و CLI مادختساب ASA ةمزح طاقتلا نيوكت ASDM

تايوتحملا

<u>ةمدقملا</u> <u>قيساسالا تابلطتملا</u> تابلطتملا <u>ةمدختسملا تانوكملا</u> <u>ةىساساً تامولعم</u> <u>نىوكتلا</u> <u>ةكبشلل ىطىطختلا مسرلا</u> تانىوكتلا <u>ASDM مادختساب مزحلا طاقتلا نيوكت</u> <u>(رماوألا رطس ةەجاو) CLI مادختساب مزحلا طاق تلا نىوكت</u> <u>ASA ىلع ةحاتملا طاقتلالا عاوناً</u> تاىضارتفالا <u>ةطقتلملا مزحلا ضرع</u> <u>ASA لا ىلع</u> <u>لاصتا نود ليلحتال ASA نم ليزنتاا</u> <u>طاقتلا حسم</u> <u>طاقتلا فاقىا</u> <u>ةحصلا نم ققحتلا</u> اهحالصإو ءاطخألا فاشكتسا

ەمدقملا

ةيامح رادج نيوكت ةيفيك دنتسملا اذه فصي Gisco ASA مي المح رادج نيوكت قيفيك دنتسمل الله فصي قبول طمل المزحل الما مادختساب CLI وأ CLI مادختساب

ةيساسألا تابلطتملا

تابلطتملا

ءارجإب CLI وأ Cisco ASDM ل حامسلل ەنيوكت متو لماكلاب لمعي ASA نأ ءارجإلا اذه ضرتفي نيوكتلا تارييغت.

ةمدختسملا تانوكملا

.ةغيص ةيجمرب وأ زاهج صاخ ىلاٍ ةقيثو اذه ديقي ال

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألاا نم دنتسملا اذه يف ةدراولا تامولعملا عاشنا مت. تناك اذا .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجألا عيمج تأدب رمأ يأل لمتحملا ريثأتلل كمهف نم دكأتف ،ليغشتلا ديق كتكبش.

ةلصلا تاذ تاجتنملا

:ةيلاتلا Cisco تاجتنم عم اضيأ نيوكتلا اذه مادختسإ متي

- ثدحألاا تارادصإلاو Cisco نم (5)9.1 تارادصإلا ASA
- Cisco ASDM، رادصإلا 7.2.1

ةيساسأ تامولعم

نم Cisco Adaptive Security Appliance (ASA) Next-Generation Firewall نيوكت ةيفيك دنتسملا اذه حضوي وأ Command وأ Cisco Adaptive Security Device Manager (ASDM) امإ مادختساب ةبولطملا مزحلا طاقتلا لجأ Line Interface (CLI) (ASDM).

ةبقارم وأ امحالصإو لاصتالا ءاطخأ فاشكتسال ةديفم ةمزحلا طاقتلا ةيلمع نوكت عاونأ ليلحتل ةددعتم تاطقل ءاشنإ نكمملا نم ،كلذ ىلإ ةفاضإلاب .ةەوبشملا ةطشنألا ةددعتم تامجاو ىلع رورملا ةكرح نم ةفلتخم.

نيوكتلا

اذه يف ةحضوملا ةمزحلا طاقتلا تازيم نيوكتل ةمدختسملا تامولعملا مسقلا اذه رفوي دنتسملا

ةكبشلل يطيطختلا مسرلا

يلاتال ةكبشلا دادعإ دنتسملا اذه مدختسي:



192.168.10.10/24

تانيوكتلا

اينوناق ليكشت اذه يف لمعتسي ةطخ ناونع سيل ip اي routable مه .تنرتنإلاا ىل routable اينوناق ليكشت اذه يف لمعتسي ةئيب ربتخم يف تلمعتسا نوكي نأ ناونع.

ASDM مادختساب مزحلا طاقتلا نيوكت

لاصتالا رابتخإ ءانثأ اهلاسرإ متي يتلا مزحلا طاقتلا يف اذه نيوكتلا لاثم مادختسإ متي (ةكبشلا جراخ) 1هجوملا يلإ (ةكبشلا لخاد) 1مدختسملا نم

ASDM: مادختساب ASA ىلع ةمزحلا طاقتلاا ةزيم نيوكتل تاوطخلا هذه لمكأ

1. حضوم وه امك ،ةمزحلا طاقتلا نيوكت ءدبل Wizards > Packet Capture Wizard ىلإ لقتنا:



2 - Capture Wizard رقنا .حتفي Next.

| Capture Wizard | |
|-----------------------|--|
| Packet Capture Wizard | Overview of Packet Capture (Step 1 of 6) |
| Q. | Use this wizard to configure and run capture. The wizard will run one capture on each of the ingress and egress interfaces. After capturing you can save the captures to your PC for examination or replay in a packet analyzer. The wizard will guide you through the following tasks: |
| | Select an ingress interface. Select an egress interface. Set the buffer parameters. Run the captures. Save the captures to your PC (optional). |
| | Egress |
| | < Back Next > Finish Cancel Help |

رورم ةكرح طاقتلاا يف اهمادختسإ متي يتلا تاملعملا ريفوتب مق ،ةديدجلا ةذفانلا يف 3.0 لخدملا.

متيس يتلا مزحلل ةمجولاو ردصملل IP نيوانع رفوتو Ingress Interface لجأ نم inside ديدحت 3.1 .ةمدقملا ةلباقملا ةحاسملا يف ،اهب صاخلا ةيعرفلا ةكبشلا عانق عم ،اهطاقتلا

ةراتخملا ةمزحلا عون وه ASA (IP ةطساوب اهيلع ءاليتسالا متيس يتلا ةمزحلا عون رتخأ 3.2 حضوم وه امك ،(انه:

| Capture Wizard | | | | X |
|-----------------------|-------------------------|------------------|----------------------------|-------------------|
| Packet Capture Wizard | Ingress Traffic Selecto | r (Step 2 of 6) | | |
| A State of the second | Point of Ingress | | | |
| and the second | Select interface: | inside 👻 | | |
| | Use backplane cha | annel | | |
| 120 | | Ingress | | |
| and the second | -+ | | <u> </u> | |
| | | inside | | ' |
| | Packet Match Criteria - | | | |
| 100 m | Select access list: | botnet-exclude + | Manage | |
| 14 JA 1 | Specify packet pa | rameters | | |
| | Source Host: | 192.168.10.10 | Source Network: | 255.255.255.255 + |
| | Destination Host: | 203.0.113.3 | Destination Network: | 255.255.255.255 • |
| The | Protocol: | ip - | • | |
| IT AT | | | | |
| | | | | |
| 9.21 | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | <back next=""> Fini</back> | sh Cancel Help |
| | | | | |

.3.3 رقنا Next

ةكبشلا عانق عم ،ةەجولاو ردصملا IP نيوانع رفوتو Egress Interface لجأ نم outside ديدحت 4.1 ةمدقملا ةلصلا تاذ تاغارفلا يف ،اەب صاخلا ةيعرفلا.

If Network Address Translation (NAT) اضيأ رابتعإلا نيعب كلذ وذخ و "ةيامحلا رادج" ىلع.

| Capture Wizard | | | × |
|--|----------------------------------|----------------------|-------------------|
| Packet Capture Wizard Egress Traffic Se | elector (Step 3 of 6) | | |
| Point of Egress | | | |
| Select inte | erface: outside 🔍 💌 | | |
| Use backg | slane channel | | |
| A CONTRACT | | Egress | |
| and the second | + | <u> </u> | -+ |
| 1 ton | | outside | <u>نه</u> |
| Packet Match Cr | riberia | | |
| O Select acc | tess list: [botnet-exclude +] [N | Manage | |
| Specify pi | acket parameters | | |
| Source Ho | st: 192.168.10.10 | Source Network: | 255.255.255.255 - |
| Destinatio | n Host: 203.0.113.3 | Destination Network: | 255.255.255.255 - |
| Protocol: | (p v | | |
| The state of the s | | | |
| | | | |
| 0.91 | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | G | < Back Next > Fini | h Cancel Help |
| | | | |

.0 رقنا 4.2 Next

تانايبلا هذه .اهنم لكل صصخملا زيحلا يف Buffer Size و Packet Size بسانملا مقرلا لخدأ 5.1 طاقتلالا ثدحي يتح ةبولطم.

5.2 نم ققحت Use circular buffer ةتقۇملا نزاخملا .يرى اد تقۇم نزخم رايخ مادختسال عبرم ادبأ اەؤلم متي ال ةيرى؛ادلا.

طاقتلالا رمتسيو مدقألا تانايبلا لهاجت متي ،هل مجح ىصقأ ىلٍ تقوْملا نزخملا لوصو عم.

رايتخالا ةناخ ديدحت متي مل كلذل ،يرىءد تقؤم نزخم مادختسإ متي ال ،لاثملا اذه يف.



.5.3 رقنا Next

6. 0 لا عن عنك عنك عنك يغبني نأ ASA (so that the لا عن عنك عن الكش تنك يغبني نأ Access-lists المن من ع المن عن لااثم اذه يف تطقتلا نوكي طبر (ip) ضبق نوكي نأ طبرلا عونو (تطقتلا نوكي).

.0 رقنا 8.1 Next



7. حضوم وه امك ،ةمزحلا طاقتلا ءدبل Start قوف رقنا:

| Capture Wizard | | | | s | |
|-----------------------|--|------------|------------------------------------|-----|--|
| Packet Capture Wizard | Run Captures (Step 6 of 6) | | | | |
| - 200.000 | Click the Start button to begin capturing. | | | | |
| Q | Start | Stop | Get Capture Buffer | | |
| | Ingress: inside | | Launch Network Sniffer Application | | |
| P.A. | | | | | |
| | | | | | |
| | | | | | |
| Sec. 1 | | | | | |
| -Harris | | | | | |
| | | | | - 0 | |
| 2 Juli IIII | Egress: management | | Launch Network Sniffer Application | - 1 | |
| The | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | Sav | e captures | Clear Buffer on Device | -1 | |
| | | , | | | |
| | | | Conce Pep | | |

متي ىتح ةيلخادلا ةكبشلا نم ةيجراخلا ةكبشلا لاصتا رابتخإ لواح ،ةمزحلا طاقتلا ءدب عم تقؤملا نزخملا ةطساوب IP نيوانع ةهجولاو ردصملا نيب قفدتت يتلا مزحلا طاقتلاا ASA. طاقتلال

8. طاقتلال تقوْملا نزخملا ةطساوب اهطاقتلا متي يتلا مزحلا ضرعل Get Capture Buffer رقنا ASA.

| 🖆 Capture Wizard | 2 |
|-----------------------|---|
| Packet Capture Wizard | Run Captures (Step 6 of 6) |
| • | Start Stop Get Capture Buffer Click the Start button to begin capturing. Ingress: inside Launch Network Sniffer Application |
| | |
| 1 Detter | Egress: outside Launch Network Sniffer Application |
| | |
| | Save captures Clear Buffer on Device |
| | < Back flext > Finish Cancel Help |

جورخلاو لوخدلا رورم ةكرح نم لكل ةذفان اذه يف ةطقتلملا مزحلا رهظت.

9. رقنا Save captures رقنا.

| Capture Wizard | | | | | × |
|-----------------------|-----------------------------|-----------------------|------------------|------------------------------------|-------------|
| Packet Capture Wizard | Run Captures (Step 6 | of 6) | | | |
| A PROPERTY OF TAXABLE | Click the Start button to b | regin capturing. | | | |
| · A ANGER | | Start | itoo 🔽 | Get Capture Buffer | |
| Q | | | | | |
| | Ingress | i inside | | Launch Network Sniffer Application | |
| 1014 | 1:03:58:37.845262 | 192.168.10.10 > 20 | 3.0.113.3: icm; | p: echo request | |
| and the second | 2: 03:58:37.845903 | 203.0.113.3 > 192.1 | 168.10.10: icm | p: echo reply | |
| | 3: 03:58:37.846941 | 192.168.10.10 > 20 | 0.0.113.3: icm | p: echo request | |
| | + 03:58:37.847520 | 203.0.113.3 > 192.1 | 168.10.10: icm | p: echo reply | |
| | 5: 03:58:37.848299 | 192.168.10.10 > 20 | 3.0.113.3: icmp | p: echo request | |
| and the second second | 6: 03:58:37.848665 | 203.0.113.3 > 192.1 | 168.10.10: icm | p: echo reply | |
| | 7: 03:58:37.849443 | 192, 168, 10, 10 > 20 | 3.0.113.3: icm | p: echo request | |
| and the second | 8: 03:58:37.849824 | 203.0.113.3 > 192.1 | 168.10.10: icm | p: echo reply | |
| St. St. | 9: 03:58:37.850618 | 192, 168, 10, 10 > 20 | 3.0.113.3: icmp | p: echo request | |
| | 10: 03:58:37.850984 | 203.0.113.3 > 192. | 168, 10, 10; icm | rp: echo reply | |
| | 11:03:58:38.868302 | 192.168.10.10 > 20 | 03.0.113.3: ion | ip: echo request | |
| | 12:03:58:38.868897 | 203.0.113.3 > 192. | 168.10.10: km | ip: echo reply | * |
| The | Egress: | outside | | Launch Network Sniffer Application | |
| | 1:03:58:37.845491 | 192, 168, 10, 10 > 20 | 3.0.113.3: icm | p: echo request | |
| | 2: 03:58:37.845873 | 203.0.113.3 > 192.1 | 168.10.10: icm | p: echo reply | |
| | 3: 03:58:37.847139 | 192.168.10.10 > 20 | 3.0.113.3: icm | p: echo request | |
| | 4: 03:58:37.847490 | 203.0.113.3 > 192.1 | 168.10.101 kmg | pi echo reply | - |
| | 5:03:58:37.848314 | 192.168.10.10 > 20 | 3.0.113.3: icmp | p: etho request | 1 |
| | 6:03:58:37.848634 | 203.0.113.3 > 192.1 | 168.10.10: icm | p: echo reply | |
| | 7: 03:58:37.849458 | 192.168.10.10 > 20 | 3.0.113.3: icm | p: echo request | |
| | 8: 03:58:37.849794 | 203.0.113.3 > 192.1 | 168.10.10: icm | p: echo reply | |
| | 9:03:58:37.850648 | 192.168.10.10 > 20 | 0.0.113.3: icm | p: echo request | |
| | 10: 03:58:37.850953 | 203.0.113.3 > 192. | 168, 10, 10; km | p: echo reply | |
| | 11:03:58:38.868500 | 192.168.10.10 > 20 | 3.0.113.3: ion | rp: echo request | |
| | 12:03:58:38.868866 | 203.0.113.3 > 192 | 168.10.10: KM | no: echo reply | |
| | | Save captu | res | Clear Buffer on Device | |
| | | | | <back next=""> Finish</back> | Cancel Help |

اطاقتلالا نزخم ظفح متيس يذلا بولطملا قيسنتلا رتخأ Save captures عقوم نم 1. ەب تقۇملا.

.قيسنتالا عامسأ راوجب دوجومال رايخال رز رقنا .PCAP وأ ASCII امإ هذه 10.2

.بولطم وه امك Save egress capture وأ Save ingress capture رقنا مث 10.3

.ةلضفملا ةقيرطلا يهو ،Wireshark لثم ،طاقتلالا للحم مادختساب PCAP تافلم حتف نكمي

| 🖆 Save Captures 🛛 🚺 |
|--|
| ASCII PCAP Save the buffer in the specified format to the localhost. |
| Save egress capture |
| |
| Close Help |

فلم ظفح متي ثيح ناكملاو فلملا مسا ريفوتب مق ،ةذفان Save capture file عقوم نم 11.1 طاقتلالا.

.Save رقنا 11.2

| Save capture f | ile | | | | ? 🛛 |
|------------------------|-----------------------------|----------------------------|---|----------|----------------|
| Save in: | Capture data | | • | 🗢 🗈 💣 📰• | |
| My Recent Documents | | | | | |
| My Documents | | | | | |
| My Computer | | | | | |
| My Network Places | File name: Save as type: | ingress All Files (".") | | • • | Save Cancel |

12. رقنا Finish.



قمزح طاقتلا ءارجإ لامتكا ىلإ اذه يدؤي GUI.

(رماوألا رطس ةەجاو) CLI مادختساب مزحلا طاقتلا نيوكت

:CLI لا عم ASA لا ىلع ةمس طاقتلا طبرلا تلكش steps in order to اذه تمتأ

- ةكبشلل يطيطختلا مسرلا يف حضوم وه امك ةيجراخلاو ةيلخادلا تاهجاولا نيوكتب مق .1 نامألا تايوتسمو حيحصلا IP ناونع مادختساب.
- يف .تازايتمالا يذ EXEC عضو يف capture رمألا مادختساب ةمزحلا طاقتلا ةيلمع أدبا .2 ،**يلخاد** نراقلا ىلإ مطبر .**capin** ىمسملا طاقتلالا فيرعت متي ،اذه نيوكتلا لااثم ةدئافلا رورم ةكرحلا قباطي نأ طبرلا طقف نأ حاتفملا ةملكلا **match ا**عم تنيعو تطقتلاا :

ASA# capture capin interface inside match ip 192.168.10.10 255.255.255.255 203.0.113.3 255.255.255

3. تنيعو ،**يڃراخ** نراقلا ىلإ ەطبر .**capout** ىمسملا طاقتلالا فيرعت متي ،لثامم وحن ىلعو تطقتلا ةدئافلا رورم ةكرحلا قباطي نأ طبرلا طقف نأ حاتفملا ةملكلا **match ي**عم:

ASA# capture capout interface outside match ip 192.168.10.10 255.255.255.255 203.0.113.3 255.255.255.255

أدبي عاقتلال فاقيإل .تاهجاولا نيب رورملا ةكرح قفدت طاقتلا يف نآلا ASA أدبي طاقتلالا مساب اعوبتم no capture رمألا لخدأ ،تقو

:لاثم يلي اميف

no capture capin interface inside no capture capout interface outside

ASA ىلع ةحاتملا طاقتلالاا عاوناً

.ASA لا ىلع رفوتي نوكي نأ طاقتلالا عون فلتخم مسق اذه فصي

• asa_dataplane - ةدحوو ASA نيب رمت يتلا ASA قيفلخلا ةحوللا ىلع طبر ضبق ىلع ASA • ASA • متي ماي ASA • ASA تقدحوو لثم ،قيفلخلا قحوللا مدختست.

```
ASA# cap asa_dataplace interface asa_dataplane

ASA# show capture

capture asa_dataplace type raw-data interface asa_dataplane [Capturing - 0 bytes]

• asp-drop دوك drop - مزحلا طقتلي مزحلا طقتلي .

عيرسلا نامألا راسم لالخ نم اهطاقسا متي يتلا رورملا قكرح عون طاقسإلا قرفشلا
```

```
ASA# capture asp-drop type asp-drop acl-drop
ASA# show cap
ASA# show capture asp-drop
```

2 packets captured

1: 04:12:10.428093 192.168.10.10.34327 > 10.94.0.51.15868: S 2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop) Flow is denied by configured rule 2: 04:12:12.427330 192.168.10.10.34327 > 10.94.0.51.15868: S 2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop) Flow is denied by configured rule 2 packets shown

ASA# show capture asp-drop

2 packets captured

1: 04:12:10.428093 192.168.10.10.34327 > 10.94.0.51.15868: S 2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop) Flow is denied by configured rule 2: 04:12:12.427330 192.168.10.10.34327 > 10.94.0.51.15868: S 2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop) Flow is denied by configured rule 2 packets shown

• ethernet-type ا تانرثيإلاا عاوناً نامضتت .طاقتلالل Ethernet عون ددجي - عونلا عاوناً نامضتت .طاقتلال قاموعدمل و ،ARP و ،RAP و ،RAP و ،VLAN و ،VLAN و ،VLAN

:ARP رورم ةكرح طاقتلا ةيفيك لااثملا اذه حضوي

```
ASA# cap arp ethernet-type ?
 exec mode commands/options:
  802.10
  <0-65535> Ethernet type
  arp
  ip
  ip6
  pppoed
  pppoes
  rarp
  vlan
 cap arp ethernet-type arp interface inside
 ASA# show cap arp
 22 packets captured
 1: 05:32:52.119485 arp who-has 10.10.3.13 tell 10.10.3.12
 2: 05:32:52.481862
                         arp who-has 192.168.10.123 tell 192.168.100.100
 3: 05:32:52.481878 arp who-has 192.168.10.50 tell 192.168.100.10
 4: 05:32:53.409723 arp who-has 10.106.44.135 tell 10.106.44.244
 5: 05:32:53.772085 arp who-has 10.106.44.108 tell 10.106.44.248
 6: 05:32:54.782429 arp who-has 10.106.44.135 tell 10.106.44.244
 7: 05:32:54.784695 arp who-has 10.106.44.1 tell xx.xx.xx.xx:
يف ةمزح طاقتلاا ءاهنإل .يلعفلاا تقولاا يف رارمتساب ةطقتلملا مزحلا ضرعي - real-time •
 نم no ةغيصلا مدختساً ،مئاد لكشب طاقتلالا ةلازل .Ctrl-C ىلع طغضا ،يلعفلا تقولاً
 رمالا اذه.
```

• مادختسإ دنع راىخلاا اذه معد متى ال ciuster exec capture erasecat4000_flash:.

ASA# cap capin interface inside real-time

Warning: using this option with a slow console connection may result in an excessive amount of non-displayed packets due to performance limitations. Use ctrl-c to terminate real-time capture

• Trace - قمزح بقعتم ةزيمل ةلثامم ةقيرطب اهيلع ءاليتسالا مت يتلا مزحلا عبتتي ASA.

ASA#cap in interface Webserver trace match tcp any any eq 80 // Initiate Traffic 1: 07:11:54.670299 192.168.10.10.49498 > 198.51.100.88.80: S 2322784363:2322784363(0) win 8192 <mss 1460, nop, wscale 2, nop, nop, sackOK> Phase: 1 Type: CAPTURE Subtype: Result: ALLOW Config: Additional Information: MAC Access list Phase: 2 Type: ACCESS-LIST Subtype: Result: ALLOW Config: Implicit Rule Additional Information: MAC Access list Phase: 3 Type: ROUTE-LOOKUP Subtype: input Result: ALLOW Config: Additional Information: in 0.0.0.0 0.0.0.0 outside Phase: 4 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-group any in interface inside access-list any extended permit ip any4 any4 log Additional Information: Phase: 5 Type: NAT Subtype: Result: ALLOW Config: object network obj-10.0.0.0 nat (inside, outside) dynamic interface Additional Information: Dynamic translate 192.168.10.10/49498 to 203.0.113.2/49498 Phase: 6 Type: NAT Subtype: per-session Result: ALLOW

Config: Additional Information: Phase: 7 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Phase: 8 Type: Subtype: Result: ALLOW Config: Additional Information: Phase: 9 Type: ESTABLISHED Subtype: Result: ALLOW Config: Additional Information: Phase: 10 Type: Subtype: Result: ALLOW Config: Additional Information: Phase: 11 Type: NAT Subtype: per-session Result: ALLOW Config: Additional Information: Phase: 12 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Phase: 13 Type: FLOW-CREATION Subtype: Result: ALLOW Config: Additional Information: New flow created with id 41134, packet dispatched to next module Phase: 14 Type: ROUTE-LOOKUP Subtype: output and adjacency Result: ALLOW Config: Additional Information: found next-hop 203.0.113.1 using egress ifc outside adjacency Active next-hop mac address 0007.7d54.1300 hits 3170

output-interface: outside output-status: up output-line-status: up Action: allow

طقتلت .طقف IPv4 نيوانعب مزحلا ةيساسأ ةملك يأ طقتلت ،+ASA 9.10 يف :**قظحالم** لوكوتورب ربع اهتجلاعم متي يتلا تانايبلا رورم ةكرح any6 قيساسألا ةملكلا

مزحلا طاقتلا مادختساب اەنيوكت نكمي ةمدقتم تادادعإ ەذە.

اەنييعت ةيفيك لوح رماوألل يعجرملا ليلدلا ةعجارم ءاجرلا.

- ikev1/ikev2 وأ (IKEv1) وأ (IKEv1) رادصإلا Internet Key Exchange لوكوتورب تامولعم طقتلي (IKEv1) ولالالاv1. طقف.
- isakmp حيتافملا ةرادإ لوكوتوربو تنرتنإلا نامأ نارتقا رورم ةكرح طاقتلا ىلع isakmp ةقبطلا تالوكوتورب ىلإ لوصولا قح يعرفلا ISAKMP ماظن كلتمي ال VPN تالاصتال للحم ءاضرال ةعمتجم UDP و IR ،ةيداملا تاقبطلا عم ،فئاز طاقتلا وه طاقتلالاا .ايلعلا IP. ققبط يف اهنيزخت متيو SA لدابت نم ريظنلا نيوانع ىلع لوصحلا متي PCAP
- اacp امت اذإ (LACP) تاطابترالا عيمجت يف مكحتلا لوكوتورب رورم ةكرح طاقتلا عم لمعت امدنع ديفم اذهو .يلعفلا ةهجاولا مسا وه ةهجاولا مسا نإف ،اهنيوكت EtherChannels in order to لا يلاحل كولسلا تنيع LACP.
- ة المأ ليكو نم اهريفشت كف مت يتلا ةرداصلاو ةدراولا تانايبلا طاقتلا tls-proxy رثكاً وأ ةدحاو ةمجاو يلع (TLS) لقنلا.
- webvpn لاصتال WebVPN تانايب طاقتلا.

ليطعت نم دكأت .نامألاا زاهج ءادأ ىلع كلذ رثؤي ،WebVPN طاقتلاا نيكمت دنع :**ريذحت** ءاطخألا فاشكتسال ةبولطملا طاقتلالاا تافلم ءاشنإب موقت نأ دعب طاقتلالاا اهحالصإو.

تايضارتفالا

:ASA ماظنل ةيضارتفالا ميقلا يه هذه

- . ماخ تانايب وه يضارتفالا عونلا
- . تيابوليك 512 وه يضارتفالا تقؤملا نزخملا مجح •
- . IP مزح وه يضارتفالا تنرثيإ عون •
- . تياب 1،518 وه يضارتفالا ةمزحلا لوط •

ةطقتلملا مزحلا ضرع

ASA لا ىلع

رفوي .مسإ capture لا معبتي رمأ طاقتلا ضرعلا ،ضبق ىلع طبرلا تدماش in order to تلخد مألا ضرعي .طاقتلالل تقؤملا نزخملا تايوتحمل show رمألا تاجرخم مسقلا اذه capin: ىمسملا طاقتلالل تقؤملا نزخملا تايوتحم رمألا ضرعي capin

ASA# show cap capin

8 packets captured

1: 03:24:35.526812 192.168.10.10 > 203.0.113.3: icmp: echo request 2: 03:24:35.527224 203.0.113.3 > 192.168.10.10: icmp: echo reply 3: 03:24:35.528247 192.168.10.10 > 203.0.113.3: icmp: echo request 4: 03:24:35.528582 203.0.113.3 > 192.168.10.10: icmp: echo reply 5: 03:24:35.529345 192.168.10.10 > 203.0.113.3: icmp: echo request 6: 03:24:35.529681 203.0.113.3 > 192.168.10.10: icmp: echo reply 7: 03:24:57.440162 192.168.10.10 > 203.0.113.3: icmp: echo request 8: 03:24:57.440757 203.0.113.3 > 192.168.10.10: icmp: echo reply

:capout ىمسملا طاقتلالل تقۇملا نزخملا تايوتحم رمالا ضرعي show capture capout رمألا ضرعي

ASA# show cap capout

8 packets captured

1: 03:24:35.526843 192.168.10.10 > 203.0.113.3: icmp: echo request 2: 03:24:35.527179 203.0.113.3 > 192.168.10.10: icmp: echo reply 3: 03:24:35.528262 192.168.10.10 > 203.0.113.3: icmp: echo request 4: 03:24:35.528567 203.0.113.3 > 192.168.10.10: icmp: echo reply 5: 03:24:35.529361 192.168.10.10 > 203.0.113.3: icmp: echo request 6: 03:24:35.529666 203.0.113.3 > 192.168.10.10: icmp: echo reply 7: 03:24:47.014098 203.0.113.3 > 203.0.113.2: icmp: echo request 8: 03:24:47.014510 203.0.113.2 > 203.0.113.3: icmp: echo reply

لاصتا نود ليلحتلل ASA نم ليزنتلا

لاصتا نود ليلحتال ةمزحلا طاقتال ليزنتل ناتقيرط كانه:

1. حفصتم يأ ىلع<u>https://<ip_of_asa>/admin/capture/<capture_name>/pcap</u> ىلإ لقتنا.

ريفوت متي show capture نم طقف ئفاكملا مث ،ةيساسألا ةملكلا pcap تكرت اذإ :**حيملت** رمألا جارخإ.

:طاقتلاال ليزنتل كيدل لضفملا تافلملا لقن لوكوتوربو copy capture رمألا لخدأ .1

copy /pcap capture:<capture-name> tftp://<server-ip-address>

يصوت ،مزحلا طاقتلا مادختساب اهحالصإو ام ءاطخاً فاشكتساً دنع :**حيملت** لاصتا نود ليلحتلل طاقتلالا تايلمع ليزنتب.

طاقتلا حسم

: clear capture لخدأ ،تقۇملا طاقتلالا نزخم حسمل

```
ASA# show capture
capture capin type raw-data interface inside [Capturing - 8190 bytes]
match icmp any any
capture capout type raw-data interface outside [Capturing - 11440 bytes]
match icmp any any
```

ASA# clear cap capin

ASA# clear cap capout

ASA# show capture capture capin type raw-data interface inside [Capturing - 0 bytes] match icmp any any capture capout type raw-data interface outside [Capturing - 0 bytes] match icmp any any clear capture /all أرمأ in order to أin order to أin order to أ

ASA# clear capture /all

طاقتلا فاقيإ

:رمألا اذه مادختساب لماكلاب هليطعت يه ASA ىلع طاقتلاا فاقيإل ةديحولا ةقيرطلا

no capture <capture-name>

ةحصلا نم ققحتلا

نيوكتلا اذه ةحص نم ققحتلل ءارجإ اًيلاح دجوي ال.

اهحالصإو ءاطخألا فاشكتسا

ليكشت اذه ل رفوتي ةمولعم اهحالصإو ءاطخألاا فاشكتسأ صاخ نم ام ايلاح كانه.

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما