

Zineb Crowe

CYSE 368 CRN 25090

ODU Spring 2026

Professor Teresa Duvall

TA Joshua Russel

Reflection paper 6: GEMSIS access issue

The GEMSIS access issue affecting a few users in Nautilus and Flank Speed has been resolved. This issue affected users for several months. What initially appeared to be a simple access issue required a multi-layered and multi-organization approach, involving network routing, IP whitelisting, and coordination with organizations such as DISA and Akamai as well as the Navy's enterprise teams. The issue affected users who had transitioned off NMCI to the Nautilus endpoints, and despite having the appropriate permissions and access on the NMCI based tools, users were unable to access the GEMSIS website until this issue was addressed.

An anomaly was noticed between how traffic from within Nautilus environments behaved in comparison to how traffic behaves within traditional NMCI environments. Traffic from within NMCI networks could resolve and connect to the GEMSIS website (<https://gemsis.disa.mil/>) without issues. However, traffic originating from within Nautilus environments would consistently return the error “You don’t have permission to connect” for all types of connections (Flank Speed Edge, VPN, Nautilus Virtual Desktop/NVD). This

anomaly was explored in detail, and after significant troubleshooting, it was determined that there were correct DNS resolution and routing on the Navy side, and that the issue was external to the local environment.

Our focus began to shift to the Akamai-hosted GCDS (Global Content Delivery Service) layer where the GEMSIS application is hosted. When accessing a site hosted on Akamai from a commercial or cloud-based environment, IP whitelisting is required and specific CIDRs (IP ranges) for Nautilus environments must be provided to the site administrator. The main challenge was identifying and providing these CIDRs. Initially we provided the internal IP range(s) for Nautilus environments but soon realized that the IP addresses that Akamai sees for a client are external NAT'd IP addresses. As such, the external NAT'd IP addresses for the correct environment(s) were ultimately whitelisted for GEMSIS.

This confusion and misunderstanding caused delays as we went through a couple of iterations of IP submissions and validations. Akamai logs showed the traffic coming from our environment was being blocked because the source IPs were not in the allowed whitelist. Additionally, some requests were missing client certification validation which complicated our troubleshooting process. The need to align internal understanding with how external systems interpret traffic highlighted the complexity of modern hybrid cloud environment, where internal configurations do not always reflect what external services see.

Collaboration among Navy, contractor, DISA and Akamai teams were key to resolving this issue. They constantly communicated through via emails and Teams meetings. GEMSIS personnel, Navy personnel, contractors, and Akamai engineers worked extremely hard to gather information such as test results, logs, and system configurations. Whitelisting specific sites required approval from GEMSIS leadership; the process involved many nuances. But all parties worked tirelessly and selflessly towards a fix.

After significant research, the correct external CIDRs for Nautilus Virtual Desktops were ascertained and entered in the Akamai system to whitelist Nautilus desktops. Updates were made for all relevant connection types (NVD East, NVD West, VPN East, VPN West) and access to GEMSIS has been working for all users. This is a significant development as it confirms that the root cause of the problem was IP-based access control at the application edge.

Incident resolution for GEMSIS was followed by positive changes in other processes performed by the team. We continue to provide external site administrators with external IP range for the various site-specific web servers. Proactive communication with points of contact for affected websites has been also improved. The team gained experience and increased confidence in approaching and troubleshooting future incidents like this one involving cloud providers and third-party hosting sites.

In conclusion, this GEMSIS access issue was so much more than a technical problem to solve - it was a full-on learning experience. We came to understand enough about how traffic flowed through the various system components and how different access

controls were implemented. Ultimately, we arrived at a workable fix and have since implemented changes that have worked well. Through this process, we learned a lot about ourselves and our approaches to problem solving. Primarily, we were reminded of the value of effective teamwork and flexibility in the face of constantly changing landscapes of cybersecurity and network infrastructure.