توضيح الغرض من واجهة البيانات الداخلية باستخدام الاسم NLP_INT_TAP وعنوان IP 169.254.1.1

المحتويات

المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

معلومات أساسية

التحقق من الخطأ

التحقق من نظام التشغيل

مسار الحزمة ونقاط الالتقاط

تم تعطيل الإدارة عبر واجهة البيانات

تم تمكين الإدارة عبر واجهة البيانات

ملخص

المراجع

المقدمة

يصف هذا المستند الغرض من واجهة Internal-Data nlp_int_tap مع عنوان IP 169.254.1.1.

المتطلبات الأساسية

المتطلبات

المعرفة الأساسية بالمنتج.

المكونات المستخدمة

مت إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- برنامج Secure Firewall Threat Defense (FTD) 7.x، الإصدار 10.x المدار من قبل مدير أجهزة جدار الحماية الآمن (FDM) أو جدار إدارة مركز جدار الحماية الآمن (FMC).
- Secure ASA 9.18 والإصدارات الأحدث.

معلومات أساسية

تعد واجهة البيانات الداخلية باستخدام اسم NLP_INT_TAP وعنوان IP 169.254.1.1 واجهة البيانات الذي يسمى Lina ونظام داخلية يتم استخدامها لتوفير الاتصال بين محرك Lina ونظام التشغيل الخلفي (OS).

الخدمات: هذه عامة لاتصال توفير استخدامها يتم و

- SNMP - يعمل برنامج SNMP الخفيف كعملية منفصلة في نظام التشغيل.
- كعملية SSH الخفيفة - يعمل برنامج Cisco SSH كمدس باستخدام ASA إلى SSH ووصول منفصلة في نظام التشغيل.
- كعملية SSH الخفيفة البرنامج - يعمل البيانات واجهة عبر FTD إلى SSH ووصول منفصلة في نظام التشغيل.
- إلى الوصول المتوفر يتم - FTD بروتوكول على VRF معيار مع متوافقة خارجية مصادقة مستخدم أو عام VRF تدرد في بيانات واجهة عبر الخارجية المصادقة خوادم.
- أو sftunnel لمثل الإدارة خدمات إلى الوصول يتم ،البيانات واجهات عبر FTD إدارة حالة في أي (NTP) الشبكة وقت بروتوكول أو الخارجية المصادقة أو الترخيص أو DNS تحليل واجهة عبر صريح بشكل الثابتة المسارات بتكوين التشغيل نظام يوقم لا واجهات الإدارة.

التحقق من الخطط

حسب النظام الأساسي، في محرك Lina، يتم تعيين الاسم nlp_int_tap إلى واجهة Internal-DataX/Y وتكون مرئية في مخرجات وأوامر مختلفة.

هذه مخرجات من جدران حماية مختلفة:

- جدار الحماية الآمن طراز 6170 الذي يعمل بنظام التشغيل FTD:

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 runs, 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: لغشي يذلا 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

…
```

- برنامج FTD الظاهري:

```
<#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 الظاهري:

<#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

…

النقاط الرئيسية:

- ةيساسأ ةمظنأ ىلع ةفلتخم ةيلخاد تانايب تاهجاو ىلإ nlp_int_tap مسالا نييعت متي ةفلتخم.
- تانايبلا ةهجاول IPv4 ناونع نييعت متي ،show asp table routing رمألا جرخمل اقفو IPv6 fd00:0:1::1/64. ناونعو 169.254.1.1/29و nlp_int_tap مسالا لمحت يتلا ةيلخادلا
- ەجو ىلع) Linux TUN/TAP ةهجاو يه ةهجاولا هذه نإف ،show controller رمألا جرخمل اقفو /dev/net/tun/tap_nlp. يف ةرفوتملا TAP) ديدحتلا

التحقق نم ماظن التشغيل

/dev/net/tun/tap_nlp ةهجاو يه ةطغض Linux يوتحت على نيوانع IP التالية:

- ةيضارتفالا ةزهجألا ىلع 169.254.1.2/29 :(IP) تنرتنإلا لوكوتورب نم عبارلا رادصإلا ةزهجألا ىلع 169.254.1.3/29و.
- ةزهجأ ىلع FD00:0:1:3/64و ةيضارتفالا ةزهجألا ىلع FD00:0:1::2/64 :IPv6 لوكوتورب ةزهجألا.

التحقق نم ةزهجألا ةيضارتفالا ةزهجأو FTD:

- جمانرب FTD يرهاظلا:

<#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
```

- جدار الحماية الآمن 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
```

لتوفير الاتصال مرة أخرى إلى Lina، يقوم نظام التشغيل بتثبيت قاعدة توجيه للبحث عن جدول التوجيه للحزم باستخدام عناوين IP المصدر الخاصة بواجهة 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)
```

النقاط الرئيسية:

- تقضي قواعد توجيه IPv4 و IPv6 بأنه يتم إجراء بحث المسار للحزم المستمدة من عنواين واجهة NLP_TAP في جدول التوجيه 1.
- تحتوي إصدارات IPv4 و IPv6 من جدول التوجيه 1 على مسار افتراضي مع عنوان الخطوة التالية الذي ينتمي إلى واجهة Lina nlp_int_tap.

مسار الحزمة ونقاط الالتقاط

يبدي هذا قسم الربط ممر و إلتقاط نقطة في 2 حالة مختلف:

- تم تعطيل الإدارة عبر واجهة البيانات.
- تم تمكين الإدارة عبر واجهة البيانات.

ملاحظة: هناك سيناريو إضافي مع ميزة "إستخدام واجهات البيانات كبوابة" على FDM. سيناريو برنامج FTD هذا يشبه، من منظور نقطة التوجيه والتكوين والتقاط الحزم، من إدارة عبر واجهة البيانات بوساطة FMC مع المدار.

تم تعطيل الإدارة عبر واجهة البيانات

يصف هذا القسم التحقق من الربط ممر ونقاط التقاط على FTD مع هذا التشكيل تفاصيل:

1. تتم إدارة برنامج الإرسال فائق السرعة (FTD) بوساطة وحدة التحكم FMC.
2. لا توجد إدارة عبر واجهة البيانات. وهذا يعني أنه تم إستخدام واجهة الإدارة لتوفير الاتصال بين نظام التشغيل والشبكة الخارجية:

```
<#root>

>

show network management-data-interface

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

3. تم تكوين ميزة واحدة على الأقل من هذه الميزات:

- FTD وأ SNMP على ASA.
- ASA من 9.23 في الإصدارات Cisco SSH. باستخدام مكدس ASA إلى SSH وصول
  والإصدارات الأحدث، يتم تمكين مكدس Cisco SSH والذي يمكن تعطيله.
- وصول SSH إلى FTD عبر واجهات البيانات.
- وصول HTTPS عبر واجهة البيانات على FTD المدار بوساطة FDM.

4. تم تكوين التقاط الحزم في جميع نقاط الالتقاط.

إن شكلت واحد من السابق ذكر سمة يكون، يدوي مرتين nat قاعدة شكلت تلقائيا. على حسب ميزات المنافذ/البروتوكولات، تختلف قواعد nat.

هذا مثال إخراج عم ضعف قواعد NAT يدوي للوصول إلى FTD SSH عبر واجهة البيانات:

```
<#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

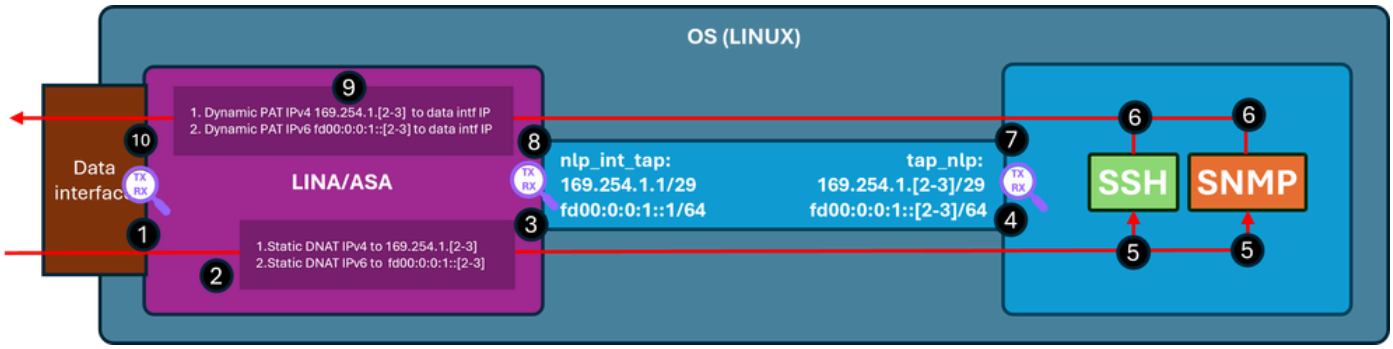
Destination - Origin: 0.0.0.0/0, Translated: 0.0.0.0/0

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
```

ملاحظة: في حالة اتصال SSH ب ASA مع Cisco SSH stack، تتم ترجمة منفذ الوجهة من 22 إلى 4122.

يبدي هذا رسم بياني الربط ممر والمفتاح نقطة:



خطوات التحقق (يمكن تطبيقها على الميزات المذكورة سابقا):

1. نقطة الالتقاط - مدخل TCP نظام ربط ل SSH من IP 192.0.2.2 إلى IP 192.0.2.1 على ميناء 22. IP 192.0.2.1 هو عنوان الواجهة الداخلية:

```
<#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. يشير تتبع الالتقاط إلى قاعدة NAT مطابقة تترجم عنوان IP للوجهة من 192.0.2.1 إلى IP NLP_INT_TAP: خرج وجهة واحدة إلى الحزم لتحويل، 169.254.1.2

```
<#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. Capture Point - يتم إرسال الحزمة ذات المنفذ IP 169.254.1.2 المنفذ 22 من خلال واجهة 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. نقطة الالتقاط - يتم إستلام الحزمة ذات المنفذ 169.254.1.2 من IP الوجهة 22 على واجهة OS 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. يستمع برنامج SSH على المنفذ 22، ويستلم حزمة SYN ويعالجه:

```
<#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. إنشاء حزمة SYN ACK. لوكوتورب موقي SSH.

7. Capture Point - يتم إرسال حزمة ACK مع مصدر IP 169.254.1.2 منفذ 22 وجهة IP 192.0.2.2 إلى واجهة 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. Capture Point - يتم تلقي حزمة ACK مع المصدر IP 169.254.1.2 المنفذ 22 وعنوان IP
Lina NLP_INT_TAP: واجهة على 192.0.2.2 للوجهة:

```
<#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. تتم معالجة حزمة ACK هذه من SYN كجزء من الاتصال الموجود/المنشأ الذي يقوم على
إلى IP 169.254.1.2 من حزمة مصدر الترجمة NAT العكسية قاعدة بتطبيق Lina كرحم أساسه
س دكم مع ASA ب SSH اتصال حالة في .مخرج واجهة الداخل في ددحيو 192.0.2.1 الداخلي IP
إلى 22: رجوع 4122 من المصدر المنفذ ترجمة تمت ،Cisco SSH

```
<#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. Capture Point - تترك الحزمة الواجهة الداخلية نحو الوجهة:

```
<#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 win
```

تم تمكين الإدارة عبر واجهة البيانات

في حالة تمكين الإدارة عبر واجهة البيانات في برنامج الإرسال فائق السرعة (FTD) المدار بواسطة FMC، تحدث هذه التغييرات تلقائيا:

1. في CLISH، البوابة الافتراضية هي واجهة البيانات. تكون العبارة الافتراضية على Lina IP 169.254.1.1: التالية إلى الخطوة إلى الإشارة مع TAP_NLP عبر OS مستوى

```
<#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. وه اذه - تانايبلا ةهجاو لالخ نم هنيوكت مت يضارتفا راسم Lina ىلع دجوي ام ةداع
نيوكت المستخدم الذي تم نشره من 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

في دليل Lina، تم تثبيت دعاوق NAT نيترم ذفنمل sfTunnel 8305 لكل نم مزح IPv4 و3. IPv6. وبالإضافة إلى ذلك، للسماح بالاتصال نم ماظن التشغيل إلى الشبكات الخارجية، يتم تكوين برض ديناميكي لعناوين IPv4 و IPv6 الخاصة بواجهة ماظن التشغيل TAP_NLP ربع واجهة البيانات.

<#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

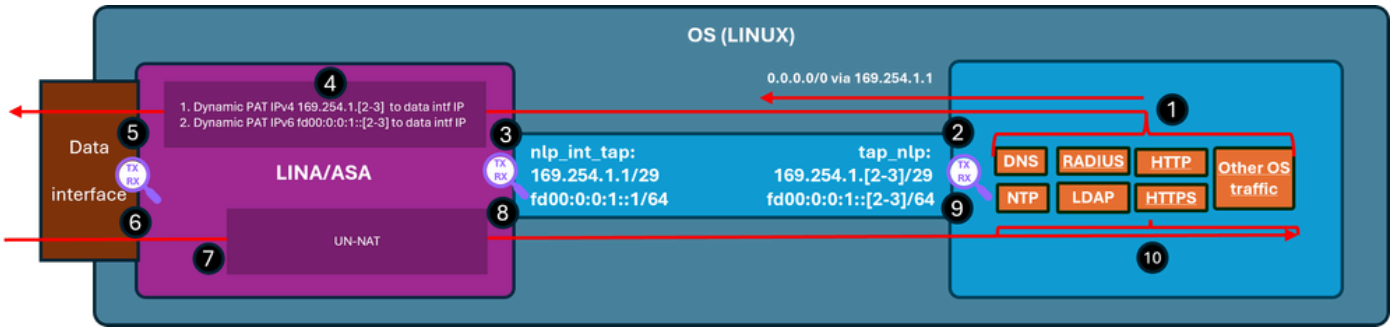
```
2 (nlp_int_tap) to (inside) source static nlp_server__sftunnel_::_intf3 interface ipv6  destination sta
translate_hits = 0, untranslate_hits = 0
```

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
```

يبدي هذا رسم بياني الربط ممر والمفتاح نقطة:



خطوات التحقق (في هذا المثال، خطوات التحقق هي لحركة مرور NTP. ينطبق نفس المنطق على أي حركة مرور تنتج عن نظام التشغيل، بما في ذلك الترخيص وما إلى ذلك):

1. يقوم عميل NTP بإنشاء حزمة موجهة لعنوان IP لخادم NTP الخارجي:


```
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
```

من منظور OS، تكون الخطوة التالية عبر واجهة tap_nlp باستخدام نفس واجهة IP 169.254.1.3 كعنوان المصدر:

```
<#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. TAP_NLP: واجهة من الحزمة إرسال يتم - التقاط نقطة

```
<#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. LINA NLP_TAP_INTERFACE: واجهة إلى الحزمة تصل - التقاط نقطة

```
<#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. قاعدة PAT، يحدد Lina الداخل كواجهة مخرج ثم يطبق قاعدة PAT. استنادا إلى بحث المسار، يحدد Lina الداخل كواجهة مخرج ثم يطبق قاعدة PAT. عنوان IP لواجهة ديناميكية التي تغير عنوان IP لمصدر الحزمة من 169.254.1.3 إلى عنوان IP لواجهة البيانات:

<#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:ج واجهة الخرو عبر إرسال الحزمة تم يتي - Capture Point

<#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:در حزمة NTP مرسل خادم ري - Capture Point

<#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

.7هذه إلى استناد . يعالج Lina الدرل جزء من الاتصالات المؤسسة ويطبق NAT العكسي
:nlp_int_tap هي واجهة المخرج ،169.254.1.3 إلى واجهة الوجهة ترجمة تتم ،المعلومات

<#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. التقاط نقطة - تم إرسال حزمة الرد عبر واجهة 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. التقاط نقطة - تصل حزمة إعادة التشغيل على واجهة TAP_NLP لنظام التشغيل:

```
<#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. تم إستهلاك حزمة الرد ومعالجتها بواسطة عميل NTP.

ملخص

تظهر واجهة OS /dev/net/tun/tap_nlp ك NLP_INT_TAP في Lina. الغرض من هذه الواجهة هو توفير الاتصال بين LINA ونظام التشغيل. تتم إدارة هذه الواجهة مع قواعد NAT المطلوبة تلقائيا بواسطة البرنامج والا تتطلب أي تدخل من المستخدم.

المراجع

- أدلة تكوين جدار الحماية الآمن

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).