vmware PRESS

VMware NSX® Micro-segmentation

Day 2

Geoff Wilmington, VCIX6-NV

Foreword by Dominick A. Delfino, Senior Vice President,
WW Sales & Systems Engineering – Software Defined Data Center

VMware NSX® Micro-segmentation

Day 2

Geoff Wilmington, VCIX6-NV

Foreword by Dominick A. Delfino, Senior Vice President,
WW Sales & Systems Engineering – Software Defined Data Center

vmware® PRESS

VMWARE PRESS

Program Managers

Katie Holms
Shinie Shaw

Technical Writer

Rob Greanias

Production Manager

Mitchell Design

Graphics Manager

Elaine Tai

Warning & Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The authors, VMware Press, VMware, and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

The opinions expressed in this book belong to the author and are not necessarily those of VMware.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA
Tel 877-486-9273 Fax 650-427-5001 www.vmware.com.

Table of Contents

List of Figures

List of Tables

About the Author

Geoff Wilmington, VCIX6-NV, is a Senior Systems Engineer within the VMware Networking and Security Business Unit, focusing on all security aspects and functions of the VMware NSX product. Geoff is a 17-year industry veteran and has worked at VMware for 2.5 years and across multiple positions within the Information Technology industry. He is a VMware Certified Implementation Expert for the VMware NSX product, and has been recognized as a VMware vExpert for technical community involvement.

Geoff has spoken at local VMware User Group meetings as both a customer and a VMware employee and has been featured at multiple sessions at VMworld US. Geoff holds a Bachelor's degree in IT Management. Follow Geoff on Twitter @vWilmo or visit his blog http://vwilmo.wordpress.com.

Content Contributors

Dale Coghlan is a Solution Architect in the VMware Customer Success business unit and works directly with NSX for vSphere customers from initial design all the way through to implementation and operationalisation of their new environments. Dale has over 17 years of experience in networking and security roles across many verticals and uses that experience to help customers get the best out of the NSX network virtualization platform.

Kausum Kumar is Senior Product Manager in the VMware Networking and Security business unit. Kausum has over 16 years of experience in the networking and security industry. Kausum leads the micro-segmentation and security area for VMware NSX with particular focus on firewalling, endpoint security and service chaining. Kausum has a Masters from University of Maryland, Baltimore County in Electrical Engineering with focus in wireless communications.

Additional Contributors:

Sean O'Dell
Joey Welt
Abhijit Sharma
Wade Holmes

Acknowledgements

No one person could have compiled the contents of this guide without the support and help of both the VMware NSBU and CMBU teams. I'd like to personally thank each person for their content I was able to use to create this guide. Without their knowledge and experience, this would not have been possible.

I want to first acknowledge my family for their support during the countless hours spent writing this guide – both during the day and late into the night. My wife, Heather, who is constantly encouraging and supporting me as I challenge myself in my career. My two daughters, Jacqueline and Olivia, who inspire me to be the best I can be both as a father and professionally. None of this was possible without your support. I love you all.

Thanks to Shinie Shaw and Katie Holms from the Product Marketing team for reaching out and asking me to turn my blog posts into an actual guide. Thank you for putting your trust in me and shepherding me through the process.

Thanks to the Networking and Security Business Unit, Scott Martin, Kausum Kumar, Wade Holmes, Joey Welt, and Dale Coghlan for all of their support and feedback during this process.

Thanks to Sean O'Dell, Abhijit Sharma, and Shiv Agarwal and the rest of his Cloud Management Business Unit team for their help with both the blogs and the content used to write this guide.

Geoff Wilmington, VCIX6-NV

Preface

VMware NSX Micro-segmentation – Day 2 is a guide designed to help organizations understand how to operationalize micro-segmentation in their environments. *VMware NSX Micro-segmentation – Day 2* provides a primer on leveraging tools – VMware vRealize® Log Insight™, Application Rule Manager, and VMware vRealize® Network Insight™ – to build rulesets necessary to facilitate micro-segmentation.

Foreword

As I sit down to write this foreword, I think back over recent tumultuous events affecting IT security. Network operators and information security professionals have had to deal with quite a string of ransomware attacks which wreaked havoc for those infected. Are industry leaders finally at a point, scratching their heads, wondering why we haven't solved this problem? I think it is important to take a step back and understand why we keep getting hacked. Why do application developers and owners view enterprise infrastructure as insufficiently agile and nimble, preferring go around it to solve their challenges?

When I look back at my own career, while we have made many technology transitions over the past 20+ years, some areas of infrastructure continue to lag significantly. Given that an infrastructure should operate as an entity of one, this lag in the network and its security has been and continues to be the largest obstacle to building a secure and agile infrastructure. Much of the innovation in modern day networking happened during the dot com boom of the late 1990s. Y2K preparation and transition saw trillions of dollars being pumped into networking technology. We spent years converging the many disparate networks, topologies, and protocols onto a modern day common denominator – Ethernet plus TCP/IP. Prior to this transition, we ran multitudes of physical medium, protocols, and physical plants. This, in addition to the advent of layer 3 switching, allowed us to build and operate networks at large scale. However, since these two major innovations – convergence to Ethernet + TCP/IP, layer 3 switching – not enough has changed to keep pace with the innovation in computing, data storage, and information security. We have simply received iterations of 1990s innovation to work around the shortcomings in the network and deal with the adjacent infrastructure technologies and the applications that run above them. Compute virtualization, the key fundamental and foundational element of cloud computing, was an afterthought from a networking perspective. There were two waves of compute virtualization which were highly disruptive to the network.

Wave 1: Workload Consolidation — the advent of workload consolidation solved a massive technological and financial problem for enterprise IT. Prior to compute virtualization, server sprawl was out of control. Many customers ran a single application per server in their data centers, creating huge financial, physical, and operational burdens. VMware was at the forefront of this transformation, enabling the consolidation of workloads to a much smaller number of servers. This saved businesses tremendous amounts of money by driving up asset utilization while allowing administrators to operate a large-scale environment with far greater efficiency.

Wave 2: Workload Mobility — the advent of workload mobility was a complete game changer, offering operational efficiencies while taking x86 computing to the modern era. Technologies innovated by VMware – including distributed resource scheduling, high-availability, vMotion, Site Recovery Manager, and fault tolerance – completely changed the way we architect availability and resiliency for application workloads. These technological innovations also allowed for the movement of running applications from one physical server to another – within the same rack, across a data center, or between distinct data centers.

The network was not designed with either of these innovation waves in mind. This presented a huge challenge for network operators and administrators. The toolsets required to deal with this new computing paradigm were not baked into the architecture they had spent many years designing and implementing. We had grown accustomed to the direct correlation of one application workload to one network interface. This allowed us to apply network and security policy to that interface. The workload in large part was fairly static; it was born there, it died there, and not much changed during its lifespan. Workload lifecycle management is the first major gap we face with legacy networking technology.

Fast-forward to today where we now have an entire layer of virtual switching sitting inside every virtualized host in our data centers. Workloads are highly dynamic and may move to a different interface on the same switch, another switch in the data center, to another private data center, or even into the public cloud. A workload's network policy, addressing schema, and security policies must now be able to follow the workload wherever it may go. We dealt with this in some regards by teaching administrators to build large flat layer 2 networks, a practice that has become one of the largest gaping security holes in enterprise IT today. It was not only recommended to build large flat layer 2 networks, but we were also fed more and more technologies, features, and capabilities to scale layer 2 networks. The challenge this created is that there are no scalable ways to restrict traffic on a layer 2 network; therefore everything can see and talk to everything. There is a reason it is also referred to as a "broadcast domain".

In the late 1990s securing the perimeter was a major priority. Much money was pumped into firewalling, VPN's, intrusion detection systems, and the building of DMZs. Recently, however, the game has changed dramatically. We no longer simply transact external communication via the Internet; we transact almost all business via the Internet and extranets. We are now hyper-connected with a massive exponential increase of the number of devices and addresses connected to our networks. Gone are the days of inside and outside, public and private, trusted and untrusted. The challenge is no longer keeping intruders out of your network, it is how to defeat them once they are inside! Once a guest operating systems is infected, the malicious software's ability to propagate is largely uninhibited by today's most prevalent network architectures.

This is where the security needs to change. We can no longer rely on device-specific configurations that implement fine grained controls on disparate hardware platforms with little regard for technological or

operational scalability. In comes the role of the network hypervisor or abstraction layer known as VMware NSX. NSX was born through the acquisition of Nicira; a pioneer in recreating network infrastructure and security in software. Resident in the hypervisor, this is commonly referred to as Software Defined Networking (SDN); however, we prefer to call it "network virtualization". This innovation allows us to dynamically build entire networks in software, at large scale, with the associated security services, in a highly efficient manner, agnostic from the underlying physical network.

While NSX addresses many use case areas, the most prevalent reason for adoption is dramatically increased security capabilities and automation. Enter the creation of the distributed firewall and micro-segmentation. Micro-segmentation allows for infrastructure architects to put an isolation wrapper around a VM, a collection of VMs, an application, or any general grouping of these components. NSX implements a stateful inspection distributed firewall at the vNIC level, allowing for the most granular level of control. While doing so in a distributed fashion, NSX vastly simplifies policies, rule set distribution, and operational efficiencies. The net result is a system that is far superior than what we have had historically. This also substantially mitigates the risk of unwanted traffic (e.g., malware, viruses, ransomware) propagating laterally throughout the network and the connected systems.

The second major innovation gap we have today is the differentiation between information security policy and network security implementation. InfoSec policy is most simply defined as what user has access to which applications, and what applications have access to which specific sets of data. The implementation of this policy within the network infrastructure is far more complex and most times nearly impossible. This is the second major gap we can now overcome because policy can now be implemented with the full intent of the information security policy as its standard.

It is now time to mitigate these threats and advance our infrastructure capabilities. We must as a community rethink our skills and our roles. We must build knowledge in adjacent technology domains to architect and operate infrastructure as a system. That system is now the foundation of every business, public sector institution, education system, and healthcare provider. We are responsible for this journey, and I know that this book will help educate you on how to solve the business and technology challenges we face.

Dominick A. Delfino, Senior Vice President,
WW Sales & Systems Engineering – Software Defined Data Center

Planning, Methodology, and Application Visibility

Micro-segmentation is a security concept that is used to help provide a least privilege security posture within the data center. Least privilege is defined as only allowing the minimal amount of access required to perform the function necessary. In the world of network security, VMware NSX™ allows an administrator to apply least privilege network security. Least privilege is the foundation to a Zero-Trust architecture, where only allowlisted applications are allowed to communicate. In this definition of least privilege, the administrator can restrict the application and virtual machines within the application to only allow necessary communications for the application and it's components to provide the absolute minimum necessary functionality.

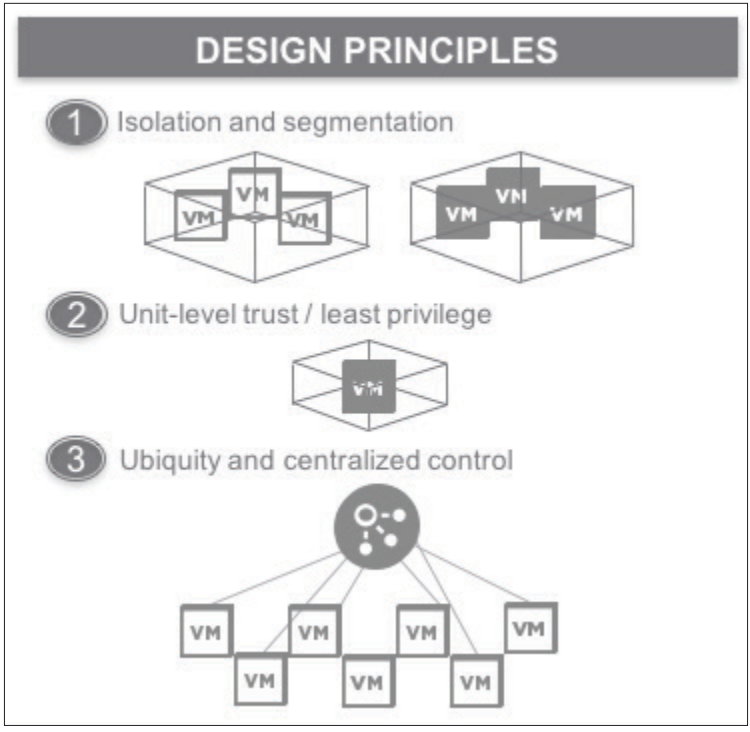


Figure 1.1 Least privilege design concepts

Modern technologies enable understanding, isolation, and segmentation of traffic from an east-west perspective in the data center, allowing for implementation of a least privilege security posture. VMware NSX is a network virtualization platform that provides the capability to apply security policy at network level of a virtual infrastructure. In a traditional model, virtual machines in a data center have unrestricted communication with every other virtual machine, regardless of whether this is truly required.

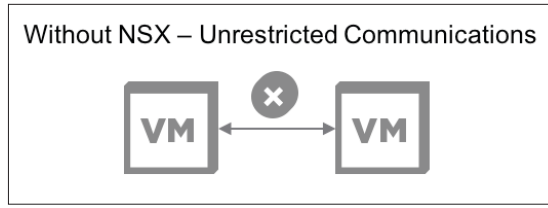


Figure 1.2 Without NSX

The VMware NSX platform instantiates a stateful firewall at the virtual network card (vNIC) of every virtual machine in the infrastructure. This stateful firewall allows creation of granular security policies for each virtual machine. These policies allow only the necessary communications between VMs; they also block traffic that is unnecessary, keeping systems from freely establishing communication with each other.

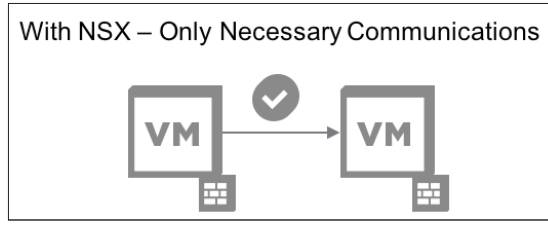


Figure 1.3 With NSX

Organizations have multiple different applications within their data centers, so providing this least privilege model can be difficult. Not every organization is familiar with how its applications communicate or how to initiate such a security posture. This guide will explore the many tools and methodologies available to create a least privilege security posture. For more information regarding VMware NSX and micro-segmentation, refer to the *VMware NSX Micro-segmentation – Day 1* guide.

Where to start?

This is the question that plagues most customers – where does an organization start with micro-segmentation? While there is no specific rule on where to begin, customers typically start with one application where the security posture of a least privilege environment is needed. This could be an application that has stricter PCI-DSS requirements or HIPAA regulation around patient data. Over time, the organization would find additional applications that require a similar security posture and expand from there.

Regardless of the selected application, the aspect of infrastructure services must also be considered. Where significant effort is spent on micro-segmenting the application, it can be easy to forget the general purpose external services and dependencies that are required for the application to function.

External application services and dependencies such as DNS, NTP, and LDAP, must be considered part of the application when securing. These are services that are global for all applications, regardless of importance. Whether or not infrastructure services are micro-segmented on their own, they must be taken into consideration when applying micro-segmentation to the application.

Understanding the Application(s)

Before beginning to secure an application, it is essential to understand its operational patterns; therefore, each application must be analyzed prior to applying a security policy. There are several tasks that can will help understand the application:

Talk with the Application Owners

Application owners should always be involved in the planning, testing, and implementing of the security policy. The application owners should be able to provide the most information about an application and its use. If the organization is lax on documentation, this is a great time to baseline each application and get appropriate documentation in place. Going forward, any new system that may need to communicate with the secured application will then have the documentation necessary to facilitate that communication.

Application Vendor's Documentation

The application vendor's documentation is another place that should house important information for the application, though not all vendor documentation includes full details of ports, protocols, and communication Flows.

Internal Documentation

Off-the-shelf software is often customized as part of its deployment, and documentation created during this process it should note organizational-specific changes that deviated from the default install. This documentation can be invaluable when used in conjunction with vendor documentation, identifying communication ports or protocols may have been modified from the release documents.

Organizations may also build their own applications. In-house developers may leverage many tools to tailor these custom-built applications specifically for the organization. For these applications, internal documentation and collaboration with the development team is essential to understanding how an application functions and what communication it requires.

Planning

Define the Application

Defining the application starts with understanding the application. What systems comprise the application? What servers does the application run on? What external dependencies does the application require to function normally? Once the components for the application are identified, they can be documented and analyzed for micro-segmentation.

Understand the Requirements

Every application addresses a business requirement; this connects its requirements not just to technical operations but also business processes. An application used for employee time card tracking dictates the scope of employees who require access. This in turn helps scope how the application's access rules are defined within the VMware NSX Distributed Firewall (DFW). If an application is accessed solely by the human resources department, the requirement may be to restrict even server-level access to only the HR department.

Define the Methodology

Each organization is at different stages of their infrastructure methodology. When they are ready to implement a least privilege model using micro-segmentation, it could be for an existing environment (i.e., brownfield) or a brand-new environment (i.e., greenfield). It is important to understand which type of deployment model the organization is going to use, as that can impact which micro-segmentation methodology to select.

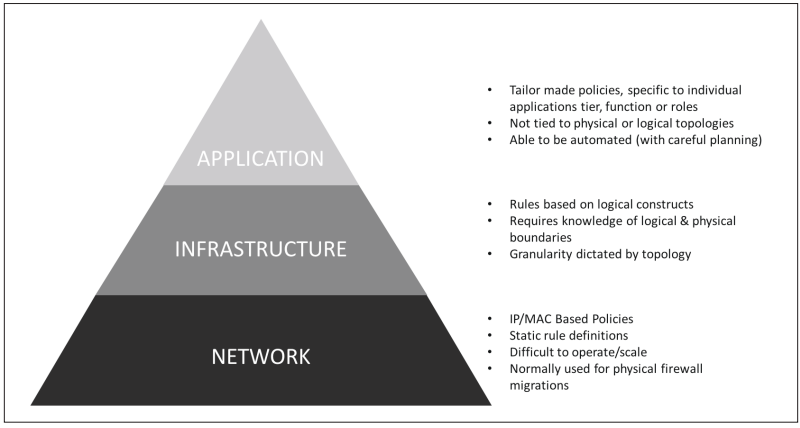


Figure 1.4 Micro-segmentation methodologies

As an organization continues down the path of micro-segmentation, it makes sense to establish which methodology best suits its requirements. Figure 1.4 presents three methodologies for micro-segmenting applications:

Application

The application-based methodology tailors the security policies to the specific application and its associated tiers. This approach may split out the web tier, app tier, and DB tier of an application and apply security policy around each component. This methodology is topology agnostic and can be automated depending on the requirements of the application.

Infrastructure

The infrastructure-based methodology requires an understanding of the underlying topology – both physical and logical. With VMware NSX, this approach provides micro-segmentation policy granularity at the VXLAN logical switch level where several machines of a specific type or tier may reside.

Network

As not every application or system is virtual, the network-based methodology is typically used when there are physical components that exist outside of an NSX domain. VMware NSX has capabilities within the platform to use IP and MAC based policies to define the security posture of an application. This methodology does not typically scale well, as maintaining IP and MAC address information can be operationally cumbersome.

Regardless of the approach used, VMware NSX can help facilitate micro-segmentation using each of these methodologies.

Layout Naming Scheme

Naming of the VMware NSX constructs is extremely important. It can make the build process of the NSX Distributed Firewall rules quick and easy, letting others know what the constructs are impacting should any changes occur to them. Naming standards should be defined and adhered to. As an organization continues further down the path of micro-segmentation, naming will become even more critical. When going from 10s to 100s to 1000s of applications, a chaotic naming scheme will cause confusion, create complexity, and increase the chance of errors. This problem can compound itself the more integrated the system of applications.

Prepare Documentation for Rules

This section provides an example of how an organization can lay out and document its rulesets. This information is just as critical as documentation on application deployment and configuration. Most documentation already includes changes to default settings for application deployment, including the names of the application servers any dependencies. How the application is secured is information that is just as important and helps complete the documentation. If an organization has minimal documentation, starting with this process can help formalize the foundation and begin to fill in the gaps.

The documentation of the NSX Distributed Firewall rules should encompass the following items:

- How the application accesses the infrastructure services
- How any remaining application communication is blocked
- The groupings that were created in NSX and used to build the rulesets
  - Security Groups for the application servers/access
  - Security Tags leveraged to tag the application servers
- Descriptions of the services necessary for the application to function

This information can be laid out in a table format that closely mimics its appearance in the NSX Distributed Firewall interface. This format makes it easy to understand and also provides a reference for any changes. Table 1.1 provides examples of this layout.

Table 1.1 Example layout

Application Access Communications:

Name	Source	Destination	Service	Action	Applied To
APP Access	Any	SG-APP-ALL	APP-SVG-ALL	Allow	SG-APP-ALL

Block All Application Communications:

Name	Source	Destination	Service	Action	Applied To
Block Inbound App	SG-APP-ALL	Any	Any	Block	SG-APP-ALL
Block Outbound App	Any	SG-APP-ALL	Any	Block	SG-APP-ALL

NSX Groupings:

Security Group	SG-Contains	SG-Inclusion Criteria
SG-APP-ALL	SG-APP-WEB	Static
SG-APP-WEB	WEB-01a	Static

Service Group	Service Included	Port
SVG-APP-ALL	SV-APP-HTTP	TCP 80

Define Application Flow Monitor Length

Understanding the application is essential to defining its associated monitoring parameters. If the application is a payroll system that runs regular billing cycles, an organization may want to monitor the payroll application for a few weeks or months. If the application is used daily, then monitoring may only be needed for a shorter period. New applications can be on boarded easily by building the application and studying the typical usage by the testing teams. Once rules are in place for micro-segmentation, full functionality testing can occur to verify proper operation before placing the application into production. By doing this, the organization is helping to ensure that they are capturing all the necessary application Flows both in and out of the application.

Create Default Allow/Block Rules as Necessary

Understanding application functionality and communication – both internal and external – is one of the biggest challenges that organizations face. New applications are brought in to solve business issues; sometimes the documentation detailing operations and connectivity is missing or incomplete. Applications of interest may not have the necessary documentation or may have been configured differently from the default process. IT faces the challenge of monitoring application functionality and communication in a non-disruptive manner and requires a solution for both pre-existing and new applications.

When VMware NSX DFW modules are deployed to VMware ESXi™ hosts, the default rule is “Allow All”. This setting allows all traffic to pass. This is contrary to a traditional hardware firewall where the final rule is usually a default “Deny All”. Since the DFW instantiates a layer 2-4 firewall at the vNIC of each virtual machine, a default deny could cause massive disruption to the virtual environment.

When beginning the process of micro-segmentation, leverage application-centric allows and blocking to monitor application functionality. This will not disrupt the application, permitting it to continue to function normally while allowing initial granular rules creation.

Start by creating an NSX Security Group for the entire application of interest, adding all VMs for the application into the group.

Next create four VMware NSX DFW rules using this Security Group, logging the hits on the rules. This will show how the application communicates.

- One rule to allow all inbound traffic to the application and log
- One rule to allow all outbound traffic to the application and log
- One rule to block all inbound traffic to the application and log
- One rule to block all outbound traffic to the application and log

The implementation of these rules is detailed in Table 1.2.

Table 1.2 Four monitoring rules

Name	RuleID	Source	Service	Service	Action	Applied To
Allow Inbound Log	1010	Any	SG-APP-ALL	Any	Allow	SG-APP-ALL
Allow Outbound Log	1011	SG-APP-ALL	Any	Any	Allow	SG-APP-ALL
Block Inbound Log	1012	Any	SG-APP-ALL	Any	Block	SG-APP-ALL
Block Outbound Log	1013	SG-APP-ALL	Any	Any	Block	SG-APP-ALL

As with hardware firewalls, the NSX Distributed Firewall checks rules top-down against a Flow. For both new and pre-existing applications, using this configuration of rules will help identify Flows for more granular analysis. At the end of the process, these general allow rules will be removed and any Flows not explicitly defined will be blocked.

Once the four monitor rules are in place, examine the NSX DFW logs to see how the application communicates.

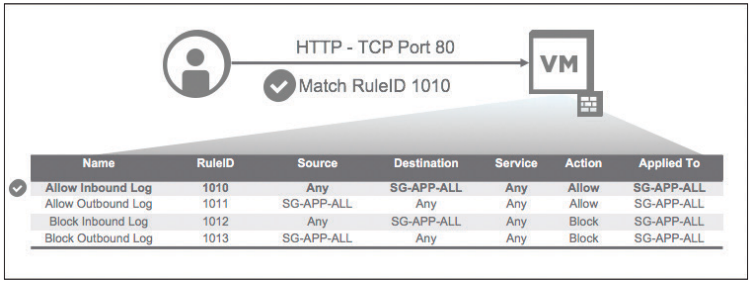
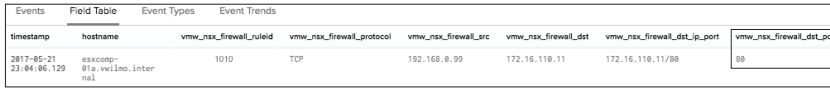


Figure 1.5 Default allow behavior

In this example, **RuleID** 1010 allows an **HTTP – TCP Port 80** Flow from any source to one of the application VMs. Log data from this rule is shown in Figure 1.6.

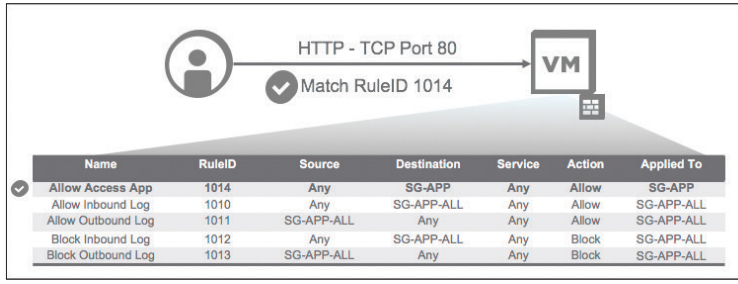


Events | Field Table | Event Types | Event Trends

timestamp	hostname	vmw_nsx_firewall_ruleid	vmw_nsx_firewall_protocol	vmw_nsx_firewall_src	vmw_nsx_firewall_dst	vmw_nsx_firewall_dst_ip_port	vmw_nsx_firewall_dst_port
2017-05-21 23:04:06.129	esxcomp-01a.vwilmo.internal	1010	TCP	192.168.0.99	172.16.110.11	172.16.110.11/80	80

Figure 1.6 Default allow log

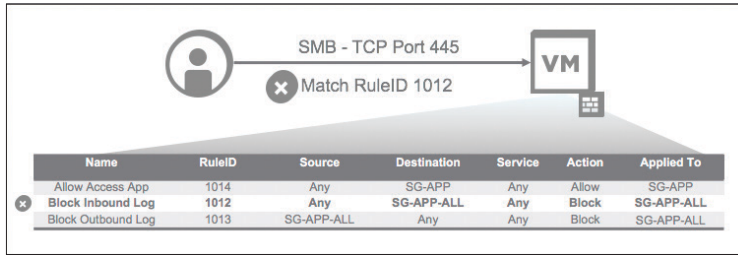
To better restrict traffic to only necessary Flows, create a more granular rule above the **Allow Inbound Log**, as seen in Figure 1.7.



Name	RuleID	Source	Destination	Service	Action	Applied To
Allow Access App	**1014**	**Any**	**SG-APP**	**Any**	**Allow**	**SG-APP**
Allow Inbound Log	1010	Any	SG-APP-ALL	Any	Allow	SG-APP-ALL
Allow Outbound Log	1011	SG-APP-ALL	Any	Any	Allow	SG-APP-ALL
Block Inbound Log	1012	Any	SG-APP-ALL	Any	Block	SG-APP-ALL
Block Outbound Log	1013	SG-APP-ALL	Any	Any	Block	SG-APP-ALL

Figure 1.7 Allow access app rule match

Traffic Flows will hit the new rule – **RuleID 1014** – instead of the **Allow Inbound Log** rule. Once all required traffic Flows have been captured, remove the allow rules so any new traffic will hit the block rules.



Name	RuleID	Source	Destination	Service	Action	Applied To
Allow Access App	1014	Any	SG-APP	Any	Allow	SG-APP
Block Inbound Log	**1012**	**Any**	**SG-APP-ALL**	**Any**	**Block**	**SG-APP-ALL**
Block Outbound Log	1013	SG-APP-ALL	Any	Any	Block	SG-APP-ALL

Figure 1.8 Block access app rule match

Review Rules to Create

Use of the tabular format shown in Table 1.3 will make it easy to fill in the fields associated with an NSX object naming scheme. Documenting the rules in a table during application monitoring will provide a reference for review prior to committing them to the NSX DFW.

Table 1.3 Review rules

Application Access Communications:

Name	Source	Destination	Service	Action	Applied To
APP Access	Any	SG-APP-ALL	APP-SVG-ALL	Allow	SG-APP-ALL

Block All Application Communications:

Name	Source	Destination	Service	Action	Applied To
Block Inbound App	SG-APP-ALL	Any	Any	Block	SG-APP-ALL
Block Outbound App	Any	SG-APP-ALL	Any	Block	SG-APP-ALL

NSX Groupings:

Security Group	SG-Contains	SG-Inclusion Criteria
SG-APP-ALL	SG-APP-WEB	Static
SG-APP-WEB	WEB-01a	Static

Service Group	Service Included	Port
SVG-APP-ALL	SV-APP-HTTP	TCP 80

Create Rules

When using the tabular approach, adding rules to the DFW interface is a simple process. The column headings – Security Groups, Security Tags, Services, and Service Tags – are all laid out.
This not only helps create the rules within the VMware NSX DFW, but also serves as a template for maintaining documentation about the application and its security posture in the organization.

Negate Source/Destination

VMware NSX provides a few simple ways to write DFW rules to reduce the number required. This helps avoid placement issues with block rules. Leverage the **Negate Source/Destination** options to build rules that do not need explicit block rules yet still provide a level of security similar to having them in place.

- If **Negate Source** is selected, the rule is applied to traffic coming from all sources except for the specific source.
- If **Negate Source** is not selected, the rule applies to traffic coming from the specific source.
- If **Negate Destination** is selected, the rule is applied to traffic going to all destinations except for the specific destination.
- If **Negate Destination** is not selected, the rule applies to traffic going to the specific destination.

A typical use case for using this feature would prevent web servers from talking to each other but allow communication from other sources. Using **Negate Source** with the web servers as the **Source** and web servers as the **Destination**, all sources will be allowed except the web servers themselves. This effectively blocks the web servers from talking to each other.

Verify Working

Verifying application operation is essential to successful implementation of micro-segmentation. Before an application can be cleared for production, all functionality must be tested against the micro-segmentation rules put in place.

Tools

Knowledge of tool availability and applicability will reduce the amount of time necessary to micro-segment an application. Three tools of specific interest include vRealize Log Insight, Application Rule Manager, and vRealize Network Insight.

vRealize Log Insight

VMware vRealize Log Insight ingests data from multiple sources and provides access using plugin functionality, enabling dashboards and advanced search capabilities. VMware® NSX Manager™ sends information to vRealize Log Insight via syslog. When combined with syslog information from the vSphere hosts, vRealize Log Insight provides rich data to assist in building micro-segmentation rules.

vRealize Log Insight works with VMware NSX, providing a logging tool for the environment. It can be deployed as a single appliance or in a cluster. The vRealize Log Insight plug-in for NSX provides several dashboards to help monitor key aspects of the NSX infrastructure. It is available for download directly from the vRealize Log Insight UI.

When to use vRealize Log Insight for Micro-segmentation Planning

vRealize Log Insight is most useful for micro-segmentation planning when there is a focus on real-time monitoring of a single application. vRealize Log Insight offers quick updates to logging information, making it an good tool for granular analysis. It does not scale well for monitoring large environments or multiple application Flows.

Application Rule Manager

Application Rule Manager (ARM) was introduced in VMware NSX 6.3 to assist with micro-segmentation on a larger scale. ARM leverages real-time Flow information to identify both inbound and outbound workload communications, allowing creation of a security model around an application. ARM can monitor up to 30 VMs in one session, with 5 sessions running simultaneously. ARM can automatically correlate information and create rulesets, significantly reducing time to value. ARM can also highlight blocked Flows and identify the specific rules responsible.

When to use Application Rule Manager for Micro-segmentation planning

ARM is designed for larger scale issues than vRealize Log Insight and is most useful for monitoring applications composed of several virtual machines. ARM can monitor Flows in these sessions for up to seven days at a time. Where vRealize Log Insight is focused on real-time activities, ARM is best leveraged where monitoring is required over several days.

vRealize Network Insight

vRealize Network Insight is a virtual appliance that can gather information from multiple data sources to provide advanced operations for multiple applications at scale. vRealize Network Insight uses this data to deliver on three distinct use cases:

- Micro-segmentation Planning
- 360˚ Network Visibility
- Advanced NSX Operations

When to use vRealize Network Insight for Micro-segmentation planning

This guide will focus on using vRealize Network Insight to help plan micro-segmentation rules. vRealize Network Insight gathers Flow data from the VMware vSphere® Distributed Switch™ using NetFlow. All traffic that traverses the vSphere Distributed Switch is sent to vRealize Network Insight for analysis. Collection over extended periods of time allows capturing of infrequent Flows that are important for the functionality of the application or its integration with other applications. Retention of 30 days of Flow history is one of the key benefits of vRealize Network Insight.

vRealize Log Insight

vRealize Log Insight is the first tool for consideration when beginning micro-segmentation planning. vRealize Log Insight provides a granular level of monitoring of traffic Flows from the ESXi DFW. These Flows, once identified, can be leveraged to build DFW rules to micro-segment the application in question.

This section will use the previously defined processes to plan and implement the micro-segmentation of a typical 3-tier application.

Define the Application

The first step is identifying and understanding the application itself; what is the nature of the application targeted for micro-segmented? In this example, it is a 3-tier application which displays the output of a query for specific authors and books in a database. The application can be accessed from either of the web servers to provide uptime in case of a web server failure.

The application consists of the servers listed in Table 2.1 and has an external dependency identified in Table 2.2.

3-Tier Application

Table 2.1 3-Tier application information

System Function	System Name	IP Address
Web Tier	Web01	172.16.110.11
Web Tier	Web02	172.16.110.12
App Tier	App01	172.16.120.11
Database Tier	DB01	172.16.130.11

Infrastructure Services

Table 2.2 Infrastructure services information

System Function	System Name	IP Address
NTP	NTP-01a	192.168.0.210

Understand the Requirements

The customer would like to provide a least privilege security posture for their 3-tier book application. They are not familiar with the communication Flows either to the application or between the its server architecture. To create a least privilege security posture, the following steps are required:

- Allow any inbound to Web01 and Web02
- Allow Web01 and Web02 to communication with App01
- Allow App01 to communicate with DB01
- Allow all servers to communicate with any external services necessary to function
- Block communications between Web01 and Web02
- Block all other communications to any server of the application unless explicitly defined in the above requirements.

Define the Methodology

This example focuses on a specific application, so the application-based methodology is appropriate. Each part of the application is broken down into its tiers and granular security policies are created for each. Refer to Figure 1.4.

A complete layout is shared in Table 2.3.

Table 2.3 3-Tier application NSX DFW rules example

Name	Source	Destination	Service	Action	Applied To
Allow 3T-App to NTP	3T-App	NTP	-	Allow	3T-App
Allow Any Into 3T-App – Negate Web Tier	Web Tier	Web Tier	-	Allow	Web Tier
Allow Web to App	Web Tier	App Tier	-	Allow	Web Tier App Tier
Allow App to DB	App Tier	DB Tier	-	Allow	App Tier DB Tier
Block Any to App Log	Any	3T-App	Any	Block	3T-App
Block App to Any Log	3T-App	Any	Any	Block	3T-App

- The top rule will cover the application's need to communication with infrastructure services (e.g., NTP).
- The second rule will Negate Source of the web tier. Negating the source allows all other sources to access the web tier except those in the web tier. This functionally works as a block, so rule order becomes arbitrary.
- The remaining set of allow rules are necessary for the intra and extra-application communication.
- The last two rules will block any other communications that are not defined as essential for the application to run.

This set of rules should effectively allowlist all traffic, allowing the application to function for the organization.

Technologies Used

Windows Clients

Table 2.4 Windows client information

System Function	System Name	IP Address
Management Jumpbox	Jumpbox-01a	192.168.0.99

VMware Products

Table 2.5 VMware product information

Product	Version	IP Address
VMware vSphere® ESXi™	6.0 Patch 4	Multiple
VMware® vCenter™ Server Appliance	6.0 Update 2a	192.168.0.111
VMware NSX Manager	6.3.0	192.168.0.120
VMware vRealize Log Insight	4.3	192.168.0.140
VMware NSX Plugin for Log Insight	3.6	-

Define Monitor Length

Real time monitoring is appropriate in this case, as this is a small application consisting of 4 servers in total. This application is run on-demand, so there are no specific time constraints to consider. With the use of NTP, calls to this external service must be taken into account.

NSX/Log Insight Management Pack Installation

Installation of vRealize Log Insight Management Pack for NSX is required for this step.

Figure 2.1 displays the dashboard upon logging into the vRealize Log Insight appliance.

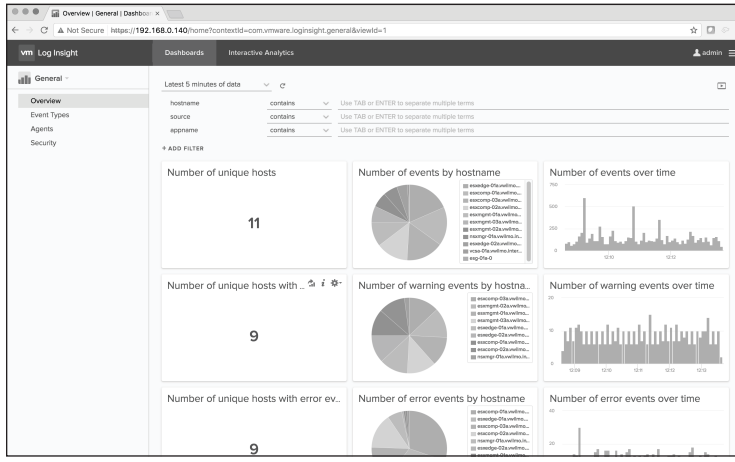


Figure 2.1 vRealize Log Insight dashboard

Click on the three lines next to ‘admin’ in the upper-right corner and select Content Packs

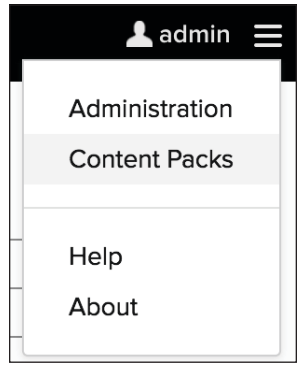


Figure 2.2 vRealize Log Insight content pack

This will present the Log Insight Content Pack Marketplace. Scroll down to the VMware – NSX-vSphere Management Pack.

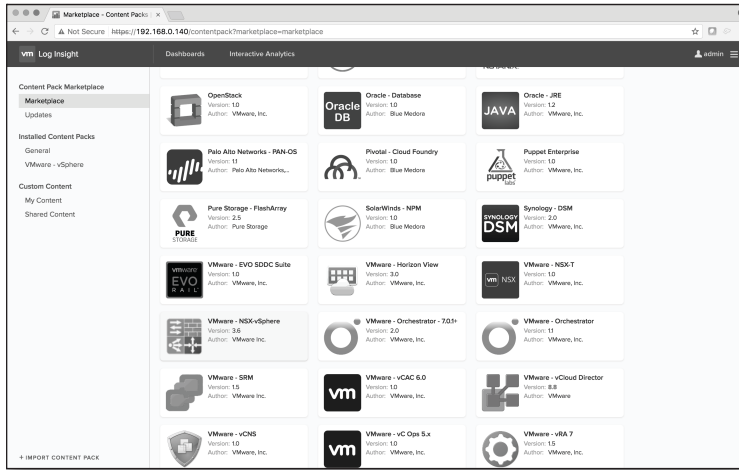


Figure 2.3 vRealize Log Insight marketplace

Upon selecting Content Pack, confirm the licensing agreement and click on Install.

Figure 2.4 shows the setup instructions required to configure forwarding of log information to vRealize Log Insight for processing.

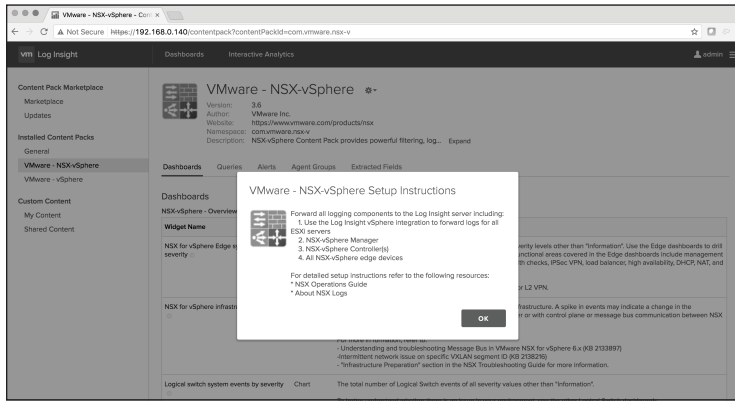


Figure 2.4 Setup instructions

As described in the Setup Instructions, configure the products to talk to vRealize Log Insight. For micro-segmentation, ensure that the ESXi hosts that could contain the application are configured to talk to the vRealize Log Insight server (192.168.0.140). Additionally, configure the VMware NSX Manager (192.168.0.120) server to talk to vRealize Log Insight.

Connect vCenter/ESXi Hosts to Log Insight

Set up the vSphere integration with vRealize Log Insight to allow configuration of the ESXi hosts with Log Insight as the syslog location.

From the Log Insight dashboard, select the same menu used to go into the Content Packs section, clicking on Administration.

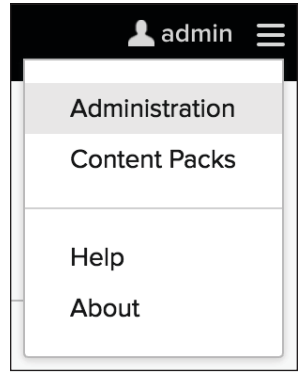


Figure 2.5 NSX Manager general settings

From the next screen, select ‘vSphere’ under the ‘Integration’ section

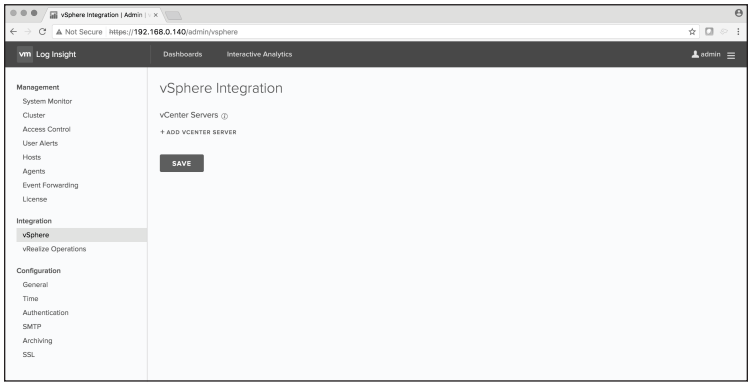


Figure 2.6 vSphere integration

The following steps will add the vCenter Server and configure hosts to send syslog to vRealize Log Insight.

- Enter the hostname of the VMware vCenter Server.®
- Enter a username that has access privileges to vCenter and can modify host objects.
- Enter the password for the username.

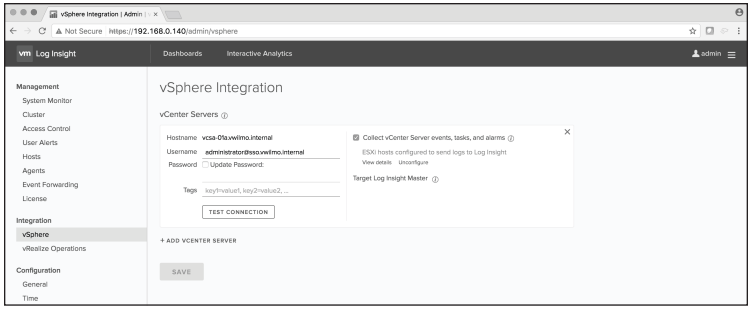


Figure 2.7 Infrastructure NSX security tags

Note that to the right of the input lines are options to ‘Collect vCenter Server events, tasks and alarms’ as well as ‘Configure ESXi hosts to send logs to Log Insight’. Under ‘Configure ESXi hosts to send logs to Log Insight’, is an ‘Advanced options…’ setting. Clicking the ‘Advanced options…’ link will allow selection of specific ESXi servers and communication protocols (e.g., TCP, UDP, or using SSL).

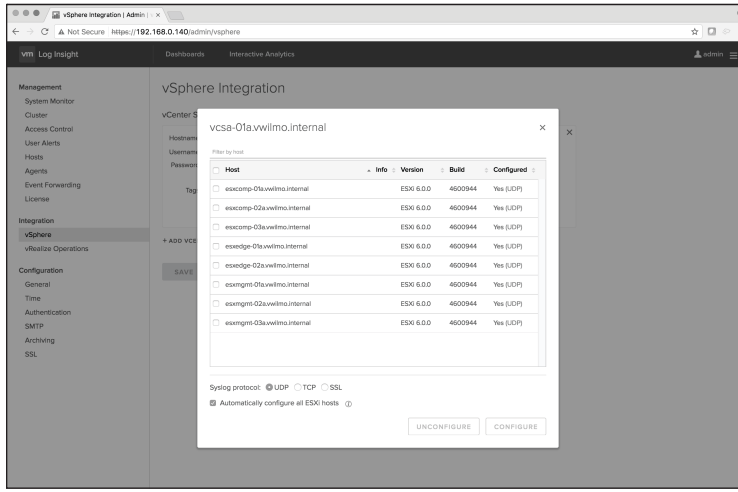


Figure 2.8 3-Tier application web NSX security group

This example configures all hosts to send their syslog data to Log Insight. Once complete, click on **OK** to complete.

Use **Test Connection** to ensure that connectivity to vCenter is working. Watch for 'Test successful' notification under the 'Test Connection' selection. Click on **Save** to complete the integration. If the hosts already have a syslog server configured, this integration will append the vRealize Log Insight server to the hosts as another syslog system.

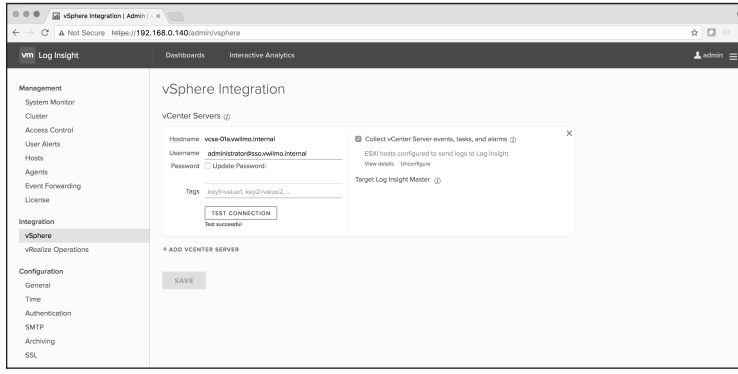


Figure 2.9 vRealize Log Insight vCenter – integration test

Connect NSX Manger to Log Insight

To begin the connection of NSX Manager to vRealize Log Insight, browse to the hostname/IP address of the NSX Manager and login.

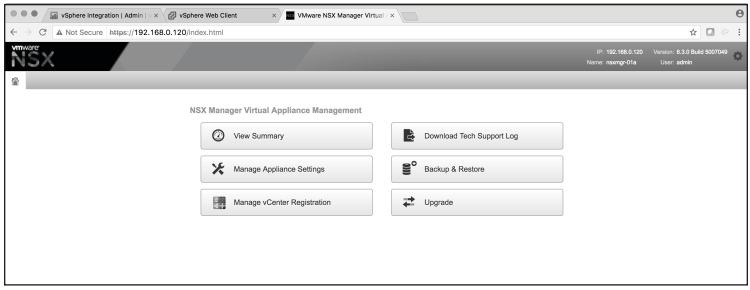


Figure 2.10 NSX Manager interface

From this screen, select **Manage Appliance Settings**

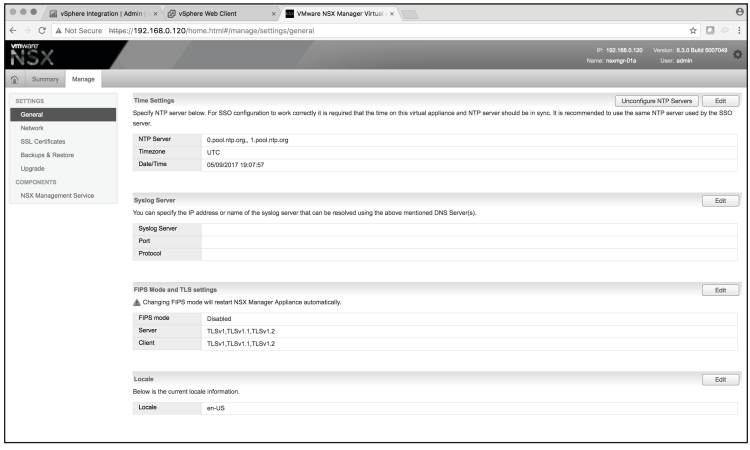


Figure 2.11 NSX Manager general settings

In this instance, the **Syslog Server** setting is not configured. Click on the **Edit** button and start the configuration.

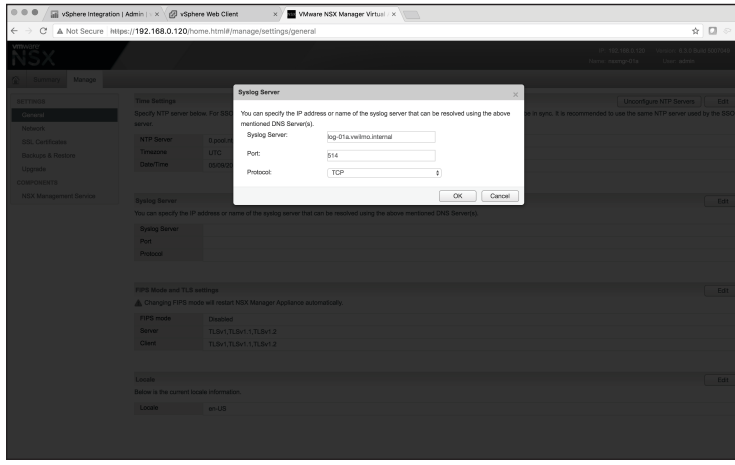


Figure 2.12 NSX Manager syslog server configuration

Enter the hostname/IP Address of the syslog server, port of 514, and select the TCP protocol. This will complete the syslog configuration for vRealize Log Insight help with micro-segmentation of the application.

Proper configuration can be validated through the dashboard. From the Log Insight web page, select the 'Dashboards' tab.

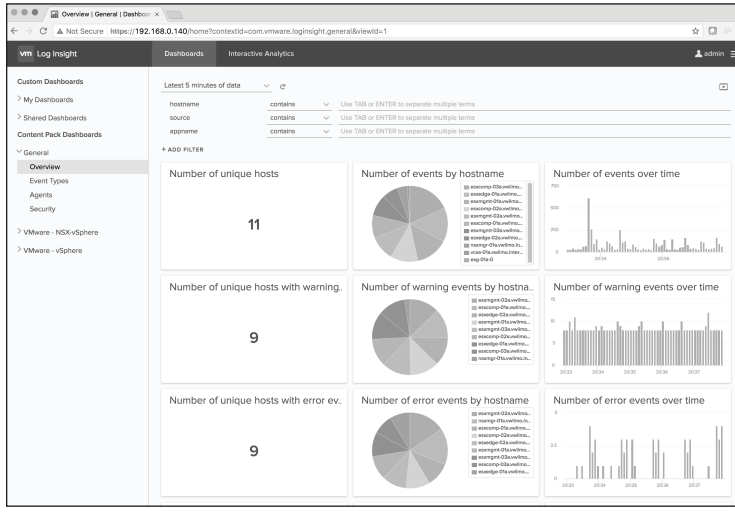


Figure 2.13 vRealize Log Insight main dashboard

Figure 2.14 shows the data populated in the dashboards interface, with the data present as expected from vCenter and the ESXi hosts.

On the left-hand side of the current dashboard is a selection option for changing to the other content pack dashboards in Log Insight. To confirm that NSX is also sending data, navigate under **Content Pack Dashboards to VMware – NSX-vSphere**.

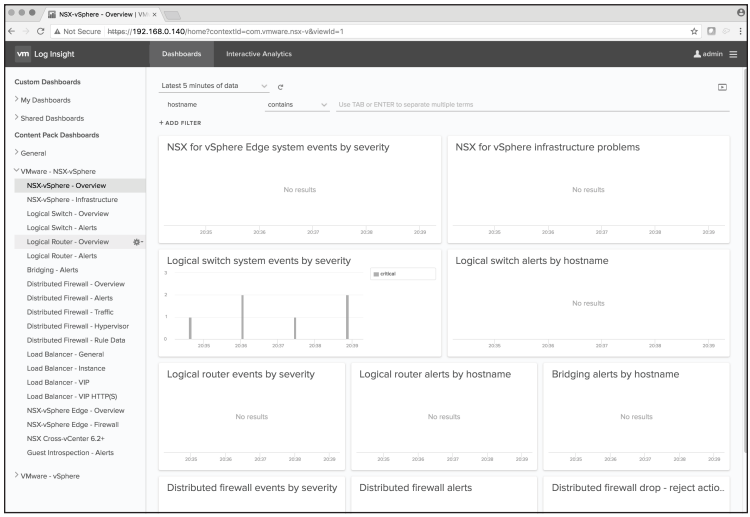


Figure 2.14 3-Tier application web applied to – web access rule

From this view, NSX data should be visible populating the dashboard.

This verifies that vCenter, the ESXi hosts, and NSX Manager are forwarding their syslog information to Log Insight. With this in place, work can begin on micro-segmenting the application.

Before starting the monitoring process, create a **Security Group** that encompasses all the application's VMs to simplify definition of block and allow rules. These initial rules will provide visibility on how the application communicates with itself and the external world. They will then be replaced by more granular rules that restrict the Flows down to only essential traffic.

Layout Naming Scheme

Table 2.6 3-Tier application naming scheme layout

Security Groups	Systems Included	Services	Security Tags
SG-3T-ALL	SG-3T-WEB, SG-3T-APP, SG-3T-DB	-	-
SG-3T-WEB	Web01, Web02	SV-3T-HTTP	ST-3T-WEB
SG-3T-APP	App01	SV-3T-APP	ST-3T-APP
SG-3T-DB	DB01	SV-3T-MYSQL	ST-3T-DB
SG-INFRA-ALL	SG-NTP-ALL	-	-
SG-NTP-ALL	NTP-01a	SV-NTP	ST-NTP-ALL

The table in Table 2.6 identifies the basic building blocks of what is known about the application. If other types of communication are discovered, they should be investigated to determine whether they are necessary for core application functionality.

Next take all the groupings and build them out in the NSX Manager. Start with **Security Tags**.

Create Security Groups – Infrastructure Services/Application

Procedure

1. Log into the **VMware vSphere® Web Client** and select **Networking and Security**.
2. Select the **NSX Managers** tab under the **Networking & Security Inventory**.
3. Select the IP address of the **NSX Manager**.
4. Select **Manage**.
5. Select **Security Tags**.
6. Click on the **New Security Tag** () icon.
7. Type the Name **ST-3T-WEB** and optional description.
8. Click **OK**.
9. Repeat this same process for App, DB, and NTP.

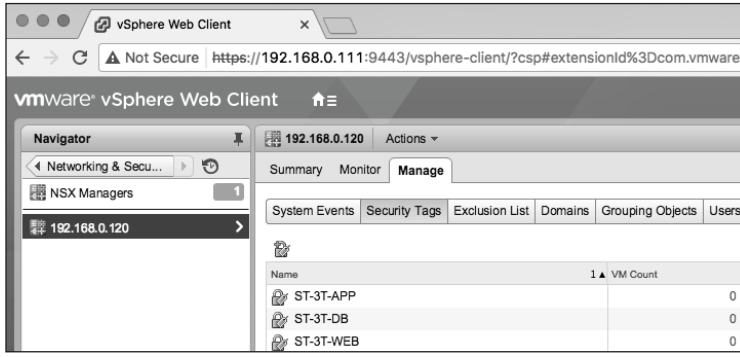


Figure 2.15 3-Tier application NSX security tags

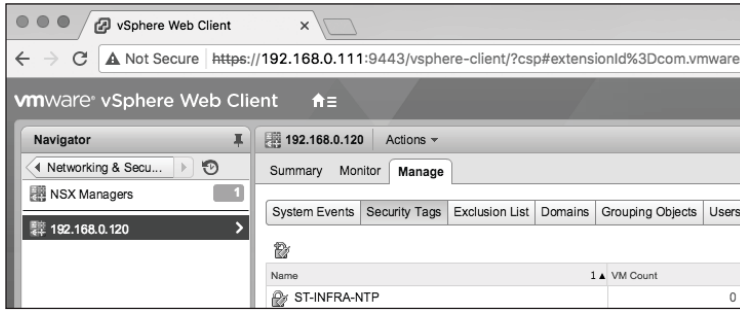


Figure 2.16 Infrastructure NSX security tags

Once the **Security Tags** are created, associate them the appropriate virtual machines.

Procedure

1. From the **Security Tags** screen, select the **ST-3T-WEB Security Tag**.
2. Click on the **Assign Security Tag** ( ) icon.
3. Filter the virtual machine list by typing **'Web0'**.
4. Add both **Web01** and **Web02** to the **Included Items** list.
5. Click **OK**.
6. Repeat the process for the App, DB, and NTP **Security Tags**.

Once the **Security Tags** are applied, the results should appear as in Figures 2.15 and 2.16.

With **Security Tags** in place, they can be used to create **Security Groups**.

Procedure

1. Log into the **vSphere Web Client** and select **Networking and Security**.
2. Select the **NSX Managers** tab under the **Networking & Security Inventory**.
3. Select the IP address of the **NSX Manager**.
4. Select **Manage**.
5. Select **Grouping Objects**.
6. Click on the **Add new Security Group** (➕) icon.
7. Type the name **SG-3T-WEB** and optional description for the **Security Group**.
8. Click **Next**.
9. Click **Next**.
10. Change Object Type to **Security Tag** and in the search box type **3T**. Select the **ST-3T-WEB Security Tag**.

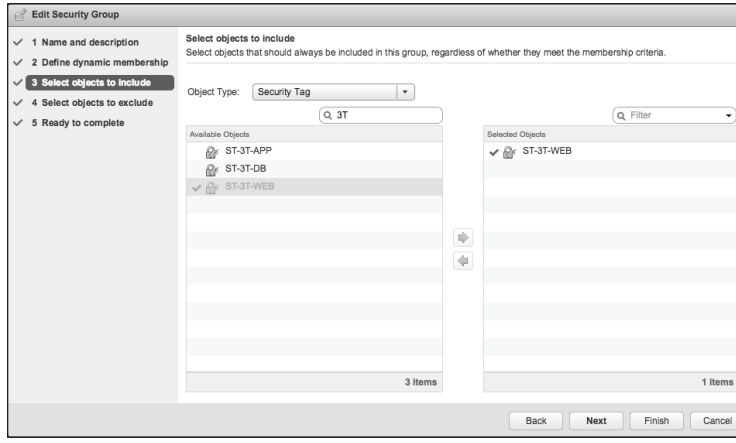


Figure 2.17 3-Tier application NSX DFW rules documentation

11. Click on **Finish**.
12. Repeat this process adding the **App01** and **DB01** to the appropriate **Security Groups**.
13. Repeat this process adding NTP-01a to the appropriate **Security Group**.

To make things easier for writing rulesets, create the **SG-3T-ALL Security Group** and nest the newly created web, app, and DB Security Groups inside. This will allow new servers added to the application to be covered by the same set of rules.

To do this, perform the same procedure as above, but instead add the newly created Security Groups rather than virtual machines at the Object Type.

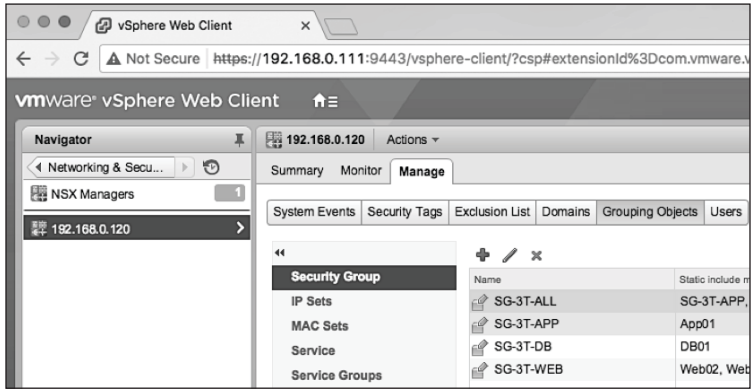


Figure 2.18 3-Tier application all NSX security groups

After building the **Security Group** and **Security Tag** layout, these constructs are used to create block and allow rules.

Build DFW Rules for Allow/Block

Build block and allow rules with logging enabled to monitor the application and see how it communicates. A basic layout for the rules it outlined in Table 2.7.

Table 2.7 3-Tier application block and allow NSX DFW rules

Name	Source	Destination	Service	Action	Applied To
Allow Any to App Log	Any	SG-3T-ALL	Any	Allow	SG-3T-ALL
Allow App to Any Log	SG-3T-ALL	Any	Any	Allow	SG-3T-ALL
Block Any to App Log	Any	SG-3T-ALL Any	Any	Block	SG-3T-ALL
Block App to Any Log	SG-3T-ALL	Any	Any	Block	SG-3T-ALL

When taking an application-based segmentation approach, use per-application block rules.

Procedure

1. Log into the **vSphere Web Client** and select **Networking and Security**.
2. Click on **Firewall**.
3. Right-click on the **Default Section Layer3** and select **Add Section**.
4. Enter the name of the Section as **Book Application**.
5. Click **Save**.
6. Right-click on the new **Book Application** Section and select **Add rule**.
7. Expand the **Book Application Section** to edit the rule.
8. Click on the **Add rule** () icon on the **Book Application** Section three more times to add the necessary rule instances.

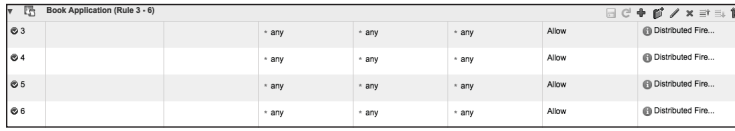


Figure 2.19 3-Tier application NSX DFW blank table

Next add the details to each rule per the table.

First Allow Rule Configuration

1. Click on the **Edit** () icon for the first rule **Name**.
2. Add name **Allow Any to App Log** and click **Save**.
3. Click on the **Edit** () icon for the first rule **Destination**.
4. Change the Object Type to **Security Group** and filter on **3T**.
5. Add the **SG-3T-ALL Security Group** and click **OK**.
6. Click on the **Edit** () icon for the first rule **Action**.
7. Click on the **Log** radio button and click **Save**.
8. Click on the **Edit** () icon for the first rule **Applied To**.
9. Uncheck the first check box.
10. Change the Object Type to **Security Group** and filter on **3T**.
11. Select the **SG-3T-ALL** and click **OK**.

Second Allow Rule Configuration

1. Click on the **Edit** ( ) icon for the second rule **Name**.
2. Add name **Allow App to Any Log** and click **Save**.
3. Click on the **Edit** ( ) icon for the second rule **Source**.
4. Change the Object Type to **Security Group** and filter on **3T**.
5. Add the **SG-3T-ALL Security Group** and click **OK**.
6. Click on the **Edit** ( ) icon for the second rule **Action**.
7. Click on the **Log** radio button and click **Save**.
8. Click on the **Edit** ( ) icon for the second rule **Applied To**.
9. Uncheck the first check box.
10. Change the Object Type to **Security Group** and filter on **3T**.
11. Select the **SG-3T-ALL** and click **OK**.

First Block Rule Configuration

1. Click on the **Edit** ( ) icon for the third rule **Name**.
2. Add name **Block Any to App Log** and click **Save**.
3. Click on the **Edit** ( ) icon for the third rule **Destination**.
4. Change the Object Type to Security Group and filter on **3T**.
5. Add the **SG-3T-ALL Security Group** and click **OK**.
6. Click on the **Edit** ( ) icon for the third rule **Action**.
7. Change the Action to **Block**.
8. Click on the **Log** radio button and click **Save**.
9. Click on the **Edit** ( ) icon for the third rule **Applied To**.
10. Uncheck the first check box.
11. Change the Object Type to Security Group and filter on **3T**.
12. Select the **SG-3T-ALL** and click **OK**.

Second Block Rule Configuration

1. Click on the **Edit** ( ) icon for the fourth rule **Name**.
2. Add name **Block App to Any** Log and click **Save**.
3. Click on the **Edit** ( ) icon for the fourth rule **Source**.
4. Change the Object Type to **Security Group** and filter on **3T**.
5. Add the **SG-3T-ALL Security Group** and click **OK**.
6. Click on the **Edit** ( ) icon for the fourth rule **Action**.
7. Change the Action to **Block**.
8. Click on the **Log** radio button and click **Save**.
9. Click on the **Edit** ( ) icon for the fourth rule **Applied To**.
10. Uncheck the first check box.
11. Change the Object Type to **Security Group** and filter on **3T**.
12. Select the **SG-3T-ALL** and click **OK**.

Once the block and allow configurations are all completed, **Publish** the rules to the virtual machines.

When complete, the NSX Manager will assign a **RuleID** for each new rule created.

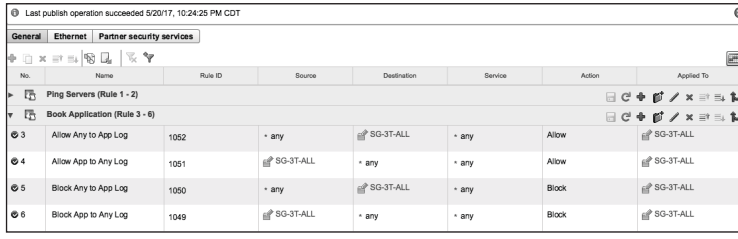


Figure 2.20 3-Tier application block and allow NSX DFW table

Monitor Traffic Flows

With all the traffic from the application now being logged to vRealize Log Insight, all Flows should now be visible. The two rules of interest in vRealize Log Insight – shown in Figure 2.20 – are **1051** and **1052**.

The first recommended test is confirmation of application functionality. With allow rules above the block rules, all traffic for the application should be Flowing without interruptions.

From the 192.168.0.99 system, check connectivity to the application through both Web01 and Web02.

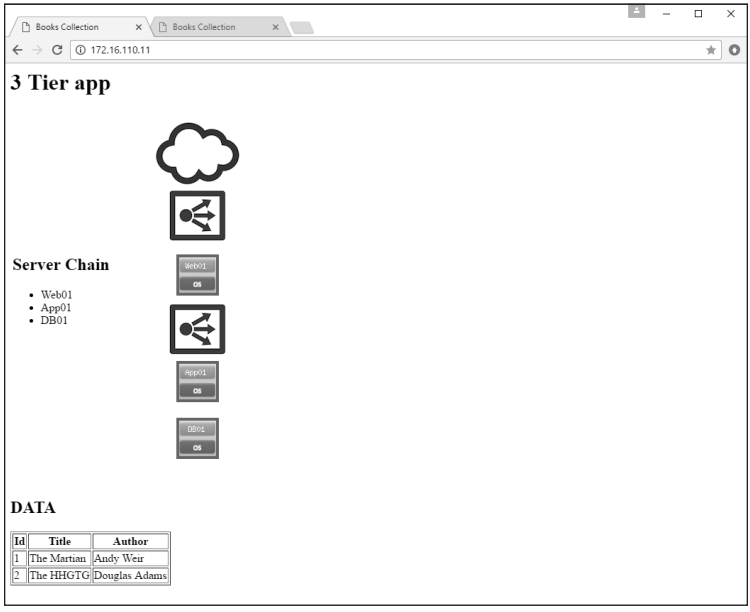


Figure 2.21 3-Tier application web 1 server functional

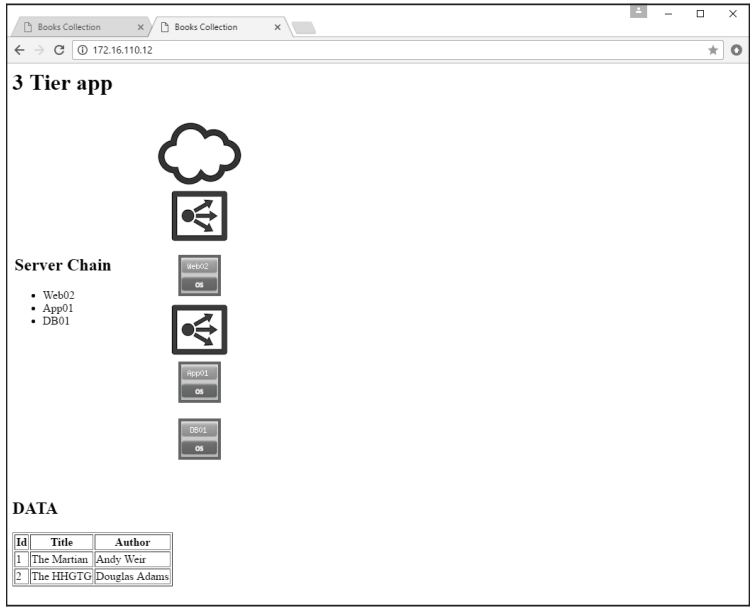


Figure 2.22 3-Tier application web 2 server functional

Figures 2.28 and 2.29 confirm that the application is functional using both of the web servers, Web01 and Web02. A review of vRealize Log Insight shows hits on RuleIDs **1051** and **1052** from the NSX DFW.

Procedure

1. Log into the vRealize Log Insight appliance.
2. Click on the **VMware – NSX-vSphere** dashboard under **Content Pack Dashboards**.
3. Click on **Distributed Firewall – Rule Data**.
4. Verify **Connections by RuleID** are showing hits on rule **1051** and **1052**.

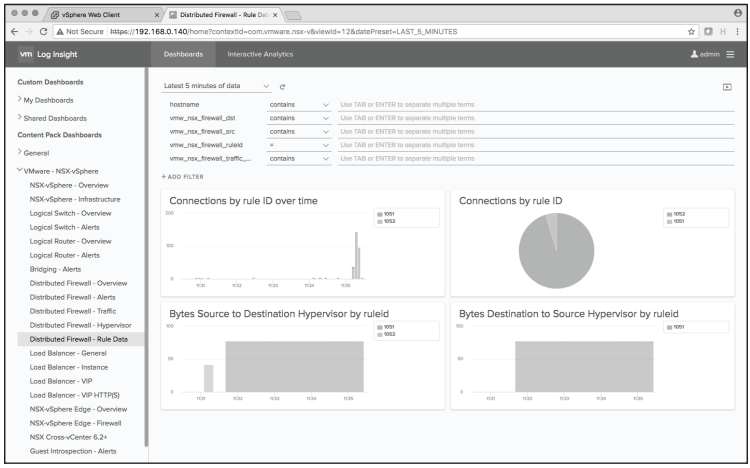


Figure 2.23 3-Tier application vRealize Log Insight NSX DFW rule data

As seen in Figure 2.23, the NSX DFW shows connections through RuleIDs **1051** and **1052**. With this verification, the next step is an analysis of application communication Flows as shown in log data.

Analyze Traffic Flows

Following the process previously laid out, first build the infrastructure services rules for the application. Place these rules at the top of the Book Application section. Then move to the granular application-specific rules to complete the micro-segmentation of the application.

Procedure

1. Log into the vRealize Log Insight appliance.
2. Click on the **VMware – NSX-vSphere** dashboard under **Content Pack Dashboards**.
3. Click on **Distributed Firewall – Rule Data**.
4. Within the **Connections by RuleID** widget select the ( ) to go into **Interactive Analytics**.
5. Select the **Field Table** and open the Fields filter window on the right.
6. Expand the **vmw_nsx_firewall_dst_port** filter to show all of the ports that vRealize Log Insight has observed from the Flow logs.

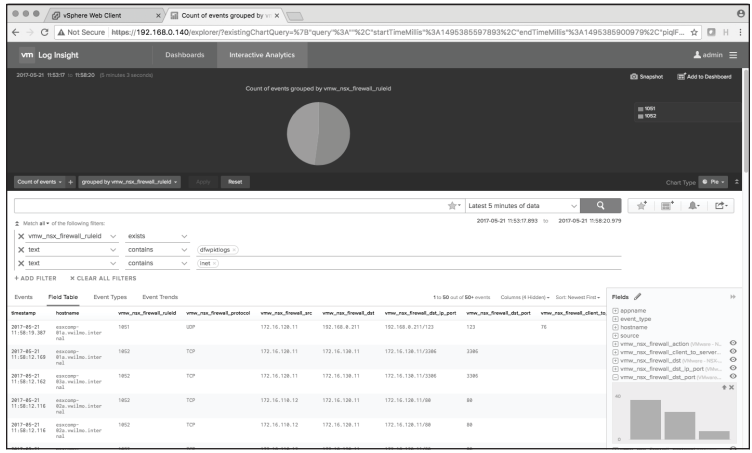


Figure 2.24 3-Tier application vRealize Log Insight field table

Port IDs are identified by hovering the mouse over the leftmost column. The filter **Fields** shows application port use – in this example ports 80, 3306, and 123.

Figure 2.25 3-Tier application vRealize Log Insight destination ports

The **Field Table** is helpful in illustrating communication between sets of servers.

Figure 2.26 3-Tier application vRealize Log Insight full field table

This output allows for extrapolation of the Flows for the application, facilitating proper grouping. The annotations in Figure 2.26 call out the following Flows:

- 172.16.110.11 (Web01), 172.16.110.12 (Web02), 172.16.120.11 (App01), and 172.16.130.11 (DB01) are talking to 192.168.0.211(NTP-01a) over UDP 123.
- 192.168.0.99 (Jumbox-01a) is talking to both 172.16.110.11 (Web01) and 172.16.110.12 (Web02) over TCP port 80.
- Both 172.16.110.11 (Web01) and 172.16.110.12(Web02) are communicating with 172.16.120.11 (App01) over TCP port 80.
- 172.16.120.11(App01) is talking to 172.16.130.11(DB01) over TCP port 3306.

Upon completing analysis, use the information to document the rules necessary to enhance micro-segmentation granularity.

Document Rules for DFW – Infrastructure Services/Application

After compiling the necessary information to write DFW rules, lay the information out in table format that is easy to read and simplifies creation within NSX.

Table 2.8 3-Tier application NSX DFW rules documentation

Infrastructure Access Communications:

Name	Source	Destination	Service	Action	Applied To
APP Access	SG-3T-ALL	SG-INFRA-NPT	SV-NTP-ALL	Allow	SG-3T-ALL SG-INFRA-NTP

NSX Groupings:

Security Group	SG-Contains	SG-Inclusion Criteria
SG-INFRA-NTP	NTP-01a	Static

Book Application Acess Communications:

Name	Source	Destination	Service	Action	Applied To
Any Access App	SG-3T-WEB (Negate Source)	SG-3T-WEB	SV-3T-HTTP	Allow	SG-3T-WEB

Intra-Book Application Communications:

Name	Source	Destination	Service	Action	Applied To
Allow Web to App	SG-3T-WEB	SG-3T-APP	SV-3T-HTTP	Allow	SG-3T-WEB SG-3T-APP
Allow App to DB	SG-3T-APP	SG-3T-DB	SV-3T-MYSQL	Allow	SG-3T-APP SG-3T-DB

Book All Book Application Communications:

Name	Source	Destination	Service	Action	Applied To
Block Inbound Infra	SG-3T-ALL	Any	Any	Block	SG-3T-ALL
Block Outbound Infra	Any	SG-3T-ALL	Any	Block	SG-3T-ALL

NSX Groupings:

Security Group	SG-Contains	SG-Inclusion Criteria
SG-3T-ALL	SG-3T-WEB SG-3T-APP SG-3T-DB	Static

Security Group	SG-Contains
SV-INFRA-NTP	UDP 123
SV-3T-HTTP	TCP 80
SV-3T-MYSQL	TCP 3306

Create Services – Infrastructure Services

With vRealize Log Insight identifying the services used by the application, they can now be built in NSX. NSX comes with a significant set of default services built into the product. These can be used for writing an organization's NSX DFW rules or creation of a custom service where one does not already exist. This example creates custom services to make them easily identifiable.

Procedure

1. Log into the **vSphere Web Client** and select **Networking and Security**.
2. Select the **NSX Managers** tab under the **Networking & Security Inventory**.
3. Select the IP address of the **NSX Manager**.
4. Select **Manage**.
5. Select **Grouping Objects**.
6. Select **Service**.
7. Click on the **Add Service** (✚) icon.
8. Enter the name **SV-INFRA-NTP**, change the protocol to **UDP**, and enter the Destination port as **123**.

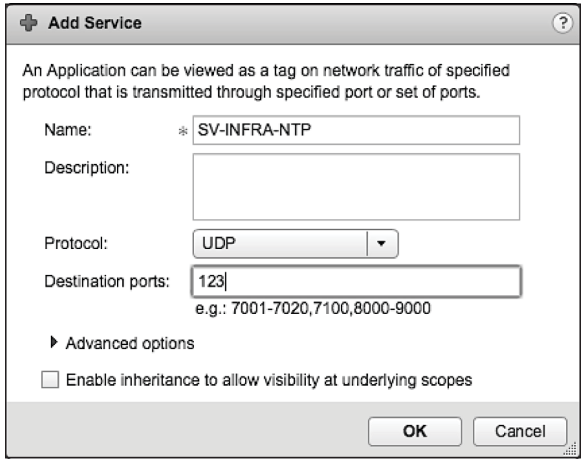


Figure 2.27 3-Tier application web source – web access rule

9. Click **OK**.

Create Services – Application

Repeat the process as with infrastructure services for the application-specific services.

Procedure

1. Log into the **vSphere Web Client** and select **Networking and Security**.
2. Select the **NSX Managers** tab under the **Networking & Security Inventory**.
3. Select the IP address of the **NSX Manager**.
4. Select **Manage**.
5. Select **Grouping** Objects.
6. Select **Service**.
7. Click on the **Add Service** (➕) icon.
8. Enter the name SV-3T-HTTP, change the protocol to TCP, enter the Destination port as 80.

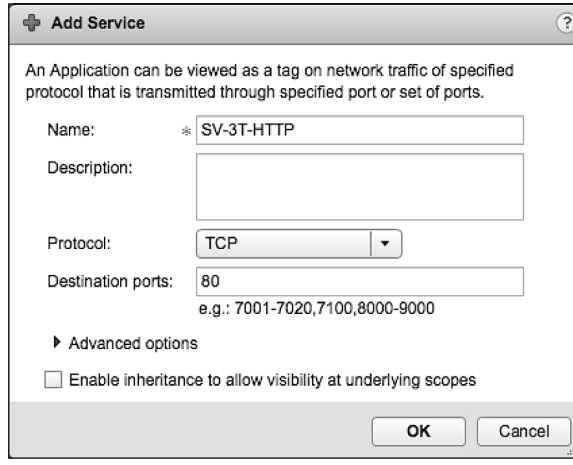


Figure 2.28 3-Tier application add HTTP service

9. Click **OK**.
10. Click on the **Add Service** (➕) icon.

11. Enter the name SV-3T-MYSQL, change the protocol to TCP, and enter the Destination port as 3306.

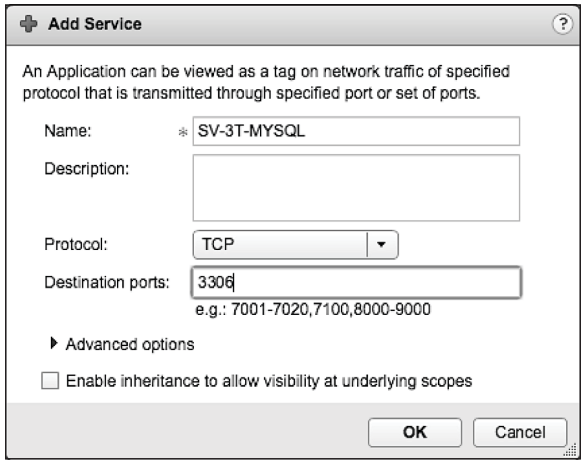


Figure 2.29 3-Tier application add MySQL service

12. Click **OK**.

Verify all services are configured.

Name	1 ▼	Protocol	Destination ports	Source ports	Scope
SV-INFRA-NTP		UDP	123	any	Global
SV-3T-MYSQL		TCP	3306	any	Global
SV-3T-HTTP		TCP	80	any	Global

Figure 2.30 3-Tier application and infrastructure NSX service verification

Build DFW Rules – Infrastructure Services

As shown from the Flows in Figure 2.30 all of the servers comprising the Book Application are communicating with the 192.168.0.211(NTP-01a) server. There is a Security Group that has all of the servers within it, making this straightforward rule to create.

Procedure

1. Log into the **vSphere Web Client** and select **Networking and Security**.
2. Click on **Firewall**.
3. Expand **Book Application Section** and the **Add rule** (+) icon.
4. Click on the **Edit** (✎) icon for the new rule **Name**.
5. Add name **Allow Access Infra** and click **Save**.
6. Click on the **Edit** (✎) icon for the new rule **Source**.
7. Change the Object Type to **Security Group** and filter on **3T**.
8. Add the **SG-3T-ALL Security Group** and click **OK**.

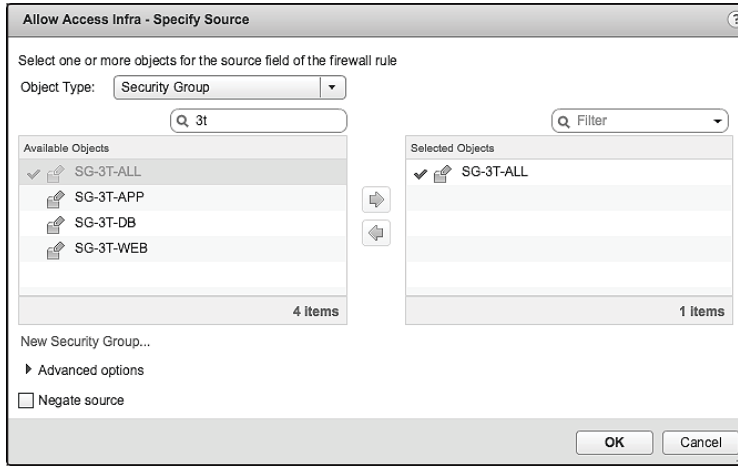


Figure 2.31 3-Tier application all source – infrastructure access rule

9. Click on the **Edit** (✎) icon for the new rule **Destination**.
10. Change the Object Type to **Security Group** and filter on **SG-INFRA**.
11. Add the **SG-INFRA-NTP Security Group** and click **OK**.

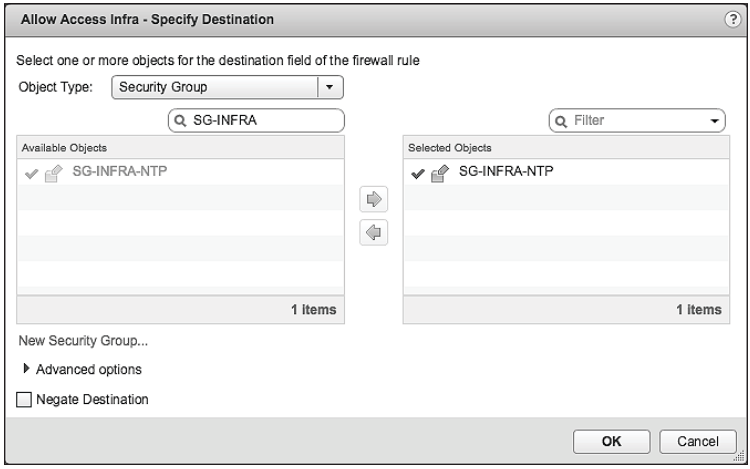


Figure 2.32 Infrastructure destination – infrastructure access rule

12. Click on the **Edit** ( ) icon for the new rule **Service**.
13. Change the Object Type to **Service** and filter on **SV-INFRA**.
14. Add the **SV-INFRA-NTP Service** and click **OK**.
15. Click on the **Edit** ( ) icon for the new rule **Action**.
16. Click on the **Log** radio button and click **Save**.

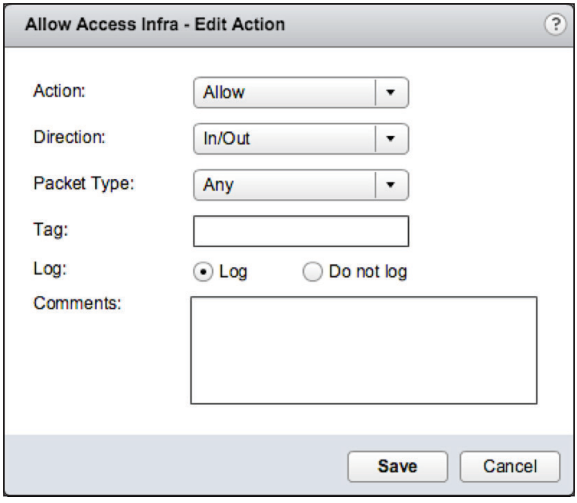


Figure 2.33 3-Tier application allow – infrastructure access rule

17. Click on the **Edit** ( ) icon for the new rule **Applied To**.
18. Uncheck the first check box.
19. Change the Object Type to **Security Group** and filter on **3T**.
20. Select the **SG-3T-ALL** and click **OK**

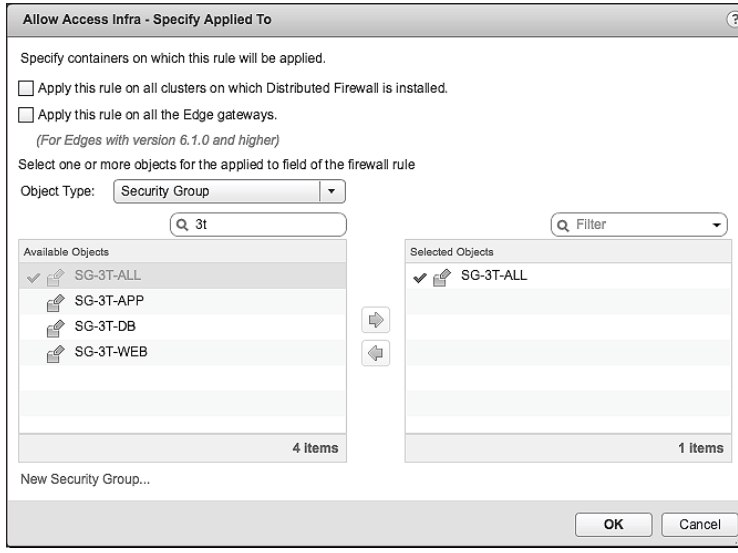


Figure 2.34 3-Tier application applied to – infrastructure access rule

Once the new infrastructure services rule is completed, **Publish** the rules down to the virtual machines. Upon completion, the NSX Manager will assign a **RuleID** for each new rule created.

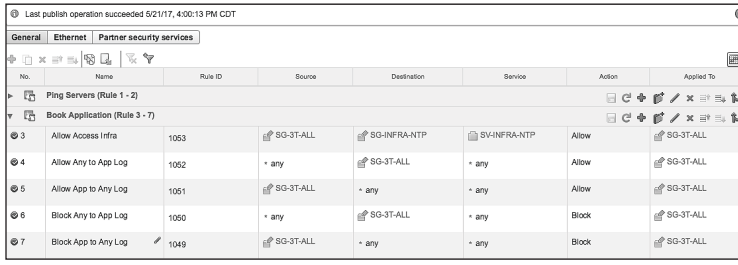


Figure 2.35 Infrastructure access NSX DFW table

Build DFW Rules – Application

Move to the Book Application rules and break out the communications with NSX DFW rules. The first rule that needs to be created is the rule to allow access to the Book Application.

Procedure

1. Log into the **vSphere Web Client** and select **Networking and Security**.
2. Click on **Firewall**.
3. Expand **Book Application Section** and click on the **Allow Access Infra** rule.
4. Click on the **Add rule** (➕) icon. This will put a new rule below the **Allow Access Infra** rule.
5. Click on the **Edit** (✎) icon for the new rule **Name**.
6. Add name **Any Access App** and click **Save**.
7. Click on the **Edit** (✎) icon for the new rule **Source**.
8. Change the Object Type to **Security Group** and filter on **3T**.
9. Add the **SG-3T-WEB Security Group** and check the **Negate Source** box and click **OK**.
   - Negating the Source functionally prevents the source – SG-3T-WEB – from communicating to itself as the destination. All other Sources are allowed.

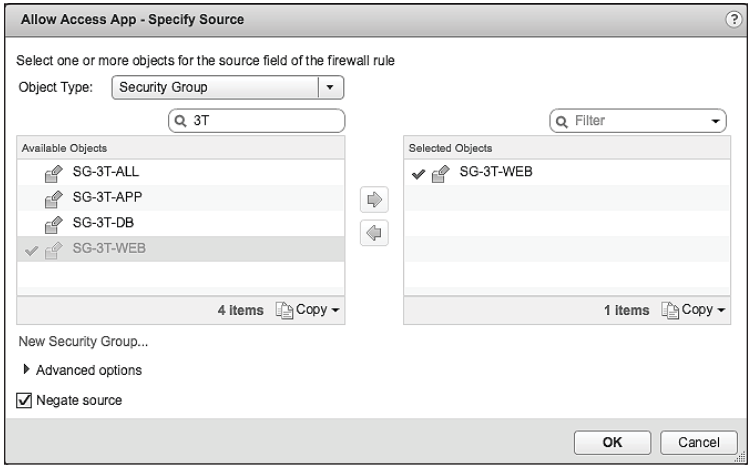


Figure 2.36 3-Tier application web source – web access rule

10. Click on the **Edit** ( ) icon for the new rule **Destination**.
11. Change the Object Type to **Security Group** and filter on **3T**.
12. Add the **SG-3T-WEB Security Group** and click **OK**.

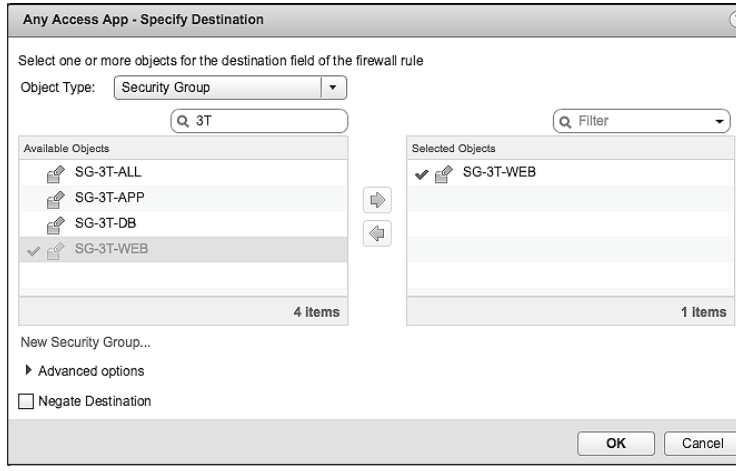


Figure 2.37 3-Tier application web destination – web access rule

13. Click on the **Edit** ( ) icon for the new rule **Service**.
14. Change the Object Type to **Security Group** and filter on **SV-3T**.
15. Add the **SV-3T-HTTP Security Group** and click **OK**.

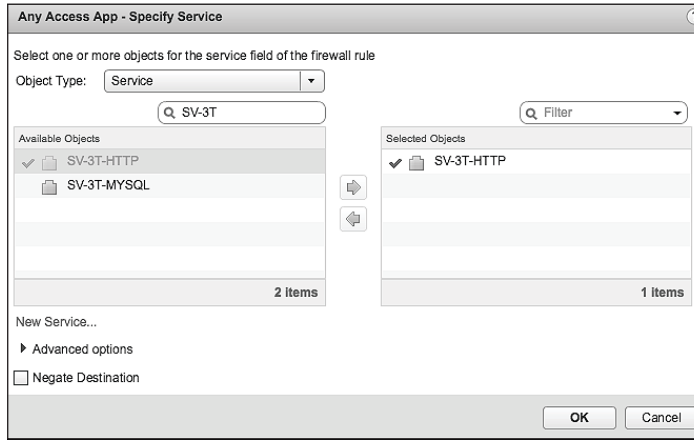


Figure 2.38 3-Tier application web service – web access rule

16. Click on the **Edit** ( ) icon for the new rule **Action**.

17. Click on the **Log** radio button and click **Save**.

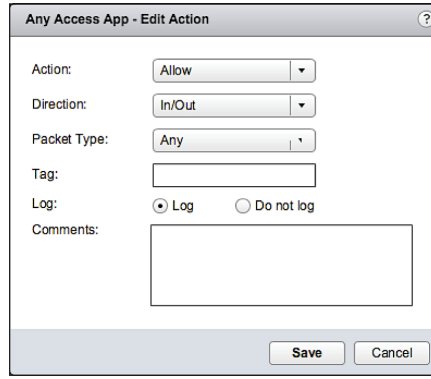


Figure 2.39 3-Tier application allow – web access rule

18. Click on the **Edit** ( ) icon for the new rule **Applied To**.

19. Uncheck the first check box.

20. Change the Object Type to **Security Group** and filter on **3T**.

21. Select the **SG-3T-WEB Security Group** and click **OK**.

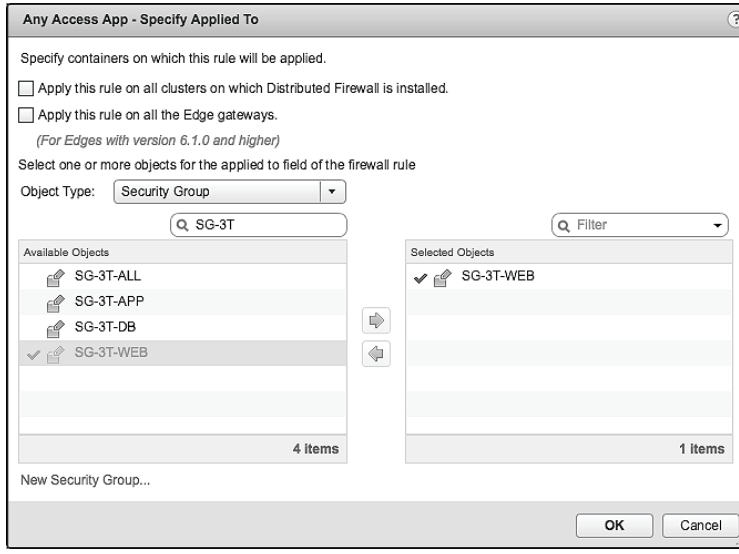


Figure 2.40 3-Tier application web applied to – web access rule

Web to App Rule

1. Click on the **Add rule** () icon. This will put a new rule below the **Any Access App** rule.
2. Click on the **Edit** () icon for the new rule **Name**.
3. Add name **Web to App** and click **Save**.
4. Click on the **Edit** () icon for the new rule **Source**.
5. Change the Object Type to **Security Group** and filter on **3T**.
6. Add the **SG-3T-WEB Security Group** and click **OK**.

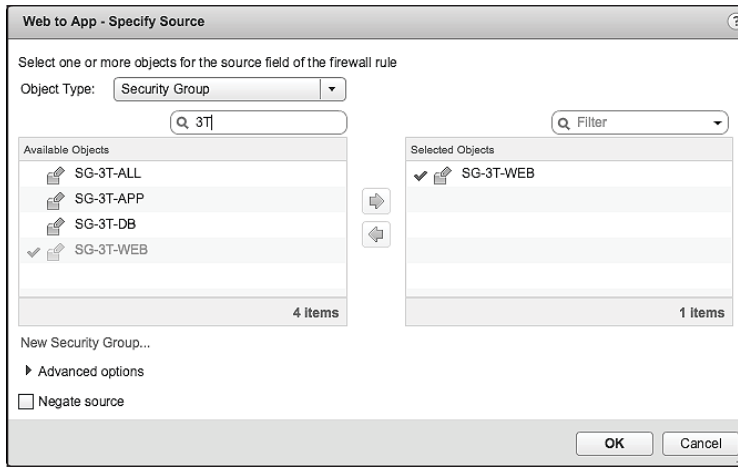


Figure 2.41 3-Tier application web source – Web to App rule

7. Click on the **Edit** () icon for the new rule **Destination**.
8. Change the Object Type to **Security Group** and filter on **3T**.

9. Add the **SG-3T-APP Security Group** and click **OK**.

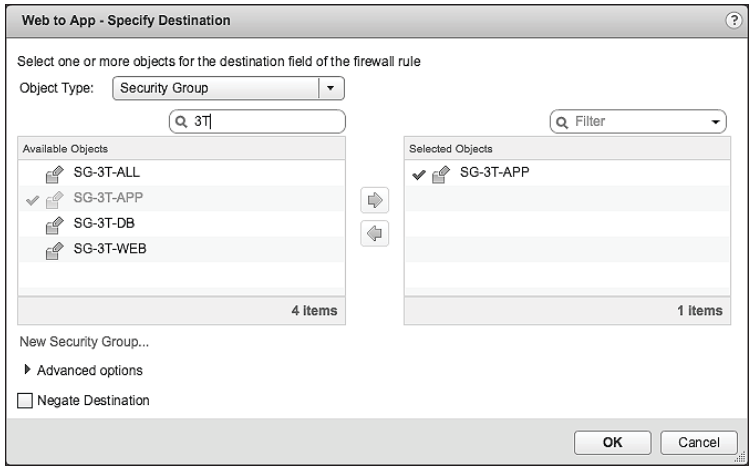


Figure 2.42 3-Tier application web service – Web to App rule

10. Click on the **Edit** ( ) icon for the new rule **Service**.
11. Change the Object Type to **Security Group** and filter on **SV-3T**.
12. Add the **SV-3T-HTTP Security Group** and click **OK**.

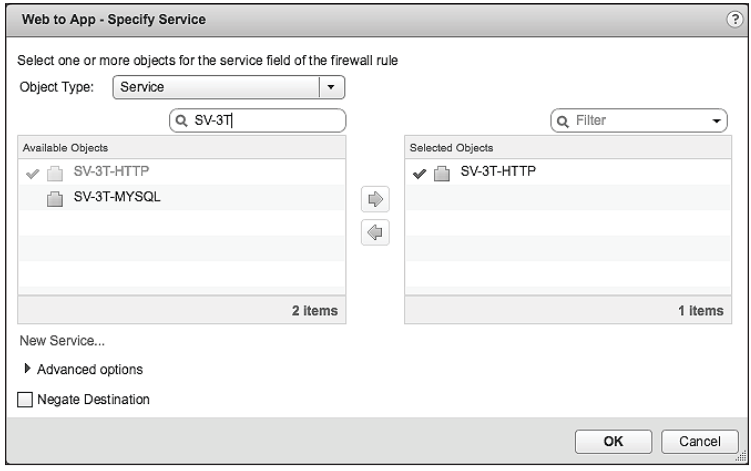


Figure 2.43 3-Tier application web service – Web to App rule

13. Click on the **Edit** ( ) icon for the new rule **Action**.

14. Click on the **Log** radio button and click **Save**.

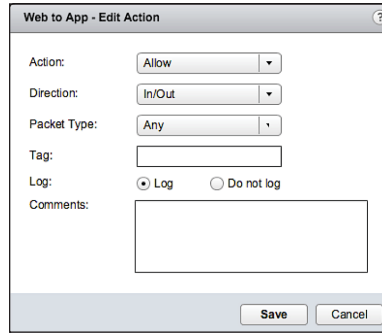


Figure 2.44 3-Tier application allow – Web to App rule

15. Click on the **Edit** ( ) icon for the new rule **Applied To**.

16. Uncheck the first check box.

17. Change the Object Type to **Security Group** and filter on **3T**.

18. Select the **SG-3T-WEB** and **SG-3T-APP Security Group** and click **OK**.

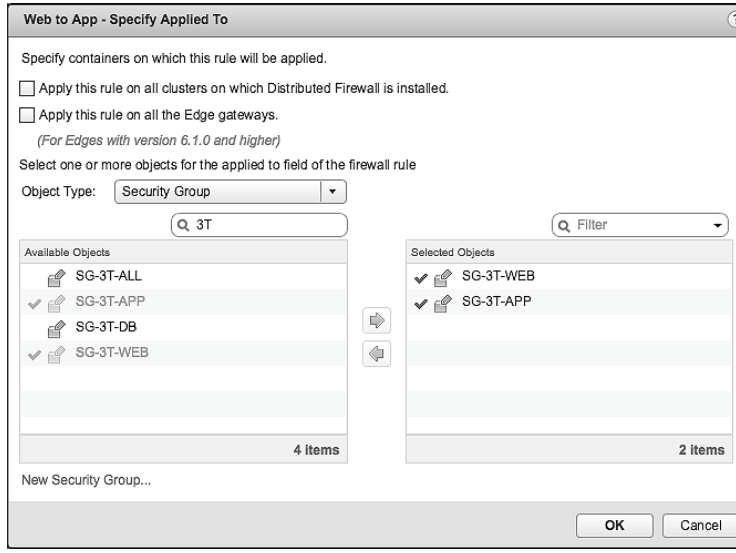


Figure 2.45 3-Tier application applied to Web and App – Web to App rule

App to DB Rule

1. Click on the **Add rule** (➕) icon. This will put a new rule below the **Web to App** rule.
2. Click on the **Edit** (✏) icon for the new rule **Name**.
3. Add name **App to DB** and click **Save**.
4. Click on the **Edit** (✏) icon for the new rule **Source**.
5. Change the Object Type to **Security Group** and filter on **3T**.
6. Add the **SG-3T-App Security Group** and click **OK**.

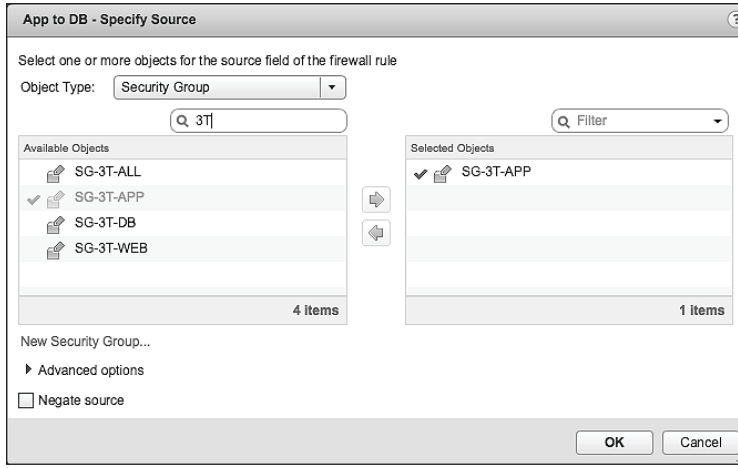


Figure 2.46 3-Tier application source app – App to DB rule

7. Click on the **Edit** (✏) icon for the new rule **Destination**.
8. Change the Object Type to **Security Group** and filter on **3T**.

9. Add the **SG-3T-DB Security Group** and click **OK**.

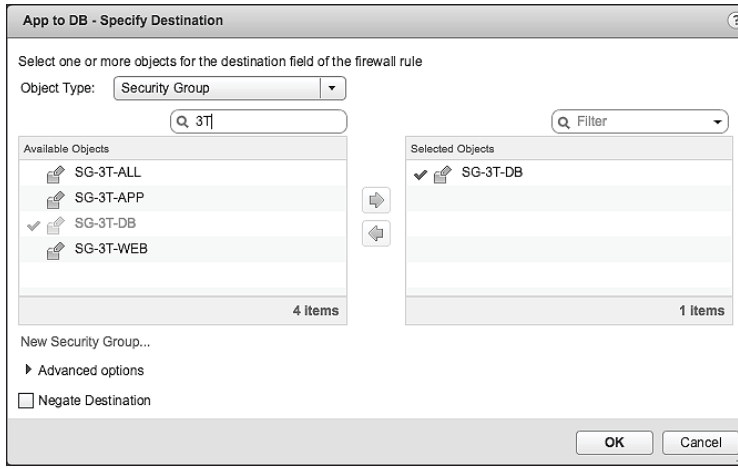


Figure 2.47 3-Tier application destination DB – App to DB rule

10. Click on the **Edit** ( ) icon for the new rule **Service**.
11. Change the Object Type to **Security Group** and filter on **SV-3T**.
12. Add the **SV-3T-MYSQL Security Group** and click **OK**.

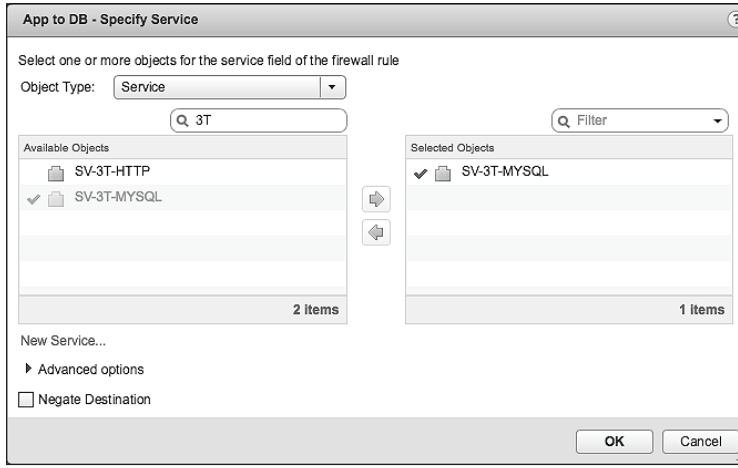


Figure 2.48 3-Tier application app service – App to DB rule

13. Click on the **Edit** ( ) icon for the new rule **Action**.
14. Click on the **Log** radio button and click **Save**.

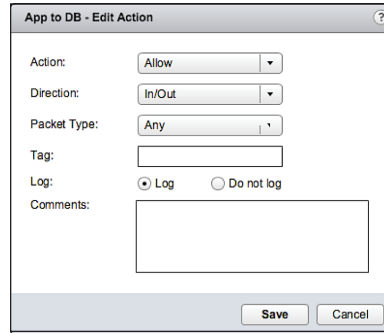


Figure 2.49 3-Tier application allow – App to DB rule

15. Click on the **Edit** ( ) icon for the new rule **Applied To**.
16. Uncheck the first check box.
17. Change the **Object Type to Security Group** and filter on **3T**.
18. Select the **SG-3T-APP** and **SG-3T-DB Security Group** and click **OK**.

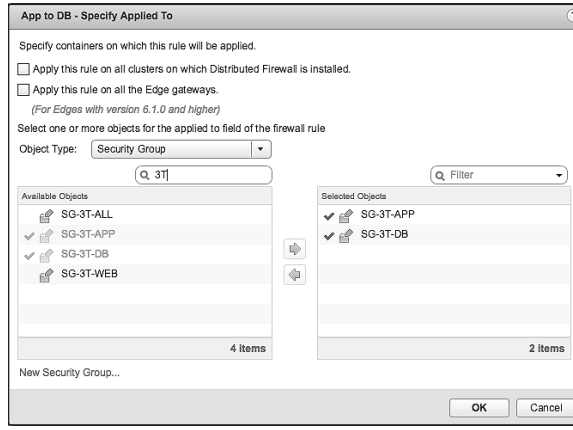


Figure 2.50 3-Tier application applied to app and DB – App to DB rule

Once the new infrastructure services rule is completed, **Publish** the rules down to the virtual machines.

Upon completion, the NSX Manager will assign a **RuleID** for each new rule created.

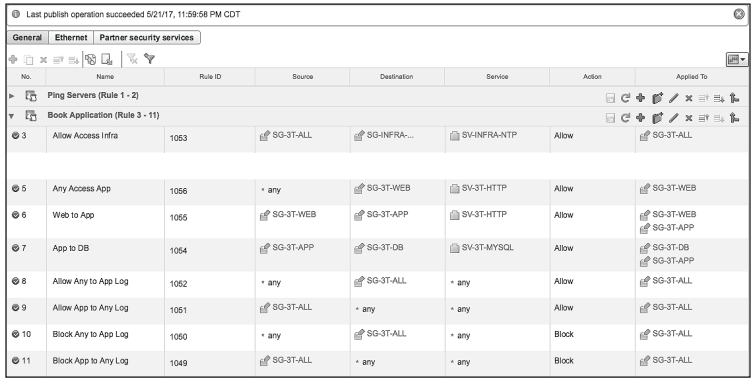


Figure 2.51 3-Tier application NSX DFW rule table

Monitor Traffic Flows

With the new rules now in place, traffic for the application should now match these more granular rules instead of the general allow rule.

Procedure

1. Log into the vRealize Log Insight appliance.
2. Click on the **VMware – NSX-vSphere** dashboard under **Content Pack Dashboards**.
3. Click on **Distributed Firewall – Rule Data**.

4. Verify **Connections by RuleID** are showing no hits on rule **1051** and **1052**.

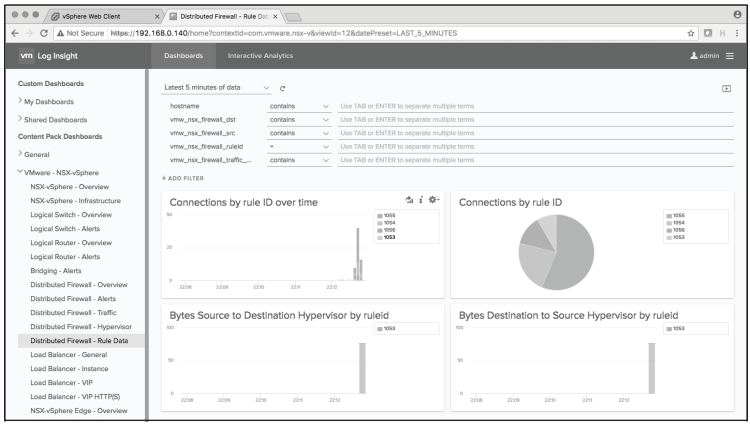


Figure 2.52 vRealize Log Insight rule data dashboard

Figure 2.53 vRealize Log Insight connections by RuleID

Figures 2.60 and 2.61 confirm Flows are no longer hitting allow rules **1051** and **1052**. The granular micro-segmentation traffic rules are working as intended; Flows are not hitting the default Allow rules. With the micro-segmentation rules in place, traffic Flows and functionality can be validated against the requirements.

Verify Shared Service/Application Functionality

Before starting the verification and functionality process, revisit the requirements for this application.

- Allow any inbound to Web01 and Web02.
- Allow Web01 and Web02 to communication with App01.
- Allow App01 to communicate with DB01.
- Allow all servers to communicate with any external services necessary to function.
- Block communications between Web01 and Web02.
- Block all other communications to any server of the application unless explicitly defined in the above requirements.

Start with verification and functionality testing of the infrastructure services rule against the requirement.

Requirements to meet

- All servers must be allowed to communicate with external services necessary for operation.

Procedure

1. Log into the vRealize Log Insight appliance.
2. Click on the **VMware – NSX-vSphere** dashboard under **Content Pack Dashboards**.
3. Click on **Distributed Firewall – Rule Data**.
4. Within the **Connections by RuleID** widget select the () to go into **Interactive Analytics**.

5. Select the **Field Table**.

6. Click on the **vmw_nsx_firewall_dst_port** of 123 and add filter **Value Is '123'**. This will only show the NTP Flows.

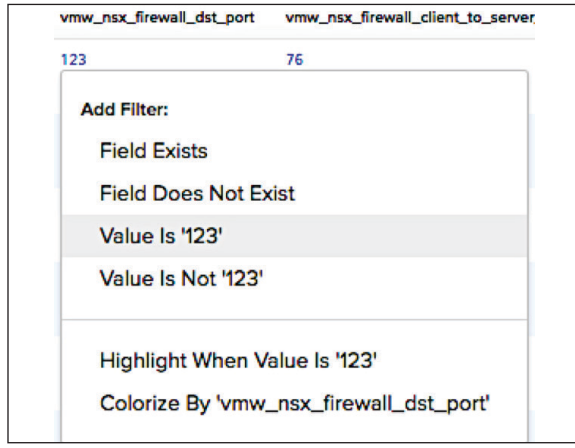


Figure 2.54 vRealize Log Insight filter field table by NTP

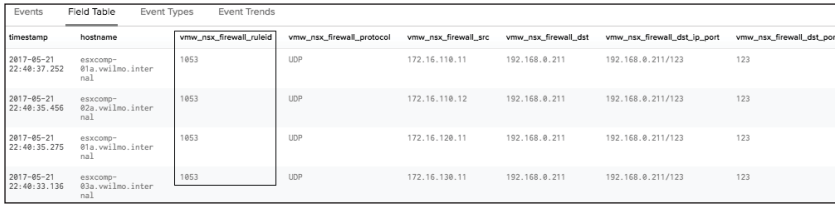


Figure 2.55 vRealize Log Insight field table – NTP

Figure 2.56 Infrastructure access NSX DFW RuleID verification

The NTP rule is now matching on RuleID **1053**. It is not being dropped, verifying that the requirement is met.

Requirements to meet

- Allow any inbound to Web01 and Web02
- Allow Web01 and Web02 to communication with App01

These requirements are the base permissions the application itself.

1. Log into the vRealize Log Insight appliance.
2. Click on the **VMware – NSX-vSphere** dashboard under **Content Pack Dashboards**.
3. Click on **Distributed Firewall – Rule Data**.
4. Within the **Connections by RuleID** widget select the ( ) to go into **Interactive Analytics**.
5. Select the **Field Table**.
6. Click on the **vmw_nsx_firewall_dst_port** of 80 and add filter **Value Is '80**. This will only show the HTTP Flows.

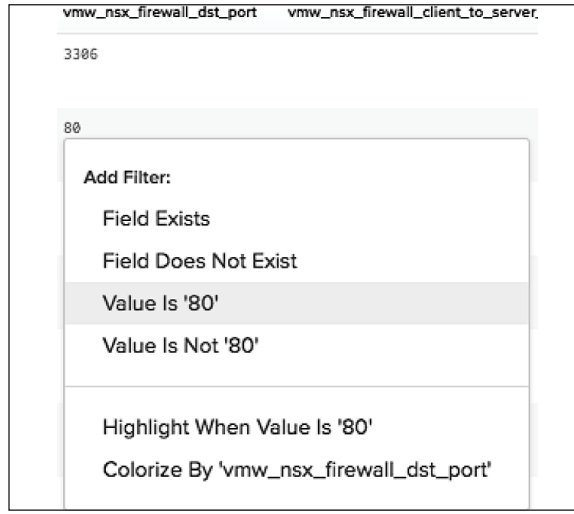
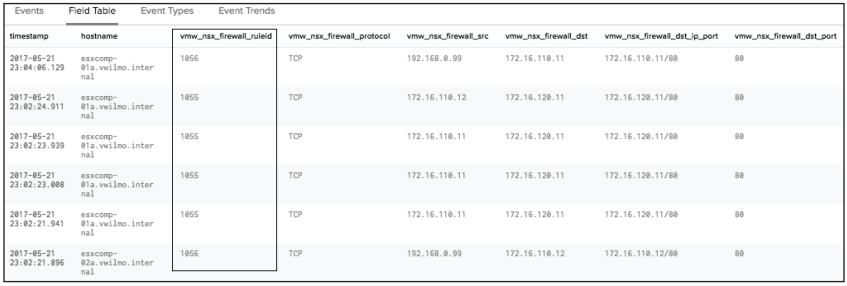


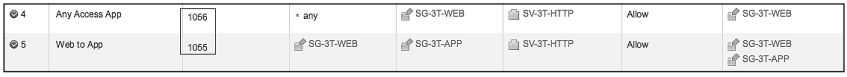
Figure 2.57 vRealize Log Insight filter field table by HTTP



Events | Field Table | Event Types | Event Trends

timestamp	hostname	vmw_nsx_firewall_ruleid	vmw_nsx_firewall_protocol	vmw_nsx_firewall_src	vmw_nsx_firewall_dst	vmw_nsx_firewall_dst_ip_port	vmw_nsx_firewall_dst_port
2017-05-21 23:04:06.129	esxcomp-01a.vwilmo.internal	1056	TCP	192.168.0.99	172.16.110.11	172.16.110.11/80	80
2017-05-21 23:02:24.911	esxcomp-01a.vwilmo.internal	1055	TCP	172.16.110.12	172.16.120.11	172.16.120.11/80	80
2017-05-21 23:02:23.939	esxcomp-01a.vwilmo.internal	1055	TCP	172.16.110.11	172.16.120.11	172.16.120.11/80	80
2017-05-21 23:02:23.008	esxcomp-01a.vwilmo.internal	1055	TCP	172.16.110.11	172.16.120.11	172.16.120.11/80	80
2017-05-21 23:02:21.941	esxcomp-01a.vwilmo.internal	1055	TCP	172.16.110.11	172.16.120.11	172.16.120.11/80	80
2017-05-21 23:02:21.896	esxcomp-02a.vwilmo.internal	1056	TCP	192.168.0.99	172.16.110.12	172.16.110.12/80	80

Figure 2.58 vRealize Log Insight filtered field table by HTTP



4	Any Access App	1056	any	SG-3T-WEB	SV-3T-HTTP	Allow	SG-3T-WEB
5	Web to App	1055	SG-3T-WEB	SG-3T-APP	SV-3T-HTTP	Allow	SG-3T-WEB SG-3T-APP

Figure 2.59 3-Tier application web access NSX DFW RuleID verification

The **Any Access App** rule to access the Book Application is now matching on RuleID **1056** and is not being dropped. The web server Flows match on RuleID 1055 and are not dropped. This verifies that the requirement is met.

Requirement to meet

- Allow App01 to communicate with DB01

Procedure

1. Log into the vRealize Log Insight appliance.
2. Click on the **VMware – NSX-vSphere** dashboard under **Content Pack Dashboards**.
3. Click on **Distributed Firewall – Rule Data**.
4. Within the **Connections by RuleID** widget select the ( ) to go into **Interactive Analytics**.
5. Select the **Field Table**.

6. Click on the **vmw_nsx_firewall_dst_port** of **3306** and add filter **Value Is '3306**. This will only show the MYSQL Flows.

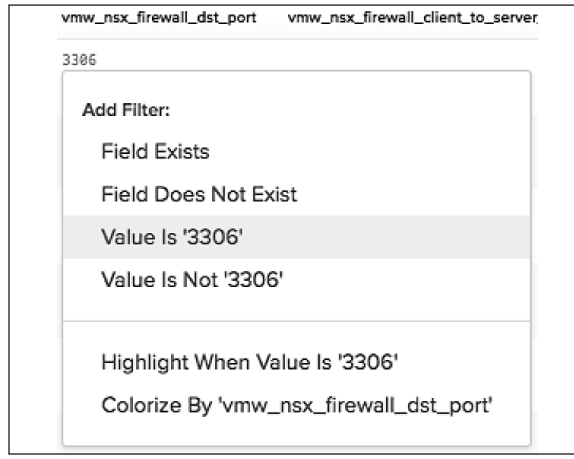


Figure 2.60 vRealize Log Insight filter field table by MySQL

Figure 2.61 vRealize Log Insight filtered field table – MySQL

Figure 2.62 3-Tier application app access DB NSX DFW RuleID verification

The **App to DB** rule now matches on RuleID **1054** and is not being dropped. This verifies that the requirement is met.

Disable/Remove Allow Rule

Before testing the block functionality and requirements, remove the allow rules from the NSX DFW for the Book Application. This is required so blocked Flows are able to reach the block rules; with an "Allow All" rule in place, that would continue override the match.

The NSX Distributed Firewall provides an easy way to disable allow rules to test whether block rules are working properly.

Procedure

1. Log into the **vSphere Web Client** and select **Networking and Security**.

2. Click on **Firewall**.

3. Expand the **Book Application Section** and click on the ( ) to disable the rule for each of the Allow Rules.

4. Click **Publish Changes to disable**.

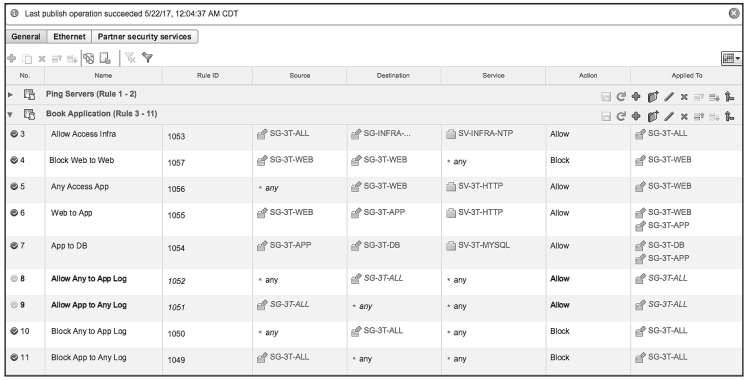


Figure 2.63 3-Tier application disable allow all NSX DFW

Requirements to meet

- Block communications between Web01 and Web02
- Block all other communications to any server of the application unless explicitly defined in the above requirements.

To verify that these blocks are working properly, attempt a connection from Web01 to Web02. Also, attempt to connect to each server via SSH.

Figure 2.64 3-Tier application web to web block – verification

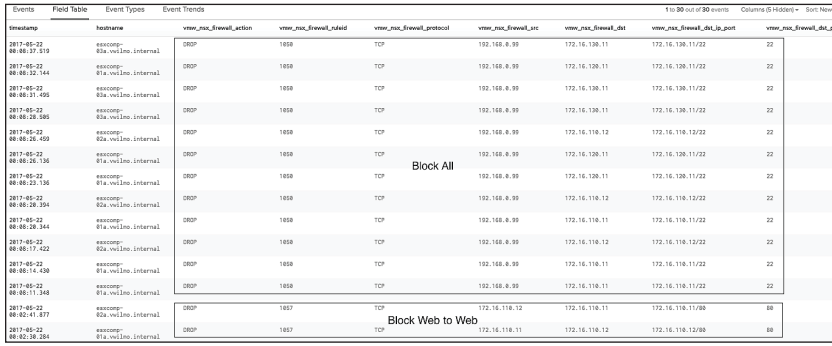


Figure 2.65 3-Tier application vRealize Log Insight field table block verification

Re-Verify Shared Service/Application Functionality

This is the last test to confirm the Book Application is functional on both web servers with the block rules in place.

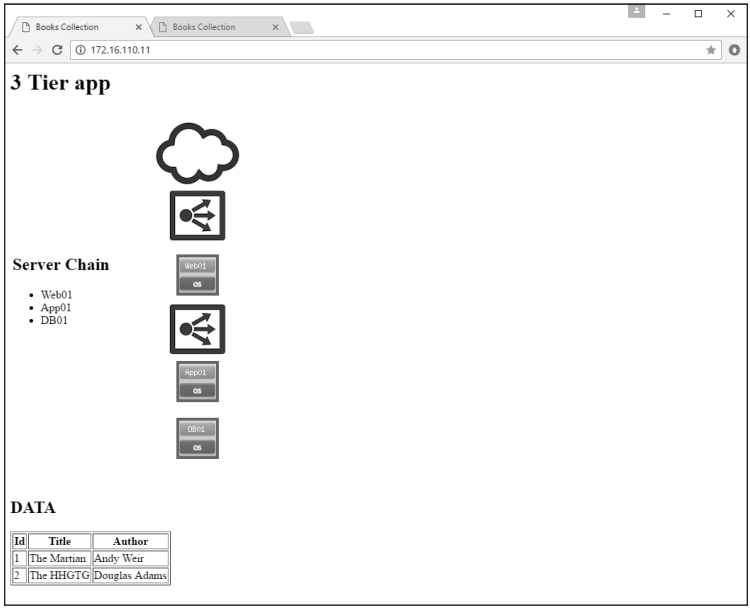


Figure 2.66 3-Tier application web 1 functional verification

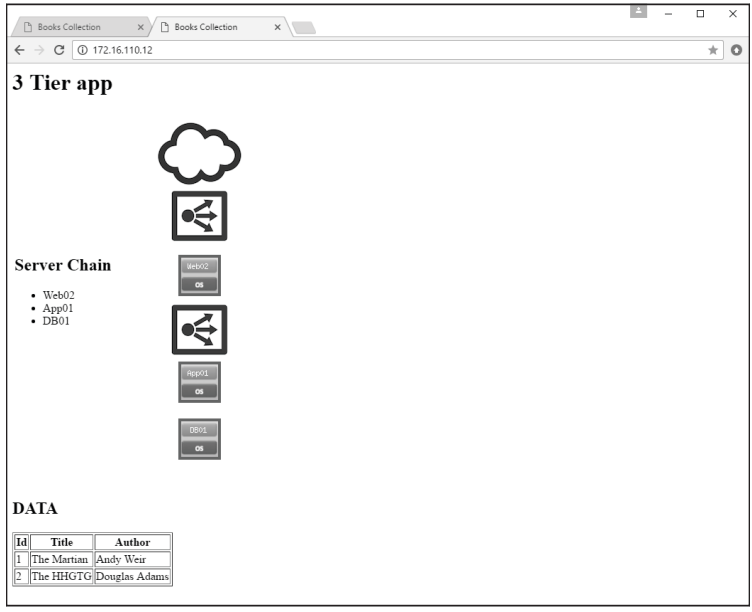


Figure 2.67 3-Tier application web 2 functional verification

This completes all of the requirements for micro-segmenting the Book Application using vRealize Log Insight. vRealize Log Insight is a great tool to use for rapid micro-segmentation of a small application. It provides significant granularity at the cost a highly manual rule creation process. The next section introduces a different tool that helps accelerate the process.

Application Rule Manager

The Application Rule Manager in VMware NSX leverages real-time flow information to discover the communication in, out, and between application workloads, enabling creation of a security model around the application. ARM can monitor up to 30 VMs in one session with up to 5 sessions running at a time. ARM can automatically correlate information that would typically require significant manual effort to review, greatly reducing time to value. ARM can also show blocked flows and identify the rules responsible. This chapter will discuss securing the same Book Application as before, this time utilizing ARM to accomplish the same result in a much faster manner.

Flow Direction

Before looking into ARM, it is important to understand the outputs of interest – specifically around flow direction.

With ARM, a flow between systems is categorized as is IN, OUT, or INTRA.

- **IN** – This type of flow represents traffic inbound to one of the VMs being monitored. This typically means the Destination VM.
- **OUT** – This type of flow represents traffic outbound from one of the monitored VMs, typically the Source VM.
- **INTRA** – This flow type represents traffic going between machines in the monitor session.

With an understanding of each flow definition, rules can be built to further restrict how two systems communicate.

Define the Application

Similar to the previous exercise, this is a 3-tier application that displays information from a database on books. It consists of two identical web servers, either of which can access the database and display information, providing resiliency to the application. The Book Application still maintains time sync with the NTP-01a (192.168.0.211) system. The Book Application is only accessed by one user – the Librarian – at this time. No other systems are allowed to communicate with the application.

The application consists of the following servers and external dependencies.

3-Tier Application

Table 3.1 Book application information

System Function	System Name	IP Address
Web Tier	Web01	172.16.110.11
Web Tier	Web02	172.16.110.12
App Tier	App01	172.16.120.11
Database Tier	DB01	172.16.130.11

Infrastructure Services

Table 3.2 Infrastructure information

System Function	System Name	IP Address
NTP	NTP-01a	192.168.0.210

Application Access

Table 3.3 Application access information

System Function	System Name	IP Address
Librarian	-	192.168.0.99

Understand the requirements

In this example, a customer has begun leveraging VMware NSX for virtual networking technology. They are creating logical networks for workload placement. The first workload targeted for migration is the Book Application. The customer has built out a 3 VXLAN-segment style topology with separation of the Book Application's web, app, and DB tiers. With the new initiative of virtualized networking, they desire to provide a least privilege security posture for the application. The customer is not familiar with the communication flows associated with the application. They are familiar with use of vRealize Log Insight for micro-segmentation but would prefer to speed up the process. The customer has also asked to restrict access to the application to one external user, the Librarian. The Librarian uses 192.168.0.99 to access the application; this address is not in the data center or secured with VMware NSX. To create a least privilege security posture, the following steps are required:

- Allow only 192.168.0.99 inbound to Web01 and Web02.
- Allow Web01 and Web02 to communication with App01.
- Allow App01 to communicate with DB01.
- Allow all servers to communicate with any external services necessary to function.
- Block communications between Web01 and Web02.
- Block all other communications to any server of the application unless explicitly defined in the above requirements.

A simple layout of the current virtualized network topology is presented in Figure 3.1.

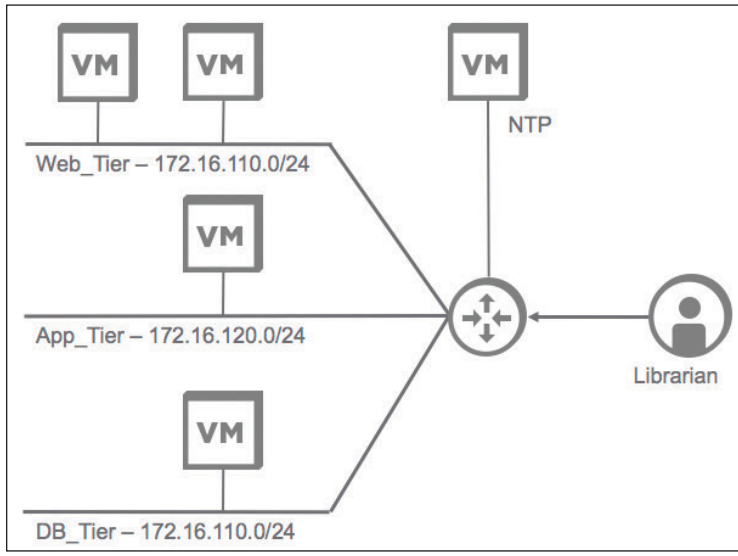


Figure 3.1 Topology logical design

Define the Methodology

With this environment, a combination of infrastructure and network methodologies can be utilized. The VMware NSX DFW can be used with either VLAN or VXLAN networks, or a combination of the two. Refer to Figure 1.4.

When complete, the layout should be similar to Table 3.4.

Table 3.4 NSX DFW rules layout

Name	Source	Destination	Service	Action	Applied To
Infrastructure Services Section					
Allow 3T-App to NTP	3T-App	NTP	-	Allow	3T-App
Book Application Section					
Allow Any Into 3T-App	192.168.0.99	Web_Tier	-	Allow	Web_Tier
Web to App	Web_Tier	App_Tier	-	Allow	Web_Tier App_Tier
App to DB	App_Tier	DB_Tier	-	Allow	App_Tier DB_Tier
Block Book Application Section					
Block Any to App Log	Any	3T-App	Any	Block	3T-App
Block App to Any Log	3T-App	Any	Any	Block	3T-App

- The top section and rule will cover the application's need to communication with infrastructure services (i.e., NTP).
- The second set of rules enables the Book Application to function. It leverages the logical network components of VMware NSX, allowing only the 192.168.0.99 machine to connect to the Book Application.
- The last two rules will block any other communications that are not defined as essential for the application to run.

These sets of rules should effectively allowlist all traffic required for the application to function.

Technologies Used

Windows Clients

Table 3.5 Windows client information

System Function	System Name	IP Address
Management Jumpbox	Jumpbox-01a	192.168.0.99

VMware Products

Table 3.6 VMware products information

Product	Version	IP Address
VMware vSphere ESXi	6.0 Patch 4	Multiple
VMware vCenter Server Appliance	6.0 Update 2a	192.168.0.111
VMware NSX Manager	6.3.0	192.168.0.120

Define Monitor Length

The Book Application still only consists of 4 servers in total. The VMware NSX Application Rule Manager can monitor a session for up to 7 days. It can also monitor the application in real time as flows come in and out of each server. This is the context for monitoring the application in the ARM section. It also is important to look at communication with external services. In this case, that service is NTP, with calls made at regular intervals.

Layout Naming Scheme

Table 3.7 Naming scheme layout

Security Groups	Systems/Logical Components Included	Services
SG-3T-ALL	Web_Tier, App_Tier, Web_Tier	-
SG-3T-ACCESS	IP-3T-ACCESS	-
SG-3T-WEB	Web_Tier	SV-3T-HTTP
SG-3T-APP	App_Tier	SV-3T-APP
SG-3T-DB	DB_Tier	SV-3T-MYSQL
SG-INFRA-ALL	SG-NTP-ALL	-
SG-NTP-ALL	NTP-01a	SV-NTP

Table 3.7 lists the basic building blocks for known information about the application. If other types of communication are discovered, investigate and determine if it is necessary communication for core application functionality.

Create Monitor Session – Infrastructure Services

The VMware NSX Application Rule Manager monitors the flows passing in and out of the vNIC of selected VMs. Run the session monitor for as long as necessary; the monitor can be stopped at any point when sufficient data has been collected and can run for up to 7 days.

To start the process, set up a session to monitor the entire Book Application and identify infrastructure-related flows.

Procedure

1. Log into the **vSphere Web Client** and select **Networking and Security**.
1. Click on **Flow Monitoring**.
2. Click on **Application Rule Manager**.
3. Click on **Start New Session**.
4. Name the Session **INFRA MONITOR**.
5. Select the servers that make up the Book Application from the list:
   - Web01
   - Web02
   - App01
   - DB01

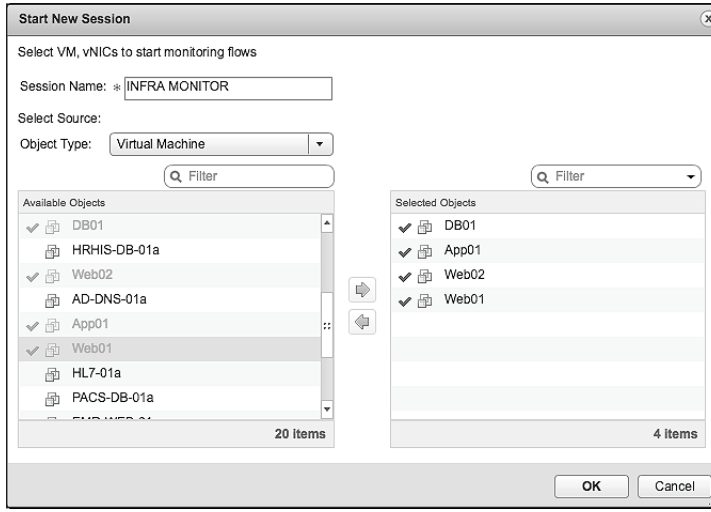


Figure 3.2 Infrastructure services create monitor session

6. Click **OK**.

This will start the monitoring process and collection of flow data from the vNICs of the virtual machines selected.

7. Click **Stop** once the appropriate amount of time has passed.

8. Click **Yes** to confirm stop.

VMware NSX Application Rule Manager will stop the collection process and display the flows it observed during the monitor session.

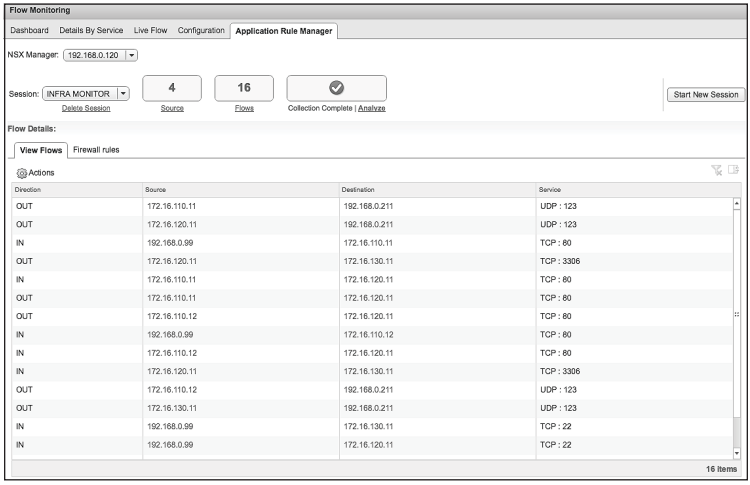


Figure 3.3 Infrastructure services processed monitor session

Analyze Monitored Session – Infrastructure Services

9. Click on **Analyze**.

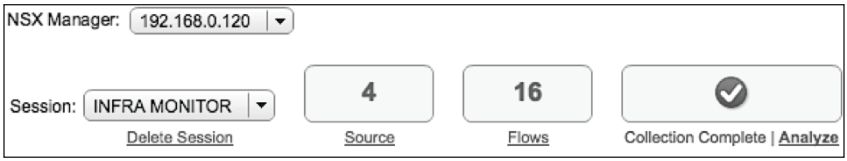


Figure 3.4 Infrastructure services analyze monitor session

This will start the analysis process for VMware NSX Application Rule Manager. ARM will attempt to match the flow information collected against VMs and VMware NSX services.

Once the analysis has finished, ARM will have matched any items or fields it could with vCenter and NSX objects.

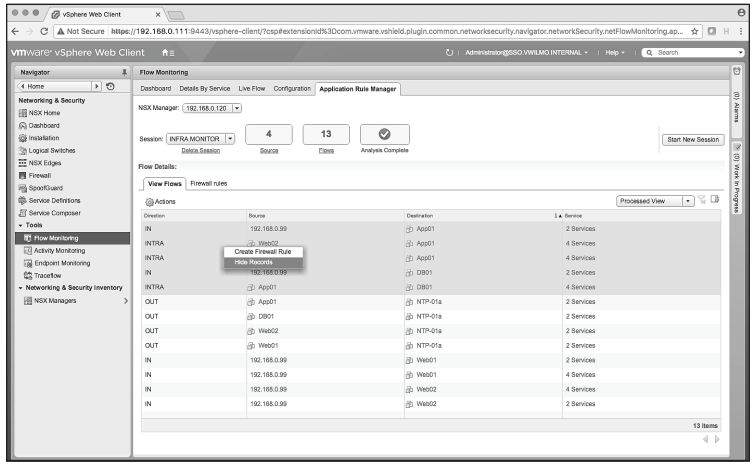


Figure 3.5 Infrastructure services monitor session analysis results

To better identify infrastructure services, sort the information by **Destination** and focus on the destination of NTP-01a. To remove uninteresting flows, highlight them and select **Hide Records**.

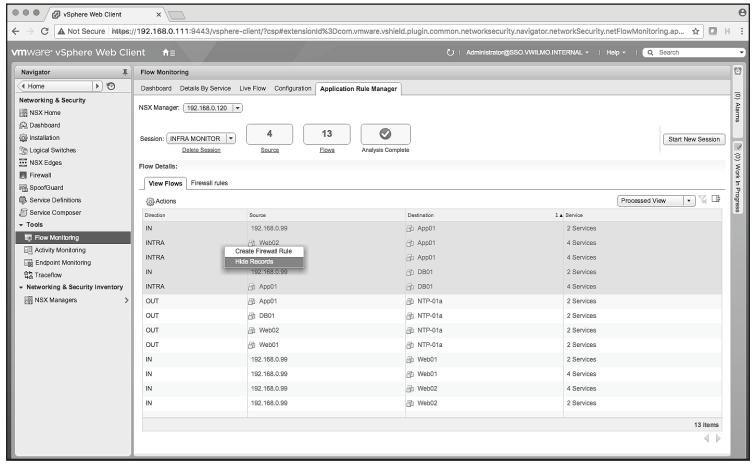


Figure 3.6 Infrastructure services monitor session clean up

Once cleaned up, the remaining data pertains only to the 4 servers and the flows talking to the NTP-01a server.

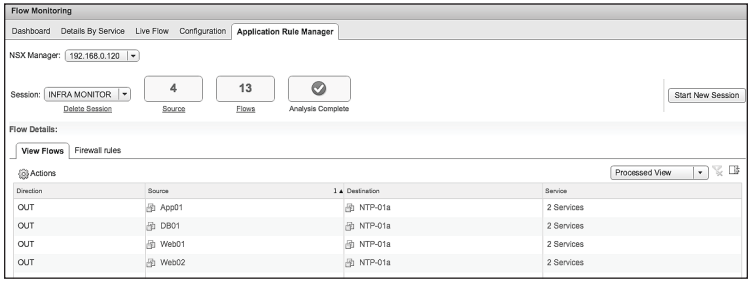


Figure 3.7 Infrastructure services monitor session clean up results

Document Rules for DFW – Infrastructure Services

Infrastructure Access Communications:

Table 3.8 Infrastructure NSX DFW rule documentation

Name	Source	Destination	Service	Action	Applied To
App Access Infra	SG-3T-ALL	SG-INFRA-NTP	SV-NTP-ALL	Allow	SG-3T-ALL

NSX Groupings:

Table 3.9 Infrastructure services NSX security group

Security Group	SG-Contains	SG-Inclusion Criteria
SG-INFRA-NTP	NTP-01a	Static

Create Security Groups – Infrastructure Services

In the monitor session for the infrastructure services, all 4 of the Book Application servers talk to NTP. Build a Security Group to put these systems into a group to align with existing infrastructure constructs.

Procedure

1. Click on one of the flows identified, and move to the ( ) icon in the **Source** field.
2. Select **Create Security Group and Replace**.
3. Type the name **SG-3T-ALL** and click **Next**.
4. Click **Next**.
5. Change the Object Type to **Logical Switch** and select:
   - Web_Tier
   - App_Tier
   - DB_Tier1

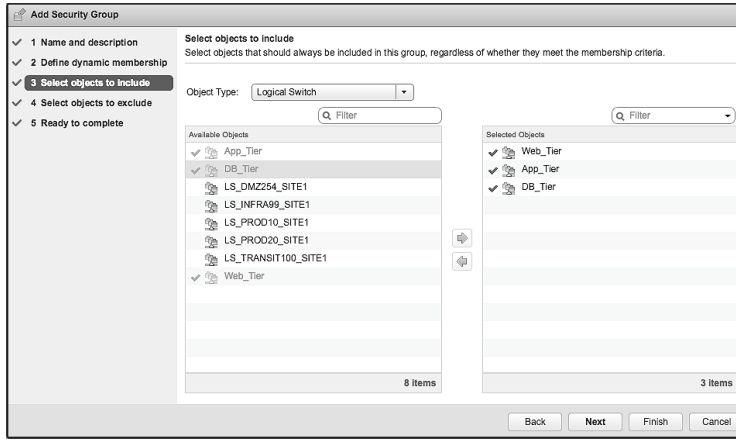


Figure 3.8 Book application all security group

6. Click **Finish**.

This will functionally add all servers with vNICs attached to those logical switches – in this case Web01, Web02, App01, and DB01.

7. Click on the ( ) icon again and select **Replace with Membership**.

8. Select the **SG-3T-ALL Security Group** and click **OK**.

9. Highlight the rest of the rules for the other 3 servers and right-click and select **Hide Records**.

This produces a **Security Group** with all the Book Application servers in it, meeting the requirement to build the infrastructure rule.

Next create a **Security Group** for the NTP-01a server.

10. Click on the flow, and move to the ( ) icon in the **Destination** field.

11. Select **Create Security Group and Replace**.

12. Type the name **SG-INFRA-NTP** and click **Next**.

13. Click **Next**.

14. Change Object Type to **Virtual Machine** and add **NTP-01a**.

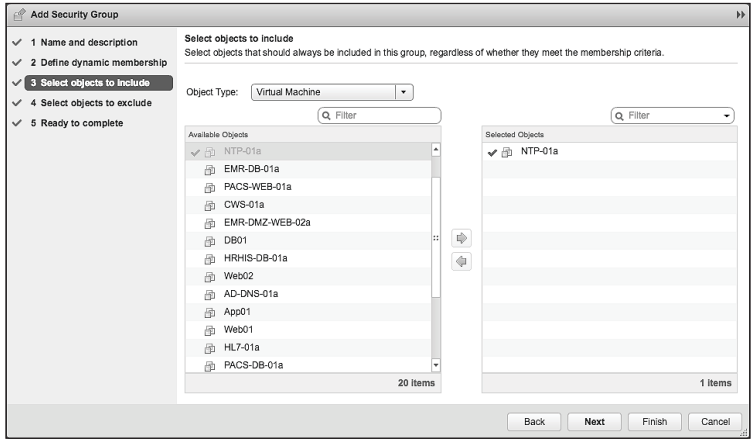


Figure 3.9 Infrastructure services create NSX security group

15. Click **Finish**.

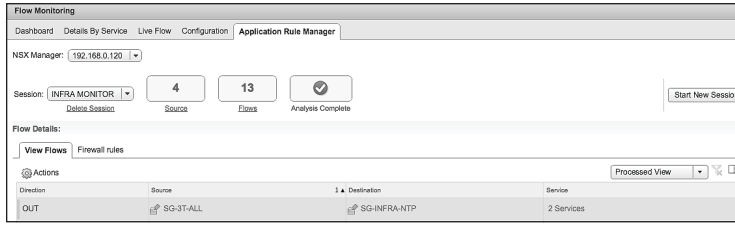


Figure 3.10 Infrastructure services NSX security group verification

Create Services – Infrastructure Services

To complete the infrastructure services section and write the NSX DFW rule, resolve the service for NTP.

Procedure

1. Click on the flow, and move to the ( ) icon in the **Service** field.
2. Select **Resolve Services**.
3. Select the **NTP** service from the list and click **OK**.

This will replace the unresolved services with the **NTP** service.

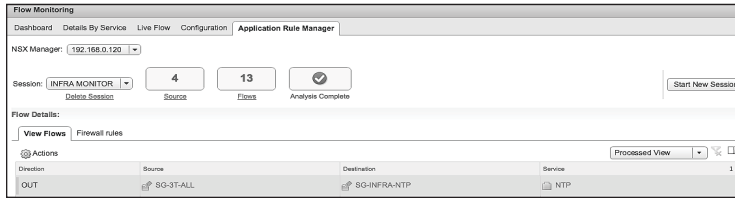


Figure 3.11 Infrastructure services resolve NTP service

Create DFW Rules – Infrastructure Services

Once all flow constructs are resolved, creation can begin on the NSX Distributed Firewall rule. Pay attention to the **Direction** column, as it will indicate in which direction to build the rule.

Procedure

1. Notice the **Direction** is **OUT**.
2. Click on the flow and right-click and select **Create Firewall Rule**.
3. Type in a Name of **Allow App to Infra**.
4. Remove the vNICs from the **Applied To** field.
5. Click on **Select** next to the **Applied To** field.
6. Change the **Object** Type to **Security Group** and filter on **3T**.
7. Add the **SG-3T-ALL Security Group** and click **OK**.
8. Change the Direction to **Out** and click **OK**.

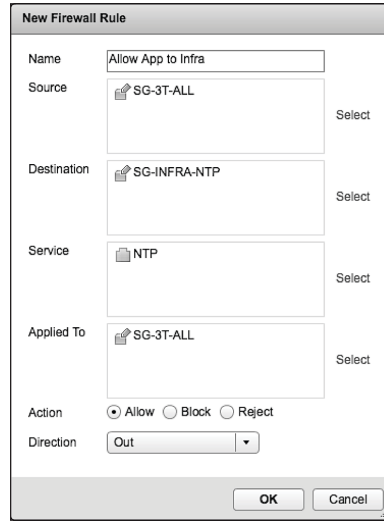


Figure 3.12 Infrastructure services create new firewall rule

Publish DFW Rules – Infrastructure Services

Procedure

1. Click on the **Firewall rules** tab.

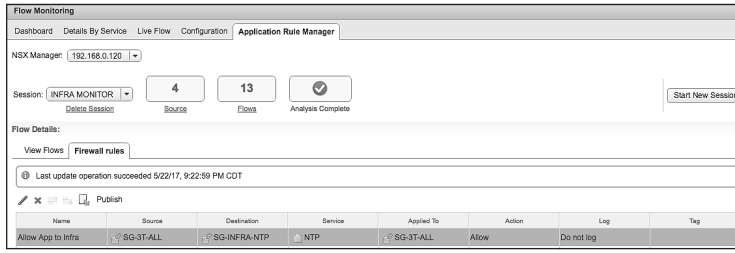


Figure 3.13 vRealize Log Insight NSX-vSphere overview

2. Verify that the rule looks accurate.
3. Click on **Publish**.
4. Type in Section name of **Infrastructure Services** and click **OK**.

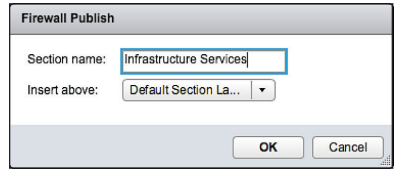


Figure 3.14 Infrastructure services create new NSX DFW section

A verification of the publish operation will show as succeeded.

5. Click on **Firewall**.
6. Expand the **Infrastructure Services** section and verify rule is in place correctly.

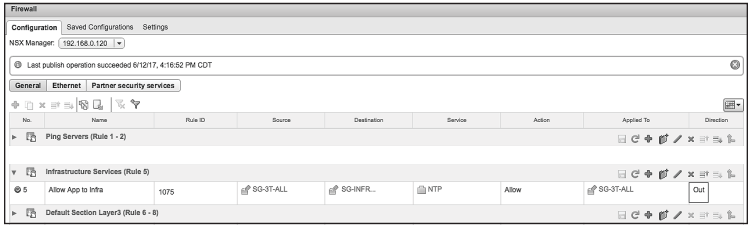


Figure 3.15 Infrastructure services NSX DFW verification

With the **Direction** column displayed, it is clear that the rule is applied to traffic coming out of the Book Application servers.

Create Monitor Session – Application

Next, write the rules for the Book Application as was done for the infrastructure services.

Procedure

1. Log into the **vSphere Web Client** and select **Networking and Security**.
2. Click on **Flow Monitoring**.
3. Click on **Application Rule Manager**.
4. Click on **Start New Session**.
5. Name the Session **APP MONITOR**.
6. Select the servers that make up the Book Application from the list:
   - Web01
   - Web02
   - App01
   - DB01

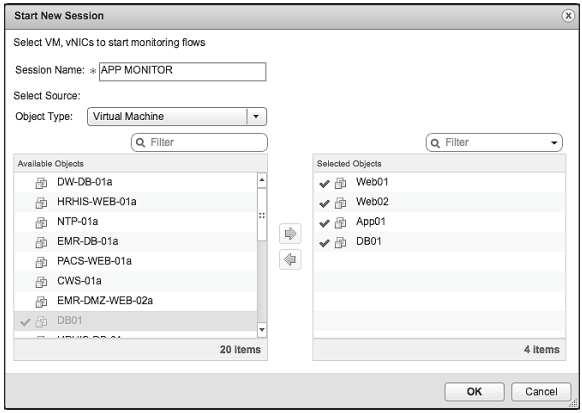


Figure 3.16 Book application create monitor session

7. Click **OK**.

This will start the monitoring process and collection of flow data from the vNICs of the selected VMs.

8. Click **Stop** once the appropriate amount of time has passed.

9. Click **Yes** to confirm stop.

VMware NSX Application Rule Manager will stop the collection process and display the flows it observed during the monitor session.

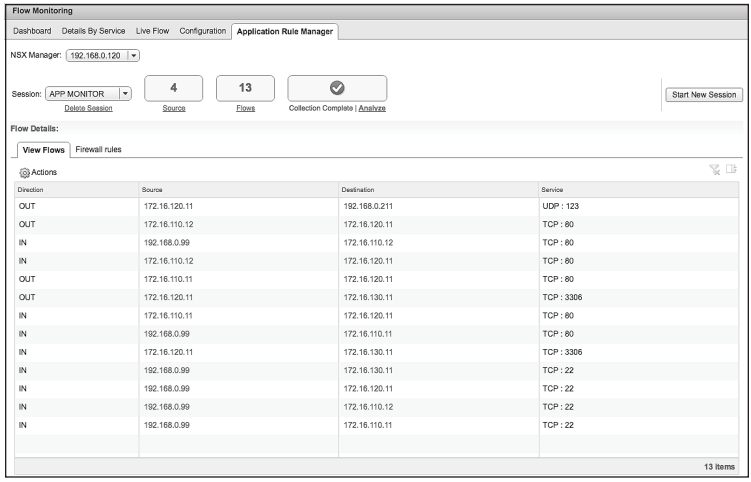


Figure 3.17 Book application processed monitor session

Analyze Monitored Session – Application

10. Click on **Analyze**.

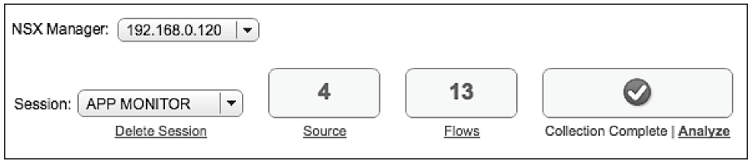


Figure 3.18 Book application analyze monitor session

This will start the analysis process for VMware NSX Application Rule Manager. ARM will attempt to match the flow information collected against virtual machines and VMware NSX services.

When the analysis has finished, ARM will have matched whatever possible with vCenter and NSX objects.

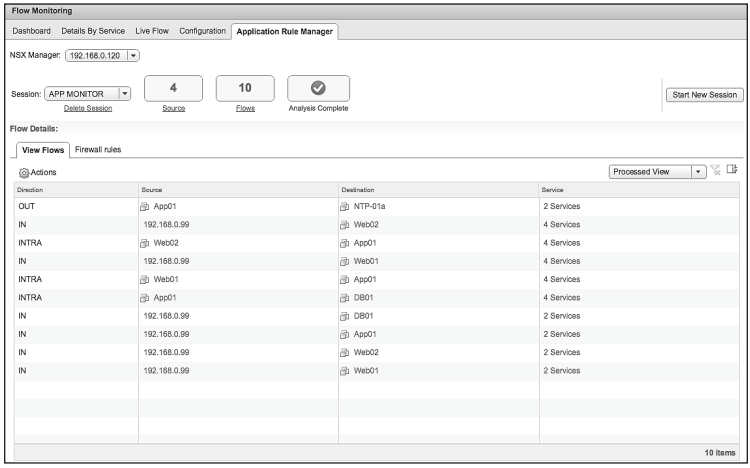


Figure 3.19 Book application monitor session analysis results

To identify the Book Application services, sort the information by **Destination**. Remove uninteresting flows such as the **Destination** of NTP-01a; they are already covered with a prior rule. As before, highlight these flows select **Hide Records**.

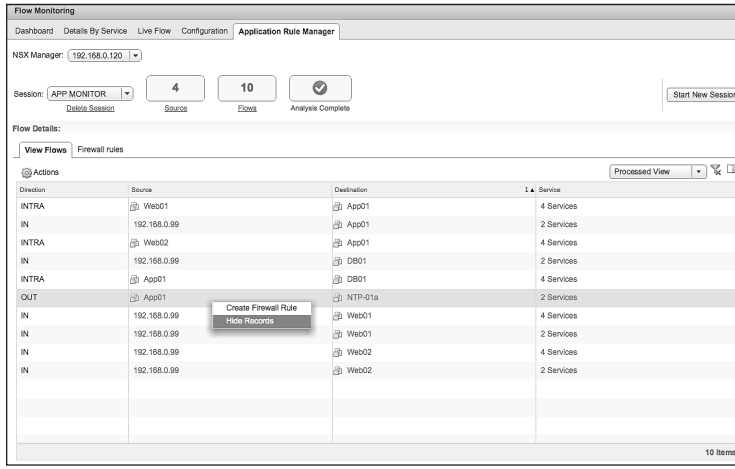


Figure 3.20 Book application monitor session clean up

Once cleaned up, several **IN** and **INTRA** flows are visible for the Book Application.

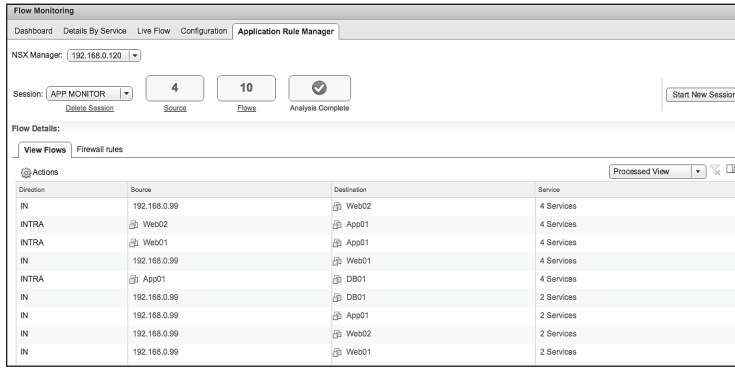


Figure 3.21 Book application monitor session clean up results

Document Rules for DFW – Application

Put the information collected from the APP MONITOR session into the table to document the necessary rules.

Table 3.10 Book application NSX DFW documentation

Book Application Acess Communications:

Name	Source	Destination	Service	Action	Applied To
Allow Librarian to Web	IP-3T-ACCESS	SG-3T-WEB	SV-3T-HTTP	Allow	SG-3T-WEB

Intra-Book Application Communications:

Name	Source	Destination	Service	Action	Applied To
Allow Web to App	SG-3T-WEB	SG-3T-APP	SV-3T-HTTP	Allow	SG-3T-WEB SG-3T-APP
Allow App to DB	SG-3T-APP	SG-3T-DB	SV-3T-MYSQL	Allow	SG-3T-APP SG-3T-DB

NSX Groupings:

Security Group	SG-Contains	SG-Inclusion Criteria
SG-3T-ALL	SG-3T-WEB SG-3T-APP SG-3T-DB	Static

IPSet	IP Address
IP-3T-ACESS	192.168.0.99

Service	Port
SV-INFRA-NTP	UDP 123
SV-3T-HTTP	TCP 80
SV-3T-MYSQL	TCP 3306

Create Security Groups – Application

Start by building the rule for access to the Book Application. Per the requirements, restrict access to the Book Application to only the Librarian's machine – IP address 192.168.0.99. There are connections from 192.168.0.99 to both Web01 and Web02. Since the 192.168.0.99 system falls outside of the VMware NSX environment, ARM was not

able to resolve the IP address to a vCenter VM; therefore, creation of an IP Set is necessary to accommodate this system. ARM will allow use of just the IP address, but use of an IP Set is recommended from a scaling perspective. Creation of an IP Set that is specifically built to facilitate access to the application allows rapid scaling by adding an IP address or CIDR block directly into the IP Set.

Procedure

1. Click on one of the flows identified for 192.168.0.99, and move to the ( ) icon in the **Source** field.

2. Select **Create IPSet and Replace**.

3. Type the name **IP-3T-ACCESS** and Click **OK**.

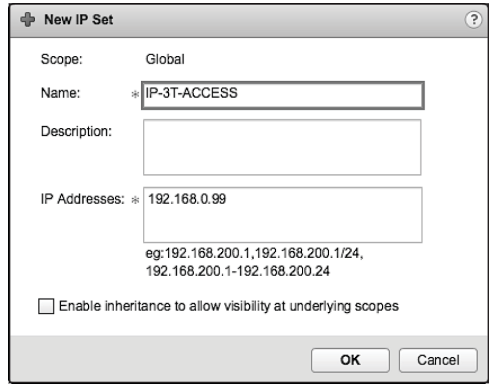


Figure 3.22 Book application create access IP set

Application Rule Manager will prompt the user if it detects multiple instances of the same IP address in the flow details. It will ask to confirm replacement all of the IP addresses with the newly created IP Set.

4. Click **Yes** to replace all.

The next step involves replacing **Source** and **Destination** VMs with Security Groups.

Procedure

1. Click on one of the flows identified for Web01 or Web02, and move to the ( ) icon in the **Source** field.

2. Select **Create Security Group and Replace**.

3. Type the name **SG-3T-WEB** and click **Next**.

4. Click **Next**.

5. Change the Object Type to **Logical Switch** and select:
   - Web_Tier

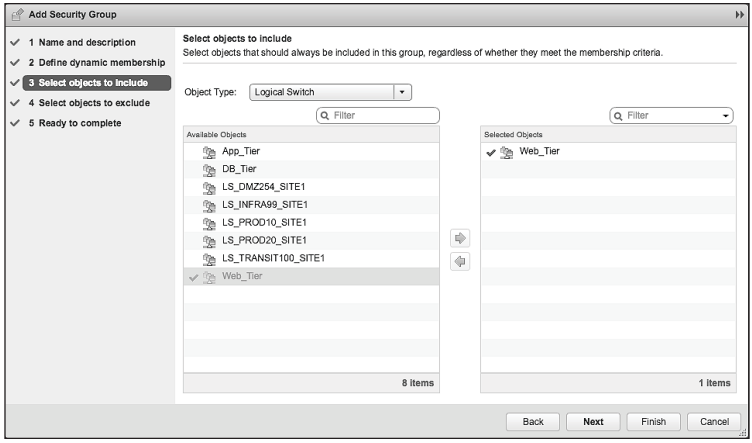


Figure 3.23 Book application create web NSX security group

6. Click **Finish**.

This will functionally add all servers with vNICs attached to that logical switch. In this case, Web01 and Web02.

7. Click on the ( ) icon again and select **Replace with Membership** for any Web01 or Web02 entries.

8. Select the **SG-3T-WEB Security Group** and Click **OK**.

9. Change the rest of the Web01 and Web02 **Source** and **Destination** VMs to the **SG-3T-WEB**.

As the **SG-3T-WEB Security Group** contains both Web01 and Web02, duplicate flows can be removed with the **Hide Records** option. This cleans up flows and reduces the number of rules required.

This leads to creation of Security Groups for App01 and DB01, which are then used to replace the VMs.

Procedure

1. Click on the flow identified for App01, and move to the ( ) icon

in the **Source** field.

2. Select **Create Security Group and Replace**.
3. Type the name SG-3T-APP and click **Next**.
4. Click **Next**.
5. Change the Object Type to **Logical Switch** and select:
   - App_Tier

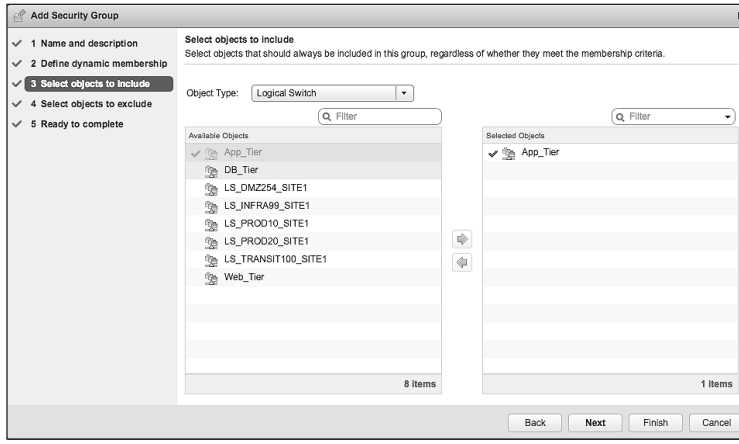


Figure 3.24 Book application create app NSX security group

6. Click **Finish**.

This will functionally add all servers with vNICs attached to that logical switch. In this case, App01.

7. Click on the ( ) icon again and select **Replace with Membership** for any App01 entries.
8. Select the **SG-3T-APP Security Group** and Click **OK**.

Finish up by exchanging the DB01 entry with its Security Group.

Procedure

1. Click on the flow identified for DB01, and move to the ( ) icon in the **Destination** field.
2. Select **Create Security Group and Replace**.

3. Type the name **SG-3T-ALL** and click **Next**.

4. Click **Next**.

5. Change the Object Type to **Logical Switch** and select:
   - DB_Tier

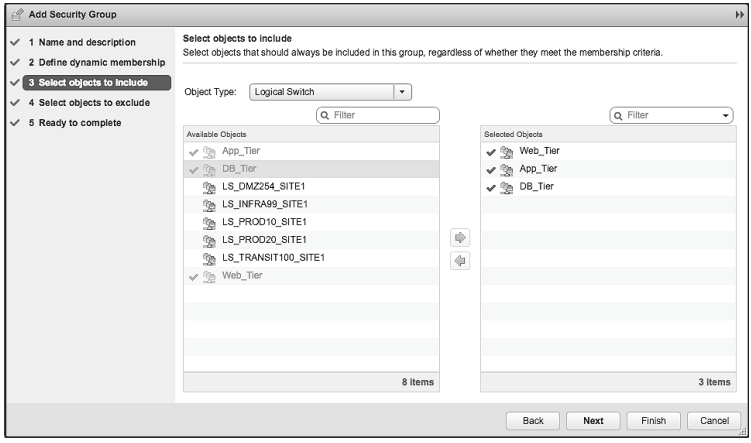


Figure 3.25 Book application create DB NSX security group

6. Click **Finish**.

This will functionally add all servers with vNICs attached to that logical switch. In this case, DB01.

7. Click on the ( ) icon again and select **Replace with Membership**.

8. Select the **SG-3T-DB Security Group** and Click **OK**.

This completes the changes and swaps for Security Groups for the new rulesets for the Book Application.

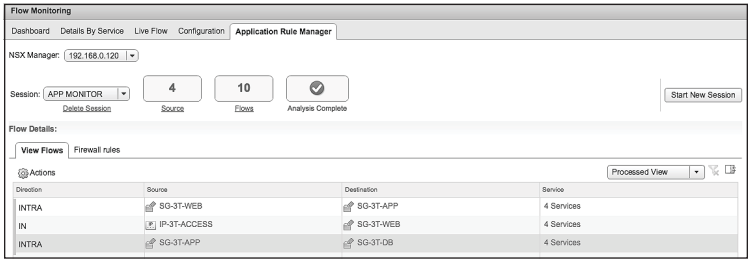


Figure 3.26 Book application security group verification

Create Services – Application

To complete the Book Application section and write the NSX DFW rules, resolve the services for each server of the Book Application. Click on the **Services** link in each flow to see the port and protocol of the communication flow. In this case:

- Web Servers are communicating with the App Server on TCP 80

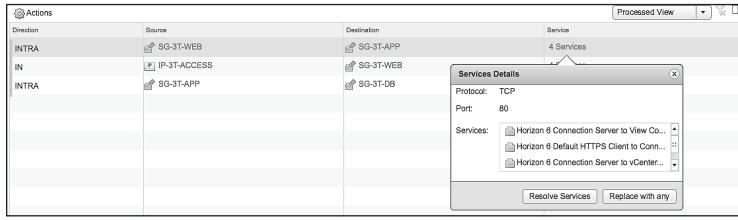


Figure 3.27 Book application resolve Web to App service

- Access to the Web Servers is communicating on TCP 80

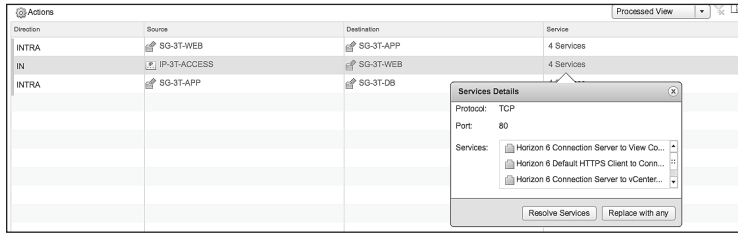


Figure 3.28 Book application resolve access to web service

- The App Server is communicating with the DB Server on TCP 3306

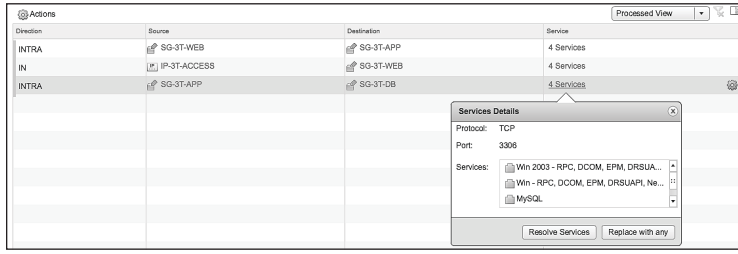


Figure 3.29 Book application resolve App to DB service

Procedure

1. Click on the first flow, and move to the ( ) icon in the **Service** field.
2. Select **Resolve Services**.
3. Select the **HTTP** service from the list and Click **OK**.

This will replace the unresolved services with the **HTTP** service.

4. Click on the second flow, and move to the ( ) icon in the **Service** field.
5. Select **Resolve Services**.
6. Select the **HTTP** service from the list and Click **OK**.

This will replace the unresolved services with the **HTTP** service.

7. Click on the last flow, and move to the ( ) icon in the **Service** field.
8. Select **Resolve Services**.
9. Select the **MySQL** service from the list and Click **OK**.

This will replace the unresolved services with the **MySQL** service.

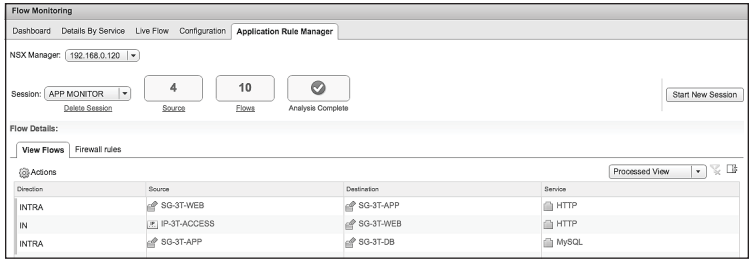


Figure 3.30 Book application services verification

Create DFW Rules – Book Application

Once all of the flow constructs are resolved, create the NSX DFW rules. Pay attention to the **Direction** column – it will indicate in which direction to build the rules.

Procedure

1. Notice the **Direction** for the first flow is **INTRA**.
2. Click on the flow and right-click and select **Create Firewall Rule**.
3. Type in a Name of **Allow Web to App**.
4. Remove the vNICs from the Applied To field.
5. Click on **Select** next to the Applied To field.
6. Change the Object Type to **Security Group** and filter on **3T**.
7. Add the **SG-3T-WEB** and **SG-3T-APP Security Groups** and Click **OK**.
8. Click **OK**.

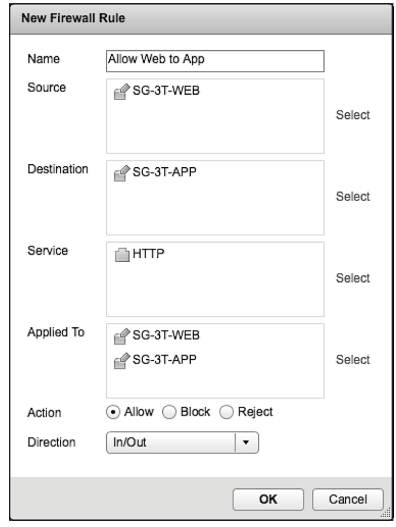


Figure 3.31 Book application create Web to App NSX DFW rule

9. Notice the **Direction** for the second flow is **IN**.
10. Click on the flow and right-click and select **Create Firewall Rule**.

11. Type in a Name of **Allow Librarian to App**.
12. Remove the vNICs from the Applied To field.
13. Click on **Select** next to the Applied To field.
14. Change the Object Type to **Security Group** and filter on **3T**.
15. Add the **SG-3T-WEB Security Group** and Click **OK**.
16. Change **Direction** to **IN**.
17. Click **OK**.

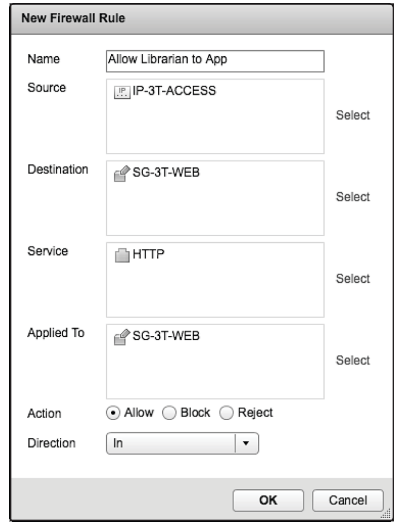


Figure 3.32 Book application create access to web NSX DFW rule

18. Notice the **Direction** for the third flow is **INTRA**.
19. Click on the flow and right-click and select **Create Firewall Rule**.
20. Type in a Name of **Allow App to DB**.
21. Remove the vNICs from the Applied To field.
22. Click on **Select** next to the Applied To field.
23. Change the Object Type to **Security Group** and filter on **3T**.
24. Add the **SG-3T-APP** and **SG-3T-DB Security Groups** and Click **OK**.
25. Click **OK**.

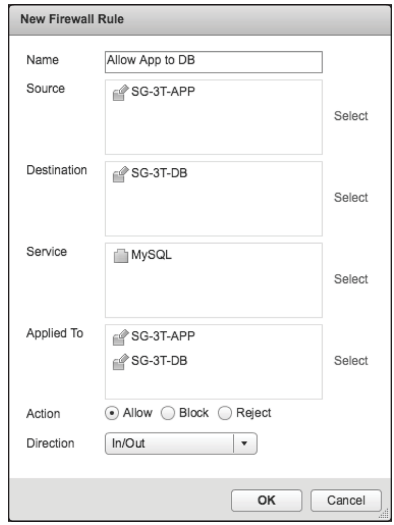


Figure 3.33 Book application create App to DB NSX DFW rule

Publish DFW Rules – Book Application

Procedure

7. Click on the **Firewall rules** tab.

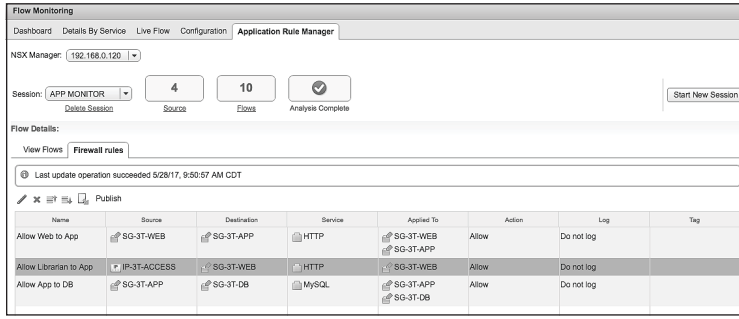


Figure 3.34 Book application publish new NSX DFW rules

8. Verify that the rule looks accurate.

9. Click on the Move Rule Up ( ) icon, and move up the **Allow Librarian to App** rule to the top.

10. Click on **Publish**.

11. Type in Section name of **Book Application** and Click **OK**.

A verification of the publish operation will show as succeeded.

12. Click on **Firewall**.

13. Expand the **Book Application** section and verify the rules are in place correctly and showing the correct Direction.

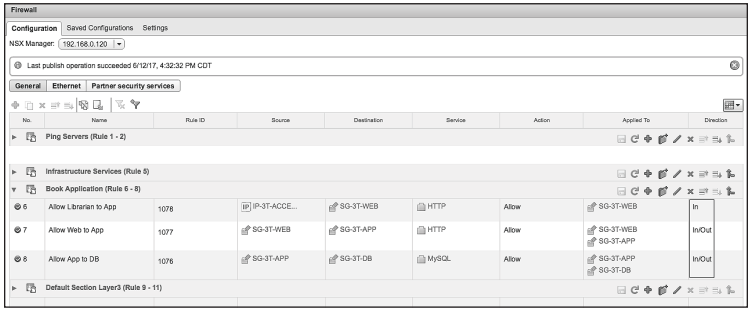


Figure 3.35 Book application NSX DFW rules verification

Build DFW Rules for Block

Add the block rules below the new rules to ensure unnecessary flows are removed per requirement.

Block All Book Application Communications:

Table 3.11 Book application block rules layout

Name	Source	Destination	Service	Action	Applied To
Block Inbound Infra	SG-3T-ALL	Any	Any	Block	SG-3T-ALL
Block Outbound Infra	Any	SG-3T-ALL	Any	Block	SG-3T-ALL

First Block Rule Configuration

1. Click on the **Add rule** (➕) icon on the **Book Application** Section two times to add the necessary rule instances.

2. Click on the **Edit** (✏) icon for the first rule **Name**.

3. Add name **Block Any to App Log** and click **Save**.

4. Click on the **Edit** ( ) icon for the first rule **Destination**.
5. Change the Object Type to **Security Group** and filter on **3T**.
6. Add the **SG-3T-ALL Security Group** and Click **OK**.
7. Click on the **Edit** ( ) icon for the first rule **Action**.
8. Change the Action to **Block**.
9. Change the **Direction** to **IN**.
10. Click on the **Log** radio button and click **Save**.

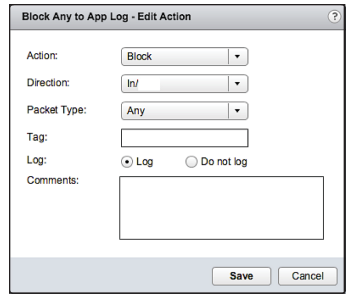


Figure 3.36 Book application block inbound rule

11. Click on the **Edit** ( ) icon for the first rule **Applied To**.
12. Uncheck the first check box.
13. Change the Object Type to **Security Group** and filter on **3T**.
14. Select the **SG-3T-ALL** and Click **OK**.

Second Block Rule Configuration

15. Click on the **Edit** ( ) icon for the second rule **Name**.
16. Add name **Block App to Any Log** and click **Save**.
17. Click on the **Edit** ( ) icon for the second rule **Source**.
18. Change the Object Type to **Security Group** and filter on **3T**.
19. Add the **SG-3T-ALL Security Group** and Click **OK**.
20. Click on the **Edit** ( ) icon for the second rule **Action**.

21. Change the Action to **Block**.

22. Click on the **Log** radio button and click **Save**.

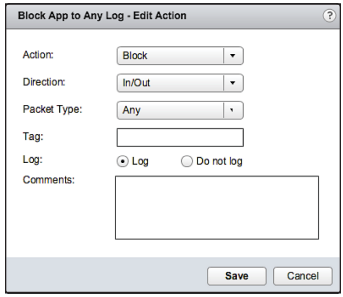


Figure 3.37 Book application block outbound rule

23. Click on the **Edit** ( ) icon for the fourth rule **Applied To**.

24. Uncheck the first check box.

25. Change the Object Type to **Security Group** and filter on **3T**.

26. Select the **SG-3T-ALL** and Click **OK**.

27. Click on the Move Rule Down ( ) icon, and move down the **Block** rules to the bottom.

Once the block configurations are completed, **Publish** the rules down to the virtual machines.

Once completed, the NSX Manager will assign a **RuleID** for each new rule created.

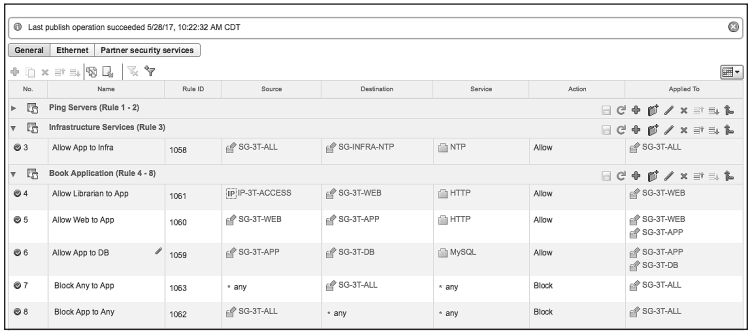


Figure 3.38 Book application block rules verification

Create Monitor Session – Infrastructure Services/Application

Once all of the NSX DFW rules are in place for the Book Application and its associated infrastructure services, create another monitoring session for all of the VMs involved. Follow that by verifying the rules are matching flows to and from the Book Application.

Procedure

1. Log into the **vSphere Web Client** and select **Networking and Security**.
2. Click on **Flow Monitoring**.
3. Click on **Application Rule Manager**.
4. Click on **Start New Session**.
5. Name the Session **VERIFY MONITOR**.
6. Select the servers that make up the Book Application from the list:
   - Web01
   - Web02
   - App01
   - DB01
   - NTP-01a
7. Click **OK**.

This will start the monitoring process and collection of flow data from the vNICs of the selected VMs.

8. Click **Stop** once the appropriate amount of time has passed.
9. Click **Yes** to confirm stop.

VMware NSX Application Rule Manager will stop the collection process and display the flows it observed during the monitor session.

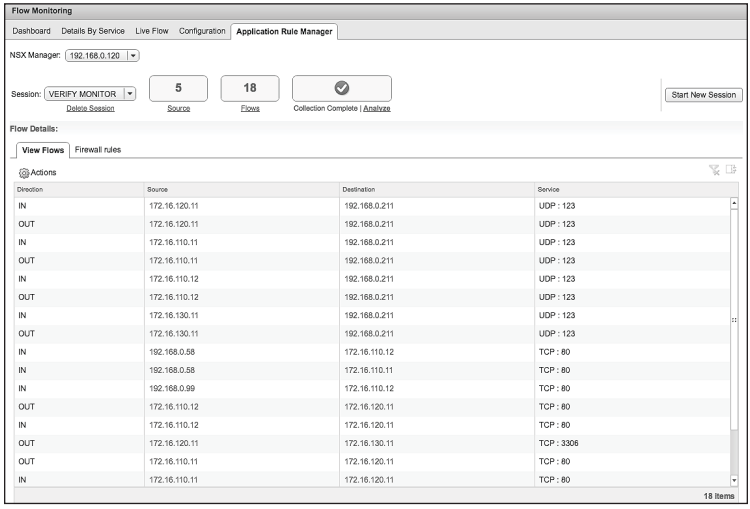


Figure 3.39 All applications monitor session verification

Analyze Monitored Session – Infrastructure Services

10. Click on **Analyze**.

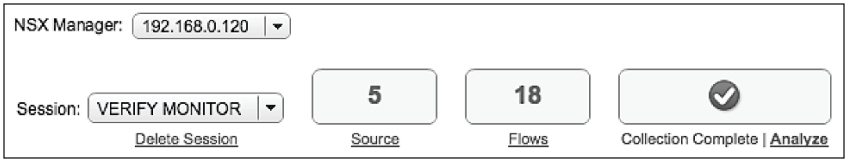


Figure 3.40 All applications analyze monitor session verification

This will start the analysis process for VMware NSX Application Rule Manager. VMware NSX Application Rule Manager will attempt to match the flow information collected against virtual machines and VMware NSX Services.

Once the analysis has finished, ARM will have matched whatever possible with vCenter and NSX objects.

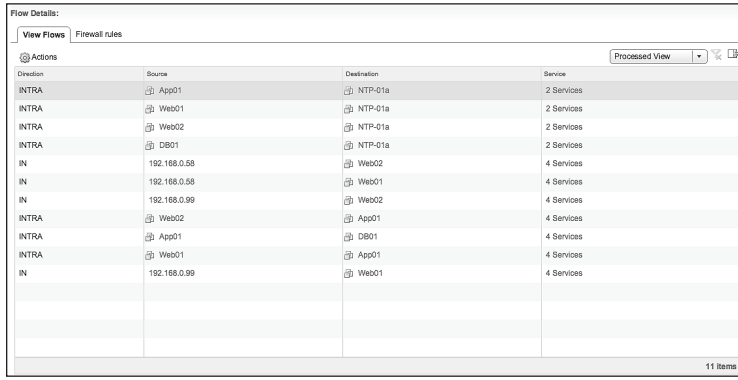


Figure 3.41 3-Tier application app destination – Web to App rule

Application Rule Manager offers a way to check which rules are being matched via a hidden column. This can be exposed through the following steps:

Procedure

1. Right-click on the title bar and select **Show/Hide Columns...**

2. Check the **RuleID** column.

This will show the RuleID number from the NSX DFW that matches each flow.

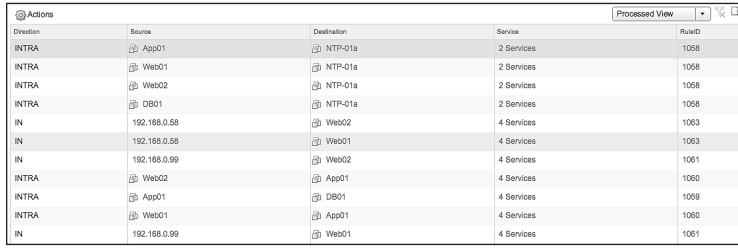


Figure 3.42 All applications monitor session RuleID verification

Verify Infrastructure Services/Application Functionality

Exposing the RuleID simplifies confirmation that rules are working. If any flows continue to reach the default 1001 rule, this indicates further work is required. Click on any RuleID link to show the associated rule from the NSX DFW.

Before starting the verification and functionality process, revisit the requirements for the application.

- Allow only 192.168.0.99 inbound to Web01 and Web02.
- Allow Web01 and Web02 to communication with App01.
- Allow App01 to communicate with DB01.
- Allow all servers to communicate with any external services necessary to function.
- Block communications between Web01 and Web02.
- Block all other communication to any server of the application unless explicitly defined in the above requirements.

Start with verification and functionality testing of the infrastructure services rule against the requirement.

Requirement to meet

- Allow all servers to communicate with any external services necessary to function.

Procedure

1. Check the flows from the table whose **Destination** is **NTP-01a**.
2. Click on the **RuleID** link to show the NSX Distributed Firewall rule, in this case **RuleID 1058**.

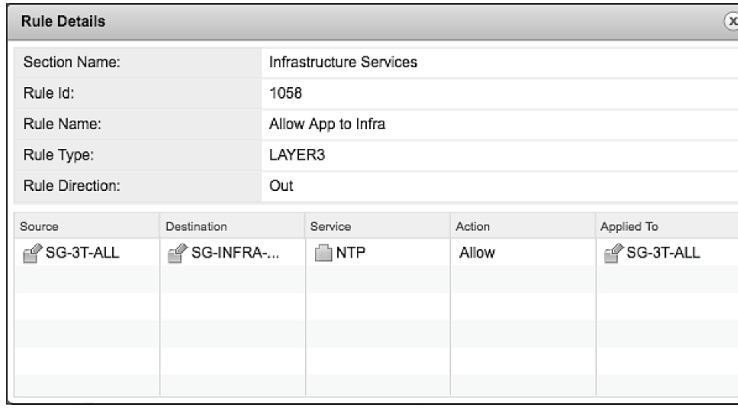


Figure 3.43 Infrastructure services monitor session RuleID details verification

The NTP rule is now matching on **RuleID 1058**; it is not being dropped. Each of the servers that comprises the Book Application has a flow to the **NTP-01a** server hitting NSX DFW **RuleID 1058**. This verifies that the requirement is met.

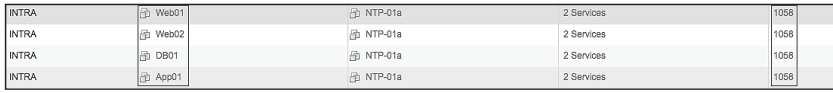


Figure 3.44 Book application monitor session access infrastructure services RuleID verification

The next set of requirements are specific to the Book Application.

- Allow only **Librarian (192.168.0.99)** inbound to **Web01** and **Web02**.
- Allow **Web01** and **Web02** to communication with **App01**.
- Allow **App01** to communicate with **DB01**.

As shown in the list of flows, there are two distinct IP addresses attempting to access servers **Web01** and **Web02**. The first requirement was to allow only **192.168.0.99** access to the **Web01** and **Web02** servers.

Figure 3.45 Book application monitor session access to web servers RuleID verification

Notice that 192.168.0.99 is hitting **RuleID 1061** and 192.168.0.58 is hitting **RuleID 1063**. **RuleID 1061** is allowing traffic from the 192.168.0.99 system access to Web01 and Web02, and **RuleID 1063** is blocking traffic from 192.168.0.58. This means the requirements are being met. ARM can show both allowed and blocked RuleIDs in a monitored session.

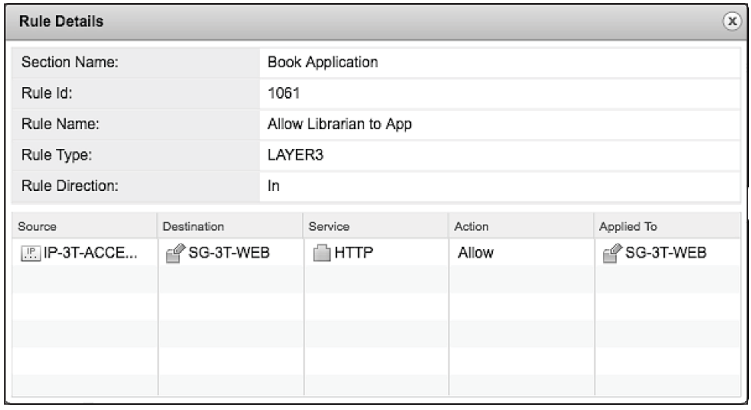


Figure 3.46 Book application monitor session accesss web servers RuleID details verification

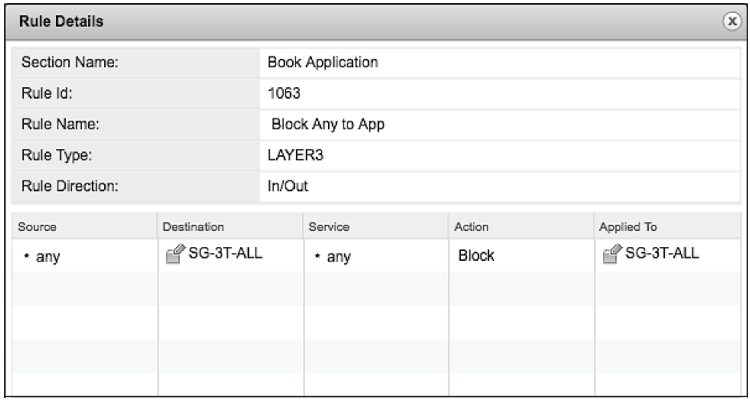


Figure 3.47 Book app monitor session block to web servers RuleID details verification

IN	192.168.0.58	Web01	Block to App	4 Services	1063
IN	192.168.0.58	Web02		4 Services	1063
IN	192.168.0.99	Web02	Allow to App	4 Services	1061
IN	192.168.0.99	Web01		4 Services	1061

Figure 3.48 Book app monitor session bock and allow to web RuleID verification

In Figure 3.48, both **Web01** and **Web02** are hitting **RuleID 1060**. This rule allows the web servers to talk to App01.

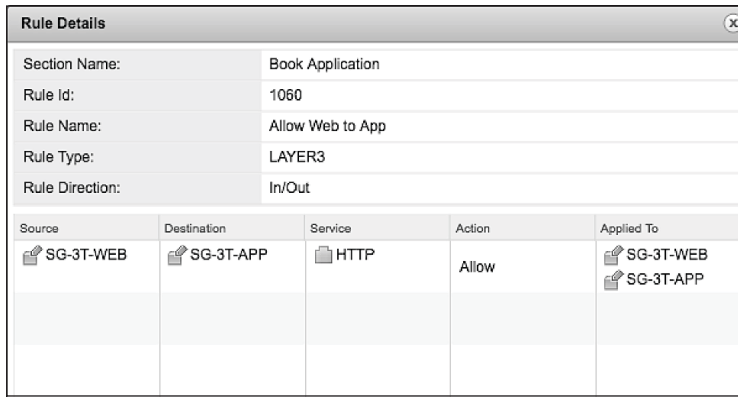


Figure 3.49 Book app monitor session allow Web/App RuleID details verification

Figure 3.50 shows that **App01** is hitting **RuleID 1059**. This rule allows **App01** to talk to **DB01**.

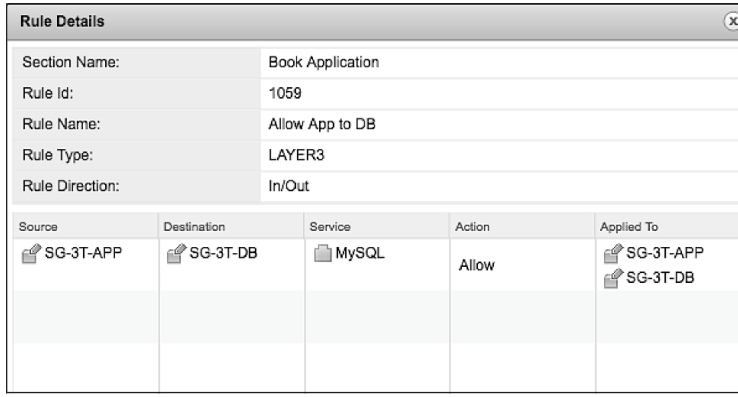


Figure 3.50 Book app monitor session allow App/DB RuleID details verification

This meets all the requirements set forth on the Book Application.

Verify Block

Finally, there are a few block requirements that must be met:

- Block communications between Web01 and Web02
- Block all other communications to any server of the application unless explicitly defined in the above requirements.

The **VERIFY MONITOR** session in Figure 3.51 shows flows from **Web01** to **Web02**, **Web02** to **Web01**, **192.168.0.58** to **Web01**, and **192.168.0.58** to **Web02**. All of these flows are hitting **RuleID 1063**. Click on the **RuleID 1063** link to see that this rule is one of the block rules.

This verifies that all of the requirements are being met.

Show Application Functional

The final verification is demonstrating the Book Application is still functional.

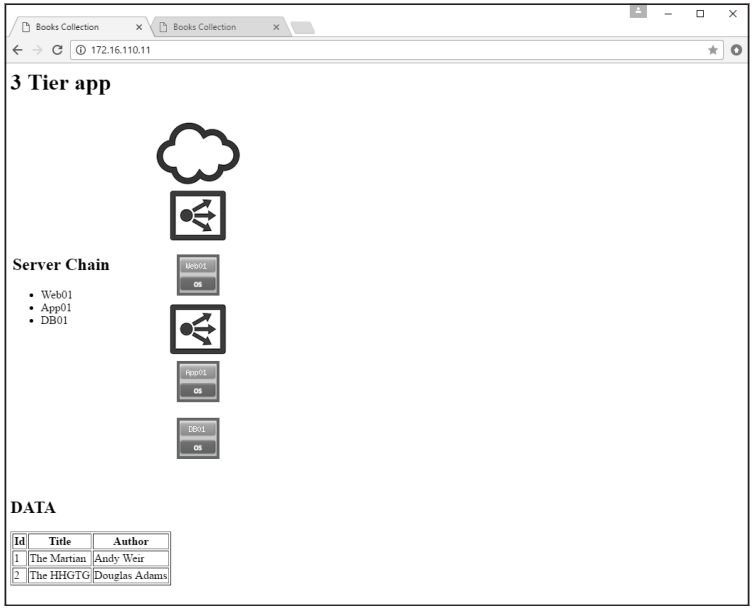


Figure 3.51 Book application web 1 functional verification

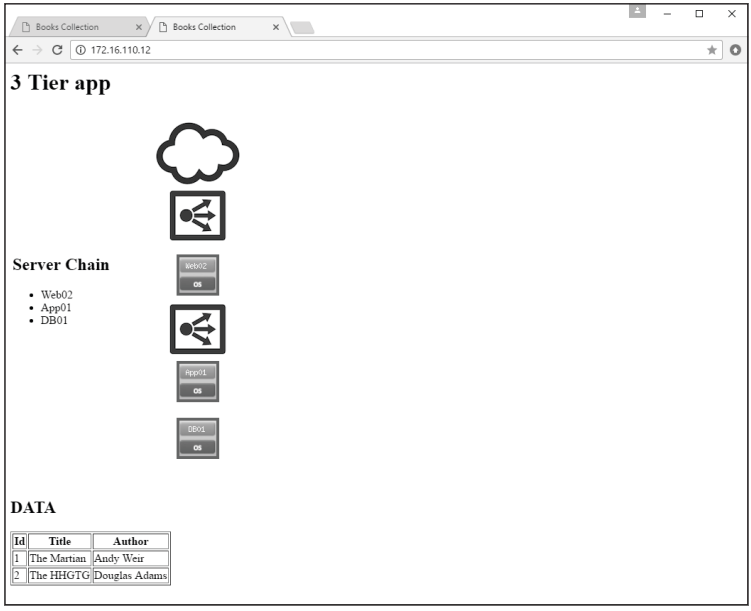


Figure 3.52 Book application web 2 functional verification

This completes all of the requirements to micro-segment the Book Application using Application Rule Manager. ARM is a great tool for speeding up the process of micro-segmentation. It reduces the volume of back-and-forth between tools to verify adherence to the NSX Distributed Firewall. This example also demonstrates adaptation of the methodology to include pre-existing infrastructure and network constructs. This highlights the versatility that ARM can bring to micro-segmentation, regardless of methodology.

Application Rule Manager simplified NSX DFW rule creation, delivering it quicker and at greater scale than vRealize Log Insight. The next chapter looks at vRealize Network Insight, which further expands solution scalability.

vRealize Network Insight

The vRealize Network Insight platform is a virtual appliance-based system that can scale to monitor tens of thousands of endpoints across a single or multiple data centers. Its clustering capabilities allow it to pull in information from multiple proxy systems, increasing its ability to scale along with an organization. The platform addresses three major use cases: micro-segmentation planning, 360o network visibility, and advanced NSX operations. For micro-segmentation planning, vRealize Network Insight provides a historical and in-depth look, at scale, of all applications and Flows within a data center. If an organization is interested in wide scale micro-segmentation covering their entire data center footprint, vRealize Network Insight is the tool for the task.

Define the Application

Similar to previous examples, this is a 3-tier application that displays information from a database on books. It consists of two identical web servers, either of which can access the database and display information, providing resiliency to the application. The Book Application maintains time sync with the NTP-01a (192.168.0.211) system.

The application consists of the following servers and external dependencies.

3-Tier Application

Table 4.1 Book application information

System Function	System Name	IP Address
Web Tier	Web01	172.16.110.11
Web Tier	Web02	172.16.110.12
App Tier	App01	172.16.120.11
Database Tier	DB01	172.16.130.11

Infrastructure Services

Table 4.2 Infrastructure services information

System Function	System Name	IP Address
NTP	NTP-01a	192.168.0.210

Application Access

Table 4.3 Application access information

System Function	System Name	IP Address
Librarian	-	192.168.0.99
Management	-	192.168.0.58

Understand the Requirements

The customer has built out a new virtual network infrastructure, leveraging VMware NSX to provide logical networks for workloads. They have moved the Book Application onto the new logical network, and have built out a 3 VXLAN-segment style topology with separation of the Book Application's web, app, and DB tiers. Where previous micro-segmentation practices leveraged infrastructure and networking constructs, this customer prefers to use VMs as they find the concepts easier to understand and maintain. The customer is not familiar with the communication Flows associated with the application and its server architecture. They are familiar with the methodologies of using vRealize Log Insight and ARM to perform micro-segmentation, but would like a tool that can scale out further. This is due to plans to onboard several hundred additional applications into the new virtual networking architecture. The customer has also asked to restrict access to the Book Application to one external user, the Librarian. The Librarian uses a desktop with the IP address 192.168.0.99 to access the application. This system is not in the data center or secured with VMware NSX. The sysadmins that maintain the infrastructure will require access to SSH to each server in the environment for maintenance purposes. They do not need access to verify the Book Application; this falls to the application team.

To create a least privilege security posture, perform the following steps:

- Allow only Librarian (192.168.0.99) inbound to Web01 and Web02.
- Allow only Management (192.168.0.58) inbound to All Servers via SSH.
- Allow Web01 and Web02 to communication with App01.
- Allow App01 to communicate with DB01.
- Allow all servers to communicate with any external services necessary to function.
- Block communications between Web01 and Web02.
- Block all other communications to any server of the application unless explicitly defined in the above requirements.

Define the Methodology

The customer has asked to move away from network and infrastructure-based methodologies, returning to an application-based model. vRealize Network Insight is a tool that will align with any of the three methodologies. vRealize Network Insight can pull information from all aspects of the network infrastructure, all the way down to the VM. With the need to block and allow specific IP addresses of machines outside of the NSX environment, there is a need to combine both networking and application-based rule methodologies. Refer to Figure 1.4.

Technologies Used

Windows Clients

Table 4.4 Windows clients information

System Function	System Name	IP Address
Librarian System	-	192.168.0.99

Mac Clients

Table 4.5 Mac client information

System Function	System Name	IP Address
Sysadmin MGMT Workstation	-	192.168.0.99

VMware Products

Table 4.6 VMware products information

Product	Version	IP Address
VMware vSphere ESXi	6.0 Patch 4	Multiple
VMware vCenter Server Appliance	6.0 Update 2a	192.168.0.111
VMware NSX Manager	6.3.0	192.168.0.120
vRealize Network Insight	3.4	192.168.0.141

Define Monitor Length

The Book Application still consists of 4 servers in total. With the VMware vRealize Network Insight, the entire infrastructure can be monitored for a period of up to 30 days. The application communicates with the external NTP service, making calls at regular intervals. It also accepts connections from the sysadmin management workstation to each server. With vRealize Network Insight, it is possible to select a specific time period to review all observed Flows.

Layout Naming Scheme

Table 4.7 Naming scheme layout

Security Groups	Systems Included	Services
SG-3T-ALL	Web01, Web02, App01, DB01	-
-	IP-3T-ACCESS	-
-	IP-3T-MGMT	SSH
SG-3T-WEB	Web01, Web02	HTTP
SG-3T-APP	App01	HTTP
SG-3T-DB	DB01	MySQL
SG-INFRA-NTP	NTP-01a	NTP

Create Security Group – Infrastructure Services

Procedure

1. Log into the **vSphere Web Client** and select **Networking and Security**.
2. Select the **NSX Managers** tab under the **Networking & Security Inventory**.
3. Select the IP address of the **NSX Manager**.
4. Select **Manage**.
5. Select **Grouping Objects**.
6. Click on the **Add new Security Group** () icon.
7. Type the name **SG-INFRA-NTP** and click **Next**.
8. Click **Next**.
9. Change Object Type to **Virtual Machine** and add **NTP-01a**.
10. Click **Finish**.

Create Security Groups – Application

Procedure

1. Log into the **vSphere Web Client** and select **Networking and Security**.
2. Select the **NSX Managers** tab under the **Networking & Security Inventory**.
3. Select the IP address of the **NSX Manager**.
4. Select **Manage**.
5. Select **Grouping Objects**.
6. Click on the **Add new Security Group** (➕) icon.
7. Type the name **SG-3T-WEB** and optional description for the **Security Group**.
8. Click **Next**.
9. Click **Next**.
10. Change Object Type to **Virtual Machine** and add Web01 and Web02.
11. Click on **Finish**.
12. Repeat this process adding the **App01** and **DB01** to the appropriate **Security Group**s.

To simplify ruleset creation, create the **SG-3T-ALL Security Group** and nest the newly created web, app, and DB Security Groups inside. This will allow addition of more servers to the application with the automated application of the same rules.

To do this, perform the same procedures as above, adding the newly created Security Groups rather than virtual machines at the Object Type.

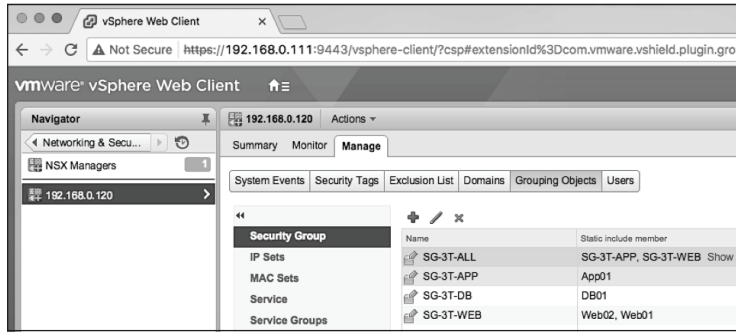


Figure 4.1 Book application all NSX security groups

After building the **Security Group** layout, use these constructs to build the block and allow rules.

Analyze Traffic Flows – Infrastructure Services

Starting with the infrastructure services, in this example the NTP-01a server, use vRealize Network Insight to show the Flows both to and from the NTP-10a server. This will help in building the NSX Distributed Firewall rulesets.

Procedure

1. Browse to the vRealize Network Insight web interface and login.

2. Select **Plan Security** from the left menu.

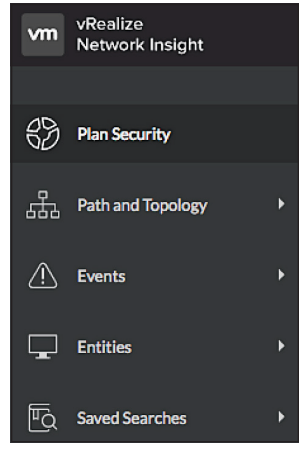


Figure 4.2 Infrastructure services plan security

3. Change the **Entity** to **Security Group**s.
4. Select the **SG-INFRA-NTP** security group from the list.
5. Leave the **Duration** at **Last 1 day**.
6. Click **Analyze**.

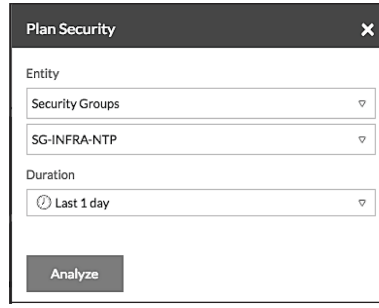


Figure 4.3 Infrastructure services select NSX security group

7. Change the **Micro-Segments** dropdown to **Other Virtual** and by **Security Group**.

This will sort the wheel wedges to show communication between members of the **SG-INFRA-NTP** Security Group and other groups.

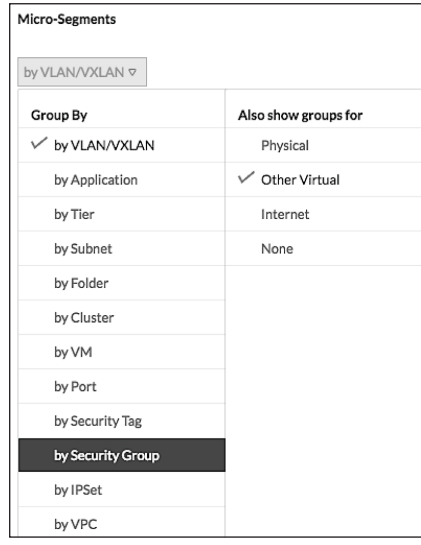


Figure 4.4 Infrastructure services filter micro-segments

8. Click on the **SG-3T-ALL** wedge.

This will highlight all the Flows from **SG-3T-ALL** to other destinations. Here there is only one Flow, from **SG-3T-ALL to SG-INFRA-NTP**. When these Security Groups were built, all the Book Application Security Groups were added to the **SG-3T-ALL** Security Group. This created an all-encompassing Security Group for the Book Application which included all the application servers.

Note the number in parenthesis in the wedge for **SG-3T-ALL**. This number represents the number of virtual machines within the Security Group, in this case **(4)**. The Book Application consists of **(4)** servers.

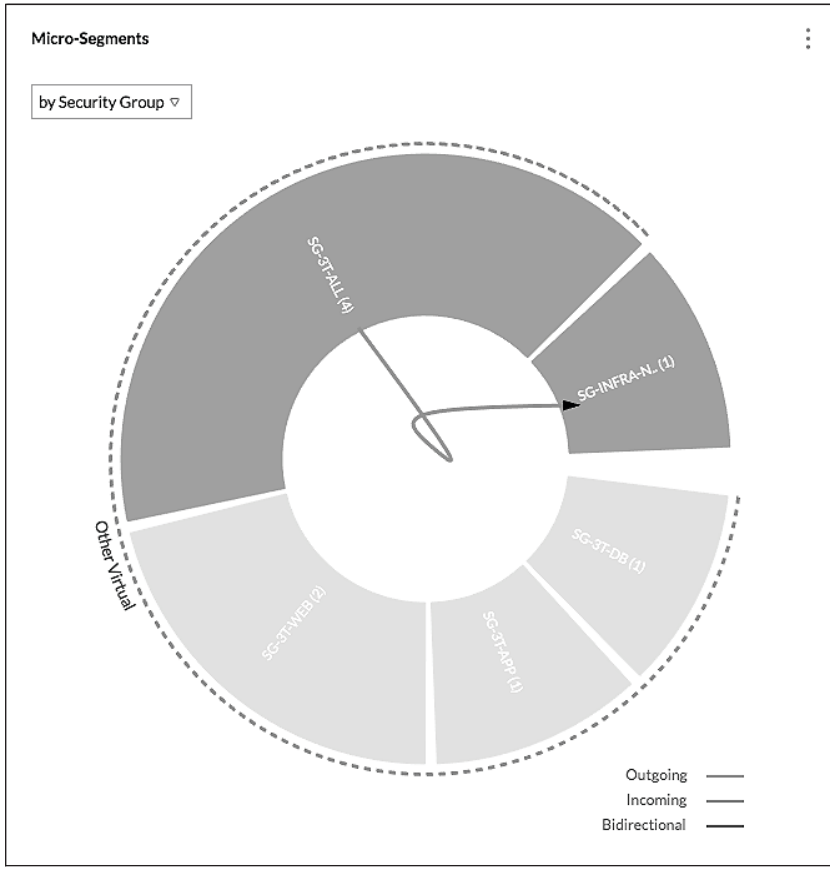


Figure 4.5 Infrastructure services micro-segment Flow results

9. Click on the **SG-3T-ALL** wedge to open the **Services and Flows for SG-3T-ALL** screen.

This screen show there are **(7)** Flows associated with **SG-3T-ALL**. Clicking on the **Flows (Incoming and Outgoing)** displays full Flow detail. Select the **Recommended Firewall Rules** tab for further examination.

10. Click on the number **(1)** below the **Recommended Firewall Rules** tab name.

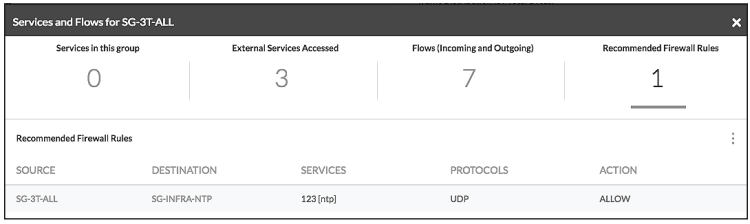


Figure 4.6 Infrastructure services recommended firewall rules

The information displayed shows rule suggestions from vRealize Network Insight based on observed data. When implemented on the NSX DFW, they will provide the desired micro-segmentation.

As with the other tool examples, this information can be logged into tables for addition to the NSX Distributed Firewall.

Table 4.8 Infrastructure services NSX DFW rules layout

Infrastructure Access Communications:

Name	Source	Destination	Service	Action	Applied To
App Access Infra	SG-3T-ALL	SG-INFRA-NTP	SV-NTP-ALL	Allow	SG-3T-ALL

NSX Groupings:

Security Group	SG-Contains	SG-Inclusion Criteria
SG-INFRA-NTP	NTP-01a	Static

Analyze traffic Flows – SG-3T-WEB

Perform a similar procedure with the web servers as was done for the NTP server.

Procedure

1. Browse to the vRealize Network Insight web interface and login.
2. Select **Plan Security** from the left menu.

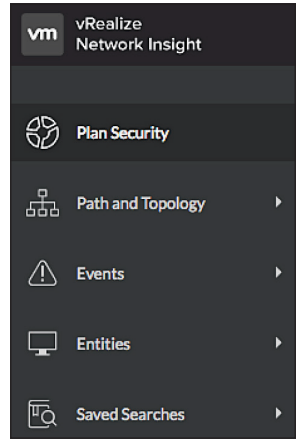


Figure 4.7 Book application web plan security

3. Change the **Entity** to **Security Group**s.
4. Select the **SG-3T-WEB** security group from the list.
5. Leave the **Duration** at **Last 1 day**.
6. Click **Analyze**.

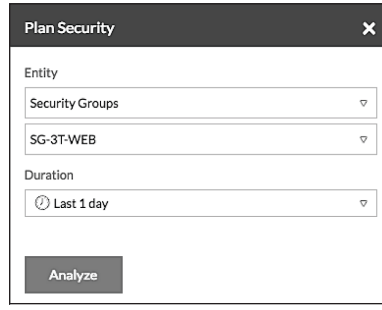


Figure 4.8 Book application select web NSX security group

7. Change the **Micro-Segments** dropdown to **Other Virtual** and **by Security Group**.

This will sort the wheel wedges to show communication between members of the **SG-3T-WEB** Security Group and other groups.

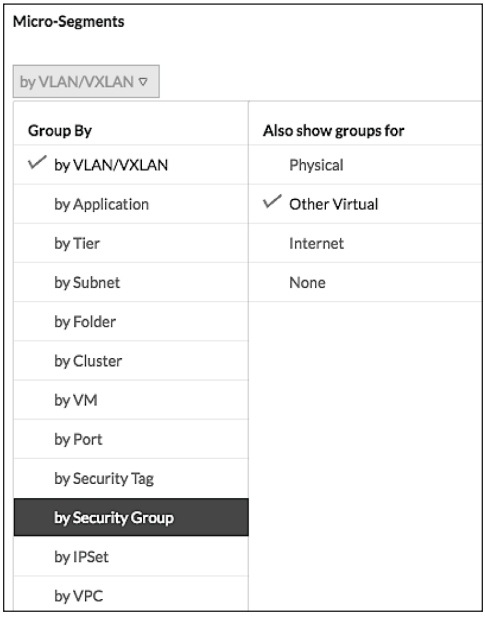


Figure 4.9 Book application web filter micro-segments

8. Click on the **SG-3T-WEB** wedge.

This will highlight all the Flows from **SG-3T-WEB** to other destinations. As before, the number in the **SG-3T-WEB** wedge represents the number of virtual machines within the Security Group. The number in this example is **(2)**, matching the **(2)** web servers in the Book Application.

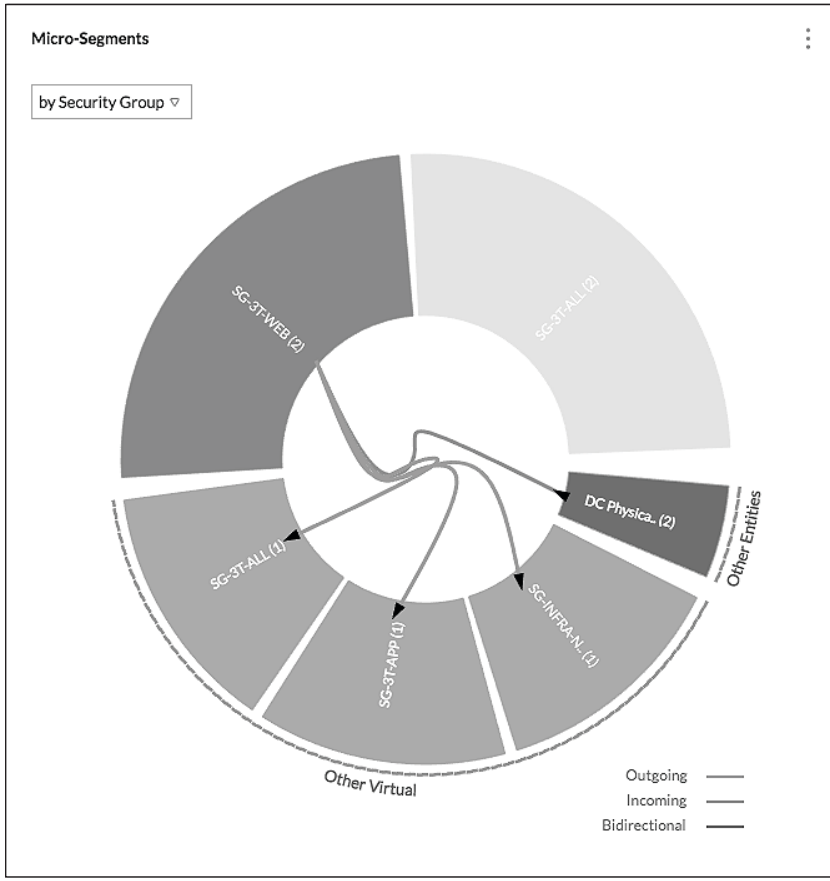


Figure 4.10 Book application web micro-segment Flow results

9. Click on the **SG-3T-WEB** wedge to open the **Services and Flows for SG-3T-WEB** screen.

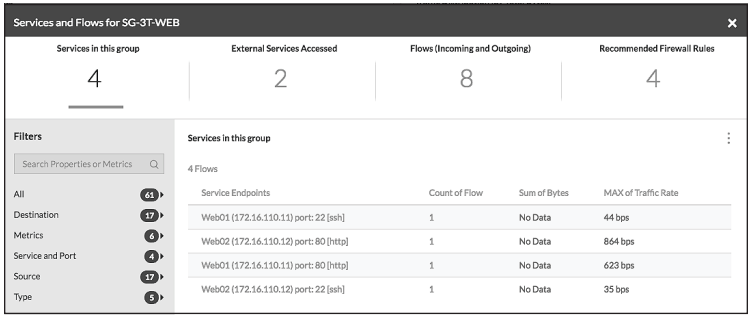


Figure 4.11 Book application web services and Flows

Figure 4.11 shows **8** Flows associated with **SG-3T-WEB**. Clicking on **Flows (Incoming and Outgoing)** displays the Flow details. Select the **Recommended Firewall Rules** tab for further examination.

10. Click on the number **4** below the **Recommended Firewall Rules** tab name.

The information displayed in Figure 4.12 shows rule suggestions from vRealize Network Insight based on observed data. When implemented on the NSX DFW, they will provide the desired micro-segmentation. This information is slightly different from previous recommendations as the **Others_DC Physical** source recommendation is also present. Further investigation of that Flow data is required to aid in rule writing. Additionally, there is a Flow from **SG-3T-WEB** to **SG-3T-ALL**, identifying communication between the web group and another group or collection of groups that exist within the **SG-3T-ALL Security Group**. Dig into the Flow details to decipher the specifics of these Flows reaching outside of the NSX/vRealize Network Insight environment.

Procedure

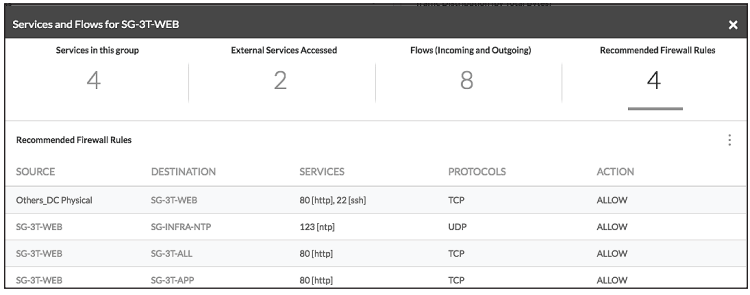


Figure 4.12 Book application web recommended firewall rules

1. Click on the number **8** under the **Flows (Incoming and Outgoing)**.

2. Click on the **Service and Port** option to the left and select **Port**. This will add the **Port** filter to the left-hand side.

3. Remove the **All** selection and check **22** for SSH. This will filter the Flows to only show port 22 traffic.

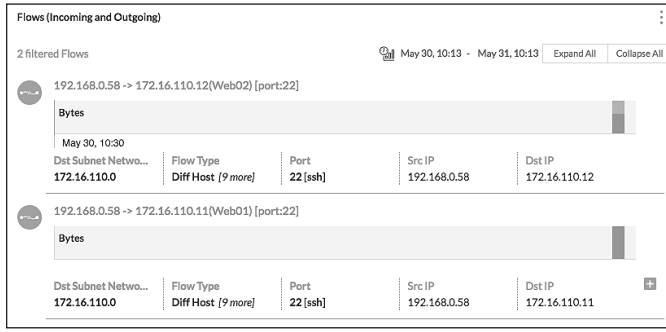


Figure 4.13 Book application web Flows incoming and outgoing SSH

Figure 4.13 shows that the IP address of **192.168.0.58** is connecting to the **Web01** and **Web02** servers over TCP port **22**. This was a requirement to allow this system access to the Book Application servers via SSH. Put this information into the table.

Table 4.9 Book application NSX DFW rules layout

Management Access Communications:

Name	Source	Destination	Service	Action	Applied To
Allow MGMT to Book Application Web	IP_MGMT_ ACCESS	SG-3T-WEB	SSH	Allow	SG-3T-WEB

IPSet	IP Address
IP-MGMT-ACCESS	192.168.0.58

Service	Port
SSH	TCP 22

Move on to the next set of Flows by port.

4. Change the **Port** number to **80** and remove **22**.

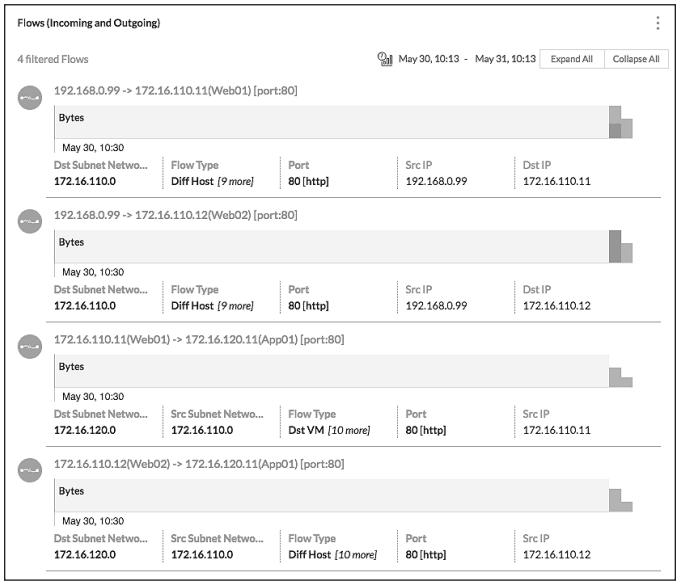


Figure 4.14 Book application web incoming and outgoing Flows HTTP

This information breaks down the Flows to the web servers. It also shows an IP address that is not defined by a virtual machine. This address, **192.168.0.99**, is the desktop that the customer has explicitly requested have access the Book Application. Put this information into the specific table.

Table 4.10 Book application web NSX DFW rules layout

Book Application Access Communications:

Name	Source	Destination	Service	Action	Applied To
Allow Librarian to Web	IP-3T-ACCESS	SG-3T-WEB	SV-3T-HTTP	Allow	SG-3T-WEB

Intra-Book Application Communications:

Name	Source	Destination	Service	Action	Applied To
Allow Web to App	SG-3T-WEB	SG-3T-APP	SV-3T-HTTP	Allow	SG-3T-WEB SG-3T-APP

NSX Groupings:

Security Group	SG-Contains	SG-Inclusion Criteria
SG-3T-WEB	Web01 Web02	Static
SG-3T-APP	App01	Static

IPSet	IP Address
IP-3T-ACCESS	192.168.0.99

Service	Port
SV-3T-HTTP	TCP 80

Analyze traffic Flows – SG-3T-APP

Perform a similar procedure as with **SG-3T-WEB** for **SG-3T-APP**.

Procedure

1. Browse to the vRealize Network Insight web interface and login.
2. Select **Plan Security** from the left menu.

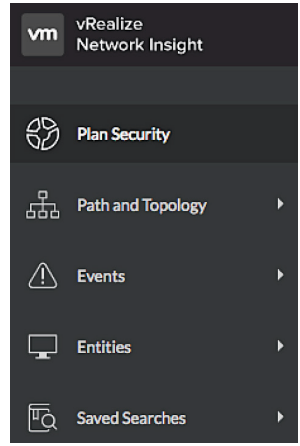


Figure 4.15 Book application app plan security

3. Change the **Entity** to **Security Group**s.
4. Select the **SG-3T-APP** security group from the list.
5. Leave the **Duration** at **Last 1 day**.
6. Click **Analyze**.

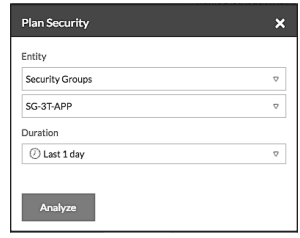


Figure 4.16 Book application app NSX security group

7. Change the **Micro-Segments** dropdown **to Other Virtual** and **by Security Group**.

This will sort the wheel wedges to show communication between members of the **SG-3T-APP** Security Group and other Security Groups.

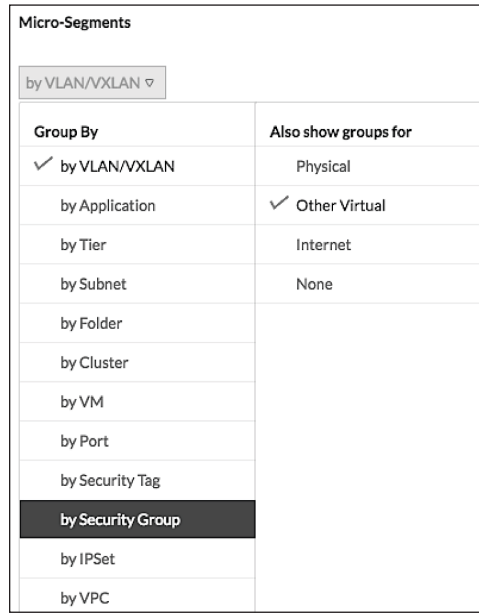


Figure 4.17 Book application app filter micro-segments

8. Click on the **SG-3T-APP** wedge.

This will highlight all the Flows from **SG-3T-APP** to other destinations. The number 1 in parenthesis in the **SG-3T-APP** wedge matches the single app server of the Book Application.

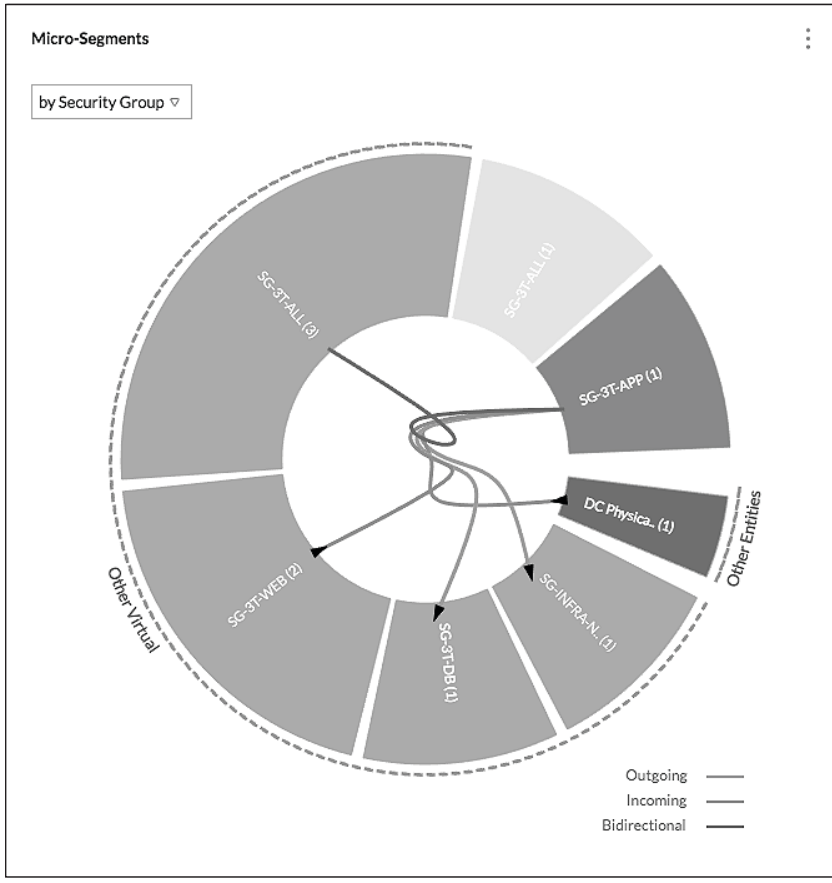


Figure 4.18 Book application app micro-segment Flow results

9. Click on the **SG-3T-APP** wedge to open the **Services and Flows for SG-3T-APP** screen.

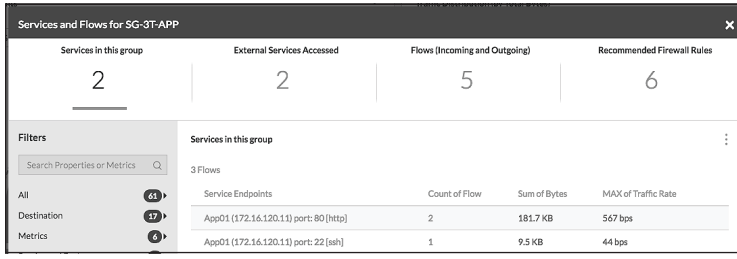


Figure 4.19 Book application app incoming and outgoing Flows

This screen shows **5** associated with **SG-3T-APP**. Click on **Flows (Incoming and Outgoing)** to see Flow details. This example specifically looks to vRealize Network Insight for rule creation suggestions. Select the **Recommended Firewall Rules** tab for further review.

10. Click on the number **6** below the **Recommended Firewall Rules** tab name.

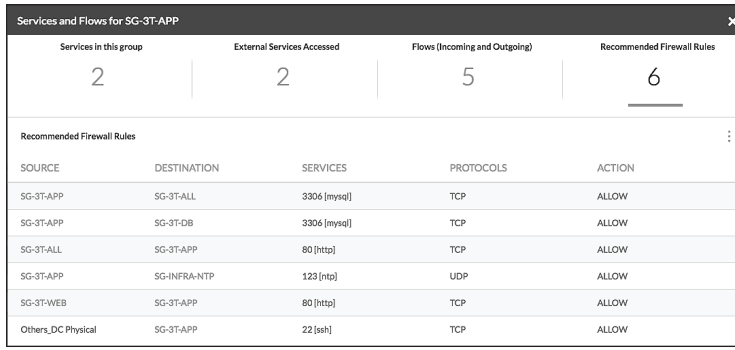


Figure 4.20 Book application app recommended firewall rules

The information displayed shows rule suggestions from vRealize Network Insight based on observed data. When implemented on the NSX DFW, they will provide the desired micro-segmentation. This information is similar to the web servers; it also shows Flows from the **Others_DC Physical** set of sources. These Flows are over TCP port 22 (i.e., SSH). Add the **SG-3T-APP Security Group** to the existing set of documented rules. Additionally, this shows Flows from **SG-3T-APP** to **SG-3T-ALL**, identifying communication between the app group and another group or collection of groups that exist within the **SG-3T-ALL Security Group**. Dig into the Flow details to decipher the specifics of these Flows reaching outside of the NSX/vRealize Network Insight environment.

Procedure

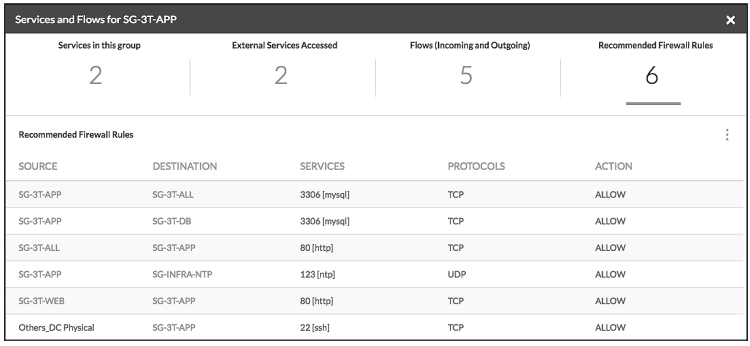


Figure 4.21 Book application app others_DC_physical Flows

1. Click on the number **5** under the **Flows (Incoming and Outgoing)**.

2. Click on the **Service and Port** option to the left and select **Port**. This will add the **Port** filter to the left-hand side.

3. Remove the **All** selection and check **22** for SSH. This will filter the Flows to only show port 22 traffic.

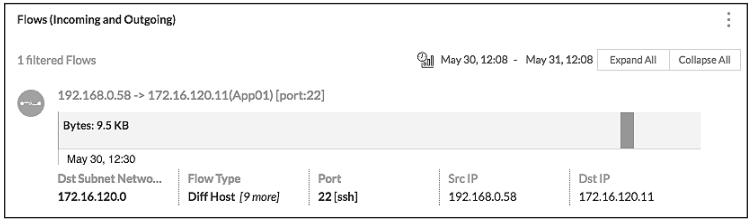


Figure 4.22 Book application app incoming Flows SSH

The IP address **192.168.0.58** is connecting to the **App01** server over TCP port **22**. This was a requirement to allow this system access to the Book Application servers via SSH. Add this information it into the table.

Table 4.11 Book application management NSX DFW rules layout

Management Access Communications:

Name	Source	Destination	Service	Action	Applied To
Allow MGMT to Book Application Web	IP_MGMT_ ACCESS	SG-3T-WEB SG-3T-APP	SSH	Allow	SG-3T-WEB SG-3T-APP

IPSet	IP Address
IP-MGMT-ACCESS	192.168.0.58

Service	Port
SSH	TCP 22

Move on to the next set of Flows by port.

4. Change the **Port** number to **80** and remove **22**.

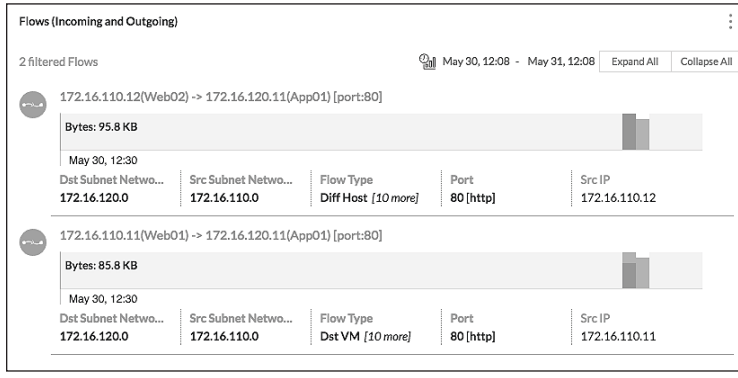


Figure 4.23 Book application Web to App outgoing Flows HTTP

These Flows verify that the **Web01** and **Web02** servers are connecting to **App01** over TCP **80**.

5. Change the **Port** number to 3306 and remove 80.

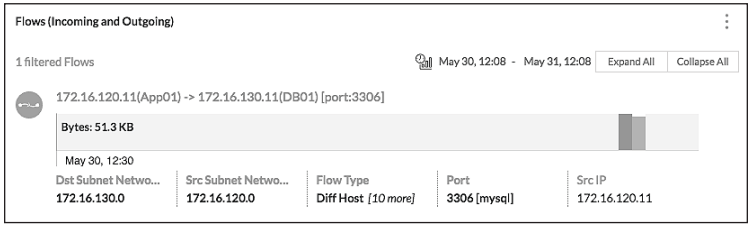


Figure 4.24 Book application App to DB outgoing Flow MySQL

Figure 4.24 confirms that **App01** is communicating with **DB01** over port TCP 3306.

Add this information and into the appropriate table.

Table 4.12 Book application app NSX DFW rules layout

Book Application Access Communications:

Name	Source	Destination	Service	Action	Applied To
Allow Librarian to Web	IP-3T-ACCESS	SG-3T-WEB	HTTP	Allow	SG-3T-WEB

Intra-Book Application Communications:

Name	Source	Destination	Service	Action	Applied To
Allow Web to App	SG-3T-WEB	SG-3T-APP	HTTP	Allow	SG-3T-WEB SG-3T-APP
Allow App to DB	SG-3T-APP	SG-3T-DB	MySQL	Allow	SG-3T-APP SG-3T-DB

NSX Groupings:

Security Group	SG-Contains	SG-Inclusion Criteria
SG-3T-WEB	Web01 Web02	Static
SG-3T-APP	App01	Static

IPSet	IP Address
IP-3T-ACCESS	192.168.0.99

Service	Port
HTTP	TCP 80
MySQL	TCP 3306

Analyze traffic Flows – SG-3T-DB

Perform a similar procedure as with the **SG-3T-WEB** and **SG-3T-APP** for **SG-3T-DB**.

Procedure

1. Browse to the vRealize Network Insight web interface and login.
2. Select **Plan Security** from the left menu.

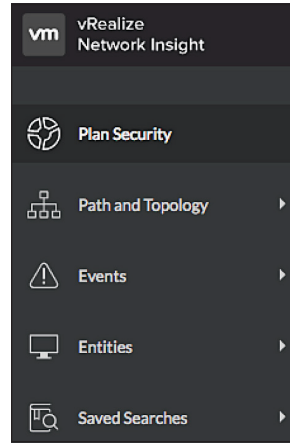


Figure 4.25 Book application DB plan security

3. Change the **Entity** to **Security Group**s.
4. Select the **SG-3T-DB** security group from the list.
5. Leave the **Duration** at **Last 1 day**.
6. Click **Analyze**.

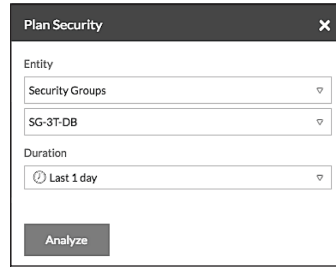


Figure 4.26 Book application DB NSX security group

7. Change the **Micro-Segments** dropdown to **Other Virtual** and by **Security Group**.

This will sort the wheel wedges to show communication between members of the **SG-3T-DB** Security Group and other security groups.

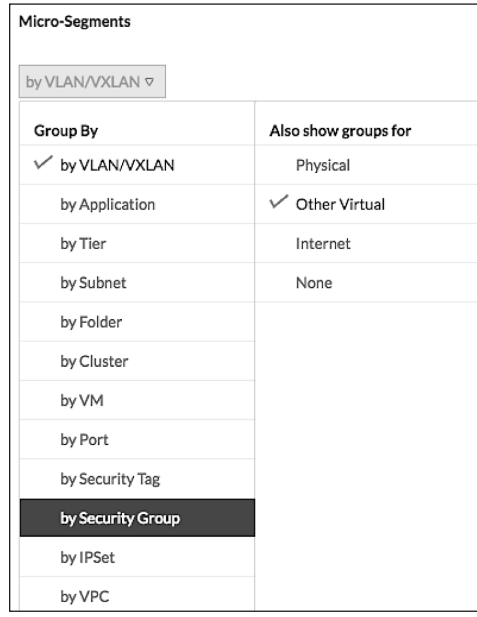


Figure 4.27 Book application DB filter micro-segments

8. Click on the **SG-3T-DB** wedge.

This will highlight all the Flows from **SG-3T-DB** to other destinations. The number 1 in parenthesis in the **SG-3T-DB** wedge represents the number of virtual machines within the Security Group and matches the single Book Application DB server.

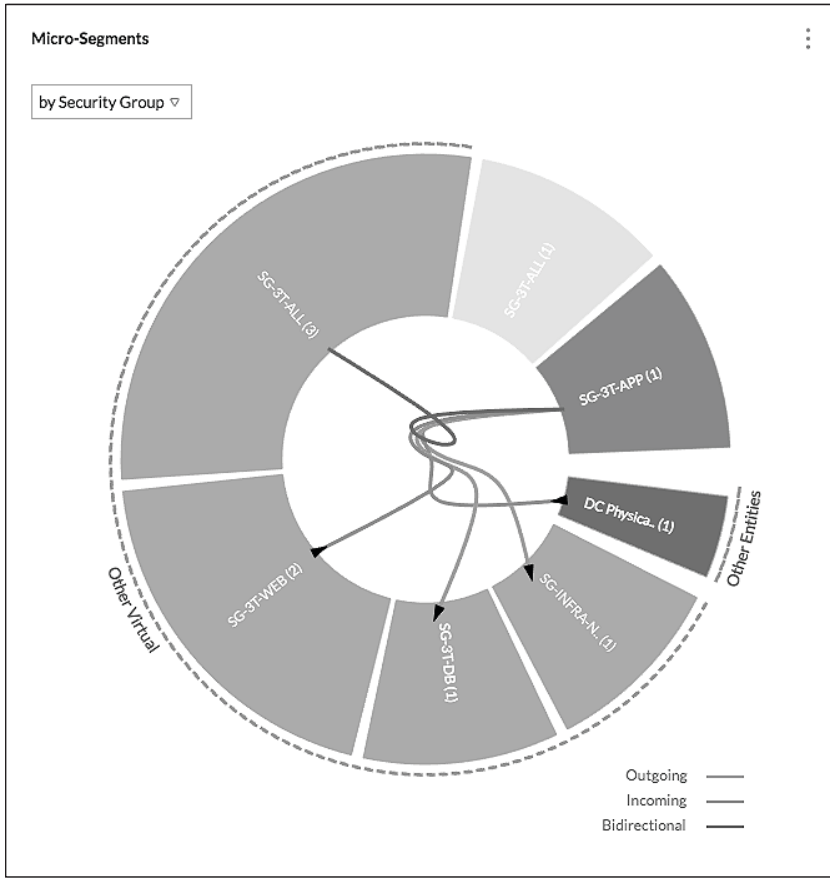


Figure 4.28 Book application DB micro-segment filter results

9. Click on the **SG-3T-DB** wedge to open the **Services and Flows for SG-3T-DB** screen.

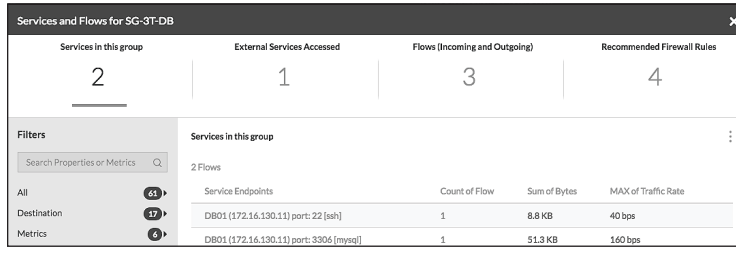


Figure 4.29 Book application DB incoming and outgoing Flows

This screen shows 4 Flows associated with **SG-3T-DB**. Click on **Flows (Incoming and Outgoing)** for additional Flow detail. Select the **Recommended Firewall Rules** tab for further rule review.

10. Click on the number **4** below the **Recommended Firewall** Rules tab name.

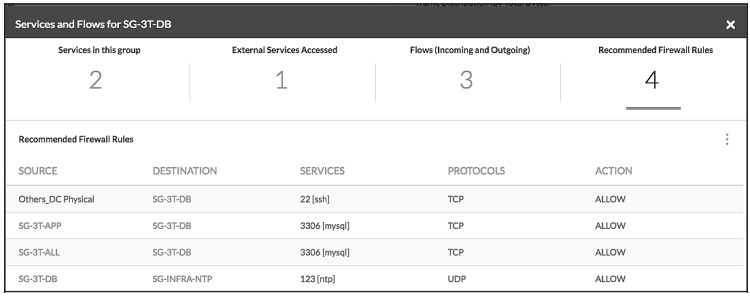


Figure 4.30 Book application DB recommended firewall rules

The information displayed shows rule suggestions from vRealize Network Insight based on observed data. When implemented on the NSX DFW, they will provide the desired micro-segmentation. This information is similar to the web servers; it also show Flows from the **Others_DC Physical** set of sources. These Flows are over TCP port **22** (i.e., SSH). Confirm that Flow originates from the same system as the other servers and add the **SG-3T-DB Security Group** to the existing documented rules. Additionally, there are Flows from **SG-3T-DB** to **SG-3T-ALL**, identifying communication between the DB group is talking and another group or collection of groups that exist within the **SG-3T-ALL Security Group**.

Dig into the Flow details to decipher the specifics of these Flows reaching outside of the NSX/vRealize Network Insight environment.

Procedure

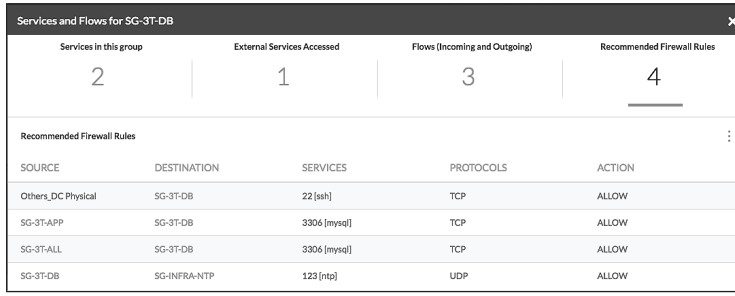


Figure 4.31 Book application DB others_DC_physical Flows

1. Click on the number **3** under the **Flows (Incoming and Outgoing)**.
2. Click on the **Service and Port** option to the left and select **Port**. This will add the **Port** filter to the left-hand side.
3. Remove the **All** selection and check **22** for SSH. This will filter the Flows to only show port 22 traffic.

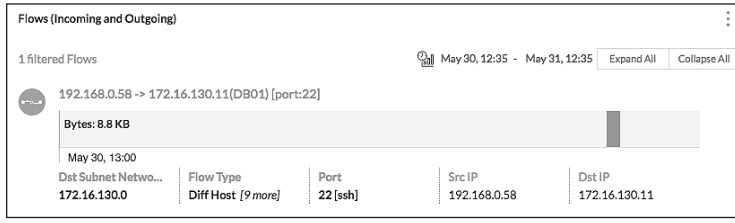


Figure 4.32 Book application DB incoming Flow SSH

Figure 4.32 shows the IP address **192.168.0.58** connecting to the **DB01** server over TCP port **22**. This was a requirement to allow this system access to the Book Application servers via SSH. Add this information into the previous table. As the management system needs access to all of the Book Application servers, replace the **Destination** and the **Applied** To fields to only use the **SG-3T-ALL Security Group**, as it already contains all of the Security Groups. This will streamline the rule.

Table 4.13 Book application management access NSX DFW rules layout

Management Access Communications:

Name	Source	Destination	Service	Action	Applied To
Allow MGMT to Book Application Web	IP_MGMT_ ACCESS	SG-3T-ALL	SSH	Allow	SG-3T-ALL

IPSet	IP Address
IP-MGMT-ACCESS	192.168.0.58

Service	Port
SSH	TCP 22

Move on to the next set of Flows by port.

4. Change the **Port** number to **3306** and remove **22**.

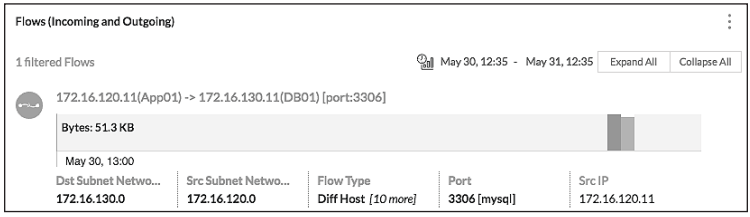


Figure 4.33 Book application DB incoming Flow MySQL

These Flows verify that the **App01** server is connecting to **DB01** over TCP **3306**.

This rule does not require addition to the table as it was previously built in the app server section.

Document Rules for DFW – Infrastructure Services/Application

Table 4.14 Book application NSX DFW documentation

Infrastructure Access Communications:

Name	Source	Destination	Service	Action	Applied To
App Access Infra	SG-3T-ALL	SG-INFRA-NTP	NTP	Allow	SG-3T-ALL

Management Access Communications:

Name	Source	Destination	Service	Action	Applied To
Allow MGMT to Book Application Web	IP_MGMT_ACCESS	SG-3T-ALL	SSH	Allow	SG-3T-ALL

Book Application Access Communications:

Name	Source	Destination	Service	Action	Applied To
Allow Librarian to Web	IP-3T-ACCESS	SG-3T-WEB	HTTP	Allow	SG-3T-WEB

Intra-Book Application Communications:

Name	Source	Destination	Service	Action	Applied To
Allow Web to App	SG-3T-WEB	SG-3T-APP	HTTP	Allow	SG-3T-WEB SG-3T-APP
Allow App to DB	SG-3T-APP	SG-3T-DB	MySQL	Allow	SG-3T-APP SG-3T-DB

NSX Groupings:

Name	Source	Destination
SG-INFRA-NTP	NTP-01a	Static
SG-3T-WEB	Web01 Web02	Static
SG-3T-APP	App01	Static
SG-3T-DB	DB01	Static
SG-3T-ALL	SG-3T-WEB SG-3T-APP SG-3T-DB	Static

Build DFW Rules – Infrastructure Services

Procedure

1. Log into the **vSphere Web Client** and select **Networking and Security**.
2. Click on **Firewall**.
3. Right-click on the **Default Section Layer3** and select **Add Section**.
4. Enter the name of the Section as **Infrastructure Services**.
5. Expand **Infrastructure Services Section** and the **Add rule** () icon.
6. Click on the **Edit** () for the new rule **Name**.
7. Add name **Allow Access Infra** and click **Save**.
8. Click on the **Edit** () icon for the new rule **Source**.
9. Change the Object Type to **Security Group** and filter on **3T**.
10. Add the **SG-3T-ALL Security Group** and click **OK**.

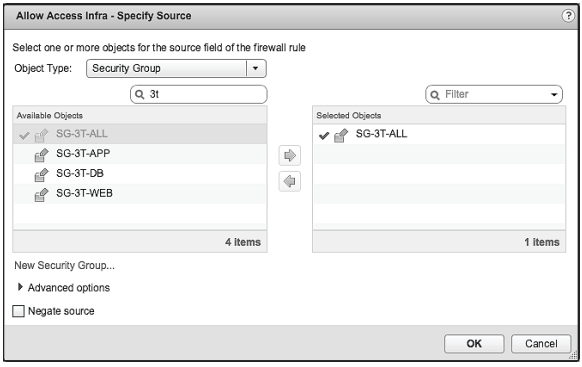


Figure 4.34 Book application all source – infrastructure access rule

11. Click on the **Edit** () icon for the new rule **Destination**.
12. Change the Object Type to **Security Group** and filter on **SG-INFRA**.
13. Add the **SG-INFRA-NTP Security Group** and click **OK**.

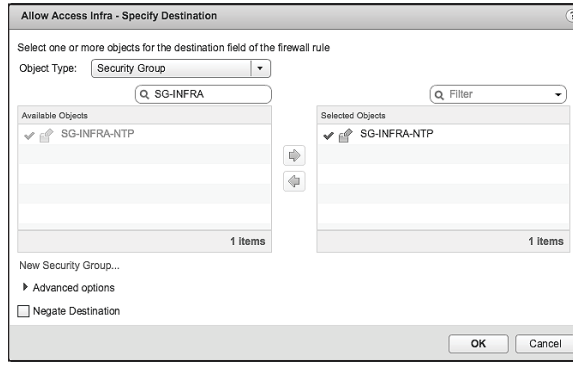


Figure 4.35 Infrastructure Destination – Infrastructure access rule

14. Click on the **Edit** ( ) icon for the new rule **Service**.
15. Change the Object Type to **Service** and filter on **NTP**.
16. Add the **NTP Service** and click **OK**.
17. Click on the **Edit** ( ) icon for the new rule **Action**.
18. Click on the **Log** radio button and click **Save**.

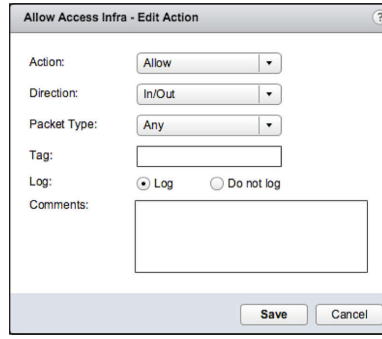


Figure 4.36 Infrastructure allow – infrastructure access rule

19. Click on the **Edit** ( ) icon for the new rule **Applied To**.
20. Uncheck the first check box.
21. Change the Object Type to **Security Group** and filter on **3T**.
22. Select the **SG-3T-ALL** and click **OK**

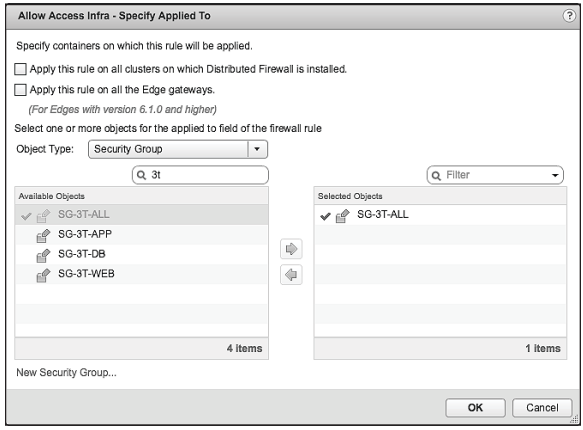


Figure 4.37 Infrastructure applied to book application – infrastructure access rule

Once the new infrastructure services rule is completed, **Publish** the rules down to the virtual machines.

When complete, the NSX Manager will assign a **RuleID** for each new rule created.

Figure 4.38 Infrastructure access NSX DFW rule verification

Build DFW Rules – Management Services

Procedure

1. Log into the **vSphere Web Client** and select **Networking and Security**.
2. Click on **Firewall**.
3. Right-click on the **Default Section Layer3** and select **Add Section**.
4. Enter the name of the Section as **Management Services**.
5. Expand **Management Services Section** and the **Add rule** () icon.
6. Click on the **Edit** () icon for the new rule **Name**.
7. Add name **Allow MGMT Access** and click **Save**.
8. Click on the **Edit** () icon for the new rule **Source**.
9. Change the Object Type to **IP Set**.
10. Click on **New IP Set...**

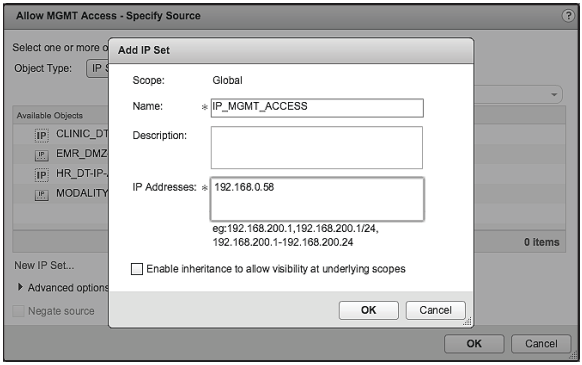


Figure 4.39 Management source – management access rule

11. Type in the Name **IP_MGMT_ACCESS**.
12. Type in the IP Address of the Management system, **192.168.0.58**.
13. Click **OK** and Click **OK** again.
14. Click on the **Edit** () icon for the new rule **Destination**.
15. Change the Object Type to **Security Group** and filter on **3T**.

16. Add the **SG-3T-ALL Security Group** and click **OK**.

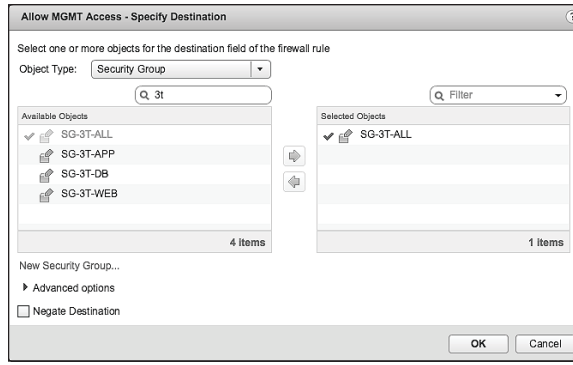


Figure 4.40 Management book application all destination – management access rule

17. Click on the **Edit** ( ) icon for the new rule **Service**.
18. Change the Object Type to **Service** and filter on **SSH**.
19. Add the **SSH Service** and click **OK**.
20. Click on the **Edit** ( ) icon for the new rule **Action**.
21. Click on the **Log** radio button and click **Save**.

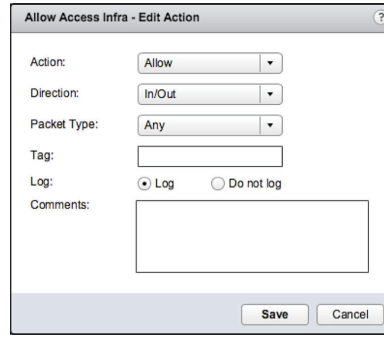


Figure 4.41 Management allow – management access rule

22. Click on the **Edit** ( ) icon for the new rule **Applied To**.
23. Uncheck the first check box.
24. Change the Object Type to **Security Group** and filter on **3T**.

25. Select the **SG-3T-ALL** and click **OK**

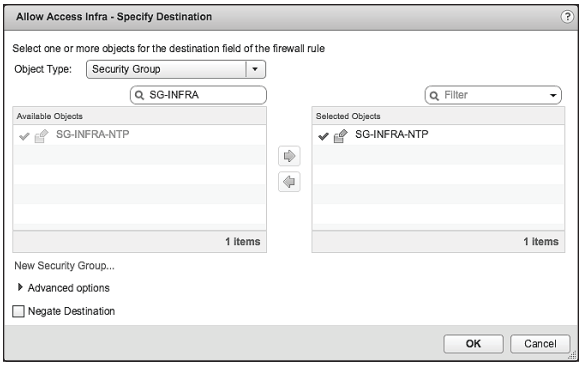


Figure 4.42 Management applied to book application – management access rule

Once the new infrastructure services rule is completed, **Publish** the rules down to the virtual machines.

When complete, the NSX Manager will assign a **RuleID** for each new rule created.

Figure 4.43 Management access NSX DFW rule verification

Build DFW Rules – Application

Procedure

1. Log into the **vSphere Web Client** and select **Networking and Security**.
2. Click on **Firewall**.
3. Right-click on the **Default Section Layer3** and select **Add Section**.
4. Enter the name of the Section as **Book Application**.
5. Expand **Book Application Section** and the **Add rule** () icon.
6. Click on the **Edit** () icon for the new rule **Name**.
7. Add name **Librarian Access App** and click **Save**.
8. Click on the **Edit** () icon for the new rule **Source**.
9. Change the Object Type to **IP Set**.
10. Click on **New IP Set...**

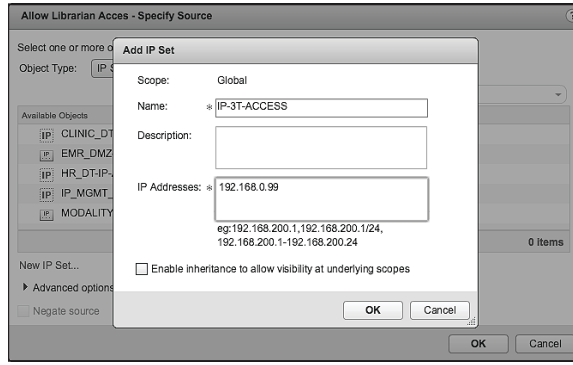


Figure 4.44 Librarian source – web access rule

11. Type in the Name **IP_3T_ACCESS**.
12. Type in the IP Address of the Management system, **192.168.0.99**.
13. Click **OK** and Click **OK** again.
14. Click on the **Edit** () icon for the new rule **Destination**.
15. Change the Object Type to **Security Group** and filter on 3T.

16. Add the **SG-3T-WEB Security Group** and click **OK**.

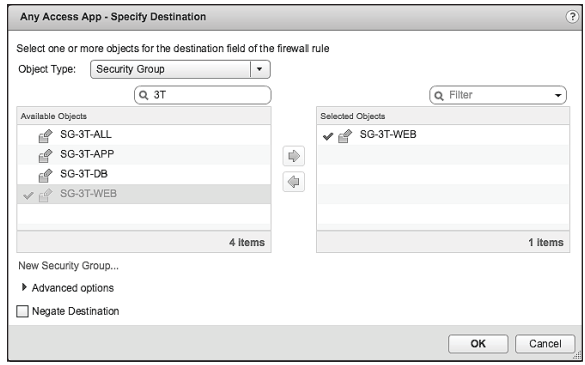


Figure 4.45 Book application web destination – web access rule

17. Click on the **Edit** ( ) icon for the new rule **Service**.
18. Change the Object Type to **Service** and filter on **HTTP**.
19. Add the **HTTP Service** and click **OK**.
20. Click on the **Edit** ( ) icon for the new rule **Action**.
21. Click on the **Log** radio button and click **Save**.

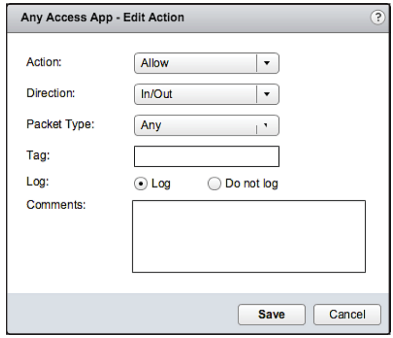


Figure 4.46 Librarian allow – web access rule

22. Click on the **Edit** ( ) icon for the new rule **Applied To**.
23. Uncheck the first check box.
24. Change the Object Type to **Security Group** and filter on **3T**.
25. Select the **SG-3T-WEB Security Group** and click **OK**.

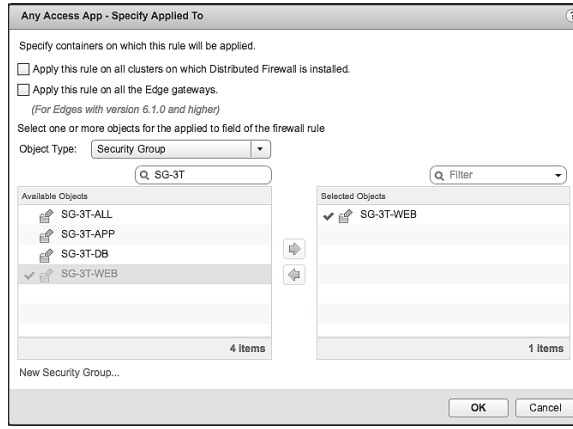


Figure 4.47 Librarian applied to web – web access rule

Web to App Rule

1. Click on the **Add rule** (➕) icon. This will put a new rule below the **Librarian Access App** rule.
2. Click on the **Edit** (✏) icon for the new rule **Name**.
3. Add name **Web to App** and click **Save**.
4. Click on the **Edit** (✏) icon for the new rule **Source**.
5. Change the Object Type to **Security Group** and filter on **3T**.
6. Add the **SG-3T-WEB Security Group** and click **OK**.

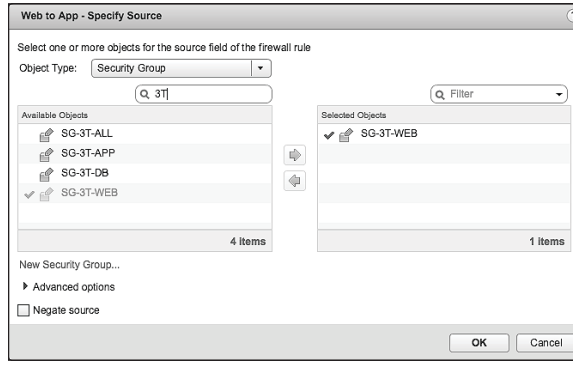


Figure 4.48 Book application web source – Web to App rule

7. Click on the **Edit** ( ) icon for the new rule **Destination**.
8. Change the Object Type to **Security Group** and filter on **3T**.
9. Add the **SG-3T-APP Security Group** and click **OK**.

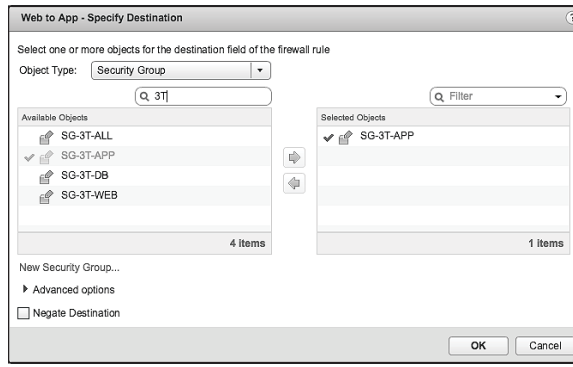


Figure 4.49 Book application app destination – Web to App rule

10. Click on the **Edit** ( ) icon for the new rule **Service**.
11. Change the Object Type to **Service** and filter on **HTTP**.
12. Add the **HTTP Service** and click **OK**.
13. Click on the **Edit** ( ) icon for the new rule **Action**.
14. Click on the **Log** radio button and click **Save**.

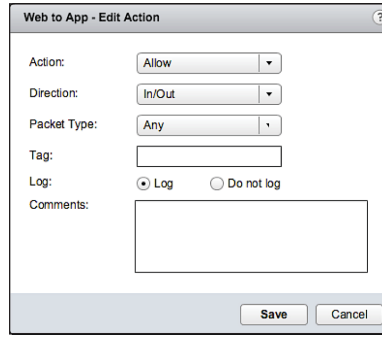


Figure 4.50 Book application web allow – Web to App rule

15. Click on the **Edit** ( ) icon for the new rule **Applied To**.

16. Uncheck the first check box.

17. Change the Object Type to **Security Group** and filter on **3T**.

18. Select the **SG-3T-WEB** and **SG-3T-APP Security Group** and click **OK**.

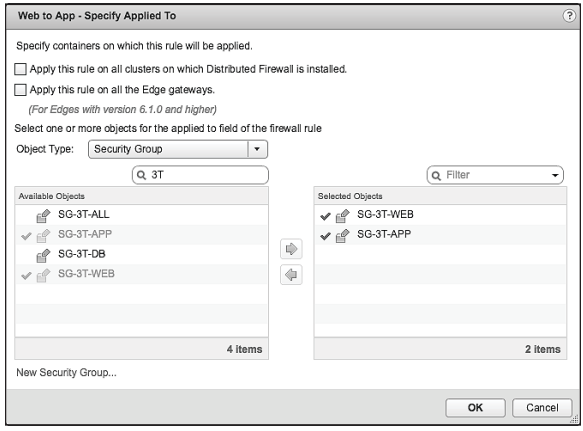


Figure 4.51 Book application applied to Web and App – Web to App rule

App to DB Rule

1. Click on the **Add rule** (➕) icon. This will put a new rule below the Web to **App rule**.

2. Click on the **Edit** (✏) icon for the new rule **Name**.

3. Add name **App to DB** and click **Save**.

4. Click on the **Edit** (✏) icon for the new rule **Source**.

5. Change the Object Type to **Security Group** and filter on **3T**.

6. Add the **SG-3T-App Security Group** and click **OK**.

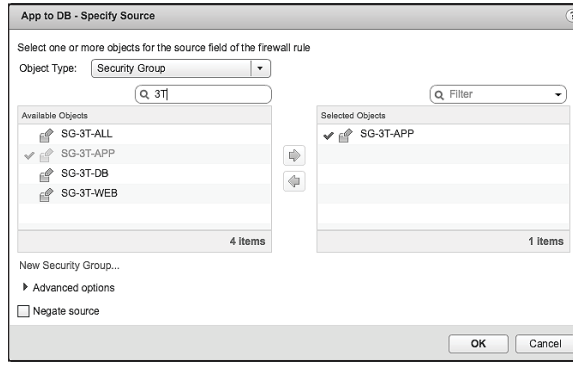


Figure 4.52 Book application app source – App to DB rule

7. Click on the **Edit** ( ) icon for the new rule **Destination**.
8. Change the Object Type to **Security Group** and filter on **3T**.
9. Add the **SG-3T-DB Security Group** and click **OK**.

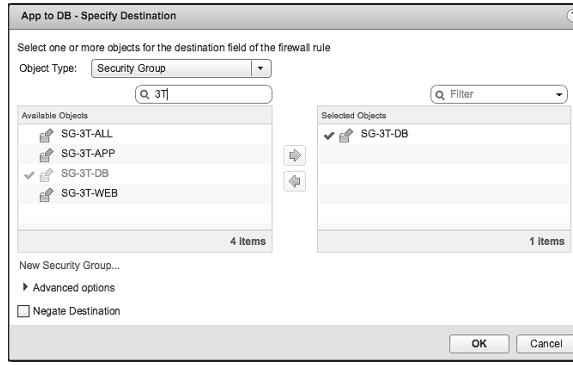


Figure 4.53 Book application DB destination – App to DB rule

10. Click on the **Edit** ( ) icon for the new rule **Service**.
11. Change the Object Type to **Service** and filter on **MYSQL**.
12. Add the **MySQL Service** and click **OK**.
13. Click on the **Edit** ( ) icon for the new rule **Action**.
14. Click on the **Log** radio button and click **Save**.

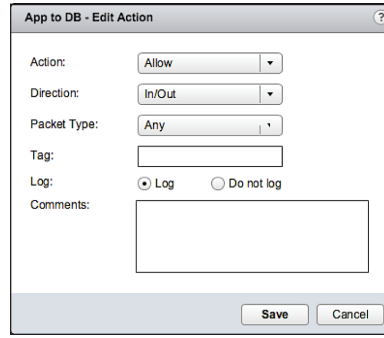


Figure 4.54 Book application app allow – App to DB rule

15. Click on the **Edit** ( ) icon for the new rule **Applied To**.
16. Uncheck the first check box.
17. Change the Object Type to **Security Group** and filter on **3T**.
18. Select the **SG-3T-APP** and **SG-3T-DB Security Group** and click **OK**.

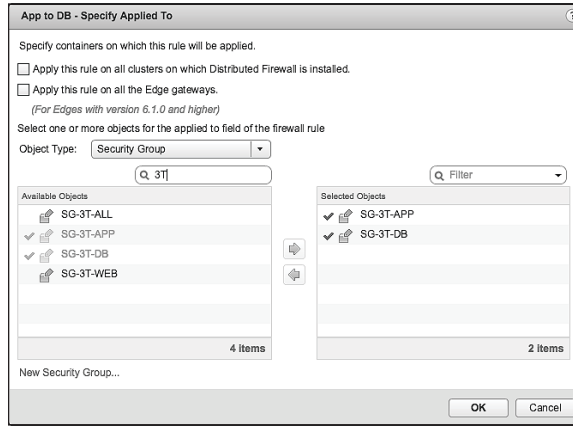


Figure 4.55 Book application applied to App and DB – App to DB rule

Once the new infrastructure services rule is completed, **Publish** the rules down to the virtual machines.

When complete, the NSX Manager will assign a **RuleID** for each new rule created.

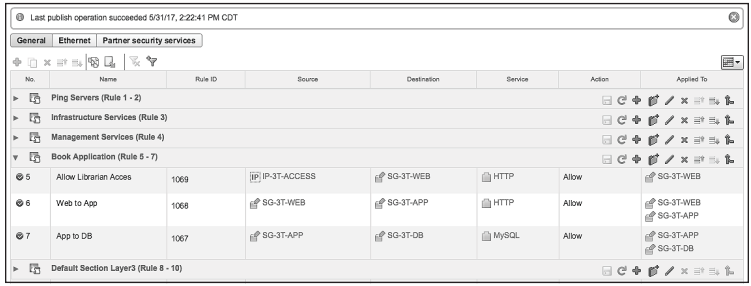


Figure 4.56 Book application NSX DFW rule verification

Build Block Rules

Procedure

First Block Rule Configuration

1. Click on the **Add rule** (➕) icon on the **Book Application** Section two times to add the necessary rule instances.
2. Click on the **Edit** (✎) icon for the first rule **Name**.
3. Add name **Block Any to App Log** and click **Save**.
4. Click on the **Edit** (✎) icon for the first rule **Destination**.
5. Change the Object Type to **Security Group** and filter on **3T**.
6. Add the **SG-3T-ALL Security Group** and click **OK**.
7. Click on the **Edit** (✎) icon for the first rule **Action**.
8. Change the Action to **Block**.
9. Click on the **Log** radio button and click **Save**.
10. Click on the **Edit** (✎) icon for the first rule **Applied To**.
11. Uncheck the first check box.
12. Change the Object Type to **Security Group** and filter on **3T**.
13. Select the **SG-3T-ALL** and click **OK**.

Second Block Rule Configuration

1. Click on the **Edit** ( ) icon for the second rule **Name**.
2. Add name **Block App to Any Log** and click **Save**.
3. Click on the **Edit** ( ) icon for the second rule **Source**.
4. Change the Object Type to **Security Group** and filter on **3T**.
5. Add the **SG-3T-ALL Security Group** and click **OK**.
6. Click on the **Edit** ( ) icon for the second rule **Action**.
7. Change the Action to **Block**.
8. Click on the **Log** radio button and click **Save**.
9. Click on the **Edit** ( ) icon for the second rule **Applied To**.
10. Uncheck the first check box.
11. Change the Object Type to **Security Group** and filter on **3T**.
12. Select the **SG-3T-ALL** and click **OK**.

Once the block configurations are all completed, disable the two new rules before the **Publish** of the rules down to the virtual machines.

When complete, the NSX Manager will assign a **RuleID** for each new rule created.

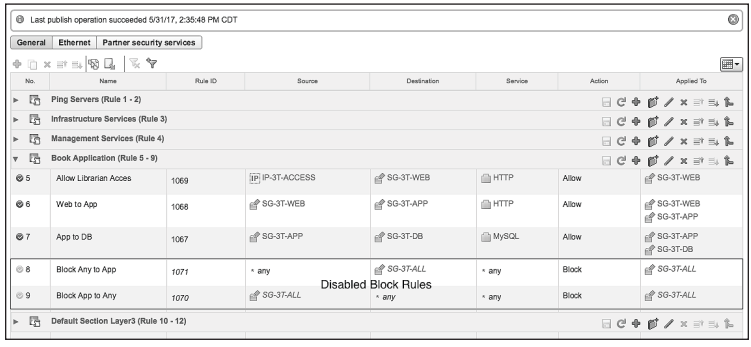


Figure 4.57 Book application disable block all rule

Verify Functionality

Before starting the verification and functionality process, revisit the requirements for this application.

- Allow only Librarian (192.168.0.99) inbound to Web01 and Web02.
- Allow only Management (192.168.0.58) inbound to All Servers via SSH.
- Allow Web01 and Web02 to communication with App01.
- Allow App01 to communicate with DB01.
- Allow all servers to communicate with any external services necessary to function.
- Block communications between Web01 and Web02.
- Block all other communications to any server of the application unless explicitly defined in the above requirements.

Begin with verification and functionality testing of the infrastructure services rule against the requirement.

Requirement to meet

- Allow all servers to communicate with any external services necessary to function.

Procedure

1. Log into the **vSphere Web Client** and select **Networking and Security**.
2. Click on **Flow Monitoring**.
3. Click on **Live Flow**.
4. Click on **Change...** to at a vNIC to monitor.
5. Filter on **NTP** and add the vNIC for **NTP-01a**
6. Click **OK**.
7. Click **Start** to begin the monitoring process.

RuleId	Direction	Flow Type	Protocol	Source IP	Source Port	Destination IP	Destination Port	State	Incoming Bytes	Incoming Packets	Outgoing Bytes	Outgoing Packets	Application Context
1065	IN	Active	UDP	172.16.110.11	123	192.168.0.211	123		76	1	76	1	
1065	IN	Active	UDP	172.16.110.12	123	192.168.0.211	123		76	1	76	1	
1065	IN	Active	UDP	172.16.120.11	123	192.168.0.211	123		76	1	76	1	
1065	IN	Active	UDP	172.16.130.11	123	192.168.0.211	123		76	1	76	1	

Figure 4.58 Flow monitoring infrastructure services RuleID verification

Figure 4.59 Infrastructure services NSX DFW RuleID verification

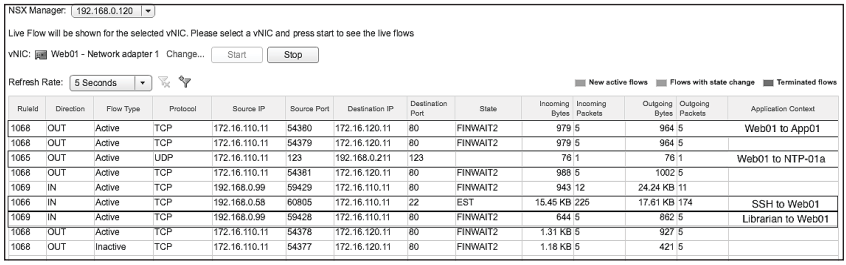
The NTP rule now matches on RuleID **1065** and is not being dropped. This verifies that the requirement is met.

Requirements to meet

- Allow only Librarian (192.168.0.99) inbound to Web01 and Web02.
- Allow only Management (192.168.0.58) inbound to All Servers via SSH.
- Allow Web01 and Web02 to communication with App01.

Procedure

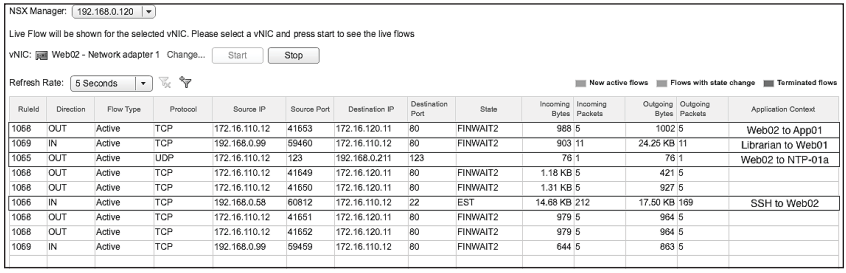
1. Log into the **vSphere Web Client** and select **Networking and Security**.
2. Click on **Flow Monitoring**.
3. Click on **Live Flow**.
4. Click on **Change...** to at a vNIC to monitor.
5. Filter on **Web** and add the vNIC for **Web01**
6. Click **OK**.
7. Click **Start** to begin the monitoring process.



RuleId	Direction	Flow Type	Protocol	Source IP	Source Port	Destination IP	Destination Port	State	Incoming Bytes	Incoming Packets	Outgoing Bytes	Outgoing Packets	Application Context
1068	OUT	Active	TCP	172.16.110.11	54380	172.16.120.11	80	FINWAIT2	979	5	964	5	Web01 to App01
1068	OUT	Active	TCP	172.16.110.11	54379	172.16.120.11	80	FINWAIT2	979	5	964	5	
1065	OUT	Active	UDP	172.16.110.11	123	192.168.0.211	123		76	1	76	1	Web01 to NTP-01a
1068	OUT	Active	TCP	172.16.110.11	54361	172.16.120.11	80	FINWAIT2	988	5	1002	5	
1069	IN	Active	TCP	192.168.0.99	59429	172.16.110.11	80	FINWAIT2	943	12	24.24 KB	11	
1066	IN	Active	TCP	192.168.0.58	60805	172.16.110.11	22	EST	15.45 KB	225	17.61 KB	174	SSH to Web01
1069	IN	Active	TCP	192.168.0.99	59428	172.16.110.11	80	FINWAIT2	644	5	862	5	Librarian to Web01
1068	OUT	Active	TCP	172.16.110.11	54378	172.16.120.11	80	FINWAIT2	1.31 KB	5	927	5	
1068	OUT	Inactive	TCP	172.16.110.11	54377	172.16.120.11	80	FINWAIT2	1.18 KB	5	421	5	

Figure 4.60 Flow monitoring web 1 RuleID verification

8. Repeat the process to monitor **Web02**.



RuleId	Direction	Flow Type	Protocol	Source IP	Source Port	Destination IP	Destination Port	State	Incoming Bytes	Incoming Packets	Outgoing Bytes	Outgoing Packets	Application Context
1068	OUT	Active	TCP	172.16.110.12	41653	172.16.120.11	80	FINWAIT2	988	5	1002	5	Web02 to App01
1069	IN	Active	TCP	192.168.0.99	59460	172.16.110.12	80	FINWAIT2	903	11	24.25 KB	11	Librarian to Web01
1065	OUT	Active	UDP	172.16.110.12	123	192.168.0.211	123		76	1	76	1	Web02 to NTP-01a
1068	OUT	Active	TCP	172.16.110.12	41649	172.16.120.11	80	FINWAIT2	1.18 KB	5	421	5	
1068	OUT	Active	TCP	172.16.110.12	41650	172.16.120.11	80	FINWAIT2	1.31 KB	5	927	5	
1066	IN	Active	TCP	192.168.0.58	60812	172.16.110.12	22	EST	14.68 KB	212	17.50 KB	169	SSH to Web02
1068	OUT	Active	TCP	172.16.110.12	41651	172.16.120.11	80	FINWAIT2	979	5	964	5	
1068	OUT	Active	TCP	172.16.110.12	41652	172.16.120.11	80	FINWAIT2	979	5	964	5	
1069	IN	Active	TCP	192.168.0.99	59459	172.16.110.12	80	FINWAIT2	644	5	863	5	

Figure 4.61 Flow monitoring web 2 RuleID verification

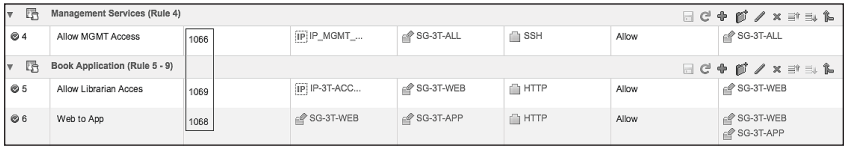


Figure 4.62 Management and librarian NSX DFW RuleID verification

Figures 4.74 and 4.75 highlight the following matches, confirming that the functionality requirements are met:

- Web-to-app traffic allowed by **RuleID 1068**
- Web servers accessible via **SSH** through **RuleID 1066**
- Access to both web servers for the **Librarian via RuleID 1069**. This verifies that the requirements are met.

Requirements to meet

- Allow only Management (192.168.0.58) inbound to All Servers via SSH.
- Allow App01 to communicate with DB01.

Procedure

1. Log into the **vSphere Web Client** and select **Networking and Security**.
2. Click on **Flow Monitoring**.
3. Click on **Live Flow**.
4. Click on **Change...** to at a vNIC to monitor.
5. Filter on **App** and add the vNIC for **App01**
6. Click **OK**.
7. Click **Start** to begin the monitoring process.

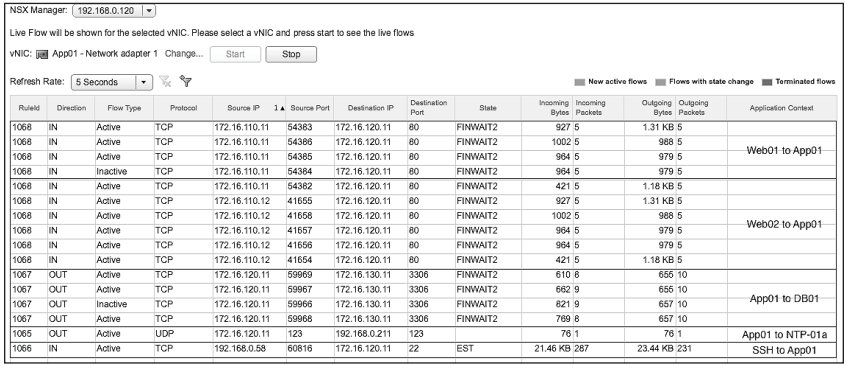


Figure 4.63 Flow monitoring Web to App and App to DB RuleID verification

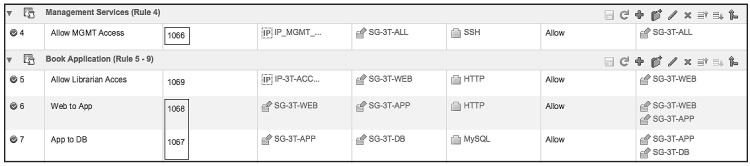


Figure 4.64 Book application Web, App, and DB RuleID verification

Figures 4.77 and 4.78 highlight the following matches, confirming that the functionality requirements are met:

- Web-to-app traffic allowed by **RuleID 1068**.
- The **App01** server is accessible via **SSH** through **RuleID 1066**.
- **App01** to **DB01** connectivity is allowed by **RuleID 1067**. This verifies that the requirements are met.

Enable Block Rules

With verification of the allow rules complete, enable the block rules to verify that the required traffic is properly blocked.

Procedure

1. Log into the **vSphere Web Client** and select **Networking and Security**.
2. Click on **Firewall**.
3. Expand the **Book Application Section**.
4. Click on the greyed-out checkmarks on the Block rules to enable.
5. **Publish Changes**.

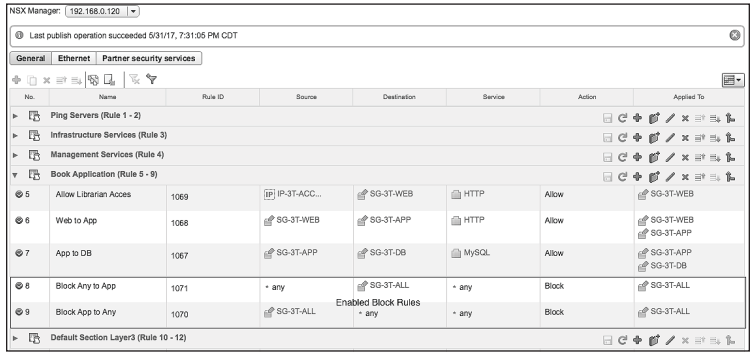


Figure 4.65 Book application block all enable verification

Verify Block

Once the block rules are enabled, verify that the requirements are met with the block rules.

Requirements to meet

- Block communications between Web01 and Web02.
- Block other communications to any server of the application unless explicitly defined in the above requirements.

Procedure

1. Log into the **vSphere Web Client** and select **Networking and Security**.
2. Click on **Flow Monitoring**.
3. Click on **Live Flow**.
4. Click on **Change...** to at a vNIC to monitor.
5. Filter on Web and add the vNIC for **Web01**.
6. Click **OK**.
7. Click **Start** to begin the monitoring process.

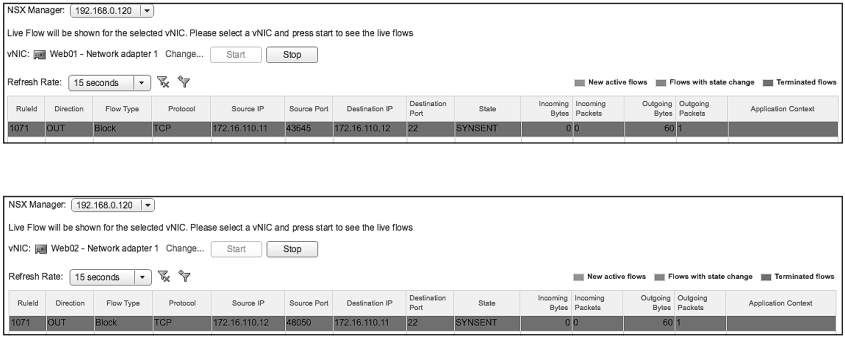


Figure 4.66 Flow monitoring Web to Web block verification

Figure 4.66 shows a blocked attempt to **SSH** from **Web01** to **Web02** and **Web02 to Web01 hitting RuleID 1071**.

This verifies the requirement to block connectivity between **Web01** and **Web02**.

The final verification is to attempting to connect to the Book Application from the **192.168.0.58** system and to attempt to **SSH** to the Book Application servers from **192.168.0.99**. The opposite is explicitly allowed in the ruleset. Figure 4.67 shows the results of these attempts.

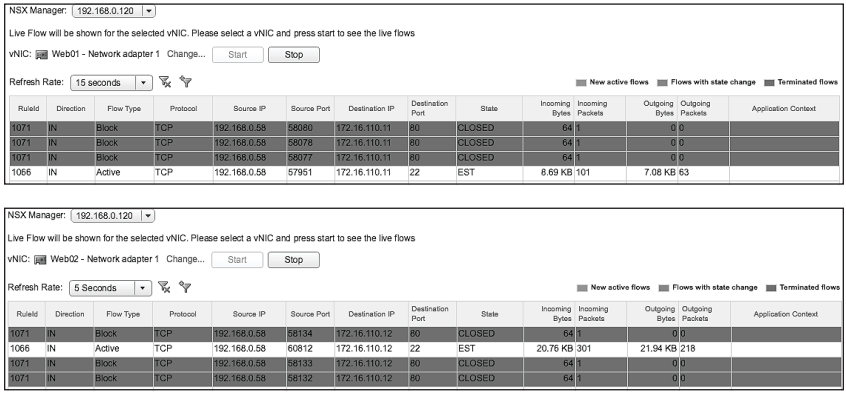


Figure 4.67 Flow monitoring web access block unauthorized verification

Reusing the **Flow Monitoring** sessions from before, it is shown that when **192.168.0.58** attempts to connect to **Web01** or **Web02**, the connections are blocked by **RuleID 1071**.

Reusing the same **Flow Monitoring** sessions for each of the Book Application servers shows that that the **SSH** block is working as well.

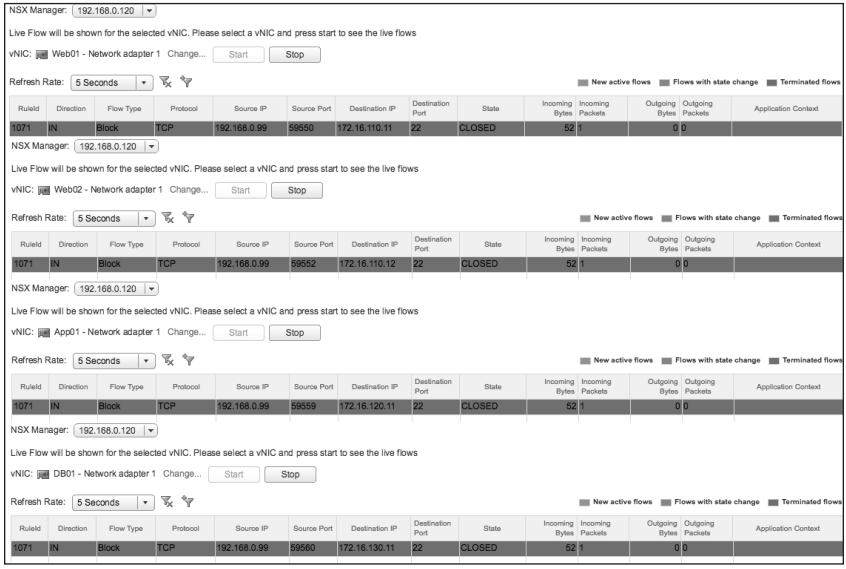


Figure 4.68 Flow monitoring book application block unauthorized SSH verification

These tests verify that the block rules are working as intended, stopping all undesired traffic.

Show Application Functional

The final test is to demonstrate that the Book Application is still functional with these rulesets are in place. Attempt to connect to each of the Book Application's web servers from the 192.168.0.99 system.

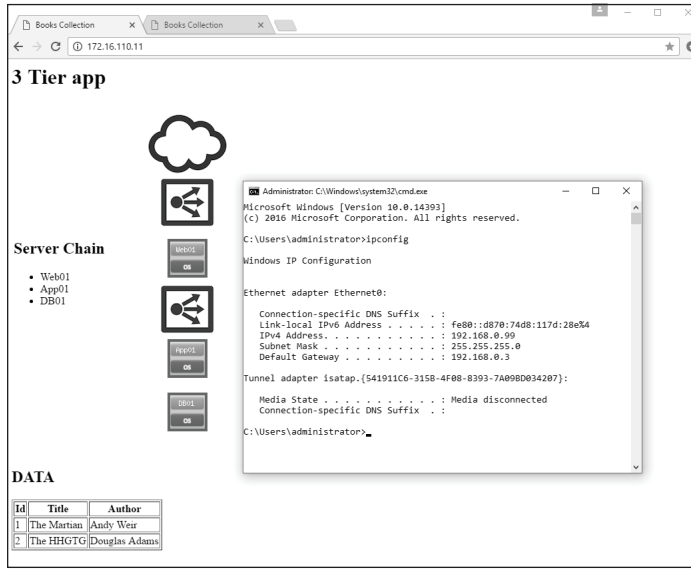


Figure 4.69 Book application web 1 functional verification

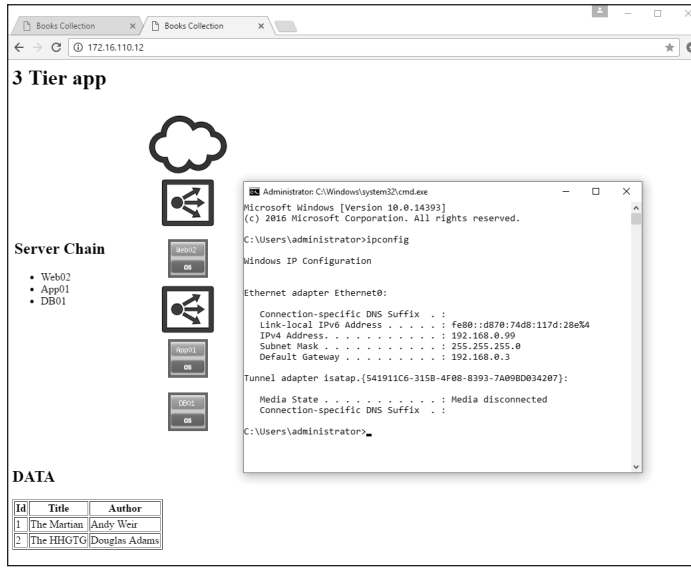


Figure 4.70 Book application web 2 functional verification

This confirms that all requirements have been met, with the Book Application micro-segmented and still functional.

Conclusion

Knowledge of where and how to begin micro-segmentation efforts is key to successfully securing applications in the software-defined data center. With a new understanding of the methodologies and toolsets available to help create a least privilege environment, an organization can now accomplish what was nearly impossible with previous toolsets. Whether building a new infrastructure or augmenting an existing environment, VMware NSX and its surrounding toolsets can be used to provide a highly granular and scalable security solution that facilitates a least privilege security model.

Reference

VMware NSX for vSphere Documentation
https://www.vmware.com/support/pubs/nsx_pubs.html

The VMware NSX Platform – Healthcare Series – Part 4.1: Micro-segmentation Practical
https://vwilmo.wordpress.com/2016/11/27/the-vmware-nsx-platform-healthcare-series-part-4-1-micro-segmentation-practical/

The VMware NSX Platform – Healthcare Series – Part 4.2: Micro-segmentation Practical with Application Rule Manager
https://vwilmo.wordpress.com/2017/03/22/the-vmware-nsx-platform-healthcare-series-part-4-2-micro-segmentation-practical-with-vmware-nsx-application-rule-manager/

The VMware NSX Platform – Healthcare Series – Part 4.3: Micro-segmentation Practical – vRealize Network Insight
https://vwilmo.wordpress.com/2017/04/07/the-vmware-nsx-platform-healthcare-series-part-4-3-micro-segmentation-practical-vrealize-network-insight/

Index

The planning of micro-segmentation can be an overwhelming task because most organizations have tens to thousands of applications in their data centers. Knowing which applications and how to start planning for the implementation of a least-privilege, Zero-Trust security posture with VMware NSX and micro-segmentation is critical. As we go through *VMware NSX Micro-segmentation – Day 2*, we will arm you with the knowledge you need to begin building a scalable methodology and planning for the applications you are going to secure. For immediate micro-segmentation needs, we'll take a look at VMware Log Insight. We'll cover NSX Application Rule Manager, which scales up our ability to plan and implement Distributed Firewall Rulesets. And finally, we'll look at vRealize Network Insight, a product that introduces data center scale security planning and operations. We will compare and contrast when to use each tool, and demonstrate detailed step-by-step processes for using them.

About the Author

Geoff Wilmington, VCIX6-NV, is a Senior Systems Engineer within the VMware Networking and Security Business Unit, focusing on all security aspects and functions of the VMware NSX product. Geoff is a 17-year industry veteran and has worked at VMware for 2.5 years and across multiple positions within the Information Technology industry. He is a VMware Certified Implementation Expert for the VMware NSX product, and has been recognized as a VMware vExpert for technical community involvement.

Geoff has spoken at local VMware User Group meetings as both a customer and a VMware employee and has been featured at multiple sessions at VMworld US. Geoff holds a Bachelor's degree in IT Management. Follow Geoff on Twitter @vWilmo or visit his blog http://vwilmo.wordpress.com.

Cover design:
VMware

Cover photo:
Vertigo3d / iStock

ISBN-13: 978-0-9986104-1-2
ISBN-10: 0-9986104-1-0

9 780998 610412

$12.99

vmware PRESS

www.vmware.com/go/run-nsx