Microsegmentation in practice

• Robert Kloosterhuis
Robert Kloosterhuis

• Senior Engineer
• Focus on NSX en vSAN

• Healthcare
• Standardized SDDC
• Application Delivery
Agenda

• Firewalls
• Micro-Segmentation
• DFW Best Practices
• Know your flows
• Automation
• Take Aways
Firewalls

Why are we doing this again?
• Centralized Model
• Constrained by costs / performance
• Hairpins traffic flow
Defense in-depth

- Policy, Procedures, Awareness
- Physical Security
- Perimeter
- Networks
- Host
- Application
- Data
Zero Trust

‘Whitelist’ what is allowed

Block **everything else**
VMware NSX Data Center
a.k.a. “NSX-V” and “NSX-T”

Data Plane
Distributed switching, routing, firewall

Control Plane

Management Plane

Source: VMware
Traffic Flow
When you say ‘micro-segmentation’

- Segment **network space** using VXLAN overlays
  - Distributed Logical Router (DLR)

- Segment ‘**workloads**’ using per-VM firewalling
  - Distributed Firewall (DFW)

... Do both?
Micro-segmentation

With the NSX Distributed Firewall (DFW)
Firewall

Sections:

Rules:
<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Applied To</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>C01_Global_Prod_ADDS</td>
<td>dg_c01_allVMs</td>
<td>sg_c01_prod_adds</td>
<td>DNS</td>
<td>Distributed Firewall</td>
<td>Allow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>DNS-UDP</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Things I can use:
• Ports
• MAC’s
• Networks
• IP Addresses
• IP Sets
• AD users (maybe)

Things I can use:
• Datacenters
• Clusters
• VM
• VM Properties
• vApp
• vNICs
• Resource Pools
• Legacy Port groups
• Distributed Port Groups
• MAC Sets
• Security Tags
• Networks
• IP Addresses
• IP Sets
• vNICs
• vSwitch
• dvSwitch
• Logical Switch (vxlan)
• AD Users
• Nested Security Groups
Group by user (guest introspection)
Firewalling Strategy

• What are you trying to protect?

• What are you protecting against?

• Brownfield vs Greenfield

• Everything at once, or per-app?

• Is ‘zero trust’ the end-goal?
• NSX DFW default final rule is ‘any-any-any-allow’

• ‘Zero Trust’ is all about that final default rule

• If you switch it to ‘block’, can you guarantee nothing will break?
NSX Distributed Firewall Best Practices
Avoid use of ‘any’ in rules – make things explicit

Avoid direct VM references. Always try to abstract with groups
Make rules as explicit as possible

Specify flow direction clearly

Avoid multiple groups in source or destination

Keep things modular - Maintain overview
Use sections to logically group rules together

Sections can be edited and published separate from each other

Building block for automation
Dynamic Security Groups give you most flexibility and potential for automation

Nesting Security Groups is powerful, but keeping overview and troubleshooting can be a challenge
Avoid Regular Expression membership criteria, NSX Manager doesn’t like it

Instead use ‘Entity’ (object relationships)
### Security Tags

Security Tags are the most flexible way to categorize VMs.

- **Highly modular** – tags can have any scope.
- **As Granular as you like**
- **Makes automation much easier**

```powershell
PS C:\> get-NsxSecurityTag KALI | New-SecuritytagAssignment -ApplyToVM (get-vm kaliSQL1)
```
Define **Dynamic group** membership by which **security tag** is applied to a VM
1. Security Tags assigned to VM
2. Tag Triggers Dynamic Group Membership
3. Rules reference the dynamic groups
Avoid too many tags – NSX Manager doesn’t like it, and neither will you!

Have a clear naming convention established

Avoid duplicate or unclear tags – Be explicit!
Know your flows
• Brownfield vs Greenfield

• How much do you already know?

• What tools can help you?

• Which people do you need?

• Application / Vendor documentation

• Layer 4 vs layer 7
Layer 4 vs 7
## Application Rule Manager

### Exchange Tst run

- Analysis complete 318 flows
- Global (Objects)

### Flows

<table>
<thead>
<tr>
<th>Direction</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>OUT</td>
<td>C04-EXCO1, C01-SRV-EXCH-11</td>
<td></td>
<td>5 Services</td>
</tr>
<tr>
<td>IN</td>
<td>C04-ADD002</td>
<td>C01-SRV-EXCH-12</td>
<td>3 Services</td>
</tr>
<tr>
<td>OUT</td>
<td>C04-EXCO1, C01-SRV-EXCH-11</td>
<td>C04-ADD002</td>
<td>3 Services</td>
</tr>
<tr>
<td>INTRA</td>
<td>C04-SRV-EXCH-12</td>
<td>C04-EXCO1, C01-SRV-EXCH-11</td>
<td>2 Services</td>
</tr>
<tr>
<td>IN</td>
<td>C04-ADD002</td>
<td>C04-EXCO1, C01-SRV-EXCH-11</td>
<td>2 Services</td>
</tr>
<tr>
<td>INTRA</td>
<td>C04-EXCO1, C01-SRV-EXCH-11</td>
<td>C01-SRV-EXCH-12</td>
<td>2 Services</td>
</tr>
<tr>
<td>INTRA</td>
<td>C04-EXCO1, C01-SRV-EXCH-11</td>
<td>C01-SRV-EXCH-12</td>
<td>2 Services</td>
</tr>
<tr>
<td>INTRA</td>
<td>C04-EXCO1, C01-SRV-EXCH-11</td>
<td>C01-SRV-EXCH-12</td>
<td>2 Services</td>
</tr>
<tr>
<td>OUT</td>
<td>C04-EXCO1, C01-SRV-EXCH-11</td>
<td></td>
<td>3 Services</td>
</tr>
<tr>
<td>OUT</td>
<td>C04-EXCO1, C01-SRV-EXCH-11</td>
<td></td>
<td>2 Services</td>
</tr>
<tr>
<td>IN</td>
<td>C04-ADD002</td>
<td>C04-EXCO1, C01-SRV-EXCH-11</td>
<td>2 Services</td>
</tr>
</tbody>
</table>
### Flow Monitoring

#### Live Flow

**NSX Manager:** 10.0.10.150 | Standalone

Live Flow will be shown for the selected vNIC. Please select a vNIC and press start to see the live flows.

**vNIC:** C01-SRV-KAL-01 - Network adapter 1

**Refresh Rate:** 30 Seconds

<table>
<thead>
<tr>
<th>Rule ID</th>
<th>Direction</th>
<th>Flow Type</th>
<th>Protocol</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>State</th>
<th>Incoming Bytes</th>
<th>Incoming Packets</th>
<th>Outgoing Bytes</th>
<th>Outgoing Packets</th>
<th>Application Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>1005</td>
<td>IN</td>
<td>BLOCK</td>
<td>UDP</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>CLOSED</td>
<td>0 Bytes</td>
<td>0</td>
<td>76 Bytes</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1005</td>
<td>IN</td>
<td>BLOCK</td>
<td>UDP</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>CLOSED</td>
<td>0 Bytes</td>
<td>0</td>
<td>76 Bytes</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1005</td>
<td>IN</td>
<td>BLOCK</td>
<td>TCP</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>CLOSED</td>
<td>0 Bytes</td>
<td>0</td>
<td>76 Bytes</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1005</td>
<td>OUT</td>
<td>BLOCK</td>
<td>UDP</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>CLOSED</td>
<td>0 Bytes</td>
<td>0</td>
<td>76 Bytes</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1005</td>
<td>IN</td>
<td>BLOCK</td>
<td>TCP</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>CLOSED</td>
<td>0 Bytes</td>
<td>0</td>
<td>76 Bytes</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1005</td>
<td>IN</td>
<td>BLOCK</td>
<td>UDP</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>CLOSED</td>
<td>0 Bytes</td>
<td>0</td>
<td>76 Bytes</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1005</td>
<td>OUT</td>
<td>BLOCK</td>
<td>UDP</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>CLOSED</td>
<td>0 Bytes</td>
<td>0</td>
<td>76 Bytes</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1005</td>
<td>IN</td>
<td>BLOCK</td>
<td>TCP</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>CLOSED</td>
<td>0 Bytes</td>
<td>0</td>
<td>76 Bytes</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1006</td>
<td>OUT</td>
<td>ACTIVE</td>
<td>UDP</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>CLOSED</td>
<td>0 Bytes</td>
<td>0</td>
<td>76 Bytes</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1006</td>
<td>IN</td>
<td>BLOCK</td>
<td>UDP</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>CLOSED</td>
<td>0 Bytes</td>
<td>0</td>
<td>76 Bytes</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1006</td>
<td>OUT</td>
<td>ACTIVE</td>
<td>UDP</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>CLOSED</td>
<td>0 Bytes</td>
<td>0</td>
<td>76 Bytes</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1006</td>
<td>IN</td>
<td>BLOCK</td>
<td>UDP</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>CLOSED</td>
<td>0 Bytes</td>
<td>0</td>
<td>76 Bytes</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1006</td>
<td>OUT</td>
<td>INACTIVE</td>
<td>UDP</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>CLOSED</td>
<td>0 Bytes</td>
<td>0</td>
<td>76 Bytes</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1006</td>
<td>IN</td>
<td>BLOCK</td>
<td>TCP</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>CLOSED</td>
<td>0 Bytes</td>
<td>0</td>
<td>76 Bytes</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1006</td>
<td>OUT</td>
<td>INACTIVE</td>
<td>UDP</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>CLOSED</td>
<td>0 Bytes</td>
<td>0</td>
<td>76 Bytes</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1006</td>
<td>IN</td>
<td>BLOCK</td>
<td>TCP</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>CLOSED</td>
<td>0 Bytes</td>
<td>0</td>
<td>76 Bytes</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1006</td>
<td>OUT</td>
<td>INACTIVE</td>
<td>UDP</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>CLOSED</td>
<td>0 Bytes</td>
<td>0</td>
<td>76 Bytes</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1006</td>
<td>IN</td>
<td>BLOCK</td>
<td>TCP</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>138</td>
<td>CLOSED</td>
<td>0 Bytes</td>
<td>0</td>
<td>76 Bytes</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
All flows hit the last rule in the section

If set to ‘allow’
You can check if you missed anything

If set to ‘block’
You are now logging all that is being blocked

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Applied To</th>
<th>Action</th>
<th>Log</th>
</tr>
</thead>
<tbody>
<tr>
<td>c01_Prod_Kali_Internal</td>
<td>dg_c01_prod_kali</td>
<td>dg_c01_prod_kali</td>
<td>Any</td>
<td>dg_c01_prod_kali</td>
<td>Allow</td>
<td></td>
</tr>
<tr>
<td>c01_Prod_Kali_ssh Inc.</td>
<td>dg_c01_allVMs</td>
<td>dg_c01_prod_kali</td>
<td>SSH</td>
<td>dg_c01_prod_kali</td>
<td>Allow</td>
<td></td>
</tr>
<tr>
<td>c01_Prod_Kali_Default</td>
<td>Any</td>
<td>Any</td>
<td>Any</td>
<td>dg_c01_prod_kali</td>
<td>Block</td>
<td></td>
</tr>
</tbody>
</table>
VMware Network Insight
• How many man-hours do you want to spend on maintaining firewall rules?

• How fast do you want to be able to act? Don’t be the bottleneck!

• Identify quick-wins

• Start small

• Some automation is better than non at all
Standardization

• Consistent naming

• Human Readable (where possible)

• Consistent way of doing things

• Consistent scope

• Repeatable
Application Deployment Automation

- VM Deployment
- NSX Network Environment
- NSX DFW Security
- OS Deployment / Config
- Application Deployment
- Application Configuration
- User access / AD
- Etc...

Think of firewall rules as just another part of ‘application (deployment) policy’
VMware vRealize Automation
Take Aways
Take aways

• Micro-segmentation can significantly increase security in-depth

• New ways of thinking about your security model – have a strategy

• Scope is extremely flexible – have a design and plan in place before you start

• Will increase administrative overhead if not mitigated through standardization and automation

• More granular means more automation required
Take aways

• Use **dynamic** features and approach where possible

• Requires **DevOps**-style approach to deploy and manage

• Start thinking about ‘**application security policy**’ instead of ‘firewall rules’

• Automate firewall rules and tagging as part of **application deployment**

• Leverage **LogInsight** and **NetworkInsight**
Thank you!

Any Questions?

Robert Kloosterhuis

www.linkedin.com/in/robertkloosterhuis/
@thefluffysysop