ECE용 pfSense 커뮤니티 로드 밸런서 구성

목차

소개

이 문서에서는 ECE(Enterprise Chat and Email)용 로드 밸런서로 pfSense Community Edition을 설정하고 구성하는 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ECE 12.x
- pfSense 커뮤니티 버전

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- ECE 12.6(1)
- pfSense Community Edition 2.7.2

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

pfSense 설치

솔루션 개요

pfSense Community Edition은 방화벽, 로드 밸런서, 보안 스캐너 및 기타 여러 서비스를 단일 서버에서 제공하는 다기능 제품입니다. pfSense는 무료 BSD에 구축되며 하드웨어 요구 사항이 최소화됩니다. 로드 밸런서는 HAProxy의 구현이며, 제품을 구성하기 위해 사용하기 쉬운 GUI가 제공됩니다.

이 로드 밸런서는 ECE 및 CCMP(Contact Center Management Portal)에서 모두 사용할 수 있습니다. 이 문서에서는 ECE에 대해 pfSense를 구성하는 단계를 설명합니다.

준비

1단계. pfSense 소프트웨어 다운로드

pfSense 웹 사이트를 사용하여 iso 설치 관리자 이미지를 다운로드합니다.

2단계. VM 구성

최소 요구 사항으로 VM을 구성합니다.

· 64비트 amd64(x86-64) 호환 CPU

· 1GB 이상의 RAM

· 8GB 이상의 디스크 드라이브(SSD, HDD 등)

· 하나 이상의 호환 가능한 네트워크 인터페이스 카드

· 초기 설치용 부팅 가능 USB 드라이브 또는 대용량 옵티컬 드라이브(DVD 또는 BD)

실습 설치의 경우 NIC(네트워크 인터페이스)가 하나만 필요합니다. 어플라이언스를 실행하는 방법에는 여러 가지가 있지만 단일 NIC를 사용하는 것이 가장 쉽고 원 암 모드라고도 합니다. 원 암(one-arm) 모드에서는 네트워크와 통신하는 단일 인터페이스가 있습니다. 이것은 쉬운 방법이고 실험실에 적합한 방법이지만, 가장 안전한 방법은 아니다.

어플라이언스를 구성하는 보다 안전한 방법은 NIC가 2개 이상 있는 것입니다. NIC 하나는 WAN 인터페이스이며 공용 인터넷과 직접 통신합니다. 두 번째 NIC는 LAN 인터페이스이며 내부 기업 네트워크와 통신합니다. 보안 및 방화벽 규칙이 서로 다른 네트워크의 다양한 부분과 통신하기 위해 인터페이스를 추가할 수도 있습니다. 예를 들어, NIC 하나가 공용 인터넷에 연결되고, 하나는 모든 외

부 액세스 가능 웹 서버가 있는 DMZ 네트워크에 연결되고, 다른 하나는 기업 네트워크에 연결되도록 할 수 있습니다. 이렇게 하면 내부 및 외부 사용자가 DMZ에 유지되는 동일한 웹 서버 세트에 안전하게 액세스할 수 있습니다. 구현하기 전에 모든 설계의 보안 영향을 이해해야 합니다. 특정 구현에 대한 모범 사례를 준수하려면 보안 엔지니어에게 문의하십시오.

설치

1단계. VM에 ISO 마운트

2단계. VM의 전원을 켜고 프롬프트에 따라 설치합니다.

단계별 지침은 이 문서를 참조하십시오.

네트워크 설정

컨피그레이션을 계속하려면 어플라이언스에 IP 주소를 할당해야 합니다.

✎ 참고: 이 문서에서는 원 암(one-arm) 모드로 구성된 어플라이언스를 보여줍니다.

1단계. VLAN 구성

VLAN 지원이 필요한 경우 첫 번째 질문에 y를 입력합니다. 그렇지 않으면 n으로 응답합니다.

2단계. WAN 인터페이스 할당

WAN 인터페이스는 2암(two-arm) 모드에서는 어플라이언스의 비보안 측면이며 1암(one-arm) 모드에서는 유일한 인터페이스입니다. 프롬프트가 표시되면 인터페이스 이름을 입력합니다.

3단계. LAN 인터페이스 할당

LAN 인터페이스는 투암(two-arm) 모드에서 어플라이언스의 보안 측면입니다. 필요한 경우 프롬프트가 표시되면 인터페이스 이름을 입력합니다.

4단계. 기타 인터페이스 할당

특정 설치에 필요한 다른 인터페이스를 구성합니다. 이는 선택 사항이며 일반적이지 않습니다.

5단계. 관리 인터페이스에 IP 주소 할당

네트워크에서 DHCP를 지원하는 경우 할당된 IP 주소가 콘솔 화면에 표시됩니다.

```
browser:
                http://14.10.172.250/

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: b2d05c55bab7b75fe6c2

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> vmx0       -> v4: 14.10.172.250/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

pfSense 콘솔

할당된 주소가 없거나 특정 주소를 할당하려면 다음 단계를 수행합니다.

1. 콘솔 메뉴에서 옵션 2를 선택합니다.
2. DHCP를 비활성화하려면 n을 입력합니다.
3. WAN 인터페이스의 IPv4 주소를 입력합니다.
4. 넷마스크(비트 수)를 입력합니다. (24 = 255.255.255.0, 16 = 255.255.0.0, 8 = 255.0.0)
5. WAN 인터페이스의 게이트웨이 주소를 입력합니다.
6. 이 게이트웨이를 어플라이언스의 기본 게이트웨이로 지정하려면 게이트웨이 프롬프트에 y를 입력하고 그렇지 않으면 n을 입력합니다.
7. 원하는 경우 IPv6용 NIC를 구성합니다.
8. 인터페이스에서 DHCP 서버를 비활성화합니다.
9. WebConfigurator 프로토콜에서 HTTP를 활성화하려면 y를 입력합니다. 이는 다음 단계에서 사용됩니다.

그러면 설정이 업데이트되었다는 확인 메시지가 표시됩니다.

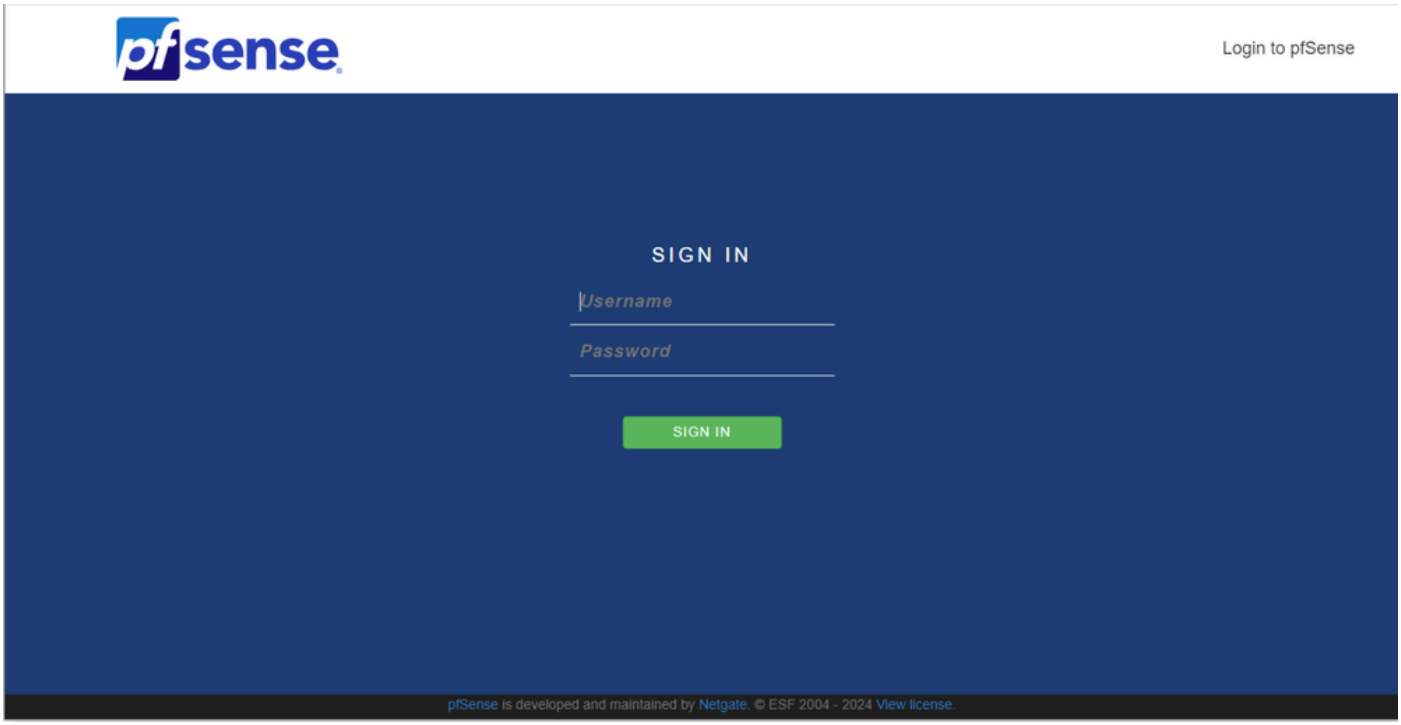
```
The IPv4 WAN address has been set to 14.10.172.250/25
You can now access the webConfigurator by opening the following URL in your web
browser:
                http://14.10.172.250/

Press <ENTER> to continue.
```

pfSense 확인

초기 설정 완료

1단계. 웹 브라우저를 열고 http:// <ip_address_of_appliance>로 이동합니다.

✎ 참고: 처음에는 HTTPS가 아닌 HTTP를 사용해야 합니다.

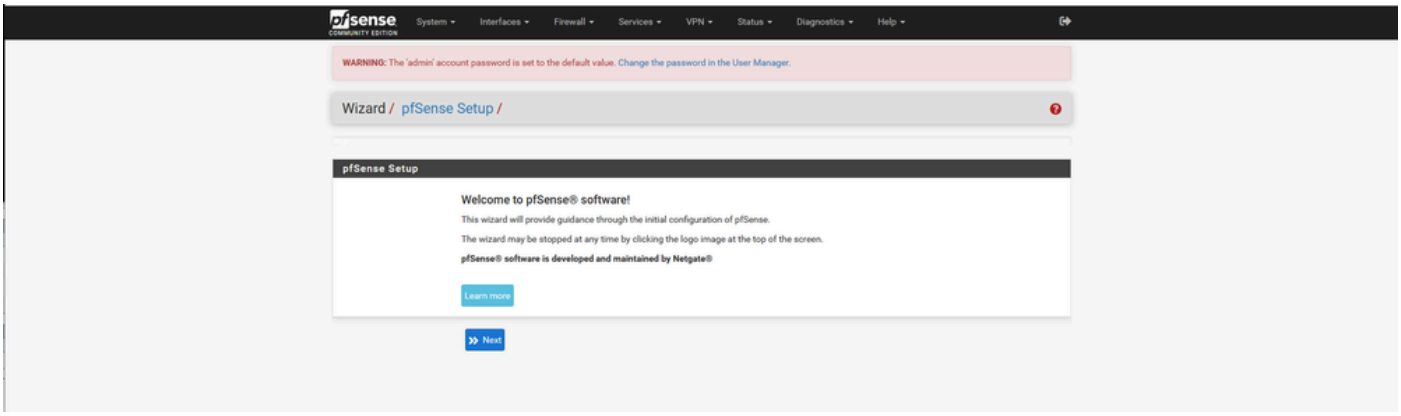


pfSense 관리자 로그인

2단계. admin/pfSense의 기본 로그인으로 로그인합니다.

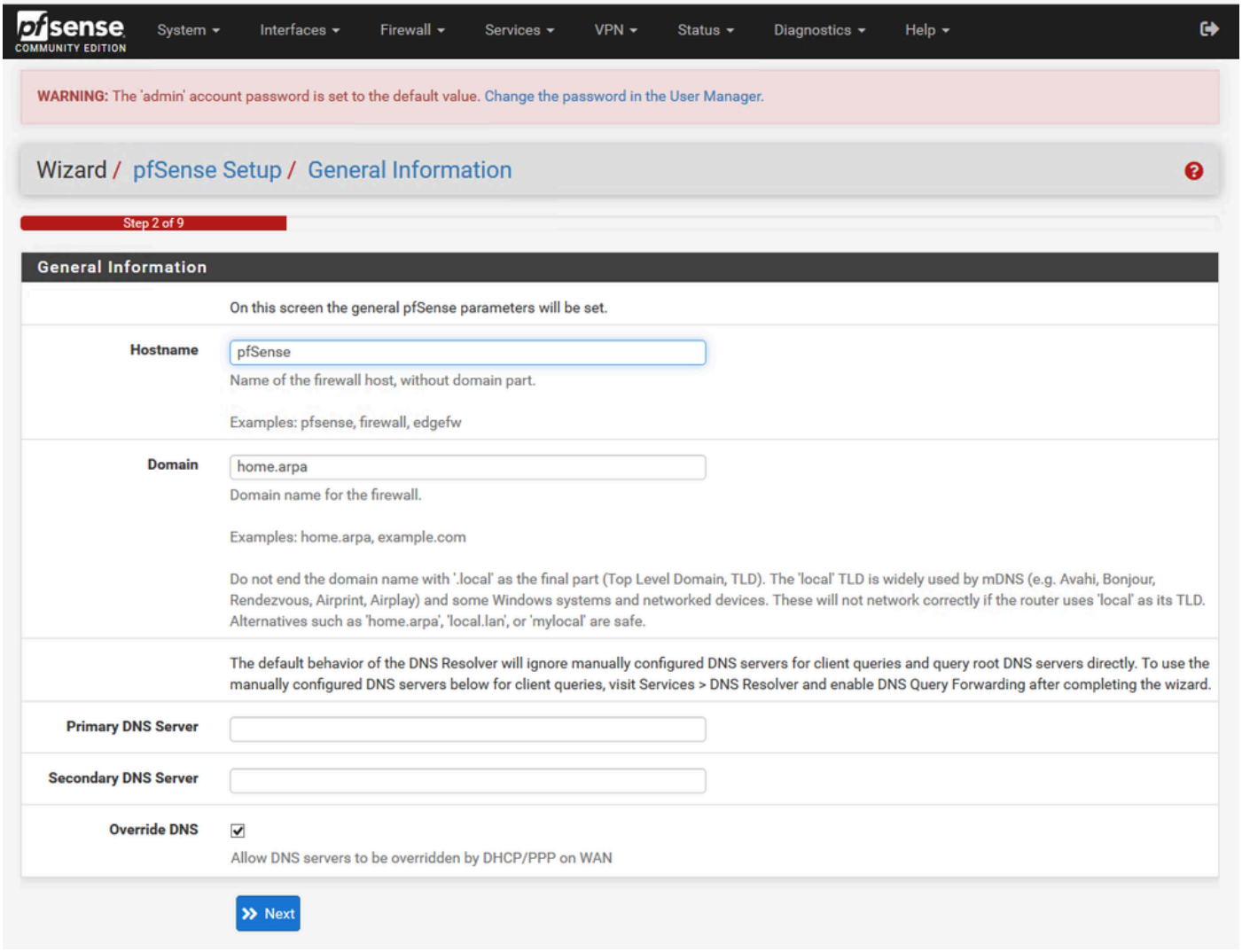
3단계. 초기 설정 완료

처음 두 화면에서 next(다음)를 클릭합니다.



pfSense 설치 마법사 - 1

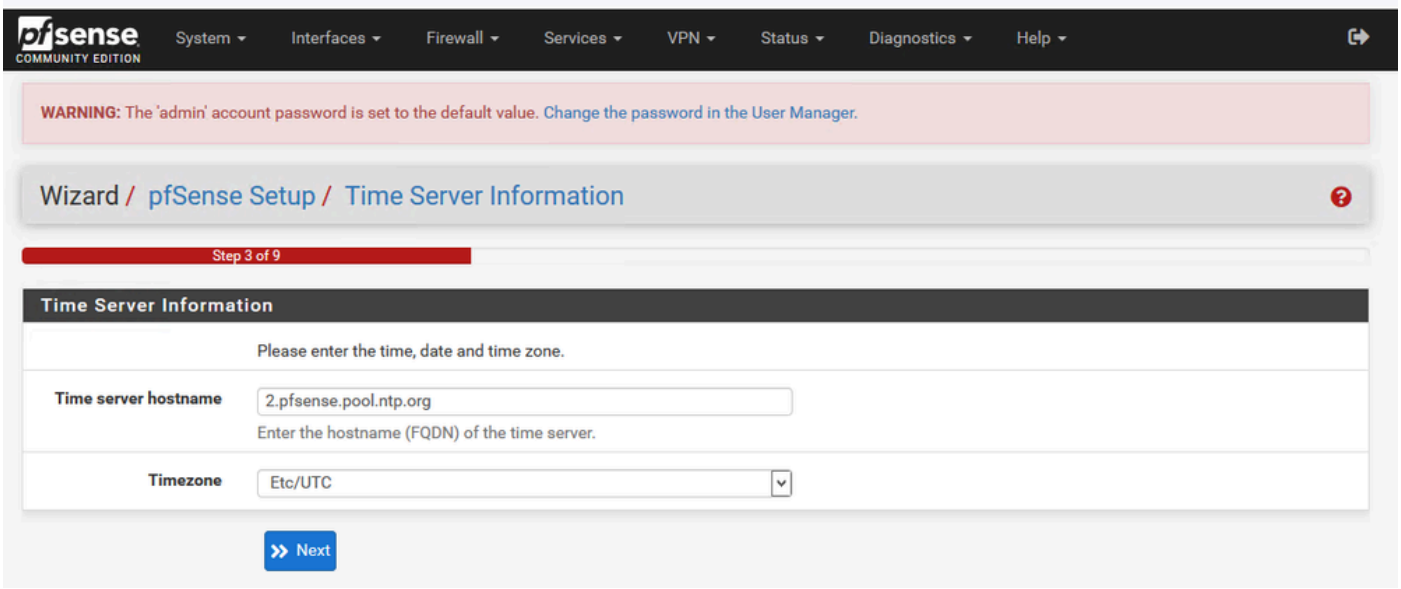
호스트 이름, 도메인 이름 및 DNS 서버 정보를 제공합니다.



pfSense 설치 마법사 - 2

IP 주소 정보를 확인합니다. 처음에 DHCP를 선택한 경우 지금 변경할 수 있습니다.

NTP 시간 서버 호스트 이름을 제공하고 드롭다운에서 올바른 시간대를 선택합니다.



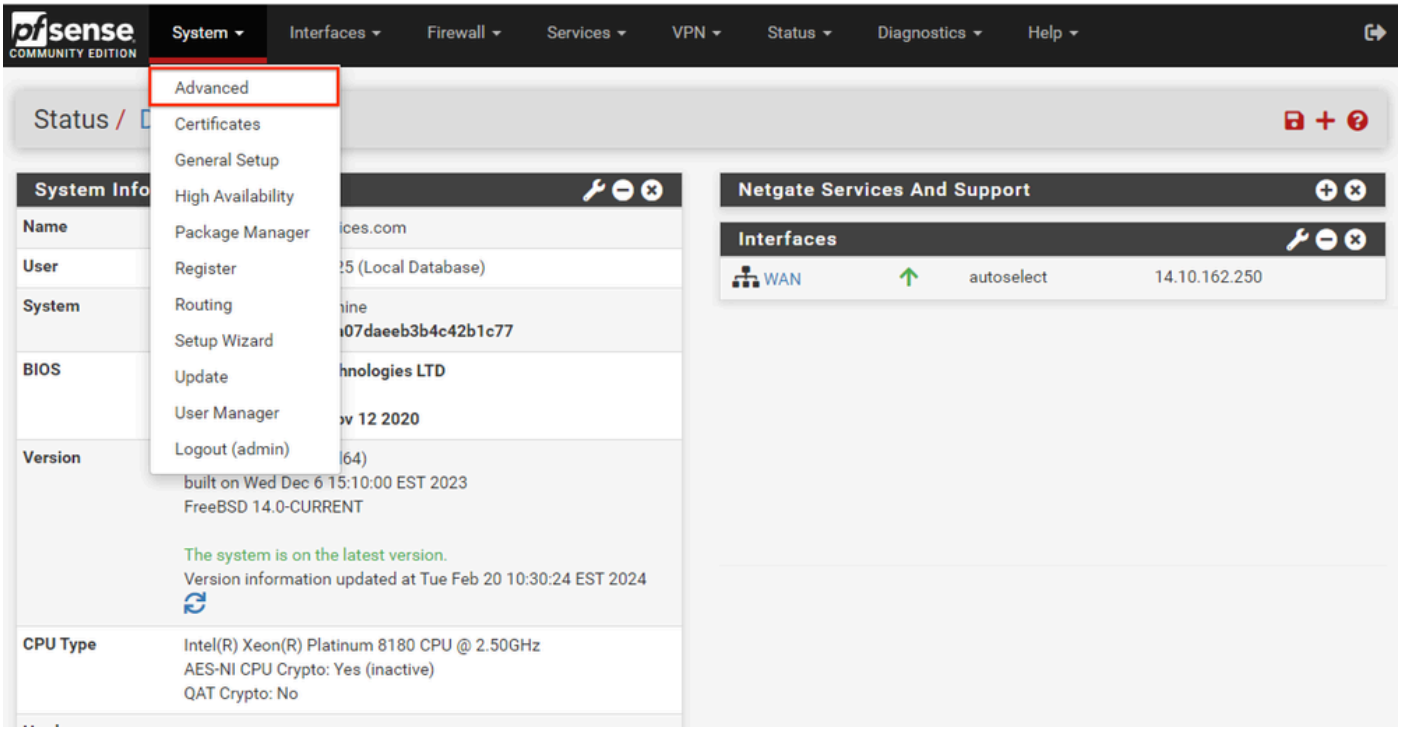
pfSense 설치 마법사 - 3

끝까지 설치 마법사를 계속 진행합니다. 인터페이스 GUI가 다시 시작되고 완료되면 새 URL로 리디렉션됩니다.

기본 관리 설정 구성

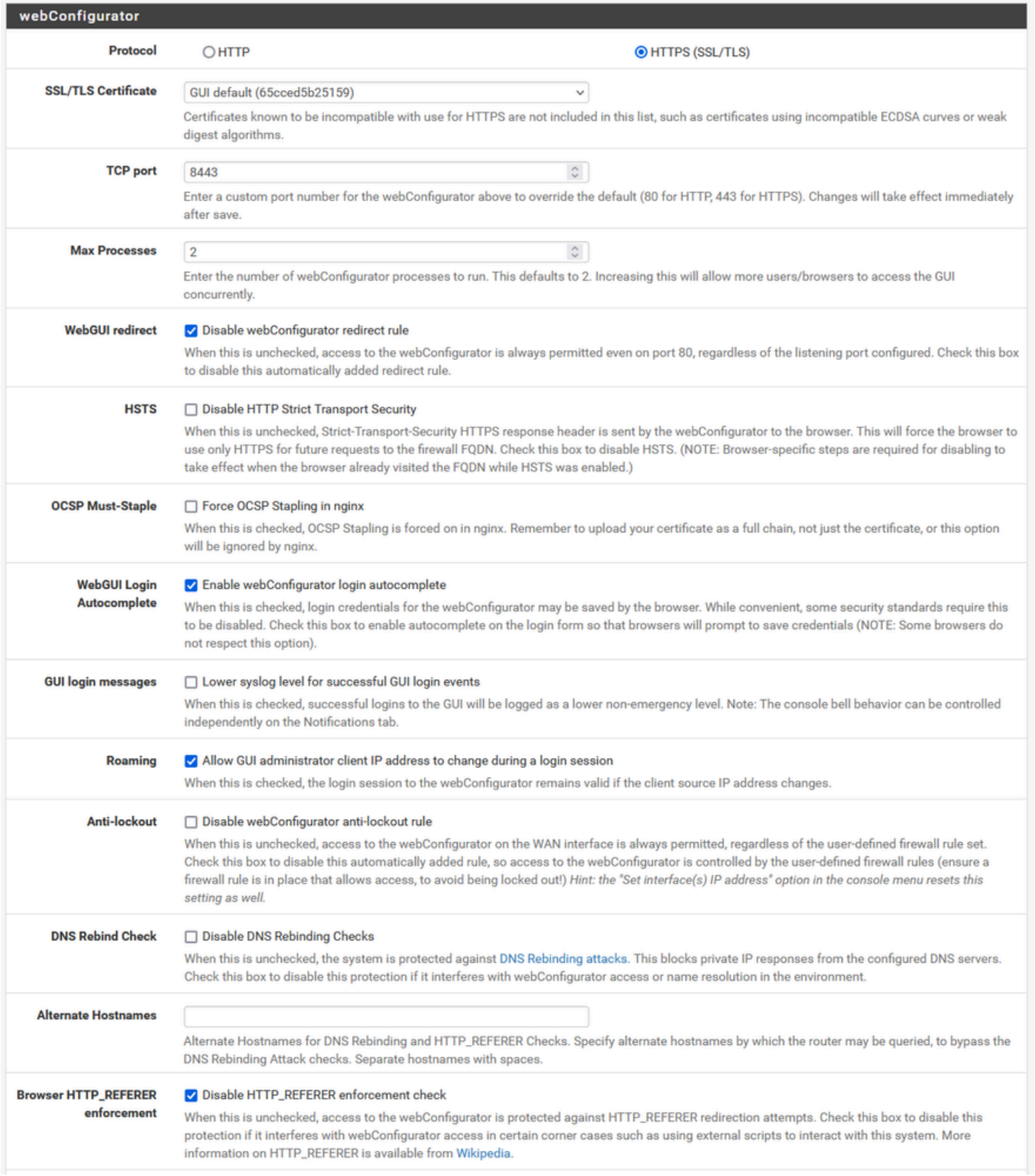
1단계. 관리자 인터페이스에 로그인합니다

2단계. 시스템 드롭다운 메뉴에서 고급을 선택합니다



pfSense GUI - Admin(관리) 드롭다운

3단계. WebConfigurator 설정 업데이트



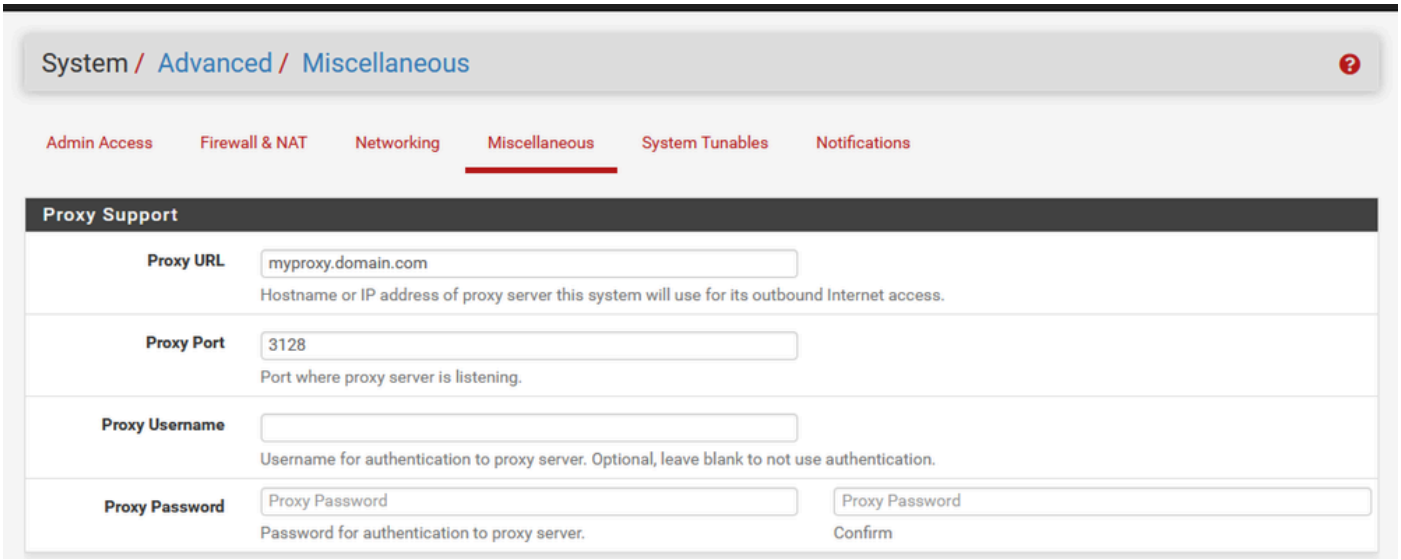
pfSense GUI - 관리 컨피그레이션

1. HTTPS(SSL/TLS) 프로토콜을 선택합니다.
2. 현재 SSL/TLS 인증서를 자체 서명 인증서에 그대로 둡니다.
3. TCP 포트를 443 이외의 포트로 변경하여 인터페이스 보안을 강화하고 포트 중복 문제를 방지합니다.
4. 포트 80에서 관리 인터페이스를 비활성화하려면 WebGUI 리디렉션 옵션을 선택합니다.
5. Browser HTTP_REFERER 시행 옵션을 선택합니다.
6. Enable Secure Shell(보안 셸 활성화) 옵션을 선택하여 보안 셸을 활성화합니다.

참고: 계속 진행하기 전에 저장 단추를 선택해야 합니다. 그런 다음 새 https 링크로 리디렉션 됩니다.

4단계. 필요한 경우 프록시 서버 구성

필요한 경우 Miscellaneous(기타) 탭에서 프록시 정보를 구성합니다. 설정 및 컨피그레이션을 완료하려면 어플라이언스에 인터넷 액세스가 있어야 합니다.



pfSense GUI - 프록시 컨피그레이션

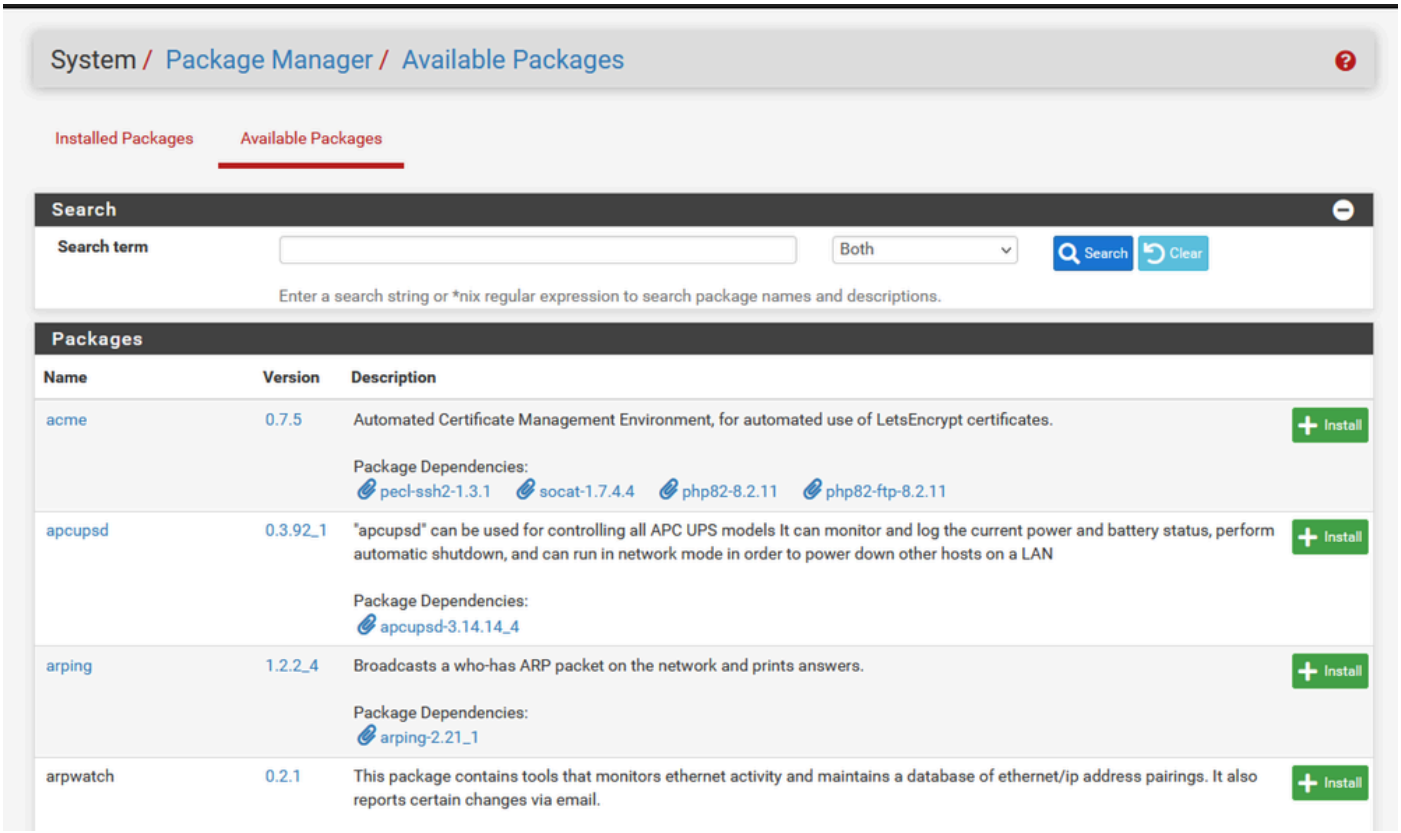
참고: 변경한 후 저장 단추를 선택해야 합니다.

필수 패키지 추가

1단계. 시스템 > 패키지 관리자를 선택합니다

2단계. 사용 가능한 패키지 선택

참고: 사용 가능한 모든 패키지를 로드하는 데 몇 분 정도 걸릴 수 있습니다. 이 시간이 초과되면 DNS 서버가 올바르게 구성되었는지 확인합니다. 어플라이언스를 재부팅하면 인터넷 연결이 수정되는 경우가 많습니다.



pfSense GUI - 패키지 목록

3단계. 필요한 패키지 찾기 및 설치

1. 하프록시
2. Open-VM 툴

참고: happroxy-devel 패키지는 선택하지 마십시오.

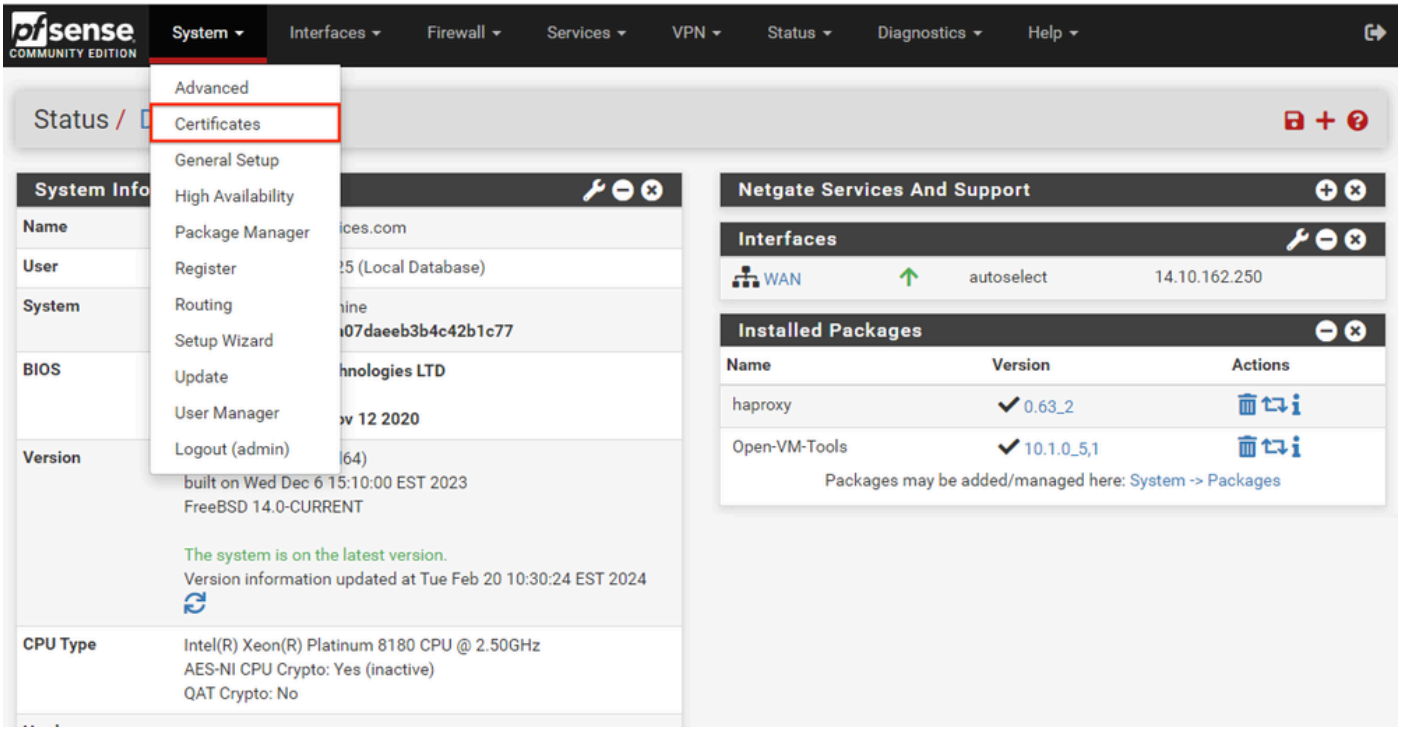
인증서 구성

pfSense는 자체 서명 인증서를 만들거나 공용 CA, 내부 CA와 통합할 수 있으며 CA의 역할을 하고 CA 서명 인증서를 발급할 수 있습니다. 이 가이드에서는 내부 CA와 통합하는 단계를 보여줍니다.

이 섹션을 시작하기 전에 이러한 항목을 사용할 수 있는지 확인하십시오.

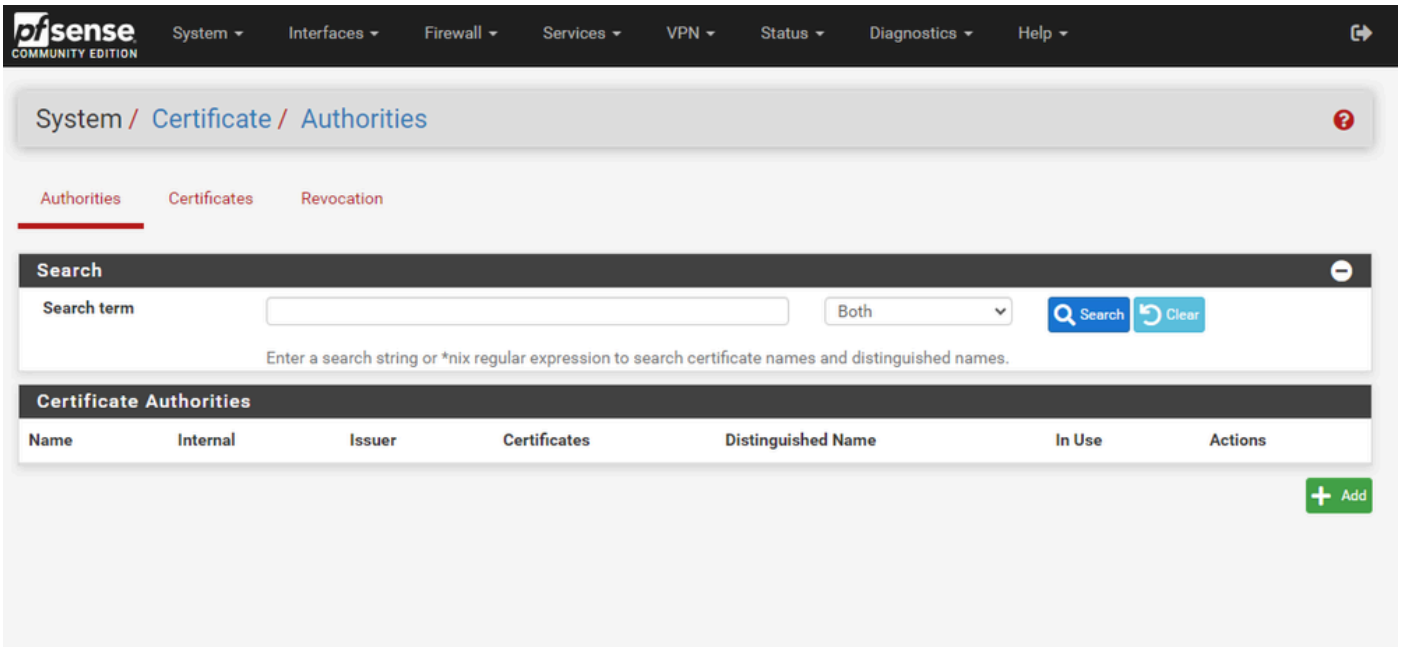
1. PEM 또는 Base-64 인코딩 형식으로 저장된 CA의 루트 인증서
2. PEM 또는 Base-64 인코딩 형식으로 저장된 CA의 모든 중간(발급이라고도 함) 인증서

1단계. 시스템 드롭다운 메뉴에서 인증서를 선택합니다.



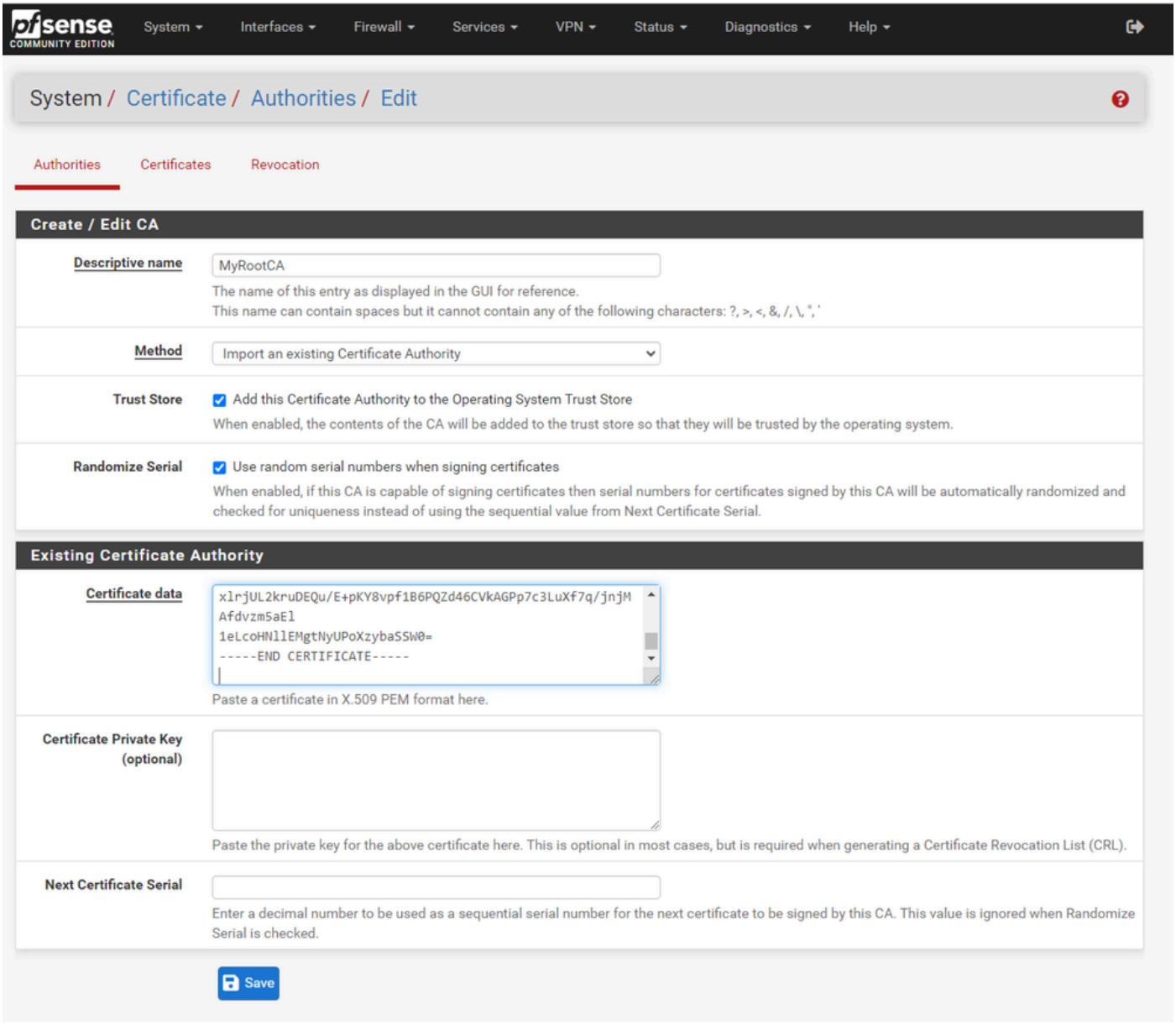
pfSense GUI - 인증서 드롭다운

2단계. CA 루트 인증서 가져오기



pfSense GUI - CA 인증서 목록

Add(추가) 버튼을 선택합니다.



pfSense GUI - CA 가져오기

그림에서 볼 수 있듯이:

1. 고유한 설명적 이름을 제공합니다.

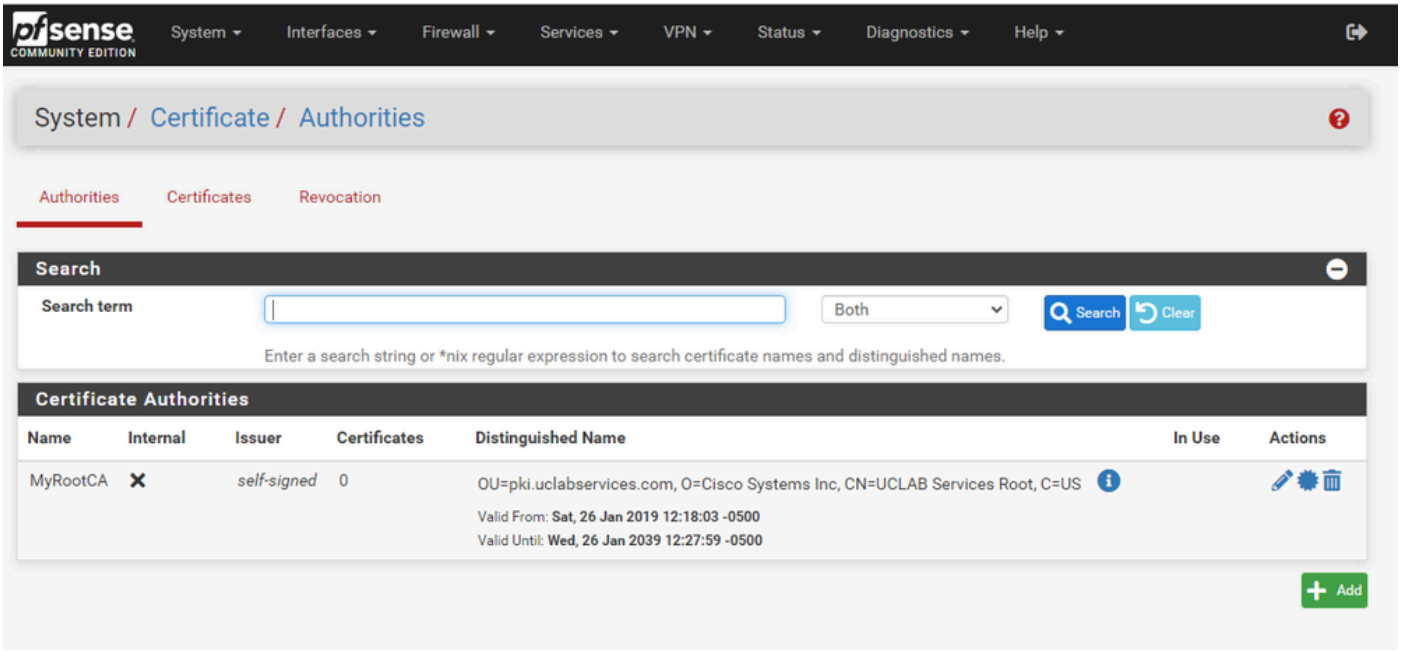
2. 방법 드롭다운에서 기존 인증 기관 임포트를 선택합니다.

3. Trust Store(신뢰 저장소) 및 Randomize Serial(시리얼 임의 설정) 확인란이 선택되었는지 확인합니다.

4. 전체 인증서를 인증서 데이터 텍스트 상자에 붙여넣습니다. -----BEGIN CERTIFICATE----- 및 -----END CERTIFICATE----- 행에 포함되었는지 확인합니다.

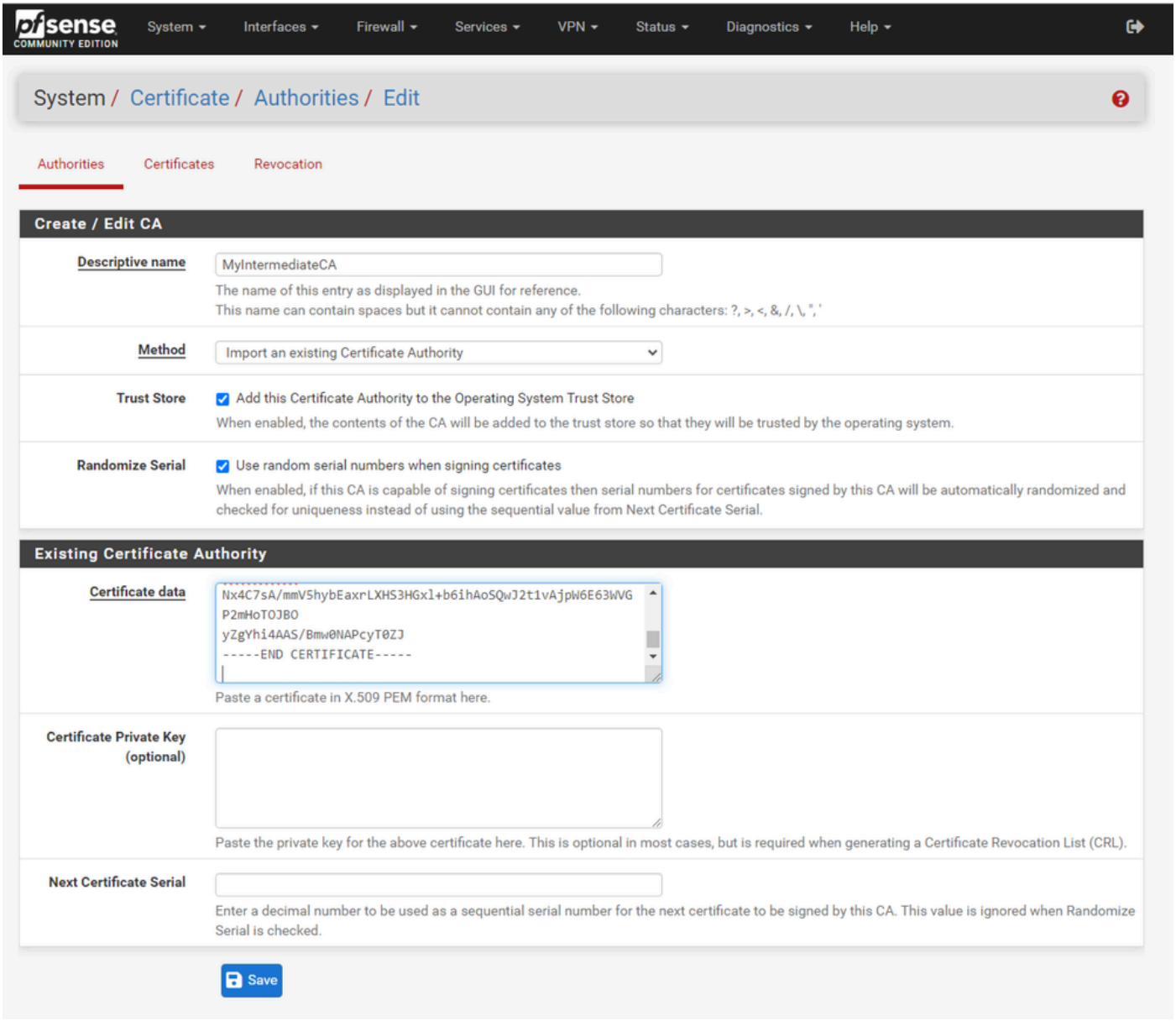
5. 저장을 선택합니다.

6. 이미지에 표시된 대로 인증서를 가져왔는지 확인합니다.



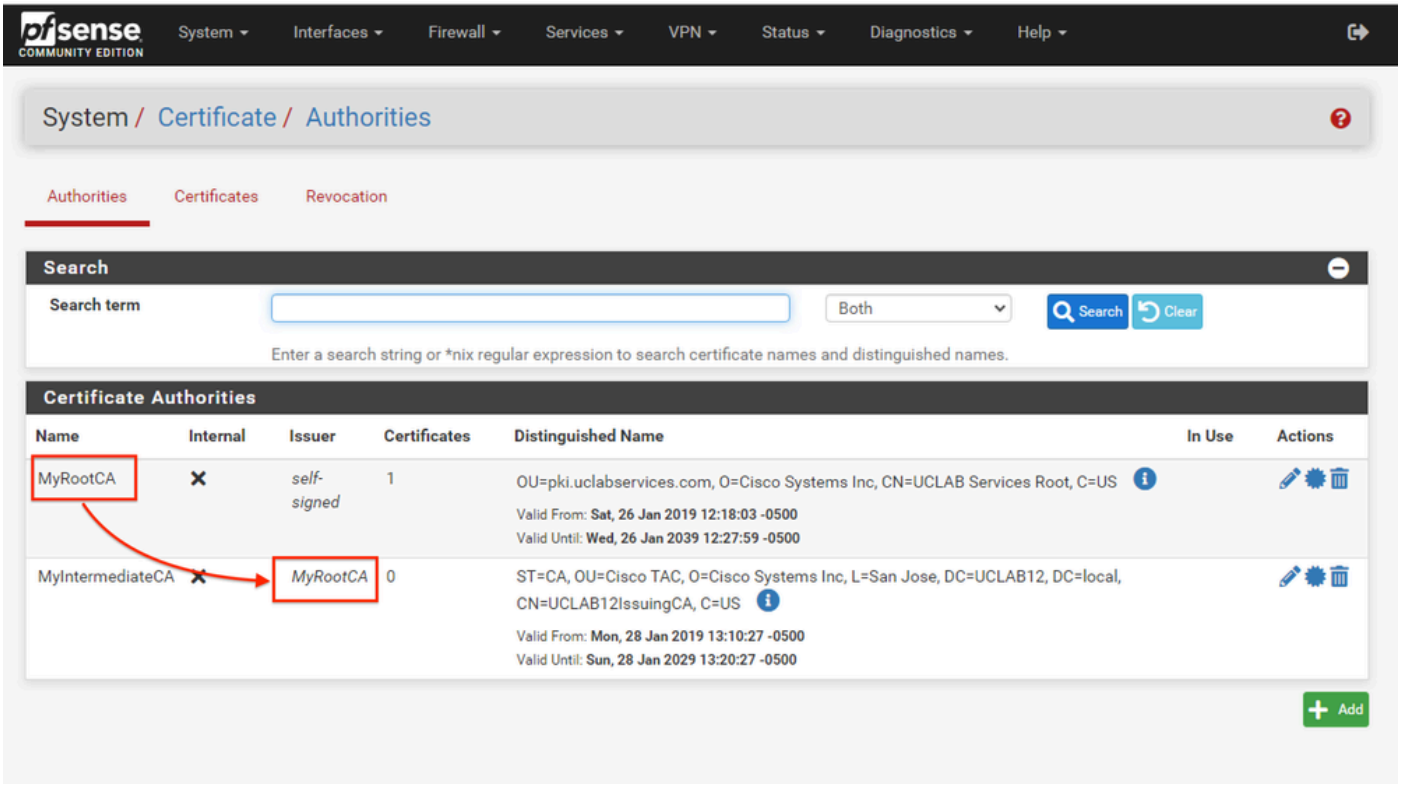
pfSense GUI - CA 목록

3단계. CA 중간 인증서 가져오기



pfSense GUI - CA 중간 가져오기

루트 CA 인증서를 가져와서 중간 CA 인증서를 가져오려면 단계를 반복합니다.



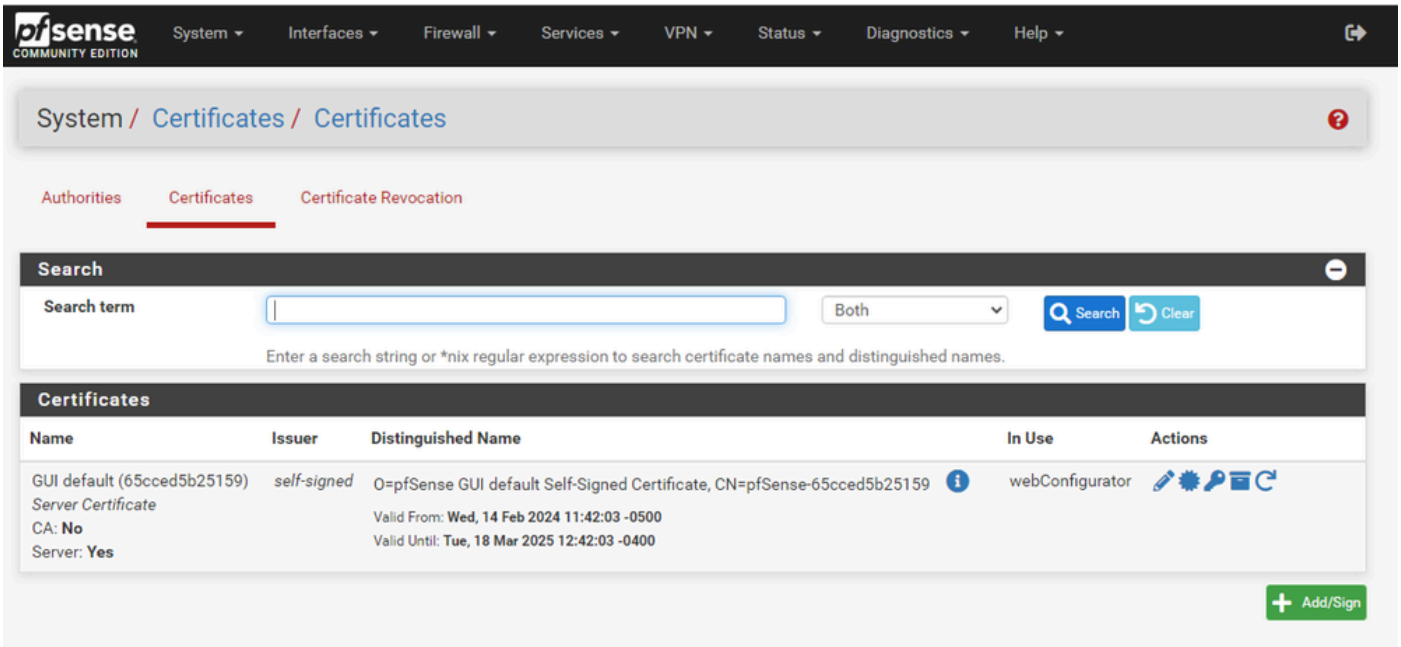
pfSense GUI - CA 링크

Certificate Authorities(인증 기관)를 검토하여 이미지에 표시된 것처럼 Intermediate(중간)가 루트 인증서에 올바르게 연결되어 있는지 확인합니다.

4단계. 부하가 분산된 웹 사이트에 대한 CSR 생성 및 내보내기

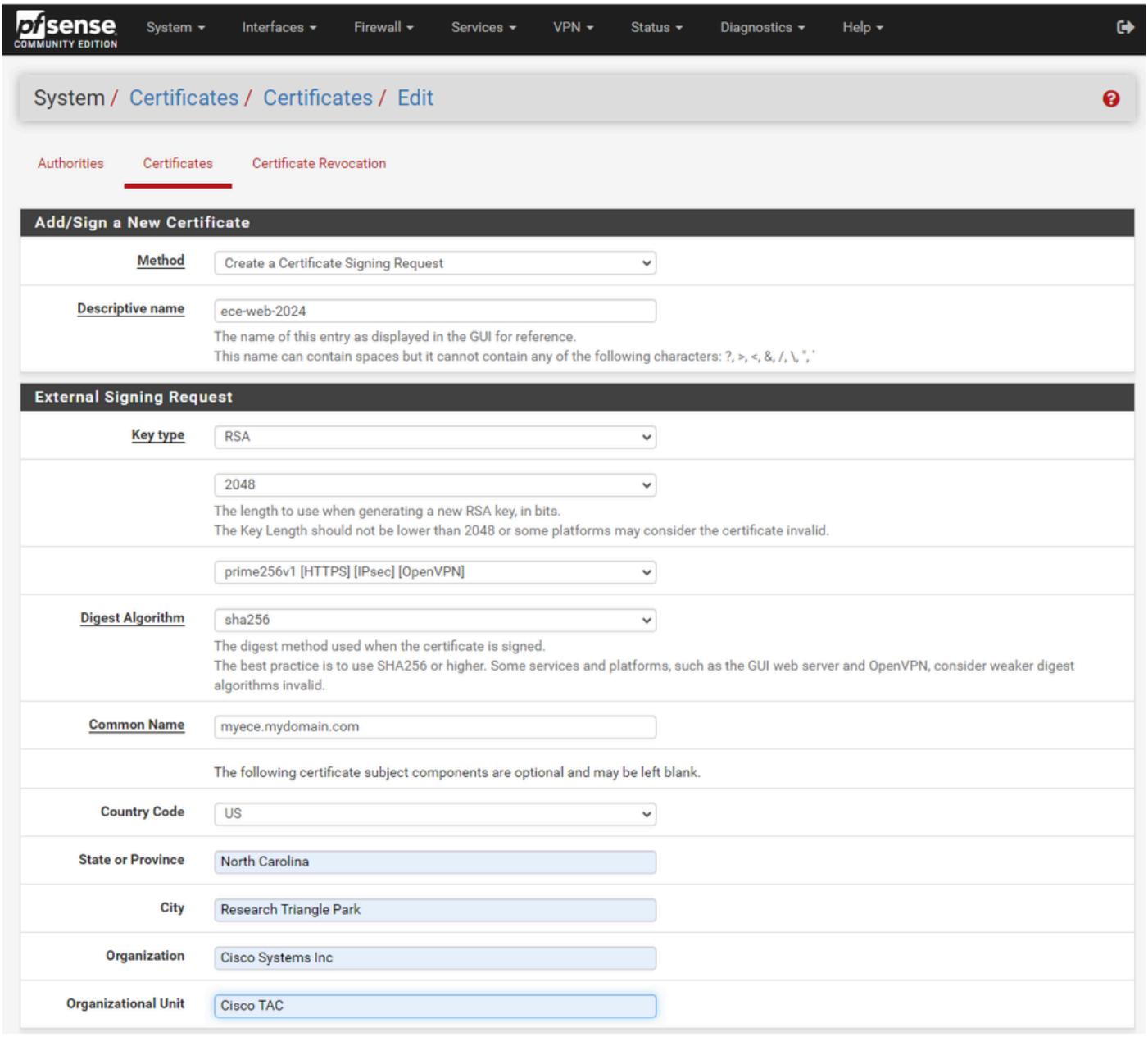
CSR을 생성하고, CSR을 내보낸 다음, 서명된 인증서를 가져오는 단계를 설명합니다. PFX 형식의 기존 인증서가 이미 있는 경우 이 인증서를 가져올 수 있습니다. 이러한 단계에 대해서는 pfSense 설명서를 참조하십시오.

1. 인증서 메뉴를 선택한 다음 추가/서명 버튼을 선택합니다.



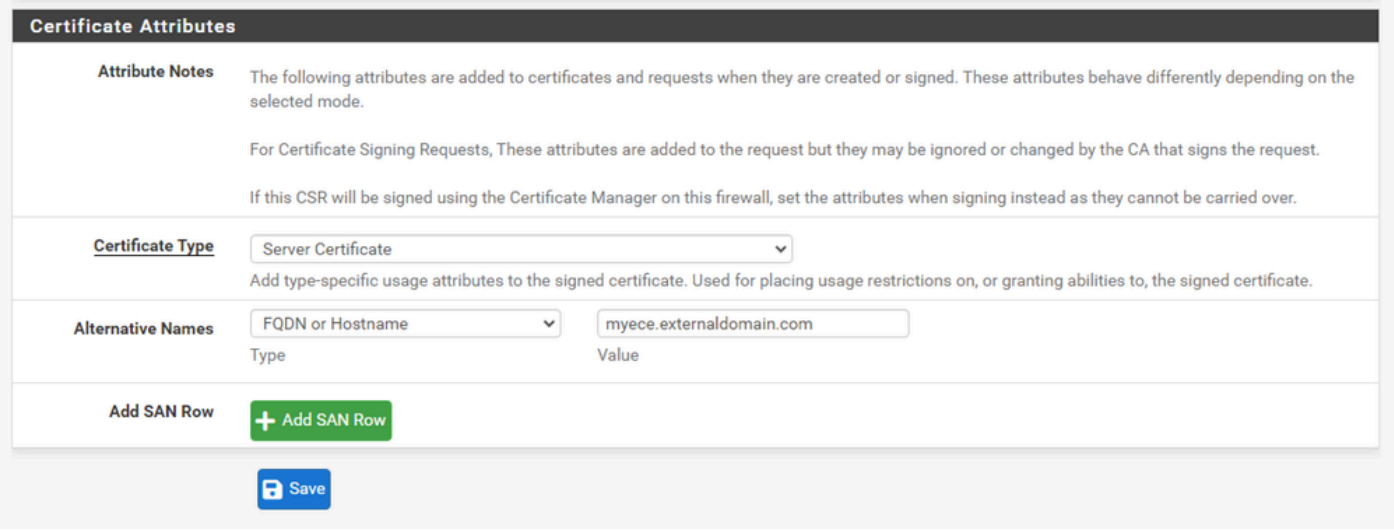
pfSense GUI - 인증서 목록

2. CSR(Certificate Signing Request) 양식을 작성합니다.



pfSense GUI - CSR 생성

- 방법: 드롭다운에서 Create a Certificate Signing Request(인증서 서명 요청 생성)를 선택합니다.
- 설명 이름: 인증서의 이름을 제공합니다.
- 키 유형 및 다이제스트 알고리즘: 요구 사항과 일치하는지 검토합니다.
- Common Name(공통 이름): 정규화된 도메인 이름 웹 사이트를 제공합니다.
- 환경에 필요한 나머지 인증서 정보 제공



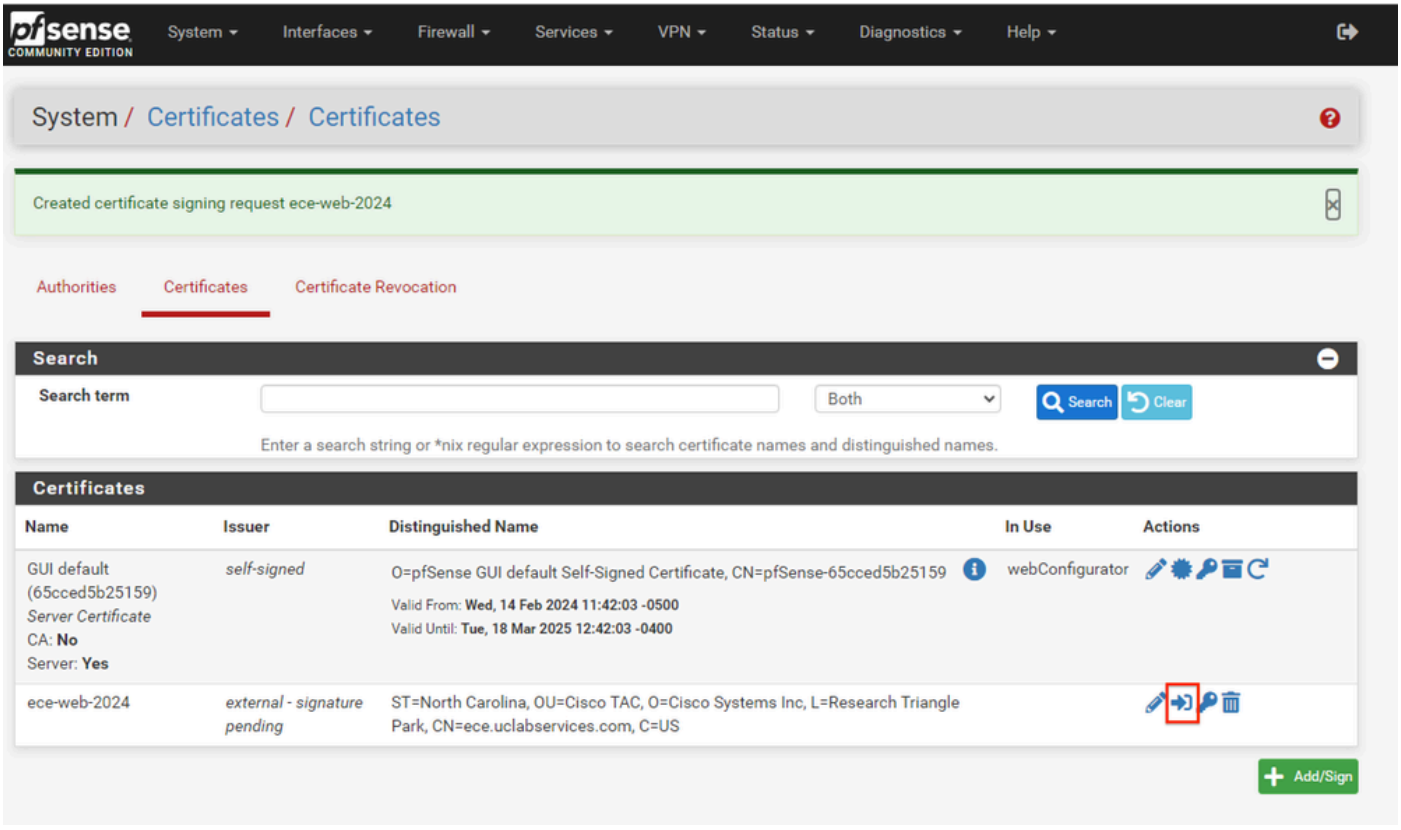
pfSense GUI - CSR 고급

- Certificate Type(인증서 유형): 드롭다운에서 Server Certificate(서버 인증서)를 선택합니다.
- 대체 이름: 구현에 필요한 SAN(주체 대체 이름)을 제공합니다.

참고: SAN 필드에 공용 이름이 자동으로 추가됩니다. 필요한 추가 이름만 추가하면 됩니다.

모든 필드가 올바르면 저장을 선택합니다.

3. CSR을 파일로 내보냅니다.

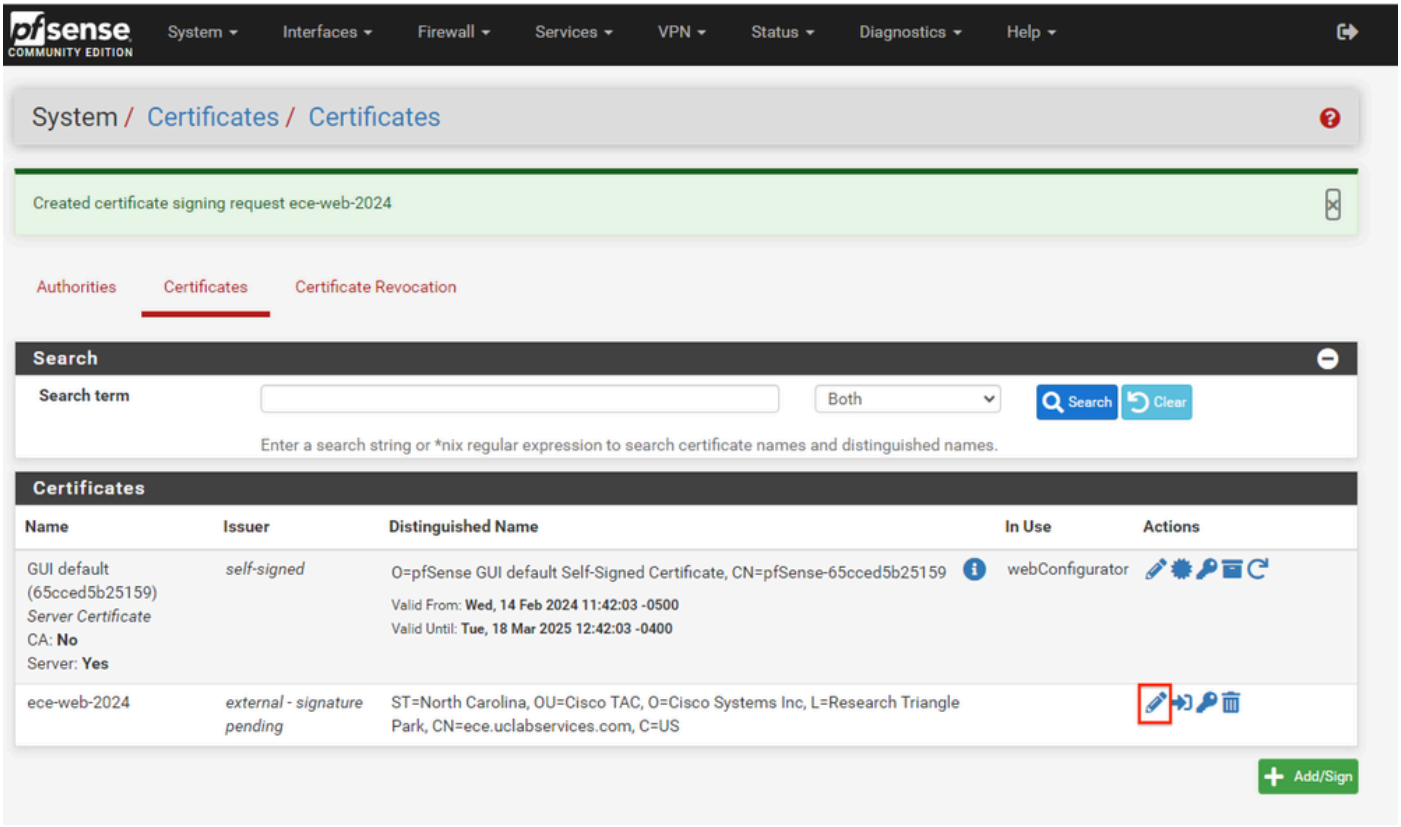


pfSense GUI - CSR 내보내기

Export(내보내기) 버튼을 선택하여 CSR을 저장한 다음 CA에 서명합니다. 서명된 인증서가 있으면

이 인증서를 PEM 또는 Base-64 파일로 저장하여 프로세스를 완료합니다.

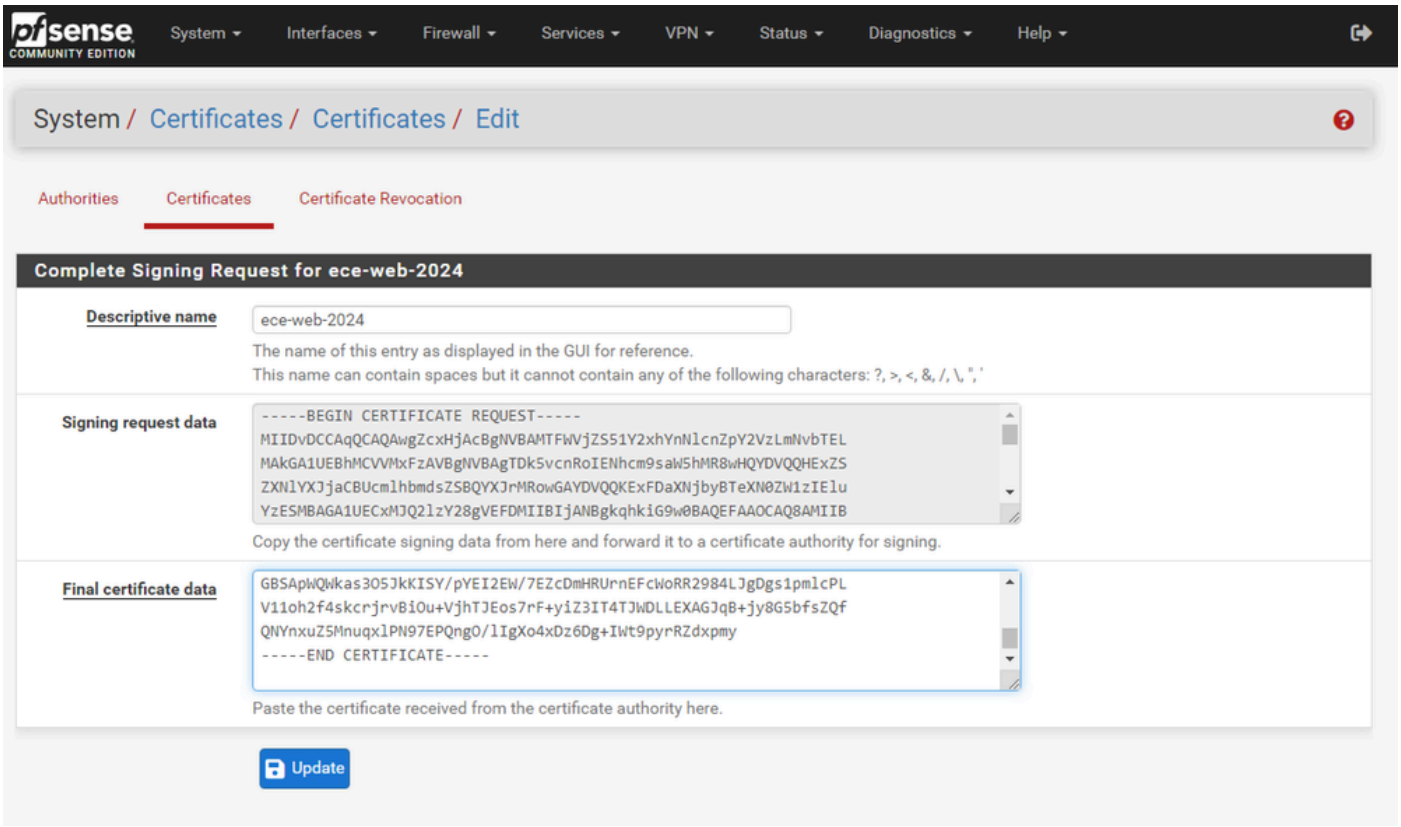
4. 서명된 인증서를 가져옵니다.



pfSense GUI - 인증서 가져오기

서명된 인증서를 가져오려면 연필 아이콘을 선택합니다.

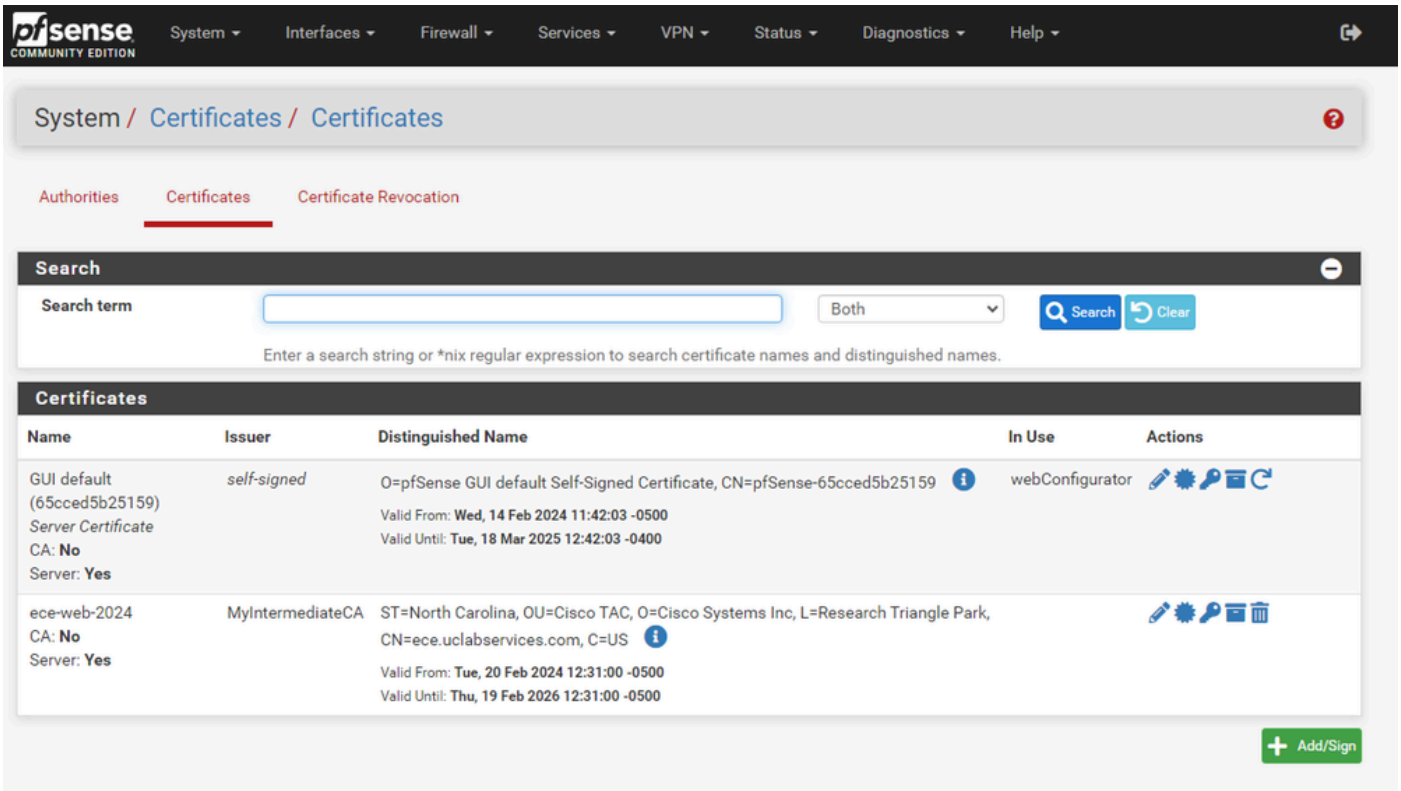
5. 양식에 인증서 데이터를 붙여넣습니다.



pfSense GUI - 인증서 가져오기

인증서를 저장하려면 Update(업데이트)를 선택합니다.

6. 인증서 데이터가 정확한지 검토합니다.



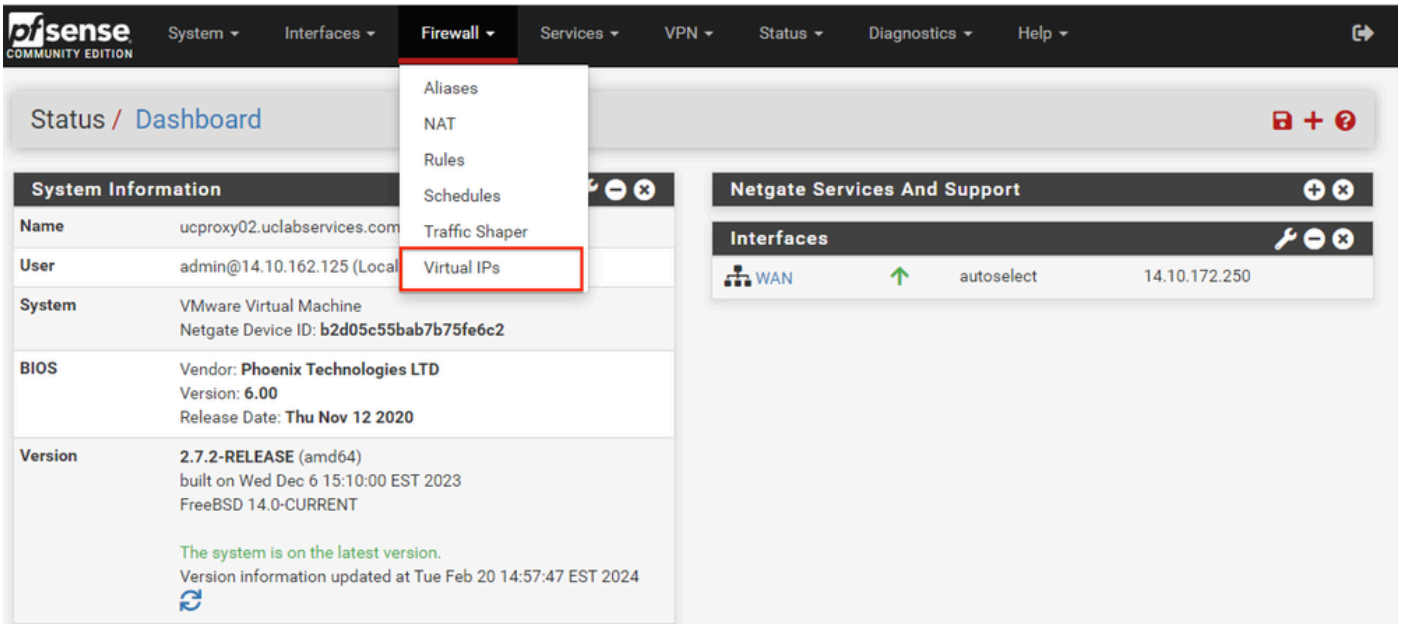
pfSense GUI - 인증서 목록

7. 이 pfSense에서 여러 사이트를 호스팅하려면 이 프로세스를 반복합니다.

가상 IP 추가

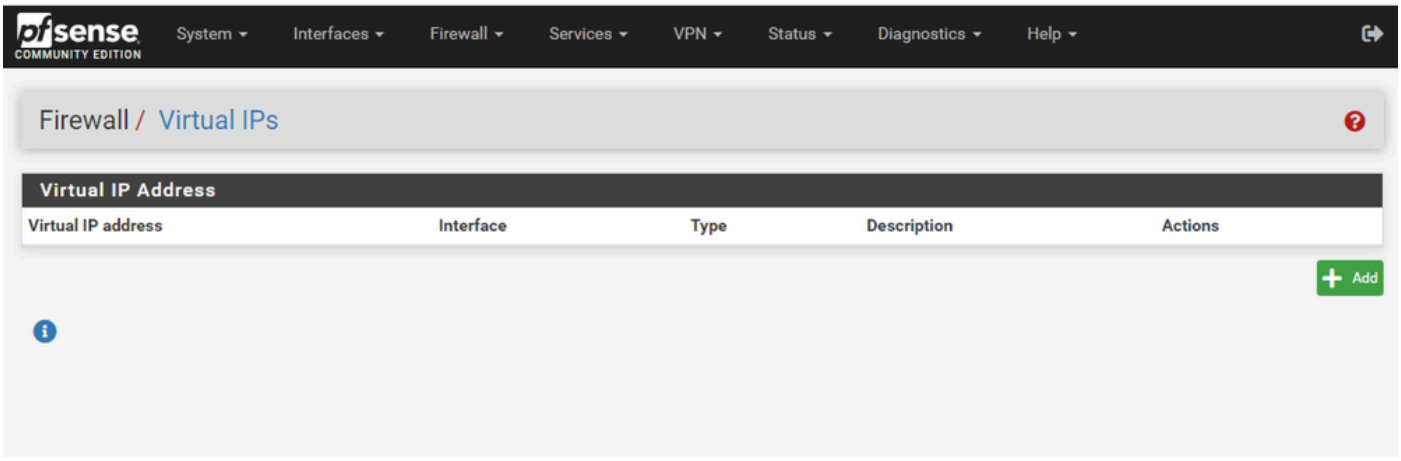
pfSense에서 웹 사이트를 호스팅하려면 하나 이상의 IP가 필요합니다. pfSense에서는 VIP(Virtual IP)를 통해 수행됩니다.

1단계. Firewall(방화벽) 드롭다운에서 가상 IP를 선택합니다.



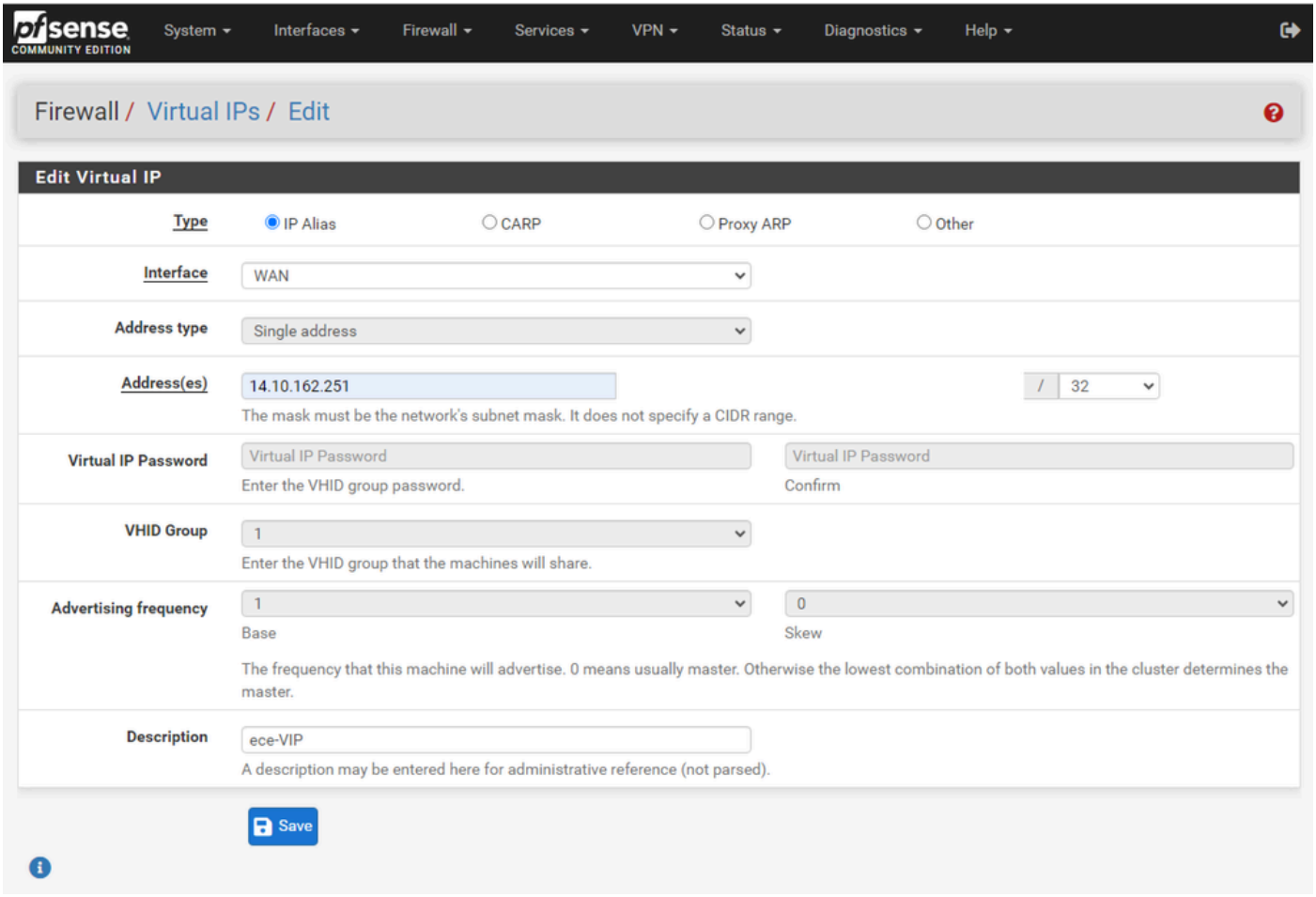
pfSense GUI - VIP 드롭다운

2단계. Add(추가) 버튼을 선택합니다



pfSense GUI - VIP 랜딩 페이지

3단계. 주소 정보 제공



pfSense GUI - VIP 컨피그레이션

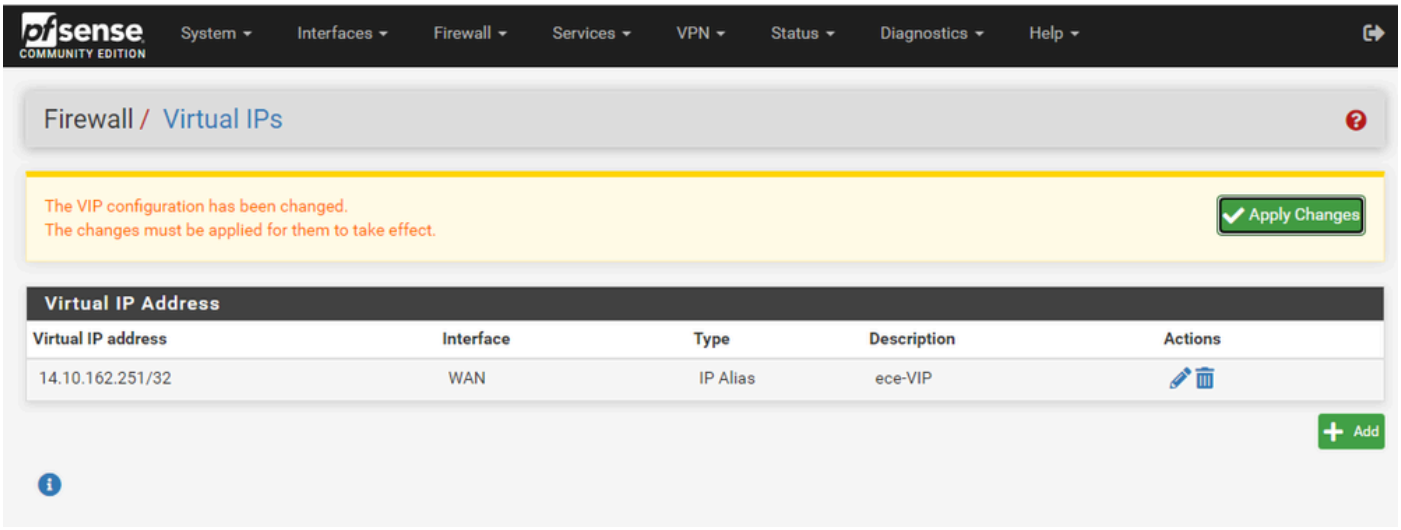
정보를 사용하여 VIP를 추가합니다.

- 유형: IP 별칭 선택
- Interface(인터페이스): 브로드캐스트할 이 IP 주소의 인터페이스를 선택합니다
- 주소: IP 주소를 입력합니다.
- 주소 마스크: 로드 밸런싱에 사용되는 IP 주소의 경우 마스크는 /32여야 합니다.
- Description(설명): 나중에 구성을 쉽게 이해할 수 있도록 짧은 텍스트를 입력하십시오.

Save(저장)를 선택하여 변경 사항을 커밋합니다.

컨피그레이션에 필요한 각 IP 주소에 대해 이 단계를 반복합니다.

4단계. 컨피그레이션 적용



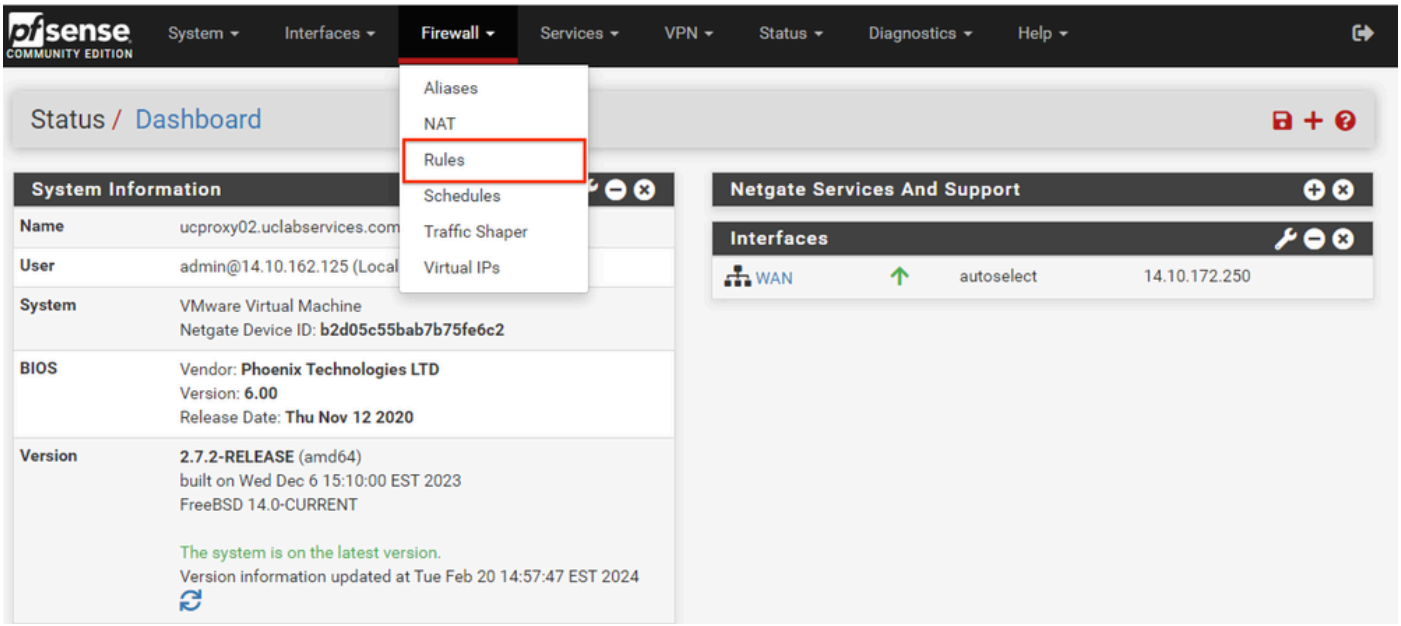
pfSense GUI - VIP 목록

모든 VIP가 추가된 후 Apply Changes(변경 사항 적용) 버튼을 선택합니다.

방화벽 구성

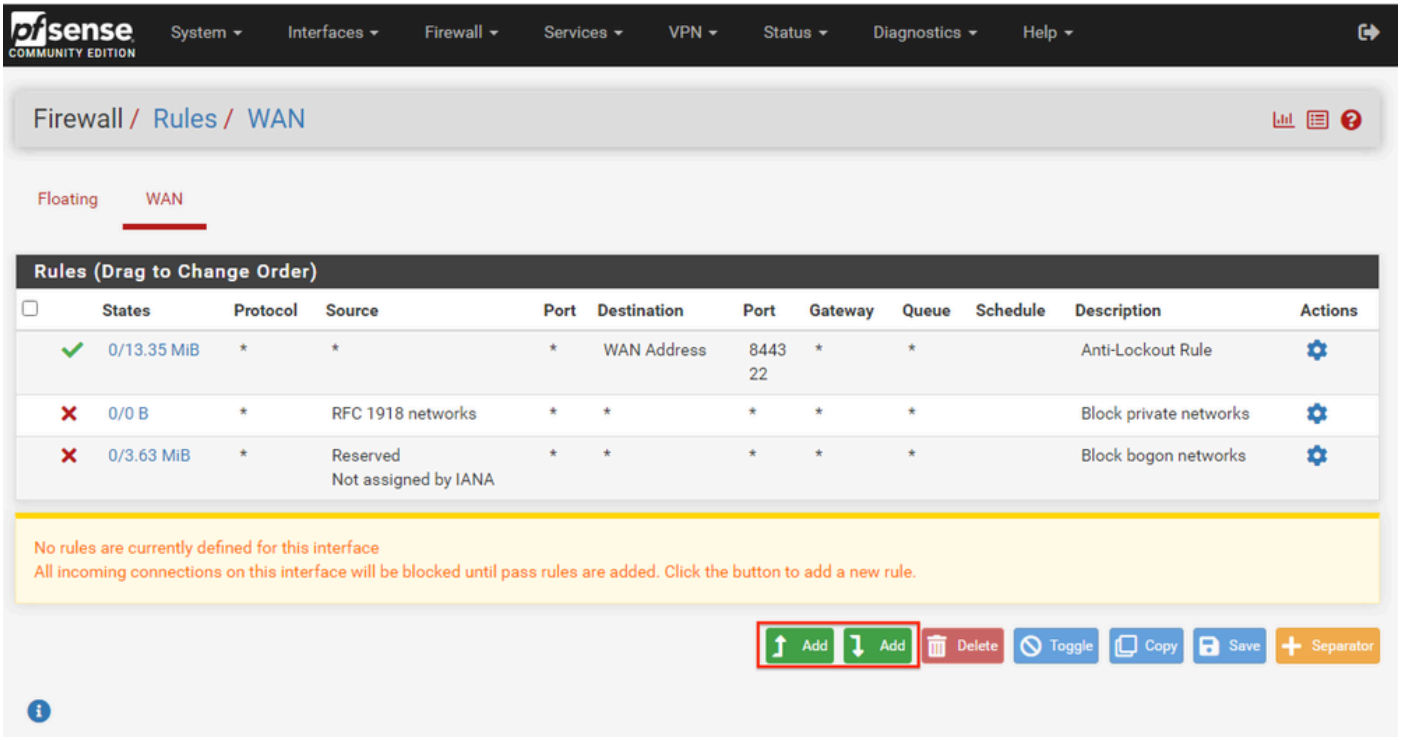
pfSense에는 방화벽이 내장되어 있습니다. 기본 규칙 집합은 매우 제한적입니다. 어플라이언스를 프로덕션 환경에 구축하기 전에 포괄적인 방화벽 정책을 구축해야 합니다.

1단계. 방화벽 드롭다운에서 Rules(규칙)를 선택합니다.



pfSense GUI - 방화벽 규칙 드롭다운

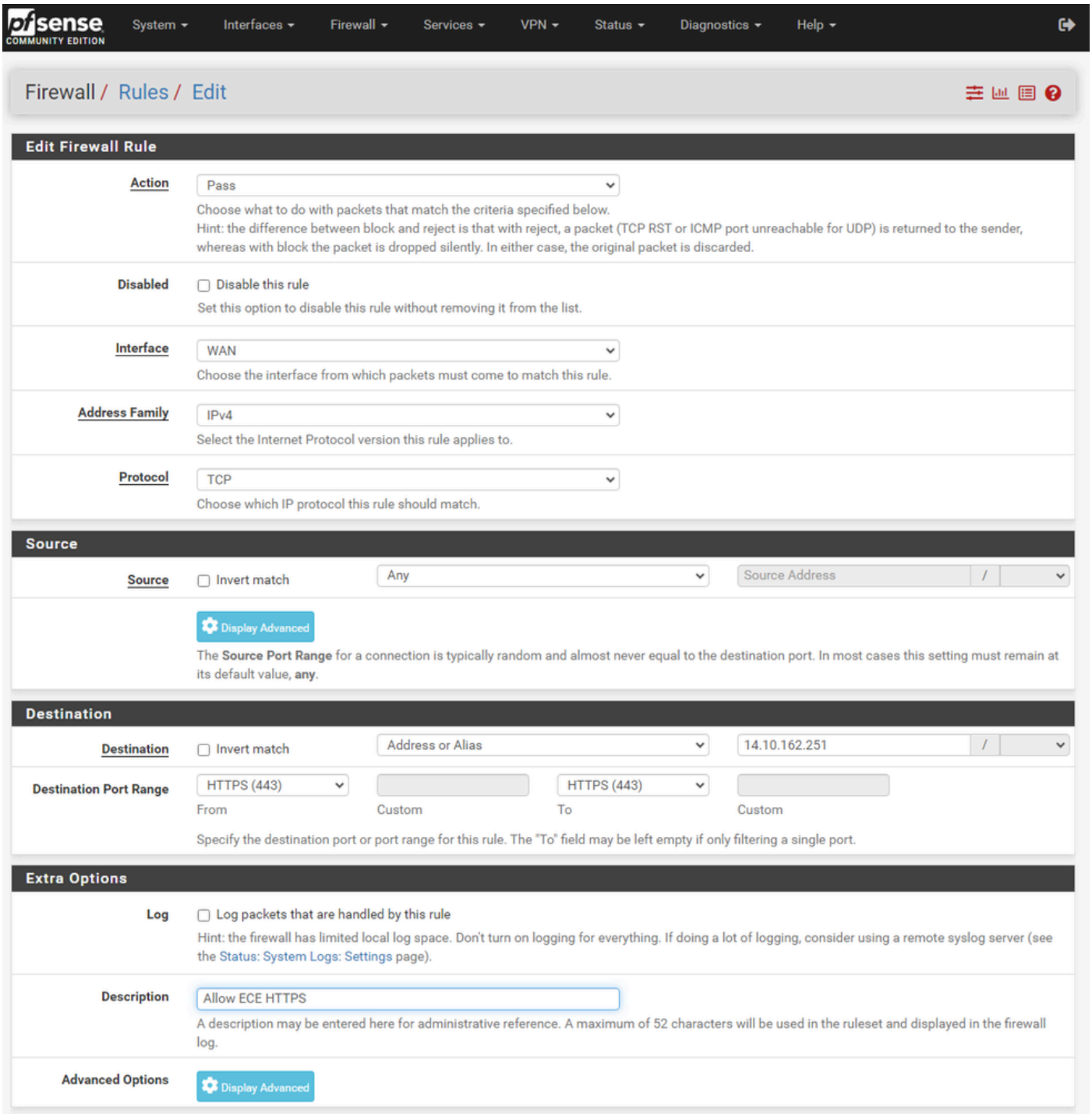
2단계. 추가 단추 중 하나를 선택합니다



pfSense GUI - 방화벽 규칙 목록

한 단추는 선택한 행 위에 새 규칙을 추가하고 다른 단추는 선택한 규칙 아래에 규칙을 추가합니다. 두 버튼 중 하나를 첫 번째 규칙에 사용할 수 있습니다.

3단계. IP 주소에 대해 포트 443으로의 트래픽을 허용하는 방화벽 규칙 만들기



pfSense GUI - 방화벽 통과 규칙 컨피그레이션

정보를 사용하여 규칙을 생성합니다.

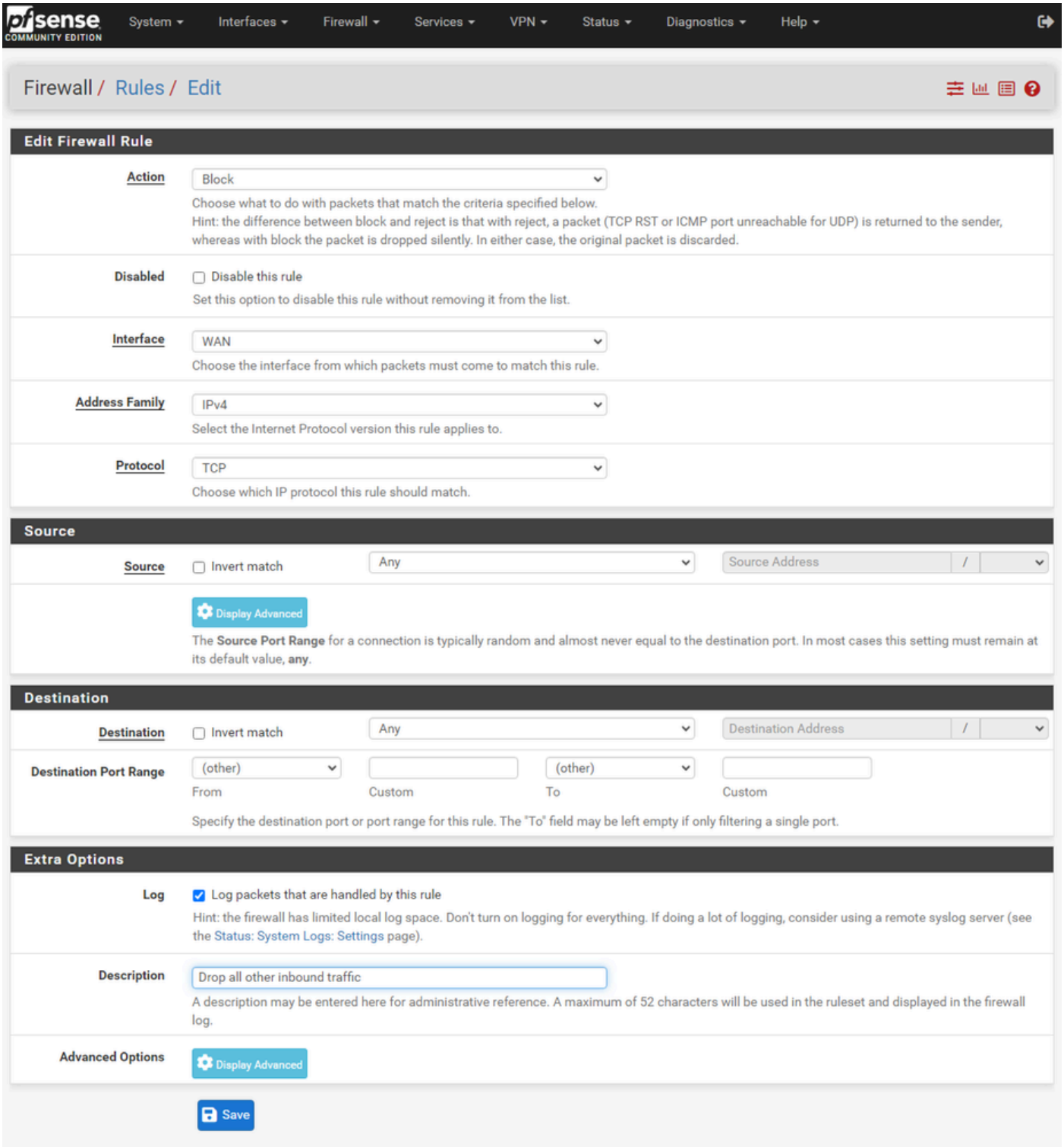
- Action(작업): Pass(통과) 선택
- Interface(인터페이스): 규칙이 적용되는 인터페이스를 선택합니다
- 주소군 및 프로토콜: 필요에 따라 선택
- Source(소스): Leave selected as Any(선택한 항목 그대로 유지)
- Destination(대상): Destination(대상) 드롭다운에서 Address(주소) 또는 Alias(별칭)를 선택한 다음 규칙이 적용되는 IP 주소를 입력합니다
- Destination Port Range(대상 포트 범위): From(시작) 및 To(종료) 드롭다운 모두에서 HTTPS(443)를 선택합니다.
- Log(로그): 이 규칙과 일치하는 모든 패킷을 어카운팅에 기록하려면 확인란을 선택합니다

- Description(설명): 나중에 규칙을 참조할 수 있도록 텍스트를 제공합니다.

저장을 선택합니다.

4단계. 다른 모든 트래픽을 pfSense로 삭제하기 위한 방화벽 규칙 만들기

Add(추가) 버튼을 선택하여 새로 생성된 규칙 아래에 규칙을 삽입합니다.



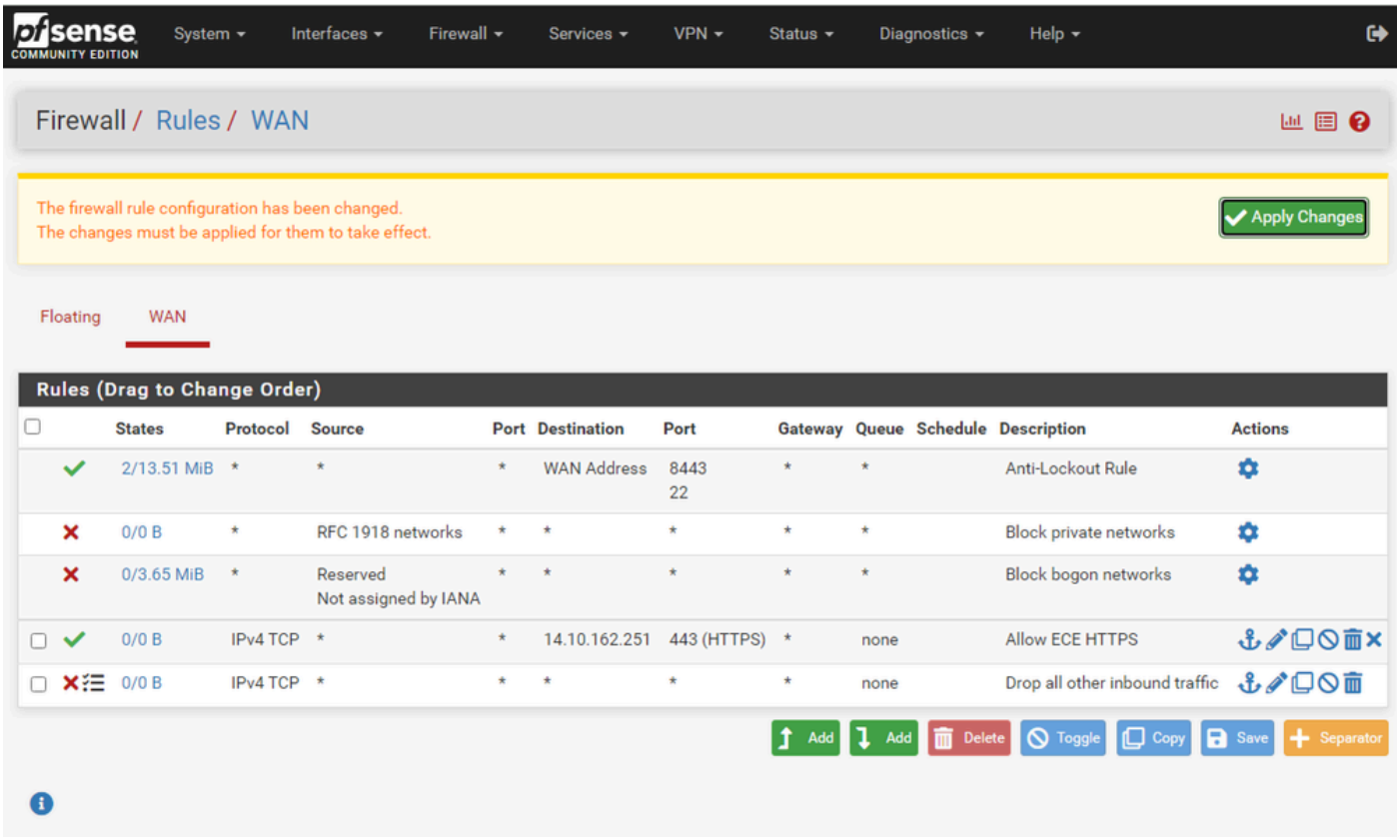
pfSense GUI - 방화벽 삭제 규칙 컨피그레이션

- 작업: 차단 선택

- Interface(인터페이스): 규칙이 적용되는 인터페이스를 선택합니다
- 주소군 및 프로토콜: 필요에 따라 선택
- Source(소스): Leave selected as Any(선택한 항목 그대로 유지)
- Destination(대상): Leave selected as Any(선택한 항목 그대로 유지)
- Log(로그): 이 규칙과 일치하는 모든 패킷을 어카운팅에 기록하려면 확인란을 선택합니다
- Description(설명): 나중에 규칙을 참조할 수 있도록 텍스트를 제공합니다.

저장을 선택합니다.

5단계. 규칙을 검토하고 차단 규칙이 아래쪽에 있는지 확인합니다



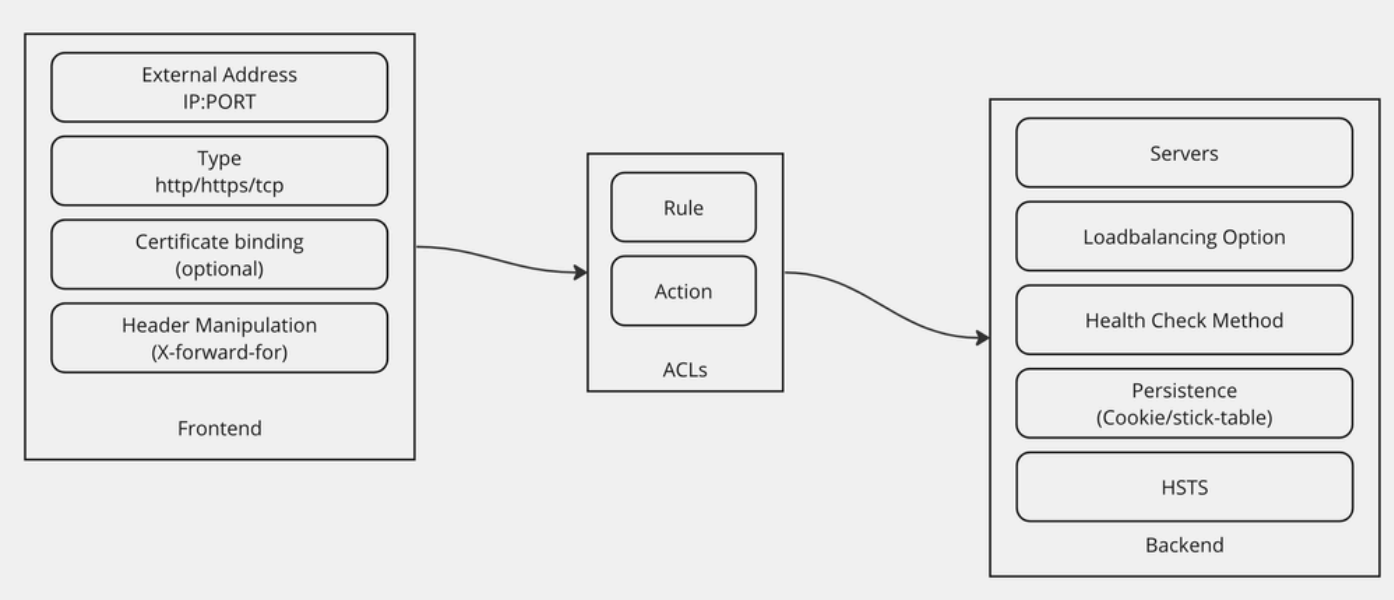
pfSense GUI - 방화벽 규칙 목록

필요한 경우 규칙을 드래그하여 정렬합니다.

환경에 필요한 순서대로 방화벽 규칙이 적용되면 Apply Changes(변경 사항 적용)를 선택합니다.

HAProxy 구성

HAProxy 개념



HAProxy 개념

HAProxy는 프런트 엔드/백엔드 모델로 구현됩니다.

Frontend는 고객이 통신하는 프록시의 측면을 정의합니다.

프런트 엔드는 IP 및 포트 조합, 인증서 바인딩으로 구성되며 일부 헤더 조작을 구현할 수 있습니다.

백엔드는 물리적 웹 서버와 통신하는 프록시의 측면을 정의합니다.

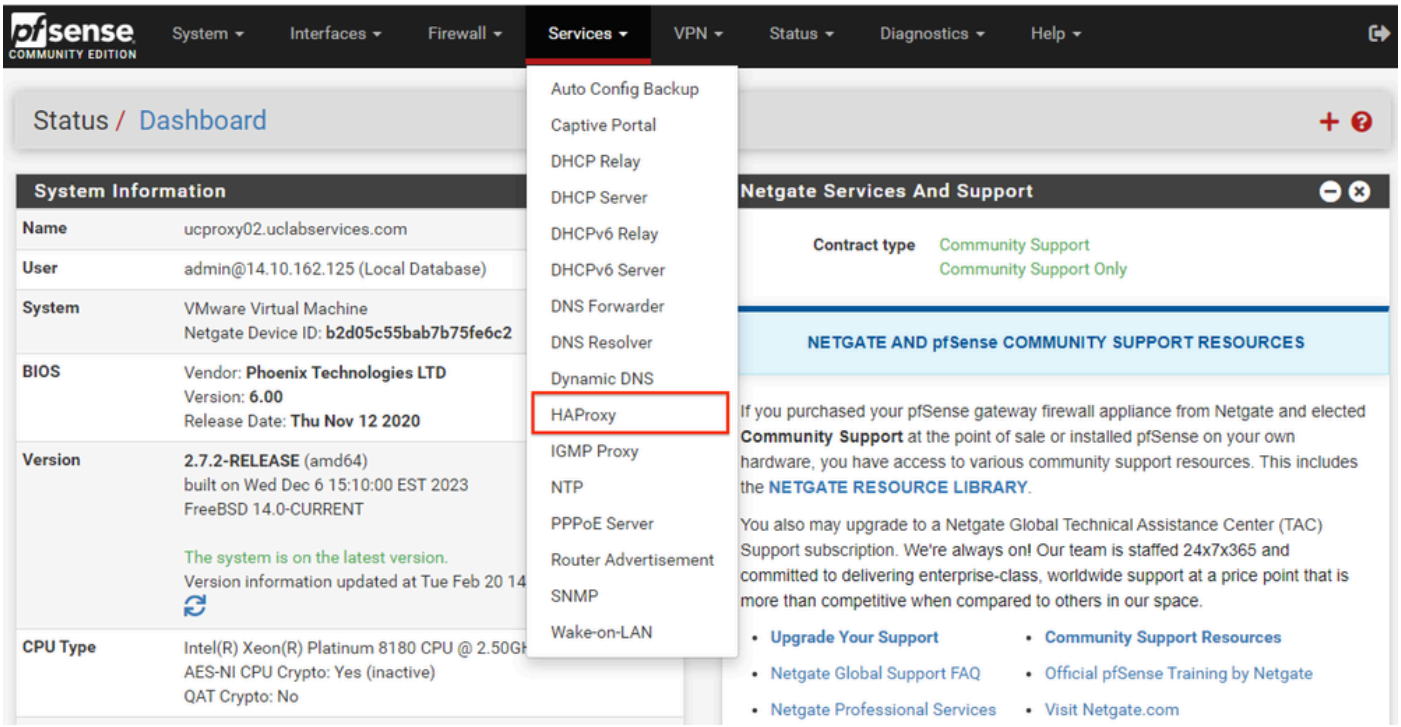
백 엔드는 실제 서버 및 포트, 초기 할당을 위한 로드 밸런싱 방법, 상태 확인 및 지속성을 정의합니다.

프런트 엔드는 전용 백 엔드 또는 ACL을 사용하여 어떤 백 엔드와 통신해야 하는지 알고 있습니다.

ACL은 지정된 프런트 엔드가 다양한 사물에 따라 서로 다른 백엔드와 통신할 수 있도록 서로 다른 규칙을 생성할 수 있습니다.

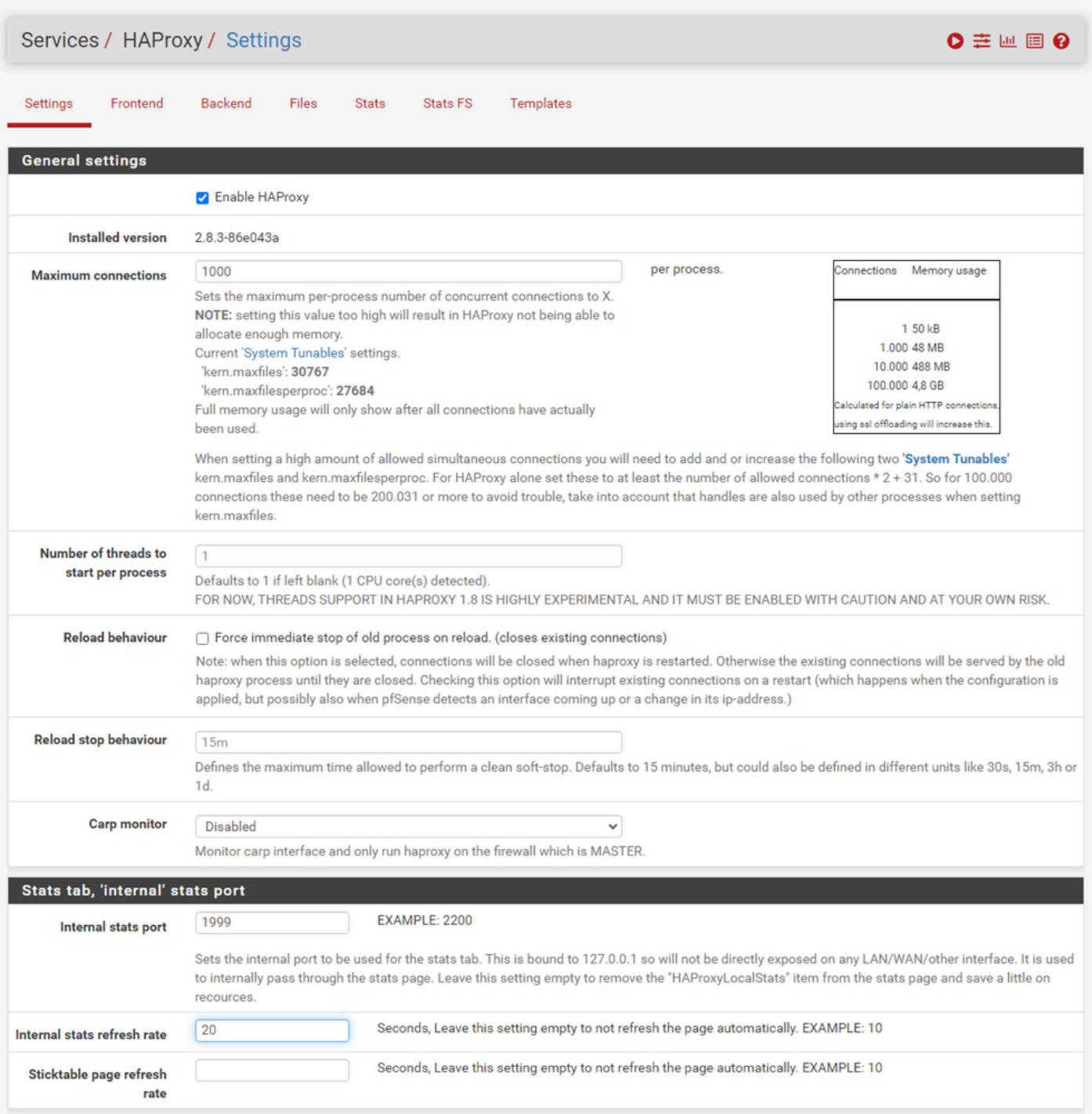
초기 HAProxy 설정

1단계. 서비스 드롭다운에서 HAProxy를 선택합니다.



pfSense GUI - HAProxy 드롭다운

2단계. 기본 설정 구성



pfSense GUI - HAProxy 기본 설정

Enable HAProxy(HAProxy 활성화) 확인란을 선택합니다.

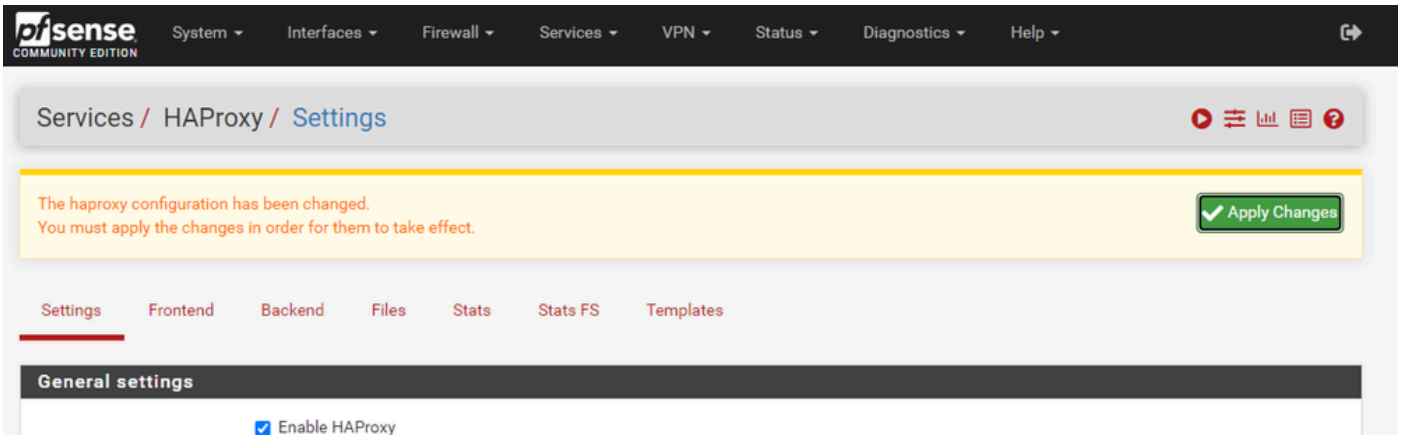
Maximum Connections(최대 연결) 값을 입력합니다. 필요한 메모리에 대한 자세한 내용은 이 섹션의 차트를 참조하십시오.

Internal stats 포트의 값을 입력합니다. 이 포트는 어플라이언스에 대한 HAProxy 통계를 표시하는 데 사용되지만 어플라이언스 외부에 노출되지 않습니다.

내부 통계 새로 고침 빈도 값을 입력합니다.

나머지 컨피그레이션을 검토하고 환경에 필요한 대로 업데이트합니다.

저장을 선택합니다.

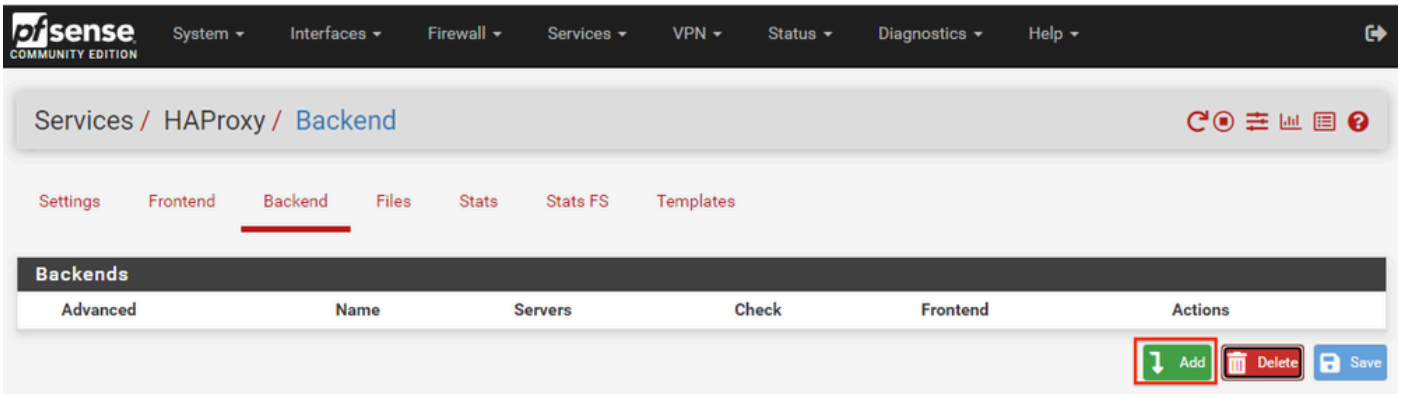


pfSense GUI - HAProxy 변경 사항 적용

참고: 컨피그레이션 변경은 Apply Changes(변경 사항 적용) 버튼을 선택할 때까지 활성화되지 않습니다. 여러 컨피그레이션을 변경하고 한 번에 모두 적용할 수 있습니다. 다른 섹션에서 사용하기 위해 컨피그레이션을 적용할 필요가 없습니다.

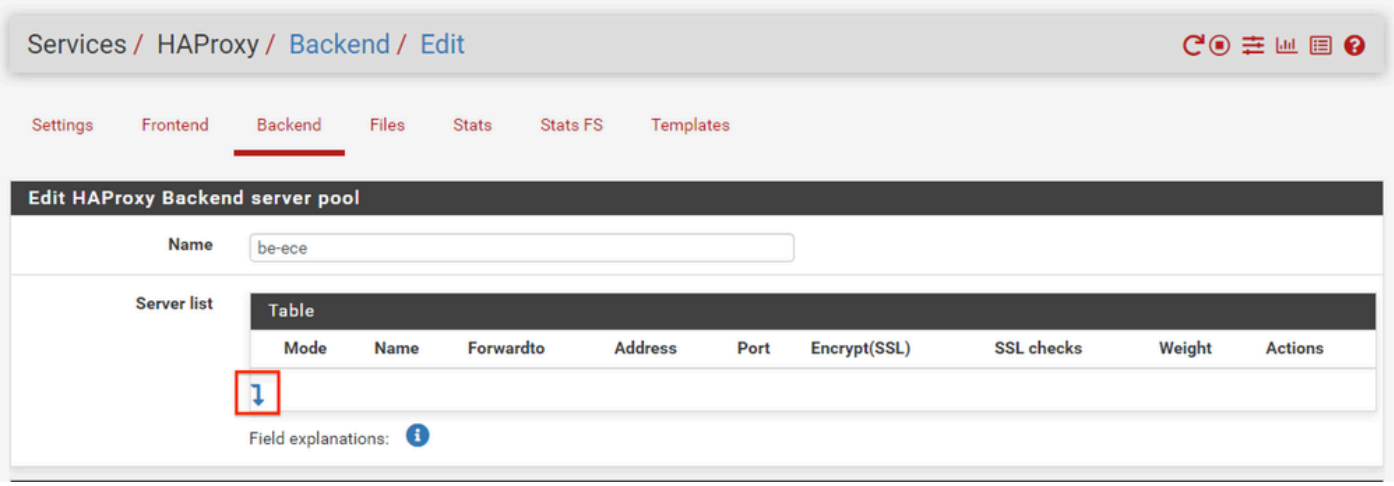
HAProxy 백엔드 구성

백엔드로 시작합니다. 그 이유는 프런트 엔드가 백엔드를 참조해야 하기 때문입니다. 백엔드 메뉴를 선택했는지 확인합니다.



pfSense GUI - HAProxy 백엔드 추가

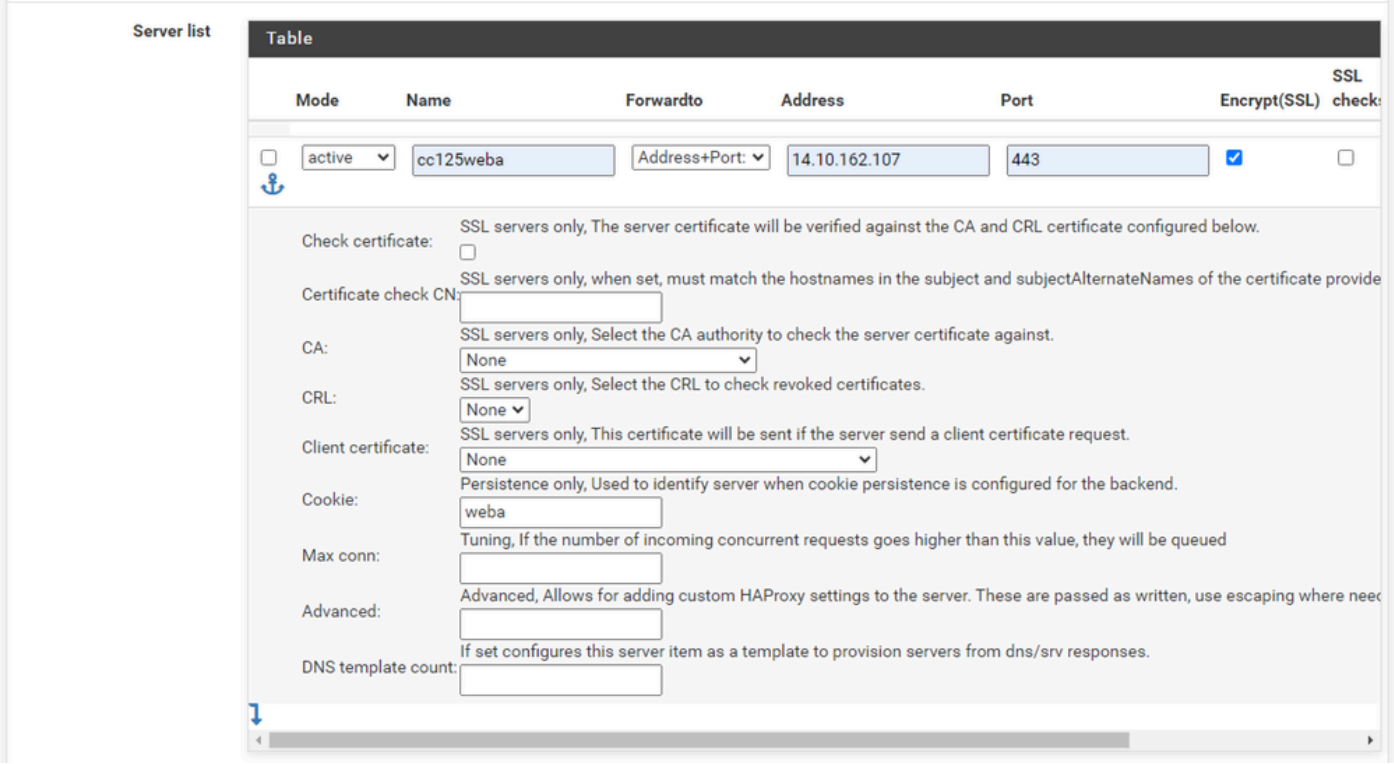
Add(추가) 버튼을 선택합니다.



pfSense GUI - HAProxy 백엔드 시작

백 엔드의 이름을 입력합니다.

아래쪽 화살표를 선택하여 서버 목록에 첫 번째 서버를 추가합니다



백 엔드 - 서버 목록

서버를 참조할 이름을 제공합니다. 실제 서버 이름과 일치할 필요는 없습니다. 통계 페이지에 표시되는 이름입니다.

서버의 주소를 입력합니다. 이는 FQDN에 대한 IP 주소로 구성할 수 있습니다.

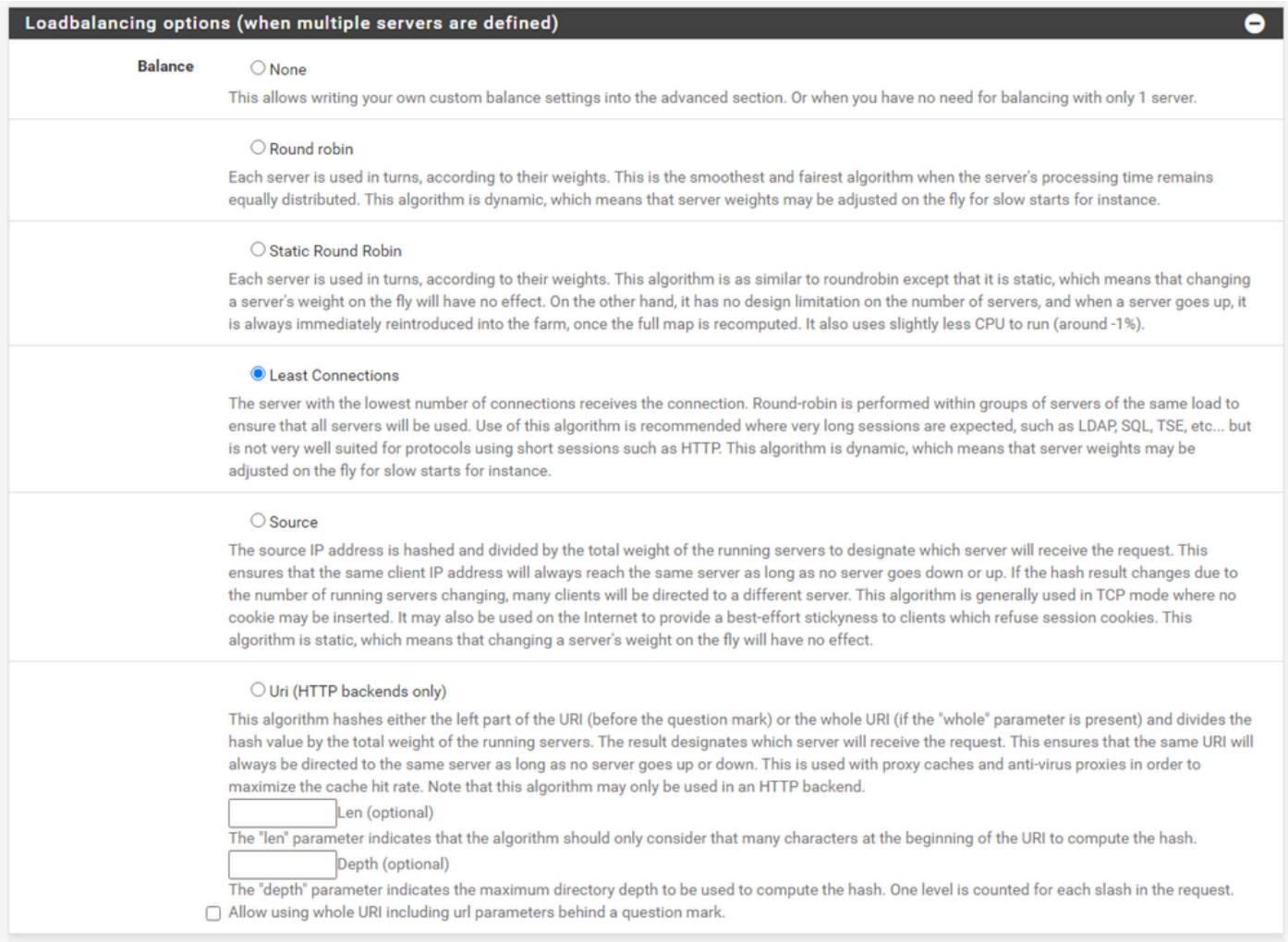
연결할 포트를 제공합니다. ECE의 포트 443이어야 합니다.

Encrypt(SSL)(암호화(SSL)) 확인란을 선택합니다.

Cookie(쿠키) 필드에 값을 입력합니다. 세션 고착성 쿠키의 내용이며 백엔드 내에서 고유해야 합니

다.

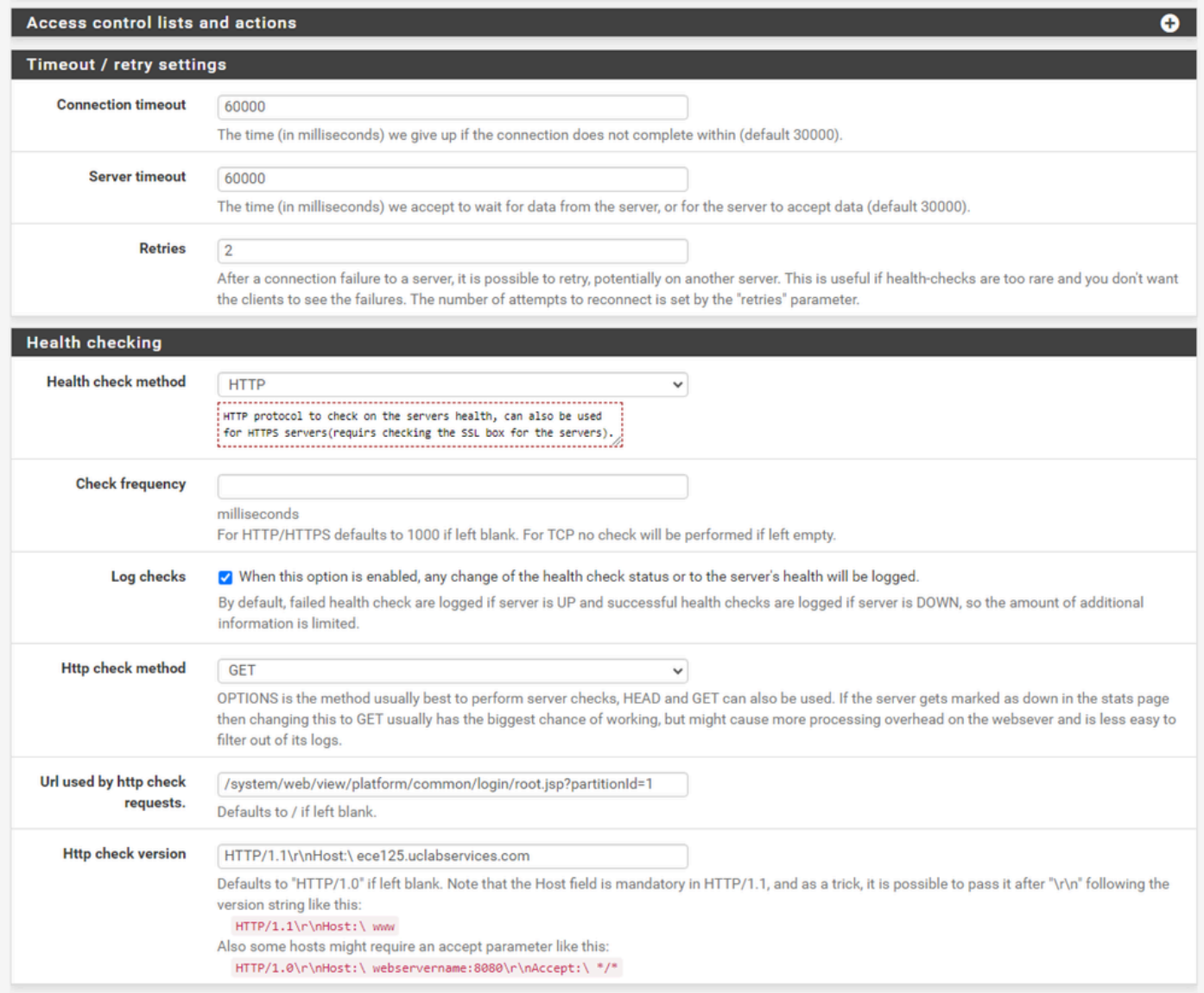
첫 번째 서버가 구성된 후 아래쪽 화살표를 선택하여 환경의 다른 웹 서버를 구성합니다.



HAProxy 백엔드 - 로드 밸런싱

Loadbalancing 옵션을 구성합니다.

ECE 서버의 경우 이 값을 Least Connections로 설정해야 합니다.



HAProxy 백엔드 - 상태 확인

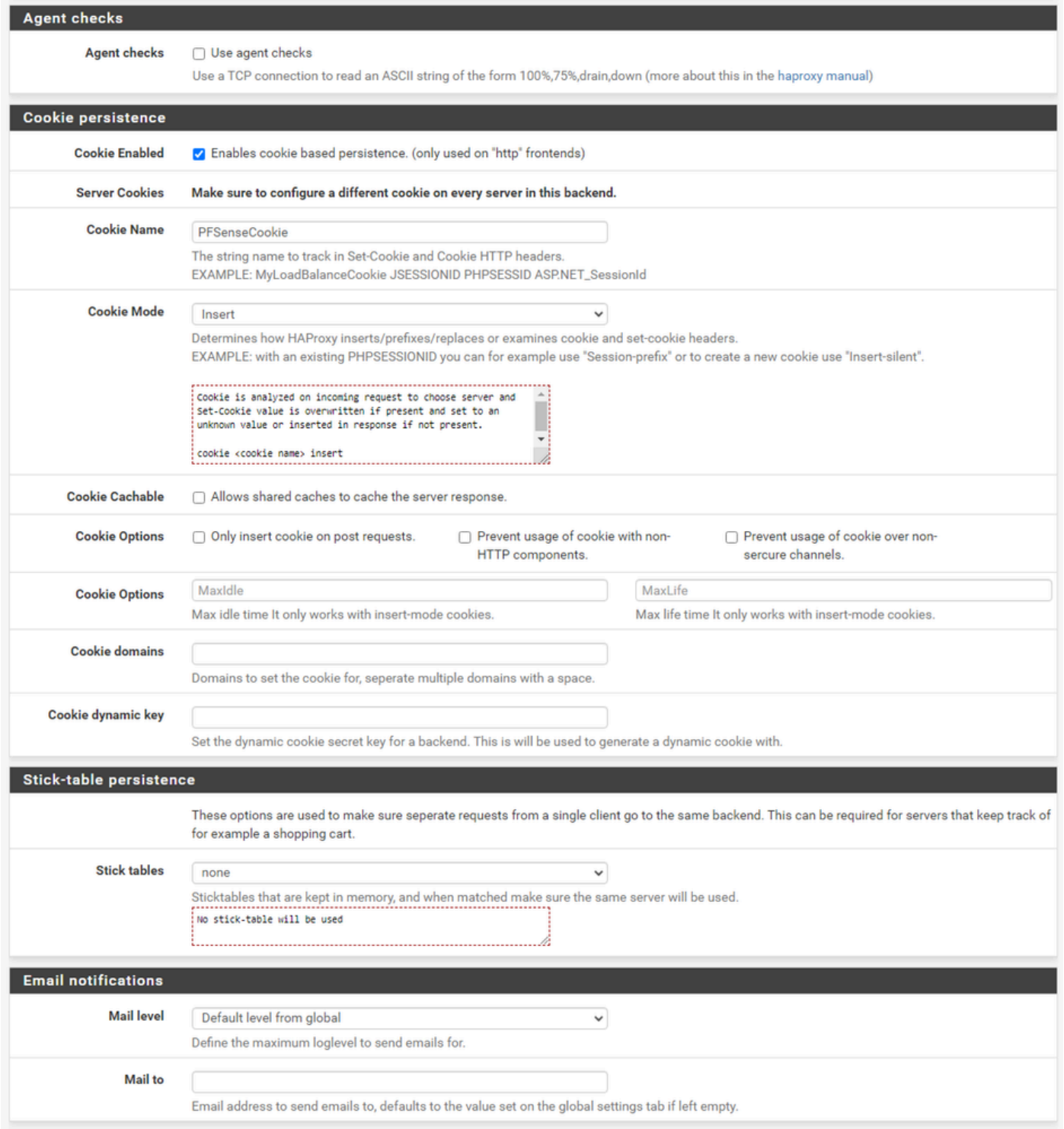
이 컨피그레이션에서는 액세스 제어 목록을 사용하지 않습니다.

시간 초과/재시도 설정은 기본 컨피그레이션에 그대로 둘 수 있습니다.

Health checking(상태 검사) 섹션을 구성합니다.

1. 상태 확인 방법: HTTP
2. Check frequency(빈도 확인): 기본값을 1초마다 사용하려면 비워 둡니다.
3. 로그 확인: 상태 변경 사항을 로그에 기록하려면 이 옵션을 선택합니다.
4. Http 확인 방법: 목록에서 GET을 선택합니다.
5. http 확인 요청에 사용되는 URL.: ECE 서버의 경우 /system/web/view/platform/common/login/root.jsp?partitionId=1을 입력합니다.
6. HTTP 검사 버전: Enter, HTTP/1.1\r\n\Host:\ {fqdn_of_server}

최종 백슬래시 뒤가 아닌 서버의 FQDN 앞에 공백을 포함해야 합니다.

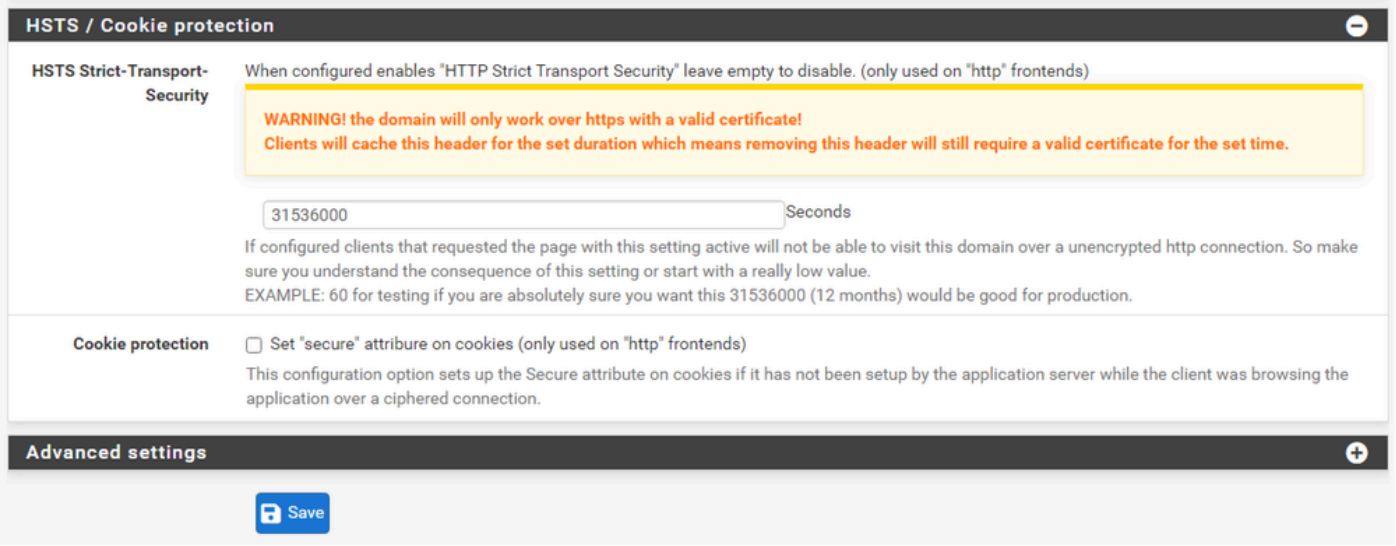


HAProxy 백엔드 - 쿠키 지속성

에이전트 검사를 선택하지 않은 상태로 둡니다.

쿠키 지속성을 구성합니다.

1. Cookie Enabled(쿠키 활성화): 쿠키 기반 지속성을 활성화하려면 선택합니다.
2. Cookie Name(쿠키 이름): 쿠키의 이름을 제공합니다.
3. Cookie Mode(쿠키 모드): 드롭다운 상자에서 Insert(삽입)를 선택합니다.
4. 나머지 옵션은 그대로 둡니다.



HAProxy 백엔드 - HSTS

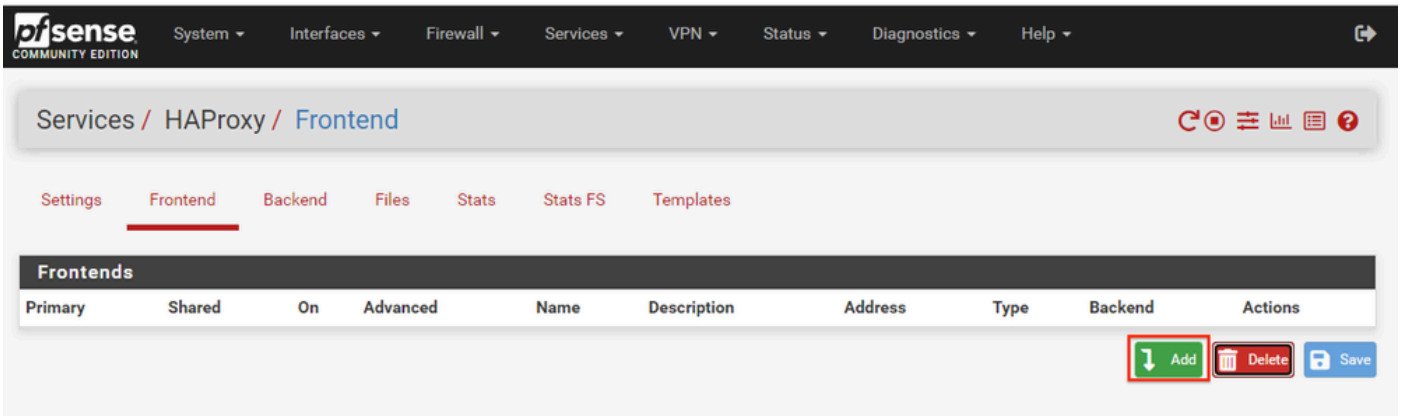
백엔드 컨피그레이션 양식의 나머지 섹션은 기본 설정에 남아 있을 수 있습니다.

HSTS를 구성하려면 이 섹션에서 시간 초과 값을 구성합니다. ECE는 HSTS 쿠키도 삽입하므로 이 컨피그레이션은 이중화됩니다.

Save(저장)를 선택합니다.

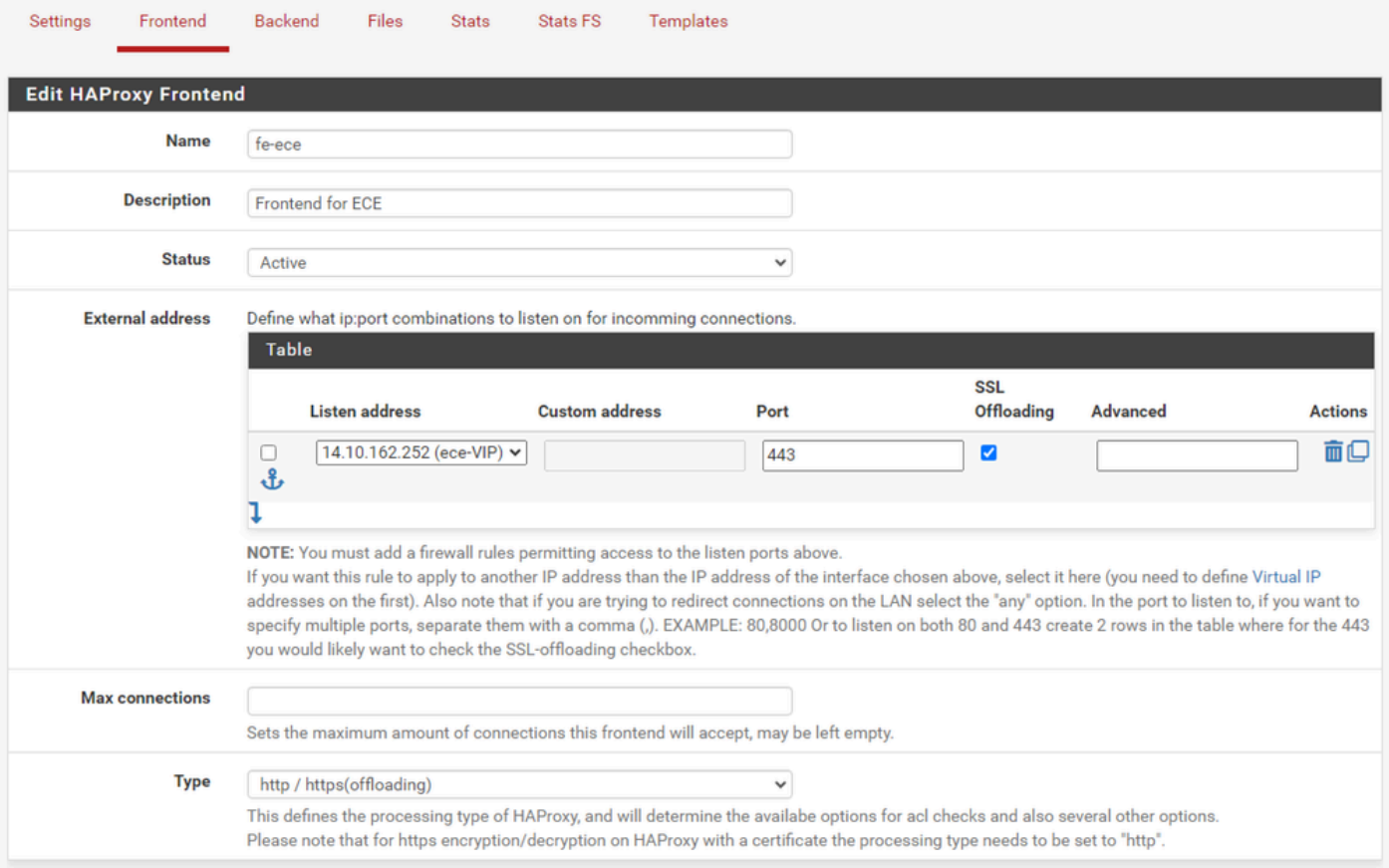
HAProxy 프런트 엔드 구성

프런트 엔드 메뉴로 변경합니다.



pfSense GUI - HAProxy 프런트 엔드 추가

추가 단추를 선택합니다.



HAProxy - 프런트 엔드 헤더

프런트 엔드의 이름을 입력합니다.

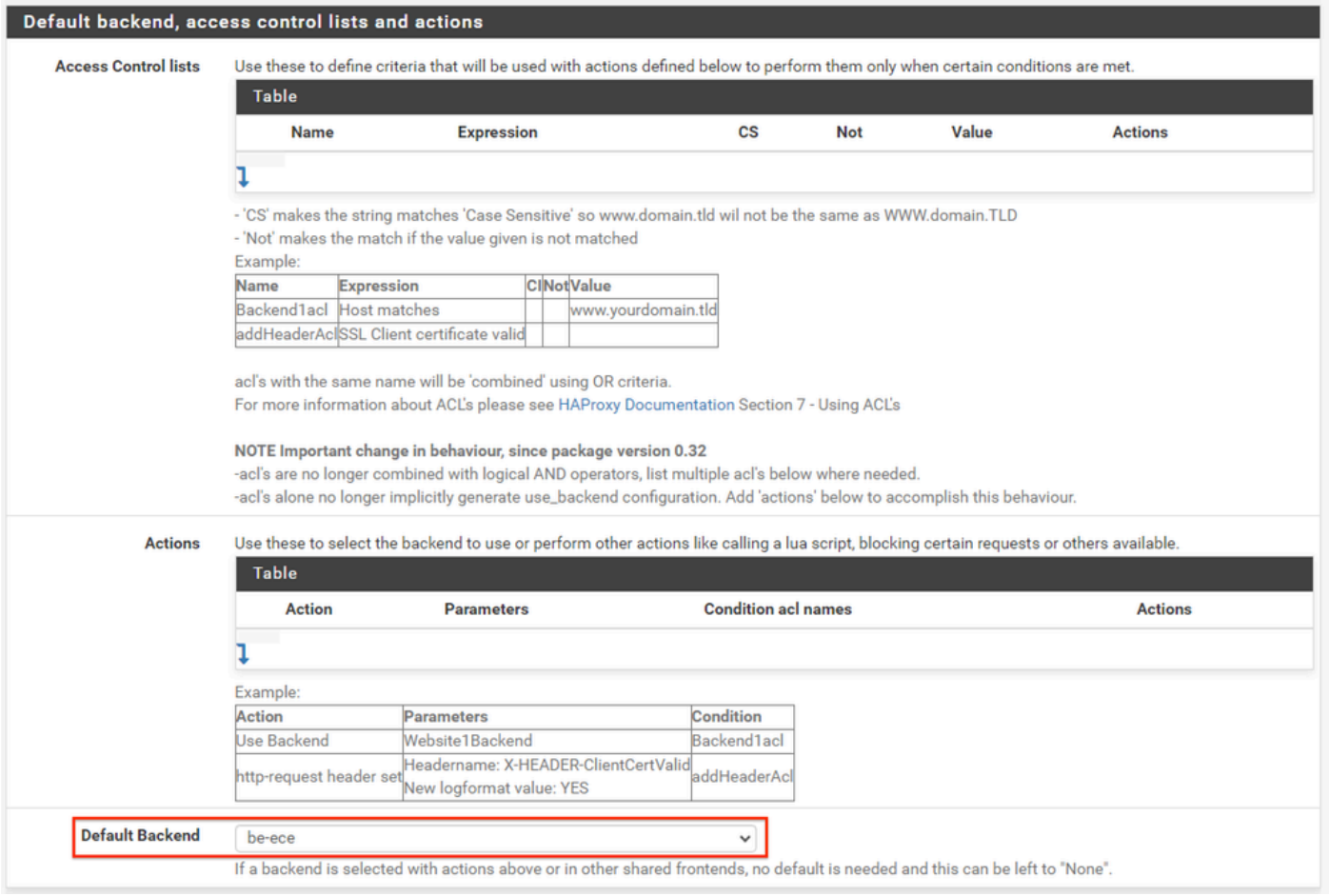
나중에 프런트 엔드를 식별할 수 있도록 설명을 제공합니다.

외부 주소 테이블에서:

1. 수신 대기 주소: 이 웹 사이트에 대해 만든 VIP를 선택합니다.
2. Port(포트): 443을 입력합니다.
3. SSL 오프로딩: 세션 쿠키를 삽입할 수 있도록 이 옵션을 선택합니다.

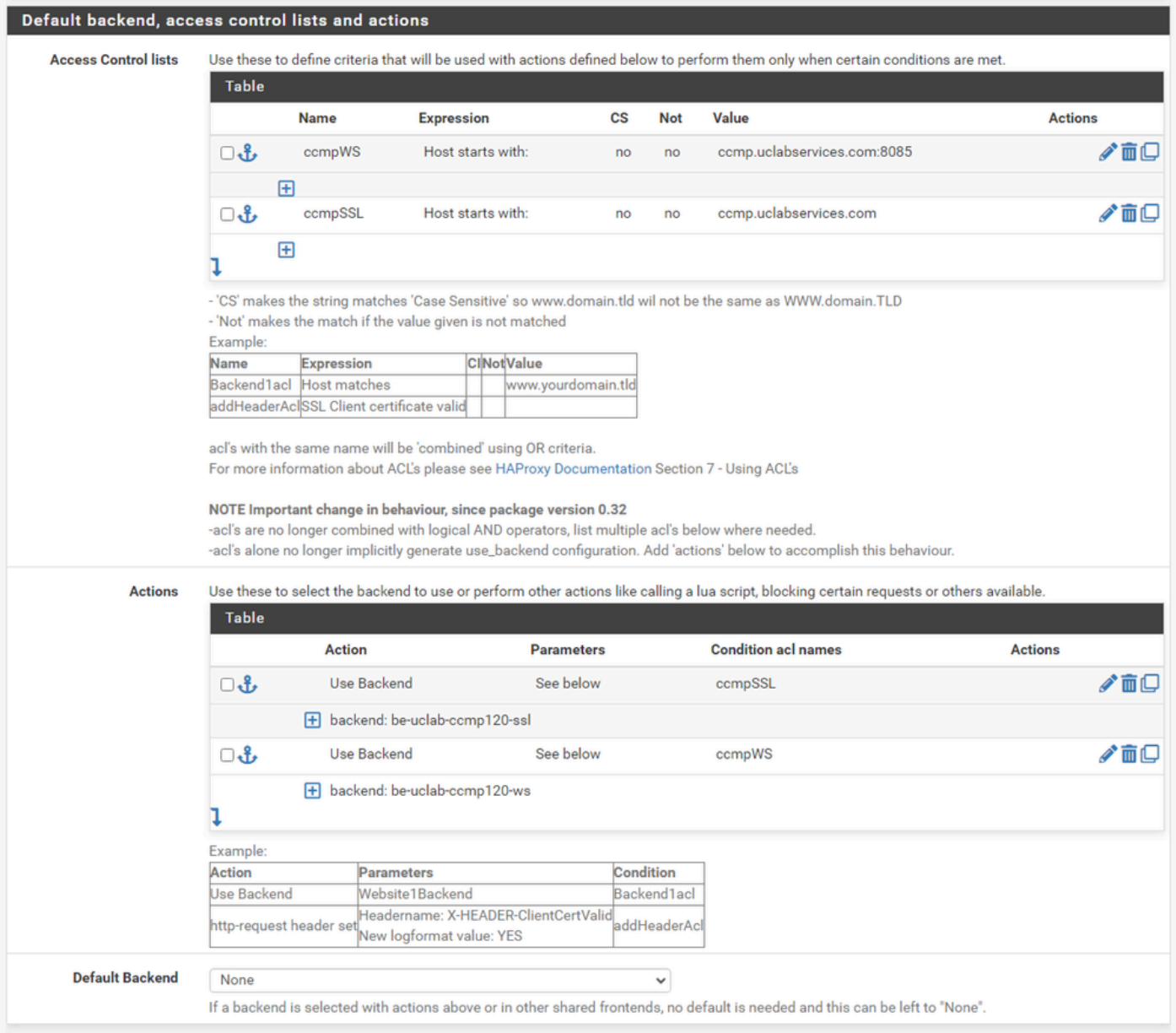
Max connections(최대 연결)는 비워둡니다.

유형이 http/https(오프로딩)로 선택되었는지 확인합니다.



HAProxy 백엔드 - 기본 백엔드 선택

가장 쉬운 컨피그레이션은 드롭다운에서 기본 백엔드를 선택하는 것입니다. 이는 VIP가 단일 웹 사이트를 호스팅하는 경우 선택할 수 있습니다.

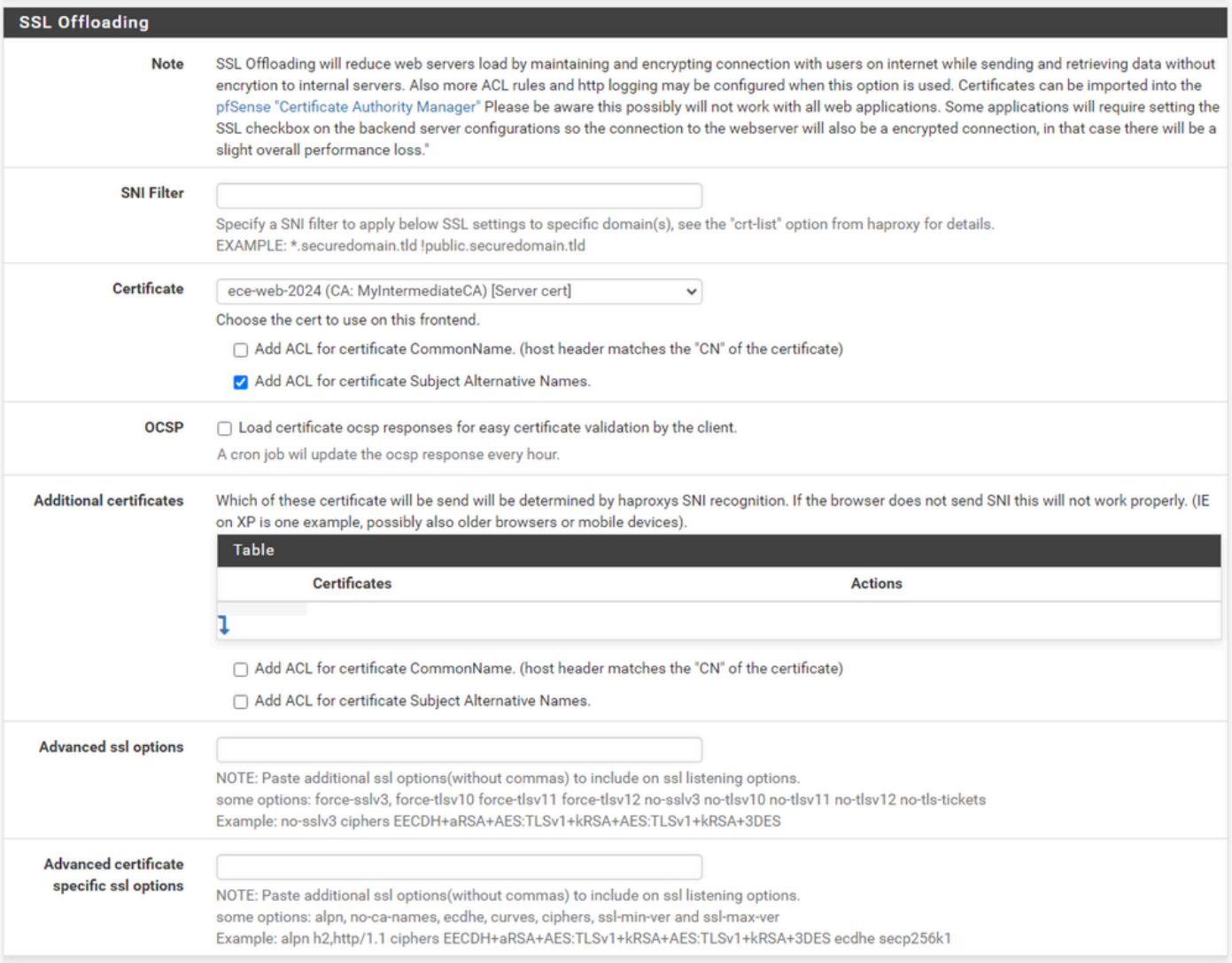


HAProxy 백엔드 - ACL 고급

이미지에 표시된 것처럼 ACL을 사용하여 단일 프런트 엔드를 조건에 따라 여러 백 엔드로 리디렉션할 수 있습니다.

ACL에서 요청의 호스트가 이름 및 포트 번호로 시작하는지 또는 단순히 이름으로 시작하는지 확인하는 것을 볼 수 있습니다. 이를 기반으로 특정 백엔드가 사용됩니다.

이는 ECE에서 흔히 볼 수 있는 일이 아닙니다.



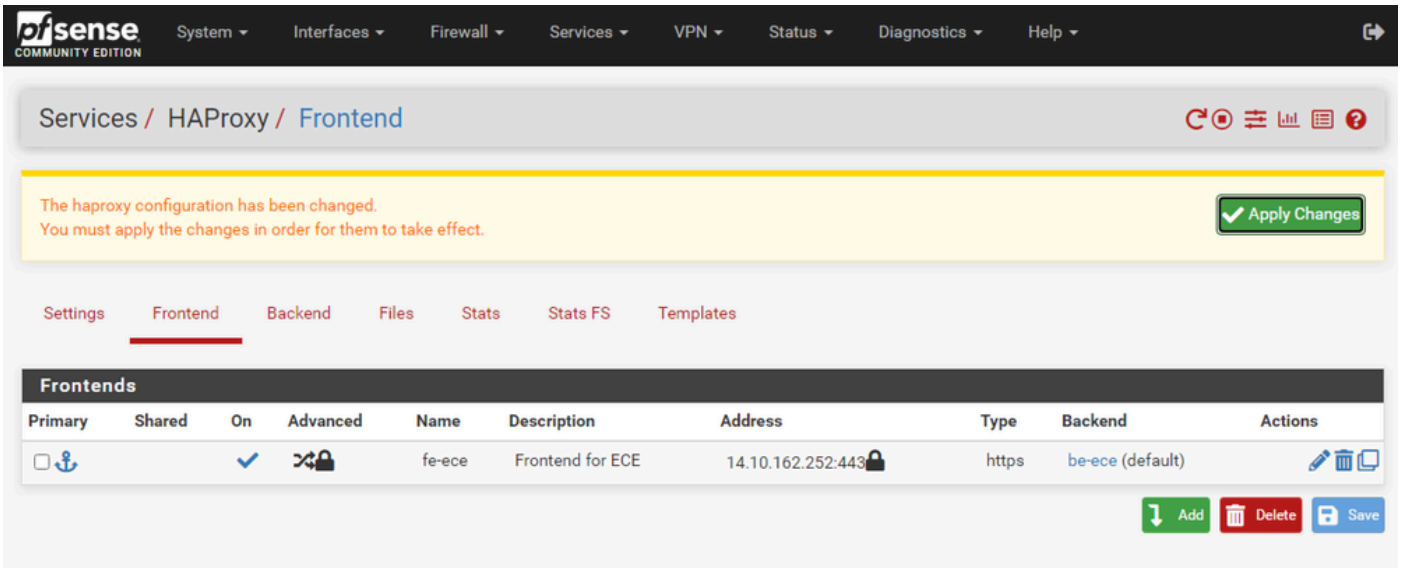
HAProxy 프런트 엔드 - 인증서 바인딩

SSL Offloading(SSL 오프로딩) 섹션에서 이 사이트와 함께 사용하도록 생성된 인증서를 선택합니다. 이 인증서는 서버 인증서여야 합니다.

Add ACL for certificate Subject Alternative Names(인증서 주체 대체 이름에 ACL 추가) 옵션을 선택합니다.

나머지 옵션은 기본값으로 둘 수 있습니다.

이 양식의 끝에 저장을 선택합니다.



HAProxy - 컨피그레이션 적용

프런트 엔드 및 백엔드 변경 사항을 실행 중인 컨피그레이션에 커밋하려면 Apply Changes(변경 사항 적용)를 선택합니다.

축하합니다. pfSense의 설정 및 컨피그레이션을 완료했습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.