

# في DNS/PTR ن ع ثحبالا ةمزح ةيؤر لكاشم FTD 7.4 ةمزح تاطقل

## ةلأسم

(FTD) ةيامحلل رادج ديدهت ةيامح ةمزح طاقتلل ضرعي ال ،نامألا تامولعم ةطساوب اهرطح دن ع رهظت .FTD نامأ تامولعم ةطساوب اهرطح متي يتللا ةراضللا تالاجملل لىل DNS تامالعتسا موقى يذلا DNS مداخل نم تانايبلا رورم ةكرح FTD قاطنللا لىل ةدوجومللا لاصتالا ثادحأ تامولعم ربع هذه مالعتساللا تاباجتسا رطح موقى FTD نأ دكؤتو لاجملل ن ع مالعتسالاب ريغ FTD لىل لوصوللا جهن ةدعاق لىل قباطت اضياأ ثدحلل سفن رهظي ،كلذ عم و .نامألا تامولعم شح م مزلح لعافت ةيفيكب قلعتت ةلكشملا نأ رهظي .يجذومن لكشب ةعقوتم اذرهظي نأ نكمي .ةراضللا لاجملل تامالعتسا رطح دن ع FTDS لىل DNS (سكع) PTR و نامألا ةينمألا تارابختساللا لوصوللا ةدعاق نيلامتجاللا الك قباطي ائدح

## ةئيبللا

- لباق) (Firepower (FMC) / CDfmc / FDM ةرادا زكرم) Cisco Secure Firewall Firepower 7.4 (نامألا ءاكذ مدختست يتللا ةمظنألا عيجم لىل قيبطتلل)
- مدختست يتللا ةمظنألا عيجم لىل قيبطتلل لباق) (7.4.2 / 7.4.2.4 :جمانربلا رادصا (ةينمأ تامولعم)
- نيب قاطنللا ي ف دوجومللا FirePOWER نامأ زاهج ةبقارمب ةصاخلا DNS تانايب رورم ةكرح CIRA ةباحسو InfoBlox DNS مداخل
- DNS ريفشت ن ع بيقننتلا تاديدهت رطلل نامألا تامولعم نيوكت
- جاتنالا ةداعل FPR2100 و FPR2110 ةزهجأ نمضتي يللمعم ططخم
- static.vdc.vn :لاجملل فدهتسي يذلا DNS مالعتسا
- تاقاطنللا ءامسأ ماظنل رفشملل نيدهتلا ديدهت :ديدهتلا فينصت
- FirePOWER زاهج لىل لاصتالا او مزلحلا طاقتللا ثادحأ ليلحت
- ةيلخاد DNS ةينبك InfoBlox DNS مداخل

## رارق

1. لىل DNS مداخل نم DNS تاراسفتسا رطح ديكاأتل FTD لىل لاصتالا ثادحأ ليلحتب مق 1.

IP ناونع ةظحالم متي .راض لاجم دوجو ببسب "نامألا تامولعم" لبق نم يجرالال لاجملا يتلا لوصولا ةسايس ةدعاق ىلع قباطت عضو ثدحلل نكميو ةدحمالا ةهوجل او رصملا لاضيا هسفن ثدحل رهظي ،كلذ عمو .ةهوجل ىلا رصملا نم PTR ل يلوألا ثحب لابل حمست حضاو لكشب مالعست لال URL ناونع ديدحت ءانثا ةروظحم ةينمأ تامولعم

لاصتا ا شح

للاثم:

vdc.vn.يكي تاتسا نكاس :لاجملا  
DNS ريفشت نيديعت ديدعت) روظحم :ءارجالا

2. في .ةلصلال تاذ IP نيوانع نيب DNS رورم ةكرح فدهتسي يذلا FTD ىلع ةمزح طاقنلا ادبا .  
DNS مالعستسا ىلع روثلعل متي مل ،يلصلال IP ناونع نم طاقنلال Wireshark ليلحت  
ةمزحل طاقنلال جارخا في راضلال لاجملا لاصيصخ

EQ 53 فيضملا SRCIP UDP فيضملا ةقباطملا CAP ةهجاو ىلع FTD#

(ةعقوتملا مزحلل جارخا دجوي ال)

- في مكحتلا نم ةركبم ةلحرم نامألا تامولعم ةيفصت نوكت ،Cisco قنائلول اقفو  
ديزم لبق اهطاقسا نكمي ،ةينمأ تامولعم ةلتك ةمئاق عم ةمزح تقباطت اذا .لوصولا  
،لوصولا في مكحتلا كلذ في امب) ىرخأ تاسايس ةطساوب اهتجالعم لبقو وصحفال نم  
(DNS صحفو ،مزحل طاقنلالو
  - .ةريثك دراوم بلطتي يذلا صحفال لبق نامألا تامولعم ةيفصت متي
  - ةطساوب نامألا تامولعم ةطساوب ةروظحملا مزحل طاقنلال ايجألا ضعب في متي ال  
زاهجال ىلع ةيسايقلا مزحل طاقنلال تايلا
  - .ةيورلا ىلع اضيا نامألا ءاكذ رثوي نأ لبق قبسمل ةيفصتلا لماع دعاوق ميريقت مت
3. نيب PTR شحب تايلمع عبنتل FTD ل CLISH في system support url-si-debug رمالا مدختسا .  
FTD لخاد اهرظحو رورملا ةكرح ةجالعم متت نيأو ةيفيكمه فل ةهوجل او رصملا IP نيوانع  
مزحلل رصملا ذفانم ةظحالمو

url-si-debug ماطنلا معد >

```
SRCIP 37046 -&gt;: DSTP 53 17 as=0 id=39 gr=1-1 InsightDnsListEventHandler:  
num_list_match [1], status 0x00010000, insight_find (0x00010000) | SHMDB (1), static.vnpt.vn,  
si_list [ 1048652]  
SRCIP 49094 -&gt;: DSTP 53 17 as=0 id=42 gr=1-1 InsightDnsListEventHandler:
```





ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب  
Cisco ةللخت. فرتمة مچرت مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او  
ىل إلمءءاد ءوچرلاب ةصوء و تاملرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةلصلأل ةزىل ءنل اءل دن تسمل