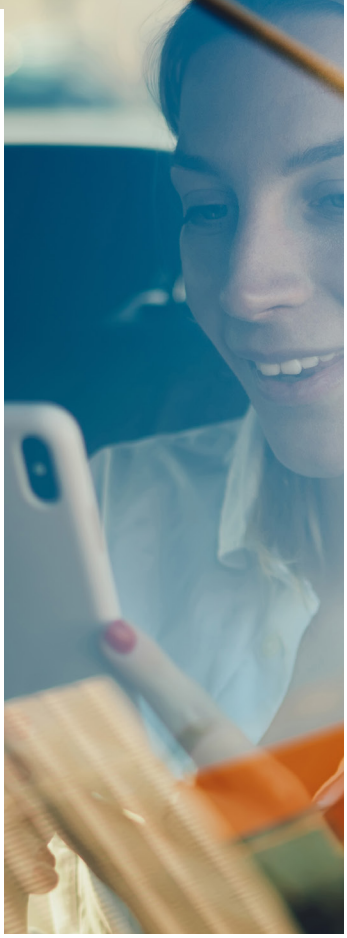
NETSCOUT

| ARTICLE |

OVERCOMING THE CHALLENGES CARRIERS FACE IMPLEMENTING 5G STANDALONE AND CLOUDIFIED NETWORKS



Accelerating the 5G Transition by Providing Optimal Packet Level Visibility in Cloud-native Environments

We know the incredible benefits that 5G Standalone (SA) will provide as it makes its way into the palm of our hands and integrates into our daily work and play environments. As carrier service providers (CSPs) look to cloudify networks in order to deliver on the promise of true 5G SA and begin to reap the potential benefits of emerging use cases, they will need to overcome a host of challenges, particularly as it relates to end-through-end visibility.

The migration to a cloudified 5G core will likely not be as fast as initially assumed for a myriad of reasons. These include the need to introduce new 5G SA service-based architectures (SBAs) with true cloud-native approaches. This will entail disaggregating traditional network elements into virtual functions using container technology. Disaggregation creates an environment that is more difficult to monitor and therefore more difficult to be certain virtualized functions are delivering as required.

Another hurdle CSPs face will be providing sufficient visibility for operations engineers to ensure performance across each communication link. As Transport Layer Security (TLS) encryption technology is deployed throughout the SBA, engineers no longer have sufficient visibility (once encryption is turned on) to the control plane and user plane packets which are also separated to allow for elasticity.

As CSPs drop in new network functions from different vendors, spinning up new functions as needed, the resulting multi-cloud architectures become increasingly complex - making visibility exponentially more difficult. While utilizing numerous specialized, independent vendors may breed greater innovation, lower costs and better products, it also creates a far more challenging environment to manage and assure that different elements can interoperate effectively.

A further challenge relates to multi-access edge computing (MEC). As CSPs look to put part of their 5G core into a hyperscaler's cloud off-premise in their availability zone, it will be incumbent on engineers to ensure near instantaneous connectivity, reducing latency serving 5G functionality for this MEC. This will require visibility from the core out to the edge including the hyperscaler infrastructure as needed.

Additional challenges CSPs face in rolling out 5G SA, include:

- New HTTPS/JSON message structures
- Underlying network complexity of linking Containers and K8 clusters together
- IP Addresses do not uniquely identify a 5G NG
- IP Addresses are transient and change for many reasons

Overcoming the Challenges of 5G SA and Cloudified Networks

As stated, one of the biggest challenges of 5G SA and cloudified networks is gaining end-through-end visibility. The visibility into the "East-West" packet level data will no longer be as simple as placing a physical tap or packet broker in place and sending the control plane and user plane traffic to a service assurance solution. This type of legacy approach using physical devices is not cloud-native and simply doesn't have the dynamic elasticity required for future 5G SA networks.

Visibility is needed from the 5G radio access network (RAN) to the edge to the access layer and into the core network infrastructure. Because 5G SA will necessitate disaggregated data in the cloud, as well as other cloud services that interact with the 5G network, engineers will require correlated user-plane information for troubleshooting and user experience monitoring. Deep visibility into the RAN is needed to gain critical insights into the cause of call drops, handoffs between 4G and 5G networks, radio interference, and congestion issues.

Finding a solution that can overcome these visibility challenges will be key to providing continuous latency measures at the MEC layer, while offering KPI measurements for each element in the 5G non-standalone (NSA) and SA network and guaranteeing that service-level agreements (SLAs) of network slices are being met.

Security will also be an important concern as CSPs pursue 5G SA. Protecting the expanded attack surface of a cloudified network will require real-time, scalable visibility that is capable of delivering early warning of anomalous behavior, is able to distinguish between human error and human malintent, and can offer threat mitigation that constantly guards against persistent threats.

A lack of visibility into the 5G SA network and the applications, services, and devices operating on that network, as well as the interconnected 4G network, makes it far more difficult for network operations, engineering, and security teams to monitor, manage, and secure the network. By focusing on achieving end-through-end visibility, CSPs can make service assurance, analytics, and security an important part of ongoing investments in 5G SA and cloudified networks. Such an approach will be instrumental to the successful roll out and support of digitalization, edge computing, network slicing, and virtualization.

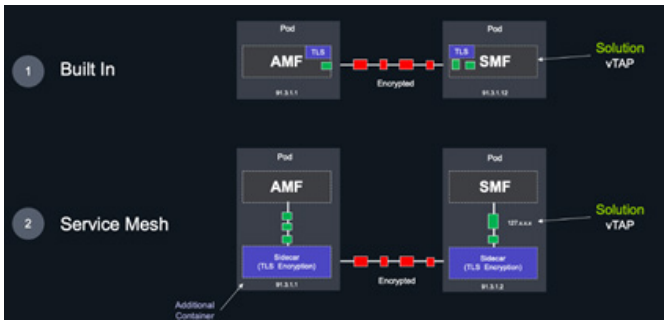
Key to achieving such visibility will be the need for a vendor independent solution that is cloud-native, can scale, and will offer critical packet level insights that ensure the network is providing the expected customer experience.

Successful 5G SA & Cloudified Networks Facilitated by Vendor-Independent Collaboration

NETSCOUT® takes a vendor independent collaboration approach that helps CSPs to overcome the challenges enumerated earlier, providing the same deep level of visibility that is currently available on 2G/3G and 4G/VoLTE networks.

By spending countless man hours collaborating with major Network Equipment Manufacturers (NEMs), NETSCOUT is now able to offer the ability to interface virtual probes (vSTREAMs) or COTS probes (ISNG) to communicate directly with the NEM's virtual tap (vTAP). This innovative NEM vTAP overcomes some of the complexity listed above by providing a 3GPP packet data stream directly to NETSCOUT, where any NEM dependencies, along with load balancing, out-of-order packets, fragmentation, and re-assembly are handled. A close working relationship with NEMs ensures continued support as updates are made.

In the case of CSPs who decide to provide their own service mesh, NETSCOUT is still able to help through its Envoy plug-in, which allows packet level traffic to flow to its probes un-encrypted.



vTAP packet access in Containers and Service Mesh.

With the advent of 5G SA has come a new telco edge – the MEC, which now calls for visibility into a cloud-based architecture and the ability to monitor key attributes of that environment – throughput and latency. Some of the real-time applications made possible by the MEC may demand latencies of less than ten milliseconds in the transport route. This raises the vital question - how do CSPs ensure that these critical SLAs are monitored and maintained?

NETSCOUT has solved this problem by collaborating with the major hyper scalers to ensure CSPs always have visibility to the applications and functions running within the cloud for MEC-based services. This collaboration facilitates a true end-through-end visibility solution – from the RAN to the MEC to the core.

So, how exactly does this work? Once NEM vTAPs send the 3GPP packet data to NETSCOUT, patented Adaptive Service Intelligence® (ASI) technology produces Smart Data, which ensures all the noise has been removed and only the most high-fidelity data remains. This data is analytics-ready, offering real-time, multi-dimensional visibility of the network, services, and technologies - down to the subscriber level.

It would be easy to assume that this innovative approach is purely aspirational. But that would be wrong. Recently, Ericsson, Swisscom and NETSCOUT teamed up to provide industry-first automatic access to packet data and the ability to analyze raw packet data, offering data-processing and network function monitoring in the cloud as part of Swisscom's newly deployed cloud-native, TLS-encrypted 5G standalone (SA) network.

This unique collaboration integrates Ericsson's dual mode 5G Core with built-in software (SW) virtual network tap and NETSCOUT's vSTREAM® virtual network probe. This ground-breaking solution gives Swisscom better visibility into their cloud network, and the ability to capture network packets from inside their cloudified network at strategic points. This allows for continuous monitoring and deep analysis of networks, dramatically increasing network service assurance, analytics and cybersecurity with NETSCOUT – all while ensuring the best 5G customer experience, significantly reducing total cost of ownership (TCO), securing sensitive data, and delivering new 5G mission-critical services within the cloud.

Removing the Barriers to 5G SA Visibility

NETSCOUT remains committed to working closely with CSPs around the globe to identify new trends that may be occurring outside of traditional sources. The collaboration with Swisscom and Ericsson only just scratches the surface of how NETSCOUT is ready, willing and able to help reduce overall cost of 5G service assurance in a virtual environment and supporting the monetization of the network. Applying the techniques and technology outlined above, NETSCOUT has demonstrated it is possible to provide full visibility by application, by subscriber/device, by consumption, by location, by data plan and much more as CSPs look to rollout 5G SA and cloudified networks.

LEARN MORE

For more information about NETSCOUT solutions visit:

www.netscout.com/solutions/5g

www.netscout.com/solutions/cloud-visibility

www.netscout.com/blog/5g-standalone-network-too-cloudy-see

NETSCOUT

Corporate Headquarters
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Phone: +1 978-614-4000
www.netscout.com

Sales Information
Toll Free US: 800-309-4804
(International numbers below)

Product Support
Toll Free US: 888-357-7667
(International numbers below)

NETSCOUT offers sales, support, and services in over 32 countries. Global addresses, and international numbers are listed on the NETSCOUT website at: www.netscout.com/company/contact-us

SPA_018_EN-2202 12/2022