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.

Copyright © 2017 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Table of Contents

Preface	XIX
Foreword	XX
Chapter 1 - Planning, Methodology, and Application Visibility	1
Where to start?	4
Understanding the Application(s)	4
Planning	5
Tools	14
Chapter 2 - vRealize Log Insight	17
Define the Application	18
Understand the Requirements	19
Define the Methodology	19
Technologies Used	20
Define Monitor Length	21
NSX/Log Insight Management Pack Installation	21
Connect NSX Manger to Log Insight	26
Layout Naming Scheme	29
Create Security Groups - Infrastructure Services/Application	29
Build DFW Rules for Allow/Block	32
Monitor Traffic Flows	36
Analyze Traffic Flows	38
Document Rules for DFW - Infrastructure Services/Application	40
Create Services - Infrastructure Services	42
Create Services - Application	43
Build DFW Rules - Infrastructure Services	45
Build DFW Rules - Application	48
Monitor Traffic Flows	57
Verify Shared Service/Application Functionality	59
Disable/Remove Allow Rule	64
Re-Verify Shared Service/Application Functionality	66
Chapter 3 - Application Rule Manager	69
Flow Direction	70
Define the Application	70
Understand the requirements	71
Define the Methodology	72
Technologies Used	73
Define Monitor Length	74
Layout Naming Scheme	74
Create Monitor Session - Infrastructure Services	75
Analyze Monitored Session - Infrastructure Services	76

	Document Rules for DFW – Infrastructure Services	78
	Create Security Groups - Infrastructure Services	79
	Create Services - Infrastructure Services	81
	Create DFW Rules - Infrastructure Services	82
	Publish DFW Rules - Infrastructure Services	
	Create Monitor Session - Application	
	Analyze Monitored Session - Application	
	Document Rules for DFW – Application	
	Create Security Groups - Application	
	Create Services - Application	93
	Create DFW Rules - Book Application	95
	Publish DFW Rules - Book Application	97
	Build DFW Rules for Block	
	Create Monitor Session - Infrastructure Services/Application	101
	Analyze Monitored Session - Infrastructure Services	102
	Verify Infrastructure Services/Application Functionality	
	Verify Block	108
	Show Application Functional	108
(Chapter 4 - vRealize Network Insight	111
	Define the Application	111 112
	Define the Application Understand the Requirements	111 112 113
	Define the Application Understand the Requirements Define the Methodology	
	Define the Application Understand the Requirements Define the Methodology Layout Naming Scheme	
	Define the Application Understand the Requirements Define the Methodology Layout Naming Scheme Create Security Group - Infrastructure Services	
	Define the Application Understand the Requirements Define the Methodology Layout Naming Scheme Create Security Group - Infrastructure Services Create Security Groups - Application	
	Define the Application Understand the Requirements Define the Methodology Layout Naming Scheme Create Security Group – Infrastructure Services Create Security Groups – Application Analyze traffic Flows – SG-3T-WEB	
	Define the Application Understand the Requirements Define the Methodology Layout Naming Scheme Create Security Group - Infrastructure Services Create Security Groups - Application Analyze traffic Flows - SG-3T-WEB Analyze traffic Flows - SG-3T-APP	
	Define the Application Understand the Requirements Define the Methodology Layout Naming Scheme Create Security Group – Infrastructure Services Create Security Groups – Application Analyze traffic Flows – SG-3T-WEB Analyze traffic Flows – SG-3T-APP Analyze traffic Flows – SG-3T-DB	
	Define the Application Understand the Requirements Define the Methodology Layout Naming Scheme Create Security Group - Infrastructure Services Create Security Groups - Application Analyze traffic Flows - SG-3T-WEB Analyze traffic Flows - SG-3T-APP Analyze traffic Flows - SG-3T-DB Document Rules for DFW - Infrastructure Services/Applicatio	
	Define the Application Understand the Requirements Define the Methodology Layout Naming Scheme Create Security Group - Infrastructure Services Create Security Groups - Application Analyze traffic Flows - SG-3T-WEB Analyze traffic Flows - SG-3T-APP Analyze traffic Flows - SG-3T-DB Document Rules for DFW - Infrastructure Services/Applicatio Build DFW Rules - Infrastructure Services	
	Define the Application Understand the Requirements Define the Methodology Layout Naming Scheme Create Security Group – Infrastructure Services Create Security Groups – Application Analyze traffic Flows – SG-3T-WEB Analyze traffic Flows – SG-3T-APP Analyze traffic Flows – SG-3T-DB Document Rules for DFW – Infrastructure Services/Applicatio Build DFW Rules – Infrastructure Services Build DFW Rules – Management Services	112 112 113 114 115 115 116 121 127 127 135 n141 142 145
	Define the Application Understand the Requirements Define the Methodology Layout Naming Scheme Create Security Group - Infrastructure Services Create Security Groups - Application Analyze traffic Flows - SG-3T-WEB Analyze traffic Flows - SG-3T-APP Analyze traffic Flows - SG-3T-DB Document Rules for DFW - Infrastructure Services/Applicatio Build DFW Rules - Infrastructure Services Build DFW Rules - Management Services Build DFW Rules - Application	111 112 112 113 115 115 115 115 116 127 127 127 127 141 142 145 148
	Define the Application Understand the Requirements Define the Methodology Layout Naming Scheme Create Security Group - Infrastructure Services Create Security Groups - Application Analyze traffic Flows - SG-3T-WEB Analyze traffic Flows - SG-3T-APP Analyze traffic Flows - SG-3T-DB Document Rules for DFW - Infrastructure Services/Applicatio Build DFW Rules - Infrastructure Services Build DFW Rules - Management Services Build DFW Rules - Application	111 112 113 114 115 115 115 115 116 121 127 127 141 142 145 148 167
	Define the Application Understand the Requirements Define the Methodology Layout Naming Scheme Create Security Group - Infrastructure Services Create Security Groups - Application Analyze traffic Flows - SG-3T-WEB Analyze traffic Flows - SG-3T-APP. Analyze traffic Flows - SG-3T-DB Document Rules for DFW - Infrastructure Services/Applicatio Build DFW Rules - Infrastructure Services Build DFW Rules - Management Services Build DFW Rules - Application Conclusion	
	Define the Application Understand the Requirements Define the Methodology Layout Naming Scheme Create Security Group - Infrastructure Services Create Security Groups - Application Analyze traffic Flows - SG-3T-WEB. Analyze traffic Flows - SG-3T-APP Analyze traffic Flows - SG-3T-DB. Document Rules for DFW - Infrastructure Services/Applicatio Build DFW Rules - Infrastructure Services. Build DFW Rules - Management Services Build DFW Rules - Application Conclusion Reference	111 112 113 114 115 115 115 115 116 127 135 n141 142 145 167 169 171

List of Figures

Figure 1.1 Least privilege design concepts	2
Figure 1.2 Without NSX	3
Figure 1.3 With NSX	3
Figure 1.4 Micro-segmentation methodologies	6
Figure 1.5 Default allow behavior	10
Figure 1.6 Default allow log	11
Figure 1.7 Allow access app rule match	11
Figure 1.8 Block access app rule match	11
Figure 2.1 vRealize Log Insight dashboard	21
Figure 2.2 vRealize Log Insight content pack	22
Figure 2.3 vRealize Log Insight marketplace	22
Figure 2.4 Setup instructions	23
Figure 2.5 NSX Manager general settings	23
Figure 2.6 vSphere integration	24
Figure 2.7 Infrastructure NSX security tags	24
Figure 2.8 3-Tier application web NSX security group	25
Figure 2.9 vRealize Log Insight vCenter - integration test	25
Figure 2.10 NSX Manager interface	26
Figure 2.11 NSX Manager general settings	26
Figure 2.12 NSX Manager syslog server configuration	27
Figure 2.13 vRealize Log Insight main dashboard	27
Figure 2.14 3-Tier application web applied to - web access rule	28
Figure 2.15 3-Tier application NSX security tags	30
Figure 2.16 Infrastructure NSX security tags	30
Figure 2.17 3-Tier application NSX DFW rules documentation	31
Figure 2.18 3-Tier application all NSX security groups	32
Figure 2.19 3-Tier application NSX DFW blank table	33
Figure 2.20 3-Tier application block and allow NSX DFW table	35
Figure 2.21 3-Tier application web 1 server functional	36
Figure 2.22 3-Tier application web 2 server functional	37
Figure 2.23 3-Tier application vRealize Log Insight NSX DFW rule data	38
Figure 2.24 3-Tier application vRealize Log Insight field table	39
Figure 2.25 3-Tier application vRealize Log Insight destination ports	39
Figure 2.26 3-Tier application vRealize Log Insight full field table	40
Figure 2.27 3-Tier application web source - web access rule	42
Figure 2.28 3-Tier application add HTTP service	43
Figure 2.29 3-Tier application add MySQL service	44
Figure 2.30 3-Tier application and infrastructure NSX service verification	44
Figure 2.31 3-Tier application all source - infrastructure access rule	45

Figure 2.32	Infrastructure destination - infrastructure access rule	.46
Figure 2.33	3-Tier application allow - infrastructure access rule	.46
Figure 2.34	3-Tier application applied to - infrastructure access rule	47
Figure 2.35	Infrastructure access NSX DFW table	47
Figure 2.36	3-Tier application web source - web access rule	.48
Figure 2.37	3-Tier application web destination - web access rule	.49
Figure 2.38	3-Tier application web service - web access rule	.49
Figure 2.39	3-Tier application allow - web access rule	.50
Figure 2.40	3-Tier application web applied to - web access rule	.50
Figure 2.41	3-Tier application web source - Web to App rule	51
Figure 2.42	3-Tier application web service - Web to App rule	52
Figure 2.43	3-Tier application web service - Web to App rule	52
Figure 2.44	3-Tier application allow - Web to App rule	53
Figure 2.45	3-Tier application applied to Web and App - Web to App rule.	53
Figure 2.46	3-Tier application source app - App to DB rule	.54
Figure 2.47	3-Tier application destination DB - App to DB rule	55
Figure 2.48	3-Tier application app service - App to DB rule	55
Figure 2.49	3-Tier application allow - App to DB rule	. 56
Figure 2.50	3-Tier application applied to app and DB - App to DB rule	. 56
Figure 2.51	3-Tier application NSX DFW rule table	57
Figure 2.52	vRealize Log Insight rule data dashboard	. 58
Figure 2.53	vRealize Log Insight connections by RuleID	. 58
Figure 2.54	vRealize Log Insight filter field table by NTP	.60
Figure 2.55	vRealize Log Insight field table - NTP	.60
Figure 2.56	Infrastructure access NSX DFW RuleID verification	.60
Figure 2.57	vRealize Log Insight filter field table by HTTP	61
Figure 2.58	vRealize Log Insight filtered field table by HTTP	62
Figure 2.59	3-Tier application web access NSX DFW RuleID verification	62
Figure 2.60	vRealize Log Insight filter field table by MySQL	.63
Figure 2.61	vRealize Log Insight filtered field table - MySQL	. 63
Figure 2.62	3-Tier application app access DB NSX DFW RuleID	67
Eiguro 263	Z-Tior application disable allow all NSY DEW/	.03 64
Figure 2.64	Z Tier application web to web block _ verification	.04 65
Figure 2.64	7 Tier application vDealize Leg Insight field table block	.05
Figure 2.65	verification	. 65
Figure 2.66	3-Tier application web 1 functional verification	.66
Figure 2.67	3-Tier application web 2 functional verification	67
Figure 3.1 T	opology logical design	72

Figure 3.2	Infrastructure services create monitor session	75
Figure 3.3	Infrastructure services processed monitor session	76
Figure 3.4	Infrastructure services analyze monitor session	76
Figure 3.5	Infrastructure services monitor session analysis results	77
Figure 3.6	Infrastructure services monitor session clean up	77
Figure 3.7	Infrastructure services monitor session clean up results	78
Figure 3.8	Book application all security group	79
Figure 3.9	Infrastructure services create NSX security group	80
Figure 3.10	Infrastructure services NSX security group verification	81
Figure 3.11	Infrastructure services resolve NTP service	81
Figure 3.12	Infrastructure services create new firewall rule	82
Figure 3.13	vRealize Log Insight NSX-vSphere overview	
Figure 3.14	Infrastructure services create new NSX DFW section	
Figure 3.15	Infrastructure services NSX DFW verification	
Figure 3.16	Book application create monitor session	
Figure 3.17	Book application processed monitor session	
Figure 3.18	Book application analyze monitor session	
Figure 3.19	Book application monitor session analysis results	
Figure 3.20) Book application monitor session clean up	87
Figure 3.21	Book application monitor session clean up results	87
Figure 3.22	2 Book application create access IP set	
Figure 3.23	Book application create web NSX security group	90
Figure 3.24	Book application create app NSX security group	91
Figure 3.25	5 Book application create DB NSX security group	
Figure 3.26	δ Book application security group verification	
Figure 3.27	⁷ Book application resolve Web to App service	
Figure 3.28	Book application resolve access to web service	
Figure 3.29	Book application resolve App to DB service	93
Figure 3.30) Book application services verification	94
Figure 3.31	Book application create Web to App NSX DFW rule	95
Figure 3.32	2 Book application create access to web NSX DFW rule	96
Figure 3.33	3 Book application create App to DB NSX DFW rule	97
Figure 3.34	4 Book application publish new NSX DFW rules	97
Figure 3.35	5 Book application NSX DFW rules verification	98
Figure 3.36	δ Book application block inbound rule	
Figure 3.37	⁷ Book application block outbound rule	100
Figure 3.38	Book application block rules verification	100
Figure 3.39	All applications monitor session verification	102
Figure 3.40	O All applications analyze monitor session verification	102

Figure 3.41 3-Tier application app destination - Web to App rule	103
Figure 3.42 All applications monitor session RuleID verification	103
Figure 3.43 Infrastructure services monitor session RuleID details verification	105
Figure 3.44 Book application monitor session access infrastructure services RuleID verification	105
Figure 3.45 Book application monitor session access to web servers RuleID verification	105
Figure 3.46 Book application monitor session accesss web servers RuleID details verification	106
Figure 3.47 Book app monitor session block to web servers RuleID details verification	106
Figure 3.48 Book app monitor session bock and allow to web RuleID verification	106
Figure 3.49 Book app monitor session allow Web/App RuleID details verification	107
Figure 3.50 Book app monitor session allow App/DB RuleID details verification	107
Figure 3.51 Book application web 1 functional verification	108
Figure 3.52 Book application web 2 functional verification	109
Figure 4.1 Book application all NSX security groups	117
Figure 4.2 Infrastructure services plan security	117
Figure 4.3 Infrastructure services select NSX security group	118
Figure 4.4 Infrastructure services filter micro-segments	118
Figure 4.5 Infrastructure services micro-segment Flow results	119
Figure 4.6 Infrastructure services recommended firewall rules	120
Figure 4.7 Book application web plan security	121
Figure 4.8 Book application select web NSX security group	121
Figure 4.9 Book application web filter micro-segments	122
Figure 4.10 Book application web micro-segment Flow results	123
Figure 4.11 Book application web services and Flows	124
Figure 4.12 Book application web recommended firewall rules	124
Figure 4.13 Book application web Flows incoming and outgoing SSH	125
Figure 4.14 Book application web incoming and outgoing Flows HTTP	126
Figure 4.15 Book application app plan security	128
Figure 4.16 Book application app NSX security group	128
Figure 4.17 Book application app filter micro-segments	129
Figure 4.18 Book application app micro-segment Flow results	130
Figure 4.19 Book application app incoming and outgoing Flows	130
Figure 4.20 Book application app recommended firewall rules	131

Figure 4.21 Book application app others_DC_physical Flows	132
Figure 4.22 Book application app incoming Flows SSH	132
Figure 4.23 Book application Web to App outgoing Flows HTTP	133
Figure 4.24 Book application App to DB outgoing Flow MySQL	134
Figure 4.25 Book application DB plan security	135
Figure 4.26 Book application DB NSX security group	135
Figure 4.27 Book application DB filter micro-segments	136
Figure 4.28 Book application DB micro-segment filter results	137
Figure 4.29 Book application DB incoming and outgoing Flows	137
Figure 4.30 Book application DB recommended firewall rules	138
Figure 4.31 Book application DB others_DC_physical Flows	139
Figure 4.32 Book application DB incoming Flow SSH	139
Figure 4.33 Book application DB incoming Flow MySQL	140
Figure 4.34 Book application all source - infrastructure access rule	142
Figure 4.35 Infrastructure Destination - Infrastructure access rule	143
Figure 4.36 Infrastructure allow - infrastructure access rule	143
Figure 4.37 Infrastructure applied to book application - infrastructure	3
access rule	144
Figure 4.38 Infrastructure access NSX DFW rule verification	144
Figure 4.39 Management source - management access rule	145
Figure 4.40 Management book application all destination -	
management access rule	
Figure 4.41 Management allow - management access rule	
Figure 4.42 Management applied to book application – management	1 4 7
access rule	
Figure 4.43 Management access NSX DF w rule verification	
Figure 4.44 Librarian source - web access rule	148
Figure 4.45 Book application web destination – web access rule	149
Figure 4.46 Librarian allow - web access rule	149
Figure 4.47 Librarian applied to web - web access rule	150
Figure 4.48 Book application web source - web to App rule	150
Figure 4.49 Book application app destination – web to App rule	
Figure 4.50 Book application web allow - web to App rule	
Figure 4.51 Book application applied to web and App - web to App ru	152 JIE
Figure 4.52 Book application app source - App to DB rule	153
Figure 4.55 BOOK application DB destination - App to DB rule	153 154
Figure 4.54 Book application app allow - App to DB rule	154
Figure 4.55 Book application applied to App and DB - App to DB rul	e154
Figure 4.56 BOOK application INSX DEVV rule verification	155

Figure 4.57	Book application disable block all rule	156
Figure 4.58	Flow monitoring infrastructure services RuleID verification	158
Figure 4.59	Infrastructure services NSX DFW RuleID verification	158
Figure 4.60	Flow monitoring web 1 RuleID verification	159
Figure 4.61	Flow monitoring web 2 RuleID verification	159
Figure 4.62	Management and librarian NSX DFW RuleID verification	159
Figure 4.63	Flow monitoring Web to App and App to DB RuleID	
	verification	.160
Figure 4.64	Book application Web, App, and DB RuleID verification	.160
Figure 4.65	Book application block all enable verification	161
Figure 4.66	Flow monitoring Web to Web block verification	162
Figure 4.67	Flow monitoring web access block unauthorized verification	163
Figure 4.68	Flow monitoring book application block unauthorized SSH	
	verification	.164
Figure 4.69	Book application web 1 functional verification	165
Figure 4.70	Book application web 2 functional verification	165

List of Tables

Table 1.1	Example layout	8
Table 1.2	Four monitoring rules	
Table 1.3	Review rules	12
Table 2.1	3-Tier application information	
Table 2.2	Infrastructure services information	
Table 2.3	3-Tier application NSX DFW rules example	19
Table 2.4	Windows client information	
Table 2.5	VMware product information	
Table 2.6	3-Tier application naming scheme layout	
Table 2.7	3-Tier application block and allow NSX DFW rules	
Table 2.8	3-Tier application NSX DFW rules documentation	41
Table 3.1	Book application information	
Table 3.2	Infrastructure information	71
Table 3.3	Application access information	71
Table 3.4	NSX DFW rules layout	73
Table 3.5	Windows client information	73
Table 3.6	VMware products information	74
Table 3.7	Naming scheme layout	74

Table 3.8	Infrastructure NSX DFW rule documentation	
Table 3.9	Infrastructure services NSX security group	78
Table 3.10	Book application NSX DFW documentation	
Table 3.11	Book application block rules layout	
Table 4.1	Book application information	
Table 4.2	Infrastructure services information	
Table 4.3	Application access information	
Table 4.4	Windows clients information	
Table 4.5	Mac client information	
Table 4.6	VMware products information	
Table 4.7	Naming scheme layout	115
Table 4.8	Infrastructure services NSX DFW rules layout	120
Table 4.9	Book application NSX DFW rules layout	125
Table 4.10	Book application web NSX DFW rules layout	
Table 4.11	Book application management NSX DFW rules layout	133
Table 4.12	Book application app NSX DFW rules layout	134
Table 4.13	Book application management access NSX DFW rules la	yout140
Table 4.14	Book application NSX DFW documentation	141

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 largescale 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, highavailability, 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 laver 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 laver 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 quest 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 microsegmentation. 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.

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

 Table 1.2
 Four monitoring rules

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.

	O -	HTTP - To Match Ru	CP Port 80 IleID 1010	→[`	/M 	
Name	RuleID	Source	Destination	Service	Action	Applied To
Name Allow Inbound Log	RuleID	Source	Destination SG-APP-ALL	Service Any	Action	Applied To SG-APP-ALL
Name Allow Inbound Log Allow Outbound Log	RuleID 1010 1011	Source Any SG-APP-ALL	Destination SG-APP-ALL Any	Service Any Any	Action Allow Allow	Applied To SG-APP-ALL SG-APP-ALL
Name Allow Inbound Log Allow Outbound Log Block Inbound Log	RuleID 1010 1011 1012	Source Any SG-APP-ALL Any	Destination SG-APP-ALL Any SG-APP-ALL	Service Any Any Any	Action Allow Allow Block	Applied To SG-APP-ALL SG-APP-ALL SG-APP-ALL

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 Ev	ent Types	Event Trends					
timestamp	hostname	vmw_ns	x_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.inter nal		1010	ТСР	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.

	O -	HTTP - To Match Ru	CP Port 80 IleID 1014	\ \	м	
Name	RuleID	Source	Destination	Service	Action	Applied To
Name Allow Access App	RuleID	Source	Destination SG-APP	Service Any	Action Allow	Applied To SG-APP
Name Allow Access App Allow Inbound Log	RuleID 1014 1010	Source Any Any	Destination SG-APP SG-APP-ALL	Service Any Any	Action Allow Allow	Applied To SG-APP SG-APP-ALL
Name Allow Access App Allow Inbound Log Allow Outbound Log	RuleID 1014 1010 1011	Source Any Any SG-APP-ALL	Destination SG-APP SG-APP-ALL Any	Service Any Any Any	Action Allow Allow Allow	Applied To SG-APP SG-APP-ALL SG-APP-ALL
Name Allow Access App Allow Inbound Log Allow Outbound Log Block Inbound Log	RuleID 1014 1010 1011 1012	Source Any Any SG-APP-ALL Any	Destination SG-APP SG-APP-ALL Any SG-APP-ALL	Service Any Any Any Any	Action Allow Allow Allow Block	Applied To SG-APP SG-APP-ALL SG-APP-ALL 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.



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.

Iddie I.J INEVIEW I UIES	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	Security Group SG-Contains	
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.

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			

3-Tier Application

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 applicationbased 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.

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

 Table 2.3
 3-Tier application NSX DFW rules example

- 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	Table 2.4	Window	s client	information
--------------------------------------	-----------	--------	----------	-------------

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

VMware Products

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.

💄 admin	
Administration	
Content Packs	
Help	
About	

Figure 2.5 NSX Manager general settings

From the next screen, select 'vSphere' under the 'Integration' section

●●● / I vSphere Integration ← → C ▲ Not Secure http					
vm Log Insight	Dashiboards Interactive Analytics	🔺 admin 🚍			
Management	vSphere Integration				
System Monitor	Pontos Sonioro m				
Access Control	voluter betvers ()				
Liser Alerte	+ ADD VCENTER SERVER				
Hosts					
Agents	SAVE				
Event Forwarding					
License					
late					
Integration					
vSphere vRealize Operations					
Wearze Operations					
Configuration					
General					
Time					
Authentication					
SMTP					
Archiving					
SSL					

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.

🔍 🕘 Vishnee Integration (Admin) x 📃				
← → C ▲ Not Secure https://192	168.0.140/admin/vsphere		x 🛛 🕫 🗄	
vm Log Insight			⊥ admin ≡	
Management System Monitor Custer Access Control User Alerts Hosts Agents Event Forwarding License	VSphere Integration vCenter Servers @ Hettorie vs disvibusizerse Uterran administratives.verver Peersond "Under Persond. Tegr Supforduct_Sp_relate2 Tetr consection	Collect (Conter Server overst, takis, and alarma () (EX) Instance and yourd Is and taking to Log Instight we ensite	×	
vSphere vRealize Operations	+ ADD VCENTER SERVER			
Configuration General Time	SAVE			

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).

vSphere Integration Ad	min () × / []							e
← → C A Not Secure Amps://	192.168.0.140/adm	Investing Analytics						·
ym Log Insignt Maragement System Koveter Course Alerta Noas Alerta Noas Alerta Swell	Cashoosh VSphel VCenter 5 Honnen Honnen Hannen Hannen Hannen Hannen Hannen Hannen Hannen Hannen Hannen	brendere Ankylei brendere An	Infe Version Exe 6.00 Exe 6.00	Build 4600344 4600344 4600344 4600344 4600344 4600344	E Configured Yes (LDP) Yes (LDP) Yes (LDP) Yes (LDP) Yes (LDP) Yes (LDP) Yes (LDP) Yes (LDP) Yes (LDP) Yes (LDP)	×	×	Lun =

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.

e e e 🖉 võphere Integration (Admin) x				
← → C A Not Secure https://192	168.0.140/admin/vsphere	☆ 🖸 😔 🗄		
vm Log Insight	Dashboards Interactive Analytics	≜ sdmin ≡		
Management System Monitor Cluster	vSphere Integration vCenter Servers ⊕			
Access Control User Alerts Hosts Agents Event Forwarding License Integration	Hostener vela Kavelina hitereti Collect. Center Server vents, taris, and ziema () X Denerme a dativisationelise.ukma izenat EXI host configued to solo tog to Log inopit Velamide Collect. Newsell: Teger Log Neglet. Mader () Teger Log Neglet. Mader () Teger Log Neglet. Mader ()			
vSphere				
vRealize Operations	+ ADD VCENTER SERVER			
Configuration General Time Authentication SMTP Archiving SSL	SAVE			

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.

• • • / 🖬 vSphere Integration Admin 🛛 × 🖉 vSphere We	Client × 🔤 VMware NSX Manager Virt	tael/×		Θ
← → C ▲ Not Secure https://192.168.0.120/index.ht	ni			☆ 🖬 🔗 🗄
NSX			IP: 192.168.0.120 Nome: nsxmgr-01a	Vanion: 6.3.0 Build 5007049 🔅 User: admin
2				
NSX M	anager Virtual Appliance Management			
(View Summary	Download Tech Support Log		
:	K Manage Appliance Settings	Backup & Restore		
	Manage vCenter Registration	Upgrade		

Figure 2.10 NSX Manager interface

From this screen, select Manage Appliance Settings

	Admin v × 🖉 vSpł	ere Web Client 🛛 × 🔤 VMware NSX Manager Virtual 🗴		Θ
← → C A Not Secure http	ps://192.168.0.120/h	me.html#/manage/settings/general	☆ 🖸	01
NSX		P: 192.168.0.120 \Vesion: 6.1 Norre: naverge61a User: ad	ua Build 500704 min	• •
Summary Manage				
SETTINGS General Network	Time Settings Specify NTP server b server.	Liteoring and the back constant by Lis required that the time on this visual appliance and NTP server should be in sync. It is recommended to use the same NTP server	ers Ed used by the S	80 80
SSL Certificates	NTP Server	0.pool.mp.org, 1.pool.mp.org		
Backups & Restore	Timezone	UTC		
Upgrade	Date/Time	05/08/2017 19:07:57		
COMPONENTS				
NSX Management Service	Syston Samer		Ed	-
	You can specify the IP	address or name of the syslog server that can be resolved using the above mentioned DNS Server(s).		
	System Server			
	Port			
	Protocol			
	FIPS Mode and TLS	settings	Ed	sie)
	A Changing FIPS m	de will restart NSX Manager Appliance automatically.		_
	FIPS mode	Disabled		
	Server	TLSv1,TLSv1.1,TLSv1.2		
	Client	TL9v1,TL9v1.1,TL9v1.2		
	Locale		Ed	8
	Below is the current in	cale information.		
	Locale	en-US		

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**.

• • • Visit-vSphere - Overview Visit	×				Θ
← → C ▲ Not Secure https://192.1	68.0.140/home?contextid=com.vmware.nsx-v&viewId=1				☆ 🖸 🖉 🗄
vm Log Insight	Dashboards Interactive Analytics				🛓 admin 😑
Custom Deshboerds	Latest 5 minutes of data v C				
> My Dashboards	hostname contains v Us	e TAB or ENTER to separate multi	ple terms		
> Shared Dashboards	+ ADD SUTER				
Content Pack Dashboards					
General	NSX for vSphere Edge system events by	y severity	NSX for vSphere in	nfrastructure problems	
VMware - NSX-vSphere					
NSX-vSphere - Overview	No results			No results	
NSX-vSphere - Infrastructure					
Logical Switch - Overview					
Logical Switch - Alerts	2025 2026 2027	2020 2020	20:26	2026 2027 2028	22:29
Logical Router - Overview -					
Logical Router - Alerts	Logical switch system events by severit	v	Logical switch aler	ts by hostname	
Bridging - Alerts	3	III official			
Distributed Firewall - Overview					
Distributed Firewall - Alerts	2			No results	
Distributed Firewall - Traffic					
Distributed Firewall - Hypervisor					
Distributed Firewall - Rule Data	2039 2039 2037 2038	20.39	20.35	2038 2037 2038	20.39
Load Balancer - General					
Load Balancer - Instance	Logical router events by severity	Logical router alert	s by hostname	Bridging alerts by hostname	9
Load Balancer - VIP					
Load Balancer - VIP HTTP(S)					
NSX-vSphere Edge - Overview	No results	No re	suits	No results	
NSX-vSphere Edge - Firewall					
N5X Cross-vCenter 6.2+					
Guest mirospection - Alerts	2025 2026 2027 2028 2029	2026 2026	2027 2028 2029	2025 2026 2027 1	12.20 20.20
> VMware - vSphere	Distributed firewall events by severity	Distributed firewall	alerts	Distributed firewall drop - re	eject actio

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

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

Table 2.6 3-Tier application naming scheme layout

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

- 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.

Sphere Web Client x										
← → C ▲ Not Secure https://192.168.0.111:9443/vsphere-client/?csp#extensionId%3Dcom.vmware.v										
vmware [,] vSphere Web Client										
Navigator II 192.168.0.120 Actions -										
A Networking & Secu 🕨 🔊	Networking & Secu > 🔊 Summary Monitor Manage									
NSX Managers										
**	System Events	Security Tags	Exclusion List	Domains	Grouping Objects	Users				
ap 192.168.0.120	ŧ.									
	Name 1 A VM Count									
	😥 ST-3T-DB 0									
	ST-3T-WEB					0				



Sphere Web Client ×											
\leftarrow \rightarrow C A Not Secure https://192.168.0.111:9443/vsphere-client/?csp#extensionId%3Dcom.vmware.w											
vmware [,] vSphere Web Client											
Navigator I	Navigator II 22.168.0.120 Actions -										
A Networking & Secu 🕨 🧐	Summary Monitor Manage										
NSX Managers											
E: 100 100 0 100	System Events Security Tags	Exclusion List Dom	ains Grouping Objects Users								
₩ 192.168.0.120 ²											
	Name 1 VM Count										
	ST-INFRA-NTP		0								

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**.

Edit Security Group								**
 ✓ 1 Name and description ✓ 2 Define dynamic membership 	Select objects Select objects t	to include hat should alway	vs be included in	this group, reç	ardless o	of whether they meet the	nembership criteria.	
 ✓ 3 Select objects to include ✓ 4 Select objects to exclude 	Object Type:	Security Tag	0.27	•			(O Eilbor	
✓ 5 Ready to complete	Available Objects		(d 3)			Selected Objects	Q Filter	
	@ ST-31	-APP				V ST-3T-WEB		
	@r ST-31	-DB				-		
	🗸 👸 ST-31	-WEB						
					•			
				3 items				1 items
						Back	Next Finish	Cancel

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.

••• Øvsphere Web Client ×										
← → C A Not Secure https://192.108.0.111:9443/vsphere-client/?csp#extensionid%3Dcom.vmware.v										
Navigator										
Networking & Secu Secu Secu Secu Secu Secular Secular	Summary Monitor Manage									
驛 192.168.0.120 >	System Events Security Tags	Exclusion List Domains G	rouping Objects Users							
	Security Group	Name	Static include m							
	IP Sets MAC Sets	SG-3T-ALL	SG-3T-APP, App01							
	Service Service Groups	☆ SG-3T-DB ☆ SG-3T-WEB	DB01 Web02, Web							

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.

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

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

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.
- Click on the Add rule (
) icon on the Book Application Section three more times to add the necessary rule instances.

т 🖺 Воо	🗄 Book Application (Rule 3 - 6) 📃 🖯 🕈 💕 🦯 🗙 클러 🖦 🋱									
© 3		* any	+ any	∘ any	Allow	Distributed Fire				
© 4		* any	* any	* any	Allow	Distributed Fire				
© 5		* any	* any	* any	Allow	Distributed Fire				
© 6		* any	- any	* any	Allow	Distributed Fire				

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 (\mathcal{J}) icon for the first rule Name.
- 2. Add name Allow Any to App Log and click Save.
- 3. Click on the Edit (\mathscr{J}) 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** (\mathscr{M}) 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** (\mathscr{M}) 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 (\mathcal{N}) 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 (\mathcal{N}) 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 (\checkmark) 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 (\mathscr{M}) 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.

C Last) Last publish operation succeeded 5/20/17, 10:24:25 PM CDT										
General	Jeneral Ethernet Partner security services										
+ ⊡ ×											
No.	Namo	Rule ID	Source	Destination	Service	Action	Applied To				
► 1 <u>5</u>	- 12 Ping Servers (Rule 1 - 2) 📃 C + 💕 🖌 x 🖃 🖦 🖡										
v 13	1 🔁 Book Application (Rule 3 - 6) 🛛 🔂 C 🕈 🗊 🖌 🖬										
© 3	Allow Any to App Log	1052	* any	💕 SG-3T-ALL	* any	Allow	🔐 SG-3T-ALL				
€4	Allow App to Any Log	1051	SG-3T-ALL	* any	* any	Allow	💕 SG-3T-ALL				
© 5	Block Any to App Log	1050	* any	SG-3T-ALL	* any	Block	💣 SG-3T-ALL				
© 6	Block App to Any Log	1049	💕 SG-3T-ALL	* any	* any	Block	SG-3T-ALL				

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, WebO1 and WebO2. 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**.

O O VSphere Web Client	X Bistributed Firewall - Role Dati X	θ
← → C ▲ Not Secure https://19	2.168.0.140/home?contextid=com.vmware.nsx-v&viewid=12&datePreset=LAST_5_MINUTES	☆ 🛛 H 🗄
vm Log Insight	Dashboards Interactive Analytics	🛦 admin 🗮
Custom Deshboards My Deshboards Shared Deshboards Content Pack Deshboards General 'Whware - NSX-sphere NSX-sphere - Verview	Latest 5 minutes of data v c NoteInter contains v wmc,ruc, Newel, Just contains v vumc,ruc, Newel, Just contains v vumc, Num, Newel, Just contains v	D
NSX-vSphere - Infrastructure Logical Switch - Overview Logical Switch - Alerts Logical Router - Overview Logical Router - Alerts Bridging - Alerts Distributed Firewall - Overview Distributed Firewall - Overview	Connections by rule ID over time) # 007
Unitability of Present - Aren's Distributed Firewall - Tartfit Distributed Firewall - Tartfit Distributed Firewall - Naperhoot Distributed Firewall - Naperhoot Load Balance - Jestime Load Balance - VP Hold Balance - VP NSX-ophene Eige - Drenwal NSX-ophene Eige - Trenwal NSX-ophene Eige - Christian Distributed - Christian - Christian NSX-ophene Eige - Christian	Bytes Source to Destination HyperVisor by ruleid Bytes Destination to S Bytes Destination to S Byte	eurce Hypervisor by ruleid at ea ea

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.
- 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.

	Ø vSphere Web Cli	ient ×	Count of events grouped	by m ×						Θ
é ⇒ G	A Not Secure	https://192.168.0.1	40/explorer/?existingC	hartQuery=%78°q	uery'%3A**%2C*st	artTimeMillis*%3A14953	385597893%2C"endTi	meMilis*%3A14953	85900979%2C*piql	6. 🕁 🚺 H 🗄
vm Loj	a Insight	Dast	hboards Interact	ive Analytics						上 admin 😑
2017-05-21 1	153:17 to 1158:20 (5 m)	inutes 3 seconds)	0	unt of events grouped					🖸 Snapoline	Add to Desitioned
									₩ 1061 ₩ 1092	
Court of eve	nts + grouped by	www.rax_frewell_soled +	Apply Paset						Ch	at Type • Be + ±
Metch all Metch all X vmw_n X text X text X text + ADD FILT	of the following liters: sx_firewall_ruleid	 exists contains contains 	✓ (dfwpktlogs ≥) ✓ (inet ≥)				2017-05-21 11:53:17:893	0 2017-05-21 11:58:2	0.979	
Events -	hostname	verse erer forwall minid	where the formula performal	www.ens.formal.err	www.exe formal dat	115 50 557 c	verse new formal dat port	ere - sort Newell-oil -	e appname	
2017-85-21 11:58:19.387	esscomp- 81a.vwilmo.inter nal	1051	UCP	172.16.128.11	192.168.0.211	192.168.0.211/123	123	76	+ event_type + hostneme • source	
2017-05-21 11:50:12.169	esxcomp- 01a.vwilno.inter nel	1852	TOP	172.16.128.11	172.16.128.11	172.16.128.11/2286	3385		+ vmw_nix_frewal_s vmw_nix_frewal_s vmw_nix_frewal_s vmw_nix_frewal_s	Sent_to_server
2017-05-21 11:58:12:162	esscomp- 83a.vwilmo.inter nal	1052	TOP	172.16.128.11	172.16.130.11	172.16.138.11/3386	3395		 vmw_nax_frewal_c 	×
2017-85-21 11:58:12.116	escosp- 02s.vellmo.inter nel	1452	TOP	172.16.118.12	172.16.128.11	172.16.128.11/00	53			
2017-85-21 11:58:12:116	esscomp- 82a.vwilno.ister nal	1052	TOP	172.16.118.12	172.16.128.11	172.16.128.11/88	88			
		1.000								

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.

vmw_nsx_firewall_dst_port: 80 26
vmw_nsx_firewall_dst_port: 3306 8
vmw_nsx_firewall_dst_port: 123 37

Figure 2.25 3-Tier application vRealize Log Insight destination ports

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

Events	Field Table Event	Types Event Trends				1 to 50 out (of 50+ events Columns (6 H
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 12:09:08.950	esxcomp- 02a.vwilmo.inter nal	1051	UDP	172.16.110.12	192.168.0.211	192.168.0.211/123	123
2017-05-21 12:09:07.173	esxcomp- 01a.vwilmo.inter nal	1051	Infrastructure Ser	172.16.110.11	192.168.0.211	192.168.0.211/123	123
2017-05-21 12:09:03.649	esxcomp- 03a.vwilmo.inter nal	1051	UDP	172.16.130.11	192.168.0.211	192.168.0.211/123	123
2017-05-21 12:09:01.249	esxcomp- 01a.vwilmo.inter nal	1051	UDP	172.16.120.11	192.168.0.211	192.168.0.211/123	123
2017-05-21 12:08:46.216	esxcomp- 01a.vwilmo.inter nal	1052	Web to App	172.16.110.11	172.16.120.11	172.16.120.11/80	80
2017-05-21 12:08:45.199	esxcomp- 01a.vwilmo.inter nal	1052	TCP	172.16.110.11	172.16.120.11	172.16.120.11/80	80
2017-05-21 12:08:44.227	esxcomp- 01a.vwilmo.inter nal	1052	TCP Ext. to Web	192.168.0.99	172.16.110.11	172.16.110.11/80	80
2017-05-21 12:08:44.227	esxcomp- 01a.vwilmo.inter nal	1052	TCP App to DB	172.16.120.11	172.16.130.11	172.16.130.11/3306	3306
2017-05-21 12:08:43.259	esxcomp- 01a.vwilmo.inter nal	1052	TCP	172.16.110.12	172.16.120.11	172.16.120.11/80	80
2017-05-21 12:08:42.182	esxcomp- 01a.vwilmo.inter nal	1052	TCP	172.16.110.12	172.16.120.11	172.16.120.11/80	80
2017-05-21 12:08:41.933	esxcomp- 02a.vwilmo.inter nal	1052	TCP	172.16.110.12	172.16.120.11	172.16.120.11/80	80
2017-05-21 12:08:41.193	esxcomp- 01a.vwilmo.inter nal	1052	TCP	172.16.110.11	172.16.120.11	172.16.120.11/80	80
2017-05-21 12:08:41.192	esxcomp- 01a.vwilmo.inter nal	1052	TCP	172.16.110.12	172.16.120.11	172.16.120.11/80	80
2017-05-21 12:08:40.968	esxcomp- 02a.vwilmo.inter nal	1052	TCP Ext. to App	192.168.0.99	172.16.110.12	172.16.110.12/80	80

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**.

+ Add Service		?
An Application can be v protocol that is transmit	viewed as a tag on network traffic of specified ted through specified port or set of ports.	
Name: *	SV-INFRA-NTP	
Description:		
Protocol:	UDP	
Destination ports:	123	
	e.g.: 7001-7020,7100,8000-9000	
Advanced options	5	
Enable inheritance	e to allow visibility at underlying scopes	
	OK Cano	xel

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 applicationspecific 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.

+ Add Service		?
An Application can be protocol that is transmi	viewed as a tag on network traffic of specified tted through specified port or set of ports.	
Name: #	SV-3T-HTTP	
Description:		
Protocol:	TCP	
Destination ports:	80	
	e.g.: 7001-7020,7100,8000-9000	
Advanced option	s	
Enable inheritan	ce to allow visibility at underlying scopes	
	OK Cano	cel

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.

+ Add Service		?
An Application can be v protocol that is transmit	iewed as a tag on network traffic of specified ted through specified port or set of ports.	
Name: *	SV-3T-MYSQL	
Description:		
Protocol:	TCP	
Destination ports:	3306	
	e.g.: 7001-7020,7100,8000-9000	
Advanced options	5	
Enable inheritanc	e to allow visibility at underlying scopes	
	OK Cano	xel

Figure 2.29 3-Tier application add MySQL service

12. Click **OK**.

Verify all services are configured.

Name 1 v	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** (**4**) 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.

Allow Access	Infra - Specify Source					?
Select one or m	ore objects for the source fie	eld of the firewall r	ule			
Object Type:	Security Group	•				
	Q, 3t				Q Filter	•
Available Objects			Selected	Objects		
🗸 💣 SG-3T	-ALL		 ✓ I 	SG-3T-ALL		
💣 SG-3T	-APP	Ę				
SG-3T	-DB					
G-3T	-WEB	4				
		4 items				1 items
New Security G	roup					
Advanced op	otions					
Negate sour	ce					
					ОК	Cancel

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.

Allow Access	Infra - Specify Destination						?
Select one or m	ore objects for the destination	n field of th	e firewall r	ule			
Object Type:	Security Group	•)				
	Q SG-INFRA)		1	Q Filter	-
Available Objects				Selected C	Dbjects		
🖌 💣 SG-IN	FRA-NTP			✓ I	SG-INFRA-NTF	>	
		1 items					1 items
New Security G	roup						
Advanced op	otions						
Negate Dest	ination						
						ОК	Cancel

Figure 2.32 Infrastructure destination - infrastructure access rule

- 12. Click on the Edit (\checkmark) 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 (\mathscr{J}) icon for the new rule Action.
- 16. Click on the Log radio button and click Save.

Allow Access Inf	ra - Edit Action
Action: Direction: Packet Type:	Allow • In/Out • Any •
Tag:	
Log: Comments:	• Log O not log
	Save Cancel

Figure 2.33 3-Tier application allow - infrastructure access rule
- 17. Click on the Edit (\checkmark) 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

Allow Access	Infra - Specify Applied To					?		
Specify containe	ers on which this rule will be applie	d.						
Apply this rul	Apply this rule on all clusters on which Distributed Firewall is installed.							
Apply this rul	Apply this rule on all the Edge gateways.							
(For Edges w	ith version 6.1.0 and higher)							
Select one or me	ore objects for the applied to field o	f the firewall r	ule					
Object Type:	Security Group	•						
	Q. 3t				Q Filter	-		
Available Objects			Selected Obje	ects				
🖌 💣 SG-3T	-ALL		🖌 💣 🛛 SG	9-3T-ALL				
💣 SG-3T	-APP							
SG-3T	-DB							
SG-3T	-WEB							
	4 ite	ms				1 items		
New Security G	roup							
					ок	Cancel		

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.

last) Last publish operation succeeded 5/21/17, 4:00:13 PM CDT							
General	Seneral Ethernet Partner security services							
Ф 🗋 Ж	* # # % 🖟 🕅 * *						-	
No.	Name	Rule ID	Source	Destination	Service	Action	Applied To	
► 🗄	Ping Servers (Rule 1 - 2)					🖂 C 🕈	$\beta^* \times \times \oplus \oplus \mathbb{N}$	
v 🖫	Book Application (Rule 3 - 7)					🖂 C 🕈	$\beta^* \times \times \oplus \oplus \mathbb{I}_{+}$	
© 3	Allow Access Infra	1053	f SG-3T-ALL	SG-INFRA-NTP	SV-INFRA-NTP	Allow	SG-3T-ALL	
⊗4	Allow Any to App Log	1052	* any	SG-3T-ALL	* any	Allow	💣 SG-3T-ALL	
© 5	Allow App to Any Log	1051	f SG-3T-ALL	* any	* any	Allow	SG-3T-ALL	
Ø 6	Block Any to App Log	1050	* any	SG-3T-ALL	* any	Block	💣 SG-3T-ALL	
© 7	Block App to Any Log 🧳	1049	🔗 SG-3T-ALL	* any	* any	Block	💣 SG-3T-ALL	

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.

Allow Access	App - Specify Source					?
Select one or mo	ore objects for the source	field of the firewall rule				
Object Type:	Security Group	· · ·				
	Q. 3T			0	ξ Filter	-
Available Objects			Selected Object	ots		
SG-3T	-ALL		🖌 💣 SG-	-3T-WEB		
SG-3T	-APP					
SG-3T	-DB					
✓ 💣 SG-3T	-WEB	4				
	4 items	Copy -			1 items	Copy 🗸
New Security G	roup					
Advanced op	tions					
Negate source	be					
					ОК	Cancel

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

- 10. Click on the Edit (\mathscr{J}) 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.

Any Access A	pp - Specify Destination				?
Select one or m Object Type:	Security Group	n field of the firewal	rule	Q Filter	•
Available Objects			Selected Objects		
GG-3T	-ALL		🖌 💣 SG-3T-WEE	В	
SG-3T	-APP				
💣 SG-3T	-DB				
🖌 💣 SG-3T	-WEB				
		4 items			1 items
New Security G	roup				
Advanced op	otions				
Negate Dest	ination				
				ОК	Cancel

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

- 13. Click on the Edit (\checkmark) 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.

Any Access A	pp - Specify Service						?
Select one or m	nore objects for the service t	ield of the firew	vall rule				
Object Type:	Service	•					
	Q SV-3T				Q Filt	ər	•
Available Objects				Selected Objects			
🖌 🗋 SV-3T	-HTTP			🖌 📄 SV-3T-HTT	ſP		
SV-3T	-MYSQL						
			4				
		2 items					1 items
New Service							
Advanced o	ptions						
Negate Desi	tination						
						ок	Cancel

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

- 16. Click on the Edit (\mathscr{J}) icon for the new rule Action.
- 17. Click on the **Log** radio button and click **Save**.

Any Access App	Edit Action	?
Action:	Allow	
Direction:	In/Out 🔹	
Packet Type:	Any I	
Tag:		
Log:	Log Do not log	
Comments:		
	Save Cancel	

Figure 2.39 3-Tier application allow - web access rule

- 18. Click on the Edit (\checkmark) 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.

Any Access A	pp - Specify Applied To					?		
Specify contain	Specify containers on which this rule will be applied.							
Apply this ru	Apply this rule on all clusters on which Distributed Firewall is installed.							
Apply this ru	le on all the Edge gateways.							
(For Edges v	vith version 6.1.0 and higher)							
Select one or m	ore objects for the applied to field of the	firewall ru	le					
Object Type:	Security Group)						
	Q SG-3T)			Q Filter	-		
Available Objects			Selected	Objects				
GG-3T	-ALL		✓ I	SG-3T-WEB				
💣 SG-3T	-APP							
G-3T	-DB							
🗸 💣 SG-3T	-WEB							
	4 items					1 items		
New Security G	roup							
					ОК	Cancel		

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.

Web to App -	Specify Source					?
Select one or m	ore objects for the source fie	eld of the firewall ru	le			
Object Type:	Security Group	•				
	Q 3T				Q Filter	•
Available Objects			Selected	Objects		
💣 SG-3T	-ALL		 ✓ @ 	SG-3T-WEB		
💣 SG-31	-APP	4				
💣 SG-31	-DB					
🖌 🖉 SG-31	-WEB	4				
		4 items				1 items
New Security G	roup					
Advanced op	otions					
Negate sour	ce					
					ок	Cancel

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.

Web to App - S	Specify Destination				?
Select one or m	ore objects for the destinatio	n field of the firewa	all rule		
Object Type.	Q 31			Q Filter	•
Available Objects			Selected Objects		
💣 SG-3T	-ALL		🖌 💣 SG-3T-	-APP	
🖌 💣 SG-31	-APP				
💣 SG-31	-DB				
💣 SG-3T	-WEB	4			
		4 items			1 items
New Security G	roup				
Advanced op	otions				
Negate Dest	ination				
					K Cancel

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

- 10. Click on the Edit (\checkmark) 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.

Web to App - S	Specify Service					?
Select one or m	ore objects for the service	e field of the firew	vali rule			
Object Type:	Service	•				
	Q SV-31				Q Filter	•
Available Objects				Selected Objects		
🖌 📄 SV-3T-	-HTTP			🖌 📋 SV-3T-HTTP		
SV-3T	-MYSQL					
			4			
		2 items				1 items
New Service						
Advanced op	otions					
Negate Dest	ination					
					ок	Cancel

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

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

Web to App - Edit	Action	?
Action:	Allow	•
Direction:	In/Out	•
Packet Type:	Any	,
Tag:		
Log:	💿 Log	Do not log
Comments:		
		Save Cancel

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

- 15. Click on the Edit (\checkmark) 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.

Web to App - S	Specify Applied To					?		
Specify contain	Specify containers on which this rule will be applied.							
Apply this ru	le on all clusters on which Distributed Fi	rewall is in	nstalled.					
Apply this ru	le on all the Edge gateways.							
(For Edges v	vith version 6.1.0 and higher)							
Select one or m	ore objects for the applied to field of the	firewall ru	ıle					
Object Type:	Security Group							
	Q 3T)			Q Filter	•		
Available Objects			Selected	Objects				
💣 SG-31	-ALL		✓ (SG-3T-WEB				
🖌 🔐 SG-31	-APP		< ₽	SG-3T-APP				
💣 SG-3T	-DB							
🖌 🔐 SG-31	-WEB							
	4 items					2 items		
New Security G	roup							
					ОК	Cancel		

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

App to DB Rule

- 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.

App to DB - S	pecify Source					?
Select one or m	ore objects for the source field of the	firewall rule				
Object Type:	Security Group	•				
	Q 31	\supset			Q Filter	-
Available Objects			Selected	Objects		
💣 SG-31	-ALL		✓ @	SG-3T-APP		
🖌 💣 SG-31	APP					
💣 SG-31	-DB					
💣 SG-31	-WEB	4				
	4 item	s				1 items
New Security G	roup					
Advanced op	otions					
Negate sour	ce					
					ОК	Cancel

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.

App to DB - Sp	pecify Destination								?
Select one or m Object Type:	Security Group	n field of the firev	wall rule			6	Filter		- -
Available Objects	<u>(•)</u>		Se	elected (Objects	9			
💣 SG-3T	ALL		*	1	SG-3T-DB				
💣 SG-3T	-APP	Ę							
🖌 💣 SG-3T	-DB		5						
SG-3T	-WEB		-						
		4 items						1 iten	ıs
New Security G	roup								
Advanced op	otions								
Negate Dest	ination								
							ок	Cano	el

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

- 10. Click on the Edit (\checkmark) 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.

App to DB - S	pecify Service				?
Select one or m Object Type:	OPE OBJECTS for the service field	Id of the firewall rul	3	Q Filter	•
Available Objects			Selected Objects		
SV-3T	-HTTP		🖌 📋 SV-3T-MYSQI	L	
✓ 📋 SV-3T	-MYSQL				
		2 items			1 items
New Service					
Advanced op	ptions				
Negate Dest	tination				
				ОК	Cancel

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

- 13. Click on the Edit (\mathscr{J}) icon for the new rule Action.
- 14. Click on the **Log** radio button and click **Save**.

App to DB - Edit	Action		?
Action:	Allow	•	
Direction:	In/Out	•	
Packet Type:	Any		
Tag:			
Log:	 Log 	Do not log	
Comments:			
		Save	Cancel

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

- 15. Click on the Edit (\checkmark) 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.

App to DB - S	pecify Applied To						?
Specify contain	ers on which this rule will	be applied.					
Apply this ru	le on all clusters on which	Distributed Fire	wall is ir	nstalled.			
Apply this ru	le on all the Edge gateway	/S.					
(For Edges v	vith version 6.1.0 and high	er)					
Select one or m	ore objects for the applied	to field of the fi	irewall ru	le			
Object Type:	Security Group	•					
	Q. 3T					Q Filter	•
Available Objects				Selected	Objects		
😭 SG-31	Γ-ALL			< ₫	SG-3T-APP		
🖌 💣 SG-31	F-APP		4-	< ₫	SG-3T-DB		
🗸 💣 SG-31	F-DB						
💣 SG-31	r-web						
		4 items					2 items
New Security G	iroup						
						ОК	Cancel

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.

🕼 Last	Last publish operation succeeded 5/21/17, 11:59:58 PM CDT								
General	General Ethernet Partner security services								
0 🗇 🛛	= = 8 G \ V								
No.	Name	Rule ID	Source	Destination	Service	Action	Applied To		
► 🗄	Ping Servers (Rule 1 - 2)								
v 🔄	▼ 📴 Book Application (Rule 3 - 11) 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日 日								
© 3	Allow Access Infra	1053	ピ SG-3T-ALL	SG-INFRA	SV-INFRA-NTP	Allow	ピ SG-3T-ALL		
© 5	Any Access App	1056	< any	SG-3T-WEB	SV-3T-HTTP	Allow	SG-3T-WEB		
Ø 6	Web to App	1055	SG-3T-WEB	SG-3T-APP	SV-3T-HTTP	Allow	e SG-3T-WEB SG-3T-APP		
© 7	App to DB	1054	∯ SG-3T-APP	@ SG-3T-DB	SV-3T-MYSQL	Allow	e SG-3T-DB SG-3T-APP		
08	Allow Any to App Log	1052	* any	ef SG-3T-ALL	* any	Allow	₽ SG-3T-ALL		
© 9	Allow App to Any Log	1051	🔮 SG-3T-ALL	* any	* any	Allow	∯ SG-3T-ALL		
© 10	Block Any to App Log	1050	* any	@ SG-3T-ALL	* any	Block	ef SG-3T-ALL		
© 11	Block App to Any Log	1049	ピ SG-3T-ALL	* any	* any	Block	ピ SG-3T-ALL		

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.
- 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.
- 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.

vmw_nsx_firewall_client_to_server
76
kist
'alue Is '123'
_nsx_firewall_dst_port'

Figure 2.54 vRealize Log Insight filter field table by NTP

Events	Field Table Event T	ypes 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 22:40:37.252	esxcomp- 01a.vwilmo.inter nal	1053	UDP	172.16.110.11	192.168.0.211	192.168.0.211/123	123
2017-05-21 22:40:35.456	esxcomp- 02a.vwilmo.inter nal	1053	UDP	172.15.110.12	192.168.0.211	192.168.0.211/123	123
2017-05-21 22:40:35.275	esxcomp- 01a.vwilmo.inter nal	1053	UDP	172.16.120.11	192.168.0.211	192.168.0.211/123	123
2017-05-21 22:40:33.136	esxcomp- 03a.vwilmo.inter nal	1053	UDP	172.16.130.11	192.168.0.211	192.168.0.211/123	123



v 13	Book Application (Rule 3 - 10	1)				C d	⊧ø⁄×≕=⊧⊾
© 3	Allow Access Infra	1053	SG-3T-ALL	SG-INFRA	SV-INFRA-NTP	Allow	💣 SG-3T-ALL

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.
- 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.

Add Filter: Field Exists Field Does Not Exist	
Field Exists Field Does Not Exist	
Field Does Not Exist	
Value Is '80'	
Value Is Not '80'	

Figure 2.57 vRealize Log Insight filter field table by HTTP

Events F	Field Table Event T	ypes 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.inter nal	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.inter nal	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.inter nal	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.inter nal	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.inter nal	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.inter nal	1056	TCP	192.168.0.99	172.16.110.12	172.16.110.12/80	80



© 4	Any Access App	1056	* any	SG-3T-WEB	SV-3T-HTTP	Allow	SG-3T-WEB
Ø 5	Web to App	1055	SG-3T-WEB	SG-3T-APP	SV-3T-HTTP	Allow	Contraction of the second seco

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.
- 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.

mw_nsx_firewall_dst_port	vmw_nsx_firewall_client_to_serve
Add Filter:	
Field Exists	
Field Does Not E	xist
Value Is '3306'	
Value Is Not '330	6'
Highlight When V	/alue ls '3306'
Colorize By 'vmw	_nsx_firewall_dst_port'

Figure 2.60 vRealize Log Insight filter field table by MySQL

Events	Field Table Event T	ypes 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 23:16:41.133	esxcomp- 01a.vwilmo.inter nal	1054	TCP	172.16.120.11	172.16.130.11	172.16.130.11/3306	3306

Figure 2.61 vRealize Log Insight filtered field table - MySQL

@ 6	App to DB	1054	SG-3T-APP	SG-3T-DB	SV-3T-MYSQL	Allow	GG-3T-DB
							SG-3T-APP

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.

last p	B Last publish operation succeeded 5/22/17, 12:04:37 AM CDT							
General	General Ethernet Partner security services							
Ф 🗓 х								
No.	Neme	Rule ID	Source	Destination	Service	Action	Applied To	
► 🖪	Ping Servers (Rule 1 - 2)					C C	ΦØ/×≕⇒⊾⊾	
v B	Book Application (Rule 3 - 11)					🖂 C ⁱ	Φ Ø / × Β Β β.	
© 3	Allow Access Infra	1053	😭 SG-3T-ALL	SG-INFRA	SV-INFRA-NTP	Allow	SG-3T-ALL	
© 4	Block Web to Web	1057	SG-3T-WEB	SG-3T-WEB	* any	Block	SG-3T-WEB	
© 5	Any Access App	1056	^ any	SG-3T-WEB	SV-3T-HTTP	Allow	ef SG-3T-WEB	
© 6	Web to App	1055	SG-3T-WEB	SG-3T-APP	SV-3T-HTTP	Allow	SG-3T-WEB	
© 7	App to DB	1054	SG-3T-APP	SG-3T-DB	SV-3T-MYSQL	Allow	SG-3T-DB	
© 8	Allow Any to App Log	1052	* any	🔮 SG-3T-ALL	* any	Allow	ef SG-3T-ALL	
© 9	Allow App to Any Log	1051	SG-3T-ALL	* any	* any	Allow	ef SG-3T-ALL	
@ 10	Block Any to App Log	1050	* any	@ SG-3T-ALL	* any	Block	ef SG-3T-ALL	
© 11	Block App to Any Log	1049	💣 SG-3T-ALL	* any	* any	Block	SG-3T-ALL	

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

Events Field Table	Event Types Eve	nt Trends					1 to 30 out of 30 events C	olumns (5 Hidden) + Sort: Newest F
timestamp	hostname	vmw_nsx_firewall_action	vmw_nsx_frewall_ruleid	vmw_nsx_firewall_protocol	vmw_nsx_frewall_arc	vmw_nsx_firewal_dst	vmw_nsx_firewall_dst_ip_port	vmw_nsx_frewail_dst_port
2017-05-22 08:08:37.519	esxcomp- @la.vwilno.internal	CROP	1050	TOP	192.168.0.99	172.16.130.11	172.16.138.11/22	22
2017-05-22 08:08:32.144	essconp- 01a.vwilno.internal	CROP	1050	TOP	192.168.0.99	172.16.120.11	172.16.128.11/22	22
2017-05-22 08:08:31.495	esxcomp- 03a.vwilno.internal	CROP	1050	TOP	192.168.0.99	172.16.130.11	172.16.138.11/22	22
2017-05-22 08:06:28.505	esxcomp- @3a.vwilno.internal	CROP	1050	TOP	192.168.0.99	172.16.130.11	172.16.138.11/22	22
2017-05-22 08:06:26.459	esscomp- 02s.vwilno.internal	CROP	1058	тор	192.168.0.99	172.16.110.12	172.16.110.12/22	22
2017-05-22 08:06:26.136	esscomp- @1a.vwilmo.internal	CROP	1058	Block All	192.168.0.99	172.16.120.11	172.16.128.11/22	22
2017-05-22 08:06:23.136	esscomp- @1a.vwilno.internal	CROP	1058	TOP	192.168.0.99	172.16.120.11	172.16.128.11/22	22
2817-05-22 08:06:28.394	exxcomp- 02a.vwilno.internal	CROP	1058	тор	192.168.0.99	172.16.110.12	172.16.110.12/22	22
2817-05-22 08:08:28.344	excomp- @1a.vwilno.internal	CROP	1058	тор	192.148.0.99	172.16.110.11	172.16.110.11/22	22
2817-05-22 08:06:17.422	excomp- 02a.vwilno.internal	CROP	1058	тор	192.168.0.99	172.16.110.12	172.16.110.12/22	22
2817-05-22 08:06:14.430	excomp- @1a.vwilno.internal	CROP	1058	тор	192.168.0.99	172.16.110.11	172.16.110.11/22	22
2817-05-22 08:06:11.348	excomp- @1a.vwilno.internal	CROP	1058	тор	192.168.0.99	172.16.110.11	172.16.110.11/22	22
2817-05-22 08:02:41.877	eaxcomp- 02a.vwilno.internal	CROP	1857	Block Web to We	172.16.118.12	172.16.110.11	172.16.110.11/80	80
2817-05-22 08:02:38.284	eaxcomp- 01a.vwilno.internal	CROP	1057	TCP TCP	172.16.118.11	172.16.110.12	172.16.110.12/88	80

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.

Books Collection X Books Collection X	1	-		×
← → C ① 172.16.110.11			*	0
3 Tier app				
Server Chain • Web01 • DB01 • DB01 • EE • DB01 • EE •				
DATA				
Ital Title Author [1] The Martian Audy Weir [2] The HHGTG Douglas Adams				

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-O1a (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

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	

Table 3.1 Book application information

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 a	ccess information
10010 010	/ (pplication a	00000011101111011110111

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.

Name	Source	Destination	Service	Action	Applied To			
Infrastructure Services Section								
Allow 3T-App to NTP	3T-App	NTP	-	Allow	3T-App			
Book Application Sec	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			

 Table 3.4
 NSX DFW rules layout

- 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

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

 Table 3.6
 VMware products information

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

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 Naming scheme layout

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

Start New Session				×
Select VM, vNICs to start monitoring flows				
Session Name: * INFRA MONITOR				
Select Source:				
Object Type: Virtual Machine	•			
Q Filter			Q Filter	•
Available Objects		Selected Objects		
✓ 🗗 DB01	A	🖌 🗗 DB01		
HRHIS-DB-01a		🖌 🗗 App01		
✓		🖌 🗗 Web02		
AD-DNS-01a		🖌 🔂 Web01		
✓ in App01	::			
✓ → Web01				
🗗 HL7-01a				
PACS-DB-01a				
	70 iéorro			d literano.
	20 nems			+ nems
			ОК	Cancel

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.

Flow Monitoring				_
Dashboard Details By S	Service Live Flow Configuration Applic	ation Rule Manager		
NSX Manager: 192.168.0 Session: INFRA MONITO Deleto Sessi	0.120 v A 16 Flows	Collection Complete I Analyze	Start New Sess	sion
Flow Details:				
View Flows Firewall	rules			
@ Actions			R.	13
Direction	Source	Destination	Service	
OUT	172.16.110.11	192.168.0.211	UDP : 123	*
OUT	172.16.120.11	192.168.0.211	UDP : 123	
IN	192.168.0.99	172.16.110.11	TCP: 80	
OUT	172.16.120.11	172.16.130.11	TCP: 3306	
IN	172.16.110.11	172.16.120.11	TCP: 80	
OUT	172.16.110.11	172.16.120.11	TCP : 80	
OUT	172.16.110.12	172.16.120.11	TGP: 80	::
IN	192.168.0.99	172.16.110.12	TCP: 80	
IN	172.16.110.12	172.16.120.11	TCP: 80	
IN	172.16.120.11	172.16.130.11	TCP : 3306	
OUT	172.16.110.12	192.168.0.211	UDP : 123	
OUT	172.16.130.11	192.168.0.211	UDP : 123	
IN	192.168.0.99	172.16.130.11	TCP : 22	T.
IN	192.168.0.99	172.16.120.11	TCP : 22	
			16 iter	ms

Figure 3.3 Infrastructure services processed monitor session

Analyze Monitored Session – Infrastructure Services

9. Click on Analyze.

NSX Manager: 192.168.0.120 -			
Session: INFRA MONITOR	4	16	
Delete Session	Source	Flows	Collection Complete 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.

→ C A Not Secure https://discurre/https//discurre/https//discurre/https//discurre/https//discurre/https	/192.168.0.111:9443/vsphe	re-client/?csp#extensionId%3Dcc	om.vmware.vshield.plugin.common.networkse	curity.navigator.networkSecurity.netFlowMonitoring.ap 🛧	ВН
n ware [,] vSphere Web Clie			🖑 i Administra	ongsso.vvilmo.internal + i Help + i Q. Starth	
Mixarare Vispelare Web Differ Haman Sharara Haman Sharara Di Sh	Int Me Fore Monitoring Fore Monitoring Desticate Deals 95 Service NOX Manager (102.166.0.120 Destication) Service (102.166.0.120 Desticatio	Lan Pare Configuration Aquitation	Accession Contraction Contraction	PROSONALIZATION (Provide the set of the set	alan alan alan alan alan alan alan alan
	OUT OUT IN IN IN	 Webb2 Webb1 192,168.0.99 192,168.0.99 192,168.0.99 192,168.0.99 192,168.0.99 	값) MTP-01a 값) MTP-01a 값) Wee01 값) Wee02 값) Wee02 값) Wee02	2 Services 2 Services 2 Services 4 Services 4 Services 2 Services	
				13 its	2015

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**.

• • • / Ø vSphere Web Client	O Ø visibhere Web Client x				
← → C ▲ Not Secure https:/	/192.168.0.111:9443/vsp	here-client/?csp#extension/d%3Dc	om.vmware.vshield.plugin.common.networkse	curity.navigator.networkSecurity.netFlowMon	toring.ap 🏠 🛄 H
vmware [,] vSphere Web Clie	ont n ≣		🖒 i Administra	meggsso.vvilmo.internal + i Heip + i (Q. Search
Navigator II	Flow Monitoring				2
(4 Home) 🔊	Dashboard Details By Serv	ice Live Flow Configuration Applica	tion Rule Manager		_
Networking & Security	NSX Manager: 192.168.0.12	0 +			0
R Dashboard					
@ installation	Session: INFRA MONITOR	4 13	0		Start New Session
Cogical Switches	Dekte Session	Source Fizee	Analysis Complete		40
Nax Eoges	Flow Details:				3
in SpoolGuard	New Flows Firewall rule	16			x av
Service Definitions	(3) Actions			Processe	i View 🔹 😵 📑 👌
Service Composer	Direction	Source	Destination	1 . Service	3
* Tools	IN	192.168.0.99	Gb App01	2 Services	
E Flow Monitoring	INTRA	/8 Web02	(D App01	4 Services	
Activity Monitoring	INTRA	Create Firewall Rule	db App01	4 Services	
Ligg Endpoint Monitoring	IN	192.168.0.99	(D) DB01	2 Services	
Networking & Security Inventory	INTRA	At App01	- DB01	4 Services	
I NSX Managers >	OUT	App01	(E) NTP-01a	2 Services	_
	OUT	At D801	db NTP-01a	2 Services	
	OUT	A Web02	AD NTP-01a	2 Services	
	OUT	@t Web01	dt NTP-01a	2 Services	
	IN	192,168.0.99	/ib Web01	2 Services	
	IN	192.168.0.99	(b) Web01	4 Services	
	IN	192,168.0.99	/ib Web02	4 Services	
	IN	192.168.0.99	(E) Web02	2 Services	
					13 items

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.

Flow Monitoring	Flow Monitoring				
Dashboard Details By Service Liv	ve Flow Configuration	Application Rule Manager			
NSX Manager: 192.168.0.120 +					
Session: INFRA MONITOR + Delete Session	4 Source	13 O Flows Analysis Comple		Start New Session	
Flow Details:					
View Flows Firewall rules					
(a) Actions				Processed View 🔹 📡	
Direction	Source	14	Destination	Service	
OUT	App01		A NTP-01a	2 Services	
OUT	曲 DB01		A NTP-01a	2 Services	
OUT	Web01		A NTP-01a	2 Services	
OUT	ළි Web02		母 NTP-01a	2 Services	

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

Add Security Group	🔗 Add Security Group			
 1 Name and description 2 Define dynamic membership 	Select objects to include Select objects that should always be included in this group, re	regardless of whether they meet the membership criteria.		
 3 Select objects to include 4 Select objects to exclude 5 Ready to complete 	Object Type: Logical Switch	Q Filter •		
	Availabo Objects	slacked objects V @ Web_Tar V @ Nop_Tar V @ DB_Tar DB_Tar S Backed objects S Stems		
		Back Next Finish Cancel		

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-O1a 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.

Add Security Group							
 ✓ 1 Name and description ✓ 2 Define dynamic membership 	Select objects to include Select objects that should always be included in this group, regardless of whether they meet the membership criteria.						
 3 Select objects to include 4 Select objects to exclude 5 Ready to complete 	Object Type: Virtua	Machine	•			Q Filter	
 Treaty to complete 	Availado Copesa Vertical Copesa PARC-B-01a PARC-B-01a PARC-B-01a PARC-B-01a PARC-B-01a PARC-B-01a PARC-B-01a PARC-B-01a PARC-B-01a PARC-B-01a PARC-B-01a PARC-B-01a	11a EB-02a a	• 		Second Opera		1 items
					Back	Next Finish	Cancel

Figure 3.9 Infrastructure services create NSX security group

15. Click Finish.

Flow Monitoring				
Dashboard Details By Service Liv	e Flow Configuration	Application Rule Manager		
NSX Manager: (192.168.0.120 •				
Session: INFRA MONITOR V	4 Source	13 Since Analysis Comple	te	Start New Session
Flow Details: View Flows Flowsal fules				
Actions Processed View				
Direction	Source	1.	Destination	Service
OUT	🔗 SG-3T-ALL		SG-INFRA-NTP	2 Services

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.

Flow Monitoring					
Dashboard Details By Service Live Flow Configuration Application Rule Manager					
NSX Manager: 192.168.0.120	9				
Session INFRA MONITOR					
Flow Detalls:					
View Flows Firewall rules					
🛞 Actions Processed View 🔹 😵 🕞					
Direction	Source		Destination	Service	1.4
OUT	ef SG-3T-ALL		© [®] SG-INFRA-NTP	MTP	

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**.

New Firewall	Rule	
Name	Allow App to Infra	1
Source	ger SG-3T-ALL	
		Select
Destination	SG-INFRA-NTP	
		Select
Service	MTP	
		Select
Applied To	SG-3T-ALL	
		Select
Action	Allow Block Reject	
Direction	Out	
	ОК	Cancel

Figure 3.12 Infrastructure services create new firewall rule
Publish DFW Rules - Infrastructure Services

Procedure

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

Flow Monitoring						
Dashboard Details By Service Live Flow Configura	ation Application R	ule Manager				
NSX Manager: 192.168.0.120						
Session: INFRA MONITOR V Delete Session Source	13 Flows	Analysis Complete				Start New Session
Flow Details:						
View Flows Firewall rules						
Last update operation succeeded 5/22/17, 9:22:59	PM CDT					
🖋 🛪 📰 🖦 🔤 Publish						
Name Source	Destination	Service	Applied To	Action	Log	Tag
Allow App to Infra	SG-INFRA-NTP	○ NTP	SG-3T-ALL	Allow	Do not log	

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.

Firewall Publish	
Section name: Insert above:	Infrastructure Services Default Section La
	OK Cancel

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.

Firewall								
Configura	tion Saved Configurations Set	Ings						
NSX Mana	ger: 192.168.0.120 v							
🕲 Last	Last publish operation succeeded 61/2/17, 4:16:52 PM CDT							
General	Ethernet Partner security se	rvices						
$\Phi \odot x$	* # # 18 🖳 🕅 🖓 🕈 -							- 1
No.	Name	Rule ID	Source	Destination	Service	Action	Applied To	Direction
► 🖪	Ping Servers (Rule 1 - 2)						⊟ C + Ø ,	× mas ta
v 🖪	Infrastructure Services (Rule 5)						⊟ C + Ø /	× er s. %
© 5	Allow App to Infra	1075	SG-3T-ALL	SG-INFR	MTP NTP	Allow	SG-3T-ALL	Out
► 🖪	Default Section Layer3 (Rule 6 -	8)						× st s. S.

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.

- 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

Start New Session					×
Select VM, vNICs to start monitoring flows					
Session Name: * APP MONITOR					
Select Source:					
Object Type: Virtual Machine	•				
Q Filter)			Q Filter	•
Available Objects			Selected Objects		
🗗 DW-DB-01a	*		🖌 🔂 Web01		
HRHIS-WEB-01a			🖌 👘 Web02		
B NTP-01a	::	-	🖌 🔂 App01		
B EMR-DB-01a			🖌 🔂 DB01		
PACS-WEB-01a					
Di CWS-01a					
EMR-DMZ-WEB-02a					
✓ 🗗 DB01	_				
	20 items				d literano.
	20 items				4 items
				OK	Canaal
				UK	

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.

Flow Monitoring				
Dashboard Details By	y Service Live Flow Configuration Applicat	ion Rule Manager		
NSX Manager: 192.16 Session: APP MONITO Delete Se	8.0.120 - DR - Source Flows	Collection Complete <u>Analyze</u>	Start N	lew Session
Flow Details: View Flows Firew	all rules			
(a) Actions				
Direction	Source	Destination	Service	
OUT	172.16.120.11	192.168.0.211	UDP : 123	
OUT	172.16.110.12	172.16.120.11	TCP : 80	
IN	192.168.0.99	172.16.110.12	TCP : 80	
IN	172.16.110.12	172.16.120.11	TCP: 80	
OUT	172.16.110.11	172.16.120.11	TCP : 80	
OUT	172.16.120.11	172.16.130.11	TCP : 3306	
IN	172.16.110.11	172.16.120.11	TCP: 80	
IN	192.168.0.99	172.16.110.11	TCP : 80	
IN	172.16.120.11	172.16.130.11	TCP : 3306	
IN	192.168.0.99	172.16.130.11	TCP : 22	
IN	192.168.0.99	172.16.120.11	TCP : 22	
IN	192.168.0.99	172.16.110.12	TCP : 22	
IN	192.168.0.99	172.16.110.11	TCP : 22	
				13 items

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.

Flow Monitoring	Flow Monitoring			
Dashboard Details By Service	Live Flow Configuration Application Rule Manager			
NSX Manager: 192.168.0.120				
Session: APP MONITOR	ession: APP MONITOR • 4 10 Start New Session. Data Starts Source Fixes Analysis Complete			
Flow Details:				
View Flows Firewall rules				
@ Actions			Processed View	
Direction	Source	Destination	Service	
OUT	@ App01	A NTP-01a	2 Services	
IN	192.168.0.99	B Web02	4 Services	
INTRA	B Web02	合 App01	4 Services	
IN	192.168.0.99	B Web01	4 Services	
INTRA	Web01	App01	4 Services	
INTRA	App01	2b DB01	4 Services	
IN	192.168.0.99	@ DB01	2 Services	
IN	192.168.0.99	App01	2 Services	
IN	192.168.0.99	B Web02	2 Services	
IN	192.168.0.99	B Web01	2 Services	
			10 items	

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-O1a; they are already covered with a prior rule. As before, highlight these flows select **Hide Records**.

Flow Monitoring			
Dashboard Details B	y Service Live Flow Configuration Ap	dication Rule Manager	
NSX Manager: 192.16	88.0.120 🔍		
Session: APP MONITOR • 4 10 Start New Session Dates Session: Same From Analysis Complete			
Flow Details:			
View Flows Firew	vall rules		
Actions			Processed View 🛛 🔻 🕒
Direction	Source	Destination	1 A Service
INTRA	Web01	App01	4 Services
IN	192.168.0.99	طا App01	2 Services
INTRA	jip Web02	∄i App01	4 Services
IN	192.168.0.99	급) DB01	2 Services
INTRA	@ App01	创 DB01	4 Services
OUT	App01	D NTP-01a	2 Services
IN	192.168.0.99 Hide R	ecords 2 Web01	4 Services
IN	192.168.0.99	∄ Web01	2 Services
IN	192.168.0.99	创 Web02	4 Services
IN	192.168.0.99	创 Web02	2 Services
			10 Hame
			To herea

Figure 3.20 Book application monitor session clean up

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

Flow Monitoring				
Dashboard Details By Serv	ce Live Flow Configuration Application Rule Manag	er		
NSX Manager: 192.168.0.12	NSX Manager: 192.168.0.120 •			
Session: APP MONITOR Delete Session	ession: APP MONITOR			
Flow Details:				
View Flows Firewall rule	s			
@ Actions			Processed View	
Direction	Source	Destination	Service	
IN	192.168.0.99	B Web02	4 Services	
INTRA	创 Web02	App01	4 Services	
INTRA	급) Web01	台 App01	4 Services	
IN	192.168.0.99	@ Web01	4 Services	
INTRA	App01	@ D801	4 Services	
IN	192.168.0.99	DB01	2 Services	
IN	192.168.0.99	App01	2 Services	
IN	192.168.0.99	B Web02	2 Services	
IN	192.168.0.99	街 Web01	2 Services	

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 WebO1 and WebO2. 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.

🕂 New IP Set	(1	D
Scope:	Global	
Name: s	IP-3T-ACCESS	
Description:		
IP Addresses: >	s 192.168.0.99	
	eg:192.168.200.1.192.168.200.1/24	
	192.168.200.1-192.168.200.24	
Enable inher	itance to allow visibility at underlying scopes	
	OK Cancel	J

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.

- 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

💣 Add Security Group								₩
 1 Name and description 2 Define dynamic membership 	Select objects Select objects	to include hat should always	s be included in t	nis group, reg	ardless o	of whether they meet the m	embership criteria.	
 3 Select objects to include 4 Select objects to exclude 5 Readu to complete 	Object Type:	Logical Switch	Q Filter	•			Q. Filter	•)
 A Result to Complete 	Available Object	Tier Tier MZ254_SITE1 NFRA99_SITE1 ROD10_SITE1 ROD20_SITE1 RANSIT100_SITE Tier	51	8 items		Selected Objects		1 items
						Back	lext Finish	Cancel

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, WebO1 and WebO2.

- 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 AppO1 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

Add Security Group		**
 ✓ 1 Name and description ✓ 2 Define dynamic membership 	Select objects to include Select objects that should always be included in this group, reg	egardless of whether they meet the membership criteria.
 3 Select objects to include 4 Select objects to exclude 5 Readu to complete 	Object Type: Logical Switch C Filter	Q Filter
 Complete 	Availabil Objects	Selected Objects
	o nems	i items
		Back Next Finish Cancel

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.

- 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

💣 Add Security Group								₩
 1 Name and description 2 Define dynamic membership 	Select objects Select objects t	to include hat should always	s be included in thi	s group, reg	ardless o	of whether they meet the	e membership criteria.	
 2 Define dynamic membership 3 Select objects to include 4 Select objects to exclude 5 Ready to complete 	Object Type: Available Object V (2) APP_1 (2) (S_D) (2) (S_D) (3) (S_D) (3) (S_D) (3) (S_D) (4) (S_D) (4) (S_D) (5) (S_D)	Logical Switch (Iler or ZZ54_SITE1 HFRA99_SITE1 ROD20_SITE1 ROD20_SITE1 TIEr	Q Filter	•		Selected Objects Selected Obj	Q Filter	•) 3 items
						Back	Next Finish	Cancel

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.

Flow Monitoring			
Dashboard Details By Service Live Flow C	Configuration Application Rule Manager		
NSX Manager: 192.168.0.120			
Session: APP MONITOR	10 Rate Analysis Complex		Start New Session
Flow Details:			
View Flows Firewall rules			
@ Actions			Processed View 🔹 📡 🖽
Direction Source		Destination	Service
INTRA SG-3T	r-WEB	ef SG-3T-APP	4 Services
IN IP-3T-	ACCESS	ef SG-3T-WEB	4 Services
INTRA 💣 SG-3T	F-APP	🔮 SG-3T-08	4 Services

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

@ Actions			Processed View 🔹 😵
Direction	Source	Destination	Service
INTRA	er SG-3T-WEB	C SG-3T-APP	4 Services
IN	P-3T-ACCESS	C SG-3T-WEB	Services Details
INTRA	er SG-ST-APP	💣 SG-3T-DB	Protoco: TCP Port: 60 Service: Protoco: 6 Convection Server to View Co Protoco: Convection Server to View Co Protoco: 6 Convection Server to View Co Protoco: 6 Convection Server to View Co Protoco: 6 Convection Server to View Convection Protoco: 6 Convection Protoco: 6 Convection Server to View Convection Protoco: 6 Convection
			Resolve Services Replace with any

Figure 3.27 Book application resolve Web to App service

• Access to the Web Servers is communicating on TCP 80

(Actions			Processed View 🔹 💥 🖽
Direction	Source	Destination	Service
INTRA	SG-3T-WEB	eff SG-3T-APP	4 Services
IN	P-3T-ACCESS	ſ₽ SG-3T-WEB	4 Services
INTRA	SG-3T-APP	@ [®] SG-3T-DB	Services Details
			Protocol: TCP
			Port: 80
			Services: Horizon 6 Connection Server to Vicev Co

Figure 3.28 Book application resolve access to web service

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

@ Actions				Processed View 💌 🌾 📑
Direction	Source	Destination	Service	
INTRA	P SG-3T-WEB	ef SG-3T-APP	4 Services	
IN	IP-3T-ACCESS	SG-3T-WEB	4 Services	
INTRA	SG-3T-APP	SG-3T-DB	4 Services	@-
			Services Details Protocol: TCP Port: 3396 Services: Win 2003 - RPC, DCC Win - RPC, DCCM, El MySQL Resolve Services	XM. EPM, DRSUA

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 (0) 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.

Flow Monitoring				
Dashboard Details By Service Liv	e Flow Configuration	Application Rule Manager		
NSX Manager: 192.168.0.120				
Session: APP MONITOR	4 Source	10 S Flows Analysis Complet	lte	Start New Session
Flow Details:				
View Flows Firewall rules				
@ Actions				Processed View 💌 📡 📑
Direction	Source		Destination	Service
INTRA	P SG-3T-WEB		SG-3T-APP	П НТТР
IN	P-3T-ACCESS		SG-3T-WEB	🚔 НТТР
INTRA	💣 SG-3T-APP		ef SG-3T-DB	MySQL



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.

- 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**.

Name	Allow Web to App	
Source	SG-3T-WEB	Select
Destination	SG-3T-APP	Select
Service	ШНТТР	Select
Applied To	SG-3T-WEB	Select
Action	Allow Block Reject	
Direction	In/Out 🔹	

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**.

IP-3T-ACCESS	Select
SG-3T-WEB	Select
НТТР	Select
SG-3T-WEB	Select
Allow Block Reject	
	SG-3T-WEB

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.

New Firewall	Rule	
Name	Allow App to DB]
Source	SG-3T-APP	
		Select
Destination	SG-3T-DB	
		Select
Service	MySQL	
		Select
Applied To	SG-3T-APP	1
	<pre> SG-3T-DB </pre>	Select
Action	Allow Block Reject	
Direction	In/Out 🔹	
	ок	Cancel

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.

Flow Monitoring	Flow Monitoring							
Dashboard Details By	Dashboard Details By Service Live Flow Configuration Application Rule Manager							
NSX Manager: (192.168.0.120 •)								
Session: APP MONITOF	R V 4	10 Flows	Analysis Complete				Start New Session	
Flow Details:								
View Flows Firewal	I rules							
Last update operat	ion succeeded 5/28/17, 9:5	0:57 AM CDT						
/×==== D, P	ublish							
Name	Source	Destination	Service	Applied To	Action	Log	Tag	
Allow Web to App	SG-3T-WEB	SG-3T-APP	☐ HTTP	SG-3T-WEB	Allow	Do not log		
Allow Librarian to App	P-3T-ACCESS	SG-3T-WEB	CHTTP	SG-3T-WEB	Allow	Do not log		
Allow App to DB	SG-3T-APP	₽ SG-3T-DB	MySQL	@ SG-3T-APP @ SG-3T-D8	Allow	Do not log		

Figure 3.34 Book application publish new NSX DFW rules

- 8. Verify that the rule looks accurate.
- 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.

Firewall									
Configura	onfiguration Saved Configurations Settings								
NSX Mana	ger: 192.168.0.120 •								
@ Last	publish operation succeeded 6/12/	17, 4:32:32 PM CDT						0	
General	Ethernet Partner security s	ervices							
0 D 3									
No.	Name	Rule ID	Source	Destination	Service	Action	Applied To	Direction	
► 🗄	Ping Servers (Rule 1 - 2)						⊡ C + Ø /	х ⇒ в. %.	
▶ 🖪	Infrastructure Services (Rule 5)						- C + 💕 /	x∋t≞ife	
v 🔁	Book Application (Rule 6 - 8)							×∋ s. ≱.	
@ 6	Allow Librarian to App	1078	IP IP-3T-ACCE	SG-3T-WEB	☐ HTTP	Allow	ef SG-3T-WEB	In	
© 7	Allow Web to App	1077	SG-3T-WEB	SG-3T-APP	HTTP HTTP	Allow	SG-3T-WEB SG-3T-APP	In/Out	
08	Allow App to DB	1076	SG-3T-APP	ef SG-3T-DB	MySQL	Allow	ef SG-3T-APP ef SG-3T-DB	In/Out	
► 🖪	- 🖪 Default Section Layer3 (Rule 9 - 11) 🔤 🖒 🔶 👘 🖌 🗴 🛼								

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:

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

 Table 3.11
 Book application block rules layout

First Block Rule Configuration

- 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.

Action:	Block	•	
Direction:	In/	•	
Packet Type:	Any	•	
Tag:			
Log:	 Log 	O not log	
Comments:			
	L		

Figure 3.36 Book application block inbound rule

- 11. Click on the Edit (\checkmark) 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 (\swarrow) icon for the second rule Name.
- 16. Add name Block App to Any Log and click Save.
- 17. Click on the Edit (\checkmark) 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 (\mathscr{N}) icon for the second rule Action.

- 21. Change the Action to **Block**.
- 22. Click on the **Log** radio button and click **Save**.

Block App to Any	y Log - Edit Action
Action:	Block -
Direction:	In/Out 🔹
Packet Type:	Any
Tag:	
Log: Comments:	Log Do not log
	Save Cancel

Figure 3.37 Book application block outbound rule

- 23. Click on the Edit (\checkmark) 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.
- 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.

C Last ;	Lest publis operation succeeded 5/28/17, 10:22:32 AM COT							
0 () ×								
No.	Name	Rule ID	Source	Destination	Service	Action	Applied To	
► 🖪	Ping Servers (Rule 1 - 2)					E C	+ # / × = = 1	
v Es	Infrastructure Services (Rule 3)				- C	+ # / × == = 1	
© 3	Allow App to Infra	1058	💣 SG-3T-ALL	SG-INFRA-NTP	MTP NTP	Allow	SG-3T-ALL	
v E	Book Application (Rule 4 - 8)					e e	• ø / × ⇒ ≞ ‰	
© 4	Allow Librarian to App	1061	IP-3T-ACCESS	₫ SG-3T-WEB	☐ HTTP	Allow	SG-3T-WEB	
© 5	Allow Web to App	1060	SG-3T-WEB	SG-3T-APP	☐ НТТР	Allow	SG-3T-WEB	
© 6	Allow App to DB	1059	∯ SG-3T-APP	∰ SG-3T-DB	MySQL	Allow	eff SG-3T-APP eff SG-3T-DB	
€7	Block Any to App	1063	* any	மீ SG-3T-ALL	 any 	Block	SG-3T-ALL	
Ø 8	Block App to Any	1062	iể SG-3T-ALL	* any	* any	Block	SG-3T-ALL	

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.

Flow Monitoring					
Dashboard Details By Service Li	ve Flow Configuration Application Rule Manager				
NSX Manager: 192.166.0.120 •					
Session: VERIFY MONITOR VERIFY MONITOR	5 18 Collection Con	molete Analyze	Star	t New Session	
Flow Details:					
View Flows Firewall rules					
@ Actions				7 B	
Direction	Source	Destination	Service		
IN	172.16.120.11	192.168.0.211	UDP : 123	*	
OUT	172.16.120.11	192.168.0.211	UDP : 123		
IN	172.18.110.11	192.168.0.211	UDP : 123		
OUT	172.16.110.11	192.168.0.211	UDP : 123		
IN	172.16.110.12	192.168.0.211	UDP : 123		
OUT	172.18.110.12	192.168.0.211	UDP : 123		
IN	172.18.130.11	192.168.0.211	UDP : 123		
OUT	172.16.130.11	192.168.0.211	UDP : 123		
IN	192.168.0.58	172.16.110.12	TCP:80		
IN	192.168.0.58	172.16.110.11	TCP: 80		
IN	192.168.0.99	172.16.110.12	TCP: 80		
OUT	172.16.110.12	172.16.120.11	TCP: 80		
IN	172.16.110.12	172.16.120.11	TCP: 80		
OUT	172.16.120.11	172.16.130.11	TCP: 3306		
OUT	172.16.110.11	172.16.120.11	TCP: 80		
IN	172.16.110.11	172.16.120.11	TCP:80	v	
				18 items	

Figure 3.39 All applications monitor session verification

Analyze Monitored Session – Infrastructure Services

10. Click on Analyze.

NSX Manager: 192.168.0.120 +			
Session: VERIFY MONITOR	5	18	
Delete Session	Source	Flows	Collection Complete 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.

Flow Details:			
View Flows Fire	vali rules		
			Processed Mary
Cog Acuons	A	Desident des	Processed view
INTRA	Status	A NTD.019	2 Senine
INTRA	Ch Maked	Ch ATTO OTA	2 Convince
INTRA	E Webo	E NTP-01a	2 devices
INTRA	gi webuz	di NIP-ota	2 Services
INTRA	실g DB01	创 NTP-01a	2 Services
IN	192.168.0.58	台 Web02	4 Services
IN	192.168.0.58	යි Web01	4 Services
IN	192.168.0.99	创 Web02	4 Services
INTRA	部 Web02	创 App01	4 Services
INTRA	광 App01	급) DB01	4 Services
INTRA	∄ Web01	ැඩ App01	4 Services
IN	192.168.0.99	创 Web01	4 Services
			11 items

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.

@ Actions			Processed View	• % B
Direction	Source	Destination	Service	RuleID
INTRA	B App01	D NTP-01a	2 Services	1058
INTRA	B Web01	创 NTP-01a	2 Services	1058
INTRA	B Web02	A NTP-01a	2 Services	1058
INTRA	@ DB01	NTP-01a	2 Services	1058
IN	192.168.0.58	B Web02	4 Services	1063
IN	192.168.0.58	Web01	4 Services	1063
IN	192.168.0.99	B Web02	4 Services	1061
INTRA	@ Web02	曲 App01	4 Services	1060
INTRA	B App01	合 DB01	4 Services	1059
INTRA	B Web01	App01	4 Services	1060
IN	192.168.0.99	创 Web01	4 Services	1061

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.

- 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**.

Rule Details							
Section Name:		Infras	Infrastructure Services				
Rule Id:		1058	1058				
Rule Name:		Allow	App to Infra				
Rule Type:		LAYE	R3				
Rule Direction:		Out	Out				
Source	Destination		Service	Action	Applied To		
ピ SG-3T-ALL	SG-INFRA	·	MTP	Allow	SG-3T-ALL		

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.

INTRA	B Web01	B NTP-01a	2 Services	1058
INTRA	P Web02	命 NTP-01a	2 Services	1058
INTRA	B DB01	nTP-01a	2 Services	1058
INTRA	App01	B NTP-01a	2 Services	1058

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.

IN	192.168.0.58	B Web01	4 Services	1063
IN	192.168.0.58	B Web02	4 Services	1063
IN	192.168.0.99	凾 Web02	4 Services	1061
IN	192.168.0.99	御 Web01	4 Services	1061

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 WebO1 and WebO2, 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.

Rule Details					×		
Section Name:		Book	Book Application				
Rule Id:		1061					
Rule Name:		Allow	/ Librarian to App	I			
Rule Type:		LAYE	LAYER3				
Rule Direction:		In	In				
Source	Destination		Service	Action	Applied To		
IP-3T-ACCE	💣 SG-3T-WE	в	🛗 HTTP	Allow	SG-3T-WEB		

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

Rule Details					×
Section Name:		Book	Application		
Rule Id:		1063			
Rule Name:		Block Any to App			
Rule Type:		LAYER3			
Rule Direction:		In/Out			
Source	Destination		Service	Action	Applied To
* any	💣 SG-3T-ALI	-	∗ any	Block	💣 SG-3T-ALL

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

IN	192.168.0.58	ው Web01		4 Services	1063
IN	192.168.0.58	曲 Web02	Block to App	4 Services	1063
IN	192.168.0.99	卧 Web02	Allow to Ann	4 Services	1061
IN	192.168.0.99	曲 Web01	Allow to App	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.

Rule Details					×		
Section Name:		Book	Book Application				
Rule Id:		1060					
Rule Name:		Allow	Web to App				
Rule Type: LAY		LAYE	AYER3				
Rule Direction: In/O		In/Ou	n/Out				
Source	Destination		Service	Action	Applied To		
ピ SG-3T-WEB	ピ SG-3T-AP	Ρ	HTTP HTTP	Allow	SG-3T-WEB		

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**.

Rule Details					×		
Section Name:		Book	Book Application				
Rule Id:		1059					
Rule Name:		Allow	App to DB				
Rule Type:		LAYE	AYER3				
Rule Direction: In/Ou		n/Out					
Source	Destination		Service	Action	Applied To		
ピ SG-3T-APP	ピ SG-3T-DB		MySQL	Allow	SG-3T-APP SG-3T-DB		

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 microsegmentation, 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, 3600 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

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

 Table 4.1
 Book application information

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 applicationbased 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
	1111000110	01101100	

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

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

Table 4.7 Naming scheme layout

Create Security Group - Infrastructure Services

- 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 Groups**.

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.

Sphere Web Client	×		
\leftrightarrow \rightarrow C \land Not Secure $ $ https:	//192.168.0.111:9443/vspher	e-client/?csp#extensionId%3Dc	om.vmware.vshield.plugin.group
vmware [®] vSphere Web Cli	ent † ≣		
Navigator I	192.168.0.120 Actions -		
< Networking & Secu 🕨 🗐	Summary Monitor Manage		
NSX Managers	Sustem Events Security Tags	Evolution List Domains Grouping O	hinete Lleere
騨 192.168.0.120 >	System Events Security Tags	Exclusion List Domains Grouping O	ojects Osers
		+ / ×	
	Security Group	Name	Static include member
	IP Sets	💣 SG-3T-ALL	SG-3T-APP, SG-3T-WEB Show All
	MAC Sets	SG-3T-APP	App01
	Service	💣 SG-3T-DB	DB01
	Service Groups	P SG-3T-WEB	Web02, Web01

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.

- 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 Groups.
- 4. Select the **SG-INFRA-NTP** security group from the list.
- 5. Leave the **Duration** at **Last 1 day**.
- 6. Click Analyze.

Plan Security	×
Entity	
Security Groups	▽
SG-INFRA-NTP	▽
Duration	
🕖 Last 1 day	\bigtriangledown
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.

y VLAN/VXLAN ⊽	
Group By	Also show groups for
✓ by VLAN/VXLAN	Physical
by Application	V Other Virtual
by Tier	Internet
by Subnet	None
by Folder	
by Cluster	
by VM	
by Port	
by Security Tag	
by Security Group	
by IPSet	
by VPC	

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.

Services and Flows for SG-3T-ALL X							
Services in this group	External Services Accessed	Flows (Incoming and Outgoing)	Recommended Firewall Rules				
0	3	7	1				
Recommended Firewall Rules			:				
SOURCE DES	TINATION SERVICES	PROTOCOLS	ACTION				
SG-3T-ALL SG-I	IFRA-NTP 123 [ntp]	UDP	ALLOW				

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	curity Group SG-Contains	
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.

- 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 Groups.
- 4. Select the **SG-3T-WEB** security group from the list.
- 5. Leave the Duration at Last 1 day.
- 6. Click Analyze.

Plan Security	×
Entity	
Security Groups	⊽
SG-3T-WEB	▽
Duration	
🕖 Last 1 day	∇
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.

Micro-Segments	
by VLAN/VXLAN ⊽	
Group By	Also show groups for
V by VLAN/VXLAN	Physical
by Application	V Other Virtual
by Tier	Internet
by Subnet	None
by Folder	
by Cluster	
by VM	
by Port	
by Security Tag	
by Security Group	
by IPSet	
by VPC	

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.

Services and Flows for SG-3T-WEB X								
Services in this group	External Services Accessed	Flows (Incoming and Outs	going)	Recommended Firewall Rul	85			
4	2	8	8					
Filters	Services in this group				:			
Search Properties or Metrics Q	4 Flows							
All (1)	Service Endpoints	Count of Flow	Sum of Bytes	MAX of Traffic Rate				
Destination 17	Web01 (172.16.110.11) port: 22 [ssh]	1	No Data	44 bps				
Metrics 6	Web02 (172.16.110.12) port: 80 [http]	1	No Data	864 bps				
Service and Port	Web01 (172.16.110.11) port: 80 [http]	1	No Data	623 bps				
Type 5	Web02 (172.16.110.12) port: 22 [ssh]	1	No Data	35 bps				

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.

Services and Flows for SG-3T-WEB X								
Services in this group	Exte	ernal Services Accessed	Flows (Incoming and Outgoing)	Recommended Fire	wall Rules			
4		2	8	4	_			
Recommended Firewall Rules					:			
SOURCE	DESTINATION	SERVICES	PROTOCOLS	ACTION				
Others_DC Physical	SG-3T-WEB	80 [http], 22 [ssh]	TCP	ALLOW				
SG-3T-WEB	SG-INFRA-NTP	123 [ntp]	UDP	ALLOW				
SG-3T-WEB	SG-3T-ALL	80 [http]	TCP	ALLOW				
SG-3T-WEB	SG-3T-APP	80 [http]	TCP	ALLOW				

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.

Flows	Incoming and Outgoing)			:
2 filter	ed Flows	@ May 30, 10:13 -	May 31, 10:13 Expand All	Collapse All
	192.168.0.58 -> 172.16.110.12(Web02) [port:22]			
	Bytes			
	May 30, 10:30 Flow Type Port Dst Subnet Netwo Flow Type Diff Host [9 more] 22 [s 172.16.110.0 Diff Host [9 more] 22 [s	Src IP 192.168.0.58	Dst IP 172.16.110.12	_
	192.168.0.58 -> 172.16.110.11(Web01)[port:22]			
	Bytes			
	Dst Subnet Netwo Flow Type Port 172.16.110.0 Diff Host [9 more] 22 [s	Src IP 192.168.0.58	Dst IP 172.16.110.11	

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**.

Flows	(Incoming and Outgoing)				:
4 filter	red Flows			ୁଣା May 30, 10:13 - May 3	31, 10:13 Expand All	Collapse All
	192.168.0.99 -> 172.	16.110.11(Web01) [por	rt:80]			
	Bytes					1
	May 30, 10:30					
	Dst Subnet Netwo 172.16.110.0	Flow Type Diff Host [9 more]	Port 80 [http]	Src IP 192.168.0.99	Dst IP 172.16.110.11	
	192.168.0.99 -> 172.	16.110.12(Web02) [por	rt:80]			
	Bytes					b
	May 30, 10:30					
	Dst Subnet Netwo 172.16.110.0	Flow Type Diff Host [9 more]	Port 80 [http]	Src IP 192.168.0.99	Dst IP 172.16.110.12	
	172.16.110.11(Web0)1) -> 172.16.120.11(A;	op01) [port:80]			
	Bytes					14 M
	May 30, 10:30					
	Dst Subnet Netwo 172.16.120.0	Src Subnet Netwo 172.16.110.0	Flow Type Dst VM [10 more]	Port 80 [http]	Src IP 172.16.110.11	
	172.16.110.12(Web0	02) -> 172.16.120.11(Ap	op01) [port:80]			
	Bytes					1. A
	May 30, 10:30			1	1	
	Dst Subnet Netwo 172.16.120.0	Src Subnet Netwo 172.16.110.0	Flow Type Diff Host [10 more	Port 80 [http]	Src IP 172.16.110.12	

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.

- 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 Groups.
- 4. Select the **SG-3T-APP** security group from the list.
- 5. Leave the Duration at Last 1 day.
- 6. Click Analyze.

Entity	
Security Groups	⊽
SG-3T-APP	⊽
Duration	
🕖 Last 1 day	⊽

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.

Micro-Segments	
by VLAN/VXLAN ⊽	
Group By	Also show groups for
V by VLAN/VXLAN	Physical
by Application	V Other Virtual
by Tier	Internet
by Subnet	None
by Folder	
by Cluster	
by VM	
by Port	
by Security Tag	
by Security Group	
by IPSet	
by VPC	

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.

Services and Flows for SG-3T-APP X							
Services in this group	External Services Accessed	Flows (Incoming and Outg	oing)	Recommended Firewall Rule	s		
2	2	5		6			
Filters	Services in this group				:		
Search Properties or Metrics Q	3 Flows						
All 61	Service Endpoints	Count of Flow	Sum of Bytes	MAX of Traffic Rate			
Destination 17	App01 (172.16.120.11) port: 80 [http]	2	181.7 KB	567 bps			
Metrics 6	App01 (172.16.120.11) port: 22 [ssh]	1	9.5 KB	44 bps			

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.

ervices and Flows for 5G-3	п-арр				×
Services in this group	E	External Services Accessed	Flows (Incoming and Outgoing)	Recommended Firewa	all Rules
2		2	5	6	
Recommended Firewall Rules					:
SOURCE	DESTINATION	SERVICES	PROTOCOLS	ACTION	
SG-3T-APP	SG-3T-ALL	3306 [mysql]	TCP	ALLOW	
SG-3T-APP	SG-3T-DB	3306 [mysql]	TCP	ALLOW	
5G-3T-ALL	SG-3T-APP	80 [http]	TCP	ALLOW	
SG-3T-APP	SG-INFRA-NTP	123 [ntp]	UDP	ALLOW	
SG-3T-WEB	SG-3T-APP	80 [http]	TCP	ALLOW	
Others_DC Physical	SG-3T-APP	22 [ssh]	TCP	ALLOW	

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

Services and Flows for SG-	Services and Flows for SG-3T-APP X						
Services in this group	External Serv	ices Accessed	Flows (Incoming and Outgoing)	Recommended Firewall Rules			
2	2		5	6			
Recommended Firewall Rules					:		
SOURCE	DESTINATION	SERVICES	PROTOCOLS	ACTION			
SG-3T-APP	SG-3T-ALL	3306 [mysql]	TCP	ALLOW			
SG-3T-APP	SG-3T-DB	3306 [mysql]	TCP	ALLOW			
SG-3T-ALL	SG-3T-APP	80 [http]	TCP	ALLOW			
SG-3T-APP	SG-INFRA-NTP	123 [ntp]	UDP	ALLOW			
SG-3T-WEB	SG-3T-APP	80 [http]	TCP	ALLOW			
Others_DC Physical	SG-3T-APP	22 [ssh]	TCP	ALLOW			

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.

Flows (Incoming and Outgoing)		:
1 filter	ad Flows	(May 30, 12:08 - May 31, 12:08 Expand All	Collapse All
	192.168.0.58 -> 172.16.120.11(App01) [port:22]		
	Bytes: 9.5 KB		
	May 30, 12:30 Dst Subnet Netwo Flow Type Port	Src IP Dst IP	
	172.16.120.0 Diff Host [9 more] 22 [ssh]	192.168.0.58 172.16.120.11	

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**.

- 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 Groups.
- 4. Select the **SG-3T-DB** security group from the list.
- 5. Leave the Duration at Last 1 day.
- 6. Click Analyze.

Plan Security	×
Entity	
Security Groups	▽
SG-3T-DB	⊽
Duration	
② Last 1 day	▽
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.

Micro-Segments			
by VLAN/VXLAN ▽			
Group By	Also show groups for		
V by VLAN/VXLAN	Physical		
by Application	V Other Virtual		
by Tier	Internet		
by Subnet	None		
by Folder			
by Cluster			
by VM			
by Port			
by Security Tag			
by Security Group			
by IPSet			
by VPC			

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.

Services and Flows for SG-3T-DB			×
Services in this group	External Services Accessed	Flows (Incoming and Outgoing)	Recommended Firewall Rules
2	1	3	4
Filters	Services in this group		:
Search Properties or Metrics Q	2 Flows		
All 🚯	Service Endpoints	Count of Flow S	um of Bytes MAX of Traffic Rate
Destination 10	DB01 (172.16.130.11) port: 22 [ssh]	1 8	.8 KB 40 bps
Metrics 📀	DB01 (172.16.130.11) port: 3306 [mysql]	1 5	1.3 KB 160 bps

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.

Services and Flows for SG-	3T-DB		name par longer of real press		×
Services in this group		External Services Accessed	Flows (Incoming and Outgoing)	Recommended Firewall Re	ules
2		1	3	4	
Recommended Firewall Rules					:
SOURCE	DESTINATION	SERVICES	PROTOCOLS	ACTION	
Others_DC Physical	SG-3T-DB	22 [ssh]	TCP	ALLOW	
SG-3T-APP	SG-3T-DB	3306 [mysql]	TCP	ALLOW	
SG-3T-ALL	SG-3T-DB	3306 [mysql]	TCP	ALLOW	
SG-3T-DB	SG-INFRA-NTP	123 [ntp]	UDP	ALLOW	

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

Services and Flows for SG-	3T-DB				×
Services in this group	Exter	rnal Services Accessed	Flows (Incoming and Outgoing)	Recommended Firewall Rules	
2		1	3	4	
Recommended Firewall Rules					:
SOURCE	DESTINATION	SERVICES	PROTOCOLS	ACTION	
Others_DC Physical	SG-3T-DB	22 [ssh]	TCP	ALLOW	
SG-3T-APP	SG-3T-DB	3306 [mysql]	TCP	ALLOW	
SG-3T-ALL	SG-3T-DB	3306 [mysql]	TCP	ALLOW	
SG-3T-DB	SG-INFRA-NTP	123 [ntp]	UDP	ALLOW	

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.

Flows (Incoming and Outgoing)		:
1 filter	ed Flows	ିଶ୍ଲା May 30, 12:35 - May 31, 12:35	Expand All Collapse All
	192.168.0.58 -> 172.16.130.11(DB01) [port:22]		
	Bytes: 8.8 KB		
	May 30, 13:00 Flow Type Port Dst Subnet Netwo Flow Type Port 172.16.130.0 Diff Host [9 more] 22[ssh]	Src IP Dst 192.168.0.58 172	IP .16.130.11

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

- 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.

Select one or m	ore objects for the source	field of the firewall	rule			
Object Type:	Security Group	•			Q Filter	•
Available Objects			Selected	Objects		
🗸 💣 SG-3	-ALL		11	SG-3T-ALL		
💣 SG-31	-APP					
💣 SG-31	-DB					
💣 SG-31	-WEB		-			
		4 items				1 items
New Security G	iroup					
Advanced o	otions					
Negate sour	ce					
					ОК	Cancel

Figure 4.34 Book application all source - infrastructure access rule

- 11. Click on the Edit (\mathscr{N}) 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.

elect one or n	nore objects for the destination	on field of the firew	all rule		
Object Type:	Security Group	•			
	Q SG-INFRA			Q Fil	ter 👻
Available Objects			Selected Of	ojects	
✓ 💣 SG-II	IFRA-NTP	4	✓ @ S	G-INFRA-NTP	
		1 items			1 items
lew Security (Group				
Advanced c	ptions				
T Magata Dar	tination				

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 (\checkmark) icon for the new rule Action.
- 18. Click on the Log radio button and click Save.

Allow Access Infr	ra - Edit Actio	n	?
Action:	Allow	•	
Direction:	In/Out	•	
Packet Type:	Any	•	
Tag:			
Log:	• Log	Do not log	
Comments:			
		Save	Cancel

Figure 4.36 Infrastructure allow - infrastructure access rule

- 19. Click on the Edit (\mathscr{J}) 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

Allow Access	Infra - Specify Applied To					?
Specify contain	ers on which this rule will be applied.					
Apply this ru	le on all clusters on which Distributed F	irewall is in	nstalled.			
Apply this ru	le on all the Edge gateways.					
(For Edges v	vith version 6.1.0 and higher)					
Select one or m	ore objects for the applied to field of th	e firewall ru	ıle			
Object Type:	Security Group)				
	Q. 3t)			Q Filter	•
Available Objects			Selected	Objects		
🗸 🔮 SG-31	ſ-ALL		 ✓ I 	SG-3T-ALL		
💣 SG-31	I-APP					
	r-DB					
💣 SG-31	I-WEB					
	4 items					1 items
New Security G	iroup					
					C	K Cancel

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.

C Last	Last publish operation succeeded 5/31/17, 1:33:17 PM COT								
General	General Ethernet Partner security services								
0 🗋 >	· = = • • • •								
No.	Name	Rule ID	Source	Destination	Service	Action	Applied To		
► EB	Ping Servers (Rule 1 - 2)					🖯 C' 4	b ø / × ⇒ s k		
v Es	Infrastructure Services (Rule 3)				🖂 C' 4	• ø / × ≥ ⇒ ‰		
© 3	Allow Access to Infra	1065	🔮 SG-3T-ALL	SG-INFRA-NTP	NTP NTP	Allow	💣 SG-3T-ALL		
► E	Default Section Layer3 (Rule 4	- 6)				🖂 C' 4	β / × ⇒ ⇒ h		

Figure 4.38 Infrastructure access NSX DFW rule verification

Build DFW Rules - Management Services

- 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...

Allow MGMT Acces	s - Specify Source	?
Select one or more o	Add IP Set	
Object Type: IP (Scope: Global	
Available Objects	Name: * IP_MGMT_ACCESS	
IP CLINIC_DT	Description:	
EMR_DMZ	IP Addresses: * 192.168.0.58	
	eg:192.168.200.1,192.168.200.1/24, 192.168.200.1-192.168.200.24	0 items
New IP Set	Enable inheritance to allow visibility at underlying scopes	
Advanced options		
Negate source	OK Cancel	
	0	K Cancel

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.

Allow MGMT	Access - Specify Destin	ation		?
Select one or m	nore objects for the destin	ation field of the firew	all rule	
Object Type:	Security Group	•		
	Q. 3t		(Q Filter -
Available Objects			Selected Objects	
🖌 💣 SG-3	T-ALL		🖌 💣 SG-3T-ALL	
SG-3	T-APP	ų		
SG-3	T-DB			
💣 SG-3	T-WEB	4		
		4 items		1 items
New Coourity (20010	4 Italia		T NOMO
New Security C	sroup			
Advanced o	ptions			
Negate Des	tination			
				OK Cancel

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.

Allow Access Infi	ra - Edit Actio	n	(
Action:	Allow	•	
Direction:	In/Out	•	
Packet Type:	Any	•	
Tag:			
Log:	• Log	Do not log	
Comments:			
		Save	Cancel

Figure 4.41 Management allow - management access rule

- 22. Click on the Edit (\mathscr{J}) 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

Allow Access	Infra - Specify Destination						?
Select one or m	nore objects for the destination	n field of the	firewall r	ule			
Object Type:	Security Group	•					
	Q. SG-INFRA					Q Filter	•
Available Objects				Selected	Objects		
🖌 💣 SG-IN	IFRA-NTP			✓ if	SG-INFRA-N	ſP	
			100				
		1 items					1 items
New Security G	Broup						
Advanced or	ptions						
Negate Desi	tination						
						OK	Cancel

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.

Last	Last publish operation succeeded 5/31/17, 146:30 PM CDT							
General	General Ethernet Partner security services							
Ф 🗋 н								
No.	Name	Rule ID	Source	Destination	Service	Action	Applied To	
▶ 🛐	Ping Servers (Rule 1 - 2)						ØZ×≣s⊾.	
▶ 🛐	Infrastructure Services (Rule 3	5)				🗆 C 🕈	p/×==k	
v E	Management Services (Rule 4)					🗆 C 🕈	ø∕×⇒s⊾.	
© 4	Allow MGMT Access	1066	IP IP_MGMT_ACCESS	er SG-3T-ALL	👜 SSH	Allow	💣 SG-3T-ALL	
► 🛐	Default Section Layer3 (Rule 5	- 7)				🗆 C 🕈	$\beta^{\prime} \times \approx \approx 1.$	

Figure 4.43 Management access NSX DFW rule verification

Build DFW Rules - Application

- 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...

Allow Librarian Acc	es - Specify Source	?
Select one or more of	Add IP Set	
Object Type: IP 5	Scope: Global	
Available Objects	Name: * IP-3T-ACCESS	
IP CLINIC_DT	Description:	
EMR_DMZ		
IP HR_DT-IP-		
IP_MGMT_	IP Addresses: * 192.168.0.99	
MODALITY		
	eg:192.168.200.1,192.168.200.1/24, 192.168.200.1-192.168.200.24	0 items
New IP Set	Enable inheritance to allow visibility at underlying scopes	
Advanced options		
Negate source	OK Cancel	
		Cancel

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.

Any Access A	pp - Specify Destination				?
Select one or m Object Type:	Security Group	on field of the firewa	II rule	Q Fill	er 🔹
Available Objects			Selected Objects		
SG-3T	-ALL		🖌 💣 SG-3T-	WEB	
💣 SG-3T	-APP	4			
💣 SG-3T	-DB	(di)			
🖌 💣 SG-3T	-WEB	4-			
		4 items			1 items
New Security G	roup				
Advanced op	otions				
Negate Dest	ination				
					OK Cancel

Figure 4.45 Book application web destination - web access rule

- 17. Click on the Edit (\checkmark) 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.

Any Access App	Edit Action	?
Action:	Allow	
Direction:	In/Out 🔹	
Packet Type:	Any	
Tag:		
Log:	Log Do not log	
Comments:		7
	Save	el

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.

Any Access A	pp - Specify Applied To					?			
Specify contain	ers on which this rule will be app	lied.							
Apply this ru	Apply this rule on all clusters on which Distributed Firewall is installed.								
Apply this ru	Apply this rule on all the Edge gateways.								
(For Edges v	ith version 6.1.0 and higher)								
Select one or m	ore objects for the applied to fiel	d of the firewall ru	le						
Object Type:	Security Group	•							
	Q SG-3T				Q Filter	-			
Available Objects			Selected	Objects					
💣 SG-31	ALL		< ₫	SG-3T-WEB					
💣 SG-31	-APP								
😭 SG-31	-DB								
🖌 🔐 SG-31	-WEB	4							
	4	items				1 items			
New Security G	roup								
					ОК	Cancel			

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 (\checkmark) 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.

Web to App - S	Specify Source					?
Select one or m	ore objects for the source fi	eld of the firewall rul	9			
Object Type:	Security Group	•				
	Q, 3T				Q Filter	•
Available Objects			Selected O	bjects		
💣 SG-3T	-ALL		🖌 💣 S	SG-3T-WEB		
💣 SG-3T	-APP	4				
💣 SG-3T	-DB					
🗸 💣 SG-3T	-WEB	44				
		4 items				1 items
New Security G	roup					
Advanced op	otions					
Negate sour	ce					
					ОК	Cancel

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.

Web to App -	Specify Destination						?
Select one or m Object Type:	Security Group	lion field of the fir	ewall r	ule		O Filter	
Available Objects	(4 01)			Selected	Objects	(4,1110)	
SG-3'	T-ALL			√ 6₽	SG-3T-APP		
🖌 🖉 SG-3	T-APP		Ŵ				
SG-3	T-DB		da l				
💣 SG-3	T-WEB		100				
		4 items					1 items
New Security C	Broup						
Advanced o	ptions						
Negate Des	tination						
						ОК	Cancel

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 (\checkmark) 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 (\checkmark) icon for the new rule Action.
- 14. Click on the Log radio button and click Save.

Web to App - Edi	Action	(
Action:	Allow	•
Direction:	In/Out	•
Packet Type:	Any	•
Tag:		
Log:	💿 Log 🛛 🔾 Do	not log
Comments:		
		Save Cancel

Figure 4.50 Book application web allow - Web to App rule

15. Click on the Edit (\checkmark) 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.

Web to App -	Specify Applied To						?		
Specify contain	ers on which this rule will b	e applied.							
Apply this ru	le on all clusters on which	Distributed Fire	wall is in	stalled.					
Apply this ru	le on all the Edge gateway	S.							
(For Edges	(For Edges with version 6.1.0 and higher)								
Select one or m	ore objects for the applied	to field of the fi	rewall ru	le					
Object Type:	Security Group	•							
	Q. 3T					Q Filter	•		
Available Objects				Selected	Objects				
💣 SG-3	ſ-ALL			✓ if	SG-3T-WEB				
🖌 💣 SG-3	F-APP			< ₫	SG-3T-APP				
SG-3	F-DB								
🗸 🔐 SG-3	I-WEB								
		4 items					2 items		
New Security (iroup								
						ОК	Cancel		

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

App to DB Rule

- 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.

App to DB - Sp	ecify Source					?
Select one or m	ore objects for the source f	ield of the firewa	l rule			
Object Type:	Security Group					
	Q. 3T				Q Filter	•
Available Objects				Selected Objects		
ſ SG-3T	-ALL			🖌 🔐 SG-3T-APP		
SG-3T-APP			\$			
SG-3T-DB			4			
SG-3T	-WEB		- Chan			
		4 items				1 items
New Security G	roup					
Advanced op	tions					
Negate source	xe					
					ОК	Cancel

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.

App to DB - Sp	pecify Destination							?
Select one or m	ore objects for the destina	tion field of the fi	rewall r	ule				
Object Type:	Security Group	•						
	Q. 3T					Q Filter		-
Available Objects				Selected	Objects			
G-3T	-ALL			 Image: A set of the set of the	SG-3T-DB			
SG-3T	-APP							
🗸 💣 SG-3T	-DB							
💣 SG-3T	-WEB		An					
		4 items						1 items
New Security G	iroup							
Advanced op	otions							
Negate Dest	ination							
							ок 🗍 🗍	Cancel

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 (\mathscr{J}) icon for the new rule Action.
- 14. Click on the Log radio button and click Save.

App to DB - Edit	Action		(
Action:	Allow	•	
Direction:	In/Out	•	
Packet Type:	Any	_ ,	
Tag:			
Log:	 Log 	 Do not log 	
Comments:			
		Save Cancel	

Figure 4.54 Book application app allow - App to DB rule

- 15. Click on the Edit (\checkmark) 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.

App to DB - S	pecify Applied To					?
Specify contain	ers on which this rule will be appl	ied.				
Apply this ru	le on all clusters on which Distrib	uted Firewall is i	installed.			
Apply this ru	le on all the Edge gateways.					
(For Edges	vith version 6.1.0 and higher)					
Select one or m	ore objects for the applied to field	of the firewall r	ule			
Object Type:	Security Group	•				
	Q. 3T				Q Filter	•
Available Objects			Selected Obje	ots		
😭 SG-3	ſ-ALL		🖌 💣 SG	-3T-APP		
🖌 💣 SG-3	F-APP		🖌 💣 SG	-3T-DB		
✓ 💣 SG-3	ſ-DB					
😭 SG-3	I-WEB					
	4	items				2 items
New Security C	iroup					
					ОК	Cancel

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 $\ensuremath{\textbf{RuleID}}$ for each new rule created.
🕲 Last	publish operation succeeded 5/31	/17, 2:22:41 PM CDT					0					
General	Ethernet Partner security	services										
Ф 🗋 э	< # 15 🖗 🖬 🕅 🖓 🖓						-					
No.	Name	Rule ID	Source	Destination	Service	Action	Applied To					
▶ 🛐	Ping Servers (Rule 1 - 2)					🖯 C 4	ØZ×≕s⊾⊾					
► 🛐	Infrastructure Services (Rule 3)				- C 4	p / x at a fa					
► 🗄	Management Services (Rule 4)					🗆 C 4	Ø/xesh					
v 🖪	Book Application (Rule 5 - 7)					🖯 C 4	ØZ×≣≞ ⊾					
© 5	Allow Librarian Acces	1069	[P] IP-3T-ACCESS	SG-3T-WEB	<u>⊜</u> нттр	Allow	SG-3T-WEB					
Ø 6	Web to App	1068	SG-3T-WEB	SG-3T-APP	Ш НТТР	Allow	C SG-3T-WEB					
©7												
► 🛐	Default Section Layer3 (Rule 8	- 10)				- C 4	p//xets.h.					

Figure 4.56 Book application NSX DFW rule verification

Build Block Rules

Procedure

First Block Rule Configuration

- 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 (\checkmark) 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 (\mathscr{J}) 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** (\mathscr{J}) 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.

\sim													
6	Lest publich operation succeeded 031/17, 236:48 PM CDT Concernal Ethermet Partner security services												
G	eneral	Ethernet Partner security :	services										
ф	i) ×	et es 🗞 🖬 🗐 🖓 🖓						-					
	No. Name Rule ID Source Destination Service Action Applied To												
Þ	3	Ping Servers (Rule 1 - 2)					🗄 C' 🕈	$\beta^{\sharp} \nearrow x \Rightarrow \equiv 1_{k}$					
Þ	5	Infrastructure Services (Rule 3)					⊟ C +	$\beta^* \nearrow \times \exists^* \exists_k \models$					
►	3	Management Services (Rule 4)					- C +	$\beta^* \nearrow x \Rightarrow = 1$					
v	2	Book Application (Rule 5 - 9)					🗆 C 🕈	ø⁄×⇒ ≞ ⊾ ⊾					
0	5	Allow Librarian Acces	1069	[P] IP-3T-ACCESS	SG-3T-WEB	HTTP HTTP	Allow	SG-3T-WEB					
0	6	Web to App	1068	SG-3T-WEB	SG-3T-APP	HTTP HTTP	Allow	I SG-3T-WEB I SG-3T-APP					
0	7	App to DB	1067	SG-3T-APP	SG-3T-DB	MySQL	Allow	ff SG-3T-APP ff SG-3T-DB					
0	© 8 Block Any to App 1071 * any @ SG-3T-ALL * any Block @ SG-3T-ALL												
0	© 9 Block App to Any 1070 @ SG-3T-ALL * any Block @ SG-3T-ALL												
Þ	5	Default Section Layer3 (Rule 10) - 12)				8 C 4	p / x er s. (s.					

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.

- 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 1	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

v B	Infrastructure Services (Rule 3)				- C 4	Ø∕×≓*≞\$
© 3	Allow Access to Infra	1065	SG-3T-ALL	SG-INFRA-NTP	MTP	Allow	SG-3T-ALL

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.

- 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.

NSX Mar	18ger: [192	.168.0.120 -	1										
Live Flow	will be show	wn for the seler	ted vNIC Plea	se select a vNIC ar	nd press star	t to see the live flo	ws						
				10 001001 0 11110 011	a proce etc.								
vNIC:	Web01 - N	vetwork adapter	r1 Change	Start	Stop								
	_												
Refresh	Rate: 5 Se	econds *] % ¥							New active fle	ows 📰 F	lows with state	change 🔳 Terminated flows
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	54381	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	



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

NSX Ma Live Flov	nager: 192 v will be sho	.168.0.120) ted vNIC. Plea	se select a vNIC a	nd press star	t to see the live flo	ws						
vNIC: 👳	Web02 - N	letwork adapte	r 1 Change	Start	Stop								
Refresh	Rate: 5 Se	econds -) 🖫 😽							New activ	re flows 📰 Fl	lows with state	change 🔳 Terminated flows
Ruleld	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	6	927	6	
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	08	FINWAIT2	644	5	863	5	

Figure 4.61 Flow monitoring web 2 RuleID verification

v 🖪	Management Services (Rule 4)					🗆 C	• ø / × ⇒ ≞ ‰
© 4	Allow MGMT Access	1056	IP IP_MGMT	SG-3T-ALL	SSH SSH	Allow	SG-3T-ALL
v 🖪	Book Application (Rule 5 - 9)					e e	Φ Ø / × ∋ ≊ ‰ ‰
Ø 5	Allow Librarian Acces	1069	IP IP-3T-ACC	SG-3T-WEB	HTTP	Allow	SG-3T-WEB
⊗ 6	Web to App	1068	SG-3T-WEB	SG-3T-APP	HTTP	Allow	SG-3T-WEB

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.

- 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.

NSX Mar	ISX Manager (192.168.0.120 •)														
Live Flow	/ will be shov	vn for the selec	ted vNIC. Plea	se select a vNIC an	d press star	to see the live flor	ws								
vNIC: ja	App01 - Ne	etwork adapter	1 Change	Start	Stop										
Refresh I	effekh Raile: Seconds 🔹 👻 🥎 🔤 New active flows 🔄 Flows with state change 📑 Terminated flows														
Ruleld	Direction	Flow Type	Protocol	Source IP 1	Source Port	Destination IP	Destination Port	State	Incoming Bytes	Incoming Packets	Outgoing Bytes	Outgoing Packets	Application Context		
1068	IN	Active	TCP	172.16.110.11	54383	172.16.120.11	80	FINWAIT2	927	5	1.31 KB	5			
1068	IN	Active	TCP	172.16.110.11	54386	172.16.120.11	80	FINWAIT2	1002	5	988	5			
1068	IN	Active	TCP	172.16.110.11	54385	172.16.120.11	80	FINWAIT2	964	5	979	5	WebU1 to AppU1		
1068	IN	Inactive	TCP	172.16.110.11	54384	172.16.120.11	80	FINWAIT2	964	5	979	5			
1068	IN	Active	TCP	172.16.110.11	54382	172.16.120.11	80	FINWAIT2	421	5	1.18 KB	5			
1068	IN	Active	TCP	172.16.110.12	41655	172.16.120.11	80	FINWAIT2	927	5	1.31 KB	5			
1068	IN	Active	TCP	172.16.110.12	41658	172.16.120.11	80	FINWAIT2	1002	5	988	5	W-1-00-1-104		
1068	IN	Active	TCP	172.16.110.12	41657	172.16.120.11	80	FINWAIT2	964	5	979	5	webu2 to Appu1		
1068	IN	Active	TCP	172.16.110.12	41656	172.16.120.11	80	FINWAIT2	964	5	979	5			
1068	IN	Active	TCP	172.16.110.12	41654	172.16.120.11	80	FINWAIT2	421	5	1.18 KB	5			
1067	OUT	Active	TCP	172.16.120.11	59969	172.16.130.11	3306	FINWAIT2	610	8	655	10			
1067	OUT	Active	TCP	172.16.120.11	59967	172.16.130.11	3306	FINWAIT2	662	9	655	10			
1067	OUT	Inactive	TCP	172.16.120.11	59966	172.16.130.11	3306	FINWAIT2	821	9	657	10	Apput to DB01		
1067	OUT	Active	TCP	172.16.120.11	59968	172.16.130.11	3306	FINWAIT2	769	8	657	10			
1065	OUT	Active	UDP	172.16.120.11	123	192.168.0.211	123		76	1	76	1	App01 to NTP-01a		
1066	IN	Active	TCP	192.168.0.58	60816	172.16.120.11	22	EST	21.46 KB	287	23.44 KB	231	SSH to App01		

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

v 🗄	Management Services (Rule 4)					e C	• 🗗 / × 🗉 🛼 🖡
⊜4	Allow MGMT Access	1066	PIP_MGMT	SG-3T-ALL	🚔 SSH	Allow	SG-3T-ALL
v 🖪	Book Application (Rule 5 - 9)					c d	+ Ø / × er s h
© 5	Allow Librarian Acces	1069	IP-3T-ACC	SG-3T-WEB	HTTP	Allow	ef SG-3T-WEB
© 6	Web to App	1068	SG-3T-WEB	@ SG-3T-APP	HTTP	Allow	C SG-3T-WEB
© 7	App to DB	1067	SG-3T-APP	💣 SG-3T-DB	MySQL	Allow	@ SG-3T-APP @ SG-3T-DB

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.

- 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.

NSX Manag	ger: (192.168.0.120 +)													
(land	Last publish operation succeeded 5/31/17,7:31:05 PM COT													
e casi	oublish operation succeeded or a fi	17, 7.31.00 PM CD1					ω							
General	eneral Ethernet Partner security services													
Ф () X														
No.	No. Name Rule ID Source Destination Service Action Applied To													
► 🖪	Ping Servers (Rule 1 - 2)					- C	• ø / × = = 1.							
► 🗄	Infrastructure Services (Rule 3					d C	+ Ø / x m s h							
▶ 🖪	Management Services (Rule 4)					- C	Φ Ø / × Β 5. Έ							
v E	Book Application (Rule 5 - 9)					C C	Φ 🖉 🖊 × 🖻 🛼 🖕							
© 5	Allow Librarian Acces	1069	IP IP-3T-ACC	SG-3T-WEB	HTTP :	Allow	ef SG-3T-WEB							
© 6	Web to App	1068	SG-3T-WEB	SG-3T-APP	HTTP	Allow	@ SG-3T-WEB @ SG-3T-APP							
© 7	App to DB	1067	SG-3T-APP	SG-3T-DB	MySQL	Allow	@ SG-3T-APP @ SG-3T-DB							
© 8	Block Any to App	1071	* any	鹶 SG-3T-ALL	* any	Block	ピ SG-3T-ALL							
© 9														
► 🖪	Default Section Layer3 (Rule 1)	0 - 12)				e e	• Ø / × er s. (s.							

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.

- 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.



NSX Ma	nager: 192.	168.0.120 -)										
Live Flov	Live Flow will be shown for the selected vNIC. Please select a vNIC and press start to see the live flows												
vNIC: 🕎	Web02 - N	ietwork adapter	1 Change	Start	Stop								
	NIC: Web02 - Network adapter 1 Change Start Stop												
Refresh	Rate: 15 se	econds 🔹	V V							New active	a flows 📰 Fi	ows with state	change 📰 Terminated flows
Refresh Ruleid	Rate: 15 se	Flow Type	Protocol	Source IP	Source Port	Destination IP	Destination Port	State	Incoming Bytes	New active Incoming Packets	Outgoing Bytes	ows with state Outgoing Packets	change Terminated flows

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.

NSX Mar	SX Manager: (192.168.0.120 ▼)												
Live Flow	e Flow will be shown for the selected vNIC. Please select a vNIC and press start to see the live flows IC: IIII Web01 - Network adapter 1 Chance Shurt Stop												
vNIC:	Web01 - N	letwork adapter	1 Change	Start	Stop								
Refrech	effesh Raie: 15 seconds 🔹 👻 🕎												
Refresit	afresh Rate: 15 seconds 🔻 🐺 🕎 🔤 New active flows 🔛 Pores with state change 📺 Terminated flows												
RuleId	Ruled Direction Flow Type Protocol Source P Source Port Destination P Port State Post Pyte Pesters Dytes Pesters Dytes Pesters												
1071	IN	Block	TCP	192.168.0.58	58080	172.16.110.11	80	CLOSED	64	1	0	0	
1071	IN	Block	TCP	192.168.0.58	58078	172.16.110.11	80	CLOSED	64	1	0	0	
1071	IN	Block	TCP	192.168.0.58	58077	172.16.110.11	80	CLOSED	64	1	0	0	
1066	IN	Active	TCP	192.168.0.58	57951	172.16.110.11	22	EST	8.69 KB	101	7.08 KB	63	
NSX Mar	nager: 192.	168.0.120 -	1										
	-												
Live Flow	will be show	vn for the selec	ied vNIC. Pleas	ie select a vNIC an	id press star	to see the live flo	ws						
vNIC: pr	Web02 - N	letwork adapter	1 Change	Start	Stop								
	_												
Refresh F	Rate: 5 Se	conds 💌	¥ ¥							New activ	e flows 🔳 F	lows with state	change 🔳 Terminated flows
Ruleld	Direction	Flow Type	Protocol	Source IP	Source Port	Destination IP	Destination Port	State	Incoming Bytes	Incoming Packets	Outgoing Bytes	Outgoing Packets	Application Context
1071	IN	Block	TCP	192.168.0.58	58134	172.16.110.12	80	CLOSED	64	1	0	0	
1066	IN	Active	TCP	192.168.0.58	60812	172.16.110.12	22	EST	20.76 KB	301	21.94 KB	218	
1071	IN	Block	TCP	192.168.0.58	58133	172.16.110.12	80	CLOSED	64	1	0	0	
1071	IN	Block	TCP	192.168.0.58	58132	172.16.110.12	80	CLOSED	64	1	0	0	

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.

Books Collection ×	×	-			×
← → C ① 172.16.110.11			7	Ł	0
3 Tier app Server Chain • Web01 • DB01 • DB01 • DB01 • DB01 • Constant • Constant	Administrator C.VWrodowskystem37.cmd.ee Kicrosoft Windows [Version 10 0.11203] (c) 2016 Microsoft Corporation. All rights reserved. C:Users/administrator3pcoffig Windows IP Configuration Ethernet adapter Ethernet0: Connection-specific DWS Suffix .: Link.local IDV& Address	×			
DATA		~			
Id Title Author 1 The Martian Andy Weir 2 The HHGTG Douglas Adams					

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 microsegmentation 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/thevmware-nsx-platform-healthcare-series-part-4-1micro-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/thevmware-nsx-platform-healthcare-series-part-4-2micro-segmentation-practical-with-vmware-nsxapplication-rule-manager/

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

Α

Application Rule Manager XIX, 14, 15, 69, 74, 75, 76, 77, 84, 85, 86, 89, 101, 102, 103, 109, 169, 174

D

Deploy. See also deployment models deployment models 6. See also Deploy

DFW 5, 9, 10, 12, 13, 17, 19, 32, 33, 35, 37, 38, 40, 42, 45, 47, 48, 57, 60, 62, 63, 64, 72, 73, 78, 81, 82, 83, 84, 88, 93, 95, 96, 97, 98, 101, 103, 104, 105, 109, 120, 124, 125, 127, 131, 133, 134, 138, 140, 141, 142, 144, 145, 147, 148, 155, 158, 159. See also Distributed Firewall

Distributed Firewall 5, 7, 8, 10, 37, 38, 57, 59, 61, 62, 64, 82, 104, 109, 117, 120, 174. *See also DFW* DNS 4

Е

East-West 2 ESXi 9, 17, 20, 23, 24, 28, 74, 114

F

Flow 5, 9, 10, 11, 14, 15, 69, 70, 71, 74, 75, 76, 77, 78, 79, 80, 81, 82, 84, 85, 86, 87, 89, 90, 91, 93, 94, 95, 96, 98, 101, 102, 103, 104, 105, 108, 111, 113, 114, 117, 119, 120, 121, 122, 123, 124, 125, 126, 127, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 157, 158, 159, 160, 162, 163, 164

G

Grouping XXIII, 8, 12, 29, 31, 40, 41, 42, 43, 78, 88, 115, 116, 120, 127, 134, 141

Н

HIPAA 4

Index

L

LDAP 4 Least Privilege 1, 2, 3, 4, 6, 167, 174 Logical Switch 7, 79, 90, 91, 92

Μ

Micro-segmentation I, III, XVI, XIX, XXIII, 1, 3, 4, 5, 6, 7, 9, 13, 14, 15, 17, 23, 27, 38, 40, 58, 67, 71, 109, 111, 113, 120, 124, 131, 138, 167, 169, 174

Monitoring 9, 10, 12, 14, 15, 17, 21, 28, 74, 76, 85, 101, 157, 158, 159, 160, 162, 163, 164

Ν

- NSX I, III, XV, XVI, XIX, XXIII, 2, 3, 5, 7, 8, 9, 10, 12, 13, 14, 15, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 35, 37, 38, 40, 41, 42, 43, 44, 47, 48, 57, 59, 60, 61, 62, 63, 64, 69, 71, 72, 73, 74, 75, 76, 77, 78, 80, 81, 82, 83, 84, 85, 86, 88, 90, 91, 92, 93, 95, 96, 97, 98, 100, 101, 102, 103, 104, 105, 109, 111, 113, 114, 115, 116, 117, 118, 120, 121, 124, 125, 127, 128, 131, 133, 134, 135, 138, 139, 140, 141, 144, 147, 154, 155, 156, 158, 159, 167, 169, 174 NSX Manager 14, 20, 23, 26, 27, 28, 29, 31, 35, 42, 43, 47, 57, 74, 100, 114, 115, 116, 144, 147, 154, 156 NTP 4, 18, 19, 20, 21, 29, 30, 31, 40, 42, 45, 46, 60, 70, 71, 73,
 - 40, 42, 45, 46, 60, 70, 71, 73, 74, 77, 78, 79, 80, 81, 86, 88, 101, 104, 105, 112, 114, 115, 117, 118, 119, 120, 121, 141, 142, 143, 157, 158

Ρ

PCI 4

R

Rule ID 10, 11, 35, 37, 38, 47, 57, 58, 59, 60, 61, 62, 63, 100, 103, 104, 105, 106, 107, 108, 144, 147, 154, 156, 158, 159, 160, 161, 163

S

Security XV, XVI, XVII, XX, XXI, XXII, XXIII, 1, 2, 3, 4, 6, 7, 8, 13, 14, 167, 174 Security Group 8, 9, 10, 12, 28, 31, 32, 33, 34, 35, 41, 45, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 78, 79, 80, 82, 88, 89, 90, 91, 92, 95, 96, 99, 100, 115, 116, 117, 118, 119, 120, 122, 124, 127, 128, 129, 131, 134, 136, 138, 139, 142, 143, 145, 146, 148, 149, 150, 151, 152, 153, 154, 155, 156 Security Tags 8, 13, 29, 30, 31, 32 Software-Defined Data Center 167 SSH 65, 113, 115, 125, 131, 132, 133, 138, 139, 140, 141, 146, 157, 158, 159, 160, 161, 163, 164 Syslog 14, 23, 24, 25, 26, 27, 28

т

Traffic XXII, XXIII, 2, 3, 9, 10, 11, 13, 15, 17, 20, 28, 36, 57, 58, 70, 73, 84, 106, 121, 125, 127, 132, 135, 139, 159, 161, 164

V

Virtual Machine 1, 2, 3, 9, 15, 30, 32, 35, 47, 57, 76, 80, 86, 100, 102, 115, 116, 119, 122, 126, 136, 144, 147, 154, 156. *See also VM* VLAN 72 VM XXIII, 70, 89, 114. *See also virtual machine* VMware I, III, IV, XV, XVI, XVII, XIX, XXI, XXIII, 1, 2, 3, 5, 7, 9, 10, 13, 14, 15, 20, 22, 24, 28, 20, 77

14, 15, 20, 22, 23, 24, 28, 29, 37, 38, 57, 59, 61, 62, 69, 71, 72, 73, 74, 75, 76, 77, 85, 86, 88, 101,

102, 113, 114, 167, 169, 174 ESXi 9, 17, 20, 23, 24, 28, 74, 114 NSX I, III, XV, XVI, XIX, XXIII, 2, 3, 5, 7, 8, 9, 10, 12, 13, 14, 15, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 35, 37, 38, 40, 41, 42, 43, 44, 47, 48, 57, 59, 60, 61, 62, 63, 64, 69, 71, 72, 73, 74, 75, 76, 77, 78, 80, 81, 82, 83, 84, 85, 86, 88, 90, 91, 92, 93, 95, 96, 97, 98, 100, 101, 102, 103, 104, 105, 109, 111, 113, 114, 115, 116, 117, 118, 120, 121, 124, 125, 127, 128, 131, 133, 134, 135, 138, 139, 140, 141, 144, 147, 154, 155, 156, 158, 159, 167, 169, 174 vRealize vRealize Log Insight 14, 15, 17, 20, 21, 22, 23, 24, 25, 26, 27, 36, 37, 38, 39, 40, 42, 57, 58, 59, 60, 61, 62, 63, 65, 67, 71, 83, 109, 113 vRealize Network Insight 14, 15, 109, 111, 114, 117, 120, 121, 124, 127, 131, 135, 138, 169, 174 vSphere XVI, 14, 15, 22, 23, 24, 28, 37, 38, 57, 59, 61, 62, 83, 114, 169 vCenter 20, 23, 24, 25, 28, 74, 77, 86, 89, 102, 114 vCenter Server Appliance 20, 74, 114 vSphere Distributed Switch 15 vSphere Web Client 29, 31, 33, 42, 43, 45, 48, 64, 75, 84, 101, 115, 116, 142, 145, 148, 157, 158, 160, 161, 162 VXLAN 7, 71, 72, 113

W

allowlist 1, 20, 73

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



vmware[®] **PRESS**

www.vmware.com/go/run-nsx

\$12.99