

# نم BGP و OSPF و EIGRP لئاسر داع بت سا FirePOWER ماحتقإ صر ف

## المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المكونات المستخدمة](#)
- [الرسم التخطيطي للشبكة](#)
- [التكوين](#)
- [مثال EIGRP](#)
- [مثال OSPF](#)
- [مثال BGP](#)
- [التحقق](#)
- [EIGRP](#)
- [بروتوكول أقصر مسار أولاً \(OSPF\)](#)
- [BGP](#)
- [استكشاف الأخطاء وإصلاحها](#)

## المقدمة

تقوم بروتوكولات التوجيه بإرسال رسائل الترحيب ورسائل keepalive لتبادل معلومات التوجيه وضمان إمكانية الوصول إلى الجيران حتى الآن. تحت الحمل الثقيل، قد يقوم جهاز أمان FirePOWER من Cisco بتأخير رسالة keepalive (دون إسقاطها) لمدة كافية لكي يعلن الموجه أن جارته سقطت. يوفر لك المستند الخطوات اللازمة لإنشاء قاعدة ثقة لاستبعاد رسائل تنشيط الاتصال وحركة مرور مستوى التحكم لبروتوكول التوجيه. هو يمكن أجهزة أو خدمات FirePOWER أن يحول حزم من مدخل إلى مخرج قارن، دون تأخير التفتيش.

## المتطلبات الأساسية

### المكونات المستخدمة

تستخدم التغييرات التي تم إجراؤها على نهج التحكم في الوصول في هذا المستند الأنظمة الأساسية للأجهزة التالية:

- (FireSIGHT Management Center (FMC
- جهاز أمان FirePOWER: الطرز فئة 7000 و 8000

**ملاحظة:** تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

## الرسم التخطيطي للشبكة

- الموجه A والموجه B متجاوران من الطبقة 2، وهما غير مدركين لجهاز FirePOWER المضمن (المسمى ب (IPS).
- الموجه A - 10.0.0.1/24
- الموجه B - 10.0.0.2/24



- لكل بروتوكول بوابة داخلي تم إختباره (OSPF و EIGRP)، تم تمكين بروتوكول التوجيه على الشبكة 24/10.0.0.0.
- عند إختبار بروتوكول BGP، تم إستخدام بروتوكول e-BGP وتم إستخدام الواجهات المادية المتصلة مباشرة كمصدر تحديث للقيم.

## التكوين

### مثال EIGRP

#### على الموجه

الموجه A:

```
router eigrp 1
network 10.0.0.0 0.0.0.255
```

الموجه B:

```
router eigrp 1
network 10.0.0.0 0.0.0.255
```

### FireSIGHT Management Center

1. حدد سياسة التحكم في الوصول المطبقة على جهاز أمان FirePOWER.
2. إنشاء قاعدة التحكم في الوصول باستخدام إجراء الثقة.
3. تحت علامة التبويب منافذ، حدد EIGRP تحت البروتوكول 88.
4. طقطقة يضيف أن يضيف الميناء إلى الغاية ميناء.
5. حفظ قاعدة التحكم بالوصول.

#### Editing Rule - Trust IP Header 88 EIGRP

The screenshot shows the configuration page for a rule named "Trust IP Header 88 EIGRP". The rule is enabled and has an action of "Trust". The "Ports" tab is selected, showing "Selected Source Ports (0)" as "any" and "Selected Destination Ports (1)" as "EIGRP (88)". The "Available Ports" list includes various protocols like AOL, Bittorrent, DNS over TCP, etc.

### مثال OSPF

## على الموجه

الموجه A:

```
router ospf 1
network 10.0.0.0 0.0.0.255 area 0
```

الموجه B:

```
router ospf 1
network 10.0.0.0 0.0.0.255 area 0
```

## FireSIGHT Management Center

1. حدد سياسة التحكم في الوصول المطبقة على جهاز أمان FirePOWER.
2. إنشاء قاعدة التحكم في الوصول باستخدام إجراء الثقة.
3. تحت علامة التبويب المنافذ، حدد OSPF بموجب البروتوكول 89.
4. طقسقة يضيف أن يضيف الميناء إلى الغاية ميناء.
5. حفظ قاعدة التحكم بالوصول.

### Editing Rule - Trust IP Header 89 OSPF

Name: Trust IP Header 89 OSPF  Enabled [Move](#)

Action: Trust  IPS: no policies Variables: n/a Files: no inspection Logging: no logging

Zones Networks VLAN Tags Users Applications **Ports** URLs Inspection Logging Comments

Available Ports  Search by name or value

- AOL
- Bittorrent
- DNS over TCP
- DNS over UDP
- FTP
- HTTPS
- HTTP
- IMAP
- LDAP
- NFS-D-TCP

Selected Source Ports (0): any

Selected Destination Ports (1): OSFP (89)

Buttons: Add to Source, Add to Destination, Save, Cancel

## مثال BGP

### على الموجه

الموجه A:

```
router bgp 65001
neighbor 10.0.0.2 remote-as 65002
```

الموجه B:

```
router bgp 65002
neighbor 10.0.0.1 remote-as 65001
```

## FireSIGHT Management Center

ملاحظة: يجب عليك إنشاء إدخالين للتحكم في الوصول، حيث إن المنفذ 179 قد يكون منفذ المصدر أو الوجهة وفقا لنظام TCP الخاص بمكبر صوت BGP الذي يقوم بإنشاء الجلسة أولا.

## القاعدة 1:

1. حدد سياسة التحكم في الوصول المطبقة على جهاز أمان FirePOWER.
2. إنشاء قاعدة التحكم في الوصول باستخدام إجراء الثقة.
3. تحت علامة التبويب منافذ، حدد (6) TCP) وأدخل المنفذ 179.
4. طققة يضيف أن يضيف الميناء إلى المصدر ميناء.
5. حفظ قاعدة التحكم بالوصول.

## القاعدة 2:

1. حدد سياسة التحكم في الوصول المطبقة على جهاز أمان FirePOWER.
2. إنشاء قاعدة التحكم في الوصول باستخدام إجراء الثقة.
3. تحت علامة التبويب المنافذ، حدد (6) TCP) وأدخل المنفذ 179.
4. طققة يضيف أن يضيف الميناء إلى الغاية ميناء.
5. حفظ قاعدة التحكم بالوصول.

3	Trust BGP TCP Source 179	any any any any any any any any	TCP (6):179	any	any	Trust	0
4	Trust BGP TCP Dest 179	any any any any any any any any	TCP (6):179	any	Trust	0	

### Editing Rule - Trust BGP TCP Source 179

Name: Trust BGP TCP Source 179  Enabled [Move](#)

Action: Trust [IPs: no policies](#) [Variables: n/a](#) [Files: no inspection](#) [Logging: no logging](#)

Zones Networks VLAN Tags Users Applications **Ports** URLs Inspection Logging Comments

Available Ports

- AOL
- Bittorrent
- DNS over TCP
- DNS over UDP
- FTP
- HTTPS
- HTTP
- IMAP
- LDAP
- NFSD-TCP

Selected Source Ports (1): TCP (6):179

Selected Destination Ports (0): any

Protocol: TCP (6) Port: Enter a port Add

Protocol: TCP (6) Port: Enter a port Add

[Save](#) [Cancel](#)

### Editing Rule - Trust BGP TCP Dest 179

Name: Trust BGP TCP Dest 179  Enabled [Move](#)

Action: Trust [IPs: no policies](#) [Variables: n/a](#) [Files: no inspection](#) [Logging: no logging](#)

Zones Networks VLAN Tags Users Applications **Ports** URLs Inspection Logging Comments

Available Ports

- AOL
- Bittorrent
- DNS over TCP
- DNS over UDP
- FTP
- HTTPS
- HTTP
- IMAP
- LDAP
- NFSD-TCP

Selected Source Ports (0): any

Selected Destination Ports (1): TCP (6):179

Protocol: TCP (6) Port: Enter a port Add

Protocol: Port: Enter a port Add

[Save](#) [Cancel](#)

التحقق

للتحقق من أن قاعدة الثقة تعمل كما هو متوقع، قم بالتقاط الحزم على جهاز أمان FirePOWER. إذا لاحظت حركة مرور EIGRP أو OSPF أو BGP في التقاط الحزمة، فلا يتم الوثوق بحركة المرور كما هو متوقع.

تلميح: قراءة للعثور على الخطوات المتعلقة بكيفية التقاط حركة مرور البيانات على أجهزة FirePOWER.

هنا بعض الأمثلة:

## EIGRP

إذا كانت قاعدة الضمان تعمل كما هو متوقع، فيجب عليك ألا ترى حركة المرور التالية:

```
IP 10.0.0.1 > 224.0.0.10: EIGRP Hello, length: 40 16:46:51.568618
IP 10.0.0.2 > 224.0.0.10: EIGRP Hello, length: 40 16:46:51.964832
```

## بروتوكول أقصر مسار أولاً (OSPF)

إذا كانت قاعدة الثقة تعمل كما هو متوقع، فيجب عليك ألا ترى حركة المرور التالية:

```
IP 10.0.0.2 > 224.0.0.5: OSPFv2, Hello, length 60 16:46:52.316814
IP 10.0.0.1 > 224.0.0.5: OSPFv2, Hello, length 60 16:46:53.236611
```

## BGP

إذا كانت قاعدة الثقة تعمل كما هو متوقع، فيجب عليك ألا ترى حركة المرور التالية:

```
IP 10.0.0.1.179 > 10.0.0.2.32158: Flags [S.], seq 1060979691, ack 3418042121, 17:10:26.871858
win 16384, options [mss 1460], length 0
IP 10.0.0.2.32158 > 10.0.0.1.179: Flags [.], ack 1, win 16384, length 0 17:10:26.872584
```

ملاحظة: لا تعد عمليات انتقال بروتوكول BGP إلى أعلى بروتوكول TCP وبروتوكولات keepalives متكررة مثل بروتوكولات العبارة الداخلية. بافتراض عدم وجود بادئات ليتم تحديثها أو سحبها، قد تحتاج إلى الانتظار لفترة أطول من الوقت للتحقق من عدم رؤية حركة مرور البيانات على المنفذ TCP/179.

## استكشاف الأخطاء وإصلاحها

إذا كنت لا تزال ترى حركة مرور بروتوكول التوجيه، فيرجى تنفيذ المهام التالية:

1. تحقق من تطبيق نهج التحكم في الوصول بنجاح من مركز إدارة FireSIGHT إلى جهاز FirePOWER. للقيام بذلك، انتقل إلى النظام < المراقبة > حالة المهمة صفحة.

2. تحقق من أن إجراء القاعدة هو Trust وليس Allow.

3. تحقق من عدم تمكين التسجيل على قاعدة الثقة.

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت  
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبل او  
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخل مه تلبل  
Cisco يخلت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه  
ىل إأمئاد ةوچرلاب ي صؤت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco  
Systems (رفوتم طبارل) ي لصلأل يزي لچن إل دن تسمل