

Terminating bgp with apipa blocks on firewalls - Avoid at all times -

The problem

[Day 1]

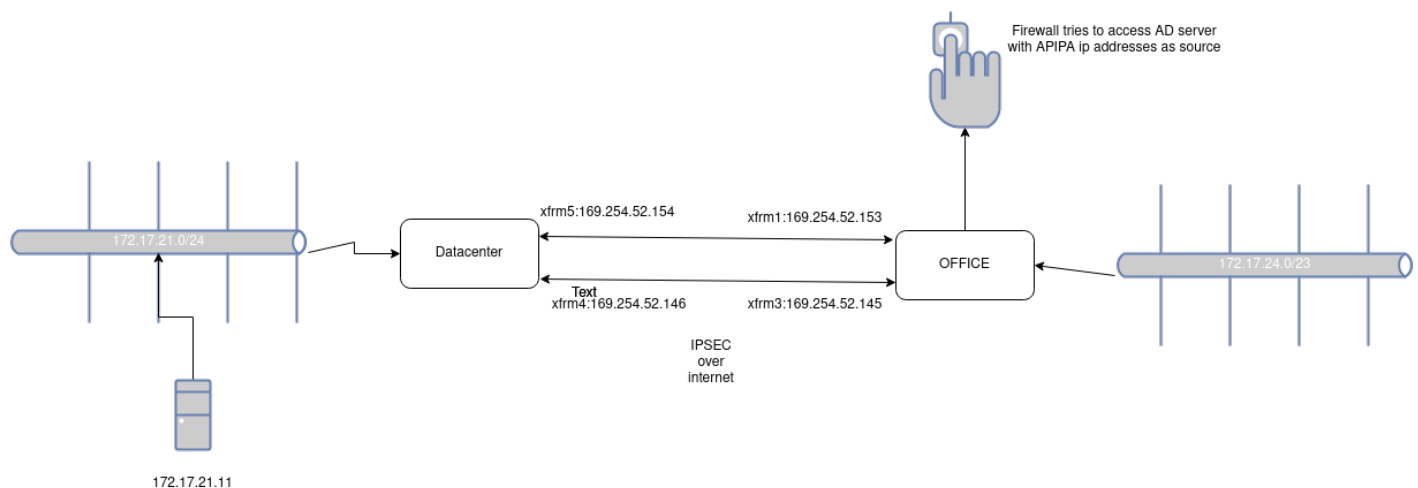
Today i got lost in sophos firewalls internal routing and nat labyrinths, what i was trying to do was a simple LDAP integration to a server at the end of a vpn tunnel. For interoperability reasons with AWS networks, we did use the famous "APIPA" block ip addresses on our bgp neighborship design.

But, there is catch !

There is always a catch and sometimes *a group of catches*. Windows server machines won't route or process apiipa address ranges. Блять right ? Anyway my options were clear

1. Change the addressing on ipsec links
2. Snat the connections getting out of the firewall

Here is the topology i was dealing with.



i got close

I thought that amazon must have a sound reason to use these blocks on their integrations. I am sure they never thought the apipa addresses were going to be used as source addresses on production links, or the CPE's might have limitations too.

I know that Fortigates have the option to specify source addresses for control plane operations however sophos doesn't have them. _insert sad emoji here _

there is one

Ok, i can always use the snat option right ? So i went with option 2 on my list.

And after two hours mangling with it i gave up and created a case, **which got the required attention immediately** from sophos, since the traffic is generated from firewall itself, a special snat entry was not going to be processed as i expect.

Apparently Postrouting operations weren't processed on **control plane chains**, and i really don't wanted to go with option 2 so a very capable and gentle guy from sophos tried helped me however we couldn't got the golden ticket today !

I did spent 3 hours working on this case learned many things about how kernel processes encrypted packets and found out good documents about how packets traverse when they are using xfrm framework. i am going to add the things i read at #further reading section below.

And will update this page on next update i get.

Further Reading

[Beautiful explanation of xfrm](#)

[How to use snat with xfrm if had a vyos](#)

This image from the post above displays the packet flow mech on linux.



[Strongswan xfrm implementation](#)

The solution

[day 5]

Apparently, there is a special section to add nat entries for "System Generated Traffic", and it is only accessible to command line interface. To do that you have to access the firewall through console using ssh and go to advanced menu as shown below.

Then you will have to type

```
cish
```

```
XGS2100_RL01_SFOS 19.0.1 MR-1-Build365# csh
Sophos Firmware Version SFOS 19.0.1 MR-1-Build365

Main Menu

  1. Network Configuration
  2. System Configuration
  3. Route Configuration
  4. Device Console
  5. Device Management
  6. VPN Management
  7. Shutdown/Reboot Device
  0. Exit

Select Menu Number [0-7]: 5

Sophos Firmware Version SFOS 19.0.1 MR-1-Build365

Device Management

  1. Reset to Factory Defaults
  2. Show Firmware(s)
  3. Advanced Shell
  4. Flush Device Reports
  0. Exit

Select Menu Number [0-4]: 3

Sophos Firewall
=====
(C) Copyright 2000-2022 Sophos Limited and others. All rights reserved.
Sophos is a registered trademark of Sophos Limited and Sophos Group.
All other product and company names mentioned are trademarks or registered
trademarks of their respective owners.

For Sophos End User Terms of Use - https://www.sophos.com/en-us/legal/sophos-end-user-terms-of-use.aspx

NOTE: If not explicitly approved by Sophos support, any modifications
done through this option will void your support.

XGS2100_RL01_SFOS 19.0.1 MR-1-Build365# cish
console> show advanced-firewall
Strict Policy : on
FtpBounce Prevention : control
Tcp Conn. Establishment Idle Timeout : 10800
UDP Timeout : 30
UDP Timeout Stream : 60
Fragmented Traffic Policy : allow
```

then you'll have to add a nat entry as shown below

```
set advanced-firewall sys-traffic-nat add destination 172.17.21.11 netmask 255.255.255.255 snatip 172.17.24.1
```

```
[
console> set advanced-firewall sys-traffic-nat add destination 172.17.21.11 netmask 255.255.255.255 snatip 172.17.24.1
console> show advanced-firewall
Strict Policy : on
FtpBounce Prevention : control
Tcp Conn. Establishment Idle Timeout : 10800
UDP Timeout : 30
UDP Timeout Stream : 60
Fragmented Traffic Policy : allow
Midstream Connection Pickup : off
TCP Seg Checking : on
TCP Window Scaling : on
TCP Appropriate Byte Count : off
TCP Selective Acknowledgements : on
TCP Forward RTO-Recovery[F-RTO] : off
TCP TIMESTAMPS : off
Strict ICMP Tracking : off
ICMP Error Message : allow
Caching for route lookups : on
IPv6 Unknown Extension Header : deny

Bypass Stateful Firewall
-----
Source Genmask Destination Genmask

NAT policy for system originated traffic
-----
Destination Network Destination Netmask Interface SNAT IP
172.17.21.11 255.255.255.255

console> ping 172.17.21.11172
ping: bad address '172.17.21.11172'
console> ^C
console> ping 172.17.21.11
PING 172.17.21.11 (172.17.21.11): 56 data bytes
64 bytes from 172.17.21.11: seq=0 ttl=127 time=6.115 ms
64 bytes from 172.17.21.11: seq=1 ttl=127 time=5.872 ms
64 bytes from 172.17.21.11: seq=2 ttl=127 time=5.662 ms
64 bytes from 172.17.21.11: seq=3 ttl=127 time=6.849 ms
64 bytes from 172.17.21.11: seq=4 ttl=127 time=6.032 ms

```

](<https://books.netdev.com.tr/uploads/images/gallery/2022-12/image-1672316296662.png>)

After you ping the destination or check the firewall you will see that the traffic is natted.

Revision #15

Created 19 December 2022 11:17:10 by Mesut Bayrak

Updated 21 October 2023 11:40:14 by Mesut Bayrak