使用nameif nlp_int_tap和IP地址169.254.1.1闡明內部資料介面的用途

目錄

簡介

本檔案介紹IP位址為169.254.1.1的內部資料nlp_int_tap介面的用途。

必要條件

需求

基本產品知識。

採用元件

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

本文中的資訊係根據以下軟體和硬體版本：

- 安全防火牆威脅防禦(FTD)7.x、10.x，由安全防火牆裝置管理器(FDM)或安全防火牆管理中心(FMC)管理。
- 安全ASA 9.18及更高版本。

背景資訊

名為nlp_int_tap和169.254.1.1 IP地址的內部資料介面是一個內部介面，用於提供名為Lina的資料平面引擎與後端作業系統(OS)之間的連線。

它用於為以下服務提供一般連線：

- SNMP - SNMP守護程式作為單獨的進程在作業系統中運行。
- 通過Cisco SSH堆疊對ASA進行SSH訪問 — SSH守護程式作為單獨的進程在作業系統中運行。
- 通過資料介面通過SSH訪問FTD - SSH守護程式作為單獨的進程在作業系統中運行。
- FTD上的VRF感知外部驗證 — 透過全域或使用者VRF中的資料介面提供對外部驗證伺服器的存取許可權。
- 在資料介面上進行FTD管理時，請訪問管理服務，例如sftunnel、DNS解析、許可、外部身份驗證、NTP，或者作業系統未通過管理介面明確配置靜態路由的任何目標。

Lina驗證

視平台而定，在Lina引擎中，nameif nlp_int_tap 會指派給Internal-DataX/Y介面，且可在不同的指令輸出中看到。

以下是來自不同防火牆的輸出：

- 執行FTD的安全防火牆6170:

```
<#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
…
```

- 運行ASA的Firepower 4145:

<#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

…

- 虚擬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

…

- 虛擬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

…

重點：

- nameif nlp_int_tap 被分配給不同平台上的不同內部資料介面。
- 根據show asp table routing 命令輸出，為名為nlp_int_tap 的內部資料介面分配IPv4地址

169.254.1.1/29和IPv6地址fd00:0:1::1/64。
- 根據show controller 命令輸出，此介面是/dev/net/tap_nlp中可用的Linux Tun/Tap介面（特別是分路器）。

作業系統驗證

/dev/net/tap/tap_nlp是具有以下IP地址的Linux分路器介面：

- IPV4:虛擬裝置上為169.254.1.2/29，硬件裝置上為169.254.1.3/29。
- IPV6:虛擬裝置上的fd00:0:0:1::2/64和硬體裝置上的fd00:0:0:1::3/64。

虛擬和硬體FTD裝置中的驗證：

- 虛擬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

- 安全防火牆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
```

為了提供與Lina的連線，OS為使用tap_nlp介面的源IP地址的資料包的路由表查詢安裝路由規則：

<#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)
```

重點：

- IPv4和IPv6路由規則規定，在路由表1中執行來自nlp_tap介面地址的資料包的路由查詢。
- 路由表1的IPv4和IPv6版本包含預設路由，其下一跳地址屬於Lina nlp_int_tap介面。

封包路徑和擷取點

本節顯示兩種不同情況中的封包路徑和擷取點：

- 已禁用資料介面管理。
- 已啟用資料介面管理。

附註：在FDM上，還有一個具有「使用資料介面作為網關」功能的方案。從路由、組態和封包擷取點的角度來看，此案例類似於FMC管理的FTD（透過資料介面進行管理）。

已禁用資料介面管理

本節介紹如何在FTD上驗證封包路徑和擷取點，並提供以下組態詳細資訊：

1. FTD由FMC管理。
2. 無資料介面管理。這意味著管理介面用於提供作業系統和外部網路之間的連線：

```
<#root>

>

show network management-data-interface


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

3. 至少配置了以下功能之一：

- ASA或FTD上的SNMP。
- 通過Cisco SSH堆疊通過SSH訪問ASA。在ASA 9.23及更高版本中，思科SSH堆疊處於啟用狀態，無法禁用。
- 透過資料介面對FTD進行SSH存取。
- 通過FDM管理的FTD上的資料介面進行HTTPS訪問。

4. 所有捕獲點都配置了資料包捕獲。

如果配置了前面提到的功能之一，將自動配置手動兩次NAT規則。根據功能埠/協定，NAT規則會有所不同。

以下是包含手動兩次NAT規則的輸出示例，用於通過資料介面進行FTD SSH訪問：

```
<#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

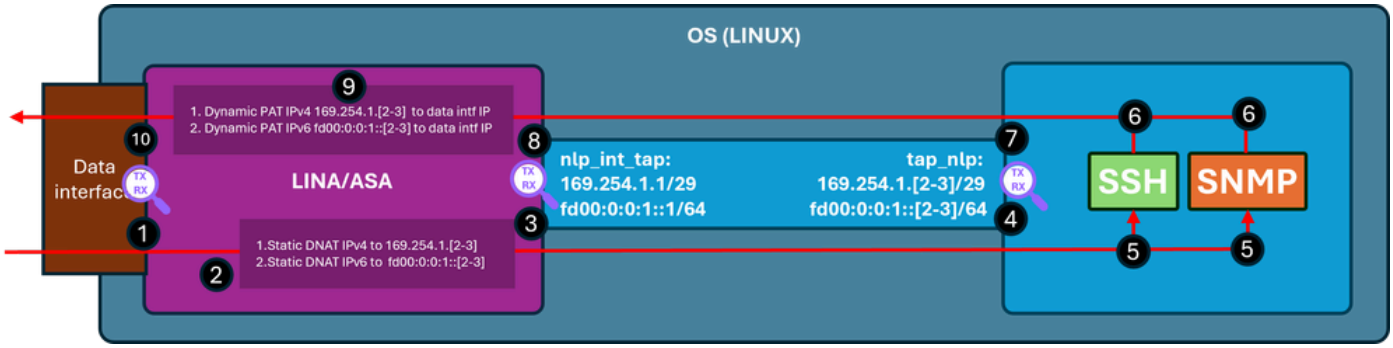
Source - Origin: fd00:0:0:1::2/128, Translated:

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

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

附註：在使用Cisco SSH堆疊通過SSH連線到ASA的情況下，目的地埠會從22轉換到4122。

此圖顯示封包路徑和擷取點：



驗證步驟（適用於前面提到的功能）：

1. 捕獲點 — 用於從IP 192.0.2.2到埠22上的IP 192.0.2.1的SSH的輸入TCP SYN資料包。 IP 192.0.2.1是內部介面的地址：

<#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.捕獲跟蹤指示匹配的NAT規則，該規則將目標IP從192.0.2.1轉換為IP 169.254.1.2，並將資料包轉發到nlp_int_tap輸出介面：

<#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.擷取點 — 目的地IP 169.254.1.2連線埠22的封包會從nlp_int_tap介面傳送：

<#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.擷取點 — 在OS tap_nlp介面上收到目的地IP為169.254.1.2連線埠22的封包：

<#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. SSH守護程式在埠22上偵聽，接收SYN資料包並進行處理：

```
<#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. SSH生成SYN ACK資料包。

7.Capture point（捕獲點）— 源IP 169.254.1.2埠22和目標IP 192.0.2.2的SYN ACK資料包通過tap_nlp介面傳送：

```
<#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.擷取點 — 在Lina nlp_int_tap介面上收到來源IP 169.254.1.2連線埠22和目的地IP位址192.0.2.2的SYN ACK封包：

```
<#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.此SYN ACK封包是作為現有/已建立連線的一部分處理，Lina引擎會根據此連線應用反向NAT規則，將封包的來源從IP 169.254.1.2轉譯到內部IP 192.0.2.1，並選擇內部作為輸出介面。在使用Cisco SSH堆疊通過SSH連線到ASA的情況下，源埠從4122轉換為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.擷取點 — 封包從內部介面前往目的地：

```
<#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
```

已啟用資料介面管理

如果在FMC管理的FTD上啟用資料介面管理，則這些變更會自動發生：

1. 在CLISH上，預設網關是data-interface。OS級預設閘道是透過tap_nlp，且下一個躍點指向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. 在Lina上，通常透過資料介面設定預設路由 — 這是從FMC部署的使用者組態：

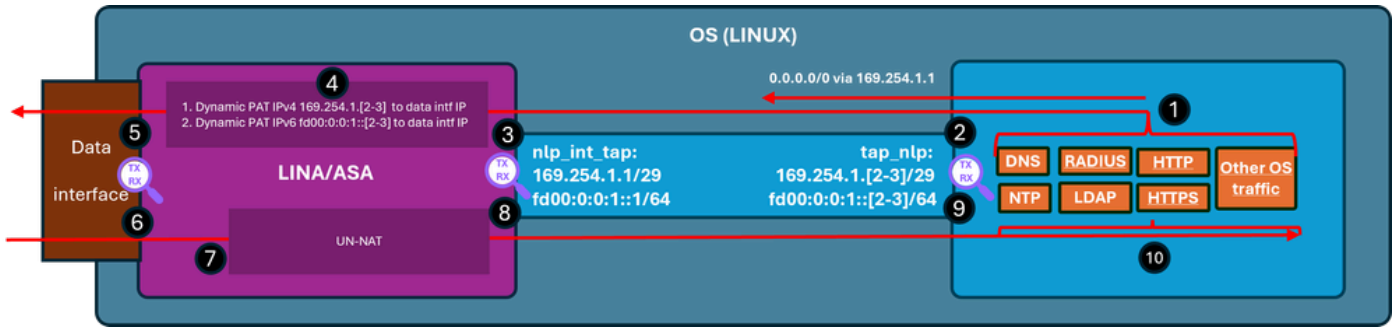
```
<#root>

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. 在Lina上，為IPv4和IPv6堆疊安裝了兩次sftunnel埠8305的NAT規則。此外，為了允許從作業系統連線到外部網路，通過資料介面為OS tap_nlp介面的IPv4和IPv6地址配置動態PAT。

```
<#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
```

此圖顯示封包路徑和擷取點：



驗證步驟(在本示例中，驗證步驟適用於NTP流量。同樣的邏輯適用於任何由作業系統生成的流量（包括許可等）：

1. NTP客戶端生成一個發往外部NTP伺服器IP地址的資料包：

<#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
```

從作業系統的角度來看，下一跳是通過tap_nlp介面，使用相同的介面IP 169.254.1.3作為源地址：

<#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. 捕獲點 — 將資料包從tap_nlp介面傳送出去：

<#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. 擷取點 — 封包到達Lina nlp_tap_interface介面：

<#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. 根據路由查詢，Lina將內部識別為輸出介面，然後應用將資料包源IP地址從169.254.1.3更改為資料介面IP地址的動態PAT規則：

```
<#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. 擷取點 — 封包透過輸出介面傳送出去：

<#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. 捕獲點 — NTP伺服器傳送回複資料包：

<#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將回覆視為已建立連線的一部分，並套用反向NAT。 根據此資訊，目的地會轉換為169.254.1.3，輸出介面為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. 捕獲點 — 應答資料包從nlp_int_tap介面傳送：

```
<#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. 捕獲點 — 重放資料包到達作業系統tap_nlp接口：

<#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. 應答資料包由NTP客戶端使用和處理。

摘要

在Lina中，OS /dev/net/tap/tap_nlp介面以nlp_int_tap形式可見。此介面的用途是提供Lina和作業系統之間的連線。此介面以及所需的NAT規則由軟體自動管理，無需使用者干預。

參考資料

- 安全防火牆配置指南

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。