How to Monitor Your WAN to Support SD-WAN and Multi-Cloud

By

NETBEEZ

Executive Summary

Today's Wide Area Networks (WAN) are more distributed and even more critical to business operations than ever. WANs enable users to access on-premise services and public clouds and to communicate with their teams, partners and customers. At the same time, complexity is increasing. Distributed organizations that operate across dozens of worldwide offices are connected by overlay networks serviced by a multitude of carriers. This growing gap between evolving WAN demands and the capabilities of widely deployed monitoring tools has resulted in increased reliance upon users for problem identification.

This guide helps network engineers, architects and executives consider key network monitoring requirements to support SD-WAN and multi-cloud deployments.

Highlights

- SD-WAN is gaining traction at distributed organizations due to cost savings and ease of centralized management.
- WAN complexity is increasing due to the introduction of Network Function Virtualization (NFV) and overlay networks as part of SD-WAN services.
- Use of Direct Internet Access (DIA) has made it more difficult for network engineers to detect and diagnose remote network performance issues.
- Traditional network monitoring tools based on SNMP are not sufficient to detect and troubleshoot remote network issues and end-user experience

How ‘Software Defined’ is changing your WAN

SD-WAN enables enterprises to reduce capex and opex (such as connectivity costs) while centralizing network management and policy enforcement. More specifically, there are three key advantages of SD-WAN over legacy WAN architectures.

Dynamic Path Selection. Traffic is automatically adjusted based on network conditions. It’s possible, for example, to dynamically distribute connections amongst multiple links to make best use of Direct Internet Access, MPLS, and LTE/5G connections. Load balancing can be configured per-flow, and some vendors even support per-packet basis. Traffic control can be based on jitter, latency, and packet loss.These values are measured in real-time via special performance probes, generally implemented with UDP packets.

Policy Based Routing. SD-WAN controllers enable centrally defined network policies to orchestrate traffic to and from WAN locations. For example, real-time traffic such as Voice-over-IP (VoIP) can be set to use low latency MPLS circuits, while bandwidth intensive applications can be routed over Internet connections. Network policies can be applied to traffic destined to public cloud providers to use the desired interconnects.

Simplified Configuration. Configuring an SD-WAN is mostly UI-driven, rather than requiring the network engineer to master a command line interface. Bandwidth management and traffic control are entirely *software-defined* while many network functions, like firewalls, DNS and caching, are virtualized (NFV).

Some of the advantages of SD-WAN however introduce new challenges to infrastructure and operation (I&O) teams.

Observability Challenges

SD-WAN and multi-cloud adoption pose new challenges to I&O teams' ability to successfully and efficiently manage their WAN and support the end-users. We identified three key challenges that should be considered:

1. Split tunnel reduces visibility to Internet resources and public clouds.
2. Parth remediation and failover don't take into account the end-user experience.
3. Virtualization impairs troubleshooting of remote performance issues.

Split tunnel reduces visibility to Internet resources and public clouds.

In a split tunnel configuration, a remote site has a direct Internet connection to reach public networks and a private connection to reach corporate resources (intranet). The private connection is established between the branch router and the company's data center via a VPN tunnel or MPLS connection.

Split tunnels limit the efficacy of centralized network monitoring solutions that cannot detect reachability or application performance degradation issues impacting users at remote sites. This is because the monitoring server is located at the data center.

Path remediation and failover don't take into account the end-user experience.

Path remediation and automatic failover enables multi-home routers to direct traffic based on the quality and reliability of underlying links. Performance probes used to implement link quality verification only consider the "last mile". For example, the router may route traffic across a link with no packet loss but with a lower data rate, slowing down the overall connection.

Path remediation and failover could have a local significance but negatively affect the overall end-to-end performance. In the case of packet duplication, the overall bandwidth available to users is reduced. As a result, applications may perform slower than before the corrective action which drives user complaints.

Virtualization impairs troubleshooting of remote performance issues.

SD-WAN routers use passive application performance monitoring to identify and profile the applications that traverse their interfaces, prioritize mission-critical data and optimize routing decisions. While this level of monitoring is key for an SD-WAN router to make routing decisions on its multiple network links, it doesn't provide a good estimate of end-user experience.

To troubleshoot remote performance issues, multiple components should be considered including: the WiFi network; the LAN; the client itself; the configuration of the SD-WAN appliance; and, the WAN/Internet links. SD-WAN solutions provide valuable information and analytics about the traffic that flows through their interfaces. Without end-to-end metrics (such

as network latency, packet loss, DNS resolution time, and HTTP loading time from the user layer), it becomes very difficult to efficiently troubleshoot remote performance issues.

Required Monitoring Capabilities

SD-WAN and multi-cloud adoption impose new monitoring capabilities, which legacy network solutions based on SNMP don't offer. In fact, these types of solutions have two major limitations that impact their efficacy:

1. They are centralized: the server runs and performs the monitoring from the data center.
2. They are device oriented: report the status and resources available of network devices.

To address new network monitoring demands, we have identified two primary requirements that every organization should consider with SD-WAN and multi-cloud deployment:

Distributed network monitoring.

Network monitoring should be performed at every location that is company-owned and/or operated. This includes locations that provide network services to corporate employees (WAN sites and headquarters), host information systems and customer-facing services (data centers and public clouds). By collecting data from the locations where traffic originates and terminates, it's possible to accurately detect and troubleshoot network and application performance issues.

For example, having a monitoring agent at a WAN location and another in a public cloud, it's possible to verify that the network can deliver the expected throughput and performance to users accessing cloud services.

Active network monitoring with end-to-end tests.

Active network monitoring with end-to-end tests is used to verify reachability and measure performance to network services and applications. This approach is very similar to service assurance delivered by IP SLA tests configured on network devices. What is different is that tests are run from the user layer and are mostly directed towards private or public applications (end-to-end), rather than just running within a portion of the network. This method enables the detection of network failures or performance issues without relying on user tickets.

IT organizations that are moving to a SD-WAN and multi-cloud should deploy network monitoring solutions that meet these two requirements.

How NetBeez Supports SD-WAN and Multi-Cloud Adoption

NetBeez is a distributed network monitoring system that meets critical SD-WAN and multi-cloud requirements. Remote physical and software agents run active, end-to-end monitoring tests at any on-prem and cloud location. These capabilities enable I&O teams to quickly detect and troubleshoot remote network problems, reducing unnecessary downtime and the wasteful deployment of skilled personnel.

Moreover, NetBeez provides these additional capabilities:

Real-time data feeds: Within seconds remote monitoring agents report telemetry data to a centralized dashboard controller for alert processing and analytics. Having real-time data allows quick analysis and alert detections within seconds versus the minutes of delay inherent with legacy monitoring solutions. This capability is key to reduce the time to detect and repair remote network issues.

Telemetry raw data versus sampled flow data: Raw data streams provide a better context and more granular visibility into remote network and application performance issues. This level of detail delivers valuable insight regarding frequency and enhances the identification of intermittent problems which could be caused by factors beyond the network.

Ease of installation, support for any network, integrations: NetBeez monitoring agents are easy to install and support any network environment, whether on-premise or cloud. The physical sensors are plugged into switches (Gigabit Ethernet) and/or connect to a 802.11 access point. The software agents support Linux and Windows operating systems, virtualization (VMware, HyperV, KVM, …) as well as Docker. They also integrate with leading infrastructure vendors, such as Cisco, Extreme Networks, and Juniper.

Conclusion

Today's Wide Area Networks are far larger, more complex and more dynamic than ever before. Driven by the adoption of SD-WAN and multi-cloud, the WAN has outgrown the capabilities of traditional network monitoring solutions. IT organizations that want to be agile need to include network monitoring in the scope of work for any SD-WAN and multi-cloud project.

Network monitoring solutions should support distributed agents that perform active, end-to-end performance measurements. These capabilities enable Infrastructure & Operations teams to efficiently manage and support the network and its users.

NetBeez caters to the recent demands of modern WANs with key capabilities that enable network teams to gain the full benefits of SD-WANs and multi-cloud deployments.