

ECE용 pfSense 커뮤니티 로드 밸런서 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[pfSense 설치](#)

[솔루션 개요](#)

[준비](#)

[설치](#)

[네트워크 설정](#)

[초기 설정 완료](#)

[기본 관리 설정 구성](#)

[필수 패키지 추가](#)

[인증서 구성](#)

[가상 IP 추가](#)

[방화벽 구성](#)

[HAProxy 구성](#)

[HAProxy 개념](#)

[초기 HAProxy 설정](#)

[HAProxy 백엔드 구성](#)

[HAProxy 프론트 엔드 구성](#)

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 [사이트](#)를 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 아닙니다.

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 문서](#)를 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>](http://<ip_address_of_appliance>)로 이동합니다.



참고: 처음에는 HTTPS가 아닌 HTTP를 사용해야 합니다.

SIGN IN

Username

Password

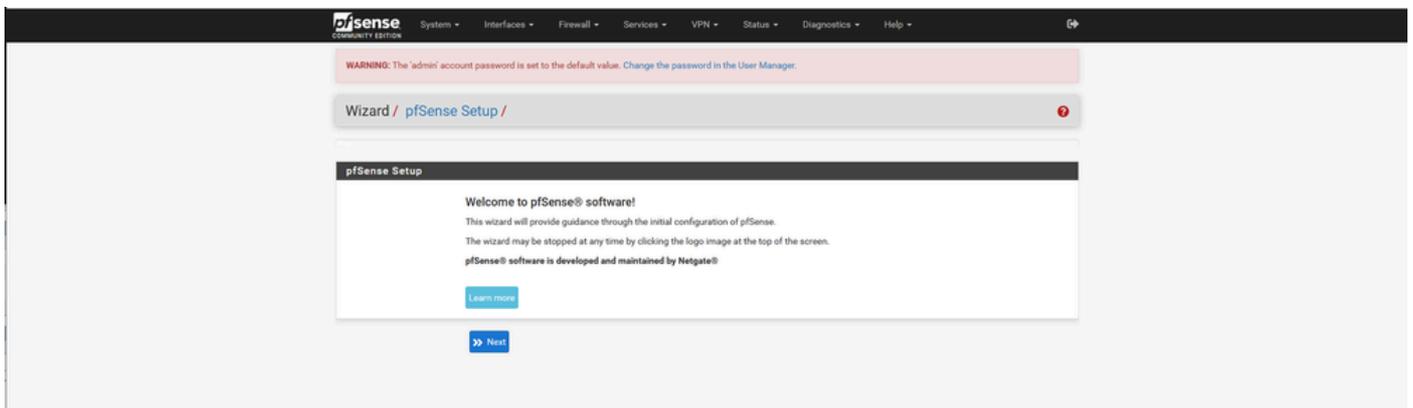
SIGN IN

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
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Wizard / pfSense Setup / General Information ?

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname
Name of the firewall host, without domain part.
Examples: pfsense, firewall, edgefw

Domain
Domain name for the firewall.
Examples: home.arpa, example.com

Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

Primary DNS Server

Secondary DNS Server

Override DNS
Allow DNS servers to be overridden by DHCP/PPP on WAN

[» Next](#)

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
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Wizard / pfSense Setup / Time Server Information ?

Step 3 of 9

Time Server Information

Please enter the time, date and time zone.

Time server hostname
Enter the hostname (FQDN) of the time server.

Timezone

[» Next](#)

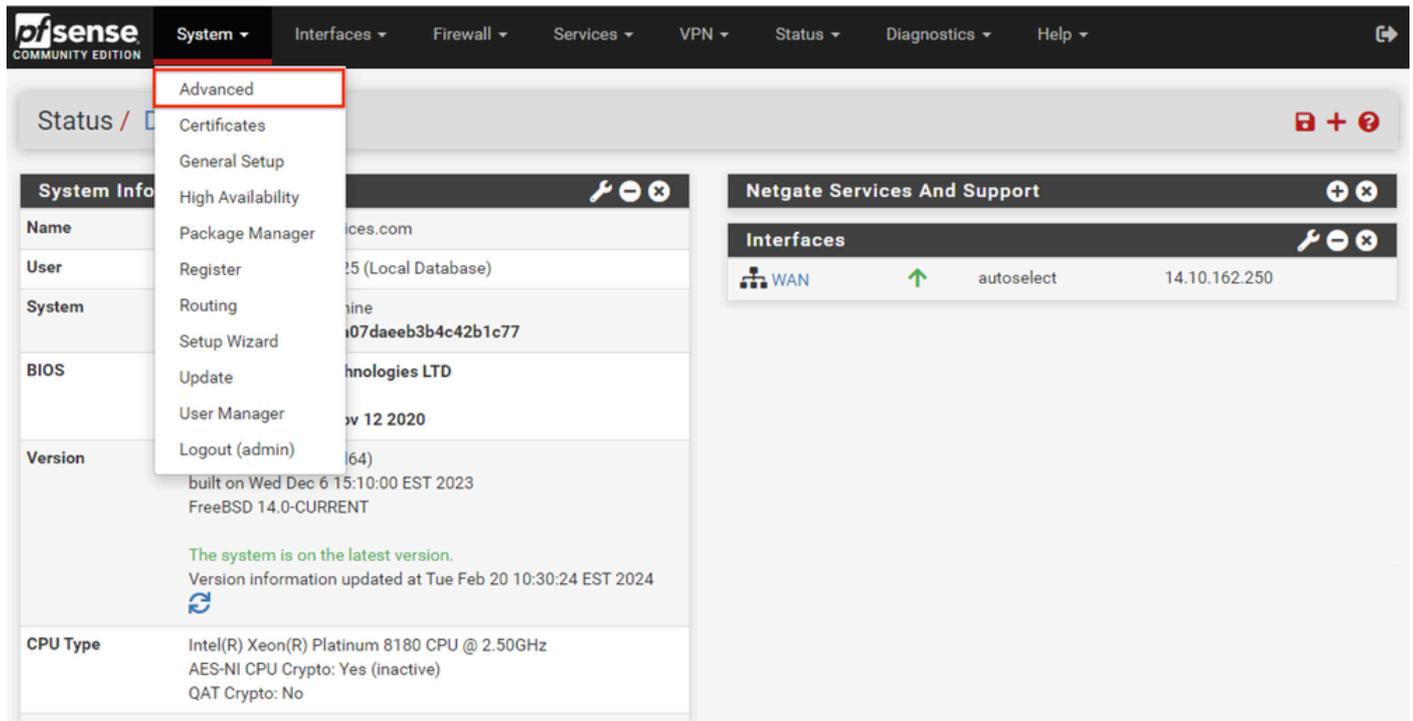
pfSense 설치 마법사 - 3

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

webConfigurator	
Protocol	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS (SSL/TLS)
SSL/TLS Certificate	GUI default (65cced5b25159) <p>Certificates known to be incompatible with use for HTTPS are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.</p>
TCP port	8443 <p>Enter a custom port number for the webConfigurator above to override the default (80 for HTTP, 443 for HTTPS). Changes will take effect immediately after save.</p>
Max Processes	2 <p>Enter the number of webConfigurator processes to run. This defaults to 2. Increasing this will allow more users/browsers to access the GUI concurrently.</p>
WebGUI redirect	<input checked="" type="checkbox"/> Disable webConfigurator redirect rule <p>When this is unchecked, access to the webConfigurator is always permitted even on port 80, regardless of the listening port configured. Check this box to disable this automatically added redirect rule.</p>
HSTS	<input type="checkbox"/> Disable HTTP Strict Transport Security <p>When this is unchecked, Strict-Transport-Security HTTPS response header is sent by the webConfigurator to the browser. This will force the browser to use only HTTPS for future requests to the firewall FQDN. Check this box to disable HSTS. (NOTE: Browser-specific steps are required for disabling to take effect when the browser already visited the FQDN while HSTS was enabled.)</p>
OCSP Must-Staple	<input type="checkbox"/> Force OCSP Stapling in nginx <p>When this is checked, OCSP Stapling is forced on in nginx. Remember to upload your certificate as a full chain, not just the certificate, or this option will be ignored by nginx.</p>
WebGUI Login Autocomplete	<input checked="" type="checkbox"/> Enable webConfigurator login autocomplete <p>When this is checked, login credentials for the webConfigurator may be saved by the browser. While convenient, some security standards require this to be disabled. Check this box to enable autocomplete on the login form so that browsers will prompt to save credentials (NOTE: Some browsers do not respect this option).</p>
GUI login messages	<input type="checkbox"/> Lower syslog level for successful GUI login events <p>When this is checked, successful logins to the GUI will be logged as a lower non-emergency level. Note: The console bell behavior can be controlled independently on the Notifications tab.</p>
Roaming	<input checked="" type="checkbox"/> Allow GUI administrator client IP address to change during a login session <p>When this is checked, the login session to the webConfigurator remains valid if the client source IP address changes.</p>
Anti-lockout	<input type="checkbox"/> Disable webConfigurator anti-lockout rule <p>When this is unchecked, access to the webConfigurator on the WAN interface is always permitted, regardless of the user-defined firewall rule set. Check this box to disable this automatically added rule, so access to the webConfigurator is controlled by the user-defined firewall rules (ensure a firewall rule is in place that allows access, to avoid being locked out!) <i>Hint: the "Set interface(s) IP address" option in the console menu resets this setting as well.</i></p>
DNS Rebind Check	<input type="checkbox"/> Disable DNS Rebinding Checks <p>When this is unchecked, the system is protected against DNS Rebinding attacks. This blocks private IP responses from the configured DNS servers. Check this box to disable this protection if it interferes with webConfigurator access or name resolution in the environment.</p>
Alternate Hostnames	<input type="text"/> <p>Alternate Hostnames for DNS Rebinding and HTTP_REFERER Checks. Specify alternate hostnames by which the router may be queried, to bypass the DNS Rebinding Attack checks. Separate hostnames with spaces.</p>
Browser HTTP_REFERER enforcement	<input checked="" type="checkbox"/> Disable HTTP_REFERER enforcement check <p>When this is unchecked, access to the webConfigurator is protected against HTTP_REFERER redirection attempts. Check this box to disable this protection if it interferes with webConfigurator access in certain corner cases such as using external scripts to interact with this system. More information on HTTP_REFERER is available from Wikipedia.</p>

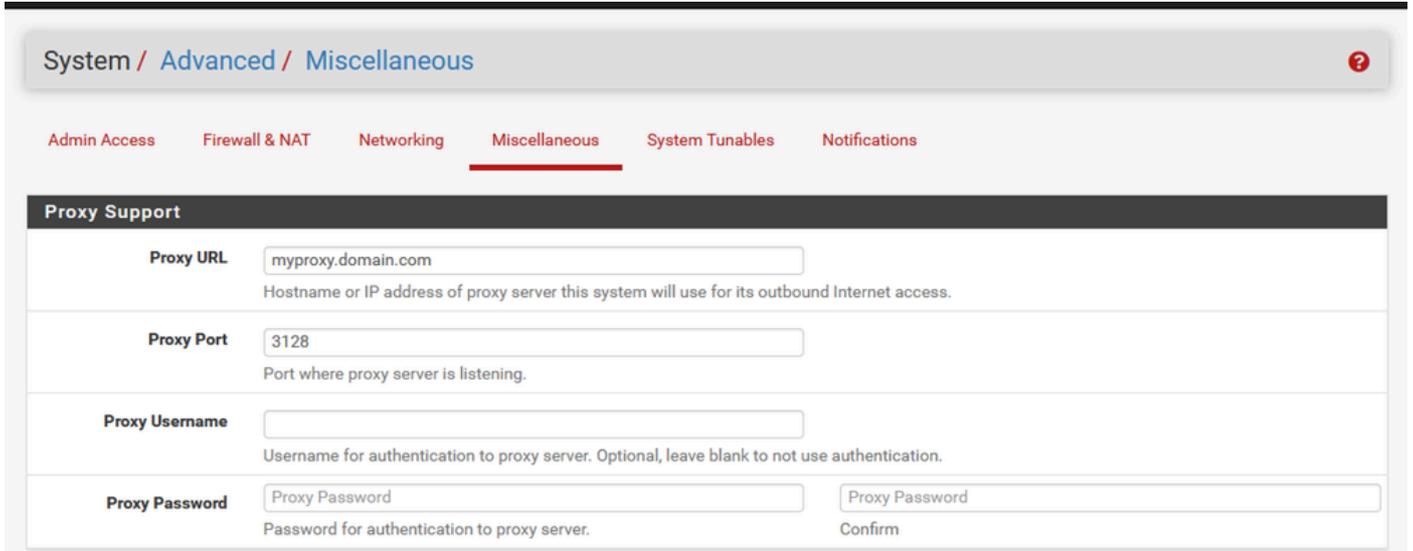
pfSense GUI - 관리 컨피그레이션

1. HTTPS(SSL/TLS) 프로토콜을 선택합니다.
2. 현재 SSL/TLS 인증서를 자체 서명 인증서에 그대로 둡니다.
3. TCP 포트를 443 이외의 포트에 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 리디렉션됩니다.

4단계. 필요한 경우 프록시 서버 구성

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



The screenshot shows the pfSense GUI configuration page for the Miscellaneous tab. The breadcrumb navigation is System / Advanced / Miscellaneous. The Miscellaneous tab is selected, and the Proxy Support section is expanded. The configuration fields are as follows:

Field	Value	Description
Proxy URL	myproxy.domain.com	Hostname or IP address of proxy server this system will use for its outbound Internet access.
Proxy Port	3128	Port where proxy server is listening.
Proxy Username		Username for authentication to proxy server. Optional, leave blank to not use authentication.
Proxy Password	Proxy Password	Password for authentication to proxy server.
Proxy Password (Confirm)	Proxy Password	Confirm

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.

Installed Packages

Available Packages

Search



Search term

Both



Search

Clear

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description	
acme	0.7.5	Automated Certificate Management Environment, for automated use of LetsEncrypt certificates. Package Dependencies: pecl-ssh2-1.3.1 socat-1.7.4.4 php82-8.2.11 php82-ftp-8.2.11	+ Install
apcupsd	0.3.92_1	*apcupsd* can be used for controlling all APC UPS models It can monitor and log the current power and battery status, perform automatic shutdown, and can run in network mode in order to power down other hosts on a LAN Package Dependencies: apcupsd-3.14.14_4	+ Install
arping	1.2.2_4	Broadcasts a who-has ARP packet on the network and prints answers. Package Dependencies: arping-2.21_1	+ Install
arpwatch	0.2.1	This package contains tools that monitors ethernet activity and maintains a database of ethernet/ip address pairings. It also reports certain changes via email.	+ Install

pfSense GUI - 패키지 목록

3단계. 필요한 패키지 찾기 및 설치

1. 하프록시
2. Open-VM 툴



참고: happroxy-devel 패키지는 선택하지 마십시오.

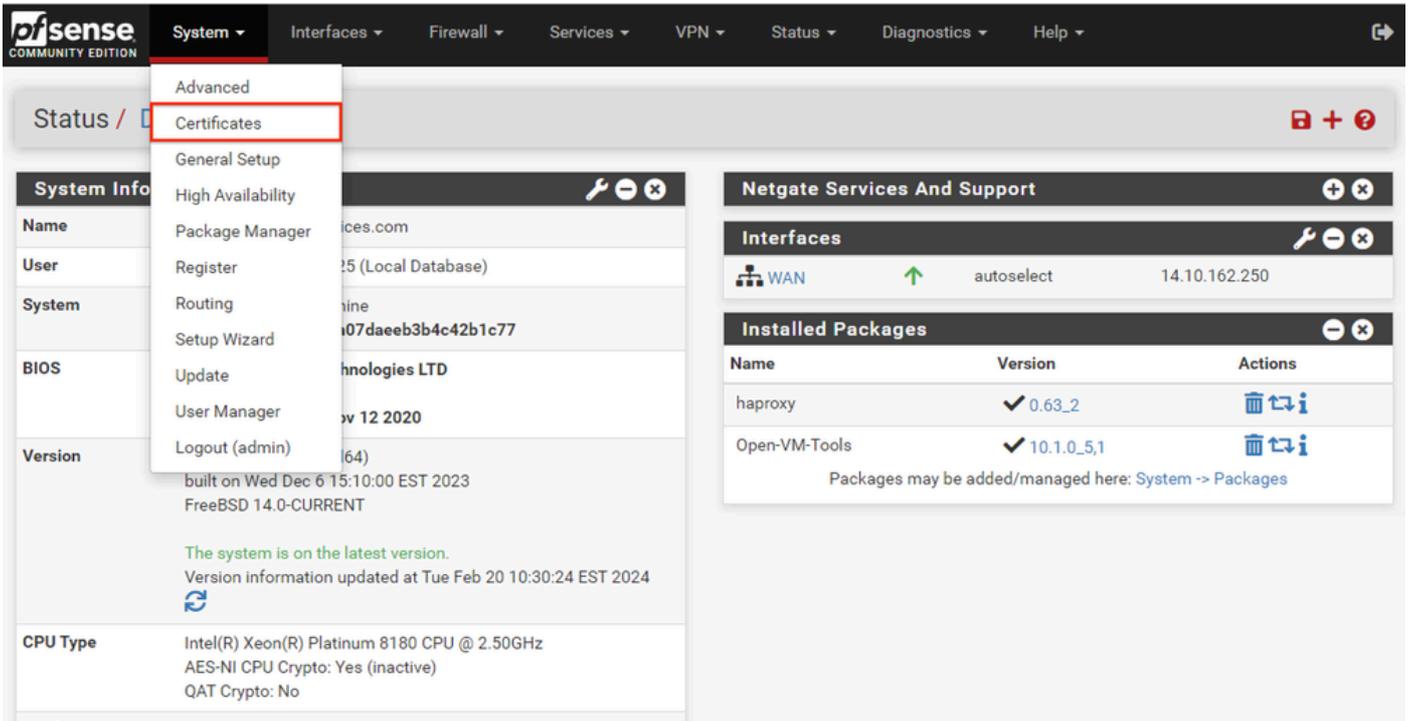
인증서 구성

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.

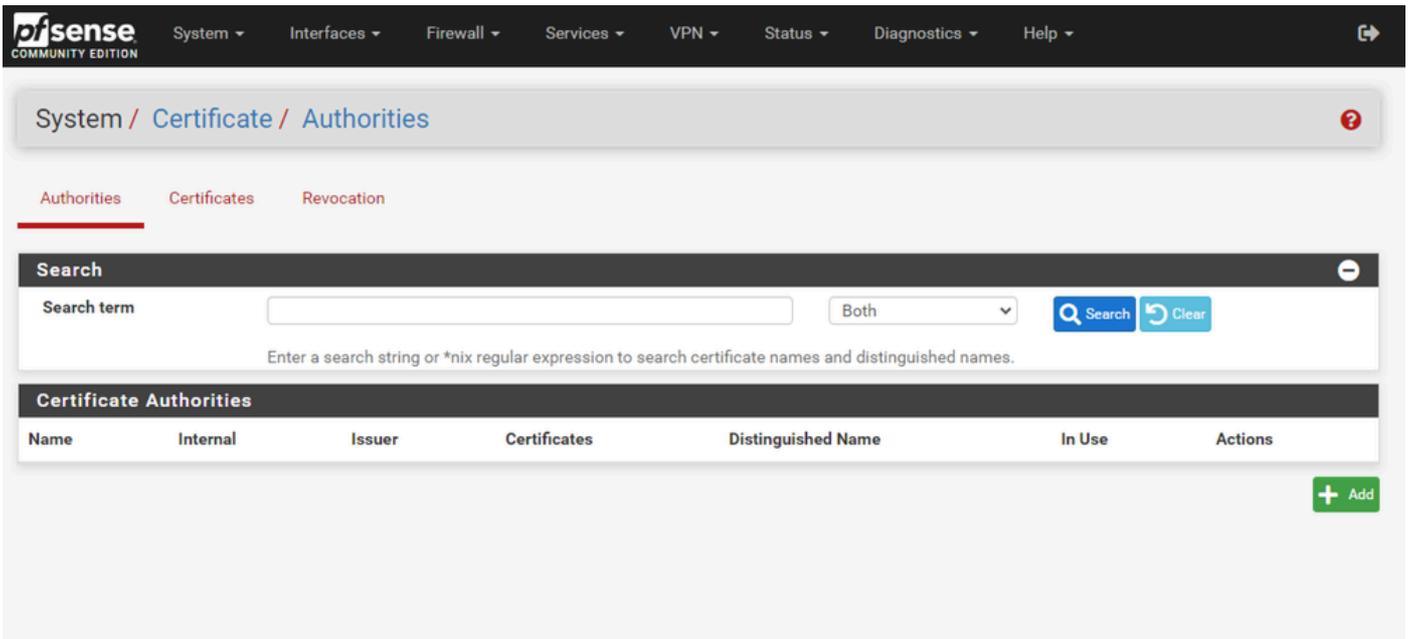
1. PEM 또는 Base-64 인코딩 형식으로 저장된 CA의 루트 인증서
2. PEM 또는 Base-64 인코딩 형식으로 저장된 CA의 모든 중간(발급이라고도 함) 인증서

1단계. 시스템 드롭다운 메뉴에서 인증서를 선택합니다.



pfSense GUI - 인증서 드롭다운

2단계. CA 루트 인증서 가져오기



pfSense GUI - CA 인증서 목록

Add(추가) 버튼을 선택합니다.

System / Certificate / Authorities / Edit

Authorities Certificates Revocation

Create / Edit CA

Descriptive name
 The name of this entry as displayed in the GUI for reference.
 This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '.

Method

Trust Store Add this Certificate Authority to the Operating System Trust Store
 When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Randomize Serial Use random serial numbers when signing certificates
 When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Existing Certificate Authority

Certificate data
 Paste a certificate in X.509 PEM format here.

Certificate Private Key (optional)
 Paste the private key for the above certificate here. This is optional in most cases, but is required when generating a Certificate Revocation List (CRL).

Next Certificate Serial
 Enter a decimal number to be used as a sequential serial number for the next certificate to be signed by this CA. This value is ignored when Randomize Serial is checked.

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.

System / Certificate / Authorities

Authorities Certificates Revocation

Search

Search term Both Search Clear

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
MyRootCA	✘	self-signed	0	OU=pki.uclabservices.com, O=Cisco Systems Inc, CN=UCLAB Services Root, C=US Valid From: Sat, 26 Jan 2019 12:18:03 -0500 Valid Until: Wed, 26 Jan 2039 12:27:59 -0500		

+ Add

pfSense GUI - CA 목록

3단계. CA 중간 인증서 가져오기

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

System / Certificate / Authorities / Edit

Authorities Certificates Revocation

Create / Edit CA

Descriptive name
 The name of this entry as displayed in the GUI for reference.
 This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, *, '.

Method

Trust Store Add this Certificate Authority to the Operating System Trust Store
 When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Randomize Serial Use random serial numbers when signing certificates
 When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Existing Certificate Authority

Certificate data
 Paste a certificate in X.509 PEM format here.

Certificate Private Key (optional)
 Paste the private key for the above certificate here. This is optional in most cases, but is required when generating a Certificate Revocation List (CRL).

Next Certificate Serial
 Enter a decimal number to be used as a sequential serial number for the next certificate to be signed by this CA. This value is ignored when Randomize Serial is checked.

pfSense GUI - CA 중간 가져오기

루트 CA 인증서를 가져와서 중간 CA 인증서를 가져오려면 단계를 반복합니다.

pfSense GUI - CA 링크

System / Certificate / Authorities

Authorities Certificates Revocation

Search

Search term Both

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
MyRootCA	✘	self-signed	1	OU=pki.uclabservices.com, O=Cisco Systems Inc, CN=UCLAB Services Root, C=US Valid From: Sat, 26 Jan 2019 12:18:03 -0500 Valid Until: Wed, 26 Jan 2039 12:27:59 -0500	<input type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Settings"/> <input type="button" value="Delete"/>
MyIntermediateCA	✘	MyRootCA	0	ST=CA, OU=Cisco TAC, O=Cisco Systems Inc, L=San Jose, DC=UCLAB12, DC=local, CN=UCLAB12IssuingCA, C=US Valid From: Mon, 28 Jan 2019 13:10:27 -0500 Valid Until: Sun, 28 Jan 2029 13:20:27 -0500	<input type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Settings"/> <input type="button" value="Delete"/>

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 - Certificates

System / Certificates / Certificates

Authorities Certificates Certificate Revocation

Search

Search term Both

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
GUI default (65cced5b25159) Server Certificate CA: No Server: Yes	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-65cced5b25159 Valid From: Wed, 14 Feb 2024 11:42:03 -0500 Valid Until: Tue, 18 Mar 2025 12:42:03 -0400	<input type="checkbox"/> webConfigurator	<input type="button" value="Edit"/> <input type="button" value="Settings"/> <input type="button" value="Delete"/> <input type="button" value="Refresh"/>

2. CSR(Certificate Signing Request) 양식을 작성합니다.

System / Certificates / Certificates / Edit

Authorities Certificates Certificate Revocation

Add/Sign a New Certificate

Method Create a Certificate Signing Request

Descriptive name ece-web-2024
 The name of this entry as displayed in the GUI for reference.
 This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '.

External Signing Request

Key type RSA

2048
 The length to use when generating a new RSA key, in bits.
 The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

prime256v1 [HTTPS] [IPsec] [OpenVPN]

Digest Algorithm sha256
 The digest method used when the certificate is signed.
 The best practice is to use SHA256 or higher. Some services and platforms, such as the GUI web server and OpenVPN, consider weaker digest algorithms invalid.

Common Name myece.mydomain.com
 The following certificate subject components are optional and may be left blank.

Country Code US

State or Province North Carolina

City Research Triangle Park

Organization Cisco Systems Inc

Organizational Unit Cisco TAC

- 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

Certificate Attributes

Attribute Notes The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.

For Certificate Signing Requests, These attributes are added to the request but they may be ignored or changed by the CA that signs the request.

If this CSR will be signed using the Certificate Manager on this firewall, set the attributes when signing instead as they cannot be carried over.

Certificate Type
 Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.

Alternative Names
 Type Value

Add SAN Row

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 COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

System / Certificates / Certificates

Created certificate signing request ece-web-2024

Authorities Certificates Certificate Revocation

Search

Search term Both

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
GUI default (65cced5b25159) Server Certificate CA: No Server: Yes	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-65cced5b25159 Valid From: Wed, 14 Feb 2024 11:42:03 -0500 Valid Until: Tue, 18 Mar 2025 12:42:03 -0400	webConfigurator	   
ece-web-2024	external - signature pending	ST=North Carolina, OU=Cisco TAC, O=Cisco Systems Inc, L=Research Triangle Park, CN=ece.uclabservices.com, C=US		  

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.

System / Certificates / Certificates

Created certificate signing request ece-web-2024

Authorities Certificates Certificate Revocation

Search

Search term Both

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Name	Issuer	Distinguished Name	In Use	Actions
GUI default (65cced5b25159) Server Certificate CA: No Server: Yes	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-65cced5b25159 Valid From: Wed, 14 Feb 2024 11:42:03 -0500 Valid Until: Tue, 18 Mar 2025 12:42:03 -0400	webConfigurator	
ece-web-2024	external - signature pending	ST=North Carolina, OU=Cisco TAC, O=Cisco Systems Inc, L=Research Triangle Park, CN=ece.uclabservices.com, C=US		

+ Add/Sign

pfSense GUI - 인증서 가져오기

서명된 인증서를 가져오려면 연필 아이콘을 선택합니다.

5. 양식에 인증서 데이터를 붙여넣습니다.

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

System / Certificates / Certificates / Edit

Authorities Certificates Certificate Revocation

Complete Signing Request for ece-web-2024

Descriptive name
 The name of this entry as displayed in the GUI for reference.
 This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ', "

Signing request data
 -----BEGIN CERTIFICATE REQUEST-----
 MIIDvDCCAqQCAQAwZcHjAcBgNVBAMTFWVjZS51Y2xhYnN1cnZpY2VzLmN1bVbTEL
 MAKGA1UEBhMCMVVMxZzAVBgNVBAGTDk5vcnRoIENhcm9saW5hMR8wHQYDVQQHEXZS
 ZXN1YXJjaCBUcm1hbmdsZSBQYXJrMR0wGAYDVQQKExFDaXNjbyBTeXN0ZW1zIEIu
 YzESMBAGA1UECzMjQ21zY28gVEFDMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
 Copy the certificate signing data from here and forward it to a certificate authority for signing.

Final certificate data
 GBSApWQkAs305JkKISY/pYEI2EW/7EZcDmHRUrnEFcWoRR2984LJgDgs1pmlcPL
 V11oh2f4skcrjrvBiOu+VjhTJEos7rF+yiZ3IT4TJwDlLEXAGJqB+jy8G5bfsZQf
 QNYnxuZ5Mnuqx1PN97EPQngO/1IgxO4xDz6Dg+Iwt9pyrRZdxpmy
 -----END CERTIFICATE-----
 Paste the certificate received from the certificate authority here.

pfSense GUI - 인증서 가져오기

인증서를 저장하려면 Update(업데이트)를 선택합니다.

6. 인증서 데이터가 정확한지 검토합니다.

pfSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

System / Certificates / Certificates

Authorities Certificates Certificate Revocation

Search

Search term Both ▾

Enter a search string or *nix regular expression to search certificate names and distinguished names.

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
GUI default (65ccd5b25159) Server Certificate CA: No Server: Yes	self-signed	O=pfSense GUI default Self-Signed Certificate, CN=pfSense-65ccd5b25159 Valid From: Wed, 14 Feb 2024 11:42:03 -0500 Valid Until: Tue, 18 Mar 2025 12:42:03 -0400	webConfigurator	
ece-web-2024 CA: No Server: Yes	MyIntermediateCA	ST=North Carolina, OU=Cisco TAC, O=Cisco Systems Inc, L=Research Triangle Park, CN=ece.uclabservices.com, C=US Valid From: Tue, 20 Feb 2024 12:31:00 -0500 Valid Until: Thu, 19 Feb 2026 12:31:00 -0500		

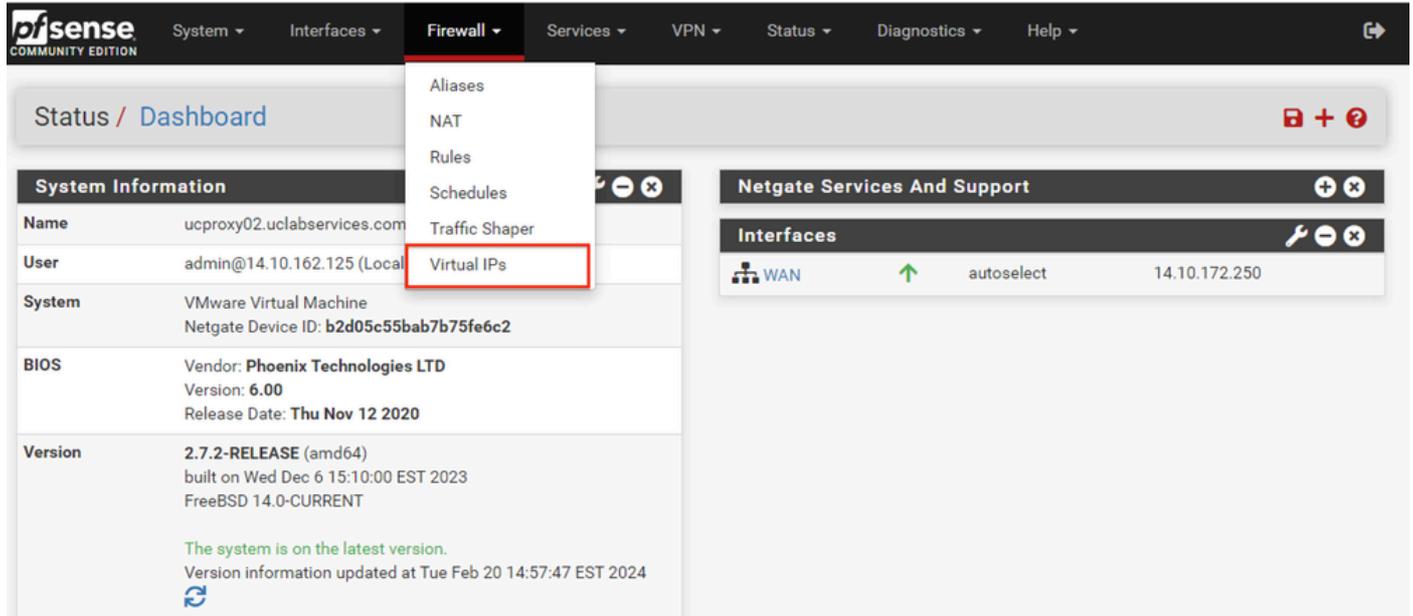
pfSense GUI - 인증서 목록

7. 이 pfSense에서 여러 사이트를 호스팅하려면 이 프로세스를 반복합니다.

가상 IP 추가

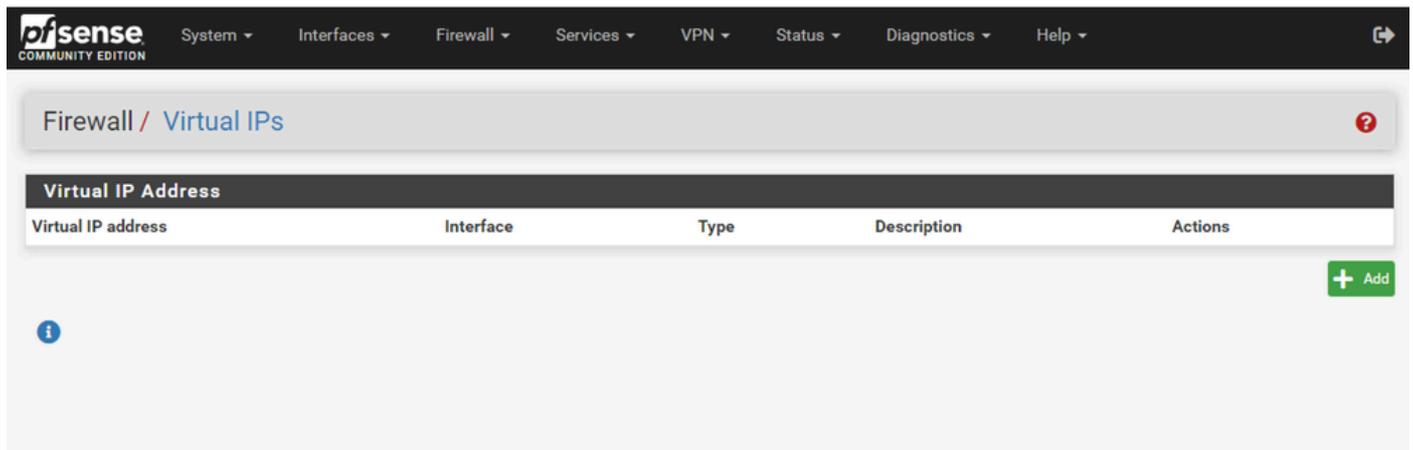
pfSense에서 웹 사이트를 호스팅하려면 하나 이상의 IP가 필요합니다. pfSense에서는 VIP(Virtual IP)를 통해 수행됩니다.

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

[System](#) ▾ [Interfaces](#) ▾ [Firewall](#) ▾ [Services](#) ▾ [VPN](#) ▾ [Status](#) ▾ [Diagnostics](#) ▾ [Help](#) ▾

Firewall / Virtual IPs / Edit ?

Edit Virtual IP

Type IP Alias CARP Proxy ARP Other

Interface WAN ▾

Address type Single address ▾

Address(es) 14.10.162.251 / 32 ▾
The mask must be the network's subnet mask. It does not specify a CIDR range.

Virtual IP Password Virtual IP Password Virtual IP Password
Enter the VHID group password. Confirm

VHID Group 1 ▾
Enter the VHID group that the machines will share.

Advertising frequency 1 ▾ 0 ▾
Base Skew
The frequency that this machine will advertise. 0 means usually master. Otherwise the lowest combination of both values in the cluster determines the master.

Description ece-VIP
A description may be entered here for administrative reference (not parsed).

i

pfSense GUI - VIP 컨피그레이션

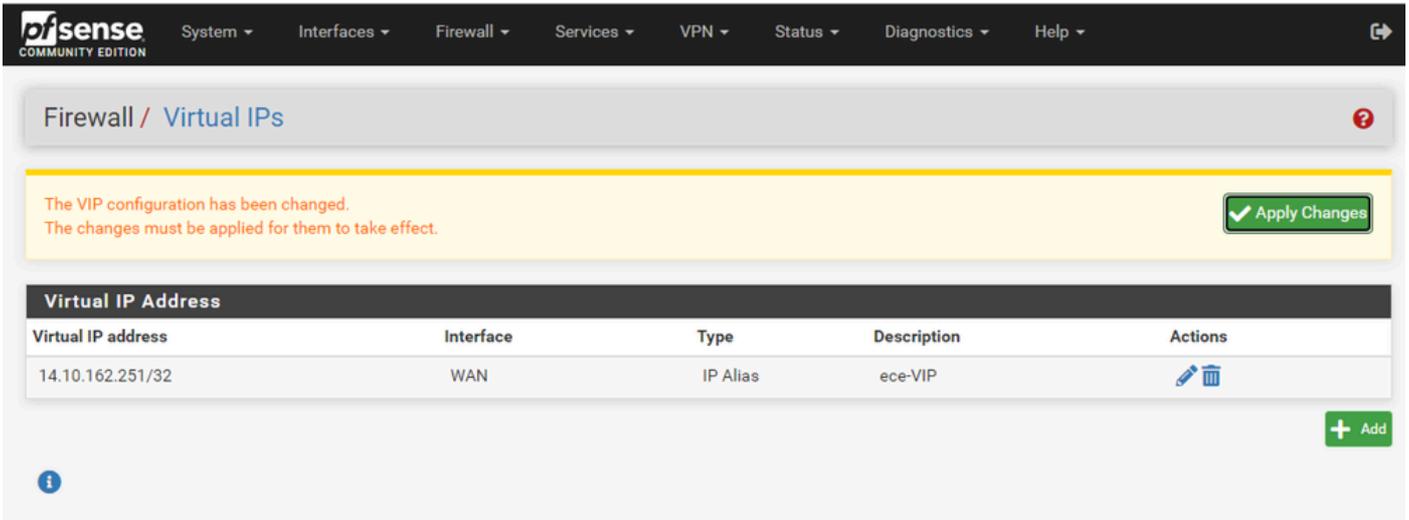
정보를 사용하여 VIP를 추가합니다.

- 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



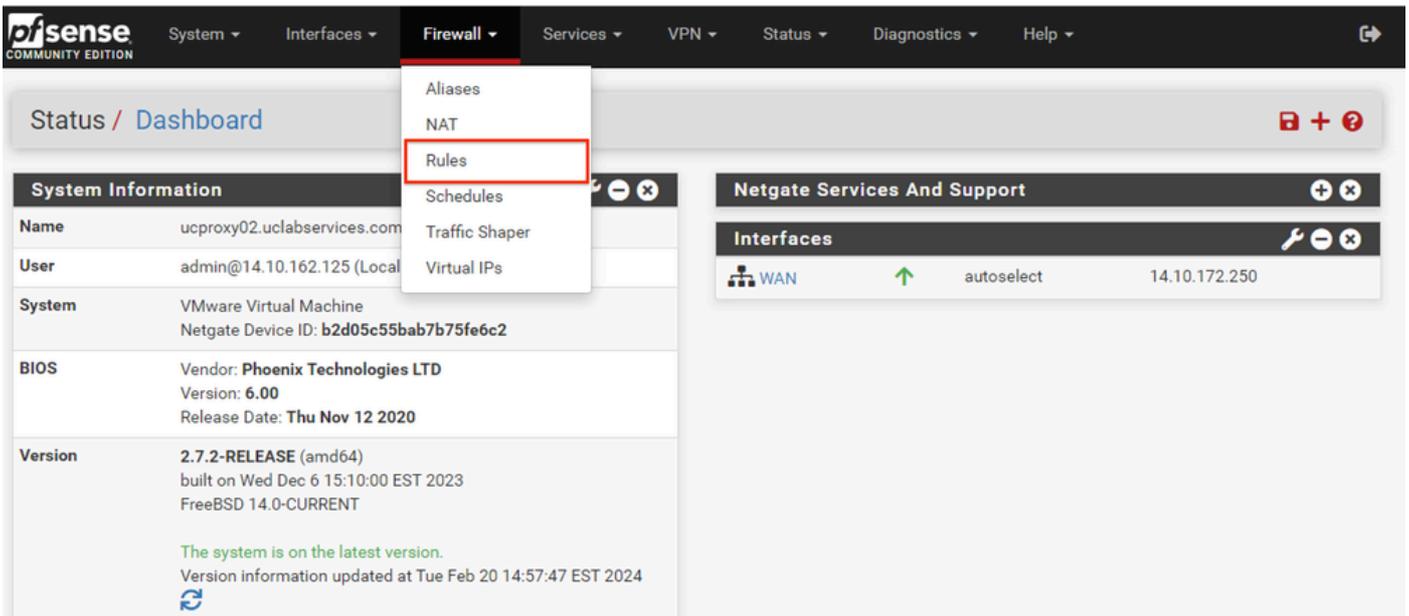
pfSense GUI - VIP 목록

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

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Firewall / Rules / WAN 📊 📄 ?

Floating WAN

Rules (Drag to Change Order)												
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
<input checked="" type="checkbox"/>	0/13.35 MiB	*	*	*	WAN Address	8443 22	*	*		Anti-Lockout Rule	⚙️	
<input checked="" type="checkbox"/>	0/0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	⚙️	
<input checked="" type="checkbox"/>	0/3.63 MiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙️	

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until pass rules are added. Click the button to add a new rule.

⬆️ Add
⬇️ Add
🗑️ Delete
🔄 Toggle
📄 Copy
💾 Save
➕ Separator

i

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
COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Firewall / Rules / Edit

Edit Firewall Rule

Action ▾
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled Disable this rule
Set this option to disable this rule without removing it from the list.

Interface ▾
Choose the interface from which packets must come to match this rule.

Address Family ▾
Select the Internet Protocol version this rule applies to.

Protocol ▾
Choose which IP protocol this rule should match.

Source

Source Invert match ▾ / ▾

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination Invert match ▾ / ▾

Destination Port Range ▾ ▾
From Custom To Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options

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.

The screenshot shows the pfSense Firewall Rules configuration page. The page title is "Firewall / Rules / Edit". The main heading is "Edit Firewall Rule".

Action: Block

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: WAN
Choose the interface from which packets must come to match this rule.

Address Family: IPv4
Select the Internet Protocol version this rule applies to.

Protocol: TCP
Choose which IP protocol this rule should match.

Source:

Source: Invert match Any Source Address /

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

Destination:

Destination: Invert match Any Destination Address /

Destination Port Range: (other) From Custom To (other) Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options:

Log: Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description: Drop all other inbound traffic
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options:

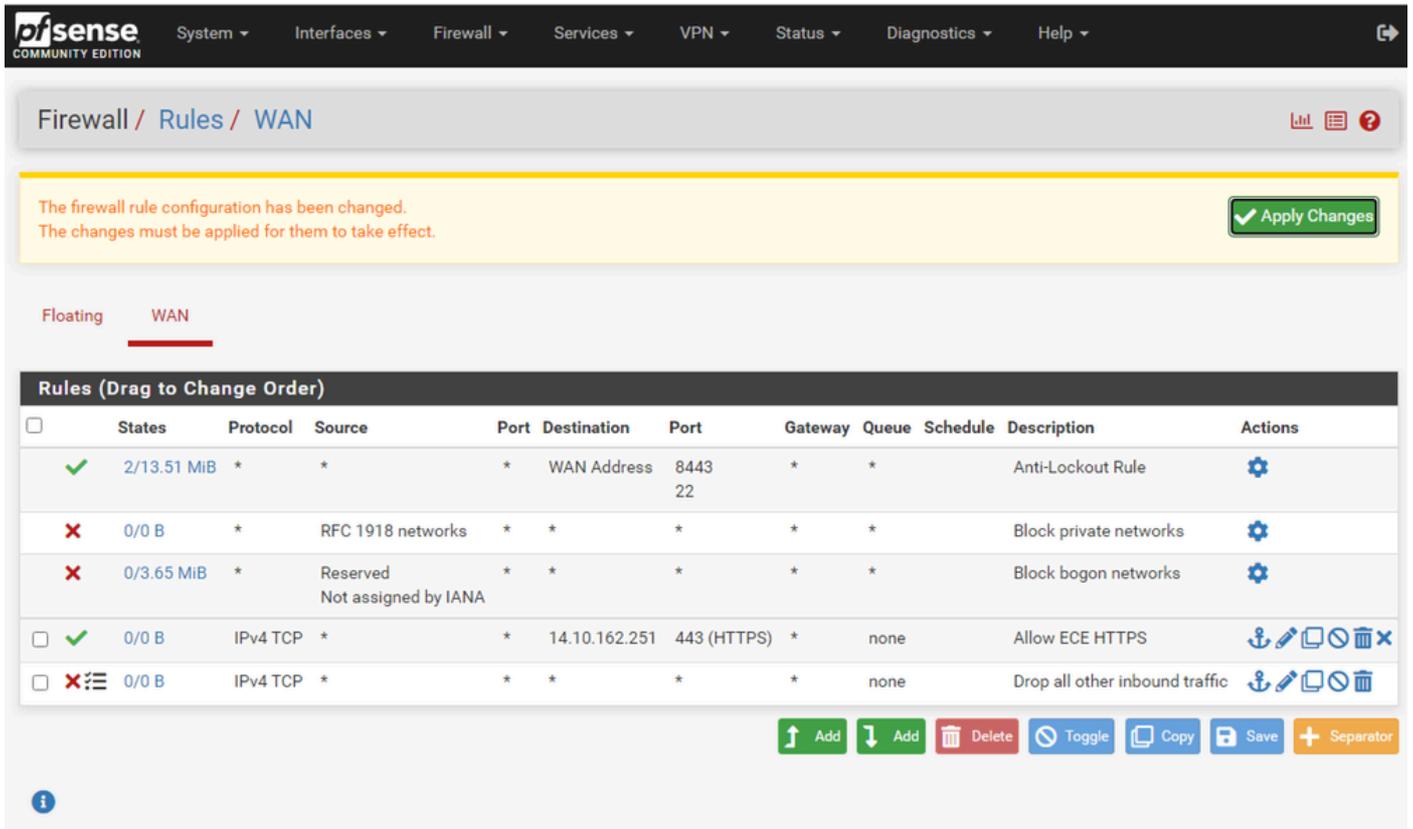
pfSense GUI - 방화벽 삭제 규칙 컨피그레이션

- 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



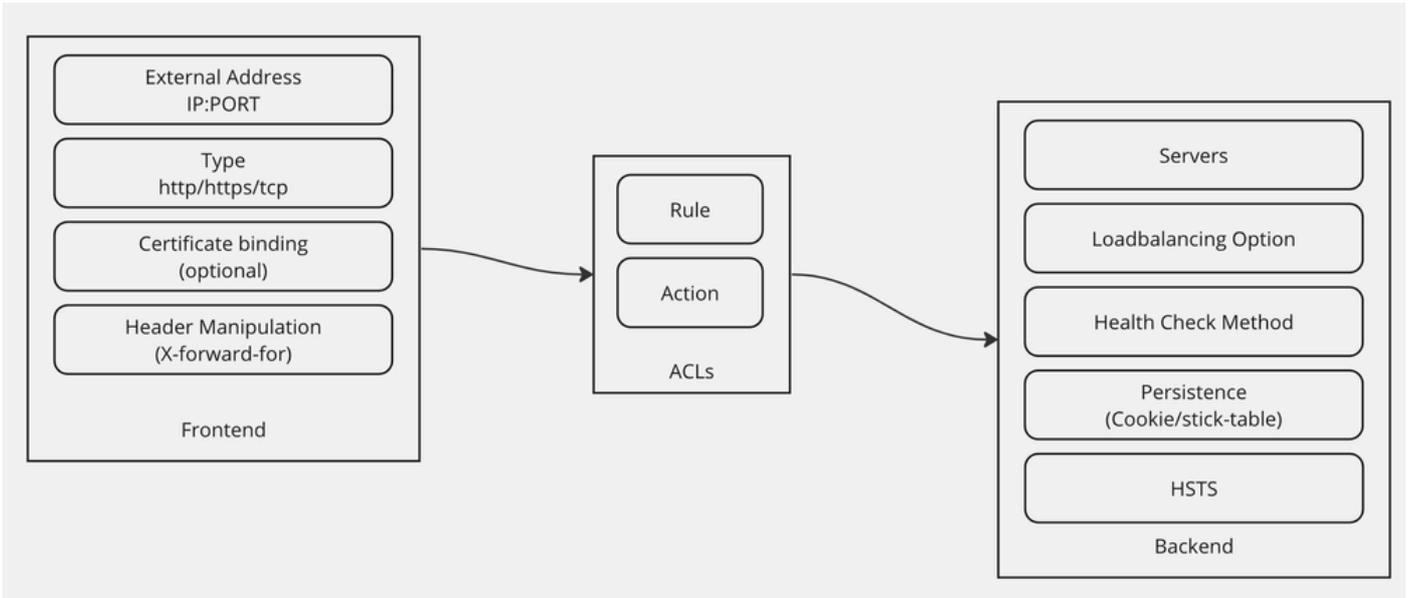
pfSense GUI - 방화벽 규칙 목록

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 프론트 엔드/백엔드 모델로 구현됩니다.

Frontend는 고객이 통신하는 프록시의 측면을 정의합니다.

프론트 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.

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

ACL은 지정된 프론트 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 COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ **Services ▾** VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Status / Dashboard

System Information	
Name	ucproxy02.uclabservices.com
User	admin@14.10.162.125 (Local Database)
System	VMware Virtual Machine Netgate Device ID: b2d05c55bab7b75fe6c2
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Thu Nov 12 2020
Version	2.7.2-RELEASE (amd64) built on Wed Dec 6 15:10:00 EST 2023 FreeBSD 14.0-CURRENT The system is on the latest version. Version information updated at Tue Feb 20 14:00:00 EST 2024
CPU Type	Intel(R) Xeon(R) Platinum 8180 CPU @ 2.50GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No

- Auto Config Backup
- Captive Portal
- DHCP Relay
- DHCP Server
- DHCPv6 Relay
- DHCPv6 Server
- DNS Forwarder
- DNS Resolver
- Dynamic DNS
- HAProxy**
- IGMP Proxy
- NTP
- PPPoE Server
- Router Advertisement
- SNMP
- Wake-on-LAN

Netgate Services And Support

Contract type **Community Support**
Community Support Only

NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES

If you purchased your pfSense gateway firewall appliance from Netgate and elected **Community Support** at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the [NETGATE RESOURCE LIBRARY](#).

You also may upgrade to a Netgate Global Technical Assistance Center (TAC) Support subscription. We're always on! Our team is staffed 24x7x365 and committed to delivering enterprise-class, worldwide support at a price point that is more than competitive when compared to others in our space.

- Upgrade Your Support
- Community Support Resources
- Netgate Global Support FAQ
- Official pfSense Training by Netgate
- Netgate Professional Services
- Visit Netgate.com

pfSense GUI - HAProxy 드롭다운

2단계. 기본 설정 구성

General settings

Enable HAProxy

Installed version 2.8.3-86e043a

Maximum connections

per process.

Sets the maximum per-process number of concurrent connections to X. **NOTE:** setting this value too high will result in HAProxy not being able to allocate enough memory.

Current 'System Tunables' settings.

'kern.maxfiles': 30767

'kern.maxfilesperproc': 27684

Full memory usage will only show after all connections have actually been used.

When setting a high amount of allowed simultaneous connections you will need to add and or increase the following two 'System Tunables' kern.maxfiles and kern.maxfilesperproc. For HAProxy alone set these to at least the number of allowed connections * 2 + 31. So for 100.000 connections these need to be 200.031 or more to avoid trouble, take into account that handles are also used by other processes when setting kern.maxfiles.

Connections	Memory usage
1	50 kB
1.000	48 MB
10.000	488 MB
100.000	4,8 GB

Calculated for plain HTTP connections, using ssl offloading will increase this.

Number of threads to start per process

Defaults to 1 if left blank (1 CPU core(s) detected).

FOR NOW, THREADS SUPPORT IN HAProxy 1.8 IS HIGHLY EXPERIMENTAL AND IT MUST BE ENABLED WITH CAUTION AND AT YOUR OWN RISK.

Reload behaviour

Force immediate stop of old process on reload. (closes existing connections)

Note: when this option is selected, connections will be closed when haproxy is restarted. Otherwise the existing connections will be served by the old haproxy process until they are closed. Checking this option will interrupt existing connections on a restart (which happens when the configuration is applied, but possibly also when pfSense detects an interface coming up or a change in its ip-address.)

Reload stop behaviour

Defines the maximum time allowed to perform a clean soft-stop. Defaults to 15 minutes, but could also be defined in different units like 30s, 15m, 3h or 1d.

Carp monitor

Monitor carp interface and only run haproxy on the firewall which is MASTER.

Stats tab, 'internal' stats port

Internal stats port

EXAMPLE: 2200

Sets the internal port to be used for the stats tab. This is bound to 127.0.0.1 so will not be directly exposed on any LAN/WAN/other interface. It is used to internally pass through the stats page. Leave this setting empty to remove the "HAProxyLocalStats" item from the stats page and save a little on resources.

Internal stats refresh rate

Seconds, Leave this setting empty to not refresh the page automatically. EXAMPLE: 10

Sticktable page refresh rate

Seconds, Leave this setting empty to not refresh the page automatically. EXAMPLE: 10

pfSense GUI - HAProxy 기본 설정

Enable HAProxy(HAProxy 활성화) 확인란을 선택합니다.

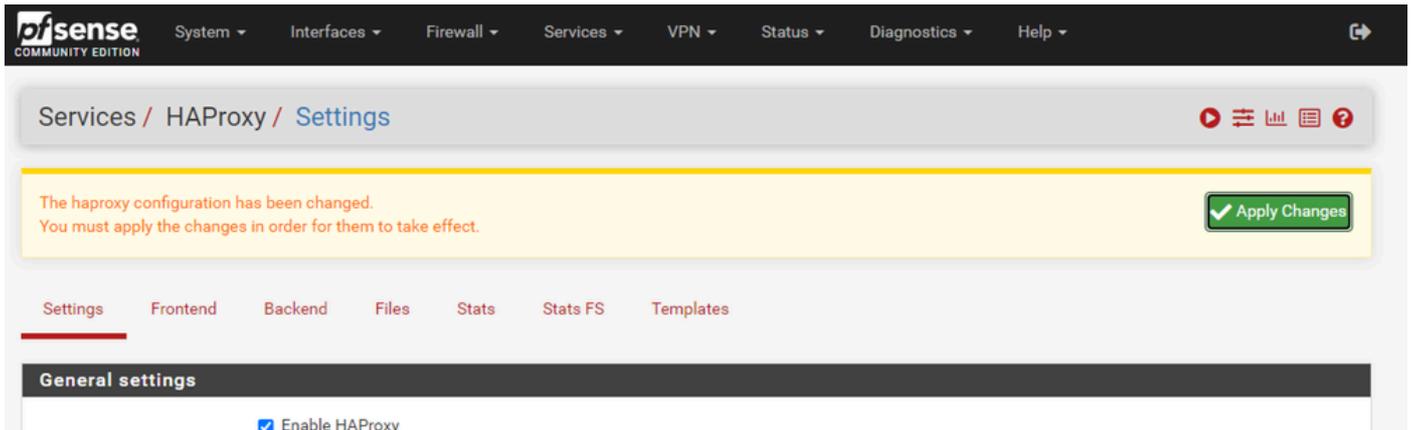
Maximum Connections(최대 연결) 값을 입력합니다. 필요한 메모리에 대한 자세한 내용은 이 섹션의 차트를 참조하십시오.

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

내부 통계 새로 고침 빈도 값을 입력합니다.

나머지 컨피그레이션을 검토하고 환경에 필요한 대로 업데이트합니다.

저장을 선택합니다.

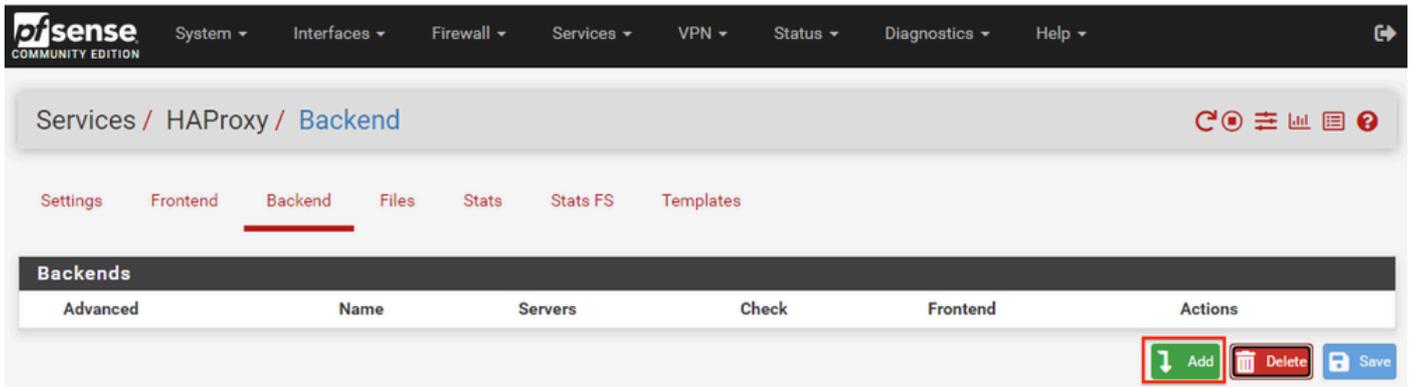


pfSense GUI - HAProxy 변경 사항 적용

 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.

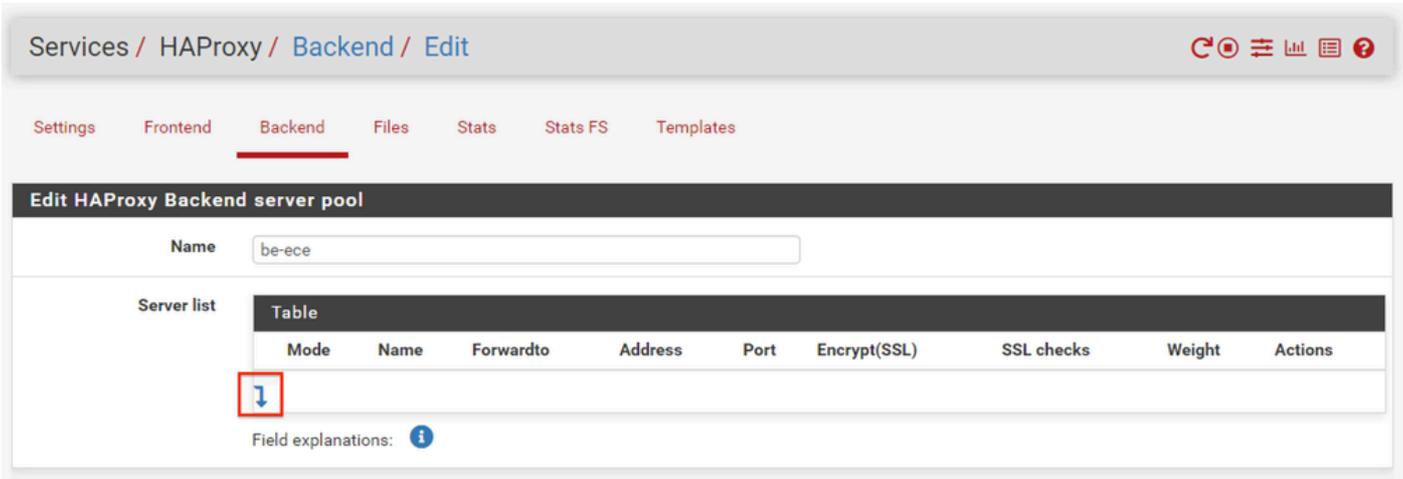
HAProxy 백엔드 구성

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



pfSense GUI - HAProxy 백엔드 추가

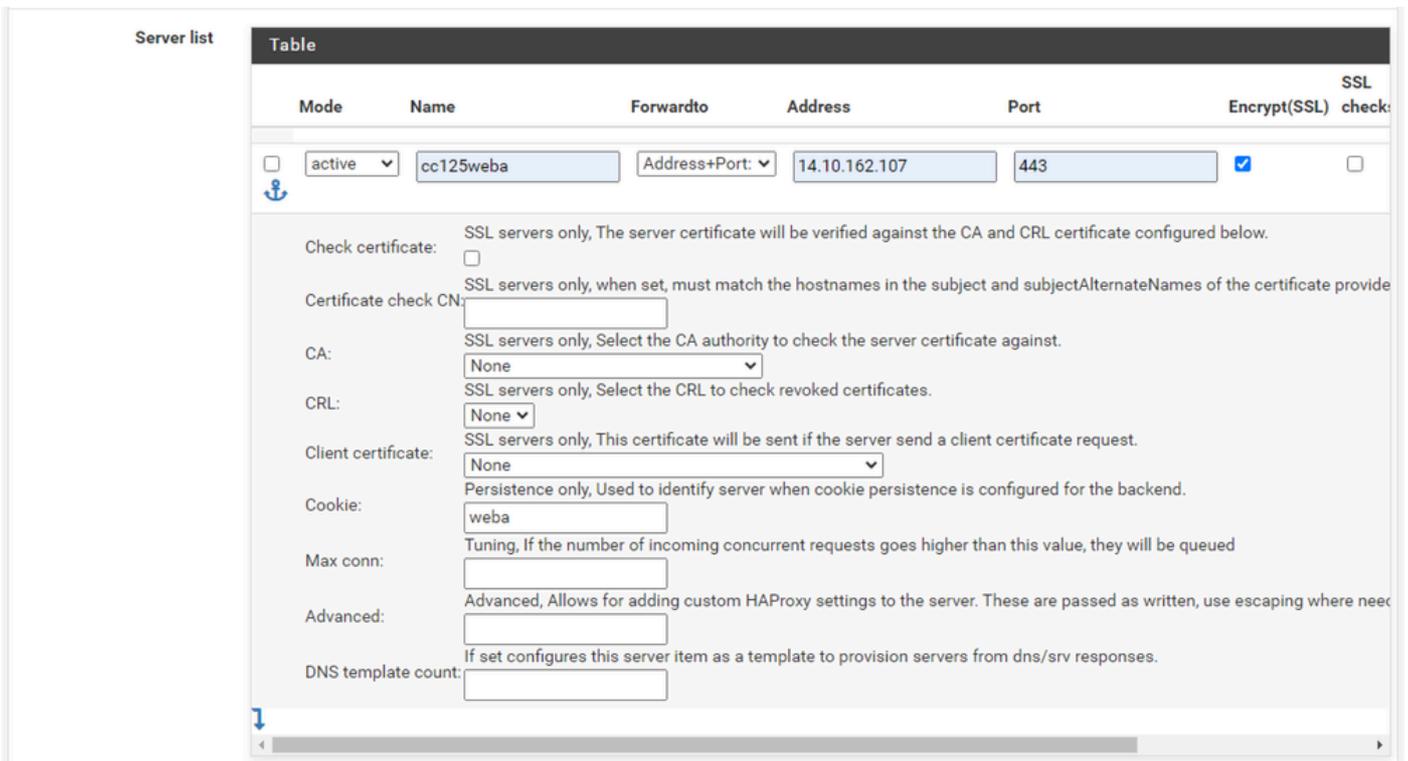
Add(추가) 버튼을 선택합니다.



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 합니다

다.

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

Loadbalancing options (when multiple servers are defined)

Balance

None
This allows writing your own custom balance settings into the advanced section. Or when you have no need for balancing with only 1 server.

Round robin
Each server is used in turns, according to their weights. This is the smoothest and fairest algorithm when the server's processing time remains equally distributed. This algorithm is dynamic, which means that server weights may be adjusted on the fly for slow starts for instance.

Static Round Robin
Each server is used in turns, according to their weights. This algorithm is as similar to roundrobin except that it is static, which means that changing a server's weight on the fly will have no effect. On the other hand, it has no design limitation on the number of servers, and when a server goes up, it is always immediately reintroduced into the farm, once the full map is recomputed. It also uses slightly less CPU to run (around -1%).

Least Connections
The server with the lowest number of connections receives the connection. Round-robin is performed within groups of servers of the same load to ensure that all servers will be used. Use of this algorithm is recommended where very long sessions are expected, such as LDAP, SQL, TSE, etc... but is not very well suited for protocols using short sessions such as HTTP. This algorithm is dynamic, which means that server weights may be adjusted on the fly for slow starts for instance.

Source
The source IP address is hashed and divided by the total weight of the running servers to designate which server will receive the request. This ensures that the same client IP address will always reach the same server as long as no server goes down or up. If the hash result changes due to the number of running servers changing, many clients will be directed to a different server. This algorithm is generally used in TCP mode where no cookie may be inserted. It may also be used on the Internet to provide a best-effort stickyness to clients which refuse session cookies. This algorithm is static, which means that changing a server's weight on the fly will have no effect.

Uri (HTTP backends only)
This algorithm hashes either the left part of the URI (before the question mark) or the whole URI (if the "whole" parameter is present) and divides the hash value by the total weight of the running servers. The result designates which server will receive the request. This ensures that the same URI will always be directed to the same server as long as no server goes up or down. This is used with proxy caches and anti-virus proxies in order to maximize the cache hit rate. Note that this algorithm may only be used in an HTTP backend.

Len (optional)
The "len" parameter indicates that the algorithm should only consider that many characters at the beginning of the URI to compute the hash.

Depth (optional)
The "depth" parameter indicates the maximum directory depth to be used to compute the hash. One level is counted for each slash in the request.

Allow using whole URI including url parameters behind a question mark.

HAProxy 백엔드 - 로드 밸런싱

Loadbalancing 옵션을 구성합니다.

ECE 서버의 경우 이 값을 Least Connections로 설정해야 합니다.

Access control lists and actions	
Timeout / retry settings	
Connection timeout	60000 The time (in milliseconds) we give up if the connection does not complete within (default 30000).
Server timeout	60000 The time (in milliseconds) we accept to wait for data from the server, or for the server to accept data (default 30000).
Retries	2 After a connection failure to a server, it is possible to retry, potentially on another server. This is useful if health-checks are too rare and you don't want the clients to see the failures. The number of attempts to reconnect is set by the "retries" parameter.
Health checking	
Health check method	HTTP <small>HTTP protocol to check on the servers health, can also be used for HTTPS servers(requires checking the SSL box for the servers).</small>
Check frequency	<input type="text"/> milliseconds For HTTP/HTTPS defaults to 1000 if left blank. For TCP no check will be performed if left empty.
Log checks	<input checked="" type="checkbox"/> When this option is enabled, any change of the health check status or to the server's health will be logged. By default, failed health check are logged if server is UP and successful health checks are logged if server is DOWN, so the amount of additional information is limited.
Http check method	GET <small>OPTIONS is the method usually best to perform server checks, HEAD and GET can also be used. If the server gets marked as down in the stats page then changing this to GET usually has the biggest chance of working, but might cause more processing overhead on the webserver and is less easy to filter out of its logs.</small>
Url used by http check requests.	<input type="text" value="/system/web/view/platform/common/login/root.jsp?partitionId=1"/> Defaults to / if left blank.
Http check version	<input type="text" value="HTTP/1.1\r\nHost:\ ece125.uclabservices.com"/> Defaults to "HTTP/1.0" if left blank. Note that the Host field is mandatory in HTTP/1.1, and as a trick, it is possible to pass it after "\r\n" following the version string like this: <code>HTTP/1.1\r\nHost:\ www</code> Also some hosts might require an accept parameter like this: <code>HTTP/1.0\r\nHost:\ webservername:8080\r\nAccept:\ */*</code>

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=1`을 입력합니다.
6. HTTP 검사 버전: Enter, `HTTP/1.1\r\nHost:\ {fqdn_of_server}`

최종 백슬래시 뒤가 아닌 서버의 FQDN 앞에 공백을 포함해야 합니다.

Agent checks

Agent checks Use agent checks
Use a TCP connection to read an ASCII string of the form 100%,75%,drain,down (more about this in the [haproxy manual](#))

Cookie persistence

Cookie Enabled Enables cookie based persistence. (only used on "http" frontends)

Server Cookies **Make sure to configure a different cookie on every server in this backend.**

Cookie Name
The string name to track in Set-Cookie and Cookie HTTP headers.
EXAMPLE: MyLoadBalanceCookie JSESSIONID PHPSESSID ASPNET_SessionId

Cookie Mode
Determines how HAProxy inserts/prefixes/replaces or examines cookie and set-cookie headers.
EXAMPLE: with an existing PHPSESSIONID you can for example use "Session-prefix" or to create a new cookie use "Insert-silent".

```
cookie is analyzed on incoming request to choose server and
set-cookie value is overwritten if present and set to an
unknown value or inserted in response if not present.

cookie <cookie name> insert
```

Cookie Cachable Allows shared caches to cache the server response.

Cookie Options Only insert cookie on post requests. Prevent usage of cookie with non-HTTP components. Prevent usage of cookie over non-secure channels.

Cookie Options
Max idle time It only works with insert-mode cookies. Max life time It only works with insert-mode cookies.

Cookie domains
Domains to set the cookie for, separate multiple domains with a space.

Cookie dynamic key
Set the dynamic cookie secret key for a backend. This is will be used to generate a dynamic cookie with.

Stick-table persistence

These options are used to make sure separate requests from a single client go to the same backend. This can be required for servers that keep track of for example a shopping cart.

Stick tables
Sticktables that are kept in memory, and when matched make sure the same server will be used.

```
No stick-table will be used
```

Email notifications

Mail level
Define the maximum loglevel to send emails for.

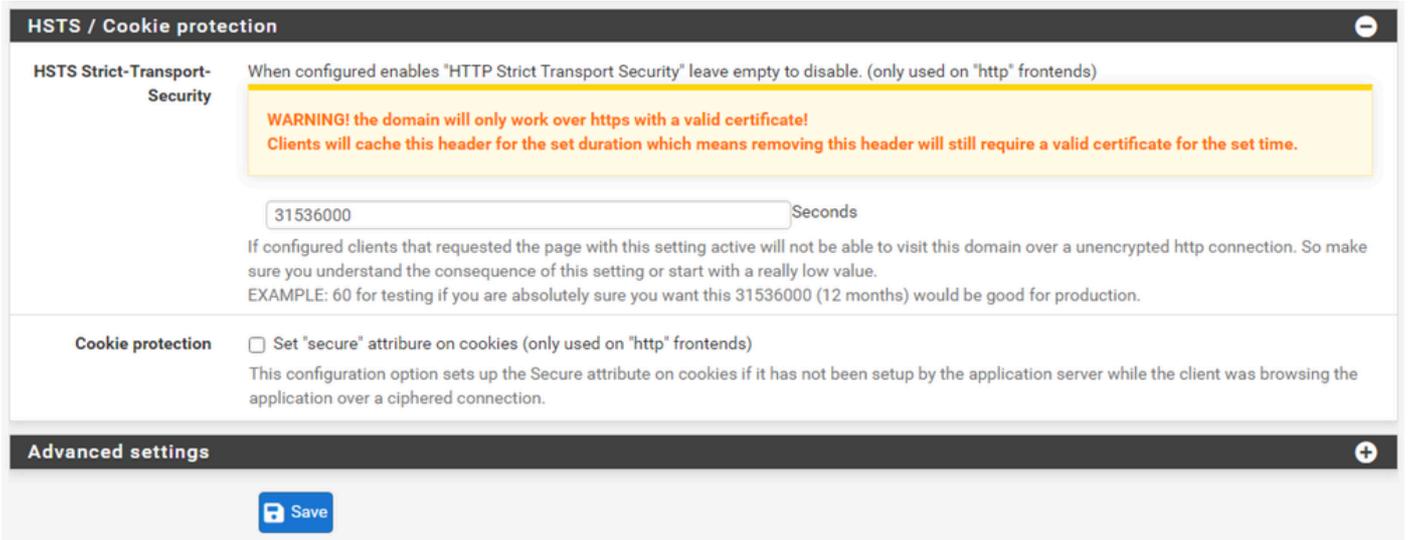
Mail to
Email address to send emails to, defaults to the value set on the global settings tab if left empty.

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

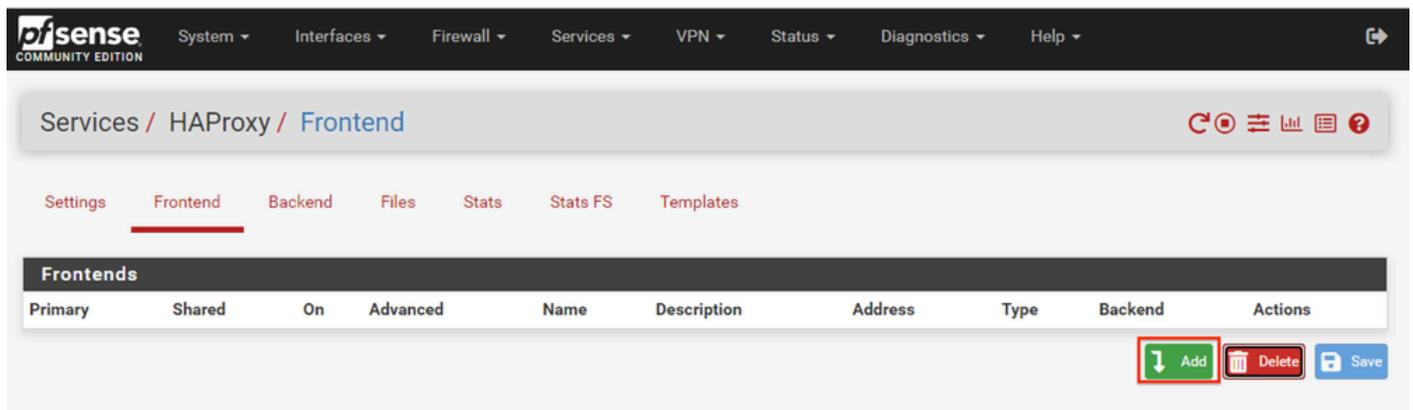
백엔드 컨피그레이션 양식의 나머지 섹션은 기본 설정에 남아 있을 수 있습니다.

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

Save(저장)를 선택합니다.

HAProxy 프론트 엔드 구성

프론트 엔드 메뉴로 변경합니다.



pfSense GUI - HAProxy 프론트 엔드 추가

추가 단추를 선택합니다.

Settings **Frontend** Backend Files Stats Stats FS Templates

Edit HAProxy Frontend

Name

Description

Status

External address Define what ip:port combinations to listen on for incoming connections.

Table						
	Listen address	Custom address	Port	SSL Offloading	Advanced	Actions
<input type="checkbox"/>	14.10.162.252 (ece-VIP)	<input type="text"/>	443	<input checked="" type="checkbox"/>	<input type="text"/>	

NOTE: You must add a firewall rules permitting access to the listen ports above.
 If you want this rule to apply to another IP address than the IP address of the interface chosen above, select it here (you need to define [Virtual IP](#) addresses on the first). Also note that if you are trying to redirect connections on the LAN select the "any" option. In the port to listen to, if you want to specify multiple ports, separate them with a comma (.). EXAMPLE: 80,8000 Or to listen on both 80 and 443 create 2 rows in the table where for the 443 you would likely want to check the SSL-offloading checkbox.

Max connections

Sets the maximum amount of connections this frontend will accept, may be left empty.

Type

This defines the processing type of HAProxy, and will determine the available options for acl checks and also several other options. Please note that for https encryption/decryption on HAProxy with a certificate the processing type needs to be set to "http".

HAProxy - 프론트 엔드 헤더

프론트 엔드의 이름을 입력합니다.

나중에 프론트 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.

Default backend, access control lists and actions

Access Control lists

Use these to define criteria that will be used with actions defined below to perform them only when certain conditions are met.

Table					
Name	Expression	CS	Not	Value	Actions

- 'CS' makes the string matches 'Case Sensitive' so www.domain.tld will not be the same as WWW.domain.TLD
- 'Not' makes the match if the value given is not matched

Example:

Name	Expression	CS	Not	Value	Actions
Backend1acl	Host matches			www.yourdomain.tld	
addHeaderAc	SSL Client certificate valid				

acl's with the same name will be 'combined' using OR criteria.

For more information about ACLs please see [HAProxy Documentation Section 7 - Using ACLs](#)

NOTE Important change in behaviour, since package version 0.32

-acl's are no longer combined with logical AND operators, list multiple acl's below where needed.

-acl's alone no longer implicitly generate use_backend configuration. Add 'actions' below to accomplish this behaviour.

Actions

Use these to select the backend to use or perform other actions like calling a lua script, blocking certain requests or others available.

Table			
Action	Parameters	Condition acl names	Actions

Example:

Action	Parameters	Condition
Use Backend	Website1Backend	Backend1acl
http-request header set	Headername: X-HEADER-ClientCertValid New logformat value: YES	addHeaderAc

Default Backend

If a backend is selected with actions above or in other shared frontends, no default is needed and this can be left to "None".

HAProxy 백엔드 - 기본 백엔드 선택

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

Default backend, access control lists and actions

Access Control lists Use these to define criteria that will be used with actions defined below to perform them only when certain conditions are met.

Table							
	Name	Expression	CS	Not	Value	Actions	
<input type="checkbox"/>		ccmpWS	Host starts with:	no	no	ccmp.uclabservices.com:8085	
<input type="checkbox"/>		ccmpSSL	Host starts with:	no	no	ccmp.uclabservices.com	

- 'CS' makes the string matches 'Case Sensitive' so www.domain.tld wil not be the same as WWW.domain.TLD
 - 'Not' makes the match if the value given is not matched
 Example:

Name	Expression	C	Not	Value
Backend1acl	Host matches			www.yourdomain.tld
addHeaderAc	SSL Client certificate valid			

 acl's with the same name will be 'combined' using OR criteria.
 For more information about ACLs please see [HAProxy Documentation Section 7 - Using ACL's](#)

NOTE Important change in behaviour, since package version 0.32
 -acl's are no longer combined with logical AND operators, list multiple acl's below where needed.
 -acl's alone no longer implicitly generate use_backend configuration. Add 'actions' below to accomplish this behaviour.

Actions Use these to select the backend to use or perform other actions like calling a lua script, blocking certain requests or others available.

Table					
	Action	Parameters	Condition acl names	Actions	
<input type="checkbox"/>		Use Backend	See below	ccmpSSL	
		backend: be-uclab-ccmp120-ssl			
<input type="checkbox"/>		Use Backend	See below	ccmpWS	
		backend: be-uclab-ccmp120-ws			

Example:

Action	Parameters	Condition
Use Backend	Website1Backend	Backend1acl
http-request header set	Headername: X-HEADER-ClientCertValid New logformat value: YES	addHeaderAc

Default Backend

If a backend is selected with actions above or in other shared frontends, no default is needed and this can be left to "None".

HAProxy 백엔드 - ACL 고급

이미지에 표시된 것처럼 ACL을 사용하여 단일 프론트 엔드를 조건에 따라 여러 백 엔드로 리디렉션 할 수 있습니다.

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

이는 ECE에서 흔히 볼 수 있는 일이 아닙니다.

SSL Offloading

Note SSL Offloading will reduce web servers load by maintaining and encrypting connection with users on internet while sending and retrieving data without encryption to internal servers. Also more ACL rules and http logging may be configured when this option is used. Certificates can be imported into the pfSense "Certificate Authority Manager" Please be aware this possibly will not work with all web applications. Some applications will require setting the SSL checkbox on the backend server configurations so the connection to the webserver will also be a encrypted connection, in that case there will be a slight overall performance loss."

SNI Filter
Specify a SNI filter to apply below SSL settings to specific domain(s), see the "crt-list" option from haproxy for details.
EXAMPLE: *.securedomain.tld !public.securedomain.tld

Certificate
Choose the cert to use on this frontend.
 Add ACL for certificate CommonName. (host header matches the "CN" of the certificate)
 Add ACL for certificate Subject Alternative Names.

OCSP Load certificate ocsp responses for easy certificate validation by the client.
A cron job wil update the ocsp response every hour.

Additional certificates Which of these certificate will be send will be determined by haproxy's SNI recognition. If the browser does not send SNI this will not work properly. (IE on XP is one example, possibly also older browsers or mobile devices).

Table	
Certificates	Actions

Add ACL for certificate CommonName. (host header matches the "CN" of the certificate)
 Add ACL for certificate Subject Alternative Names.

Advanced ssl options
NOTE: Paste additional ssl options(without commas) to include on ssl listening options.
some options: force-ssl3, force-tls10 force-tls11 force-tls12 no-ssl3 no-tls10 no-tls11 no-tls12 no-tls-tickets
Example: no-ssl3 ciphers ECDH+aRSA+AES:TLSv1+kRSA+AES:TLSv1+kRSA+3DES

Advanced certificate specific ssl options
NOTE: Paste additional ssl options(without commas) to include on ssl listening options.
some options: alpn, no-ca-names, ecde, curves, ciphers, ssl-min-ver and ssl-max-ver
Example: alpn h2,http/1.1 ciphers ECDH+aRSA+AES:TLSv1+kRSA+AES:TLSv1+kRSA+3DES ecde secp256k1

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.

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Services / HAProxy / Frontend

The haproxy configuration has been changed.
You must apply the changes in order for them to take effect. Apply Changes

Settings **Frontend** Backend Files Stats Stats FS Templates

Frontends

Primary	Shared	On	Advanced	Name	Description	Address	Type	Backend	Actions
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	fe-ece	Frontend for ECE	14.10.162.252:443	https	be-ece (default)	

Add Delete Save

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.