nameif nlp_int_tapおよびIPアドレス169.254.1.1を使用した内部データインターフェイスの目的の明確化

内容

はじめに

前提条件

- 要件
- 使用するコンポーネント

バックグラウンド情報

- Linaの検証
- OSの検証

パケットパスとキャプチャポイント

- データインターフェイス経由の管理が無効です
- データインターフェイス経由の管理が有効である

要約

参照資料

はじめに

このドキュメントでは、IPアドレス169.254.1.1を使用する内部データnlp_int_tapインターフェイスの目的について説明します。

前提条件

要件

製品の基礎知識

使用するコンポーネント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Secure Firewall Threat Defense(FTD)7.x、10.xは、Secure Firewall Device Manager(FDM)またはSecure Firewall Management Center(FMC)で管理されます。
- Secure ASA 9.18以降。

バックグラウンド情報

nameif nlp_int_tapとIPアドレス169.254.1.1を使用する内部データインターフェイスは、Linaと呼ばれるデータプレーンエンジンとバックエンドオペレーティングシステム(OS)間の接続の提供に使用される内部インターフェイスです。

これは、次のサービスに一般的な接続を提供するために使用されます。

- SNMP:SNMPデーモンは、OSの個別のプロセスとして実行されます。
- Cisco SSHスタックを使用したASAへのSSHアクセス：SSHデーモンは、OSの個別のプロセスとして実行されます。
- データインターフェイスを介したFTDへのSSHアクセス：SSHデーモンは、OSの個別のプロセスとして実行されます。
- FTDでのVRF対応の外部認証：外部認証サーバへのアクセスは、グローバルVRFまたはユーザVRFのデータインターフェイスを介して提供されます。
- データインターフェイスを介したFTD管理の場合は、sftunnel、DNS解決、ライセンス、外部認証、NTP、またはOSが管理インターフェイスを介してスタティックルートを明示的に設定していない宛先などの管理サービスへのアクセス。

Linaの検証

プラットフォームによっては、Linaエンジンでnameif nlp_int_tap がInternal-DataX/Yインターフェイスに割り当てられ、異なるコマンド出力に表示されます。

これらは、さまざまなファイアウォールからの出力です。

- FTDを実行するセキュアファイアウォール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
…
```

- ASAを実行する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

…

- 仮想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

…

- 仮想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

…

キー ポイント：

- nameif nlp_int_tapは、異なるプラットフォームの異なる内部データインターフェイスに割り当てられます。
- show asp table routing コマンドの出力によると、nameif nlp_int_tap を持つ内部データインターフェイスには、IPv4アドレス169.254.1.1/29 とIPv6アドレスfd00:0:0:1::1/64が割り当てられています。
- show controllerコマンドの出力によると、このインターフェイスは/dev/net/tun/tap_nlpで使用できるLinux Tun/Tapインターフェイス（特にtap）です。

OSの検証

/dev/net/tun/tap_nlp は、次のIPアドレスを持つLinuxのtapインターフェイスです。

- IPV4：仮想デバイス上の169.254.1.2/29およびハードウェアデバイス上の169.254.1.3/29。
- IPV6:fd00:0:0:1::2/64（仮想デバイス）とfd00:0:0:1::3/64（ハードウェアデバイス）です。

仮想およびハードウェアFTDデバイスでの検証：

- 仮想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
```

- Cisco Secure Firewall 6170:

<#root>

```
admin@CSF6170-1:~$

ip addr show dev tap_nlp


7:

tap_nlp

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

    inet 169.254.1.3/29 brd 169.254.1.7 scope global tap_nlp:1


       valid_lft forever preferred_lft forever

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


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

回線への接続を提供するために、OSによって、tap_nlpインターフェイスの送信元IPアドレスを持つパケットのルーティングテーブル検索のためのルーティングルールがインストールされます。

<#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)
```

キー ポイント：

- IPv4およびIPv6のルーティングルールでは、nlp_tapインターフェイスアドレスから送信されたパケットのルートルックアップがルーティングテーブル1で実行されます。
- ルーティングテーブル1のIPv4およびIPv6バージョンには、Lina nlp_int_tapインターフェイスに属するネクストホップアドレスでのデフォルトルートが含まれています。

パケットパスとキャプチャポイント

このセクションでは、次の2つの異なるケースにおけるパケットパスとキャプチャポイントを示します。

- データインターフェイスの管理は無効です。
- データインターフェイス経由の管理が有効になっています。

注意: FDMの「ゲートウェイとしてデータ・インタフェースを使用する」機能には、追加のシナリオがあります。ルーティング、設定、およびパケットキャプチャポイントの観点から見ると、このシナリオはデータインターフェイス経由の管理を備えたFMCによって管理されるFTDに似ています。

データインターフェイス経由の管理が無効です

このセクションでは、FTDでのパケットパスとキャプチャポイントの検証について、次の設定の詳細とともに説明します。

1. FTDはFMCによって管理されます。
2. データインターフェイスの管理は行いません。これは、管理インターフェイスを使用してOSと外部ネットワーク間の接続を提供することを意味します。

```
<#root>

>

show network management-data-interface


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

3. 次の機能の少なくとも1つが設定されています。

- ASAまたはFTDでのSNMP
- Cisco SSHスタックによる ASAへのSSHアクセス ASAバージョン9.23以降では、Cisco SSHスタックは有効になっており、無効にはできません。
- データインターフェイス経由のFTDへのSSHアクセス
- FDM管理対象FTDのデータ・インタフェースを介したHTTPSアクセス。

4. パケットキャプチャは、すべてのキャプチャポイントで設定されます。

前述のいずれかの機能が設定されている場合、手動の2倍のNATルールが自動的に設定されます。機能ポートやプロトコルによって、NATルールは異なります。

次に、データインターフェイスを介したFTD SSHアクセスに対する手動のTwice NATルールの出

力例を示します。

<#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

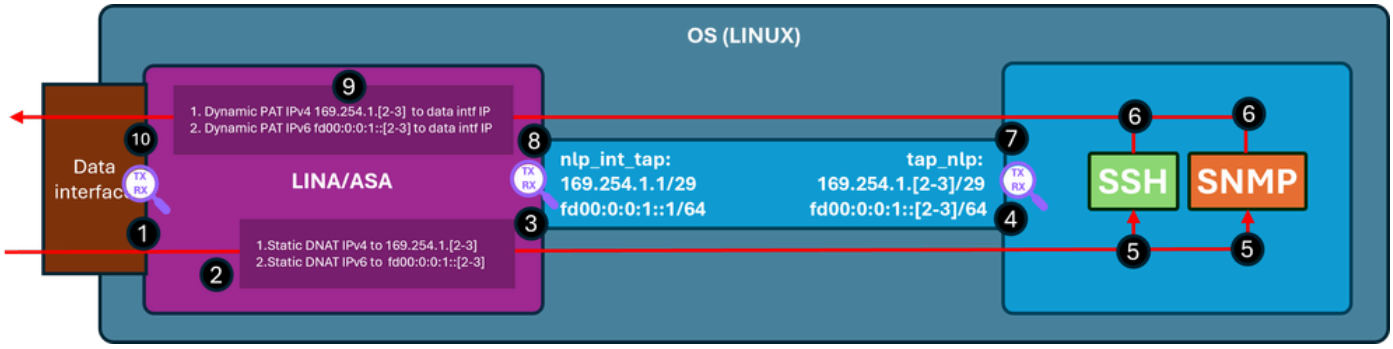
    Source - Origin: 169.254.1.2/32, Translated: 192.0.2.1/24

    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
```

注:Cisco SSHスタックを使用したASAへのSSH接続の場合、宛先ポートは22から4122に変換されます。

次の図に、パケットパスとキャプチャポイントを示します。



確認手順（前述の機能に適用）:

1. キャプチャポイント – IP 192.0.2.2からIP 192.0.2.1 のポート22へのSSHの入力TCP SYNパケット。IP 192.0.2.1は内部インターフェイスのアドレスです。

```
<#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. キャプチャトレースは、宛先IPを192.0.2.1からIP 169.254.1.2に変換し、パケットをnlp_int_tap出力インターフェイスに転送する、一致するNATルールを示しています。

<#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. キャプチャポイント – 宛先IP 169.254.1.2ポート22を持つパケットがnlp_int_tapインターフェイスから送信されます。

<#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. キャプチャポイント – 宛先IP 169.254.1.2ポート22を持つパケットがOS tap_nlpインターフェイスで受信されます。

<#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デーモンはポート22でリッスンし、SYNパケットを受信して、それを処理します。

<#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はSYN ACKパケットを生成します。

7. キャプチャポイント – 送信元IP 169.254.1.2ポート22および宛先IP 192.0.2.2を持つSYN ACKパケットがtap_nlpインターフェイスから送信されます。

<#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. キャプチャポイント – 送信元IP 169.254.1.2ポート22と宛先IPアドレス192.0.2.2を持つSYN ACKパケットがLina nlp_int_tapインターフェイスで受信されます。

<#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. このSYN ACKパケットは、既存または確立された接続の一部として処理されます。この接続に基づいて、Linaエンジンは、パケットの送信元をIP 169.254.1.2から内部IP 192.0.2.1に変換する逆NATルールを適用し、出力インターフェイスとして内部を選択します。Cisco SSHスタックを使用したASAへのSSH接続の場合、送信元ポートは4122から22に戻されます。

<#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. キャプチャポイント：パケットが内部インターフェイスから宛先に向けて送出されます。

```
<#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
```

データインターフェイス経由の管理が有効である

FMCによって管理されるFTDでデータインターフェイスの管理が有効になっている場合は、次の変更が自動的に行われます。

1. CLISHでは、デフォルトゲートウェイはdata-interfaceです。OSレベルのデフォルトゲートウェイはtap_nlpを経由し、ネクストホップはLina IP 169.254.1.1を指しています。

```
<#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. Linaには通常、データインターフェイスを介して設定されたデフォルトルートがあります。これはFMCから展開されたユーザ設定です。

```
<#root>

firewall#

show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
```

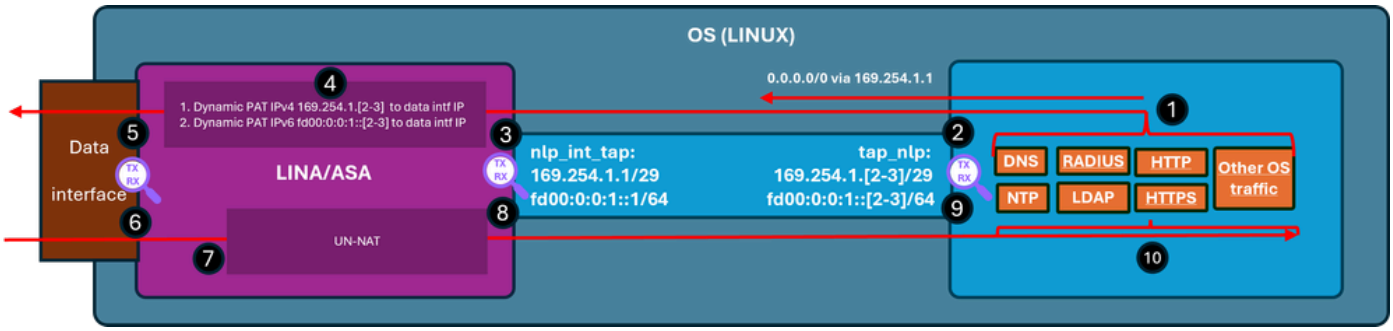
```
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - 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. Linaのマニュアルでは、sftunnelポート8305の2倍のNATルールがIPv4とIPv6の両方のスタックにインストールされています。また、OSから外部ネットワークへの接続を可能にするために、OSのtap_nlpインターフェイスのIPv4およびIPv6アドレスに対するダイナミックPATがデータインターフェイス上で設定されます。

```
<#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
```

次の図に、パケットパスとキャプチャポイントを示します。



検証手順(この例では、検証手順はNTPトラフィック用です。同じロジックが、ライセンスなどを含むOS生成トラフィックにも適用されます)。

1. NTPクライアントは、外部NTPサーバのIPアドレス宛てのパケットを生成します。

<#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
```

OSの観点からは、ネクストホップは、送信元アドレスとして同じインターフェイスIP 169.254.1.3を使用しているtap_nlpインターフェイスを経由しています。

<#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. キャプチャポイント：パケットはtap_nlpインターフェイスから送信されます。

<#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. キャプチャポイント：パケットがLina nlp_tap_interfaceインターフェイスに到着します。

<#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. ルートルックアップに基づいて、Linaは内部を出力インターフェイスとして識別し、パケットの送信元IPアドレスを169.254.1.3からデータインターフェイスIPアドレスに変更するダイナミックPATルールを適用します。

<#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. キャプチャポイント：パケットは出力インターフェイス経由で送信されます。

```
<#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. キャプチャポイント：NTPサーバが応答パケットを送信します。

```
<#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は確立された接続の一部として応答を処理し、リバースNATを適用します。この情報に基づいて、宛先は169.254.1.3に変換され、出力インターフェイスはnlp_int_tapです。

```
<#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. キャプチャポイント：応答パケットはnlp_int_tapインターフェイスから送信されます。

```
<#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. キャプチャポイント：リプレイパケットがOSのtap_nlpインターフェイスに到着します。

```
<#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. 応答パケットはNTPクライアントによって消費され、処理されます。

要約

OSの/dev/net/tun/tap_nlpインターフェイスは、Linaではnlp_int_tapとして表示されます。このインターフェイスの目的は、LinaとOS間の接続を提供することです。このインターフェイスは、必要なNATルールとともにソフトウェアによって自動的に管理されるため、ユーザの介入は必要ありません。

参照資料

- セキュアファイアウォール設定ガイド

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。