ConRes
CONTINENTAL RESOURCES

How to Implement Network Segmentation: **Virtualization is a Must**

How to Implement Network Segmentation: **Virtualization is a Must**

To say that today's networks face unprecedented challenges is an understatement. Every year, networks become larger and more dynamic, with potential threats coming from outside as well as inside your environment. From devices to data, hackers to employees, threats are everywhere and becoming more sophisticated and destructive.

A recent survey of IT professionals revealed that cybercriminals are seen as the greatest security threat to an organization, with 43% identifying them as one of their top three threats.[1] Hackers are designing ever-more disastrous malware attacks (self-propagating, network vector ransomware like WannaCry, NotPetya and Locky) which cost companies billions of dollars worldwide. And every device is at risk; **2017 saw 42.7 million mobile malware attacks affecting 4.9 million Android users alone**.[2] This is especially concerning as 87% of companies are dependent to some extent on their employees' ability to access mobile business apps from their personal smartphones.[3]

Also placing networks at risk is the explosion of unstructured data, which is growing at a rate of 62% annually.[4] Yet 80% of enterprises lack visibility into their unstructured data and are uncertain how to manage it.[4] The grim reality is that if enterprises do not understand which data is critical, where it is stored, how it is used and who has access to it, the more at risk that data can become. What's more, this data needs to remain secure as it is being moved in and out of the cloud.

Another concern facing network architects and administrators is that data governance and compliance standards are constantly changing, requiring security protocols to evolve along with them. Only 27% of executives report their company has a change management process in place to identify and incorporate changes in laws and regulations.[5]

Other organizational threats that landed among the top security concerns included software vulnerabilities (34%), application vulnerabilities (26%), and authorized users or employees (20%).[6]

2017 saw 42.7 million mobile malware attacks affecting 4.9 million Android users alone.[2]

Network segmentation is **only the beginning**

Network segmentation is the process of splitting your network into different subnetworks, which each have their own policies. This allows you to customize access, granting users access only to the data and applications they need to do their jobs — nothing else. The point of segmenting your network is not necessarily to prevent intrusion; the reality is that you will have a breach at some point. Instead, network segmentation works to contain and eliminate malicious activity in a single subnetwork before it propagates across your entire network.

Surprisingly, **while 75% of IT professionals polled strongly agree that network segmentation is an essential security measure, only 23% say their organizations actually employ network segmentation**. The number one reason why, according to those polled, is that it is too complex to implement.[7]

Indeed, segmenting access down to the user, device, application and dataset level can be an extremely difficult task, and one that is never complete. Just as external threats and internal use cases evolve, so must your segmentation strategy and policies. In pursuit of a secure environment, setting up your network incorrectly can also result in poor computing experiences.

Using a combination of firewalls and virtual local area networks (VLANs) is a common way to segment traffic within a network and prevent unauthorized lateral movement. However, it only takes one compromised device to allow hackers into your network, so endpoint security controls such as anti-malware, intrusion prevention and data loss prevention must also be put into place.

What's more, if you implement segmentation to contain perimeter or endpoint breaches, it can become more difficult to spot vulnerabilities since you're required to configure your vulnerability scanner for each individual segment.

Virtualization takes segmentation to the **next level**

Traditional network segmentation prevents unauthorized lateral movement within your network to help keep malicious activity contained. Micro-segmentation does the same thing, but on a much more granular level with flexible security policies that can be applied and even automated all the way down to an individual workload, virtual machine (VM), operating system, application or other virtual security target. Using micro-segmentation, IT administrators can define a security policy based on type of workload (web, app or database), where it might be used (development, staging, production) and what kind of data it will be accessing (financial, patient or other sensitive data). Micro-segmentation also helps administrators maintain security over workloads as they move them to and from the cloud.

*While **75% of IT professionals polled strongly agree that network segmentation is an essential security measure**, only 23% say their organizations actually employ network segmentation.*[7]

In a physical network, implementing this level of segmentation and security rules would be cost-prohibitive and extremely time-intensive, requiring ever-expanding hardware appliances to achieve granularity. And in most IT organizations it simply isn't feasible. But with network virtualization, micro-segmentation is accomplished with software, making it much easier to deploy and maintain. In fact, you can provision and manage networks in minutes (versus weeks or months) from a single dashboard.

Deploying controls on each workload also provides visibility that was not possible before network virtualization. Using visualization tools, you can easily identify the applications that are most important to protect, understand the critical connections between applications and workloads and have a better understanding of the traffic flow within your network. These tools enable more intelligent network and security policy decisions as your understanding of the purpose and context of each individual workload expands.

Micro-segmentation also provides other benefits like persistence and adaptation. Persistence means that when you create security rules for a workload or VM, those security rules stay intact even when the network environment changes. This is critical as data center topologies are ever-changing — just as the threats against them evolve constantly. Through adaptation, micro-segmentation can also detect threats, then dynamically reconfigure policies or create new ones without human intervention. Security policies can be created to provide an automated response, such as shutting down access if data is retrieved in an inappropriate way.

Micro-segmentation helps reduce firewall sprawl as well. In a typical organization, there are several thousand rules governing your network, making it difficult for administrators to keep track of them all. And when applications or infrastructure are updated, moved or deleted, the associated rules are also added, moved or deleted, further expanding the list of rules for busy administrators to manage. But with persistence and adaptation, policies are updated or deleted in response to changes in the network rather than being added to an already long list.

Done well, better security and granular control make for simpler network design that reduces local traffic, thereby improving network performance. For example, micro-segmentation allows for direct communication within subnetworks, eliminating the need to move into and out of subnetworks and, therefore, chokepoints. In short, traffic moves faster but still securely.

Getting started with virtualization and micro-segmentation

Micro-segmentation as a way to improve your network security and performance may be the best approach for your organization. But if you don't have a clear understanding of your current network, it's difficult to implement effective network virtualization and micro-segmentation that meet the demands of your business today — and have the flexibility to meet the unknown needs and threats of tomorrow.

As with most things in business, there is no one-size-fits-all solution. Using the ConRes Software-Defined Data Center (SDDC) Framework, we work closely with you to create a holistic solution that ensures every element of your infrastructure and services contributes to meeting the demands of your business. Along with your team, we complete a **virtual network assessment** to understand all traffic across your network. Next, we'll define a plan to gradually roll out micro-segmentation to different applications, testing and refining along the way. Although it is a staged implementation, you will start seeing the benefits of micro-segmentation right away as traffic and workloads become more visible.

As experts in IT and networking for more than 50 years, we offer leading virtualization solutions like VMware NSX to help clients address their security and networking concerns, including:

- **Protecting** East-West traffic
- **Reducing** costs and complexities
- **Meeting** compliance requirements
- **Improving** enterprise agility

Our team has earned more than 500 technology certifications and our configuration, testing and validation facility enables unparalleled validation of customer solutions in a live environment. Simply put, we offer the most advanced IT solutions delivered by the most experienced team while providing you with industry-leading personal service and support.

The rise of network virtualization has paved the way for micro-segmentation, ushering in greater control over lateral network traffic and improving network performance. Let ConRes help you decipher which solutions best fit your needs and develop a roadmap to get you there.

Schedule your free virtual network assessment today to receive your report within 72 hours.

[1]Gibson, S., 2017. *The State of IT.* Interop ITX.
[2]Kaspersky Lab, 2017. *Mobile Malware Evolution 2017.*
[3]Syntonic, 2016. *2016 Employer Report: BYOD Usage in the Enterprise.*
[4]Ciklum, 2017. *Big Data and the Challenge of Unstructured Data.*
[5]KPMG, 2016. *2016 Compliance Transformation Survey.*
[6]Interop ITX and InformationWeek 2017 State of IT Survey.
[7]VeraQuest, 2016. *End-to-End Network Segmentation Research.*

ConRes
CONTINENTAL RESOURCES

ConRes provides high technology IT solutions and support to business, government and educational organizations. Combining 50 years of high-tech know-how and financial stability, ConRes is a low-risk option for organizations seeking to strengthen the ROI on their technology investments.

800-937-4688 | www.conres.com