Configurazione Firewall pfSense

Questa esercitazione riguarda la configurazione di un firewall **pfSense** in ambiente virtualizzato per gestire la segmentazione della rete e implementare politiche di sicurezza granulari.

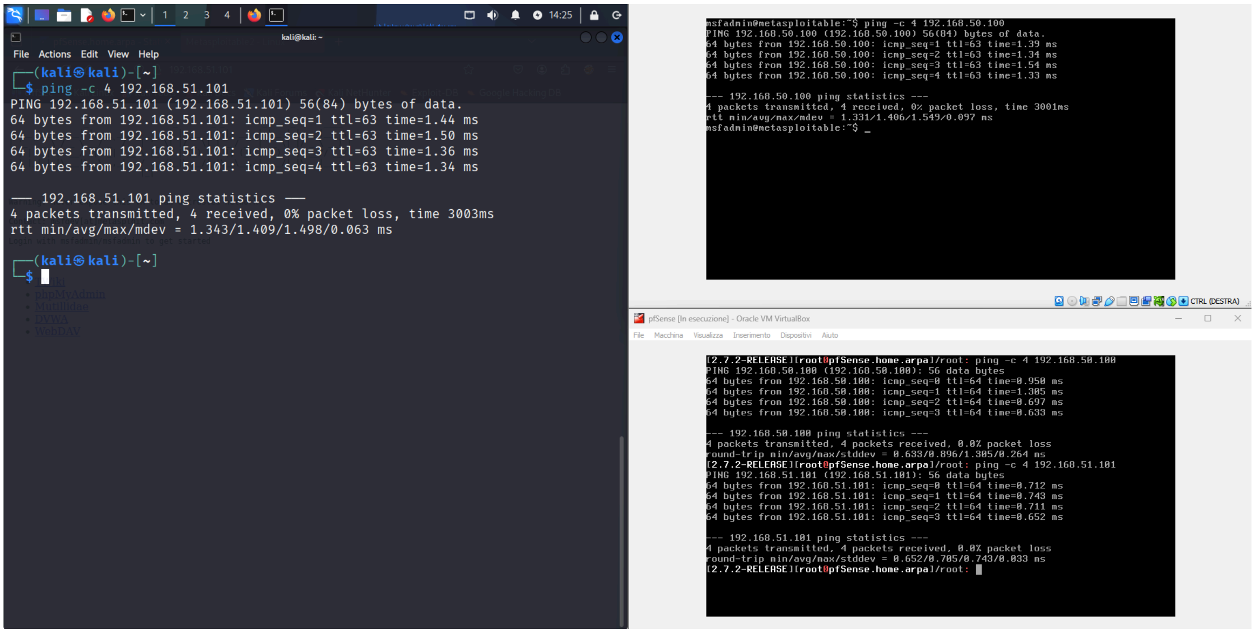
Architettura Implementata

L'infrastruttura è basata su un ambiente virtualizzato con **pfSense 2.7.2** come firewall centrale. La rete è strutturata su tre livelli:

- **WAN**: 10.2.0.15 (connessione verso Internet).
- **LAN**: 192.168.50.0/24 con pfSense come gateway (**192.168.50.1**).
    - **Kali Linux**: 192.168.50.100.
    - **Windows**: 192.168.50.102.
- **LAN2**: 192.168.51.0/24 con **pfSense** come gateway (**192.168.51.1**)
    - **Metasploitable2**: 192.168.51.101 (con **DVWA** installata)

Configurazione e Test di Connettività

Dopo aver configurato le interfacce di rete, sono stati eseguiti test di connettività per verificare il routing tra le subnet.



```
┌──(kali㉿kali)-[~]
└─$ ping -c 4 192.168.51.101
PING 192.168.51.101 (192.168.51.101) 56(84) bytes of data.
64 bytes from 192.168.51.101: icmp_seq=1 ttl=63 time=1.44 ms
64 bytes from 192.168.51.101: icmp_seq=2 ttl=63 time=1.50 ms
64 bytes from 192.168.51.101: icmp_seq=3 ttl=63 time=1.36 ms
64 bytes from 192.168.51.101: icmp_seq=4 ttl=63 time=1.34 ms

—— 192.168.51.101 ping statistics ——
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 1.343/1.409/1.498/0.063 ms

┌──(kali㉿kali)-[~]
└─$
```

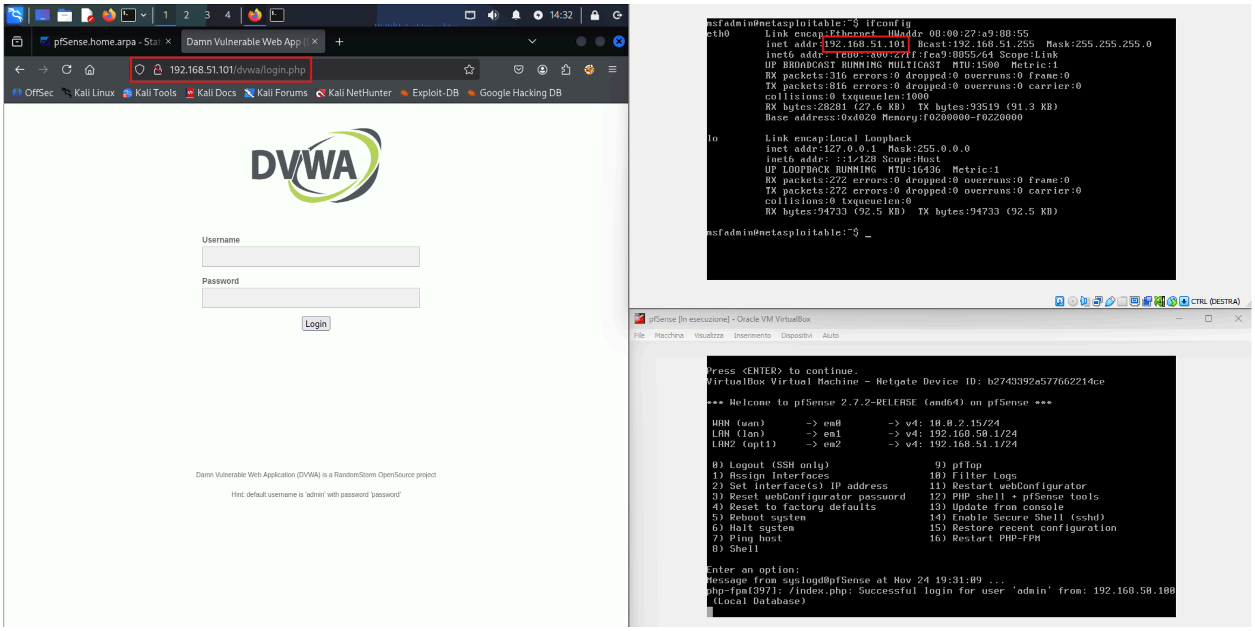
```
msfadmin@metasploitable:~$ ping -c 4 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
64 bytes from 192.168.50.100: icmp_seq=1 ttl=63 time=1.39 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=63 time=1.34 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=63 time=1.54 ms
64 bytes from 192.168.50.100: icmp_seq=4 ttl=63 time=1.33 ms

--- 192.168.50.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev = 1.331/1.406/1.549/0.097 ms
msfadmin@metasploitable:~$ _
```

```
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: ping -c 4 192.168.50.100
PING 192.168.50.100 (192.168.50.100): 56 data bytes
64 bytes from 192.168.50.100: icmp_seq=0 ttl=64 time=0.950 ms
64 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=1.305 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=0.697 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=0.633 ms

--- 192.168.50.100 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.633/0.896/1.305/0.264 ms
[2.7.2-RELEASE][root@pfSense.home.arpa]/root: ping -c 4 192.168.51.101
PING 192.168.51.101 (192.168.51.101): 56 data bytes
64 bytes from 192.168.51.101: icmp_seq=0 ttl=64 time=0.712 ms
64 bytes from 192.168.51.101: icmp_seq=1 ttl=64 time=0.743 ms
64 bytes from 192.168.51.101: icmp_seq=2 ttl=64 time=0.711 ms
64 bytes from 192.168.51.101: icmp_seq=3 ttl=64 time=0.652 ms

--- 192.168.51.101 ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.652/0.705/0.743/0.033 ms
[2.7.2-RELEASE][root@pfSense.home.arpa]/root:
```

kali@kali: ~
File Actions Edit View Help
14:25
pfSense [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
CTRL (DESTRA)

Inizialmente sono state applicate esclusivamente regole che consentano al traffico di rete di fluire liberamente e senza restrizioni tra le due subnet.

Tentando di accedere a http://192.168.51.101/dvwa/login.php da **Kali**, la connessione è andata a buon fine permettendoci di accedere alla subnet sulla **LAN2** e quindi alla **Damn Vulnerable Web Application** servita da Metasploitable.

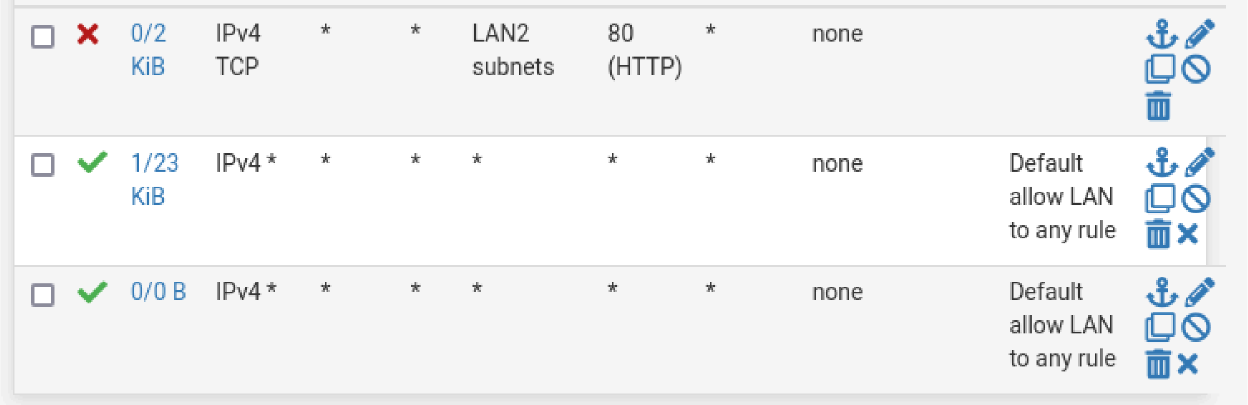


```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a9:88:55
          inet addr:192.168.51.101  Bcast:192.168.51.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea9:8855/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:316 errors:0 dropped:0 overruns:0 frame:0
          TX packets:816 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:28281 (27.6 KB)  TX bytes:93519 (91.3 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:272 errors:0 dropped:0 overruns:0 frame:0
          TX packets:272 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:94733 (92.5 KB)  TX bytes:94733 (92.5 KB)

msfadmin@metasploitable:~$ _
```

```
Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: b2743392a577662214ce

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

 WAN (wan)       -> em0        -> v4: 10.0.2.15/24
 LAN (lan)       -> em1        -> v4: 192.168.50.1/24
 LAN2 (opt1)     -> em2        -> v4: 192.168.51.1/24

 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:
Message from syslogd@pfSense at Nov 24 19:31:09 ...
php-fpm[397]: /index.php: Successful login for user 'admin' from: 192.168.50.100
 (Local Database)
```

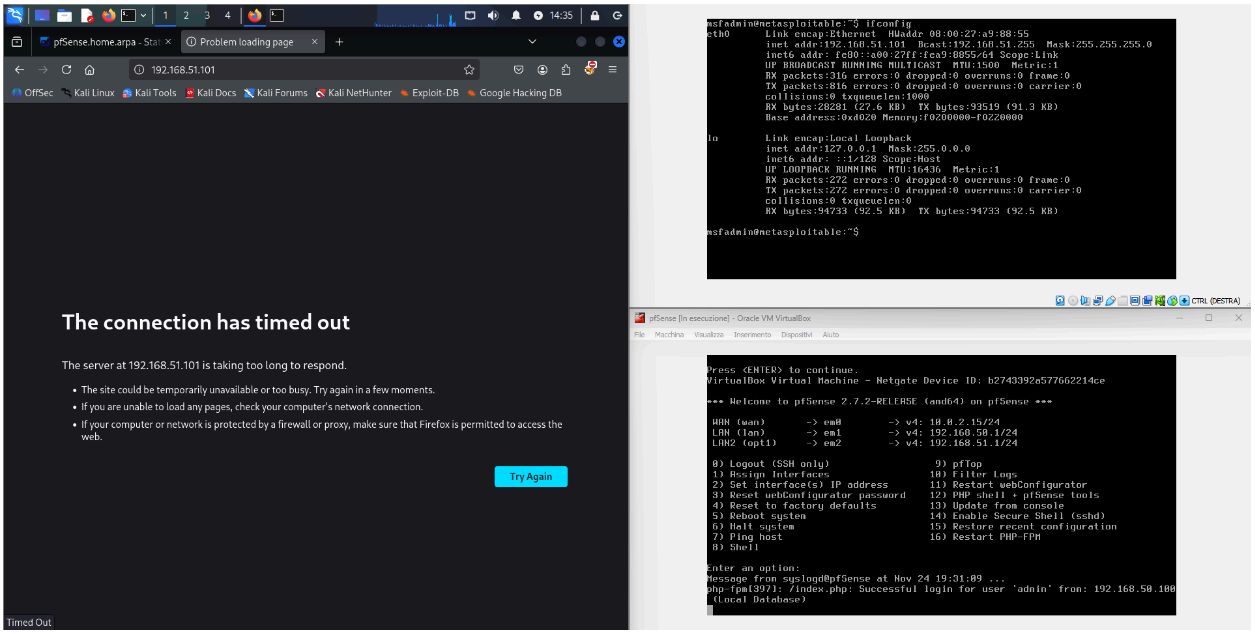
Implementazione blocco HTTP

È stata poi creata una regola firewall per bloccare il traffico **HTTP** verso **LAN2**:



□	✗	0/2 KiB	IPv4 TCP	*	*	LAN2 subnets	80 (HTTP)	*	none		
□	✓	1/23 KiB	IPv4 *	*	*	*	*	*	none	Default allow LAN to any rule	
□	✓	0/0 B	IPv4 *	*	*	*	*	*	none	Default allow LAN to any rule	

Tentando nuovamente l'accesso a http://192.168.51.101/dvwa/login.php, la connessione è andata in timeout come previsto.



The connection has timed out

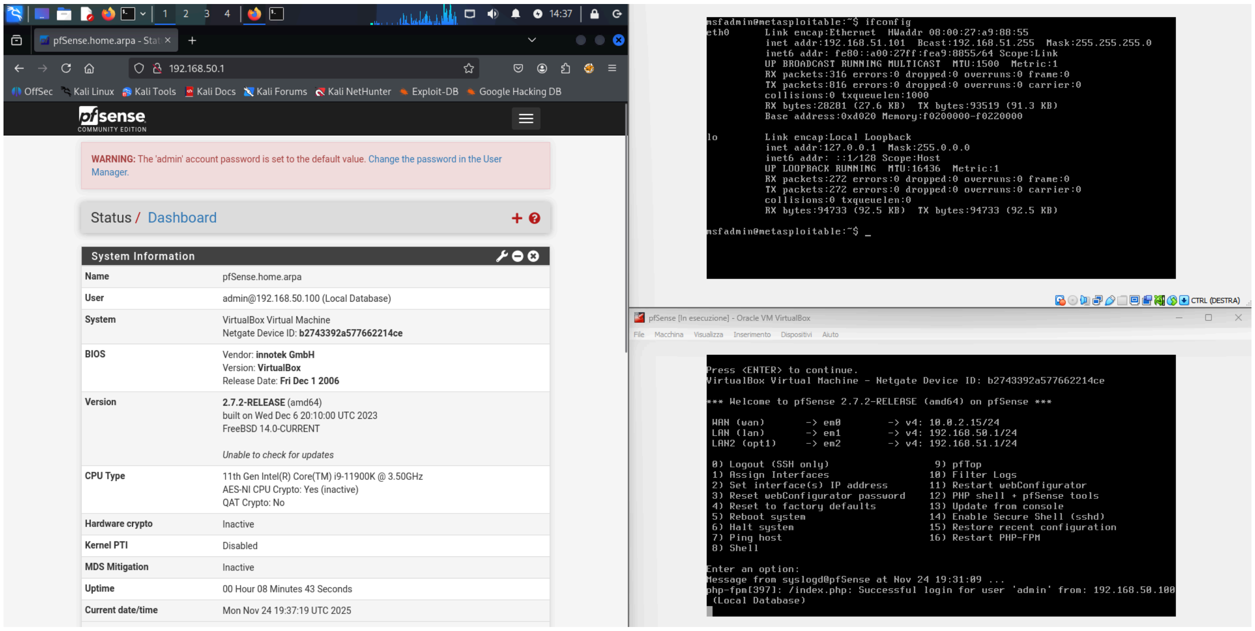
The server at 192.168.51.101 is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a9:88:55
          inet addr:192.168.51.101  Bcast:192.168.51.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea9:8855/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:316 errors:0 dropped:0 overruns:0 frame:0
          TX packets:816 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:28281 (27.6 KB)  TX bytes:93519 (91.3 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:272 errors:0 dropped:0 overruns:0 frame:0
          TX packets:272 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:94733 (92.5 KB)  TX bytes:94733 (92.5 KB)

msfadmin@metasploitable:~$
```

```
Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: b2743392a577662214ce

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

 WAN (wan)       -> em0        -> v4: 10.0.2.15/24
 LAN (lan)       -> em1        -> v4: 192.168.50.1/24
 LAN2 (opt1)     -> em2        -> v4: 192.168.51.1/24

 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:
Message from syslogd@pfSense at Nov 24 19:31:09 ...
php-fpm[397]: /index.php: Successful login for user 'admin' from: 192.168.50.100
 (Local Database)
```

Il ping da **Kali** a **Metasploitable** continua a funzionare, dimostrando che solo il traffico **HTTP** è bloccato. Oltretutto, l'accesso a `http://192.168.50.1` (dashboard di **pfSense**) funziona perfettamente, confermando che la regola blocca solo il traffico verso **LAN2** e non interferisce con altre comunicazioni **HTTP**.



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Status / Dashboard

System Information

Name	pfSense.home.arpa
User	admin@192.168.50.100 (Local Database)
System	VirtualBox Virtual Machine Netgate Device ID: **b2743392a577662214ce**
BIOS	Vendor: **innotek GmbH** Version: **VirtualBox** Release Date: **Fri Dec 1 2006**
Version	**2.7.2-RELEASE** (amd64) built on Wed Dec 6 20:10:00 UTC 2023 FreeBSD 14.0-CURRENT *Unable to check for updates*
CPU Type	11th Gen Intel(R) Core(TM) i9-11900K @ 3.50GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Disabled
MDS Mitigation	Inactive
Uptime	00 Hour 08 Minutes 43 Seconds
Current date/time	Mon Nov 24 19:37:19 UTC 2025

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a9:88:55
          inet addr:192.168.51.101  Bcast:192.168.51.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea9:8855/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:316 errors:0 dropped:0 overruns:0 frame:0
          TX packets:816 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:28281 (27.6 KB)  TX bytes:93519 (91.3 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:272 errors:0 dropped:0 overruns:0 frame:0
          TX packets:272 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:94733 (92.5 KB)  TX bytes:94733 (92.5 KB)

msfadmin@metasploitable:~$ _
```

```
Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: b2743392a577662214ce

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

 WAN (wan)       -> em0        -> v4: 10.0.2.15/24
 LAN (lan)       -> em1        -> v4: 192.168.50.1/24
 LAN2 (opt1)     -> em2        -> v4: 192.168.51.1/24

 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:
Message from syslogd@pfSense at Nov 24 19:31:09 ...
php-fpm[397]: /index.php: Successful login for user 'admin' from: 192.168.50.100
 (Local Database)
```