

Zineb Crowe

CYSE 368 CRN 25090

ODU Spring 2026

Professor Teresa Duvall

TA Joshua Russel

### Transport Team Bi-Weekly Accomplishments Essay

In the dynamic and highly secure military network environment, our Transport team has made significant strides in resolving persistent website access challenges on Nautilus machines. Facing a complex array of DNS resolution failures, certificate mismatches, authentication errors, and outdated routing configurations, we systematically restored access to critical resources across diverse connection types, Flank Speed Edge (FSE) for direct connectivity, Ubiquitous for always-available paths, VPN East and West for regional tunneling, and NVD East and West for virtual desktop routing. This comprehensive effort not only addressed immediate user disruptions but also established a robust framework for sustained operational reliability.

Our troubleshooting began with a thorough mapping of Nautilus's multi-path architecture, carefully designed to support both Atlantic (East) and Pacific (West) operations. By testing FSE, Ubiquitous, and VPN/NVD connections, we uncovered how legacy shortnames reliant on automatic DNS suffix appending in prior network setups failed outright in Nautilus environments. Even when VPN connections appeared active,

traffic was frequently misrouted to unwhitelisted endpoints, generating certificate warnings and authorization denials. This diagnostic precision enabled us to pinpoint and correct these anomalies, ensuring seamless failover between connection types.

Central to our success were targeted resolutions for DNS suffix and certificate issues. Nautilus systems lacked automatic appendages common in legacy networks, leading to pervasive access barriers. We documented essential suffix lists mirroring those from previous infrastructures and rigorously tested enhancements, particularly for critical services like print servers. Concurrently, updates to Big IP routing eliminated longstanding Flank Speed Edge blocks, including the correction of outdated taps that had been disrupting broad traffic ranges. These interventions restored consistency across all network pathways, transforming intermittent failures into reliable performance.

As Cloud engineers, we played a pivotal role, demonstrating mastery in overhauling routing tables that dictate traffic flow through our multifaceted network. We compiled consolidated lists of problematic sites, precisely categorized by optimal connection types, such as VPN West for specific resources or Ubiquitous/FSE combinations for others. Working in controlled NVD test environments, we refined next-hop directives, managed Network Address Translation (NAT) processes, and validated flows before production rollout. These precisely crafted tables overrode default firewall and peering behaviors, dramatically reducing mean time to resolution while accommodating leadership-approved workarounds for a faster ticket closure.

No less critical were our strategic partnerships with site administrators, whose collaboration proved indispensable for enterprise-scale fixes. Through proactive outreach, we delivered alternate access methods and coordinated backend authentication resolutions via CET support. Administrators verified optimal paths for FSE and NVD configurations, updated whitelists in response to our routing modifications, and bridged configuration gaps that had evaded detection behind isolated user reports. This synergy converted what could have been fragmented troubleshooting into cohesive, scalable solutions.

The outcomes of the past two weeks are both tangible and transformative. We validated full accessibility across every connection type for most sites, deployed production-ready routing tables, unblocked essential services like printing systems, and established rigorous tracking for permanent resolutions alongside immediate workarounds, though some website access issues persist.

Ultimately, this effort exemplifies integrated excellence, rapid support interventions complemented by sophisticated infrastructure engineering. Our layered approach, mastery of connection type diversity, precision routing table engineering, and administrator partnerships delivers resilient website access even in contested networks. By combining agility with strategic foresight, the Endpoint Transport team has not only resolved current challenges but positioned NNWC for sustained operational excellence in an ever-evolving cybersecurity landscape.