

7.7.0 نمآال ةياملال رادج ي ف DNS ةيامل م ه ف

تايوتحملال

[قمدقملا](#)

[ةيساسال تابلطتملا](#)

[تابلطتملا](#)

[قمدختسملا تانوكملا](#)

[ةيساسا تامولعم](#)

[قباسل رادصلال عمقنراقم](#)

[قديجلال تازيملال](#)

[صيخرتلال، قوموعدملا ةيساسال ةمظنألال: تايساسالال](#)

[FTD يريدمو ةيساسال ةمظنألال](#)

[يخرألال معدلابلناوچ](#)

[قلكشملا](#)

[قلكشملا عاشنل ةداعلا تاوطخ](#)

[لحلل](#)

[قزيملا علع قماع قرظن](#)

[اهالصل او عاوطخلال فاشكتسا](#)

قمدقملا

ىلع زيكرتلال عم، 7.7.0 "نمآال ةياملال رادج" ي ف "DNS ةيامل" ةزيم دنتسملال اذه فصى
اهالصل او هئاطخأ فاشكتساو هئاطو.

ةيساسال تابلطتملا

تابلطتملا

ةيلاتل عيضاوملاب ةفرعم كي دل نوكت ناب Cisco ي صوت:

- UDP لمع تاسلج و DNS لوكوتورب م ه ف
- هتاسلج ةراداو Snort 3 ىلع فرعتل

قمدختسملا تانوكملا

ةيلاتل ةياملال تانوكملا وچماربلال تارادصلال ىل دنتسملال اذه ي ف ةدراوال تامولعملال دنتست:

- 7.7.0 رادصلال (FTD)، نمآال ةياملال رادج ديدت دض عافدل
- 7.7.0 رادصلال (FMC)، Firepower ةرادا زكرم
- 3 رادصلال ترون

ةصاخ ةيلمعم ةئيب ي ف ةدوچوملا ةزهجال نم دنتسملال اذه ي ف ةدراوال تامولعملال عاشنل مت

تتأكد إذا (يضايرفأ) حوسمم نيوكتب دنسسما اذه يف ةمدختسُما ؤزهأاا عيمج تأدب رما يال لمتحملا ريثأااا ل كمهف نم دكأاا ف، ليغشأاا دي ق كاكبش

ةيساسأ تامولعم

ال Lina فالخب .رمعلا ؤريصق تاسلج عم UDP بلط ؤباجأاا إاا دنساي لوكتورب وه DNS ااا قنن مأي ،كلاذ نم الديو .DNS ؤباجأااا دعب اروف 3 Snort يف DNS تاسلج حسم مأي مكارأاا إاا كلاذ يديو .رأاا وأ ؤيناا 120 غلبأا قفأا ؤلهم إاا اأانأاا DNS ل مع تاسلج .إأااا UDP وأ TCP اااااااا كلاذ فالخب همأاأااا نكمي يأااا ،يروضالا ريغ ؤسلأاا

قبااالا راءااالا عم ؤنراقم

In Secure Firewall 7.6 and Below		New to Secure Firewall 7.7
The DNS session remains as a stale Snort 3 flow until it is pruned by the UDP timeout.		DNS sessions in Snort 3 are released immediately after the DNS Response is inspected and handled.

7.7 يف ؤايأا ؤزيم

ةايأااا تااااا

- ؤباجأااا ؤمزا مالاأااا دعب ؤرأااا UDP قفأا حسم إاا هأا "DNS ؤيأا" ؤزيم ل معأا .اهصأاا DNS
- Snort 3 ل نايلاأاا لاكيهلل او ميأااااا إاا ل لوكتوربلاا صأا نيسأاا اذه

صااأااا ،ةموءااا ؤيساسأاا ؤمأاااا :أااااااا

FTD يريأاا ؤيساسأاا ؤمأاااا

FTD Platforms	All
FMC on 7.7.0 FMC Rest API	Yes No
FTD Supported Versions (lowest version FMC on 7.7.0 can manage is 7.2)	7.7.0 only
Snort Support (Snort 3 is the only Snort version supported in 7.7)	Snort 3

ةموءااا ؤيساسأاا ؤمأاااا

ىرخأل معدلأ ب نأوج

FTD	
Licenses Required	Essentials, URL, Threat, Malware
Works in Evaluation Mode	Yes
IP Addressing	IPv4 IPv6
Multi-instances supported?	Yes
Supported with HA'd devices	Yes
Supported with clustered devices?	Yes
Other (only routed mode transparent mode), etc.	No Special Notes

قفاوتلأو صيخرتأل

ةلكشمأل

DNS لمع ةسلج لظت ،هذعب امو 7.6 نمألأ ةيأمأل رادج ةصأخو ،ةقبأسلأ تارادصلأل ي ةرادإ ي ف لكأشم كلذب بسويو .UDP ةلهم ةطساوب أهي قنت متي ىتح مي دق Snort 3 قفدتك ماطن تاسلج مكارتت ثيح دراوملل ءفك ريغ مادختسإلىل ي دؤي نأ نكميولمعال تاسلج عادنود تاقاطنلأ ءامسأ

ةلكشمأل ءاشنإ ةداعإ تاوطخ

بنأج نم ةطشنلأ DNS تالاصتإ نم ققحتلل lina رملأل ذي فنن تب مق ،ةلكشمأل ةبقارمل Lina:

show conn detail

امم ،UDP ةلهم ءاهتنا ىتح ةطشن DNS لمع تاسلج لظت ،هذعب امو 7.6 نمألأ ةيأمأل رادج ي ءامم دراوملأ ءافك مدعلىل ي دؤي .

لأل

قفدت حسم قيرط نع ةلكشمأل هذو 7.7.0 نمألأ ةيأمأل رادج ي "DNS ةيأم" ةزيم جلاعات صأخلأ زيزعتلأ اذو نمضويو .أهصحفو DNS ةبأجتسإ ءمزح مالتسإ دعب أروف UDP مكارت عنمي امم ،أروف Snort 3 ي تاقاطنلأ ءامسأ ماطن تاسلج ردصت نأ لوكتوربلأب دراوملأ ءافك نسحيو ةيروضلأ ريغ تاسلج

ةزيملا ىلع ةماع ةرظن

DNS ةباجتسا ةمزح مالتسا دعب ةرشابم UDP قفدت حسمب "DNS ةيامح" ةزيم موقت UDP ةلهم رهظت ىتح ريخشلا قفدت رظتني نأ بجي ال. اهصحفو

- تاقفدتلا نم لقا ددع ىلإ ةزيملا هذه يدؤت، عبرملا ىلع ةيفاك DNS رورم ةكرح دوجو دنع ةلباقملا SNORT تاقفدتل بسانملا فيظنتلا ببسب ةطشنلا
- بيذشت عارجا نود عبرملا ةطساوب TCP/UDP تالاصتا نم ديزملا ةجلاعم نكمي ماع لكشب عبرملا ةيلاعف نم نسحي امم، ةطشنلا تالاصتالل

اهحالصا وءاطخالا فاشكتسا

UDP لمع تاسلج رادصا نامضل Lina رمألا مدختسا، "DNS ةيامح" ةزيم فئاظو نم ققحتلل DNS ةباجتسا يقلت دنع

```
<#root>
```

```
>
```

```
show snort counters | begin stream_udp
```

DNS: ةيامح ةزيم نودب لاثملا جارخا

```
stream_udp sessions: 755
max: 12
created: 755
released: 0
total_bytes: 124821
```

```
<#root>
```

```
>
```

```
show snort counters | begin stream_udp
```

DNS: ةيامح ةزيم مادختساب لاثملا جارخا

```
stream_udp sessions: 899
max: 14
created: 899
released: 899
total_bytes: 135671
```

بېسانملا تقولا ي ف اهؤاشنإ مت يتل تاسلجل ا عي مج رادصإ متي هنأ ىلإ تاجرخملا ريشت
، DNS "ةيامح" ةزيمل حيحصلا ليغشتلا دكؤي امم

ةلص تاذا تامولعم

- [Cisco نمتاليزنتلا او ينفلا معدلا](#)

ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا