Why open standards-based, modular networks are key to

DOD multicloud migration

Modern multicloud platforms are proving pivotal in helping defense agencies scale faster and operate more securely in a multicloud world.

By FedScoop Staff

Defense leaders recognize the strategic importance of implementing an agile, reliable and secure cloud environment — one that can integrate and support both "general purpose" and "fit-for-purpose" clouds.

Acting Secretary of Defense Patrick M. Shanahan made that clear in DOD's ***cloud strategy,*** released publicly in February, saying: "The Department of Defense has entered the modern age of warfighting where the battlefield exists as much in the digital world as it does in the physical. Cloud is a fundamental component of the global infrastructure that will empower the warfighter with data and is critical to maintaining our military's technological advantage."

IT teams across DOD are already deploying cloud platforms capable of receiving data, hosting applications and processing information critical to enabling and supporting their mission initiatives. They're also tackling the work of migrating existing applications to the cloud and developing new, cloud-native applications.

But even DOD officials concede the Pentagon's cloud strategy depends on another critical step if it is "to make full use of the data, applications, security and resiliency cloud computing can provide," the document said. That's to design and develop a multicloud, multivendor networking environment with a unified cybersecurity architecture and simplified operational command and control.

Designing a future-ready network

While the scale and complexity of DOD's transition to a cloud-ready world is enormous, so is the potential for leveraging modern, tried-and-tested networking solutions that can integrate disparate public, private and hybrid clouds into an agile, secure and ubiquitous infrastructure.

A recent study by IDC assessed the impact of deploying enterprise-scale networking solutions from one leading provider, Juniper Networks, at large-scale organizations worldwide. Each of the organizations were supporting data center networks fraught with complex architectures, cumbersome IT plumbing, significant operating costs, but perhaps more fundamentally, they lacked the fitness and flexibility needed to support future requirements.

The experiences and benefits those organizations reported, after deploying Juniper Networks products and technologies in their data center networks, were eye-opening:

361 percent five-year ROI

56 percent lower cost of operations

30 percent lower network infrastructure cost

11 months to payback

44 percent more efficient network infrastructure staff

3 times more staff time for innovation

41 percent improvement in application performance

98 percent less unplanned downtime

*Source: **IDC White Paper** (Sponsored by Juniper Networks)*

Corporate users in the study also reported being able to scale and deploy workloads where they were needed much more quickly and confidently.

"So much of the journey from where enterprises are to where they want to be is determined by the obstacles along the way," ***observed Bikash Koley***, chief technology officer and executive vice president at Juniper Networks. "If they do not understand what those obstacles are, it is difficult to plan to overcome them."

From a networking perspective, he suggested IT and networking leaders must ensure their network design solves for five factors:

1. Multi-domain connectivity
2. Multi-vendor orchestration
3. End-to-end visibility
4. Pervasive security
5. Reduced complexity

"These primary challenge areas will lead to natural points of emphasis in architectures and create constraints within which solutions must be designed," he said. (He pointed to a ***technical guide*** Juniper Networks offers to network and cloud architects as a partial roadmap.)

The added challenge for government organizations is they "don't really know what the future will hold as far as what percentage of their workload is going to be in the cloud and where the applications they are purchasing are going to be developed — and what platforms they need to manage to be able to support them," said Ian Peterson, a senior engineer at Juniper Networks, in an interview with FedScoop. "Another uncertainty is what security mandates are going to come down the pike."

Large-scale organizations deploying enterprise SDN networking solutions reported:

56%
lower cost of operations

41%
improvement in application performance

98%
less unplanned downtime

44%
more efficient network infrastructure staff

3
times more staff time for innovation

*Source: **IDC White Paper** (Sponsored by Juniper Networks)*

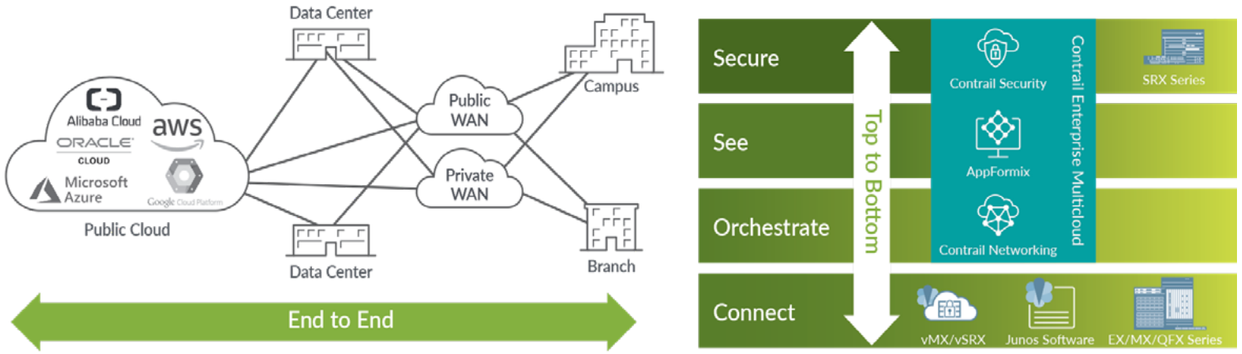


Figure 1: End-to-end and top-to-bottom multicloud design

Source: Juniper Networks

Accelerating multicloud agility at scale

The best way forward given the unknowns, say engineers like Peterson, is to move toward a single software-defined networking (SDN) platform model (Figure 1), capable of spanning physical, virtual and cloud infrastructures and readily able to handle:

- Overlay and underlay network management.
- Heterogeneous compute environments, including bare metal servers, virtual machines, containers and networking devices.
- Private and public clouds as well existing data centers.
- Networking and security orchestration policies, including micro-segmentation.
- Advanced analytics.

SDN platforms such as Juniper Network's ***Contrail Enterprise Multicloud***, for instance, give organizations the ability to manage essential networking tasks between the physical infrastructure, underlay network and the virtual networks overlaying that infrastructure.

They also streamline the process of "network service chaining." That gives network operators the ability to connect firewalls, network address translation services, intrusion protection and other capabilities into a virtual chain and assemble them in a catalog of connected and more rapidly-modifiable services.

Additionally, platforms like Contrail Enterprise Multicloud offer greater long-term flexibility, by using open standards protocols and data models, such as Ethernet VPN (EVPN) technology that can be used to interconnect Virtual Extensible Local Area Network (***VXLAN***) networks.

"Leveraging open standards allows you to take advantage of the best of the best without being locked into a vendor," said Mike Loefflad, systems engineering manager at Juniper Networks. It also supports a wider range of APIs for more seamless integrations.

That gives DOD units the ability to establish a more agile, scalable and ubiquitous network model, rather than having to focus on maintaining hundreds of independent networks, he said. As a result, they can scale and deploy applications faster. And they are better prepared to accommodate the growing use of mobile and Internet of Things devices and other endpoints to a network.

That's especially important for DOD network operators charged with supporting systems and applications on premises, in the cloud and at the tactical edge. It's also critical to their efforts to seamlessly move toward, manage and operate a combination of general purpose and fit-for-purpose cloud solutions.

Meeting cyber challenges

Beyond that, however, the new breed of SDN platforms like Contrail Enterprise Multicloud also give network operators substantially more capabilities to safeguard multicloud networks.

The ability to monitor, analyze and manage network overlay and underlay activity — across multiple vendors' systems and equipment — means operators have greater visibility and can diagnose and respond to security issues faster and more effectively. Operators, for instance, can isolate a server at the hypervisor level and restrict traffic from moving laterally within a virtual machine or to nearby machines.

Additionally, the ability to automate and deploy unified multicloud policies ensures that application platforms in both private and public clouds adhere to the same rules. Contrail Enterprise Multicloud goes further by implementing an "intent complier" which translates high level workflows into specific rules and policies for faster provisioning and automated network and security service chaining.

The result: Security controls can be deployed and enforced more universally — but they also can be adjusted and orchestrated more rapidly as attack surfaces and cyber threats continue to change.

Extending tactical support to the edge

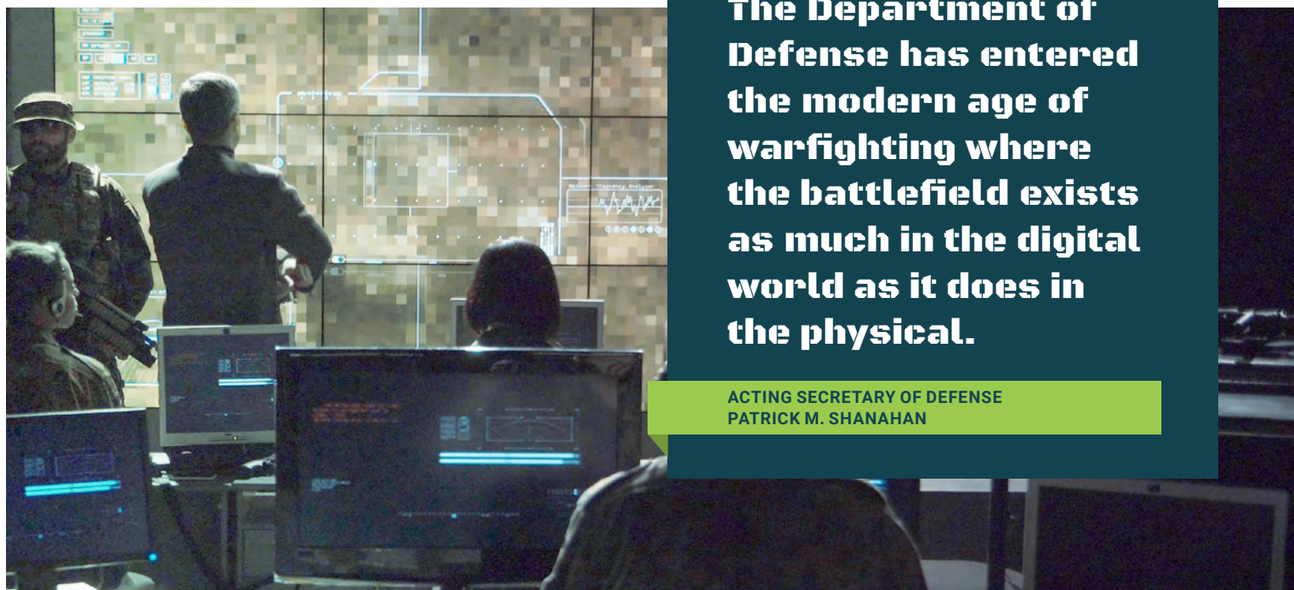
Perhaps the most important reason for implementing an SDN platform like Contrail Enterprise Multicloud is the substantial leverage it offers IT teams to extend tactical support to the warfighter at the edge. It gives DOD the ability to:

1. **Reduce locating network specialists all over the world.** Centralizing and simplifying network provisioning, orchestration and management lowers IT training and support costs and allows IT staffs to focus more on mission imperatives.
2. **Increase network performance and reduce application downtime.** That translates into greater reliability and resiliency across multiple cloud environments, giving warfighters and support teams more consistent access to real-time intelligence and analytics and greater agility on the battlefield.
3. **Capitalize on the continuous advances** being made by the private sector and emerging best-of-breed providers without getting locked into one or more vendors or proprietary applications. That means warfighters and end users across DOD are more likely to benefit sooner from the latest digital tools industry has to offer.
4. **Reduce network operating and support costs dramatically,** by streamlining multicloud network management, reducing bottlenecks and leveraging automation, giving DOD leaders the opportunity to devote resources to more innovative uses to support the warfighter.

*Find out more about how modern **software defined networks**, designed for multicloud operations, and tools like Juniper Networks' **Contrail Enterprise Multicloud**, can accelerate the Defense Department's cloud strategy.*

This special report was produced by FedScoop and sponsored by Juniper Networks.

fedscoop JUNIPER NETWORKS



> "The Department of Defense has entered the modern age of warfighting where the battlefield exists as much in the digital world as it does in the physical.
>
> ACTING SECRETARY OF DEFENSE
> PATRICK M. SHANAHAN