

# FDM ربع اهرا بتخاو AMP فلم ةسايس نيوكت

## تايتو حمل

[قم دق م ل](#)

[ةسايس الابل ط م ل](#)

[تابل ط م ل](#)

[ةمدخت س م ل تانوك م ل](#)

[تاميل عت](#)

[صيخرت ل](#)

[نيوكت ل](#)

[رابتخا](#)

[اهال ص او اعاطخ ال فاشكت سا](#)

## ةمدق م ل

"ةراض ال جمار بل ن م ةمدقت م ل ةي ام حل" فلم ةسايس نيوكت ةي فيك دن ت س م ل اذه حضوي (AMP) Firepower Device Manager (FDM) جمار بل ربع اهرا بتخاو (AMP).

## ةسايس الابل ط م ل

### تابل ط م ل

ةيلات ال عيضاوم لابل ةفر عم كي دل نوكت نابل Cisco ي صوت:

- Firepower (FDM) زا ج ري دم
- Firepower Threat Defense (FTD)

### ةمدخت س م ل تانوك م ل

- FDM لال خ ن م راد م ل Cisco ن م 7.0 راد ص ال يره اظال FTD جمار بل
- ل ث م ت . ي ح ي ض و ت ل ل ض ر ع ل ل ض ا ر غ ال م ي ي ق ت ل ل ص ي خ ر ت م د خ ت س ي ) م ي ي ق ت ل ل ص ي خ ر ت ( م ا د خ ت س ا و ح ل ل ص ص ي خ ر ت ي ل ع ل و ص ح ل ل ي ف Cisco ة ي ص و ت

ةصاخ ةي لم عم ةئي ب ي ف ةدوجوم ل ةزه ج ال ن م دن ت س م ل اذه ي ف ةدراول تامول عم ل عاش ن ا م ت ن ا ك ا ذ ا . (يضا ر ت ف ا) ح و س م م ن ي و ك ت ب دن ت س م ل اذه ي ف ةمدخت س م ل ةزه ج ال ع ي م ج ت ا د ب ر م ا ي ال ل م ح م ل ر ي ث ا ت ل ل ك م ه ف ن م د ك ا ت ف ، ل ي غ ش ت ل ل د ي ق ك ت ك ب ش

## تاميل عت

### صيخرت ل

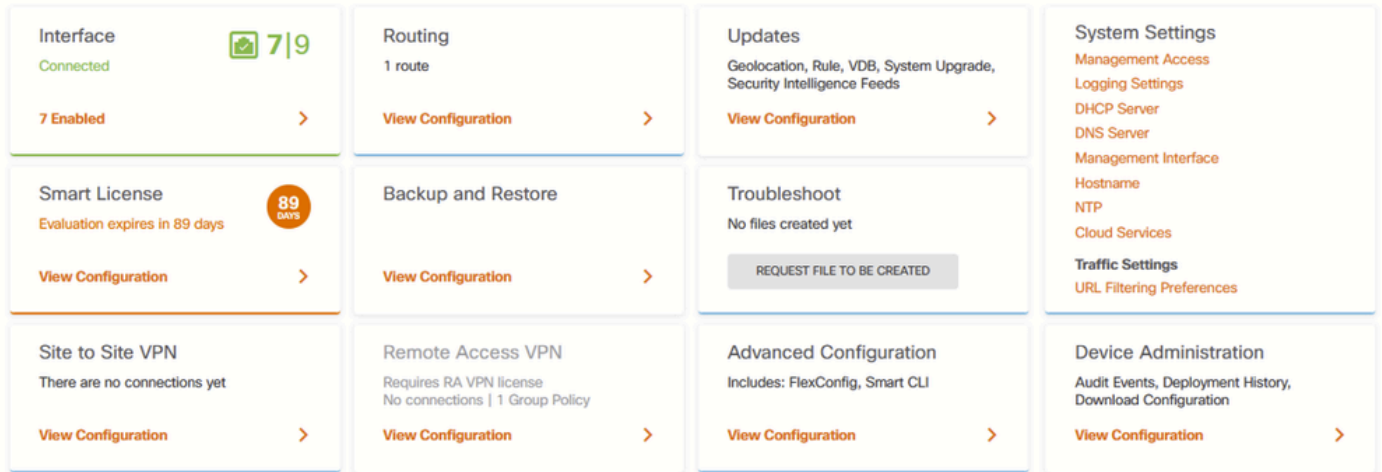
مدخت س م ل ةه ج او ي ل ع زا ج ل ا ح ف ص ي ل ل ق ت ن ا ، ةراض ال جمار بل صيخرت ني ك م ت ل .

## FDM ل (GUI) ةيموسرللا



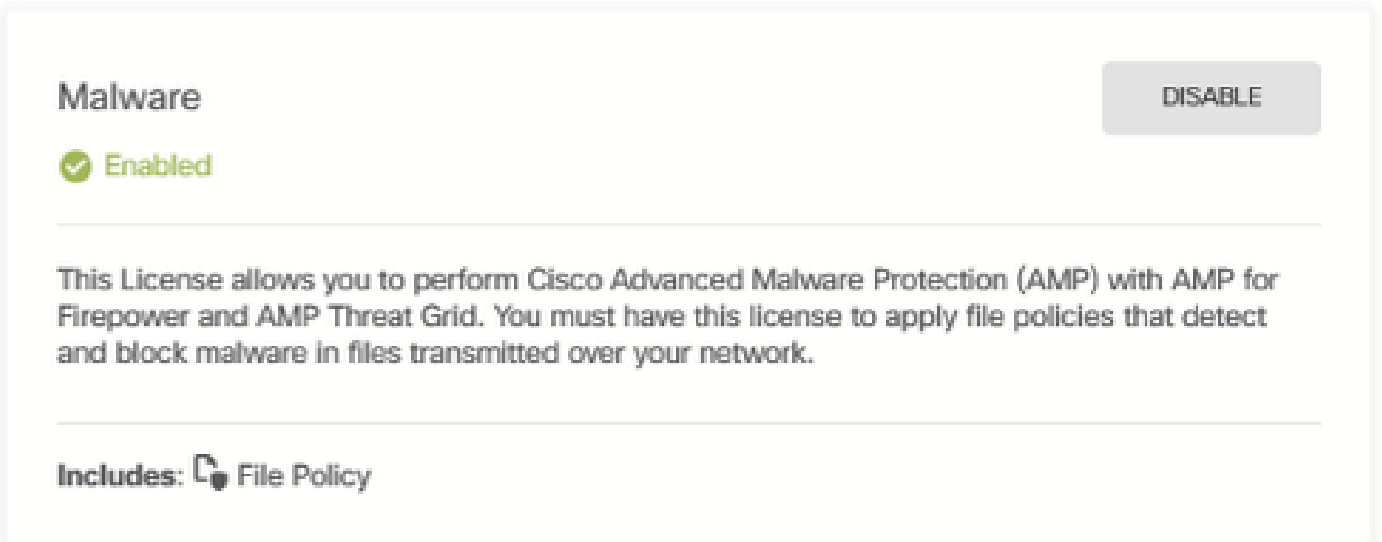
FDM زاھج بېوېت ةمالة

### 2. نېوكتلا ضرع قوف رقن او Smart License ىمسمللا ع برمللا ناكم ددح.



FDM زاھج ةحفص

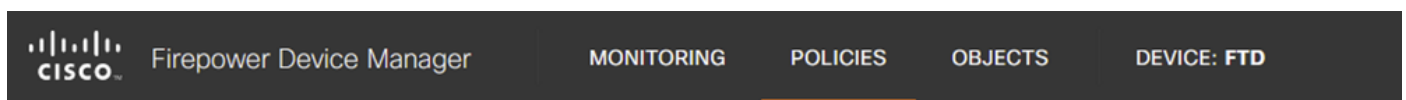
### 3. ةراضلا جماربلا ىمسمللا صيخرتلا نېوكت ب مق.



ةراضلا جماربلا صيخرت

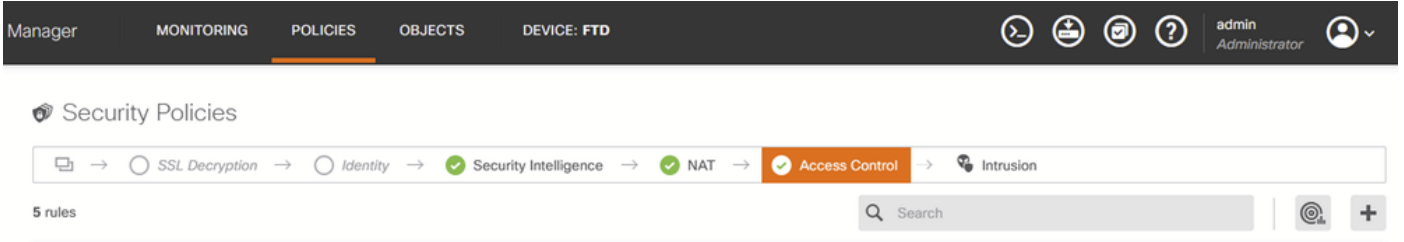
## نېوكتلا

### 1. FDM ي ف تاسايسلا ةحفص ىل لقتنا.



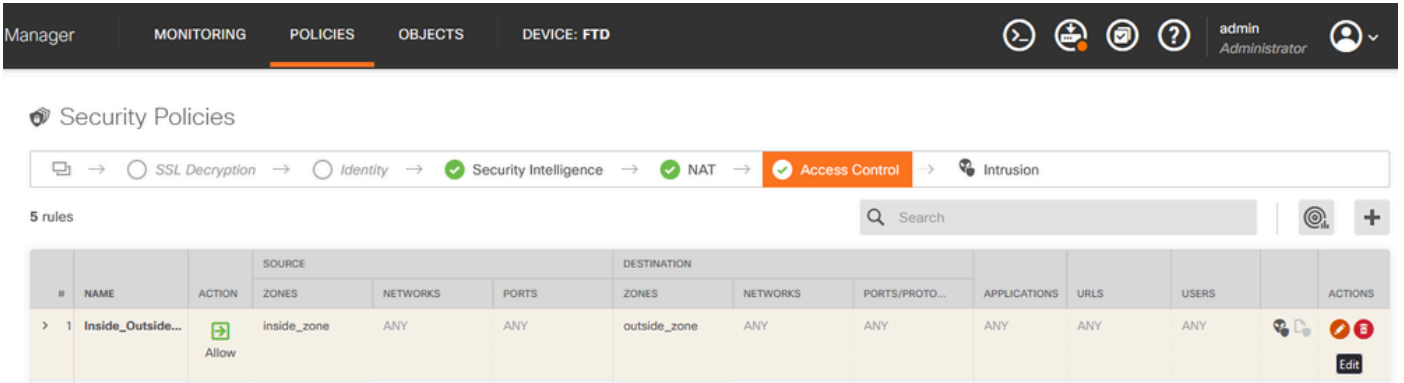
FDM تاسايس بېوېتلا ةمالة

2. لوصول في مكحتال مسق ىل لقتنا ، نامأل تاسايس تحت .



FDM ىل لوصول في مكحتال بيوبت عمال ع

3. لوصول ءدعاق ررحم قوف رقنا . فللمل جهن نيوكتل اهؤاشنل وأ لوصول ءدعاق نع شحبل .  
[طابترال](#) اذه ىل عجرا ، لوصول ءدعاق عاشنل ءيفيك لوح تاميلعت ىلع لوصول



FDM ىل لوصول في مكحتال ءدعاق

4. نم لضفملم فلمل جهن رايل دل دحو لوصول ءدعاق في فلمل جهن مسق قوف رقنا .  
ءدعاق ىلع اهؤارج مت يتل تاريخيغتل ظفحل قفاوم قوف رقنا . ءلدسنملم ءمئاقلا

## Edit Access Rule

Order	Title	Action
1	Inside_Outside_Rule	Allow

Source/Destination Applications URLs Users Intrusion Policy **File policy** Logging

**Evaluation Period**  
This feature needs a license to be purchased. For more details, go to [Smart License](#).

**SELECT THE FILE POLICY**

- Block Malware All
- None
- Block Malware All**
- Cloud Lookup All
- Block Office Document and PDF Upload, Block Malware Others
- Block Office Documents Upload, Block Malware Others

**CONTROLLING FILES AND MALWARE**  
Use file policies to detect malicious software, or malware, using Advanced Malware Protection for Firepower (AMP for Firepower.) You can also use file policies to perform file control, which allows control over all files of a specific type regardless of whether the files contain malware

Show Diagram  582 Reset 2023-08-30 09:55:26

CANCEL OK

FDM ل لوصول باب مكحتل ادعاق فلم ةسايس " بيوبتل ةمالع

5. جهن ةنوقيأ نيكمت نم ققحتل قيرط نع لوصول ادعاق ىلع فلمل ا جهن قيبت نم دكأت فلمل.

جهن زمر نيكمت مت فلم

Order	Title	Action	Source/Destination	Applications	URLs	Users	Intrusion Policy	File policy	Logging
1	Inside_Outside...	Allow	inside_zone	ANY	ANY	outside_zone	ANY	ANY	ANY

Block Malware All

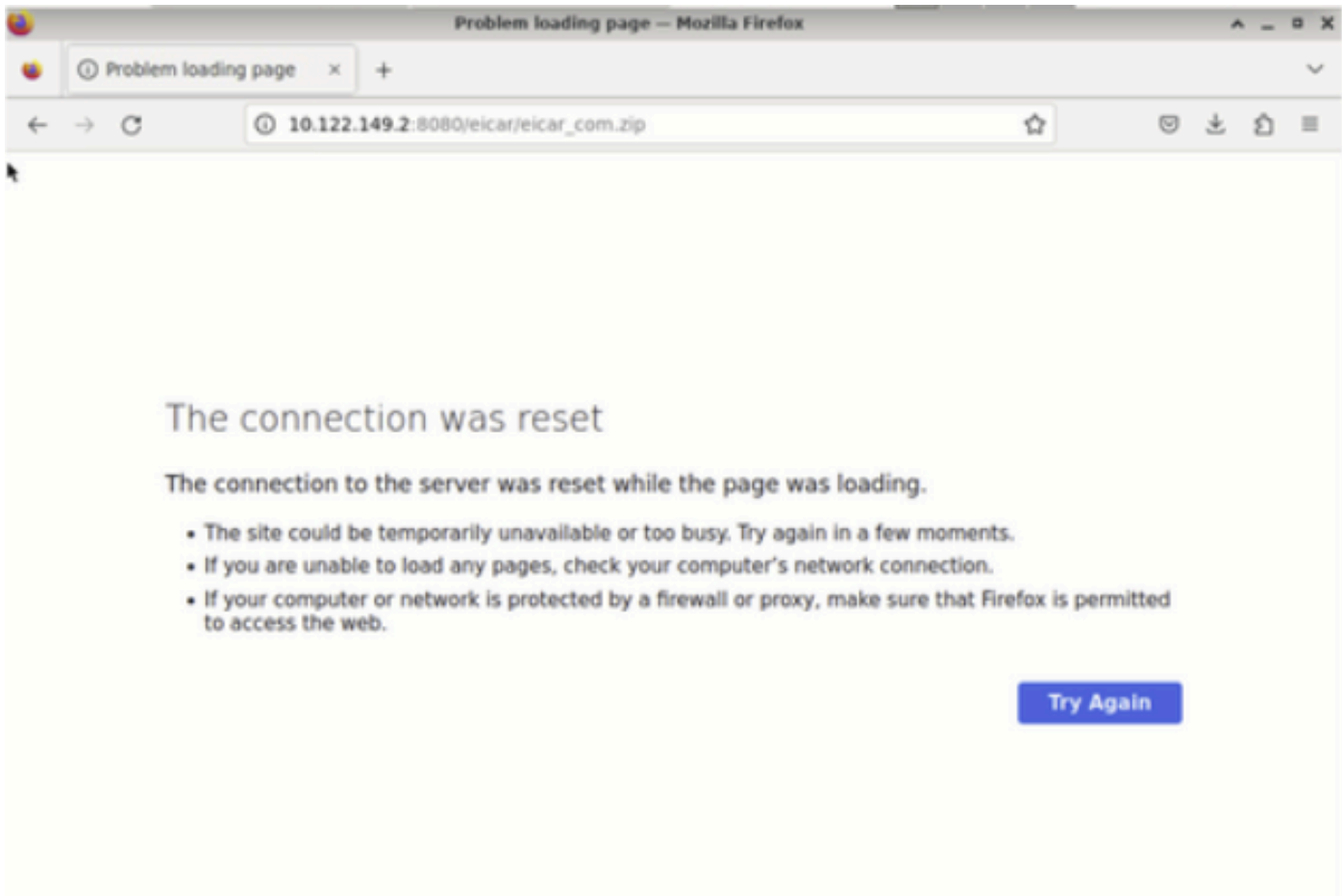
فلمل

6. رادمل زاوجل ىلع تاريغيغتلا رشنو ظفح.

رابتخا

تالواحم مدختسأ، لمعي ةراضل اجماربل اةيامل هن يوكت مت يذل فلمل ا جهن نأ نم ققحتل ل فيضمب صاخلا بيو ضرعتسم نم راض اجمانرب رابتخا فلمل ليذنتل هذه رابتخال وييرانيس يئاهن.

نم راض اجمانرب رابتخا فلمل ليذنتل ةلواحم نإف، هذه ةشاشلا ةطوقل يف ضرعم وه امك ةحجان ريغ بيولا ضرعتسم.



ضرع تسم ل ليزنت رابتخا

ةطساوب هرطرح مت فلملا ليزنت نأ ماظنلا معد عبت رهظي، FTD ل (CLI) رماوأ رطس ههجاو نم ههجاو ربع ماظنلا معد عبت ليغشت ةيفيك لوح تاميلعت يلعل لوصحلل. فلملا ةيلمع [طابت رالا](#) اذه لىا عجرا، FTD ب ةصاخلا (CLI) رماوأل رطس

```
192.168.0.10-40016 > 10.122.149.2-8080 6 AS 1 I 0 File signature verdict reject and flags 0x00005A00 for 2546dcffc5ad854d4ddc64fbf056871cd5a00f2471cb7a5bfd4ac23b6e9eedad of instance 0
192.168.0.10-40016 > 10.122.149.2-8080 6 File Process: drop /eicar/eicar_com.zip
192.168.0.10-40016 > 10.122.149.2-8080 6 IPS Event: gid 147, sid 1, drop
192.168.0.10-40016 > 10.122.149.2-8080 6 AS 1 I 0 File malware event for 2546dcffc5ad854d4ddc64fbf056871cd5a00f2471cb7a5bfd4ac23b6e9eedad named eicar_com.zip with disposition Malware and action Block Malware
192.168.0.10-40016 > 10.122.149.2-8080 6 AS 1 I 0 Archive childs been processed No
192.168.0.10-40016 > 10.122.149.2-8080 6 Snort detect_drop: gid 147, sid 1, drop
192.168.0.10-40016 > 10.122.149.2-8080 6 AS 1 I 0 deleting firewall session
192.168.0.10-40016 > 10.122.149.2-8080 6 Snort id 0, NAP id 2, IPS id 0, Verdict BLACKLIST
192.168.0.10-40016 > 10.122.149.2-8080 6 ==> Blocked by File Process
Verdict reason is sent to DAQ
```

ماظنلا معد عبت رابتخا

ةراضلا جماربالا رطرح يف فلملا جهن نيوكت حاجن دكؤي اذه

## اهحالص او ءاطخال فاشكتسا

تاجارتقا لىا عجرا، ةقباسلا تانويكتلا مادختسا دنع حاجن ةراضلا جماربالا رطرح مدع ةلاح يف ةيللاتلا اءاطخال فاشكتسا:

1. ةراضلا جماربالا صيخرت ةيخالص ءاهتنا مدع نم ققحتلا.
2. ءححص رورم ءكرح فدهتست لوصولاب مكحتلا ءءاق نأ نم دكأت.

3. ةب و ل ط م ل ا ة ي ا م ح ل ا و ة ف د ه ت س م ل ا ر و ر م ل ا ة ك ر ح ل ح ي ح ص د د ح م ل ا ت ا ف ل م ل ا ج ه ن ر ا ي خ ن ا ن م د ك ا ت .  
ة ر ا ض ل ا ج م ا ر ب ل ا ن م .

م ع د ي ل ع ل و ص ح ل ل C i s c o ن م T A C ب ل ص ت ا ف ، ل ح ل ل ة ل ب ا ق ر ي غ ل ا ز ت ا ل ة ل ك ش م ل ا ت ن ا ك ا ذ ا  
ي ف ا ض ا .

ةمچرتل هذه لوح

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت  
ملاعلاء انءمچي في نيمدختسمل معدى وتحم مي دقتل ةيرشبلاو  
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخلا مهتغب  
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه  
ىلإ أمئاد عوچرلاب يصوت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco  
Systems (رفوتم طبارلا) يصلأل يزي لچنإل دن تسمل