NSX-T based Micro-segmentation with VMware Horizon

Setting up a Distributed Firewall

Introduction:

NSX-T Micro-Segmentation is one of the many features we can use to secure communication at the Transport. We will be looking at basic approaches using Microsegmentation and the Identity Firewall in NSX-T. The objective of this exercise to ensure one understands the basics of implementing these rules and does not necessarily reflect a real world scenario.

Real World Scenarios will be vastly more complex and time consuming to configure.

Before continuing, there are some pre-requisite checks that need to be done



- 1. Implementing the Distributed Firewall
 - On your **ControlCenter** server (which is also your landing server)
 - Open your Google Chrome Browser
 - Select the **NSX Manager** icon from the **favourites bar.** (Accept the untrusted certificate to continue)

VMware	® NSX-T™	л
v m v u u u		
adasia		
aamin		
	LOG IN	

- 2. On your Browser
 - Login with Username admin
 - With the password VMware1!VMware1!
 - Select LOG IN

	«		
System Overview			DIRECTORY
Configuration		ADD ACTIVE D	IRECTORY
Appliances			Name
📃 Get Started		Edit	efire.com
E Fabric	>	Sync	Delta Server
_© ⁷ Service Deployments		Delet	te
🗅 Identity Firewall AD			

3. In the NSX Admin Console

- At the top of the NSX-T admin console select **System**
- Under Configuration, select Identity Firewall AD

- In the ACTIVE DIRECTORY area, to the left of the euc-livefire.com domain, select the 3 Dotted hyperlink
- Select Sync All



4. In the NSX Admin Console

- Select the Security tab
- In the left pane, under East West Security
 - Select Distributed Firewall



5. In Distributed Firewall area

- To the right, select the dropdown, next to ACTIONS
- Under Settings, select General Settings

General Firewall Settings	Identity Firewall Settings	
Distributed Firewall Status	Enable	
dentity Firewall Status	Enable	
Auto Save Drafts	Enable	

6. In the **General Firewall Settings**

• Select Identity Firewall Settings tab

General Firewall Settings	Identity Firewall Settings
Standalone Hosts	Disable
	Q Search
Cluster Name	Enabled/Disabled
RegionA01-COMP01	C Enable
	•
	1 - 1 61

- 7. In the **General Firewall Settings**
 - Under Identity Firewall Settings
 - Next to RegionA01-COMP01, Cluster Name, ensure the toggle is set to Enable

Select SAVE

Part 1

Pre-deployment check

Chrome	VMware Horizon Client
3	VMware Horizon Client
https://horizon.euc-livefire.com	Image: https://horizon.euc-livefi
Cancel Login	W10INST ជ ••• ជ

- 1. On your **ControlCenter** server
 - Select and launch your Horizon client
 - Select your Horizon.euc-livefire.com POD Broker
 - Login as Mark with the password VMware1! and select Login
 - Select your W10INST entitlement

	File Explorer
60	Search
	Shut down or sign out >
	Desktop
	> Type here to search
🖅 Ru	n X
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open	cmd v
	OK Cancel Browse

- 2. On your virtual Desktop
 - Select Start > Run
 - Next to Open: type cmd

```
C:\Windows\system32\cmd.exe
C:\Users\mark>ping sql.euc-livefire.com
Pinging sql.euc-livefire.com [192.168.110.45] with 32 bytes of data:
Reply from 192.168.110.45: bytes=32 time<1ms TTL=127
Reply from 192.168.110.45: bytes=32 time=1ms TTL=127
Reply from 192.168.110.45: bytes=32 time=1ms TTL=127
Ping statistics for 192.168.110.45:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\Users\mark>_
```

- 3. In the CMD interface type ping sql.euc-livefire.com
 - Note the 192.168.110.45 IP address
 - Please NOTE! Do not close your Horizon Desktop session



4. In the NSX-T admin console

- Select the Security Tab under East West Security
- Select Distributed Firewall

Security Overview East West Security Distributed Firewall Distributed IDS Distributed IDS Network Introspection (E-W) North South Security Gateway Firewall Bid URL Analysis Da Network Introspection (N-S) ALL RULES Category SPECIFIC RULES ALL RULES Category SPECIFIC RULES Ethernet (I) Ethernet (I) Ethernet (I) Image: Distributed IDS	
East West Security Image: Distributed Firewall Image: Distributed IDS Image: Distri	
ETHERNET (1) EMERGENCY (0) INFRASTRUCTURE (0) ENVIRONMENT (0) APPLICATION (1) Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed IDS Image: Distributed I	_
Image: Specific Spe	
Image: Network Introspection (E-W) North South Security Image: Network Introspection (N-S) Image: Network	d more
North South Security Image: South Security Image: South Security Image: South Security	
Image: Gateway Firewall Big URL Analysis Co Network Introspection (N-S)	Success (
Bit URL Analysis Da Network Introspection (N-S)	
Da Network Introspection (N-S)	

- 5. In the **Distributed Firewall** section
 - Ensure that Application is selected
 - Select ADD POLICY

• You will notice a Policy has been added with a default name **New Policy**

ty Overview	+ add	POLICY	+ add i	RULE	CLONE	о имро
Security	1 Unpublish	ed Change)			
uted Firewall			Name	ID	So	ources Desti
uted IDS	:>		Desktops	(0)	Applied To	DFW
rk Introspection (: >		Default L	(1)	Applied To	DFW

- 6. In the **Policy** area you have just created
 - Under Name select New Policy under Name and replace with Desktops

g Security	Inventory Plan & Troubleshoot
«	+ ADD POLICY + ADD RULE CL
	Name ID
	N Desktops (0) Applik
	Enable Logging For All Rules
	Disable Logging For All Rules
(Enable All Rules
	Disable All Rules
	Delete Policy
	Add Rule
(Add Policy Above
▼ 4	Add Policy Below

- 7. To left of your **Desktops Policy**, notice you have **3 vertical dots**.
 - Select the **3 vertical dots**
 - Select Add Rule

NSX-T						
e Networking	Secur	ity Inve	entory	Plan & Troub	leshoot	System
	*	+ ADD	POLICY	+ ADD RULE	CL	оле 🖒 илдо
ecurity Overview		(1 Unpublishe	ad Change)		
Vest Security				Name	ID	Sources
stributed Firewall		÷ ~		Desktops	(1)	Applied To DFW
stributed IDS		÷		Block ICMP to SG	L	Any
etwork Introspection (: >		Default Layer3 S.	(1)	Applied To DFW
South Security						

8. In the **New Rule interface**,

• Select New Rule and change to Block ICMP to SQL

LONE	S UNDO	DELETE	1 Unpublished Change	
ID		Sources	Destinations	Se
(1)	Applied To	DFW		
		Any	Any	A
(1)	Applied To	DFW		

9. Under **Sources**

• Select the **pencil** Icon next to **Any**

	Set \$	Sou Bloc	rce	P to S	QL	
	Negate Group	e Sele s (0)	ction	s 🔵 P Addr	No No	Negated selections
L	ADD	GROU	P	J	Name	
		:	>	0-0 0-0	External	
	\square	:	1	Ģ-Ģ	External	net

10. In the **Set Source** Window

Select ADD GROUP

Set Source Rule > Block ICMP	to SQL				
ADD GROUP	No Negate	d selections will be	shown as Example (Group	
÷	Subnet 10		*	Set Members	
	Description	Descrip	ition		Tags
	SAVE	CANCEL			

11. In the ADD GROUP interface

- Under Name type Subnet 10
- Under Compute Members select Set Members

Add Compute Members eit Compute members to defir	ther by creating one effective memory	r by directly adding th hership of the group	iem. You can also add id
Membership Criteria (0)	Members (D)	IP Addresses (0)	MAC / ddresses (0)
ACTIONS ~			
Fatar ID Addross			

- 12. In the Select Members | Subnet 10 window
 - Select the IP Addresses tab

Select Members Subnet 10	
Add Compute Members either by creating or by directly adding them. You can also add identity m Compute members to define effective membership of the group.	
Membership Criteria (0) Members (0) P Addresses (0) MAC Addresses (0) AD Gr	
ACTIONS -	
172.1610.0/24	
Ether MAC Address or AD groups can be part of a Group	
CANCEL	
ADD GROUP	
Name	Compute Members
Subnet 10	1 IPs
Description Description	
SAVE CANCEL	
ADD GROUP	
Name	
✓ : > : Subnet 10	
1-10f1Groups	
Show Only Selected	
CANCEL APPLY	

13. Under **ACTIONS**

- In the Enter IP Address area, type 172.16.10.0/24 In the bottom right-hand corner,
 Select APPLY
- 2. In the **Set Source** window select **SAVE**
- 3. Ensure that the **checkbox** next to **Subnet 10** is selected
 - Select APPLY

EM	ERGENCY (0)		NFRASTRU	JCTURE (0)	ENVIRONMENT (0)		• APPLICATION (2)
	CLONE		📋 DEL	ETE •••	1 Unpublished Change		
	ID			Sources	Destinations		Services
	(1)	Applied To	DFW				
				BB Subnet 10	Any	1	Any
tion:	(1)	Applied To	DFW				

14. Under **Destinations**

• Next to Any select the Pencil

Set Destination
Rule > Block ICMP to SQL
Negate Selections No Negated selections v
Groups (0) IP Addresses (0)
ADD GROUP
Name

- 15. In the **Set Destination** window
 - Select ADD GROUP

ADD GROUP				
	Name			
÷	SQL			*
	Description		Description	
	SAVE	CANCEL		

16. In the ADD GROUP area

• Under Name type SQL in the Group Name area

Name		Compute Members
SQL		* Set Members
Description	Description	

17. Under **Computer** Members

Select Set Members

Select Members	SQL			
Add Compute Members eit Compute members to defir	her by creating o ne effective meml	r by directly adding to pership of the group.	nem. You can also add lo	lentity r
Membership Criteria (0)	Members (0)	IP Addresses (0)	MAC Addresses (0)	AD (
ACTIONS ~				
192.168.110.45				
Either MAC Address or AD groups can be	APPLY			

- 18. In the Select Members | SQL area,
 - Select the IP Addresses tab
 - In the IP Addresses tab under Actions enter 192.168.110.45
 - In the bottom right hand corner select APPLY

ADD (GROUI	Р						
				Name				Compute Members
				SQL			*	1 IPs
				Description		Description		Tags
		_	•	SAVE	CANCEL			
	:	>	0-0 0-0	Subnet 10				View Members

19. In the ADD GROUP area

Select SAVE

e	SOL X
e) dl	ADD GROUP
e	Name
h	🗹 : > 🖽 SQL
	🗌 🗄 > 🕀 Subnet 10
Ι.	
	1 - 2 of 2 Groups
	CANCEL

- 20. Ensure the **checkbox** next to **SQL** is selected
 - In the bottom right-hand corner select APPLY

RUCTURE (0)	ENVIRONMENT (0)	APPLICATION (2)
ELETE	1 Unpublished Change		
Sources	Destinations	Services	Profiles
(
ee Subnet 10	BB SOL	Any	None
/			

21. Under Services

• Select the **Pencil** next to **Any**

Rule > Block ICN	IP to SQL	
Services (1)	Raw Port-Protocols (0)	
ICMP ALL X		
ADD SERVICE		
	Name	Service Entries
	○	ICMPv6 ICMPv4
	CMP Destination Unreachable	ICMPv4 (Destination Unre
•	Up C	
1 2 9	> 1 - 50 of 409 Services	
1 2 9	> 1-50 of 409 Services	

22. In the **Set Services** window

- Scroll down and select the checkbox next to ICMP ALL
 - HINT, by typing ICMP in the box under services, it helps to find ICMP ALL

IDSH	ICMP ALL	None	뭄 Window
2DSH	○ НТТР	None	문콤 Window
?DSH	C) HTTPC) HTTPSC) ICMP ALL	None	DFW
QL	ᠿ ICMP ALL	None	DFW

Select APPLY

- 23. In the ${\it Block}$ ICMP to ${\it SQL}$ row,
 - Under Applied To select the Pencil next to DFW



24. In the Set Applied To window

• Change the **DFW radio** button to **Groups radio** button

	Set Applied To Rule > Marketing Rule	
(Select Applied To O DFW O Groups	-
	Name Name Image: State Stat	-

- 25. In the **Set Applied To** window select the **Groups** radio button
 - Select ADD GROUP

Set Applied To								
Rule > Marketing Rule								
Select Applied To 🔘 🛛	DFW 💽 Groups							
ADD GROUP								
	Name		Compute Members					
	Windows 10	* Description	Set Members	Tags				

26. In the **Set Applied To window**

- Under the **Name** area type **Windows 10**,
- Under Compute Members select the Set Members

Select Members	Windows	10
Add Compute Members ei Compute members to defi	ther by creating o ne effective meml	r by directly bership of th
Membership Criteria (0)	Members (0)	IP Addres
+ ADD CRITERIA		

- 27. In the Select Members | Windows 10
 - Select + ADD CRITERIA

Select Members Windows 10								
Add Compute Members either by creating or by directly adding them. You can also add Identity members sepa Compute members to define effective membership of the group.								
IP Addresses (0)	MAC Addresses (0)	AD Groups (0)						
me 🗸 Starts With	W10INST							
1 - 3 of 3 Groups								
	O r by directly adding th pership of the group. IP Addresses (O)	O r by directly adding them. You can also add to pership of the group. IP Addresses (0) MAC Addresses (0)						

- 28. In the Select Members | Windows 10 window under Criteria 1 select : -
 - Virtual Machine > Computer Name > Starts With > Type W10INST
 - Select APPLY

Set Applied To Rule > Marketing Rule Select Applied To 0	FW O Groups		
ADD GROUP	Name		Compute Members
	Windows 10 Description	* Description	1 Criteria
-	SAVE CANCEL		

- 29. In the **Set Applied To** window in the **ADD GROUP** area
 - Select SAVE

				-	
Select A	pplie	d To		DFW 💽 Groups	
Windo	ws 10	×)			
ADD G	ROUP				
				Name	
	8	>	88	External	
	÷	>	88	External_net	
	÷	>	0.0	RDSH	
	:	>	0.0	SQL	
	8	>	00	Subnet 10	
	:	>		Windows 10	
		1-6	of 6 G	roups	
Show C	nlv S	elec	ted		

- 30. In the **Set Applied To** window
 - Ensure the checkbox is selected next to Windows 10
 - In the bottom right corner select **APPLY**



31. Under Action

- Select the Drop down arrow next to Allow
- Select Reject

POLICY MANAGER
Change) ACTIONS V REVERT PUBLISH
Filter by Name, Path and more
Action
🕒 Uninitialized C 🛛 🕲
• _ Reject 🗠 🔍 🕲 🖂
Success C (0) (4)
I To Action
🕒 Success 🤭 🔞
• <u>Reject v</u> 🛞 🐼
Success C 🕓 🕸

- 32. In the top right hand corner of the NSX-T Admin Console
 - Select PUBLISH
 - Notice that the status Uninitialized now changes to Success

C. (windows)aystemac/emailere									
C:\Users\mark>ping sql.euc-livefire.com									
, Pinging sql.euc-livefire.com [192.168.110.45] with 32 bytes of data: Reply from 192.168.110.45: bytes=32 time<1ms TTL=127 Reply from 192.168.110.45: bytes=32 time=1ms TTL=127 Reply from 192.168.110.45: bytes=32 time=1ms TTL=127 Reply from 192.168.110.45: bytes=32 time=1ms TTL=127									
Ping statistics for 192.168.110.45: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 0ms, Maximum = 1ms, Average = 0ms									
C:\Users\mark>ping sql.euc-livefire.com									
Pinging sql.euc-livefire.com [192.168.110.45] with 32 bytes of data: Reply from 192.168.110.45: Destination host unreachable. Reply from 192.168.110.45: Destination host unreachable. Reply from 192.168.110.45: Destination host unreachable. Reply from 192.168.110.45: Destination host unreachable.									
Ping statistics for 192.168.110.45: Packets: Sent = 4, Received = 4, Lost = θ (0% loss),									
C:\Users\mark>_									
🖗 🣮 🚊 Options 🔻 🌵 Connect USB Device 💌 🛱 Send Ctrl-Alt-D									
Help Ctrl+H Support Information About VMware Horizon Client									
Switch to Other Desktop Autoconnect to This Desktop Enable Relative Mouse Share Folders									
Allow Display Scaling									
• COm Display >									
58.110.45] 🖷 Send Ctrl-Alt-Delete									
time=ims t← Disconnect time <ims and="" disconnect="" log="" off<br="">time=Ims TT=T=ZZ</ims>									

- 33. On your **ControlCenter** server
 - Revert back to your Horizon Client session

- From the CMD Prompt ping sql.euc-livefire.com
 - You will notice now you get a Destination Host Unreachable message
- Log-off from your Horizon Client session by going to Options dropdown
- Select Disconnect and Log Off
- Select OK to log Off

Part 2: Testing further Micro-segmentation scenarios with Distributed Firewall Rules

Introduction:

In this exercise we will look at variable options implement Micro-segmentation. Even with all the limitations we have in this lab setup. The variable options when configuring are impressive. The objective of Part 2 will be to follow on from Part 1 and we look at the variable options of the rules and how they work.

vm NSX-T					
Home Networking Sec	curity Inventory Plan & Troubleshoot System				
«					
🙆 Security Overview	ALL RULES CATEGORY SPECIFIC RULES				
East West Security					
📰 Distributed Firewall	ETHERNET (1) EMERGENCY (0) IN				
Ø Distributed IDS					
다. Network Introspection (E-W)					
North South Security	: V Desktops (1) Applied To DFW				
Gateway Firewall	Block ICMP to SQL 1025				
Be URL Analysis					
믾 Network Introspection (N-S)	: > Default Layer3 Sec (1) Applied To DFW				
Endpoint Protection					
🖽 Endpoint Protection Rules					

1. On your ControlCenter server,

- Switch back to your browser with your **NSX-T** session.
 - If necessary login with the username Admin and the password VMware1!VMware1!
- Ensure you have the **Security** tab selected and under **EAST WEST Security**

• Ensure your are in the **Distributed Firewall area**



- 2. On the NSX-T Admin Console
 - Select the **3 dots** next to **Desktops**
 - Select Add Rule

+ ADD F	POLICY	+ ADD RULE		CLON	⊑ ∽ U	NDC
		Name		ID		
: ~		Desktops	(4)		Applied To	D
:		ICMP for IT Support		5096		
:		Sales Rule		4076		7

- 3. In the New Rule interface,
 - Replace the name New Rule by selecting and typing Sales Rule

	C c	LONE	S UND	0 [DELETE		1 Unpublished Change
		ID			Sources		Destinations
	(2)		Applied To	DFW			
_					Any		
L		1025			ea Subne	t 10	응용 SQL
÷С	(1)		Applied To	DFW			

4. Under Sources,

• Select the **pencil** icon, next to **Any**

Set Source
Rule > Sales Rule
Negate Selections 🔵 No
Groups (1) IP Addresses (0)

- 5. In the **Set Source** window
 - Select ADD GROUP



- 6. In the **ADD GROUP** window
 - Under Name type Sales



7. Under Compute Members

Select Set Members

Select Members	Sales			
Add Compute Members eit Compute members to defin	ther by creating o ne effective memi	r by directly adding the bership of the group.	hem. You can also add Io	dentity members separately. Ide
Membership Criteria (O)	Members (0)	IP Addresses (0)	MAC Addresses (0)	AD Groups (0)
+ ADD CRITERIA				

8. In the **Select Members | Sales Group** window

• Select the AD Groups tab

Compute members to defir	ne effective meml	pership of the grou
Membership Criteria (0)	Members (0)	IP Addresses (C
Sales X		
Name		
Sales	*	

- 9. In the **search** area
 - Type Sales,
 - Select the checkbox next to Sales
 - Select APPLY



- 10. Back to the **Set Source** window
 - Select SAVE

_	•		unu -	-	
\square	:	>	D-D	RDSH	
	÷	>	0-0 0-0	Sales	
0	÷	>	0-0	COL	
			n-n	0	
	1.				
CAI	NCEL	A	PPLY		

- 11. In the **Set Source Rule** > **Sales** rule window
 - Ensure the check box to the left of Sales is selected for this rule
 - Select APPLY

:	Sales Rule	4076	23 Sales	Any	
---	------------	------	----------	-----	--

- 12. Under **Destinations** next to **Any**
 - Select the Pencil

RDSH	×				
ADD (GROUI	P			
				Name	
	÷	>	88	Marketing	
	÷	>		RDSH	_
	÷	>	8-8 8-8	SQL	
	÷	>	8-8	Subnet 10	
			1 - 4 of 4	4 Groups	
Sho	w On	ly Se	lected		
	CA	NCEL		APPLY	

- 13. In the **Set Destination** window
 - Select the checkbox next to RDSH
 - Select **APPLY** in the bottom right corner.

DELETE	1 Unpublished Cha	ange
Destinations	Services	Profile:
RDSH	Any 🗾 🖍	None
SQL	() ICMPv6 () ICMPv4-	None

14. In the **Sales Rule** row

• Under Services select the Pencil next to Any

Se	et Se	ervi _{Sales}	CES Rule	*		
				Name		
	÷	>	0	А СІМ-НТТР		
	÷	>	0	A CIM-HTTPS		
	÷	>	0	A HTTP		
	÷	>	0	A HTTPS		
	÷	>	0	A HTTPS, net.tcp binding		
\square	:	`	\sim	Δ		
-		~				
• 9	Succe	ss C				
■ Success C [*] ▼ 1 - 30 of 30 Services						
Show Only Selected						
CANCEL						

- 15. In the **Set Services** window
 - Under Services type http. Notice you now have the HTTP and HTTPS checkboxes available to select
 - Select the HTTP and HTTPS check boxes
 - Select **APPLY**

1 Unpublished Ch	Filter by	Name,	
Services	Profiles	Applied To	Actio
C HTTP C HTTPS	None	DFW 🖍	•
ICMPv6	None	DFW	•

16. In the **Sales Rule** row

• Under Applied To select the Pencil next to DFW



17. In the **Set Applied To** window

• Select the radio button next to Groups

	:	>	88	SOL	View Members	Success C
	1	>	88	Subnet 10	View Members	Success C
	÷	>		Windows 10	View Members	Success C
1	Св	FRES	(1 - 5 of 5 Group
						Show Only Selected

- 18. In the **Set Applied To** window,
 - Select the **check box**, next to **Windows 10**.
 - Select APPLY

Applied To	Action	
	• Uninitialized	чС
문 Wind	• Allow ~	

19. Under **Action.** We will leave the default Action that being **Allow**

		POLICY	MANAGER
•	ACTIONS ¥	REVERT	PUBLISH
оми	ENT (0)	• APPLK	CATION (3)
	Filter by Name	e, Path and i	more

- 20. In the NSX-T Admin Console
 - In the top right corner **PUBLISH**
 - We will now create a DENY ALL Groups Rule in addition to what we have just created

			Name		ID	
÷	~		Desktops	(2)		A¢
:			Marketing R	ule		
		\square	Riock ICMD	to	3048	
	Add	Rule				
Delete Rule I) A					A¢	
Clone Rule						
	Сор	y Rule				
	Past	e Rule				
	-					

- 21. In the NSX-T Admin Console > Security > Distributed Firewall
 - Right-Click the **3 DOTS** next the **BLOCK ICMP to SQL** checkbox
 - Select Add Rule

	Name		ID
: ~	Desktops	(4)	Apr
:	ICMP for IT Support		5096
:	Sales Rule		4076
	Deny All Groups		4074

22. Under your Sales Rule

In the New Rule section rename New Rule to Deny All Groups

					QF
÷.	Deny All Groups		Any	Any 🗾	Any
:	Block ICMP to SQL	3048	Subne	88 SOL	Ок Ск

23. In **Deny All Groups** rule row

• Under **Destinations** select the **Pencil** next to **Any**

Set Destination Rule > Deny All Groups Negate Selections () No Negated selections will be shown as i Groups (1) IP Addresses (0)						
ADD GROUP						
Name						
□ : > ^{DO} _{D-0} Marketing						
✓ : > 88 RDSH						
□ : > \$\$ SQL						
U : > BB Windows 10						
1-5 of 5 Groups						
Show Only Selected						
CANCEL						

- 24. In the **Set Destination** window,
 - Select the **checkbox** next to **RDSH**
 - Select APPLY

	Name		ID	Sources	Destinations	Services	Profiles	A
: ~	Desktops	(3)	Applied To	DFW				
1	Marketing Rule			80 Marke	SS RDSH	🔿 НТТР	None	
						🔿 HTTPS		
:	Deny All Groups			Any	88 RDSH	Any 🧪	None	[
:	Block ICMP to SQL		3048	Subne	SS SQL	C ICMPv	None	ſ
						C ICMPv		
: >	Default Layer3 Section	(1)	Applied To	DFW				

- 25. In the **Deny All Groups** row under **Services**
 - Select the **Pencil** next to **Any**

Set Services								
Ru	Rule > Deny All Groups							
S	Services (0) Raw Port-Protocols (0)							
[http							
C	ADD :	SERVI	CE					
					Name			
			>	0	В СІМ-НТТР			
			>	0				
			>	0	аттн			
			>	0	₿ HTTPS			
			>	0	HTTPS, net.tcp binding			
			>	0	ති Office Server Web Services. HT			
					Name			
		:	>	0	A CIM-HTTP			
	_	÷		-				
	_	-	'	0	CIM-HTTPS			
_	~		>		[⊕] HTTP 2			
1	~		>		HTTPS			
- (÷	>	0	HTTPS, net.tcp binding			
1		:	`	\sim	۵			
-		-						
-	Succe	HS C						
	Succe	255.0	1-30	of 30 Ser	vices			
	S	how O	niy Sel	ected (<u> </u>			
		¢	ANCEL	AS	PPLY			

- 26. In the **Set Services** window
 - 1. under **Services** type **http**. Notice you now have the **HTTP** and **HTTPS** checkboxes available to select
 - 2. Select the **HTTP** and **HTTPS** check boxes
 - 3. Select **APPLY**

1 Unpublished Cf	nange	Filter by	Name,
Services	Profiles	Applied To	Actio
C HTTP	None	DFW 🖍	•
CMPv6	None	DFW	•

27. In the **Deny All Groups** row under **Applied To** select the **Pencil** next to **DFW**

	Set Applied To Rule > Marketing Rule
C	Select Applied To 🔿 DFW 💿 Groups
	ADD GROUP
	Name Marketing

28. In the **Set Applied To** window select the **Groups** radio button

ADD	GROU	•				EXPAND ALL
				Name	Compute Members	Status
	÷	>	80	Marketing	View Members	● Success C
	÷	>	88	RDSH	View Members	● Success C
	÷	>	88	SOL	View Members	Success C
	÷	>	88	Subnet 10	View Members	● Success C
		>	88	Windows 10	View Members	Success C

29. In the Set Applied To window

- Select the Windows 10 group checkbox
- Select Apply

DELETE	1 Unpublished Cha	nge	Filter by	Name, Path a	nd more	Ŧ
Destinations	Services	Profiles	Applied To	Action		
				•	Success (. 0 @
88 RDSH	C HTTPS	None	0-0 Windows	Allow	<u>~</u>	@ 🖸
88 RDSH	HTTP HTTPS	None	0-0 Windows	Allow	× •	@
SQL	C ICMP ALL	None	0-0 Windows	 Reject 		ø 🛛
				•	Success (; © ¢

30. In the **Deny All Groups** row

- Under Action select the Dropdown
- Select Drop

nges) ACTIO	NS REVERT	PUBLISH
ICATION (4)		
Filter by Name	, Path and more	_ =
Applied To	Action	
	Success C	00
문급 Windo		@ №
BB Windo	• Drop 🗸 🌑	@ 🗠
DFW	• Reject V	¢ 🗠
	Success C	C @

- 31. In the top right corner, of the NSX-T Admin Console
 - Select PUBLISH
 - We have now completed two rules both based on the Source .
 - Our last set of Rules will Aimed at the Destination Server services

Home Networking	Security Inventory Plan & Troubles
~	
Security Overview	ALL RULES CATEGORY SPECIF
East West Security	
🖽 Distributed Firewall	ETHERNET (1)
Distributed IDS	+ ADD POLICY + ADD RULE
믹 Network Introspection (E-W)	Name
North South Security	: > Desktops
🔠 Gateway Firewall	:> Default Layer3 Secti
Gateway Firewall हिह्। URL साम्याप्रडाड	
밐 Network Introspection (N-S)	

- 32. NSX-T Admin Console > Security > Distributed Firewall
 - Under CATEGORY SPECIFIC RULES in the APPLICATION section select +ADD POLICY

	ETHERNET (1) EMERG
0	+ ADD POLICY + ADD RULE
	Name
	: > New Policy
	> Desktops
)	Default Layer3 Section
·	

33. You will notice you have a **New Policy** .1st in the policy order. We will now re-order this policy

+ ADD POLICY	+ ADD RULE	CLONE	ς n	ido į	Î] DELETE
	Name		ID	5	Sources
: >	New Policy	(0)	Αŗ	oplied To	DFW
	Desktops	(3)	A	oplied To	DFW
	- New Policy	(0)	A	pplied To	DFW
·:> □	Default Layer3 Sect	ion (1)	Ap	oplied To	DFW
ETHE	ERNET (1)	EMERGENCY (0)			
+ ADD PO	LICY + ADD RULE	CLONE	S UN		
	Name	I	D		
: >	Desktops	(3)	Ap		
2	New Policy	(0)	Ap		
S)	Default Layer3 Sect	tion (1)	Ap		

- 34. In the NSX-T Admin Console > Security > Distributed Firewall
 - Select with a left click and hold your mouse on the 3 DOTS at the beginning of the New Policy Line
 - Drag the New Policy down till just after Desktop Policy and release your mouse
 - Your **New Policy** should appear in the order in the second screenshot of this image

	· · · · ·	~	
Security Overview	ALL RULES	CATEGORY SPECIFIC	RULES
East West Security			
🖽 Distributed Firewall	ETHER	NET (1) E	MERGENCY (0)
Ø Distributed IDS	+ ADD POLIC	CY + ADD RULE	CLONE SUNDO
고 Network Introspection (E-W)		Name	ID
North South Security	: > □	Desktops	(3) Applied 1
Gateway Firewall	: > □	Server Access	(0) Applied 1
Bel URL Analysis	:> [Default Layer3 Section	n (1) Applied 1
믾 Network Introspection (N-S)			
Endpoint Protection			

35. In the NSX-T Admin Console > Security > Distributed Firewall

• In the New Policy interface, rename New Policy to Server Access

Ē	3	DISTI	RIBUT	ED FIREW	/ALL	?		
A	LL F	RULE	S	CATEGO	RY SPE	ECIFIC	RULES	
		E	THERNE	ET (1)		E	MERGENCY (0)
	+ 4		POLICY	+ A	DD RUL	E	CLONE	∽ ر
				Name				ID
)	>		Desktor	os		(3)	4
	`			Server /	100000		(0)	Ļ
		Ena	ble Lo	gging For	All Ru	les	(1)	Ļ
		Ena	ble All	Rules	r All Ru	lies		
		Disa	able Al	I Rules				
		Dele	ete Po	licy				
		Add	l Rule]			
		Add	l Polic	y Below				
:	>			Desktops			(3)	
1	~			Server Ad	cess		(1)	
3				New Rule				
1	>			Default L	ayer3 Se	ection	(1)	

36. In the **NSX-T Admin Console** > **Security** > **Distributed Firewall**

- Select the 3 DOTS in front of your Server Access Policy and select Add rule
 - Notice you now have a new rule called New Rule that is part of the Server Access Policy



37. In the New Rule section,

Rename New Rule to Permit Win 10 to RDSH

	E	THERNET	(1)	EMERGENCY (C))	INFRASTRUCTURE	E (0) ENV
	+ add	POLICY	+ ADD RULE	CLONE	S UNDO	III DELETE	··· 2 Unpubl
			Name		ID	Sources	Destinations
	: >		Desktops	(3)	Applied	To DFW	
	: ~		Server Access	(1)	Applied	TO DFW	
	÷		Permit Win 10 to RD	DSH		Any 🧪	Any
_	: >		Default Layer3 Sect	tion (1)	Applied	To DFW	

38. In the **Permit Win10 to RDSH** section

• Under Sources, select the Pencil next to Any

	200		2 Addr	esses (0)		
Wind	dows 1	0 X				
ADD	GROU	IP				EXPAND ALL
				Name	Compute Members	Status
0	÷	>	88	External	View Members	Success C
	÷	>	28	External_net	View Members	Success C
0	1	>	88	Marketing	View Members	Success C
		>	20	RDSH	View Members	Success C
0	÷	>	20	SQL	View Members	😑 Success 🖱
0	÷	>	20	Subnet 10	View Members	Success C
2		>	80	Windows 10	View Members	Success C
1	CR	EFRES	н			1 - 7 of 7 Group

39. In the **Set Source** window,

- Select the checkbox next to Windows 10
- Select APPLY

E	DIST	RIBUTE	D FIREWALL					
	ALL RULE	es o	CATEGORY SPECIFI	C RULES				
	E	THERNET	τω	EMERGENCY (0)	INF	FRASTRUCTURE	: (0)	ENVIRONMENT (
	+ ADD I	POLICY	+ ADD RULE	CLONE	UNDO	ी DELETE	••• 2 Ur	npublished Change
			Name	ID		Sources	Destinations	Services
	: >		Desktops	(3)	Applied To	DFW		
	÷ ~		Server Access	(1)	Applied To	DFW		
	÷		Permit Win 10 to RDS	SH		So Windo	Any 🧪	Any
Į	: >		Default Layer3 Section	on (1)	Applied To	DFW		

40. In the **Permit Win10 to RDSH** section

• Under **Destinations**, select the **Pencil** next to **Any**

Broup	os (1)	IF	> Addr	resses (0)	or we way	
RDSH	нх					
ADD	GROU	Ρ				EXPAND ALL
				Name	Compute Members	Status
	÷	>	80	Marketing	View Members	Success C
2		>	88	RDSH	View Members	Success C
	÷	>	80	SQL	View Members	Success C
	÷	>	80	Subnet 10	View Members	Success C
	:	>	00	Windows 10	View Members	Success C
1	C R	EFRES	н			1 - 5 of 5 Grou
						Show Only Selected

- 41. On the **Set Destination** window,
 - Select the **checkbox** next to **RDSH**
 - Select APPLY

			EMERGENCY (0)		INFRASTRUCTUR	E (0) E	NVIRONMENT (0)	
+ ADD	POLICY	+ ADD RULE	CLONE	S UNDO	III DELETE	(2 Uni	oublished Changes	
		Name		ID	Sources	Destinations	Services	Profiles
: >		Desktops	(3)	Applied 1	TO DFW			
: ~		Server Access	(1)	Applied 1	TO DFW			
£		Permit Win 10 to RD	SH		😵 Windo	28 RDSH	Any 🧪	None
: >		Default Layer3 Secti	on (1)	Applied 1	To DFW			

- 42. In the **Permit Win 10 to RDSH** row under **Services** select the **Pencil** next to **Any**
 - Set Services Rule > Deny All Groups 0 http ADD SERVICE □ : > ○ @ CIM-HTTP □ : > ○ @ CIM-HTTPS 🗌 : > 🔿 🔒 нттр □ : > ○ ⊕ HTTPS □ : > ○ @ HTTPS, net.tcp binding □ : > O Ô Office Server Web Services. HT. □ : > ○ ⊕ CIM-HTTPS HTTP 2 > ₿ HTTPS 🔒 HTTPS, net.tcp bi Show Only Selected 3 CANCEL
- 43. In the **Set Services** window
 - 1. Under **Services** type **http**. Notice you now have the **HTTP** and **HTTPS** checkboxes available to select
 - 2. Select the HTTP and HTTPS check boxes
 - 3. Select **APPLY**

2 Uni	oublished Changes	Filter by Name, Path and			
estinations	Services	Profiles	Applied To	Action	
				•	
RDSH	🔿 нттр	None	DFW 🧪	Allow	
	C HTTPS]	
				•	

44. In the **Permit Win 10 to RDSH** row

• Under Applied To select the Pencil next to DFW

Set Applied To Rule > Marketing Rule
Select Applied To 🔿 DFW 💽 Groups
ADD GROUP

45. In the **Set Applied To** window select the **Groups** radio button

ect	Appi	ed to	.0	DPW U Groups		
RDS	+×)					
NDD	GROU	Ρ				EXPAND A
				Name	Compute Members	Status
	÷	>	88	IT Support	View Members	Success C
	÷	>	88	Marketing	View Members	Success C
~		>	80	RDSH	View Members	Success C
	÷	>	88	SQL	View Members	Success C
	÷	>	88	Subnet 10	View Members	Success C
	÷	>	88	Windows 10	View Members	Success C
1	CR	FRES				1 - 6 of 6 (

46. In the **Set Applied To window**

- Select the **RDSH** group **checkbox**
- Select Apply

nges ACTIONS REVERT PUBLISH
Filter by Name, Path and more
Applied To Action
🌒 Success 🔿 🔞
0 @
Po Windo • Allow ~ 💽 🛞 🖂
🌒 Success 🔿 🔘 🏟

47. Select **PUBLISH** in the top right corner



49. Please NOTE: When **Identity Based Firewall** rules are applied, it is essential, to logon after the rules have been applied. Any Active VMware Horizon sessions that you are logged into, **Disconnect and Log Off** before starting with Part 3

Part 3. Testing the results

Some background information about our setup and what we are going to test.

- In this setup we have a Horizon Instant Clone Desktop pool with 4 Virtual machines
- The Desktop Pool has two Active Directory security groups entitled to this Desktop Pool
 - IT-Support
 - Sales
- All 4 virtual Machines are running on the 172.16.10.0 / 24 subnet and have a VLAN ID 10 for this subnet configured for its NSX-T segment.
- As part of the test we have a server with IIS installed called RDSH-01a
- Note this exercise is teaching Micro-segmentation functionality and one should not read anything into the choice of group name for this exercise.
 - We will first Test *Mark Debio* and *Jill Verneo who are members* of the **Sales** group. Mark and Jill will do a HTTP connection to the **RDSH-01a** server.
 - We will then test **Kim Markez** who is *not a member* of the **Sales** Group and see what happens when attempt to do a connection request to **RDSH-01a**

Part 3 :



- 1. On your **ControlCenter** desktop,
 - Launch the Horizon client
 - Launch the Horizon .euc-livefire.com POD
 - On the Login window next to
 - User name: Mark
 - Password : VMware1!
 - Select Login
 - Select the W10INST entitlement



- 2. On your ControlCenter desktop, launch the Horizon client
 - Launch the Horizon.euc-livefire.com POD
 - On the Login window next to
 - User name: Jill
 - Password : VMware1!
 - Select Login
 - Select the W10INST entitlement



- 3. On your ControlCenter desktop, open the Remote Desktops folder
 - 1. Launch the **RDP** client for **W10Ext01a.RDP**
 - Login as administrator@euc-livefire.com with password VMware1!
 - 2. On the W10 client Launch the Horizon client
 - Launch the Horizon.euc-livefire.com POD
 - On the login window next to
 - User name: kim
 - Password : VMware1!
 - Select Login
 - Select the W10INST entitlement

••• 🕸 🏎		
	$\beta = g_{\text{those}} + \delta d_{\text{convergent Decker + \Delta \text{ sense}} + \delta (22345)e^{-\delta - \delta e_{\text{c}} X_{\text{term}}} - \delta \times$	
0 13		
Bropile Sie Blad Bare Backrasser	- 🔁 🗗 🖂 IIS Windows Server X + V - D X	
💷 📰	← → Ů ⑥ odot-01aeuc-livefire.com/	
Without Without	🗮 Windows Server	
Catalor Mangad	Internet Information Services	
All and a second		
100 Palar Lass Palar	Appendence de la construcción de la constru	
Kongood Kongood	Rem-vindo Kalvúz Apópo	
RE-PENAL	vinger oplostic Valcommen ≌18181417 norakosana ldaväzõijaik.	
1.50 Kappani	Microsoft Wilkommen Mikommen Water	
10 million		1 8
100 miles (100 miles)		
and a star		NE
and the second second		K
E P Type here	re to search 28 🤮 15 Windows Servar 🕞 🏦	^ 〒 40 436 AM

- 4. Select your Mark Horizon client session
 - On the Desktop, select and launch the Edge Browser in the Task Bar
 - In the Edge Browser address, type http://rdsh-01a.euc-livefire.com
 - As you can see we are able to connect to the web service on the server as Mark.
 - Repeat the same test for Jill



- 5. Switch to your **Kim** Horizon client session running from **W10EXT01a**
 - On the Desktop, select and launch the Edge Browser in the Task Bar
 - In the Edge Browser address, type http://rdsh-01a.euc-livefire.com
 - **Kim** is not a member of the **Sales Group** and would therefore be denied access. Our **Identity Firewall** only allows for **Sales** to communicate with the **RDSH-01a** server.
 - From the Horizon Client
 - Select the **3 dots** in the right corner
 - From the dropdown, select Logoff Desktop
 - In the Disconnect and log off desktop? window,
 - Select OK



- 6. Switch back to your NSX-T admin console. Ensure you are still in **Security** > **Distributed Firewall**
 - Select 3 Dots next to Desktops Policy and select Add Rule,
 - Notice you now have a New Rule

wall ETHERNET (1) EMERGENCY (0) INFRAST bection (E-W) + ADD POLICY + ADD RULE CLONE UNDO III Name ID Sources III Desktops (4) Applied To DFW III I ICMP for IT supp Any	5M	ALL RULES	CATEGORY SPEC		
Hection (E-W) + ADD POLICY + ADD POLICY + ADD POLICY + ADD RULE CLONE • Oundo • Oundo <td>wall</td> <td>ETH</td> <td>IERNET (1)</td> <td>EMERGENCY (0)</td> <td>INFRAST</td>	wall	ETH	IERNET (1)	EMERGENCY (0)	INFRAST
Image:	ection (E-W)	+ ADD PC	Name	CLONE	Sources
	3]]	÷ ↓ ÷	Desktops (4) ICMP for IT supr.	Applied To	DFW Any

7. In the New Rule row replace New Rule with ICMP for IT Support

+ ADD POLI	сү	+ ADD RU	JLE	CLONE	S UNDO	DELETE
		Name		ID	Sources	Destina
: •		Desktops	(4)	Applied To	DFW	
: 0		ICMP for IT Cu	pr -		Any 📝	Any
: 0		Marketing Rul	e	3049	Harketing	분용 RI

8. In the ICMP for IT Support row under SourcesSelect the Pencil next to ANY

Set Source
Rule > ICMP for IT Support
Negate Selections No Negated selections
Groups (0) IP Addresses (0)
ADD GROUP
Name

9. In the Set Source window select ADD GROUP

ADD GROUP				
	Name		Compute Members	
	IT Support		Set Members	
	Description	Description	Та	gs
	SAVE CANCEL			

- 10. Under the **ADD GROUP** area under **Name** type **IT Support**
 - Under Compute Members, select Set Members

Membership Criteria (0) Members (0)	IP Addresses (0)	MAC Addresses (0)	AD Groups (0
IT supp			
Name			
IT Support			
Name			
IT Support			
1 - 1 of 1 AD Groups			
groups can be part of a Group			

- 11. In the Select Members | IT Support window
 - Select the AD Groups tab
 - Under AD Groups start typing IT Supp
 - Select the checkbox next to IT Support
 - Select **APPLY** in the bottom right corner

Name		Com	pute Members
IT Support		* 1 AD	Groups
Description	Description		
SAVE CAN	ICEL		
	-		
1 - 5 of 5 Groups	5		
elected 🔵)		
	Name IT Support Description SAVE CAN 1 - 5 of 5 Groups Gelected	Name IT Support Description Description I - 5 of 5 Groups Gelected	Name Com IT Support 1AD Description Description SAVE CANCEL 1 - 5 of 5 Groups Selected ①

12. Select **SAVE**

• Select **APPLY** to close the **Set Source** window

LICY	+ ADD RULE	CLONE	UNDO C	Ü DELETE	1 Unpublish
	Name	ID	Sources	Destinations	Services
	Desktops (4)	Applied To	DFW		
	ICMP for IT Su		Hand IT Support	rt Any 🧪	Any
	Marketing Rule	3049	0-0 0-0 Marketing	g 🚼 RDSH	() НТТР() НТТРS

- 13. In the ICMP for IT Support row under Destinations
 - Select the **Pencil** next to Any

ule >	ICM	P for	IT Sup	port
legate	e Sele	ection	is O	No Negated selection
Group	s (I)	11	Addr	esses (O)
RDSH	IX)			
ADD	GROU	Р		
		_		Name
		>	0-0	IT Support
-			80	Marketing
0	-	>	66	Marketing
	1	>		RDSH
	÷	>	80	SQL
			1 -	6 of 6 Groups
Shou	~ ~	alv	مام	sted
51101	101	iny .	00101	
ſ				
	C	NIC	EL.	

- 14. In the **Set Destination** window
 - Select the **checkbox** next to **RDSH**
 - Select Apply

		n no lo nico e no nico (oy		
LONE	S UNDO	ÎII DELETE •••	1 Unpublished Ch	ange
	Sources	Destinations	Services	Profiles
pplied To	DFW			
	B-B IT Suppo	rt 🖁 RDSH	Any 🖍	None
	₽₽ Marketin	g 🔡 RDSH	🛟 НТТР 🌔 НТТРS	None

15. In the **ICMP for IT Support** row

• Under Services select the Pencil next to Any

Set Services Rule > ICMP for IT Support
Services (0) Raw Port-Protocols (0)
ADD SERVICE
Name

16. In the **Set Services** window , type **ICMP**

	ADD SERVICE
	Name
	ICMP ALL
	Success C
	Success C
-	Success C
	1 - 23 of 23 Services
	Show Only Selected
	CANCEL

- 17. Select the **checkbox** next to **ICMP ALL**
 - Select APPLY

	1 Unpublished Ch	ange	Filter by	Nam
ons	Services	Profiles	Applied To	Ac
н	CMP ALL	None	DFW 🧪	
н	673 НТТР	None	₽₽ Window	-

- 18. In the ICMP for IT Support row under Applied To
 - Select the **Pencil** next to **DFW**

Set Applied To
Select Applied To 💿 DFW 🔵 Groups

- 19. In the **Set Applied To** window
 - Change the **DFW radio** button to the **Groups radio** button

Sot	Anr	lior		
Rule >	ICMI	P for I	IT Sup	port
Select	Appl	ed To		DFW 💿 Groups
Wind	nue 1			
ADD	SROU	P		
				Name
	÷	>	80	IT Support
	÷	>	20	Marketing
	ł	>	00	RDSH
	÷	>	9-0 0-0	SQL
	÷	>	80	Subnet 10
		>	88	Windows 10
				1 - 6 of 6 Groups
Sł	nov	or	nly S	elected 🔵
				_
	ſ	CA	NCE	L APPLY

20. In the Groups Area

- Select the checkbox next to Windows 10
- Select APPLY

+ ADD	POLICY	+ ADD RULE	CLONE	S UNDO 🗍	DELETE	1 Unpublished Ch	ange
		Name	ID	Sources	Destinations	Services	Profiles
• •		Desktops (4)	Applied To	DFW			
:		ICMP for IT Su_	3052	Po IT Support	88 RDSH	C ICMP ALL	None
:		Marketing Rule	3049	BO Marketing	Sta RDSH	HTTP HTTPS	None
:		Deny All Grou	3050	Any	28 RDSH	O HTTP	None
:		Block ICMP to	3048	5-0 Subnet 10	SS SOL	C ICMP ALL	None

21. In the **Deny All Groups** row under **Services**, select the **Pencil** next to **HTTP/HTTPS**

S	iet S	Serv	vice	S		
R	ule >	Deny	/ All (Groups	S	
5	Service	es (2)		Raw P	ort-Proto	ocols (0)
	HTTP	×	НТ	TPS X)	
Ч	ADD S	SERVI	CE			J
					Name	
		:	>	0	₿ ICMF	P ALL
-	\square	:	>	ch	A	

22. In the **Set Services** window under **Services** type **icmp**

HTTP X HTTPS X ICMP ALL X icmp ADD SERVICE ADD SERVICE Name Image: Service in the	Servic	es (3))	каw н	OFT-PLOTOCOIS (O)
HTTP X HTTPS X ICMP ALL X icmp Name ADD SERVICE Name Image: Service Image: Service Image: Success C Image: Success C					
ICMP ADD SERVICE Image: Supervise of the second s	HTTF	×	HT	TPS 🗙	ICMP ALL X
ADD SERVICE Name Image: Success C Success C Success C 1-23 of 23 Services	icmp				
ADD SERVICE Name Image: Supervise in the second s					
Name Image: Name <	ADD	SERVI	CE		
Name Image: Name <					
 ICMP ALL ICMP Destination Unrea ICMP Destination Unrea ICMP Destination Unrea Success C Success C Success C Success C 1-23 of 23 Services 					Name
		÷	>	0	A ICMP ALL
□ : > ○ ICMP Destination Unreal □ : > ○ A ICMP Echo Reply ● Success C					
ICMP Destination Unrea			>	0	£
Success C Success C 1-23 of 23 Services					ICMP Destination Unrea
Success C Success C 1-23 of 23 Services	\square	:	>	<i>6</i> %	A ICMP Echo Reply
Success C Success C 1 - 23 of 23 Services	• s	lucces	ss C		
Success C 1 - 23 of 23 Services	• 5	lucces	ss C		
Success C 1 - 23 of 23 Services					
1 - 23 of 23 Services	_ S	lucces	ss C		*
				1-3	23 of 23 Services
Show Only Selected		Sh	ow O	nly Se	lected 🔵
			_		
			с	ANCE	L APPLY
CANCEL AFFET			_		
CANCEL					

- 23. Select the **check box** next **ICMP ALL**
 - Select APPLY

)48	뭅 Subnet	器 SQL	CMP A	None
Applied To	DFW			
)51	₽-ª Windo	RDSH	♦ HTTP ♦ HTTPS	None
Applied To	DFW			

- 24. Expand the Server Access Policy
 - In the **Permit W10 to RDSH** row under **Services**, select the **Pencil** next to **HTTP/HTTPS**

Set Services
Rule > Permit W 10 to RDSH
Services (2) Raw Port-Protocols (0)
HTTP X HTTPS X
ADD SERVICE
Name
□ : > ۞ A ICMP ALL

25. In the **Set Services** window under **Services** type **icmp**

				Name
	÷	>	0	A ICMP ALL
cess C	:	>	0	· · · · · · · · · · · · · · · · · · ·
Show C	nly S	- 23 of Select	ed (

- 26. Select the **check box** next **ICMP ALL**
 - Select APPLY

	Q	Â	?`	admin ~
1 Total Unpublished Char	nge A	CTIONS ~	REVERT	PUBLISH
	ATION (6)			

27. Select PUBLISH

E	THERNET	r eta 🔰 i	EMERGEN	CY (0)	INFRASTRUCTU	RE (0)	ENVIRONMENT (0)		APPLICATION (6)		
+ ADD I	POLICY	+ ADD RULE	CL0		🗍 DELETE	@	Unpublished Change		Filter by Na	me, Path and more	-
		Name		ID	Sources	Destinations	Services	Profiles	Applied To	Action	
- ×		Desktops	(4)	Applied To	DFW					Succe	ss C O
:		ICMP for IT Support		3052	SS IT Supp	SS RDSH	C ICMP A	None	SS Windo	• Allow ~	0 @ 5
:		Marketing Rule		3049	88 Marketi	28 RDSH	O HTTP O HTTPS	None	88 Windo.	• Alow 🗸	0 @ 0
:		Deny All Groups		3050	Any	22 RDSH	O HTTP HTTPS C ICMP A	None	22 Windo.	• Reject ~	0 @ 0
:		Block ICMP to SQL		3048	Stubnet	88 SOL	C ICMP A	None	DFW	🔸 Reject 🗸 🌘	0 0 0
- ×		Server Access	(1)	Applied To	DFW					Succe	sc O
:		Permit W 10 to RDSH		3051	Be Windo	BB RDSH	HTTP HTTPS CICMP A	None	22 Windo	• Alow 🗸	0 @ 0
>		Default Layer3 Sectio	in (1)	Applied To	DFW					Succe	sc o

28. Review your **Policies** and associated **Rules**

🖧 https://horizon.euc-livefire.com	
kim	
•••••	
Cancel Login	
VMware Horizon Client	
<	
ttps://horizon.euc-livefire.com	
WIDINST	
WIDClientI - WIDClientI Lauc-livefie.com - Fernete Dastop Connection Ø ♀ Ø ♀ Ø ♀ Ø ♀ Ø ♀	- 🗆 ×
Nay Alfa de Margari Par Jan Sangari Nanga, Dalam Par Jan	
And a man and a man a man and a man and a man and a ma	S S
Construction of programs Nation councers a single and the second se	

29. On your WinEXT10 RDP session.

- Using the Horizon client login again as Kim with the password VMware1!
- Launch the **W10INST**, entitlement
- From the **Start** menu > **RUN** > type **cmd.exe**
- Select OK



- 30. In the **cmd.exe** window type, ping **rdsh-01a.euc-livefire.com**.
 - Your micro-segmentation rules using the Identity Firewall setting should **ALLOW** and you should get a reply.



31. On your **ControlCenter** server desktop, revert back to your **Mark horizon** client session

- If the session is disconnected and logged off. Log back in as Mark with the password VMware1!
- Launch CMD.exe window from RUN if this is closed.
- In the **cmd.exe** window type, ping **rdsh-01a.euc-livefire.com**.
 - Your micro-segmentation rules using the Identity Firewall setting should DENY and you should not get a reply.

References

VMware documentation

- https://docs.vmware.com/en/VMware-NSX-T-Data-Center/3.0/administration/ GUID-41CC06DF-1CD4-4233-B43E-492A9A3AD5F6.html
- https://docs.vmware.com/en/VMware-NSX-Data-Center-for-vSphere/6.3/ com.vmware.nsx.admin.doc/GUID-C7A0093A-4AFA-47EC-9187-778BDDAD1C65.html

NSX-T Data Center and EUC Design Guide

<u>https://communities.vmware.com/docs/DOC-40565</u>

Acknowledgements

A huge thank you to Baldeep Birdy from the NSX Livefire Team.

Without his support in troubleshooting and help in the development of this session

Notes about the author Reinhart Nel

https://www.livefire.solutions/meet-the-team/reinhartnel/

For any questions related to this session, email Reinhart at RACE-Livefire-EUC@vmware.com