

NSX-T based Micro-segmentation with VMware Horizon

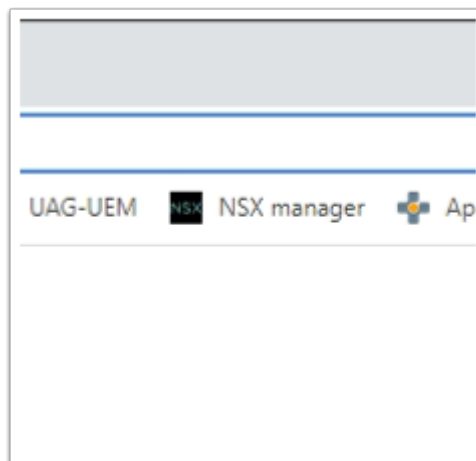
Setting up a Distributed Firewall

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 Micro-segmentation 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.

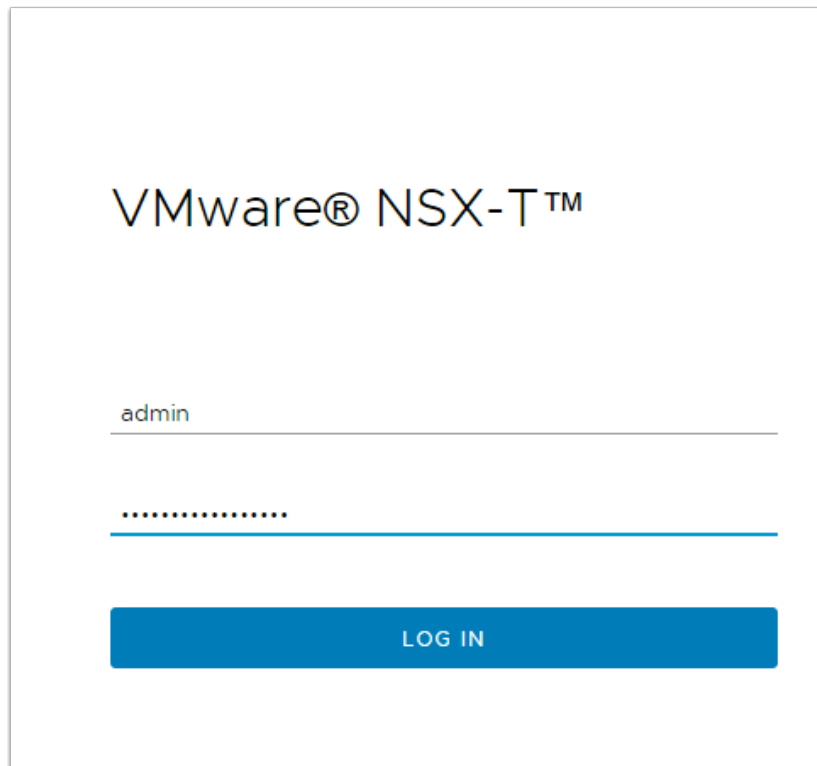
Real World Scenarios will be vastly more complex and time consuming to configure.

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™

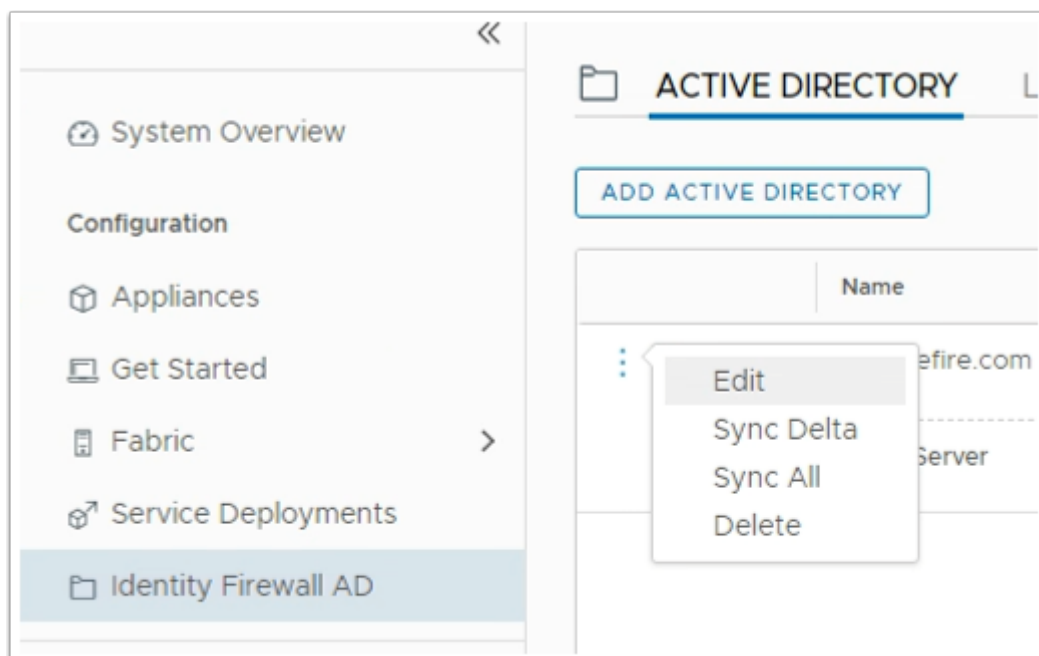
admin

.....

LOG IN

2. On your Browser

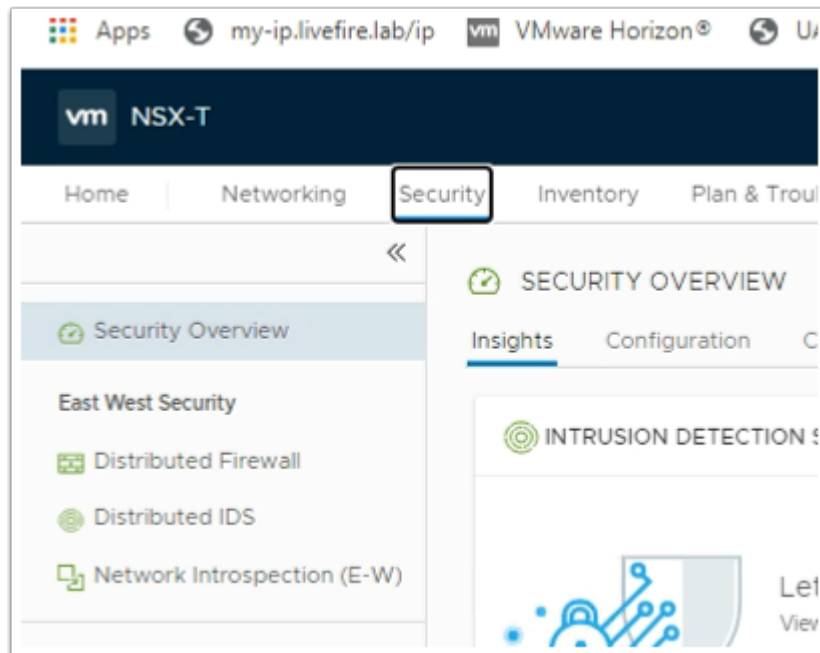
- Login with Username **admin**
- With the password **VMware1!VMware1!**
- Select **LOG IN**



3. In the NSX Admin Console

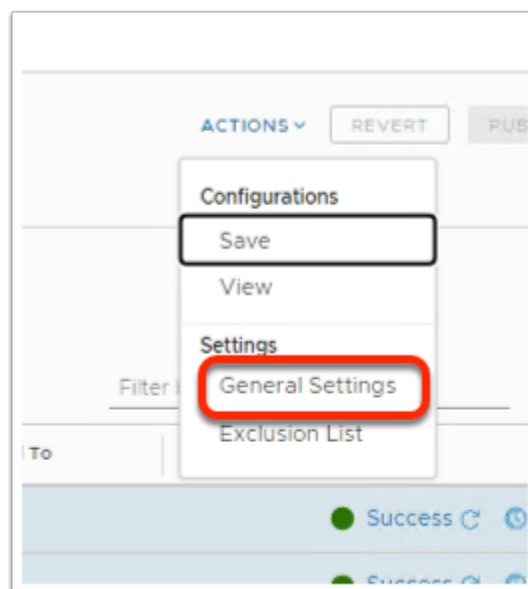
- At the top of the NSX-T admin console select **System**
- Under **Configuration**, select **Identity Firewall AD**

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



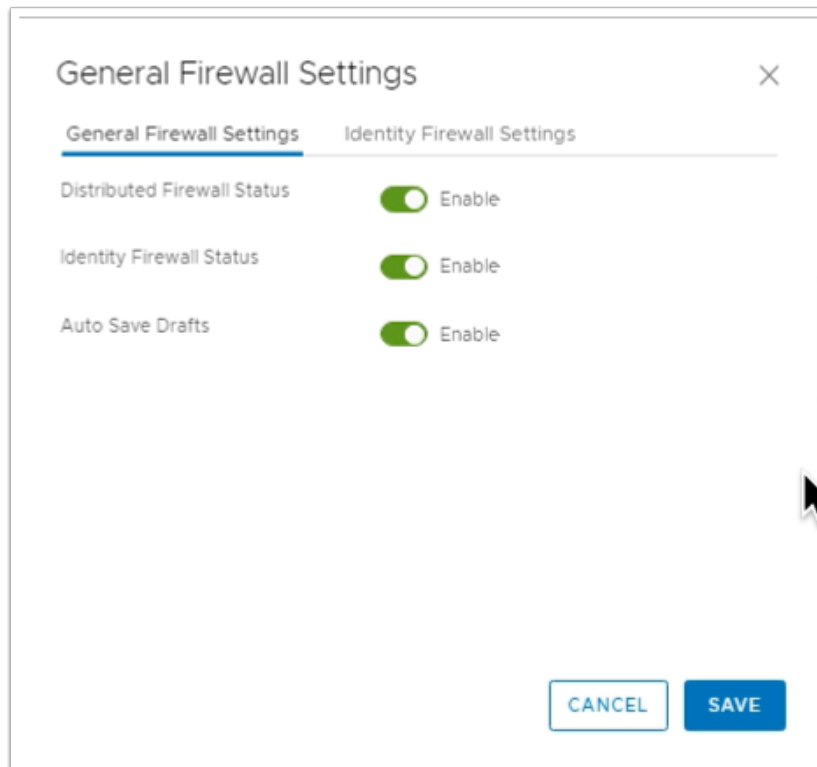
4. In the NSX Admin Console

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

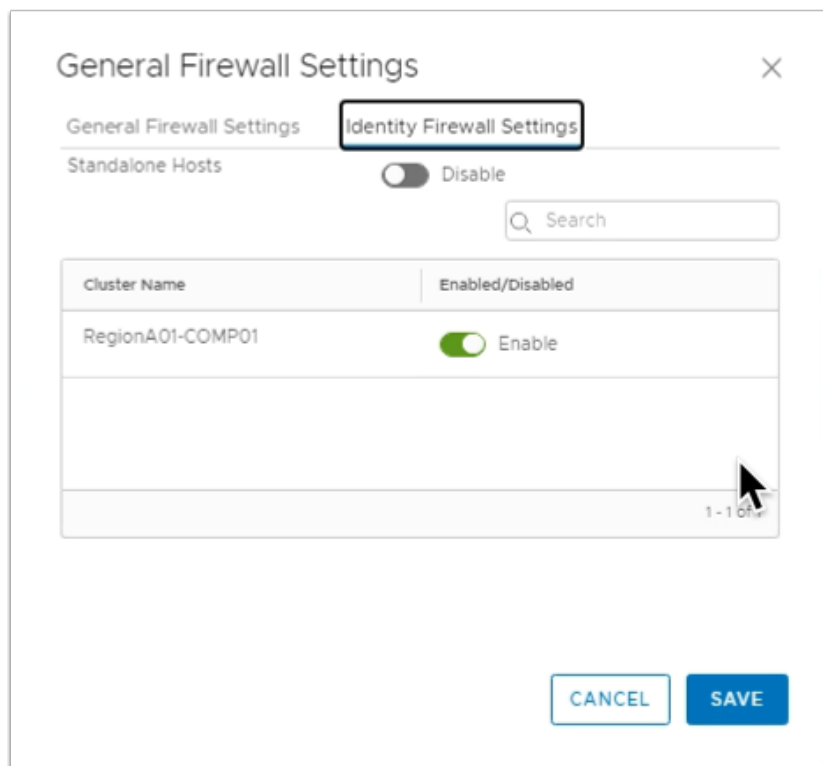


5. In **Distributed Firewall** area

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



6. In the **General Firewall Settings**
- Select **Identity Firewall Settings** tab

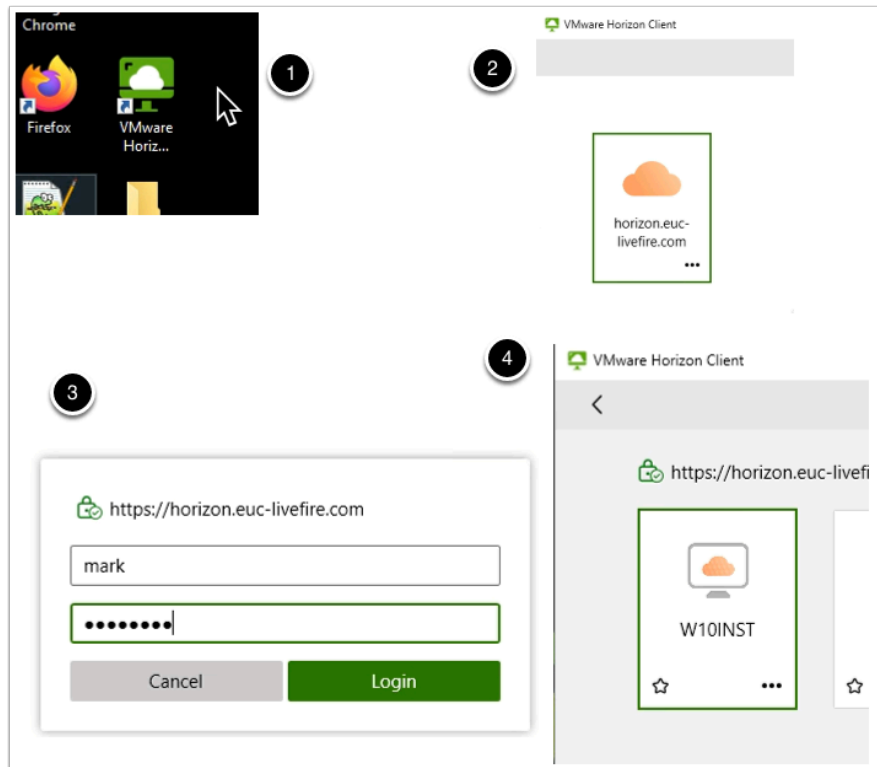


7. In the **General Firewall Settings**
- Under **Identity Firewall Settings**
 - Next to **RegionA01-COMP01, Cluster Name**, ensure the **toggle** is set to **Enable**

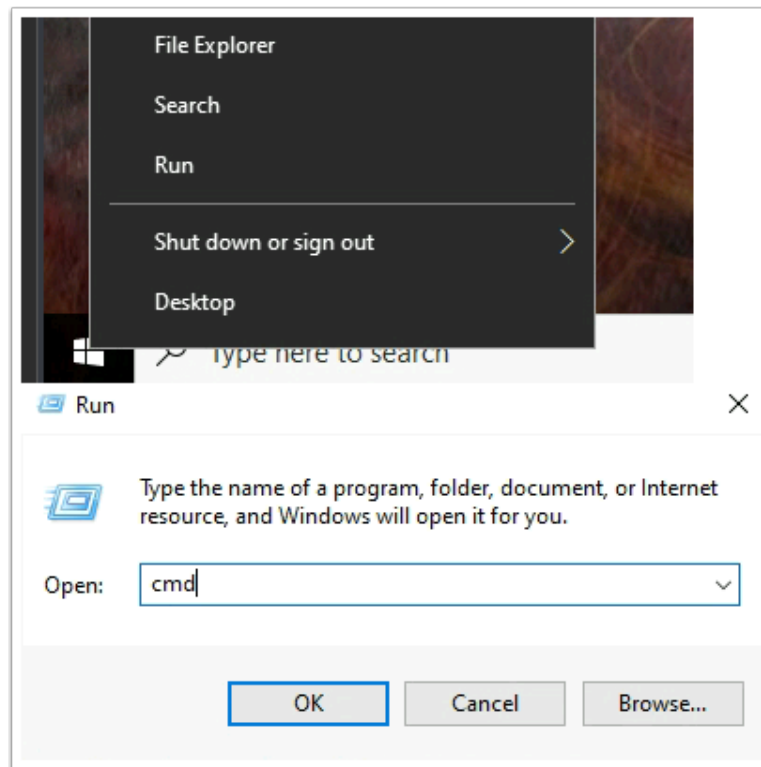
- Select **SAVE**

Part 1

Pre-deployment check



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



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

```
C:\Windows\system32\cmd.exe

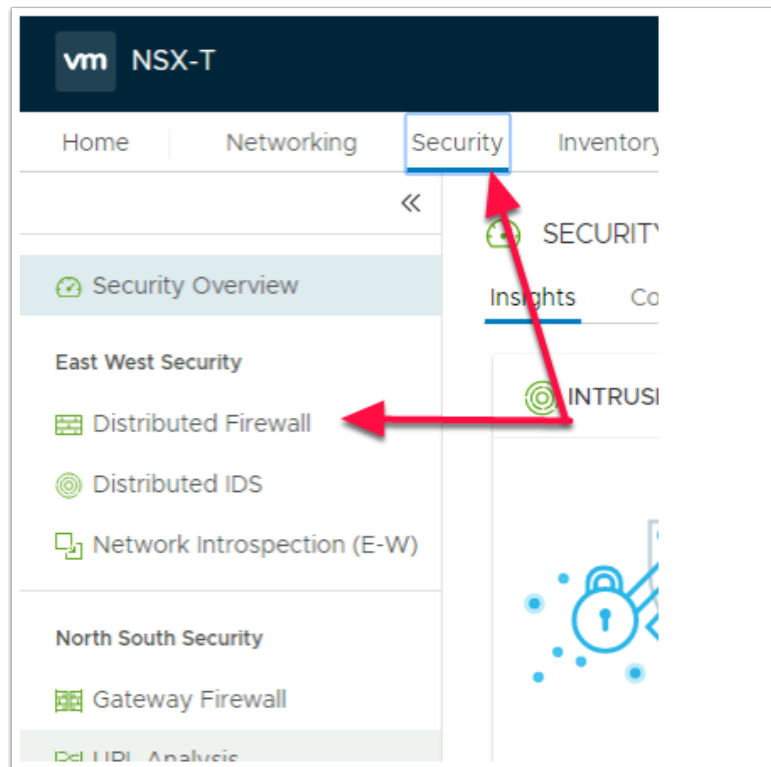
C:\Users\mark>ping sql.euc-livfire.com

Pinging sql.euc-livfire.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

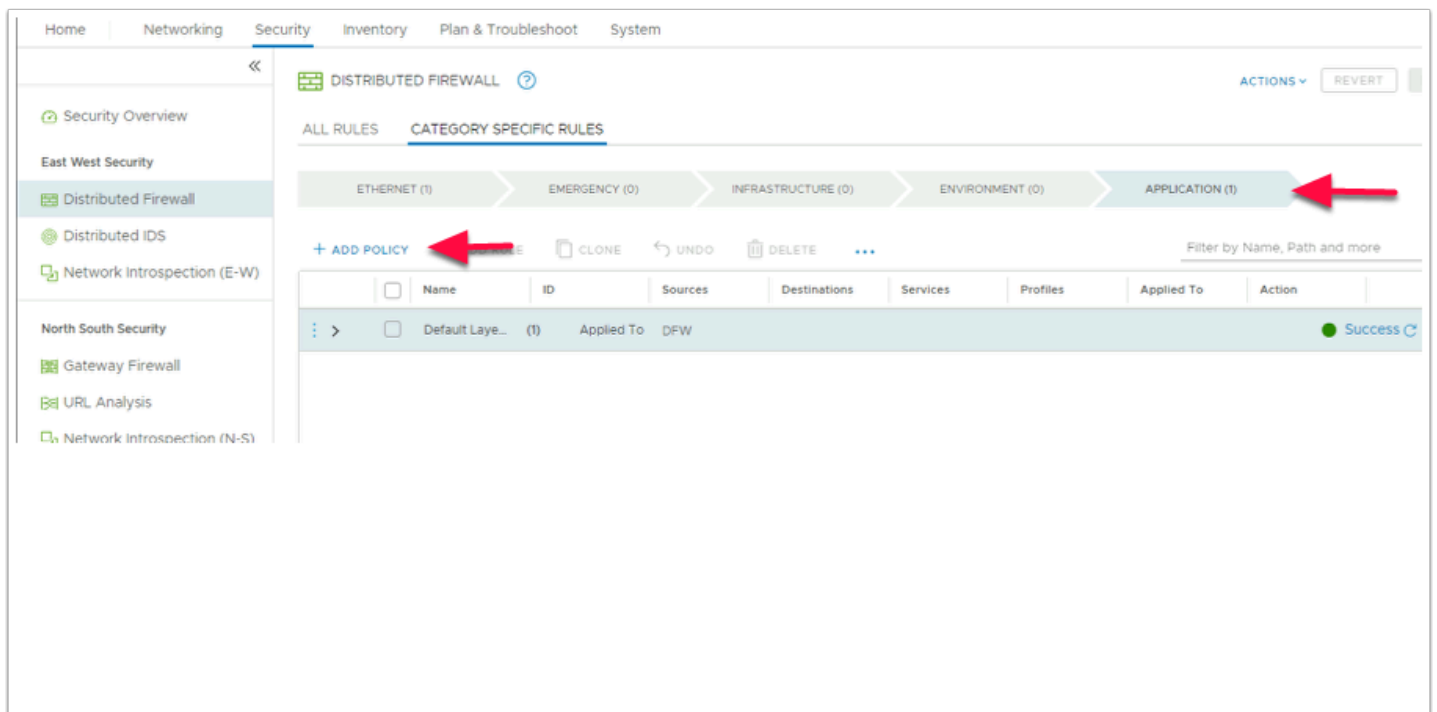
C:\Users\mark>
```

3. In the **CMD** interface type **ping sql.euc-livfire.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

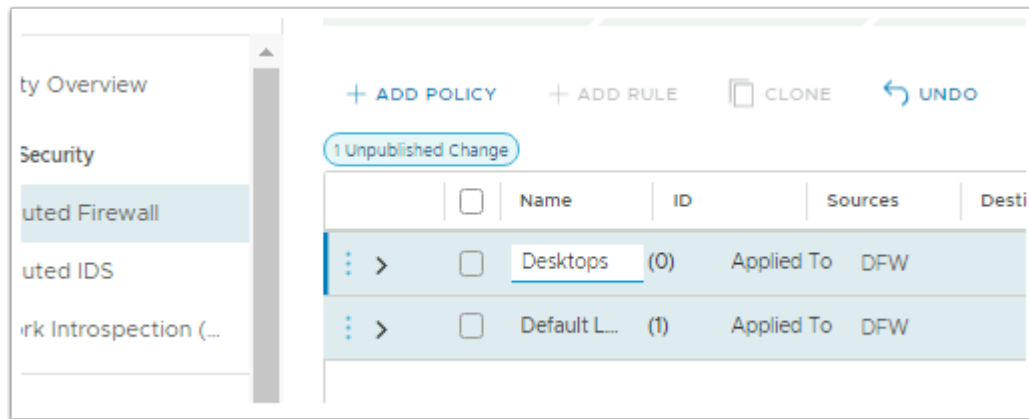
- Select the **Security** Tab under **East West Security**
- Select **Distributed Firewall**



5. In the **Distributed Firewall** section

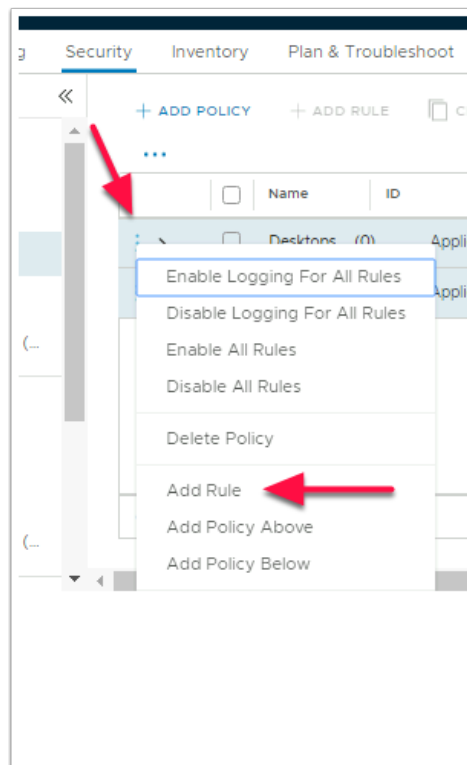
- Ensure that **Application** is selected
- Select **ADD POLICY**

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



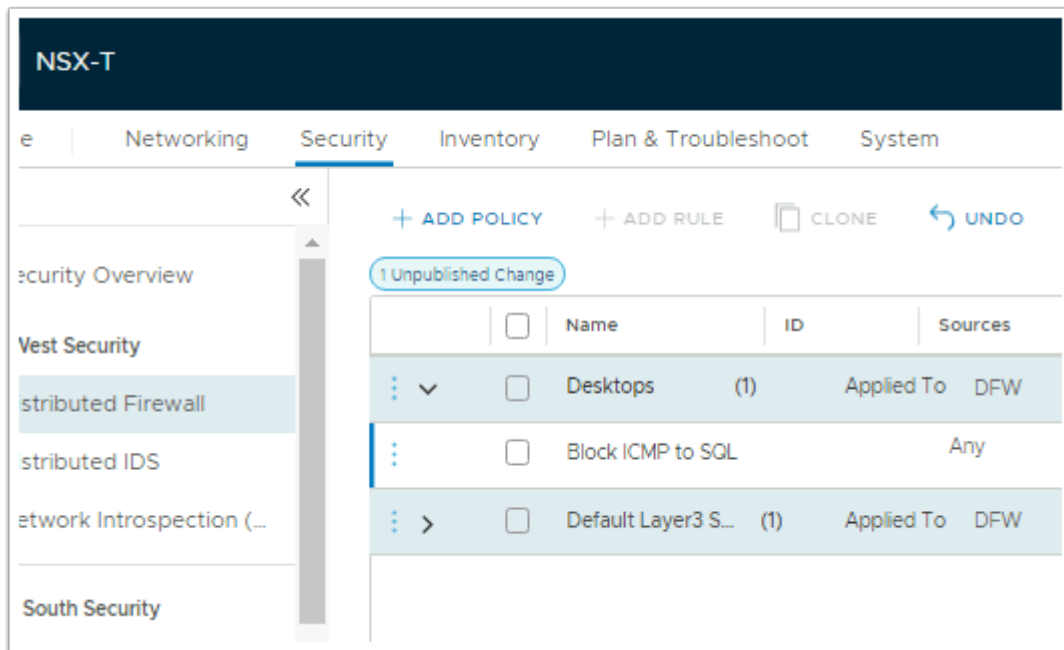
6. In the **Policy** area you have just created

- Under **Name** select **New Policy** under **Name** and replace with **Desktops**



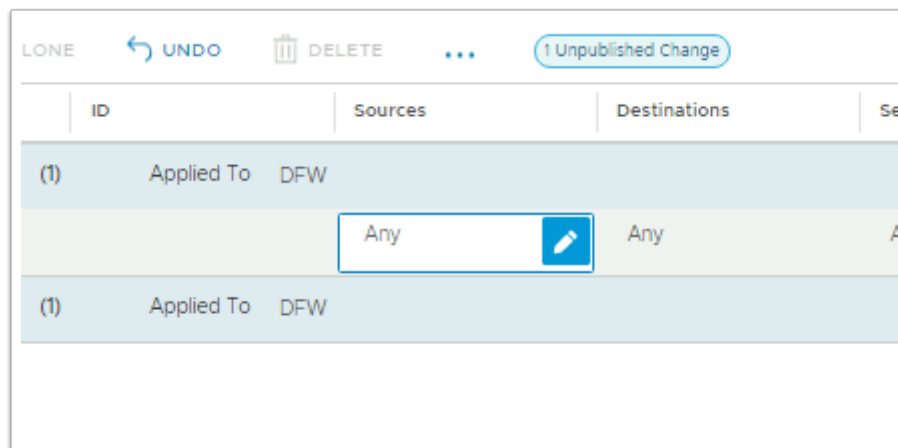
7. To left of your **Desktops Policy**, notice you have **3 vertical dots**.

- Select the **3 vertical dots**
- Select **Add Rule**



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

- Select **New Rule** and change to **Block ICMP to SQL**



9. Under **Sources**

- Select the **pencil** icon next to **Any**

Set Source

Rule > Block ICMP to SQL

Negate Selections ☐ No Negated selections

Groups (0) IP Addresses (0)

ADD GROUP

	Name
<input type="checkbox"/>	External
<input type="checkbox"/>	External net

10. In the **Set Source** Window

- Select **ADD GROUP**

Set Source

Rule > Block ICMP to SQL

Negate Selections ☐ No | Negated selections will be shown as ~~Example Group~~

ADD GROUP

	Name	Compute Members
⋮	Subnet 10	* Set Members
Description		Tags

SAVE

CANCEL

11. In the **ADD GROUP** interface

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

Select Members | Subnet 10

Add Compute Members either by creating or by directly adding them. You can also add Id Compute members to define effective membership of the group.

Membership Criteria (0) Members (0) **IP Addresses (0)** MAC Addresses (0)

ACTIONS ▾

Enter IP Address

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 Id Compute members to define effective membership of the group.

Membership Criteria (0) Members (0) **IP Addresses (0)** MAC Addresses (0) AD Gr

ACTIONS ▾

172.16.10.0/24

Other MAC Address or ID group can be part of a Group

1

ADD GROUP

2

Name: Subnet 10 Compute Members: 1 IPs

Description: Description

SAVE **CANCEL**

ADD GROUP

Name: Subnet 10

3

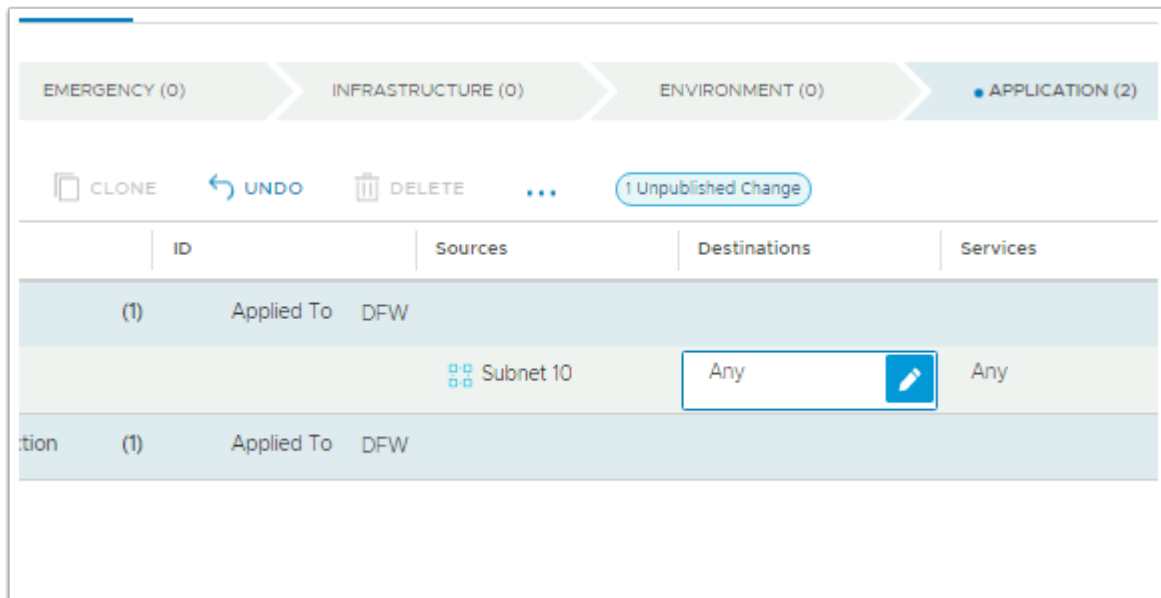
1 - 1 of 1 Groups

Show Only Selected: ☐

CANCEL **APPLY**

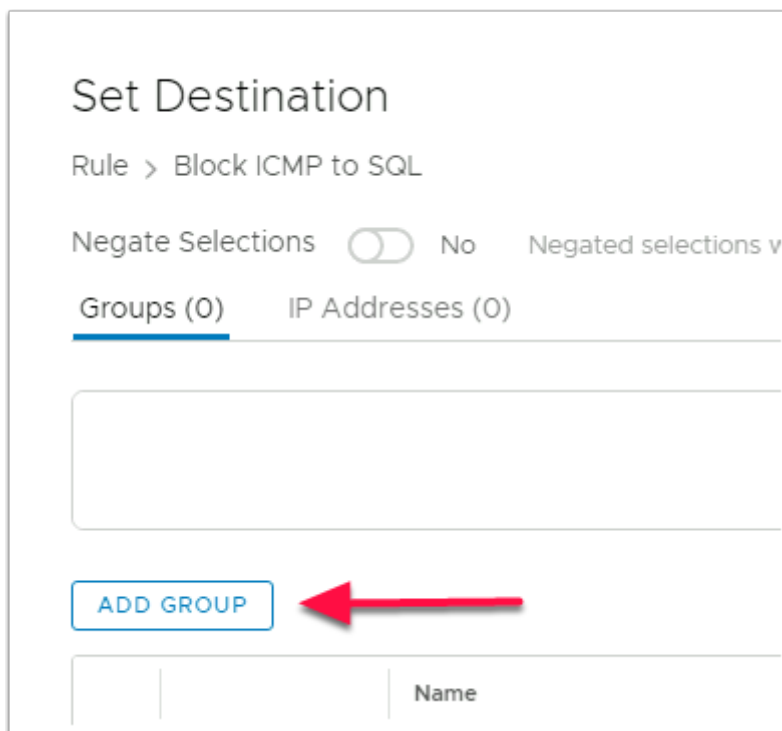
13. Under **ACTIONS**

1. 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**



14. Under **Destinations**

- Next to **Any** select the **Pencil**



15. In the **Set Destination** window

- Select **ADD GROUP**

ADD GROUP

Name	Description
SQL *	

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 either by creating or by directly adding them. You can also add Identity n Compute members to define effective membership of the group.

Membership Criteria (0) Members (0) IP Addresses (0) MAC Addresses (0) AD G

ACTIONS ▾

192.168.110.45

Either MAC Address or AD groups can be part of a Group

CANCEL **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 GROUP

Name	Compute Members
SQL	1 IPs

Description

Tags

SAVE **CANCEL**

☐ **Subnet 10** [View Members](#)

19. In the **ADD GROUP** area
 - Select **SAVE**

SQL X

ADD GROUP

	Name
<input checked="" type="checkbox"/>	SQL
<input type="checkbox"/>	Subnet 10

1 - 2 of 2 Groups

CANCEL APPLY

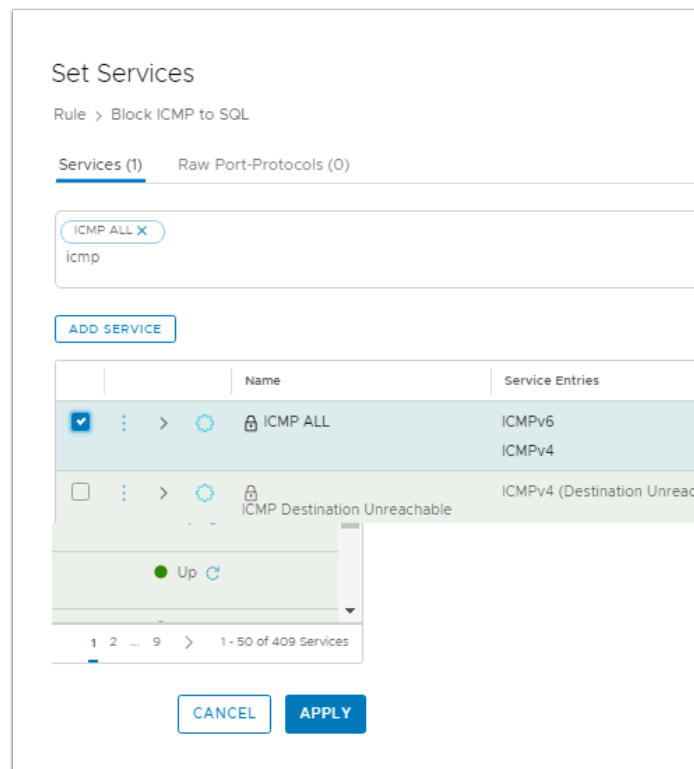
20. Ensure the **checkbox** next to **SQL** is selected
- In the bottom right-hand corner select **APPLY**

STRUCTURE (0) ENVIRONMENT (0) APPLICATION (2)

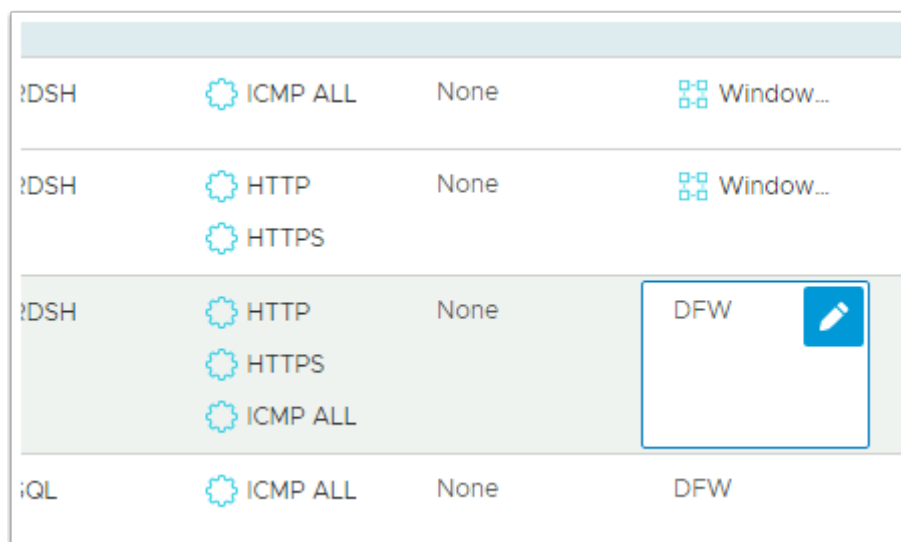
DELETE ... 1 Unpublished Change

Sources	Destinations	Services	Profiles
Subnet 10	SQL	Any	None

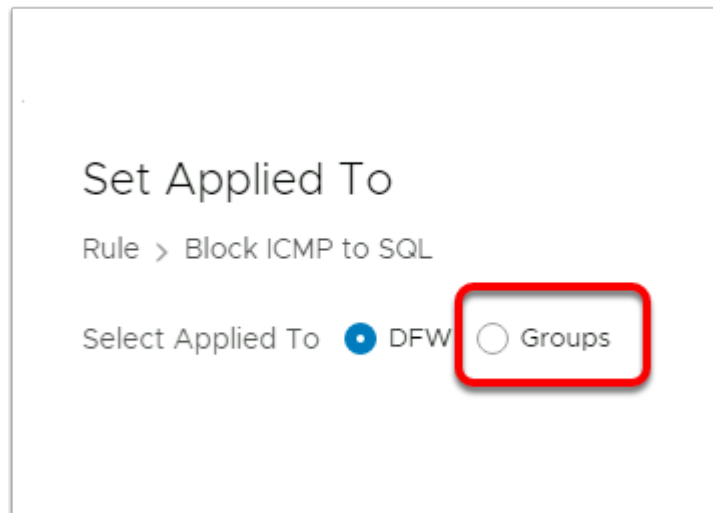
21. Under **Services**
- Select the **Pencil** next to **Any**



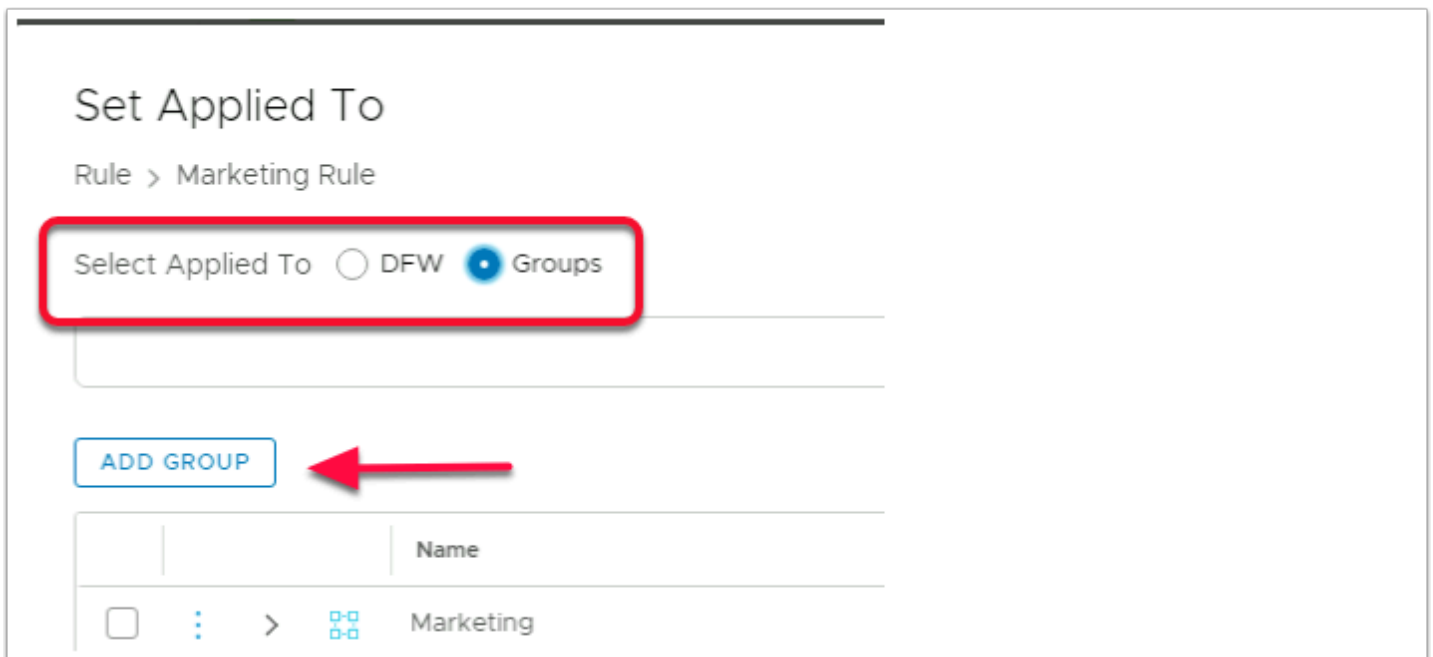
22. In the **Set Services** window
- Scroll down and select the **checkbox** next to **ICMP ALL**
 - HINT, by typing ICMP in the box under services, it helps to find ICMP ALL
 - Select **APPLY**



23. In the **Block ICMP to 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



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
<input type="text" value="Windows 10"/> <div>1</div> Description <input type="text"/>	Set Members <div>2</div> 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 either by creating or by directly Compute members to define effective membership of th

Membership Criteria (0) Members (0) IP Address

+ 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 separately to define effective membership of the group.

Membership Criteria (1) Members (0) IP Addresses (0) MAC Addresses (0) AD Groups (0)

[+ ADD CRITERIA](#)

▼ Criteria 1

Virtual Machine ▼ Computer Name ▼ Starts With ▼ W10INST

1 - 3 of 3 Groups

[CANCEL](#) [APPLY](#)

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 ☐ DFW ☒ Groups

[ADD GROUP](#)

Name	Compute Members
Windows 10	1 Criteria
Description	Description

[SAVE](#) [CANCEL](#)

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

Set Applied To

Rule > Block ICMP to SQL

Select Applied To ☐ DFW ☒ Groups

Windows 10 X

ADD GROUP

	Name
<input type="checkbox"/>	External
<input type="checkbox"/>	External_net
<input type="checkbox"/>	RDSH
<input type="checkbox"/>	SQL
<input type="checkbox"/>	Subnet 10
<input checked="" type="checkbox"/>	Windows 10

1 - 6 of 6 Groups

Show Only Selected ☐

CANCEL APPLY

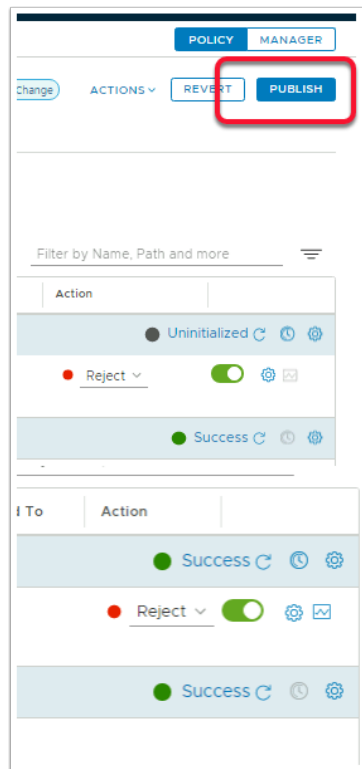
30. In the **Set Applied To** window

- Ensure the **checkbox** is selected next to **Windows 10**
- In the bottom right corner select **APPLY**

To	Action
	<div> <div>●</div> <div>Allow</div> <div>▼</div> </div> <div> <div>Allow</div> <div>Drop</div> <div>Reject</div> </div>

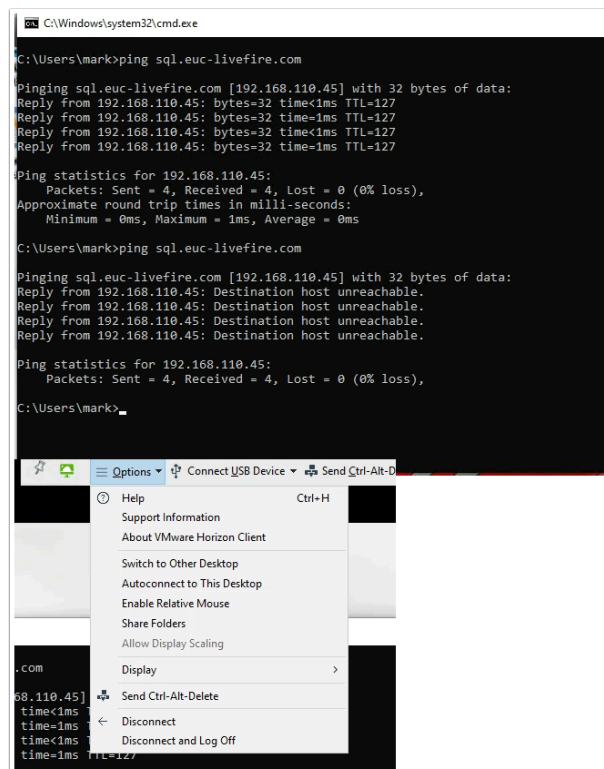
31. Under **Action**

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



32. In the top right hand corner of the NSX-T Admin Console

- Select **PUBLISH**
- Notice that the status **Uninitialized** now changes to **Success**



33. On your **ControlCenter** server

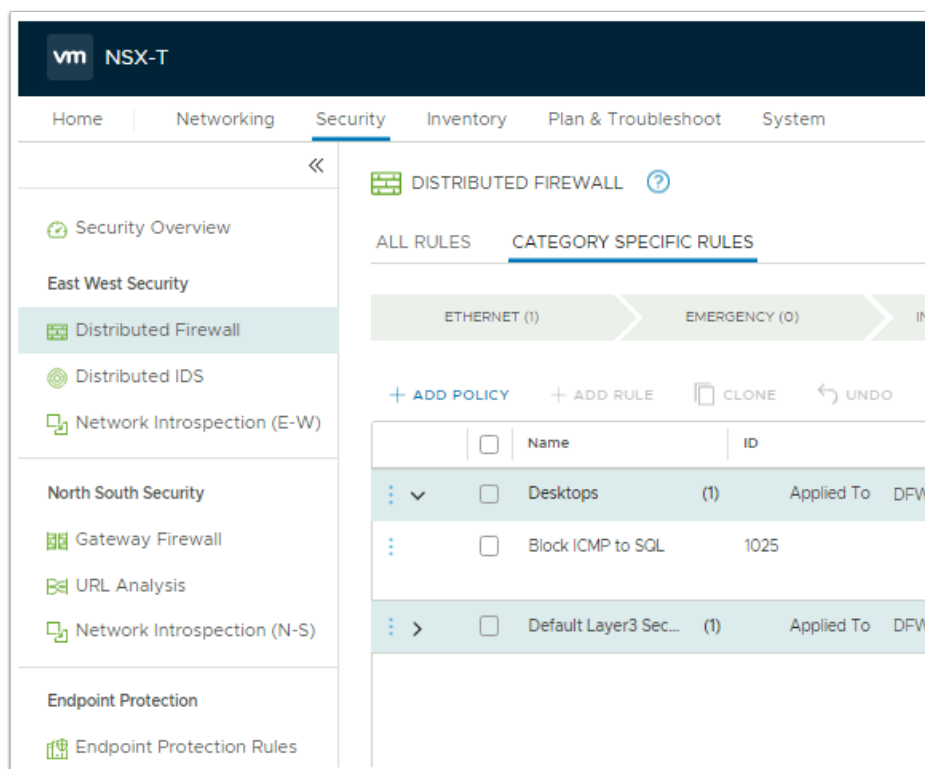
- Revert back to your **Horizon Client** session

- From the **CMD Prompt** [ping sql.euc-livewire.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

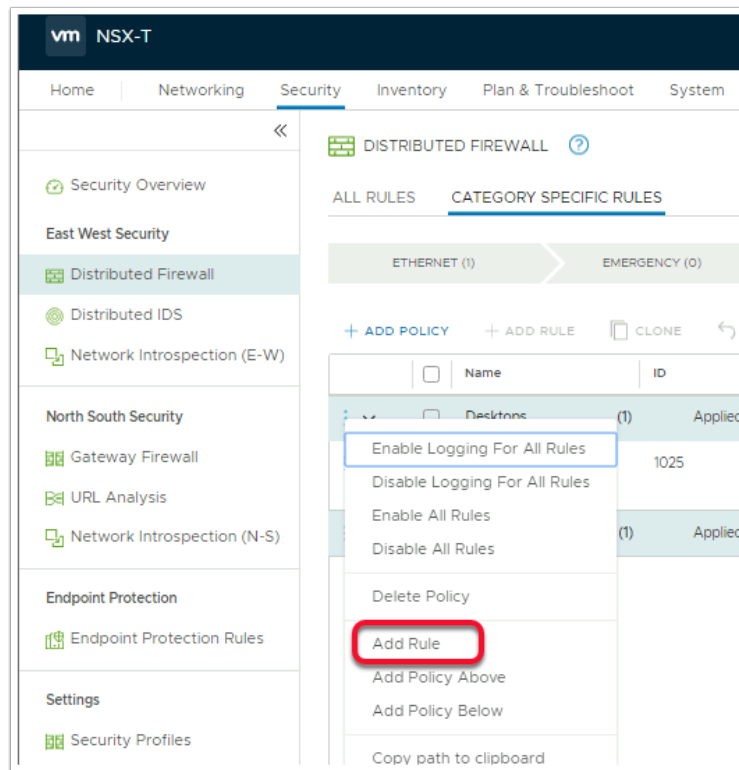
Introduction:

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.



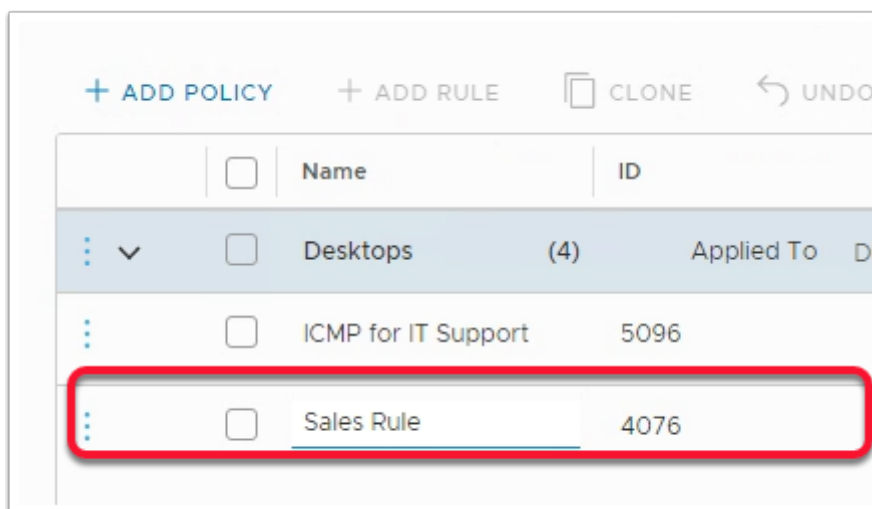
1. On your **ControlCenter** server,
 - Switch back to your browser with your **NSX-T** session.
 - If necessary login with the username **Admin** and the password **VMware1!VMware1!**
 - Ensure you have the **Security** tab selected and under **EAST WEST Security**

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



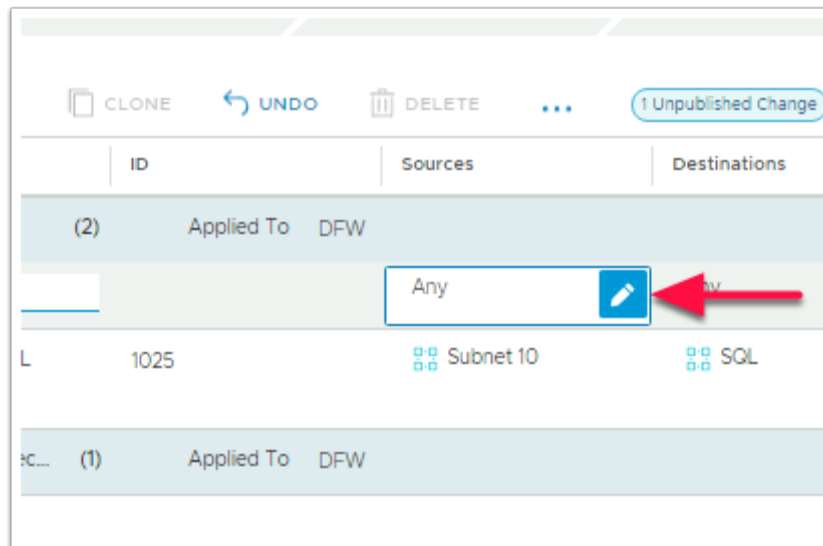
2. On the NSX-T Admin Console

- Select the **3 dots** next to **Desktops**
- Select **Add Rule**

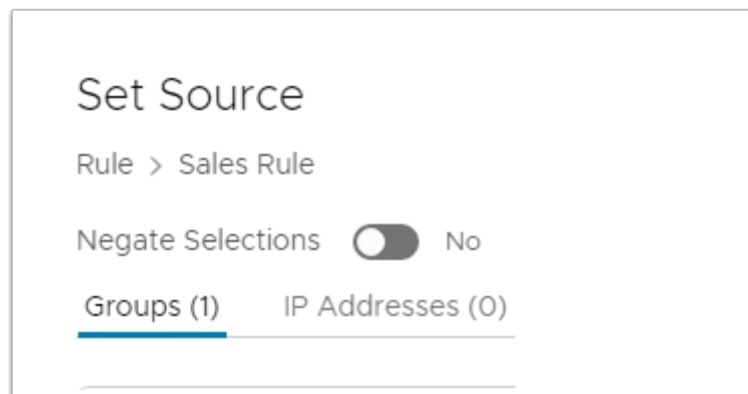


3. In the **New Rule** interface,

- Replace the name **New Rule** by selecting and typing **Sales Rule**



4. Under **Sources**,
 - Select the **pencil** icon, next to **Any**



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**

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

- Select the **AD Groups** tab

Select Members | Sales

Add Compute Members either by creating or by directly adding the Compute members to define effective membership of the group.

Membership Criteria (0) Members (0) IP Addresses (0)

Sales X

Name
<input checked="" type="checkbox"/> Sales

1 - 1 of 1 AD Groups

Either MAC Address or AD groups can be part of a Group

CANCEL APPLY

9. In the **search** area

- Type **Sales**,
- Select the **checkbox** next to **Sales**
- Select **APPLY**

Name

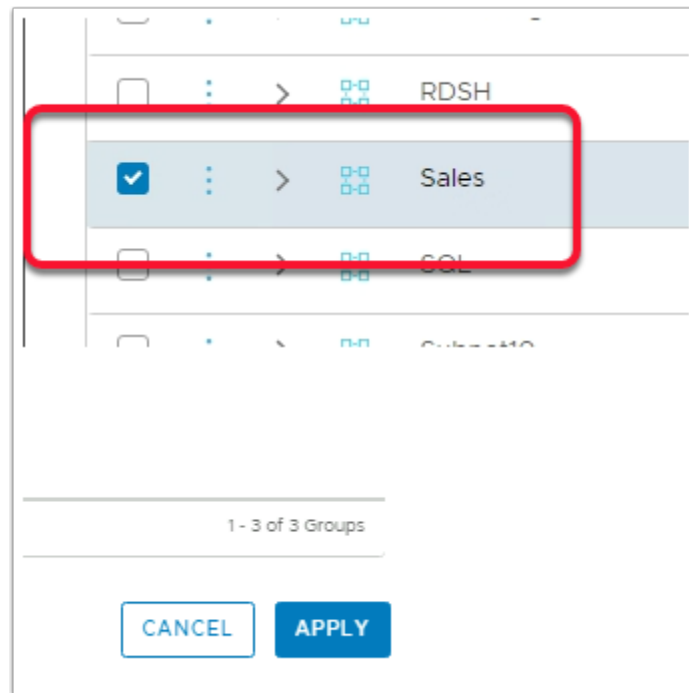
Sales

Description

SAVE CANCEL

10. Back to the **Set Source** window

- Select **SAVE**



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**



12. Under **Destinations** next to **Any**

- Select the **Pencil**

RDSH X

ADD GROUP

	Name
<input type="checkbox"/>	Marketing
<input checked="" type="checkbox"/>	RDSH
<input type="checkbox"/>	SQL
<input type="checkbox"/>	Subnet 10

1 - 4 of 4 Groups

Show Only Selected ☐

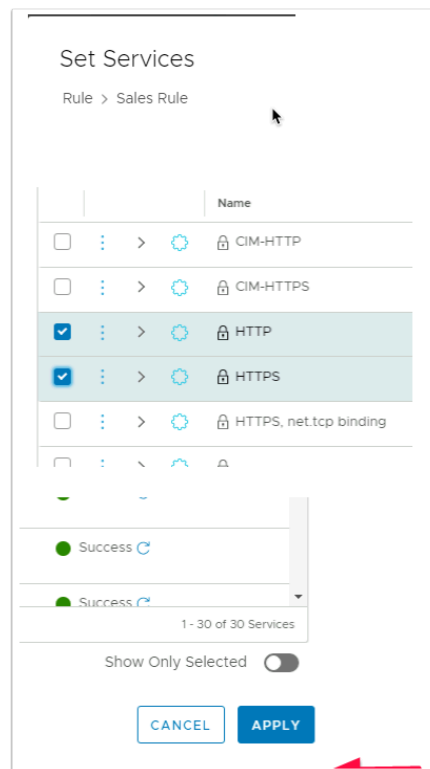
CANCEL APPLY

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

DELETE ... 1 Unpublished Change

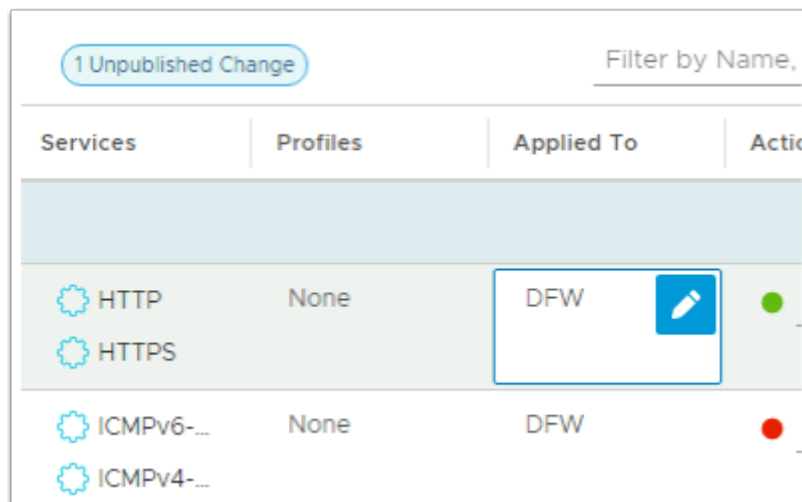
Destinations	Services	Profile:
RDSH	Any	None
SQL	ICMPv6-...	None
	ICMPv4-	

14. In the **Sales Rule** row
- Under **Services** select the **Pencil** next to **Any**



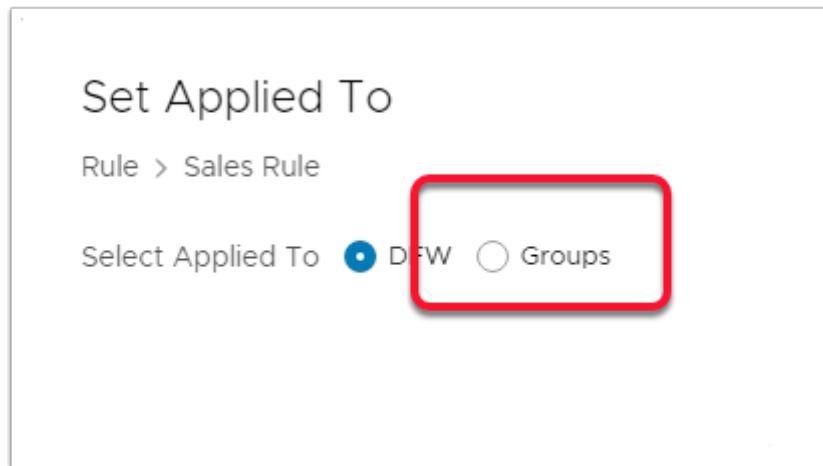
15. In the **Set Services** window

- 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**

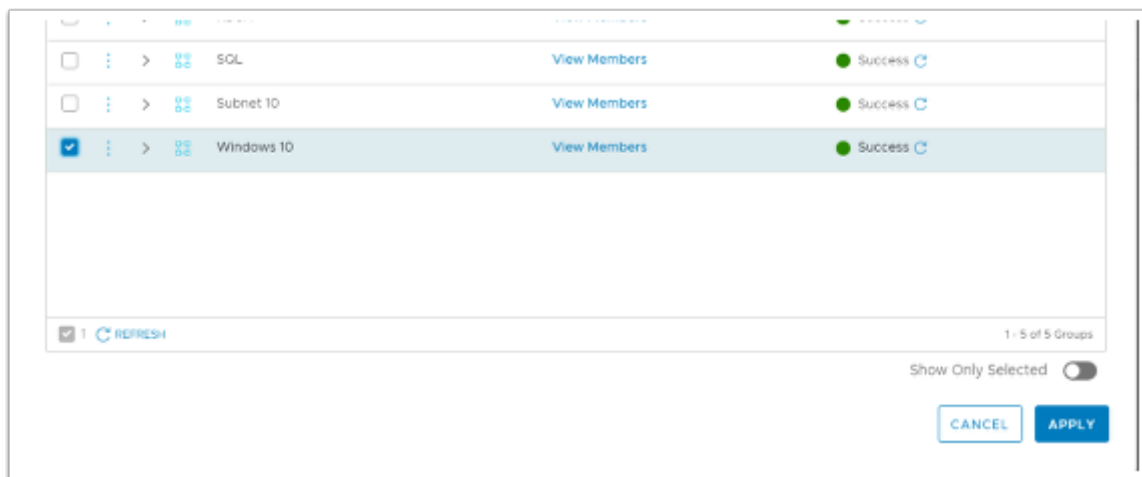


16. In the **Sales Rule** row

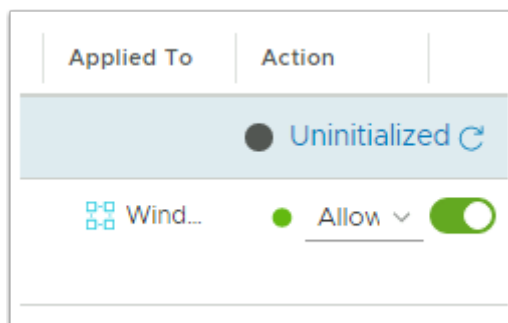
- Under **Applied To** select the **Pencil** next to **DFW**



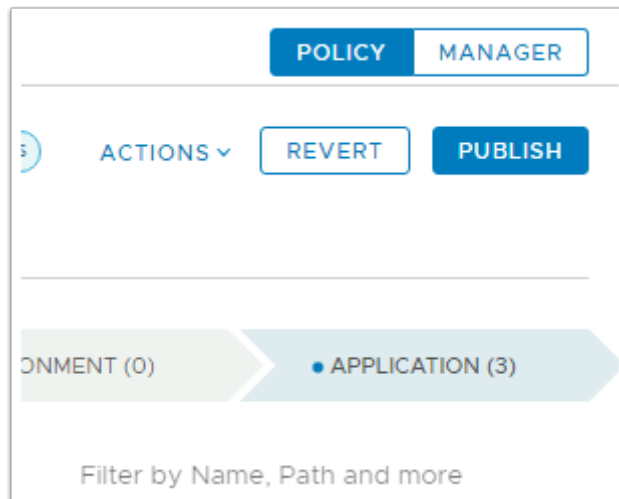
17. In the **Set Applied To** window
- Select the **radio button** next to **Groups**



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

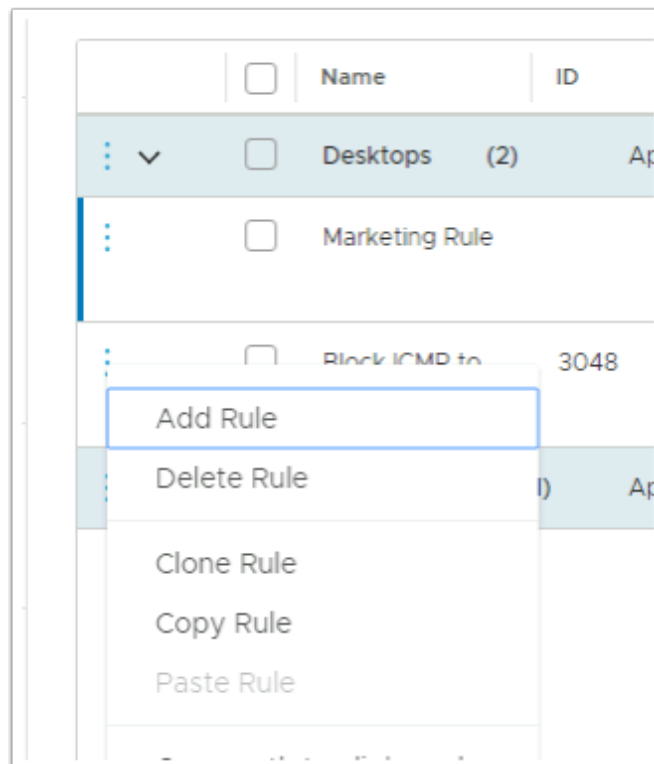


19. Under **Action**. We will leave the default Action that being **Allow**



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



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**

<input type="checkbox"/>	Name	ID
<input type="checkbox"/>	Desktops (4)	App
<input type="checkbox"/>	ICMP for IT Support	5096
<input type="checkbox"/>	Sales Rule	4076
<input type="checkbox"/>	Deny All Groups	4074

22. Under your **Sales Rule**

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

<input type="checkbox"/>	Deny All Groups	Any	Any	<input type="checkbox"/>	Any
<input type="checkbox"/>	Block ICMP to SQL	3048	Subne...	SQL	IK

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)

RDSH X

ADD GROUP

	Name
<input type="checkbox"/>	Marketing
<input checked="" type="checkbox"/>	RDSH
<input type="checkbox"/>	SQL
<input type="checkbox"/>	Subnet 10
<input type="checkbox"/>	Windows 10

1 - 5 of 5 Groups

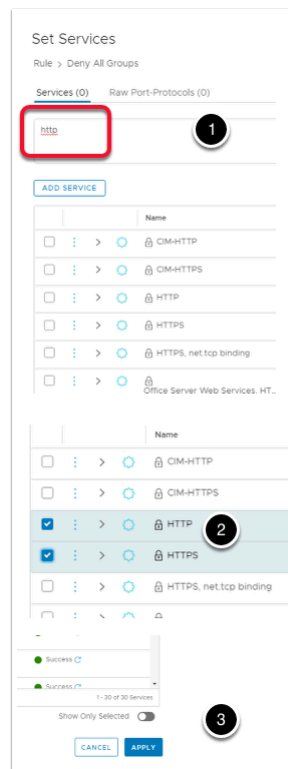
Show Only Selected ☐

CANCEL APPLY

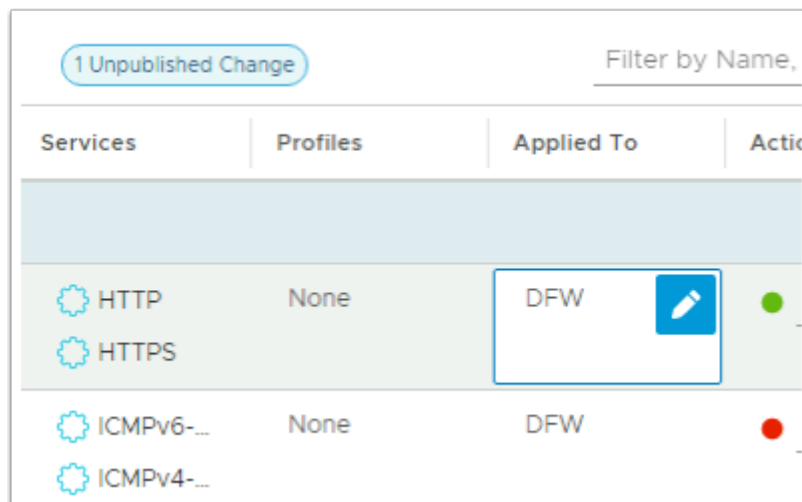
24. In the **Set Destination** window,
- Select the **checkbox** next to **RDSH**
 - Select **APPLY**

	<input type="checkbox"/>	Name	ID	Sources	Destinations	Services	Profiles	Appl...
	<input type="checkbox"/>	Desktops	(3)	Applied To	DFW			
	<input type="checkbox"/>	Marketing Rule		Marke...	RDSH	HTTP HTTPS	None	
	<input type="checkbox"/>	Deny All Groups		Any	RDSH	Any	None	
	<input type="checkbox"/>	Block ICMP to SQL	3048	Subne...	SQL	ICMPv... ICMPv...	None	
	<input type="checkbox"/>	Default Layer3 Section	(1)	Applied To	DFW			

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



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**




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

Set Applied To

Rule > Marketing Rule

☐ DFW ☒ Groups

ADD GROUP

	Name
<input type="checkbox"/> ... > 	Marketing

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

Set Applied To

Rule > Deny All Groups

Select Applied To

☐ DFW
 ☒ Groups

Windows 10 X

ADD GROUP

EXPAND ALL

	Name	Compute Members	Status
<input type="checkbox"/>	> Marketing	View Members	Success
<input type="checkbox"/>	> RDSH	View Members	Success
<input type="checkbox"/>	> SQL	View Members	Success
<input type="checkbox"/>	> Subnet 10	View Members	Success
<input checked="" type="checkbox"/>	> Windows 10	View Members	Success

☒ 1
 [REFRESH](#)

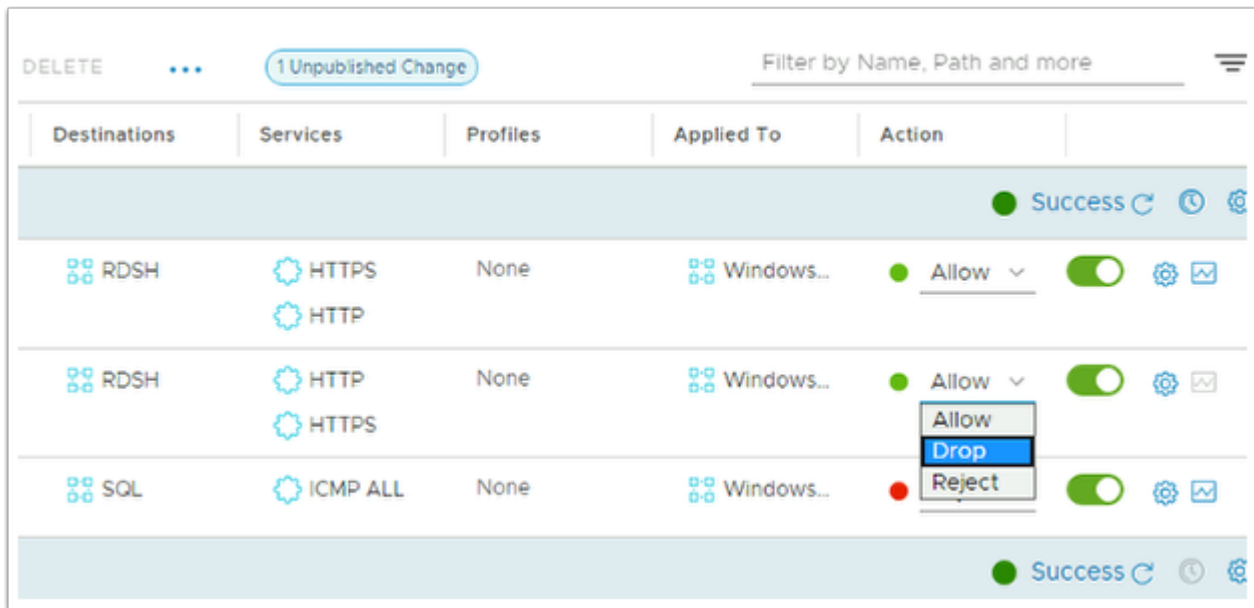
1 - 5 of 5 Groups

Show Only Selected

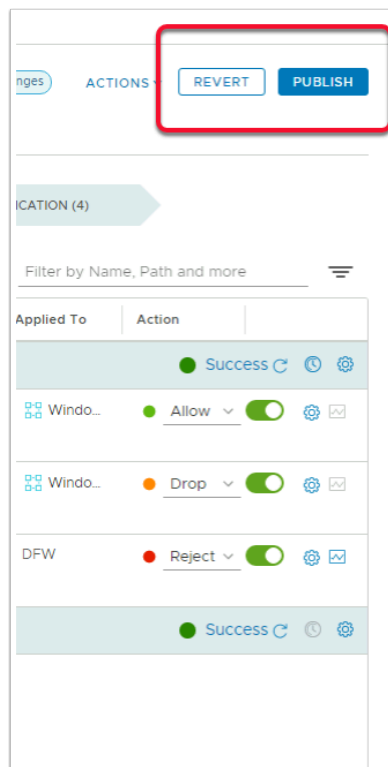
CANCEL

APPLY

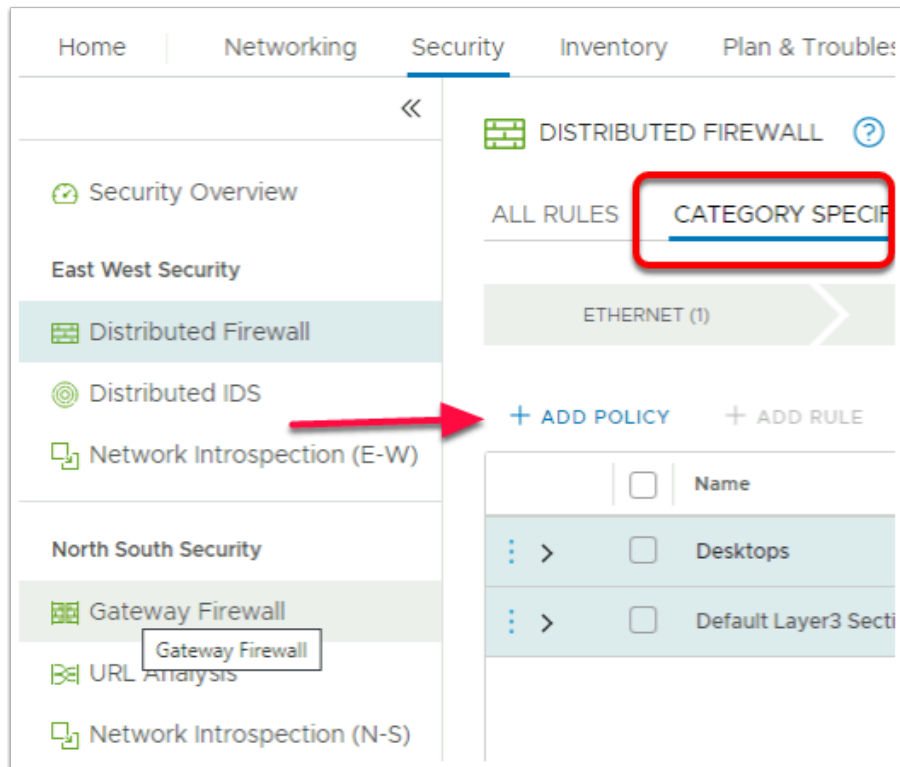
29. In the **Set Applied To** window



30. In the **Deny All Groups** row
- Under **Action** select the **Dropdown**
 - **Select Drop**

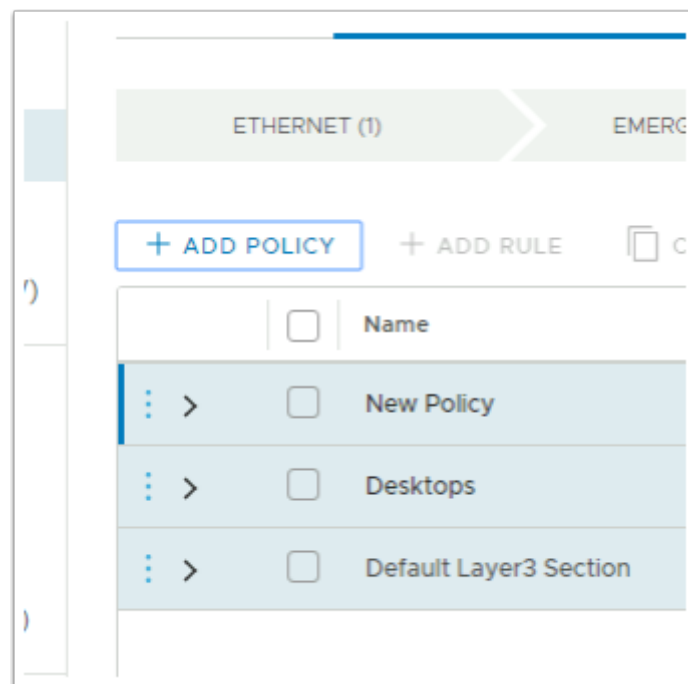


31. In the top right corner, of the NSX-T Admin Console
- Select **PUBLISH**
 - We have now completed two rules both based on the Source .
 - Our last set of Rules will Aimed at the Destination Server services

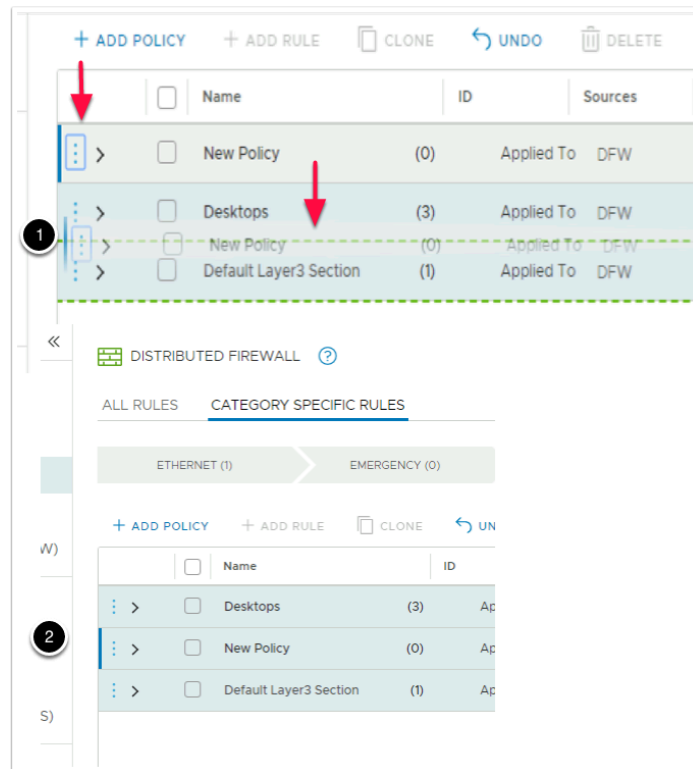


32. NSX-T Admin Console > Security > Distributed Firewall

- Under **CATEGORY SPECIFIC RULES** in the **APPLICATION** section select **+ADD POLICY**

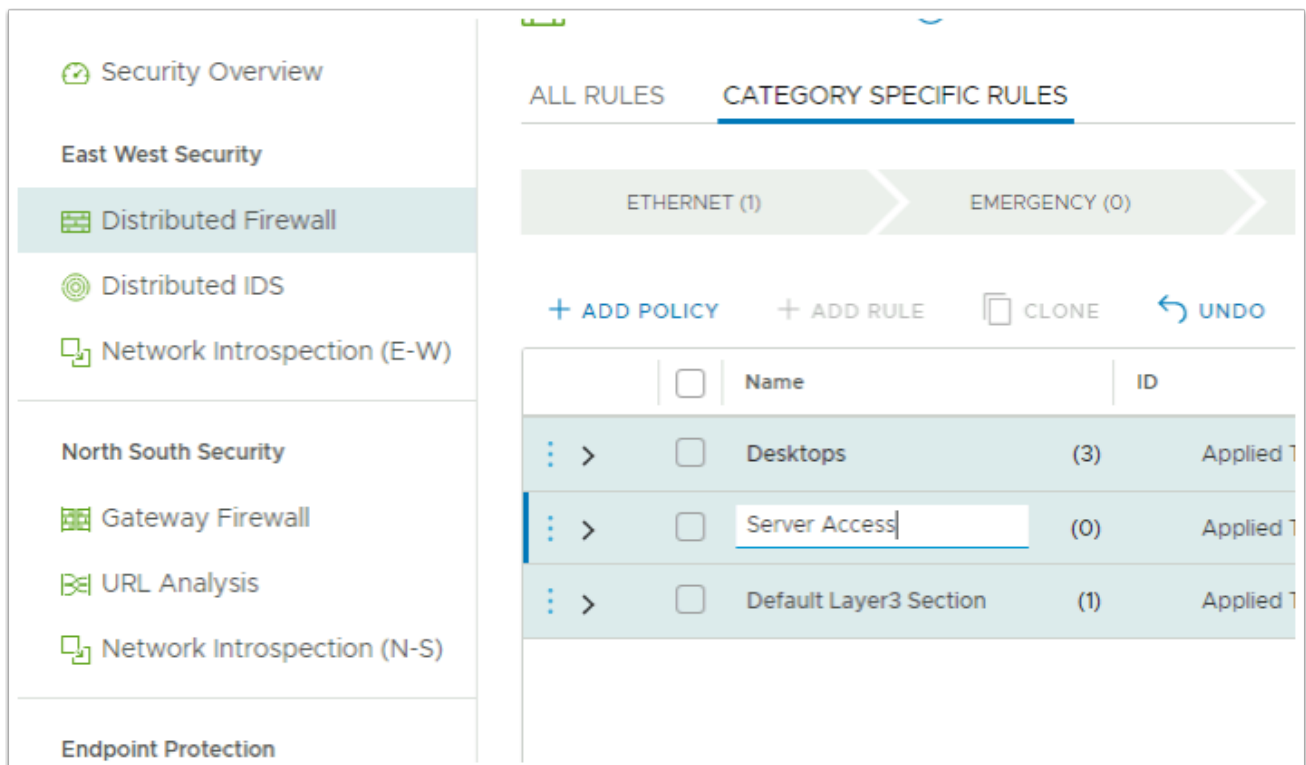


33. You will notice you have a **New Policy** .1st in the policy order. We will now re-order this policy

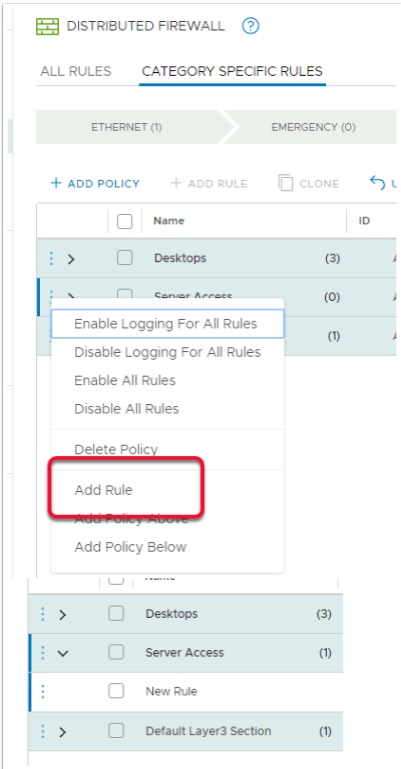


34. In the NSX-T Admin Console > Security > Distributed Firewall

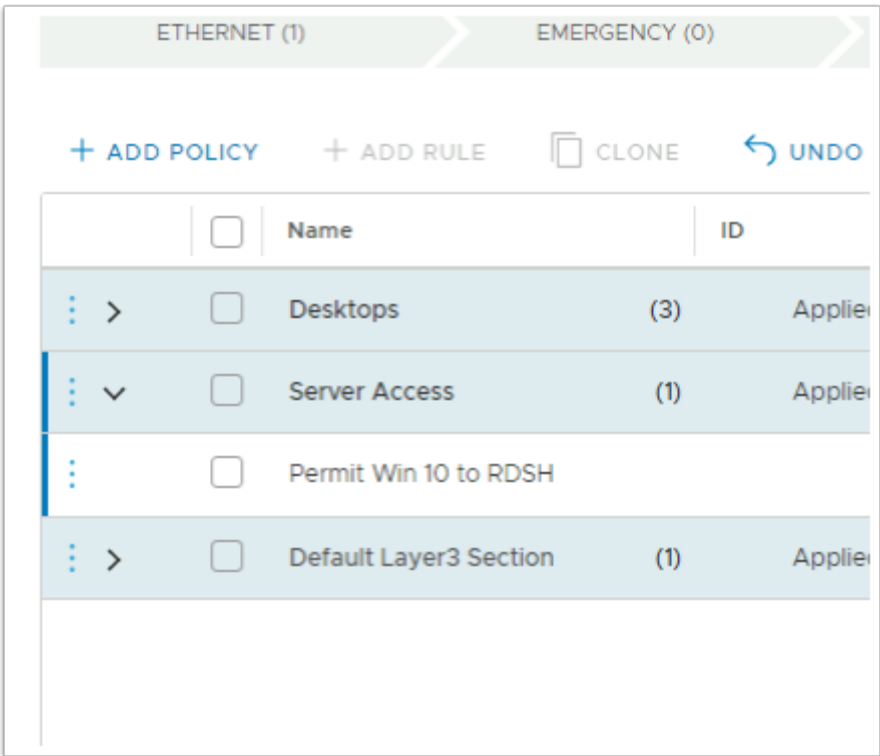
- Select with a **left click and hold your mouse** on the **3 DOTS** at the beginning of the **New Policy** Line
- **Drag** the **New Policy** down till just after **Desktop Policy** and **release your mouse**
- Your **New Policy** should appear in the order in the second screenshot of this image



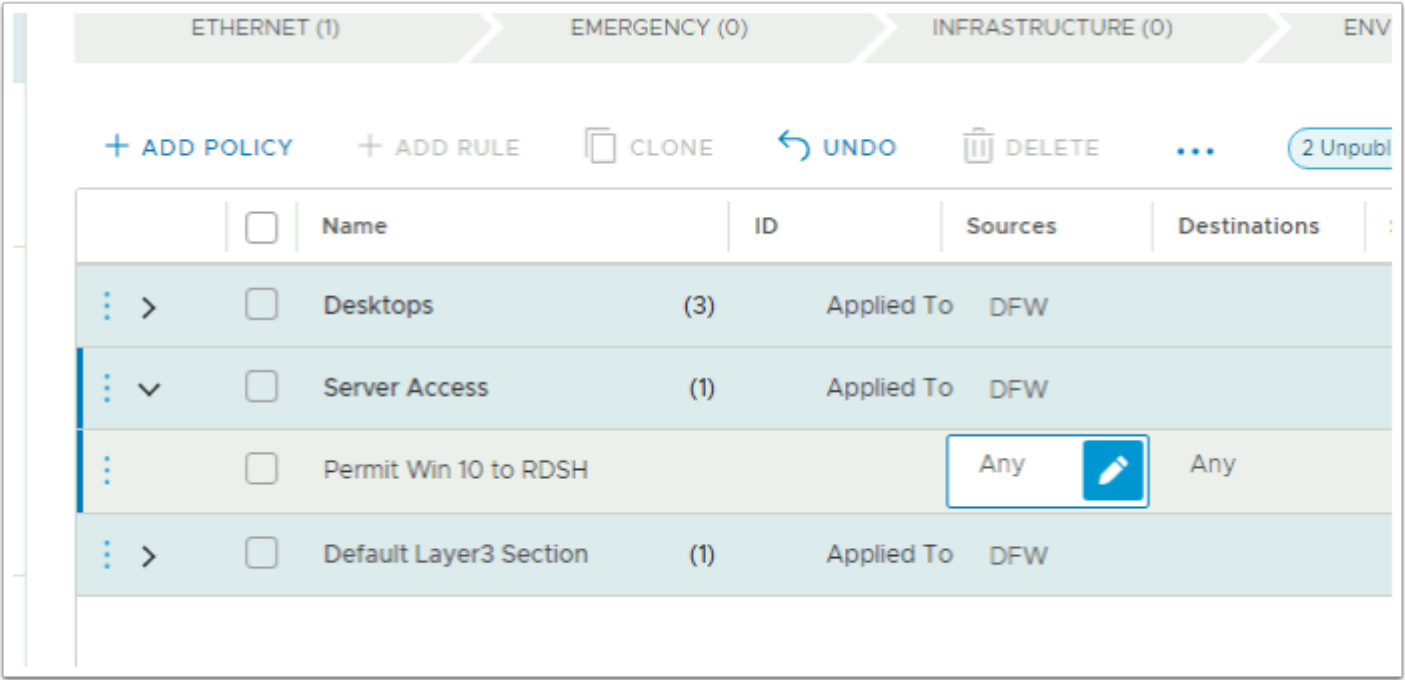
35. In the **NSX-T Admin Console > Security > Distributed Firewall**
- In the **New Policy** interface, rename **New Policy** to **Server Access**



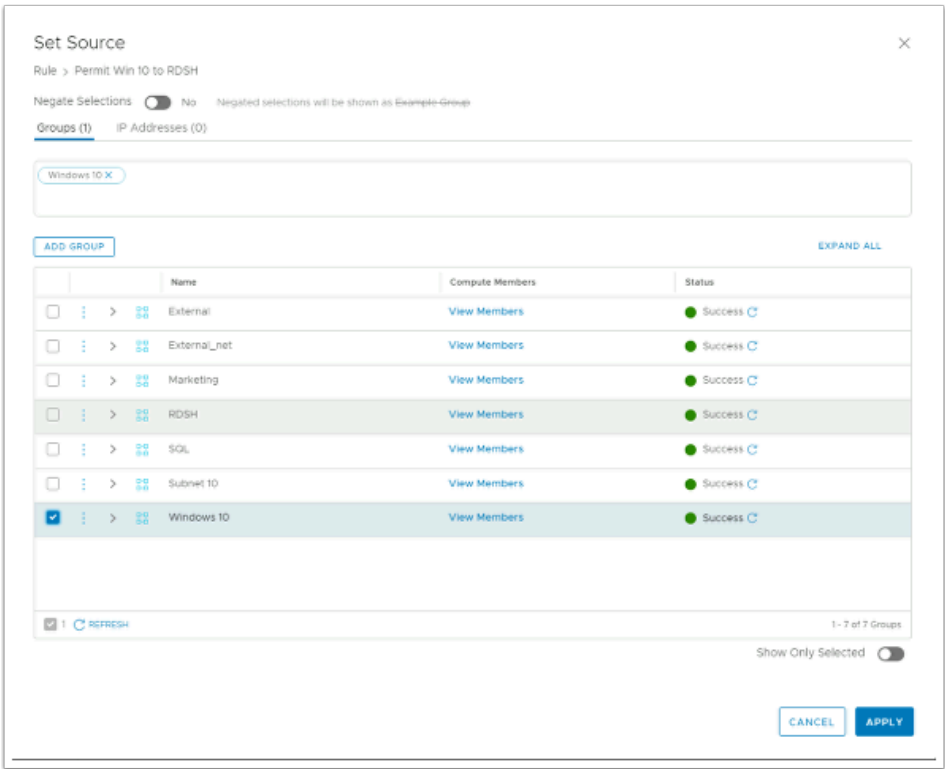
36. In the **NSX-T Admin Console > Security > Distributed Firewall**
- Select the **3 DOTS** in front of your Server Access Policy and select **Add rule**
 - Notice you now have a new rule called **New Rule** that is part of the **Server Access** Policy



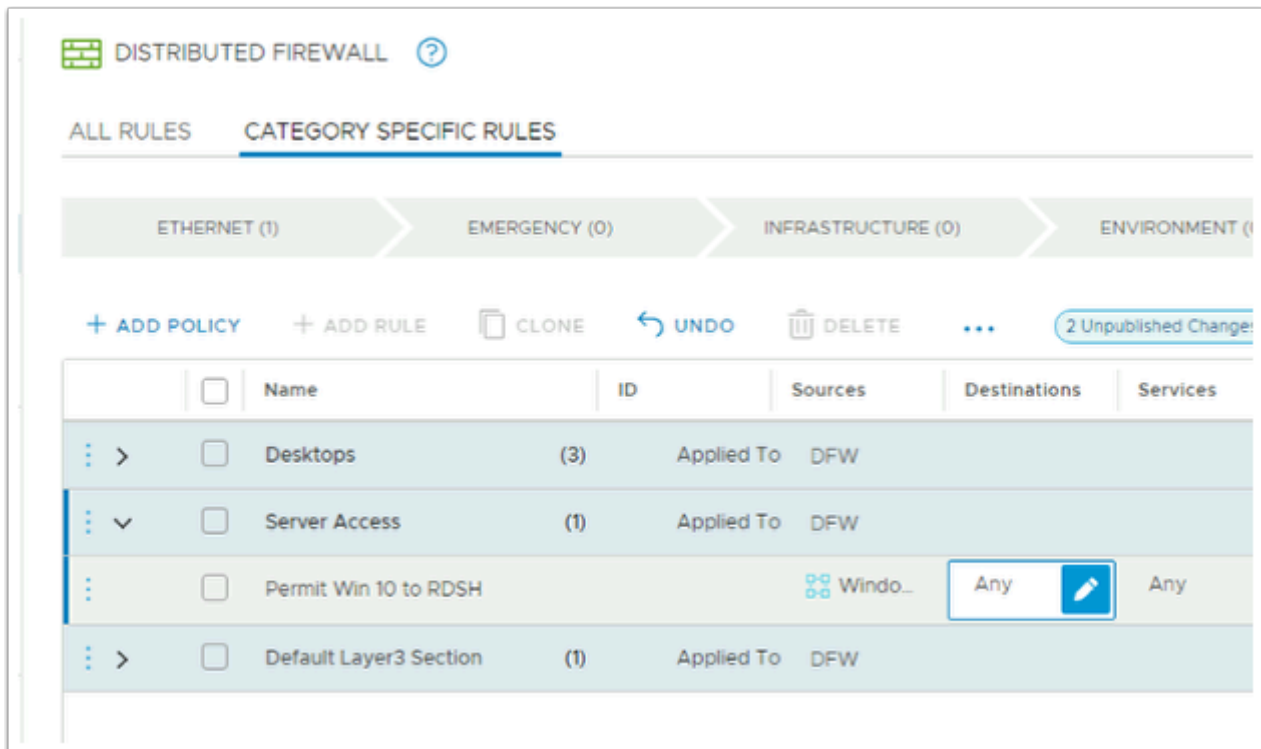
37. In the **New Rule** section,
- Rename **New Rule** to **Permit Win 10 to RDSH**



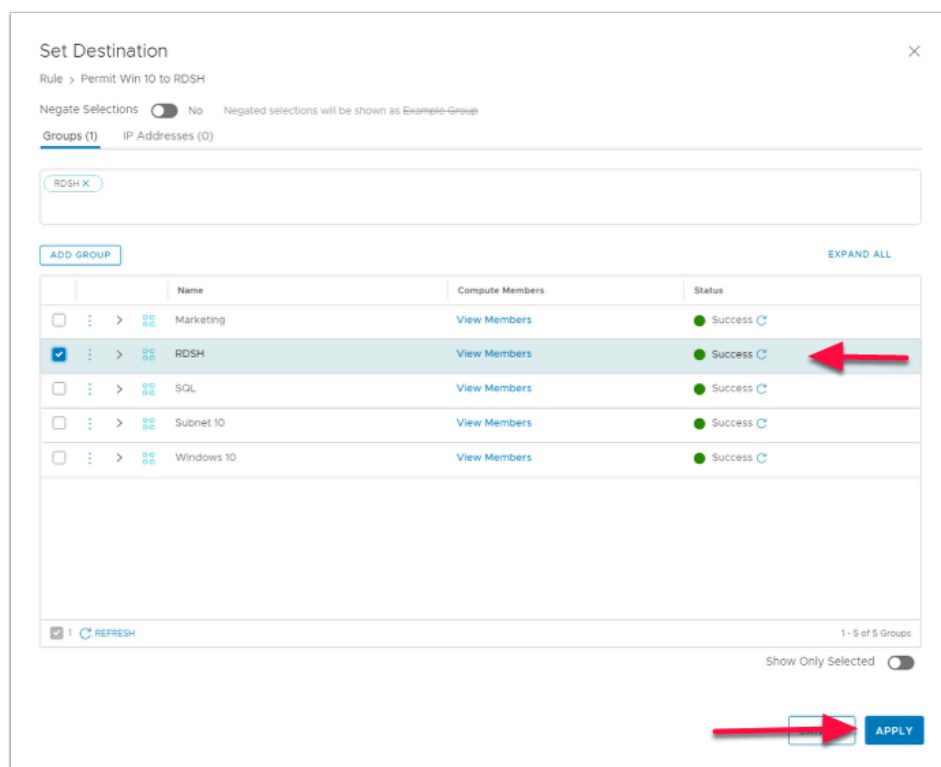
38. In the **Permit Win10 to RDSH** section
- Under **Sources**, select the **Pencil** next to **Any**



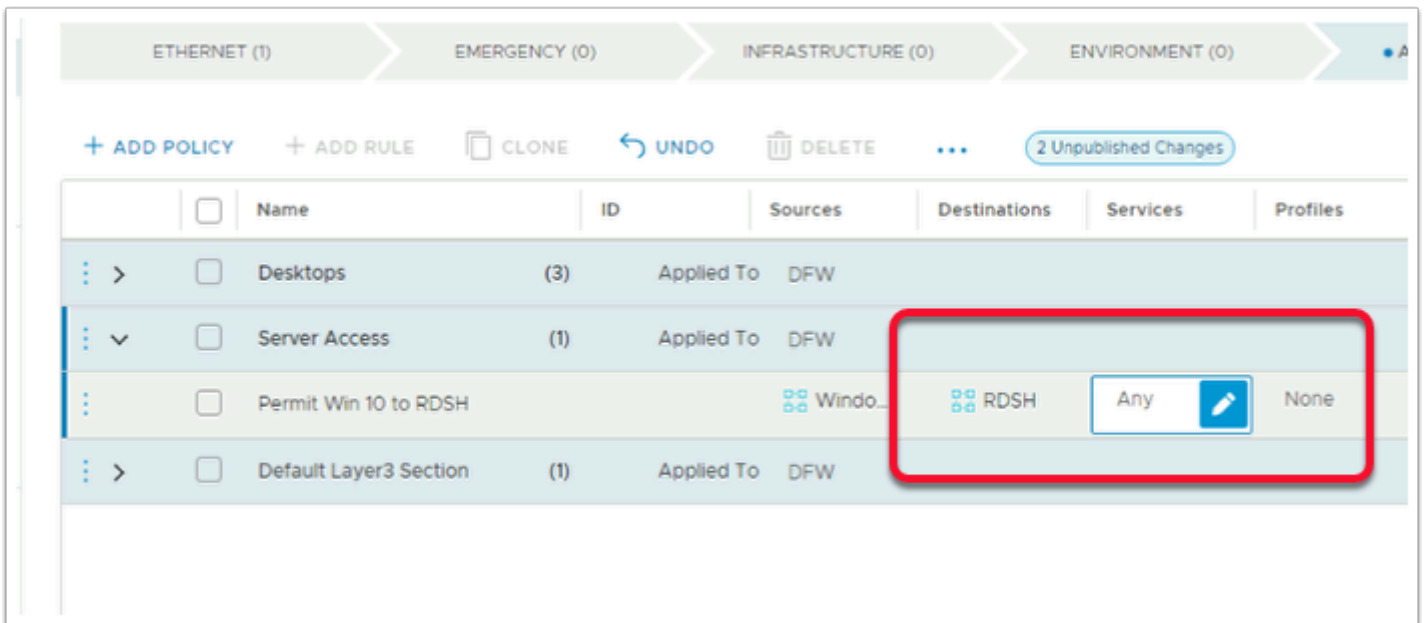
39. In the **Set Source** window,
- Select the **checkbox** next to **Windows 10**
 - Select **APPLY**



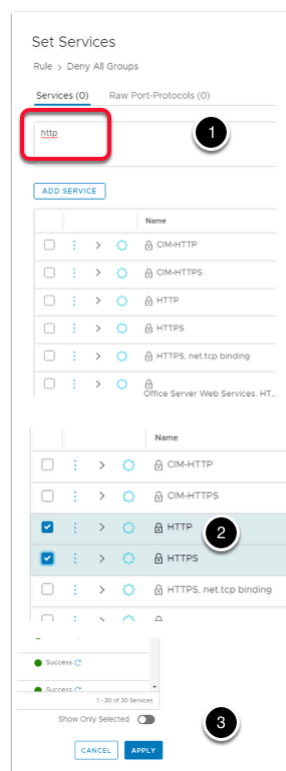
40. In the **Permit Win10 to RDSH** section
- Under **Destinations**, select the **Pencil** next to **Any**



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



42. In the **Permit Win 10 to RDSH** row under **Services** select the **Pencil** next to **Any**



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 Unpublished Changes Filter by Name, Path and

Destinations	Services	Profiles	Applied To	Action
RDSH	HTTP HTTPS	None	<div>DFW </div>	Allow

44. In the **Permit Win 10 to RDSH** row
- Under **Applied To** select the **Pencil** next to **DFW**

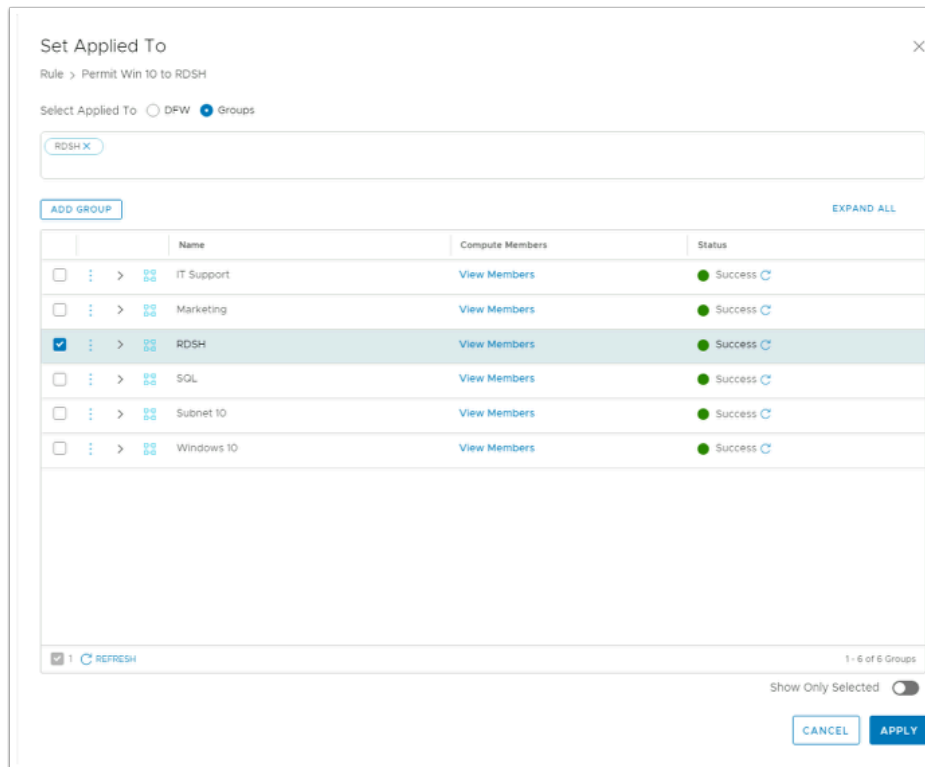
Set Applied To

Rule > Marketing Rule

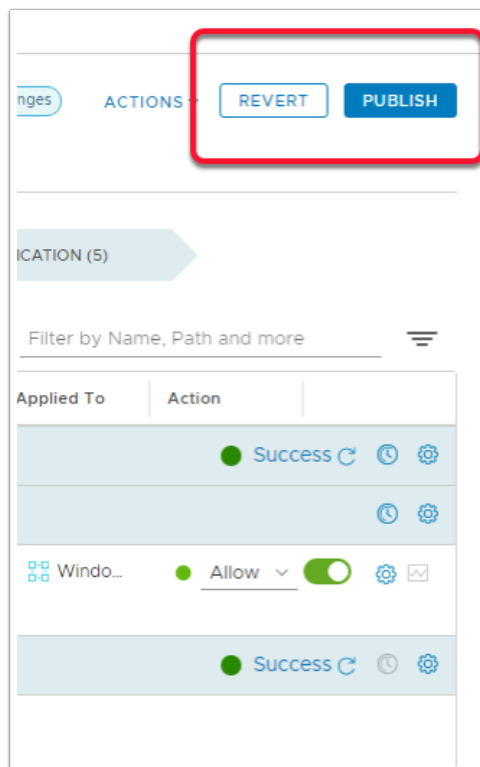
Select Applied To ☐ DFW ☒ Groups

[ADD GROUP](#)

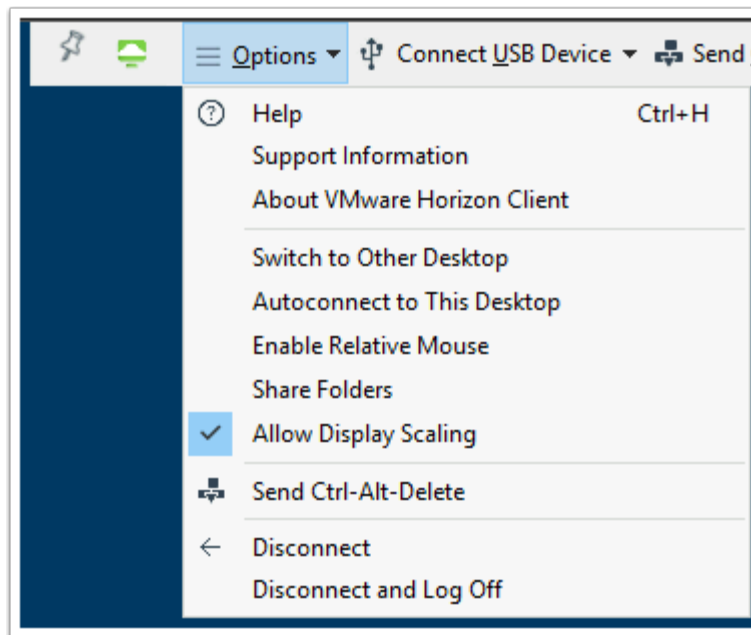
45. In the **Set Applied To** window select the **Groups** radio button



46. In the **Set Applied To** window
- Select the **RDSH** group **checkbox**
 - Select **Apply**



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



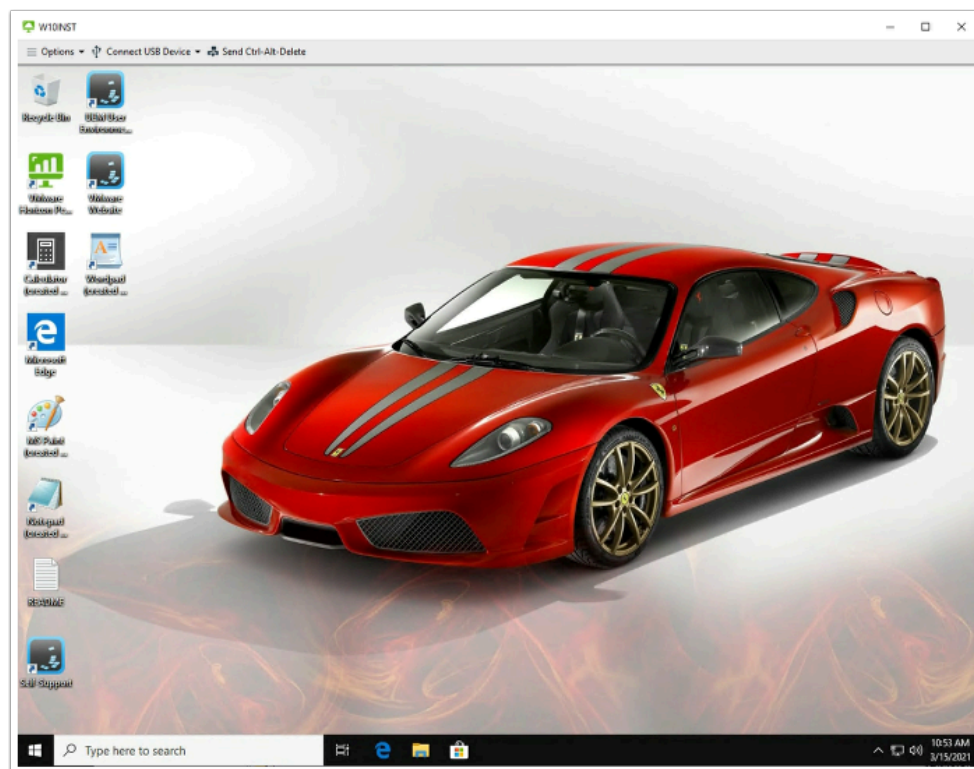
49. Please NOTE: When **Identity Based Firewall** rules are applied, it is essential, to logon after the rules have been applied. Any Active VMware Horizon sessions that you are logged into, **Disconnect and Log Off** before starting with Part 3

Part 3. Testing the results

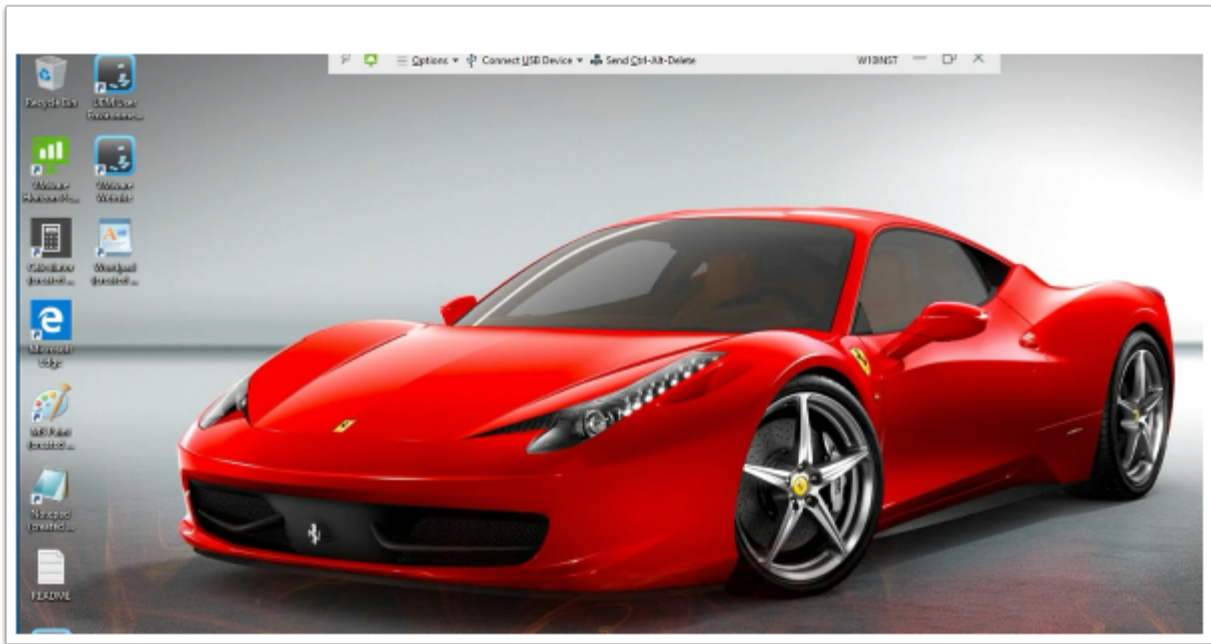
Some background information about our setup and what we are going to test.

- 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**

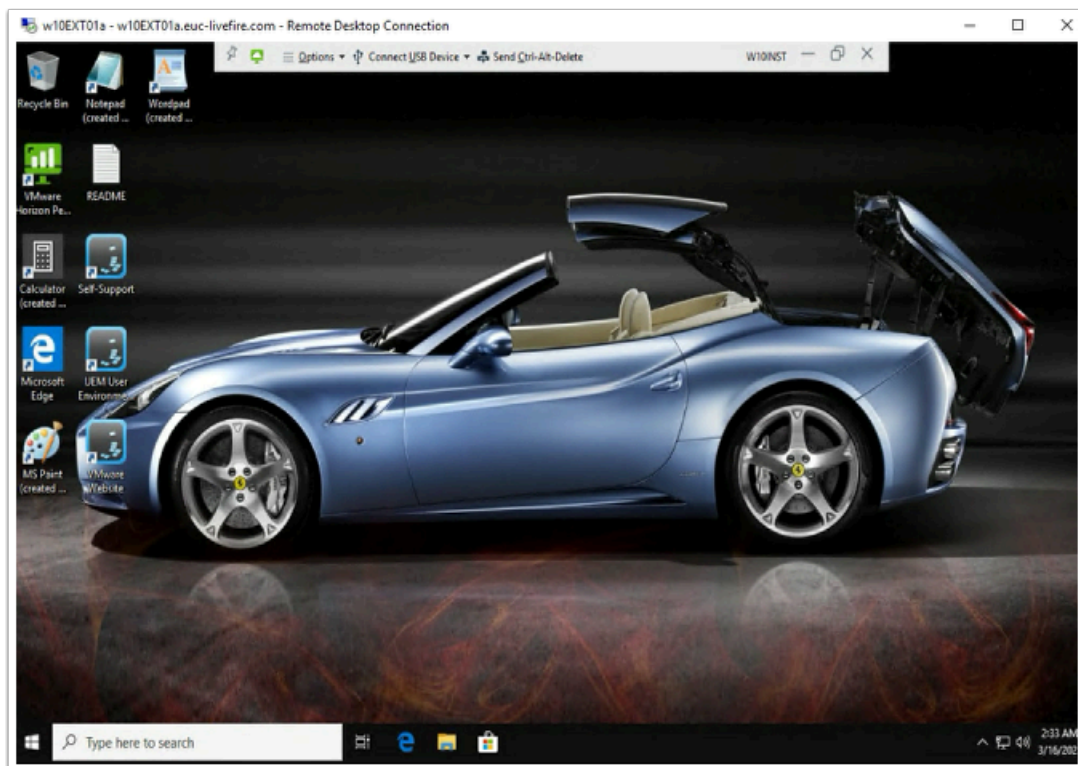
Part 3 :



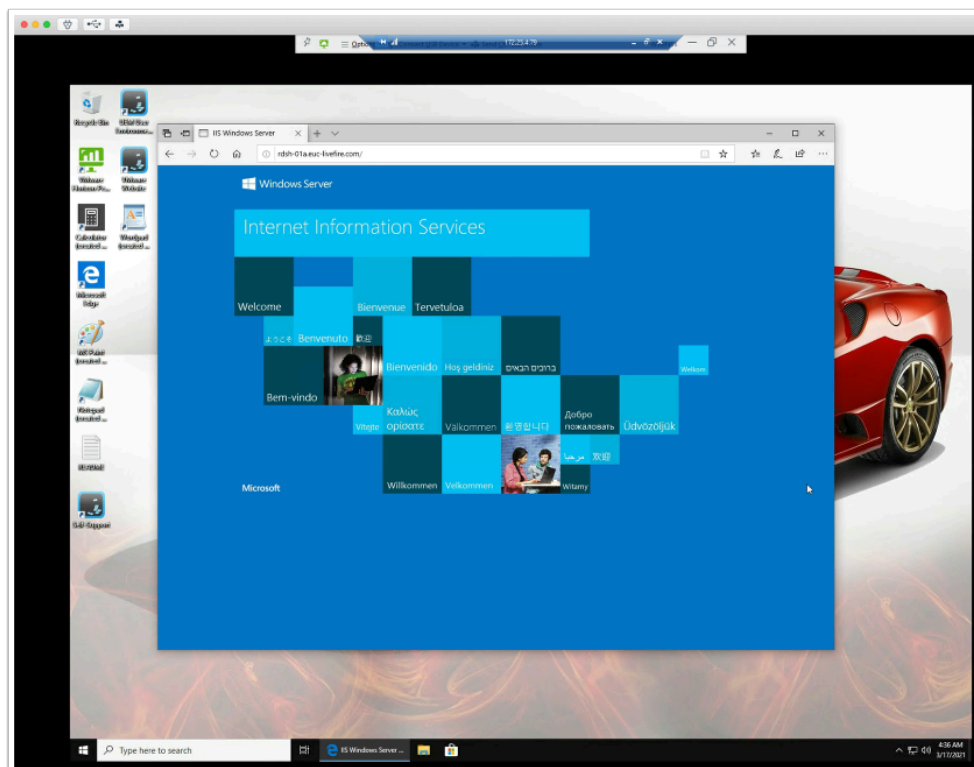
1. On your **ControlCenter** desktop,
 - Launch the **Horizon client**
 - Launch the **Horizon .euc-livewire.com** POD
 - On the Login window next to
 - User name: **Mark**
 - Password : **VMware1!**
 - Select **Login**
 - Select the **W10INST** entitlement



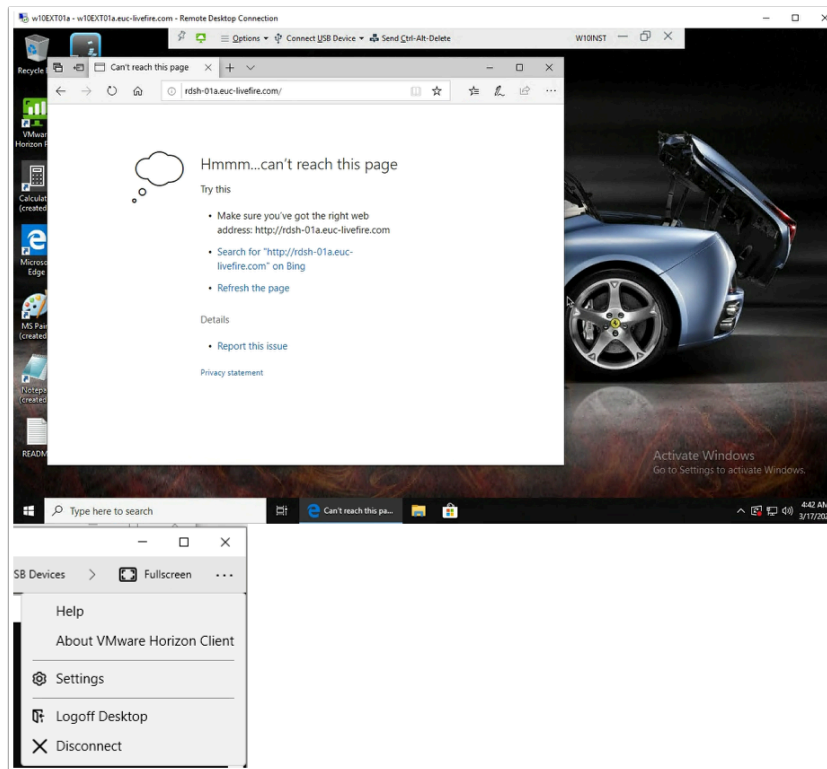
2. On your **ControlCenter** desktop, launch the **Horizon client**
 - Launch the **Horizon.euc-livefire.com** POD
 - On the Login window next to
 - User name: **Jill**
 - Password : **VMware1!**
 - Select **Login**
 - Select the **W10INST** entitlement



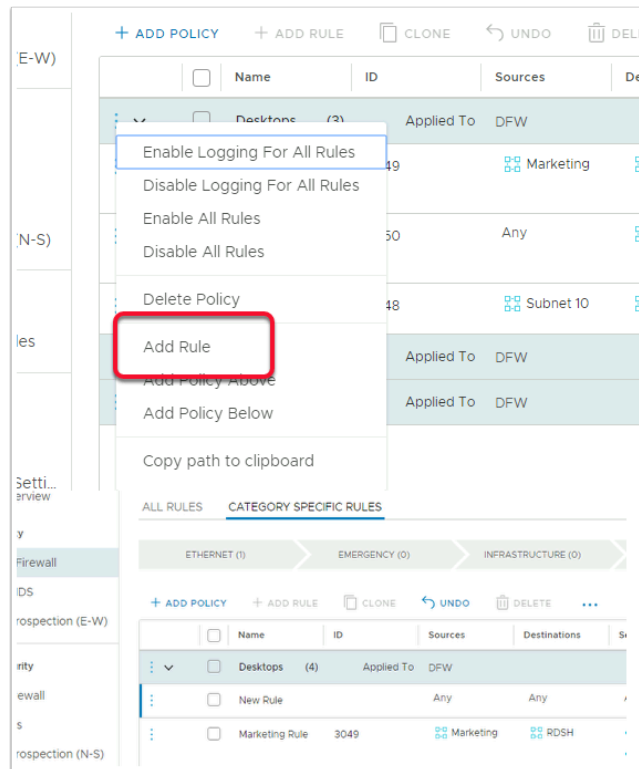
3. On your **ControlCenter** desktop, open the **Remote Desktops** folder
 1. Launch the **RDP** client for **W10Ext01a.RDP**
 - Login as **administrator@euc-livefire.com** with password **VMware1!**
 2. On the **W10 client** Launch the **Horizon client**
 - Launch the **Horizon.euc-livefire.com** POD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



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

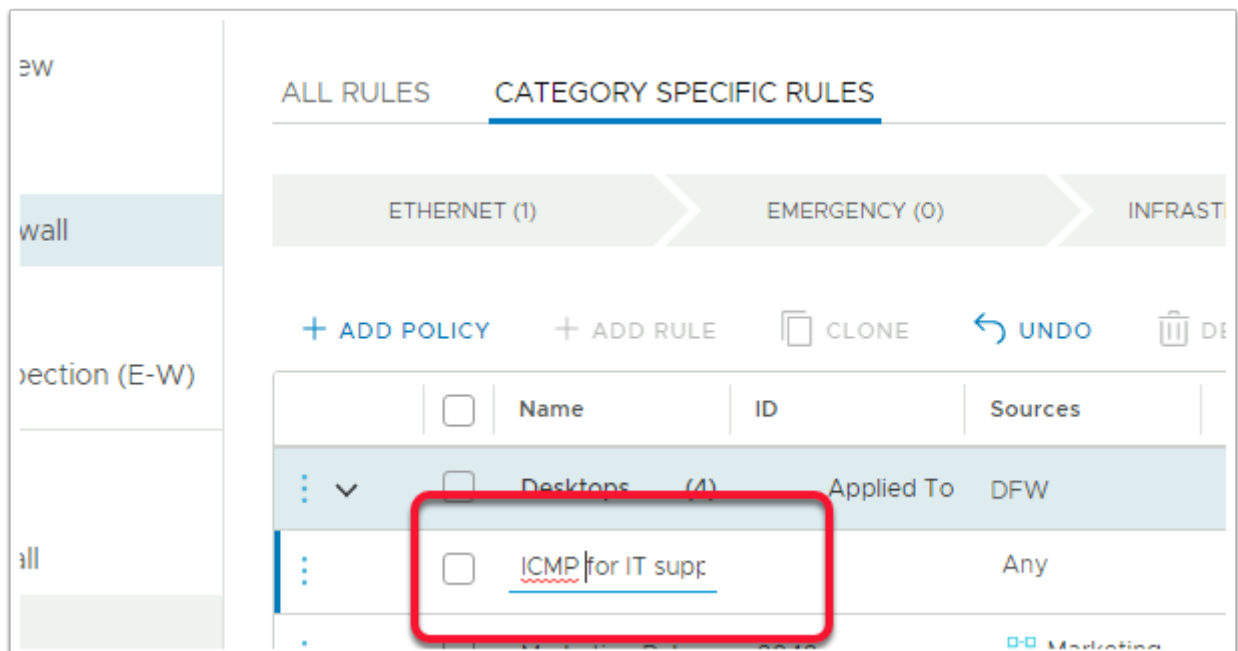


5. Switch to your **Kim** Horizon client session running from **W10EXT01a**
 - On the Desktop, select and launch the **Edge Browser** in the **Task Bar**
 - In the **Edge Browser** address, type **<http://rdsh-01a.euc-livewire.com>**
 - **Kim** is not a member of the **Sales Group** and would therefore 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**

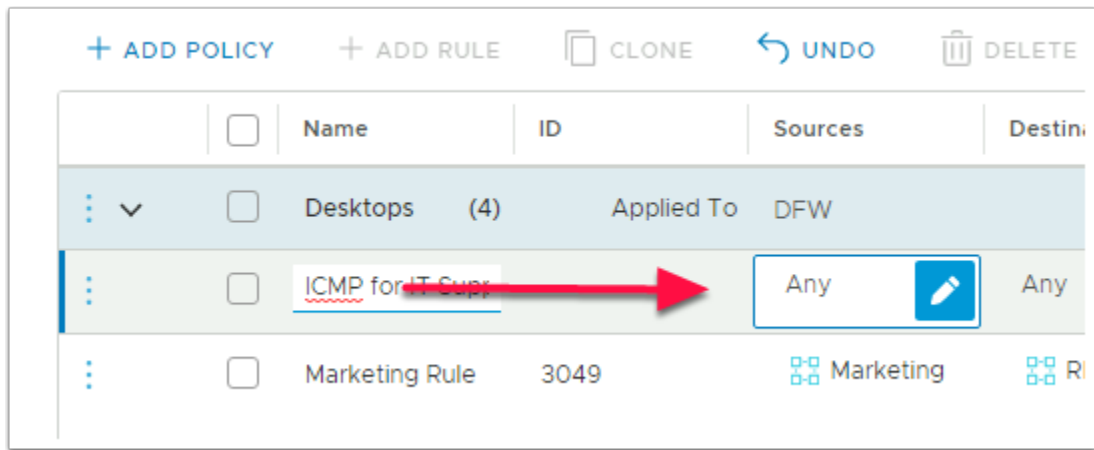


6. Switch back to your NSX-T admin console. Ensure you are still in **Security > Distributed Firewall**

- Select **3 Dots** next to **Desktops Policy** and select **Add Rule**,
- Notice you now have a **New Rule**



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



8. In the **ICMP for IT Support** row under **Sources**
 - Select 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

Tags

SAVE CANCEL

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

Select Members | IT Support

Add Compute Members either by creating or by directly adding them. You can also add Identity members separately. Compute members to define effective membership of the group.

Membership Criteria (0) Members (0) IP Addresses (0) MAC Addresses (0) **AD Groups (0)**

IT supp

Name
<input type="checkbox"/> IT Support

Name
<input checked="" type="checkbox"/> IT Support

1 - 1 of 1 AD Groups

groups can be part of a Group

CANCEL APPLY

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

12. Select **SAVE**
 - Select **APPLY** to close the **Set Source** window

POLICY	+ ADD RULE	CLONE	UNDO	DELETE	...	1 Unpublish
<input type="checkbox"/>	Name	ID	Sources	Destinations	Services	
<input type="checkbox"/>	Desktops	(4)	Applied To	DFW		
<input type="checkbox"/>	ICMP for IT Su...		IT Support	Any	Any	
<input type="checkbox"/>	Marketing Rule	3049	Marketing	RDSH	HTTP HTTPS	

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

Set Destination

Rule > ICMP for IT Support

Negate Selections ☐ No Negated selections will

Groups (1) IP Addresses (0)

RDSH X

ADD GROUP

	Name
<input type="checkbox"/>	IT Support
<input type="checkbox"/>	Marketing
<input checked="" type="checkbox"/>	RDSH
<input type="checkbox"/>	SOL

1 - 6 of 6 Groups

Show Only Selected ☐

CANCEL APPLY

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

ONE	UNDO	DELETE	...	1 Unpublished Change
Sources	Destinations	Services	Profiles	
Applied To: DFW				
IT Support	RDSH	Any	None	
Marketing	RDSH	HTTP HTTPS	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
<input type="checkbox"/> ⋮ > ⚙️ 🔒	ICMP ALL

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

ADD SERVICE

	Name
<input checked="" type="checkbox"/> ⋮ > ⚙️ 🔒	ICMP ALL

● Success ↻

● Success ↻

● Success ↻

1 - 23 of 23 Services

Show Only Selected ☐

CANCEL

APPLY


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

- Select **APPLY**

...

1 Unpublished Change

Filter by Name

Names	Services	Profiles	Applied To	Actions
H	ICMP ALL	None	DFW	
H	HTTP	None	Window	

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

Set Applied To

Rule > ICMP for IT Support

Select Applied To

☒ DFW
☐ Groups

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

Set Applied To

Rule > ICMP for IT Support

Select Applied To ☐ DFW ☒ Groups

Windows 10 X

ADD GROUP

	Name
<input type="checkbox"/>	IT Support
<input type="checkbox"/>	Marketing
<input type="checkbox"/>	RDSH
<input type="checkbox"/>	SQL
<input type="checkbox"/>	Subnet 10
<input checked="" type="checkbox"/>	Windows 10

1 - 6 of 6 Groups

Show Only Selected ☐

CANCEL **APPLY**

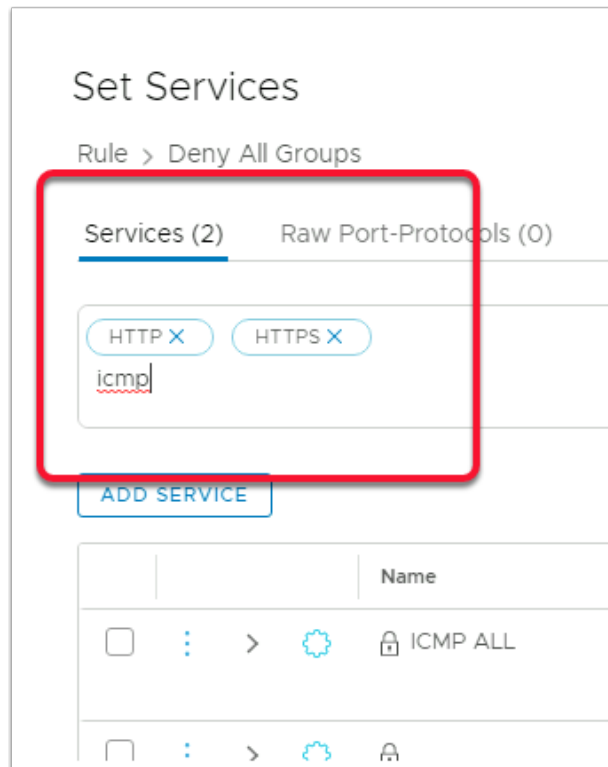
20. In the **Groups Area**

- Select the **checkbox** next to **Windows 10**
- Select **APPLY**

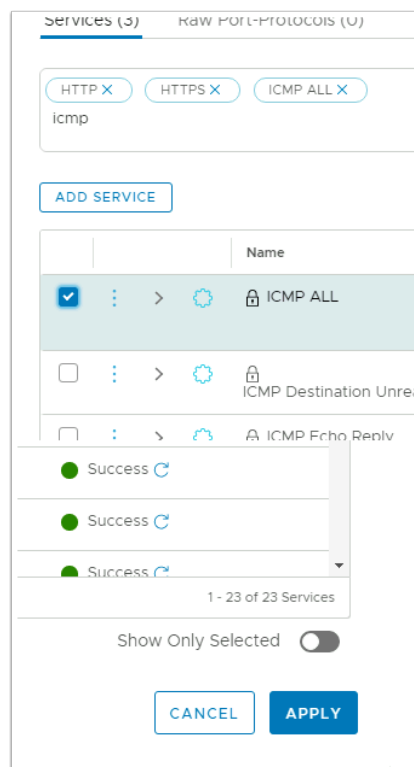
+ ADD POLICY **+ ADD RULE** **CLONE** **UNDO** **DELETE** **...** **1 Unpublished Change**

	<input type="checkbox"/>	Name	ID	Sources	Destinations	Services	Profiles
▼	<input type="checkbox"/>	Desktops (4)	Applied To	DFW			
⋮	<input type="checkbox"/>	ICMP for IT Su...	3052	IT Support	RDSH	ICMP ALL	None
⋮	<input type="checkbox"/>	Marketing Rule	3049	Marketing	RDSH	HTTP HTTPS	None
⋮	<input type="checkbox"/>	Deny All Grou...	3050	Any	RDSH	HTTP HTTPS	None
⋮	<input type="checkbox"/>	Block ICMP to ...	3048	Subnet 10	SQL	ICMP ALL	None

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

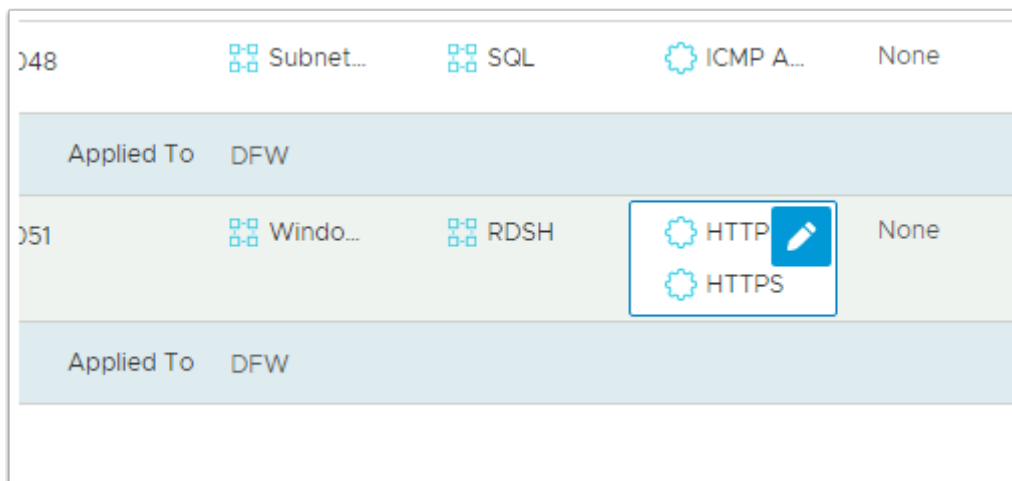


22. In the **Set Services** window under **Services** type **icmp**



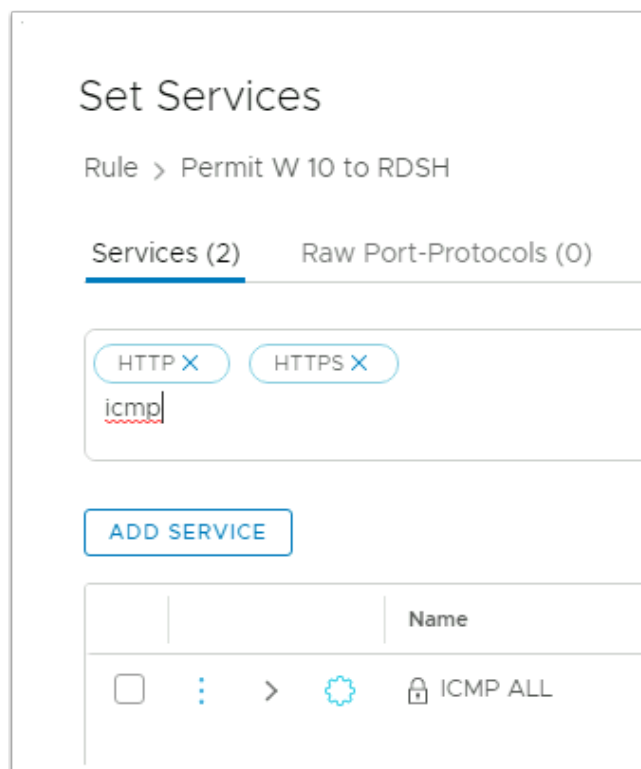
23. Select the **check box** next **ICMP ALL**

- Select **APPLY**

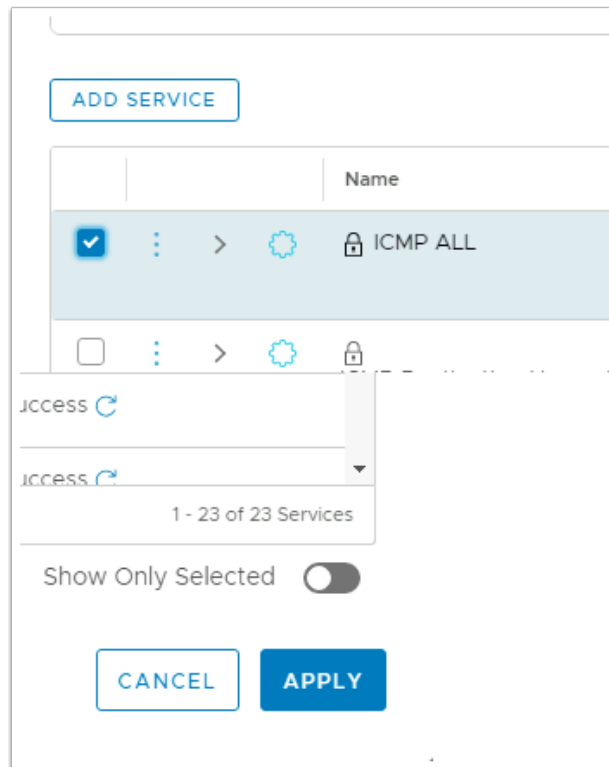


24. Expand the **Server Access** Policy

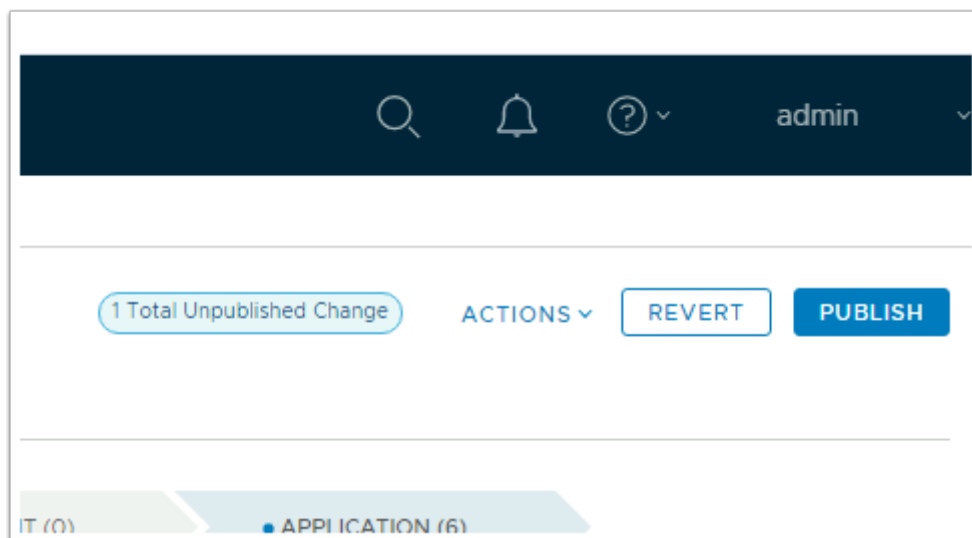
- In the **Permit W10 to RDSH** row under **Services**, select the **Pencil** next to **HTTP/HTTPS**



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



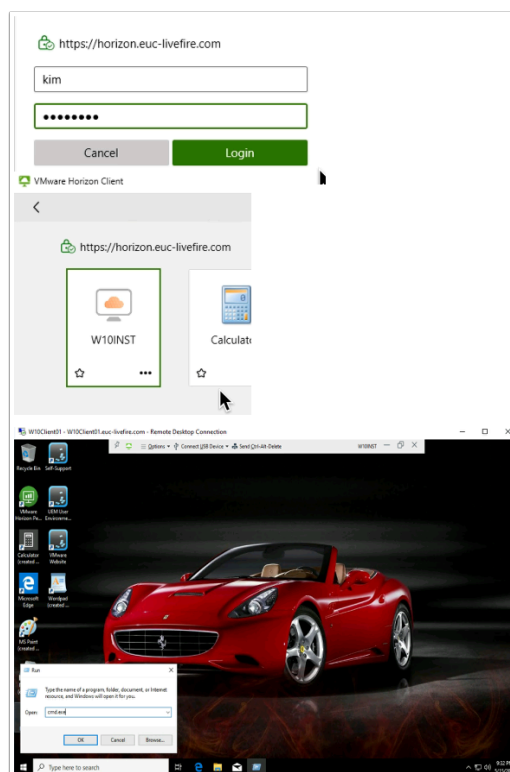
26. Select the **check box** next **ICMP ALL**
- Select **APPLY**



27. Select **PUBLISH**

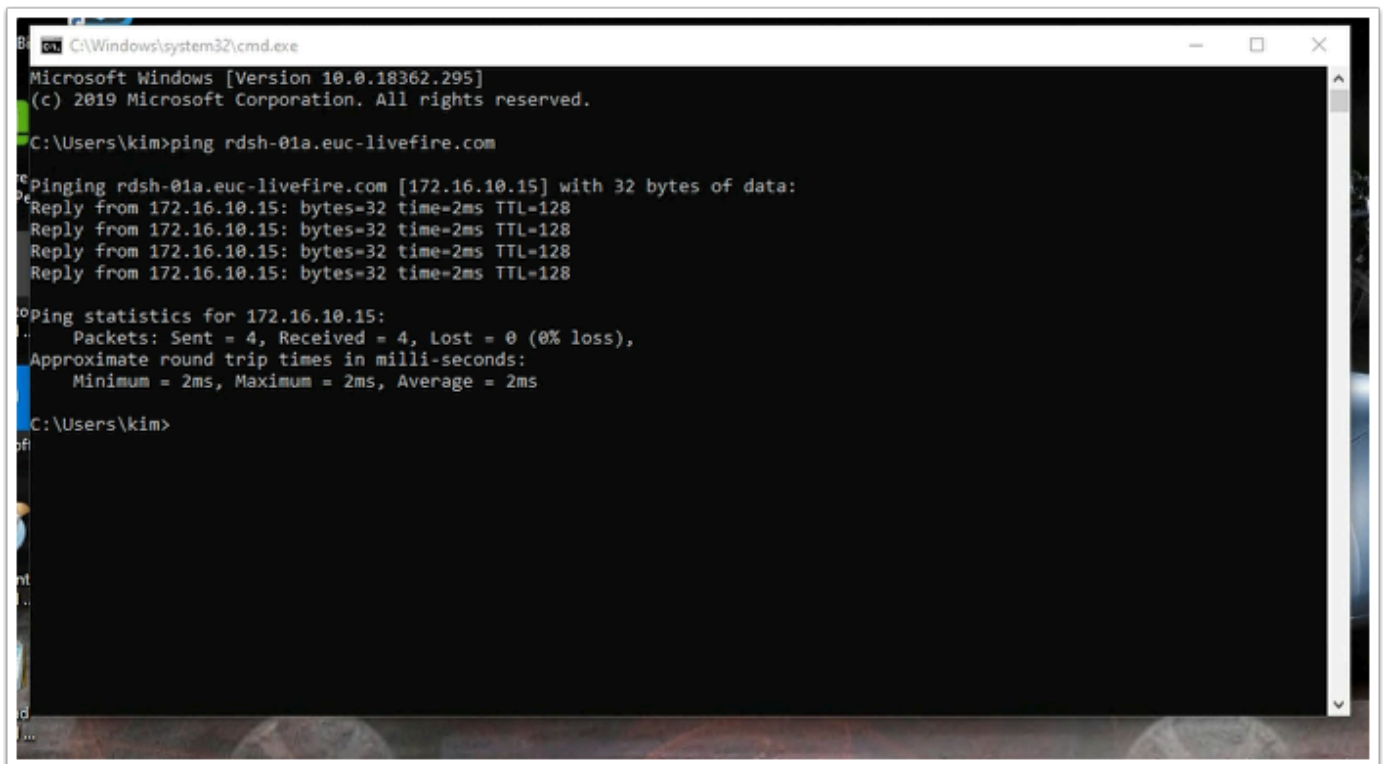
ETHERNET (1) EMERGENCY (0) INFRASTRUCTURE (0) ENVIRONMENT (0) APPLICATION (6)									
+ ADD POLICY + ADD RULE CLONE UNDO DELETE ... 1 Unpublished Change Filter by Name, Path and more									
	Name	ID	Sources	Destinations	Services	Profiles	Applied To	Action	
⌵	Desktops	(4)	Applied To	DFW				Success	ⓘ ⚙
⋮	ICMP for IT Support	3052	IT Sup...	RDSH	ICMP A...	None	Windo...	Allow	⌵ ⓘ ⚙
⋮	Marketing Rule	3049	MarketL...	RDSH	HTTP HTTPS	None	Windo...	Allow	⌵ ⓘ ⚙
⋮	Deny All Groups	3050	Any	RDSH	HTTP HTTPS ICMP A...	None	Windo...	Reject	⌵ ⓘ ⚙
⋮	Block ICMP to SQL	3048	SubnetL...	SQL	ICMP A...	None	DFW	Reject	⌵ ⓘ ⚙
⌵	Server Access	(1)	Applied To	DFW				Success	ⓘ ⚙
⋮	Permit W10 to RDSH	3051	Windo...	RDSH	HTTP HTTPS ICMP A...	None	Windo...	Allow	⌵ ⓘ ⚙
⌵	Default Layer3 Section	(1)	Applied To	DFW				Success	ⓘ ⚙

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



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**



```
Microsoft Windows [Version 10.0.18362.295]
(c) 2019 Microsoft Corporation. All rights reserved.

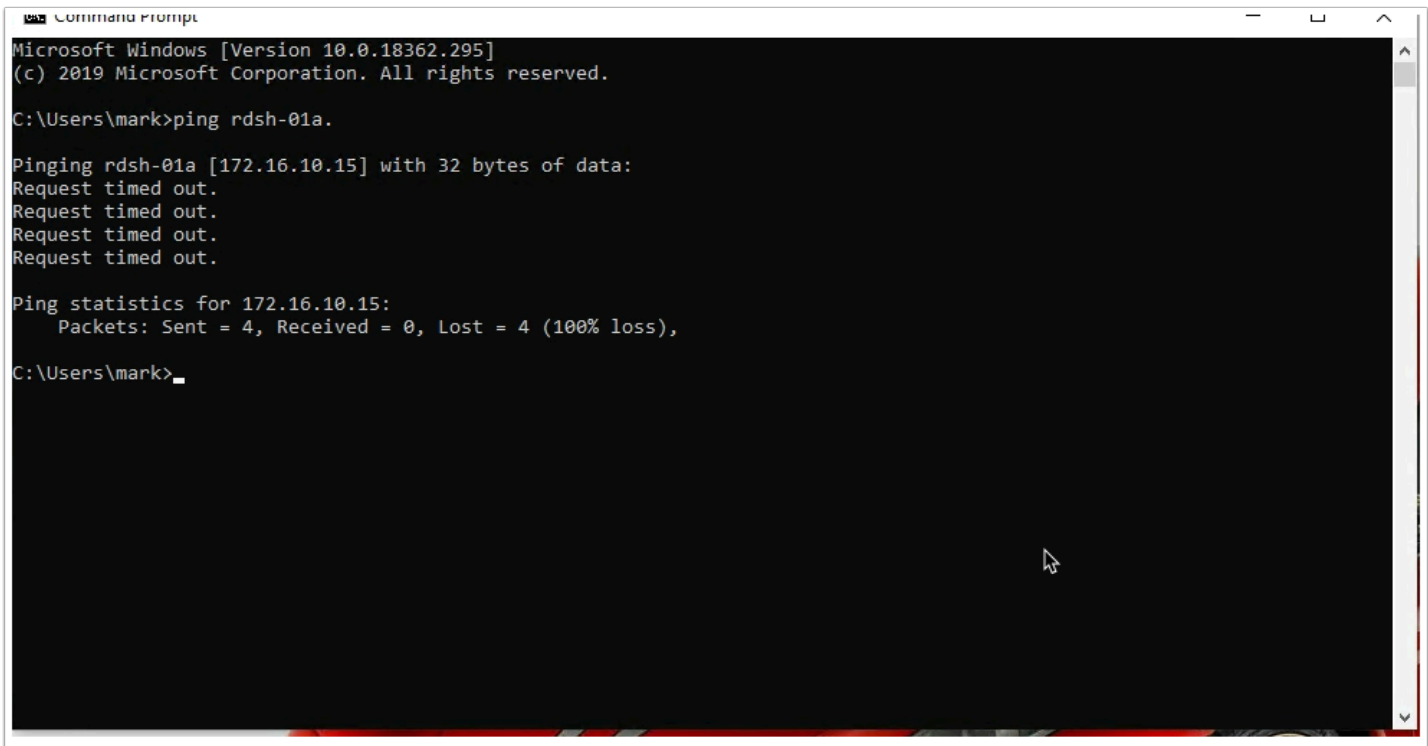
C:\Users\kim>ping rdsh-01a.euc-livewire.com

Pinging rdsh-01a.euc-livewire.com [172.16.10.15] with 32 bytes of data:
Reply from 172.16.10.15: bytes=32 time=2ms TTL=128
Reply from 172.16.10.15: bytes=32 time=2ms TTL=128
Reply from 172.16.10.15: bytes=32 time=2ms TTL=128
Reply from 172.16.10.15: bytes=32 time=2ms TTL=128

Ping statistics for 172.16.10.15:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\Users\kim>
```

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



```
Microsoft Windows [Version 10.0.18362.295]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\mark>ping rdsh-01a.

Pinging rdsh-01a [172.16.10.15] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 172.16.10.15:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\mark>
```

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-livfire.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

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

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.livfire.solutions/meet-the-team/reinhartnel/>

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