Adressage et justifications

Adresses publiques utilisées par les équipements

Les équipements qui nécessitent une adresse publique sont ceux qui communiquent directement avec Internet ou exposent des services (par exemple, un routeur ou un serveur).

Ces adresses publiques doivent être configurées sur les interfaces externes (WAN) des équipements.

Equipement	Adresse publique	Rôle
Passerelle/Routeur	190.70.1.1	Adresse principale pour le NAT (vers Internet)
Firewall	190.70.1.2	Interface pour sécuriser les connexions entrantes et sortantes
Serveur Web Intranet	190.70.1.3	Hébergement des services accessibles publiquement
Serveur de Messagerie	190.70.1.4	Serveur courriel accessible depuis internet
Serveur de Diffusion	190.70.1.5	Accès public pour streaming ou autres services

Adresses IP privées pour chaque département

Chaque département dispose d'un sous-réseau local attribué à ses équipements. Ces sous-réseaux privés doivent être routés vers Internet via NAT, configuré sur le routeur principal.

Département	Sous réseau privé	Plage DHCP réservée	Exemples d'adresses attribuées
Marketing	192.168.1.0/24	192.168.1.100 - 192.168.1.200	Poste de travail : 192.168.1.101 Imprimantes : 192.168.1.110
Production		192.168.2.100 - 192.168.2.200	Poste de travail : 192.168.2.101 Serveur Diffusion (LAN) : 192.168.2.2
Développement		192.168.3.100 - 192.168.3.200	Poste de travail : 192.168.3.101

Raisons de Limiter les adresses publiques

- **Utilisation de NAT** : Éviter d'attribuer des adresses publiques aux postes de travail ou imprimantes. Ces équipements utilisent des adresses privées et passent par le NAT pour accéder à Internet.
- **Réserve d'adresses publiques** : Il reste des adresses publiques disponibles (par exemple, `190.70.1.6` à `190.70.1.29`) pour de futurs équipements ou services.

Raisons de ne pas utiliser des IP publiques pour les Switchs :

1. **Exposition aux menaces extérieures :**
    a. Si un switch a une adresse IP publique, il devient accessible depuis Internet, ce qui expose son interface de gestion à des attaques potentielles (comme des scans, des tentatives de connexion, ou des exploits).
    b. Les Switchs sont rarement conçus pour être directement accessibles depuis Internet.
2. **Gestion interne préférable :**
    a. Les Switchs sont des équipements internes, utilisés pour gérer la connectivité des machines locales. Ils n'ont pas besoin d'interagir directement avec Internet.
    b. Une adresse IP privée (par exemple, dans le sous-réseau des départements) est suffisante pour leur interface de gestion.
3. **Utilisation inefficace des adresses publiques :**
    a. Les adresses IP publiques sont limitées. Les gaspiller sur des switchs n'apporte aucun avantage fonctionnel.
    b. Il est préférable de réserver ces adresses pour les équipements et services nécessitant un accès direct à Internet (comme des serveurs Web ou des passerelles NAT).

Objectifs des ACLs :

- Sécuriser l'accès à Internet pour les départements.
- Restreindre les communications entre les départements sauf si nécessaire (les serveurs partagés).
- Protéger les serveurs sensibles (messagerie, intranet, etc.).
- Gérer l'accès à la DMZ pour les services exposés à Internet.