Verduidelijk het doel van de interface voor interne gegevens met de naam nlp_int_tap en IP-adres 169.254.1.1

Inhoud

Inleiding

Dit document beschrijft het doel van de Internal-Data nlp_int_tap-interface met het IP-adres 169.254.1.1.

Voorwaarden

Vereisten

Basisproductkennis.

Gebruikte componenten

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Secure Firewall Threat Defense (FTD) 7.x, 10.x wordt beheerd door de Secure Firewall Device Manager (FDM) of het Secure Firewall Management Center (FMC).
- Beveilig ASA 9.18 en hoger.

Achtergrondinformatie

De Internal-Data interface met de naam nlp_int_tap en het IP-adres 169.254.1.1 is een interne interface die wordt gebruikt om connectiviteit te bieden tussen de dataplane-engine genaamd Lina en het backend-besturingssysteem (OS).

Het wordt gebruikt om algemene connectiviteit te bieden voor deze diensten:

- SNMP – De SNMP-daemon wordt als een apart proces in het besturingssysteem uitgevoerd.
- SSH-toegang tot ASA met de Cisco SSH-stack – de SSH-daemon wordt als een afzonderlijk proces in OS uitgevoerd.
- SSH toegang tot FTD via data-interface – de SSH daemon draait als een apart proces in OS.
- Externe verificatie met VRF op FTD – toegang tot externe verificatieservers wordt geboden via een data-interface in een globale of gebruikersvriendelijke VRF.
- In het geval van FTD-beheer via data-interfaces, toegang tot beheerdiensten zoals sftunnel, DNS-resolutie, licenties, externe verificatie, NTP of bestemmingen waarvoor het besturingssysteem geen expliciet geconfigureerde statische routes over de beheerinterface heeft.

Lina Verification

Afhankelijk van het platform wordt in de Lina-engine de naam nlp_int_tap toegewezen aan de interface Internal-DataX/Y en is deze zichtbaar in verschillende opdrachtuitgangen.

Dit zijn uitgangen van verschillende firewalls:

- Secure Firewall 6170 met 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 met 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

…

- Virtuele 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

…

Belangrijkste punten:

- De naam nlp_int_tap wordt toegewezen aan verschillende Internal-Data interfaces op verschillende platforms.
- Volgens de show asp tabel routing opdracht uitvoer, de Internal-Data interface met de naam nlp_int_tap is toegewezen IPv4-adres 169.254.1.1/29 en IPv6-adres fd00:0:0:1::1/64.
- Volgens de show controller command output is deze interface een Linux Tun/Tap interface (specifiek tap) beschikbaar in /dev/net/tun/tap_nlp.

Verificatie van besturingssysteem

/dev/net/tun/tap_nlp is een Linux-tapinterface met deze IP-adressen:

- IPV4: 169.254.1.2/29 op virtuele apparaten en 169.254.1.3/29 op hardwareapparaten.
- IPV6: fd00:0:0:1:2/64 op virtuele apparaten en fd00:0:0:1:3/64 op hardwareapparaten.

Verificatie in virtuele hardware en FTD-apparaten:

- Virtuele 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
```

- Beveiligde 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
```

Om connectiviteit terug te bieden aan de Lina installeert het OS een routeringsregel voor het opzoeken van pakketten in de routeringstabel met de bron-IP-adressen van de 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)
```

Belangrijkste punten:

- IPv4- en IPv6-routeringsregels schrijven voor dat het opzoeken van routes voor pakketten afkomstig van de nlp_tap-interfaceadressen wordt uitgevoerd in routeringstabel 1.
- IPv4- en IPv6-versies van routeringstabel 1 bevatten standaardroute met het volgende hopadres dat behoort tot de Lina nlp_int_tap-interface.

Pakketpad en vastlegpunten

In dit gedeelte worden het pakketpad en de opnamepunten in 2 verschillende gevallen weergegeven:

- Beheer via de gegevensinterface is uitgeschakeld.
- Beheer via data-interface is ingeschakeld.

Opmerking: Er is een extra scenario met de functie "Gebruik de gegevensinfrastructuur als gateway" op FDM. Vanuit het perspectief van routering, configuratie en pakketregistratiepunt is dit scenario vergelijkbaar met de door de FMC beheerde FTD met beheer via data-interface.

Beheer via gegevensinterface is uitgeschakeld

In dit gedeelte wordt de verificatie van pakketpaden en opnamepunten op FTD beschreven met de volgende configuratiedetails:

1. FTD wordt beheerd door FMC.
2. Geen beheer via data-interface. Dit betekent dat de beheerinterface wordt gebruikt om connectiviteit te bieden tussen het besturingssysteem en het externe netwerk:

```
<#root>

>

show network management-data-interface


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

3. Ten minste één van deze functies is geconfigureerd:

- SNMP op ASA of FTD.
- SSH toegang tot ASA met de Cisco SSH stack. In ASA-versies 9.23 en hoger is de Cisco SSH-stack ingeschakeld en kan deze niet worden uitgeschakeld.
- SSH-toegang tot FTD via data-interfaces.
- HTTPS-toegang via data-interface op FDM-beheerde FTD.

4. Packet captures worden geconfigureerd in alle opnamepunten.

Als een van de eerder genoemde functies is geconfigureerd, worden automatisch twee handmatige NAT-regels geconfigureerd. Afhankelijk van de functiepoorten/protocollen zijn de NAT-regels anders.

Dit is een voorbeelduitvoer met twee handmatige NAT-regels voor FTD SSH-toegang via de data-interface:

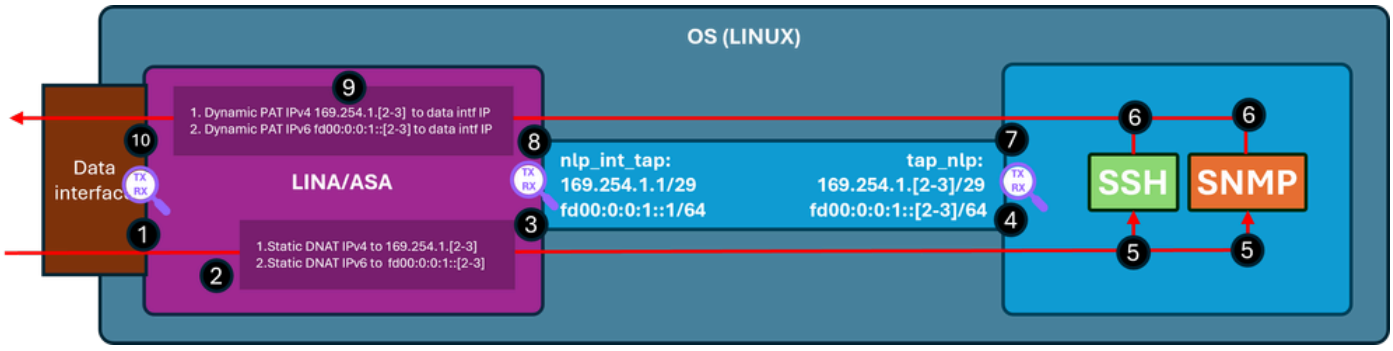
<#root>

```
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
```

Opmerking: In het geval van SSH-verbinding met de ASA met de Cisco SSH-stack wordt de bestemmingspoort vertaald van 22 naar 4122.

Dit diagram toont het pakketpad en de opnamepunten:



Verificatiestappen (van toepassing op eerder genoemde functies):

1. Opnamepunt – TCP SYN-pakket voor SSH binnendringen van IP 192.0.2.2 tot IP 192.0.2.1 op poort 22. IP 192.0.2.1 is het adres van de interne 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. Opnametracering geeft een overeenkomende NAT-regel aan die het IP-doel van 192.0.2.1 naar IP 169.254.1.2 vertaalt en pakketten naar de nlp_int_tap-uitgang-interface leidt:

<#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. Opnamepunt – het pakket met de bestemming IP 169.254.1.2-poort 22 wordt verzonden via de 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. Opnamepunt – het pakket met de bestemming IP 169.254.1.2-poort 22 wordt ontvangen op de 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. De SSH-daemon luistert op poort 22, ontvangt het SYN-pakket en behandelt het:

<#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. De SSH genereert een SYN ACK-pakket.

7.Opnamepunt – het SYN ACK-pakket met de bron IP 169.254.1.2-poort 22 en bestemming IP 192.0.2.2 wordt verzonden via de 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. Opnamepunt – het SYN ACK-pakket met het IP 169.254.1.2-poort 22 en het IP-adres van de bestemming 192.0.2.2 wordt ontvangen op de 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. Dit SYN ACK-pakket wordt behandeld als onderdeel van de bestaande/gevestigde verbinding op basis waarvan de Lina-engine de reverse NAT-regel toepast om de bron van het pakket te vertalen van IP 169.254.1.2 naar de binnenkant van IP 192.0.2.1 en selecteert binnenkant als de uitgang-interface. In het geval van SSH-verbinding met de ASA met de Cisco SSH-stack wordt de bronpoort vertaald van 4122 terug naar 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. Opnamepunt – het pakket verlaat de interne interface naar de bestemming:

<#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
```

Beheer via gegevensinterface is ingeschakeld

Als beheer via data-interface is ingeschakeld bij FTD die door het FMC wordt beheerd, vinden deze wijzigingen automatisch plaats:

1. Op CLISH is de standaardgateway de data-interface. De standaardgateway op OS-niveau is via tap_nlp met de volgende hop die naar de Lina IP 169.254.1.1 wijst:

```
<#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. Op Lina is er meestal een standaardroute geconfigureerd via de data-interface - dit is de gebruikersconfiguratie die wordt geïmplementeerd vanuit 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
```

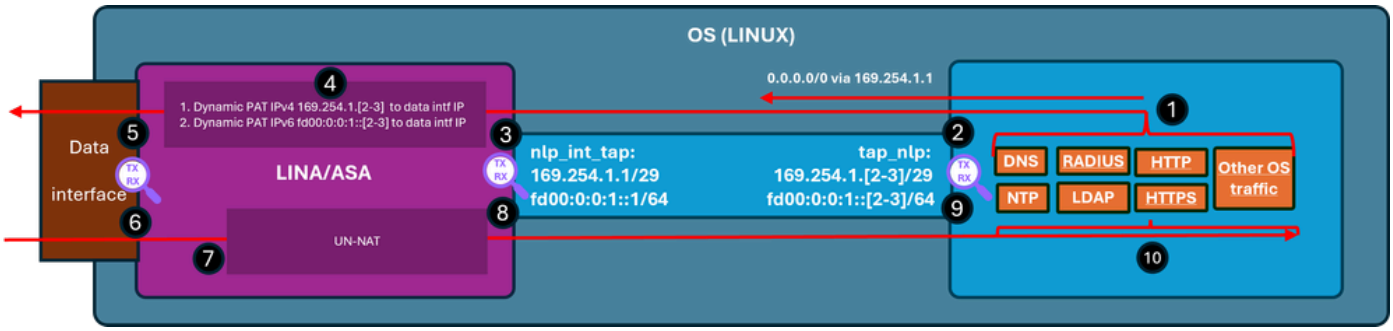
3. Op Lina handleiding tweemaal NAT regels voor sftunnel poort 8305 zijn geïnstalleerd voor zowel IPv4 en IPv6 stacks. Om connectiviteit van het besturingssysteem naar externe netwerken mogelijk te maken, wordt bovendien een dynamische PAT voor de IPv4- en IPv6-adressen van de tap_nlp-interface van het besturingssysteem geconfigureerd via de 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
```

Dit diagram toont het pakketpad en de opnamepunten:



Verificatiestappen (In dit voorbeeld zijn de verificatiestappen voor NTP-verkeer. Dezelfde logica is van toepassing op elk OS-gegenereerd verkeer (inclusief licenties enz.):

1. NTP-client genereert een pakket dat is bestemd voor een extern IP-adres van de NTP-server:

```
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
```

Vanuit het perspectief van het besturingssysteem is de volgende hop via de tap_nlp-interface met dezelfde interface IP 169.254.1.3 als het bronadres:

<#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. Opnamepunt – het pakket wordt verzonden via de 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. Opnamepunt – het pakket arriveert op de 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. Op basis van het opzoeken van de route identificeert Lina de binnenkant als de uitgang-interface en past vervolgens een dynamische PAT-regel toe die het IP-adres van de pakketbron verandert van 169.254.1.3 naar het IP-adres van de gegevensinterface:

```
<#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. Opnamepunt – het pakket wordt verzonden via de uitgang-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. Opnamepunt - NTP-server verzendt een antwoordpakket:

```
<#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 behandelt het antwoord als onderdeel van gevestigde verbindingen en past reverse NAT toe. Op basis van deze informatie wordt de bestemming vertaald naar 169.254.1.3, de uitgang-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. Opnamepunt – het antwoordpakket wordt verzonden via de 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. Opnamepunt – het replay-pakket wordt geleverd via de tap_nlp-interface van OS:

<#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. Het antwoordpakket wordt geconsumeerd en verwerkt door NTP-client.

Samenvatting

De interface OS /dev/net/tun/tap_nlp is zichtbaar als nlp_int_tap in Lina. Het doel van deze interface is om connectiviteit te bieden tussen Lina en het besturingssysteem. Deze interface samen met de vereiste NAT-regels wordt automatisch beheerd door de software en vereist geen tussenkomst van de gebruiker.

Referenties

- Configuratiehandleidingen voor veilige firewall

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.