Pare-feu

1 – Qu'est-ce qu'un pare-feu

Un pare-feu est un système, ou un groupe de systèmes,
qui impose une politique de contrôle d'accès entre des réseaux.

Avantages	Limitations
• Il empêche les utilisateurs non fiables d'accéder aux hôtes, aux ressources et aux applications sensibles. • Il bloque les données malveillantes provenant des serveurs et des clients. • Il simplifie la gestion de la sécurité en confiant la majeure partie du contrôle d'accès réseau à quelques pares-feux sur le réseau.	• Un pare-feu mal configuré peut constituer un point de défaillance unique. • Les performances du réseau peuvent baisser. • Le trafic non autorisé peut être placé en tunnel ou masqué comme trafic légitime à travers le pare-feu.

Filtrage avec ou sans état
Avec état : on parle d'état de la connexion, où le pare-feu garde dans sa table d'état une trace des connexions (journal d'état) entre les hôtes (qui discute avec qui). Par exemple, le message de retour à un hôte du réseau privé n'est pas bloqué par le pare-feu lorsqu'il provient du réseau public.
Sans état : il n'y a pas de journal d'état de la connexion entre deux hôtes sur des réseaux différents.

2 - Types de pare-feu

Pare-feu de filtrage (Sans état) de paquets
C'est en général le pare-feu d'un routeur qui autorise ou interdit le trafic en fonction des informations des couches 3 et 4.

Quelques inconvénients :
- Il est vulnérable face à une usurpation d'adresse IP.
- Les filtres de paquets ne filtrent pas de manière fiable les paquets fragmentés (données sur plusieurs trames). Le premier fragment contenant les informations d'en-tête TCP est filtré mais pas les autres.
- Les sessions qui utilisent des négociations de port dynamiques sont difficiles à filtrer sans ouvrir l'accès à toute une série de ports.

Pare-feu dynamique (Avec état - Stateful)
C'est un pare-feu couramment utilisé qui effectue un filtrage dynamique à l'aide d'informations de connexion mises à jour dans une table d'états. Il analyse le trafic au niveau des couches OSI 4 et 5.

Avantages	Limitations
• Très bon filtrage des paquets. • Défense contre l'usurpation d'identité et les attaques DoS. • Journal de données détaillé.	• Aucune inspection de la couche application. • Suivi limité des protocoles sans état.

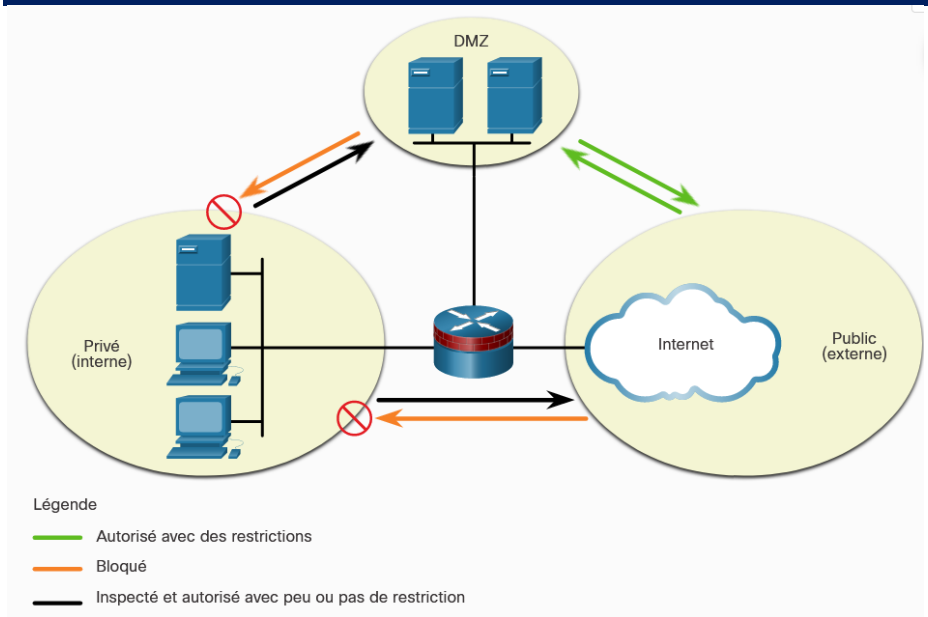
Pare-feu passerelle d'application (Proxy)
Un pare-feu de passerelle d'application (pare-feu proxy), filtre les informations des couches 3, 4, 5 et 7 du modèle OSI. La majeure partie du contrôle et du filtrage des pare-feu est effectuée par le logiciel.

Le pare-feu de nouvelle génération (NGFW)
La prévention des intrusions est intégrée.
La reconnaissance et le contrôle des applications pour détecter et bloquer celles qui présentent un risque**.**

Règles de bonnes pratiques

- Positionnez les pare-feux aux limites de la sécurité.
- Refuser tout le trafic par défaut.
- Autorisez uniquement les services nécessaires.
- Assurez-vous que l'accès physique au pare-feu est contrôlé.
- Surveillez régulièrement les journaux du pare-feu.
- Les pare-feux protègent principalement contre les attaques provenant de l'extérieur.

3 - Zone démilitarisée



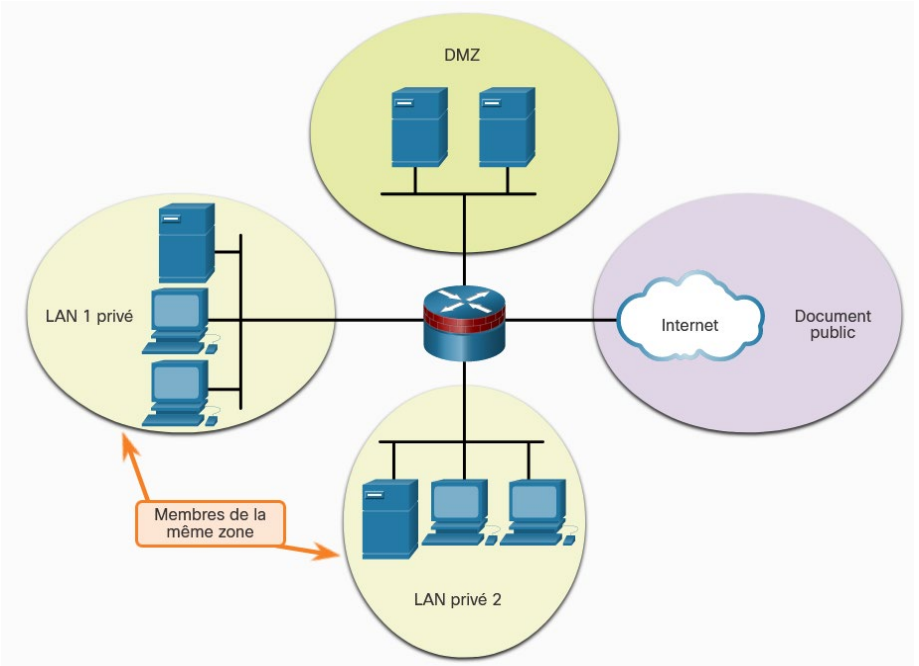
Une zone démilitarisée (DMZ) est un système de pare-feu comportant généralement une interface interne connectée au réseau privé, une interface externe connectée au réseau public et une interface DMZ, comme illustré à la figure.

Le trafic provenant du réseau privé est inspecté lorsqu'il se déplace vers le réseau public ou la DMZ. Ce trafic est autorisé avec peu ou pas de restriction. Le trafic inspecté revenant de la DMZ ou du réseau public au réseau privé est autorisé.

Inspecté => suivi de la connexion avec un journal d'état

- Le trafic provenant du réseau DMZ et se déplaçant vers le réseau privé est généralement bloqué.
- Le trafic provenant du réseau DMZ et voyageant vers le réseau public est autorisé de manière sélective.
- Le trafic provenant du réseau public et voyageant vers la DMZ est inspecté et autorisé de manière sélective (e-mail, DNS, HTTP ou HTTPS).
- Le trafic provenant du réseau public et voyageant vers le réseau privé est bloqué.

4 - Pare-feu à politique basée sur les zones (ZPF)



Ce pare-feu (ZPF) utilise le concept de zones. Une zone est un groupe d'une ou plusieurs interfaces partageant des fonctions similaires.

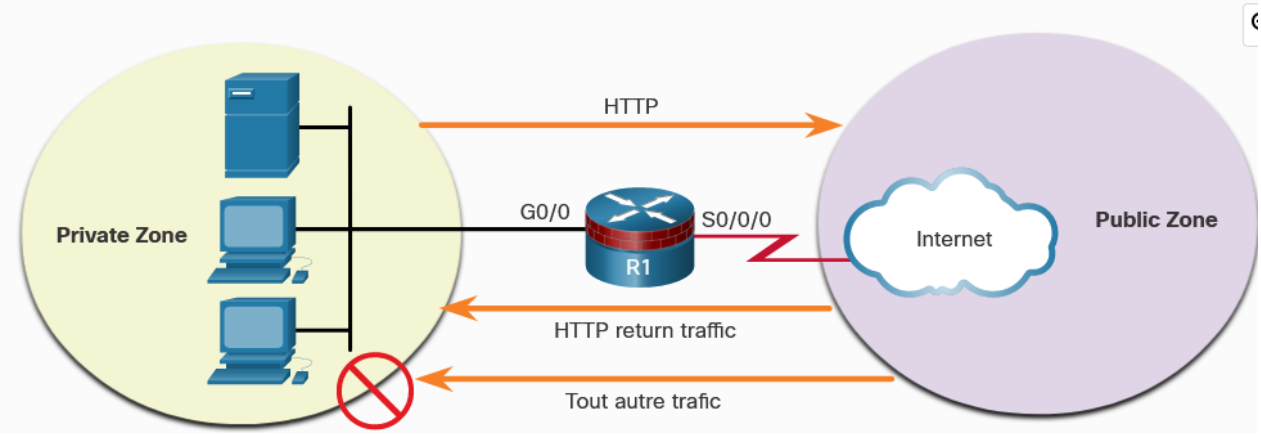
Sur la figure, les politiques de sécurité des LAN 1 et LAN 2 sont semblables et peuvent être regroupées dans la même zone.

Par défaut, le trafic entre les interfaces de la même zone ne fait l'objet d'aucune politique et passe librement.

Tout le trafic entre les zones est bloqué sauf si une politique de sécurité permettant ou inspectant le trafic a été configurée.

Les politiques de sécurité sont définies en fonction de la zone et non par les réseaux IP qui communiquent via une interface donnée. Plusieurs interfaces peuvent devenir membres d'une zone et des politiques de zone sont appliquées à ces interfaces.

Exemple : étapes de configuration du pare-feu avec politique basée sur les zones



Dans l'exemple de topologie, nous avons deux interfaces, deux zones et un trafic circulant dans une seule direction. Le trafic provenant de la zone publique ne sera pas autorisé.

Etape 1 : Création des zones à l'aide de la commande "zone security"

```
R1(config)# zone security PRIVATE
R1(config-sec-zone)# exit
R1(config)# zone security PUBLIC
R1(config-sec-zone)# exit
R1(config)#
```

Etape 2 : Identification du trafic (mappage de classe)

Une classe est un moyen d'identifier un ensemble de paquets en fonction de son contenu (http, dns ou …). Une classe est définie avec des mappages de classes.

Syntaxe :

R1(config)# class-map type inspect match-any **NOM_CLASSE**

- **claas-map type inspect** : permet de définir un mappage de classe de type inspection de paquets.
- **match-any** ou **match-all** : les paquets doivent répondre à l'un des critères de correspondance **(any)** ou à tous les critères de correspondance **(all)** pour être considérés comme membres de la classe.
- On termine la ligne de commande avec le nom que l'on donne à la classe : ici **NOM_CLASSE**.

Ensuite, il faut préciser les instructions de correspondance

```
Router(config-cmap)# match access-group {acl-# | acl-name }
Router(config-cmap)# match protocol protocol-name
Router(config-cmap)# match class-map class-map-name
```

On peut rechercher une correspondance avec une ACL, un protocole ou un autre mappage de classe.

Dans notre exemple, le trafic HTTP est autorisé à traverser R1 de la zone PRIVÉE à la zone PUBLIC. Lorsque vous autorisez le trafic HTTP, il est recommandé d'inclure spécifiquement les protocoles HTTPS et DNS. Le trafic peut correspondre à l'une des instructions (match-any) pour devenir membre de la classe HTTP-TRAFFIC.

```
R1(config)# class-map type inspect match-any HTTP-TRAFFIC
R1(config-cmap)# match protocol http
R1(config-cmap)# match protocol https
R1(config-cmap)# match protocol dns
```

Que faire si on tombe sur une correspondance. Il faut passer à l'action !

Etape 3 : Action en cas de correspondance

Il faut mettre en place l'action (inspecter, abandonner ou passer) à appliquer au trafic membre d'une classe.

R1(config)# **policy-map type inspect** *policy-map-name*
R1(config-pmap)# **class type inspect** *class-map-name*
R1(config-pmap-c)# {**inspect | drop | pass**}

On précise le nom de la politique de mappage, puis on précise à quelle classe elle est associée puis on précise l'action : **inspect | drop | pass.**

Par exemple, dans notre cas, la classe HTTP-TRAFFIC qui a été configurée à l'étape précédente est associée à un nouveau mappage de politiques nommé PRIV-TO-PUB-POLICY. La troisième commande **inspect** configure R1 pour conserver les informations d'état pour tout le trafic membre de la classe HTTP-TRAFFIC.

R1(config)# **policy-map type inspect PRIV-TO-PUB-POLICY**
R1(config-pmap)# **class type inspect HTTP-TRAFFIC**
R1(config-pmap-c)# **inspect**

- **inspecter -** cette action permet de contrôler le trafic en fonction de l'état. Par exemple, si le trafic circulant de la zone PRIVÉ vers la zone PUBLIC est inspecté, le routeur conserve les informations de connexion ou de session pour le trafic TCP et UDP. Le routeur autorise alors le trafic de retour envoyé par les hôtes de la zone PUBLIC en réponse aux demandes de connexion de la zone PRIVÉ.

- **drop -** il s'agit de l'action par défaut pour tout le trafic. Semblable au **deny any** implicite à la fin de chaque ACL, il y a une **drop** explicite appliquée par l'IOS à la fin de chaque policy-map. Elle est répertoriée comme classe **class-default** dans la dernière section de toute configuration de mappage de politiques.

- **pass -** cette action permet au routeur de transférer le trafic d'une zone à une autre. Cela n'assure pas le suivi de l'état des connexions ou des sessions. Le laissez-passer n'autorise le trafic que dans une seule direction. Une politique correspondante doit être appliquée pour permettre au trafic de retour de passer dans la direction opposée.

Etape 4 : Identification d'une paire de zones et mise en correspondance avec une politique

La quatrième étape consiste à identifier une paire de zones et à l'associer à un mappage de politiques.

- Créez une zone-pair avec la commande **zone-pair security.**
- Spécifier le nom de la zone d'où vient le trafic.
- Spécifier le nom de la zone à laquelle le trafic est destiné.
- Le mot clé indique si le trafic ira vers ou depuis le routeur lui-même.
- Utilisez ensuite la commande **service-policy type inspect** pour associer un mappage de politiques.

Router(config)# **zone-pair security** zone-pair-name **source** {*source-zone-name* | **self**} **destination** {*destination-zone-name* | **self**}
Router(config-sec-zone-pair)# **service-policy type inspect** *policy-map-name*
Dans notre cas, une paire de zones nommée PRIV-PUB est créée avec PRIVATE comme zone source et PUBLIC comme zone de destination. Ensuite, le mappage de politiques est associé à la paire de zones.

R1(config)# zone-pair security **PRIV-PUB** source **PRIVATE** destination **PUBLIC**
R1(config-sec-zone-pair)# service-policy type inspect **PRIV-TO-PUB-POLICY**

Etape 5 : Attribuer des zones aux interfaces

L'association d'une zone à une interface applique immédiatement la politique de sécurité associée à la zone. Si aucune politique de sécurité n'est encore configurée pour la zone, tout le trafic de transit est abandonné.
Utilisez la commande **zone-member security** pour attribuer une zone à une interface.

Exemple d'attribution :

R1(config)# interface GigabitEthernet 0/0
R1(config-if)# zone-member security PRIVATE

R1(config-if)# interface Serial 0/0/0

R1(config-if)# zone-member security PUBLIC

La politique de service est maintenant active. Le trafic HTTP, HTTPS et DNS provenant de la zone PRIVATE et destiné à la zone PUBLIC sera inspecté. Le trafic provenant de la zone PUBLIC et destiné à la zone PRIVATE ne sera autorisé que s'il fait partie de sessions initiées à l'origine par les hôtes de la zone PRIVATE.

Vérifier une configuration ZPF

Vérifiez une configuration ZPF en affichant la configuration en cours d'exécution.
R1# show running-config ou R1# show running-config | begin class-map

R1# show policy-map type inspect zone-pair sessions (affiche les infos : nombre de paquets matchés)

R1# **show class-map type inspect** (affiche ce qu'il doit inspecter)

R1# **show zone security** (affiche les zones de sécurité)

R1# **show zone-pair security** (affiche les paires de zone)

R1# **show policy-map type inspect** (affiche la politique associée à une paires de zone)

Quelques règles à retenir

Règles appliquées par le pare-feu dans le cas d'une politique basée sur les zones (ZPF)

Interface source membre de la zone ?	Interface de destination membre de la zone ?	Paire de zone ?	Politique de sécurité ?	Résultat
NON	NON	N/A	N/A	Passer
OUI	NON	N/A	N/A	Abandon
NON	OUI	N/A	N/A	Abandon
OUI (privé)	OUI (privé)	N/A	N/A	Passer
OUI (privé)	OUI (publique)	NON	N/A	Abandon
OUI (privé)	OUI (publique)	OUI	NON	Passer
OUI (privé)	OUI (publique)	OUI	OUI	Inspecter

- Le routeur ne filtre jamais le trafic entre les interfaces dans la même zone.
- Une interface ne peut pas appartenir à plusieurs zones. Pour créer une réunion de zones de sécurité, spécifiez une nouvelle zone et les paires de politiques et de mappages de zones appropriées.
- ZPF peut coexister avec le pare-feu classique, mais ne peut pas être utilisé sur la même interface. Supprimez la commande **ip inspect** interface configuration avant d'appliquer la commande **zone-member security.**
- Le trafic ne peut jamais circuler entre une interface affectée à une zone et une interface qui n'a pas été affectée à une zone. L'application de la commande **zone-member** configuration entraîne toujours une interruption temporaire du service jusqu'à ce que l'autre zone-member soit configuré.
- La politique interzone par défaut consiste à abandonner tout le trafic, sauf autorisation contraire spécifique de la politique de service configurée pour la paire de zones.
- La commande **zone-member** ne protège pas le routeur lui-même (le trafic vers et depuis le routeur n'est pas affecté), sauf si les paires zone- sont configurées à l'aide de la zone self prédéfinie.

Les règles par défaut sont appliquées au trafic de transit en fonction de la configuration des interfaces d'entrée et de sortie et de l'existence de politiques. Par exemple, si aucune interface d'entrée ou de sortie n'est définie comme membre d'une zone, le trafic est autorisé à quitter l'interface de sortie. De même, si les deux interfaces sont membres de la même zone, le trafic est autorisé à passer. Cependant, si une interface est membre d'une zone et l'autre pas, le trafic est abandonné.