TRANSPARENT FIREWALL DENGAN PFSENSE

Artikel ini ane tulis karena pas kemarin ngerjain ginian buat salah satu kantor, dengan kebijakan, semua client harus dapet ip dari router, dari hasil nyilem dan solawatan digugel akhirnya nemu juga, bikin bridge di pfsense. Model kaya gini biasa disebut Transparent Firewall.

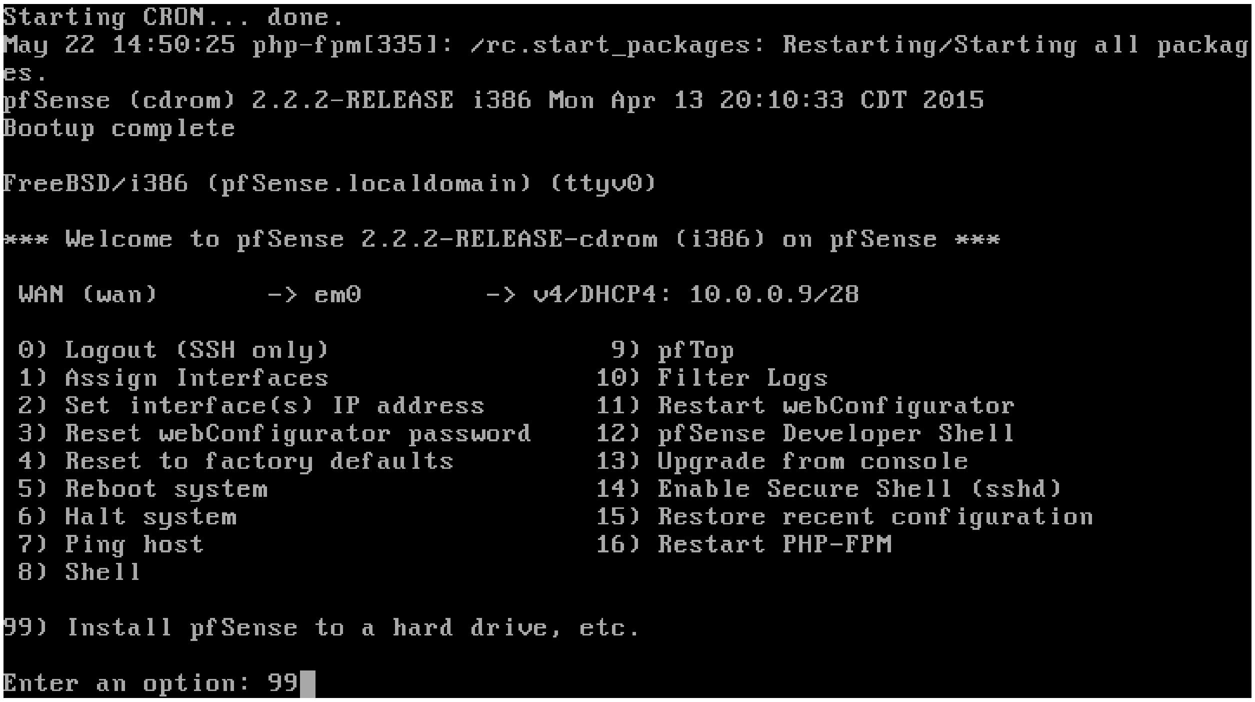
Pfsense adalah salah satu opensource firewall yang menggunakan base system freebsd. Biasa di install di server atau board firewall seperti gambar dibwah

Oke sebelum membahas cara membuat transparent firewall dengan pfsense, ane bahas dikit tentang apa itu transparent firewall. Transparent Firewall (juga dikenal sebagai bridging firewall) bukanlah sebuah firewall yang murni, tetapi ia hanya berupa turunan dari stateful Firewall. Daripada firewall-firewall lainnya yang beroperasi pada lapisan IP ke atas, transparent firewall bekerja pada lapisan Data-Link Layer, dan kemudian ia memantau lapisan-lapisan yang ada di atasnya. Selain itu, transparent firewall juga dapat melakukan apa yang dapat dilakukan oleh packet-filtering firewall, seperti halnya stateful firewall dan tidak terlihat oleh pengguna (karena itulah, ia disebut sebagai Transparent Firewall).

Sumber : http://id.wikipedia.org/wiki/Tembok_api

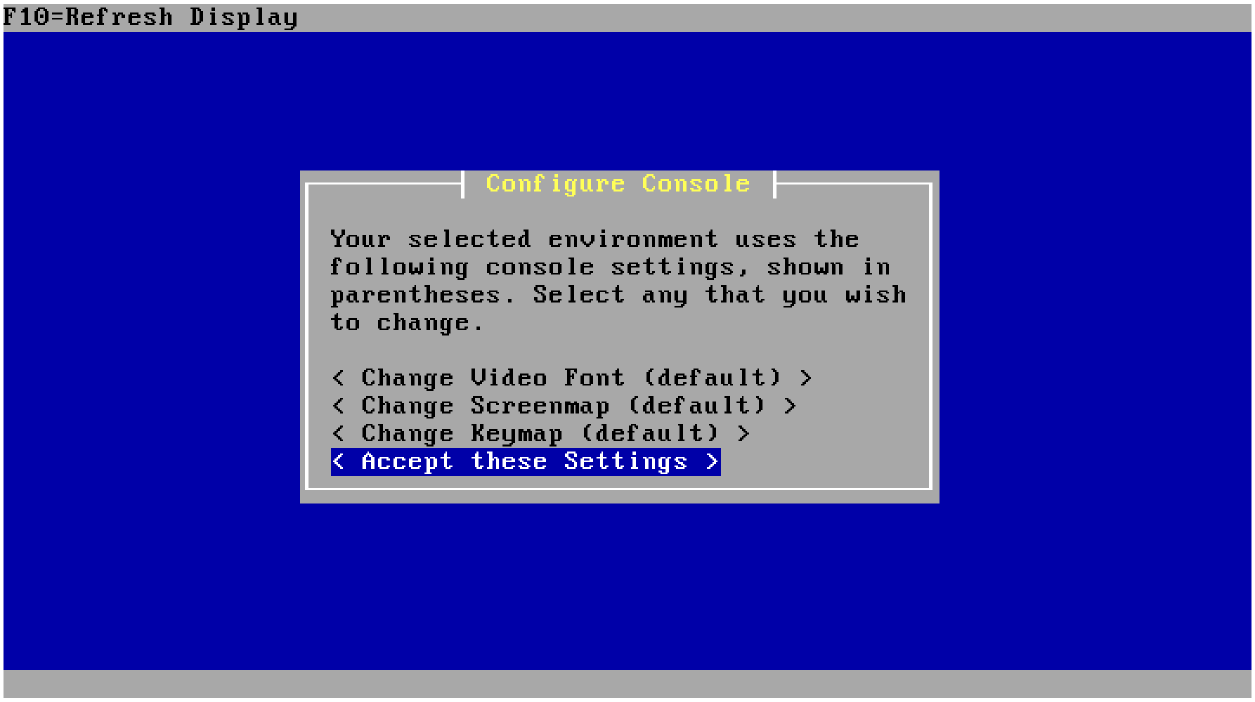
Oke langsung aja ke tutorial membuat transparent firewall nya, pertama siapin pfsense nya, disini ane pake pfsense 2.2 .

Pertama boot ke pfsense bisa pake cd atau flashdisk, pilih nomer 99 buat install ke harddisk atau cf card.



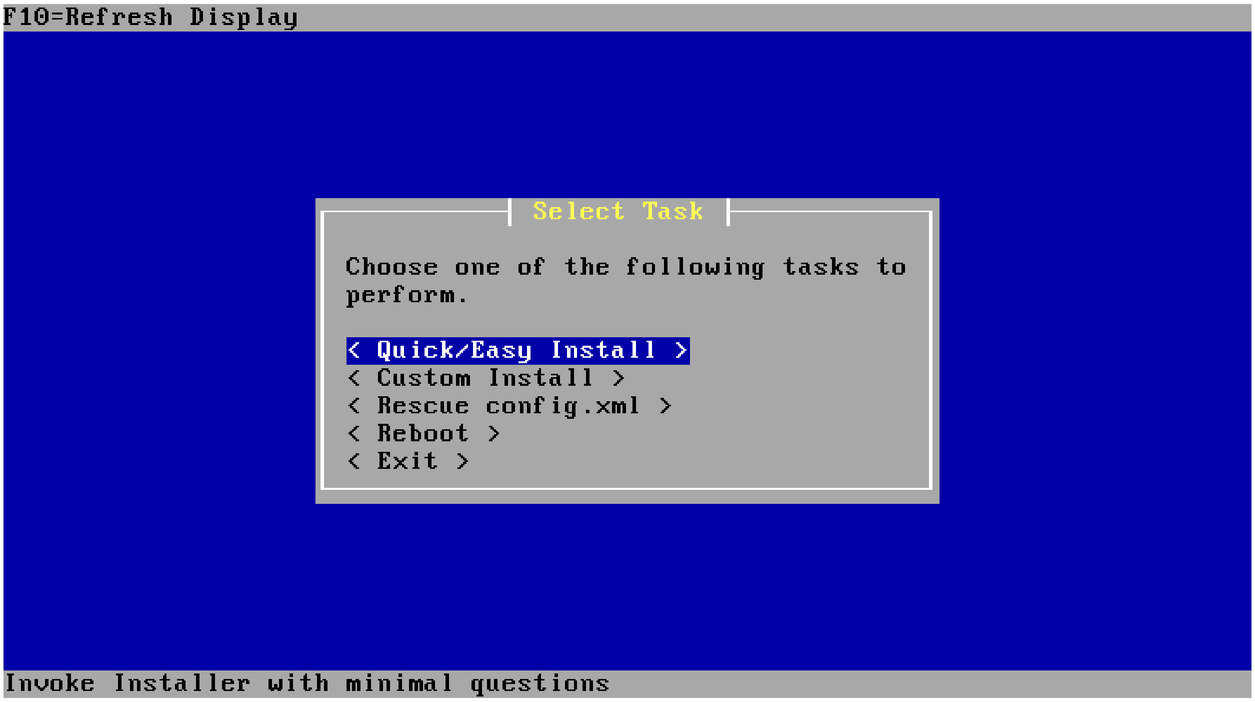
```
Starting CRON... done.
May 22 14:50:25 php-fpm[335]: /rc.start_packages: Restarting/Starting all packag
es.
pfSense (cdrom) 2.2.2-RELEASE i386 Mon Apr 13 20:10:33 CDT 2015
Bootup complete

FreeBSD/i386 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.2.2-RELEASE-cdrom (i386) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 10.0.0.9/28

 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) pfSense Developer Shell
 4) Reset to factory defaults         13) Upgrade 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

99) Install pfSense to a hard drive, etc.

Enter an option: 99
```

Terus konfigurasi keymap, font, video pas disini ane biarin default jadi langsung pilih accept



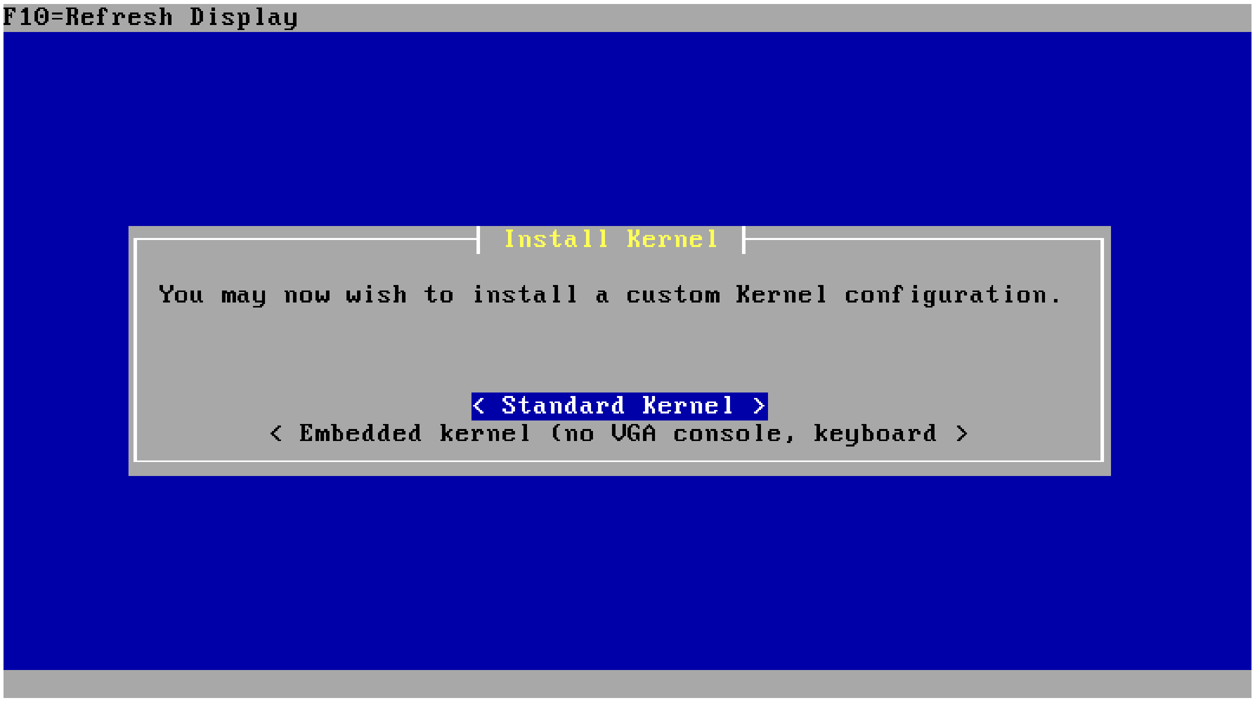
```
F10=Refresh Display

                    Configure Console

         Your selected environment uses the
         following console settings, shown in
         parentheses. Select any that you wish
         to change.

         < Change Video Font (default) >
         < Change Screenmap (default) >
         < Change Keymap (default) >
         < Accept these Settings >
```

Pilih tipe install, ane pake quick install



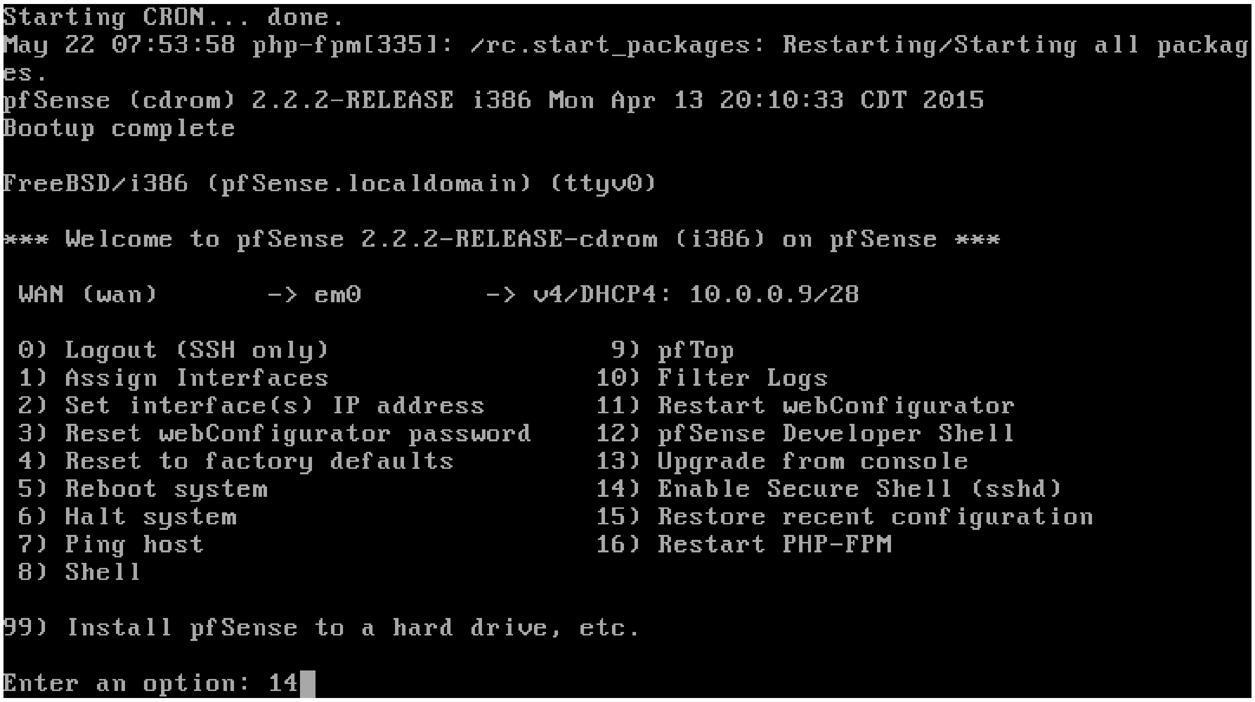
```
F10=Refresh Display

                      Select Task

          Choose one of the following tasks to
          perform.

          < Quick/Easy Install >
          < Custom Install >
          < Rescue config.xml >
          < Reboot >
          < Exit >

Invoke Installer with minimal questions
```

Pilih mode kernel, buat instalasi di server, pc, atau virtual pilih standar kernel. Kalo installnya di firewall board kaya di atas pilih yang embedded kernel.



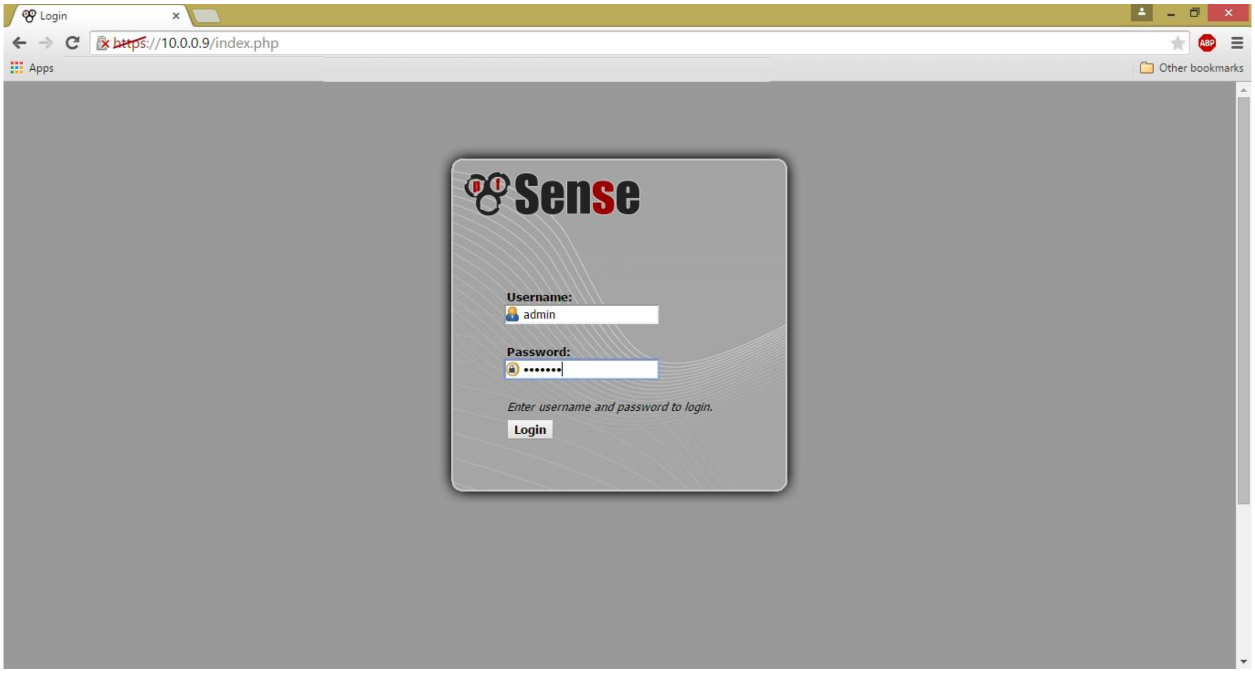
```
F10=Refresh Display

                         Install Kernel

     You may now wish to install a custom Kernel configuration.


                        < Standard Kernel >
              < Embedded kernel (no VGA console, keyboard >
```

Tunggu sampe installnya selesai, kalo udah selesai akan restart otomatis, dan masuk ke menu CLI pfsense.



```
Starting CRON... done.
May 22 07:53:58 php-fpm[335]: /rc.start_packages: Restarting/Starting all packag
es.
pfSense (cdrom) 2.2.2-RELEASE i386 Mon Apr 13 20:10:33 CDT 2015
Bootup complete

FreeBSD/i386 (pfSense.localdomain) (ttyv0)

*** Welcome to pfSense 2.2.2-RELEASE-cdrom (i386) on pfSense ***

 WAN (wan)       -> em0        -> v4/DHCP4: 10.0.0.9/28

 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) pfSense Developer Shell
 4) Reset to factory defaults         13) Upgrade 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

99) Install pfSense to a hard drive, etc.

Enter an option: 14
```

Selanjutnya login ke web configurator (default user : admin | password : pfsense). Masukin IP ke web browser dengan https.

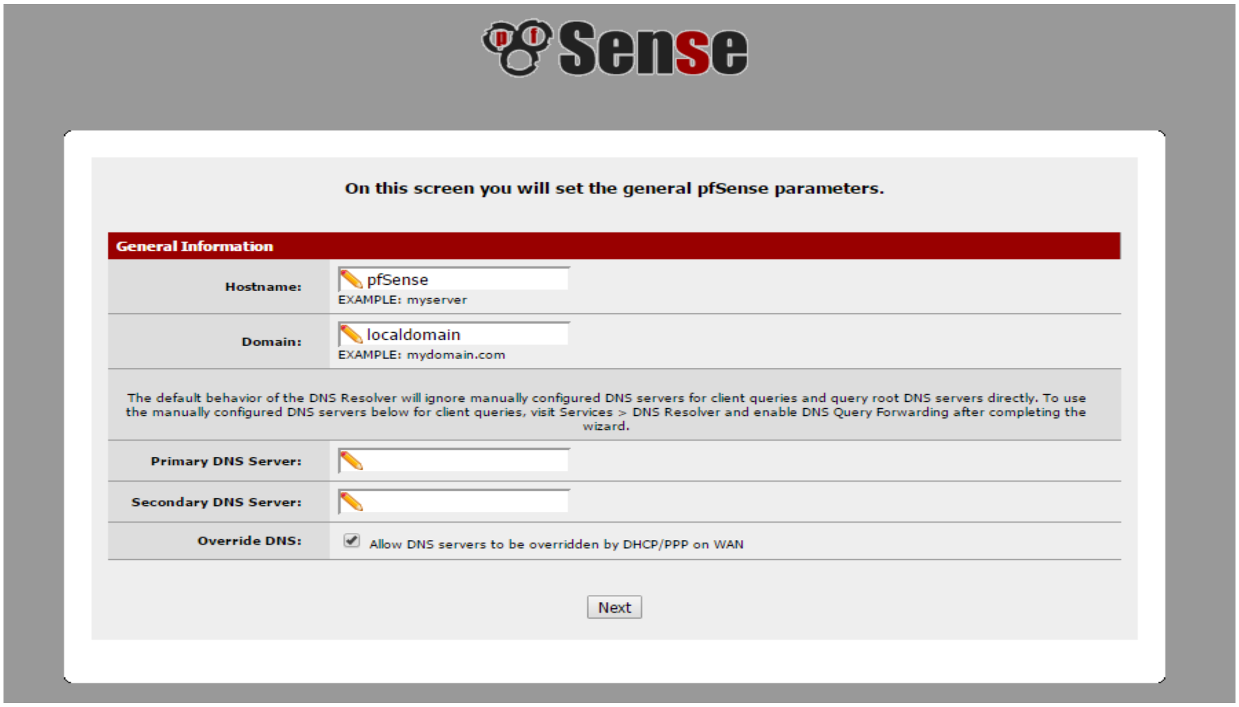


Username: admin

Password: •••••••

Enter username and password to login.

Selanjutnya setup hostname dan dns, disini ane pilih allow dns from wan



On this screen you will set the general pfSense parameters.

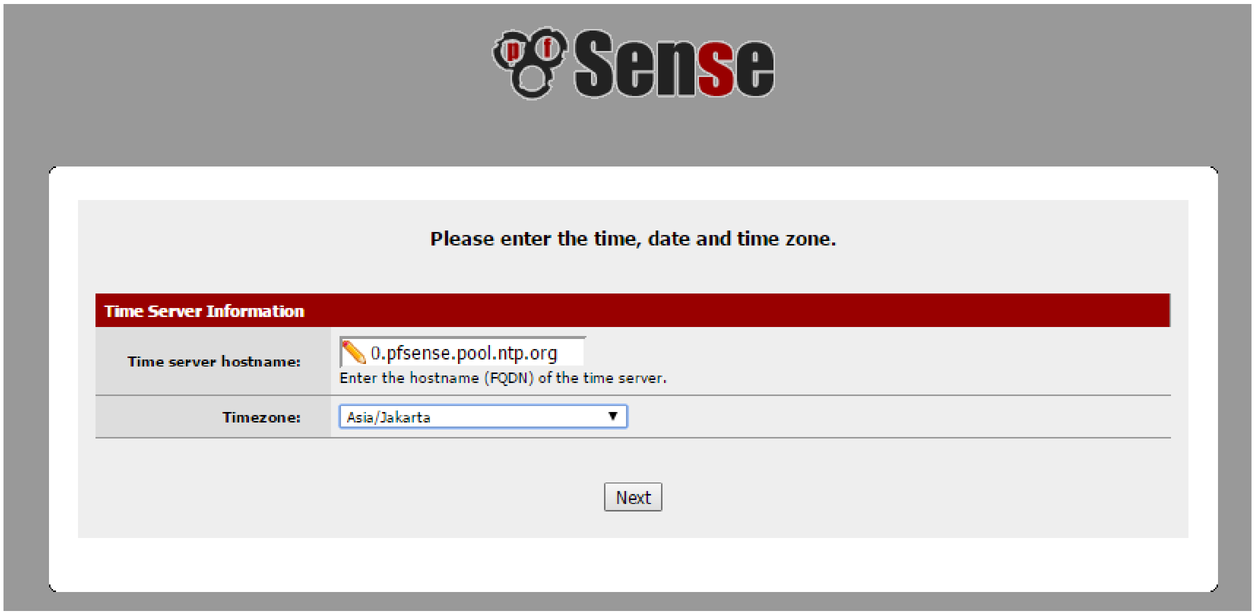
General Information

Hostname:	pfSense EXAMPLE: myserver
Domain:	localdomain EXAMPLE: mydomain.com

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

Setting waktu dan pilih timezone

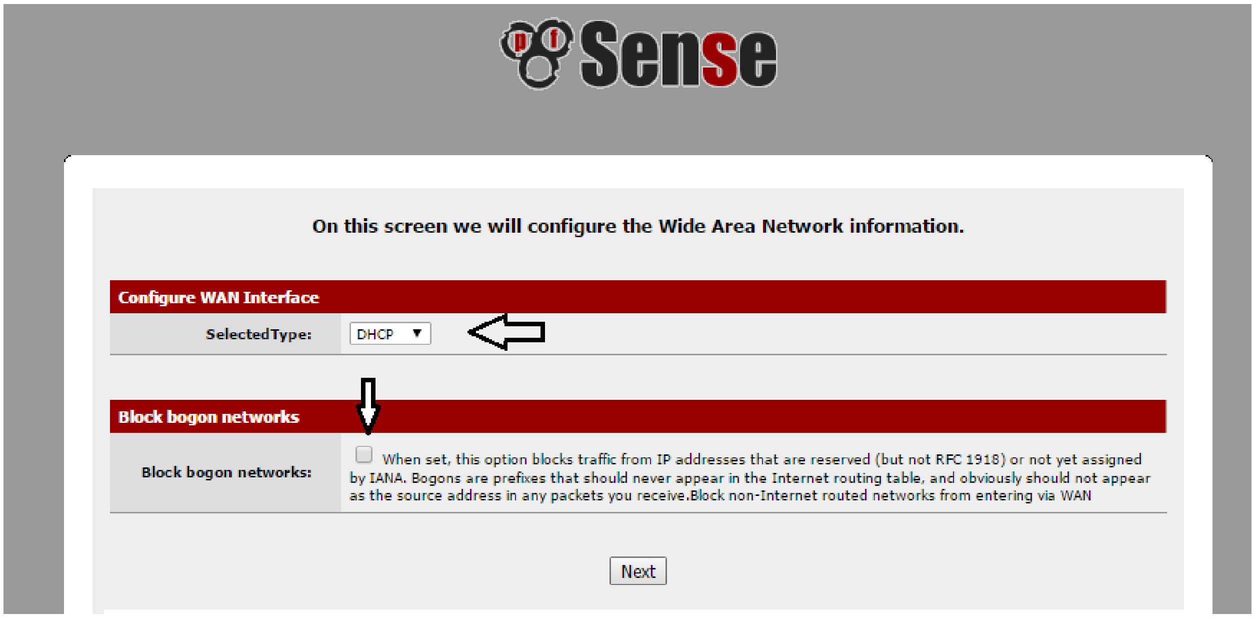


Please enter the time, date and time zone.

Time Server Information

Time server hostname:	0.pfsense.pool.ntp.org Enter the hostname (FQDN) of the time server.
Timezone:	Asia/Jakarta

Setup wan IP, karena firewall ini ada di bawah router yang ngeluarin dhcp, makanya ane pilih dhcp



On this screen we will configure the Wide Area Network information.

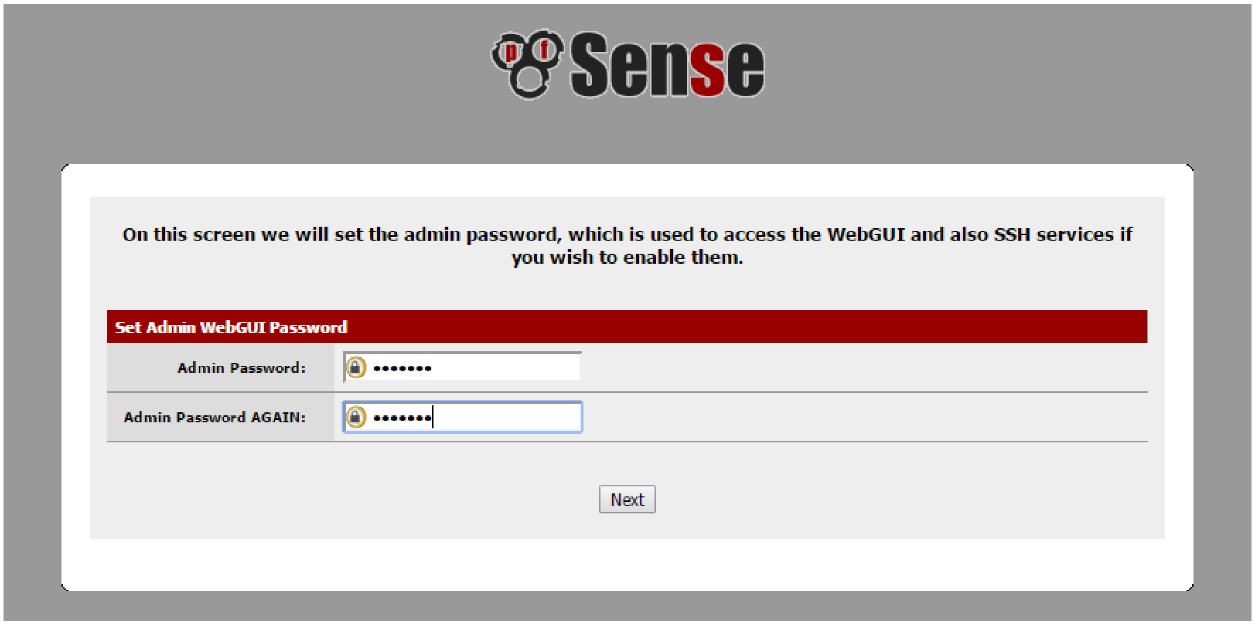
Configure WAN Interface

SelectedType:	DHCP

Block bogon networks

Block bogon networks:	□ When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets you receive.Block non-Internet routed networks from entering via WAN

Selanjutnya ganti password default

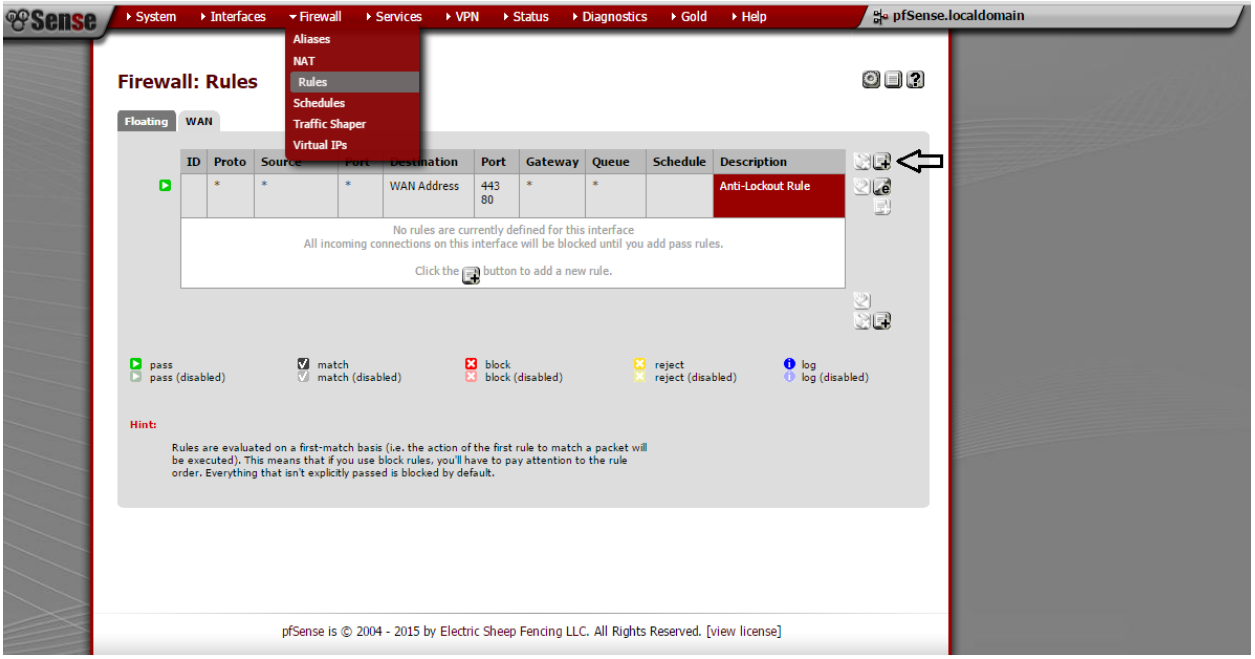


On this screen we will set the admin password, which is used to access the WebGUI and also SSH services if you wish to enable them.

Set Admin WebGUI Password

Admin Password:	•••••••
Admin Password AGAIN:	•••••••

Selanjutnya buat rule akses dari wan, soalnya nanti kalo udah di aktifin interface lan nya semua akses konfigurasi Cuma bisa dari interface lan.



Firewall: Rules

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
🟩		*	*	*	WAN Address	443 80	*	*		Anti-Lockout Rule

No rules are currently defined for this interface
All incoming connections on this interface will be blocked until you add pass rules.

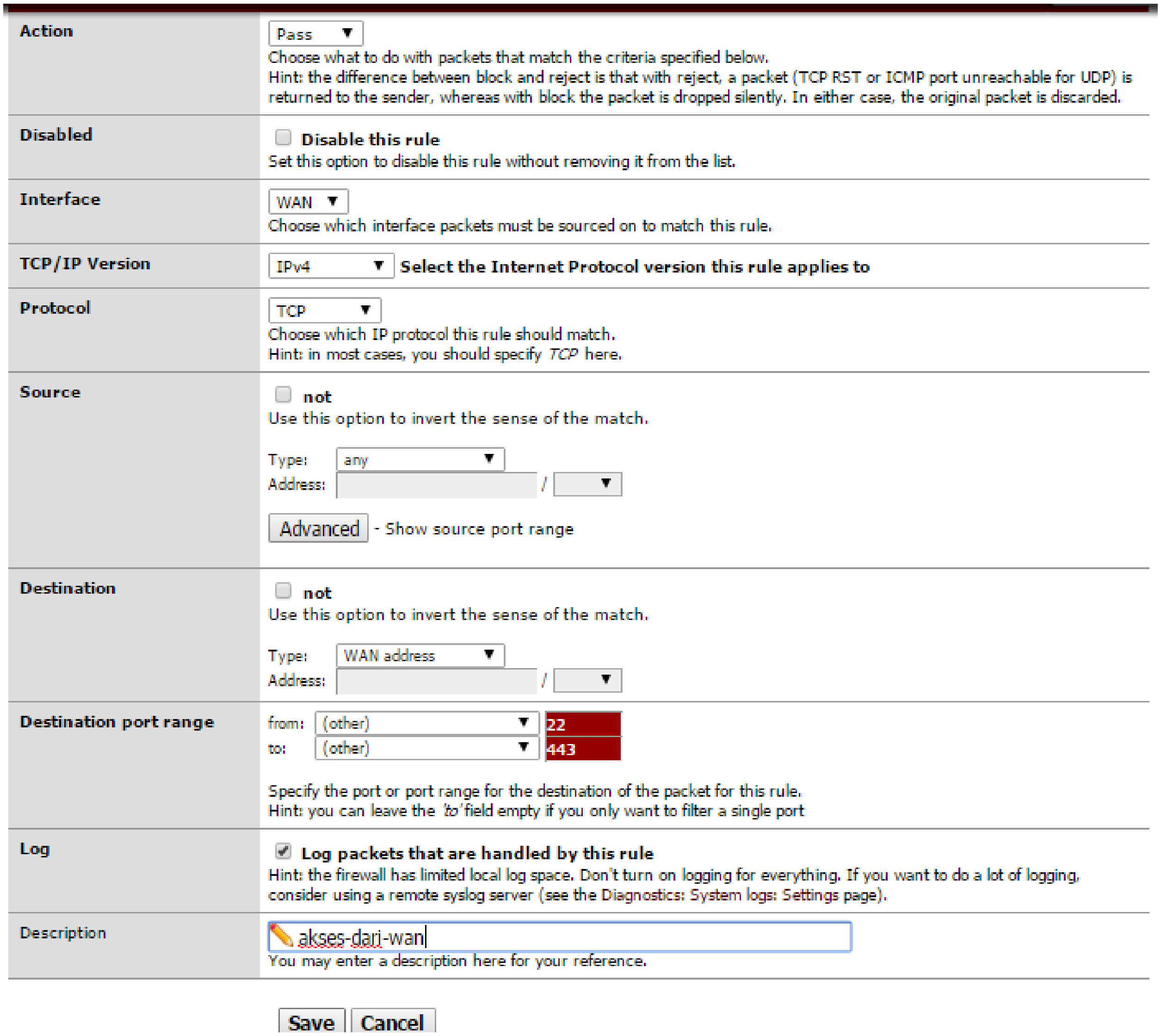
Click the ⊞ button to add a new rule.

🟩 pass	☑ match	☒ block	☒ reject	● log
pass (disabled)	match (disabled)	block (disabled)	reject (disabled)	log (disabled)

Hint:

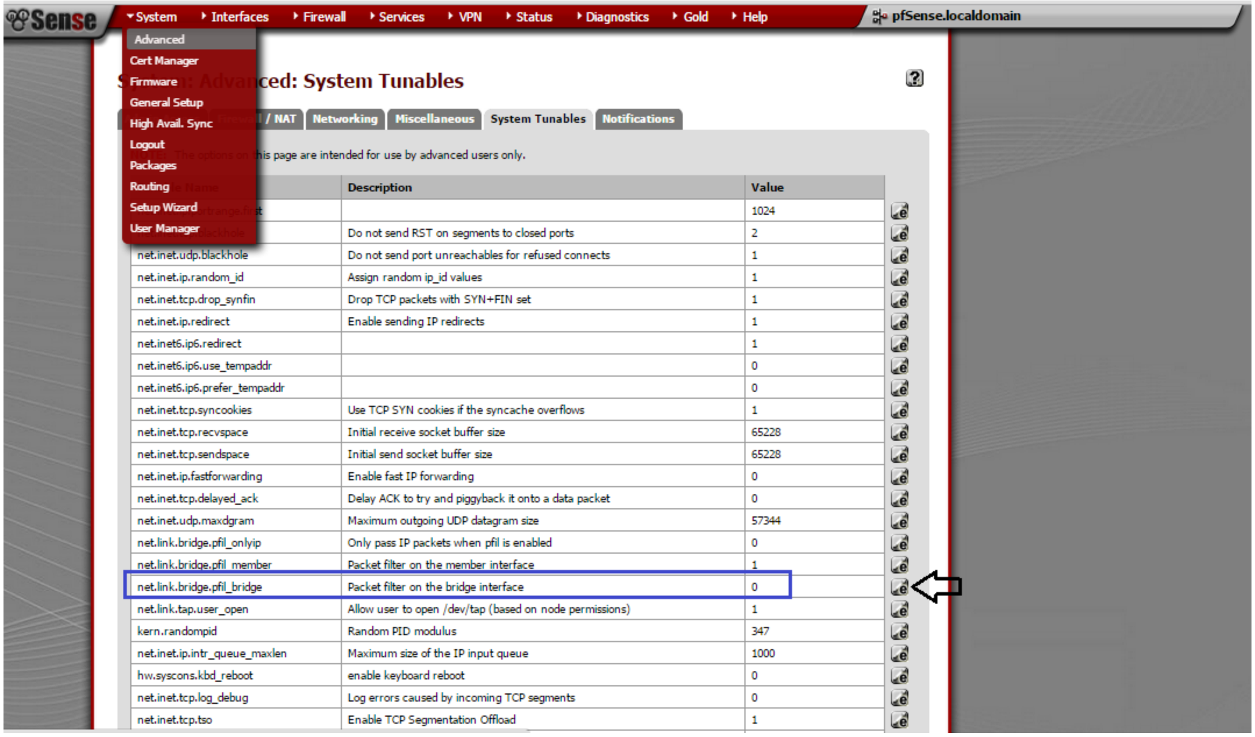
Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

pfSense is © 2004 - 2015 by Electric Sheep Fencing LLC. All Rights Reserved. [view license]



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 which interface packets must be sourced on to match this rule.
TCP/IP Version	IPv4 ▼ **Select the Internet Protocol version this rule applies to**
Protocol	TCP ▼ Choose which IP protocol this rule should match. Hint: in most cases, you should specify *TCP* here.
Source	□ **not** Use this option to invert the sense of the match. Type: any ▼ Address: / ▼ Advanced - Show source port range
Destination	□ **not** Use this option to invert the sense of the match. Type: WAN address ▼ Address: / ▼
Destination port range	from: (other) ▼ 22 to: (other) ▼ 443 Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the *'to'* field empty if you only want to filter a single port
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 you want to do a lot of logging, consider using a remote syslog server (see the Diagnostics: System logs: Settings page).
Description	akses-dari-wan You may enter a description here for your reference.

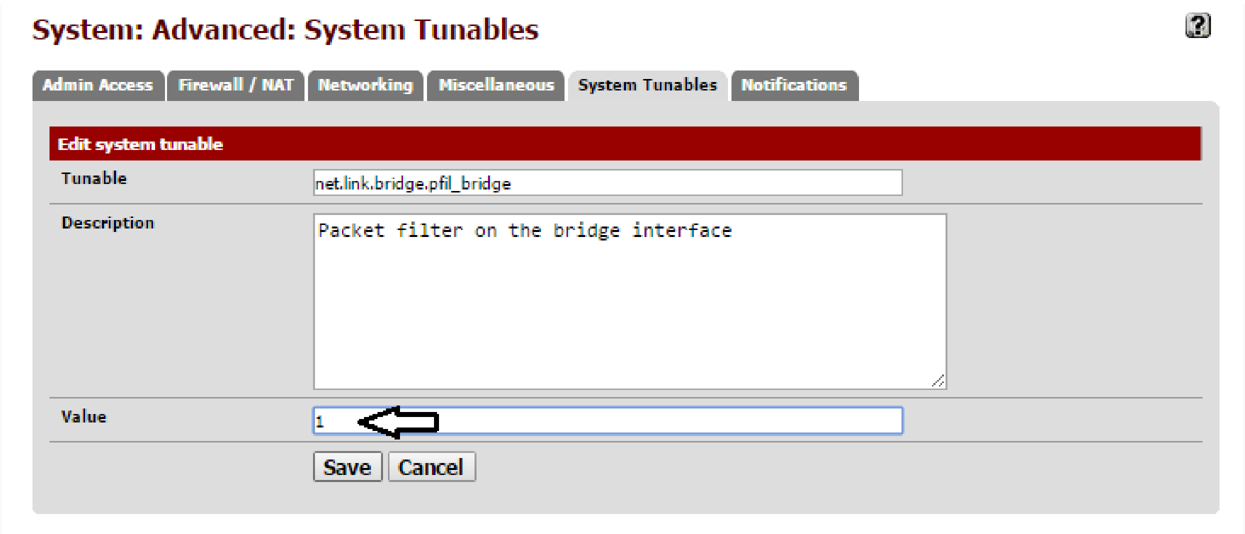
Selanjutnya enable service bridge, buat aktifin mode bridge



System: Advanced: System Tunables

NOTE: The options on this page are intended for use by advanced users only.

Tunable Name	Description	Value
net.inet.ip.portrange.first		1024
net.inet.tcp.blackhole	Do not send RST on segments to closed ports	2
net.inet.udp.blackhole	Do not send port unreachables for refused connects	1
net.inet.ip.random_id	Assign random ip_id values	1
net.inet.tcp.drop_synfin	Drop TCP packets with SYN+FIN set	1
net.inet.ip.redirect	Enable sending IP redirects	1
net.inet6.ip6.redirect		1
net.inet6.ip6.use_tempaddr		0
net.inet6.ip6.prefer_tempaddr		0
net.inet.tcp.syncookies	Use TCP SYN cookies if the syncache overflows	1
net.inet.tcp.recvspace	Initial receive socket buffer size	65228
net.inet.tcp.sendspace	Initial send socket buffer size	65228
net.inet.ip.fastforwarding	Enable fast IP forwarding	0
net.inet.tcp.delayed_ack	Delay ACK to try and piggyback it onto a data packet	0
net.inet.udp.maxdgram	Maximum outgoing UDP datagram size	57344
net.link.bridge.pfil_onlyip	Only pass IP packets when pfil is enabled	0
net.link.bridge.pfil_member	Packet filter on the member interface	1
net.link.bridge.pfil_bridge	Packet filter on the bridge interface	0
net.link.tap.user_open	Allow user to open /dev/tap (based on node permissions)	1
kern.randompid	Random PID modulus	347
net.inet.ip.intr_queue_maxlen	Maximum size of the IP input queue	1000
hw.syscons.kbd_reboot	enable keyboard reboot	0
net.inet.tcp.log_debug	Log errors caused by incoming TCP segments	0
net.inet.tcp.tso	Enable TCP Segmentation Offload	1

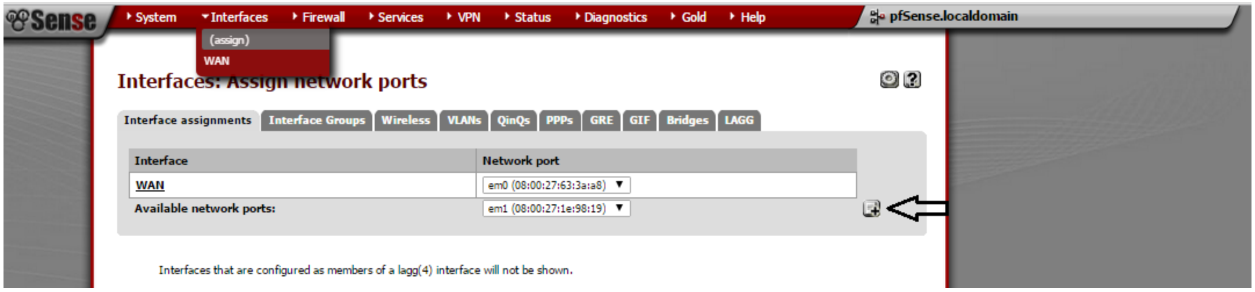


System: Advanced: System Tunables

Edit system tunable

Tunable	net.link.bridge.pfil_bridge
Description	Packet filter on the bridge interface
Value	1

Selanjutnya tabahin interface lan

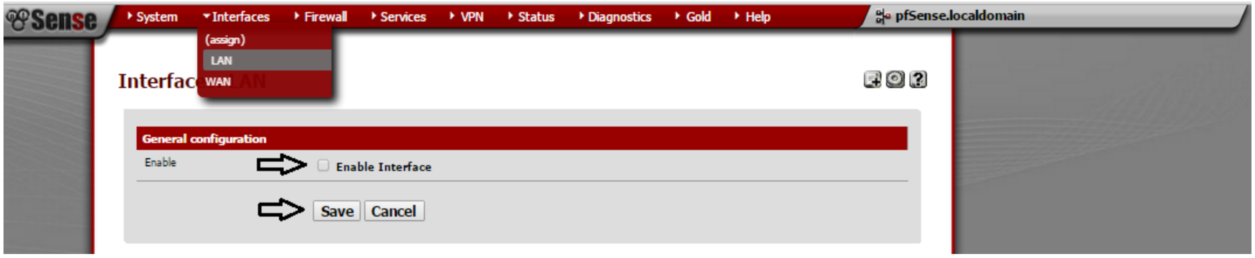


Interfaces: Assign network ports

Interface	Network port
WAN	em0 (08:00:27:63:3a:a8)
Available network ports:	em1 (08:00:27:1e:98:19)

Interfaces that are configured as members of a lagg(4) interface will not be shown.

Enable interface lan yang baru ditambahin

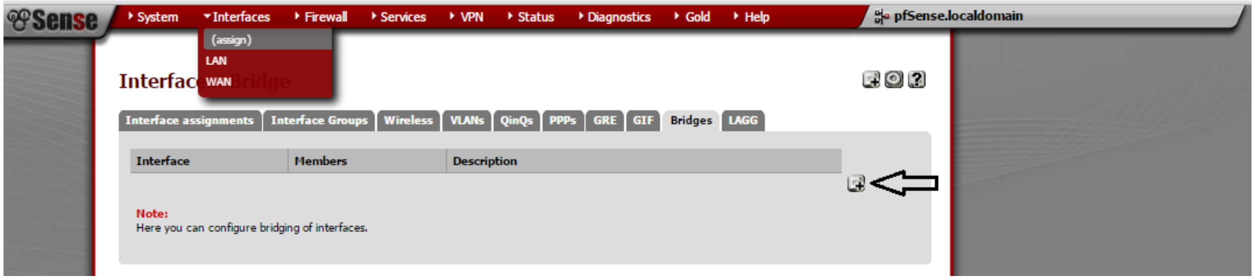


Interfaces: LAN

General configuration

Enable □ Enable Interface

Tamabah interface bridge

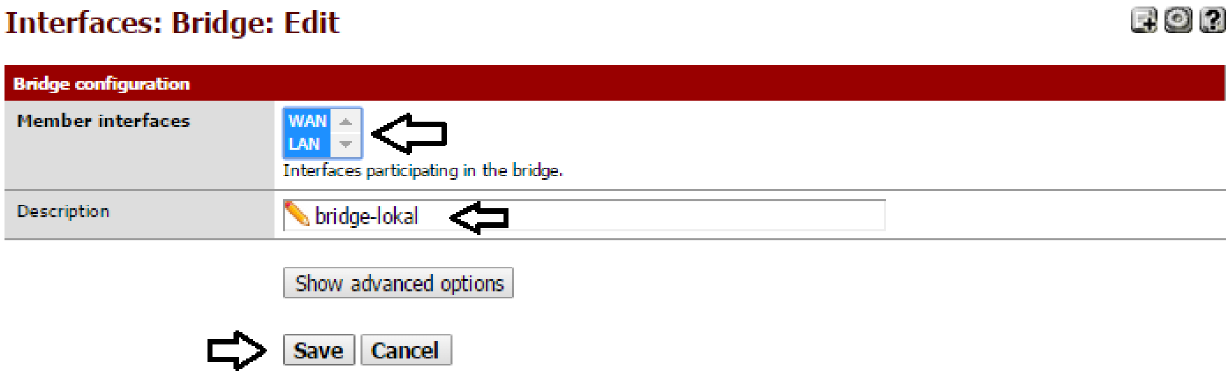


Interfaces: Bridge

Interface	Members	Description

Note:
Here you can configure bridging of interfaces.

Pilih member yang mau didaftarin ke bridge

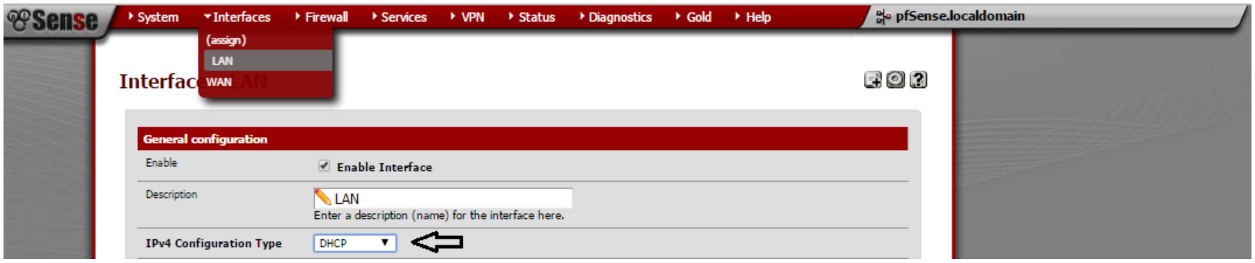


Interfaces: Bridge: Edit

Bridge configuration

Member interfaces	WAN LAN Interfaces participating in the bridge.
Description	bridge-lokal

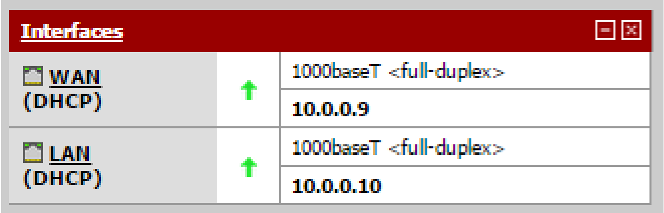
Aktifin dhcp di interface lan



General configuration

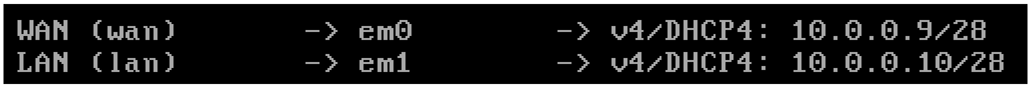
Enable	☑ Enable Interface
Description	LAN Enter a description (name) for the interface here.
IPv4 Configuration Type	DHCP

Berhasil membuat transparent firewall, tingall install paket paket sesuai kebutuhan.



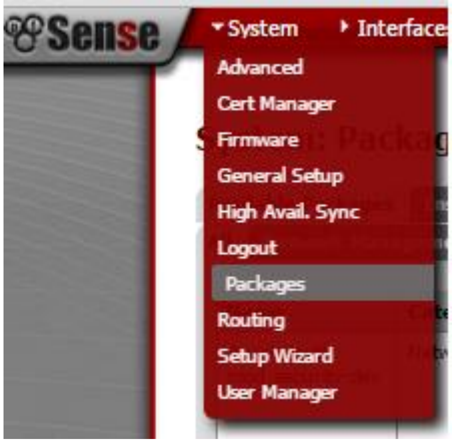
Interfaces

WAN (DHCP)	↑	1000baseT <full-duplex> 10.0.0.9
LAN (DHCP)	↑	1000baseT <full-duplex> 10.0.0.10

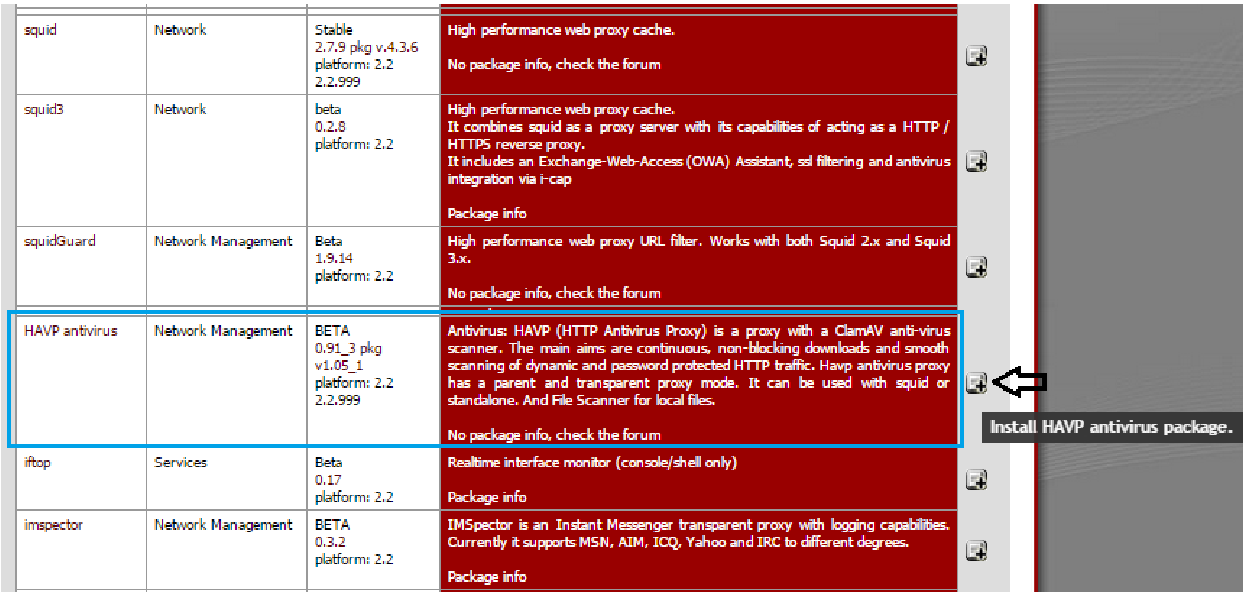


```
WAN (wan)        -> em0        -> v4/DHCP4: 10.0.0.9/28
LAN (lan)        -> em1        -> v4/DHCP4: 10.0.0.10/28
```

Menu buat install paket



Berapa contoh paket paket paket yang disedisediain. Jadi firewall ini bisa dibuat jadi proxy cache, proxy antivirus, IDS, Network monitor, Router dan lain lain.



squid	Network	Stable 2.7.9 pkg v.4.3.6 platform: 2.2 2.2.999	High performance web proxy cache. No package info, check the forum
squid3	Network	beta 0.2.8 platform: 2.2	High performance web proxy cache. It combines squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, ssl filtering and antivirus integration via i-cap Package info
squidGuard	Network Management	Beta 1.9.14 platform: 2.2	High performance web proxy URL filter. Works with both Squid 2.x and Squid 3.x. No package info, check the forum
HAVP antivirus	Network Management	BETA 0.91_3 pkg v1.05_1 platform: 2.2 2.2.999	Antivirus: HAVP (HTTP Antivirus Proxy) is a proxy with a ClamAV anti-virus scanner. The main aims are continuous, non-blocking downloads and smooth scanning of dynamic and password protected HTTP traffic. Havp antivirus proxy has a parent and transparent proxy mode. It can be used with squid or standalone. And File Scanner for local files. No package info, check the forum
iftop	Services	Beta 0.17 platform: 2.2	Realtime interface monitor (console/shell only) Package info
imspector	Network Management	BETA 0.3.2 platform: 2.2	IMSpector is an Instant Messenger transparent proxy with logging capabilities. Currently it supports MSN, AIM, ICQ, Yahoo and IRC to different degrees. Package info

Sampai ketemu di tutorial selanjutnya (nulis kaya gini biar kaya orang orang)

Sekian, Semoga bermanfaat.