

# Filtrage des requêtes

Alain Patrick AINA

[aalain@trstech.net](mailto:aalain@trstech.net)

Atelier DNS/CCTLD

Yaounde, 17-21 Decembre 2004



# Les listes de contrôle d'accès (acl) (1)

- ◆ Les acl sont des listes d'adresses et de clés TSIG correspondantes utilisées pour le contrôle d'accès au serveur par l'utilisation de allow-transfer, allow-query, allow-recursion, blackhole etc.....

```
acl nom-de-acl {  
    address_match_list  
  
};
```

```
address_match_list = address_match_list_element ;
```

```
[ address_match_list_element; ... ]
```

```
address_match_list_element = [ ! ] (ip_address [/length] |
```

```
key key_id | acl_name | { address_match_list } )
```

# Les listes de contrôle d'accès (acl) (2)

```
acl clients-recursifs { !10.0.0.1; 10.0.0.0/23; };
```

```
acl esclave { 81.199.105.10; };
```

```
acl tsig { key ns1-ns2; };
```

```
acl filtre-transfert { esclave; key ns1-ns2; };
```

## Les acls prédéfinis :

none, any, localhost, localnets

# Filtrage des accès sur les serveurs primaires(1)

## Filtrage des transferts de zone par IP ou clé TSIG

```
zone "cm" {  
    type master;  
    file "db.cm";  
    allow-transfer { esclave; };  
};  
  
zone "cf" {  
    type master;  
    file "db.cf";  
    allow-transfer { filtre-transfert; };  
};
```

# Filtrage des accès sur les serveurs primaires (2)

## Filtrage des transferts de zone par IP et clé TSIG

Accepter uniquement les demandes de transfert de zone signés avec la clé ns1-ns2 et venant de l'esclave 192.168.1.2

```
acl tout-sauf-192.168.1.2 { !192.168.1.2; any; };
```

```
zone "ga" {  
    type master;  
    file "db.ga";  
    allow-transfer { !tout-sauf-192.168.1.2; key ns1-ns2; };  
};
```

# Filtrage des accès sur les serveurs esclaves

Désactiser le transfert de zone sur les esclaves qui ne servent pas d'autres esclaves

```
allow-transfer { none; };
```