3. Pare-feu et listes de contrôle d'accès

Pare-feu ou firewall

- Equipement ou un ensemble d'équipements qui restreint l'accès entre un réseau protégé et l'Internet ou entre plusieurs réseaux
- Il permet:
  - d'empêcher des utilisateurs externes non autorisés d'accéder à des ressources internes
  - d'empêcher des utilisateurs internes de quitter des zones sécurisées
- Firewall matériels ou logiciels
- Firewall à états (statefull)
  - Conserve en mémoire l'état des connexions réseaux
- Firewall sans états (stateless)

Pare-feu ou firewall

Sonicwall TZ300

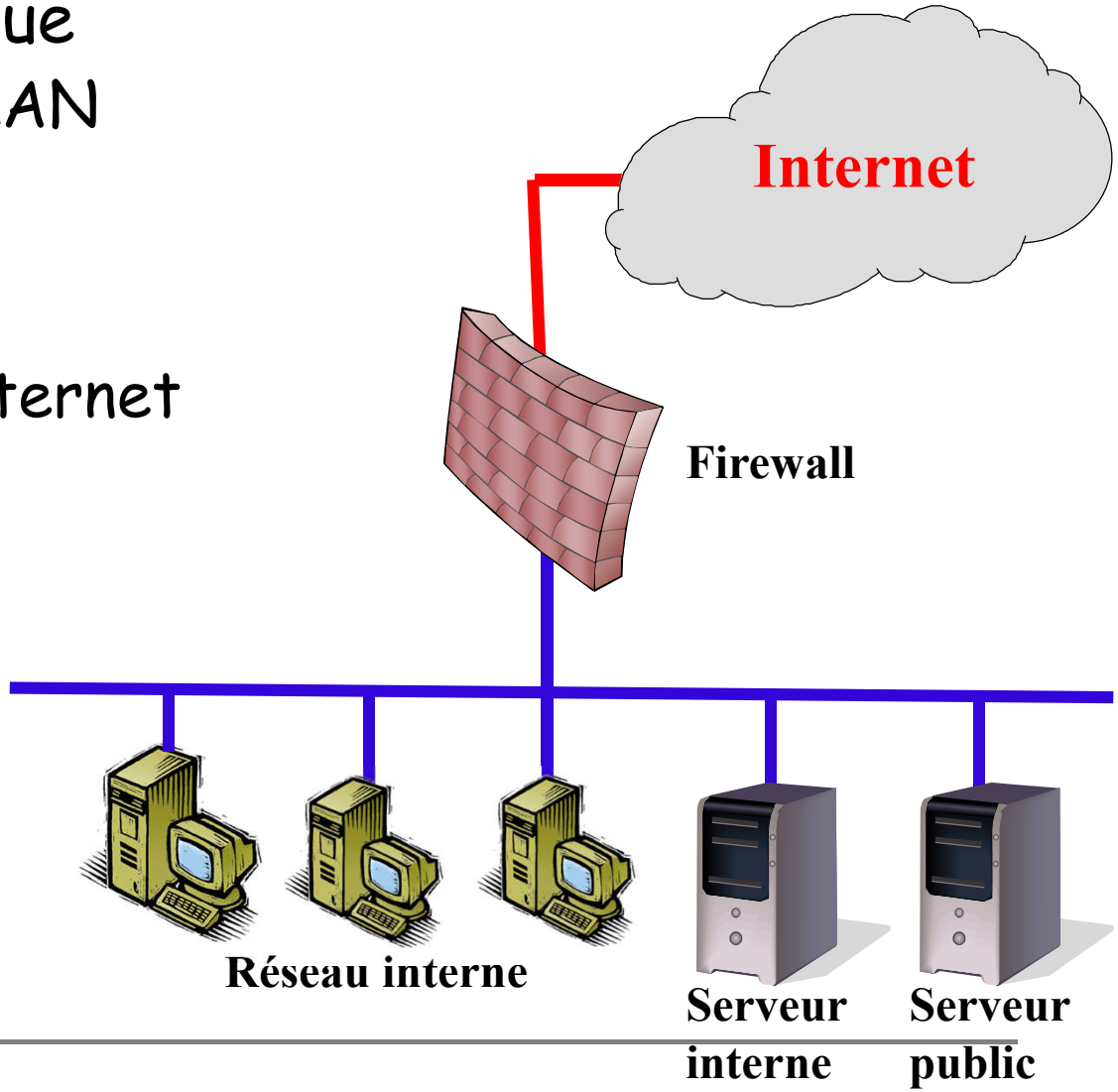
Cisco ASA 5510

ZoneAlarm

Pfsense

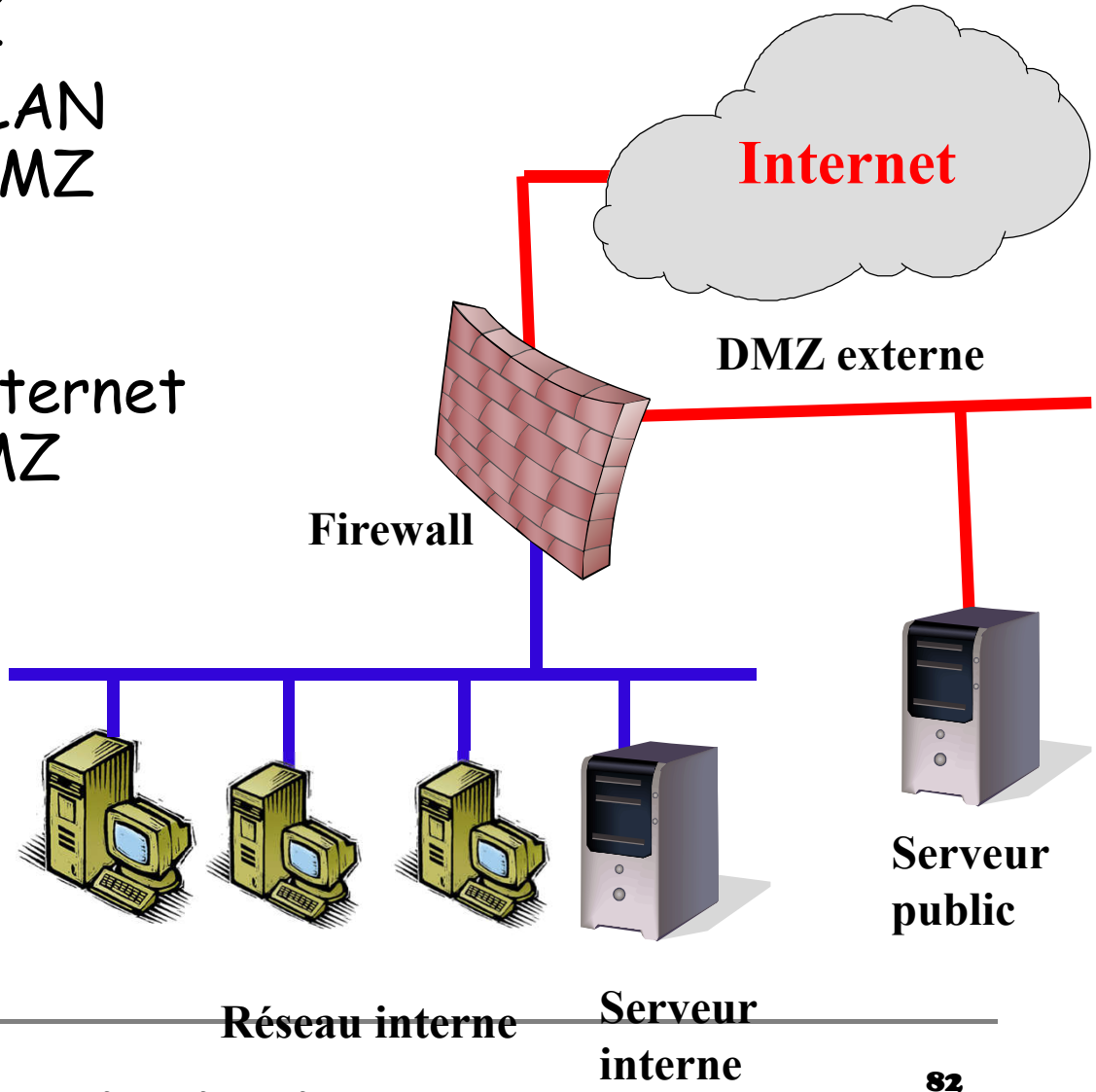
Architecture firewall (1/4)

- Architecture basique
  - Firewall entre le LAN et l'Internet
  - Accès au serveurs publics depuis l'Internet et dans le LAN
  - **Pas de sécurité en interne dans le LAN pour les serveurs internes et externes**



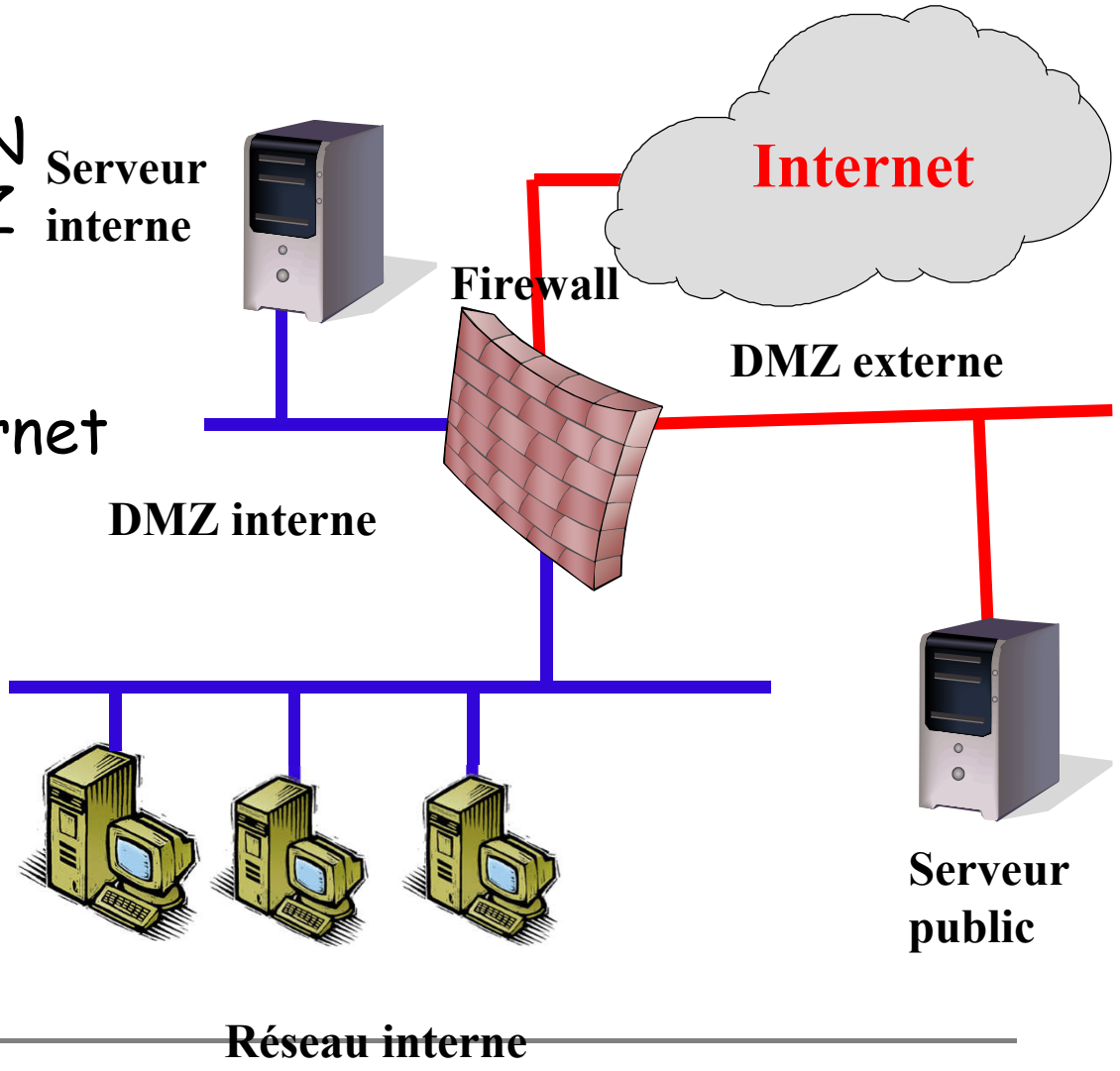
Architecture firewall (2/4)

- Architecture DMZ
  - Firewall entre le LAN l'Internet et la DMZ
  - Accès au services publics depuis l'Internet au niveau de la DMZ
  - **Pas de sécurité en interne dans le LAN pour les serveurs internes**



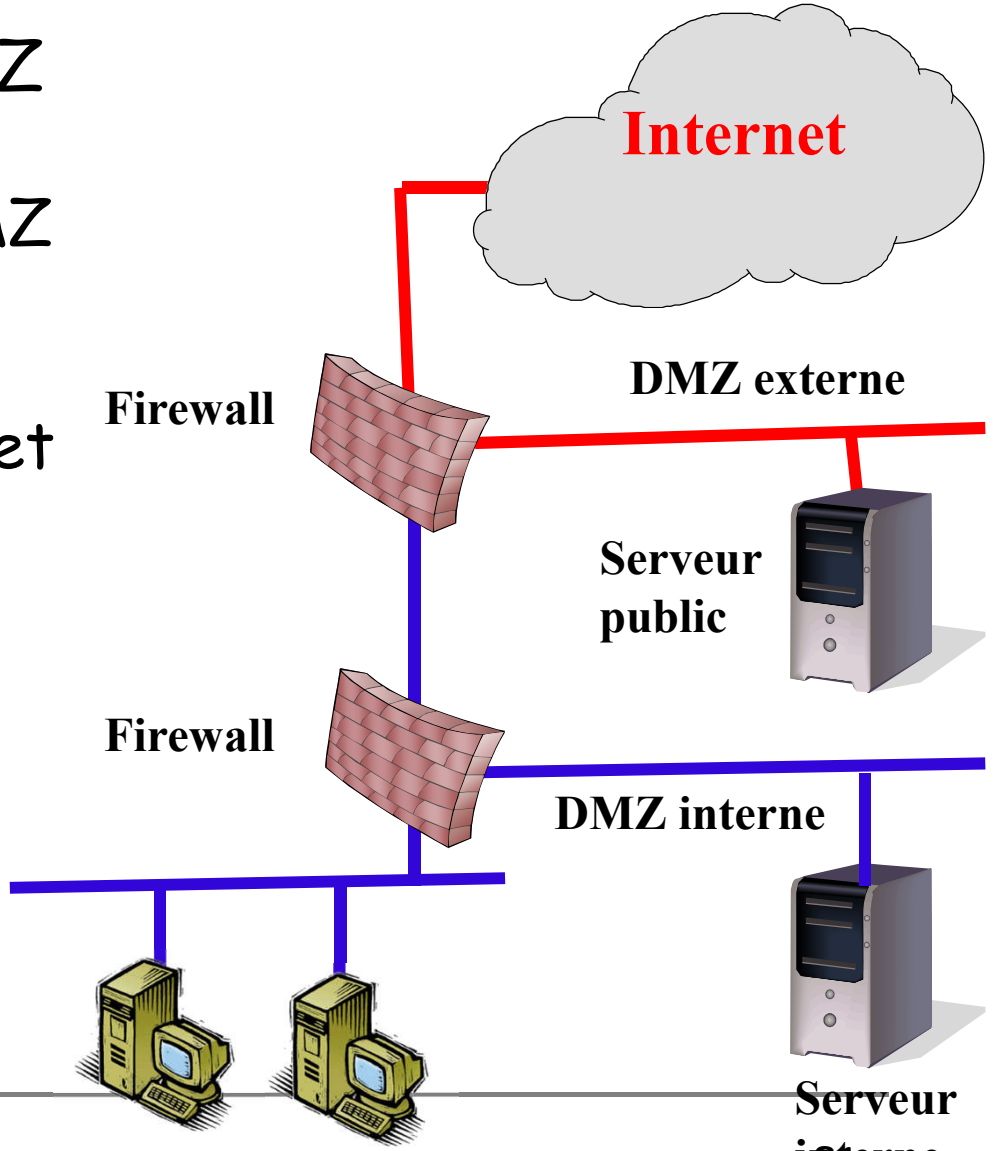
Architecture firewall (3/4)

- Architecture DMZ
  - Firewall entre le LAN l'Internet et la DMZ
  - Accès au services publics depuis l'Internet au niveau de la DMZ
  - Accès au services interne depuis le LAN au niveau de la DMZ
  - **Un point unique de défaillance**



Architecture firewall (4/4)

- Architecture deux DMZ
  - Firewalls entre le LAN l'Internet et les 2 DMZ
  - Accès au services publics depuis l'Internet au niveau de la DMZ externe
  - Accès au services internes depuis le LAN au niveau de la DMZ interne



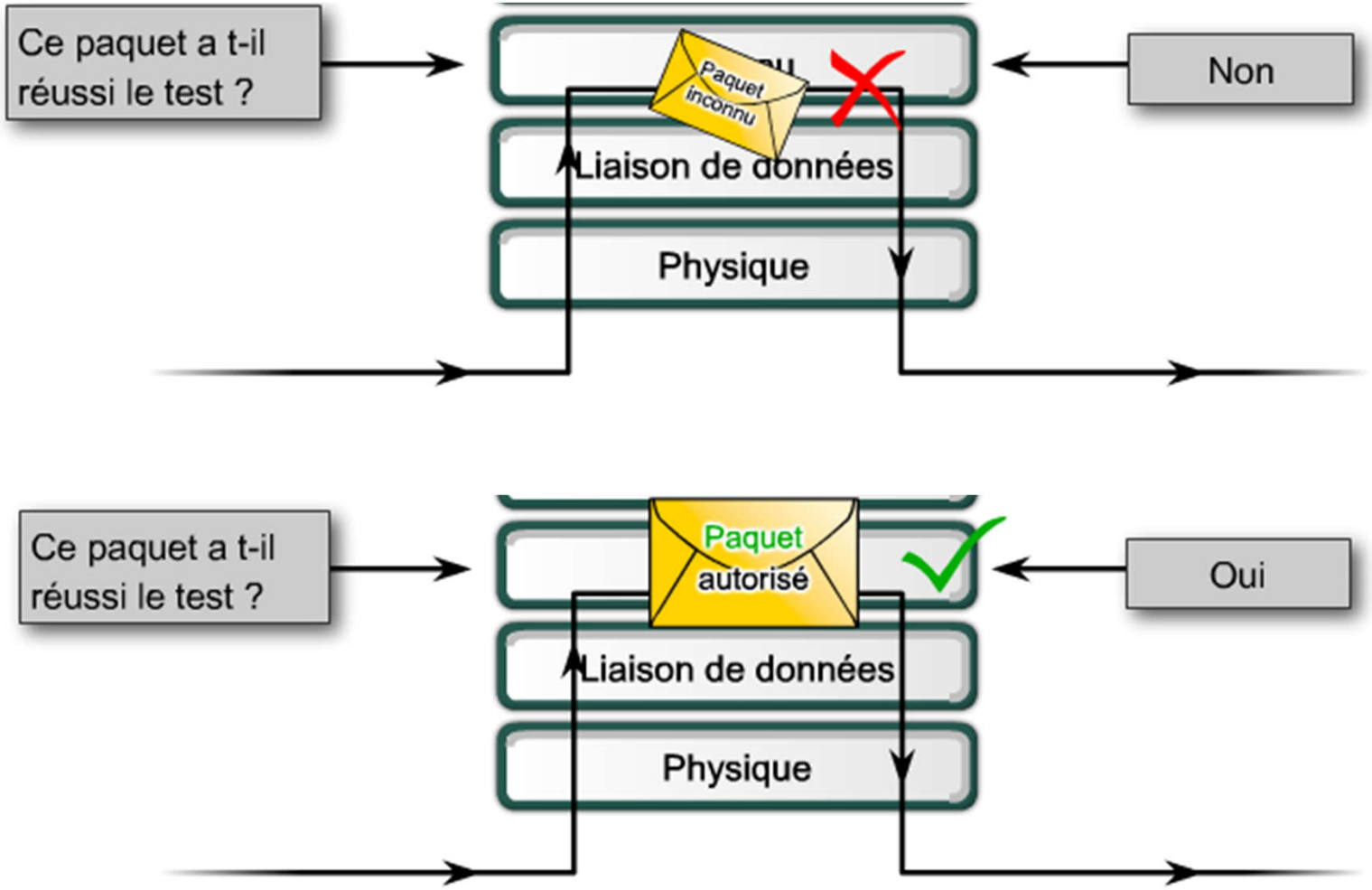
Pare-feu et ACL

- Pare-feu ou firewall permet de mettre en œuvre des stratégies de sécurité
- La pare-feu s'appuie sur des fonctions de filtrage à l'aide des listes de contrôle d'accès (ACL)
- Mécanisme de sécurité très utilisé par les administrateurs
- Assure le filtrage du trafic
  - Bloquer ou autoriser le trafic suivant des règles
- Les ACL s'appliquent
  - Aux adresses IP, aux protocoles de couche réseau
  - Aux protocoles des couches supérieures, etc.

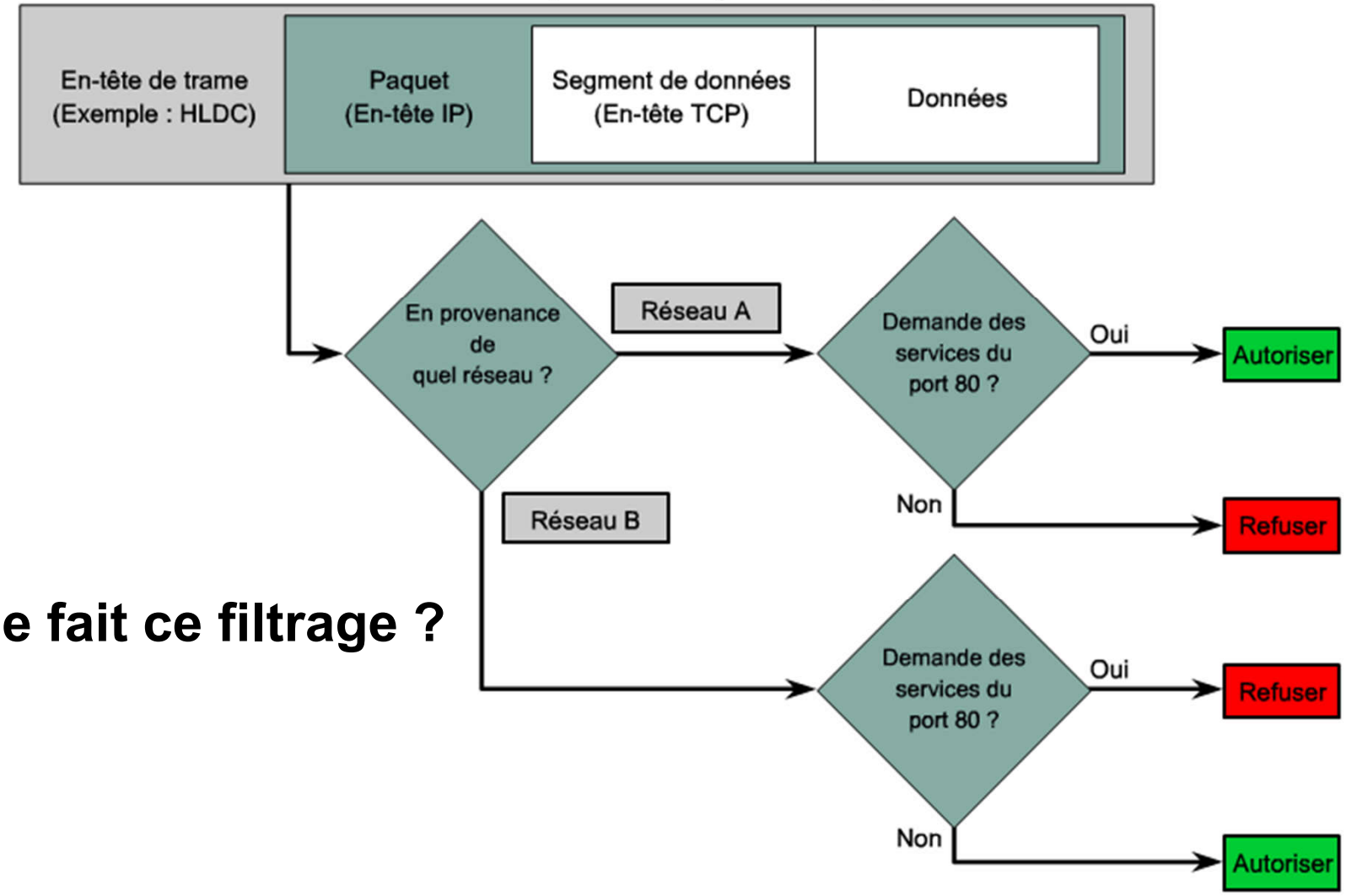
Filtrage des paquets

- Filtrage des paquets par le routeur
  - Autorisations ou interdictions suivant les règles définis dans les ACL
- Filtrage effectué au niveau 3 ou 4
- Lecture des informations de niveau 3 :
  - Adresse IP source
  - Adresse IP de destination
  - Type de message (IP, ICMP, etc..)
- Lecture des informations de niveau supérieur :
  - Port source TCP/UDP
  - Port de destination TCP/UDP

Principe du filtrage des paquets



Exemple de filtrage des paquets



Que fait ce filtrage ?

Liste de contrôle d'accès ou ACL

- Scripts de configurations contrôlant l'autorisation ou le refus de passages des paquets
- Sans ACL, les paquets sont routés en fonction des informations contenues dans la table de routage
- On peut configurer :
  - Une liste de contrôle d'accès par protocole
  - Une liste de contrôle d'accès par direction
  - Une liste de contrôle d'accès par interface
- Avantages
  - Limitent le trafic (filtrage) → performances
  - Sécurité (restriction des accès)

Fonctionnement des ACL

- Listes de contrôle d'accès entrantes
  - Traitement des paquets entrants par l'ACL
  - Si le paquet réussit le test il subit le routage
- Listes de contrôle d'accès sortantes
  - Paquets routés vers l'interface de sortie
  - Traitement des paquets sortants par l'ACL
- Instructions des ACL séquentielles
  - Paquet soumis aux instructions de haut en bas
- **Une instruction implicite finale s'applique à tous les paquets qui n'ont pas répondu aux conditions. Elle se solde par une instruction de refus de tous les autres paquets**

Numérotation et nomination

- Numérotation associée au type d'ACL

- Les numéros suivants s'appliquent au protocole IP
  - De 1 à 99 et de 1300 à 1399 → ACL standards
  - De 100 à 199 et de 2000 à 2699 → ACL étendues

- D'autres numéros sont utilisés pour d'autre protocoles différents de IP (IPX, AppleTalk)

- On peut associer à une ACL un nom (ACL nommée)

Les ACL standards

- Autoriser ou refuser du trafic
  - Associer un numéro à l'ACL
  - ACL défini en fonction de l'@IP source
- L'@IP de destination et le port de sortie n'ont pas d'influence → pas de prise en compte du protocole
- Exemple
  - Autoriser tout trafic provenant de 192.168.3.0/24
  - **acces-list 10 permit 192.168.3.0 0.0.0.255**
- Une instruction **deny all implicite** empêche tout paquet ne provenant pas de ce réseau précis d'être acheminé

Syntaxe ACL standard

- Syntaxe ACL standard

```
access-list {acl-#} {permit | deny | remark} source-addr [source-wildcard][log]
```

- Syntaxe ACL standard nommée

```
Router(config)# ip access-list [standard | extended] name_of_ACL
```

```
Router(config-std-nacl)# {permit | deny | remark} {source [source-wildcard] | any}
```

Les ACL étendues

- Autoriser ou refuser du trafic en fonction
  - @IP source et destination
  - Ports TCP et UDP source et de destination
  - Type de protocole (IP, ICMP, UDP, TCP, etc..)

- Exemple
  - Autoriser le trafic web (HTTP) provenant du réseau 192.168.3.0/24 vers tout réseau de destination
  - **acces-list 101 permit tcp 192.168.3.0 0.0.0.255 any eq 80 (www)**
- Une instruction deny all implicite empêche tout autre type de paquet

Syntaxe ACL étendue

- Syntaxe ACL étendue

```
access-list acl-# {permit | deny | remark} protocol source-addr [source-wildcard]
dest-addr [dest-wildcard][operator port][established]
```

- Syntaxe ACL étendue nommée

```
Router(config)# ip access-list [standard | extended] name_of_ACL
```

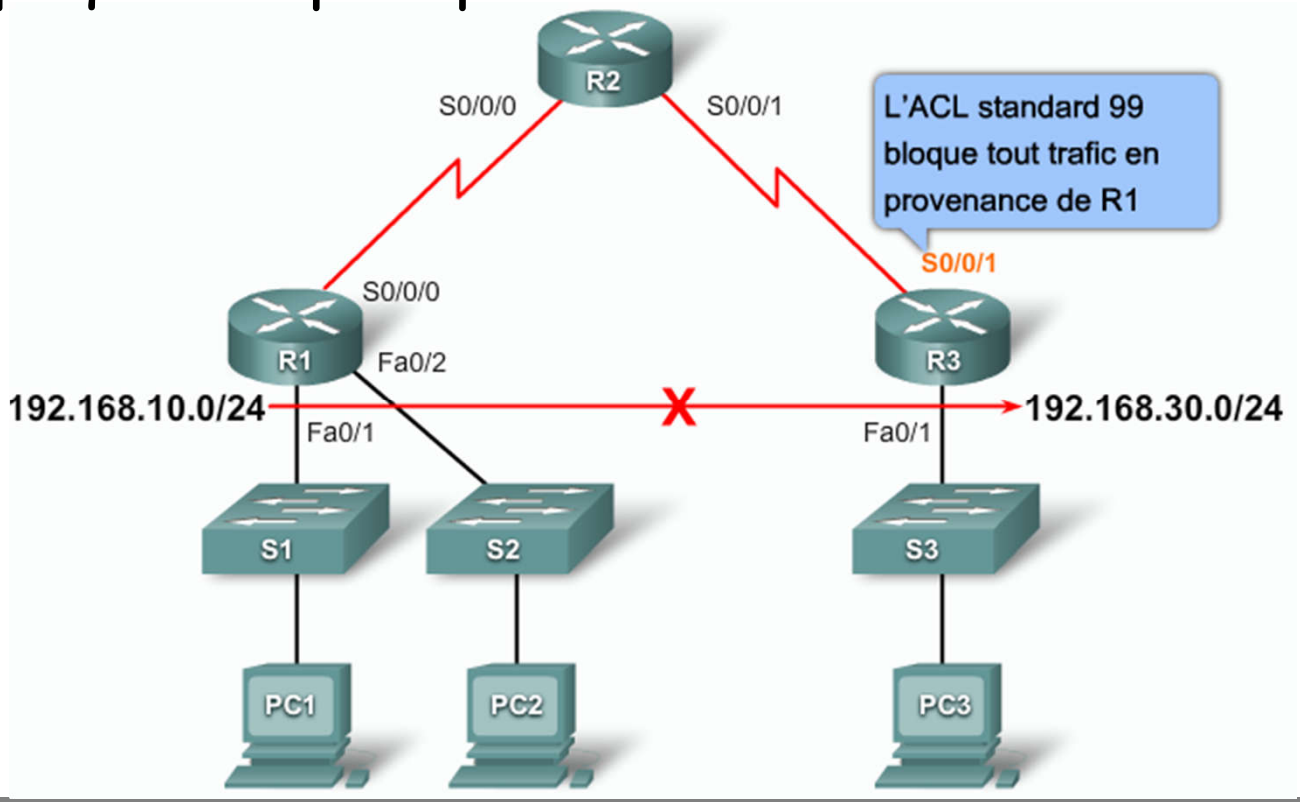
```
Router(config-ext-nacl)# {permit | deny | remark} protocol source-addr [source-wildcard]
dest-address [dest-wildcard] [operator port]
```

Positionnement des ACL

- Quelques règles de placement des ACL
  - Placez les listes de contrôle d'accès étendues le plus près possible de la source du trafic refusé. Ainsi, le trafic indésirable est filtré sans traverser l'infrastructure réseau
  - Étant donné que les listes de contrôle d'accès standard ne précisent pas les adresses de destination, placez-les le plus près possible de la destination
- Exemple
  - Empêcher l'accès du trafic provenant du réseau 192.168.10.0/24 vers le réseau 192.168.30.0/24 avec un ACL étendue. Donner l'ACL ?

Positionnement des ACL

- Appliquer l'ACL sur l'interface de Fa 0/1 de R1
  - Bloque tout trafic dès la source
- Appliquer le plus proche de la source



Règles de saisie des instructions

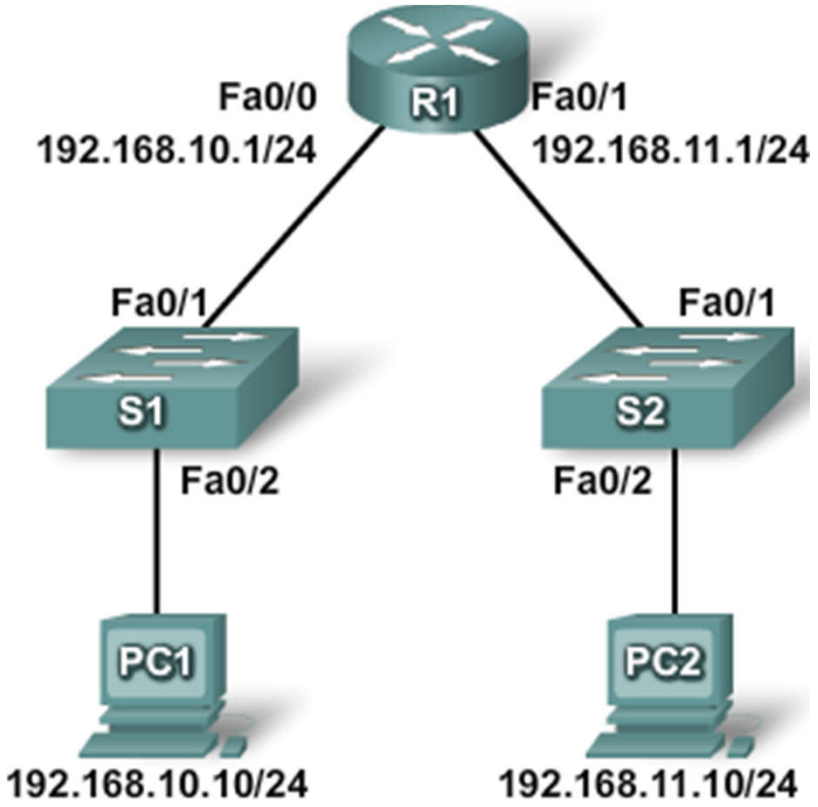
- Le trafic accédant au routeur est comparé aux instructions de la liste de contrôle d'accès selon leur ordre d'entrée. Tant qu'une concordance n'a pas été détectée, le routeur traite les instructions de la liste de contrôle d'accès. C'est pourquoi il est recommandé de faire figurer en tête de liste l'entrée la plus couramment utilisée. Si le routeur a parcouru toute la liste sans détecter de concordance, le trafic est refusé.
- Une liste de contrôle d'accès doit comporter au moins une instruction d'autorisation (permit), sans quoi tout le trafic est bloqué.

Quelques règles spécifique

- Empêcher toute connexion TCP
  - acces-list 101 deny tcp any any
- Empêcher tout trafic UDP
  - acces-list 101 deny udp any any
- Empêcher un protocole de routage
  - acces-list 101 deny [routing] any any

Exemple

- Est-ce que les ACL 101 et 102 sont semblables ?
- Est-ce que le réseau 192.168.11.0 peut-il traverser le routeur ?
- Comment modifier pour que seuls ces deux réseaux puissent traverser le routeur ?



ACL 101

```
access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
```

ACL 102

```
access-list 102 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
access-list 102 deny ip any any
```

Syntaxe d'une ACL standard

Paramètre	Description
numéro-liste-accès	Numéro d'une liste de contrôle d'accès. C'est un nombre décimal entre 1 et 99, ou entre 1300 et 1999 (pour une liste de contrôle d'accès standard).
deny	Refuse l'accès si les conditions sont respectées.
permit	Autorise l'accès si les conditions sont respectées.
remark	Ajoutez une remarque sur les entrées dans une liste de contrôle d'accès IP pour en faciliter la compréhension et la recherche.
source	Numéro du réseau ou de l'hôte d'où provient le paquet. Il existe deux moyens de spécifier la *source* : • Utilisez une séquence de 32 bits en notation décimale à quatre parties. • Utilisez le mot clé any comme abréviation d'une *source* et le *masque-générique-source* 0.0.0.0 255.255.255.55.
masque-générique-source	(Facultatif) Bits de masque générique à appliquer à la source. Il existe deux moyens de spécifier le masque-générique-source : • Utilisez une séquence de 32 bits en notation décimale à quatre parties. Placez les uns dans les positions de bits à ignorer. • Utilisez le mot clé any comme abréviation d'une *source* et le *masque-générique-source* 0.0.0.0 255.255.255.55.
log	(Facultatif) Provoque un message de journalisation informatif au sujet du paquet

```
R1(config)# access-list 10 remark Permit hosts from the 192.168.10.0 LAN
R1(config)# access-list 10 permit 192.168.10.0
R1(config)# exit
```

Masques génériques

- Les ACL fonctionnent avec les masques génériques
- Même rôle que le masque standard
  - Bit 0 de masque générique : permet de vérifier la valeur du bit correspondant dans l'adresse.
  - Bit 1 de masque générique : permet d'ignorer la valeur du bit correspondant dans l'adresse

	Adresse décimale	Adresse binaire
Adresse IP à traiter	192.168.10.0	11000000.10101000.00001010.00000000
Masque générique	0.0.255.255	00000000.00000000.11111111.11111111
Adresse IP résultante	192.168.0.0	11000000.10101000.00000000.00000000

- Pour obtenir le masque générique faire 255-X ou X est la valeur de l'octet sur le masque standard

Options hosts et any

- Option ***host***
  - Permet de ne pas utiliser un masque 0.0.0.0
  - Désigne une interface en particulier

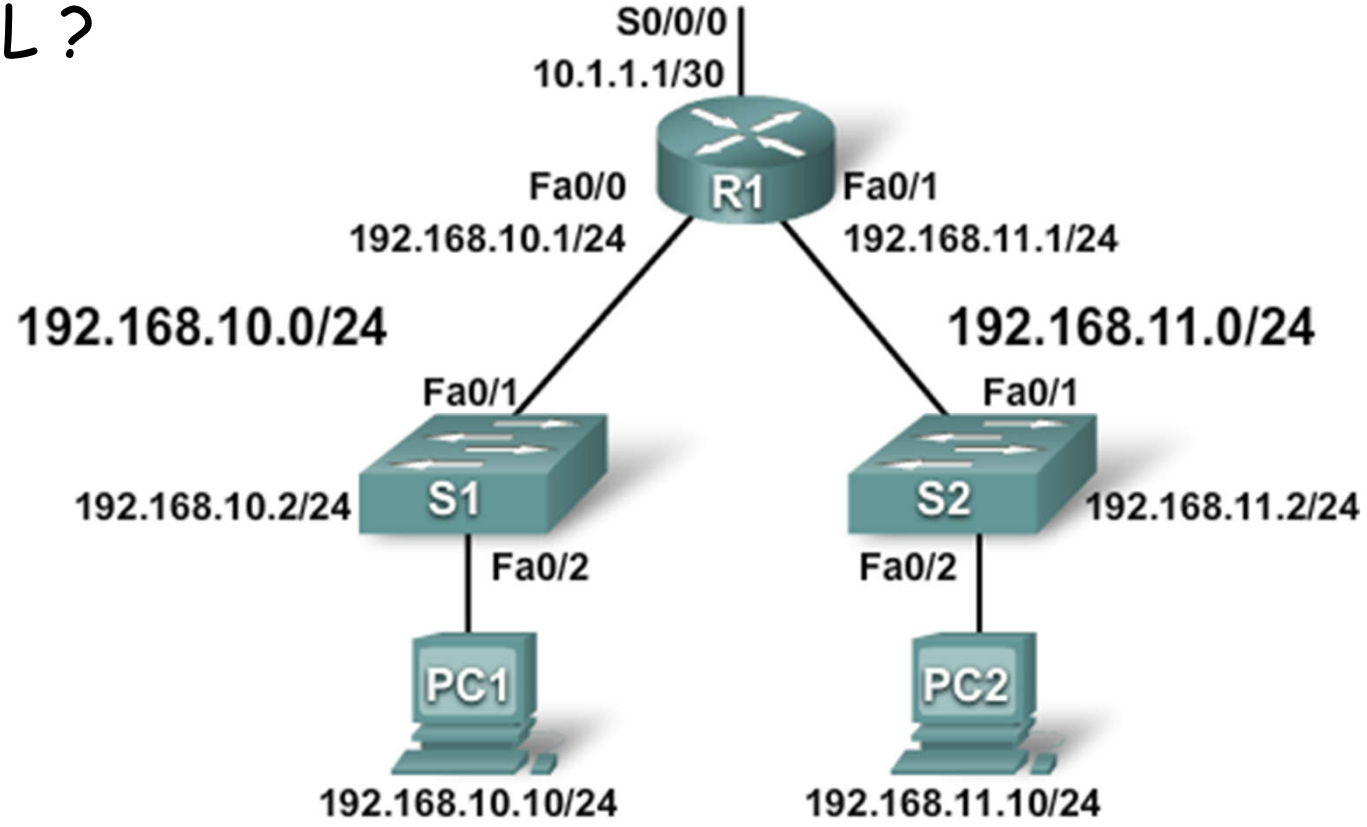
```
R1(config)#access-list 1 permit 192.168.10.10 0.0.0.0
R1(config)#access-list 1 permit host 192.168.10.10
```

- Option **any**
  - Permet de ne pas utiliser un masque 255.255.255.255
  - Désigne toutes les machines

```
R1(config)#access-list 1 permit 0.0.0.0 255.255.255.255
R1(config)#access-list 1 permit any
```

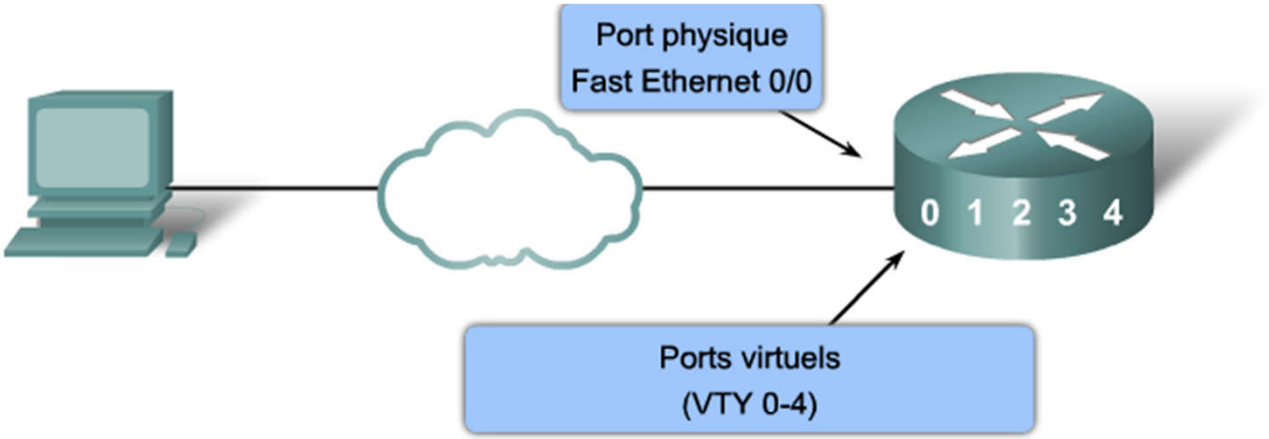
Exercice

- Donner l'ACL permettant d'interdire uniquement la machine d'@IP 192.168.10.10 d'accéder au réseau 192.168.11.0/24. Quelle interface appliquez cette ACL ?



ACL pour les lignes VTY

- Seuls les réseaux 192.168.10.0 et 192.168.11.0 à accéder aux lignes VTY 0 - 4. L'accès aux lignes VTY est refusé à tous les autres réseaux.




```
R1(config)#access-list 21 permit 192.168.10.0 0.0.0.255
R1(config)#access-list 21 permit 192.168.11.0 0.0.0.255
R1(config)#access-list 21 deny any

R1(config)#line vty 0 4
R1(config-line)#login
R1(config-line)#password secret
R1(config-line)#access-class 21 in
```

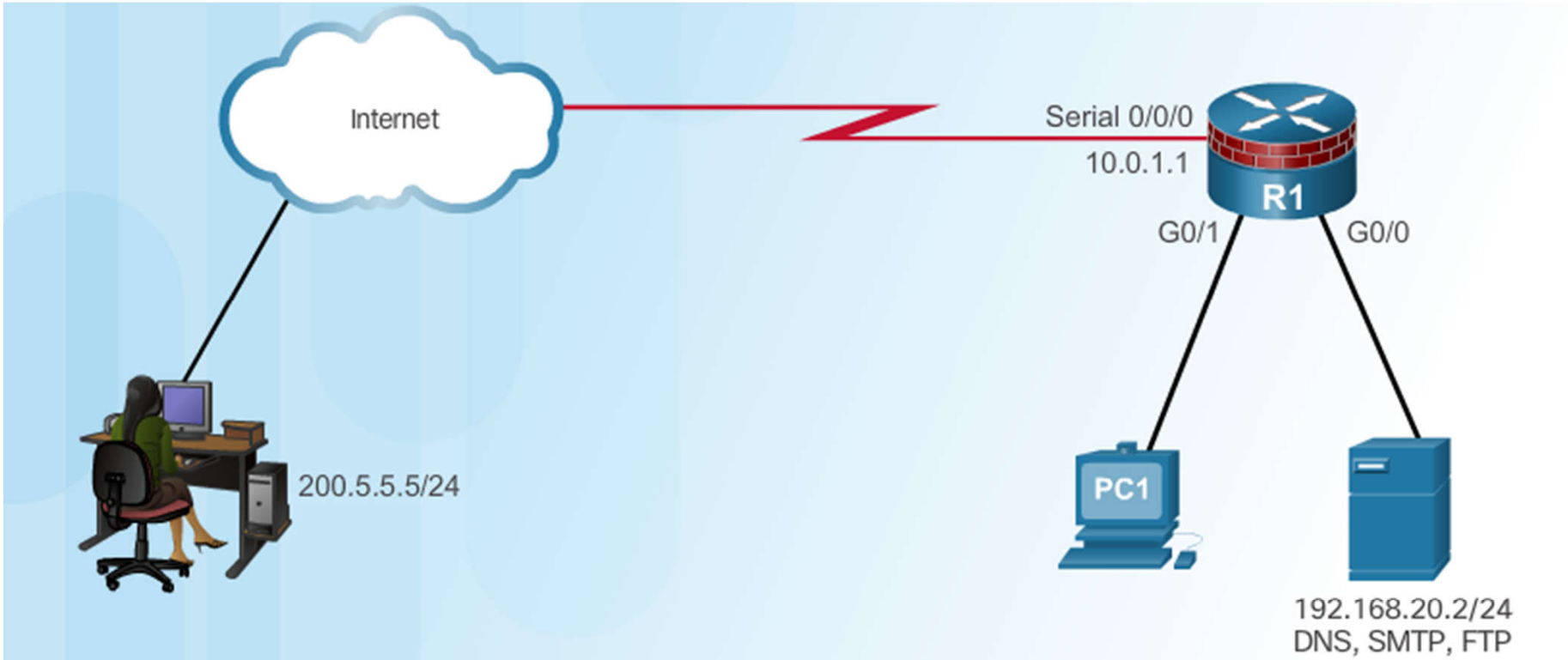
Les ACL étendues

- Autoriser ou refuser du trafic en fonction
  - @IP source et destination
  - Ports TCP et UDP source et de destination
  - Type de protocole (IP, ICMP, UDP, TCP, etc..)
- Filtrage plus intelligent que les ACL standards
  - Offre un niveau de sécurité plus élevé
  - Utiliser des numéros de ports ou des services

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 23
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 21
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 20
```

```
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq ftp-data
```

ACL pour les DMZ



Inbound on Serial 0/0/0

```
R1(config)# access-list 180 permit udp any host 192.168.20.2 eq domain
R1(config)# access-list 180 permit tcp any host 192.168.20.2 eq smtp
R1(config)# access-list 180 permit tcp any host 192.168.20.2 eq ftp
```

Conclusion

- ACL permettent de filtrer du trafic
- ACL standard
  - Adresse IP source
- ACL étendue
  - Adresse IP source et destination, Ports TCP ou UDP et type de protocole
- Mécanisme de sécurité indispensable pour les réseaux IP