jamk.fi

LAB-04-ConfigurationsFile

Author Adam Pawełek

Teacher: Markku Vajaranta
Group: TTKS0700-3001
Jamk number: AA4917

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

1 Find suitable CIS Benchmarks for Windows and Linux versions in target environment (registration is needed for downloads).

1.1 Linux:

-> CIS Ubuntu Linux 20.04 LTS Benchmark

1.2 Windows

-> CIS Microsoft Windows 7 Workstation Benchmark v3.2.0 - End of LifeFile

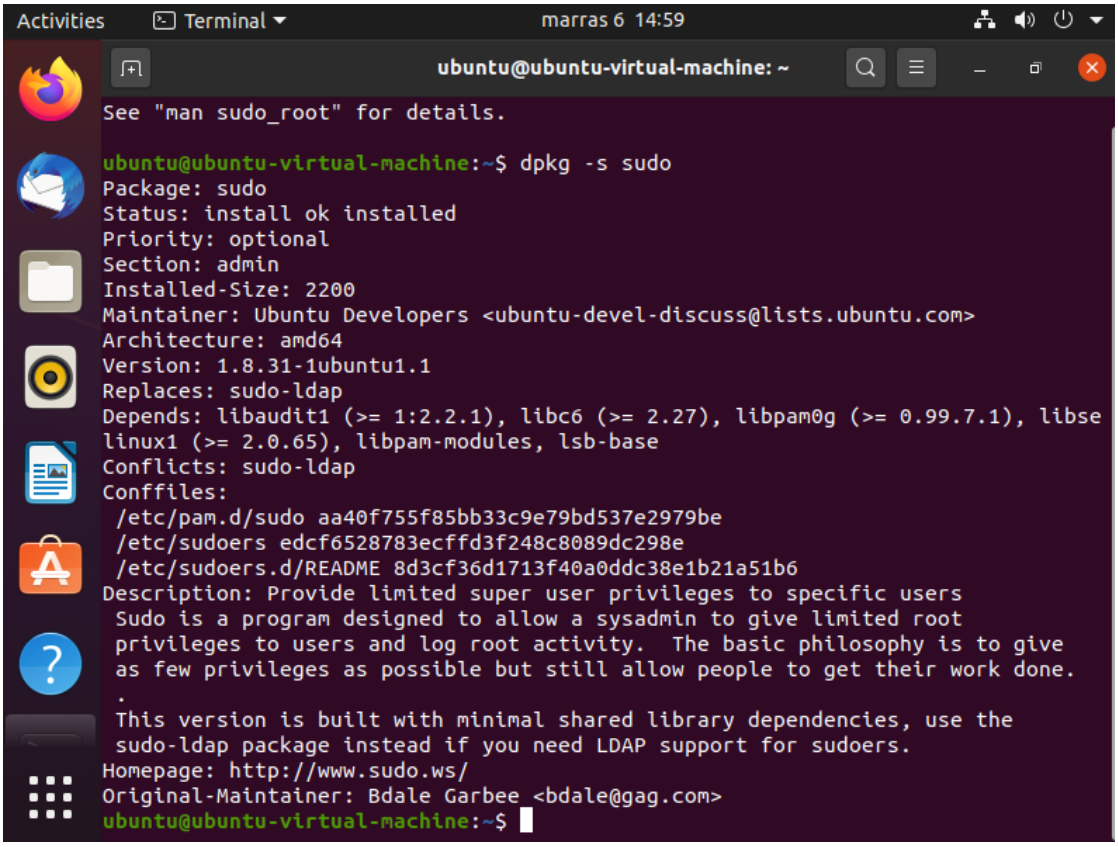
2 Select one area (second level header 1.1, 1.2, 2.1 etc.) from each guide and check the configurations

2.1 Configure sudo (1.3)

2.1.1 Ensure sudo is installed (Automated)

Audit:

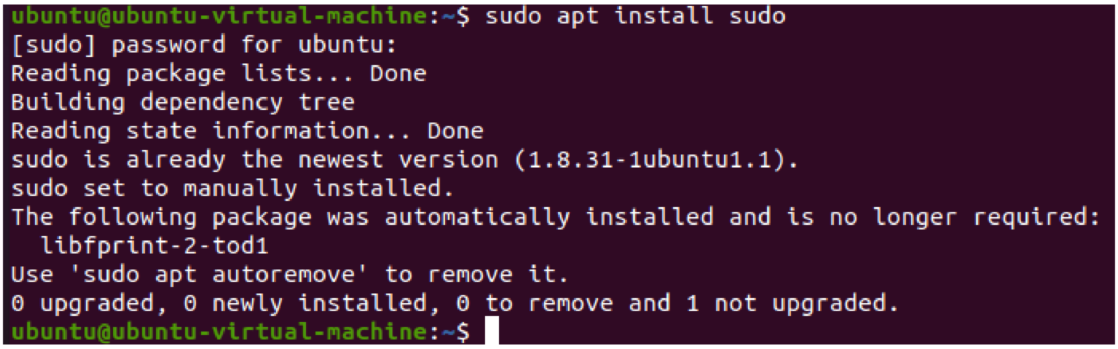
Verify that sudo in installed. Run the following command and inspect the output to confirm that sudo is installed:



```
See "man sudo_root" for details.

ubuntu@ubuntu-virtual-machine:~$ dpkg -s sudo
Package: sudo
Status: install ok installed
Priority: optional
Section: admin
Installed-Size: 2200
Maintainer: Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
Architecture: amd64
Version: 1.8.31-1ubuntu1.1
Replaces: sudo-ldap
Depends: libaudit1 (>= 1:2.2.1), libc6 (>= 2.27), libpam0g (>= 0.99.7.1), libse
linux1 (>= 2.0.65), libpam-modules, lsb-base
Conflicts: sudo-ldap
Conffiles:
 /etc/pam.d/sudo aa40f755f85bb33c9e79bd537e2979be
 /etc/sudoers edcf6528783ecffd3f248c8089dc298e
 /etc/sudoers.d/README 8d3cf36d1713f40a0ddc38e1b21a51b6
Description: Provide limited super user privileges to specific users
 Sudo is a program designed to allow a sysadmin to give limited root
 privileges to users and log root activity.  The basic philosophy is to give
 as few privileges as possible but still allow people to get their work done.
 .
 This version is built with minimal shared library dependencies, use the
 sudo-ldap package instead if you need LDAP support for sudoers.
Homepage: http://www.sudo.ws/
Original-Maintainer: Bdale Garbee <bdale@gag.com>
ubuntu@ubuntu-virtual-machine:~$
```

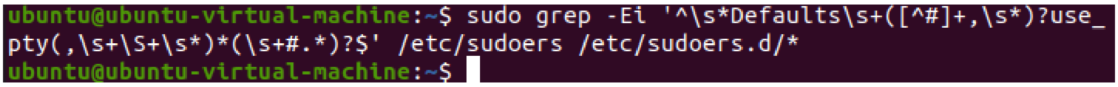
Remediation:
Install sudo using the following command.



```
ubuntu@ubuntu-virtual-machine:~$ sudo apt install sudo
[sudo] password for ubuntu:
Reading package lists... Done
Building dependency tree
Reading state information... Done
sudo is already the newest version (1.8.31-1ubuntu1.1).
sudo set to manually installed.
The following package was automatically installed and is no longer required:
  libfprint-2-tod1
Use 'sudo apt autoremove' to remove it.
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
ubuntu@ubuntu-virtual-machine:~$
```

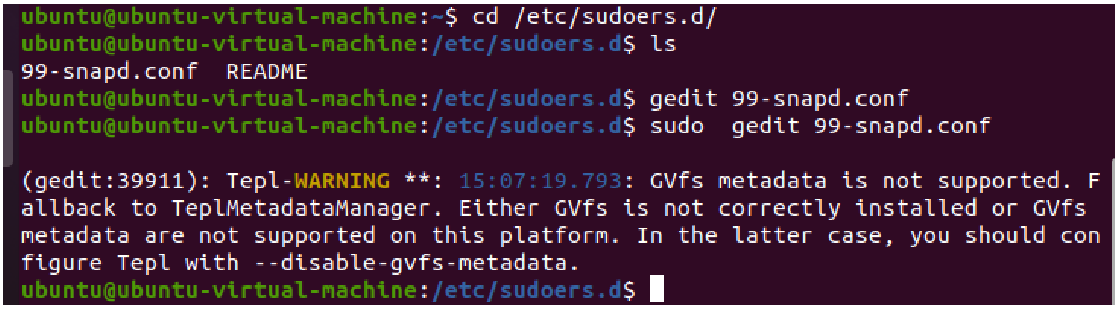
2.1.2 Ensure sudo commands use pty (Automated)

Audit:
Verify that sudo can only run other commands from a pseudo-pty Run the following



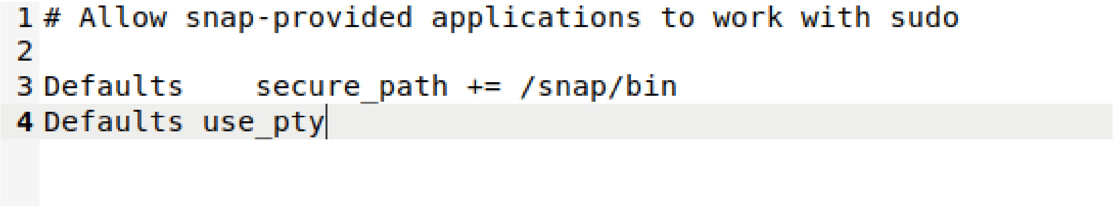
```
ubuntu@ubuntu-virtual-machine:~$ sudo grep -Ei '^\s*Defaults\s+([^#]+,\s*)?use_
pty(,\s+\S+\s*)*(\s+#.*)?$' /etc/sudoers /etc/sudoers.d/*
ubuntu@ubuntu-virtual-machine:~$
```

Remediation:
Edit the file `/etc/sudoers` or a file in `/etc/sudoers.d/` with visudo -f and add the following line:



```
ubuntu@ubuntu-virtual-machine:~$ cd /etc/sudoers.d/
ubuntu@ubuntu-virtual-machine:/etc/sudoers.d$ ls
99-snapd.conf  README
ubuntu@ubuntu-virtual-machine:/etc/sudoers.d$ gedit 99-snapd.conf
ubuntu@ubuntu-virtual-machine:/etc/sudoers.d$ sudo  gedit 99-snapd.conf

(gedit:39911): Tepl-WARNING **: 15:07:19.793: GVfs metadata is not supported. F
allback to TeplMetadataManager. Either GVfs is not correctly installed or GVfs
metadata are not supported on this platform. In the latter case, you should con
figure Tepl with --disable-gvfs-metadata.
ubuntu@ubuntu-virtual-machine:/etc/sudoers.d$
```

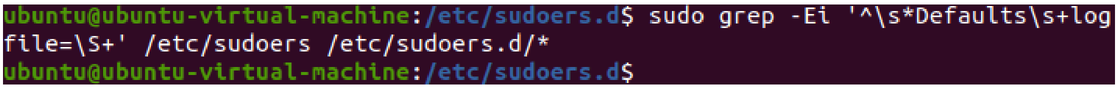


```
# Allow snap-provided applications to work with sudo

Defaults     secure_path += /snap/bin
Defaults use_pty
```

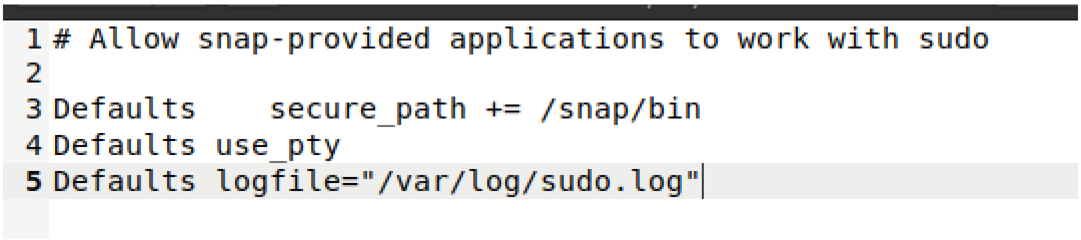
2.1.3 Ensure sudo log file exists (Automated)

Audit:
Verify that sudo has a custom log file configured Run the following command:



```
ubuntu@ubuntu-virtual-machine:/etc/sudoers.d$ sudo grep -Ei '^\s*Defaults\s+log
file=\S+' /etc/sudoers /etc/sudoers.d/*
ubuntu@ubuntu-virtual-machine:/etc/sudoers.d$
```

Remediation:
Edit the file `/etc/sudoers` or a file in `/etc/sudoers.d/` with visudo -f and add the following line: and add the following line:



```
# Allow snap-provided applications to work with sudo

Defaults     secure_path += /snap/bin
Defaults use_pty
Defaults logfile="/var/log/sudo.log"
```

2.2 Notice that there are LEVEL-1 and LEVEL-2 –settings. Find out what these LEVELS mean

Source -> CIS Ubuntu Linux 20.04 LTS Benchmark

Profile Definitions

The following configuration profiles are defined by this Benchmark:

□ **Level 1 - Server**

Items in this profile intend to:

o be practical and prudent;
o provide a clear security benefit; and
o not inhibit the utility of the technology beyond acceptable means.

This profile is intended for servers.

□ **Level 2 - Server**

This profile extends the "Level 1 - Server" profile. Items in this profile exhibit one or more of the following characteristics:

o are intended for environments or use cases where security is paramount.
o acts as defense in depth measure.
o may negatively inhibit the utility or performance of the technology.

This profile is intended for servers.

□ **Level 1 - Workstation**

Items in this profile intend to:

o be practical and prudent;
o provide a clear security benefit; and
o not inhibit the utility of the technology beyond acceptable means.

This profile is intended for workstations.

□ **Level 2 - Workstation**

This profile extends the "Level 1 - Workstation" profile. Items in this profile exhibit one or more of the following characteristics:

o are intended for environments or use cases where security is paramount.
o acts as defense in depth measure.
o may negatively inhibit the utility or performance of the technology.

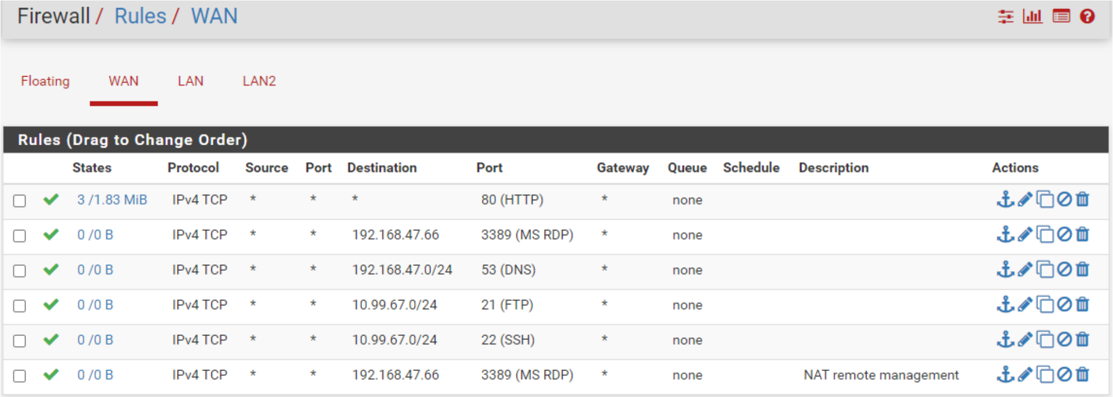
This profile is intended for workstations.

3 Audit pfsense –firewall RULES using following checklist

->https://www.sans.org/media/score/checklists/FirewallChecklist.pdf

(Select applicable parts from the checklist)

3.1 Review the rulesets

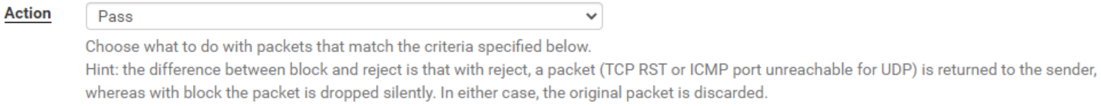


Rules (Drag to Change Order)

		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓	3 /1.83 MiB	IPv4 TCP	*	*	*	80 (HTTP)	*	none			⚓✏⧉⊘🗑
□	✓	0 /0 B	IPv4 TCP	*	*	192.168.47.66	3389 (MS RDP)	*	none			⚓✏⧉⊘🗑
□	✓	0 /0 B	IPv4 TCP	*	*	192.168.47.0/24	53 (DNS)	*	none			⚓✏⧉⊘🗑
□	✓	0 /0 B	IPv4 TCP	*	*	10.99.67.0/24	21 (FTP)	*	none			⚓✏⧉⊘🗑
□	✓	0 /0 B	IPv4 TCP	*	*	10.99.67.0/24	22 (SSH)	*	none			⚓✏⧉⊘🗑
□	✓	0 /0 B	IPv4 TCP	*	*	192.168.47.66	3389 (MS RDP)	*	none		NAT remote management	⚓✏⧉⊘🗑

-This Firewall have 6 rules all are for IPv4 TCP protocol in WAN, LAN2 have only rules in IPv4 TCP/UDP, LAN1 have one rule in IPv6 and IPv4.

-The rules are made for ports (80, 3389, 53,21,22).



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.

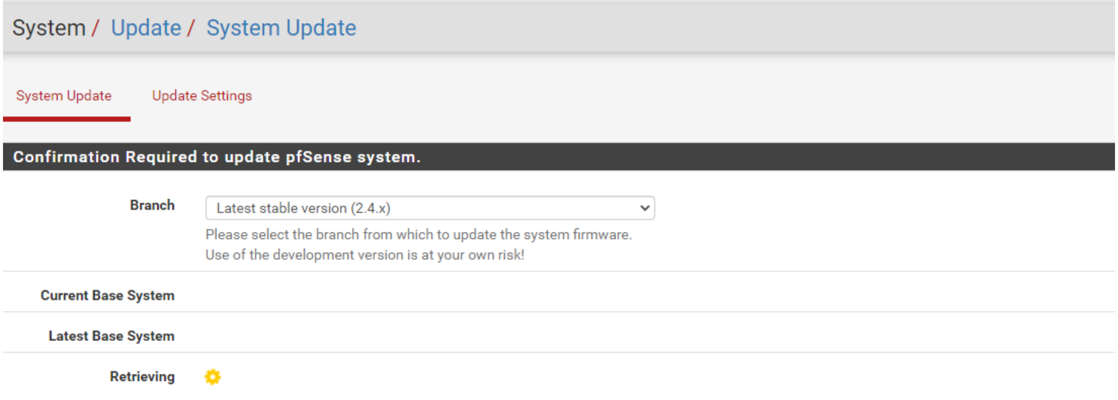
-All rules have Pass action

-Don’t have anti-spoofing filters

-Don’t have any deny and allerts

3.2 Application based firewall

This FireWall don’t have any rules which blocks malicious sites.



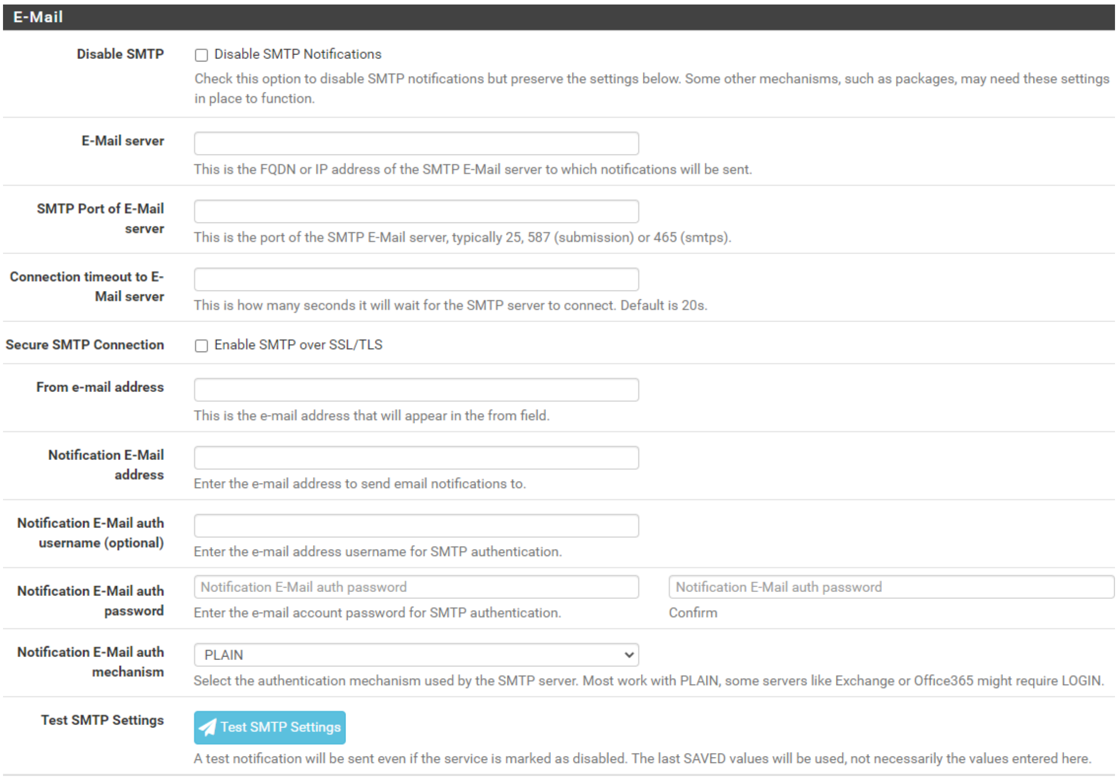
System / Update / System Update

System Update | Update Settings

Confirmation Required to update pfSense system.

Branch	Latest stable version (2.4.x) Please select the branch from which to update the system firmware. Use of the development version is at your own risk!
Current Base System	
Latest Base System	
Retrieving	

Firewall have option to update sytem and settings. There are no set SMTP settings in this Firewall.



E-Mail

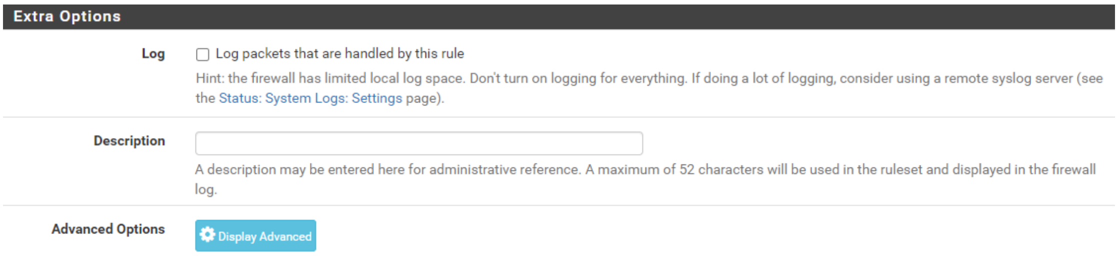
Disable SMTP	□ Disable SMTP Notifications Check this option to disable SMTP notifications but preserve the settings below. Some other mechanisms, such as packages, may need these settings in place to function.
E-Mail server	This is the FQDN or IP address of the SMTP E-Mail server to which notifications will be sent.
SMTP Port of E-Mail server	This is the port of the SMTP E-Mail server, typically 25, 587 (submission) or 465 (smtps).
Connection timeout to E-Mail server	This is how many seconds it will wait for the SMTP server to connect. Default is 20s.
Secure SMTP Connection	□ Enable SMTP over SSL/TLS
From e-mail address	This is the e-mail address that will appear in the from field.
Notification E-Mail address	Enter the e-mail address to send email notifications to.
Notification E-Mail auth username (optional)	Enter the e-mail address username for SMTP authentication.
Notification E-Mail auth password	Notification E-Mail auth password Enter the e-mail account password for SMTP authentication. Notification E-Mail auth password Confirm
Notification E-Mail auth mechanism	PLAIN Select the authentication mechanism used by the SMTP server. Most work with PLAIN, some servers like Exchange or Office365 might require LOGIN.
Test SMTP Settings	Test SMTP Settings A test notification will be sent even if the service is marked as disabled. The last SAVED values will be used, not necessarily the values entered here.

3.3 Stateful inspection

I didn’t find any timeouts rules. In Wan rules they don’t have any source filters but Firewall have Destination filter. In LAN network it have LAN net filter and in destination it have Lan Adress filter. LAN2 don’t have any destination and source filter.

3.4 Logging

In all rules Log is disabled.



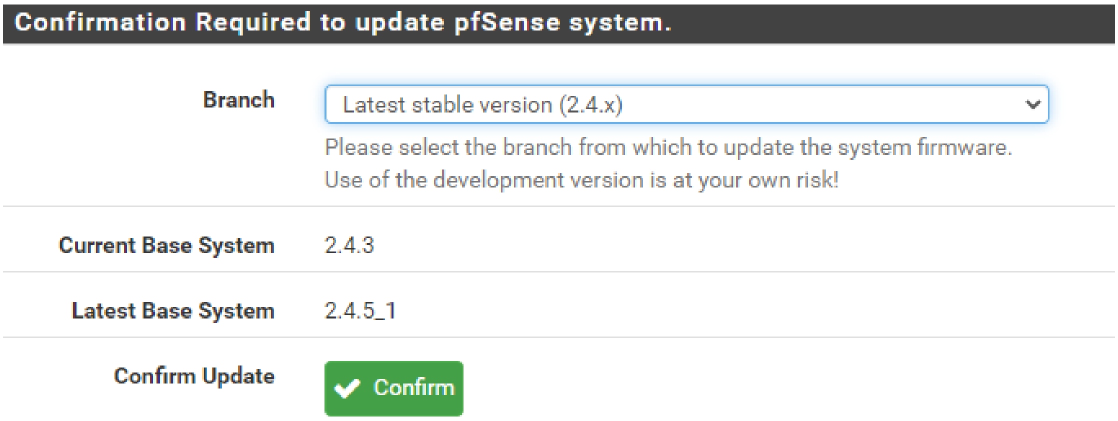
Extra Options

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

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

Advanced Options

3.5 Patches and updates



Confirmation Required to update pfSense system.

Branch: Latest stable version (2.4.x)
Please select the branch from which to update the system firmware.
Use of the development version is at your own risk!

Current Base System: 2.4.3

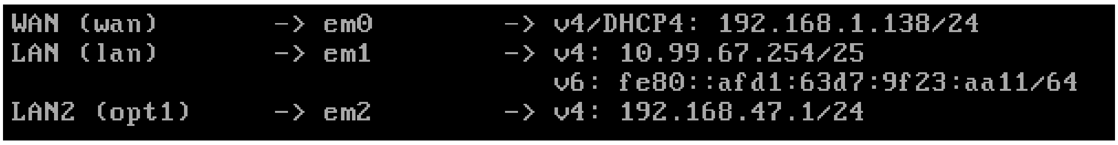
Latest Base System: 2.4.5_1

Confirm Update

Firewall system should be updated beceouse Current Base System is 2.4.3 but the Latest Base System is 2.4.5_1.

3.6 Location – DMZ

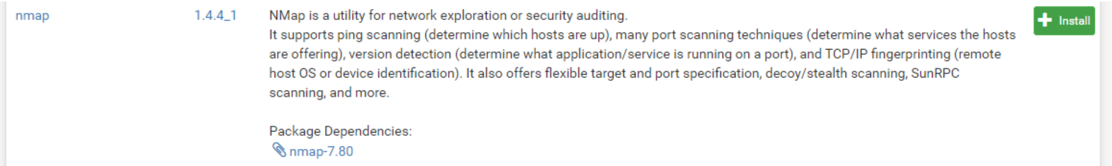
There are 3 FireWalls one for WAN, one for LAN and one for LAN2.



```
WAN (wan)        -> em0        -> v4/DHCP4: 192.168.1.138/24
LAN (lan)        -> em1        -> v4: 10.99.67.254/25
                                  v6: fe80::afd1:63d7:9f23:aa11/64
LAN2 (opt1)      -> em2        -> v4: 192.168.47.1/24
```

3.7 Vulnerability assessments/ Testing

Nmap package is not instaled.



nmap 1.4.4_1

NMap is a utility for network exploration or security auditing.
It supports ping scanning (determine which hosts are up), many port scanning techniques (determine what services the hosts are offering), version detection (determine what application/service is running on a port), and TCP/IP fingerprinting (remote host OS or device identification). It also offers flexible target and port specification, decoy/stealth scanning, SunRPC scanning, and more.

Package Dependencies:
nmap-7.80

3.8 Compliance with security policy

I don’t know whcich organisation rulset I should compare Firewall too.

3.9 Ensure that the following spoofed, private (RFC 1918) and illegal addresses are blocked

In Firewall rules there are no illegal adress blocked.

3.10 Ensure that loose source routing and strict source routing (lsrsr & ssrr) are blocked and logged by the firewall.

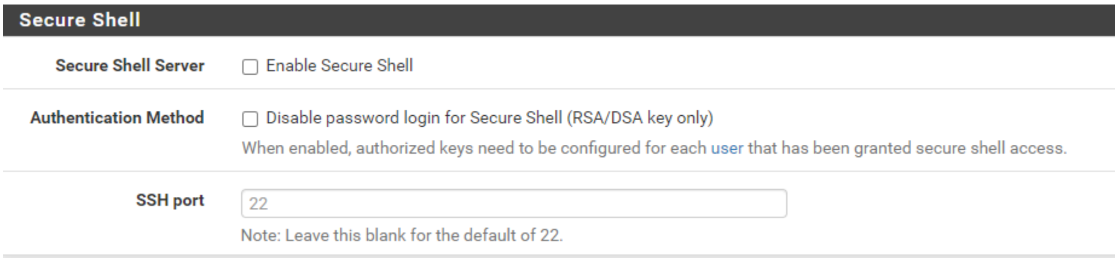
I could acces to lan network witch my another virtual machine (which was not included in Data Security Virtual Machines without any problems. Firewall give virtual machine ip and acess to lan without any changes in Firewall. (So source routing is not blocked)

3.11 Port restrictions The following ports should blocked: Service Port.

Ports allowed to traffic (80, 3389,53,21,22).

DNS zone Transffer, Port Type TCP, Port number 53 should be blocked but is open.
FTP TCP 21 – should be blocked
SSH TCP 22 – should be blocked

3.12 Remote access



Secure Shell

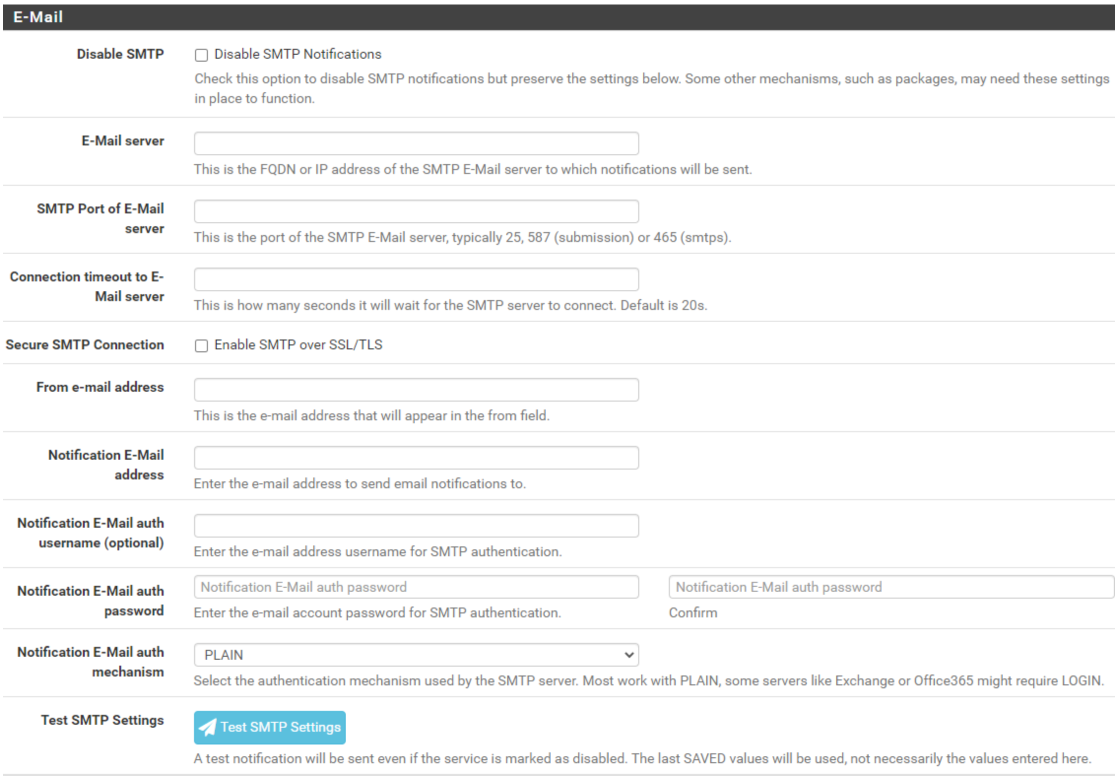
Secure Shell Server	□ Enable Secure Shell
Authentication Method	□ Disable password login for Secure Shell (RSA/DSA key only) When enabled, authorized keys need to be configured for each user that has been granted secure shell access.
SSH port	22 Note: Leave this blank for the default of 22.

Secure Shell is disabled.

3.13 File Transfers

We don’t have file server

3.14 Mail Traffic



E-Mail

Disable SMTP	□ Disable SMTP Notifications Check this option to disable SMTP notifications but preserve the settings below. Some other mechanisms, such as packages, may need these settings in place to function.
E-Mail server	This is the FQDN or IP address of the SMTP E-Mail server to which notifications will be sent.
SMTP Port of E-Mail server	This is the port of the SMTP E-Mail server, typically 25, 587 (submission) or 465 (smtps).
Connection timeout to E-Mail server	This is how many seconds it will wait for the SMTP server to connect. Default is 20s.
Secure SMTP Connection	□ Enable SMTP over SSL/TLS
From e-mail address	This is the e-mail address that will appear in the from field.
Notification E-Mail address	Enter the e-mail address to send email notifications to.
Notification E-Mail auth username (optional)	Enter the e-mail address username for SMTP authentication.
Notification E-Mail auth password	Notification E-Mail auth password Enter the e-mail account password for SMTP authentication. Notification E-Mail auth password Confirm
Notification E-Mail auth mechanism	PLAIN Select the authentication mechanism used by the SMTP server. Most work with PLAIN, some servers like Exchange or Office365 might require LOGIN.
Test SMTP Settings	Test SMTP Settings A test notification will be sent even if the service is marked as disabled. The last SAVED values will be used, not necessarily the values entered here.

There is no e-mail server.

3.15 ICMP (ICMP 8, 11, 3)

There are no rules blocking ICMP echo request.

3.16 IP Readdressing/IP Masquerading

Firewall have Readdressing (we could see that in exercise 2)

3.17 Zone Transfers

In subsection 11 we coudl see that DNS zone Transffer, Port Type TCP, Port number 53 should be blocked but is open.

3.18 Egress Filtering

There is no log rules in this Firewall.

3.19 Critical servers

We don’t have any organizational requirements.

3.20 Personal firewalls

Laptop users have appropriate training regarding the threats.

3.21 Distributed firewalls

This conditions are failed.

3.22 Stealth Firewalls

User and password are default.

3.23 Ensure that ACK bit monitoring

----------------- ?

3.24 Continued availability of Firewalls

There is a hot standby for the primary firewall.