

# CONFIGURATIONS DE BASE SUR PFSENSE

## I- PRESENTATION DES INTERFACES RESEAU DANS PFSENSE

PFsense est un pare-feu open-source qui offre une grande flexibilité et une sécurité robuste pour les réseaux informatiques. L'une des clés de sa puissance réside dans sa capacité à gérer et à configurer diverses interfaces réseau, permettant ainsi aux administrateurs de créer des réseaux complexes et sécurisés. Les interfaces réseau de PFSense permettent de connecter et de configurer différents types de réseaux, tels que les réseaux locaux, les réseaux étendus, les réseaux Wi-Fi, les réseaux virtuels et les connexions VPN. Chaque interface réseau peut être configurée pour répondre à des besoins spécifiques, tels que la sécurité, la performance et la gestion du trafic. En comprenant les différentes interfaces réseau de PFSense, les administrateurs peuvent créer des réseaux sécurisés et efficaces qui répondent aux besoins de leur organisation.

PFsense offre plusieurs interfaces réseau pour configurer et gérer vos réseaux. Voici quelques-unes des principales interfaces réseau de PFSense :

- **LAN (Local Area Network)** : Interface pour configurer le réseau local, généralement utilisée pour les ordinateurs et les appareils du réseau interne.
- **WAN (Wide Area Network)** : Interface pour configurer la connexion à Internet, généralement utilisée pour les connexions DSL, câble ou fibre optique.
- **DMZ (Demilitarized Zone)** : Interface pour configurer un réseau DMZ, utilisée pour isoler les serveurs publics du réseau interne.
- **OPTx (Optional)** : Interfaces optionnelles pour configurer des réseaux supplémentaires, tels que des réseaux Wi-Fi, des réseaux de machines virtuelles, etc.
- **VPN (Virtual Private Network)** : Interface pour configurer des connexions VPN, utilisée pour établir des connexions sécurisées entre des réseaux distants.
- **Bridge** : Interface pour configurer des ponts réseau, utilisée pour connecter plusieurs réseaux ensemble.
- **VLAN (Virtual Local Area Network)** : Interface pour configurer des réseaux VLAN, utilisée pour diviser un réseau physique en plusieurs réseaux logiques.
- **WLAN (Wireless Local Area Network)** : Interface pour configurer des réseaux Wi-Fi, utilisée pour connecter des appareils sans fil au réseau.

Ces interfaces réseau permettent de configurer et de gérer vos réseaux de manière flexible et sécurisée avec PFSense.

Pour activer une interface réseau sur pfSense, suivez les étapes ci-dessous :

### ❖ Accéder à l'interface Web de pfSense

- Ouvrez un navigateur web et connectez-vous à l'interface pfSense en utilisant l'adresse IP de votre pare-feu par exemple, <https://192.168.147.2>.
- Entrez vos identifiants administrateur.

### ❖ Naviguer vers la configuration des interfaces

- Une fois connecté, allez dans le menu **Interfaces** en haut de la page.
- Sélectionnez **Assignments** pour voir les interfaces disponibles.

### ❖ Ajouter ou activer une interface

- Si vous souhaitez activer une interface existante :
  1. Sous **Interface Assignments**, identifiez l'interface que vous voulez activer.
  2. Cliquez sur l'interface (par exemple, em0, em1, etc.).
  3. Cochez la case **Enable** pour activer l'interface.
- Si vous voulez ajouter une nouvelle interface :
  1. Dans la section **Available Network Ports**, sélectionnez l'interface physique que vous voulez ajouter.
  2. Cliquez sur **Add** pour l'ajouter à la liste des interfaces assignées.
  3. Cliquez sur l'interface nouvellement ajoutée pour configurer ses paramètres.

### ❖ Configurer l'interface

- Configurez l'interface selon vos besoins :
  - **IPv4 Configuration Type** : Choisissez entre Static, DHCP, etc.
  - **IPv6 Configuration Type** : Choisissez le type d'adresse IPv6 si nécessaire.
  - **IP Address** : Entrez l'adresse IP si vous avez choisi Static.
  - Configurez les autres paramètres comme le masque de sous-réseau, la passerelle, etc.

### ❖ Sauvegarder la configuration

- Une fois les paramètres configurés, cliquez sur **Save** pour enregistrer les modifications.
- Appliquez les changements en cliquant sur **Apply Changes** en haut de la page.

### ❖ Vérifier l'activation

- Retournez à la page **Interfaces , Assignments** et vérifiez que l'interface est activée.
- Vous pouvez également aller dans **Status ,Interfaces** pour voir l'état actuel de toutes les interfaces activées.

## II-CONFIGURATION DU DHCP

Le **DHCP** (Dynamic Host Configuration Protocol) est un protocole réseau essentiel qui automatise l'attribution des paramètres IP aux dispositifs connectés à un réseau. Grâce au DHCP, les périphériques comme les ordinateurs, les smartphones, et les imprimantes peuvent obtenir automatiquement les informations nécessaires pour se connecter et communiquer sur un réseau sans avoir besoin d'une configuration manuelle.

## A-Fonctionnement du DHCP

1. **Découverte DHCP (DHCP Discover) :**
  - Lorsqu'un appareil (le **client DHCP**) se connecte à un réseau pour la première fois ou lorsqu'il cherche à renouveler son adresse IP, il envoie un message **DHCP Discover** sur le réseau pour localiser un serveur DHCP disponible.
2. **Offre DHCP (DHCP Offer) :**
  - En réponse, un serveur DHCP reçoit la requête et vérifie dans son pool d'adresses IP disponibles. Il propose ensuite une adresse IP et d'autres paramètres réseau au client en envoyant un message **DHCP Offer**.
3. **Demande DHCP (DHCP Request) :**
  - Le client DHCP choisit une offre (généralement la première reçue) et répond au serveur en envoyant un message **DHCP Request** pour accepter l'adresse IP proposée.
4. **Accusé de réception DHCP (DHCP Acknowledge) :**
  - Enfin, le serveur DHCP envoie un message **DHCP Acknowledge** au client pour confirmer que l'adresse IP a été attribuée. Le client peut alors configurer son interface réseau avec cette adresse IP et les autres paramètres reçus.

## B-Composants Principaux du DHCP

- **Serveur DHCP :** C'est l'appareil ou le logiciel qui gère le pool d'adresses IP et attribue ces adresses aux clients sur le réseau. Les routeurs domestiques et les serveurs d'entreprise remplissent souvent cette fonction.
- **Client DHCP :** Tout appareil ou hôte qui se connecte au réseau et nécessite une adresse IP, comme un ordinateur, un smartphone, une imprimante, etc.
- **Pool d'adresses IP :** Une plage d'adresses IP disponibles que le serveur DHCP peut attribuer dynamiquement aux clients. Par exemple, dans un réseau avec un pool 192.168.1.100 à 192.168.1.200, le serveur DHCP peut assigner n'importe quelle adresse IP dans cette plage aux clients.
- **Bail DHCP :** Chaque adresse IP attribuée par le DHCP est allouée pour une période de temps spécifique appelée **bail**. Une fois le bail expiré, le client doit demander une nouvelle adresse IP ou renouveler l'actuelle.

## C-Avantages du DHCP

- **Automatisation :** Le DHCP élimine le besoin de configurer manuellement les paramètres IP sur chaque appareil connecté au réseau, ce qui simplifie considérablement la gestion du réseau, en particulier dans les grandes entreprises ou les environnements à forte densité de dispositifs.
- **Flexibilité :** Les adresses IP sont attribuées dynamiquement en fonction de la disponibilité, ce qui évite les conflits d'adresses IP et permet une utilisation efficace des adresses disponibles.
- **Gestion centralisée :** Le DHCP permet une gestion centralisée des paramètres réseau, facilitant ainsi la mise en place de modifications et d'ajustements, comme la modification des adresses de passerelle ou des serveurs DNS.
- **Facilité d'extension du réseau :** Lorsque de nouveaux dispositifs sont ajoutés au réseau, ils peuvent immédiatement obtenir une adresse IP et se connecter sans nécessiter d'intervention manuelle.

## D-Limites et Considérations

- **Dépendance au serveur DHCP** : Si le serveur DHCP tombe en panne, les nouveaux dispositifs ne pourront pas obtenir d'adresse IP, ce qui pourrait entraîner une interruption du service réseau.
- **Sécurité** : Le DHCP est vulnérable à certaines attaques, comme les attaques par usurpation de serveur DHCP (Rogue DHCP), où un attaquant peut configurer un serveur DHCP malveillant sur le réseau.
- **Problèmes de connectivité** : Si le pool d'adresses IP est épuisé, de nouveaux dispositifs ne pourront pas se connecter au réseau, ce qui peut nécessiter une gestion proactive du pool IP.

## E-DHCP dans les Scénarios Réels

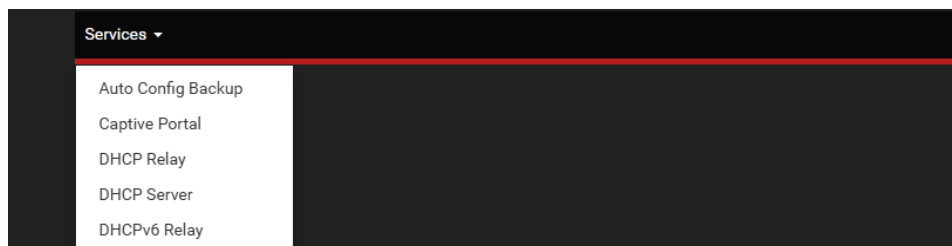
- **Réseaux domestiques** : Dans un environnement domestique, le routeur fournit généralement les services DHCP. Il attribue automatiquement les adresses IP aux appareils connectés, comme les ordinateurs, téléphones, tablettes, et appareils IoT.
- **Réseaux d'entreprise** : Dans les réseaux d'entreprise, des serveurs DHCP dédiés sont souvent utilisés pour gérer de grandes quantités de dispositifs, avec des configurations avancées telles que l'attribution d'adresses IP fixes (par réservation DHCP) à des dispositifs spécifiques, ou la segmentation du réseau avec des sous-réseaux.
- **Environnements temporaires** : Le DHCP est aussi utile dans des environnements temporaires, comme des événements ou des conférences, où il est nécessaire de connecter rapidement et efficacement un grand nombre de dispositifs à un réseau.

Le DHCP est un protocole essentiel qui simplifie la gestion des réseaux en automatisant l'attribution des adresses IP et d'autres paramètres réseau. Il est largement utilisé dans presque tous les types de réseaux, des petits réseaux domestiques aux grands réseaux d'entreprise, offrant des avantages significatifs en termes de gestion, de flexibilité et d'efficacité. Bien que le DHCP présente certaines limitations, il reste un composant fondamental des infrastructures réseau modernes.

## APPLICATION

Pour configurer le DHCP server sur pfSense nous devons suivre les étapes suivantes :

- ❖ Dans l'option service , choisir DHCPserver puis sélectionner l'interface sur laquelle on aimerait effectuer la configuration .



- ❖ Dans general option , cliquer sur Enable pour activer le service.
- ❖ Remplir les cases suivantes à partir de vos préférences .

- ❖ Ensuite au niveau de Range , choisir la plage d'adresse dans laquelle sera octroyer les adresses IP des utilisateurs.
- ❖ Continuer les configurations ensuite cliquer sur save.

LAN
DMZ

General DHCP Options

DHCP Backend	ISC DHCP
Enable	<input checked="" type="checkbox"/> Enable DHCP server on LAN interface
BOOTP	<input checked="" type="checkbox"/> Ignore BOOTP queries
Deny Unknown Clients	<div>Allow all clients</div> <p>When set to <b>Allow all clients</b>, any DHCP client will get an IP address within this scope/range on this interface. If set to <b>Allow known clients from any interface</b>, any DHCP client with a MAC address listed in a static mapping on <b>any</b> scope(s)/interface(s) will get an IP address. If set to <b>Allow known clients from only this interface</b>, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.</p>
Ignore Denied Clients	<input type="checkbox"/> Ignore denied clients rather than reject This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.
Ignore Client Identifiers	<input type="checkbox"/> Do not record a unique identifier (UID) in client lease data if present in the client DHCP request This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

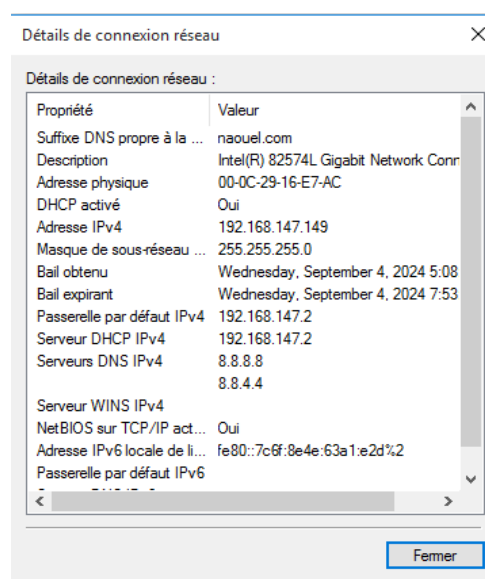
Primary Address Pool

Subnet	192.168.147.0/24	
Subnet Range	192.168.147.1 - 192.168.147.254	
Address Pool Range	<div>192.168.147.3</div> From	<div>192.168.147.245</div> To

The specified range for this pool must not be within the range configured on any other address

Une fois la configuration terminée , nous allons nous rendre vers notre machine windows qui un client pour tester les configurations.

- Dans la machine Windows, aller dans panneau de configuration , accéder aux paramètre de la carte reseau
- Faire un clic gauche sur la carte reseau et verifier au niveau de ipv4 adress pour voir l'adresse ip octroyer a notre client windows



- Si la configuration a belle et bien marcher , nous allons nous rentre sur notre tableau de bord de pfsense, sur status CHOISIR DHCP Leases pour voir les client en reseau avec le pfsense.

Status / DHCP Leases

ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit [System > Advanced > Networking](#) to switch DHCP backend.

Search

Search Term:  All

Enter a search string or \*nix regular expression to filter entries.

IP Address	MAC Address	Hostname	Description	Start	End	Action
192.168.147.149	00:0c:29:16:e7:ac	DESKTOP-EDTOHC9		2024/09/04 05:53:40	2024/09/04 07:53:40	<input type="button" value="+"/>

Lease Utilization

Interface	Pool Start	Pool End	Used	Capacity	Utilization
LAN	192.168.147.3	192.168.147.245	1	243	0% of 243

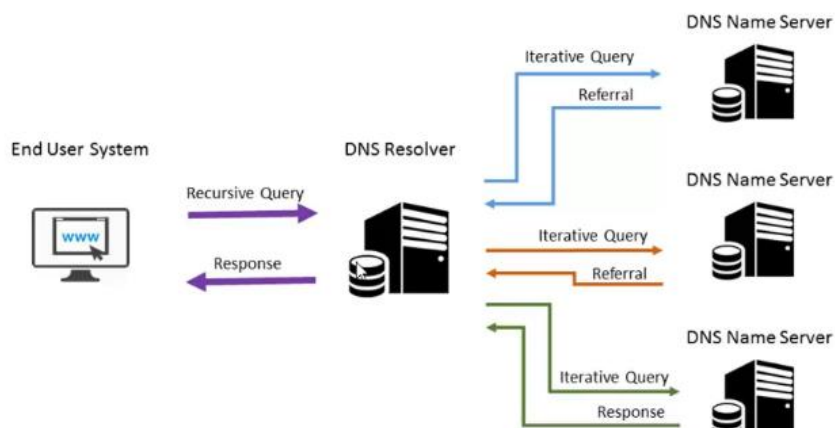
### III-CONFIGURATION DU DNS

Le DNS, ou Domain Name System, est un système qui traduit les noms de domaine lisibles par l'homme (comme [www.example.com](http://www.example.com)) en adresses IP numériques que les ordinateurs utilisent pour se connecter entre eux (par exemple, 192.168.1.1). En gros, c'est comme un annuaire téléphonique de l'internet : il permet de trouver l'adresse IP d'un serveur à partir du nom de domaine que vous saisissez dans votre navigateur.

Sans DNS, il serait beaucoup plus difficile pour les utilisateurs de se connecter à des sites web, car ils devraient connaître et se souvenir des adresses IP exactes. Le DNS simplifie l'accès à l'information sur Internet en associant des noms de domaine plus intuitifs à leurs adresses IP correspondantes.

Les principaux types de DNS de PFsense sont :

#### 1. DNS Resolver



Un **DNS Resolver** (ou résolveur DNS) est un serveur qui reçoit des requêtes DNS de clients (comme votre navigateur web) et retourne l'adresse IP associée au nom de domaine demandé. Il sert d'intermédiaire entre les clients et les serveurs DNS autoritaires (les serveurs qui possèdent les informations DNS originales).

Dans pfSense, un **DNS Resolver** (généralement basé sur Unbound) est utilisé pour résoudre les noms de domaine pour les clients du réseau local. Voici quelques fonctionnalités spécifiques de DNS Resolver dans pfSense :

- **Résolution DNS récursive** : Le DNS Resolver peut interroger directement les serveurs DNS racine, les serveurs TLD, et les serveurs DNS autoritaires pour résoudre les requêtes, plutôt que de s'appuyer sur des serveurs DNS publics comme Google DNS ou OpenDNS.
- **Mise en cache** : Le DNS Resolver de pfSense met en cache les réponses DNS, ce qui améliore les performances en réduisant les temps de résolution pour les requêtes répétées.
- **Host Overrides** : Vous pouvez définir des enregistrements DNS personnalisés pour des noms d'hôtes spécifiques, permettant de rediriger certaines requêtes DNS vers des adresses IP locales ou spécifiques.
- **Domain Overrides** : Vous pouvez rediriger toutes les requêtes DNS pour un domaine particulier vers un serveur DNS spécifique.
- **Sécurité** : Le DNS Resolver de pfSense prend en charge DNSSEC (DNS Security Extensions), une technologie qui permet de vérifier l'intégrité et l'authenticité des réponses DNS, protégeant ainsi contre les attaques de type spoofing.

### Avantages du DNS Resolver

- **Rapidité** : En utilisant un cache local, les résolveurs DNS peuvent fournir des réponses rapidement pour les requêtes fréquentes.
- **Sécurité** : En configurant des fonctionnalités comme DNSSEC, vous pouvez protéger votre réseau contre certaines menaces DNS.
- **Contrôle** : Avec un DNS Resolver comme celui de pfSense, vous avez un contrôle total sur la manière dont les requêtes DNS sont résolues, y compris la possibilité de créer des overrides pour des noms d'hôtes ou des domaines spécifiques.

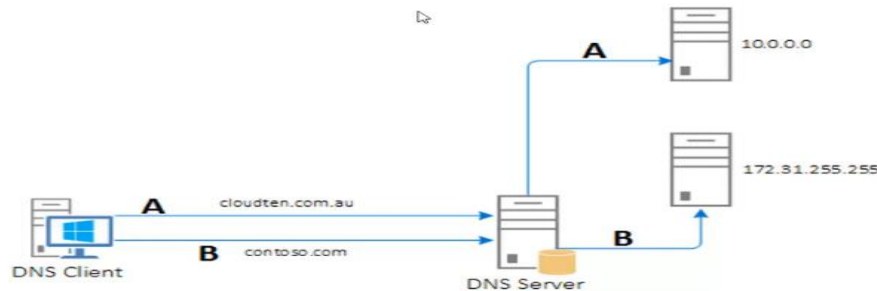
### Limites et Considérations

- **Complexité** : Configurer et maintenir un DNS Resolver peut être complexe, surtout si vous gérez un grand réseau.
- **Dépendance** : Si le DNS Resolver tombe en panne, il peut y avoir des interruptions de service, car les requêtes DNS ne peuvent pas être résolues.

En résumé, le DNS Resolver est un composant fondamental du réseau qui assure la résolution efficace des noms de domaine en adresses IP, tout en offrant des possibilités de contrôle, de sécurité et de performance améliorées pour les administrateurs réseau.

## DNS Forwarder ou transfert DNS

Le **DNS Forwarder** est un composant réseau qui joue un rôle clé dans la résolution des noms de domaine en facilitant et optimisant le processus de requêtes DNS. Contrairement au **DNS Resolver**, qui peut effectuer des requêtes récursives pour résoudre un nom de domaine, le DNS Forwarder agit comme un intermédiaire, redirigeant les requêtes DNS reçues vers un autre serveur DNS.



## Fonctionnement du DNS Forwarder

1. **Réception de la requête** : Lorsqu'un client (par exemple, votre ordinateur) envoie une requête DNS pour résoudre un nom de domaine (comme `www.example.com`), cette requête est d'abord reçue par le DNS Forwarder configuré sur votre réseau.
2. **Transfert de la requête** : Au lieu de résoudre la requête lui-même, le DNS Forwarder transmet cette requête à un autre serveur DNS, souvent appelé serveur DNS amont ou serveur DNS parent. Ce serveur peut être un serveur DNS public (comme Google DNS ou OpenDNS) ou un serveur DNS interne configuré pour votre réseau.
3. **Réponse à la requête** : Le serveur DNS amont résout la requête en traduisant le nom de domaine en adresse IP. Il renvoie ensuite cette information au DNS Forwarder.
4. **Renvoi de la réponse au client** : Enfin, le DNS Forwarder transmet la réponse au client d'origine, lui fournissant l'adresse IP associée au nom de domaine demandé.
5. **Mise en cache** : Souvent, le DNS Forwarder met en cache les réponses reçues. Cela permet d'accélérer les requêtes futures pour le même nom de domaine, car il pourra fournir une réponse immédiate à partir de son cache sans avoir à interroger le serveur DNS amont à nouveau.

## Cas d'utilisation du DNS Forwarder

- **Réseaux d'entreprise** : Dans les réseaux d'entreprise, un DNS Forwarder est souvent utilisé pour centraliser et contrôler les requêtes DNS des utilisateurs. Cela permet de filtrer ou de rediriger certaines requêtes, tout en réduisant le trafic DNS sortant vers l'Internet.
- **Optimisation des performances** : En utilisant un DNS Forwarder avec mise en cache, les entreprises et les utilisateurs domestiques peuvent réduire la latence des requêtes DNS, car les réponses pour les noms de domaine fréquemment demandés sont stockées localement.
- **Contrôle des DNS** : Un DNS Forwarder permet aux administrateurs réseau de choisir à quels serveurs DNS les requêtes sont transférées. Cela peut être utile pour appliquer des politiques de sécurité, comme l'utilisation de serveurs DNS qui bloquent les sites malveillants.



## DNS Forwarder dans pfSense

Dans pfSense, le DNS Forwarder (basé sur **dnsmasq**) est une fonctionnalité qui peut être activée pour rediriger les requêtes DNS reçues des clients vers un ou plusieurs serveurs DNS amont. Voici quelques caractéristiques spécifiques du DNS Forwarder dans pfSense :

- **Configuration simple** : Le DNS Forwarder de pfSense est facile à configurer via l'interface web, permettant aux administrateurs de définir quels serveurs DNS doivent être utilisés pour le transfert des requêtes.
- **Mise en cache** : Le DNS Forwarder met en cache les réponses DNS, ce qui réduit le temps de réponse pour les requêtes répétées.
- **Overrides** : Comme avec le DNS Resolver, vous pouvez définir des overrides pour rediriger des requêtes DNS spécifiques vers des adresses IP locales ou d'autres serveurs DNS, en contournant les serveurs DNS publics.
- **Compatibilité** : Le DNS Forwarder est souvent utilisé dans des environnements où un DNS Resolver n'est pas nécessaire ou souhaité, notamment dans des réseaux plus simples ou avec des configurations spécifiques qui nécessitent un transfert DNS direct.

## Avantages du DNS Forwarder

- **Simplicité** : Le DNS Forwarder est plus simple à configurer et à gérer que le DNS Resolver, surtout dans des environnements où la résolution récursive n'est pas nécessaire.
- **Contrôle** : Il offre un contrôle sur les serveurs DNS utilisés pour résoudre les requêtes, ce qui est utile pour la sécurité et la conformité.
- **Performance** : Grâce à la mise en cache des réponses DNS, les requêtes répétées peuvent être résolues plus rapidement.

## Limitations et Considérations

- **Dépendance** : Le DNS Forwarder dépend des serveurs DNS amont pour résoudre les requêtes. Si ces serveurs sont lents ou indisponibles, cela peut affecter les performances.
- **Fonctionnalité limitée** : Contrairement au DNS Resolver, le DNS Forwarder ne peut pas effectuer de résolution DNS récursive complète. Il ne fait que transférer les requêtes.

## Conclusion

Le DNS Forwarder est une solution efficace pour la gestion des requêtes DNS dans des environnements où la simplicité, le contrôle des serveurs DNS utilisés, et l'optimisation des performances grâce à la mise en cache sont prioritaires. Il est particulièrement adapté aux réseaux d'entreprise ou domestiques qui ont besoin de rediriger les requêtes DNS vers des serveurs spécifiques tout en offrant une résolution rapide et contrôlée des noms de domaine.

Dans pfSense, les fonctionnalités **Domain Override** et **Host Overrides** sont des options de configuration du **DNS Resolver** (Unbound) qui permettent de rediriger les requêtes DNS pour des domaines ou des hôtes spécifiques vers des serveurs DNS ou des adresses IP de votre choix. Voici ce que chacune de ces options signifie :

## 1. Host Overrides

### Description



La fonction **Host Overrides** permet de définir des enregistrements DNS personnalisés pour des noms d'hôtes spécifiques. Cela signifie que lorsque quelqu'un dans votre réseau essaie de résoudre un nom de domaine particulier, le DNS Resolver de pfSense fournira l'adresse IP que vous avez spécifiée dans la configuration de l'override.

### Utilisation :

Par exemple, si vous avez un serveur local avec le nom `naouel.com` et que vous voulez que ce nom résolve toujours à une adresse IP spécifique par exemple, `192.168.1.100`), vous pouvez ajouter un **Host Override**.

Ainsi, toute requête DNS pour `naouel.com` retournera `192.168.147.2` au lieu de rechercher cette information sur Internet ou un autre serveur DNS.

- **Configuration :**
  - Dans l'interface Web pfSense, allez dans **Services > DNS Resolver**.
  - Faites défiler jusqu'à la section **Host Overrides**.
  - Cliquez sur **Add** pour ajouter un nouvel override.
  - Remplissez les champs nécessaires :
    - **Host** : Le nom d'hôte que vous souhaitez rediriger (ex. : `server`).
    - **Domain** : Le domaine associé (ex. : `local`).
    - **IP Address** : L'adresse IP à laquelle le nom d'hôte doit pointer.
  - Enregistrez et appliquez les modifications.

Host Overrides				
Host	Parent domain of host	IP to return for host	Description	Actions
ordi	naouel.com	192.168.147.2	Redirection de ordi.naouel.com vers 192.168.147.2	 

Afin de pouvoir tester ces configurations, on se dirige vers un pc client etant dans le meme reseau et on tape les suites de commandes suivantes :

```
Invite de commandes - nslookup
Microsoft Windows [version 10.0.10240]
(c) 2015 Microsoft Corporation. Tous droits réservés.
C:\Users\naouel>nslookup
Serveur par défaut : pfSense-naouel.naouel.com
Address: 192.168.147.2
> ordi.naouel.com
Serveur : pfSense-naouel.naouel.com
Address: 192.168.147.2
Nom : ordi.naouel.com
Address: 192.168.147.2
>
```

## 2. Domain Override

### Description

La fonction **Domain Override** vous permet de rediriger les requêtes DNS pour des domaines entiers vers un serveur DNS spécifique. Cela est utile lorsque vous avez un serveur DNS dédié pour un domaine particulier (par exemple, un domaine interne ou un domaine géré par un serveur DNS différent de votre fournisseur habituel).

- **Utilisation :**
  - Par exemple, si vous avez un domaine interne appelé `naouel.com` et que vous souhaitez que toutes les requêtes pour ce domaine soient envoyées à un serveur DNS spécifique (par exemple, `192.168.18.3`), vous pouvez utiliser un **Domain Override**.
  - Cela signifie que toute tentative de résolution d'un nom de domaine sous `naouel.com` sera traitée par le serveur DNS `192.168.18.3` au lieu d'être envoyée au serveur DNS par défaut ou à Internet.
- **Configuration**
  - Allez dans **Services > DNS Resolver**.
  - Faites défiler jusqu'à la section **Domain Overrides**.
  - Cliquez sur **Add** pour ajouter un nouvel override.
  - Remplissez les champs nécessaires :
    - **Domain** : Le nom de domaine que vous souhaitez rediriger par exemple `naouel.com`.
    - **IP Address** : L'adresse IP du serveur DNS qui est en effet l'IP de la machine cliente du réseau qui doit gérer les requêtes pour ce domaine.
  - Enregistrez et appliquez les modifications

Services / DNS Resolver / General Settings / Edit Domain Override

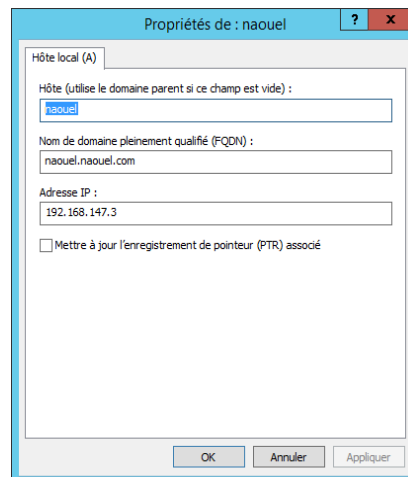
#### Domains to Override with Custom Lookup Servers

<b>Domain</b>	<input type="text" value="naouel.com"/>
Domain whose lookups will be directed to a user-specified DNS lookup server.	
<b>IP Address</b>	<input type="text" value="192.168.18.3"/>
IPv4 or IPv6 address of the authoritative DNS server for this domain. e.g.: 192.168.100.100 To use a non-default port for communication, append an '@' with the port number.	
<b>TLS Queries</b>	<input type="checkbox"/> Use SSL/TLS for DNS Queries forwarded to this server When set, queries to all DNS servers for this domain will be sent using SSL/TLS on the default port of 853.
<b>TLS Hostname</b>	<input type="text" value="DNSWINSRY"/>
An optional TLS hostname used to verify the server certificate when performing TLS Queries.	
<b>Description</b>	<input type="text"/>
A description may be entered here for administrative reference (not parsed).	

This page is used to specify domains for which the resolver's standard DNS lookup process will be overridden, and the resolver will query a different (non-standard) lookup server instead. It is possible to enter 'non-standard', 'invalid' and 'local' domains such as 'test', 'nas.home.arpa', 'mycompany.localdomain', or '1.168.192.in-addr.arpa', as well as usual publicly resolvable domains such as 'org', 'info', or 'google.co.uk'. The IP address entered will be treated as the IP address of an authoritative lookup server for the domain (including all of its subdomains), and other lookup servers will not be queried.

Ensuite nous allons nous rendre vers la machine cliente et installer le serveur DNS. Ici, nous allons nous rediriger vers Windows Serveur afin d'installer le DNS Serveur.

- Après avoir installé le serveur DNS, on se redirige vers mon service DNS, dans le service de service de recherche directes, créer un nouvel hôte.



Afin de tester les configurations, on se redirige vers le terminal de notre machine windows et on tape les suites de commandes suivantes :

```
>
C:\Users\naouel>ipconfig /flushdns

Configuration IP de Windows

Cache de résolution DNS vidé.

C:\Users\naouel>nslookup
Serveur par défaut :  pfSense-naouel.naouel.com
Address:  192.168.147.2

> naouel.naouel.com
Serveur :  pfSense-naouel.naouel.com
Address:  192.168.147.2

Réponse ne faisant pas autorité :
Nom :    naouel.naouel.com
Address: 192.168.147.3
```

**Host Overrides** vous permet de rediriger les requêtes pour des noms d'hôte spécifiques, tandis que **Domain Override** redirige les requêtes pour des domaines entiers vers un serveur DNS particulier. Ces options sont très utiles pour gérer les résolutions DNS dans un environnement réseau complexe, où différents domaines et hôtes doivent être résolus différemment.

## NOTION DU DNS DYNAMIQUE

Le DNS dynamique (Dynamic DNS ou DDNS) est un service qui permet d'associer un nom de domaine à une adresse IP qui change fréquemment. Cela est particulièrement utile pour les utilisateurs dont l'adresse IP publique est fournie par un fournisseur d'accès à Internet (FAI) et est susceptible de changer à tout moment. Le DNS dynamique met automatiquement à jour les enregistrements DNS pour que le nom de domaine pointe toujours vers la bonne adresse IP.

## Fonctionnement du DNS Dynamique

1. **Adresse IP dynamique** : La plupart des FAI attribuent des adresses IP dynamiques aux utilisateurs résidentiels. Cela signifie que chaque fois que votre routeur se reconnecte à Internet, il peut obtenir une adresse IP différente. Si vous hébergez un serveur ou un service sur votre réseau domestique, cela rend difficile l'accès via un nom de domaine, car l'adresse IP liée au domaine peut changer.
2. **Service de DNS dynamique** : Pour résoudre ce problème, un service de DNS dynamique est utilisé. Ce service permet de mettre à jour automatiquement l'enregistrement DNS à chaque changement d'adresse IP. Le service DDNS attribue un nom de domaine fixe (par exemple, `monserveur.ddns.net`) à votre adresse IP dynamique.
3. **Client DDNS** : Pour fonctionner, le DNS dynamique nécessite un client DDNS installé sur votre routeur ou votre appareil. Ce client surveille les changements d'adresse IP publique. Chaque fois que l'adresse IP change, le client DDNS envoie la nouvelle adresse au service DDNS, qui met à jour l'enregistrement DNS associé.
4. **Accès constant via le nom de domaine** : Une fois configuré, vous pouvez accéder à vos services hébergés localement (comme un serveur web, un serveur FTP, ou un système de surveillance) via le nom de domaine fourni par le service DDNS, peu importe comment et quand votre adresse IP change.

## Scénarios d'Utilisation

- **Hébergement de serveurs** : Si vous hébergez un site web, un serveur de jeux, ou d'autres services sur votre réseau domestique, un service DDNS vous permet de rendre ces services accessibles via un nom de domaine, même si votre adresse IP change.
- **Accès à distance** : Si vous souhaitez accéder à votre réseau domestique à distance (par exemple, pour des fichiers ou un bureau à distance), un service DDNS vous permet de vous connecter en utilisant un nom de domaine au lieu de devoir connaître l'adresse IP actuelle.
- **Systèmes de surveillance** : Beaucoup de caméras de sécurité et systèmes de surveillance utilisent DDNS pour permettre un accès à distance simple via un nom de domaine.

## Configuration du DNS Dynamique

1. **Choisir un service DDNS** : Plusieurs services DDNS gratuits et payants sont disponibles, comme No-IP, DynDNS, et DuckDNS. Vous devrez créer un compte et choisir un nom de domaine.
2. **Configurer le client DDNS** : La plupart des routeurs modernes et des systèmes d'exploitation (comme Windows, macOS, Linux) prennent en charge les clients DDNS. Vous devrez entrer les informations de votre compte DDNS dans les paramètres du client.
3. **Mettre à jour les enregistrements DNS** : Le client DDNS surveille les changements d'adresse IP et met à jour automatiquement les enregistrements DNS lorsque votre adresse IP change.
4. **Tester l'accès** : Une fois configuré, vous pouvez tester l'accès à votre service ou appareil via le nom de domaine assigné par le service DDNS.

## Avantages et Limitations

**Avantages :**

- Accès constant via un nom de domaine, même avec des adresses IP changeantes.
- Simplifie l'accès à distance aux services hébergés localement.
- Configurable sur la plupart des routeurs et systèmes.

**Limitations :**

- Peut nécessiter un service payant pour des fonctionnalités avancées ou pour éviter les expirations.
- Le temps de propagation DNS peut parfois causer de courts délais lors de la mise à jour de l'adresse IP.
- Certains FAI peuvent bloquer certains ports nécessaires pour le serveur à domicile.

En somme, le DNS dynamique est un outil précieux pour quiconque doit gérer un réseau ou des services avec des adresses IP dynamiques, permettant un accès facile et constant via un nom de domaine personnalisé.