

Partie 1.0

On utilise VMware Workstation 17 Pro pour la virtualisation.

On ajoute 3 cartes réseaux en LAN segment (réseau interne) sur lequel on attribue les noms DMZ, LAN1, LAN2 et WAN. Et une carte en NAT pour l'accès à internet.

On attribue 35 Gb pour Pfsense en espace disque et 20 Gb pour les machines Debian. On attribue aussi 2 cpu pour chacun.

On attribue 2Gb de RAM pour Pfsense et 512Mb pour les machines Debian.

On décompresse le fichier Pfsense.tar.gz et on charge l'ISO dans VMWare Workstation.

Partie 1.1

On configure une machine Debian, on se contente d'installer un serveur ssh et le grub sur la partition racine. Il s'agit d'un bastion qui va nous permettre de nous connecter à Pfsense en web.

On peut utiliser awesome pour l'interface graphique ou GNOME (si on a plus de ressources)

On aura une 3ème VM sous Debian pour l'utiliser comme serveur avec du hardening.

Partie 1.2

On installe Pfsense et on coche l'option non pour la configuration avancé.

On sélectionne shell et on change le clavier en français.

Partie 1.3

Pour passer le clavier en Français dans pfSense.

Dans le menu taper 8 pour accéder au Shell

Ensuite kbdmap

Sélectionner French ISO-8859-1 (accent keys)

Source : <https://www.linuxaga.com/linux/divers/17-passer-le-clavier-de-pfsense-en-francais>

Partie 1.4

On désactive pfsense avec `pfctl -d`

On se connecte à l'interface web avec admin et pfsense

Voici la carte local LAN 192.168.1.100

On modifie pour que ce soit la passerelle du réseau DMZ 192.168.100.254

192.168.100.254 DMZ - VM1 - Pfsense - Pfsense

Partie 1.5

On configure *mntui* nmtui pour le bastion
192.168.100.240

```
systemctl restart networking
systemctl restart NetworkManager
dhclient -r eth0
```

Partie 1.6

On modifie la plage d'adresse du serveur DHCP pour la DMZ
192.168.100.50 192.168.100.100

Partie 1.7

On modifie l'adresse et les noms des interfaces LAN devient DMZ, OP1 et OP2 deviennent LAN1 et LAN2
On oublie pas d'activer les interfaces.
On configure le masque en /24 pour les interfaces LAN1 et LAN2

On configure :
192.168.101.254 LAN1 - VM1 - Pfsense - Pfsense
192.168.102.254 LAN2 - VM1 - Pfsense - Pfsense

Partie 1.8

On se rend sur Firewall Rules DMZ on laisse tel quel
On se rend sur LAN1
Tout protocole
Description allow all et log packet à vrai
Puis on fait la même chose pour LAN2
Enfin on fait apply changes.

Partie 1.9

On configure le dhcp pour les interfaces LAN1 et LAN2
Du .50 au .100

Partie 2.1

On configure le server à hardening on réinstalle Debian
Ou bien on clone la VM2 en régénérant les addresses MAC.

Cette VM3 sera sur le réseau DMZ tandis que la VM2 sera sur le réseau LAN1
On conserve l'interface NAT pour l'accès à internet.
De préférence avec un disque en mode LVM pour l'instant non chiffré.

Partie 2.2

On se connecte avec l'utilisateur lab

```
nano /etc/sudoers.d/vagrant
vagrant ALL=(ALL:ALL) NOPASSWD: ALL
```

Afin d'éviter de faire scanner les ports par défaut on change l port 22 en 2222 dans */etc/ssh/sshd_config* On complique la tâche aux bots.

S'authentifier avec une clé ssh

ssh-keygen avec une passphrase
On copie le fichier *id_rsa.pub* dans le fichier *authorized_keys*

Partie 2.3

On bloque le tmp avec noexec

```
nano /etc/fstab
tmpfs /tmp tmpfs defaults,nodev,nosuid,noexec 0 0
mount -a
sudo /tmp/script.sh
```

Partie 2.4

On installe sudo sur la machine Debian avec la commande

```
apt-get update -y && apt-get install sudo -y
```

On crée un script bash pour configurer notre machine Debian avec du hardening (de la protection avancée).

On configure le domaine en *efrei.local*

On configure .254

```
apt-get update -y && apt-get install awesome xinit xterm -y
```

On installe aussi firefox

```
apt-get update -y && apt-get install firefox-esr -y
```

Partie 2.5

On change les règles de firewall du DMZ que 53, 80, 443 en sortie

On utilise portquiz.net:8080 pour tester les ports ouverts. notamment ici le port 8080

https://192.168.116.133/pkg_mgr.php -> vm tools et squid que l'on installe et on active le service squid proxy qui est un web proxy et de gérer du cache mais aussi de filtrer des URL.

Il va dans services -> squid proxy

On va dans services -> squid proxy -> local cache et on sauvegarde pour éviter d'avoir une erreur.

On active avec enable squid proxy et enable access logging

On active les logs

On va dans services -> squid proxy -> ACLs -> blacklist

neverssl.com

*.neverssl.com

openai.com

*.openai.com

On peut supprimer la version de squid : avec suppress squid proxy dans les headers car on évite de donner des informations sur le serveur. Pour des vulnérabilités potentiels.

neverssl.com dans la liste des blacklist du proxy

neverssl.com est un site qui permet de tester les sites en http sans passer par du https.

On va dans acl

Partie 2.6 :

On va dans System -> cert manager

cert manager

add

PROXY CA

Create an internal certificate authority

Ajout dans le trust store

sha256

Durée 365 J

CN : EFREI-CA

COUNTRY code : FR

STATE: FRANCE

CITY: PARIS

ORGANIZATION : EFREI

OU: LAB

Partie 2.7

Dans service -> squid proxy server

ssl man in the middle filtering

enable ssl filtering

CA -> proxy ca

Il faut whitelister les sites du gouvernement, les sites bancaires.

visible hostname : EFREI PROXY

Administrator's Email : service.informatique@efrei.local

Partie 2.8

installer squidguard à l'aide du package manager. Ensuite on fait apply

on ajoute du logging

Partie 2.9

On ajoute

https://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz

On va dans l'onglet blacklist

-> download

-> common acl

- Do not allow IP-Addresses in URL true
- dans target rules list

adult dating drogue gambling phishing publicite vpn à bloquer

```
sudo apt-get install -y open-vm-tools-desktop
```

Partie 3.1

On crée une nouvelle VM Debian sans interface graphique

srv-web1

On va effectuer du hardening sur cette machine (aussi sur cette VM)

On effectue un spliceall dans MITM mode pour ssl man in the middle filtering

Partie 3.1.2

On va dans package -> proxy server:cache

Services -> Squid proxy Proxy Server -> Cache Management -> Local Cache

On clique sur le bouton Clear Disk Cache NOW

Et on modifie le SSL MITM MODE en splice all à nouveau

Puis il passe par l'EFREI

Partie 3.1.3

Installation de lightsquid

Partie 3.2

On copie le certificat :

```
sudo cp efrei-ca.crt /usr/local/share/ca-certificates/.
```

```
sudo update-ca-certificates
sudo apt install -y lynx sudo lnav
sudo apt install -y apache2 nmap openssl
```

```
nano /etc/sudoers.d/vagrant
vagrant ALL=(ALL:ALL) NOPASSWD: ALL
```

Partie 3.3

On va dans system Certmanager -> CA -> add -> add this to trust store

WEB-EFREI -- ST=FRANCE, OU=LAB, O=EFREI, L=PARIS, CN=WEB-SERVERs, C=FR

Pour éviter que le certificat soit fuité ou usurpé il existe un délai d'expiration afin de garantir l'intégrité.

Au minimum 1 an au maximum 2 ans. Mais surtout il peuvent usurpés l'autorité de certifications.

srv1.efrei.local

Partie 3.4

On va dans system Certmanager -> Certificates ->

server certificate

descriptive name : SRV-WEB1

365J

CN srv1.efrei.local

FR

France

Paris

efrei

lab

type : server certificate

fqdn or hostname : srv1.efrei.local

On télécharge la clé privée et le certificat.

Partie 3.5

```
systemctl enable --now apache2
/etc/apache2/sites-available/000-default.conf
/etc/apache2/sites-available/default-ssl.conf
```

```
a2enmod ssl
a2ensite default-ssl.conf
```

```
systemctl restart apache2
nano /etc/ssl/certs/ssl-cert-efrei-srv1.pem
```

Dans le fichier efrei-ca.crt on greffe tout le contenu de PROXY-CA.crt télécharger précédemment dans le certmanager :

```
nano efrei-ca.crt
```

On le copie (efrei-ca.crt) et on colle dans le dossier /usr/local/share/ca-certificates/.

Ensuite on update avec `sudo update-ca-certificates`

On utilise openssl

```
/etc/ssl/private/ssl-cert-efrei-srv1.key
```

```
nmap -p 7443 --script ssl-cert 192.168.100.53
```

```
netstat -tunlp
```

Partie 3.6

On ajoute dans DNS resolver : host srv1
domain efrei.local
ip address 192.168.100.51

Dans System -> services -> DNS resolver
enable dns resolver true

Partie 3.7

https://192.168.116.133/pkg_mgr_install.php

On recherche snort à installer depuis le package manager

On va dans services -> snort

zero trust network et zero trust a devoir montrer pate blanche avec un sso ou un portail captif.

sso avec okata ou keycloak

wallix

open-bastion

teleport
clés api de snort

Partie 3.8

tempmail
<https://temp-mail.org/fr/>

rahox84579@duscore.com
42b45af55b7bcdd9b92d1cefde35b81177bb33b 0

soxet89719@pgobo.com

enable snort vrt pattern de rules

enable snort gplv2

enable **et open** emerging threats rules développé par Proofpoint (américain)

à valider :

- Hide Deprecated Rules Categories :
- Click to clear all blocked hosts added by Snort when removing the package.
Update Interval : 1 day : règles update toutes les 24H
Remove Blocked Hosts Interval : 12 hours : serait débloquent après 12H éviter de surcharger la base de blocage.

Partie 3.9

Il faut mettre à jour : https://192.168.116.133/snort/snort_download_updates.php

On active le service pour les WAN et DMZ
interface WAN
envoie Send Alerts to System Log

On active les alertes suivantes : Dans Services -> Snort -> Interface Settings -> DMZ -> Categories
p2p scan shellcode smtp sql snmp telnet tor trojan user-agents exploit dshield java exploit-kit

Partie 3.10

On peut utiliser un outil de reconnaissance des failles web avec nikto

Partie 4.1

On vérifie les alerts snorts dans https://192.168.116.133/snort/snort_alerts.php?instance=0

Partie 4.2

- Block Offenders : Checking this option will automatically block hosts that generate a Snort alert.
- Changer IPS Mode à legacy mode pour blocking mode.

Partie 4.3

status -> system logs -> system -> general

```
sudo nmap -A -vvv 192.168.100.0/24
```

Partie 4.4

On crée une nouvelle VM pour Zabbix avec 30Gb de Stockage.

shodan.io et sansys sont des outils pour scanner les vulnérabilités publiques.

Partie 4.5

```
sudo apt update -y
wget https://repo.zabbix.com/zabbix/6.4/debian/pool/main/z/zabbix-release/zabbix-
release_6.4-1+debian11_all.deb
dpkg -i zabbix-release_6.4-1+debian11_all.deb
apt update
apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-
sql-scripts zabbix-agent
```

```
sudo apt install -y mariadb-server

mysql -uroot -p
password
mysql> create database zabbix character set utf8mb4 collate utf8mb4_bin;
mysql> create user zabbix@localhost identified by 'password';
mysql> grant all privileges on zabbix.* to zabbix@localhost;
mysql> set global log_bin_trust_function_creators = 1;
mysql> quit;
```

'%' peut remplacer localhost

```
zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql --default-character-set=utf8mb4 -uzabbix -p
zabbix
```

```
echo "DBPassword=password" >> /etc/zabbix/zabbix_server.conf
```

```
sudo reboot
```

```
systemctl restart zabbix-server zabbix-agent apache2
```

```
systemctl enable zabbix-server zabbix-agent apache2
```

Partie 4.6

On rajoute uniquement sur le client kali

deb <http://deb.debian.org/debian> bullseye main contrib non-free

Dans le fichier cat /etc/apt/sources.list

On ajoute le client

```
sudo apt-get install -y zabbix-agent
```

```
sudo systemctl enable zabbix-agent
```

Depuis l'interface web de Zabbix : nom : WEB-SRv1 et ClientKali

template : os -> linux by zabbix agent

groups linuxserver

agent :

fichier de conf /etc/zabbix/zabbix_agentd.conf

Server=ip_zabbix 192.168.100.56

ServerActive à commenter car on veut que l'agent soit passif.

Partie 4.7

zabbix déclencheurs

uptime.is pour gérer le SLA

Partie 4.8

mode maintenance de zabbix

Partie 4.9

ajouter règle firewall ntp

Partie 5.1 : outils

pfBlockerNG

empoisonnement du cache arp

Partie 5.2

En défense je propose un :

- fail2ban
- adguard ou pihole
- hids
- un tunnel VPN avec wireguard
- mettre en place le portail captif
- openVPN via pfsense
- mise en place sur pfsense avec le paquet arpwat
- mise en place freeradius3
- mise en place de ntopng
- mise en place de zeeek
- mise en place de darkstat
- mail pgp
- lvm chiffré

Partie 5.3

Sélectionner : Services – Captive Portal

+ADD

Nom du portail : CaptivePortal

Activer "Enable Captive Portal"

Sélectionner l'interface "LAN"

Maximum concurrent connections : 1 : Limite le nombre de connexions simultanées d'un même utilisateur

Idle timeout (Minutes) : Choisir entre 1 à 5 : Les clients seront déconnectés après la période d'inactivité

Activer "Enable logout popup window"

Définir "Pre-authentication Redirect URL" : URL HTTP de redirection par défaut. Les visiteurs ne seront redirigés vers cette URL après authentification que si le portail captif ne sait pas où les rediriger

Définir After authentication Redirection URL : URL HTTP de redirection forcée. Les clients seront redirigés vers cette URL au lieu de celle à laquelle ils ont initialement tenté d'accéder après s'être authentifiés

Activer "Disable Concurrent user logins" : seule la connexion la plus récente par nom d'utilisateur sera active

Activer "Disable MAC filtering" : nécessaire lorsque l'adresse MAC du client ne peut pas être déterminée

Sélectionner "Use an Authentication backend"

Sélectionner "Local Database" pour "Authentication Server"

Il faut faire attention à éviter de laisser cocher "Local Database" pour "Secondary Authentication Server"

On active "Local Authentication Privileges" pour autoriser uniquement les utilisateurs avec les droits de "Connexion au portail captif"

Puis on "sauvegarde"

Partie 5.4

VPN -> OpenVPN -> Wizards

Type of Server -> Local User Access -> Proxy CA -> SRV-WEB1

Description : VPN OPENVPN

DH Parameters Length : 4096

Data Encryption Algorithms : AES-256-GCM

Auth digest algorithm : SHA512 512 BIT

la partie Tunnel settings :

Tunnel Network : 192.168.254.0/28

Local Network : adresse réseau de la DMZ : 192.168.100.0/24

Client settings : laisser tel quel.

On coche la case Firewall Rule et OpenVPN rule

System -> User Manager -> Add ->

Définissez son nom d'utilisateur qui correspond à son login (compte de connexion), son nom complet et attribuez-lui un mot de passe.

Cochez la case Click to create a user certificate

Descriptive name : Vagrant cert

Lifetime : 365

System -> Package Manager -> available packages -> openvpn-client-export

VPN-> OpenVPN -> Client Export

Remote Access Server -> OpenVPN Clients -> Remote Access Server laisser par défaut

Dans Export on dispose de plusieurs liens de téléchargement pour obtenir la configuration nécessaire à la connexion VPN -> 10/2016/2019 | Windows Installer

On lance OpenVPN GUI." Un double clic sur l'icône présent sur le bureau aura pour effet d'ouvrir l'application dans la barre des tâches représentée par un petit écran avec un cadenas."

"Faites un double-clic sur cet écran cadenassé. La connexion VPN est en train de se mettre en place et les identifiants seront demandés. Lors de la 1ère connexion, Windows vous demandera une exception dans le pare-feu local, cochez les cases et autorisez l'accès."

On saisit l'utilisateur et le mot de passe.

On vérifie avec ipconfig.

Source : <https://neptunet.fr/openvpn-pfsense/>

Partie 5.5

System -> Package Manager -> Available packages -> recherchez ntopng -> Install.

Diagnostics -> ntopng Settings

Cochez l'option "Enable ntopng" afin d'activer les services correspondants.

On définit un mot de passe admin via l'option "ntopng Admin Password" et l'option juste en dessous pour la confirmation.

On rajoute une règle en TCP pour le port 3000 : ALLOW NTOPNG 3000 avec log packet

Partie 5.6

System -> Package Manager -> Available packages -> recherchez zeek -> Install.

https://192.168.116.136/pkg_edit.php?xml=zeek.xml&id=0

Partie 5.7

System -> Package Manager -> Available packages -> recherchez filer -> Install. Diagnostics -> Edit file -> browse

Partie 5.8

System -> Package Manager -> Available packages -> recherchez darkstat -> Install. Ajout d'une rule pour le port 666 en TCP avec log packet darkstat 666 https://192.168.116.136/pkg_edit.php?xml=darkstat.xml Enable darkstat à vrai Enable darkstat DMZ https://192.168.116.136/darkstat_redirect.php

Partie 5.9

On installe pi-hole à l'aide de Docker

```
sudo apt-get update -y
sudo apt-get install -y docker.io docker-compose

mkdir -p /home/vagrant/pi-hole-docker/
nano /home/vagrant/pi-hole-docker/docker-compose.yml
```

```
version: "3"
# More info at https://github.com/pi-hole/docker-pi-hole/ and https://docs.pi-hole.net/
services:
  pihole:
    container_name: pihole
    image: pihole/pihole:latest
    ports:
      - "53:53/tcp"
      - "53:53/udp"
      - "67:67/udp" # Only required if you are using Pi-hole as your DHCP server
      - "8082:80/tcp"
    environment:
      TZ: 'America/Chicago'
      WEBPASSWORD: 'password'
    volumes:
      - './etc-pihole:/etc/pihole'
      - './etc-dnsmasq.d:/etc/dnsmasq.d'
    cap_add:
      - NET_ADMIN # Required if you are using Pi-hole as your DHCP server, else
not needed
    restart: unless-stopped
```

```
cd /home/vagrant/pi-hole-docker/  
sudo docker-compose up -d  
ip a
```

On ajoute TCP ALLOW PIHOLE 8082 dans les règles du Firewall Pfsense.

On ajoute le DNS : <https://192.168.116.136/system.php> 192.168.100.56

Pour plus tard

On aura un qcm sur la partie théorique

On devra présenter et créer infrav3

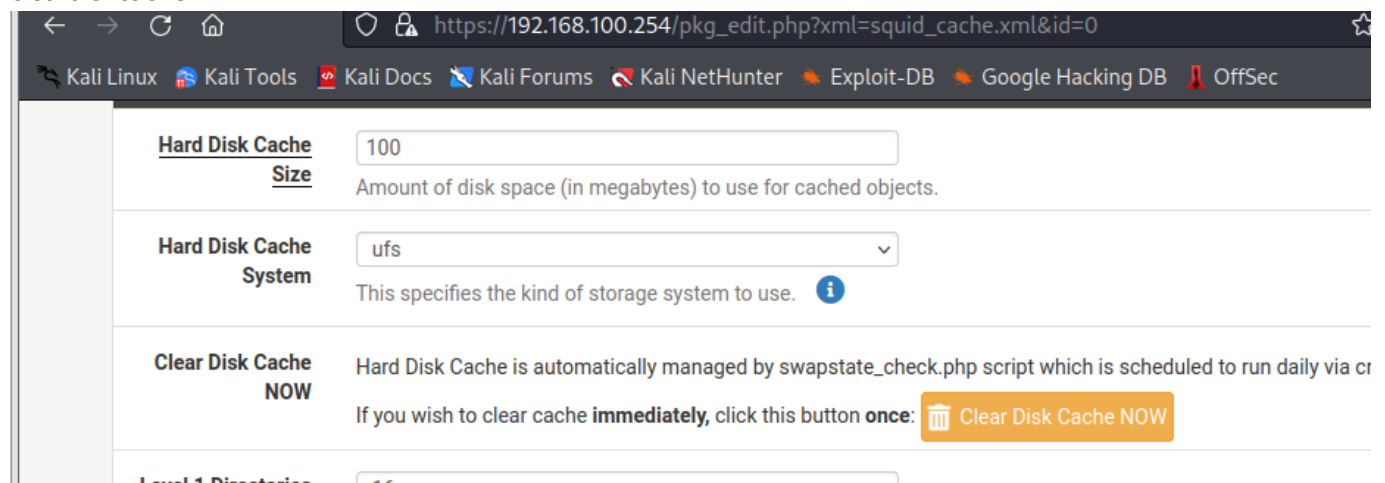
- dnsfiltering
- trafic shapping

Plan d'adressage :

- NAT :
 - 192.168.116.129 - nat - VM2 - Debian - Bastion
 - 192.168.116.131 - nat - WAN - VM1 - Pfsense - Pfsense
 - 192.168.1.1 - nat - VM1 - Pfsense - Pfsense
- DMZ :
 - 192.168.100.254 dmz - VM1 - Pfsense - Pfsense



Annexes images de la partie 5.1 à 5.9

cleardiskcache



dnsresolver

Save

Host Overrides				
Host	Parent domain of host	IP to return for host	Description	Actions
srv1	efrei.local	192.168.100.54	web server	 

zabbix-server-dashboard

ZABBIX

zabbix-server

Tableaux de bord

Surveillance

Services

Inventaire

Rapports

Collecte de données

Alertes

Utilisateurs

Administration

Support

Intégrations

Aide

Paramètres utilisateur

Déconnexion

Global view

Tous les tableaux de bord / Global view

Top hosts by CPU utilization

Utilization 1m avg 5m avg 15m avg Proc

Zabbix server

4.14 % 0.63 0.50 0.22

1.39↑

Zabbix server

Values per sec...

Information système

Paramètre	Valeur	Détails
Le serveur Zabbix est en cours d'exécution	Oui	localhost:10051
Nombre d'hôtes (activé/désactivé)	1	1 / 0
Nombre de modèles	270	
Nombre d'éléments (activés/désactivés/non supportés)	110	99 / 0 / 11
Nombre de déclencheurs (activés/désactivés [problème/ok])	64	64 / 0 [1 / 63]
Nombre d'utilisateurs (en ligne)	2	1

Disponibilité de l'hôte

1 Disponible	0 Non disponible	0 Inconnu	1 Total
--------------	------------------	-----------	---------


Problems by severity

0 Désastre	0 Haut	0 Moyen	1 Avertissement	0 Information	0 Non classé
------------	--------	---------	-----------------	---------------	--------------

Current problems

Temps	Info	Hôte	Problème • Sévérité	Durée	Actualiser	Actions	Tags
15:00:30		Zabbix server	Zabbix server has been restarted (uptime < 10m)	2m 10s	Actualiser		class: os component: system scope: notice ***

Carte géographique



hostserver

ZABBIX

zabbix-server

Tableaux de bord

Surveillance

Problèmes

Hôtes

Dernières données

Cartes

Découverte

Services

Inventaire

Rapports

Collecte de données

Alertes

Utilisateurs

Administration

Hôtes

Hôte ajouté

Nom

Groupes d'hôtes

IP

DNS

Port

Sévérité

État

Tags

Ajouter

Afficher les hôtes en maintenance

Afficher les problèmes supprimés

Enregistrer sous

Appliquer

Réinitialiser

Nom	Interface	Disponibilité	Tags	État	Dernières données	Problèmes	Graphiques	Tableaux de bord
WEB-SRV1	192.168.100.54:10050	ZBX	class: os target: linux	Activé	Dernières données 94	Problems	Graphiques 22	Tableaux de bord 2
Zabbix server	127.0.0.1:10050	ZBX	class: os class: software target: linux ...	Activé	Dernières données 137	1	Graphiques 25	Tableaux de bord 4

zabbix

```
GNU nano 5.4 /etc/zabbix/zabbix_agentd.conf
# Mandatory: no
# Default:
# LogRemoteCommands=0

##### Passive checks related

### Option: Server
# List of comma delimited IP addresses, optionally in CIDR notation, or DNS names of Zabbix s
# Incoming connections will be accepted only from the hosts listed here.
# If IPv6 support is enabled then '127.0.0.1', '::127.0.0.1', '::ffff:127.0.0.1' are treated
# and '::/0' will allow any IPv4 or IPv6 address.
# '0.0.0.0/0' can be used to allow any IPv4 address.
# Example: Server=127.0.0.1,192.168.1.0/24,::1,2001:db8::/32,zabbix.example.com
#
# Mandatory: yes, if StartAgents is not explicitly set to 0
# Default:
# Server=

Server=192.168.100.56
```

ntopng

em1 (DMZ)

468.40 bit/s

5 9 2 13

Contribute

Contribute to the project by sending encrypted anonymous telemetry data to [ntop.org](#).

Confi

Host: clientkali

Traffic Packets DSCP Ports Peers Apps DNS HTTP

(Router/AccessPoint) MAC Address	Vmware_C9:83:51	Computer
IP Address	192.168.100.55 [192.168.100.0/24]	Host Pool: Default
Name	clientkali	
Active Monitoring	Add ICMP Monitor	
First / Last Seen	25/05/2023 09:26:51 [44:26 ago]	25/05/2023 10:11:10 [00:07 ago]
Sent vs Received Traffic Breakdown	<div>SentRcvd</div>	
Traffic Sent / Received	1,186 Pkts / 112.7 KB	1,323 Pkts / 914 KB
	As Client	As Server
Flows: Active / Total / Alerted / Port Unreach	12 / 213 / 114 / 0	0 / 5 / 0 / 0

darkstats

Non sécurisé

192.168.116.136:666

darkstat 3.0.719

graphs

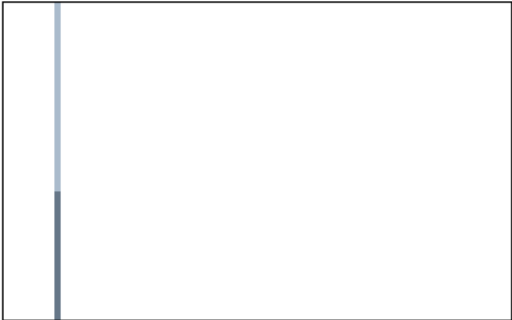
hosts

homepage

Graphs

Measuring for 2 mins, 24 secs, since 2023-05-25 10:26:58 CEST+0200.

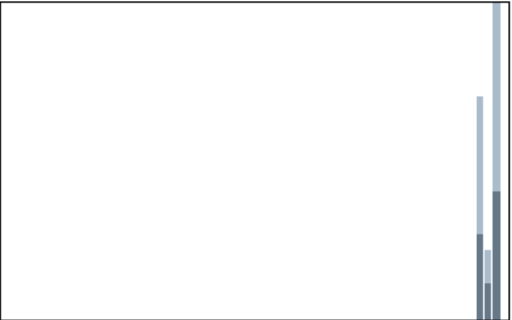
Seen 85,101 bytes, in 206 packets. (208 captured, 0 dropped)



in ■ min: 0.2 KB/s, avg: 0.0 KB/s, max: 0.2 KB/s

out ■ min: 0.4 KB/s, avg: 0.0 KB/s, max: 0.4 KB/s

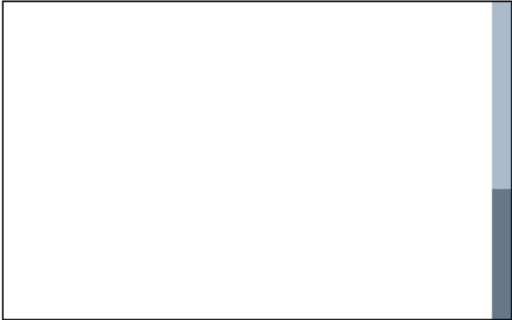
last 60 seconds



in ■ min: 0.0 KB/s, avg: 0.0 KB/s, max: 0.0 KB/s

out ■ min: 0.0 KB/s, avg: 0.0 KB/s, max: 0.0 KB/s

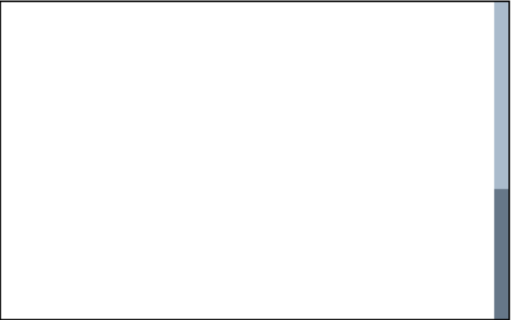
last 60 minutes



in ■ min: 0.0 KB/s, avg: 0.0 KB/s, max: 0.0 KB/s

out ■ min: 0.0 KB/s, avg: 0.0 KB/s, max: 0.0 KB/s

last 24 hours



in ■ min: 0.0 KB/s, avg: 0.0 KB/s, max: 0.0 KB/s

out ■ min: 0.0 KB/s, avg: 0.0 KB/s, max: 0.0 KB/s

last 31 days

reload graphs

- automatic reload is:

off

dnsresolvers

DNS server(s)

- 127.0.0.1
- 192.168.116.2
- 1.1.1.1
- 8.8.8.8
- 192.168.100.56

17 / 28

darkstat

darkstat 3.0.719	graphs	hosts	homepage
------------------	--------	-------	----------

Hosts

(1-30 of 129)

IP	Hostname	MAC Address	In	Out	Total	Last seen
192.168.100.56		00:50:56:20:11:22	6,060,473	3,135,521	9,195,994	1 sec
192.168.100.57		00:0c:29:c9:83:51	2,085,339	4,871,988	6,957,327	7 secs
192.168.100.54		00:0c:29:3c:a6:96	1,003,932	1,205,208	2,209,140	1 sec
192.168.100.254		00:0c:29:a3:b5:a0	354,228	429,926	784,154	1 sec
192.168.100.55		00:0c:29:c9:83:51	424,704	195,915	620,619	1 sec
192.168.100.58		00:0c:29:3c:a6:96	4,299	96,934	101,233	16 secs
192.168.116.136		00:0c:29:a3:b5:a0	7,386	74,881	82,267	3 hrs, 21 mins, 25 secs
255.255.255.255		ff:ff:ff:ff:ff:ff	37,036	0	37,036	(never)
fe80::20c:29ff:fe9:8351		00:0c:29:c9:83:51	5,296	17,952	23,248	44 secs
34.149.100.209		00:0c:29:a3:b5:a0	14,003	5,481	19,484	1 hr, 37 mins, 49 secs
fe80::20c:29ff:fea3:b5a0		00:0c:29:a3:b5:a0	3,552	15,280	18,832	1 min, 44 secs
34.117.65.55		00:0c:29:a3:b5:a0	10,982	1,632	12,614	1 hr, 37 mins, 51 secs
fe80::cddb:6f08:d642:f237		00:50:56:20:11:22	1,136	11,404	12,540	4 mins, 31 secs
ff02::16		33:33:00:00:00:16	11,368	0	11,368	(never)
ff02::1:2		33:33:00:01:00:02	11,040	0	11,040	(never)
34.107.221.82		00:0c:29:a3:b5:a0	4,718	2,066	6,784	1 hr, 37 mins, 49 secs
fe80::20c:29ff:fe3c:a696		00:0c:29:3c:a6:96	3,448	2,736	6,184	1 hr, 2 mins, 16 secs
192.168.116.141		00:0c:29:3c:a6:96	0	5,248	5,248	2 hrs, 34 mins, 4 secs
192.168.254.2		00:0c:29:a3:b5:a0	2,360	2,362	4,722	53 secs
ff02::1		33:33:00:00:00:01	4,416	0	4,416	(never)
34.160.144.191		00:0c:29:a3:b5:a0	2,209	1,754	3,963	1 hr, 37 mins, 49 secs
2600:1901:0:38d7::		00:0c:29:a3:b5:a0	3,760	0	3,760	(never)
0.0.0.0		00:0c:29:c9:83:51	0	3,580	3,580	1 min, 50 secs
172.217.20.196		00:0c:29:a3:b5:a0	3,360	0	3,360	(never)
224.0.0.251		01:00:5e:00:00:fb	2,955	0	2,955	(never)
142.250.178.132		00:0c:29:a3:b5:a0	1,920	0	1,920	(never)
216.58.214.170		00:0c:29:a3:b5:a0	1,200	0	1,200	(never)
44.225.227.241		00:0c:29:a3:b5:a0	600	0	600	(never)

openvpn

```

PS C:\Users\utilisateur> ping 192.168.100.54

Envoi d'une requête 'Ping' 192.168.100.54 avec 32 octets de données :
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.100.54:
    Paquets : envoyés = 1, reçus = 0, perdus = 1 (perte 100%),
Ctrl+C
PS C:\Users\utilisateur> ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet :

    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . :

Carte inconnue Connexion au réseau local :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . : fe80::36e:6be:911d:ddf3%49
    Adresse IPv4. . . . . : 192.168.254.2
    Masque de sous-réseau. . . . . : 255.255.255.240
    Passerelle par défaut. . . . . :

```

Ajout des menus

Diagnostics ▾

Help ▾

ARP Table

Authentication

Backup & Restore

Command Prompt

darkstat

darkstat Settings

DNS Lookup

Edit File

Factory Defaults

Filer

Halt System

Limiter Info

NDP Table

ntopng

ntopng Settings

Packet Capture

pfInfo

pfTop

Ping

Reboot

Des

VP

certmanager

System / Certificate Manager / CAs

CAs

Certificates

Certificate Revocation

Search

Search term










Both

Search

Clear

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

Certificate Authorities

Name	Internal	Issuer	Certificates	Distinguished Name	In Use	Actions
PROXY CA	✓	self-signed	1	ST=FRANCE, OU=LAB, O=EFREI, L=PARIS, CN=efrei-ca, C=FR Valid From: Mon, 22 May 2023 13:34:58 +0200 Valid Until: Tue, 21 May 2024 13:34:58 +0200	OpenVPN Server Squid (1)	   
WEB-EFREI	✓	self-signed	1	ST=FRANCE, OU=LAB, O=EFREI, L=PARIS, CN=WEB-SERVERS Valid From: Mon, 22 May 2023 20:44:49 +0200 Valid Until: Tue, 21 May 2024 20:44:49 +0200		    

certs

System / Certificate Manager / Certificates

CAs

Certificates

Certificate Revocation

Search

Search term













Both

Search

Clear

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

Certificates

Name	Issuer	Distinguished Name	In Use	Actions
webConfigurator default (6468f5d84c07b) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-6468f5d84c07b Valid From: Sat, 20 May 2023 18:31:20 +0200 Valid Until: Fri, 21 Jun 2024 18:31:20 +0200	webConfigurator	   
SRV-WEB1 Server Certificate CA: No Server: Yes	WEB-EFREI	ST=FRANCE, OU=LAB, O=EFREI, L=PARIS, CN=srv1.efrei.local, C=FR Valid From: Mon, 22 May 2023 20:46:55 +0200 Valid Until: Tue, 21 May 2024 20:46:55 +0200	OpenVPN Server	   
Vagrant cert User Certificate CA: No Server: No	PROXY CA	ST=FRANCE, OU=LAB, O=EFREI, L=PARIS, CN=vagrant, C=FR Valid From: Thu, 25 May 2023 08:59:23 +0200 Valid Until: Fri, 24 May 2024 08:59:23 +0200	User Cert	   

openvpn

VPN / OpenVPN / Servers

Servers

Clients






Client Specific Overrides

Wizards

Client Export

Shared Key Export

OpenVPN Servers

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	192.168.254.0/28	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-GCM, AES-256-CBC Digest: SHA512 D-H Params: 4096 bits	VPN OPENVPN	    

Add

Règle-dmz

Non sécurisé | https://192.168.116.136/firewall_rules.php?if=lan

The changes must be applied for them to take effect.

Floating WAN **DMZ** LAN1 LAN2 OpenVPN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0 / 701 KiB	*	*	*	DMZ Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0 / 0 B	IPv4 TCP	*	*	*	8082	*	none		ALLOW PIHOLE 8082	
<input type="checkbox"/>	0 / 0 B	IPv4 TCP	*	*	*	666	*	none		allow darkstat 666	
<input type="checkbox"/>	0 / 0 B	IPv4 TCP	*	*	*	3000 (HBCI)	*	none		ALLOW NTPNG 3000	
<input type="checkbox"/>	0 / 2 KiB	IPv4 TCP	*	*	*	80 (HTTP)	*	none		ALLOW HTTP	
<input type="checkbox"/>	0 / 4.64 MiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none		ALLOW HTTPS	
<input type="checkbox"/>	0 / 341 KiB	IPv4 UDP	*	*	192.168.100.254	53 (DNS)	*	none		ALLOW DNS	
<input checked="" type="checkbox"/>	0 / 0 B	IPv4 TCP	*	*	*	9000	*	none		ALLOW PORTAINER 8082	

Add Add Delete Save Separator

Règles WAN

Non sécurisé | https://192.168.116.136/firewall_rules.php?if=wan

The changes must be applied for them to take effect.

Floating WAN **DMZ** LAN1 LAN2 OpenVPN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0 / 537 KiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
<input checked="" type="checkbox"/>	0 / 205 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input type="checkbox"/>	0 / 0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		OpenVPN VPN OPENVPN wizard	
<input type="checkbox"/>	0 / 0 B	IPv4 TCP	*	*	WAN address	3000 (HBCI)	*	none		ALLOW NTPNG 3000	
<input type="checkbox"/>	0 / 0 B	IPv4 TCP	*	*	*	8082	*	none		ALLOW PIHOLE 8082	

Add Add Delete Save Separator

Ping avec OpenVPN

```
PS C:\Users\utilisateur> ping 192.168.100.254

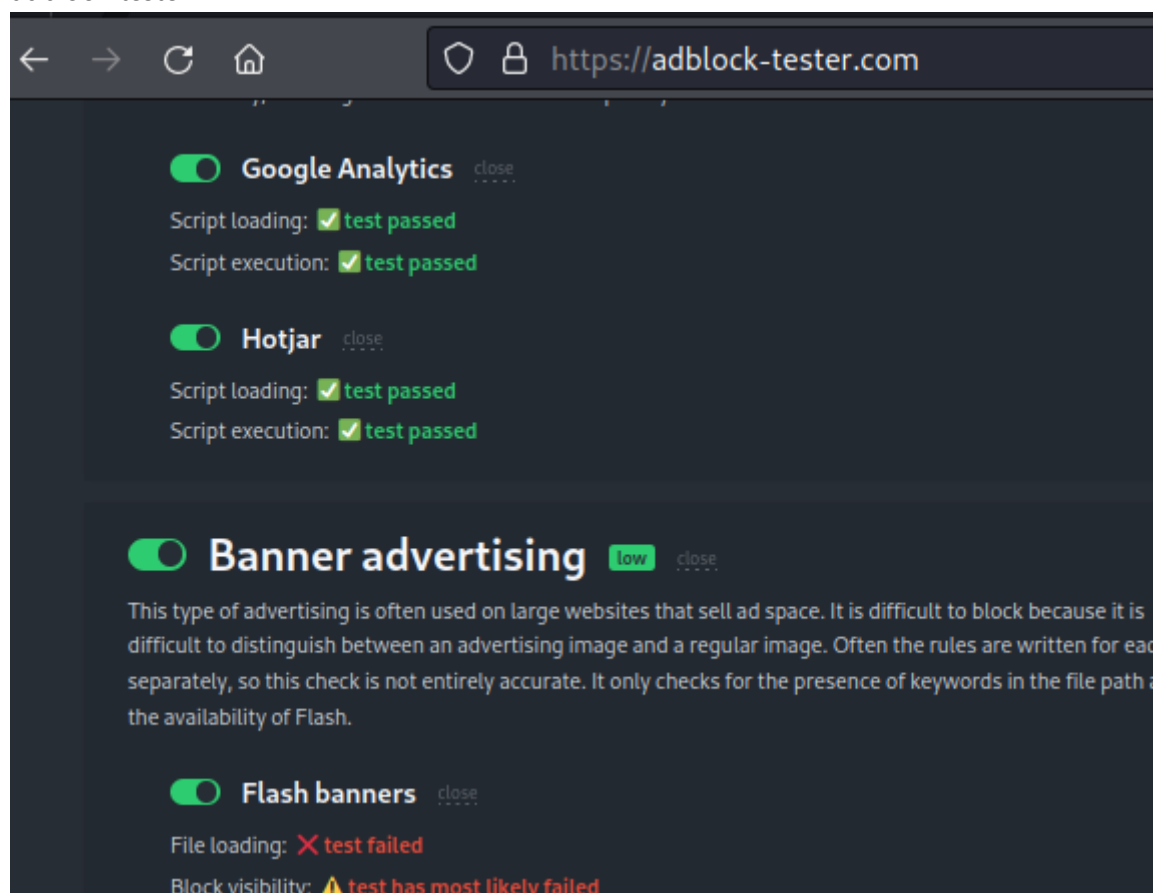
Envoi d'une requête 'Ping' 192.168.100.254 avec 32 octets de données :
Réponse de 192.168.100.254 : octets=32 temps<1ms TTL=64
Réponse de 192.168.100.254 : octets=32 temps=1 ms TTL=64

Statistiques Ping pour 192.168.100.254:
    Paquets : envoyés = 2, reçus = 2, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 1ms, Moyenne = 0ms
Ctrl+C
PS C:\Users\utilisateur> ping 192.168.100.55

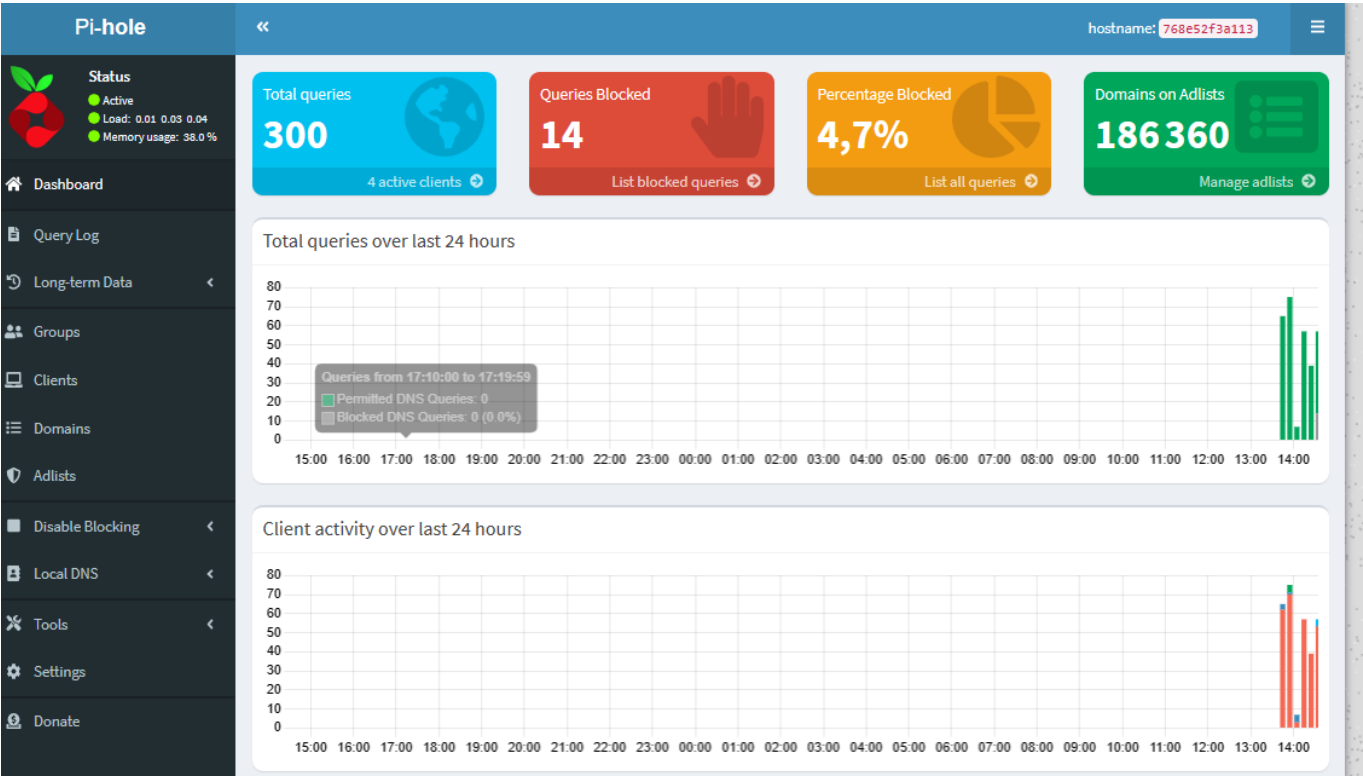
Envoi d'une requête 'Ping' 192.168.100.55 avec 32 octets de données :
Réponse de 192.168.100.55 : octets=32 temps=1 ms TTL=63

Statistiques Ping pour 192.168.100.55:
    Paquets : envoyés = 1, reçus = 1, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 1ms, Moyenne = 1ms
Ctrl+C
```

adblock-tester



adblock-pihole



adblock-pihole-logs

The screenshot shows the Pi-hole Query Log with the following details:

- Header:** Pi-hole logo, status, and hostname: 768e52f3a113.
- Section:** Recent Queries (showing up to 100 queries), [show all](#)
- Search:** Type / Domain / Client
- Table:**

Time	Type	Domain	Client	Status	Reply	Action
2023-05-25 14:35:11	AAAA	www.google-analytics.com	192.168.100.55	Blocked (gravity)	IP (0.1ms)	Whitelist
2023-05-25 14:35:11	A	www.google-analytics.com	192.168.100.55	Blocked (gravity)	IP (0.2ms)	Whitelist
2023-05-25 14:35:11	AAAA	pagead2.googlesyndication.com	192.168.100.55	Blocked (gravity)	IP (0.1ms)	Whitelist
2023-05-25 14:35:11	A	pagead2.googlesyndication.com	192.168.100.55	Blocked (gravity)	IP (0.1ms)	Whitelist
2023-05-25 14:35:11	AAAA	static.hotjar.com	192.168.100.55	Blocked (gravity)	IP (0.1ms)	Whitelist
2023-05-25 14:35:11	A	static.hotjar.com	192.168.100.55	Blocked (gravity)	IP (0.2ms)	Whitelist
2023-05-25 14:35:11	AAAA	an.yandex.ru	192.168.100.55	Blocked (gravity)	IP (0.1ms)	Whitelist

Annexes : images de toutes les parties

AVANTCHANGEMENT

Firewall / Rules / DMZ

Floating WAN DMZ LAN1 LAN2

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0 / 0 B	*	*	*	DMZ Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0 / 0 B	IPv4 *	DMZ net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0 / 0 B	IPv6 *	DMZ net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add Add Delete Save Separator

ApresCHANGEMENT

Floating WAN DMZ LAN1 LAN2

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0 / 0 B	*	*	*	DMZ Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0 / 0 B	IPv4 TCP	*	*	*	443 (HTTPS)	*	none		ALLOW HTTPS	
<input type="checkbox"/>	0 / 0 B	IPv4 TCP	*	*	*	80 (HTTP)	*	none		ALLOW HTTP	
<input type="checkbox"/>	0 / 0 B	IPv4 UDP	*	*	*	53 (DNS)	*	none		Easy rule passed from firewall DNS	

Add Add Delete Save Separator

squid

Non sécurisé | https://192.168.116.133/pkg_edit.php?xml=squid.xml&id=0

Sets the "Not Before" (setValidBefore)
Sets CN property (setCommonName)

See [sslsproxy_cert_adapt](#) directive documentation and [Mimic original SSL server certificate](#) wiki article for details.

Logging Settings

Enable Access Logging

☒ This will enable the access log.
Warning: Do NOT enable if available disk space is low.

Log Store Directory

The directory where the logs will be stored; also used for logs other than the Access Log above. Default: /var/squid/logs
Important: Do NOT include the trailing / when setting a custom location.

Rotate Logs

Defines how many days of logfiles will be kept. Rotation is disabled if left empty.

Log Pages Denied by SquidGuard

☐ Makes it possible for SquidGuard denied log to be included on Squid logs.
[Click Info for detailed instructions.](#)

Headers Handling, Language and Other Customizations

Visible Hostname

This is the hostname to be displayed in proxy server error messages.

Administrator's Email

This is the email address displayed in error messages to the users.

Error Language

Select the language in which the proxy server will display error messages to users.

blockingmode-legacy

Block Settings

Block Offenders

☒ Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

IPS Mode

Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.

Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnxt, cc, cxgbe, cxl, em, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.

Kill States

☒ Checking this option will kill firewall established states for the blocked IP. Default is checked.

Which IP to Block

curl-portquiz8080

```
(lab@ClientKali)-[~]  
$ curl portquiz.net:8080  
^C
```

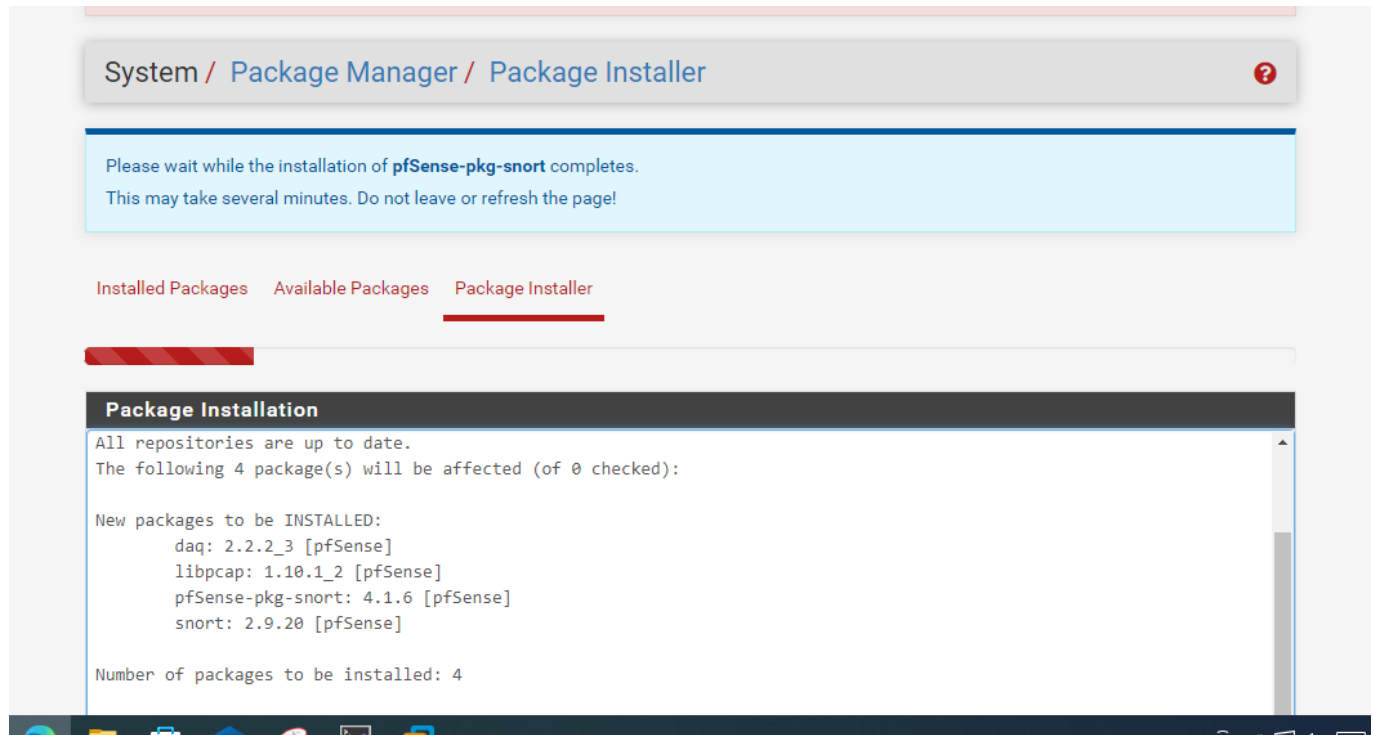
snort-ruleswan-2

<input type="checkbox"/>	emerging-deleted.rules	<input type="checkbox"/>	snort_content-replace.rules	<input type="checkbox"/>	snort_file-java.so.rules
<input type="checkbox"/>	emerging-dns.rules	<input type="checkbox"/>	snort_deleted.rules	<input type="checkbox"/>	snort_file-multimedia.so.rules
<input type="checkbox"/>	emerging-dos.rules	<input checked="" type="checkbox"/>	snort_exploit-kit.rules	<input type="checkbox"/>	snort_file-office.so.rules
<input type="checkbox"/>	emerging-drop.rules	<input type="checkbox"/>	snort_file-executable.rules	<input type="checkbox"/>	snort_file-other.so.rules
<input checked="" type="checkbox"/>	emerging-dshield.rules	<input type="checkbox"/>	snort_file-flash.rules	<input type="checkbox"/>	snort_file-pdf.so.rules
<input checked="" type="checkbox"/>	emerging-exploit.rules	<input type="checkbox"/>	snort_file-identify.rules	<input type="checkbox"/>	snort_indicator-shellcode.so.rules
<input type="checkbox"/>	emerging-ftp.rules	<input type="checkbox"/>	snort_file-image.rules	<input type="checkbox"/>	snort_malware-cnc.so.rules
<input type="checkbox"/>	emerging-games.rules	<input checked="" type="checkbox"/>	snort_file-java.rules	<input type="checkbox"/>	snort_malware-other.so.rules
<input type="checkbox"/>	emerging-icmp.rules	<input type="checkbox"/>	snort_file-multimedia.rules	<input type="checkbox"/>	snort_netbios.so.rules
<input type="checkbox"/>	emerging-icmp_info.rules	<input type="checkbox"/>	snort_file-office.rules	<input type="checkbox"/>	snort_os-linux.so.rules

snort-ruleswan

<input type="checkbox"/>	emerging-irc.rules	<input type="checkbox"/>	snort_indicator-shellcode.rules	<input type="checkbox"/>	snort_protocol-dns.so.rules
<input type="checkbox"/>	emerging-mobile_malware.rules	<input type="checkbox"/>	snort_indicator-shellcode.rules	<input type="checkbox"/>	snort_protocol-nntp.so.rules
<input type="checkbox"/>	emerging-netbios.rules	<input type="checkbox"/>	snort_local.rules	<input type="checkbox"/>	snort_protocol-other.so.rules
<input checked="" type="checkbox"/>	emerging-p2p.rules	<input type="checkbox"/>	snort_malware-backdoor.rules	<input type="checkbox"/>	snort_protocol-scada.so.rules
<input type="checkbox"/>	emerging-policy.rules	<input type="checkbox"/>	snort_malware-cnc.rules	<input type="checkbox"/>	snort_protocol-snmp.so.rules
<input type="checkbox"/>	emerging-pop3.rules	<input type="checkbox"/>	snort_malware-other.rules	<input type="checkbox"/>	snort_protocol-tftp.so.rules
<input type="checkbox"/>	emerging-rpc.rules	<input type="checkbox"/>	snort_malware-tools.rules	<input type="checkbox"/>	snort_protocol-voip.so.rules
<input type="checkbox"/>	emerging-scada.rules	<input type="checkbox"/>	snort_netbios.rules	<input type="checkbox"/>	snort_pua-p2p.so.rules
<input checked="" type="checkbox"/>	emerging-scan.rules	<input type="checkbox"/>	snort_os-linux.rules	<input type="checkbox"/>	snort_server-iis.so.rules
<input checked="" type="checkbox"/>	emerging-shellcode.rules	<input type="checkbox"/>	snort_os-mobile.rules	<input type="checkbox"/>	snort_server-mail.so.rules
<input checked="" type="checkbox"/>	emerging-smtp.rules	<input type="checkbox"/>	snort_os-other.rules	<input type="checkbox"/>	snort_server-mysql.so.rules
<input checked="" type="checkbox"/>	emerging-snmp.rules	<input type="checkbox"/>	snort_os-solaris.rules	<input type="checkbox"/>	snort_server-oracle.so.rules
<input checked="" type="checkbox"/>	emerging-sql.rules	<input type="checkbox"/>	snort_os-windows.rules	<input type="checkbox"/>	snort_server-other.so.rules
<input type="checkbox"/>	emerging-telnet.rules	<input type="checkbox"/>	snort_policy-multimedia.rules	<input type="checkbox"/>	snort_server-webapp.so.rules

snortinstall



Cours :

5 piliers de la sécurité

- Intégrité : garantir que les données sont celles spécifiées
- Disponibilité : comme la redondance, un SLA.
- Confidentialité : seul la personne destinataire a le droit de le lire : gpg.
- Non répudiation : être sur que c'est bien la bonne personne et que ça lui qui l'ait envoyé comme pour les mails SPF et signatures
- Authentification : que seul les personnes soient autorisés à accéder aux ressources
- CIDTN :
- reverse proxy
- firewall
- une note de l'infra v3
monitoring avoir un visuel sur l'infrastructure

Sources

<https://www.provya.net/?d=2021/06/08/09/46/24-pfsense-la-gestion-des-packages-sous-pfsense>

http://gelit.ch/td/linux/Golliet_RTb.pdf
<https://pixelabs.fr/installation-configuration-pfsense-workstation/>
<https://neptunet.fr/openvpn-pfsense/>
<https://github.com/shadonet/pfSense-pkg-zeek/blob/master/README.md>
<https://www.pc2s.fr/pfsense-portail-captif-avec-authentification-utilisateur/>

<https://www.swisstransfer.com/d/2b874a0a-2ca4-446a-87fe-ce0dc21def4b>