

Compte-rendu

Contexte :

La société Amine nous a demandé d'intervenir afin de concevoir un réseau à haute disponibilité à l'aide du protocole CARP qui permet de faire de la redondance avec un basculement automatique. Celui-ci permet de partager une adresse IP pour automatiser le basculement sur les routeurs, le routeur maître est le propriétaire de l'adresse partagée mais une fois qu'il tombe en panne c'est le routeur esclave qui la possède. On mettra en place une adresse IP virtuelle qui n'est connectée à aucun hôte, celle-ci va recevoir les paquets envoyés par les deux routeurs pour ensuite communiquer avec la station cliente en Windows 10. Enfin, on installe un package nommé Snort qui permet de détecter et prévenir des intrusions. La règle qui nous intéresse est celle qui bloque les téléchargement en peer to peer car ce protocole permet d'échanger des fichiers d'une station à une autre sans passer par un serveur. En entreprise, c'est un problème car la plupart des fichiers mis à disposition par ce protocole sont des fichiers soumis à des droits d'auteurs.

Sommaire:

- 1 - Configuration des routeurs Pfsense avec CARP (protocole de redondance et haute disponibilité)
- 2 - Configuration et mise en place d'un VIP (adresse virtuelle privée)
- 3 - Mise en place de Snort
- 4 - Test de la redondance sur le poste client

Prérequis :

- Deux routeurs Pfsense
- Poste client Windows 10

Explication :

Tout d'abord, nous allons installer deux routeurs Pfsense configurés avec trois interfaces.

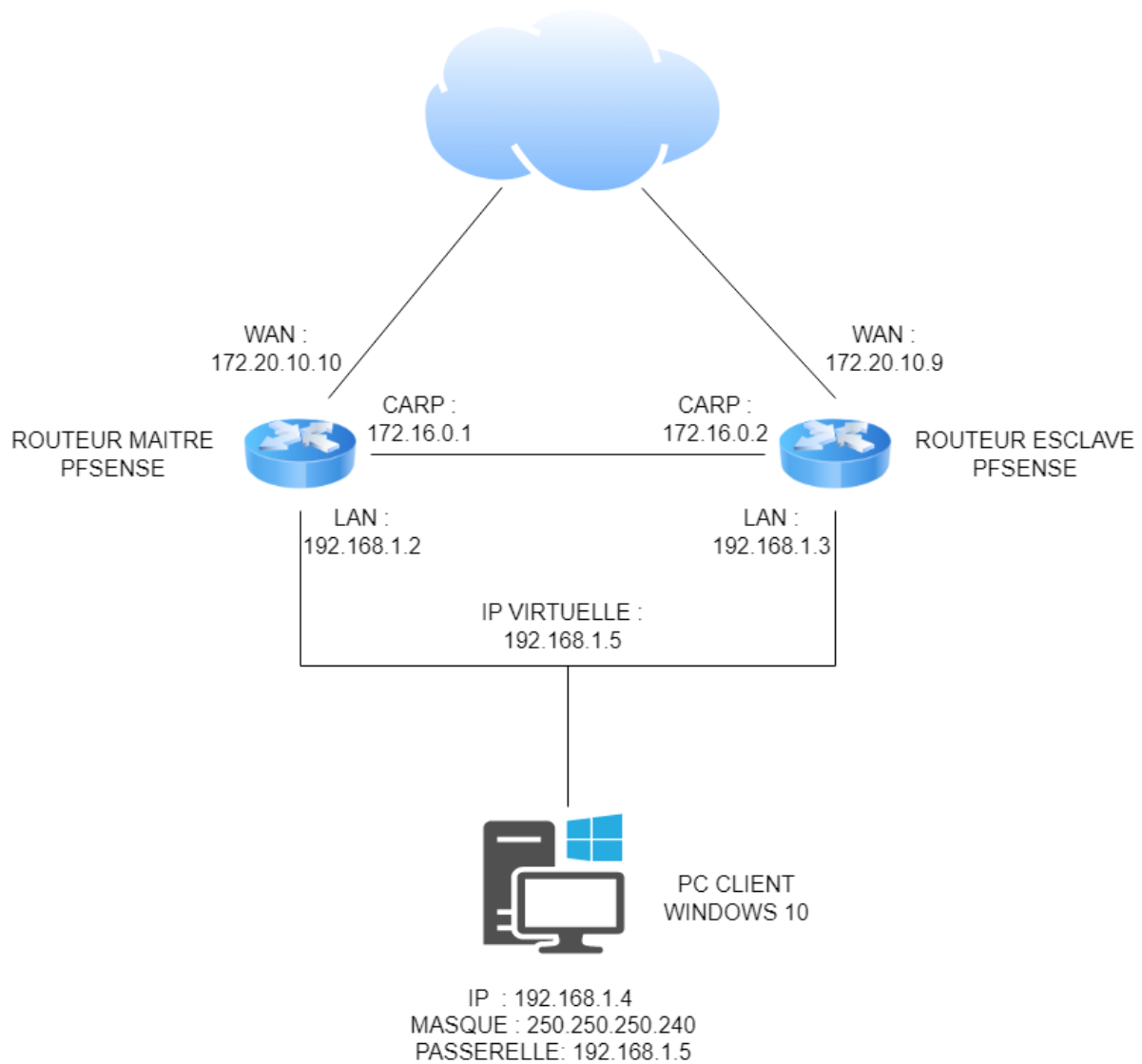
Ensuite, nous allons configurer ses deux routeurs en configurant la haute disponibilité.

Puis, on mettra en place une adresse virtuel privé (VIP). Il faut savoir qu'un PC ne peut ajouter qu'une seule passerelle dans sa carte réseau donc c'est pour cela qu'on est obligé de passer par une adresse ip virtuelle qui se chargera de recevoir les paquets des deux routeurs.

On installera et on configurera un package nommé Snort.

Enfin, nous allons effectuer des tests avec les routeurs Pfsense pour vérifier la redondance de ceux-ci.

Schéma de la mission :



Tutoriel:

1- Configuration des routeurs Pfsense avec CARP (protocole de redondance et haute disponibilité)

Routeur Pfsense Maître :

```
done.
pfSense 2.5.2-RELEASE amd64 Fri Jul 02 15:33:00 EDT 2021
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

VMware Virtual Machine - Netgate Device ID: c09d2de3404294efc072

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 172.20.10.10/28
LAN (lan)      -> em1      -> v4: 192.168.1.2/28
CARP (opt1)    -> em2      -> v4: 172.16.0.1/28

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) 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: █
```

Routeur Pfsense Esclave :

```
Starting package snort...done.
pfSense 2.5.2-RELEASE amd64 Fri Jul 02 15:33:00 EDT 2021
Bootup complete

FreeBSD/amd64 (pfSense.home.arp) (ttyv0)

VMware Virtual Machine - Netgate Device ID: d40dba71610ed73630fd

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 172.20.10.9/28
LAN (lan)      -> em1      -> v4: 192.168.1.3/28
CARP (opt1)    -> em2      -> v4: 172.16.0.2/28

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) 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: █
```

On assigne une troisième interface qu'on appellera CARP pour faire communiquer les paquets entre les deux routeurs.

Système / Synchronisation haute disponibilité

Paramètres de synchronisation d'état (pfsync)

Etat de la synchronisation

☒ Messages de pfsync pour état d'insertion, transfert, et suppression entre firewalls.

Chaque pare-feu envoie ces messages via multicast sur une interface spécifiée, en utilisant le protocole PFSYNC (protocole IP 240). Il écoute également cette interface pour des messages similaires provenant d'autres pare-feux et les importe dans la table d'état locale. Ce paramètre devrait être activé sur tous les membres d'un groupe de basculement. Cliquer sur "Enregistrer" forcera une synchronisation de configuration Si elle est activée! (Voir Paramètres de synchronisation de configuration ci-dessous)

Synchroniser l'interface

CARP

Si les états de synchronisation sont activés, cette interface sera utilisée pour la communication. Il est recommandé de configurer cette option sur une interface autre que LAN ! Une interface dédiée fonctionne le mieux. Une IP doit être définie sur chaque machine participant à ce groupe de basculement. Une IP doit être affecté à l'interface sur les nœuds de synchronisation participants.

IP de synchronisation pfsync du pair

172.16.0.2

Le réglage de cette option obligera Pfsync à synchroniser sa table d'état avec cette adresse IP. La sélection par défaut est multicast dirigé.

Paramètres de synchronisation de configuration (XMLRPC Sync)

Synchroniser la configuration avec IP

172.16.0.2

Entrez l'adresse IP du pare-feu à laquelle les sections de configuration sélectionnées doivent être synchronisées.

La synchronisation XMLRPC n'est actuellement prise en charge que sur les connexions utilisant le même protocole et le même port que ce système - assurez-vous que le port et le protocole du système distant sont définis en conséquence ! N'utilisez pas l'option Synchroniser la configuration sur IP et le mot de passe sur les membres du cluster de sauvegarde!

Nom d'utilisateur du système distant

admin

Entrez le nom d'utilisateur de WebConfigurator du système saisi ci-dessus pour la synchronisation de la configuration. N'utilisez pas l'option Synchroniser la configuration sur IP et le nom d'utilisateur sur les membres du cluster de sauvegarde !

Mot de passe du système distant

Confirmer

Entrez le mot de passe du système de configuration Internet configuré ci-dessus pour la synchronisation de la configuration. N'utilisez pas l'option Synchroniser la configuration sur IP et mot de passe sur les membres du cluster de sauvegarde !

Synchronize admin

☐ synchronize admin accounts and autoupdate sync password.

By default, the admin account does not synchronize, and each node may have a different admin password. This option automatically updates XMLRPC Remote System Password when the password is changed on the Remote System Username account.

Sélectionnez les options à synchronizer

☒ Gestion d'utilisateurs: Utilisateurs et Groupes

☒ Serveurs d'authentification (e.g LDAP, RADIUS)

☒ Listes des Autorités de Certification, Certificats, et Certificats de Révocation

☒ Règles du Pare-feu

☒ Planifications du Pare-feu

☒ alias du Pare-feu

☒ Configuration NAT

☒ Configuration IPsec

☒ OpenVPN configuration (Implies CA/Cert/CRL Sync)

☒ Paramètres du serveur DHCP

☒ Paramètres du serveur WoL

☒ Configuration des routes statiques

☒ Adresses IP virtuel

☒ Configuration du régulateur de flux

☒ Configuration des limitations du régulation du trafic

☒ Configurations du DNS Forwarder et du DNS Resolver

☒ Portail captif

☒ Toggle All

On synchronise le routeur maître avec le routeur esclave en spécifiant l'interface qui permet de communiquer les deux routeurs. On spécifie aussi l'ip du routeur esclave qui prendra le relais. On choisit de cocher toutes les options à synchroniser si jamais le routeur esclave doit prendre le relais.

Système / Synchronisation haute disponibilité

Paramètres de synchronisation d'état (pfsync)

Etat de la synchronisation

☒ Messages de pfsync pour état d'insertion, transfert, et suppression entre firewalls.
Chaque pare-feu envoie ces messages via multicast sur une interface spécifiée, en utilisant le protocole PFSYNC (protocole IP 240). Il écoute également cette interface pour des messages similaires provenant d'autres pare-feux et les importe dans la table d'état locale.
Ce paramètre devrait être activé sur tous les membres d'un groupe de basculement.
Cliquer sur "Enregistrer" forcera une synchronisation de configuration Si elle est activée! (Voir Paramètres de synchronisation de configuration ci-dessous)

Synchroniser l'interface

CARP

Si les états de synchronisation sont activés, cette interface sera utilisée pour la communication.
Il est recommandé de configurer cette option sur une interface autre que LAN ! Une interface dédiée fonctionne le mieux.
Une IP doit être définie sur chaque machine participant à ce groupe de basculement.
Une IP doit être affecté à l'interface sur les nœuds de synchronisation participants.

IP de synchronisation pfsync du pair

172.16.0.1

Le réglage de cette option obligera Pfsync à synchroniser sa table d'état avec cette adresse IP. La sélection par défaut est multicast dirigé.

On fait de même sur le routeur esclave en spécifiant l'interface et l'ip du routeur Maître. Ici, il ne faut pas remplir les autres sections car on veut seulement que celui-ci soit un routeur de secours.

2- Configuration et mise en place d'un VIP (adresse virtuelle privée)

Pare-feu / IPs virtuels / Modifier

Modifier l'IP virtuelle

Type

☐ Alias IP

☒ CARP

☐ Mandataire (proxy) ARP

☐ Autre

Interface

LAN

Type d'adresse

Adresse unitaire

Adresse(s)

192.168.1.5

/ 28

Le masque doit être le masque de sous-réseau du réseau. Il ne spécifie pas une plage CIDR.

Mot de passe d'IP virtuelle

.....

.....

Entrez le mot de passe du groupe VHID.

Confirmer

Groupe VHID

1

Entrez le nom du groupe VHID qui sera partagé.

Fréquence d'annonce

1

0

Base

Biais

La fréquence à laquelle cette machine effectue ses annonces. Autrement, la plus petite combinaison des valeurs de la grappe déterminera le maître.

Description

IPV

Une description peut être saisie ici à des fins de référence administrative (non analysée).

Enregistrer

On ajoute une adresse ip virtuelle sur nos deux routeurs qui permettra de communiquer des paquets avec celle-ci.

3- Mise en place de Snort (Système qui détecte et prévient des intrusions)

Services / **Snort** / Global Settings ?

Snort Interfaces Global Settings **Mises à jour** Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Snort Subscriber Rules

Enable Snort VRT ☒

Click to enable download of Snort free Registered User or paid Subscriber rules

[Sign Up for a free Registered User Rules Account](#)
[Sign Up for paid Snort Subscriber Rule Set \(by Talos\)](#)

Snort Oinkmaster Code

195fecb40b2d27de80e7d0ee11d921c43754e5b9

Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL!)

Snort GPLv2 Community Rules

Enable Snort GPLv2 ☐

Click to enable download of Snort GPLv2 Community rules

The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.

Emerging Threats (ET) Rules

Enable ET Open ☐

Click to enable download of Emerging Threats Open rules

ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.

Enable ET Pro ☐

Click to enable download of Emerging Threats Pro rules

[Sign Up for an ETPro Account](#)
ETPro for Snort offers daily updates and extensive coverage of current malware threats.

Sourcefire OpenAppID Detectors

Enable OpenAppID ☐

Click to enable download of Sourcefire OpenAppID Detectors

The OpenAppID Detectors package contains the application signatures required by the AppID preprocessor and the OpenAppID text rules.

OpenAppID Version

Enable AppID Open Text Rules ☐

Click to enable download of the AppID Open Text Rules

Note - the AppID Open Text Rules file is maintained by a volunteer contributor and hosted by the pfSense team. The URL for the file is https://files.netgate.com/openappid/appid_rules.tar.gz.

FEODO Tracker Botnet C2 IP Rules

Enable FEODO Tracker Botnet C2 IP Rules

☐ Click to enable download of FEODO Tracker Botnet C2 IP rules

Feodo Tracker tracks certain families that are related to, or that evolved from, Feodo. Originally, Feodo was an ebanking Trojan used by cybercriminals to commit ebanking fraud. Since 2010, various malware families evolved from Feodo, such as Cridex, Dridex, Geodo, Heodo and Emotet.

Rules Update Settings

Update Interval

1 DAY

Please select the interval for rule updates. Choosing NEVER disables auto-updates.

Update Start Time

00:00

Enter the rule update start time in 24-hour format (HH:MM). Default is 00 hours with a randomly chosen minutes value. Rules will update at the interval chosen above starting at the time specified here. For example, using a start time of 00:08 and choosing 12 Hours for the interval, the rules will update at 00:08 and 12:08 each day. The randomized minutes value should be retained to minimize the impact to the rules update site from large numbers of simultaneous requests.

Hide Deprecated Rules Categories

☐ Click to hide deprecated rules categories in the GUI and remove them from the configuration. Default is not checked.

Disable SSL Peer Verification

☐ Click to disable verification of SSL peers during rules updates. This is commonly needed only for self-signed certificates. Default is not checked.

Paramètres généraux

Remove Blocked Hosts Interval

1 HOUR

Please select the amount of time you would like hosts to be blocked. In most cases, one hour is a good choice.

Remove Blocked Hosts After Deinstall

☐ Click to clear all blocked hosts added by Snort when removing the package. Default is checked.

Keep Snort Settings After Deinstall

☒ Click to retain Snort settings after package removal.

Startup/Shutdown Logging

☐ Click to output detailed messages to the system log when Snort is starting and stopping. Default is not checked.

Enregistrer

On active Snort VRT en spécifiant le code qu'on nous a donné sur le site de Snort en s'inscrivant à l'abonnement gratuit de 30 jours. On choisit l'intervalle de mise à jour à un jour.

Update Your Rule Set

Last Update

Dec-19 2022 00:00

Result: Success

Update Rules

Update Rules

Force Update

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

Il faut s'assurer que la mise à jour des règles soit effectuée.

Services / Snort / Interface Settings / WAN - Categories

Snort Interfaces
Global Settings
Mises à jour
Alerts
Blocked
Pass Lists
Suppress
IP Lists
SID Mgmt
Log Mgmt
Sync

WAN Paramètres
WAN Categories
WAN Règles
WAN Variables
WAN Preprocs
WAN IP Rep
WAN Journaux

Automatic Flowbit Resolution

Resolve Flowbits

☒ If checked, Snort will auto-enable rules required for checked flowbits. Default is Checked.
 Snort will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

Snort Subscriber IPS Policy Selection

Use IPS Policy

☐ If checked, Snort will use rules from one of three pre-defined IPS policies in the Snort Subscriber rules. Default is Not Checked.
 Selecting this option disables manual selection of Snort Subscriber categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort VRT.

Select the rulesets (Categories) Snort will load at startup

☒ - Category is auto-enabled by SID Mgmt conf files
☐ - Category is auto-disabled by SID Mgmt conf files

Select All

Unselect All

Enregistrer

<input type="checkbox"/>	snort_file-multimedia.rules	<input type="checkbox"/>	snort_protocol-snmp.so.rules
<input type="checkbox"/>	snort_file-office.rules	<input type="checkbox"/>	snort_protocol-tftp.so.rules
<input type="checkbox"/>	snort_file-other.rules	<input type="checkbox"/>	snort_protocol-voip.so.rules
<input type="checkbox"/>	snort_file-pdf.rules	<input checked="" type="checkbox"/>	snort_pua-p2p.so.rules
<input type="checkbox"/>	snort_finger.rules	<input type="checkbox"/>	snort_server-iis.so.rules
<input type="checkbox"/>	snort_ftp.rules	<input type="checkbox"/>	snort_server-mail.so.rules
<input type="checkbox"/>	snort_icmp-info.rules	<input type="checkbox"/>	snort_server-mysql.so.rules
<input type="checkbox"/>	snort_icmp.rules	<input type="checkbox"/>	snort_server-oracle.so.rules
<input type="checkbox"/>	snort_imap.rules	<input type="checkbox"/>	snort_server-other.so.rules
<input type="checkbox"/>	snort_indicator-compromise.rules	<input type="checkbox"/>	snort_server-webapp.so.rules
<input type="checkbox"/>	snort_indicator-obfuscation.rules		
<input type="checkbox"/>	snort_indicator-scan.rules		

Il faut décocher la deuxième case pour pouvoir choisir les règles que l'on veut activer. La règle qui nous intéresse ici est celle du téléchargement par peer to peer.

4- Test de la redondance sur notre poste client

État / CARP

Désactiver temporairement CARP

Entrer en mode de maintenance CARP persistant

Interfaces CARP		
Interface CARP	adresse IP virtuelle	État
LAN@1	192.168.1.5/28	MASTER

Noeuds pfSync

noeuds pfSync:

20e3187c
6051b403
97e43a71
ee77e98e
ff374f27

État / CARP

Désactiver temporairement CARP

Quitter le mode de maintenant CARP persistant

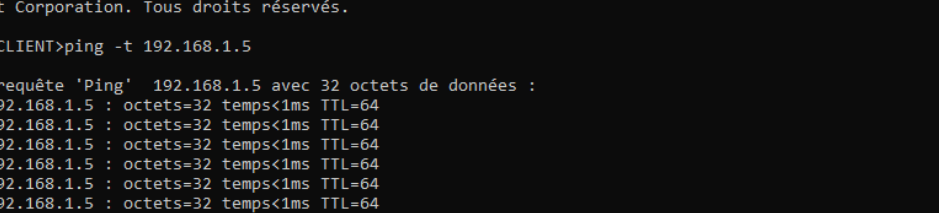
Interfaces CARP		
Interface CARP	adresse IP virtuelle	État
LAN@1	192.168.1.5/28	BACKUP

Noeuds pfSync

noeuds pfSync:

20e3187c
 6051b403
 97e43a71
 ee77e98e
 ff374f27

On vérifie d'abord si les routeurs sont bien mis en place pour permettre une haute disponibilité. On voit le routeur maître à un état valide en master et le routeur esclave à l'état backup en pause.



The screenshot shows a Windows command prompt window titled "Invite de commandes - ping -t 192.168.1.5". The window content displays the output of a continuous ping command to the IP address 192.168.1.5. The output shows 10 successful responses, each with a time of less than 1ms and a TTL of 64. The command prompt is at the C:\Users\PC CLIENT directory.

```
Microsoft Windows [version 10.0.19045.2006]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\PC CLIENT>ping -t 192.168.1.5

Envoi d'une requête 'Ping' 192.168.1.5 avec 32 octets de données :
Réponse de 192.168.1.5 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.5 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.5 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.5 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.5 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.5 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.5 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.5 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.5 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.5 : octets=32 temps<1ms TTL=64
Délai d'attente de la demande dépassé.
Réponse de 192.168.1.5 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.5 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.5 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.5 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.5 : octets=32 temps<1ms TTL=64
```

On désactive le routeur maître et on remarque qu'en faisant un ping continu, le deuxième routeur prend le relais juste après.



Le routeur esclave devient donc le maître jusqu'à ce que le principal routeur revienne.

Conclusion :

On a bien rempli la mission qui est de mettre en place deux routeurs dans notre architecture réseau pour avoir un backup si jamais le premier tombe en panne. Celui-ci possède un package qui permet de bloquer les téléchargements en peer to peer pour éviter d'avoir des incidents dans notre entreprise. On a mis en place une adresse ip virtuelle pour faire transiter les paquets des deux routeurs par cette ip qui n'est attaché à aucun hôte.