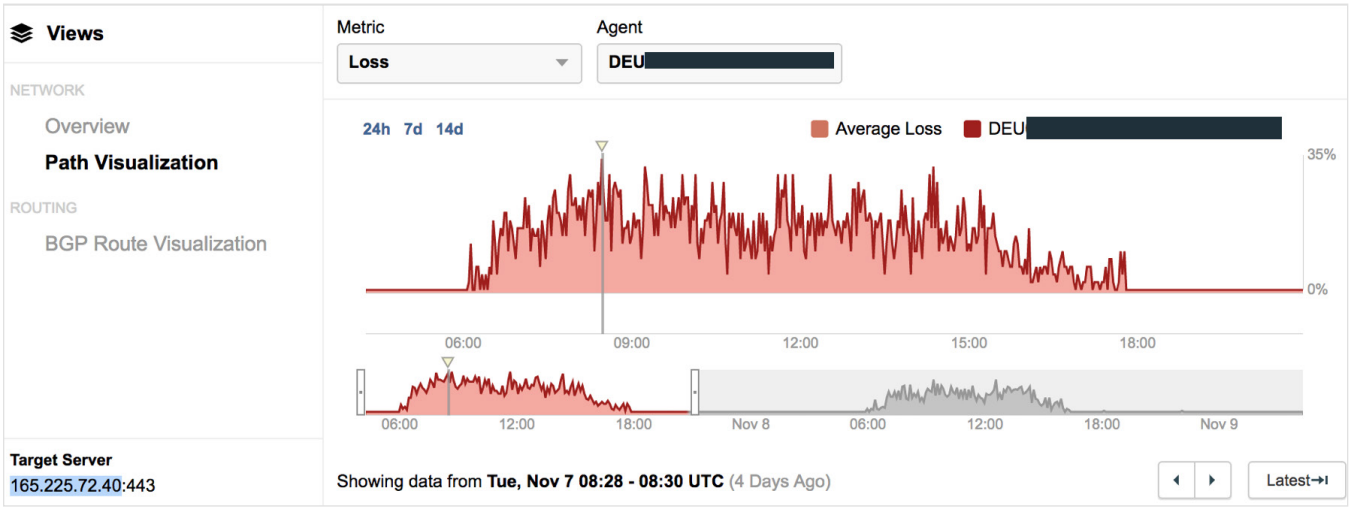


Figure 7

Monitoring upstream connectivity from cloud proxy to SaaS provider

The final component of network path monitoring is the upstream connectivity from the cloud proxy to the target SaaS application, in this case, Salesforce. ThousandEyes monitors the network latency, jitter and packet loss on a per-hop and end-to-end basis and quickly points out where the issue is occurring. This gives IT admins unprecedented visibility into the health of upstream network connectivity from the cloud security provider, including multiple transit ISPs and network connectivity into the SaaS provider.

In figure 8, we see the end-to-end path from the ThousandEyes agent in our branch office, going through the Zscaler Frankfurt ZEN's upstream provide Zayo to na38.salesforce.com. More specifically, traffic is carried over the Zayo network from Frankfurt to Amsterdam, then to London, across the Atlantic to Washington D.C. where it is handed off to Salesforce's network edge co-located in an Equinix Washington D.C. facility in Ashburn. The traffic then goes through the Salesforce internal network to Phoenix, AZ where the service instance is hosted.

We can also see that as the traffic enters the GRE tunnel, the MTU has reduced from 1500 to 1476 (due the 24-byte GRE header overhead) - as shown in the Blue callout below. This information can be crucial when trying to troubleshoot MTU related performance issues.

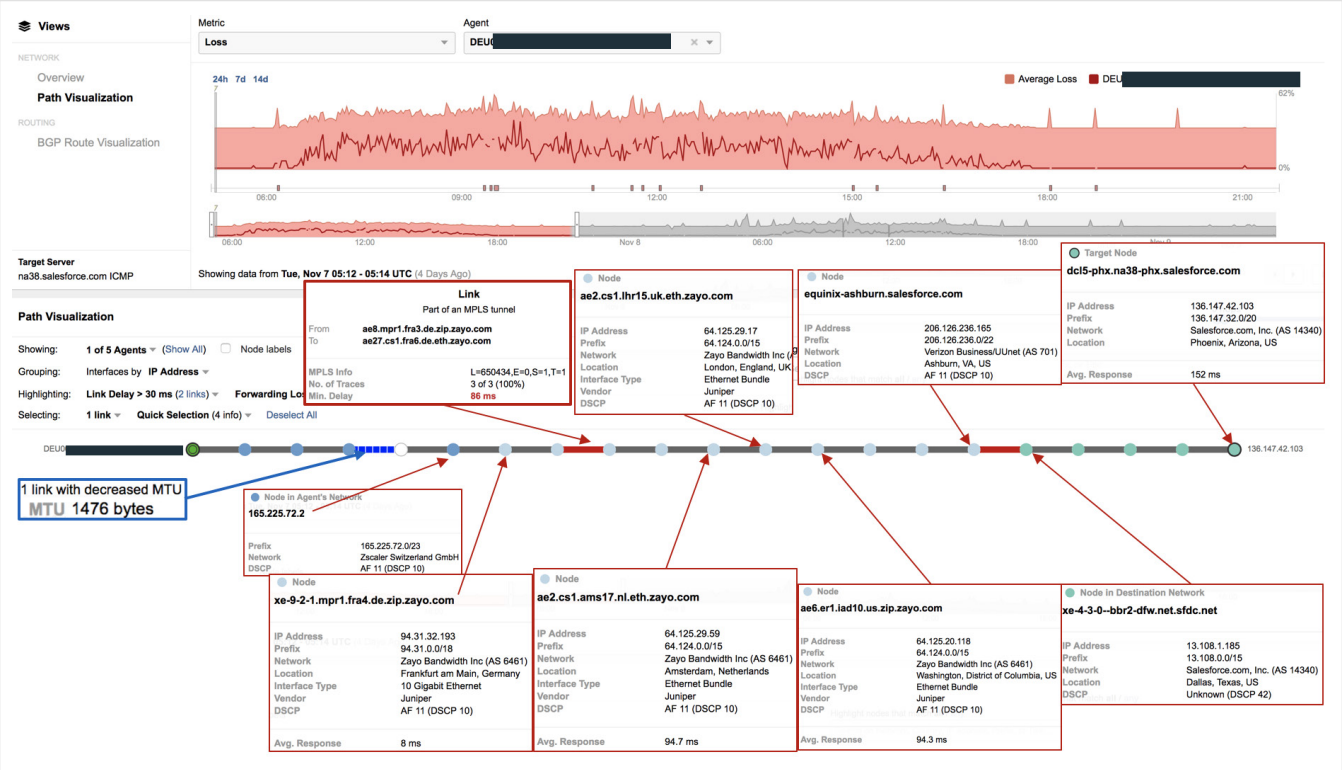


Figure 8

Root Cause Analysis and Data-Driven Service Escalation

ThousandEyes Network Intelligence offers end-to-end network path insights across internal, Internet and cloud provider networks, correlated with application and service performance. Network Intelligence helps IT and network teams quickly find the root cause of complex performance issues. In this case, Path Visualization revealed that high packet loss in specific routers in the Ecotel Communications network connecting a branch office with a cloud SWG provider was causing a bad end-user experience and impacting business processes running on Salesforce.

Being armed with detailed insights transforms service escalations and cloud vendor accountability from fraught negotiations into data-driven processes that are more productive for everyone. ThousandEyes makes it easy to share interactive root cause analyses and visualizations with providers like Zscaler, Ecotel and Salesforce.

Conclusion

The move to the cloud means that IT teams depend on an ecosystem of application and service providers including cloud-based security services like SWG, DNS, CDN, and DDoS mitigation. All of these services depend on Internet-based connectivity that can be a serious operational blindspot. ThousandEyes Network Intelligence enables IT and network teams to see, understand and improve every connected experience, across any provider and network path. If you'd like to learn more about how ThousandEyes can help you gain greater visibility into your network as you prepare for a move to the cloud, find more information at www.thousandeyes.com

ThousandEyes

201 Mission Street, 17th Floor
San Francisco, CA 94105
(415) 513-4526

www.thousandeyes.com

About ThousandEyes

ThousandEyes is a network intelligence platform that delivers visibility into every network your organization relies on, enabling you to resolve issues faster, improve application delivery and run your business smoothly.