

snort3 دعواق مهف

تايوتحمل

[عمدقملا](#)

[قيساسألابلطتملا](#)

[تابلطتملا](#)

[صيخرتلا](#)

[عمدختسملاتانوكملا](#)

[قيساسأتامولعم](#)

[Snort3 دعواق](#)

[عمدقلا تاءارجا](#)

[عمدقلا حيرشت](#)

[عمدقلا تازيم](#)

[قلمألا](#)

[قصاللاتقؤملا نزملا http و http uri عمدخسأرعملا](#)

[فلملا عمدخسأرعملا](#)

[قلمص تاذطباور](#)

عمدقملا

CISCO Secure Firewall Threat Defense (FTD) لاي ف كرحم لل Snort3 عمداق عقيثواذه فصبي

قيساسألابلطتملا

تابلطتملا

ةيلالاي عيضاوملاب عمفرعم كيذل نوك ت ناب Cisco ي صوت

- CISCO Secure Firewall Threat Defense (FTD)
- Intrusion Prevention System (IPS)
- سولمجاناب Snort2

صيخرتلا

نيمضت متي امك ،اي فاك يساسأل صيخرتلا دعيو ،عمدخم صيخرت تابلطتم دجوت ال ردصملا عموتفم Snort3 تارادصا ي فو FTD لخاد Snort كرحم ي ف عروكملا تازيملا

عمدختسملاتانوكملا

ةيلالاي عيداملا تانوكملا وجماربلل تارادصا ي لى دن تسملا اذه ي ف عمراول تامولعملل دن تست

- CISCO Secure Firewall Threat Defense (FTD)، CISCO Secure Firewall Management Center (FMC) عم 7.0+ رادصا لى Snort3.

صاخه لعممة ئىب ىف ءءوءملا ءزهأالا نم ءنئسملا اءه ىف ءءراوللا ءامولعمللا ءاشنإ مئناك اءا. (ىضارءفا) ءوسمم نىوكئب ءنئسملا اءه ىف ءمءءئسملا ءزهأالا ءىمء ءأءب. رمأ ىل لمءءملا رىءأئلل كمهف نم ءكأءف، لىغشءللا ءىق كئكبش.

ءىساسأ ءامولعمل

لىءسءو ىلعفللا ءقوللا ىف ءانائىبللا رورم ءكء لىلءء ىلع رءاقللا Cisco IPS كءرم وه Snort مءءللا.

ءامءهلا فاشءكلاو، ىوءءملا نع ءءبللاو، لوكوءوربلل لىلءء ءارء Snort.

ءءءءءم ءرب ءىنئب ءوزم Snort2 زارء (IPS) ءاقارءءالا ءنم مائن نم ءءءم راءصإ نع ءرابع Snort3 ماءءءسالا ءلوهسو رىووءءللا ءىلباقو ءالكشملا فاشءكلاو ءاءالا نىسءء ىلع لمءء.

Snort3 ءءاوق

ءبائكلاو ءءارقلا ىف ءلوهسو رءكأ ءءاوقلا لءءل اءه Lua قىسئء نوئمءءئسى Snort3 ققءءللاو.

ءءءاقللا ءاءارء

ءءءءللا ءافىرءءللا نوكةو، ءءءاقللا ءاءارء رىغءب ءءءللا راءصإلا اءه موقى:

- Pass: ءمءللا لباءم ءىلئلا ءءاوقلا مىقء فاقى: Pass
- Alert: طقف ءءء ءاشنإ: Alert
- Block: ىقبءملا ءسلء رظء، ءمءللا طاقسإ: Block
- Drop: طقف ءمءللا طاقسإ: Drop
- Rewrite: لاءبءسالا رايءللا ماءءئسإ ءلاء ىف بولطم: Rewrite
- React: HTML ءلئك ءباجئسإ ءءفص لاسرا: React
- Reject: هىللا لوصوللا رءءئى ىءل ICMP وأ TCP RST لاءءا: Reject

ءءءاقللا ءىرئشء

وه ءىرئشءللا:



ءفنملاو ءهءوللا رءصملا (ءاكبش) ءكبشو لوكوءوربللا ءارءللا ىلع ءءءاقللا سار ىوءءى (ءفنملا).

ءىلئلا ءارايءللا ءءا ءءءاقللا سار نوكة نأ نكمى Snort3، ىف

- ءمءللا ءءءاقللا سار

```
<inline" lang="lua">alert http
(
msg:"Alert HTTP rule";
flow:to_client,established;
content:"evil", nocase;
sid:1000001;
)
```

- فللمل ددعاق سار

```
alert file
(
msg: "Alert File example";
file_data;
content:"malicious_stuff";
sid:1000006;
)
```

- ةيديلققتل ددعاقال سار

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS
(
msg:"Alert HTTP rule";
flow:to_client,established;
content:"evil", nocase;
sid:1000001;
)
```

ددعاقال تازيم

يه ةديدجل تازيمال ضعب

- (صاخال هرطس ىلع راىخ لك) ةيئاوشع ءاضيب ةحاسم

```
alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS
(
msg:"Alert TCP rule";
flow:to_client,established;
content:"evil", nocase;
sid:1000000;
)
```

- ؛ و ، ل قستمل مادختسال

```
content:"evil", offset 5, depth 4, nocase;
```

- ةيراي تخ | ذفان مل او تاكبش لل

```
alert http ( Rule body )
```

- (لمالك الة مئاق الة تسيل هذة) ةقصال الة تقؤم الة نزاخم الة نم ديزم الة فاض |

```
http_uri  
http_raw_uri  
http_header  
http_raw_header  
http_trailer  
http_raw_trailer  
http_cookie  
http_raw_cookie  
http_true_ip  
http_client_body  
http_raw_body  
http_method  
http_stat_code  
http_stat_msg  
http_version  
http2_frama_header  
script_data  
raw_data
```

- طم ن الة تاقي لعت C

```
alert http  
(  
msg:"Alert HTTP rule"; /* I can write a comment here */  
...  
)
```

- (rem) ةظحال مة يساس الة مل ك ال

```
alert http  
(  
msg:"Alert HTTP rule";  
flow:to_client,established;  
rem:"Put comments in the rule anywhere";  
content:"evil", nocase;  
sid:1000001;
```

)

- appids ل ةيساسأ تاملك

```
alert tcp $HOME_NET any -> $EXTERNAL_NET any
(
msg:"Alert on apps";
appids:"Google, Google Drive";
content:"evil", nocase;
sid:1000000;
)
```

- sd_pattern ةيفصتل
- HyperFlex ةينقت مادختسا عم Regex ةيساسألا ةملكلا
- ةيولألا ةانايبال ةمدخلل ةيساسألا ةملكلا لدبتست

ةلثمألا

قصاللا تقوُملا نزخمل http_uri و http ةمدخ سَأر عم لاثم

HTTP ل URI في malicious ةملكلا فشكت ةدعاق بتكا: ةمهمل

لحل:

```
alert http
(
msg:"Snort 3 http_uri sticky buffer";
flow:to_server,established;
http_uri;
content:"malicious", within 20;
sid:1000010;
)
```

فلمل ةمدخ سَأر عم لاثم

PDF. تافلم فشكت ةدعاق بتكا: ةمهمل

لحل:

```
alert file
(
msg:"PDF File Detected";
file_type: "PDF";
sid:1000008;
```

)

ةلص تاذا طباور

[ليغشتلا دعاوق و IDS چمانرب لي زنت](#)

[پوښېچ](#)

ةمچرتل هذه ل و ح

ةل آل ا ت ا ي 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 ي 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 ل آل ا 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 م ا ة 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