



Une formation
Alphorm.com

Formation pfSense

Le firewall open source de référence



Hamza KONDAH



Une formation
Alphorm.com

Introduction

Firewall OpenSource de référence

OpenBSD packet Filter (PF)

2001

Première version : 2006

webGUI

Fonctionnalités de plus en plus riches





Une formation
Alphorm.com

Pourquoi pfSense ?

Open Source

Stable

Multifonctions

Performant

Modulable

Plugins

Peut être
configuré
comme UTM



Une formation
Alphorm.com

Scénarios de déploiement





Plan de la formation

Introduction

Les VPNs

Redondance et haute disponibilité

Configuration du CARP

Routing et Bridging

Une formation
Alphorm
com



Plan de la formation (suite)

Packages complémentaires

Troubleshooting et test de sécurité

Benchmarking

Conclusion et perspectives

Une formation
Alphorm
com



Une formation
Alphorm.com

Public concerné

Administrateur réseau
Technicien Réseau
Responsable sécurité
Ingénieur réseaux / sécurité
Intégrateur
Et tout le monde 😊



Une formation
Alphorm.com

Objectifs de la formation

Installation, configuration et
administration
Déploiement dans plusieurs scénarios
Test de sécurité
Firewalking
Capacity planning
PfSense comme UTM 😊



Prérequis

Notions de bases en réseaux
informatiques

Éventuellement une première
expérience dans le firewalling

Une formation
Alphorm
.com



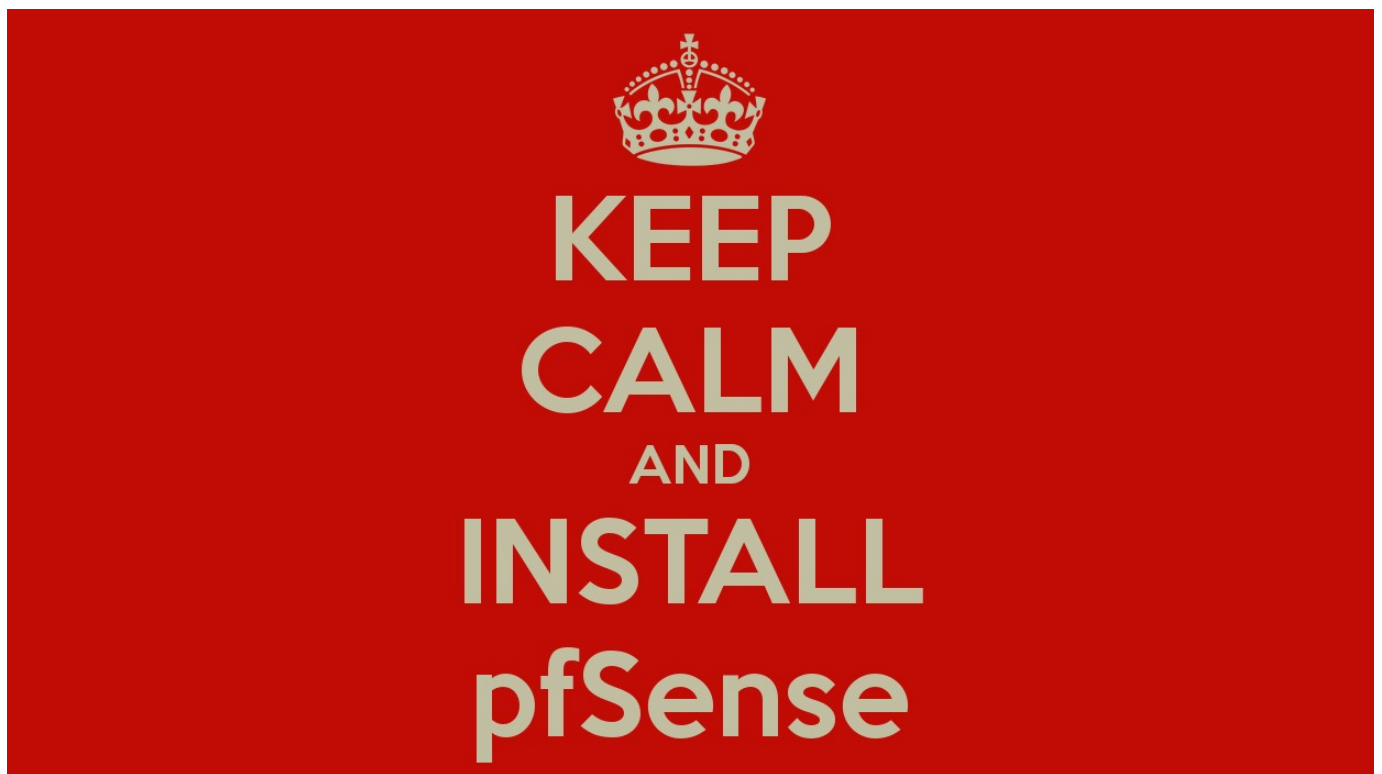
Prérequis

Formation pfSense (1/2) : Le firewall open source de référence

Comprendre et déployer avec succès le firewall open source pfSense



Une formation
Alphorm
.com



Introduction aux VPNs



Hamza KONDAH



Une formation
Alphorm.com

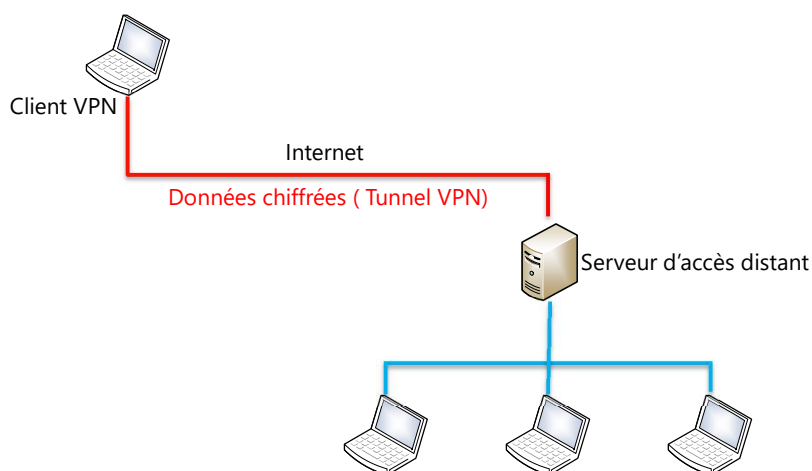
Plan

Introduction
Types de VPNs
IPSEC
L2TP
OpenVPN
Comparaisons



Une formation
Alphorm.com

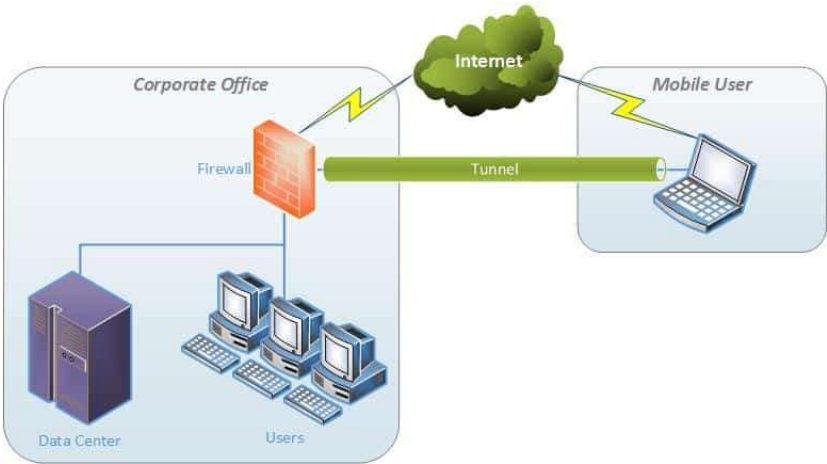
Introduction





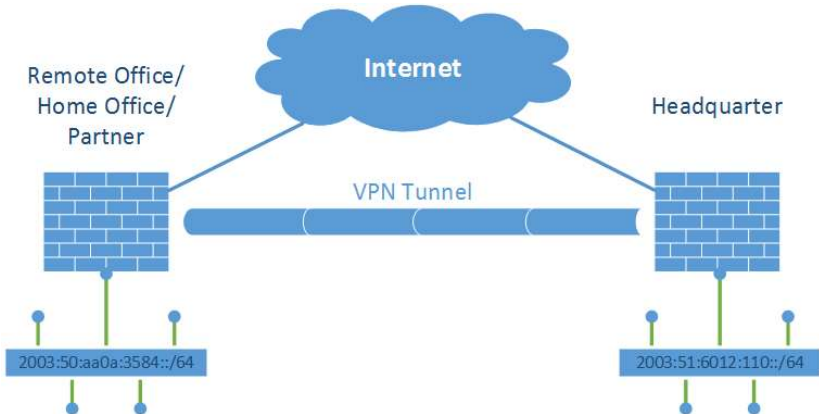
Une formation
Alphorm.com

VPN Point-To-Site



Une formation
Alphorm.com

VPN Site-To-Site





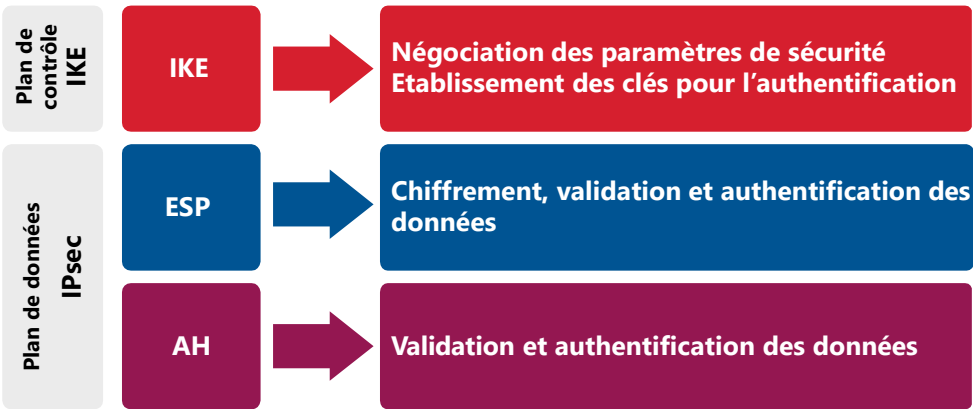
IPSEC

Une connexion VPN est composée de deux tunnels :

- 1. Un tunnel IKE pour l'échange des paramètres de sécurité entre entités
- 2. Un tunnel IPSec qui sert au transfert de données entre entités



IPSEC





Une formation
Alphorm.com

IPSEC : SA

Accord sur les paramètres de sécurité entre deux entités

Il est nécessaire que les deux entités soient d'accord sur les réglages de sécurité

L'ensemble de ces réglages est appelé Security Association (SA)



Une formation
Alphorm.com

IPSEC

IKE automatise le processus d'échange de clés entre entités pour la mise en œuvre d'un tunnel IPsec

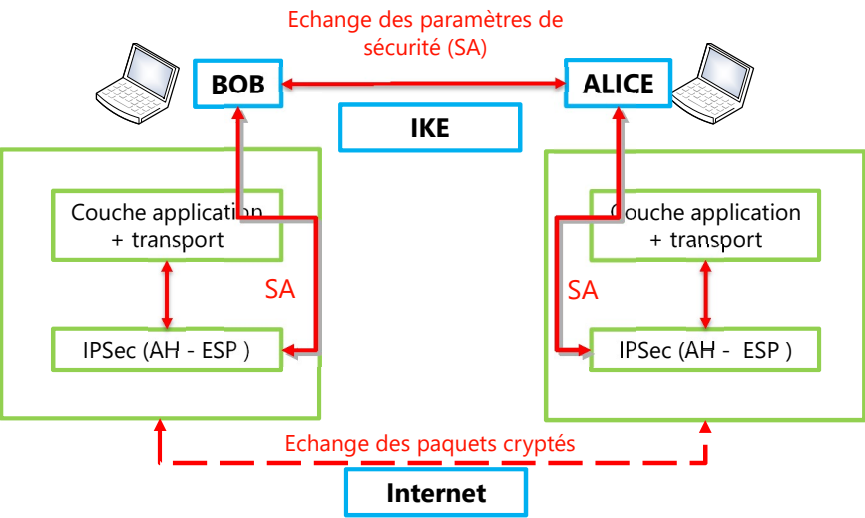
Négociation des paramètres de sécurité au travers d'une SA (Security Association)

Génération automatique des clés



Une formation
Alphorm.com

IPSEC



Une formation
Alphorm.com

IPSEC

Mode
Transport

Mode
Tunnel



L2TP

Le protocole Layer 2 Tunneling (L2TP)
Protocole de tunneling utilisé pour les (VPN)
Il n'a pas de cryptage ou de confidentialité
Il s'appuie sur un protocole de cryptage
(comme IPSec) qui passe dans le tunnel
pour assurer la confidentialité

Une formation
Alphorm.com



OpenVPN

Une application informatique ouverte pour
la mise en place de techniques des réseaux
privés virtuels
Connexions sécurisées point-par-point ou
site-par-site
Il exploite un protocole de sécurité sur
mesure qui utilise SSL/TLS pour les
échanges des clés

Une formation
Alphorm.com



OpenVPN

Un protocole Open VPN permet à des homologues de s’authentifier mutuellement en utilisant une clé secrète pré-partagée, des certificats ou un nom d’utilisateur / mot de passe



Comparaison

Protocol	Client included in OS	Client available for OS	Support multi-WAN	Firewall friendliness	Cryptographically secure
IPSec	Windows , macOS X	Windows, Linux macOS X	YES	Only with NAT-T	YES
L2TP	Client included in OS	Windows, Linux	YES	YES	NO (no encryption at all)
OpenVPN	Linux	Windows ,Linux macOS X	YES	YES	YES

Merci



Configuration d'IPSEC

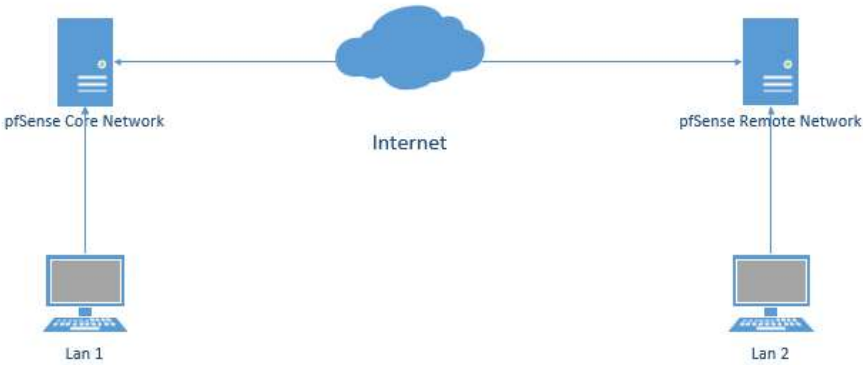


Hamza KONDAH



Une formation
Alphorm.com

Architecture du Lab



Une formation
Alphorm.com

Lab : VPN IPSEC

VPN / IPsec / Tunnels / Edit Phase 1

Tunnels Mobile Clients Pre-Shared Keys Advanced Settings

General Information

Disabled

☐ Set this option to disable this phase1 without removing it from the list.

Key Exchange version

V1

Select the Internet Key Exchange protocol version to be used. Auto uses IKEV2 when initiator, and accepts either IKEV1 or IKEV2 as responder.

Internet Protocol

IPv4

Select the Internet Protocol family.

Interface

WAN

Select the interface for the local endpoint of this phase1 entry.

Remote Gateway

ipsectest.duckdns.org

Enter the public IP address or host name of the remote gateway

Description

IPsec test tunnel

A description may be entered here for administrative reference (not parsed).

Phase 1 Proposal (Authentication)

Authentication Method

Mutual PSK

Must match the setting chosen on the remote side.

Negotiation mode

Main

Aggressive is more flexible, but less secure.

My identifier

My IP address

Peer identifier

Peer IP address

Pre-Shared Key

Enter the Pre-Shared Key string.

Merci



Configuration de l'OPENVPN

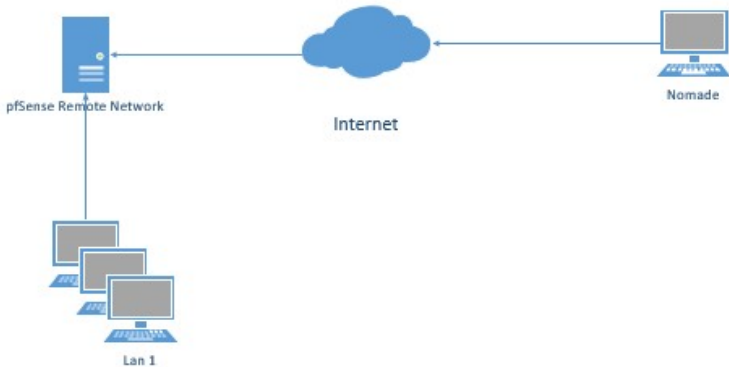


Hamza KONDAH



Une formation
Alphorm.com

Architecture du Lab



Une formation
Alphorm.com

Lab : OPENVPN

pfSense
COMMUNITY EDITION

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

Wizard / OpenVPN Remote Access Server Setup /

OpenVPN Remote Access Server Setup

This wizard will provide guidance through an OpenVPN Remote Access Server Setup .
The wizard may be stopped at any time by clicking the logo image at the top of the screen.

Select an Authentication Backend Type

Type of Server Local User Access ▾

NOTE: If unsure, leave this set to "Local User Access."

» Next

Merci



Introduction à la Redondance et haute disponibilité



Hamza KONDAH



Une formation
Alphorm.com

Plan

Définition
Load Balancing
Algorithmes LB
La redondance



Une formation
Alphorm.com

Définitions

Redondance

Haute disponibilité



Une formation
Alphorm.com

Load Balancing

Gateway load
balancing

Server load balancing

Et peut être :

Software

Hardware



Une formation
Alphorm.com

Algorithmes LB

Random

Round robin

Weighted
round robin

Least
Connection

Least Traffic

Least latency

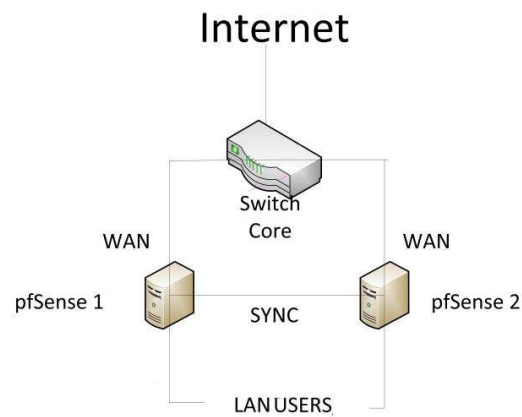
Ip hash

Url hash

SDN adaptive



La redondance



Une formation
Alphorm.com

Merci



Une formation
Alphorm.com

Configuration Load Balancing



Hamza KONDAH



Une formation
Alphorm.com

Lab : Configuration LB

Services / Load Balancer / Pools / Edit

Add/Edit Load Balancer - Pool Entry

Name

Mode

Load Balance

Description

Port

This is the port the servers are listening on. A port alias listed in Firewall -> Aliases may also be specified here.

Retry

Optionally specify how many times to retry checking a server before declaring it down.

Add Item to the Pool

Monitor

ICMP

Server IP Address

IP Address

+ Add to pool

Current Pool Members

Members

Disabled

Enabled (Default)

Remove

Remove

Move to enabled list

Move to disabled list

Merci



Configuration du Failover



Hamza KONDAH



Une formation
Alphorm.com

Plan

Introduction

Pfsync

Lab : Configuration du Failover



Une formation
Alphorm.com

Introduction

Protocole CARP

Common Address Redundancy
Protocol

Mise en place du FailOver

Groupe de plusieurs hôtes

Partage de l'@IP

Alternative sécurisé



Pfsync

Pfsync
Protocole de synchronisation
Gestion de plusieurs hôtes via une
seule interface
Interface dédiée



Lab : pfSense & Failover

Status / CARP

Temporarily Disable CARPEnter Persistent CARP Maintenance Mode

CARP Interfaces		
CARP Interface	Virtual IP	Status
WAN1@1	10.0.2.1/24	MASTER
LAN@2	172.16.1.10/24	MASTER

pfSync Nodes

- 388bc6c4
- 6562a1ee
- c87ed532

Merci



Introduction



Hamza KONDAH



Une formation
Alphorm.com

Plan

Le Routing
Le Bridging



Une formation
Alphorm.com

Le Routing

Une des principales fonctions d'un pare-feu
Routage paraît transparent
Peu de configurations supplémentaires
Grande facilité



Une formation
Alphorm.com

Le Routing

Important : Si vous avez un routeur connecté à l'un des réseaux internes de pfSense, pfSense ne saura pas comment acheminer le trafic vers les nœuds connectés au routeur, à moins que vous ne définissiez un itinéraire statique pour celui-ci.



Une formation
Alphorm.com

Le Bridging

N'est pas quelque chose qui est fait dans les configurations des réseaux typiques

Normalement, chaque interface a son propre domaine de diffusion



Une formation
Alphorm.com

Le Bridging

Cependant, il est souvent utile ou nécessaire de combiner (ou de mettre en pont) deux interfaces afin qu'elles soient dans le même domaine de diffusion, de la même manière qu'elles le seraient si elles étaient sur le même commutateur



Une formation
Alphorm.com

Le Bridging

« La différence entre deux interfaces pontées et un commutateur est qu'avec les interfaces pontées, les règles de pare-feu s'appliquent toujours »

Merci



Bridging avec pfSense



Hamza KONDAH



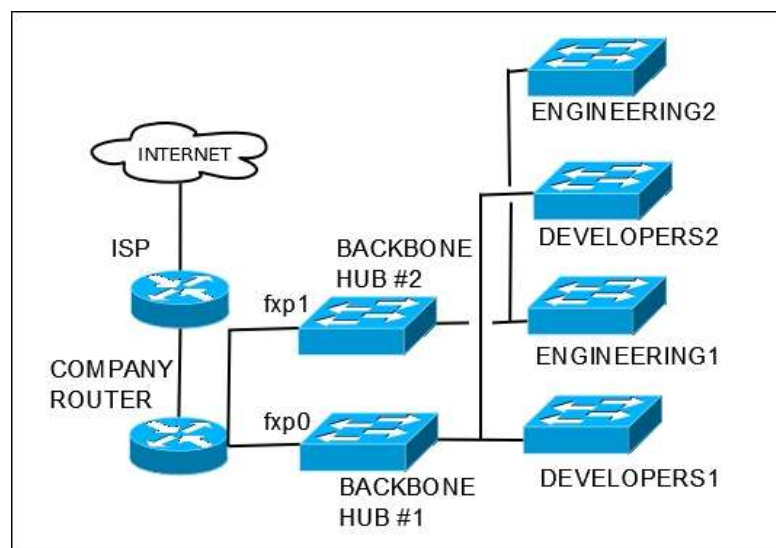
Plan

Introduction
Protocole STP
Protocole RSTP
Lab : Bridging

Une formation
Alphorm.com



Introduction

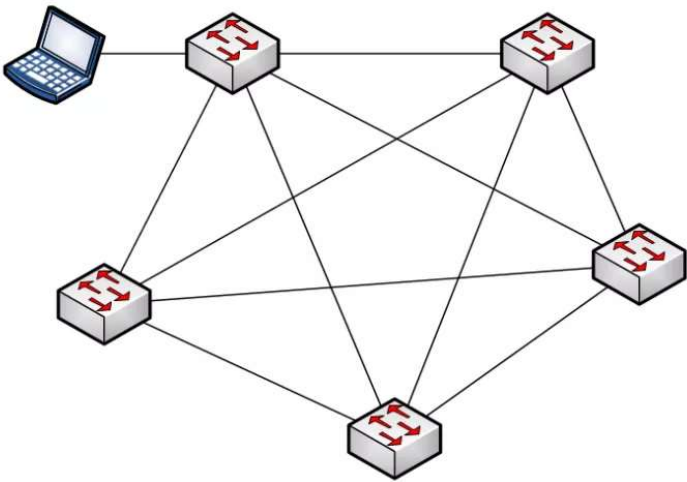


Une formation
Alphorm.com



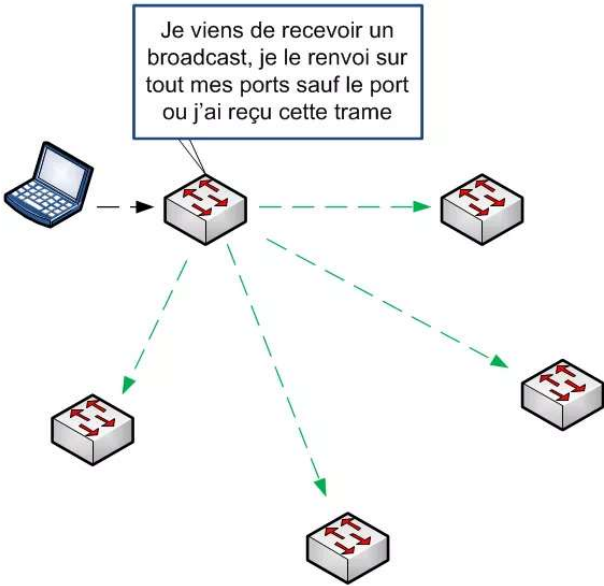
Une formation
Alphorm.com

Protocole STP



Une formation
Alphorm.com

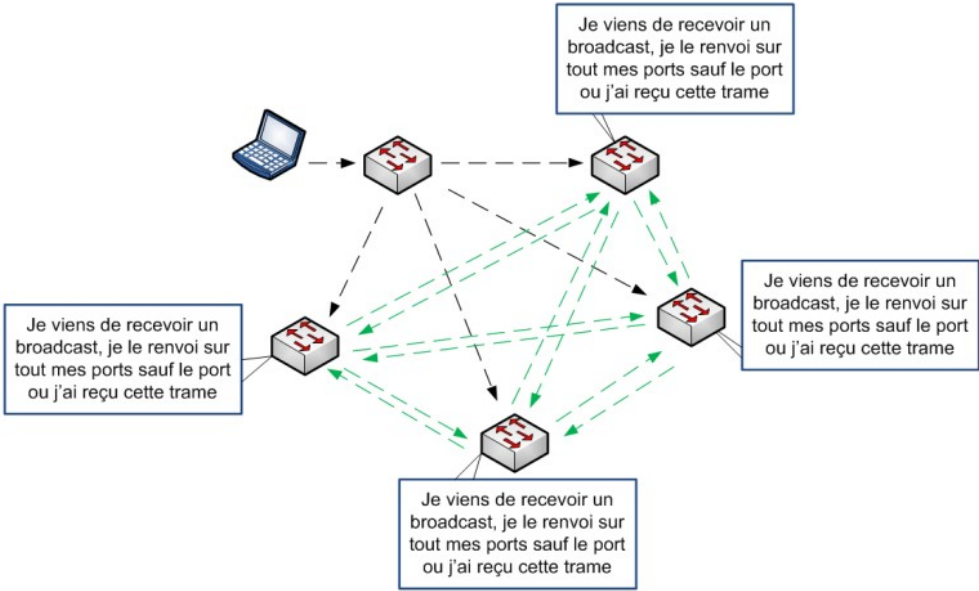
ETAPE 1





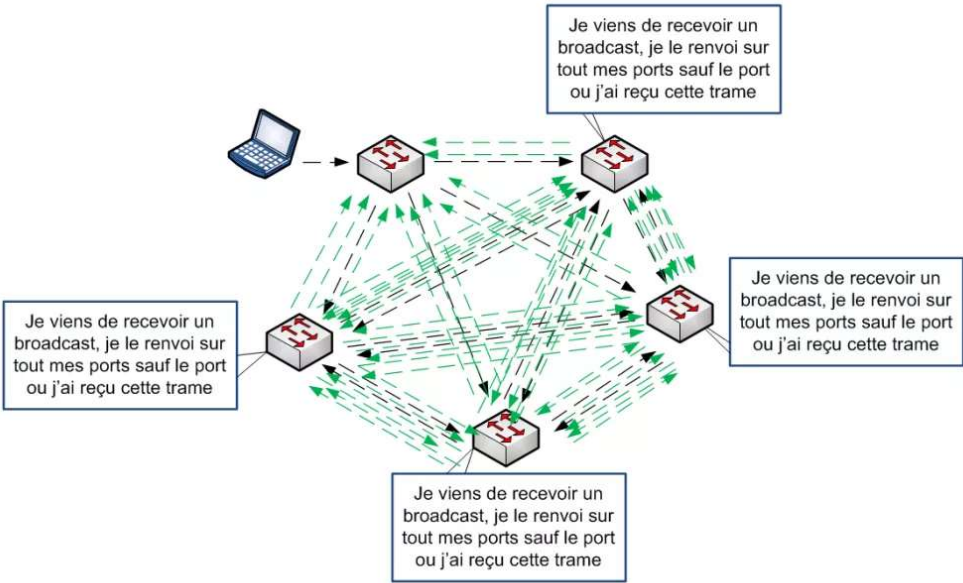
Une formation
Alphorm.com

ETAPE 2



Une formation
Alphorm.com

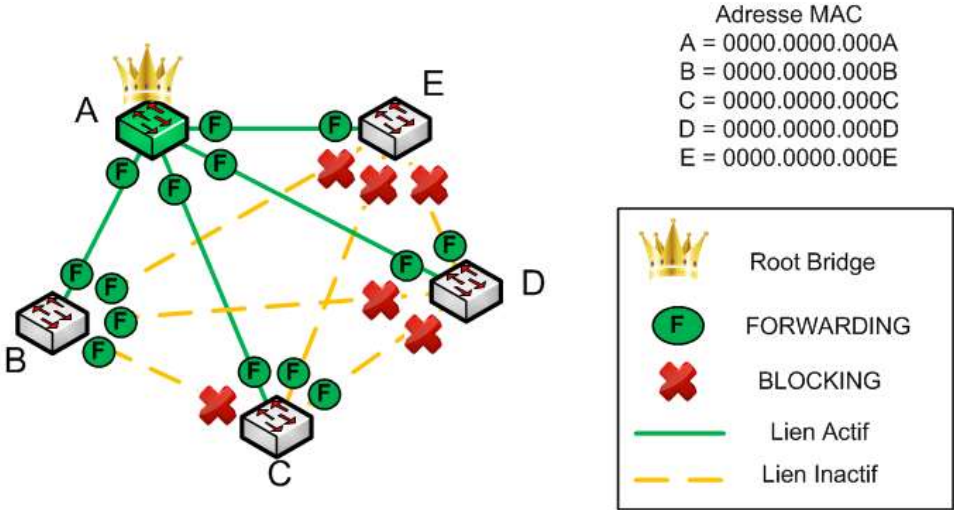
ETAPE 3





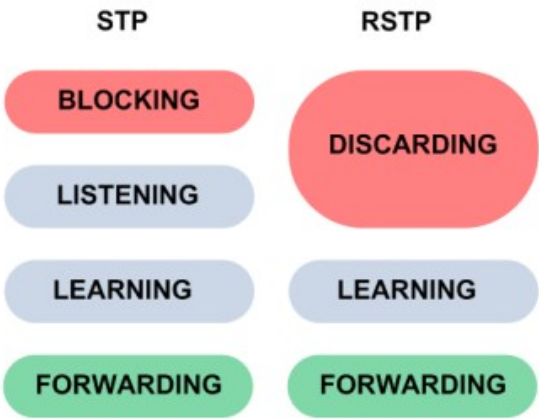
Une formation
Alphorm.com

Protocole STP



Une formation
Alphorm.com

Protocole RSTP





Designated-port



Une formation
Alphorm.com



Etat des connexions

Point-to-point (P2P)

Cette connexion est une connexion en FULL-DUPLEX, RSPT estime que cette liaison est une liaison point à point

Une formation
Alphorm.com



Une formation
Alphorm.com

Etat des connexions

Shared

Cette connexion est une connexion HALF-DUPLEX, elle est partagée (Shared) entre plusieurs équipements via un Hub

Edge

Cette connexion est une connexion entre un Switch et un Client



Une formation
Alphorm.com

Lab : Bridging

Interfaces / Bridges / Edit

Bridge Configuration

Member Interfaces

WAN
LAN

Interfaces participating in the bridge.

Description

Advanced Options

Hide Advanced

Advanced Configuration

Cache Size

Set the size of the bridge address cache. The default is 2000 entries.

Cache expire time

Set the timeout of address cache entries to this number of seconds. If seconds is zero, then address cache entries will not be expired. The default is 1200 seconds.

Span Port

WAN
LAN

Add the interface named by interface as a span port on the bridge. Span ports transmit a copy of every frame received by the bridge. This is most useful for snooping a bridged network passively on another host connected to one of the span ports of the bridge.
The span interface cannot be part of the bridge member interfaces.

Edge Ports

WAN
LAN

Set interface as an edge port. An edge port connects directly to end stations and cannot create bridging loops in the network; this allows it to transition straight to forwarding.

Merci



Routage avec pfSense



Hamza KONDAH



Plan

Le routage statique

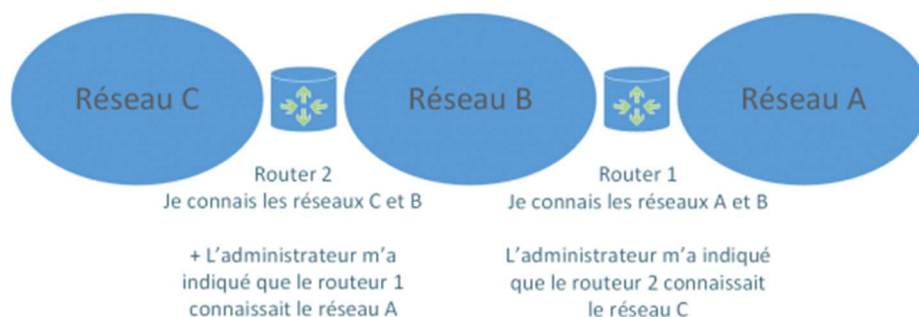
Le routage dynamique

Lab : Routage avec pfSense

Une formation
Alphorm
.com



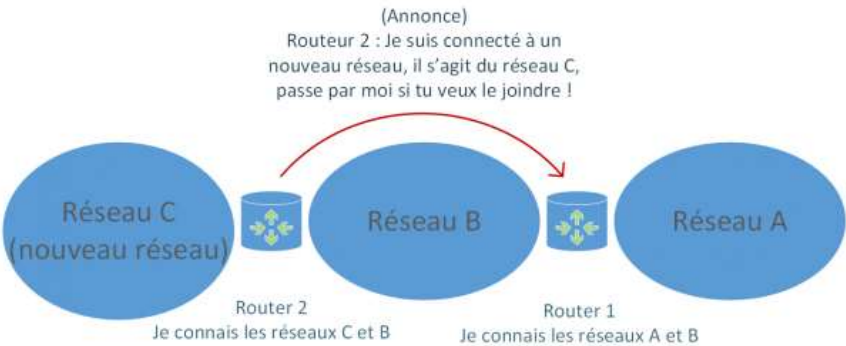
Le routage statique



Une formation
Alphorm
.com



Routage dynamique



Routage dynamique

Package name	Routing protocol supported
OpenBGPD	BGP
Quagga OSPF	OSPF
routed	RIP v1 and v2



Lab : Routage avec PfSense



Une formation
Alphorm.com

Merci



Une formation
Alphorm.com

Multi WAN



Hamza KONDAH



Une formation
Alphorm.com

Plan

Introduction

Procédure

Lab : Multi Wan



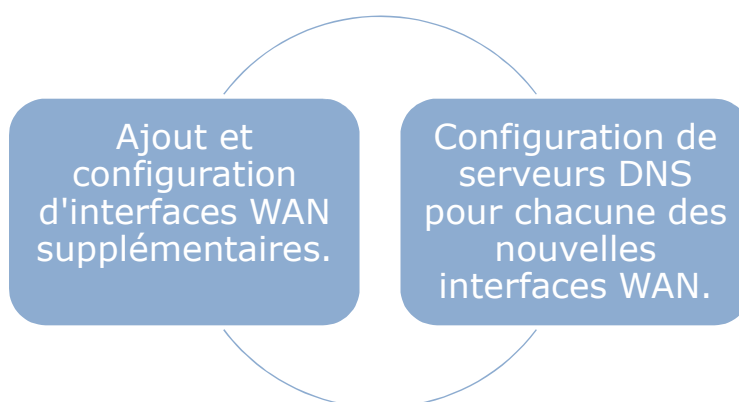
Introduction



Une formation
Alphorm.com



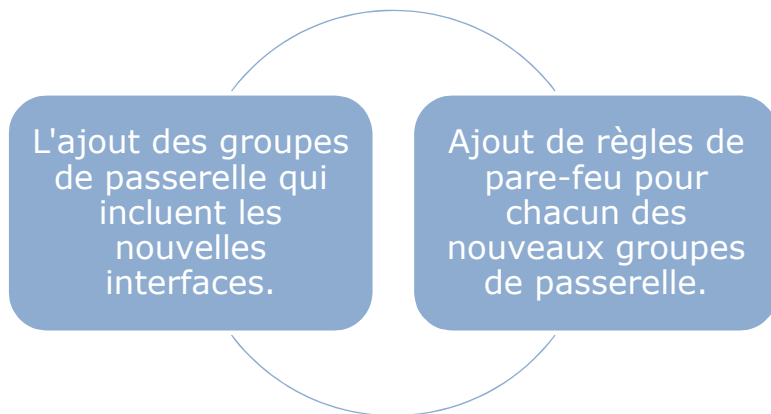
Procédure



Une formation
Alphorm.com



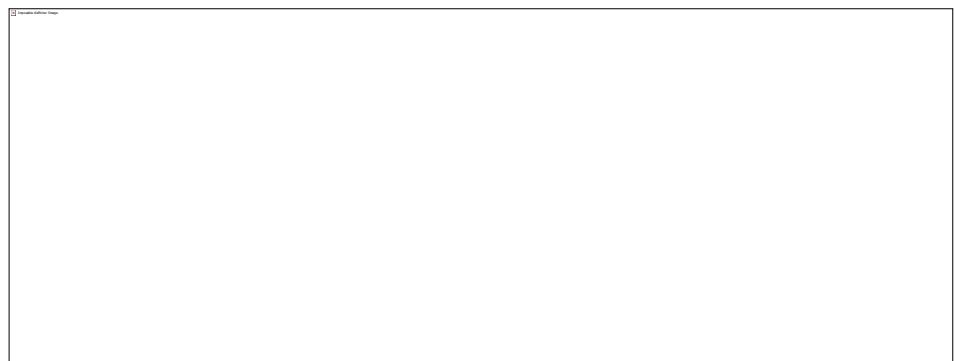
Procédure



Une formation
Alphorm.com



Lab : Multi Wan



Une formation
Alphorm.com

Merci



Introduction aux packages avec PfSense



Hamza KONDAH



Introduction

Modules ou packages
complémentaires

Amélioration de l'efficacité de PfSense

Possibilité de le rendre aussi efficace
qu'un UTM

Multifonctions !

Une formation
Alphorm
com

Merci



Une formation
Alphorm.com

Snort



Hamza KONDAH



Une formation
Alphorm.com

Plan

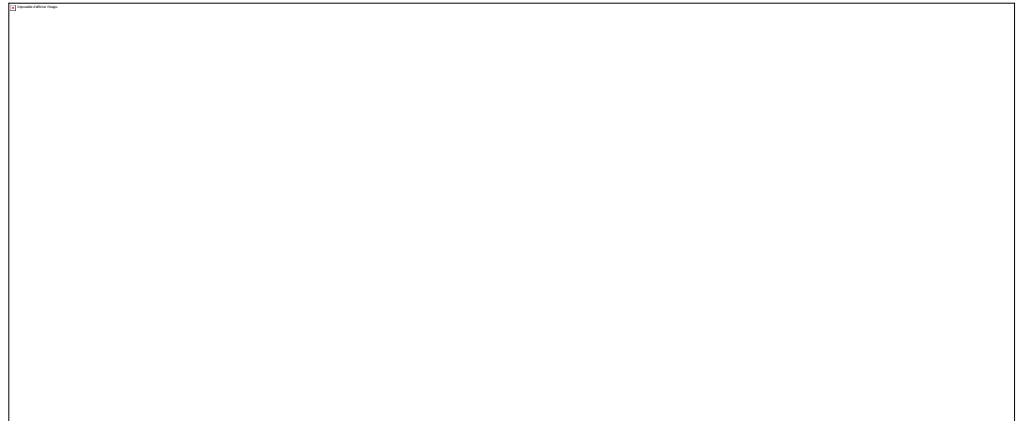
Les IDS

Snort

Lab : Le package Snort



Les IDS



Une formation
Alphorm.com



Snort



C'est un système de détection d'intrusion
réseau (ou NIDS)

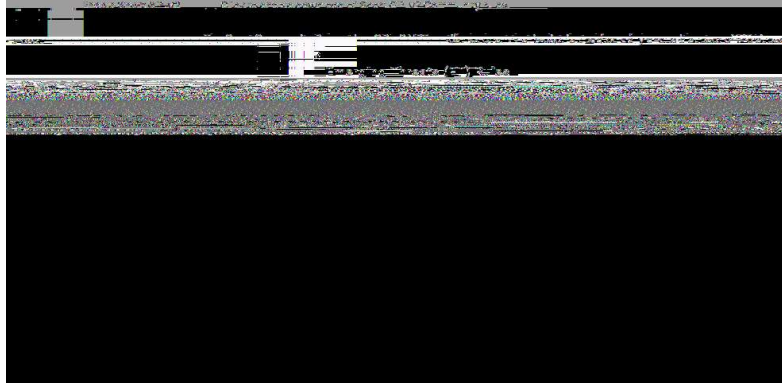
Open Source

C'est un des plus actifs NIDS Open Source et
possède une communauté importante
contribuant à son succès

Une formation
Alphorm.com



Lab : Le package Snort



Une formation
Alphorm.com

Merci



Une formation
Alphorm.com

Squid/SquidGuard



Hamza KONDAH



Une formation
Alphorm.com

Plan

Les Proxys

Squid

SquidGuard

Lab : Squid/SquidGuard



Les Proxys



Une formation
Alphorm.com



Squid

Un serveur Proxy et Reverse Proxy
Il gère les protocoles FTP, HTTP, Gopher,
et HTTPS
Il gère toutes les requêtes en un seul
processus d'entrée/sortie asynchrone
OpenSource

Une formation
Alphorm.com



SquidGuard

Orienté Web

Filtrage URL

BlackList

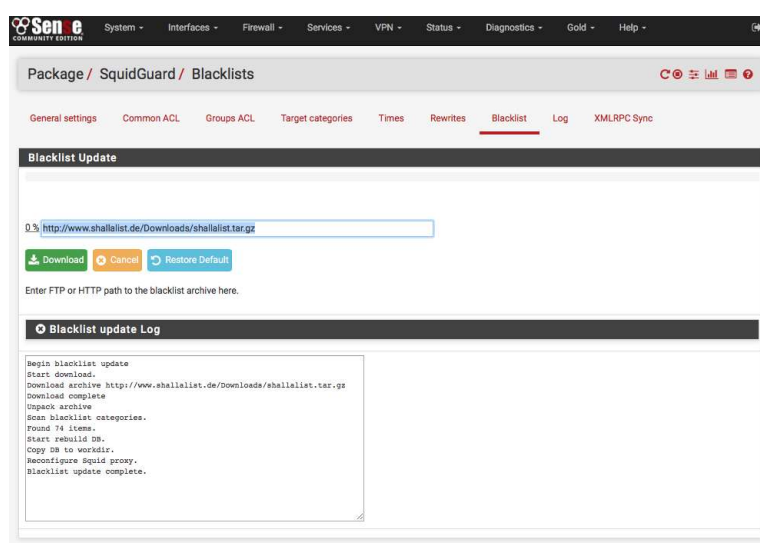
Combinaison avec Squid

Une formation
Alphorm.com



Lab : Squid/SquidGuard

Une formation
Alphorm.com



Merci



pfBlockerNg



Hamza KONDAH



Une formation
Alphorm.com

Plan

Introduction

Architecture

Lab : pfBlockerNg



Une formation
Alphorm.com

Introduction

Paquet très puissant

Permet d'étendre les fonctionnalités

Dépasse le filtrage traditionnel
(L2/L3/L4)

Filtrage avancé



Une formation
Alphorm.com

Introduction

Filtrage basé sur :

Géolocalisation

Domaine
source

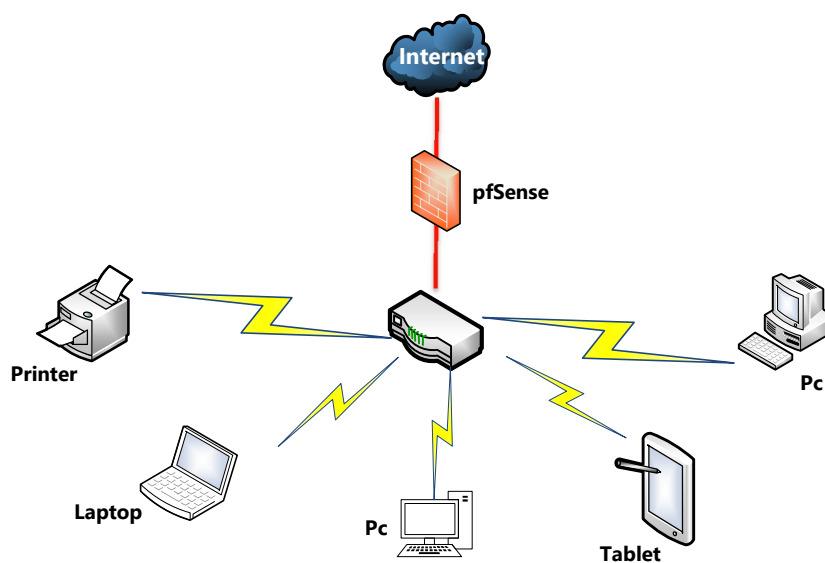
Alexa

Etc ...



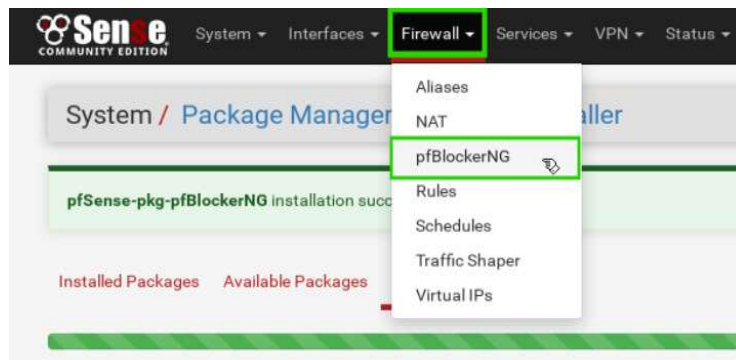
Une formation
Alphorm.com

Architecture





Lab : pfBlockerNg



Une formation
Alphorm.com

Merci



Une formation
Alphorm.com

NtopNG



Hamza KONDAH



Une formation
Alphorm.com

Plan

Introduction

Lab : NtopNG



Introduction

Supervision des réseaux

Visualisation de l'état des nœuds en
temps réel

Très beaux graphs 😊

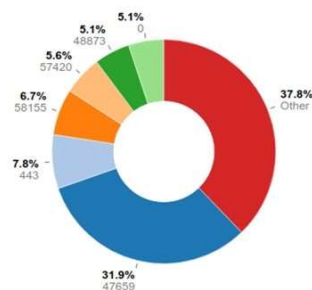
Interface Web

Une formation
Alphorm.com

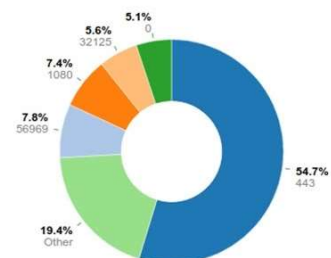


Lab : NtopNG

Top Client Ports



Top Server Ports



Une formation
Alphorm.com

Merci



Suricata



Hamza KONDAH



Plan

Introduction

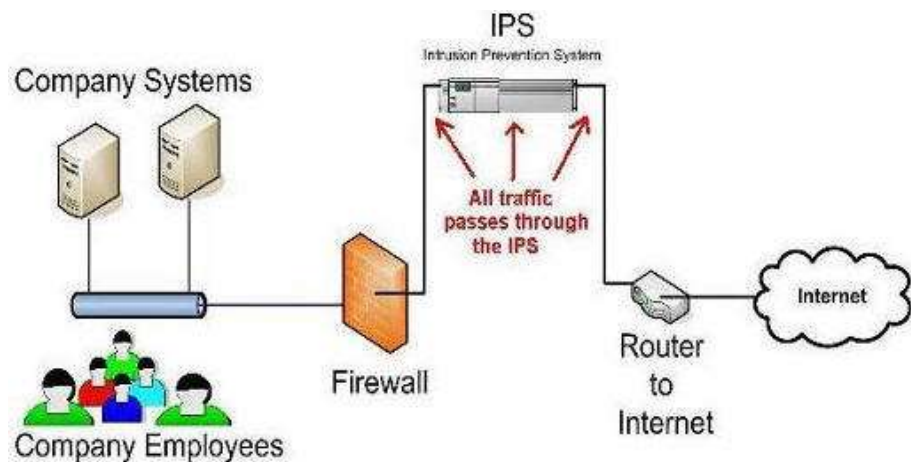
Suricata

Lab : Suricata

Une formation
Alphorm.com



Introduction



Une formation
Alphorm.com



Suricata

Parmi les IPS les plus performants

Très puissant

Open Source

Modulable

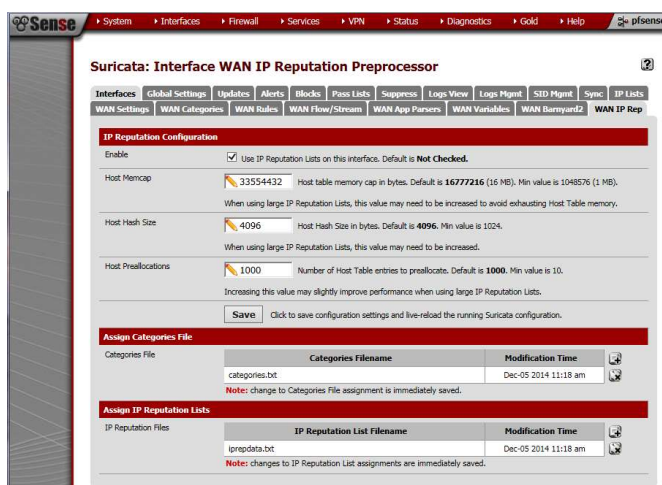
Protection Efficace

PS : Le positionnement est important !

Une formation
Alphorm.com



Lab : Suricata



Une formation
Alphorm.com

Merci



Squid/SquidGuard Partie 2

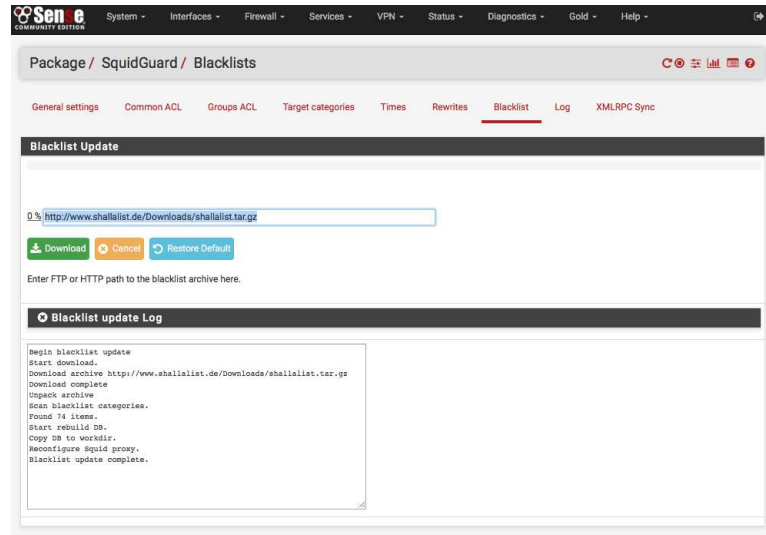


Hamza KONDAH



Une formation
Alphorm.com

Lab : Squid/SquidGuard



Merci



Une formation
Alphorm.com

Monitoring et Logging



Hamza KONDAH



Une formation
Alphorm.com

Monitoring et Logging

Les Logs représentent une mine d'or
La supervision et la transformation des logs
en informations décisionnelles est plus que
primordiale
Troubleshooting mais aussi analyse des
menaces



Monitoring et Logging

Logs

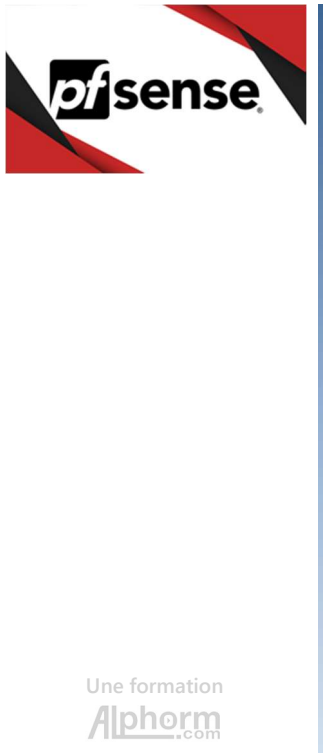
Solutions SIEM

Solutions de gestion et corrélation de
logs

Analyse des états du FW

Une formation
Alphorm
com

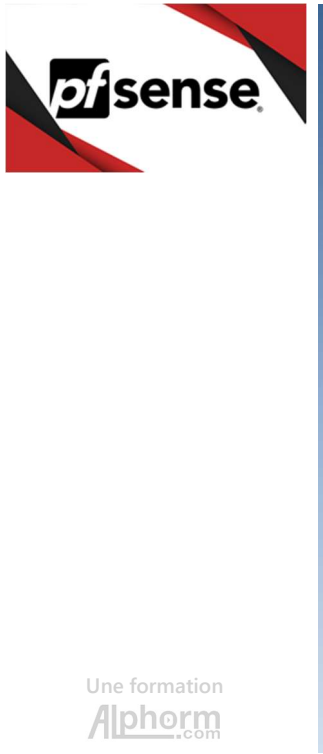
Merci



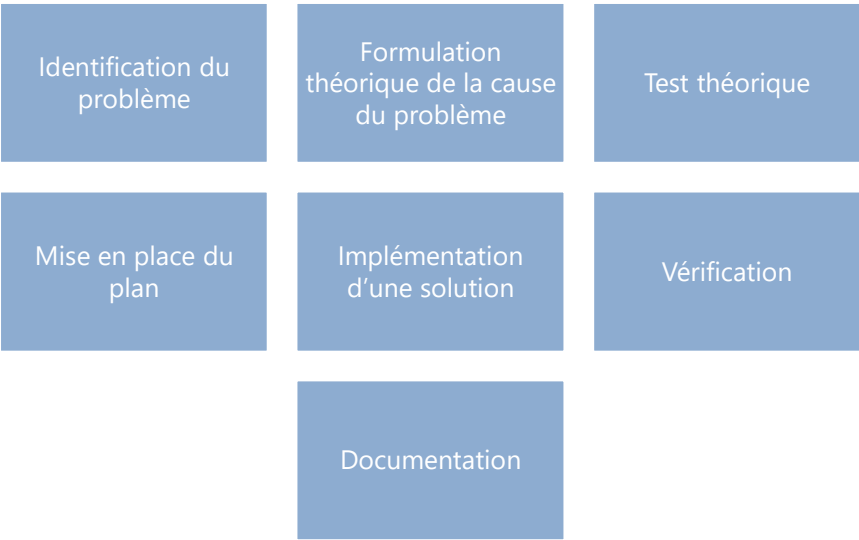
Troubleshooting



Hamza KONDAH



Procédure Troubleshooting



Merci



Test de règles de sécurité



Hamza KONDAH



Plan

NMAP

TCPDUMP/WIRESHARK

Lab : Test de règles

Une formation
Alphorm
com



NMAP

Scanner de sécurité

La référence ABSOLUE !

Complet pour le scan mais aussi les
tests de sécurité

NSE : Langage de Scripting !

Une formation
Alphorm
com



Une formation
Alphorm.com

TCPDUMP

Débogage réseau

Analyse de trafic

Ligne de commande

Graphique → Wireshark

Analyse et développement de
protocoles



Une formation
Alphorm.com

TCPDUMP

Débogage réseau

Analyse de trafic

Ligne de commande

Graphique → Wireshark

Analyse et développement de
protocoles



Lab : Test de règles

```
root@laptop:/home/synner# hping3 -S -c 1 -s 5151 10.0.0.4
HPING 10.0.0.4 (wlan0 10.0.0.4): S set, 40 headers + 0 data bytes
len=46 ip=10.0.0.4 ttl=64 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=1.2 ms

--- 10.0.0.4 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 1.2/1.2/1.2 ms
```

```
21:14:56.759191 IP 10.0.0.6.5151 > 10.0.0.4.0: Flags [S], seq 2088421809, win 512, length 0
21:14:56.760302 IP 10.0.0.4.0 > 10.0.0.6.5151: Flags [R.], seq 0, ack 2088421810, win 0, length 0
```

Merci



Une formation
Alphorm.com

Stress Testing



Hamza KONDAH



Une formation
Alphorm.com

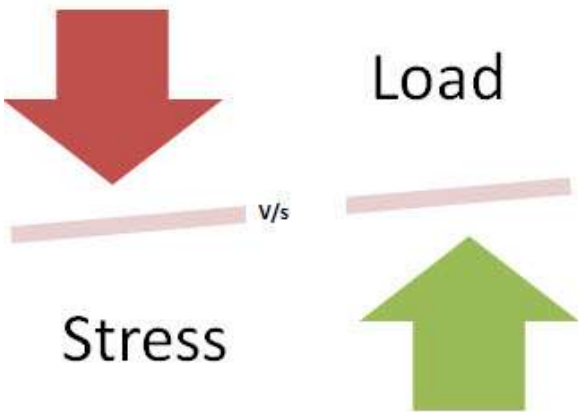
Plan

Introduction

Lab : Stress Testing



Introduction



Une formation
Alphorm.com



Lab : Stress Testing

```
root@lotusblack: ~  
File Edit View Search Terminal Help  
root@lotusblack:~# ./goldeneye.py -h  
bash: ./goldeneye.py: Permission denied  
root@lotusblack:~# chmod 777 goldeneye.py  
root@lotusblack:~# ./goldeneye.py -h  
-----  
USAGE: ./goldeneye.py <url> [OPTIONS]  
  
OPTIONS:  
Flag Description D  
default  
-w, --workers Number of concurrent workers (0  
default: 50)  
-s, --sockets Number of concurrent sockets (0  
default: 30)  
-m, --method HTTP Method to use 'get' or 'post' or 'random' (default: get)  
-d, --debug Enable Debug Mode [more verbose output] (default: False)  
-h, --help Shows this help
```

Une formation
Alphorm.com

Merci



Conclusion et Perspectives



Hamza KONDAH



Bilan

Introduction

Les VPNs

La Haute Disponibilité

La redondance

Routing et Bridging

Une formation
Alphorm
com



Bilan

Packages

Troubleshooting et test de sécurité

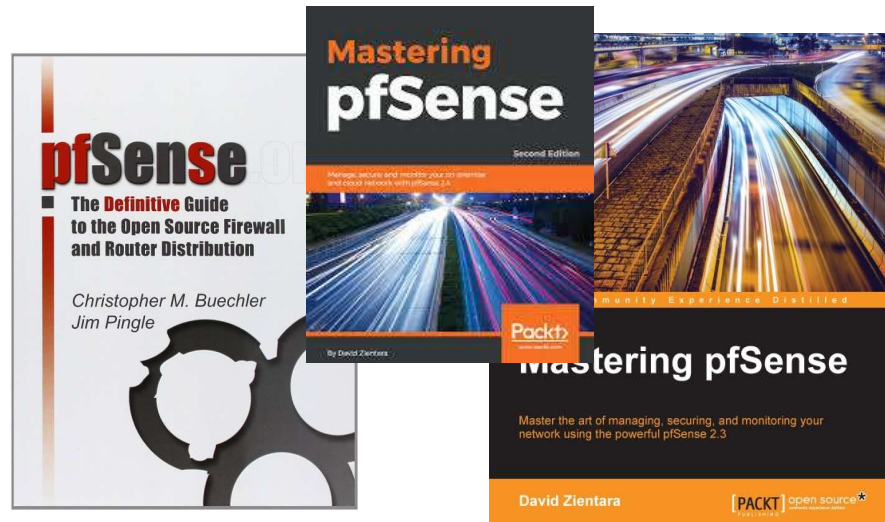
Benchmarking

Conclusion

Une formation
Alphorm
com



Bibliographie



Une formation
Alphorm.com



Prochainement



Une formation
Alphorm.com



Merci