Clarify the Purpose of Internal-Data Interface with nameif nlp_int_tap and IP Address 169.254.1.1

Contents

Introduction

This document describes the purpose of the Internal-Data nlp_int_tap interface with the IP address 169.254.1.1.

Prerequisites

Requirements

Basic product knowledge.

Components Used

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure

that you understand the potential impact of any command.

The information in this document is based on these software and hardware versions:

- Secure Firewall Threat Defense (FTD) 7.x, 10.x managed by the Secure Firewall Device Manager (FDM) or Secure Firewall Management Center (FMC).
- Secure ASA 9.18 and later.

Background Information

The Internal-Data interface with the nameif **nlp_int_tap** and the 169.254.1.1 IP address is an internal interface that is used to provide connectivity between the dataplane engine called **Lina** and the backend operating system (OS).

It is used to provide general connectivity for these services:

- SNMP – The SNMP daemon runs as a separate process in OS.
- SSH access to ASA with the Cisco SSH stack – the SSH daemon runs as a separate process in OS.
- SSH access to FTD over data interface – the SSH daemon runs as a separate process in OS.
- VRF-aware external authentication on FTD – access to external authentication servers is provided via a data interface in a global or user VRF.
- In case of FTD management over data interfaces, access to management services such as sftunnel, DNS resolution, licensing, external authentication, NTP or any destinations to which the OS does not have explicitly configured static routes over the management interface.

Lina Verification

Depending on the platform, in the Lina engine the nameif **nlp_int_tap** is assigned to Internal-DataX/Y interface and is visible in different command outputs.

These are outputs from different firewalls:

- Secure Firewall 6170 running FTD:

```
<#root>

CSF6170-1#

show interface ip brief


Interface                  IP-Address      OK?          Method Status      Protocol
…

Internal-Data1/1           169.254.1.1     YES          unset  up          up
```

…

CSF6170-1#

show controller

Internal-Data1/1:

ASA IPS/VM Internal Management Data Interface en_vtun rev00, port id 10

Major Configuration Parameters

Device Name : en_vtun

Linux Tun/Tap Device : /dev/net/tun/tap_nlp

…

CSF6170-1#

show interface detail | begin nlp_int_tap

<-- Output except Internal-Data slot and port ID is similar in other devices

Interface Internal-Data1/1 "nlp_int_tap", is up, line protocol is up

Hardware is en_vtun rev00

, BW Unknown Speed-Capability, DLY 1000 usec
(Full-duplex), (1000 Mbps)
Input flow control is unsupported, output flow control is unsupported
MAC address 0000.0100.0001, MTU 1500
IP address 169.254.1.1, subnet mask 255.255.255.248
12409 packets input, 837229 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
0 pause input, 0 resume input
0 L2 decode drops, 0 demux drops
12371 packets output, 816494 bytes, 0 underruns
0 pause output, 0 resume output
0 output errors, 0 collisions, 0 interface resets

```
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (0/0)
        output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
        12409 packets input, 663503 bytes
        12371 packets output, 643300 bytes
        43 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
        Interface number is 7
        Interface config status is active
        Interface state is active


CSF6170-1#

capture nlp interface ?

<-- Same as in other devices
  cplane       Capture packets on controlplane interface
  data-plane   Capture packets on dataplane interface

  nlp_int_tap  Capture packets on nlp_int_tap interface



Available interfaces to listen:
  eventing     Name of interface Management1/2
  inside       Name of interface Ethernet1/1
  management   Name of interface Management1/1


CSF6170-1#

show asp table interfaces

<-- Same as in other devices
…
Soft-np interface 'nlp_int_tap' is up
    context single_vf, nicnum 10, mtu 1500
        vlan <None>, Not shared, seclvl 100
        12409 packets input, 12371 packets output
        flags 0x0
…


CSF6170-1#

show asp table routing

                  <-- Same as in other devices
route table timestamp: 37
…
```

in 169.254.1.0 255.255.255.248 nlp_int_tap

in fd00:0:0:1::1 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff nlp_int_tap
in fd00:0:0:1:: ffff:ffff:ffff:ffff:: nlp_int_tap
out 255.255.255.255 255.255.255.255 nlp_int_tap
out

169.254.1.1 255.255.255.255 nlp_int_tap

out 169.254.1.0 255.255.255.248 nlp_int_tap
out 224.0.0.0 240.0.0.0 nlp_int_tap

out fd00:0:0:1::1 ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff nlp_int_tap

out fd00:0:0:1:: ffff:ffff:ffff:ffff:: nlp_int_tap

out fe80:: ffc0:: nlp_int_tap
out ff00:: ff00:: nlp_int_tap
…

- Firepower 4145 running ASA:

<#root>

asa#

show interface ip brief

Interface IP-Address OK? Method Status Protocol
…

Internal-Data0/2 169.254.1.1 YES unset up up

…

asa#

show controller

Internal-Data0/2:

ASA IPS/VM Internal Management Data Interface en_vtun rev00, port id 4102

Major Configuration Parameters

Device Name : en_vtun

Linux Tun/Tap Device : /dev/net/tun/tap_nlp

…

- Virtual FTD:

<#root>

firewall#

show interface ip brief

Interface IP-Address OK? Method Status Protocol

…

Internal-Data0/1 169.254.1.1 YES unset up up

…

firewall#

show controller

Internal-Data0/1:

ASA IPS/VM Internal Management Data Interface en_vtun rev00, port id 12

Major Configuration Parameters

Device Name : en_vtun

Linux Tun/Tap Device : /dev/net/tun/tap_nlp

…

- Virtual ASA:

```
<#root>
asav#
show interface ip brief

…
Internal-Data0/0           169.254.1.1     YES unset  up                    up

…
firewall#
show controller

Internal-Data0/0:

   ASA IPS/VM Internal Management Data Interface en_vtun rev00, port id 4

     Major Configuration Parameters

         Device Name           : en_vtun

         Linux Tun/Tap Device  : /dev/net/tun/tap_nlp

…
```

Key points:

- The nameif **nlp_int_tap** is assigned to different Internal-Data interfaces on different platforms.
- According to the **show asp table routing** command output, the Internal-Data interface with the nameif **nlp_int_tap** is assigned IPv4 address **169.254.1.1/29** and IPv6 address **fd00:0:0:1::1/64.**
- According to the **show controller** command output, this interface is a Linux Tun/Tap interface (specifically tap) available in **/dev/net/tun/tap_nlp.**

OS Verification

/dev/net/tun/tap_nlp is a Linux tap interface with these IP addresses:

- IPV4: **169.254.1.2/29** on virtual devices and **169.254.1.3/29** on hardware devices.
- IPV6: **fd00:0:0:1::2/64** on virtual devices and **fd00:0:0:1::3/64** on hardware devices.

Verification in virtual and hardware FTD devices:

- Virtual FTD:

<#root>

admin@firewall:~$

ip addr show dev tap_nlp

14:

tap_nlp

: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 06:dd:c8:b9:e9:cc brd ff:ff:ff:ff:ff:ff

    inet 169.254.1.2/29 brd 169.254.1.7 scope global tap_nlp:1

       valid_lft forever preferred_lft forever

    inet6 fd00:0:0:1::2/64 scope global

       valid_lft forever preferred_lft forever
    inet6 fe80::4dd:c8ff:feb9:e9cc/64 scope link
       valid_lft forever preferred_lft forever

- Secure Firewall 6170:

<#root>

admin@CSF6170-1:~$

ip addr show dev tap_nlp

7:

tap_nlp

```
: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether b2:5b:a0:bf:f6:69 brd ff:ff:ff:ff:ff:ff

    inet 169.254.1.3/29 brd 169.254.1.7 scope global tap_nlp:1


       valid_lft forever preferred_lft forever

    inet6 fd00:0:0:1::3/64 scope global


       valid_lft forever preferred_lft forever
    inet6 fe80::b05b:a0ff:febf:f669/64 scope link
       valid_lft forever preferred_lft forever
```

To provide connectivity back to the Lina the OS installs a routing rule for the routing table lookup of packets with the source IP addresses of the **tap_nlp** interface:

```
<#root>

admin@firewall:~$

ip rule show


0:      from all lookup local

32765:  from 169.254.1.2 lookup 1


<-- For packets sourced from 169.254.1.2 (or .3 in case of hardware devices), the routing table 1 is us
32766:  from all lookup main
32767:  from all lookup default

admin@firewall:~$

ip -6 rule show


0:      from all lookup local

32765:  from fd00:0:0:1::2 lookup 1


<-- For packets sourced from xxxx::2 (or xxxx:3 in case of hardware devices), the routing table 1 is us
32766:  from all lookup main

admin@firewall:~$

ip route show table 1
```

```
default via 169.254.1.1 dev tap_nlp

<-- Next hop for the default route in table 1 is 169.254.1.1 (Lina)

admin@firewall:~$

ip -6 route show table 1



default via fd00:0:0:1::1 dev tap_nlp

metric 1024 pref medium <-- Next hop for the default route in table 1 is fd00:0:0:1::1 (Lina)
```

Key points:

- IPv4 and IPv6 routing rules dictate that route lookup for packets sourced from the **nlp_tap** interface addresses is performed in routing table **1**.
- IPv4 and IPv6 versions of the routing table **1** contain default route with the next hop address that belongs to the Lina **nlp_int_tap** interface.

Packet Path and Capture Points

This section shows the packet path and capture points in 2 different cases:

- Management over data interface is disabled.
- Management over data interface is enabled.

Note: There is an additional scenario with the “Use the Data Interfaces as the Gateway” feature on FDM. From the routing, configuration and packet capture point perspective this scenario is similar to the FMC-managed FTD with management over data interface.

Management over data Interface is Disabled

This section describes the verification of packet path and capture points on FTD with these configuration details:

1. FTD is managed by FMC.
2. No management over data interface. This means the management interface is used to provide connectivity between the OS and the external network:

```
<#root>

>
```

```
show network management-data-interface


Physical Interface              Name of the Interface <-- empty output indicates disabled feature
```

3. At least one of these features is configured:

- SNMP on ASA or FTD.
- SSH access to ASA with the Cisco SSH stack. In ASA versions 9.23 and later the Cisco SSH stack is enabled and cannot be disabled.
- SSH access to FTD over data interfaces.
- HTTPS access over data interface on FDM-managed FTD.

4. Packet captures are configured in all capture points.

If one of previous mentioned features is configured, manual twice NAT rules are automatically configured. Depending on the feature ports/protocols, the NAT rules are different.

This is an example output with manual twice NAT rules for FTD SSH access over data interface:

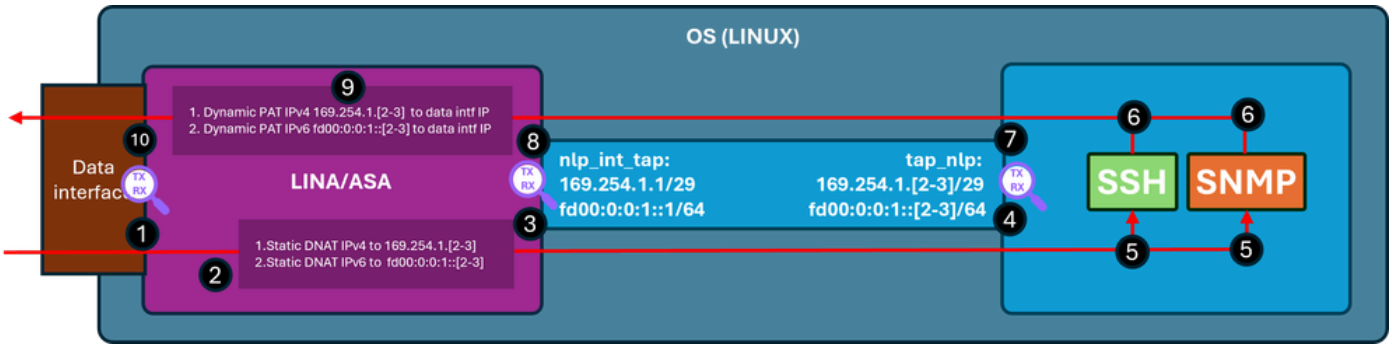
<#root>

```
firewall#

show nat detail


Manual NAT Policies Implicit (Section 0)
1 (nlp_int_tap) to (inside) source static nlp_server__ssh_0.0.0.0_intf3 interface  destination static 0
    translate_hits = 6, untranslate_hits = 6

    Source - Origin: 169.254.1.2/32, Translated: 192.0.2.1/24



    Destination - Origin: 0.0.0.0/0, Translated: 0.0.0.0/0



    Service - Protocol: tcp Real: ssh Mapped: ssh



2 (nlp_int_tap) to (inside) source static nlp_server__ssh_::_intf3 interface ipv6  destination static 0
    translate_hits = 0, untranslate_hits = 0

    Source - Origin: fd00:0:0:1::2/128, Translated:
```

```
    Destination - Origin: ::/0, Translated: ::/0


    Service - Protocol: tcp Real: ssh Mapped: ssh


3 (nlp_int_tap) to (inside) source dynamic nlp_client_0_0.0.0.0_6proto22_intf3 interface  destination s
    translate_hits = 0, untranslate_hits = 0


    Source - Origin: 169.254.1.2/32, Translated: 192.0.2.1/24


    Destination - Origin: 0.0.0.0/0, Translated: 0.0.0.0/0


    Service - Origin: tcp destination eq ssh , Translated: tcp destination eq ssh


4 (nlp_int_tap) to (inside) source dynamic nlp_client_0_ipv6_::_6proto22_intf3 interface ipv6  destinat
    translate_hits = 0, untranslate_hits = 0

    Source - Origin: fd00:0:0:1::2/128, Translated:


    Destination - Origin: ::/0, Translated: ::/0


    Service - Origin: tcp destination eq ssh , Translated: tcp destination eq ssh
```

Note: In the case of SSH connection to the ASA with the Cisco SSH stack, the destination port is translated from **22** to **4122.**

This diagram shows the packet path and capture points:



Verification steps (applicable to previously mentioned features):

1. Capture point – ingress TCP SYN packet for SSH from IP **192.0.2.2** to IP **192.0.2.1** on port **22**. IP **192.0.2.1** is the address of the inside interface:

```
<#root>

firewall#

show run ssh


ssh 0.0.0.0 0.0.0.0 inside
ssh ::/0 inside

firewall#

show ip


System IP Addresses:
Interface                Name                IP address      Subnet mask     Method
GigabitEthernet0/0

inside



192.0.2.1

        255.255.255.0   manual
Current IP Addresses:
Interface                Name                IP address      Subnet mask     Method
GigabitEthernet0/0

inside                  192.0.2.1

        255.255.255.0   manual

firewall#
```

```
show capture


capture capi type raw-data trace interface inside [Capturing - 218 bytes]
  match tcp any any

capture nlp type raw-data trace interface nlp_int_tap [Capturing - 218 bytes]
  match tcp any any

firewall#

show capture capi


1 packets captured
   1:

19:52:27.776830       192.0.2.2.22420 > 192.0.2.1.22

: S 240217016:240217016(0) win 8192
```

2. Capture trace indicates a matching NAT rule that translates the destination IP from **192.0.2.1** to IP **169.254.1.2**, and diverts packets to the **nlp_int_tap** egress interface:

```
<#root>

firewall#

show capture capi trace packet-number 1


Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 22936 ns
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 22936 ns
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: UN-NAT
Subtype: static
Result: ALLOW
Elapsed time: 11224 ns
Config:
```

nat (nlp_int_tap,inside) source static nlp_server__ssh_0.0.0.0_intf3 interface destination static 0_0.0.

<-- matching NAT rule
Additional Information:

NAT divert to egress interface nlp_int_tap(vrfid:0)

<-- Egress interface is nlp_int_tap

Untranslate 192.0.2.1/22 to 169.254.1.2/22

<-- Destination address was translated to 169.254.1.2
…

Phase: 15
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Elapsed time: 13664 ns
Config:
Additional Information:

Found next-hop 169.254.1.2 using egress ifc nlp_int_tap(vrfid:0)

<-- next hop is the nlp_int_tap with IP 169.254.1.2

Phase: 16
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Elapsed time: 2440 ns
Config:
Additional Information:

Found adjacency entry for Next-hop 169.254.1.2 on interface nlp_int_tap

Adjacency :Active

MAC address 06dd.c8b9.e9cc hits 1 reference 1

<-- next hop MAC address

Phase: 17
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 8296 ns
Config:
Additional Information:
MAC Access list

Result:

input-interface: inside(vrfid:0)

```
input-status: up
input-line-status: up
```

output-interface: nlp_int_tap(vrfid:0)

```
output-status: up
output-line-status: up
Action: allow
Time Taken: 191292 ns
```

3. Capture point – the packet with the destination IP **169.254.1.2** port **22** is sent out the **nlp_int_tap** interface:

<#root>

```
firewall#
```

show capture nlp

```
1 packets captured
   1: 19:52:27.776998
```

192.0.2.2.22420 > 169.254.1.2.22

```
: S 1456431278:1456431278(0) win 8192
```

4. Capture point – the packet with the destination IP **169.254.1.2** port **22** is received on the OS **tap_nlp** interface:

<#root>

```
admin@firewall:~$
```

sudo tcpdump -n -i tap_nlp tcp

```
Password:
HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tap_nlp, link-type EN10MB (Ethernet), capture size 262144 bytes
```

19:52:27.796029 IP 192.0.2.2.22420 > 169.254.1.2.22: Flags [S], seq 1456431278, win 8192, length 0

5. The SSH daemon listens on port **22**, receives the SYN packet and handles it:

<#root>

admin@firewall:~$

sudo netstat -pan | grep :22

Password:

tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 6026/sshd: /usr/sbi

tcp6 0 0 :::22 :::* LISTEN 6026/sshd: /usr/sbi

6.The SSH generates a SYN ACK packet.

7.Capture point – the SYN ACK packet with the source IP **169.254.1.2** port **22** and destination IP **192.0.2.2** is sent out the **tap_nlp** interface:

<#root>

admin@firewall:~$

sudo tcpdump -n -i tap_nlp tcp

Password:
HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tap_nlp, link-type EN10MB (Ethernet), capture size 262144 bytes
19:52:27.796029 IP 192.0.2.2.22420 > 169.254.1.2.22: Flags [S], seq 1456431278, win 8192, length 0

19:52:27.796112 IP 169.254.1.2.22 > 192.0.2.2.22420: Flags [S.], seq 2122129677, ack 1456431279, win 642

8. Capture point – the SYN ACK packet with the source IP **169.254.1.2** port **22** and destination IP address **192.0.2.2** is received on the Lina **nlp_int_tap** interface:

<#root>

firewall#

show capture nlp

```
2 packets captured

   1: 19:52:27.776998       192.0.2.2.22420 > 169.254.1.2.22: S 1456431278:1456431278(0) win 8192

   2: 19:52:27.777776       169.254.1.2.22 > 192.0.2.2.22420: S 2122129677:2122129677(0) ack 1456431279
```

9. This SYN ACK packet is handled as part of the existing/established connection based on which the Lina engine applies the reverse NAT rule to translate the source of the packet from IP **169.254.1.2** to the inside IP **192.0.2.1** and selects inside as the egress interface. In the case of SSH connection to the ASA with the Cisco SSH stack, the source port is translated from **4122** back to **22:**

<#root>

```
firewall#

show capture nlp trace packet-number 2


2 packets captured
   1: 19:52:27.776998       192.0.2.2.22420 > 169.254.1.2.22: S 1456431278:1456431278(0) win 8192

   2: 19:52:27.777776       169.254.1.2.22 > 192.0.2.2.22420: S 2122129677:2122129677(0) ack 1456431279



Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 2196 ns
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 2196 ns
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Elapsed time: 2928 ns
Config:
Additional Information:

Found flow with id 239305, using existing flow
```

Phase: 4
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Elapsed time: 10736 ns
Config:
Additional Information:

Found next-hop 192.0.2.2 using egress ifc inside(vrfid:0)

Phase: 5
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Elapsed time: 1952 ns
Config:
Additional Information:

Found adjacency entry for Next-hop 192.0.2.2 on interface inside

Adjacency :Active

MAC address 0000.0000.1234 hits 0 reference 1

Phase: 6
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 10736 ns
Config:
Additional Information:
MAC Access list

Result:

input-interface: nlp_int_tap(vrfid:0)

input-status: up
input-line-status: up

output-interface: inside(vrfid:0)

output-status: up
output-line-status: up
Action: allow

```
Time Taken: 30744 ns
```

10. Capture point – the packet leaves the **inside** interface toward the destination:

```
<#root>
firewall#
show capture capi

2 packets captured
   1: 19:52:27.776830       192.0.2.2.22420 > 192.0.2.1.22: S 240217016:240217016(0) win 8192
   2: 19:52:27.777807       192.0.2.1.22 > 192.0.2.2.22420: S 2835714564:2835714564(0) ack 240217017 wir
```

Management over data Interface is Enabled

If management over data Interface is enabled at FMC-managed FTD these changes automatically take place:

1. On CLISH, the default gateway is the **data-interface**. The OS-level default gateway is via **tap_nlp** with the next hop pointing to the Lina IP **169.254.1.1:**

```
<#root>
>
show network management-data-interface

Physical Interface              Name of the Interface
Ethernet1/2             inside

>
show network

===============[ System Information ]===============
Hostname                  : FPR1150-2
DNS from router           : enabled
Management port           : 8305
```

IPv4 Default route

** Gateway   : data-interfaces**

```
==================[ management0 ]===================
Admin State               : enabled
Admin Speed               : 1gbps
Operation Speed           : 1gbps
Link                      : up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 4C:E1:75:DD:89:00

----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 192.0.2.29
Netmask                   : 255.255.255.0
----------------------[ IPv6 ]----------------------
Configuration             : Disabled

===============[ Proxy Information ]================
State                     : Disabled
Authentication            : Disabled
```

======[System Information - Data Interfaces]======

DNS Servers   :

Interfaces   : Ethernet1/2

==================[Ethernet1/2]===================

State   : Enabled

Link   : Up

```
Name                    : inside

MTU                     : 1500

MAC Address             : 4C:E1:75:DD:89:25

----------------------[ IPv4 ]----------------------

Configuration           : Manual

Address                 : 198.51.100.254

Netmask                 : 255.255.255.0

Gateway                 : 198.51.100.1

----------------------[ IPv6 ]----------------------
Configuration           : Disabled

admin@firewall:~$

ip route show default

default via 169.254.1.1 dev tap_nlp
```

2. On Lina typically there is a default route configured via the data interface – this is user configuration deployed from FMC:

```
<#root>

firewall#

show route
```

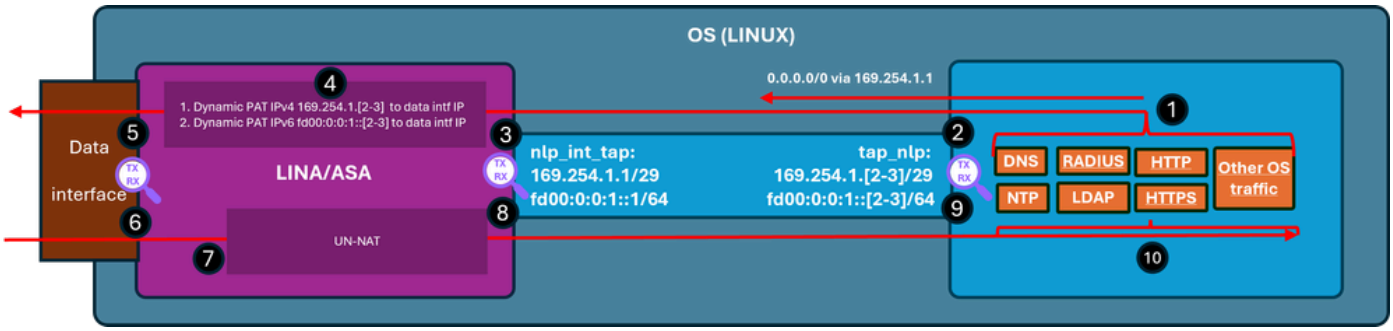
```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 198.51.100.1 to network 0.0.0.0


S*       0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, inside


C        198.51.100.0 255.255.255.0 is directly connected, inside

L        198.51.100.254 255.255.255.255 is directly connected, inside
```

3. On Lina manual twice NAT rules for sftunnel port 8305 are installed for both IPv4 and IPv6 stacks. Additionally, to allow connectivity from OS to external networks a dynamic PAT for the IPv4 and IPv6 addresses of the OS **tap_nlp** interface is configured over the data interface.

```
<#root>

firewall#

show nat detail


Manual NAT Policies Implicit (Section 0)
1 (nlp_int_tap) to (inside) source static nlp_server__sftunnel_0.0.0.0_intf3 interface  destination sta
    translate_hits = 6, untranslate_hits = 6

    Source - Origin: 169.254.1.3/32, Translated: 198.51.100.254/24



    Destination - Origin: 0.0.0.0/0, Translated: 0.0.0.0/0



    Service - Protocol: tcp Real: 8305 Mapped: 8305



2 (nlp_int_tap) to (inside) source static nlp_server__sftunnel_::_intf3 interface ipv6  destination sta
    translate_hits = 0, untranslate_hits = 0

    Source - Origin: fd00:0:0:1::3/128, Translated:
```

```
    Destination - Origin: ::/0, Translated: ::/0


    Service - Protocol: tcp Real: 8305 Mapped: 8305


3 (nlp_int_tap) to (inside) source dynamic nlp_client_0_intf3 interface
    translate_hits = 64, untranslate_hits = 0

    Source - Origin: 169.254.1.3/32, Translated: 198.51.100.254/24

<-- Dynamic IPv4 PAT on inside interface

4 (nlp_int_tap) to (inside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
    translate_hits = 0, untranslate_hits = 0

    Source - Origin: fd00:0:0:1::3/128, Translated:

<-- Dynamic IPv6 PAT on inside interface
```

This diagram shows the packet path and capture points:



Verification steps (In this example, the verification steps are for NTP traffic. Same logic applies to any OS-generate traffic including licensing etc):

1. NTP client generates a packet destined for an external NTP server IP address:

<#root>

```
admin@firewall:~$

sudo ntpq -pn
```

```
Password:
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*192.0.2.222  192.0.2.111    2 u   31   64  377   27.540   +0.104   0.105

 127.127.1.1     .LOCL.          10 l 1093   64    0    0.000   +0.000   0.000
```

From OS perspective the next hop is via the **tap_nlp** interface using the same interface IP **169.254.1.3** as the source address:

```
<#root>

admin@firewall:~$

ip route get 192.0.2.222



192.0.2.222 via 169.254.1.1 dev tap_nlp src 169.254.1.3 uid 101


    cache
```

2. Capture point – the packet is sent out the **tap_nlp** interface:

```
<#root>

admin@firewall:~$

sudo tcpdump -n -i tap_nlp udp and port 123


HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tap_nlp, link-type EN10MB (Ethernet), capture size 262144 bytes
22:39:59.728791 IP

169.254.1.3.123 > 192.0.2.222.123

: NTPv4, Client, length 48
```

3. Capture point – the packet arrives on the Lina **nlp_tap_interface** interface:

```
<#root>
```

```
firewall#

show capture



capture nlp type raw-data trace interface nlp_int_tap

 [Capturing - 10600 bytes]


match udp any any eq ntp



firewall#

show capture nlp


96 packets captured
   3: 22:39:59.726112

169.254.1.3.123 > 192.0.2.222.123

:  udp 48
```

4. Based on the route lookup Lina identifies the inside as the egress interface and then applies a dynamic PAT rule that changes the packet source IP address from **169.254.1.3** to data interface IP address:

```
<#root>
firewall#

show capture nlp trace packet-number 3


96 packets captured


   3: 22:39:59.726112       169.254.1.3.123 > 192.0.2.222.123:  udp 48



Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 4608 ns
Config:
Additional Information:
MAC Access list
```

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 4608 ns
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: INPUT-ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Elapsed time: 24576 ns
Config:
Additional Information:

Found next-hop 198.51.100.1 using egress ifc inside(vrfid:0)

…
Phase: 6
Type: NAT
Subtype:
Result: ALLOW
Elapsed time: 853 ns
Config:

nat (nlp_int_tap,inside) source dynamic nlp_client_0_intf3 interface

Additional Information:

Dynamic translate 169.254.1.3/123 to 198.51.100.254/58840

…
Phase: 13
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Elapsed time: 8192 ns
Config:
Additional Information:

Found next-hop 198.51.100.1 using egress ifc inside(vrfid:0)

Phase: 14
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Elapsed time: 3072 ns

Config:
Additional Information:

Found adjacency entry for Next-hop 198.51.100.1 on interface inside

Adjacency :Active

MAC address c02c.1782.2cbf hits 5 reference 3

Phase: 15
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 11264 ns
Config:
Additional Information:
MAC Access list

Result:

input-interface: nlp_int_tap(vrfid:0)

input-status: up
input-line-status: up

output-interface: inside(vrfid:0)

output-status: up
output-line-status: up
Action: allow
Time Taken: 173567 ns

firewall#

show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF, BI - BGP InterVRF
Gateway of last resort is 198.51.100.1 to network 0.0.0.0

S*   0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, inside

```
C        198.51.100.0 255.255.255.0 is directly connected, inside
L        198.51.100.254 255.255.255.255 is directly connected, inside
```

5. Capture point – the packet is sent out via the egress interface:

<#root>

```
firewall#
```

show capture capi

```
112 packets captured
```

1: 22:39:59.726387 198.51.100.254.58840 > 192.0.2.222.123: udp 48

6. Capture point - NTP server sends a reply packet:

<#root>

```
firewall#
```

show capture capi

```
112 packets captured
   1: 22:39:59.726387       198.51.100.254.58840 > 192.0.2.222.123:  udp 48
```

2: 22:39:59.756796 192.0.2.222.123 > 198.51.100.254.58840: udp 48

7. Lina handles the reply as part of established connections and applies reverse NAT. Based on this information, the destination is translated to **169.254.1.3**, the egress interface is **nlp_int_tap**:

<#root>

```
firewall#
```

show capture capi trace packet-number 2

```
120 packets captured
```

2: 22:39:59.756796 192.0.2.222.123 > 198.51.100.254.58840: udp 48

…

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Elapsed time: 6144 ns
Config:
Additional Information:

Found flow with id 1226, using existing flow

Phase: 4
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Elapsed time: 11264 ns
Config:
Additional Information:

Found next-hop 169.254.1.3 using egress ifc nlp_int_tap(vrfid:0)

Phase: 5
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Elapsed time: 3072 ns
Config:
Additional Information:

Found adjacency entry for Next-hop 169.254.1.3 on interface nlp_int_tap

Adjacency :Active

MAC address 9641.fdd8.1038 hits 4159 reference 4

Phase: 6
Type: CAPTURE
Subtype:
Result: ALLOW
Elapsed time: 17920 ns
Config:
Additional Information:
MAC Access list

Result:

input-interface: inside(vrfid:0)

```
input-status: up
input-line-status: up

output-interface: nlp_int_tap(vrfid:0)


output-status: up
output-line-status: up
Action: allow
Time Taken: 47104 nsw
```

8. Capture point – the reply packet is sent out **nlp_int_tap** interface:

```
<#root>

firewall#

show capture nlp


132 packets captured

   3: 22:39:59.726112       169.254.1.3.123 > 192.0.2.222.123:  udp 48

   4: 22:39:59.756903       192.0.2.222.123 > 169.254.1.3.123:  udp 48
```

9. Capture point – the replay packet arrives on OS **tap_nlp** interface:

```
<#root>

admin@firewall:~$

sudo tcpdump -n -i tap_nlp udp and port 123


HS_PACKET_BUFFER_SIZE is set to 4.
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on tap_nlp, link-type EN10MB (Ethernet), capture size 262144 bytes
22:39:59.728791 IP 169.254.1.3.123 > 192.0.2.222.123: NTPv4, Client, length 48

22:39:59.759683 IP 192.0.2.222.123 > 169.254.1.3.123: NTPv4, Server, length 48
```

10. The reply packet is consumed and handled by NTP client.

Summary

The OS /**dev/net/tun/tap_nlp** interface is visible as **nlp_int_tap** in Lina. The purpose of this interface is to provide connectivity between Lina and the OS. This interface along with required NAT rules is automatically managed by the software and requires no user intervention.

References

- **Secure Firewall Configuration Guides**