How 5G Networks Are Secured and Enabled By SASE

By Kelly Ahuja, Versa Networks CEO

As more organizations consider their own 5G MEC (Multi-Access Edge Computing) roll outs and environments, there are important deployment and security considerations. While still a fairly new technology, adoption rates of 5G have increased significantly, currently at three times that of 4G. The buzz has been growing around 5G for some time, as the new networking standard promises faster speeds, greater bandwidth, and optimized mobility.

The technology has quickly gone from concept to reality as the demand for an enhanced digital experience, along with the increase in personal and IoT devices, as well as workload transition to cloud, have driven the need for 5G.

With 5G, it is extremely important for organizations to consider security solutions that can enforce consistent security posture across public cloud, hybrid cloud, and on-premises environments, or any combination of these environments. 5G introduces a whole host of security threats and vulnerabilities, such as kernel bypass, DDOS attacks on 5G service interfaces, and exploitation of software or hardware vulnerabilities leading to zero-day exploits.

5G and Potential Security Risks

5G network edges are designed to support various use cases that will prove extremely important to organizations across the board, including video analytics, location services, Internet of Things (IoT), Augmented Reality (AR), optimized local content distribution, and more.

It is well documented that 5G comes with promising advancements of greater speeds, higher bandwidth, improved connectivity, and lower latency, all while handling millions to billions of devices. However, along with these advantages 5G also introduces new security challenges. 5G not only increases the *number* of devices but *types* of devices to protect, including IoT devices, sensors, cameras, virtual assistants, etc. This expands the network's attack surface, resulting in more network vulnerabilities and holes for attackers to exploit.

SASE is Crucial to 5G Succeeding

Secure Access Service Edge (SASE) is crucial to a successful 5G environment, since it enables improved services and performance, increased security, and faster infrastructure rollout and management. SASE delivers end-to-end security, visibility, and telemetry for 5G infrastructure and services; and enforces compliance through a consistent security posture across public cloud, hybrid cloud, on-premises and MEC.

SASE interworks with 5G network slicing to guarantee aggressive 5G SLAs with end-to-end security and enables flexible implementation of Gi-LAN services in various form factors.

Secure SD-WAN, a SASE component, combined with network slicing guarantees that Service Level Agreements are met, and provides end-to-end security, including UTM, IDS/IPS, Anti-Virus, and more.

SASE can also enable automated 5G rollout of thousands of devices with true zero-touch provisioning using a SASE orchestrator, and leverages elastic auto-scaling and network intelligence to meet real-time capacity demands.

5G Deployment and Environmental Considerations

Preparing for and supporting 5G networks can seem daunting. With the right tools in place, including Secure SD-WAN and other SASE functions, organizations are prepared to best take advantage of all the benefits 5G has to offer, while addressing new security threats.

Organizations can dramatically lower CAPEX and OPEX of their 5G networks by choosing:

A multi-tenant uCPE architecture. One of the key use cases for 5G is to enable multiple virtual network operators' (MVNOs') use of a shared 5G infrastructure. This is done to provide differentiated services based on the application requirement (or network slice requirement) while keeping overall costs low. This approach delivers advantages of centralized management, reducing appliance sprawl and improving adaptability. One of the core components to its success is multi-tenancy. Each tenant can have multi-

level RBAC (role-based access control) to manage the network based on the roles and responsibilities with full segmented security. Advanced solutions deliver complete segregation of control-plane, data-plane, and management-plane for each of its tenants.

A solution with options for software and hardware-accelerated encryption and decryption capabilities that provide faster processing and tamper-resistant key storage. The solutions should also support chaining the services that are running on different nodes, including third-party service functions. All of these directly tie into the 5G vision of providing unparalleled application and user performance without any compromise in security.

A single pass parallel architecture for maximum performance and lowering latency. As seen above, 5G comes with very aggressive SLA demands and organizations must change their current infrastructure to meet these demands. In a traditional mobile architecture, there are silos of point and dedicated appliances that have different functions. However, this type of fragmented architecture simply can't scale in the new era of 5G.

A single pass architecture ensures that the majority of services are performed in the same cloud-service stack, at the same location, and at the same time. This approach has the advantage of needing to decrypt a data packet only once, which is important for optimal security. This is important because the requirement to open, parse, re-encrypt and forward traffic happens only once. This also avoids expensive, high-latency packet copying, and service inconsistency, therefore ensuring that 5G SLAs are adhered to.

A solution with a single management interface to manage, configure and monitor complete 5G and SASE services, such as Secure SD-WAN and the host of additional security services mentioned above.

For all organizations, security breaches, power outages, or any accidents resulting in down-time can be extremely costly. Whether it’s a school, manufacturing facility, or a large global enterprise, ensuring a rapid 5G rollout is crucial for agile IT and meeting the new networking and security requirements of users. 5G solutions built with automation capabilities such as zero-touch provisioning can help enable rapid deployment.

About the Author

Kelly Ahuja, CEO of Versa Networks is a seasoned industry veteran with more than 20 years of experience in networking and telecommunications. He currently serves on the board of directors for two startups in Silicon Valley. Kelly spent 18 years at Cisco rooted in the design and deployment of telecommunications networks. He was most recently SVP of Service Provider Business, Products and Solutions at Cisco where he was responsible for developing and managing the service provider segment strategy and portfolio. Kelly held several other senior executive roles at Cisco, including SVP and GM of the Mobility Business Group, Chief Architect for the Service Provider business, and SVP and GM of the Service Provider Routing Technology Group.

Earlier in his career, Kelly served as VP of Marketing at optical networking startup BlueLeaf Networks and product management leader at Stratacom. He also managed the design and deployment of data and voice networks for AT&T Canada, Bank of Canada and Telesat Canada. Kelly holds a Bachelor of Science in Electrical Engineering from the University of Calgary.

https://www.linkedin.com/in/kelly-ahuja-5820772

https://twitter.com/kahuja

Company website: https://versa-networks.com/

CYBER DEFENSE MAGAZINE

WHERE INFOSEC KNOWLEDGE IS POWER

www.cyberdefensetv.com
www.cyberdefenseradio.com
www.cyberdefenseawards.com
www.cyberdefenseconferences.com
www.cyberdefensemagazine.com