

# **Service Assurance and Performance Management for Enterprise Site-to-Site VPNs**

---

*A White Paper*

---



[www.brixnet.com](http://www.brixnet.com)

## Overview

Virtual Private Networks (VPNs) are networks that offer the connectivity, security, and performance associated with private networks, but over a shared infrastructure. Enterprises continue to deploy and manage their own VPNs in an effort to replace more expensive and less flexible leased line and Frame Relay solutions.

Today's self-managed VPNs use the public Internet as the shared infrastructure (see Figure 1). Leveraging the Internet gives enterprises instant access to a global network that can immediately connect distant offices and remote users. For each location, the enterprise has the flexibility to utilize the most appropriate Internet access technology (e.g., T-1, DSL, cable, dial-up) and service provider for the region. The flexibility and ubiquity of Internet access can provide a cost savings of more than 60% compared with traditional private networks.

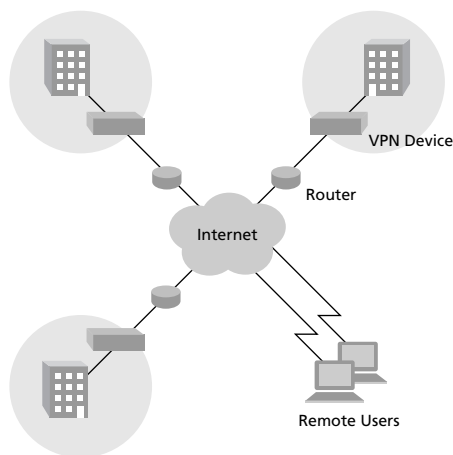


FIGURE 1: Enterprise VPN

But what the Internet offers in flexibility it may also lack in security. Therefore, to carve out a private portion of this shared network, VPN gateways and software clients are deployed throughout the network and on end-user PCs. The VPN devices are then used to open IP Security (IPSec) tunnels to carry the encrypted VPN traffic.

To some extent, VPN performance can be guaranteed by the service level agreements (SLAs) offered by leading service providers. However, in large VPN deployments, a number of Tier 1, Tier 2, broadband, and dial-up ISPs are typically used to interconnect branch offices and remote users (see Figure 2).

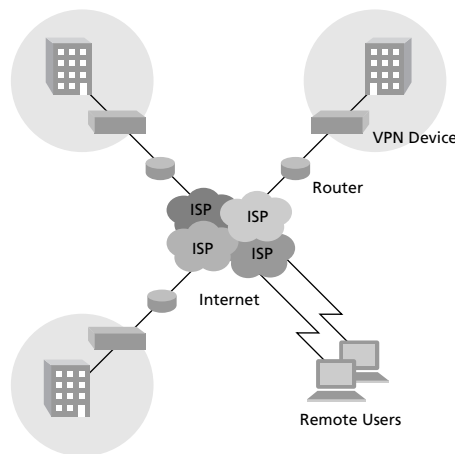


FIGURE 2: VPN Network Complexity

As a result, individual VPN connections can traverse a number of ISPs and the performance of each of these intermediate networks can vary widely. Some providers may not even offer SLAs. It is because of the Internet's dynamic nature, unlike the more predictable and often sole-sourced private network it replaces, that continuous service level management of enterprise VPNs is required.

---

***It is because of the Internet's dynamic nature that continuous service level management of enterprise VPNs is required.***

---

This White Paper describes how the Brix System monitors the public IP infrastructure to assure high-quality VPN service by:

- Continuously testing the network;
- Integrating with VPN gateway solutions;
- Detecting and warning of service degradation; and
- Identifying the responsible ISP or ISPs.

---

## VPN Monitoring Strategy

Several things must occur in order to effectively maintain VPN performance.

1. VPN software or hardware must successfully look up (resolve) the DNS name for the target VPN device, which depends on the availability and performance of the ISPs' domain name service.
2. Network traffic must be exchanged across the VPN with acceptable performance, i.e., have low-to-moderate latency and low packet loss.
3. Sessions must traverse stable paths that avoid short-term packet loss and latency variation associated with path changes.

---

***To accurately monitor VPN performance, service measurements must be performed from end-to-end, and provide visibility into the network outside the VPN tunnel.***

---

Networks not meeting these basic requirements result in:

- Increased operational costs as IT spends too much time troubleshooting poor network performance or unavailability;
- Decreased productivity as critical applications are either unavailable or perform poorly; and
- Dissatisfied end-users.

To accurately monitor VPN performance, service measurements must be performed from end-to-end, and provide visibility into the network outside the VPN tunnel.

Relying on the performance monitoring and reporting capabilities of the VPN system are not sufficient. The toughest challenges IT managers typically face involve troubleshooting why connections can't be made, or why tunnels drop prematurely. The VPN system can only report on the performance of successful VPN tunnels.

VPN tunnels also obscure the underlying IP infrastructure. A measurement taken across the VPN network

will not identify any behavior between the origination and the termination of the VPN tunnel.

## Instrument the Network

VPN locations, all requiring some level of performance monitoring, can be grouped into the following three categories:

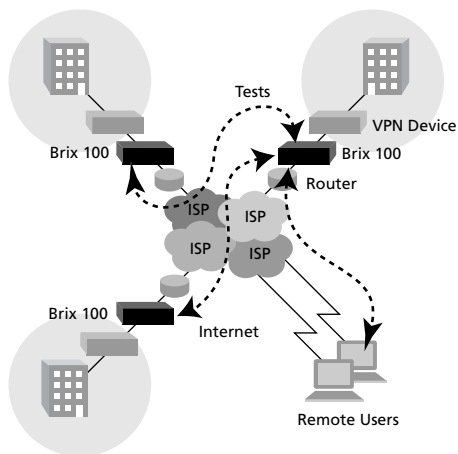
- **On-Network:** Locations with dedicated IP access and virtually permanent VPN connections that provide LAN-to-LAN connectivity. Before IP VPNs, these locations would typically be connected using private lines or Frame Relay Permanent Virtual Circuits (PVCs). Connections between on-net locations should be continuously monitored.
- **Off-Network:** Remote users, such as telecommuters with broadband access and road warriors dialing in from hotels and airports, have less permanent connections. These connections are, by definition, intermittent and require a testing infrastructure that can be dynamically provisioned.
- **Extranet:** Business partners who are not full members of the VPN, but are given limited access. The shared control of extranet connections requires dynamic testing from one partner when a VPN connection is opened.

### Brix Networks Verifiers

For on-net locations, Brix Verifiers, purpose-built hardware appliances, are deployed between the customer edge router and the VPN gateway or firewall. From this perspective outside the VPN tunnel, Verifiers avoid being "trapped" in the VPN tunnel and have complete visibility into the ISP and across the public Internet.

### VPN Server Integration

For off-net and extranet locations, Verifiers at the on-net locations are used to test outwardly to the remote sites (see Figure 3). With remote users, not only might their physical locations change, but most broadband connections use dynamically-allocated IP addresses.



**FIGURE 3: Pervasive VPN Performance Management Using Brix Solutions**

Therefore, testing from these centrally located Verifiers to off-net and extranet locations requires integration with the VPN server and the ability to dynamically provision network tests.

This is accomplished by integrating the BrixWorx™ central site management software system with VPN servers, such as Check Point’s Firewall-1 and Nortel’s Contivity. By monitoring the opening and closing of VPN tunnels, network tests can be automatically provisioned on an as-needed basis from a Brix Verifier located near the VPN server to the end-user. To troubleshoot dropped VPN connections, the test may be provisioned to continue running after a tunnel is closed to capture additional performance data.

### Active and Passive Testing

A complete VPN performance management solution includes both active *and* passive testing.

Active testing offers full control over all aspects of testing, including test scheduling, length and number of transactions, and origination and termination locations. It is only with an active-based testing regimen that an enterprise can be assured of full and continuous testing coverage.

Active testing also makes it possible to both establish standardized quality metrics (i.e., what constitutes

acceptable performance?) and meaningfully compare performance over time, location, and even application.

Most importantly, because active testing can be done independently of users, enterprises can continuously collect performance measurements and are proactively alerted to developing performance issues. A proactive approach reduces — and even eliminates — costly network incidents, allowing IT managers to address these problems *before* end-users feel their impact.

Passive testing also plays a vital role in managing VPN performance. While active testing provides the most accurate and proactive measurement of network performance, passive testing is used to profile the flow of traffic across the network.

Passive testing is primarily used to track utilization of VPN access links. Monitoring link utilization aids capacity management by helping network managers “right-size” the network. Capacity is only expanded where correlated active and passive test measurements show that high utilization rates are negatively impacting network and application performance.

---

***A complete VPN performance management solution includes both active and passive testing.***

---

Just as importantly, passive testing also reports how the network is being used. By tracking Virtual Local Area Networks (VLANs), classes of service, and application usage, network administrators can adjust to shifting traffic and application usage patterns to ensure that critical applications continue to meet their performance objectives.

## Testing Recommendations

Testing a self-managed VPN requires the following types of tests (see Table 1):

- **Verify Hostname Resolution:** The Brix DNS Active Test monitors external DNS resolution of VPN device names by the local ISPs.
- **Verify Network Performance:** The Brix Ping and

UDP Active Tests measure availability, packet loss, and round trip time (RTT) between VPN sites.

- **Verify Path Stability:** The Brix Traceroute Active Test maps the external paths between VPN locations.
- **Monitor Network Utilization:** The Brix Network Utilization Passive Test reports network and application utilization of VPN access links.

DNS Test Configuration	
Frequency:	15 minutes
Parameters:	DNS server query
Results:	Response time
ICMP/UDP Echo Test Configuration	
Frequency:	5 minutes
Parameters:	Target host
Results:	Round trip time Jitter
Traceroute Test Configuration	
Frequency:	5 minutes, or automatically triggered by another test
Parameters:	Target host
Results:	Number of hops Route Latency
Network Utilization Test Configuration	
Frequency:	5 minutes
Parameters:	Monitor IP traffic
Results:	Utilization, distribution of application traffic

TABLE 1: VPN Testing Recommendations

The first step when a VPN client attempts to open a tunnel to the VPN server is to resolve the address of the server. The Brix DNS Active Test monitors the ability of external DNS servers to resolve the VPN server's name. The tests should be run on Brix Verifiers using the same public DNS servers that the VPN software uses.

After a connection is established, the quality of the connection depends on the performance and stability of the underlying public IP infrastructure. The Brix Ping (ICMP) and UDP Echo Active Tests should be used to test the performance among Verifiers deployed at on-net locations and between Verifiers and remote users.

If any performance degradation is experienced, the

results provided by the Brix Traceroute Active Test contain valuable troubleshooting data. Monitoring the external path and performance of the VPN connection Ping and Traceroute Tests record the network performance and path from each remote site to the VPN target device.

For on-net locations, monitoring network and application utilization tells network managers when access links need to be upgraded, or even downgraded, to handle changing capacity.

## Testing Example

The following example covers three days of testing that took place in an actual Brix customer deployment. The top line (see Figure 4) shows the Traceroute hop count from a Brix Verifier to the VPN target, and the bottom line shows the round trip time. The path changes every 24 hours when a network access point exchange provider reroutes traffic to their peering points.

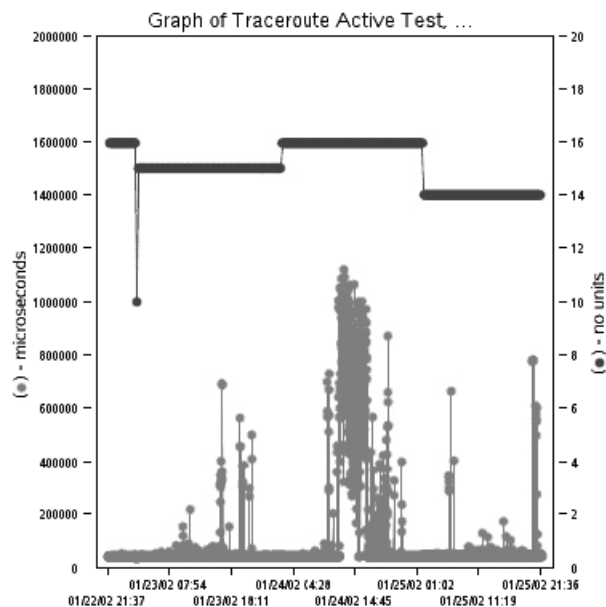


FIGURE 4: Correlated Ping and Traceroute Test Results

Historical data shows that whenever this provider chooses to route traffic over a particular ISP, performance degrades. This is reflected in the center of the graph where a route change correlates with RTTs of more

than one second. This disruption was corrected 24 hours later when routes were again recalculated. Unfortunately, the optimal route, resulting in a hop count of 10, is almost never selected. This information is very helpful to IT managers when trying to troubleshoot and optimize the performance of their VPN.

At the same time, network utilization of the fractional T-1 connecting this site to the VPN was constant and well within acceptable limits (see Figure 5). Over-utilization did not contribute to the longer round trips experienced at this VPN site.

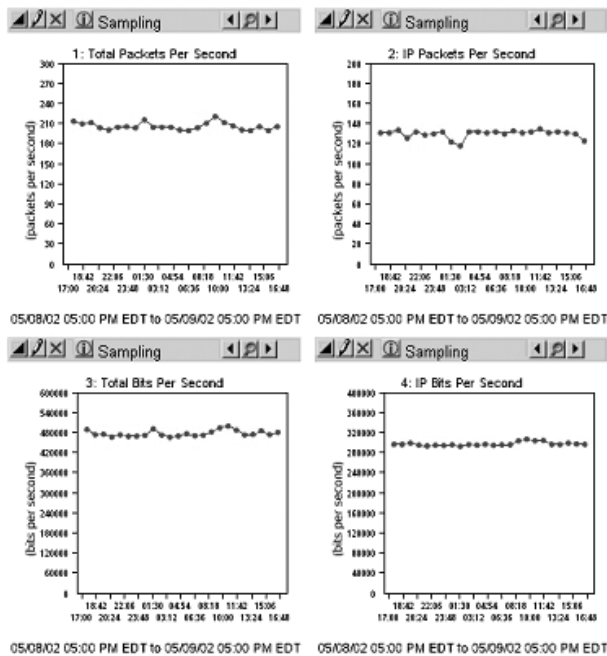


FIGURE 5: Network Utilization

## Conclusion

With enterprises increasingly being dependent on Internet VPNs to deliver critical applications and services to their branch offices, remote users, and extranet business partners, incorporating thorough service assurance and performance management is no longer a tactical afterthought, but a strategic imperative.

***With the Brix System, enterprises have a comprehensive IP service assurance and performance management solution.***

Network professionals at large enterprises and government agencies who manage their own VPNs benefit immensely from the Brix System by using site-to-site testing and VPN server integration to provide new visibility into the performance of their VPNs. With the Brix System, enterprises also have a comprehensive service assurance and performance management solution that allows the testing and verifying of all advanced IP services from one platform with real-time, proactive notification of any degradation in service levels. As a result, enterprises using IP VPN services “Built with Brix™” can:

- Quickly identify cause of network and VPN performance degradation;
- Shorten connectivity and performance troubleshooting;
- Use historical data to improve VPN performance at remote sites;
- Verify ISPs service level agreements; and
- Improved capacity planning.



285 Mill Road • Chelmsford, MA 01824

978-367-5600 • 978-367-5700 (f) • 888-BRIXNET • info@brixnet.com • www.brixnet.com

Brix 100, Brix 1000, Brix 2500, BrixWorx, Brix, Brix Networks, Brixnet, A Measure Above, Built with Brix, and the Brix Networks logo are trademarks of Brix Networks, Inc. All other product or company names mentioned may be trademarks of their respective holders.

Service Assurance and Performance Management for Enterprise Site-to-Site VPNs

Copyright © 2002 Brix Networks, Inc. All rights reserved. Permission to reproduce in any form is required. Exceptions are references for attribution.