Esclareça a Finalidade da Interface de Dados Internos com nlp_int_tap e o Endereço IP 169.254.1.1

Contents

Introdução

Este documento descreve a finalidade da interface Internal-Data nlp_int_tap com o endereço IP 169.254.1.1.

Pré-requisitos

Requisitos

Conhecimento básico do produto.

Componentes Utilizados

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

As informações neste documento são baseadas nestas versões de software e hardware:

- Secure Firewall Threat Defense (FTD) 7.x, 10.x gerenciada pelo Secure Firewall Device Manager (FDM) ou pelo Secure Firewall Management Center (FMC).
- Secure ASA 9.18 e posterior.

Informações de Apoio

A interface Internal-Data com o nome nlp_int_tap e o endereço IP 169.254.1.1 é uma interface interna usada para fornecer conectividade entre o mecanismo do plano de dados chamado Lina e o sistema operacional de back-end (SO).

É usado para fornecer conectividade geral para estes serviços:

- SNMP - O daemon SNMP é executado como um processo separado no SO.
- Acesso SSH ao ASA com a pilha Cisco SSH - o daemon SSH é executado como um processo separado no SO.
- Acesso SSH ao FTD através da interface de dados - o daemon SSH é executado como um processo separado no SO.
- Autenticação externa com reconhecimento de VRF em FTD - o acesso a servidores de autenticação externos é fornecido através de uma interface de dados em um VRF global ou de usuário.
- No caso de gerenciamento de FTD sobre interfaces de dados, acesso a serviços de gerenciamento como sftunnel, resolução DNS, licenciamento, autenticação externa, NTP ou qualquer destino para o qual o SO não tenha rotas estáticas configuradas explicitamente sobre a interface de gerenciamento.

Verificação de Lina

Dependendo da plataforma, no mecanismo Lina o nome nlp_int_tap é atribuído à interface Internal-DataX/Y e é visível em diferentes saídas de comando.

Estas são saídas de diferentes firewalls:

- Secure Firewall 6170 executando o 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 executando 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 virtual:

```
<#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 virtual:

<#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
```

…

Pontos principais:

- O nome nlp_int_tap é atribuído a diferentes interfaces Internal-Data em diferentes plataformas.
- De acordo com a saída do comando show asp table routing, a interface Internal-Data com o nome se nlp_int_tap recebe o endereço IPv4 169.254.1.1/29 e o endereço IPv6 fd00:0:0:1::1/64.
- De acordo com a saída do comando show controller, essa interface é uma interface Linux Tun/Tap (especificamente tap) disponível em /dev/net/tun/tap_nlp.

Verificação do SO

/dev/net/tun/tap_nlp é uma interface de toque Linux com estes endereços IP:

- IPV4: 169.254.1.2/29 em dispositivos virtuais e 169.254.1.3/29 em dispositivos de hardware.
- IPV6: fd00:0:0:1::2/64 em dispositivos virtuais e fd00:0:0:1::3/64 em dispositivos de hardware.

Verificação em dispositivos FTD virtuais e de hardware:

- FTD virtual:

<#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
```

- Firewall seguro 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
```

Para fornecer conectividade de volta ao Lina, o SO instala uma regra de roteamento para a consulta da tabela de roteamento de pacotes com os endereços IP origem da 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)
```

Pontos principais:

- As regras de roteamento IPv4 e IPv6 determinam que a pesquisa de rota para pacotes originados nos endereços de interface nlp_tap seja executada na tabela de roteamento 1.
- As versões IPv4 e IPv6 da tabela de roteamento 1 contêm a rota padrão com o endereço do próximo salto que pertence à interface Lina nlp_int_tap.

Caminho do pacote e pontos de captura

Esta seção mostra o caminho do pacote e os pontos de captura em 2 casos diferentes:

- O gerenciamento na interface de dados está desabilitado.
- O gerenciamento pela interface de dados está habilitado.

Note: Há um cenário adicional com o recurso "Usar as Interfaces de Dados como o Gateway" no FDM. Do ponto de vista de roteamento, configuração e captura de pacotes, esse cenário é semelhante ao FTD gerenciado pelo FMC com gerenciamento pela interface de dados.

O gerenciamento pela interface de dados está desativado

Esta seção descreve a verificação do caminho do pacote e os pontos de captura no FTD com estes detalhes de configuração:

1. O DTF é gerido pelo CVP.
2. Sem gerenciamento na interface de dados. Isso significa que a interface de gerenciamento é usada para fornecer conectividade entre o SO e a rede externa:

```
<#root>

>

show network management-data-interface


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

3. Pelo menos um destes recursos está configurado:

- SNMP em ASA ou FTD.
- Acesso SSH ao ASA com a pilha Cisco SSH. Nas versões 9.23 e posteriores do ASA, a pilha do Cisco SSH está habilitada e não pode ser desabilitada.
- Acesso SSH ao FTD em interfaces de dados.
- Acesso HTTPS pela interface de dados no FTD gerenciado pelo FDM.

4. As capturas de pacotes são configuradas em todos os pontos de captura.

Se um dos recursos mencionados anteriormente estiver configurado, as regras manuais de NAT duas vezes serão configuradas automaticamente. Dependendo das portas/protocolos do recurso, as regras de NAT são diferentes.

Esta é uma saída de exemplo com duas regras NAT manuais para acesso SSH FTD sobre interface de dados:

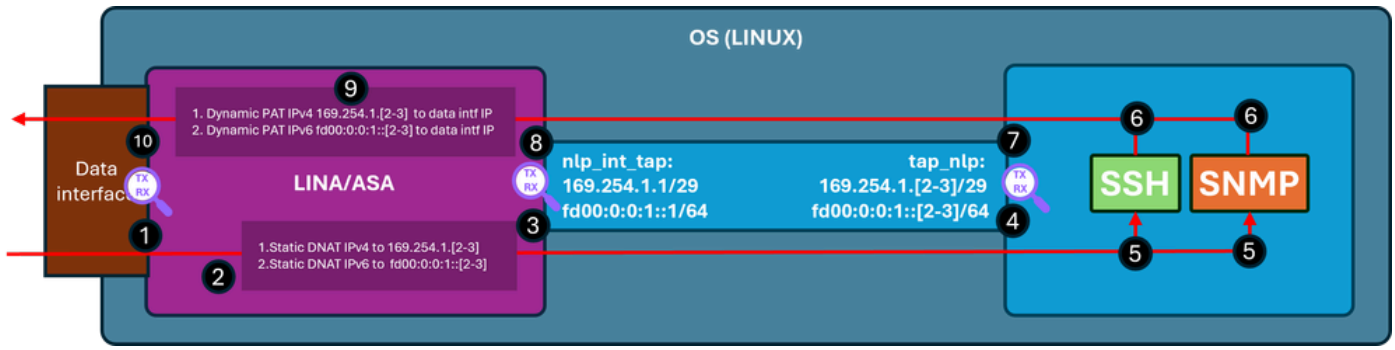
<#root>

```
firewall#

show nat detail


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

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



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



    Service - Protocol: tcp Real: ssh Mapped: ssh



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

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



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



    Service - Protocol: tcp Real: ssh Mapped: ssh



3 (nlp_int_tap) to (inside) source dynamic nlp_client_0_0.0.0.0_6proto22_intf3 interface  destination s

    translate_hits = 0, untranslate_hits = 0
```

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

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

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

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

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

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

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

Note: No caso da conexão SSH com o ASA com a pilha Cisco SSH, a porta de destino é convertida de 22 para 4122.

Este diagrama mostra o caminho do pacote e os pontos de captura:



Etapas de verificação (aplicáveis aos recursos mencionados anteriormente):

1. Ponto de captura - pacote TCP SYN de entrada para SSH de IP 192.0.2.2 para IP 192.0.2.1 na porta 22. O IP 192.0.2.1 é o endereço da interface interna:

<#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. O rastreamento de captura indica uma regra NAT correspondente que converte o IP de destino de 192.0.2.1 para IP 169.254.1.2 e desvia pacotes para a interface de saída 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. Ponto de captura - o pacote com o IP destino 169.254.1.2 porta 22 é enviado para fora da

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. Ponto de captura - o pacote com o IP destino 169.254.1.2 porta 22 é recebido na interface do SO 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
```

5. O daemon SSH escuta na porta 22, recebe o pacote SYN e o manipula:

<#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. O SSH gera um pacote SYN ACK.

7.Ponto de captura - o pacote SYN ACK com o IP origem 169.254.1.2 porta 22 e o IP destino 192.0.2.2 são enviados pela 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. Ponto de captura - o pacote SYN ACK com o IP origem 169.254.1.2 porta 22 e o endereço IP destino 192.0.2.2 é recebido na 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. Este pacote SYN ACK é manipulado como parte da conexão existente/estabelecida com base

na qual o mecanismo Lina aplica a regra NAT reversa para converter a origem do pacote do IP 169.254.1.2 para o IP interno 192.0.2.1 e seleciona inside como a interface de saída. No caso da conexão SSH com o ASA com a pilha Cisco SSH, a porta de origem é convertida de 4122 de volta para 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. Ponto de captura - o pacote deixa a interface interna em direção ao destino:

<#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
```

O gerenciamento pela interface de dados está habilitado

Se a gestão através da interface de dados estiver ativada no FTD gerido pelo FMC, estas alterações ocorrem automaticamente:

1. No CLISH, o gateway padrão é a interface de dados. O gateway padrão no nível do sistema operacional é via tap_nlp com o próximo salto apontando para o 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. Em Lina, normalmente há uma rota padrão configurada através da interface de dados - essa é a configuração do usuário implantada no 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. No manual Lina, as regras de NAT para a porta de sftunnel 8305 são instaladas para as pilhas IPv4 e IPv6. Além disso, para permitir a conectividade do SO para redes externas, um PAT dinâmico para os endereços IPv4 e IPv6 da interface tap_nlp do SO é configurado na interface de dados.

<#root>

firewall#

show nat detail

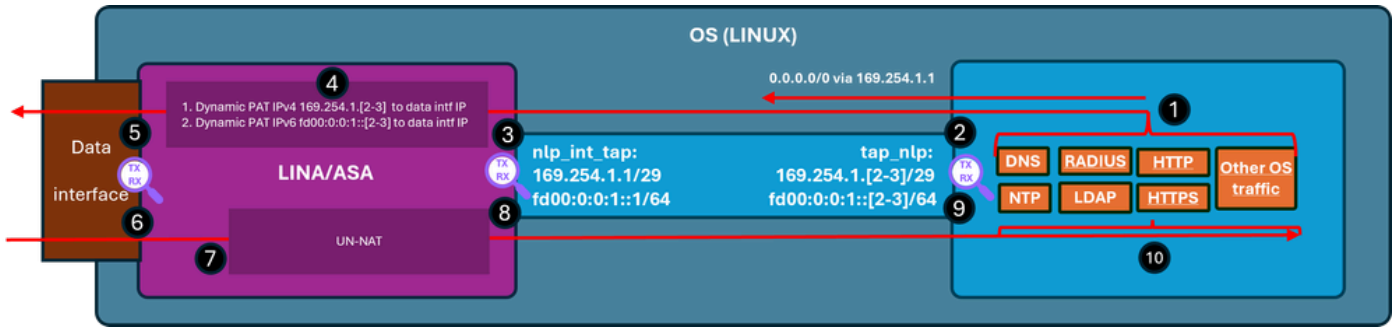
Manual NAT Policies Implicit (Section 0)
1 (nlp_int_tap) to (inside) source static nlp_server__sftunnel_0.0.0.0_intf3 interface destination sta
    translate_hits = 6, untranslate_hits = 6

    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
```

Este diagrama mostra o caminho do pacote e os pontos de captura:



Etapas de verificação (Neste exemplo, as etapas de verificação são para o tráfego NTP. A mesma lógica se aplica a qualquer tráfego gerado pelo SO, incluindo licenciamento, etc.):

1. O cliente NTP gera um pacote destinado a um endereço IP de servidor NTP externo:

```
<#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
```

Do ponto de vista do SO, o próximo salto é através da interface tap_nlp usando o mesmo IP da interface 169.254.1.3 que o endereço de origem:

```
<#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. Ponto de captura - o pacote é enviado pela 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. Ponto de captura - o pacote chega à 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. Com base na pesquisa de rota, Lina identifica o interior como a interface de saída e, em seguida, aplica uma regra PAT dinâmica que altera o endereço IP origem do pacote de 169.254.1.3 para o endereço IP da interface de dados:

```
<#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. Ponto de captura - o pacote é enviado por meio da interface de saída:

```
<#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. Ponto de captura - o servidor NTP envia um pacote de resposta:

```
<#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 lida com a resposta como parte das conexões estabelecidas e aplica NAT reverso.

Com base nessas informações, o destino é convertido em 169.254.1.3, a interface de saída é 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. Ponto de captura - o pacote de resposta é enviado pela 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. Ponto de captura - o pacote de repetição chega à interface do OS 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

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

10. O pacote de resposta é consumido e tratado pelo cliente NTP.

Summary

A interface OS /dev/net/tun/tap_nlp está visível como nlp_int_tap em Lina. A finalidade dessa interface é fornecer conectividade entre Lina e o SO. Essa interface, juntamente com as regras de NAT necessárias, é gerenciada automaticamente pelo software e não requer intervenção do usuário.

Referências

- Guias de configuração de firewall seguro

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.