CONFIGURATION VPN IPSEC SITE À SITE
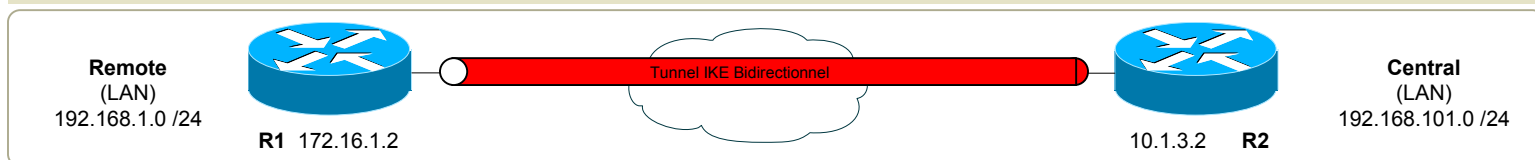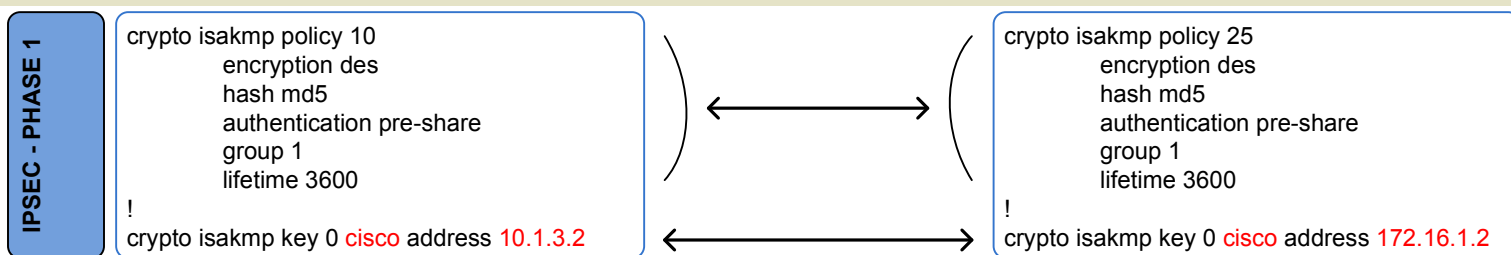
Etapes de configuration

Les étapes nécessaires sont:
- Configurer la policy ISAKMP   (Phase 1)
- Configurer le transform-set   (Phase 2 / Tunnel termination)
- Configurer l'ACL   (Trafic intéressant / Transfert sécurisé)
- Configurer la crypto map   (Phase 2)
- Appliquer la crypto-map à l'interface   (Phase 2)
- Appliquer l'ACL pour le trafic IPSec
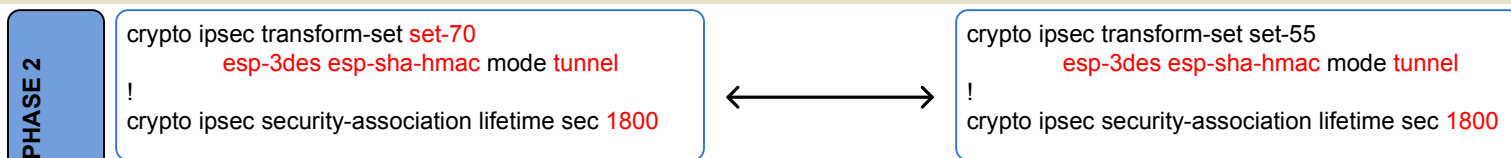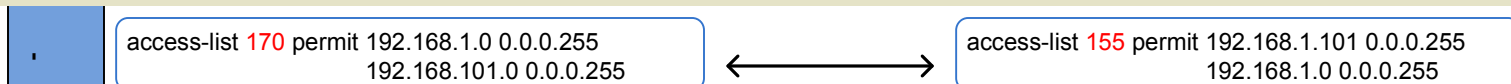
Topologie

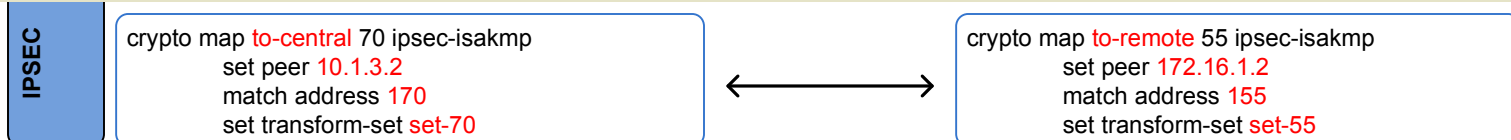**Remote**
(LAN)
192.168.1.0 /24
R1   172.16.1.2

Tunnel IKE Bidirectionnel

Central
(LAN)
192.168.101.0 /24
10.1.3.2   R2

1) Policy ISAMP

IPSEC - PHASE 1

```
crypto isakmp policy 10
    encryption des
    hash md5
    authentication pre-share
    group 1
    lifetime 3600
!
crypto isakmp key 0 cisco address 10.1.3.2
```

```
crypto isakmp policy 25
    encryption des
    hash md5
    authentication pre-share
    group 1
    lifetime 3600
!
crypto isakmp key 0 cisco address 172.16.1.2
```

2) IPSec Transform-set

PHASE 2

```
crypto ipsec transform-set set-70
    esp-3des esp-sha-hmac mode tunnel
!
crypto ipsec security-association lifetime sec 1800
```

```
crypto ipsec transform-set set-55
    esp-3des esp-sha-hmac mode tunnel
!
crypto ipsec security-association lifetime sec 1800
```

3) ACL - Définition du trafic intéressant

```
access-list 170 permit 192.168.1.0 0.0.0.255
                192.168.101.0 0.0.0.255
```

```
access-list 155 permit 192.168.1.101 0.0.0.255
                192.168.1.0 0.0.0.255
```

4) Crypto map

IPSEC

```
crypto map to-central 70 ipsec-isakmp
    set peer 10.1.3.2
    match address 170
    set transform-set set-70
```

```
crypto map to-remote 55 ipsec-isakmp
    set peer 172.16.1.2
    match address 155
    set transform-set set-55
```

5) Appliquer la crypto-map à l'interface

```
Interface serial 3/2
    ip address 172.16.1.2 255.255.255.0
    crypto map to-central
```

```
Interface serial 3/2
    ip address 10.1.3.2 255.255.255.0
    crypto map to-remote
```

6) ACL – Autorisation du trafic IPSec

```
access-list 110 permit ahp host 10.1.3.2 host 172.16.1.2
access-list 110 permit esp host 10.1.3.2 host 172.16.1.2
access-list 110 permit udp host 10.1.3.2 host 172.16.1.2 eq isakmp
!
interface serial 3/2
    ip access-group 110 in
```

```
access-list 110 permit ahp host 172.16.1.2 host 10.1.3.2
access-list 110 permit esp host 172.16.1.2 host 10.1.3.2
access-list 110 permit udp host 172.16.1.2 host 10.1.3.2 eq isakmp
!
interface serial 3/2
    ip access-group 110 in
```