WHITE PAPER – **FEBRUARY 2018**

TIPS AND TRICKS FOR DEPLOYING NEXT-GENERATION CYBERSECURITY USING MICRO-SEGMENTATION

Rethinking security strategy to meet next-generation security challenges

vmware®

Table of Contents

Hacking has become a multibillion-dollar industry designed to steal critical data and gain access to organizations' most sensitive systems. It is supported by talented hackers and engineers who have substantial financial resources. And companies are finding that traditional, perimeter-focused security strategies are no longer effective.

Breaches will happen. Enterprise security professionals need to be right every time; the hacker has to be right only once. Ponemon data makes this clear: Based on its research, 89% of organizations have experienced a data breach.[1] Hackers also focus on stealing privileged administrator credentials that will get them inside the firewall with wide access across IT infrastructure. This necessitates that new cybersecurity strategies be deployed inside the perimeter.

However, just adding a plethora of new and unique security products isn't the best approach either. Doing that adds more complexity to the security stack and requires additional scarce human resources. The right strategy must simplify daily operations, provide a foundational approach to protection and support IT agility—which is the goal of every organization. The focus must change from building a bigger fence to better protecting data and critical applications/workloads so if an organization is breached, security can stop the lateral spread of threats. Businesses need a platform designed to meet these needs, as well as to facilitate efficient interaction and deployment of policies and processes among system operations (SysOps), network operations (NetOps) and security operations (SecOps).

To achieve this new level of protection inside IT infrastructure, organizations must have complete visibility into the network and traffic. A virtual network is the optimal way to achieve this. A virtual network also provides micro-segmentation that effectively protects critical workloads inside the firewall. It supports better communication and coordination among SysOps, NetOps and SecOps, allowing them to create and deploy fine-grained security policies to protect the organization's most valuable assets. With network virtualization and micro-segmentation, the same language and terms are used across all three groups, enabling them to deploy consistent policies much more simply. Consistent visibility is also provided to the groups to enable their specific tasks and activities.

Virtualizing the network provides more than just security benefits

This white paper focuses on the benefits of deploying micro-segmentation using virtual network infrastructure. However, there are other critically important benefits from a virtual network that solve common problems in small to midsize enterprises. This "solution leverage" is important in that it provides better return on the investment in a virtual network deployment. Further, using one common platform for multiple functions simplifies operations and improves efficiency.

Perhaps the most notable additional benefit is that a virtual network provides important disaster recovery (DR) capabilities. Using a virtual network platform such as VMware NSX®, an organization can move the network and security configuration to a different site or a recovery site if there is a failure. NSX automatically reconfigures IP addresses, deploys security policies and eliminates the need for manual tasks to synchronize configuration across many physical sites.

1 "The Evolving Role of CISOs and Their Importance to the Business," Ponemon Institute, Nov. 2, 2017

Another benefit is to use the virtual network's load-balancing capability. This mitigates the need for point solutions that add cost and complexity to the environment. In addition, using load balancing within the virtual network platform provides a more complete view to ensure service levels, particularly when the platform is linked with information about server loads.

Virtual networks also enhance the work life of the network and security teams. The use of a common platform for interactions between SecOps, NetOps and SysOps reduces daily frustration and eliminates demands from one group that create difficulties for the others. Everyone works on a level playing field. And while the single most important benefit of deploying micro-segmentation on a virtual network is that it stops or dramatically reduces the impact of a breach, it also protects team members' careers. Being part of a team that allowed a substantial data breach is never a resume builder.

Getting started with micro-segmentation

Micro-segmentation is a new cybersecurity solution for many small to medium-size enterprises. For the solution to succeed, however, teams must develop an effective process for deploying it. There are three important steps that provide a starting point for the process:

1. **Determine the network flows in your organization.** The focus should be on data flows into, out of and within the data center. This activity is also likely to uncover inefficiencies that impact application latency and create loads on the network. To start the analysis, review perimeter firewall rules and identify north-south and east-west traffic. Different tools can be used to collect and analyze traffic flows. A starting point is to use IPFIX, a flow monitoring protocol, to collect and analyze traffic. You can go the next step and use commercial monitoring tools to develop a deeper level of analysis and correlate traffic flows with firewall policies.
2. **Identify patterns and relationships in the traffic.** The initial set of security policies for the micro-segmentation model can be created by correlating the flow patterns collected in the previous step with the current perimeter firewall policies. The flow patterns provide the key information about relationships between workloads within the data center. It is important to understand how workloads interact with each other. This includes how one specific workload interacts with shared IT services, other applications and other workloads. It is also important to understand interactions across different environments, such as production and development/test. Once these relationships are known and documented, you'll have key input data for defining micro-segments and the policies for how they will interact.
3. **Create and apply the policy model.** One proven approach to this is to apply micro-segmentation one application at a time. This approach has many merits in that it is not overly taxing on staff and lets the organization deploy micro-segmentation at its own pace. Many small to midsize enterprises start with a "default block" approach that prohibits all communication between workloads for the application they are focused on. Then they can start to open communication based on the analysis of their traffic patterns. If additional communication is needed, it can be opened up based on demand. However, if you are concerned about a service interruption by deploying a default block approach, it is possible to start with a "default allow," enabling open communications. Use this approach with the utmost caution.

Restrictions can be added as they prove to have no impact on the application. In addition, as new application, user and data requirements become known, the micro-segmentation model can be updated to reflect them. To make this process even simpler, VMware NSX also provides Application Rule Manager, an automated tool that suggests micro-segmentation policies based on that data.

Tips and tricks for a successful micro-segmentation deployment

As with any technology solution, there are specific tips and tricks that can help make deployment more efficient and effective. Some of the most important include the following:

- Utilize the VMware Application Rule Manager (ARM) – ARM is a feature that gathers all of the flow information you might need or want to evaluate for a subset of virtual machines in the environment. ARM then automatically suggests micro-segmentation policies based on the tool's own analytic intelligence. It can then push those policies to the rule table in just a few clicks.
- Map out your security groups first – Starting with a sense of the structure and definition of your security groups will ensure that you begin with a starting point that is appropriate to your organization.
- Develop consistent naming conventions for security groups – The naming conventions and actual names are an important facilitator of a cohesive micro-segmentation deployment. The naming convention should be consistent and agreed to by SysOps, SecOps and NetOps prior to it being used.
- Build a cross-functional team to support the micro-segmentation deployment – The success of a micro-segmentation deployment is directly impacted by the support of the three key groups that will be using it. For that reason, it is essential the team that designs and deploys the solution includes staff from SysOps, SecOps and NetOps.

Gaining executive support for a micro-segmentation initiative

To ensure support for the investment and that you have the resources necessary for the project to succeed, it is important to gain support from both executive management and IT management. Speaking in their language is essential.

Executive/top management

Top executives will be focused on business benefits. The primary discussion with them should focus on the ability to reduce the impact of any data breach by stopping attackers from gaining access to sensitive applications and data. Micro-segmentation also helps meets compliance directives by reducing or eliminating data loss.

Executives should also be told that new applications, changes in business processes and new security demands are easily managed and accounted for using micro-segmentation. From a cost perspective, deploying micro-segmentation on a virtual network such as NSX will save money by reducing the requirement for separate DR and load-balancing tools. The story for these executives is about a single, much more cost-efficient platform that delivers enhanced security and other benefits.

CIO and VP of IT

These executives are likely to already understand the basic benefits of micro-segmentation, so the focus of the discussion should be on how micro-segmentation delivers on the things they worry most about: data security, agility and cost efficiencies.

From the data security perspective, micro-segmentation is the best tool, providing effective protection for sensitive data and applications. In addition, it supports agile protection for applications and data by allowing real-time security policy modification. This is the lead-in to agility. As new apps are released or new data sources are defined, micro-segmentation policies can be used to protect these assets very quickly, eliminating "security lag."

Micro-segmentation also supports clear communication and coordination among SecOps, NetOps and SysOps to ensure consistency. And the virtual network platform that delivers micro-segmentation provides DR and load-balancing functionality, eliminating the need to purchase other, costly solutions.

Summary and key takeaways

Small and midsize enterprises face the same cybersecurity demands as the largest enterprises, but they have far fewer resources to protect the organization. For that reason, these companies must work smarter and more efficiently to deploy cyberprotection. Micro-segmentation is an excellent match for these demands. It augments the perimeter firewall by delivering protection against threats that manage to breach perimeter security by precluding them from gaining additional access to sensitive systems. It also is a simpler solution to operate.

Not only does micro-segmentation on a virtual network improve cybersecurity, but the virtual network provides other critical operational benefits, such as DR and load balancing, without having to purchase additional costly solutions. For more information, consider these additional resources:

- Five Steps to Micro-segmentation
- Forrester: The Total Economic Impact™ of VMware NSX
- Micro-segmentation for Dummies, 2nd Edition
- VMware Virtual Network Assessment

These resources, along with the tips and tricks in this document, will help you successfully deploy this important technology.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Copyright © 2018 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: VMWARE_TT_CE23_0118
2/18