

يلع ةيفاضا Snort 3 دعاوق تاءارجا نيوكت FMC

تايوتحمل

[ةمدقمل](#)

[ةيساسا تامولعم](#)

[ةيساسا انا تابلطتم](#)

[تابلطتم](#)

[ةمدختسم انا نوكم](#)

[ةزيمل لي صافت](#)

[بكل اويس ما فا](#)

ةمدقمل

ةيفاضا انا "Snort 3 دعاوق تاءارجا" ةزيمل (FMC) Firepower ةرادا زكرم معد دن تسم انا اذ ه فص ي 7.1 رادص انا يف اه تفاضا تم ت ي تل

ةيساسا تامولعم

ةسايس دعاوقل تاءارجا ةعبس معد ي (FTD) ةيران ل ا قاطلا ديده ت دص ع ا ف د ل ا ن ا م م ر ل ا يلع ن ا ا 7.0 يف طاقس انا رورم ل ا ةبات ك ل ا دعا ا / ص ف ر ل ا / ر ط ح ل ا / ل ي ط ع ت ل ا / ه ي ب ن ت ل ا ي ه و ل ل س ت ل ا "ه ي ب ن ت": snort 3 دعاوقل ط ق ف تاءارجا ة ثا ل ت ت م ع د (FMC) ة د ح و م ل ا ة ر ا د ا ل ا ي ف م ك ح ت ل ا ة د ح و "ر ط ح" و "ل ي ط ع ت" و

ةديج دعاوق تاءارجا نيوكت FMC معد ت 7.1.0 Firepower ن م

ةيساسا انا تابلطتم

تابلطتم

ةيلال انا ع ي ص ا و م ل ا ب ة ف ر ع م ك ي د ل نوكت ن ا ب Cisco ي ص و ت:

- ر د ص م ل ا ح و ت ف م ر ي خ ش ل ا ة ف ر ع م
- Firepower (FMC) 7.1.0+ ة ر ا د ا ز ك ر م
- (FTD) 7.0.0+ ة ي ر ا ن ل ا ق ا ط ل ا د ي د ه ت د ص ع ا ف د ل ا ج م ا ن ر ب

ةمدختسم انا نوكم

ةيلال انا ة ي د ا م ل ا ت ا ن و ك م ل ا و ج م ا ر ب ل ا ت ا ر ا د ص ا ي ل ا د ن ت س م ل ا ا ذ ه ي ف ة د ر ا و ل ا ت ا م و ل ع م ل ا د ن ت س ت

- 3 ر ا د ص ا ل ا ل غ ش ت ي ت ل ا FirePOWER ت ا ص ن م ع ي م ج ي ل ع د ن ت س م ل ا ا ذ ه ق ب ط ن ي
- ر ا د ص ا ب ل م ع ي ي ذ ل ا Cisco ن م FirePOWER ديده ت معد ي ي ذ ل ا (FTD) ي ر ه ا ط ل ا ع ا ف د ل ا ج م ا ن ر ب
- 7.4.2 ج م ا ن ر ب ل ا
- Firepower Management Center Virtual (FMC) ي ذ ل ا ل غ ش ي ي ذ ل ا 7.4.2 ر ا د ص ا ل ا ل غ ش ي ي ذ ل ا ج م ا ن ر ب ل ا

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 لمحتحمل ريثأتلل كمهف نم دكأتف ،ليغشتل ديق كتكبش

ةزيملا ليصافت

لي امك اهتافصوو ةديجال Snort 3 ةدعاق تاءارجا ةفاضل تمت

دعاوق ي أ لبق نم ميقيقتل نم ديزم نود رورملاب ةمزحلل حمسي ،ثدح عاشنإ متي مل :رورم ةقجال snort .

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

اذه ي ف ةيفاضلا تانايل رورم ةكرح عنمي و ،ةقباطملا ةمزحلل عطقيو ،ثدح دلوي :ضفر ي فيضم يلا هيل لوصول رذعتي يذل ICMP ذفم وأ TCP طبض ةدعا ل لسري و لاصتالا ةهوجل و روصملا

ةدعاقل ي ف لادبتسالا راخي لعل ءانب ةمزحلل تايوتحم لدبتسي و ثدح دلوي :ةباتكلا ةدعا

بكلل اويس مإ فإ

كلذ دعب ام، FMC Policies > Access Control > Intrusion، ماحتقإ ةسايس ي ف Snort 3 دعاوق ضرعل ي ف حضوم وه امك ،ةسايسلا نم نميألا يولعل نكرل ي ف Snort 3 رادصا راخي لعل 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 > ياساسأ جهن قوف رقنا ماطنلا ةطساوب ةفرعمل 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

Rule Action | 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

GID:SID	Rule Details	Rule Action	Set By	Assigned Groups
1:28496	BROWSER-IE Microsoft Internet ...	Reject	Rule Override	Malicious File, Drive...
1:32478	BROWSER-IE Microsoft Internet ...	Alert (Default)	Base Policy	Malicious File, Drive...
1:32479	BROWSER-IE Microsoft Internet ...	Alert (Default)	Base Policy	Malicious File, Drive...
1:26633	BROWSER-IE Microsoft Internet ...	Alert (Default)	Base Policy	Malicious File, Inter...

دعاوقال اراج ريغت

اهزواج مت يتل دعاوقال > تايطختل نمض اهزواج مت يتل دعاوقال ىلع روثع ال 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

Rule Action | 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
1:28496	BROWSER-IE Microsoft Internet ...	Reject	Rule Override	Malicious File, Drive...

اهزواج مت يتل دعاوقال

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نء مء 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 مء دقء ةللأل ةل فارتحال ةمچرتل عم لءال وه
ىل إءمءءاد ءوچرلاب ةصوء و تءمچرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةل صأل ةل ءل ءن إءل دن تسمل