

# ECE J PfSense عم تجم لمح نزاوم نيوكت

## تايوت حمل

[عم دق م](#)

[عم ساس الابل ط م](#)

[تابل ط م](#)

[عم دخت س م تانوك م](#)

[PfSense تي ب ث](#)

[لحل اى لع عماع قرظن](#)

[ري ض ح ت](#)

[بي ك ر ت ل ا](#)

[Network Setup \(دع ا\)](#)

[ي ل و ال ا دادع ال ا ل ا م ك](#)

[عم ساس ال ا ق ر ا د ا ل ا ت ا د ا د ا ل ا ن ي و ك ت](#)

[ق ب و ل ط م ل ا م ز ح ل ا ق ف ا ض ا](#)

[ت ا د ا ه ش ل ا ن ي و ك ت](#)

[ق ي ر و ا ط ل ا I P ن ي و ا ن ع ق ف ا ض ا](#)

[ق ي ا م ح ل ا ر ا د ج ن ي و ك ت](#)

[SHARoxy ن ي و ك ت](#)

[ي س ك و ر ب ا و ل ا م ي و ا ف م](#)

[ت ق م ل ا ن ي و ك ت ل ا ق ر ك ا ذ ل ق ي ل و ال ا ت ا د ا د ا ل ا](#)

[SHARoxy ق ي ف ل خ ل ا ن ي و ك ت](#)

[SHARoxy ق م ج ا و ن ي و ك ت](#)

## عم دق م

ةش دردل لمح نزاومك هنيوكتو Pfsense عم تجم رادصا دادع ا تاوطخ دن تسم ل ا اذه فص ي (ECE) تاسس وم ل ل ي نورتك ل ال ا ديرب ل او

## عم ساس الابل ط م

### تابل ط م

ةي ل ل ا ل ا ع ي ض ا و م ل ا ب ة ف ر ع م ك ي د ل ن و ك ت ن ا ب Cisco ي ص و ت:

- ECE 12.x
- pfSense عم تجم رادصا

### عم دخت س م تانوك م

ةي ل ل ا ل ا ج م ا ر ب ل ا ت ا ر ا د ص ا ي ل ا دن ت س م ل ا اذه ي ف ة د ر ا و ل ا ت ا م و ل ع م ل ا دن ت س ت

- (1) 6-12 رادصلإلا ،ابوروال ةي داصتقالا ةنجللا
- PfSense Community ، رادصلإلا 2.7.2

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجالا نم دنتسمل اذه يف ةدراول تامولعمل عاشنإ مت تناك اذإ .(يضارتفا) حوسمم نيوكتب دنتسمل اذه يف ةمدختسمل ةزهجالا عيمج تادب رما يال لمحتل ريثاتلل كمهف نم دكأتف ،ليغشتلا ديق كتكبش

## PfSense تيبتت

### لحلل عل ةماع ةرظن

ةحسامو ليحت نزاومو ةيامح رادج رفوي فئاظولا ددعتم اجتتم PFsense عم تجم رادصا دعى فرعم لعل PfSense جم انرب انب مت .دحاو مداخ يف ىرخالا تامدخال نم ديدعلالو ناما ةئبوض ليحتل نزاوم .ةزهجالا تابللطم نم ىندال دخال لعل يوتحي امك ،يناجملا (BSD) دروملا ةئب نيوكتل مادختسال ةلهس (GUI) ةيموسر مدختسم ةهجاو ريفوت متي و SHARoxy ل ذيفنت وه جتتملا

يطعي .(CCMP) لاصلالا زكرم و ECE ةرادا لخدم نم لك عم اذه ليحتل نزاوم مادختسا كنكمي ECE ل pfSense لكشي نأ تاوطلال ةقيثو اذه

### ريضحت

pfSense جم انرب لي زنت 1. ةوطلال

ISO تبتم ةروص لي زنتل [بيولا لعل PfSense](#) عقوم مدختسا

VM نيوكت 2. ةوطلال

تابلطتملا لقاب (VM) يضارتفا زاهج نيوكت

· (للكب x86-64 ةعرب) تب 64 ةئب AMD64 زارط عم ةقفاوتم (CPU) ةيزكرم ةجالعم ةدحو

· رثكأ وأ تياباجي 1 ةعس (RAM) يئاوشع لوصو ةركاذ

· ةبلص تانوكم نم ةعونصم ةركاذب دوزم صارقأ كرحم) ربكأ وأ تياباجي 8 ةعس صارقأ كرحم (كلذ لئلا امو ،(HDD) ةتبات صارقأ كرحمو (SSD)

· ةقفاوتم رثكأ وأ ةدحاو ةكبش ةهجاو ةقاطب

· (BD وأ DVD) ةعسال لعل ةئبوض صارقأ كرحم وأ ليحتلل لباق USB صارقأ كرحم يلوألا تيبتتلل

نكل ،زاهجالا ليغشتل قرط ةدع كانه .طقف (NIC) ةدحاو ةكبش ةهجاو مزلي ،ربتخم تيبتتل عضو اضيأ اهليلق لطي يتلاو ،ةدحاو (NIC) ةكبش ةهجاو ةقاطب مادختسا يه ققيرط لهسا هذه نأ نم مغرلا لعلو .ةكبشلاب لصتت ةدحاو ةهجاو كانه ،دحاوال عارذلا عضو يف .دحاوال عارذلا انام رثكألا ققيرطلا تسيل انال ،ربتخم لل ةبسانمو ةلهس ققيرط

للال لعل (NICs) ةكبش ةهجاو اتقاطب كي دل نوكي نأ يه زاهجالا نيوكتل انام رثكأ ققيرط

اهنأ امك (WAN) قاطنلا ةعساو لاصتالا ةكبش ةهجاو (NIC) ةكبشلا ةهجاو تاقاطب نيب نمو ةهجاو يه ةيناثلا (NIC) ةكبشلا ةهجاو ةقاطب. ةماعلا تنرتنالا ةكبش ةرشابم لصتت ةيفاضا تاهجاو ةفاضلا اضيا كنكمي. ةيلخادلا ةكرشلا ةكبش لصتتو، LAN ةكبش يلع. ةيامحلا رادجو نامألل ةفلتخم دعاوق يلع ويوتحت ةكبشلا نم ةفلتخم ءازجاب لاصتالل ماعلا تنرتنالا دحاو (NIC) ةكبش ةهجاو ةقاطب لاصتا كي دل نوكي نأ كنكمي، لاثملا ليبس، ايجراخ اهلا لوصولا كنكمي يتلا بيولا مداوخ عيمج نوكت ثيح DMZ ةكبش دحاو لاصتاو ي دل نوكي نأ كل حيتي اذهو. ةكرشلا ةكبش (NIC) ةكبش ةهجاو ةقاطب ثلاث لاصتاو متي يتلا بيولا مداوخ ةومجم سفن يلى نمأ لوصولا نييجراخلاو نييلخادلا نييمدختسملا قيبطتلا لبق ميمصت يأل ةينمألا تاريثأتلا مهف نم دكأت. DMZ يف اهب ظافتحالا صاخ لكشب كذيفنتل تاسرامملا لضفأ عابتا نم دكأتلل ي نمأ سندنهم رشتسا

## بيكرتلا

يرهاظلا زاهجلا يلع ISO بيكرت 1. ةوطخلا

تبيثتلا تابلاطم عبتاو (VM) يرهاظلا زاهجلا ليغشتب مق 2. ةوطخلا

ةوطخب ةوطخ تاداشرا يلع لوصولل [دنتسمل](#) اذه يلى عجرا

## Network Setup (ةكبشلا دادع)

نيوكتلا ةعباتمل زاهجلا IP نيوانع نييعت بجي

ةدحاو لعارذلا عضو يف هنيوكت مت ازاهج دنتسمل اذه رهظي: ةظحالم

VLAN تاكبش نيوكت 1. ةوطخلا

n بجأ، كلذ فالخ. لوألا لؤسلا يلع y ب بجأ، VLAN ةكبش معد يلى ةجاحب تنك اذا

WAN ةهجاو نييعت 2. ةوطخلا

يف ةديحولا ةهجاو لنيعارذلا عضو يف زاهجلا نم نمآلا ريغب بناجلا يه WAN ةكبش ةهجاو اهبلط دنع ةهجاو ل مسا لخدا. دحاو لعارذلا عضو

LAN ةكبش ةهجاو نييعت 3. ةوطخلا

ابولطم ناك اذا. نيعارذلا عضو يف زاهجلا نم نمآلا بناجلا يه (LAN) ةيلحملا ةكبشلا ةهجاو اهبلط دنع ةهجاو ل مسا لخدا.

يرخأ تاهجاو ياصيصختب مق 4. ةوطخلا

ةيرايخ لئاسولا هذو. كب صاخلا ددحملا تبيثتلا اهجاتحت يرخأ تاهجاو ي نيوكتب مق ةعئاش تسيلو.

ةرادلا ةهجاو ل IP ناوانع نييعت 5. ةوطخلا

ةدحو ةشاش يف ني عمل IP ناو نع ضرع م تي سف ، DHCP لوكوتورب معدت كتك بش تنك اذا  
مكحت لل.

```
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:
```

مكحت pfSense ةدحو

هذه ذي فنتب مقف ، ددحم ناو نع ني يعت يف بغرت تنك اذا وا ، ناو نع ني يعت م تي مل اذا  
تاوطخلل.

1. مكحت لل ةدحو ةمئاق نم 2 رايخلل رتخأ.
2. DHCP لي طعتل n ةباجا.
3. WAN ةهجاو ل IPv4 ناو نع لخدأ.
4. تب ال ددعب ةكبش ال عانق لخدأ. (24 = 255.255.255.0, 16 = 255.255.0.0, 8 = 255.0.0)
5. WAN ةهجاو ل ةباو ال ناو نع لخدأ.
6. ةباجا ال اب مقف ، زاهجلل ةيضا رتفال ال ةباو ال يه ةباو ال هذه نوكت نا يف بغرت تنك اذا  
N. يلع بجأف ال او ، ةباو ال ةبلاطمل Y يلع
7. ابولطم كلذناك اذا IPv6 ل (NIC) ةكبش ال ةهجاو ل ةقابط ني وكتب مق.
8. ةهجاو ل ال يلع DHCP مداخ لي طعتب مق.
9. يف ءارجال اذه مادختسا م تي . WebConfigurator لوكوتورب يلع HTTP ني كم تل y يلع درل .  
ةيلا لل تاوطخلل

اهثي دحت مت دق تا ددع ال نا ب اديكأت ي ق ل تت م ث

```
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.
```

مكحت pfSense دي

ي لوال دادع ال لامك ا



**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 - 2 | ج ا ب ح د ه و ز ح ط ق ك ل م ن

نآل اذہ رپیغت كن كمی، ٲیادب ل ی DHCP ترتخأ اذآ. IP ناونع تامولعم ءحص نم ققحت ءمءاقل ی ف ءحیحص لآ ءینمزلآ ءقطنم لآ ددحو NTP تقو مداخ فیضم مس ا ریفوتب مق ءلدسنم لآ ءل.

**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**

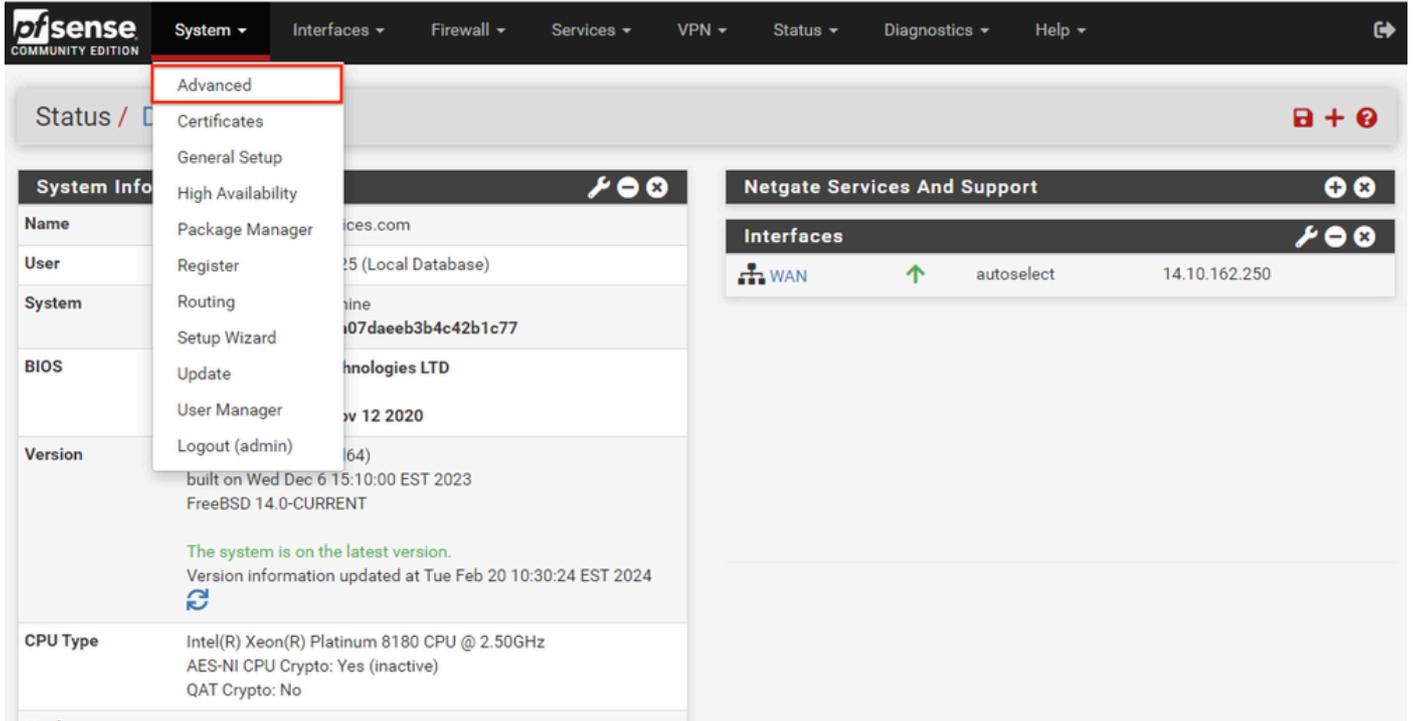
[Next](#)

(GUI) ةيموسررلا مدختسمل ةهجاو ليغشت ةداع متت. ةياهنلا ىتح دادعلا جلاعم لالخرمتسا هلامتكا درجم بديدل URL ناونع ىل لكهيجوت ةداع متيو ةهجاولل

## ةيساسال ةرادال تاداع نيوكت

لوؤسمل ةهجاو ىل لوخدلا ليحست 1. ةوطخلا

ماظنلا ةلدسنملا ةمئاقلا نم مدقتم دح 2. ةوطخلا



Admin ليژنت - PfSense ل (GUI) ةيموسررلا مدختسمل ةهجاو

ببول نوكم تاداع ثيحت 3. ةوطخلا

webConfigurator	
Protocol	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS (SSL/TLS)
SSL/TLS Certificate	<input type="text" value="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	<input type="text" value="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	<input type="text" value="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 <a href="#">DNS Rebinding attacks</a>. 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 <a href="#">Wikipedia</a>.</p>

لوؤس م ل ن ي و ك ت - PfSense GUI

1. HTTPS (SSL/TLS) ل و ك و ت و ر ب د د ح .
2. ت ق و ل ا ا ذ ه ي ف ا ي ت ا ذ ة ع ق و م ل ة د ا ه ش ل ا ل ا | SSL/TLS ة د ا ه ش ك ر ت ا .
3. ر س ي ا ع م ر ا د ص ا ع ن م ي و ن ر ا ق ل ل ن م و ي ل ل ص ف ا ن ا 443 ن م ر خ ا ع ا ن ي م ل ا ل ا ع ا ن ي م T C P ل ا ت ر ي غ ل ا خ ا د ت .
4. 80 ذ ف ن م ل ا ل ا ع ل و و س م ل ا ة ه ج ا و ل ي ط ع ت ل WebGUI ه ي ج و ت ة د ا ع ا ر ا ي خ د ح .
5. ض ر ع ت س م ل ا ل HTTP\_REFERER ض ر ف ر ا ي خ د ح .
6. Secure Shell ن ي ك م ت ر ا ي خ ل ا د ي د ح ت ل ا ل خ ن م Secure Shell ن ي ك م ت ب م ق .

✎ إلى كهيجوت ةداعإ كلذ دع ب متت .ةعباتملا لبق ظفح رزلا ديحت نم دكأت :ةظحالم  
ديدل https طابترا

رمألا مزلا اذا ليكولا مداخل نيوكت .4 ةوطخلا

دادعإلامكإل . "تاعونتم" بيوبتلا ةمالة في ليكولا تامولعم نيوكتب مق ،ابولطم ناك اذا  
ت.نرتنإلا لوصول قح زاهجال يدل نوكي نأ بجي ،نيوكتلاو

System / Advanced / Miscellaneous ?

Admin Access Firewall & NAT Networking **Miscellaneous** System Tunables Notifications

### Proxy Support

Proxy URL	<input type="text" value="myproxy.domain.com"/>	Hostname or IP address of proxy server this system will use for its outbound Internet access.	
Proxy Port	<input type="text" value="3128"/>	Port where proxy server is listening.	
Proxy Username	<input type="text"/>	Username for authentication to proxy server. Optional, leave blank to not use authentication.	
Proxy Password	<input type="text" value="Proxy Password"/>	<input type="text" value="Proxy Password"/>	Confirm

PFsense GUI - ليكولا نيوكت

✎ تاريغتلا ءارج دع ب ظفح رزلا ديحت نم دكأت :ةظحالم

ةبولطملا مزحلا ةفاضإ

مزحلا ري دم > ماظن ددح .1 ةوطخلا

ةرفوتملا مزحلا ديحت .2 ةوطخلا

✎ ،ةلهملا تهتنا اذا .قئاقد عضب ةرفوتملا مزحلا عي مج ليحت قرغتسي دق :ةظحالم  
زاهجال ديهمت ةداعإ ةيلمع موقت ،ةداع .ححص لكشب DNS مداوخ نيوكت نم ققحتف  
ت.نرتنإلا لاصتا حالصاب

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.	<a href="#">+ Install</a>
Package Dependencies:			
<a href="#">pecl-ssh2-1.3.1</a> <a href="#">socat-1.7.4.4</a> <a href="#">php82-8.2.11</a> <a href="#">php82-ftp-8.2.11</a>			
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	<a href="#">+ Install</a>
Package Dependencies:			
<a href="#">apcupsd-3.14.14_4</a>			
arping	1.2.2_4	Broadcasts a who-has ARP packet on the network and prints answers.	<a href="#">+ Install</a>
Package Dependencies:			
<a href="#">arping-2.21_1</a>			
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.	<a href="#">+ Install</a>

مزجلا ةمئاق - PfSense نم (GUI) ةيموسرلا مدختسملا ةهجاو

## اهتبيثتو ةبولطملا مزجلا نع ثحبلا 3. ةوطخلا

- يسكورباه
- ةيضارتفالا ةزهجالل ةحوتفم تاودأ.



لفيد-رولباهلا ةمزح ددحت ال: ةظحالم

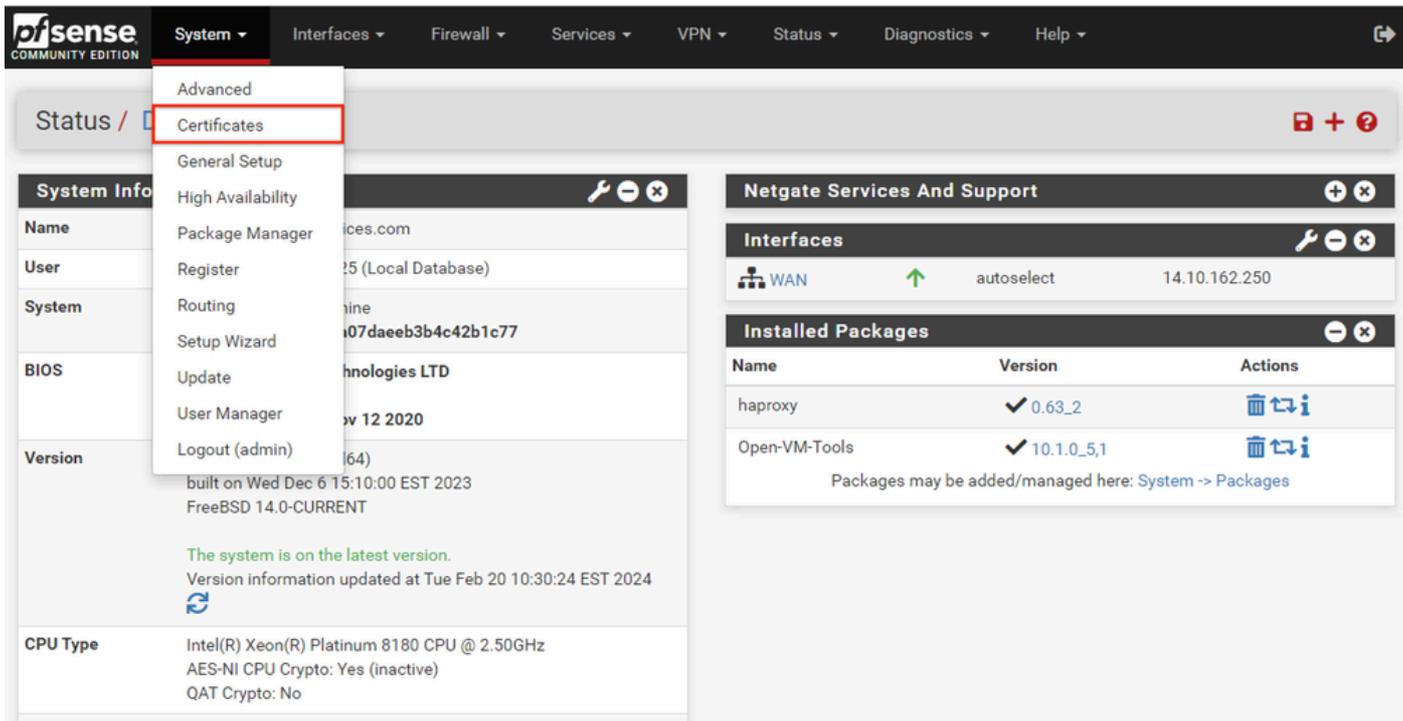
## تاداهشلا نيوكت

ماع قدصم عجرم عم لمكتت نأ نكمي وأ ايتاذ ةعقوم ةداهش عاشناب pfSense موقت نأ نكمي ليلدلا اذه حضوي CA نم ةعقوم تاداهش ردتو CA ك لمعت نأ نكمي وأ ،يلخاد قدصم عجرم .يلخاد قدصم عجرم عم لمكتل تاوطخ

كيدل رصانعلا هذه رفوت نم دكأت ،مسقلا اذه ادب لبق

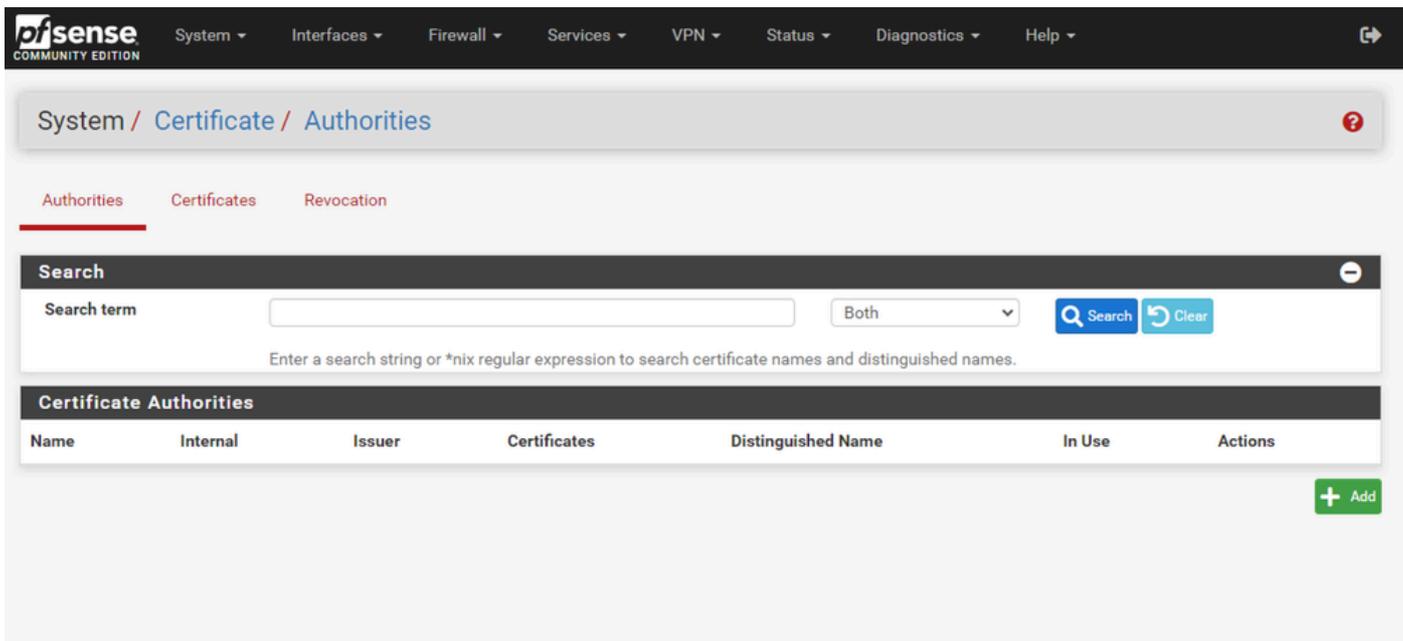
- زمرملا Base-64 قيسنت وأ PEM قيسنتب قدصملا عجرملا رزجلا ةداهشلا ظفح مت
- وأ PEM رفشم قيسنتب ةظوفحم CA ل (رادصا انايحا يمست) ةطيسولا تاداهشلا لك Base-64.

ماظنلا ةلدسنملا ةمئاقلا نم صيخارت ددح 1. ةوطخلا



تاداهش لى ةلدسنم ةمئاق - PfSense جمانرب مادختساب (GUI) ةيموسرلا مدختسمل ةهجاو

قصدصملا عجرملا رذج ةداهش داريتسا. 2. ةوطخلا



PFsense GUI - CA تاداهش ةمئاق

ةفاضلا رزلا ددح.

**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.

CA داري تساب - PfSense جمانرب مادختساب (GUI) ةيموسرلا مدختسالم ةهجاو

ةروصلال ي ف حضوم وه امك

1. ديرف ي ف صوم سا ريفوت
2. ل دس نالم بولسأل نم دوجوم تاداهش عجرم داري تساب ددح.
3. Trust Store و Randomize Serial رايتخالال ةناخ دي دحت نم دكأت.
4. ءدب— طوطخ نم ني م ضت نم دكأت. ةداهشال تانايب صن ع برم ي ف اهل مكأب ةداهشال قصل.
5. ةداهشال ةياهن — و— ةداهشال.
6. طفح ددح.
7. ةروصلال ي ف حضوم وه امك ةداهشال داري تساب نم دكأت.

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

System / Certificate / Authorities ?

**Authorities** Certificates Revocation

**Search** ⊖

Search term  Both Q 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 <span>i</span> Valid From: Sat, 26 Jan 2019 12:18:03 -0500 Valid Until: Wed, 26 Jan 2039 12:27:59 -0500		<span>✎</span> <span>⚙</span> <span>🗑</span>

+ Add

PfSense GUI - عمىاق - CA

CA ل عطيصولا عءاهشلا ءاريتسا. 3 عوطخل

**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.

طيسول CA داريتسا - PfSense جمانرب مادختساب (GUI) ةيموسرلا مدختسلا ةهجاو

قدصملا عجرملا ةداهش داريتسال رذجال قدصملا عجرملا ةداهش داريتسال تاوطلال ررك  
 طيسولا.

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="button" value="i"/>	<input type="button" value="edit"/> <input type="button" value="gear"/> <input type="button" value="trash"/>
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="button" value="i"/>	<input type="button" value="edit"/> <input type="button" value="gear"/> <input type="button" value="trash"/>

PFsense GUI - CA تاطابتر

وه امك رذجال ةداهشلاب حيحص لكشب لصتم طيسولا نأ نم دكأتلل ةقصدصملا عجارملا عجار ةروصلال يف حضورم.

لمحلل نزاوتم بيوعومل هريدصتو CSR ءاشنإ 4 ةوطخلل

كيدل ناك اذإ. ةعقوملا ةداهشلاب داريئسإ مث، CSR ريئصتو، CSR ءاشنإل تاوطخلل اذف صفي PfSense قئاثو عجار. ةداهشلاب هذف داريئسإ كئكمي، PFX قيسنئب ةدوجوم ةداهش لعفلاب تاوطخلل هذف ةصاخلا.

عيقوت/ةفاضل رز ددح مث، تاداهشلاب ةمئاق ددح 1.

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="button" value="i"/> webConfigurator	<input type="button" value="edit"/> <input type="button" value="gear"/> <input type="button" value="lock"/> <input type="button" value="refresh"/>

## 2. ةداهش لة عي قوت بلط جذومن لامك إ.

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

- لة دس نمل ةمئاق لة نمة داهش عي قوت بلط ءاشن إ دح: بولس أ
- ةداهش لة مس ا ريفوت: يفصولا مسالا
- كتابلطتم قباطت اهنأ نمة دك أ لة ةع ارم: صخلمل ةي مزر او خواتفملا عون
- لمالك لاب لهؤملا ل اجملا مس ا بي و ع قوم ريفوت: ءاشل مسالا
- كتئي بل بولطم وه امك ةي قوت بلط ءاشل تامولعم ريفوت

**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**

مدققت م CSR - GUI PfSense

- ةل دسننم ل ةمئاق ل ي ف مدخال ةداهش دح : ةداهش ل عون
- كذيفنن ةبولطم (SAN) عوضوم ل ةل يدب عامسأ ةيأ ريفوتب مق : ةل يدب ل عامسأ ل

✎ (SAN) نيزخت ل ةقطنم ةكبش ل قح ل ةل ايئاق ل ةئاش ل مسال ةفاضل متت : ةظحال م ةبولطم ةي ةفاضل عامسأ ةفاضل ل طوق جاتحت

ةجحص لوقح ل لك نوكت نأ درجمب ظفح دح.

3. فلم ل CSR ري دصت.

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

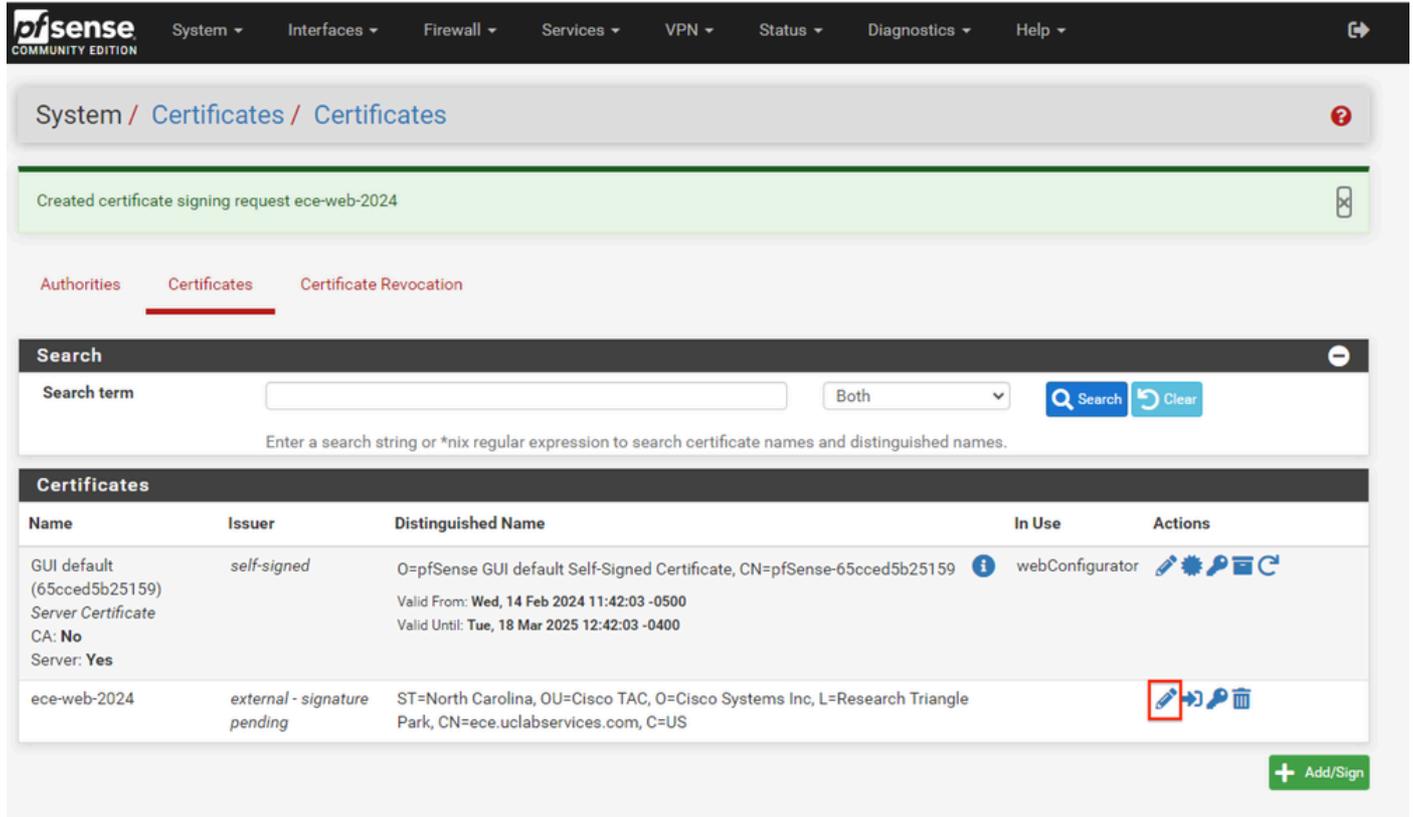
Enter a search string or \*nix regular expression to search certificate names and distinguished names.

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	<input type="button" value="edit"/> <input type="button" value="refresh"/> <input type="button" value="lock"/> <input type="button" value="refresh"/>
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		<input type="button" value="edit"/> <input type="button" value="add"/> <input type="button" value="lock"/> <input type="button" value="refresh"/>

CSR ري دصت - GUI PfSense

يلع لصحت نأ درجم ب. قدصم ل عجرم ل عم اذه عيقوتب مق م ث، CSR ظفحل "ريدصت" رزلا دح  
ة. لملعل ل لامك إل Base-64 أو PEM فلمك اذه ظفحا، ةعقوم ل ةداهش ل

4. ةعقوم ل ةداهش ل داري ت س ا.



The screenshot shows the pfSense web interface. At the top, there is a navigation bar with the pfSense logo and various menu items: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below the navigation bar, the breadcrumb path is System / Certificates / Certificates. A green notification bar at the top of the main content area states "Created certificate signing request ece-web-2024". Below this, there are tabs for Authorities, Certificates (which is selected), and Certificate Revocation. A search bar is present with a search term input field, a dropdown menu set to "Both", and buttons for Search and Clear. Below the search bar, there is a table of certificates with the following columns: Name, Issuer, Distinguished Name, In Use, and Actions. The table contains two entries: "GUI default (65cced5b25159) Server Certificate" and "ece-web-2024". The "ece-web-2024" entry has a red box around its Actions column, which contains icons for edit, refresh, and delete. At the bottom right of the table, there is a green "Add/Sign" button.

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		  

ةداهش ل داري ت س ا - PfSense ل (GUI) ةيموسر ل مدختسم ل ةه او

ةعقوم ل صيخرت ل داري ت س ا ل صاصر ل ملق ل ةنوقيأ دح.

5. جذومن ل ي ف ةداهش ل تانايب قصل ا.

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**  
 GBSApWQkcas305JkKISY/pYEI2EW/7EZcDmHRURnEFcWoRR2984LJgDgs1pmlcPL  
 V11oh2f4skcrjrvBiOu+VjhTJEos7rF+yIz3IT4TJwDLLEXAGJqB+jy8G5bfsZQf  
 QNYnxuZ5Mnuqx1PN97EPQngO/1IgxO4xDz6Dg+Iwt9pyrRZdxpmy  
 -----END CERTIFICATE-----  
 Paste the certificate received from the certificate authority here.

ةداهشلا داري تس | - PfSense ل (GUI) ةيموسرلا مدختس مل ةهجاو

ةداهشلا ظفحل شي دحت دح.

اهتحص نم دكأت لل ةداهشلا تانايب ةعجارم 6.

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 (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 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		

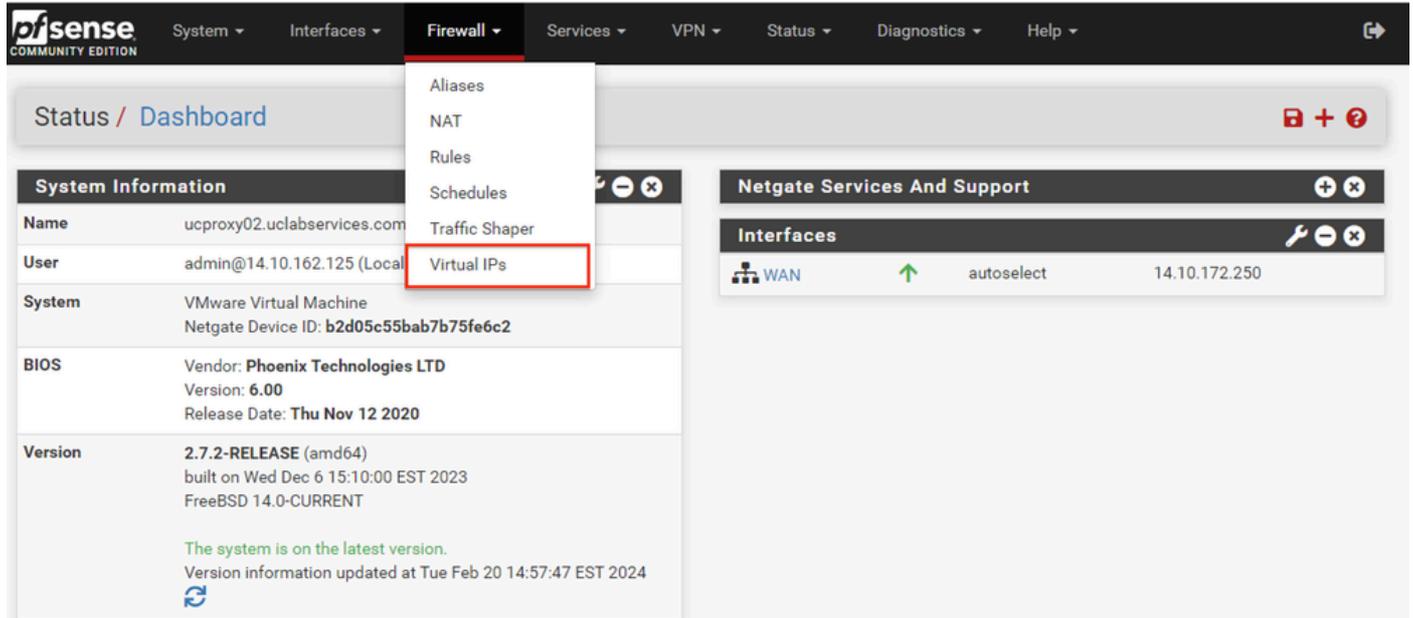
تاداهشلا ةمئاق - PfSense ل (GUI) ةيموسرلا مدختس مل ةهجاو

7. اذه PfSense ىل ع ددعت م ع قاوم ة فاضتس ا يف ب غرت تنك اذا ة يف لمع ال هذه ررك .

## ة يف ره اظال IP ني وان ع ة فاضا ا

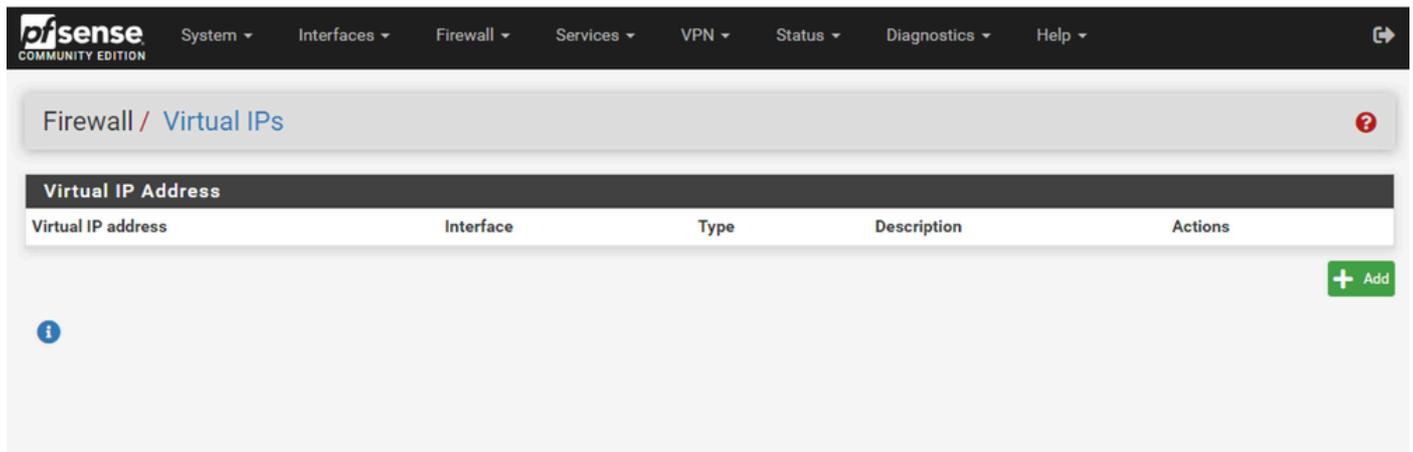
م ادختس ا يف و . PfSense ىل ع بيول ع قاوم ة فاضتس ال ل ق ال ا ىل ع دح او IP نا ون ع دوج و مزلي (VIPs). ة يف ره اظال IP ني وان ع م ادختس اب ك لذ ب م ا يف ق ال م تي . PfSense.

ة يف امحل ر ادجل ة لدس ن م ال ة م ئاق ال ن م ة يف ره اظال IP ني وان ع دي دحت . 1. ة و طخ ال



ة م هم ال تا يف صخ ش ال ل ة لدس ن م ال ة م ئاق ال - PfSense ج م ان رب م ادختس اب (GUI) ة يف م و س ر ال م دختس م ال ة ه او

## ة فاضا رزل ا ددح . 2. ة و طخ ال



ة م هم ال تا يف صخ ش ال ال ل و ص و ال ة ح ف ص - PfSense ج م ان رب م ادختس اب (GUI) ة يف م و س ر ال م دختس م ال ة ه او

## نا ون ع ال تامول ع م ري فوت . 3. ة و طخ ال

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).

VIP ةئيهت - PfSense جمانرب مادختساب (GUI) ةيموسرلر مدختسمل ةهجاو

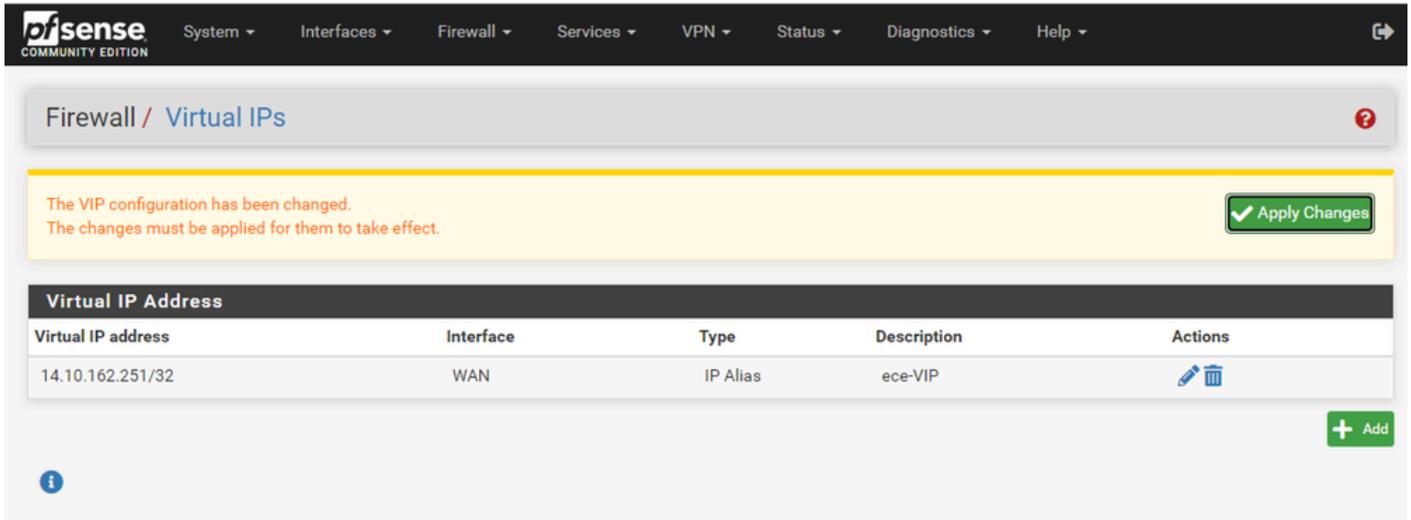
ةمه ةي صخش ةفاضال تامولعمل مدختسأ

- IP ل راعتسمل مسالا ديدحت :عونلا
- ثبلل اذه IP ناوعب ةصاخلا ةهجاو اول دح :ةهجاو اول
- IP ناوع لخدأ : (نيناوعلا) ناوعلا
- /32 عانقلا نوكي نأ بجي ،لمحلا ةنزاومل ةمدختسمل IP نيناوعلا :ناوعلا عانق
- اقحال نيوكتلل مهف لي هسئل ازجوم اصن لخدأ :فصولا

ريغتلا ذيفنتل ظفح دح

كب صاخلا نيوكتلل بولطم IP ناوع لك ل اذه ررك

نيوكتلل قيبت 4. ةوطخال



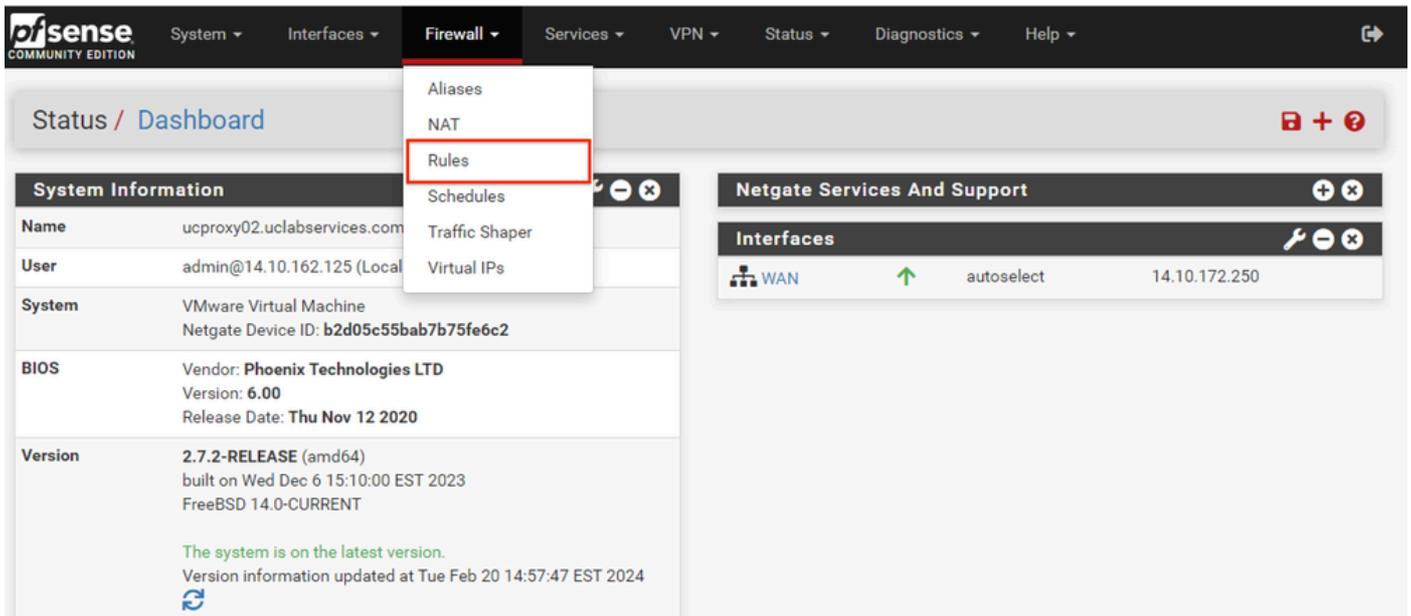
مهمه لايصخش لةمئاق - PfSense جمانرب مادختساب (GUI) ةيموسرلر مدختسمل ةهجاو

مهمه لايصخش لةمئاق ةفاضل دعب تاريغيغتل قيبطت رزل دح

## ةيامحل راج نيوكت

عضو لبق .ادج ةدودحم ةيضارتفال دءاوقل ةومجم .جمدم ةيامح راج لىل PFsense يوتحي ةلماش ةيامح راج ةسايس ءاشناب موقت كنأ نم دكأت ،جاتنال ةيلمع يف زاھل

ةيامحل راجل ةلدسنم لةمئاق ل نم دءاوق ديحت 1. ةوطخل



ةيامحل راج دءاوقل ةلدسنم لةمئاق ل - PfSense جمانرب مادختساب (GUI) ةيموسرلر مدختسمل ةهجاو

## ةفاضل رارزأ دح 2. ةوطخل

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

Firewall / Rules / WAN

Floating **WAN**

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0/13.35 MiB	*	*	*	WAN Address	8443 22	*	*	*	Anti-Lockout Rule	⚙️
✗ 0/0 B	*	RFC 1918 networks	*	*	*	*	*	*	Block private networks	⚙️
✗ 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

ةيامل راج دعاوق ةمئاق - PfSense ل (GUI) ةيموسرلا مدختسمل ةهجاو

ةفاضاب رخآل موقوي امنيب ددحمل رطسل قوف ةديدل دعاقل فيضي رارزالا دحأ نأ طحال  
ىلوالا دعاقلل رزي أ مادختسا نكمي .ةدحمل دعاقل لفسأ دعاقل

ناونعل 443 ريدي نأ رورم ةكرحمسي نأ دعاقل ةيامل راج تقلخ 3. ةوطخلا

pfSense COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Firewall / Rules / Edit

### Edit Firewall Rule

**Action** Pass  
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 /

[Display Advanced](#)  
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 Address or Alias 14.10.162.251 /

**Destination Port Range** HTTPS (443) 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** Allow ECE HTTPS  
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** [Display Advanced](#)

فيما حل راجد رورم دة عاق نيوكت - PfSense نم (GUI) ةيموسررلا مدختسملا ةهجاو

ةدعاقلا عاشنإل تامولعمل مدختسأ

- ريرمت ديدحت :ءارجإل
- ةدعاقلا اهيلع قبطنت يتلا ةهجاو ال رتخأ :ةهجاو ال
- بسانم وه امك دح :لوكوت ورب ال او نيوانع ال ةومجم
- يأك دح مل كرت :ردصم ال
- IP ناوع لخدأ مث ،ةهجو لل ةلدسنم ال ةمئاق ال نم راعتسم ال مسال او ناوع ال دح :ةهجو ال ةدعاقلا هيلع قبطنت يتلا
- لدسنم ال "ل"و "نم" نم لك يف HTTPS (443) ،ديدحت :ةهجو ال ذفنم قاطن
- ةبساحم لل ةدعاقلا هذه قباطت مزح ية ليحستل رايخ ال ةناخ دح :لجس ال
- اقح ال ةدعاقلا ال ةراش ال صن ريفوت :فصولا

ظفح ددح.

PfSense لى رورملا تاكرح عيجم طاقسإ ةدعاق ءاشنإ. 4 ةوطخل

اثيرح اهؤاشنإ مت يئرلا ةدعاقلا لفسأ ةدعاقلا جارءال "ةفاضإ" رزلا ددح.

The screenshot shows the 'Edit Firewall Rule' configuration page in PfSense. The page is divided into several sections:

- Edit Firewall Rule:**
  - Action:** Block. Hint: 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: /
  - Display Advanced:** 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 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:**  Display Advanced

At the bottom of the page, there is a **Save** button.

ةيامحل رادح طاقسإ ةدعاق نيوكت - PfSense ل (GUI) ةيموسرلا مدختسملا ةهءاو

- ةلئت ك ديرحت :ءارءال
- ةدعاقلا اهيلع قبطنت يئرلا ةهءاول رتخأ :ةهءاول
- بسانم وه امك ددح :لوكوت وربلال ونيوانعلا ةوموم

- يأك ددحملا كرت: ردصملا
- يا هنا ىلع ددحملا كرت: ةهجوملا
- ةبساحملا ةدعاقلا هذه قباطت مزح يا ليجستل رايخالالا ةناخ ددح: لجسلا
- اقحال ةدعاقلا ىلإ ةراشلال صن ريفوت: فصولا

ظفح ددح.

لفسألا يف رطحلا ةدعاق نا نم دكأتلاو دعاقولا ةعجارم 5. ةوطخل

Firewall / Rules / WAN

The firewall rule configuration has been changed.  
The changes must be applied for them to take effect.

Apply Changes

Floating WAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	2/13.51 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"/>	0/3.65 MiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	*	*	14.10.162.251	443 (HTTPS)	*	none	Allow ECE HTTPS	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	*	*	*	*	none		Drop all other inbound traffic	

↑ Add ↓ Add Delete Toggle Copy Save + Separator

ةيامحل رادج دعاقو ةمئاق - PfSense ل (GUI) ةيموسرلا مدختسملا ةهجاو

مهزرفل دعاقولا بحسا، ابولطم ناك اذا.

كتئيبل بولطملا بيترتللاب ةيامحلا رادج دعاقو نوكت نا درجم بتاريغيغتللا قيبتت ددح.

SHARoxy نيوكت

يسكوروباهللا ميهافم



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: <b>Phoenix Technologies LTD</b> Version: <b>6.00</b> Release Date: <b>Thu Nov 12 2020</b>
Version	<b>2.7.2-RELEASE</b> (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 - ShaRoxy لمدسة نملة اقلال

ةيساس ال ادادعإل نيوك ت. 2 ةوطخإل

## 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 ل ShaRoxy تاداعال - اإل

SHAroxy نيكمت رايخالال ةناخ ددح

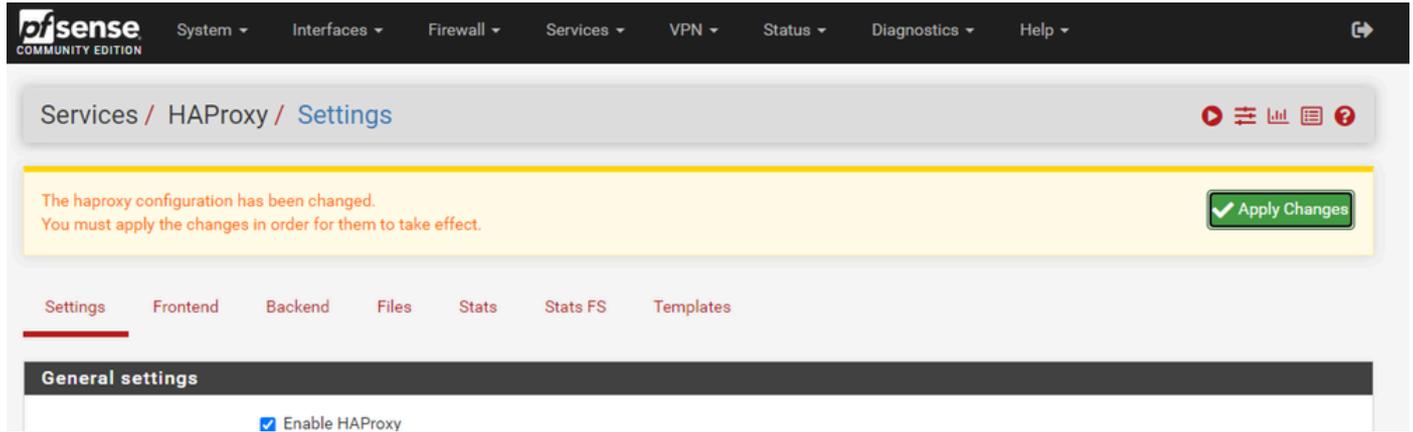
لعل لوصحلل مسقلا اذه يف دوجوملا ططخمل عجار .تالاصتالال لصقألال دحلل ةميق لخدا ةبولطملا ةركاذلا لوح لىصافات

لعل SHAroxy تايئاصح| ضرعل ذفنملا اذه مادختسا| متي .ءانيم ةلود لىلخالل ةميق تلخد زاهجال جراخ هفشك متي ال هنكل وزاهجال

ةلىلخالل تالاحل شيدحت لدعمل ةميق لخدا

كئئيبول بولطم وه ام بسح شيدحتلالو يقبتملا نيوكتلا عجار

ظفح ددح.

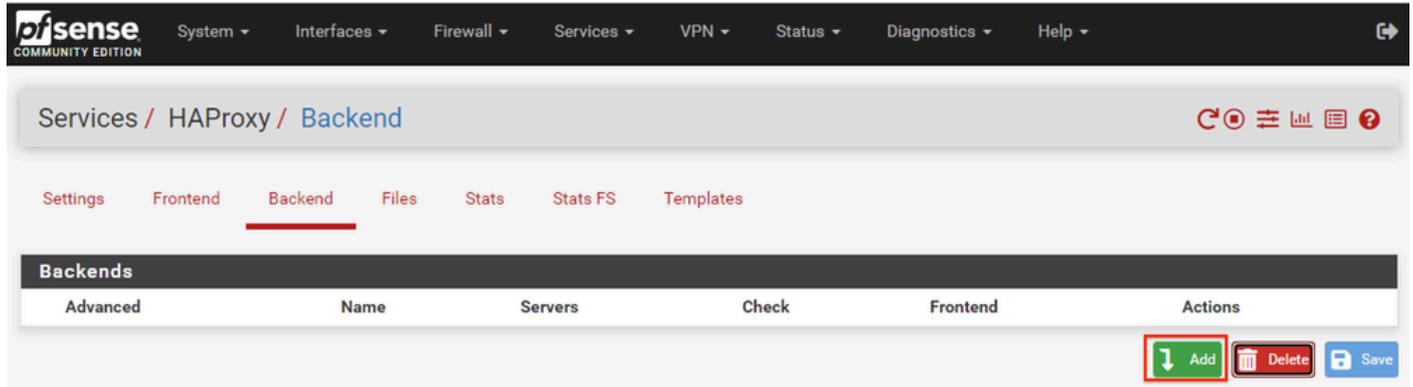


تاريغيغلتا قيبطت - pfSense GUI

قيبطت رزلا ديدحتب موقت ىتح نيوكتلا تاريغيغت طيشنت متي ال: طخالم تقوي فاعيمج اهقيبطتو نيوكتلا يفة ددعتم تاريغيغت ارجا كنكمي. تاريغيغلتا رخا مسق يفة مادختسا متيل نيوكتلا قيبطت مزلي ال. دحاو

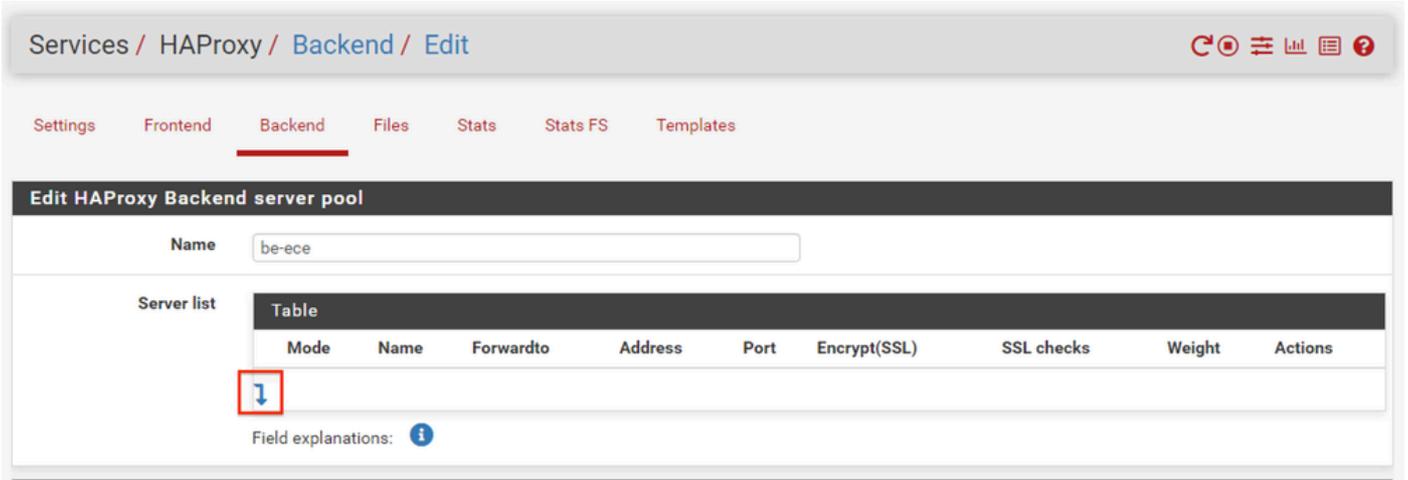
## SHARoxy فيلخلل نيوكت

يفلخلل فرطالا لىل ريشي نا بجي يمامالا طخال نا وه كلذ يفة ببسلا. يفلخلل اعزلاب ادبا. فيلخلل عمئاق ديدحتب تمق كنانم دكات



ةيفلخ فاضا - PfSense نم (GUI) ةيموسرلا مدختسمل اةهجاو

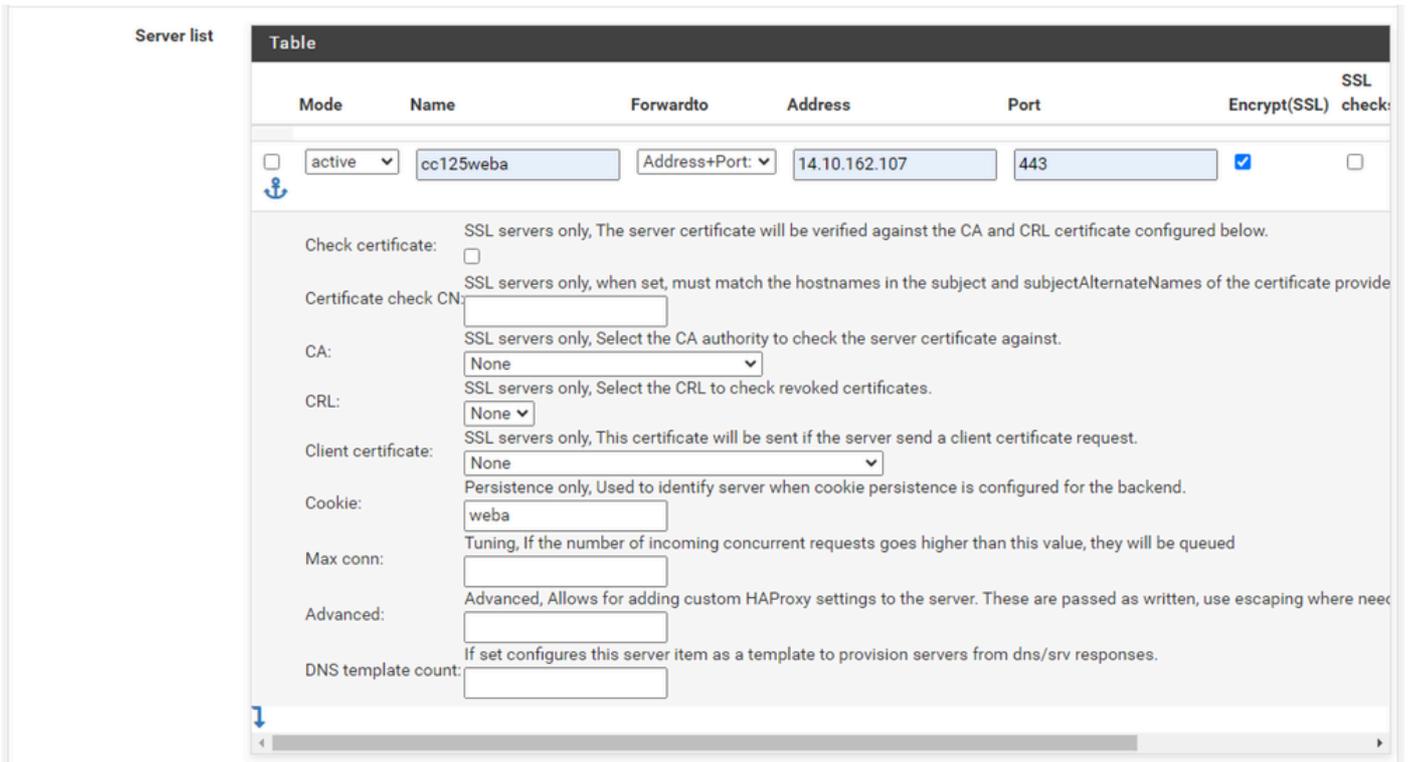
ةفاضل رزلا ددح.



PfSense GUI - ShaRoxy لىغشش ءءب -

ي.فلفل فرطلل مسا ريفوتب مق

مءاوخل ءمئاق لىل لءال مءاخال ءفاضال لفسال مهسال ءءح



مءاوخل ءمئاق - ءىفلفل ءىاهنل

وه اءه .يلىل مءاخال مسا عم اءه قءاطل نأ مزلى ال .مءاخال لىل ءراشلل مسا ريفوتب مق ءالءال ءءفص يف رهائل مسال

مءاخال لىل ءمئاق .مءاخال ناونءال ريفوتب مق

مءاخال لىل 443 ءمئاق .هبل لاصلال ءىرل ءىل ءفنم ريفوتب مق

مءاخال لىل ءمئاق (SSL).

مءاخال لىل ءمئاق .مءاخال لىل ءمئاق

ةيفلخلاللخاد اديرف نوكي نأ بجي ولعمل الةسلج قصللمب صاخلا

ةئيبلا يف رخأ بيو مداوخ ي نيوكتل لفسأل مهسال دح، لوالل مداخلل نيوكتل دعب

### 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.

لمح ةنزاوم - HubRoxy Backend

للمحتل الةنزاوم تاراخي نيوكتل بمق

للقا الالصت اىلع ك لذ نييغت بجي، ECE مداوخل ةبسنلاب

Access control lists and actions	
<b>Timeout / retry settings</b>	
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.
<b>Health checking</b>	
Health check method	HTTP HTTP protocol to check on the servers health, can also be used for HTTPS servers(requires checking the SSL box for the servers).
Check frequency	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 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.
Url used by http check requests.	/system/web/view/platform/common/login/root.jsp?partitionId=1 Defaults to / if left blank.
Http check version	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 Backend - ةحصلا صرّف

ن.نيوكتلا اذه يف لوصولا يف مكحتلا مئاق مءاوق مءاخستسا متي ال

اهل يضارتفالا نيوكتلا دنع ةلواحملا ةءاعا / ةلهملا تءاءاعا كرت نكمي

ةحصلا نم ققحتلا مسق نيوكتب مق

1. HTTP: ةحصلا نم ققحتلا بولسا أ.
2. ةيناث لكل ةيضارتفالا ةميقلا مءاخستسال ةءراف ةحاسملا كرتا: كيشلا راركت.
3. لء ةحصلا ب قلعئت تارييغت يا ةباتكل رايءال اذه دءح: لءسلا نم ققحتلا تايءمع. تالءسلا.
4. ةمءاقلا نم GET دءح: HTTP: نم ققحتلا بولسا أ.
5. ECE مءاخ لاءءال: HTTP: نم ققحتلا تابءل طءساوب مءخستسملا URL ناوع. /system/web/view/platform/common/login/root.jsp?partitionId=1
6. HTTP: ءءءر، HTTP/1.1\r\nHost:\ {fqdn\_of\_server}

مءاخلا ب ةصءال FQDN لبق نكلو ةيئاهنلا ةيفلءال ةطرش دءب ةحاسم نيءمضت نم دءا

### 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.

طابترالال فيرعت فلم تابث - ةيفلخال HubRoxy

ةددم ريغ ليمعال نم ققحتال تايلمع كرت

طابترالال فيرعت فلم ةيرارمتسا نيوك:

1. تافلم الة دنتسمال ةيرارمتسالال نيكم تل دح: ةنكممال طابترالال فيرعت تافلم . طابترالال فيرعت
2. طابترالال فيرعت فلمل مسا ريفوتب مق: طابترالال فيرعت فلمل مسا .
3. لدسنمال عبرمال نم جاردل دح: طابترالال فيرعت فلمل عضو .
4. ةطوبضم ريغ ةيقبتمال تاراخال كرتأ .

**HSTS / Cookie protection**

**HSTS Strict-Transport-Security** When configured enables "HTTP Strict Transport Security" leave empty to disable. (only used on "http" frontends)

**WARNING!** the domain will only work over https with a valid certificate!  
Clients will cache this header for the set duration which means removing this header will still require a valid certificate for the set time.

31536000 Seconds

If configured clients that requested the page with this setting active will not be able to visit this domain over a unencrypted http connection. So make sure you understand the consequence of this setting or start with a really low value.  
EXAMPLE: 60 for testing if you are absolutely sure you want this 31536000 (12 months) would be good for production.

**Cookie protection**  Set "secure" attribute on cookies (only used on "http" frontends)  
This configuration option sets up the Secure attribute on cookies if it has not been setup by the application server while the client was browsing the application over a ciphered connection.

**Advanced settings**

[Save](#)

HubRoxy Backend - HSTS

ةيضا رت ف ال ا ه ا د ا د ع ا ي ف ي ف ل خ ل ل ف ر ط ل ا ل ن ي و ك ت ج ذ و م ن ن م ة ي ق ب ت م ل ا م ا س ق ا ل ا ك ر ت ن ك م ي .

ف ل م ج ا ر د ا ب ECE م و ق ت . م س ق ا ذ ه ي ف ة م ي ق ل ي ط ع ت ت ل ك ش ، HSTS ل ك ش ي ن ا ت ن ا د ي ر ي ن ا ر ر ك ت م ن ي و ك ت ل ا ا ذ ه ن و ك ي ش ي ح ب ا ي ا HSTS ط ا ب ت ر ا ف ي ر ع ت .

ظ ف ح ا ، د د ح .

ة ه ج ا و ن ي و ك ت SHARoxy

ة ي م ا م ا ل ا ة ه ج ا و ل ا ة م ا ق ا ل ا ر ي ر ي غ ت .

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

Services / HAProxy / Frontend

Settings Frontend Backend Files Stats Stats FS Templates

**Frontends**

Primary	Shared	On	Advanced	Name	Description	Address	Type	Backend	Actions
									<a href="#">Add</a> <a href="#">Delete</a> <a href="#">Save</a>

pfSense GUI - HapRoxy ة ف ا ض ا ة ه ج ا و ل ا ة ي م ا م ا ل ا

ة ف ا ض ا ر ز ل ا د د ح

Settings Frontend Backend Files Stats Stats FS Templates

### Edit HAProxy Frontend

**Name** fe-ece

**Description** Frontend for ECE

**Status** Active

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

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

**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** http / https(offloading)

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".

ي م ا ل س أ ر ل ل - HapRoxy

ي م ا ل ف ر ط ل ل م س ا ر ي ف و ت ب م ق .

ا ق ح ا ل ة ي م ا ل ا ة ه ج ا و ل ا د ي د ح ت ي ف ة د ع ا س م ل ل ف ص و ر ي ف و ت ب م ق .

ة ي ج ر ا خ ل ل ن ي و ا ن ع ل ل و د ج ي ف :

1. ا ذ ه ب ي و ل ا ع ق و م ل ا ه ت ا ش ن ا ي ت ل ل ة م ه م ل ا ة ي ص خ ش ل ل ا د ح : ا غ ص ا ل ا ن ا و ن ع .
2. 443 ل خ د ا : ذ ف ن م ل ا .
3. ل م ع ل ل ا س ل ج ط ا ب ت ر ا ف ي ر ع ت ف ل م ج ا ر د ا ن ك م ي ث ي ح ب ر ا ي خ ل ل ا ذ ه د ح : S S L ل ي م ح ت ا غ ل ا .

ة غ ر ا ف ت ا ل ا ص ت ا ل ل ي ص ق ا ل ا د ح ل ك ر ت ا .

ا ل ي م ح ت ل ل ا غ ل ل ) http / https ك ع و ن ل ل د ي د ح ت ن م د ك ا ت .

## 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

be-ecce

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

IncidentRoxy Backend - يضا رتفالا ةيفلخ لال دي دحت -

ةلدس نمل ةمئاق لال ن م يضا رتفالا ةيفلخ ةطقن رايتخ | يه ةئيه ةيلمع لسا ربت عت  
دحاو بي و ع قوم ةفاضت ساب ةمهمل ةيصخش لال موقت ام دنع كلذ دي دحت نكم ي

## 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 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	
<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

None

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

عمدقتم (ACL) لوصولو يف مكحتلال عمئاق - HubRoxy Backend

هيجوت ةداعإل (ACL) لوصولو يف مكحتلال مئاقو مادختسا نكمي، ةوصولو يف حضوم وه امك فورظلا ىلإ ادانتسا ةددعتم تايفلخ ىلإ ةدحاو ةهواو.

يف فيضملا ناك اذا ام ةفرعمل ققحتت (ACL) لوصولو يف مكحتلال عمئاق نأ ىرت نأ كنكمي ةيفلخ مادختسا متي، اذه ىلإ ادانتسا. مسالا ةطاسبب وأ. ذفنملا مقرور مسالاب أدبي بلطلال ةددم.

ابوروال ةيداصتقالا ةنجللال عم اعئاش سيل اذهو.

**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).

Certificates	Actions
<input type="checkbox"/> Add ACL for certificate CommonName. (host header matches the "CN" of the certificate)	
<input type="checkbox"/> 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 EECDH+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 EECDH+aRSA+AES:TLSv1+kRSA+AES:TLSv1+kRSA+3DES ecde secp256k1

داهشال طبر - ةيمامأل IncidentRoxy ةهجاو

نأ بجي .عقوملا اذه عم مادختسالل اهؤاشنإ مت يتلا ةداهشال دح ،SSL ليمحت اءاغل مسق يف مءاخ ةداهش ةداهشال هذه نوكت

ةداهشال عوضومل ةليدب ءامسأل (ACL) لوصولاب مكحتلا ةمئاق فضا ،رايخال دح

ةيضا رتفال اهميق دن ع ةيقبتمل تارايلال كرت كنكمي

جذومنل اذه ةيانهن يف ظفحا ،دح

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)	<a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Copy</a>

[Add](#) [Delete](#) [Save](#)

نيوكتال قيبطت - SHAraxy

ي راجل نيوكتال لى ع فخل او ة ج اول تاريغي غت ذيفن تل اه قيبطت م تال تاريغي غت لادح له لغشت

PfSense. جم ان رب نيوكتو دادع! م تي هت نا دقل ، اني ناهت

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسمل اذ ه Cisco ت مچرت  
ملاعلاء نأ عي مچ ي ف ن ي م دخت سمل ل معد ي و تح م مي دقت ل ة يرش ب ل و  
امك ة ق ي قد ن و ك ت ن ل ة ل آل ة مچرت ل ض ف أن ة ظ حال م ي ج ر ي . ة ص ا خ ل م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems (رف و ت م ط بار ل ا) ي ل ص أ ل ا ي ز ي ل ج ن ا ل ا دن تسمل ا