Modernizing Navy Tactical WAN, Afloat Networks, and Remote Site Connectivity with Versa Networks

Supporting next-generation network modernization priorities

Contents

Executive summary

The U.S. Navy is preparing for a significant shift in how its networks are governed, modernized, and delivered across platforms, hubs, fleet concentration areas, and global operations. As Afloat networks, Navy tactical WAN infrastructure, and transport services evolve under a unified governance umbrella and the Navy accelerates SD-WAN adoption, the need for a consistent, scalable, and secure edge architecture becomes increasingly critical.

Ships require predictable and resilient network performance while underway and the same experience when tied up at the pier. The Navy's target end state includes one gigabit per platform, ten gigabits per pier, and one hundred gigabits per fleet concentration area. Achieving this requires not only additional bandwidth, but an architectural shift that reduces complexity, supports Zero Trust, and enables centralized governance.

Versa aligns directly with these goals. Versa provides a unified SD-WAN and security architecture that simplifies ship to shore networking, supports bandwidth targets, strengthens security enforcement, and significantly reduces the amount of custom engineering currently required within Navy tactical WAN pier environments. Versa also provides a scalable, software-defined platform that fits naturally into centralized governance and long range modernization planning.

How Versa supports the Navy's FY26 and FY27 direction

Operational impact at the pier and fleet concentration area

Operationally, this approach simplifies how ships connect and how piers operate at scale. A Versa- based Navy tactical WAN architecture reduces the number of discrete network and security devices required at each pier, minimizes per- ship configuration changes, and shortens the time required to establish full connectivity when a platform ties up. Instead of rebuilding NAT rules, VLAN mappings, and enclave-specific routing for each arrival, network operators apply standardized policy templates that behave consistently across ship classes and fleet concentration areas. This results in faster ship pull-ins, fewer configuration errors, reduced accreditation scope at the pier, and a more predictable operational experience for both sailors and network operators. Over time, these efficiencies compound, directly reducing sustainment burden while improving readiness and availability.

A platform that fits under unified governance

Bringing afloat networks, tactical WAN infrastructure, and transport services under a single governance construct requires technologies that behave consistently across shipboard, hub, and fleet concentration area environments. Versa supports this requirement by providing a common set of routing, segmentation, and security capabilities that can be applied uniformly across all domains.

This consistency reduces architectural variation between programs, one of the primary obstacles to delivering predictable shipboard and hub side connectivity today.

An enabler for accelerated SD-WAN adoption

The organization has clearly stated its intent to accelerate SD-WAN adoption. Versa is purpose built for large, distributed, security focused environments and combines routing, segmentation, traffic steering, and Zero Trust enforcement into a single centrally managed platform. This significantly reduces manual configuration at the pier and simplifies enterprise wide governance.

Versa's support for identity-based routing reduces the number of ship specific configurations required when different ship classes arrive at a pier, directly supporting the Navy's objective to move toward standardized, policy driven network architectures.

Navy tactical WAN consolidation: Reducing hub-side complexity through platform unification

A persistent challenge within the Navy tactical WAN is the accumulation of point solutions at the pier edge. Traditional Navy tactical WAN architectures often include separate routers, multiple firewall platforms, standalone IDS/IPS devices, VPN gateways, and enclave specific security appliances. Each component introduces additional accreditation, sustainment, and configuration overhead.

Versa enables Navy tactical WAN consolidation by collapsing these discrete network and security functions into a single, software-defined platform. Routing, SD-WAN, next generation firewall, intrusion prevention, secure web gateway, Zero Trust access enforcement, and conditional access are delivered through the VersaONE platform as an integrated capability rather than as individually engineered systems.

This consolidation reduces physical footprint, power, and rack space requirements, and the number of devices that must be accredited and sustained at each pier. From a governance perspective, it enables standardized architectural patterns across fleet concentration areas, reducing site-specific engineering and accelerating deployment timelines.

Ship-to-shore modernization and high bandwidth targets

The Navy has established clear throughput goals: one gigabit per platform, ten gigabits per pier, and one hundred gigabits per fleet concentration area. Versa's architecture supports these performance levels by reducing protocol overhead, improving path selection, and removing many of the IPv4 centric barriers that slow ship to shore transfers today.

Consistent user experience for ships at the pier

Ships arriving at a pier expect immediate network availability. Today, overlapping IPv4 address space, NAT complexity, and enclave specific routing changes often delay connectivity and introduce errors. Versa allows multiple enclaves to be delivered over a single physical connection with clean logical separation, eliminating the need to rebuild temporary routing constructs for each mooring.

More reliable data movement

Versa improves ship-to-shore throughput and reliability by:

- Reducing reliance on NAT
- Supporting clean IPv6 end-to-end identities
- Using more efficient forwarding and traffic steering mechanisms
- Automatically and intelligently utilizing multiple available links

These improvements enable more reliable delivery of software updates, baseline pushes, container images, and other high-volume data, directly supporting operational readiness.

Tenant-based networking for scale, mobility, and operational flexibility

A key advantage of the Versa architecture is its support for tenant-based networking, which enables the Navy to scale more effectively while supporting dynamic operational movement. Tenants provide logical isolation that is independent of physical location, allowing ship networks, mission enclaves, and support environments to move without redesigning the underlying infrastructure. This enables ship-to-shore connectivity during operations, seamless transition as ships move between areas of responsibility, and consistent policy enforcement as platforms connect to different hubs or coalition networks. Tenants can also move between ships, supporting scenarios such as embarked staffs, mission teams, detachments, or temporary capabilities without readdressing or rebuilding network services. By decoupling identity and policy from physical topology, tenant-based networking allows the Navy to operate a globally consistent architecture that adapts to fleet movement rather than constraining it.

Operational vignette: Destroyer transition from Region A to Region B

A guided missile destroyer completes maintenance at a Region A fleet concentration area and prepares to relocate to Region B. While in Region A, the ship connects to the pier using a Versa-enabled Navy tactical WAN edge, where its assigned tenant provides access to maintenance networks, update repositories, training systems, and logistics segments. All routing, security policy, and segmentation are applied automatically based on the ship's identity, without custom NAT or ship specific reconfiguration.

As the ship departs Region A and transits to Region B, the same tenant and policy set remains intact. When the ship connects at a Region B hub, it connects to a different Navy tactical WAN installation that uses the same Versa templates and governance baseline. The ship's tenant is recognized immediately, and the appropriate networks are presented without redesign or manual intervention. Security policies, logging, and performance controls remain consistent across both locations.

During operations, the destroyer establishes ship-to-shore connectivity with another platform operating under a different tenant while maintaining strict separation between mission enclaves. Later, an embarked staff element temporarily moves from the destroyer to another ship. Their tenant moves with them, preserving access controls, logging, and Zero Trust enforcement without readdressing or rebuilding services.

From an operational perspective, the ship experiences a consistent network environment across regions. From a governance perspective, centralized governance board maintains uniform visibility, policy enforcement, and accreditation across Region A and Region B without ship- specific exceptions. The result is faster pier connectivity, reduced engineering effort, and a network architecture that adapts to fleet movement rather than constraining it.

Supporting a Navy-wide modernization roadmap

Simplified and consolidated architecture

Versa Secure SD-WAN simplifies enterprise networks not only through modern routing and IPv6 enablement, but by consolidating network and security functions traditionally delivered through separate appliances. Within Navy tactical WAN environments, this consolidation reduces reliance on complex NAT constructs, layered ACLs, and one off pier configurations designed solely to make disparate systems interoperate.

By providing a unified policy model for routing, segmentation, and security enforcement, Versa reduces vendor sprawl, lowers sustainment burden, and shortens troubleshooting timelines. This consolidated approach enables a predictable, repeatable pier architecture that can be governed centrally under centralized governance board oversight.

Alignment with Zero Trust

Versa ties routing and access decisions to identity rather than ports and IP addresses. This enables stronger Zero Trust enforcement across shipboard networks, hubs, and fleet concentration areas while simplifying threat detection, correlation, and response.

Ready for IPv6 and future network constructs

IPv6 is a foundational requirement for the Navy's future network architecture. Versa supports IPv6 natively, allowing gradual transition without operational disruption while enabling cleaner identity, simpler segmentation, and easier cross program integration.

Fit within a centralized governance board

Centralized governance depends on technologies that behave consistently, can be centrally monitored, and support standardized configuration patterns. Versa enables a centralized governance board to define templates, policies, and baselines that propagate uniformly across Navy tactical WAN hubs and fleet concentration areas.

A better way to deliver networks to ships

Versa addresses several long standing challenges within the Navy's hub to ship delivery model.

- **Automatic identification of ship networks**
  Ships no longer require unique NAT or VLAN modifications when connecting. Versa automatically applies routing and segmentation policies based on ship identity.
- **Multiple enclaves over a single physical interface**
  Versa delivers multiple fully isolated enclaves to a platform over a single connection, eliminating additional cabling and switch reconfiguration.
- **Consolidation as an operational advantage for Navy tactical WAN**
  By replacing multiple hub side appliances with a single integrated platform, Versa reduces configuration errors, accelerates ship pull ins, and improves first connection success rates. This consolidated model scales to support higher bandwidth and more dynamic mission requirements without a linear increase in complexity or cost.
- **Consistent performance across fleet concentration areas**
  Versa's SD-WAN core provides predictable, policy driven traffic management that behaves consistently across all bases, supporting the Navy's Way Ahead objectives.

Conclusion

Versa is strongly aligned with the Navy's FY26 and FY27 modernization priorities and provides a practical path to modernizing Navy tactical WAN. By consolidating network and security capabilities into a unified, policy-driven platform, Versa reduces hub-side complexity, lowers sustainment costs, simplifies accreditation, and improves ship to shore operational consistency.

This consolidation directly enhances readiness, resiliency, and the user experience for Sailors while enabling unified governance across Afloat networks, Navy tactical WAN infrastructure, and transport services. Versa helps remove unnecessary complexity from the Navy's shore and Afloat architecture, positioning the fleet for future bandwidth growth, Zero Trust adoption, and IPv6-enabled operations.

About Versa
Versa, a global leader in SASE, enables organizations to create self-protecting networks that radically simplify and automate their network and security infrastructure. Powered by AI, the VersaONE Universal SASE platform delivers converged SSE, SD-WAN, and SD-LAN solutions that protect data and defend against cyberthreats while delivering a superior digital experience. Thousands of customers globally, with hundreds of thousands of sites and millions of users trust Versa with their mission critical networks and security.

About Red Pill Resilience
Red Pill Resilience is a cybersecurity and systems engineering firm built for the U.S. Navy and DoW, delivering solutions across network modernization, DevSecOps, observability, and Zero Trust architecture. The company operates with deep familiarity across NAVWAR, PEO C4I, and PEO Digital, aligning emerging technologies to mission requirements in complex, constrained, and disconnected environments. Partnering with leading technology providers, Red Pill Resilience serves as a lab-driven, operationally grounded integrator for organizations operating at the edge of national defense.

Versa Networks, Inc
2550 Great America Way, Suite 350
Santa Clara, CA 95054
Tel: +1 408.385.7660
Email: info@versa-networks.com
www.versa-networks.com

Part# JSB_NAVYWANREDPILL-01.0