Clarifiez l'objectif de l'interface de données internes avec nameif nlp_int_tap et l'adresse IP 169.254.1.1

Table des matières

Introduction

Ce document décrit l'objectif de l'interface nlp_int_tap Données internes avec l'adresse IP 169.254.1.1.

Conditions préalables

Exigences

Connaissances de base sur les produits.

Composants utilisés

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Secure Firewall Threat Defense (FTD) 7.x, 10.x géré par Secure Firewall Device Manager (FDM) ou Secure Firewall Management Center (FMC).
- Sécurisez ASA 9.18 et versions ultérieures.

Informations générales

L'interface Internal-Data avec le nom if nlp_int_tap et l'adresse IP 169.254.1.1 est une interface interne qui est utilisée pour fournir la connectivité entre le moteur de plan de données appelé Lina et le système d'exploitation (OS) principal.

Il est utilisé pour fournir une connectivité générale pour ces services :

- SNMP : le démon SNMP s'exécute en tant que processus distinct dans le système d'exploitation.
- Accès SSH à ASA avec la pile Cisco SSH : le démon SSH s'exécute en tant que processus distinct dans le système d'exploitation.
- Accès SSH à FTD sur l'interface de données - le démon SSH s'exécute comme un processus distinct dans OS.
- Authentification externe compatible VRF sur FTD : l'accès aux serveurs d'authentification externes est fourni via une interface de données dans un VRF global ou utilisateur.
- En cas de gestion FTD sur des interfaces de données, accès à des services de gestion tels que sftunnel, résolution DNS, gestion des licences, authentification externe, NTP ou toute destination vers laquelle le système d'exploitation n'a pas explicitement configuré les routes statiques sur l'interface de gestion.

Vérification Lina

Selon la plate-forme, dans le moteur Lina, le nom nlp_int_tap est attribué à l'interface Internal-DataX/Y et est visible dans différentes sorties de commande.

Voici les résultats de différents pare-feu :

- Pare-feu sécurisé 6170 exécutant 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 exécutant 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

…
```

- FTD virtuel :

```
<#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

…

- ASA virtuel :

<#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

…

Principaux points :

- Le nom if nlp_int_tap est attribué à différentes interfaces Internal-Data sur différentes plates-formes.
- Selon le résultat de la commande show asp table routing, l'interface Internal-Data avec le nom nlp_int_tap est affectée à l'adresse IPv4 169.254.1.1/29 et à l'adresse IPv6 fd00:0:0:1::1/64.
- Selon le résultat de la commande show controller, cette interface est une interface Linux Tun/Tap (en particulier tap) disponible dans /dev/net/tun/tap_nlp.

Vérification du système d'exploitation

/dev/net/tun/tap_nlp est une interface de tap Linux avec ces adresses IP :

- IPV4: 169.254.1.2/29 sur les périphériques virtuels et 169.254.1.3/29 sur les périphériques matériels.
- IPV6 : fd00:0:0:1::2/64 sur les périphériques virtuels et fd00:0:0:1::3/64 sur les périphériques matériels.

Vérification dans les périphériques FTD virtuels et matériels :

- FTD virtuel :

<#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
```

Pour rétablir la connectivité avec la liaison LAN, le système d'exploitation installe une règle de routage pour la recherche dans la table de routage des paquets avec les adresses IP source de l'interface tap_nlp :

<#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)
```

Principaux points :

- Les règles de routage IPv4 et IPv6 stipulent que la recherche de route pour les paquets provenant des adresses d'interface nlp_tap est effectuée dans la table de routage 1.
- Les versions IPv4 et IPv6 de la table de routage 1 contiennent une route par défaut avec l'adresse de tronçon suivant qui appartient à l'interface Lina nlp_int_tap.

Chemin des paquets et points de capture

Cette section présente le chemin des paquets et les points de capture dans 2 cas différents :

- La gestion sur interface de données est désactivée.
- La gestion sur l'interface de données est activée.

Remarque : Il existe un scénario supplémentaire avec la fonctionnalité « Use the Data Interfaces as the Gateway » sur FDM. Du point de vue du routage, de la configuration et de la capture de paquets, ce scénario est similaire au FTD géré par FMC avec gestion sur interface de données.

La gestion sur l'interface de données est désactivée

Cette section décrit la vérification du chemin des paquets et des points de capture sur FTD avec les détails de configuration suivants :

1. FTD est géré par FMC.
2. Pas de gestion sur interface de données. Cela signifie que l'interface de gestion est utilisée pour assurer la connectivité entre le système d'exploitation et le réseau externe :

<#root>

>

show network management-data-interface

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

3. Au moins une de ces fonctions est configurée :

- SNMP sur ASA ou FTD.
- Accès SSH à ASA avec la pile SSH de Cisco. Dans ASA versions 9.23 et ultérieures, la pile Cisco SSH est activée et ne peut pas être désactivée.
- Accès SSH à FTD sur des interfaces de données.
- Accès HTTPS sur interface de données sur FTD géré par FDM.

4. Les captures de paquets sont configurées dans tous les points de capture.

Si l'une des fonctions mentionnées précédemment est configurée, les deux règles NAT manuelles sont automatiquement configurées. Selon les ports/protocoles de la fonctionnalité, les règles NAT sont différentes.

Voici un exemple de sortie avec deux règles NAT manuelles pour l'accès FTD SSH sur l'interface de données :

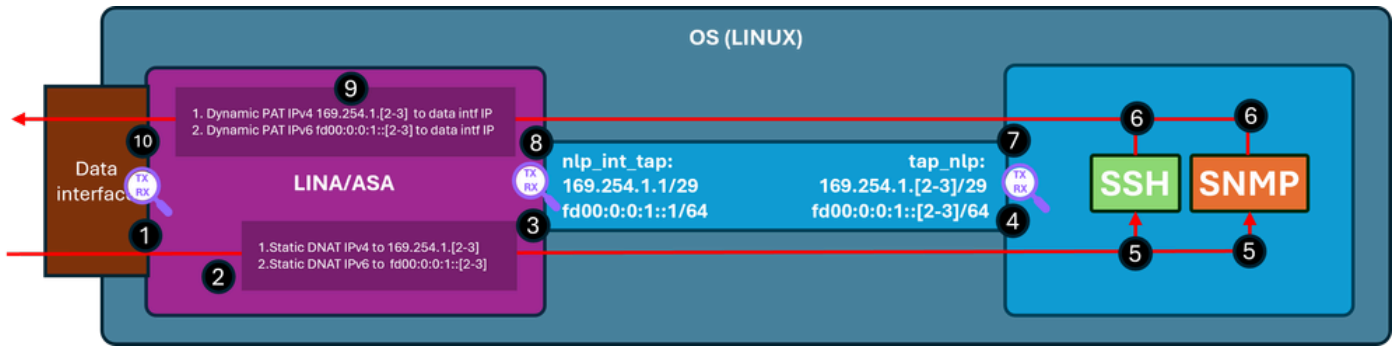
<#root>

```
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
```

Remarque : Dans le cas d'une connexion SSH à l'ASA avec la pile SSH de Cisco, le port de destination est traduit de 22 à 4122.

Ce schéma montre le chemin des paquets et les points de capture :



Étapes de vérification (applicables aux fonctions mentionnées précédemment) :

1. Point de capture : paquet SYN TCP entrant pour SSH de l'adresse IP 192.0.2.2 à l'adresse IP 192.0.2.1 sur le port 22. IP 192.0.2.1 est l'adresse de l'interface interne :

<#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 indique une règle NAT correspondante qui traduit l'adresse IP de destination de 192.0.2.1 à l'adresse IP 169.254.1.2, et détourne les paquets vers l'interface de sortie nlp_int_tap :

<#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. Point de capture : le paquet avec le port 22 de l’adresse IP de destination 169.254.1.2 est

envoyé par l'interface nlp_int_tap :

<#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. Point de capture : le paquet avec le port 22 de l'adresse IP de destination 169.254.1.2 est reçu sur l'interface tap_nlp du système d'exploitation :

<#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. Le démon SSH écoute le port 22, reçoit le paquet SYN et le traite :

<#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.Le SSH génère un paquet SYN ACK.

7.Point de capture : le paquet SYN ACK avec l'adresse IP source 169.254.1.2, le port 22 et l'adresse IP de destination 192.0.2.2 est envoyé à l'interface tap_nlp :

<#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. Point de capture : le paquet SYN ACK avec l’adresse IP source 169.254.1.2, le port 22 et l’adresse IP de destination 192.0.2.2 est reçu sur l’interface Lina nlp_int_tap :

<#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. Ce paquet SYN ACK est traité dans le cadre de la connexion existante/établie sur la base de

laquelle le moteur Lina applique la règle NAT inverse pour traduire la source du paquet de l'adresse IP 169.254.1.2 à l'adresse IP interne 192.0.2.1 et sélectionne l'adresse IP interne comme interface de sortie. Dans le cas d'une connexion SSH à l'ASA avec la pile SSH de Cisco, le port source est traduit de 4122 en 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. Point de capture : le paquet quitte l'interface interne vers la 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
```

La gestion sur l'interface de données est activée

Si la gestion sur l'interface de données est activée au niveau du FTD géré par FMC, ces modifications ont lieu automatiquement :

1. Sur CLISH, la passerelle par défaut est l'interface de données. La passerelle par défaut au niveau du système d'exploitation est via tap_nlp avec le saut suivant pointant vers l'IP Lina 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. Sur Lina, une route par défaut est généralement configurée via l'interface de données. Il s'agit d'une configuration utilisateur déployée à partir de 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. Sur le manuel Lina, deux règles NAT pour le port sftunnel 8305 sont installées pour les piles IPv4 et IPv6. En outre, pour permettre la connectivité du système d'exploitation aux réseaux externes, une PAT dynamique pour les adresses IPv4 et IPv6 de l'interface OS tap_nlp est configurée sur l'interface de données.

<#root>

firewall#

show nat detail

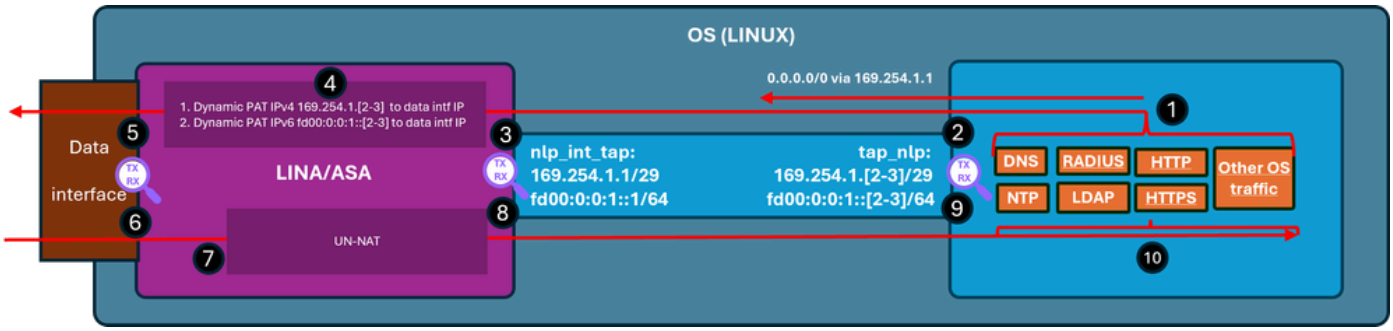
Manual NAT Policies Implicit (Section 0)
1 (nlp_int_tap) to (inside) source static nlp_server__sftunnel_0.0.0.0_intf3 interface destination sta
    translate_hits = 6, untranslate_hits = 6

    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
```

Ce schéma montre le chemin des paquets et les points de capture :



Étapes de vérification (dans cet exemple, les étapes de vérification concernent le trafic NTP. La même logique s'applique à tout trafic généré par le système d'exploitation (licence, etc.) :

1. Le client NTP génère un paquet destiné à une adresse IP de serveur NTP externe :

<#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
```

Du point de vue du système d'exploitation, le saut suivant se fait via l'interface tap_nlp en utilisant la même interface IP 169.254.1.3 que l'adresse source :

<#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. Point de capture : le paquet est envoyé par l'interface tap_nlp :

<#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. Point de capture : le paquet arrive sur l'interface Lina nlp_tap_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. En fonction de la recherche de route, Lina identifie l'intérieur comme l'interface de sortie, puis applique une règle PAT dynamique qui modifie l'adresse IP source du paquet de 169.254.1.3 en adresse IP de l'interface de données :

<#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. Point de capture : le paquet est envoyé via l'interface de sortie :

```
<#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. Point de capture : le serveur NTP envoie un paquet de réponse :

```
<#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 gère la réponse dans le cadre des connexions établies et applique la NAT inverse. Sur

la base de ces informations, la destination est traduite en 169.254.1.3, l'interface de sortie est 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. Point de capture : le paquet de réponse est envoyé via l'interface nlp_int_tap :

<#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. Point de capture : le paquet de relecture arrive sur l'interface tap_nlp du système d'exploitation :

<#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. Le paquet de réponse est consommé et géré par le client NTP.

Résumé

L'interface OS /dev/net/tun/tap_nlp est visible sous la forme nlp_int_tap dans Lina. L'objectif de cette interface est de fournir la connectivité entre Lina et le système d'exploitation. Cette interface ainsi que les règles NAT requises sont automatiquement gérées par le logiciel et ne nécessitent aucune intervention de l'utilisateur.

Références

- Guides de configuration du pare-feu sécurisé

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.