www.pipelinepub.com
Volume 20, Issue 8

Law Enforcement Agency Enhances Connectivity with NaaS

By: Larry Thompson

As technology consultants for municipalities, we try not to spend too much time talking about technology. Throw around jargon like "network as-a-service" (NaaS) or "edge," and you can watch your clients' eyes glaze over. Buzzwords don't interest them. They care about benefits, costs, impact on operations. Sometimes though, the jargon signifies something genuinely new and worth exploring. Take the NaaS solution we recently implemented for one of our most important municipal clients in rural South Carolina.

This client serves a relatively small population (just over 100,000 citizens) but covers a vast area spanning nearly 700 square miles, much of which has limited or no network infrastructure. As a result, they were constantly bumping up against the challenges of complying with two technology mandates governing law enforcement.

- **Real-time video capture**: Like municipalities across the United States, this client had outfitted officers with vehicle and body cameras, along with other digital tools to better track law enforcement activity and interactions with the public

- **Secure video transmission**: This client must also comply with regulatory mandates like the Criminal Justice Information Services (CJIS) security policy, which require strict confidentiality when transmitting law enforcement data, including using private interfaces with end-to-end encryption.

See the problem? Officers might collect gigabytes of video during a deployment, but with spotty or nonexistent coverage across much of the region, they have to return to central city locations to upload it to the municipal core network. In practical terms, officers must build extra time into every shift for secure data upload. Whether they cut short deployments or wait until the end of

a shift (delaying officers starting the next deployment), the result is the same: Technology intended to make officers more effective ends up *reducing* the time they spend out on patrol.

Anyone living or working in rural areas is familiar with network coverage gaps and the issues they create for digital applications, most of which seem designed to assume that high-speed access is always available. We implemented a novel solution for when it's not. Using new NaaS technology deployed strategically across the region, our client can not only comply with stringent security mandates, but can do it in a way that strengthens relationships with local communities.

Envisioning a New Network Edge

We had explored several alternatives to enable secure data upload in the field, including virtual private networks (VPNs) tethered to cellular connections. But given the lack of reliable connectivity, none were viable. Even when officers could establish a connection, the poor quality meant that VPN clients constantly dropped. We needed something that just didn't exist in much of rural South Carolina: wide-area network (WAN)-style security and performance, without having to build our own WAN.

Our firm had previously established a secure private network in the city center — basically just access points at various sites, where we owned the equipment and used the internet to VPN back to the city core. We realized that by extending this model to more dispersed locations, we could give officers more options for uploading data while deployed. The problem was, we didn't own sites in most of the areas where law enforcement routinely patrolled. But other organizations did. It was the seed of an intriguing idea: What if we asked them to partner with us?

The vision quickly fell into place. We would approach local businesses, churches, and other community organizations, and ask if they'd like to participate in our secure municipal network. Participation would be simple. Partners needed only have a secure edge device and access point deployed at their location and be willing to let us piggyback on their wireline broadband connection (typically at night, when it wasn't being used). Officers could then stop at these locations while out on patrol to securely, seamlessly upload their data. And participating sites would benefit from an increased police presence by default.

Inside the Implementation

The solution is based on Graphiant Network-as-a-Service technology, which aims to provide the security and guaranteed performance of MPLS WAN, without the cost or overhead of conventional site-to-site tunneling. First, we deploy a Graphiant Edge platform at the partner site, along with a dedicated wireless access point to provide a private interface. The edge device maintains a secure tunnel to the Graphiant Stateless Core Network (Figure 1, next page) — a high-throughput, stateless, multi-tenant private network that Graphiant controls. Officers can upload video and other data through the edge device, using a dedicated high-speed wireless connection. The data is then routed through Graphiant's private network back to the municipal core network and applications while remaining fully encrypted end to end.

The solution enables more flexible end-to-end privacy thanks to its unique architecture and stateless software-defined routing. Instead of establishing static tunnels between sites, edges need only maintain a secure connection to the Graphiant core. Using metadata programmed into

packet headers (based on policy we define), Graphiant's network can route each packet using the optimal path at any moment without ever decrypting the client's data. In other words, we gain a secure, private network from any edge site to our client's core network (or any other edge site or cloud), without having to configure and maintain site-to-site tunnels.

Building Better Edge Options

The new NaaS solution delivers a variety of benefits. First and foremost, it allows law enforcement personnel to spend more time in the field interacting with the community and less time in central locations waiting on the technology. At the same time, the model we've adopted involves building and strengthening relationships with local community organizations by design, a core tenet of this municipality's mission.

Sites used as edges will typically be locations where both the municipality and local residents want a greater law enforcement presence. For example, the first partner site, a community church, was having problems with mail theft. So, we designed that site with a designated parking spot for officers to use when uploading data. Officers now visit that spot multiple times throughout the night, where they have excellent secure connectivity—and an unobstructed view of the mailbox. Church leaders are thrilled with the arrangement, and they've already asked us to expand the partnership to a second location.

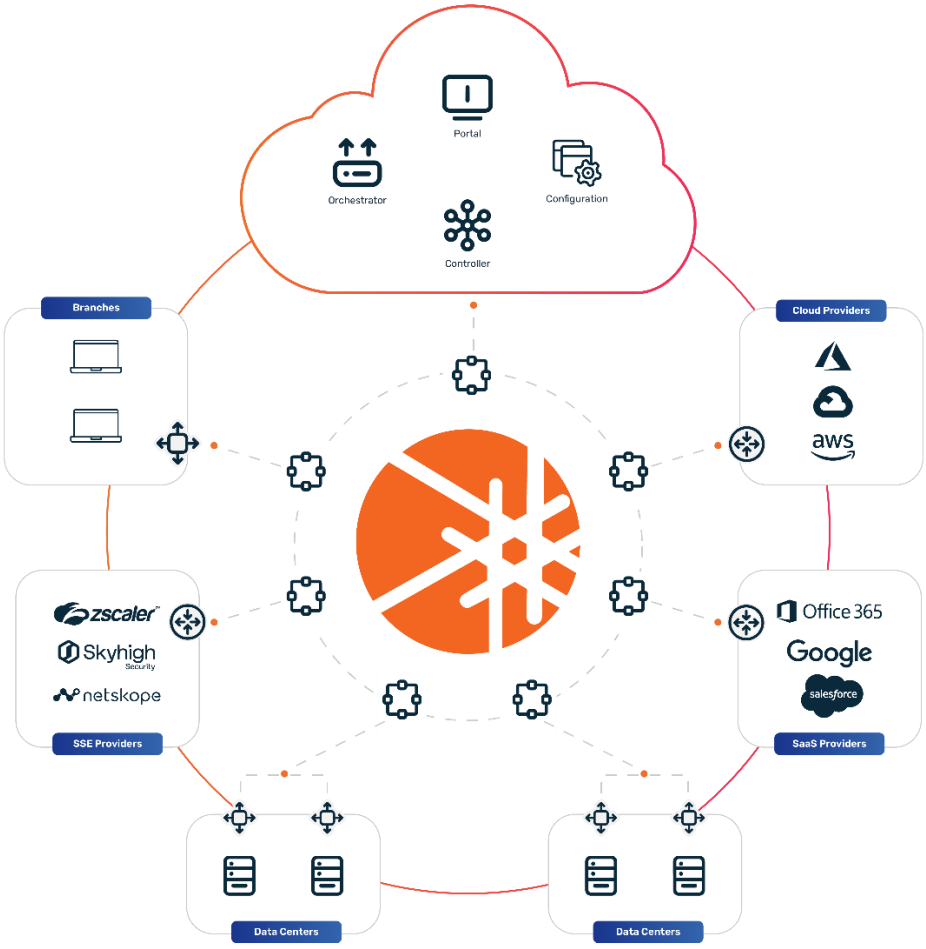

Figure 1- Graphiant Stateless Core

From a technical perspective, the NaaS solution has proven just as impressive. We've solved our client's longstanding problem, expanding secure high-speed connectivity to more areas where it's needed without adding more IT overhead. Once deployed, the edge solutions are basically zero-touch. There's no need to constantly update and maintain site-to-site tunnels, so the edges require far less time and attention from our staff, translating to lower costs for our client. (We're actually in the process of completely transitioning away from VPN at remote sites for this reason.) And since the NaaS solution is delivered as a consumption-based subscription, the municipality only pays for the bandwidth they use.

As we continue to add locations, we anticipate further benefits in the future. For example, Graphiant's private core network already offers direct high-performance paths to major cloud datacenters. As we move more of our client's environment to public cloud in the coming years, we'll likely see better performance than the existing municipal connection, along with all the other advantages of using what's effectively a dynamic private WAN.

Looking Ahead

It's hard to see our NaaS model as anything but a win-win. The municipality can empower officers with new technologies while strengthening its ties to the community. Local residents get more consistent law enforcement presence where they need it. Meanwhile, our own IT and security staff can keep the client securely connected and compliant, with far less effort and cost.

Just as exciting, we're demonstrating a novel public-private partnership approach to edge connectivity that can be replicated in any municipality struggling with similar issues. The challenges that come with unreliable or nonexistent network coverage are widespread, affecting rural and less-populous regions worldwide. Yet they're also strangely hidden, in the sense that many digital solutions don't even seem to acknowledge them.

When supporting rural municipalities, especially law enforcement officers in the field, you're unlikely to find prepackaged products that address their unique requirements. There just aren't many other segments that have mobile units collecting data, with stricter compliance requirements than most Fortune 500 companies. But that doesn't mean these problems can't be solved. Companies like Graphiant don't necessarily pitch their technology as a municipal law enforcement solution. But look beyond the buzzwords at what these technologies are actually doing, and you can find creative solutions.