تكوين الوصول الآمن باستخدام جدار حماية Fortigate

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين الوصول الآمن باستخدام جدار حماية Fortigate.

المتطلبات الأساسية

- تكوين توفير المستخدم
- تكوين مصادقة ZTNA SSO
- تكوين الوصول الآمن إلى VPN للوصول عن بعد

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- جدار حماية الإصدار 7.4.x من Fortigate
- الوصول الآمن
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA
- زتنا بدون زواي

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى:

- جدار حماية الإصدار 7.4.x من Fortigate
- الوصول الآمن
- Cisco Secure Client - VPN
- Cisco Secure Client - ZTNA

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

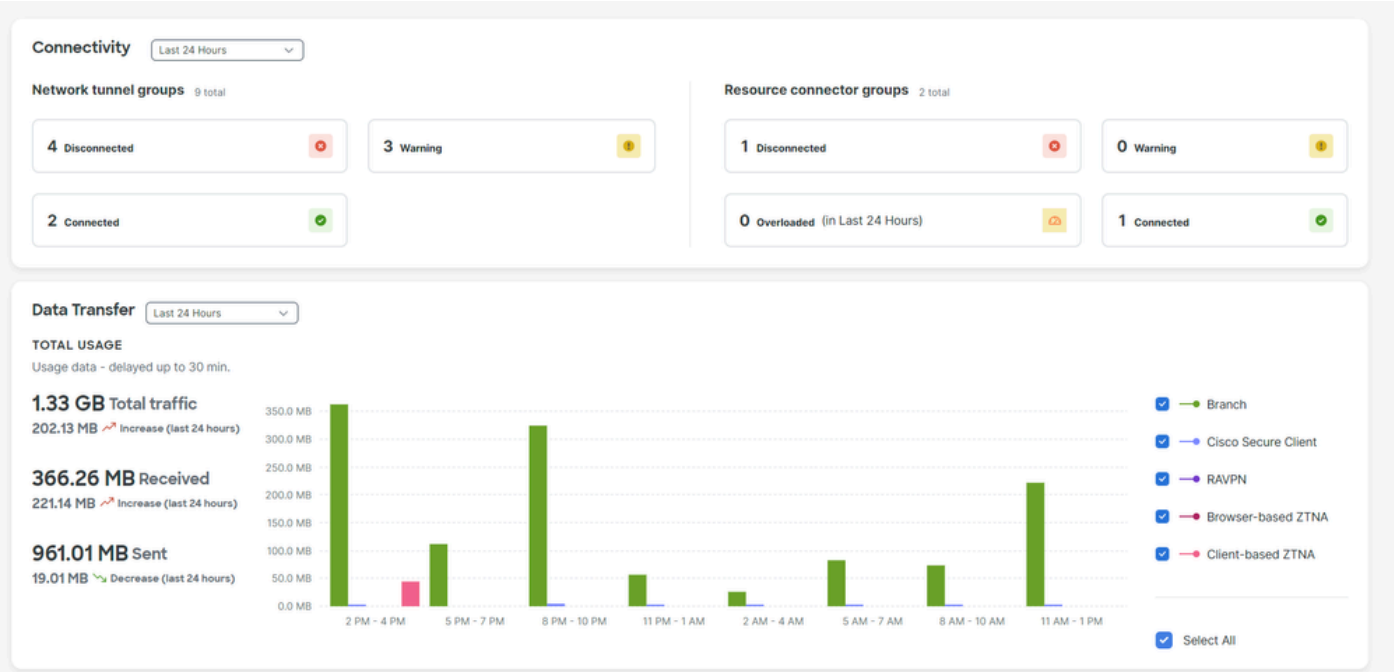
معلومات أساسية

صممت Cisco Secure Access لحماية التطبيقات الخاصة وتوفير الوصول إليها، على أساس محلي وقائمة على الشبكات. كما أنه يضمن الاتصال من الشبكة إلى الإنترنت. ويتحقق ذلك من خلال تطبيق أساليب وطبقات أمنية متعددة، تهدف جميعها إلى الحفاظ على المعلومات عند الوصول إليها عبر السحابة.

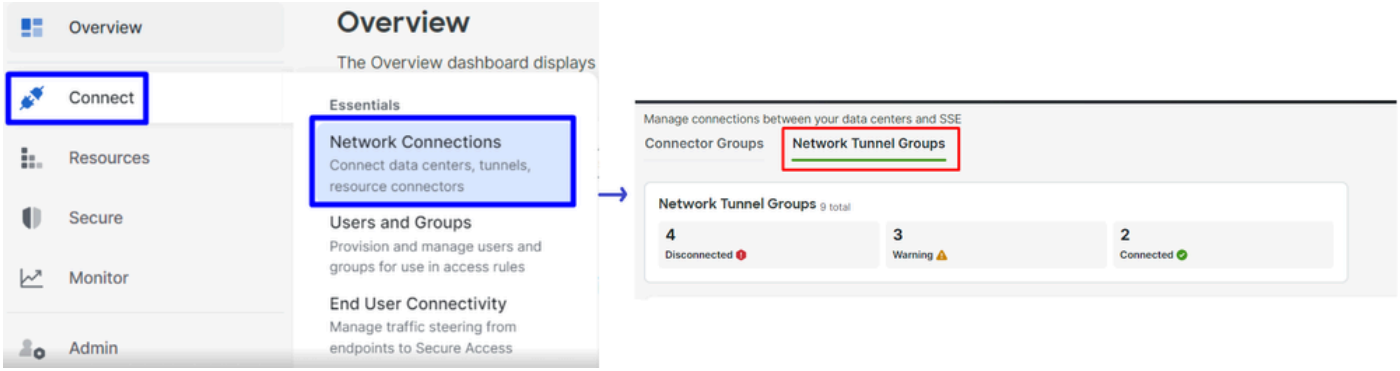
التكوين

تكوين شبكة VPN على الوصول الآمن

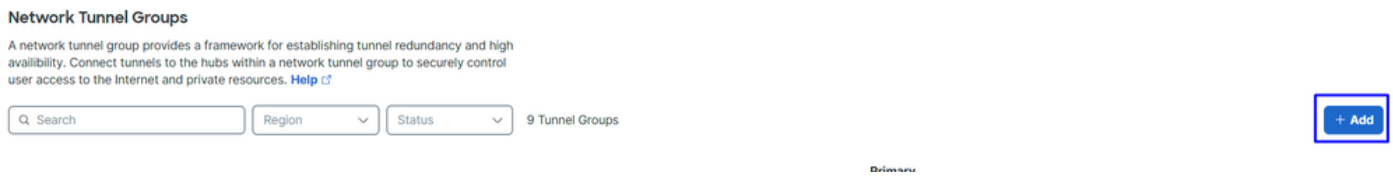
انتقل إلى لوحة الإدارة الخاصة ب Secure Access.



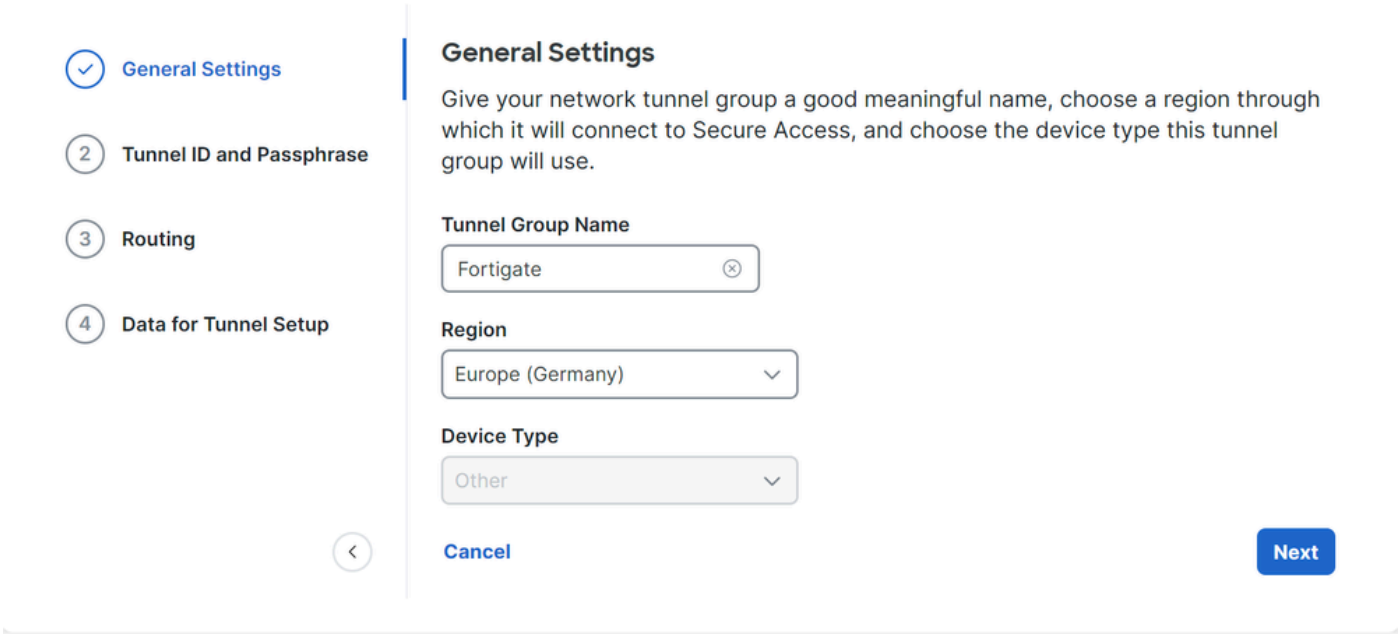
- انقر فوق Connect > Network Connections > Network Tunnels Groups

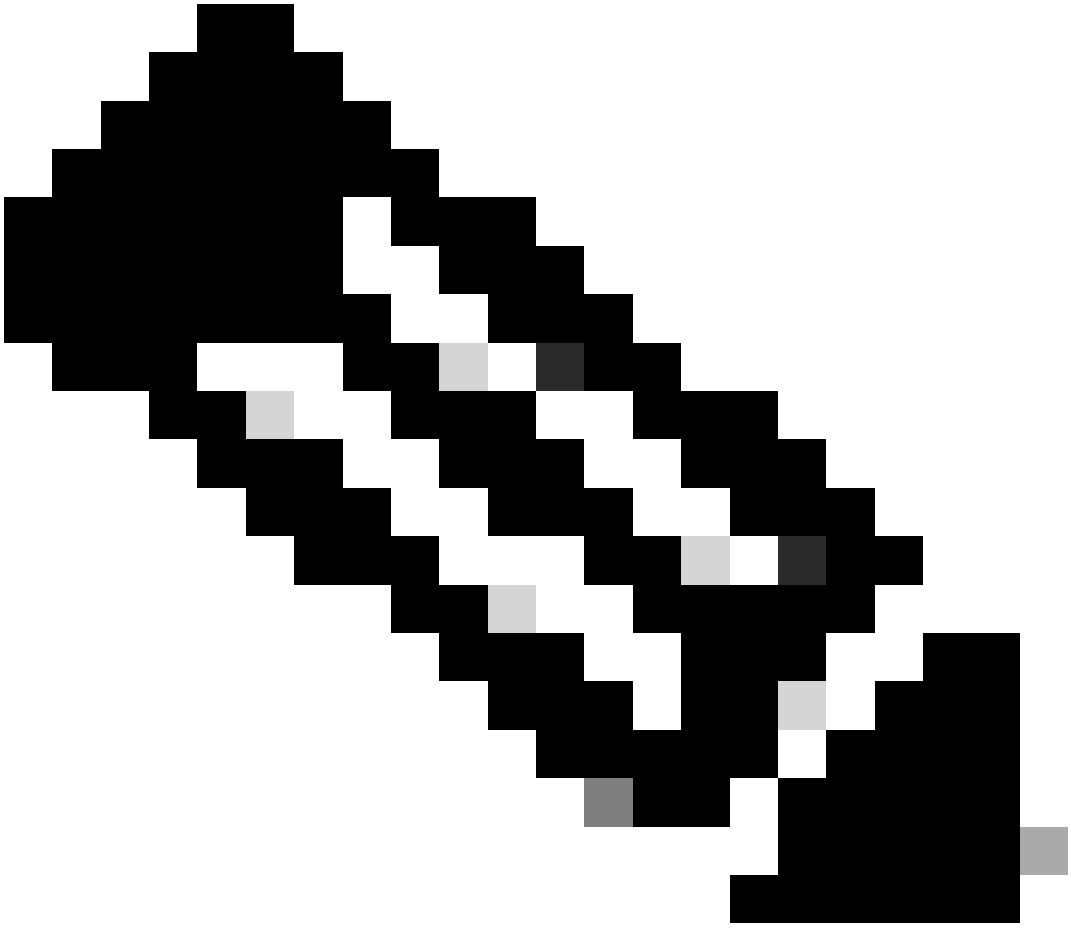


- تحت النقرNetwork Tunnel Groups فوق + Add



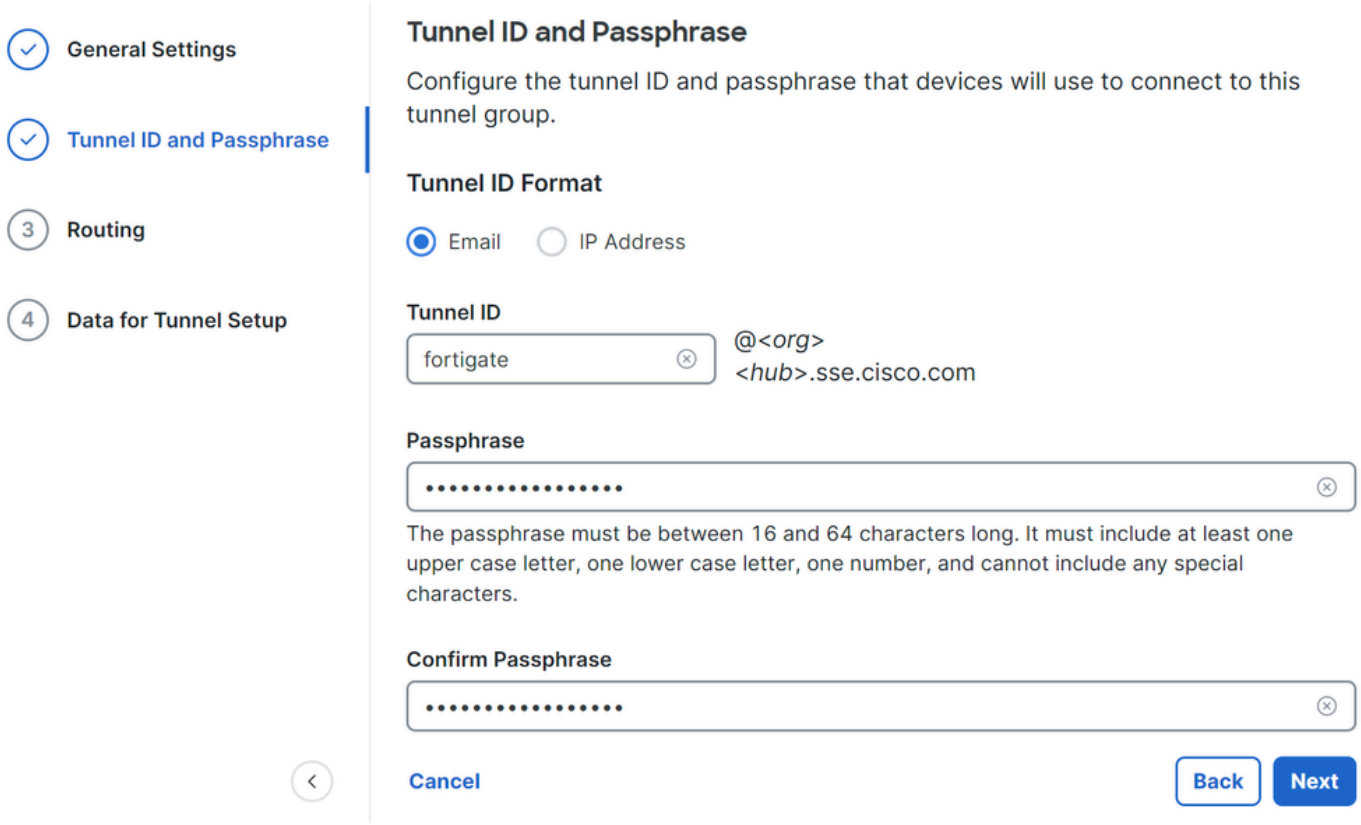
- التكوين Tunnel Group Name، Region و Device Type
- انقر **Next**


General Settings
2
Tunnel ID and Passphrase
3
Routing
4
Data for Tunnel Setup
General Settings
Give your network tunnel group a good meaningful name, choose a region through which it will connect to Secure Access, and choose the device type this tunnel group will use.
Tunnel Group Name
Fortigate
Region
Europe (Germany)
Device Type
Other
Cancel
Next



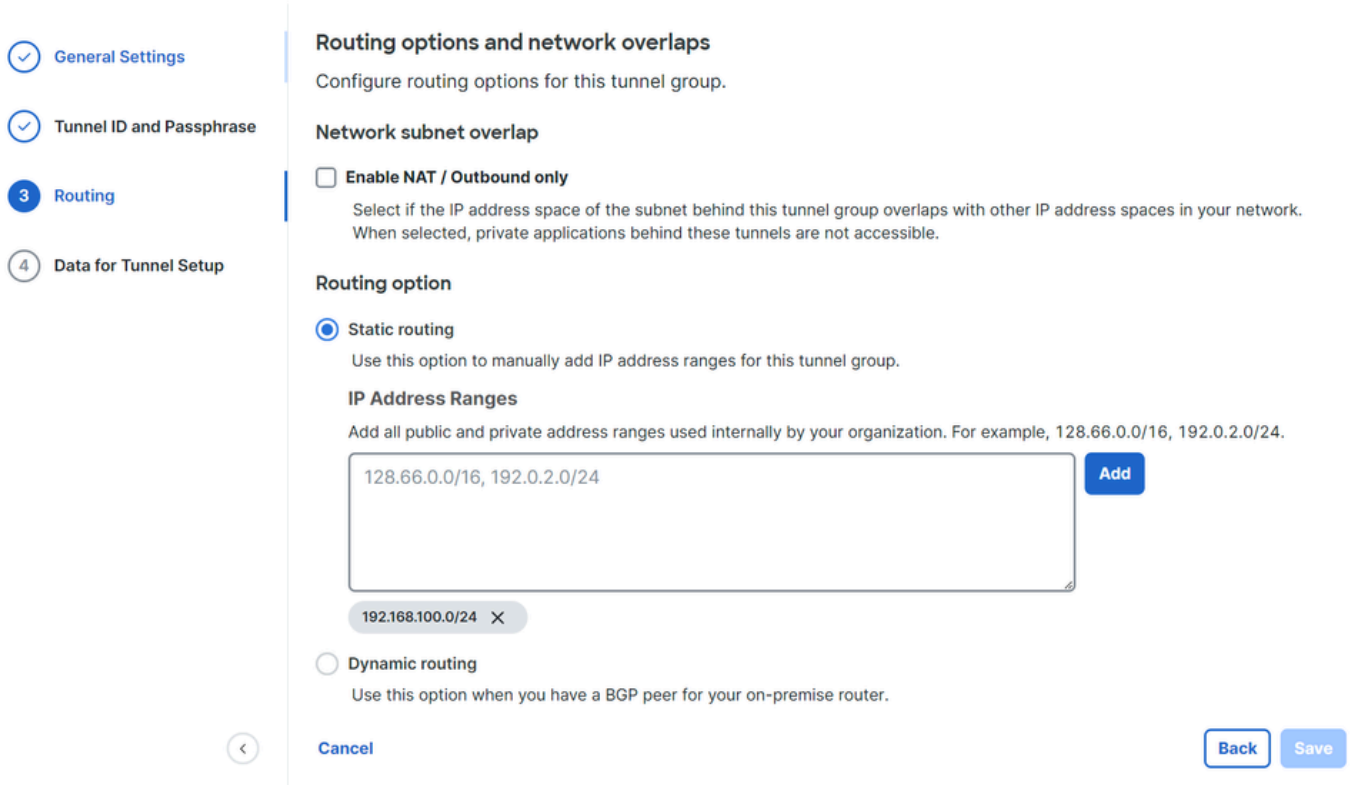
ملاحظة: أختر أقرب منطقة إلى موقع جدار الحماية.

- قم بتكوين Passphrase و Tunnel ID Format
- انقرNext



- قم بتكوين نطاقات عناوين IP أو البيئات المضيفة التي قمت بتكوينها على الشبكة وتريد تمرير حركة المرور من خلال الوصول الآمن

- انقرSave



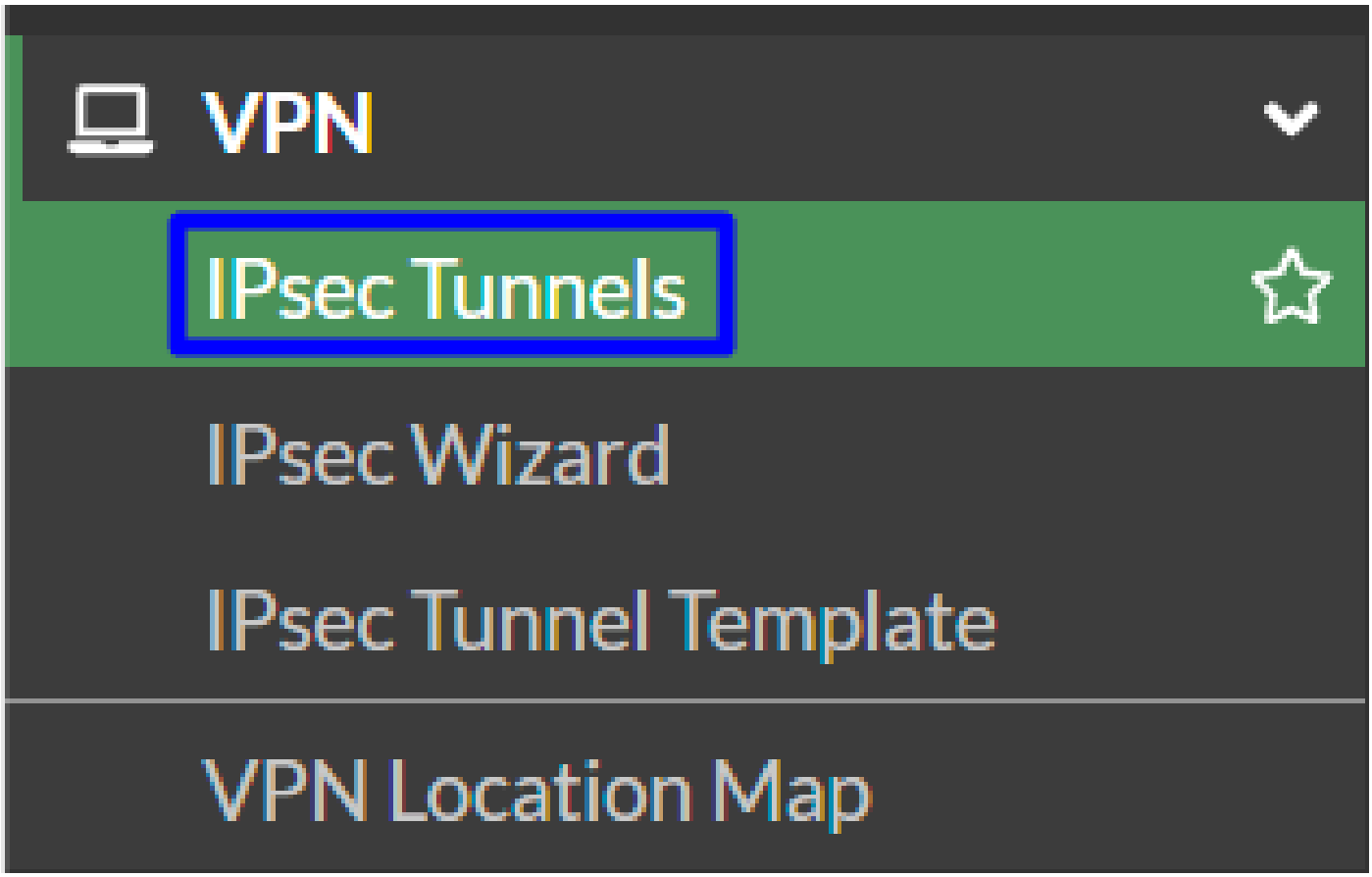
بعد النقر فوق المعلومات **Save** حول عرض النفق، الرجاء حفظ تلك المعلومات للخطوة التالية، **Configure the VPN Site to Site on Fortigate**.

بيانات النفق

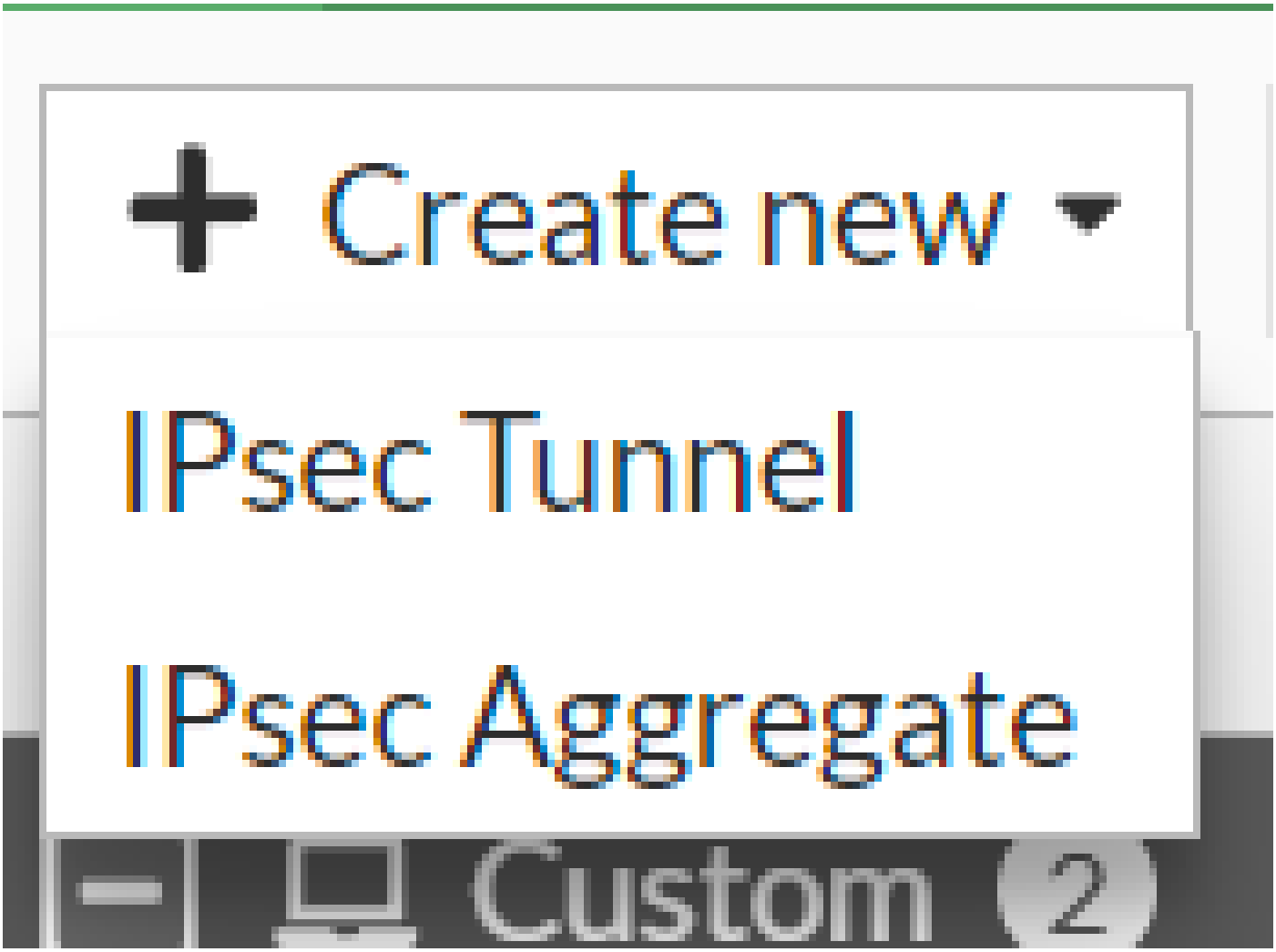
تكوين موقع VPN إلى موقع على Fortigate

انتقل إلى لوحة معلومات Fortigate.

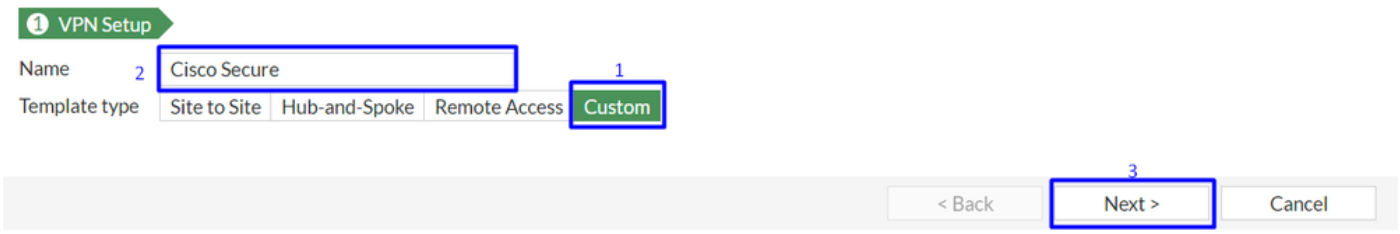
- انقر VPN > IPsec Tunnels



- انقر Create New > IPsec Tunnels

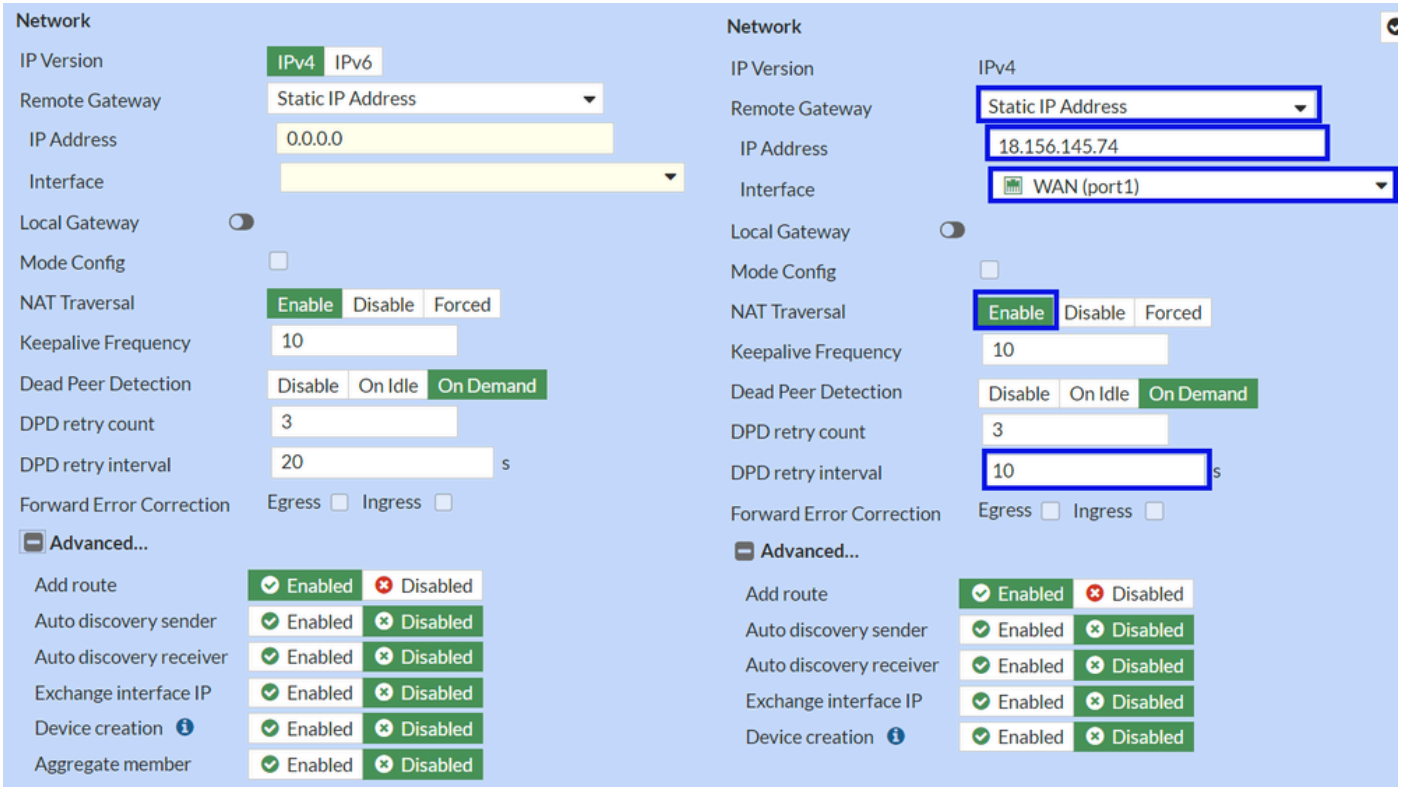


- انقر Custom، قم بتكوين a **Name** وانقر **Next**.



في الصورة التالية، رأيت كيف أنت تحتاج أن يشكل العملية إعداد **Network** للجزء.

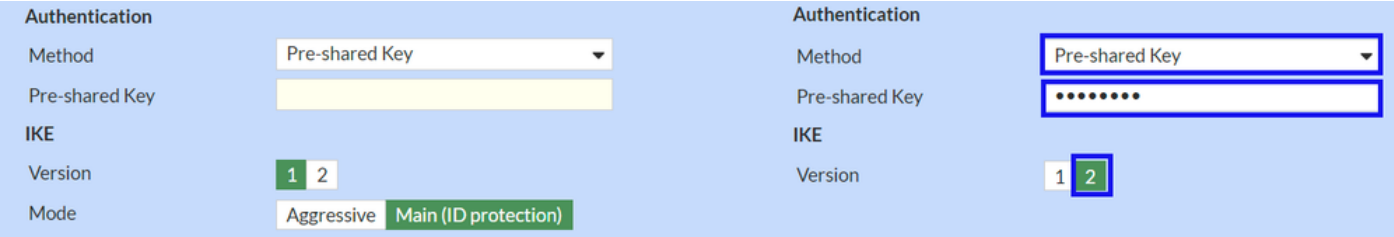
الشبكة



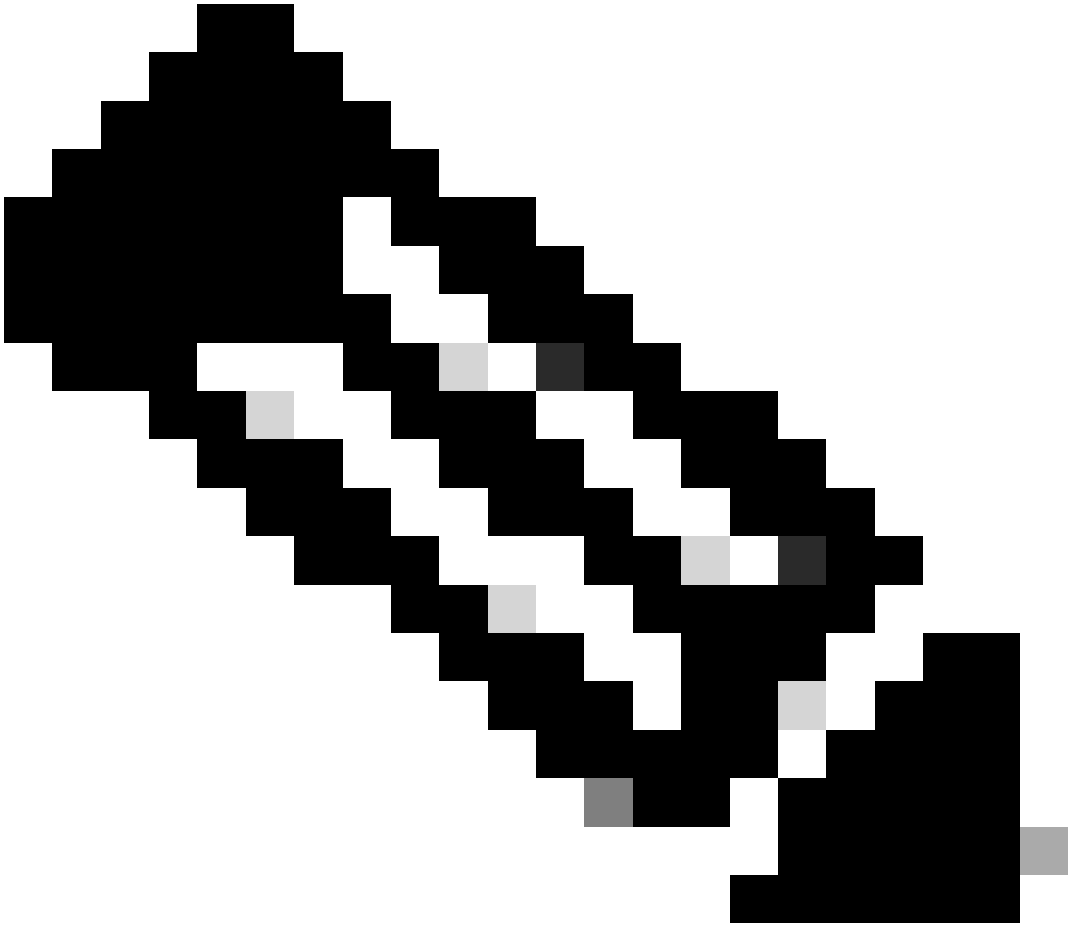
- Network
    - IP Version : IPv4
        - **Remote Gateway** :عنوان IP الثابت
        - IP Address: إستخدام IP Primary IP Datacenter IP Address,الموجود في بيانات نفق الخوطة
        - **Interface** : إختيار واجهة WAN التي خططت لاستخدامها لإنشاء النفق
        - **Local Gateway** : تعطيل كافتراضي
        - **Mode Config** : تعطيل كافتراضي
        - **NAT Traversal** :تمكين
        - **Keepalive Frequency** :10
        - Dead Peer Detection : حسب الطلب
        - **DPD retry count** :3
        - **DPD retry interval** :10
        - **Forward Error Correction** : ال تضع علامة في أي مربع.
        - **Advanced...**: قم بتكوين خصوصة.

قم الآن بتكوين IKE **Authentication**.

المصادقة



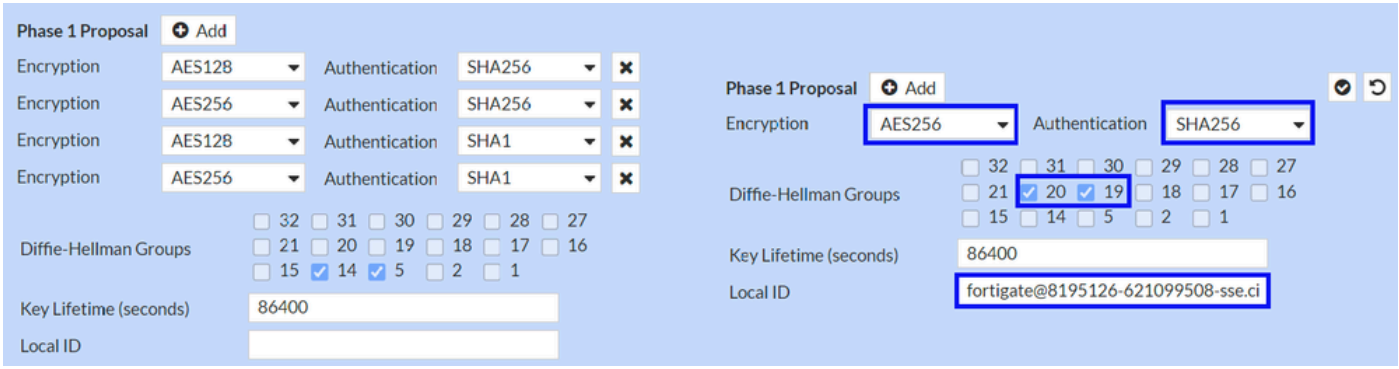
- **Authentication**
  - **Method** : مفتاح مشترك مسبقا كافتراضي
    - **Pre-shared Key** : إستخدام **Passphrase**لمعطى في قفل بيانات الخطوة
- **IKE**
  - Version : أختر الإصدار 2.



ملاحظة: يدعم Secure Access الإصدار الثاني من بروتوكول IKEv فقط

قم الآن بتكوين **Phase 1 Proposal**.

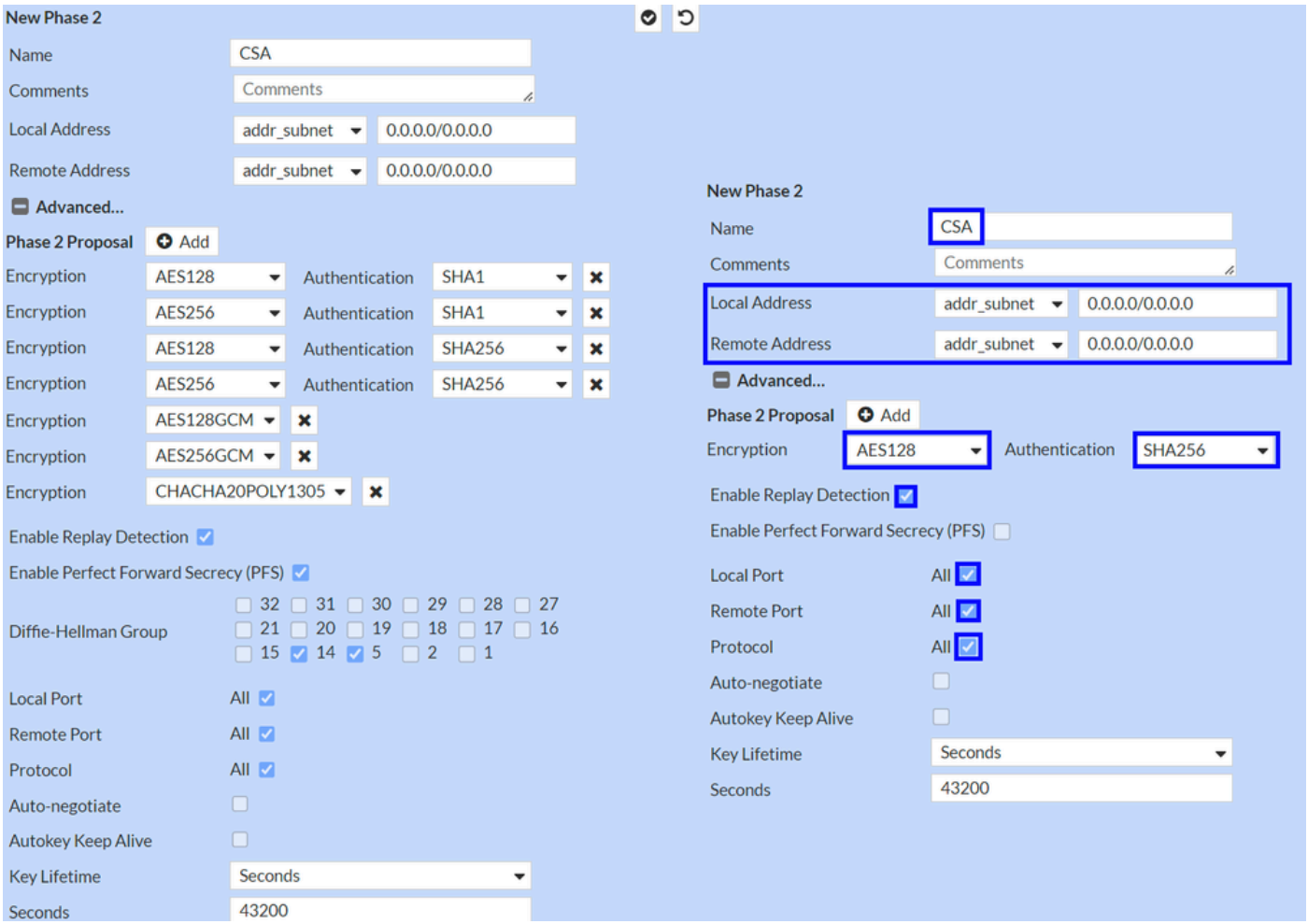
اقتراح المرحلة الأولى



- Phase 1 Proposal
    - Encryption : أختر AES256
        - Authentication : أختر SHA256
        - Diffie-Hellman Groups : حدد المربع 19 و 20
        - Key Lifetime (seconds) : 86400 كافتراضي
        - Local ID : إستخدام Primary Tunnel ID، المحدد في بيانات النفق بالخطوة

قم الآن بتكوين **Phase 2 Proposal**.

اقتراح المرحلة الثانية

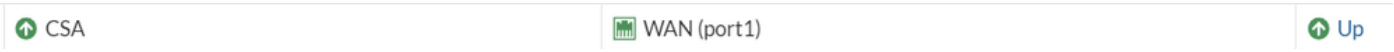


- New Phase 2
  - **Name** : كإعداد افتراضي (يتم أخذ هذه من اسم الشبكة الخاصة الظاهرية (VPN) لديك)
    - **Local Address** : كإعداد افتراضي (0.0.0.0/0.0.0.0)
    - **Remote Address** : كإعداد افتراضي (0.0.0.0/0.0.0.0)
- Advanced
  - **Encryption** : أختر AES128
    - **Authentication** : أختر SHA256
    - **Enable Replay Detection** : كن بشكل افتراضي (ممكن)
    - **Enable Perfect Forward Secrecy (PFS)** : إلغاء تحديد خانة الاختيار
    - **Local Port** :

كن بشكل افتراضي (ممكن)

- **Remote Port**: كن بشكل افتراضي (ممكن)
- **Protocol** : كن بشكل افتراضي (ممكن)
- **Auto-negotiate** : تعيين كقيمة افتراضية (بدون علامة)
- **Autokey Keep Alive** : تعيين كقيمة افتراضية (بدون علامة)
- **Key Lifetime** : تعيين كقيمة افتراضية (بالثواني)
- **Seconds** : ليكن الوضع الافتراضي (43200)

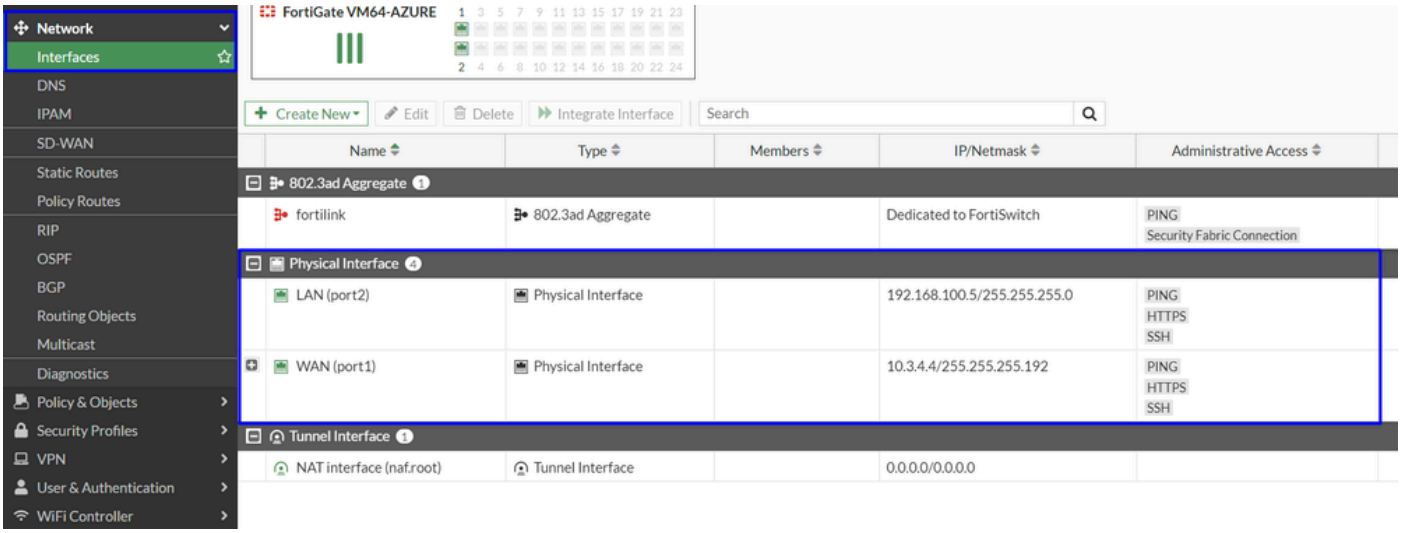
بعد ذلك، انقر فوق موافق. يمكنك بعد مرور بعض الدقائق أن الشبكة الخاصة الظاهرية (VPN) قد تم إنشاؤها باستخدام "الوصول الآمن"، ويمكنك المتابعة بالخطوة التالية، **Configure the Tunnel Interface.**



تكوين واجهة النفق

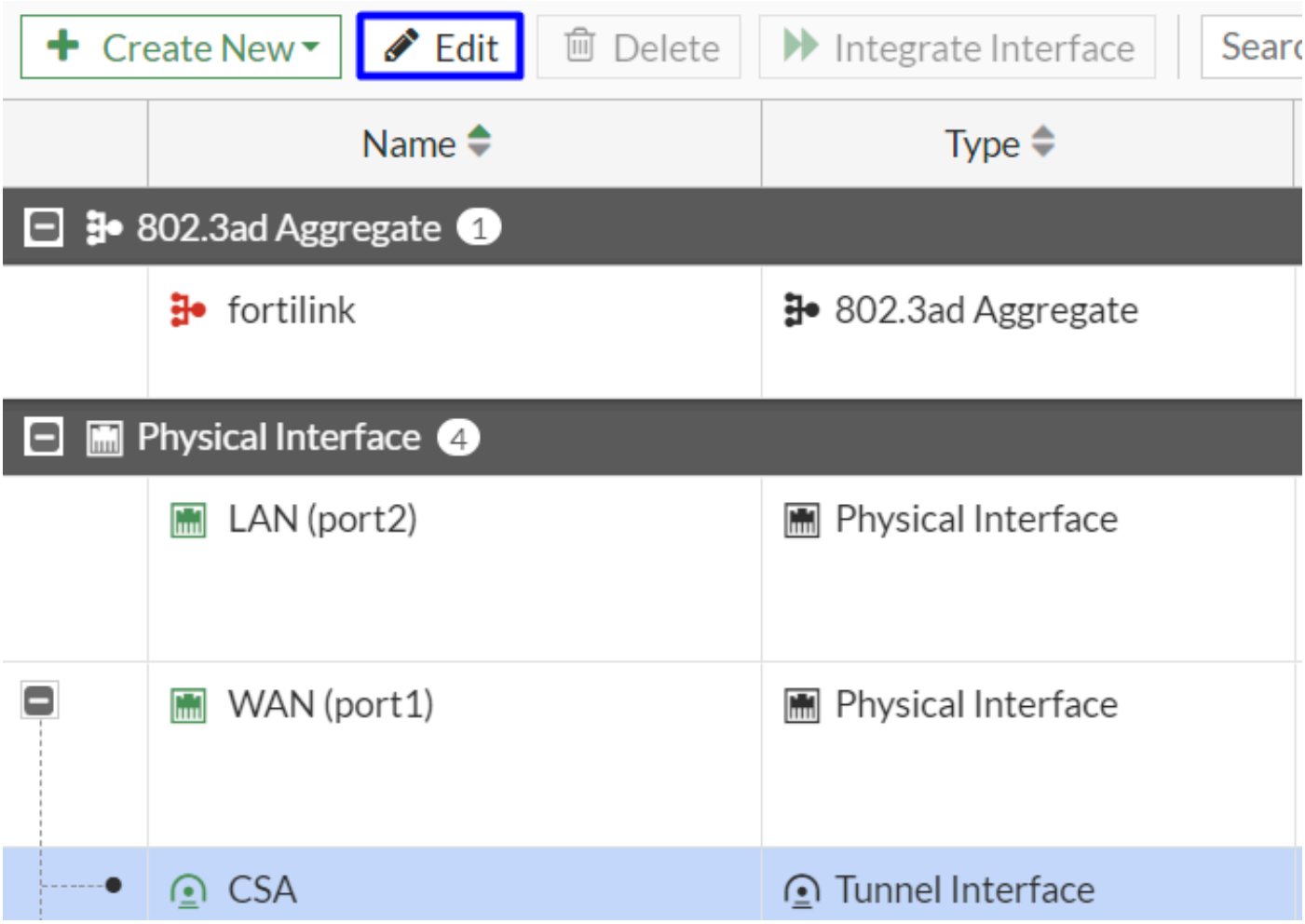
بعد إنشاء النفق، تلاحظ أن لديك واجهة جديدة خلف المنفذ الذي تستخدمه كواجهة WAN للاتصال بالمنافذ الآمنة.

للتحقق من ذلك، الرجاء الانتقال إلى **Network** > **Interfaces**.

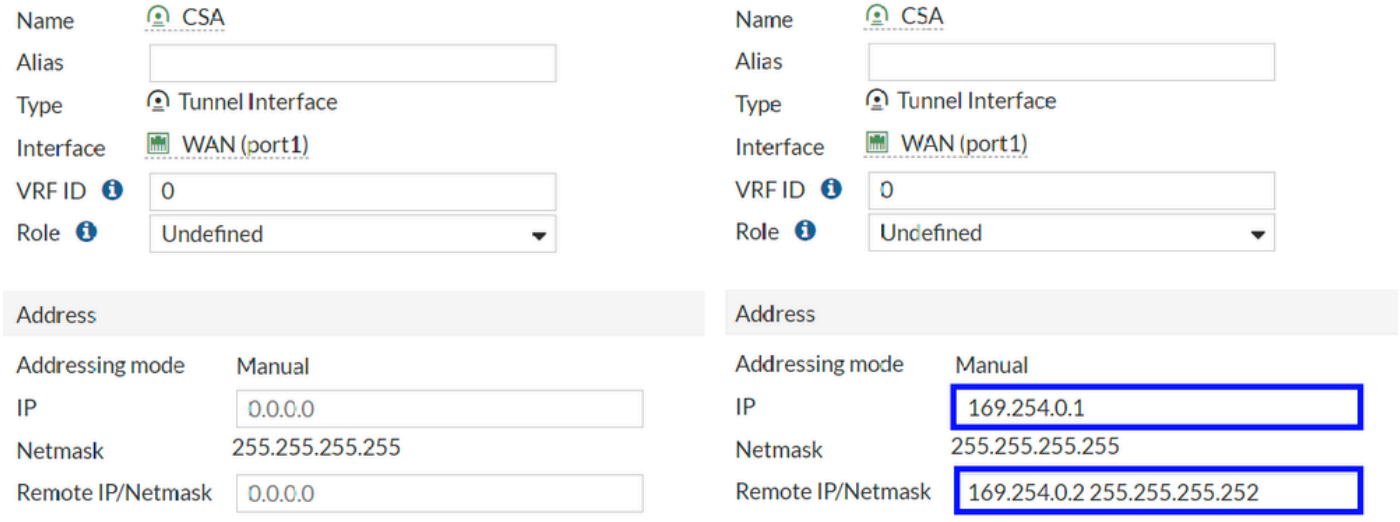


قم بتوسيع المنفذ الذي تستخدمه للاتصال ب Secure Access؛ في هذه الحالة، **WAN** الواجهة.

- انقر فوق **Tunnel Interface** ثم انقر فوق **Edit**



- لديك الصورة التالية التي تحتاج إلى تكوينها



- Interface Configuration

- IP : تكوين IP غير قابل للتوجيه ليس لديك في الشبكة (169.254.0.1)

- Remote IP/Netmask : قم بتكوين IP عن بعد كعنوان IP التالي لواجهة IP الخاصة بك باستخدام قناع الشبكة 30 (169.254.0.2 255.255.255.252)

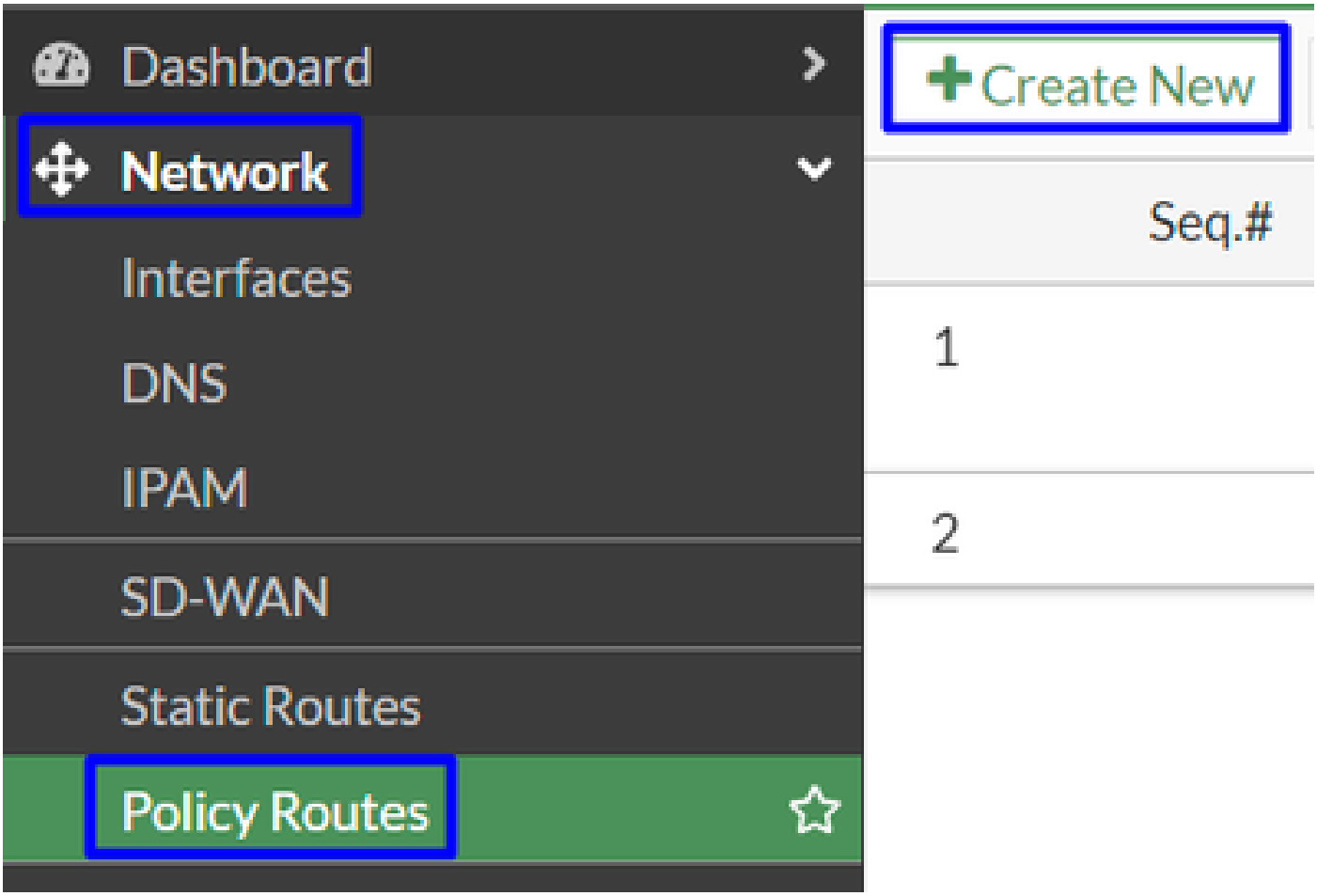
بعد ذلك، انقر **OK** لحفظ التكوين ومتابعة الخطوة التالية، Configure Policy Route (التوجيه المستند إلى الأصل).

تحذير: بعد هذا الجزء، يجب تكوين سياسات جدار الحماية على FortiGate للسماح لحركة المرور من الجهاز أو السماح لها بتأمين الوصول ومن الوصول الآمن إلى الشبكات التي تريد توجيه حركة المرور.

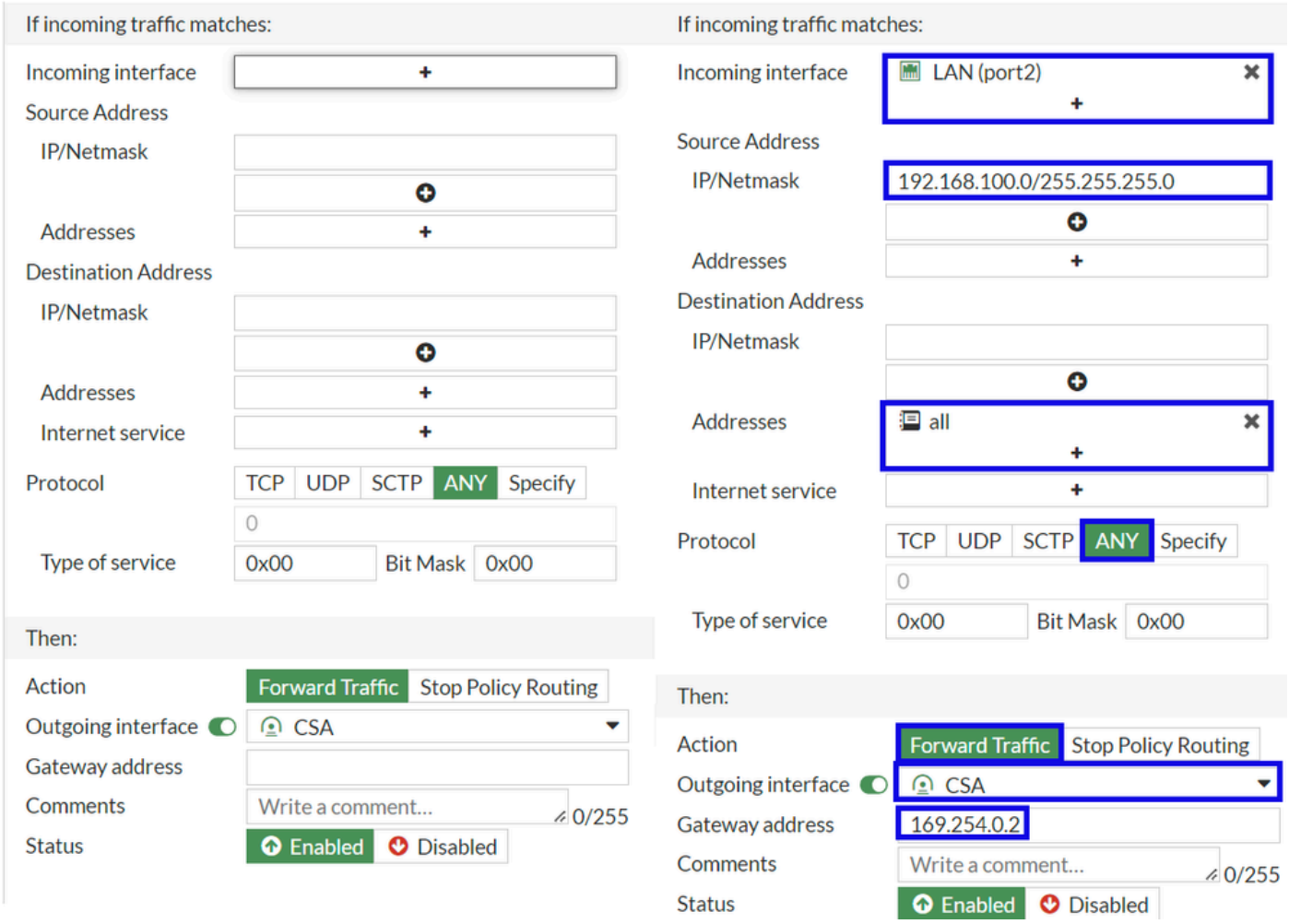
تكوين مسار السياسة

عند هذه النقطة، لديك شبكة VPN الخاصة بك تم تكوينها وإنشاءها لتأمين الوصول، والآن، يجب عليك إعادة توجيه حركة مرور البيانات لتأمين الوصول لحماية حركة المرور أو الوصول إلى التطبيقات الخاصة الخاصة بك خلف جدار حماية FortiGate.

- انتقل إلى Network > Policy Routes



- تكوين النهج



- If Incoming traffic matches
  - Incoming Interface : أختر الواجهة من حيث تخطط لإعادة توجيه حركة المرور إلى الوصول الآمن (أصل حركة المرور)
- Source Address
  - IP/Netmask : أستخدم هذا الخيار إذا قمت بتوجيه شبكة فرعية واجهة فقط
    - Addresses : أستخدم هذا الخيار إذا كان لديك الكائن الذي تم إنشاؤه ومصدر حركة المرور أتي من واجهات متعددة وشبكات فرعية متعددة
- Destination Addresses

- Addresses:اخترَ all

- Protocol:اخترَ **ANY**

- Then

- Action: **Choose Forward Traffic**

- Outgoing Interface : أختر واجهة النفق التي قمت بتعديلها على الخطوة، قم بتكوين واجهة النفق
- Gateway Address: تكوين IP البعيد الذي تم تكوينه على الخطوة و RemoteIPNetmask
- Status : أختر ممكن

انقر **OK** لحفظ التكوين، فأنت الآن جاهز للتحقق من إعادة توجيه حركة مرور الأجهزة إلى Secure Access.

التحقق من الصحة

للتحقق من إعادة توجيه حركة مرور بيانات الجهاز إلى "الوصول الآمن"، لديك خياران، يمكنك التحقق من الإنترنت والبحث عن IP العام الخاص بك، أو يمكنك تشغيل الأمر التالي باستخدام curl:

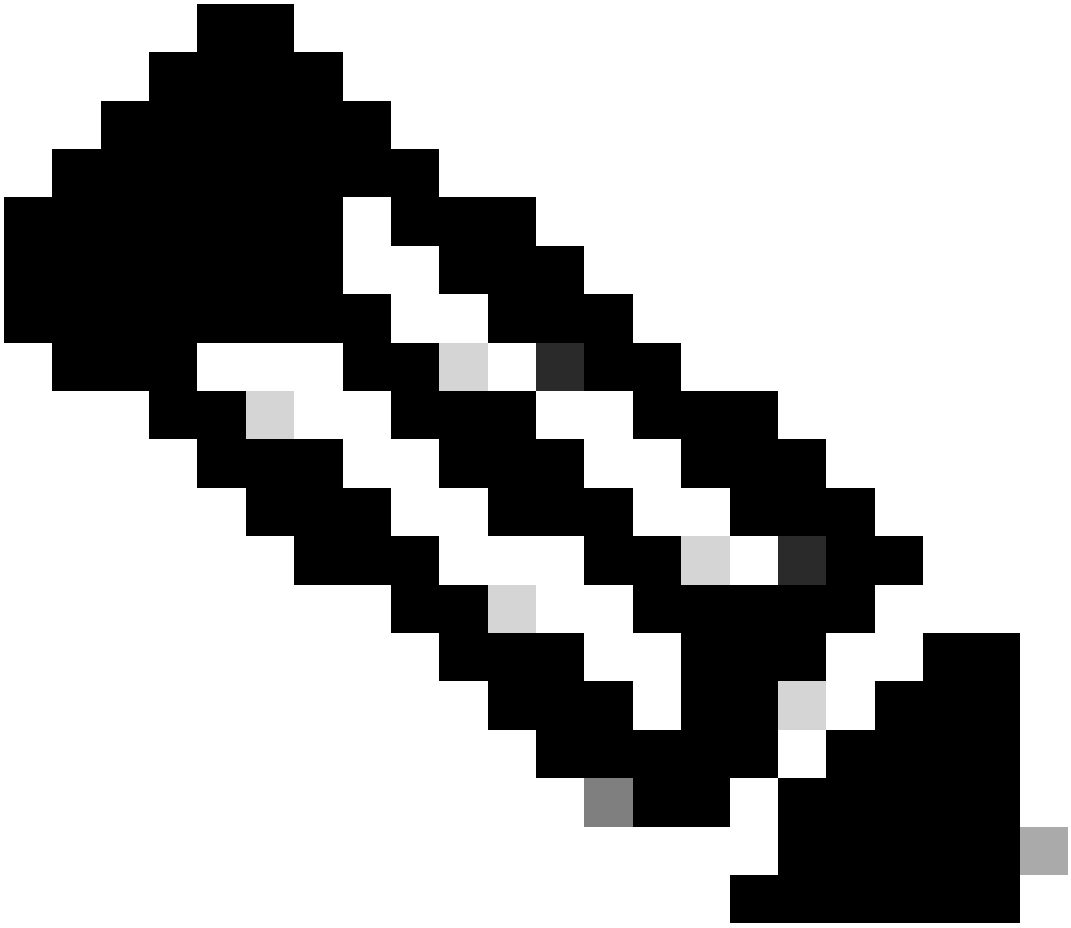
<#root>

```
C:\Windows\system32>curl ipinfo.io { "ip": "151.186.197.1", "city": "Frankfurt am Main", "region": "Hes
```

النطاق العام من حيث يمكن توقع حركة المرور الخاصة بك هو:

Min Host:151.186.176.1

Max Host :151.186.207.254



ملاحظة: تكون عناوين IP هذه عرضة للتغيير، مما يعني أن Cisco قد تقوم بتوسيع هذا النطاق في المستقبل.

إذا رأيت تغيير IP العام الخاص بك، فهذا يعني أنك محمي بواسطة Secure Access، ويمكنك الآن تكوين التطبيق الخاص بك على لوحة معلومات Secure Access للوصول إلى تطبيقاتك من VPNaS أو ZTNA.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).