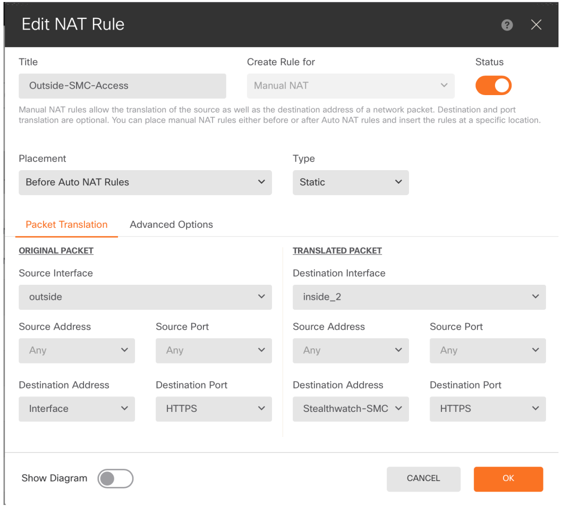
How To Configure Port Fowarding On FirePower Using FDM

1. Log into FDM and then click on the Policies section at the top of the page.
2. Click on NAT under Security Policies
3. Click the + on the right-hand side of the page to add a NAT rule
4. Enter a title for your NAT rule
5. Set Create Rule for to Manual NAT
6. Change Placement to Before Auto NAT Rules
7. Set type to Static
8. Under Original Packet
    a. Set Source Interface to your external interface
    b. Set Destination Address to Interface
    c. Set Destination Port to the port you're forwarding
9. Under Translated Packet
    a. Set Destination Interface to the appropriate internal interface
    b. Set Destination Address to the internal device you're sending data to.
        i. If the device object does not already exist, click the option Create new Network to define it first, then select it.
    c. Set the Destination Port to the port you're forwarding
10. Click OK

Sample NAT Rule:



Edit NAT Rule

Title: Outside-SMC-Access
Create Rule for: Manual NAT
Status: on

Manual NAT rules allow the translation of the source as well as the destination address of a network packet. Destination and port translation are optional. You can place manual NAT rules either before or after Auto NAT rules and insert the rules at a specific location.

Placement: Before Auto NAT Rules
Type: Static

Packet Translation | Advanced Options

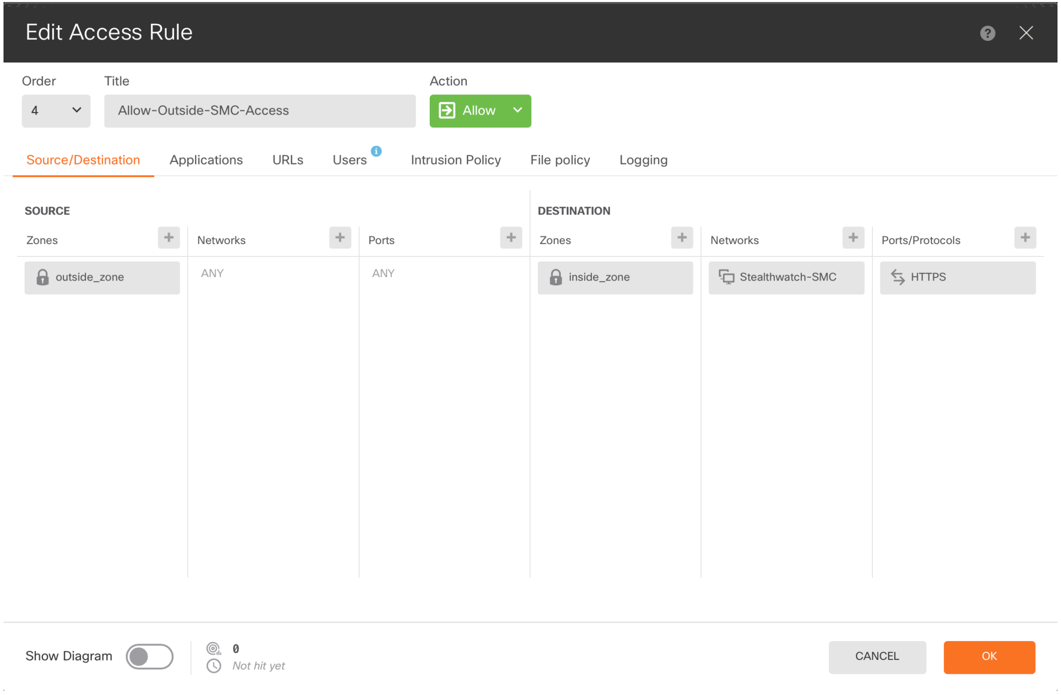
ORIGINAL PACKET
Source Interface: outside
Source Address: Any
Source Port: Any
Destination Address: Interface
Destination Port: HTTPS

TRANSLATED PACKET
Destination Interface: inside_2
Source Address: Any
Source Port: Any
Destination Address: Stealthwatch-SMC
Destination Port: HTTPS

11. At the top of the page, click on Access Control under Security Policies
12. Click the + on the right-hand side of the page to add an Access Control policy
13. Click the drop down under Order and select the appropriate spot. (You probably towards the top.)
14. Under Source:
    a. Click + next to Zones and select your outside zone
15. Under Destination:
    a. Click the + next to Zones and select your inside zone

b. Click the + next to Networks and select the internal host you will be sending the port forward to
c. Click the + next to Ports/Protocols and select the port you will be forwarding

Sample Access Rule:



Edit Access Rule

Order: 4

Title: Allow-Outside-SMC-Access

Action: Allow

SOURCE			DESTINATION		
Zones	Networks	Ports	Zones	Networks	Ports/Protocols
outside_zone	ANY	ANY	inside_zone	Stealthwatch-SMC	HTTPS

16. *Optional* Set the Intrusion & File Policies, and/or set the Logging option
17. Click OK

Click the icon at the top of the screen, and deploy your changes.