﷽



**جامعة القدس المفتوحة/ فرع سلفيت**

**تقرير لمقرر أمن شبكات الحاسوب و الويب 1379**

**إعـــــــــــــــــداد :هديل فؤاد فاروق حرب**

**الرقم الجامعي:0123012110056**

**المشــــــــــــرف :أ.راضي مازن راضي علاونة**

##### **الفهرس:**

**الموضوع الصفحة**

# [**المقدمة** 3](#_Toc184819539)

## [**وظائفه الأساسية** **3**](#_Toc184819540)

# [**أنواع الجدران النارية** 3](#_Toc184819541)

## [**السياسات الداخلية للجدار الناري** 4](#_Toc184819542)

# [**تطبيق السياسات باستخدام برنامج pfSense** 4](#_Toc184819543)

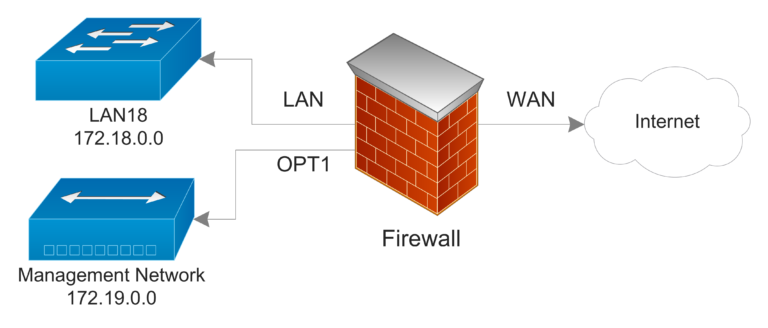
## [**كيفية تطبيق السياسات الأمنية باستخدام pfSense** 5](#_Toc184819544)

# [**مثال على سياسة أمان** 6](#_Toc184819545)

**المقدمة:**

في ظل التطور التكنولوجي المتسارع، أصبحت حماية الشبكات أمرًا بالغ الأهمية لضمان أمان البيانات ومنع الاختراقات. يُعد الجدار الناري (Firewall) من أهم الأدوات المستخدمة في هذا المجال، حيث يعمل كحاجز أمني بين الشبكة الداخلية والإنترنت أو أي شبكات خارجية أخرى. يهدف هذا التقرير إلى تقديم تصور شامل حول عمل الجدار الناري والسياسات الأمنية الداخلية وكيفية تطبيقها باستخدام برنامج مثلpfSense.

الجدار الناري (Firewall) هو نظام أمني يهدف إلى حماية الشبكات عن طريق مراقبة حركة البيانات الواردة والصادرة، ومنع أي نشاط غير مصرح به. يعمل كحاجز بين الشبكة الداخلية والجهات الخارجية، مما يضمن أمان المعلومات وسلامة الأنظمة من الاختراقات والتهديدات السيبرانية.



* **وظائفه الأساسية:**

1. **مراقبة حركة المرور:** تحليل البيانات الواردة والصادرة.
2. **منع الوصول غير المصرح به:** باستخدام قواعد وصول مخصصة.
3. **تصفية المحتوى:** منع البرامج الضارة والمواقع غير الموثوقة.
4. **الإبلاغ عن الأنشطة المشبوهة:** تسجيل المحاولات الفاشلة للوصول أو الهجمات.

* **أنواع الجدران النارية:**

1. **:Hardware Firewall** أجهزة مستقلة تُستخدم في المؤسسات الكبيرة.
2. **:** **Software Firewall**تطبيقات تُثبت على أنظمة التشغيل.
3. **:Cloud Firewall** تعمل عبر السحابة لحماية الشبكات الموزعة.

**السياسات الداخلية للجدار الناري :**

* **مفهومها:**

السياسات الداخلية هي مجموعة من القواعد التي تحدد كيفية التعامل مع البيانات المتبادلة داخل الشبكة. تعتمد على تحديد السماح (Allow)أو الحظر (Deny) بناءً على معايير مثل عنوان IP، المنفذ (Port)، والبروتوكول.

* **أمثلة على السياسات:**

1. **سياسات السماح/الحظر:** السماح بالوصول إلى خوادم معينة أو حظر مواقع معينة.
2. **سياسات التفتيش العميق للحزم : (DPI)** فحص محتوى الحزم بحثًا عن تهديدات.
3. **سياسات الحد من النطاق الترددي : (Bandwidth)** إدارة حركة المرور لمنع ازدحام الشبكة.
4. **قواعد إدارة المستخدمين:** السماح للمستخدمين المصرح لهم فقط باستخدام الموارد.

**تطبيق السياسات باستخدام برنامج pfsense:**

* **ما هو pfsense؟**

pfSense هو جدار ناري مفتوح المصدر يعمل كمنصة شاملة لإدارة الشبكات، يستند إلى نظام التشغيل FreeBSD يوفر مجموعة واسعة من الميزات المتقدمة التي تجعله خيارًا مثاليًا للشركات الصغيرة والمتوسطة، وكذلك المستخدمين الفرديين الذين يبحثون عن حماية قوية ومرونة في الإدارة.

* **المميزات الأساسية:**

1. **مفتوح المصدر:** مجاني مع إمكانية تخصيصه حسب احتياجاتك.
2. **واجهة سهلة الاستخدام:** واجهة ويب رسومية تسهّل الإعداد والإدارة.
3. **مرونة التكوين:** دعم كبير للشبكات الافتراضية الخاصة (VPN)، وجود سياسات معقدة للجدار الناري.
4. **تحديثات مستمرة:** يتلقى تحسينات أمان دورية.
5. **مجتمع دعم كبير:** موارد تعليمية وأدلة متاحة للمساعدة.

* **الاستخدامات:**
* إدارة حركة المرور (Traffic Management)
* تأمين الشبكات باستخدام VPN
* مراقبة الأداء وإصدار تقارير عن النشاط.
* تطبيق سياسات الأمان مثل تصفية المحتوى وحظر الوصول.



**كيفية تطبيق السياسات الأمنية باستخدام pfSense:**

. 1**التثبيت والإعداد الأولي:**

* القيام بتحميل نسخة pfSense من الموقع الرسمي وتثبيتها على جهاز مخصص أو افتراضي.
* البدء بإعداد عنوان IP الخاص بالجدار الناري، القيام بتوصيله بالشبكة.

. 2**إنشاء القواعد الأساسية:**

* الانتقال إلى واجهة الويب الخاصة بـ pfSense.
* الذهاب إلى قسم **Firewall > Rules** لإنشاء قواعد جديدة.
* تحديد الشبكة المصدر (Source) والشبكة الهدف (Destination)، وإضافة القواعد اللازمة مثل:
  + السماح بحركة المرور الداخلية فقط.
  + منع الوصول إلى عناوين أو منافذ غير معروفة.

.3 **إعداد VPNشبكة افتراضية خاصة:**

* لزيادة الأمان، نقوم بإعداد VPN باستخدام قسم **VPN**
* يدعم pfSense بروتوكولات مثل OpenVPN وIPSec
* يسمح ذلك بإنشاء قناة مشفرة بين المستخدمين والشبكة.

. 4**تصفية المحتوى وحظر المواقع:**

* استخدام ميزة Squid Proxy مع إضافة SquidGuard لتصفية حركة المرور.
* إضافة قائمة بالمواقع المحظورة أو السماح فقط بمواقع محددة.

.5 **إعداد سجل الأنشطة: (Logging)**

* القيام بتفعيل تسجيل الأحداث من خلال الذهاب إلى **Status > System Logs**
* يساعد هذا في مراقبة الأنشطة وتحديد التهديدات المحتملة.

.6 **تحديث قاعدة بيانات التهديدات:**

* القيام بإضافة حزمة Snort أو Suricata للكشف عن التهديدات المتقدمة.
* تعمل هذه الأدوات على تحليل البيانات بشكل عميق والإبلاغ بأي محاولات اختراق.

.7 **إعداد إشعارات الأمان:**

* الانتقال إلى **System > Advanced > Notifications** لتفعيل الإشعارات.
* القيام بتوصيل الجدار الناري بخادم بريد إلكتروني لإرسال تنبيهات عند اكتشاف تهديدات.
* **مثال على سياسة أمان:**

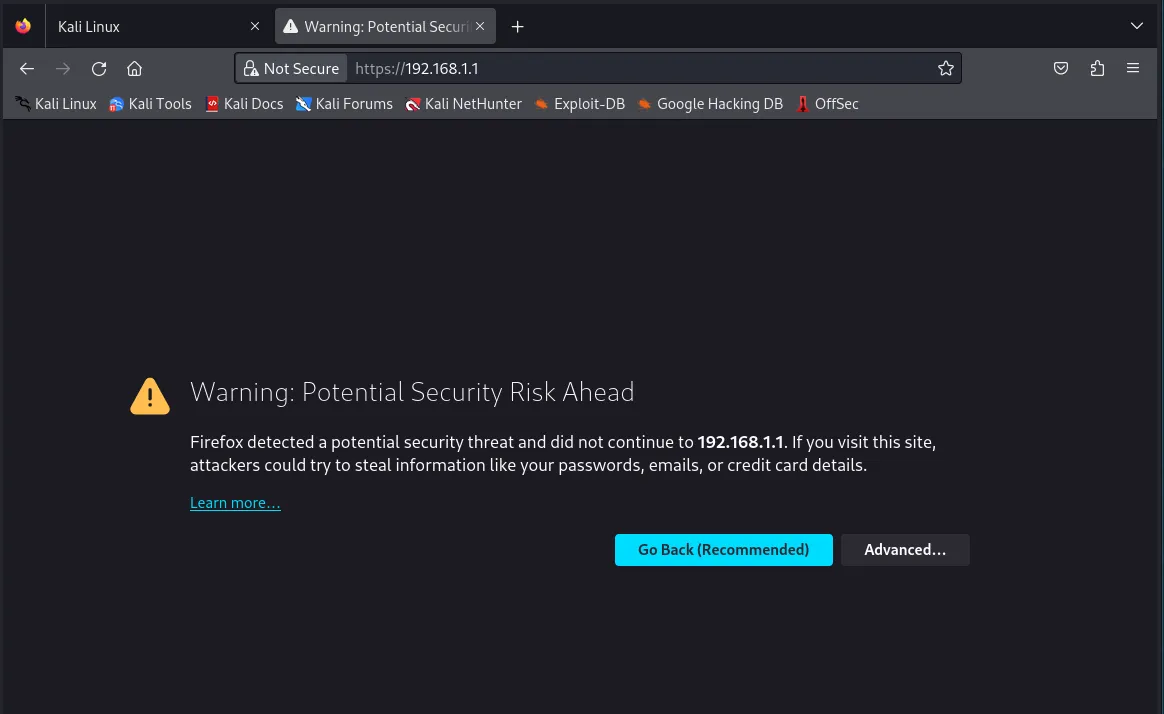
**الهدف:** السماح فقط بحركة مرور HTTP/HTTPS من الشبكة المحلية إلى الإنترنت

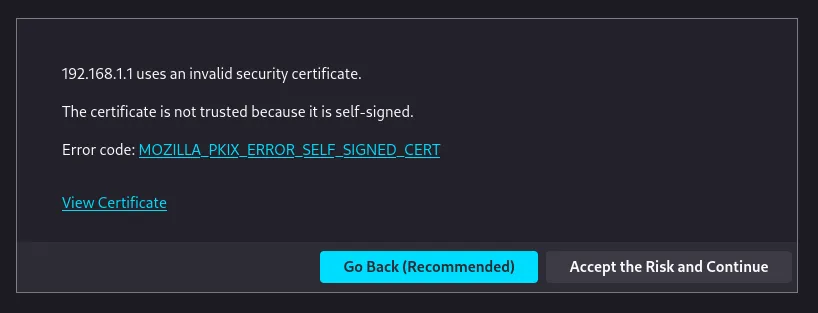
**IPV4 HTTP&HTTPS NAT AND FIREWALL RULES**

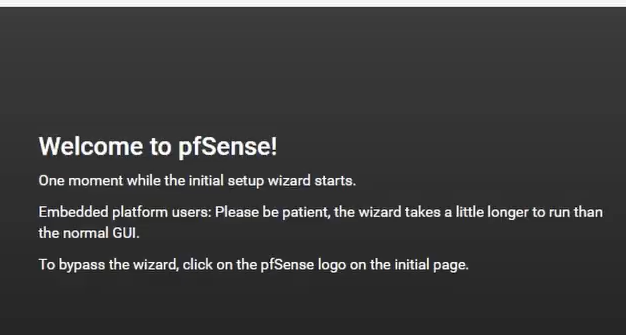
1. **القانون الأول:**
   * المصدر: الشبكة المحلية (LAN)
   * الهدف: الإنترنت (WAN)
   * البروتوكولTCP:
   * المنافذ: 80 (HTTP) و443 (HTTPS)
2. **القانون الثاني (الافتراضي):**
   * المصدر: الشبكة المحلية.
   * الهدف: الكل.
   * الإجراء: حظر (Deny)

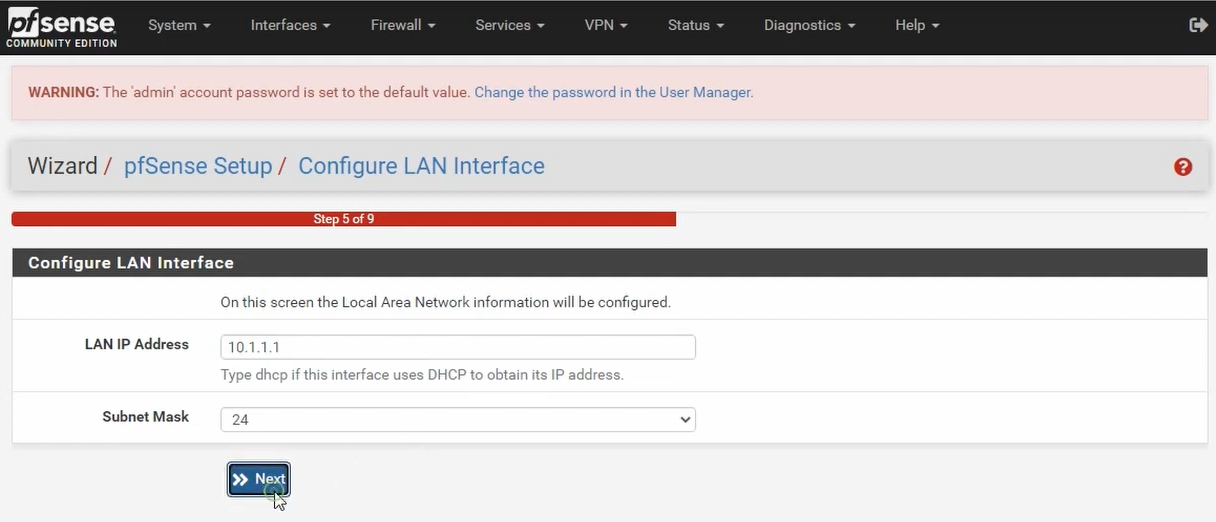
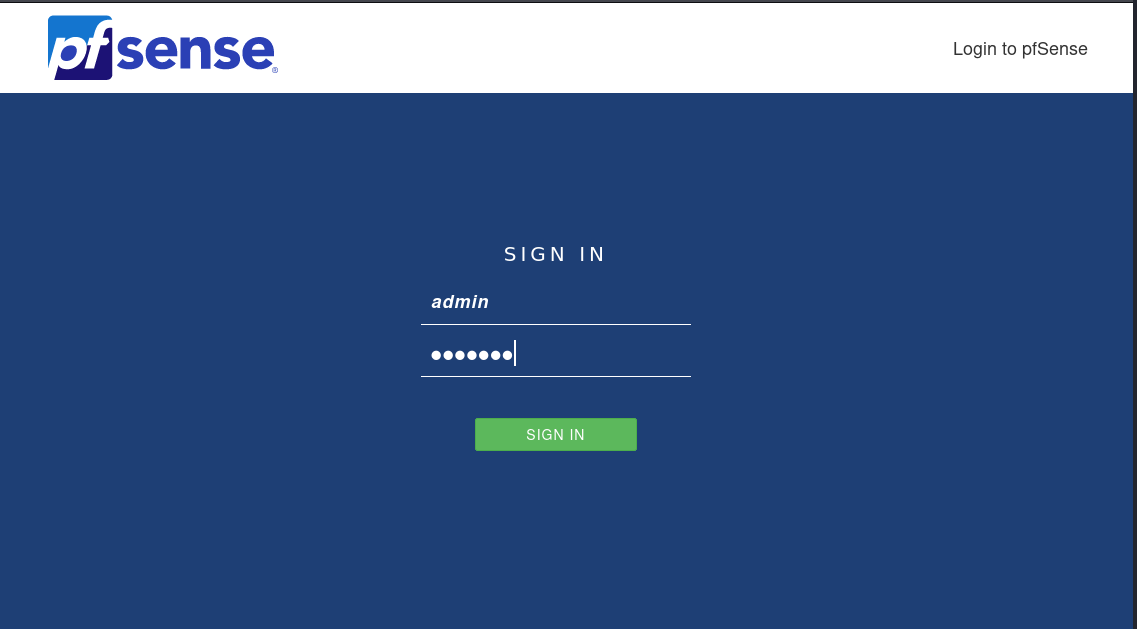
الخطوة 1: تسجيل الدخول إلى pfSense

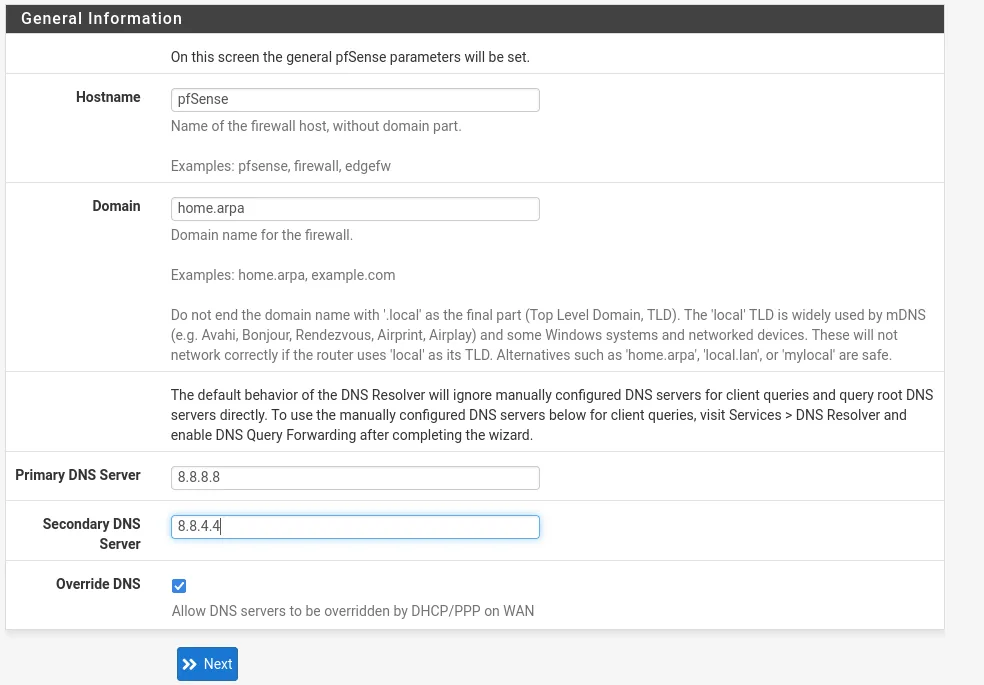
1. فتح متصفح الويب web browser و الدخول إلى واجهة إدارة pfSense
2. ادخال عنوان IP الخاص بـ pfSense (افتراضيًا: http://192.168.1.1).
3. تسجيل الدخول باستخدام بيانات الاعتماد:
   * اسم المستخدم: admin.
   * كلمة المرور: pfsense

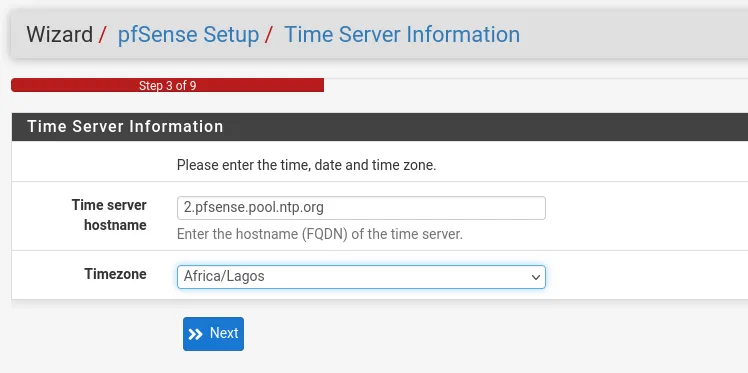






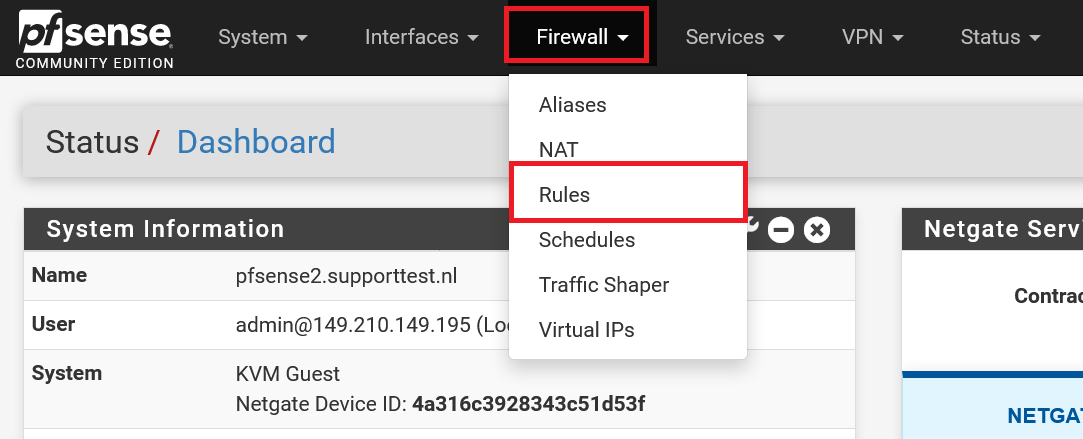






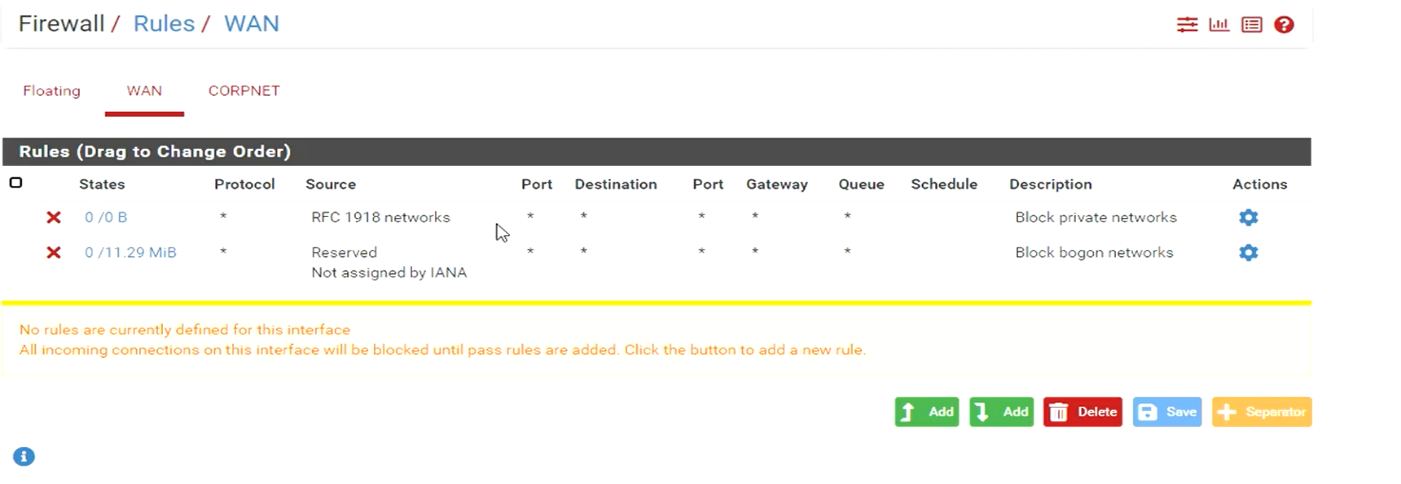
**الخطوة 2: الانتقال إلى إعدادات الجدار الناري**

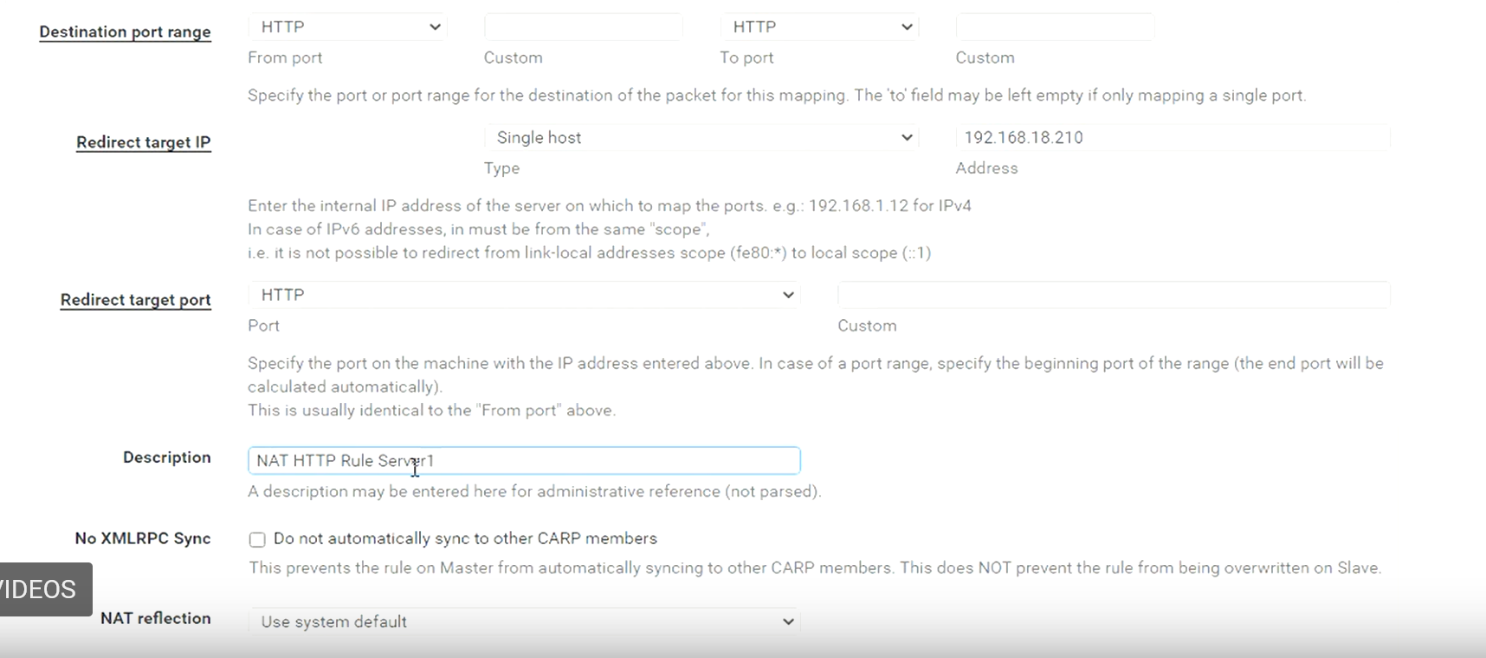
1. من القائمة الرئيسية، الانتقال إلى **Firewall > Rules**
2. اختيار علامة التبويب  **LAN** لتحديد قواعد الشبكة المحلية.

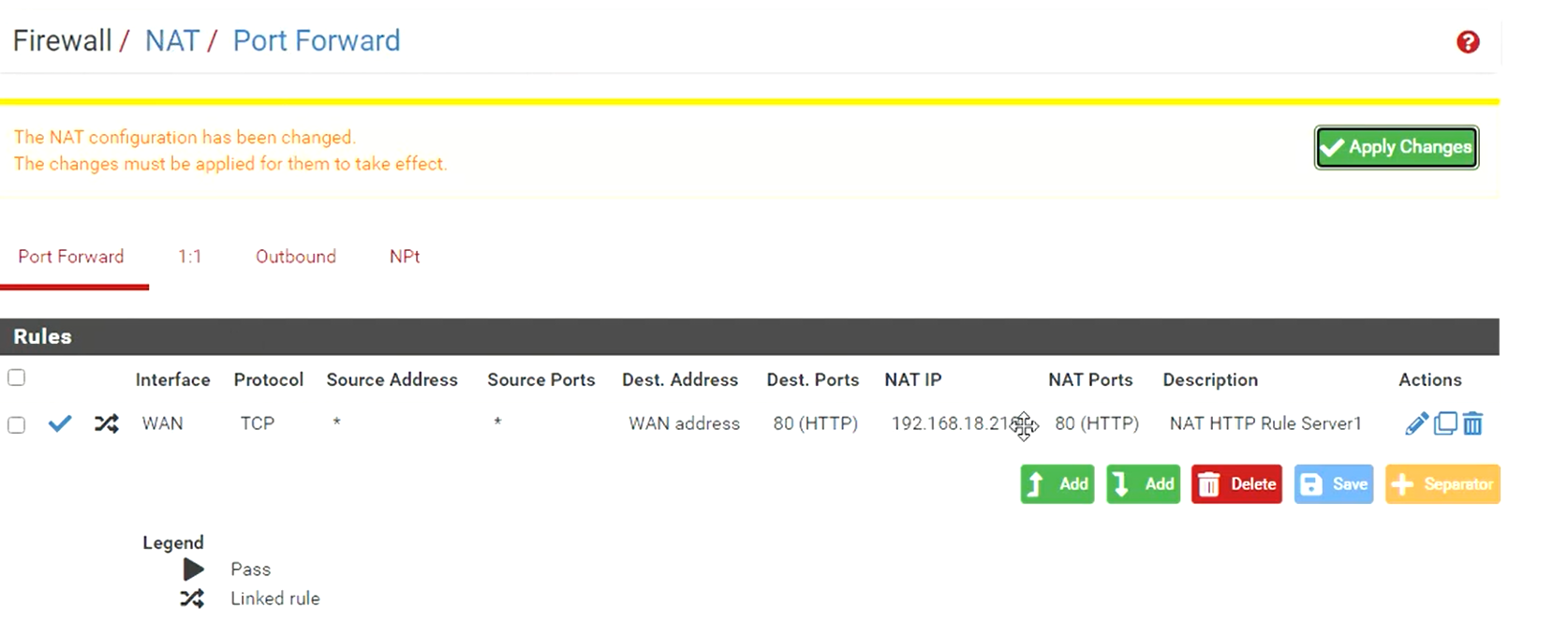


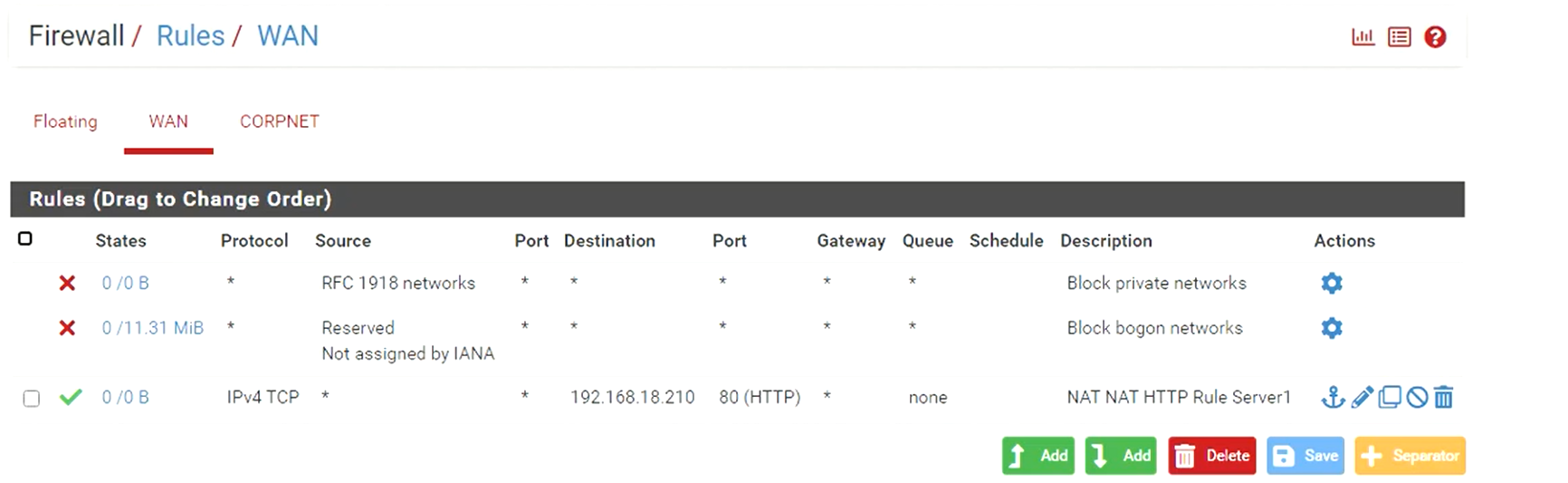
**الخطوة 3: إضافة قاعدة السماح لحركة مرور HTTP/HTTPS**

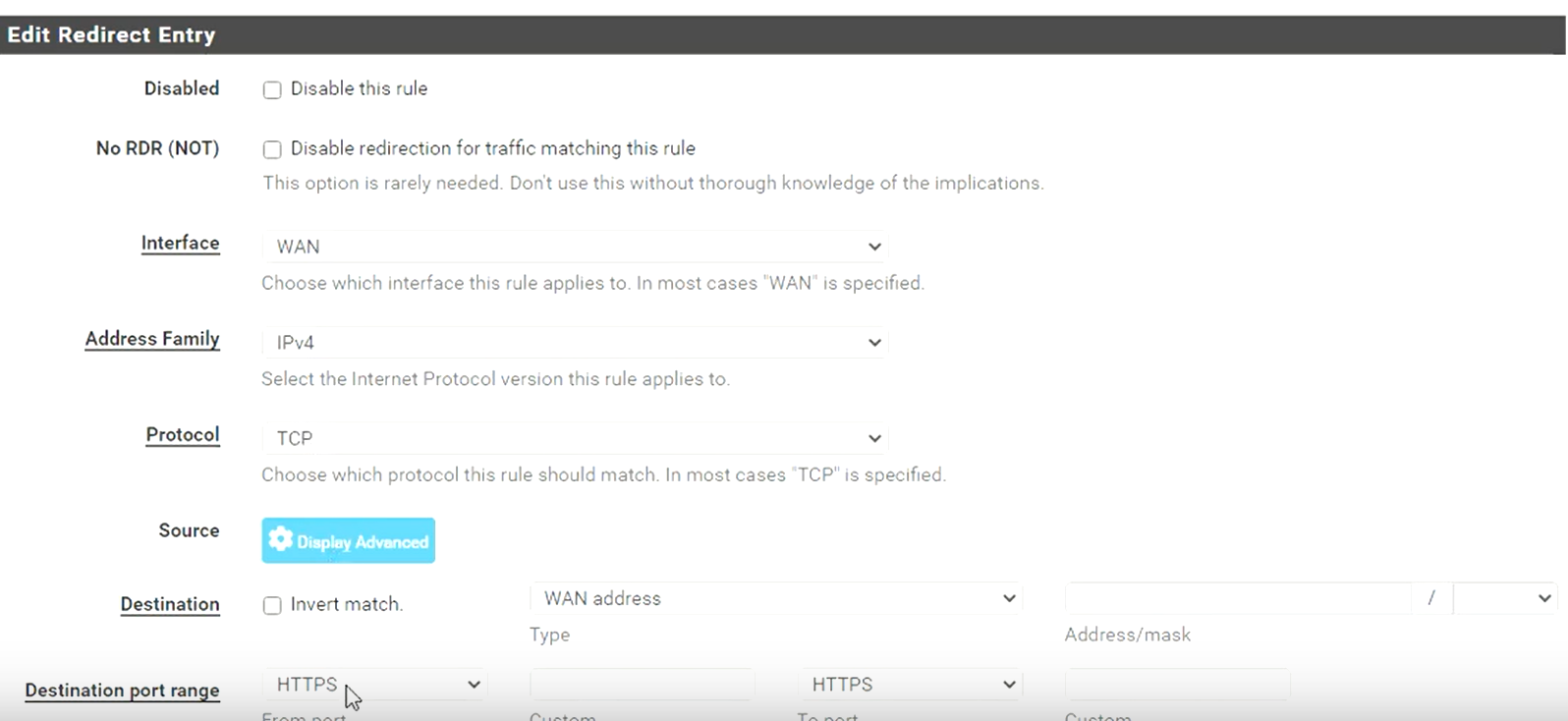
1. الضغط على زر **Add** موجودة أسفل صفحة القواعد و اختيار التبويب Port Forward.
2. القيام بتعبئة الحقول كما يلي:
   * **:** **Action**اختيار **Pass** سماح.
   * **:** **Interface**تحديد **WAN**
   * **:** **Protocol**اختيار **TCP**
   * **:Destination**
     + **:** **Type** تحديد واجهة الإنترنت (WAN) كوجهة لحركة المرور.
   * **:Destination Port Range**
     + **:** **From**اختيار **HTTP (80)**
     + **:** **To**اختيار **HTTPS (443)**
3. في مربع الوصف (Description)، نكتب: "" NAT HTTP/HTTPS Rule Server1
4. الضغط على  **Save** لحفظ القاعدة، ثم الضغط على  **Apply Changes** لتطبيقها.

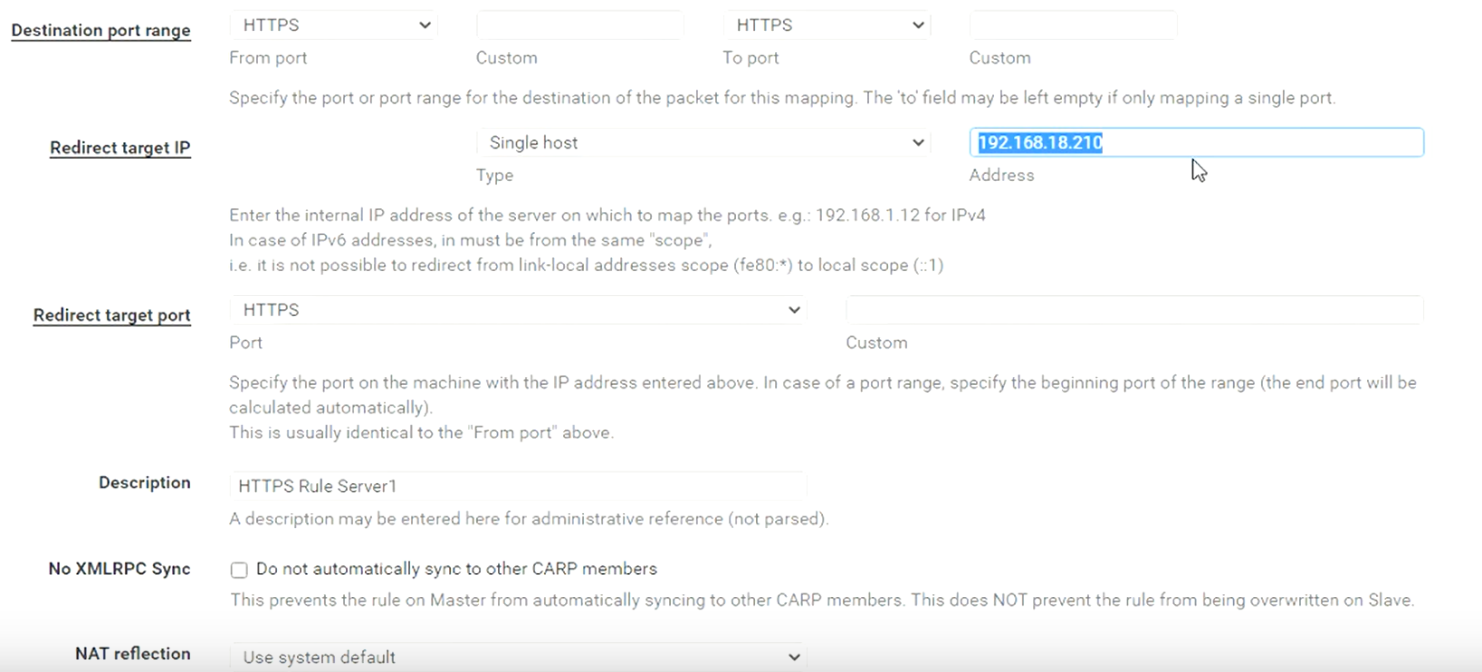


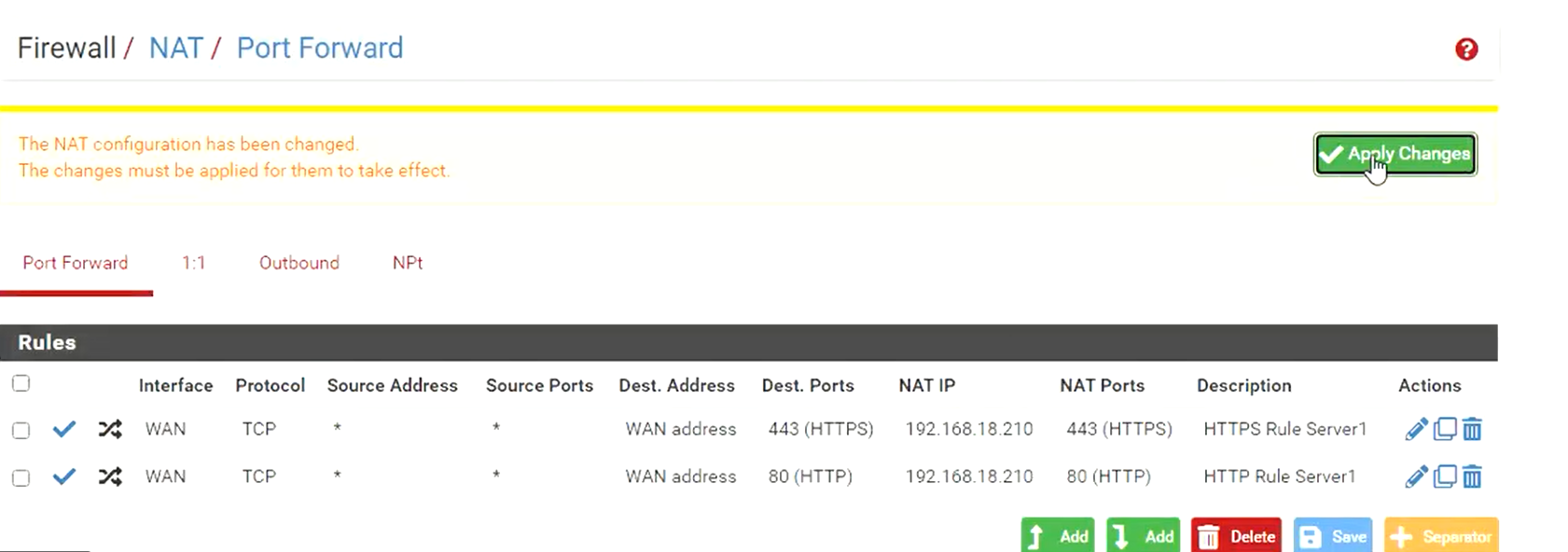


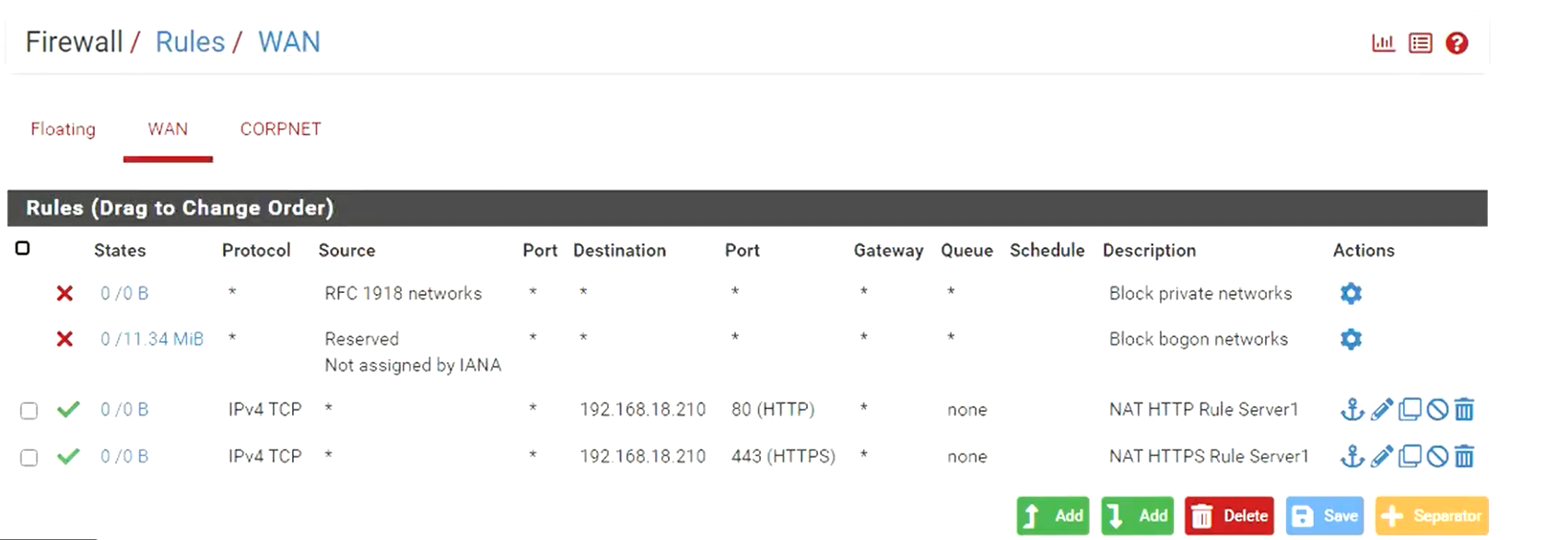


****

****

****

****

****

**الخطوة الرابعة: ترتيب القواعد:**

**السحب والإفلات:** التأكد من أن القاعدة الجديدة تقع في أعلى قائمة القواعد. هذا يضمن تطبيقها قبل أي قواعد أخرى.

**الخطوة 5: التحقق من السياسات**

1. الانتقال إلى **Status > System Logs > Firewall**
2. التحقق من سجلات حركة المرور للتأكد من أن:
   * حركة مرور HTTP/HTTPS مسموحة.
   * جميع الحركات الأخرى محظورة.