

يلع ةيفاضا Snort 3 دعاوق تاءارجا نيوكت FMC

تايوتحمل

[ةمدقملا](#)

[ةيساسا تامولعم](#)

[ةيساسالا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةزيمللا ليصافت](#)

[بكللاوييس مافا](#)

ةمدقملا

ةيفاضالا "Snort 3 دعاوق تاءارجا" ةزيمل (FMC) Firepower ةرادا زكرم معد دنتسملا اذه فصيا 7.1 رادصالا يف اهتفاضلا تمت يتلا

ةيساسا تامولعم

ةسايس دعاوقل تاءارجا ةعبس معددي (FTD) ةيرانلا ةقاطلا ديدهت دص عافدلا نأ نم مغرلا يلع نأ الا 7.0 يف طاقسالا/رورملا/ةباتكلا ةداعا/ضفرل/رطحل/الليطعتلا/هيبنتلا يه ولسلا "هيبنت": snort 3 دعاوقل طقف تاءارجا ةثالث تمعد (FMC) ةدحوملا ةرادالا يف مكحتلا ةدحو "رطح" و "ليطعت" و

ةديج دعاوق تاءارجا نيوكت FMC معدت، Firepower 7.1.0 نم

ةيساسالا تابلطتملا

تابلطتملا

ةيلالاتلا عيضاوملاب ةفرعم كي دل نوكت نأ Cisco ي صوت:

- رصملا حوتفم ريخشلا ةفرعم
- Firepower (FMC) 7.1.0+ ةرادا زكرم
- (FTD) 7.0.0+ ةيرانلا ةقاطلا ديدهت دص عافدلا جم انرب

ةمدختسملا تانوكملا

ةيلالاتلا ةيداملا تانوكملا وجم انربلا تارادصا يلا دنتسملا اذه يف ةدراولا تامولعملا دنتست

- 3 رادصالا لغشت يتلا FirePOWER تاصنم عيمج يلع دنتسملا اذه قبطني
- رادصاب لمعي يذلا Cisco نم FirePOWER ديدهت معددي يذلا (FTD) يرهظلا عافدلا جم انرب
- 7.4.2 جم انربلا
- جم انربلا نم 7.4.2 رادصالا لغشي يذلا (FMC) Firepower Management Center Virtual

صاخ ةي لمعم ةئي ب ي ف ةدوجومل ةزهجال نم دنتسمل اذه ي ف ةدراول تامولعمل عاشنإ مت تناك اذإ .(يضا رتفا) حوسمم نيوكتب دنتسمل اذه ي ف ةمدختسمل ةزهجال عي مج تادب رم أ يال لمحتمل ريثأتلل كمهف نم دكأتف ،ليغشتل ديق كتكبش

ةزيمل ل ي صا فت

ي لي امك اهتافصوو ةدي دجل ال Snort 3 ةدعاق تاءارجا ةفاضا تمت

دعاوق ي أ لبق نم مي ي قتل نم ديزم نود رورمل اب ةمزحلل حمسي ،ثدح عاشنإ متي مل :رورم ةقحال snort .

لاصتالا اذه ي ف رخأ رورم ةكرح رطح مدعو ةقباطملا ةمزحلل طاقساو ،ثدح عاشنإ :طاقسا

اذه ي ف ةي فاضلا تانا ي بل رورم ةكرح عنمي و ،ةقباطملا ةمزحلل عطق ي و ،ثدح دلوي :ضفر ي فيضم يلا هيل لوصولا رذعتي يذل ICMP ذفم وأ TCP طبض ةدعاق لسري و لاصتالا ةهوجل و روصملا

ةدعاقل ي ف لادبتسالا را ي خ يلع انب ةمزحلل تايوتحم لدبتسي و ثدح دلوي :ةباتكلا ةدعاق

بكلل اوي س ما فإ

كلذ دع ب ام، FMC Policies > Access Control > Intrusion، امحتق اسي ي ف Snort 3 دعاوق ضرعل ي ف حضوم وه امك ،ةسايسلا نم نم يال يولعل نكرل ي ف Snort 3 رادصا را ي خ يلع رقنا ةروصل:

| Intrusion Policy | Description | Base Policy | Usage Information |
|------------------|------------------------------------|-------------|---|
| FTD_Intrusion | Balanced Security and Connectivity | | No Access Control Policy No Zero Trust Application Policy No Device |

رادصا Snort 3

دعاوق ةفاكل ةيضا رتفالا تاءارجالا ةدهاشم كنكمي ،دعاوقلا عي مج > يساسا جهن قوف رقنا ماطنلا ةطساوب ةفرعمل ال Snort 3

< Policies / Intrusion / FTD_Intrusion

Used by: No Access Control Policy | No Zero Trust Application Policy | No Device

Base Policy: Balanced Security and Connectivity | Mode: Prevention

Active Rules 9693 | Alert 474 | Block 9219

Base Policy → Group Overrides → Recommendations **Not in use** → **Rule Overrides** | Summary

Rule Overrides Back To Top

102 items All x v | Rule Action v | Search by CVE, SID, Reference Info, or Rule Message

49,532 rules | Presets: Alert (474) | Block (9,219) | Disabled (39,839) | Overridden (0) | Advanced Filters

✔ Rule action changed successfully x

| | GID:SID | Rule Details | Rule Action | Set By | Assigned Groups |
|--------------------------|---------|-----------------------------------|-----------------|---------------|--------------------------|
| <input type="checkbox"/> | 1:28496 | BROWSER-IE Microsoft Internet ... | Reject | Rule Override | Malicious File, Drive... |
| <input type="checkbox"/> | 1:32478 | BROWSER-IE Microsoft Internet ... | Alert (Default) | Base Policy | Malicious File, Drive... |
| <input type="checkbox"/> | 1:32479 | BROWSER-IE Microsoft Internet ... | Alert (Default) | Base Policy | Malicious File, Drive... |
| <input type="checkbox"/> | 1:26633 | BROWSER-IE Microsoft Internet ... | Alert (Default) | Base Policy | Malicious File, Inter... |

دعاوقال عارج ريغت

اهزواج مت يتل دعاوقال > تايطختل نمض اهزواج مت يتل دعاوقال ىلع روثل نكمي

< Policies / Intrusion / FTD_Intrusion

Used by: No Access Control Policy | No Zero Trust Application Policy | No Device

Base Policy: Balanced Security and Connectivity | Mode: Prevention

Active Rules 9693 | Alert 473 | Block 9219 | Others 1

Base Policy → Group Overrides → Recommendations **Not in use** → **Rule Overrides** | Summary

Rule Overrides Back To Top

102 items All x v | Rule Action v | Search by CVE, SID, Reference Info, or Rule Message

1 rule | Presets: Alert (0) | Block (0) | Disabled (0) | **Overridden (1)** | Advanced Filters | Reject (1)

| | GID:SID | Rule Details | Rule Action | Set By | Assigned Groups |
|--------------------------|---------|-----------------------------------|---------------|---------------|--------------------------|
| <input type="checkbox"/> | 1:28496 | BROWSER-IE Microsoft Internet ... | Reject | Rule Override | Malicious File, Drive... |

اهزواج مت يتل دعاوقال

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة و مچم مادختساب دن تسملا اذه Cisco تچرت
ملاعل اءان اءمچ يف نمة دختسملل معد ىوتحم مة دقتل ةيرشبلا و
امك ةققة نوك ت نل ةللأل ةمچرت لصف أن ةظحال مچرئ. ةصاغل مة تغلب
Cisco يلخت. فرتحم مچرت مة دقتل ةللأل ةفارتحال ةمچرتلا عم لاللا و
ىل اءءاد ءوچرلاب ىصوؤت و تامچرتل هذه ةققة نء اهتئل وئسم Cisco
Systems (رفوتم طبارلا) ىلصألل ىزىلچنللا دن تسملا