ACCEDIAN

White Paper

Shed Light on the Darkspace with East-West Traffic Monitoring

In today's hybrid networks, traditional packet capture monitoring conducted North-South is failing IT operations teams. North-South traffic describes client-to-server traffic that moves between inside and outside the data center. As the name suggests, North-South traffic is depicted vertically to illustrate traffic that flows from the end user to the data center. But, North-South monitoring only provides approximately 20% of the data needed for the critical application to determine the root cause of performance issues.

This is because North-South monitoring is typically comprised of Terminal Access Points (TAPS) or hardware devices that passively captures traffic over a network, packet brokers, and switch port mirroring of the physical network, which give IT operations teams significantly less than half of the picture of what is happening in the network, and less so in virtualized environments.

When every server was on-premise and physical, it was easy to mirror traffic using distributed network analyzers (or packet brokers and capture systems) where the packet information can then later be analyzed.

But that was then and this is now.

The network monitoring systems that once reigned are no longer sufficient in architectures that require deeper visibility, and it is simply not as straightforward as it once was with traditional IT infrastructure topologies.

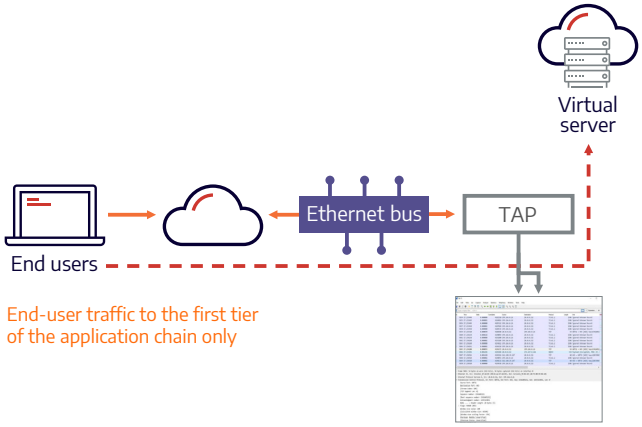

Figure 1: Traditional packet capture monitoring for North-South traffic

With the majority of today's servers residing in virtualized, software-defined networking (SDN) and cloud environments, key application traffic does not hit the physical wire. Monolithic applications are broken into smaller functions, so if IT operations only monitor the physical network, then they miss the traffic in the virtualized network. In fact, estimates show that North-South monitoring only provides approximate 20% of the data needed for the critical application to determine the root cause of performance issues. That is just not enough to deliver the best possible customer experience.

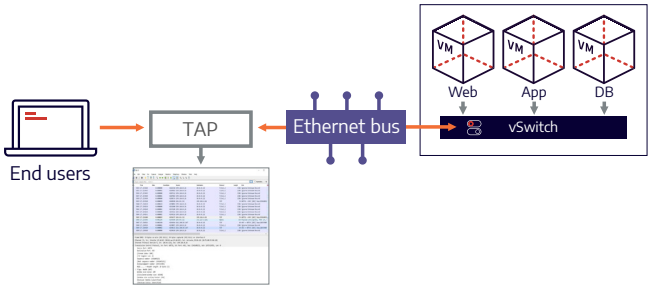

Figure 2: Limited visibility of North-South traffic with traditional monitoring tools

North-South monitoring in a virtual environment only gives IT operations visibility into the physical network. Since a significant portion of virtual machine traffic never touches a physical link, they will only see end-user traffic up to the front-end tier one web server. But, they do not see the traffic from web server to application server or application server to the database server. If a database performance problem exists, such as a slow SQL query, IT managers would not see the problem. They would thus only see the traffic between the end user and the first tier to which they connect.

Conventional East-West traffic monitoring

This raises the importance of East-West traffic monitoring. East-West traffic monitoring offers views of the transfer of data packets from server to server network traffic within a data center or the public cloud. The term originated from depicting traffic flow in the local area network (LAN) horizontally. With the adoption of a modern micro-service architecture and container application technology, East-West traffic will only grow in volume.

Conventional East-West monitoring offers one potential solution to shedding the light on blind spots which is to mirror the V-Switch traffic out to the physical network. This typically involves retrofitting all the VM hypervisors with a dedicated 10 Gbps network interface card (NIC) and copying all of the V-Switch traffic out of the dedicated NIC and into a packet broker.

This is a suitable solution if IT Operations need to monitor only a handful of hypervisors. But, if there is a need to scale beyond that, flexibility quickly becomes an issue. The volume of East-West traffic has grown exponentially as a result of virtualization and converged infrastructures. Today, network controllers, virtual machines (VMs) and other devices perform various functions and services that previously ran on physical hardware. File sharing, internal email, chat, database, and many other applications which do not exit out of the egress point run as fast as the internal switch can handle. As these components relay data to each other, they increase traffic on the network, which in turn, can cause latency issues that negatively impact network performance and end user quality of experience.

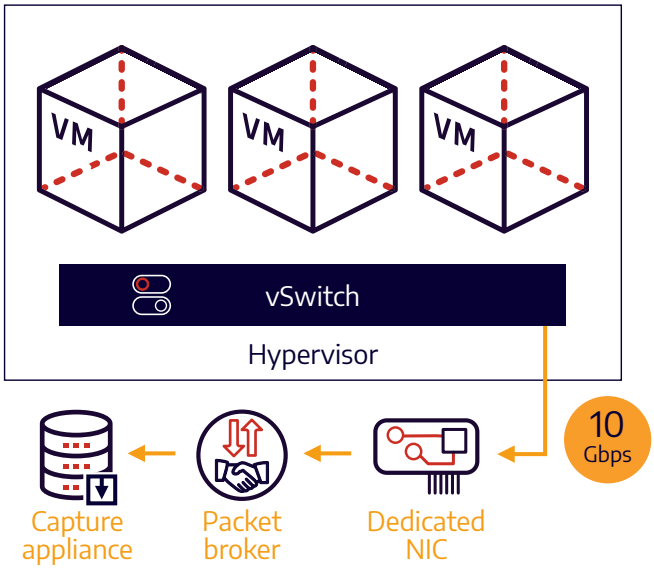

Figure 3: Typical industry solution for East-West traffic capture

There are also significant downsides to conventional East-West monitoring. Unmanaged latency, flexibility, and scalability are a few of them, but the biggest is cost. For many companies that have hundreds or thousands of servers this would require purchasing a dedicated 10 Gbps NIC and the switch ports on the packet brokers to accommodate all of the new monitoring points. The capture appliances need to have high capacity storage since the amount of raw packet traffic between all the services can be an incredibly large amount of data, even for short periods of time. That increases the cost of the monitoring solution exponentially. Also, transmitting all of that raw packet data from the capture device to the capture appliance over the cloud backbone network can severely impact cloud application performance. Clearly the prohibitive cost of doing this and the operational inefficiency would also eliminate most or all of the cost reductions obtained by moving to the cloud. It is also not a solution fit for any cloud-based networks like AWS, Microsoft Azure or Google.

The Accedian advantage

Accedian takes a unique approach to East-West traffic monitoring through the use of lightweight, agentless, software capture sensors. These are deployed in a virtual machine (VM) hypervisor on a cloud server. The capture VM or sensors listen to the East-West traffic on the virtual switch and forwards an exceedingly thin stream of metadata to a data store that can be dynamically located on any cloud server and in fact, anywhere on the network.

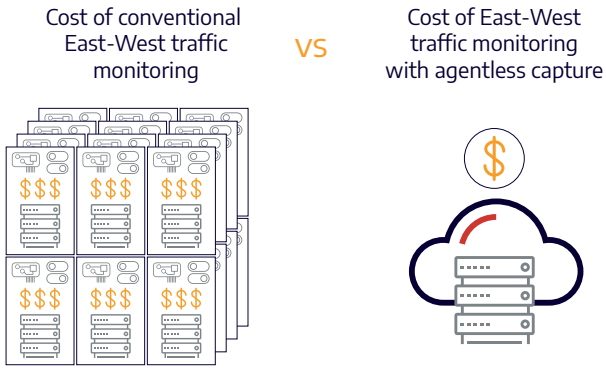

Figure 4: Cost comparison of different methods for East-West traffic monitoring

The forwarded metadata traffic generates only around 0.2%- 0.5% of the fully observed traffic. In a 10Gbps traffic capture model, this means the capture probe generates only about 20 to 50 Mbps compared to full 10Gbps captured and sent by traditional packet brokers. The metadata from the Skylight sensors is then transferred to a virtual capture appliance, where it's retained to enable real-time performance analytics.

This enables real-time performance information to be reviewed within the context of historical performance data to enhance troubleshooting and problem resolution.

In contrast to the previous example, this is a difference in an order of magnitude that will not require any changes be made to the physical hypervisors saving significant costs and is highly scalable with very little impact on IT resources. It can also be easily deployed in any environment including AWS and Azure.

With only North-South monitoring, it is likely that IT operations have a variety of blind spots. Therefore, East-West monitoring sheds light on the darkspace. It gives IT operations the complete visibility they need. IT operations will be able to explain the loss of one transaction out of thousands that happened at some point in the past. They will be able to be able to detect and respond to incidents better, and they will be able to troubleshoot problems with greater ease and speed.

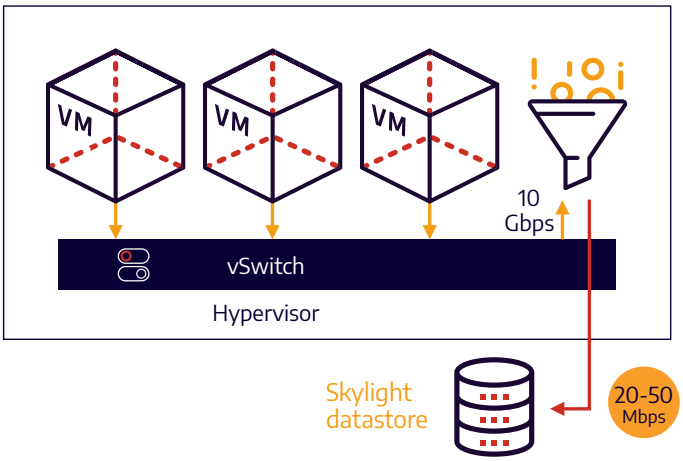

Figure 5: Accedian's agentless capture solution for East-West monitoring

About Accedian

Accedian is the leader in performance analytics and end user experience solutions, dedicated to providing our customers with the ability to assure their digital infrastructure, while helping them to unlock the full productivity of their users.

Learn more at **accedian.com**

Accedian | 2351 Blvd. Alfred Nobel, N-410 | Saint-Laurent, QC H4S 2A9 | 1 866-685-8181 | **accedian.com**