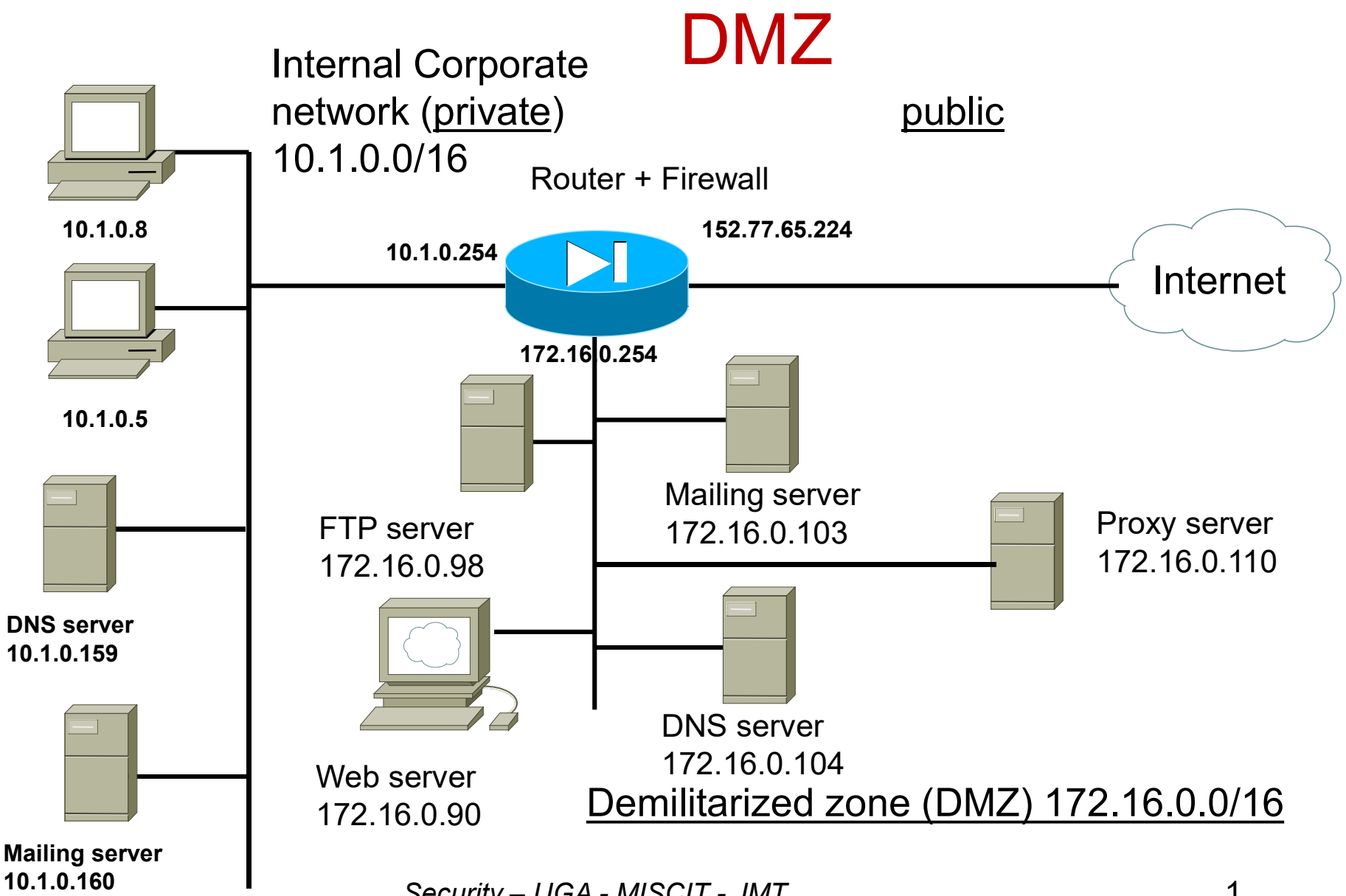
A network with a firewall/router…



Exercice 1

- Nous utilisons un pare-feu dynamique
- Les machines du réseau interne doivent pouvoir atteindre n'importe quelle machine dans la DMZ ou à l'extérieur (pour le courrier électronique)
  - Access-list 1 permit mail 10.1.0.0/16 any eq 25
- Les machines de la DMZ doivent pouvoir atteindre n'importe quelle machine à l'extérieur MAIS PAS à l'intérieur (pour le courrier électronique)
  - Access-list 1 deny mail 172.16.0.0/16 10.1.0.0/16 eq 25 (doit être avant la règle suivante!)
  - Access-list 1 permit mail 172.16.0.0/16 any eq 25
- Concernant http
  - Toute machine de l'intérieur ne doit PAS atteindre directement un http quelque part, mais la demande doit être envoyée à la machine proxy (en utilisant le port 3128)
  - Access-list 1 permit tcp/udp 10.1.0.0/16 172.16.0.110 eq 3128
  - Toute machine de la DMZ ne doit PAS atteindre directement un http quelque part, mais la demande doit être envoyée à la machine proxy (en utilisant le port 3128)
  - Pas besoin de règle
  - Le proxy devrait pouvoir atteindre n'importe quel serveur http (port 80) partout
  - Access-list 1 permit tcp 172.16.0.110 any eq 80
- Il ne faut pas oublier les aspects du DNS (port 53)
  - Access-list 1 permit tcp/udp 10.1.0.159 172.16.0.104 eq 53
  - Access-list 1 permit tcp/udp 172.16.0.104 a_specific_DNS_Server_outside eq 53
  - Access-list 1 deny any any any eq any

Exercice 2

- Soit une architecture autour d'un pare-feu à états
- On souhaite mettre en place :
  1. Toutes les machines du réseau interne doivent pinguer la DMZ ou l'extérieur.
  2. Toutes les machines de la DMZ doivent pinguer l'extérieur mais pas le réseau interne.
  3. Toutes les machines de l'intérieur doivent pouvoir sortir en http ou https en passant par le proxy
  4. Le serveur DNS du réseau interne doit pouvoir joindre le DNS de la DMZ sur le port 53.
  5. Le serveur DNS de la DMZ doit pouvoir joindre un DNS externe (IP: 143.210.47.211).
- Actions à mener
  - Si besoin, mettre en place des règles de translation
  - Ecrire les règles de filtrage et les commenter
- Audit de notre stratégie de sécurité
  - Toutes les machines du réseau interne doivent pinguer la DMZ ou l'extérieur. Est-ce une bonne stratégie ? Pourquoi ?
  - Toutes les machines de la DMZ doivent pinguer l'extérieur mais pas le réseau interne. Pourquoi cette stratégie ?

Règles de translation

- Elles sont nécessaires car nous avons utilisé des adresses privées
- 10.1.0.0/16 any 152.77.65.224 ; les machines du réseau interne sortent sur le réseau public en utilisant l'adresse publique unique 152.77.65.224
- 172.16.0.0/16 any 152.77.65.224 ; les machines de la DMZ sortent sur le réseau public en utilisant l'adresse publique unique 152.77.65.224

Règles de filtrage

Protocole	Source	Destination	Service (numéro port)	Action	Commentaire
ICMP	10.1.0.0/16	Any	Any	Pass	Réseau interne ping partout
ICMP	172.16.0.0/16	10.1.0.0/16	Any	Block	Pas de DMZ vers réseau interne
ICMP	172.16.0.0/16	Any	Any	Pass	DMZ pingue partout
TCP	10.1.0.0/16	172.16.0.110	Httpproxy	Pass	Passage flux TCP réseau interne => proxy
TCP	172.16.0.110	Any	http, https	Pass	Passage flux TCP du proxy vers les serveurs http partout
TCP,UDP	10.1.0.159	172.16.0.104	Dns (port 53)	Pass	DNS Passe du réseau interne => DMZ
TCP,UDP	172.16.0.104	143.210.47.211	Dns (port 53)	Pass	DNS passe de DMZ vers DNS externe

UGA
Université
Grenoble Alpes

Some considerations about NAT

Network Address Translation

NAT function (network address translation)

- Internet Addresses (IPv4)
  - Theory, 2^{32} addresses (~4,3.10^9 addresses)
  - Practical
    - Public addresses: ~3,2.10^9
    - Reserved addresses: test…
    - Private addresses: reserved for the internal networks (non accessible from outside)
      - 10.0.0.0 to 10.255.255.255 (prefix 10/8)
      - 172.16.0.0 to 172.31.255.255 (prefix 172.16/12)
      - 192.168.0.0 to 192.168.255.255 (prefix 192.168/16)
- NAT ensures the conversion between public and private addresses, between the internal network and the outside accesses
  - firewall,
  - sometimes a router or a computer