

pfSense - Regression #14987

``Interface Address`` is no longer an option for outbound NAT targets

11/15/2023 08:43 AM - Danilo Zrenjanin

Status:	Not a Bug	Start date:	
Priority:	Normal	Due date:	
Assignee:		% Done:	0%
Category:	Rules / NAT	Estimated time:	0.00 hour
Target version:		Affected Version:	2.7.2
Plus Target Version:		Affected Architecture:	All
Release Notes:	Default		

Description

After upgrading to version 23.09, the option to choose a Tailscale address when defining an outbound NAT rule on the Tailscale interface is no longer available.

Steps to reproduce.

- 1.) Define Tailscale setup and confirm that it is active under Status/Tailscale
- 2.) Navigate to Firewall/NAT/Outbound and define a new mapping using the Tailscale interface.
- 3.) Click on the Translation - Address drop-down menu.
- 4.) Notice that there is no option for a Tailscale address to choose.

Translation

Address

Network or Alias

Type

Address

Connections matching this rule will be mapped to the specified address. If specifying a custom network or alias, it must be a valid IP address or network.

Pool options

Default

Only Round Robin types work with Host Aliases. Any type can be used with a Subnet.

Round Robin: Loops through the translation addresses.

History

#1 - 11/15/2023 09:00 AM - Lev Prokofev

- File clipboard-202311151300-hsm4m.png added
- Status changed from New to Confirmed

Can confirm this,

tested on

23.09-RELEASE (amd64)
built on Tue Oct 31 22:56:00 MSK 2023
FreeBSD 14.0-CURRENT

Translation

Address

Network or Alias

Type

Connections matching this rule will be mapped

Pool options

Default

Only Round Robin types work with Host Aliases

- Round Robin: Loops through the translation pool until a valid address is found.
- Random: Selects an address from the translation pool at random.
- Source Hash: Uses a hash of the source IP address to select an address, ensuring that the redirection address is always the same for a given source.
- Bitmask: Applies the subnet mask and keeps only the bits specified in the bitmask.
- Sticky Address: The Sticky Address option is always mapped to the same translation pool entry.

Port or Range

Enter the external source Port or Range used for remapping the original source port on connections matching the rule.

Port ranges are a low port and high port number separated by a hyphen. Leave blank when Static Port is checked.

T

Cl

La

M

ne

Ne

Ru

ru

Sp

Sp

tie

tra

Yc

M

te

1

/ 128

- #2 - 11/15/2023 11:58 AM - aleksei prokofiev
- File clipboard-202311151456-gyk8a.png added
 - File clipboard-202311151456-da78t.png added
 - File clipboard-202311151458-eunfa.png added
 - File clipboard-202311151458-tggqd.png added

Tested
23.09-RELEASE (amd64)
built on Tue Oct 31 22:56:00 MSK 2023
FreeBSD 14.0-CURRENT

If I assign Tailscale interface, in this case it is presented

Translation

Address

TAILSCALE1 address

Network or Alias

WAN address

LAN address

TAILSCALE1 address

Port or Range

Enter the external source Port or Range used for remapping the original source port on connections matching the rule.

☐ Static Port

Interface Assignments

Interface Groups

Wireless

VLANs

QinQs

PPPs

GREs

GIFs

Bridges

LAGGs

Interface	Network port
WAN	em0 (08:00:27:ec:05:8c)
LAN	em1 (08:00:27:d7:a4:6e) <div>Delete</div>
Tailscale1	tailscale0 (tailscale0) <div>Delete</div>

- #3 - 11/25/2023 09:53 AM - Danilo Zrenjanin
- I've just tested and confirmed on 23.05.1 that there was no need to assign the Tailscale interface to have it in the list of available interfaces in the Outbound NAT rules.
- Assigning a Tailscale interface in pfSense is wrong.
- #4 - 12/12/2023 02:22 AM - Chad Wagner
- Is there a workaround until this gets fixed?

#5 - 12/12/2023 04:25 AM - Mike Moore

I second this issue. Is there a workaround.
If you are using tailscale to set a Site2Site VPN then traffic leaving the tailscale interface to a remote network learned within the tailnet must be sourced using the Tailscale interface.

Danilo - Are you saying that outbound SNAT rules are done automatically now?

#6 - 12/12/2023 04:28 AM - Mike Moore

UPDATE:
I see the Tailscale interface has now been added back in 23.09.1

Please update the ticket to let us know if this is resolved permanently

#7 - 12/12/2023 04:43 AM - Chad Wagner

I am running 23.09.1. The Tailscale address is still missing from the pull-down menu in the translation section. In the setup video by Christian McDonald it says to not assign tailscale0 to an interface. Previously it appeared the "Tailscale address" selection was available in the outbound NAT rule creation without assigning the interface.

I have mine setup per the Tailscale website instructions, but it is basically making all UDP traffic have static NAT. I would rather have only Tailscale traffic be handled with static NAT.

#8 - 12/15/2023 08:29 AM - Danilo Zrenjanin



- File clipboard-202312150919-hksmq.png added
- File clipboard-202312150922-4btvs.png added
- File clipboard-202312150928-9zksy.png added

I've tested on 23.09.1. Indeed, there is no Tailscale address from the drop-down menu in the translation section.

As a workaround, you can define an IP Alias VIP using localhost as the Parent interface and the Tailscale address of that node for IP.

Firewall / Virtual IPs

Virtual IP Address

Virtual IP address	Interface	Type	Description	Actions
100.88.202.25/32	Localhost	IP Alias	tailscaleVIP	 

+ Add

In the outbound NAT rule, the VIP address defined in the previous step will be available in the drop-down menu.

Translation

Address

100.88.202.25 (tailscaleVIP)

Type

Connections matching this rule will be mapped to the specified address. If specifying a custom network or alias, it must be routed to the firewall.

Port or Range

☐ Static Port

Enter the external source **Port or Range** used for remapping the original source port on connections matching the rule.

Port ranges are a low port and high port number separated by ":".
Leave blank when **Static Port** is checked.

Once the outbound NAT rule is configured on both sides, the traffic flows as intended in both directions.

Firewall / NAT / Outbound

Port Forward1:1OutboundNPT

Outbound NAT Mode

Mode

Automatic outbound NAT rule generation.
(IPsec passthrough included)

Hybrid Outbound NAT rule generation.
(Automatic Outbound NAT + rules below)

Manual Outbound NAT rule generation.
(AON - Advanced Outbound NAT)

Disable Outbound NAT rule generation.
(No Outbound NAT rules)

Save

Mappings

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> Tailscale	LAN subnets	*	*	*	100.88.202.25 (tailscaleVIP)	*		test tailscale	

#9 - 12/15/2023 10:59 PM - Marcos M

- Project changed from pfSense Packages to pfSense
- Subject changed from Tailscale Address option is missing in Translation Address section under Firewall/NAT/Outbound to ``Interface Address`` is no longer an option for outbound NAT targets
- Category changed from Tailscale to Rules / NAT
- Status changed from Confirmed to Not a Bug
- Assignee deleted (Christian McDonald)
- Affected Version set to 2.7.2
- Release Notes set to Default
- Affected Architecture All added

The "Interface Address" selection is no longer available due to general changes to the outbound NAT pages which bring similar features as other parts of the firewall. For example:

- Expose <interface> subnets aliases in source/destination
- Expose <interface group> networks aliases in source/destination
- Alias popup preview on the NAT Address field
- Better error handling on rules to avoid filter reload failures

With other VPN types such as OpenVPN, IPsec, or WireGuard, the option isn't needed or simply doesn't apply. However, Tailscale is an edge case that indeed benefits from having the "Interface Address" option given that it cannot have an interface assignment. In this case, the address should be entered by selecting Network or Alias. If there's a use-case that necessitates frequently changing the interface address, an option for this edge case could be considered.

#10 - 12/20/2023 04:27 AM - Jonathan Lee

Does this cause issues with layer 2 experimental rules? They are MAC address or interface based.

Files			
clipboard-202311150941-pz0q7.png	38.2 KB	11/15/2023	Danilo Zrenjanin
clipboard-202311151300-hsm4m.png	68.9 KB	11/15/2023	Lev Prokofiev
clipboard-202311151456-gyk8a.png	30.9 KB	11/15/2023	aleksei prokofiev
clipboard-202311151456-da78t.png	4.79 KB	11/15/2023	aleksei prokofiev
clipboard-202311151458-eunfa.png	27.4 KB	11/15/2023	aleksei prokofiev
clipboard-202311151458-tggqd.png	23.5 KB	11/15/2023	aleksei prokofiev
clipboard-202312150919-hksmq.png	66.4 KB	12/15/2023	Danilo Zrenjanin
clipboard-202312150922-4btvs.png	116 KB	12/15/2023	Danilo Zrenjanin
clipboard-202312150928-9zksy.png	168 KB	12/15/2023	Danilo Zrenjanin