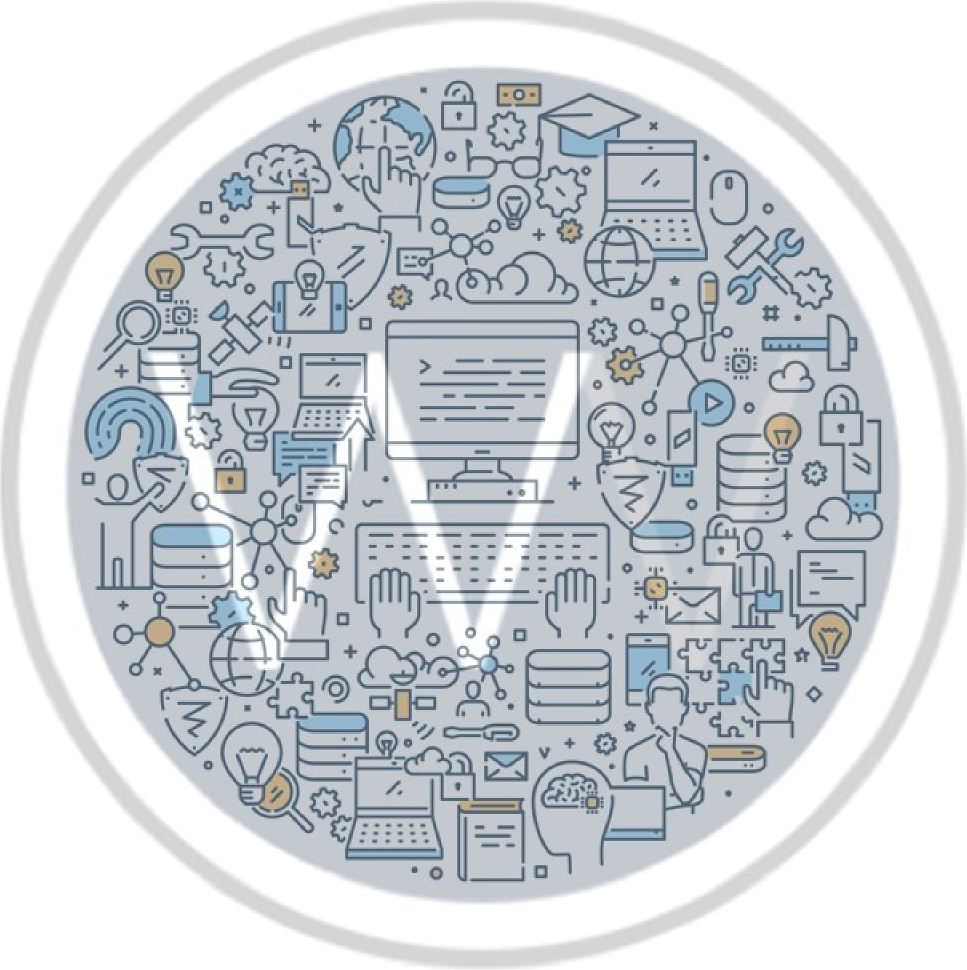
WINDVAL
technology solutions
Windval Advisory Services and Technical Solutions



Advisory Spotlight: Network Transformation

Windval Solution Guide – April 2020

Accelerate Network Transformation

with a modern approach to network segmentation and software defined networking.

Introduction

The primary purpose of this solution guide is to discuss the important intersection of three related topics in today's networking and cybersecurity landscape: Network Transformation, Software Defined Networking, and Network Segmentation. Any one of these three topics is deserving a technical deep dive, but this short technical solution guide is intended to provide high-level background on each of these topics, share how they interrelate, and discuss why they are each important in today's modern digital infrastructure.

Network Transformation

Network Transformation is an essential component of a modern, information-driven, digital transformation program for companies and their IT teams and is much more than just a buzz word today. Nearly everything and everyone in the modern technology world requires "always on" network connectivity to reach IT assets, whether they are on the internal corporate network in a datacenter, an IoT edge computing resource in a manufacturing plant or in a public or private cloud over using private or Internet connections. Today's wired and wireless networks are the technology lifeblood to make the connection to all things digital (users to systems and systems to systems). Networks must keep pace with the demand for high performance, high reliability and modern features to make the digital infrastructure agile, cost optimized and easier to manage. Networks can no longer be considered "Just speeds and feeds" or "plumbing to move packets!" Instead, networks need to be modern, agile and keep pace with the software defined and cloud computing principles of the modern IT technology industry.

Refreshing an enterprise network needs to be approached as an on-going effort and needs to be carefully planned. Gone are the days when you could install a network, walk away and not think about refreshing products and capabilities until the design, products and technology is obsolete and out of support. A network equipment refresh is an opportunity to evaluate priorities and introduce new capabilities to evolve and transform the IT environment. Product refresh intervals are a good time to evaluate changes for transformation including manufacturer and product selection, required or desired features and capabilities, new technologies and new design principles to fortify the mission of the network.

Software Defined Networking (SDN)

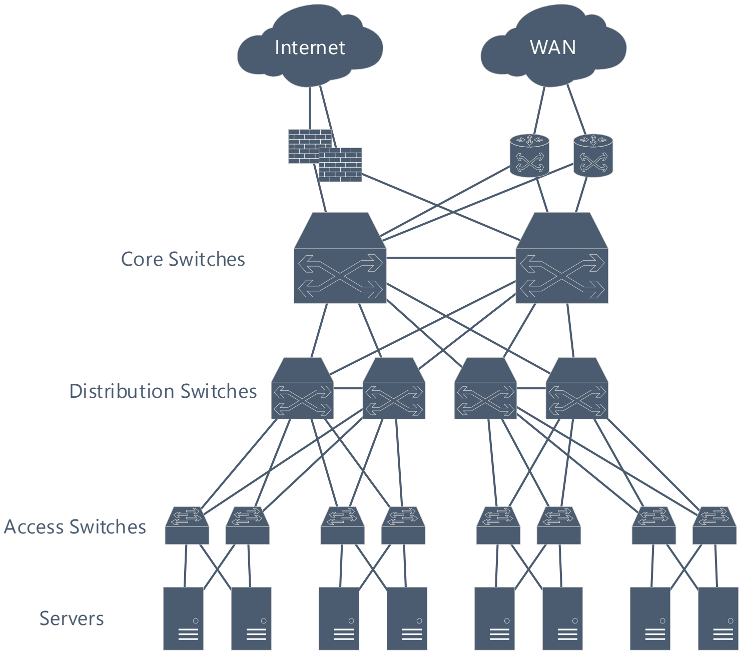
Software Defined Networking (SDN) is a small term that can encompass many things. In general, software defined networking is the practice of separating the control/management plane in a device from the data-forwarding plane in order to allow programmability to centrally control, provision, manage and monitor a collection of network devices as one logical system. Whereas traditional network management provisioning and monitoring was performed manually, on a device-by-device basis, SDN programmability leverages application programming interface (API) access to provision, control and monitor devices to allow for easier administration and provide possibilities for automation through scripting and programming. The collection and analysis of operational data from SDN-controlled devices supports the desire and need for more analytics to monitor, measure and troubleshoot a modern network as a system using network devices and their inherent intelligence to provide insights to administrators. SDN has been evolving in the industry for over ten years and continues to do so as it moves into practical applications that can and need to be implemented in a modern IT environment. Large, dynamic networks with many repetitive tasks that can be automated should consider implementing SDN technology.

SDN is a large and non-trivial set of topics. In a typical enterprise network, it is common to decompose specific SDN use cases into different portions of an enterprise network architecture because industry is evolving and implementing SDN technologies at different paces in different functional areas of an enterprise network architecture.   The ultimate goal of a SDN-driven enterprise network is to seamlessly orchestrate the entire enterprise network, end to end, with a common set of tools, polices and intent. The three most common areas for SDN implementation in a typical enterprise network architecture include: datafcenter, campus and wide area network (WAN).

Datacenter SDN

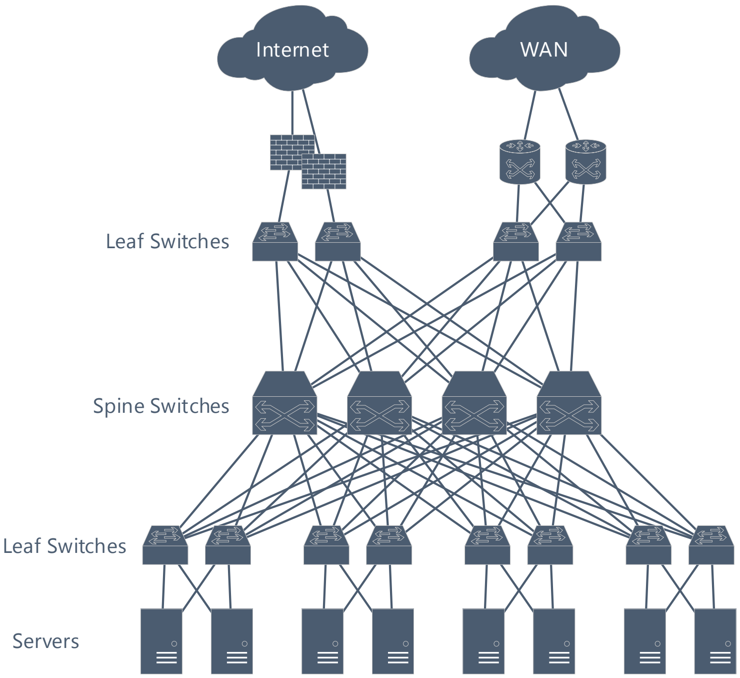
Today's modern datacenter or cloud is moving to a full software defined state and is commonly referred to using the overarching term software defined datacenter (SDDC). Compute virtualization, storage virtualization, database virtualization, network virtualization and other functions have or are moving to a software-defined paradigm. It follows that the network needs to keep pace and take a similar approach. It does not make sense to have programmability and automation in place for many datacenter technology functions only to be relying on a legacy, non-adaptive, manually provisioned datacenter network. By having all technology stacks software defined, their integration, programmability and automation can ideally be stitched together and orchestrated as a coordinated system across all technology functions.

Datacenter network architectures and topologies are changing as well to drive simplicity, high performance, high reliability and reduced costs. Traditional datacenter network topology designs were typically implemented using a 3-tier model of core, distribution and access layers (see diagram) to scale performance and function across multilayer switching products. This design served the industry well for many years and was ideally suited for the "north-south" flow of traffic between users and systems in the datacenter logically grouped into multiple functional towers or pods. As application architectures and technologies changed, so did traffic flows. In addition to north-south traffic flows, system to system flows or "east-west" became important because of the decomposition of software functions across the datacenter. This shift placed a burden on traditional hierarchical datacenter network designs and caused performance bottlenecks within the 3-tiered model. In order to support ultra-high performance, reduced network latency resiliency to hardware and link failures in the datacenter, as well as the elimination of legacy layer 2 topology management protocols such as spanning tree protocol (STP), a new network architecture design model was needed.



Traditional 3-Tier Data Center Network Architecture

New spine-leaf designs became favored due to their simplified topology, the advance of higher performance switching technology, higher Ethernet link speeds technology such as 100Gbps and 400Gbps. In addition, the use of a SDN-driven software defined virtual overlay network provides "any-to-any" layer 2 or layer 3 communication between any two points in the datacenter network in a very efficient fashion while eliminating design and operational challenges such as STP with layer 2 requirements. The advances in spine-leaf design and SDN technologies also significantly eliminated physical location dependence of any device or software function across the physical footprint of entire datacenter. Any device, software function or service could be placed physically and logically anywhere irrespective of physical dependencies of the traditional 3-tier designs of the past. This gives datacenter managers tremendous operational flexibly, scalability and agility for rapidly changing dynamics of technologies and devices in the datacenter.



Spine-Leaf Data Center Network Architecture

A network-oriented approach to datacenter SDN can be categorized two way. One is a network-centric approach where the network fabric is virtualized to take advantage of a spine-leaf design as it abstracts the physical layer of the network and provides an overlay capability for layer 2 and layer 3 communications in an any-to-any fashion. The second approach is an application-centric model that builds on a network-centric approach and provides application-layer granular visibility and control by allowing or disallowing communication across the network fabric based on application traffic aware polices.

While the network centric approach can be used to segregate or macrosegement devices and traffic based on traditional logical constructs such as layer 2 ("vlans") or layer 3 ("subnets') boundaries, the application centric approach allows a more microsegmented approach where granular level traffic constrainment can be done down to a physical or virtual device level through software defined policy. Application centric style of fabric operation is more granular and powerful from a control standpoint, but it tends to increase administrative complexity from an operations standpoint because traffic flows must be fully and accurately defined to ensure the network policy allows complete and successful communication between intended devices and ports/protocols.

Because the IT systems, applications and data "crown jewels" sit in the datacenter (or cloud), increased rigor to secure the environment for modern day inside and outside threats cannot be overemphasized. This is why IT teams need to seriously consider a modern transformation of network and security to enhance and protect. We will discuss the concept and power of microsegmentation further in a section below.

Campus SDN

Similar to granular traffic control in the datacenter, SDN technology can also be used in campus networks to perform access-level control of users and their devices and other special devices to the network. SDN in the campus involves defining granular traffic polices to allow or limit users and devices distributed across enterprise locations to access other systems on the enterprise network. While traditional networks have and generally still allow access to "everything" on the internal enterprise network, increasing security threats are driving network architects to limit or prevent network communication at the user/device access layer whether it is a wired or wireless device[1]. This capability is also and especially powerful and important for the rising use of Internet of Things (IoT) devices and technology across the enterprise environment. IoT devices typically require special traffic control or segmentation to isolate their function from the general network population and vice versa. Examples of traffic segmentation needs for security reasons include many physical security technologies such as building management systems (HVAC, lighting, etc.), IP-based security devices such as IP video surveillance and sensing controls as well as physical access control systems and badge readers. Beyond these common examples in all common building types, special environments such as manufacturing or operational process control systems also require stringent cybersecurity handling and isolation. Whereas the segmentation of these special systems used to be done with traditional mechanisms such as firewall appliances, the growth and proliferation (and in many cases mobility) of IoT for many use cases requires a software defined approach to simplify and provide consistent and secure access control and visibility across the network.

Campus SDN controls users, user devices and applications' access to the enterprise network at the access layer of the campus network, where datacenter SDN solutions control access to/from and between systems within the datacenter and across the greater enterprise network. The easy and effective threat vectors of email and web browsing at the user device level for phishing and ransomware exploits has significantly raised the focus and priority on reducing or eliminating unintended, unauthorized network communication to all internal areas of an enterprise network. Both datacenter and campus SDN demand careful consideration and prioritization for implementation.

Wide Area Network (WAN) SDN

The WAN is also leveraging the power of SDN in software-defined WAN (SD-WAN) solutions. This area of the industry is currently seeing the most activity and adoption of SDN technologies for similar reasons we discussed in datacenter and campus SDN solutions but it is further accelerated by the increased need for network resilience, traffic path optimization across different technologies and the use of public cloud computing. All of these drivers make SD-WAN a solid modern choice for adding flexibility, agility and cost optimization compared to traditional WAN designs and technologies such as Multi-Protocol Label Switching (MPLS). SD-WAN is centrally controlled in almost all designs and separated from the data plane path which makes a cloud-based, control plane commonly used.

Beyond the ease of use and flexibility SD-WAN provides to ensure secure network transport across a wide variety of technologies and topologies, it also allows for traffic segmentation over the WAN for different classes or virtual private networks (VPNs). For example, if you wanted to extend traffic segmentation for users and IoT devices from a branch office back to the datacenter and maintain strict data traffic isolation while transporting data over the WAN, SD-WAN could be used to route traffic for users and IoT devices in separate and secure virtual domains that have no visibility or awareness of each other. This SD-WAN capability is powerful from a security standpoint because SDN domains at datacenters, office buildings or branch offices can be logically isolated, carried and extended between sites for different security zones.

Given the focus on microsegmentation in this paper, datacenter and campus SDN use cases for microsegmentation are most relevant compared to SD-WAN.

Integrating Multiple SDN Domains

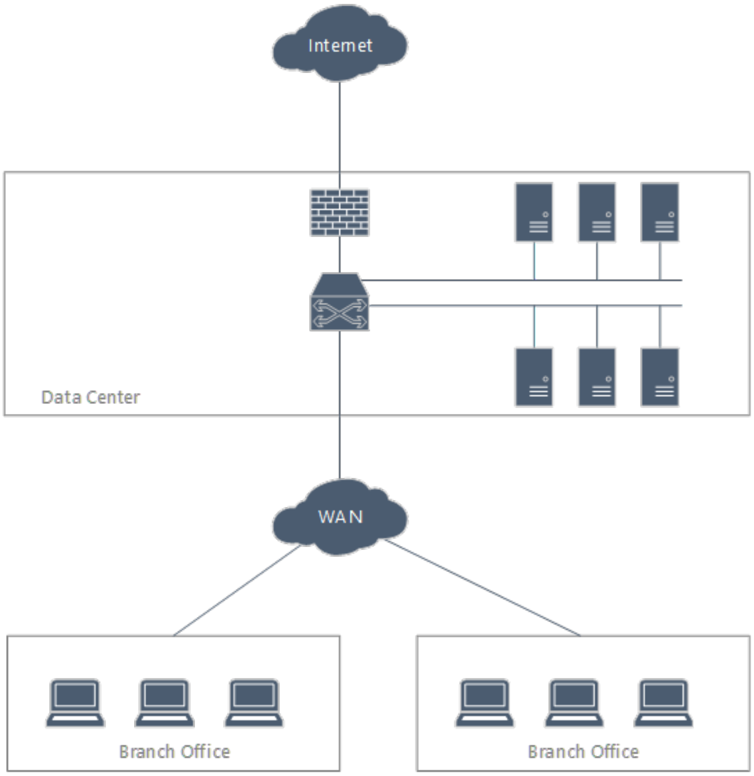
As discussed above, SDN can be a powerful solution in datacenter, campus and WAN environments. Many of these solutions evolved individually and on different product families from different manufacturers. An end to end architecture approach is evolving in the industry to allow SDNs of all types and flavors to integrate with one another so that a common policy framework can be carried end to end across an enterprise network providing the true benefits of SDN across dissimilar portions, products and functions of the enterprise network. This enterprise-wide architectural approach to SDN remains an active work in progress in the industry.

Network Segmentation

Traditional Approach

The ineffectiveness of using only perimeter defenses…

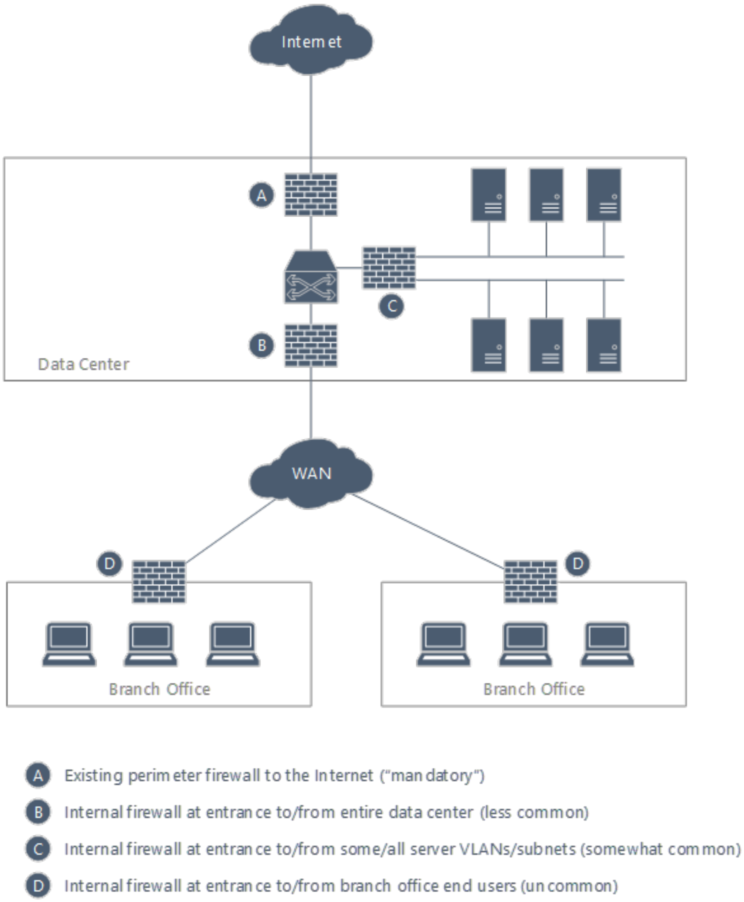
In traditional enterprise network design, a perimeter defense system was common. In this model, security devices such as firewalls would provide traffic control and separation from external networks (such as the Internet or 3rd party business partners) and the internal/private enterprise network. Perimeter defense designs were effective for many years but as the increased use of the Internet and sophistication of cyber threats and malware blossomed, it became clear that a perimeter-only defense design was no longer effective to thwart modern-day threats. Today, it is not a question of if, but when, cyber threats exist on the inside of the corporate network. Many IT and cybersecurity teams fully realize that internal corporate networks are vulnerable and may likely already be compromised, so new techniques and protection mechanisms focusing on "zero trust" are needed to provide adequate protection.



A traditional perimeter defense design with a firewall between the Internet and the enterprise network is shown in the diagram above. To be clear, without further protection in the network and/or systems across the enterprise network, traffic can flow freely between any two systems across the environment in this dated model and approach to perimeter-only security.

"Macrosegmentation"

Beyond the ability to program and automate the administration and management of a network using SDN, one of the most powerful capabilities of SDN technologies from a cybersecurity standpoint is the ability to restrict, isolate or segment users, devices and application traffic based on a robust security policy.


Internet
A
C
B
Data Center
WAN
D
D
Branch Office
Branch Office
A Existing perimeter firewall to the Internet ("mandatory")
B Internal firewall at entrance to/from entire data center (less common)
C Internal firewall at entrance to/from some/all server VLANs/subnets (somewhat common)
D Internal firewall at entrance to/from branch office end users (uncommon)

In traditional networks, firewalls were used to restrict traffic flows based on security policy between groups of devices or segments of the network. While this design method could control traffic flows between groups of devices, it did not have the reach to extend the traffic control policy to each user or device hence the term "macrosegmentation" is used for device-group level traffic control. While effective in some use cases and environments and better than no traffic segmentation at all as previously discussed, it does not provide the granular and detailed control down to an individual user device or server level required to combat modern day cyber threats. A high-level diagram showing examples of "macrosegmentation" is shown above.

Microsegmentation

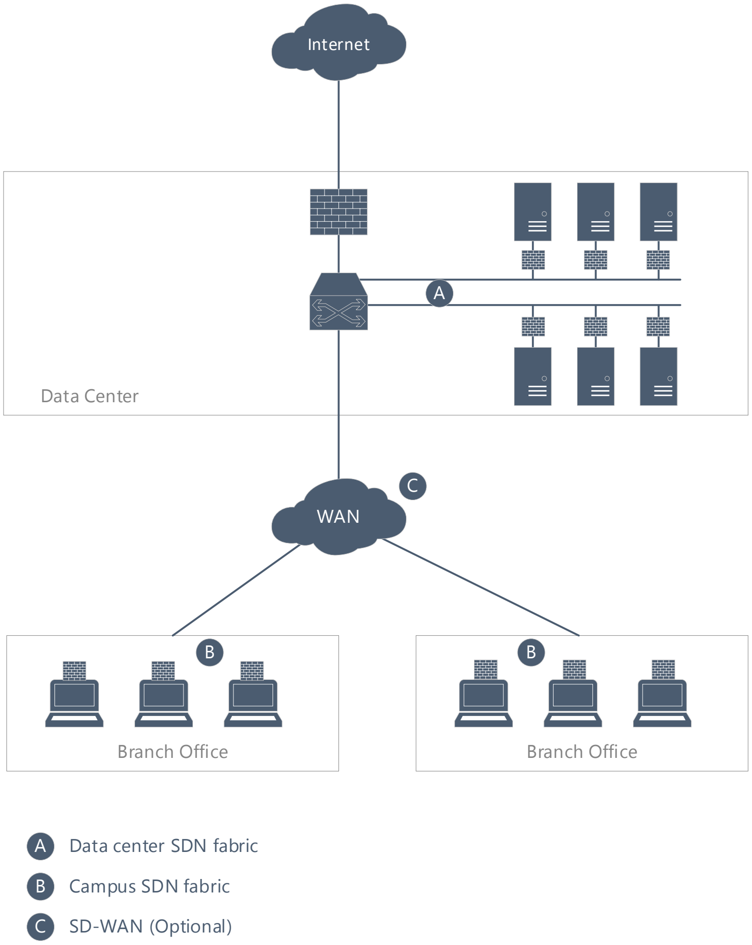
Microsegmentation is not a new topic but it has become increasingly important in a world with aggressively evolving cybersecurity threats. Zero trust and the inability to be confident in a wide open internal corporate network communication model is forcing this topic to be strongly considered and implemented more often.

As mentioned in the introduction above, Microsegmentation is a design method of creating more granular security zones to compartmentalize devices and application workloads from one another as well as "external" users and systems to offer more granular and individualized security, control and visibility. Whether you think this is best implemented in the datacenter (or cloud) or at the user access level in a campus setting or both, this topic is important and requires careful consideration.

There are many solution approaches to microsegmentation and as many industry opinions to match about what architecture and implementation is best. Some believe it should be performed by the trusted network infrastructure and can only be realistically enforced there while others believe it should be software mechanism or agent on user or datacenter systems, operating systems and applications. Like many technology tradeoffs, there are pros and cons to every approach/architecture and sometimes the answer may not be exclusive to one solution but perhaps a combination of mechanisms based on technical, financial, operational, risk and security consideration, scale and practicality.

The diagram to the right illustrates the high-level concept of granular microsegmentation and traffic enforcement at the level of each client and server using a SDN-based approach.

Today, microsegmentation as a concept and need is growing in enterprise networks. Unauthorized people and/or devices should NOT have access to sensitive systems and data. Microsegmentation is one defense tool in a series of many that deserves serious consideration by IT and security architects.



Bottom Line

Network transformation is real. It is an essential component of developing modern and agile digital infrastructure capabilities. Transformation should not be looked at as an occasional refresh event that occurs every five to ten years, but rather, an ongoing organizational effort to modernize and introduce new capabilities on a pragmatic basis. It is important to understand how stagnation and comfort zones impact organizational transformation efforts. It is equally important to recognize that proactively mitigation security threats and supporting modern IT requirements require new ways of thinking and new ways of implementing.

Transform the environment; do not just refresh traditional capabilities and designs.

SDN is a powerful technology that will continue evolve and improve. Application and use cases in an enterprise environment can be debated, but every organization needs to evaluate technology capabilities and the positive (and negative impacts) SDN can have in some or all portions of a modern digital infrastructure.

Ideally an end to end architecture approach that can build a unified, enterprise-wide awareness and capability set is a key goal for most companies. SDN (as with Microsegmentation) does not have to be an all or nothing approach. It can be selectively implemented with careful thought and planning. A practical roadmap for expansion that makes sense for your environment is a solid approach to adopting and benefiting from SDN.

Segmentation as a concept in the network and cybersecurity worlds has real merit. The degree macrosegmentation and/or microsegmentation is implemented can, and will, vary based on the needs and drivers of each business and IT ecosystem.

Even if full deployment of microsegmentation at the user access and datacenter access layers are not prudent or practical for an end to end implementation, there are still likely "selective microsegmentation" opportunities that should not be dismissed. For example, new artificial intelligence (AI) and machine learning (ML) based software to protect and control endpoints might be the best approach for a user/end user device whereas in an IoT intensive environment, the IT network team still needs SDN-capable abilities to macro and micro segment for various use cases and needs. It does not need to be an all or nothing approach for microsegmentation but having the ability to do it successfully when, and where, you need it is a key goal.

Each of these topics and the combination of them is not trivial and requires thoughtful planning and execution. How do you approach Network Transformation? Are you using, planning, or not ready for SDN? How important is a scalable microsegmentation capability in your environment?

Windval experts are ready to assist your network transformation, SDN and segmentation vision, strategy and execution plans. Schedule a discovery consultation with Windval today and learn more about our digital infrastructure expertise and how we can help you accelerate your IT transformation journey.

contact@windval.com
312.801.6282
https://www.windval.com/contact

About Windval

As used in this document, “Windval” means Windval Technology Solutions LLC.

Windval is a technology consulting organization delivering advisory services and custom technical solutions that enable enterprise organizations to optimize legacy investment, integrate modern technologies, and deliver new capabilities that transform their business.

[1] Modern IT teams are increasingly operating in a zero trust cybersecurity model and view the enterprise network as a form of “private Internet” where all systems at the user access layer or the datacenter access layer need to be protected and not assume trust and security of the internal corporate network. Modern cyber threats can emanate at the user device level or at the datacenter system level and spread laterally in an unintended manner.