Thomas FAUROUX

AIS - ADRAR 2023 2024

Sécurisation des réseaux

Firewall CISCO ASA

Table des matières

[1. Contexte 2](#_Toc136783860)

[2. Configuration des accès à une DMZ avec un FW ASA 2](#_Toc136783861)

[A. Cahier des charges 2](#_Toc136783862)

[B. Topologie 3](#_Toc136783863)

[C. Tableau routage 3](#_Toc136783864)

[D. Réseau machines 3](#_Toc136783865)

[E. Validation des tests 4](#_Toc136783866)

[3. Sécurisation de chaque site par un FW ASA sans VPN 8](#_Toc136783867)

[A. Cahier des charges 8](#_Toc136783868)

[B. Topologie 9](#_Toc136783869)

[C. Tableau routage 9](#_Toc136783870)

[D. Réseau machines 9](#_Toc136783871)

[E. Validation des tests 10](#_Toc136783872)

[4. Sécurisation de chaque site par un FW ASA avec VPN 12](#_Toc136783873)

[A. Cahier des charges 12](#_Toc136783874)

[B. Topologie 12](#_Toc136783875)

[C. Tableau routage 12](#_Toc136783876)

[D. Réseau machines 12](#_Toc136783877)

[E. Validation des tests 13](#_Toc136783878)

[5. Annexes 15](#_Toc136783879)

[A. Configuration 1 ASA 15](#_Toc136783880)

[B. Configuration 2 ASA sans VPN 16](#_Toc136783881)

[C. Configuration 2 ASA avec VPN 18](#_Toc136783882)

# Contexte

L’entreprise toulousaine TOLOSA-AERO, sous-traitant dans l’aéronautique a son siège à Toulouse et des bureaux dans certaines grandes villes comme Paris.

Pour sécuriser le réseau du siège, il a été décidé de migrer progressivement certains serveurs, initialement situés dans le LAN, dans une DMZ. Pour commencer, le serveur Intranet sera le premier à être migré dans la DMZ.

Vous venez d’intégrer le service informatique et il vous a été confié l’intégration du Firewall ASA dans le réseau.

# Configuration des accès à une DMZ avec un FW ASA

## Cahier des charges

Depuis le LAN de Toulouse

* Chaque poste du LAN de Toulouse accède par la commande ping à l’interface WAN du

routeur ISP-Paris

* Chaque poste du LAN de Toulouse doit accéder au serveur Web de la DMZ à la fois par la

commande ping que par http.

* Depuis un poste de Toulouse, le ping vers un poste de Paris doit être fonctionnel

Depuis la DMZ

* Les serveurs de la DMZ accèdent par la commande PING à l’interface WAN ISP-PARIS et au

poste du LAN PARIS

* Les serveurs de la DMZ accèdent au LAN de Toulouse (Commande ping sur un poste dans le

LAN de Toulouse)

Depuis le site de Paris

* Chaque poste du LAN de Paris accède par la commande PING à l’interface WAN du routeur

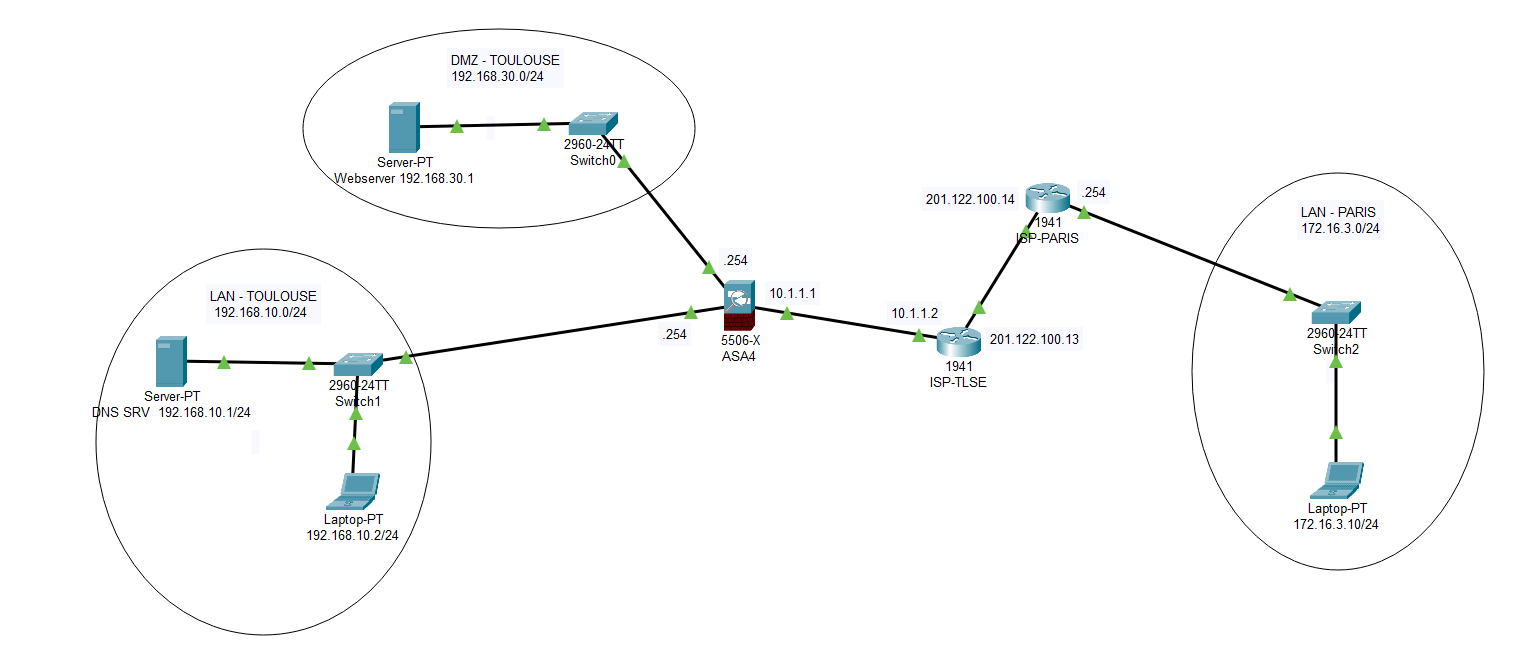
ISP-TOULOUSE

* Chaque poste du LAN de Paris doit accéder au serveur Web de la DMZ à la fois par la

commande PING et par HTTP.

* Depuis un poste de Paris, le ping vers un poste de Toulouse doit être fonctionnel

## Topologie



## Tableau routage

|  |  |  |  |
| --- | --- | --- | --- |
|  | ASA-TLSE | ISP-TLSE | ISP-PARIS |
| INSIDE | 192.168.10.254/24 | 10.1.1.2/29 | 172.16.3.254/24 |
| OUTSIDE | 10.1.1.1/24 | 201.122.100.13/30 | 201.100.14/30 |
| DMZ | 192.168.30.254/24 |  |  |
| Next Hop | 10.1.1.2 | 201.122.100.14 | 201.122.100.13 |

## Réseau machines

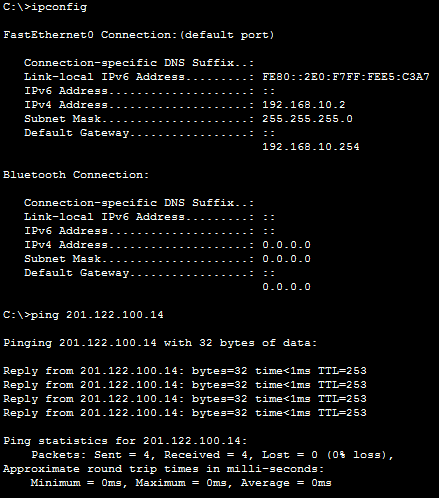
|  |  |  |  |
| --- | --- | --- | --- |
|  | Laptop TLSE | Serveur WEB TLSE | Laptop Paris |
| IP | 192.168.10.2/24 | 192.168.30.1/24 | 172.16.3.10/24 |
| Gateway | 192.168.10.254 | 192.168.30.254 | 172.16.3.254 |
| Sous-réseau | LAN TLSE | DMZ TLSE | LAN Paris |

## Validation des tests

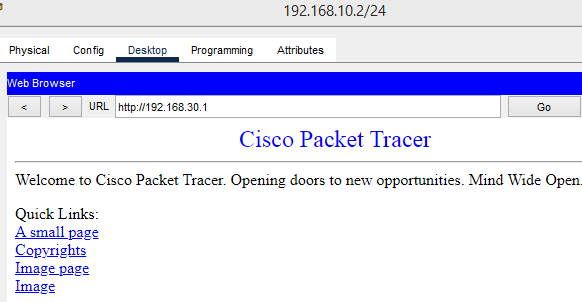
Les configurations des routeurs sont disponibles en [**annexe**](#_Configuration_1_ASA) ou sur mon github

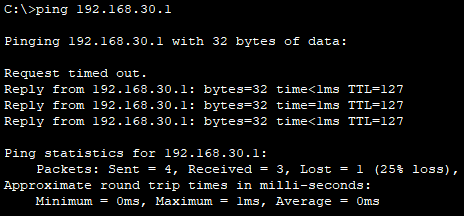
**Depuis le LAN de Toulouse**

Chaque poste du LAN de TLSE accède par la commande ping à l’interface WAN du routeur ISP-PARIS



Chaque poste du LAN de Toulouse doit accéder au serveur web de la DMZ avec la commande PING et en http

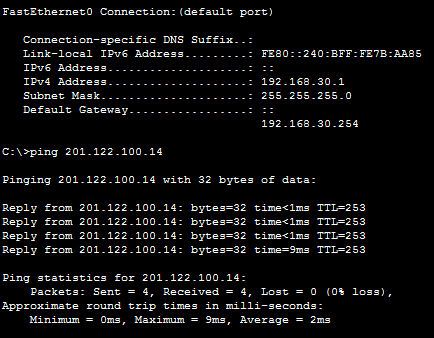


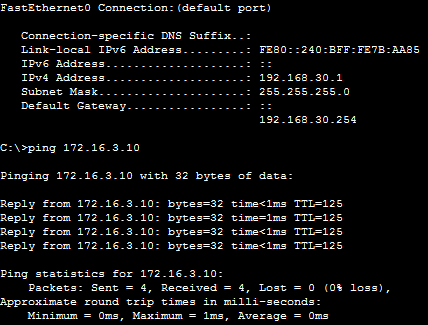


**Depuis la DMZ**

Les serveurs de la DMZ accèdent par la commande PING à l’interface WAN ISP-PARIS et au

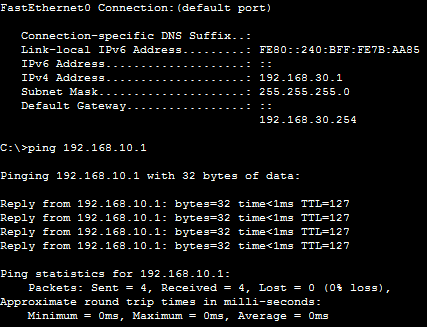
poste du LAN PARIS





Les serveurs de la DMZ accèdent au LAN de Toulouse (commande ping sur un poste dans le

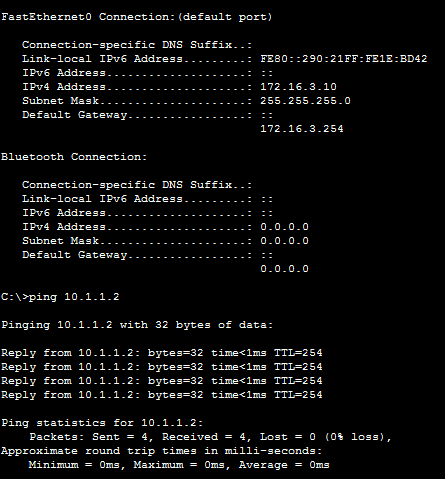
LAN de Toulouse)



**Depuis le LAN PARIS**

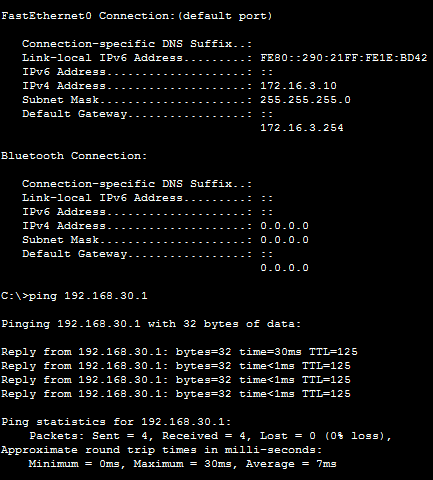
Chaque poste du LAN de Paris accède par la commande PING à l’interface WAN du routeur

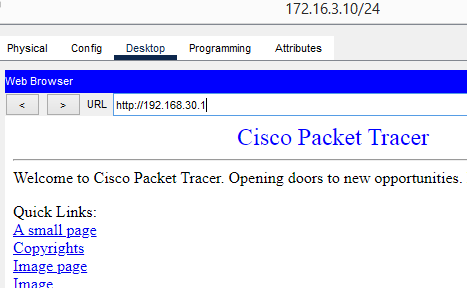
ISP-TOULOUSE



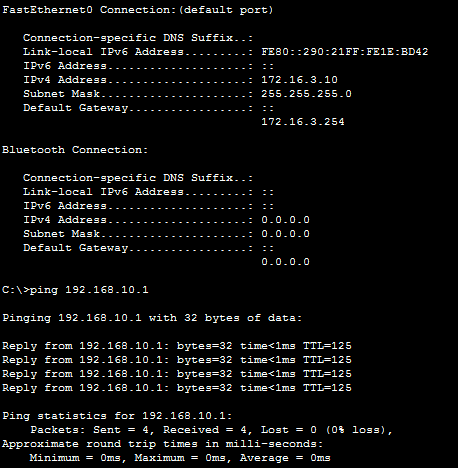
Chaque poste du LAN de Paris doit accéder au serveur Web de la DMZ à la fois par la

commande PING et par HTTP





Depuis un poste de Paris, le ping vers un poste de Toulouse doit être fonctionnel



# Sécurisation de chaque site par un FW ASA sans VPN

## Cahier des charges

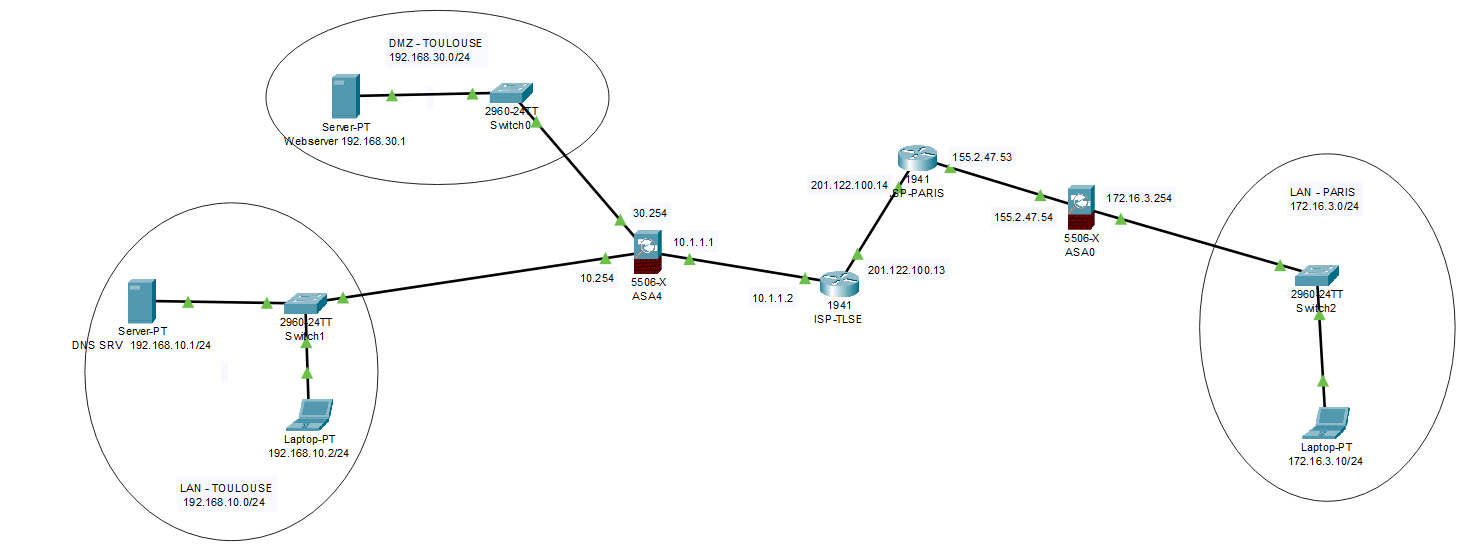
Après la première phase il a été décidé d’introduire un firewall dans chaque site pour mieux

sécuriser les sites distants.

En prenant pour site pilote celui de Paris, configurer l’ASA de Paris de sorte à permettre

l’accès au serveur de la DMZ, à partir du poste du LAN PARIS, **sans VPN**.

## Topologie



## Tableau routage

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | ASA-TLSE | ISP-TLSE | ISP-PARIS | ASA-PARIS |
| INSIDE | 192.168.10.254/24 | 10.1.1.2/29 | 155.2.47.53/30 | 172.16.3.254/24 |
| OUTSIDE | 10.1.1.1/24 | 201.122.100.13/30 | 201.100.14/30 | 155.2.47.54/30 |
| DMZ | 192.168.30.254/24 |  |  |  |
| Next Hop | 10.1.1.2 | 201.122.100.14 | 201.122.100.13 | 155.2.47.53 |

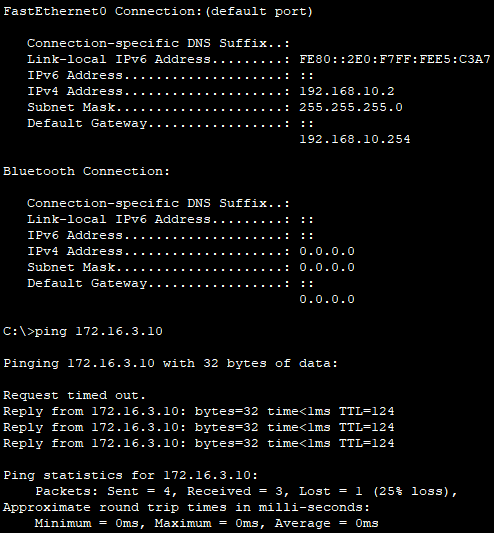
## Réseau machines

|  |  |  |  |
| --- | --- | --- | --- |
|  | Laptop TLSE | Serveur WEB TLSE | Laptop Paris |
| IP | 192.168.10.2/24 | 192.168.30.1/24 | 172.16.3.10/24 |
| Gateway | 192.168.10.254 | 192.168.30.254 | 172.16.3.254 |
| Sous-réseau | LAN TLSE | DMZ TLSE | LAN Paris |

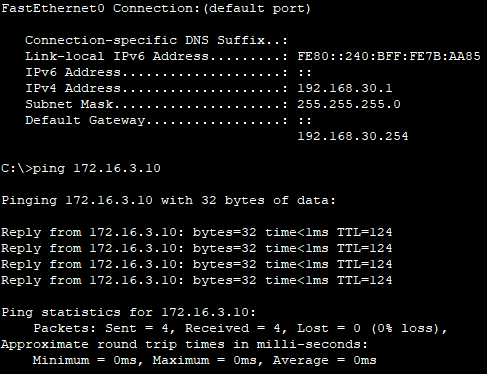
## Validation des tests

Les configurations des routeurs sont disponibles en [**annexe**](#_Configuration_2_ASA) ou sur mon github

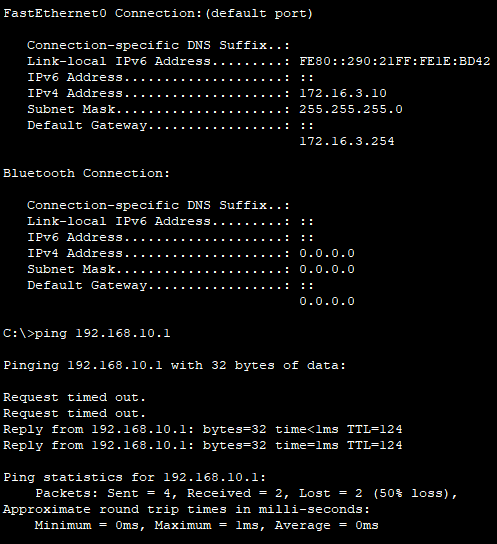
**Depuis LAN TLSE** (vers LAN PARIS)



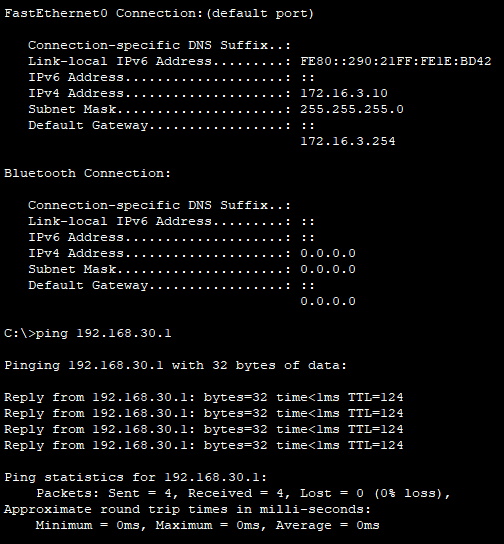
**Depuis DMZ** (vers LAN PARIS)

****

**Depuis LAN PARIS** (vers LAN TLSE)



**Depuis LAN PARIS** (vers DMZ)



# Sécurisation de chaque site par un FW ASA avec VPN

## Cahier des charges

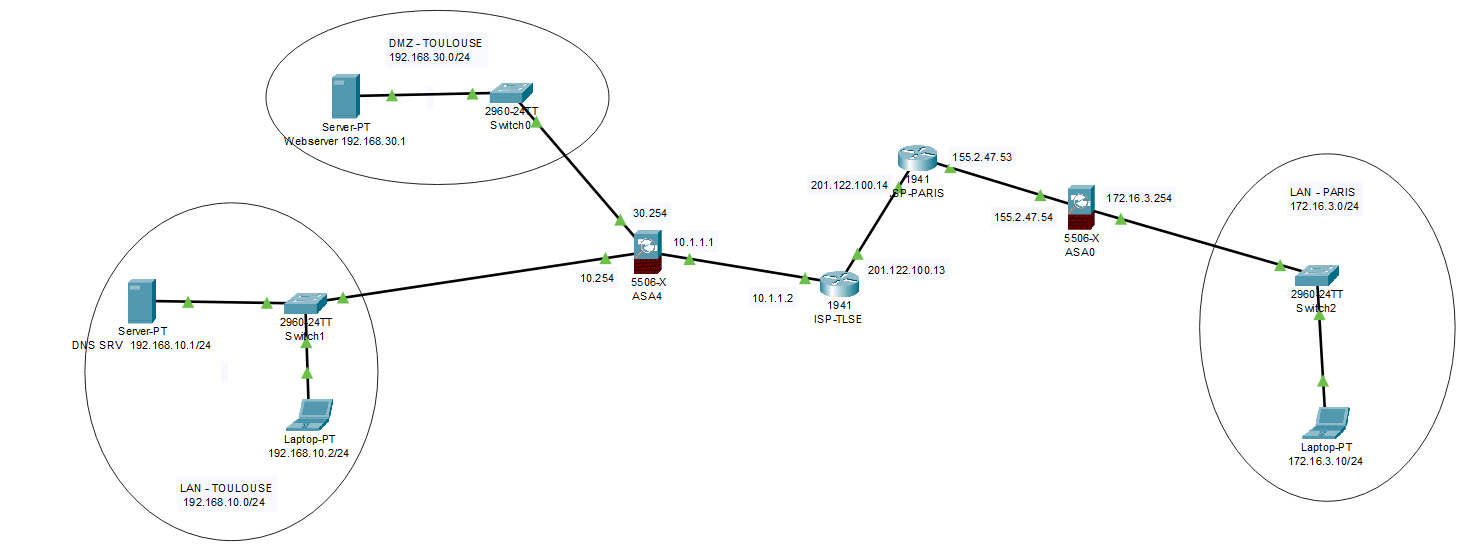
Après la première phase il a été décidé d’introduire un firewall dans chaque site pour mieux

sécuriser les sites distants.

En prenant pour site pilote celui de Paris, configurer l’ASA de Paris de sorte à permettre

l’accès au serveur de la DMZ, à partir du poste du LAN PARIS, **avec VPN**.

## Topologie



## Tableau routage

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | ASA-TLSE | ISP-TLSE | ISP-PARIS | ASA-PARIS |
| INSIDE | 192.168.10.254/24 | 10.1.1.2/29 | 155.2.47.53/30 | 172.16.3.254/24 |
| OUTSIDE | 10.1.1.1/24 | 201.122.100.13/30 | 201.100.14/30 | 155.2.47.54/30 |
| DMZ | 192.168.30.254/24 |  |  |  |
| Next Hop | 10.1.1.2 | 201.122.100.14 | 201.122.100.13 | 155.2.47.53 |

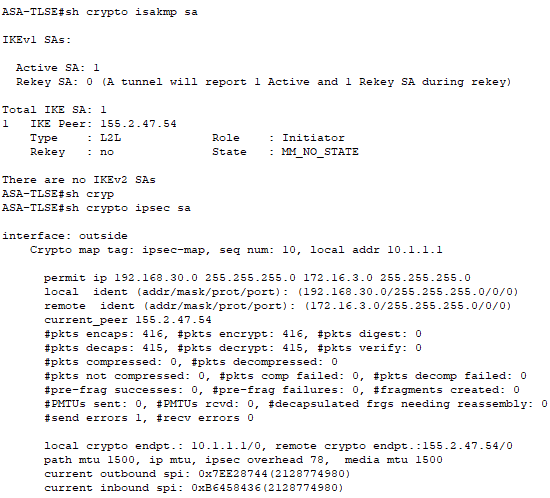
## Réseau machines

|  |  |  |  |
| --- | --- | --- | --- |
|  | Laptop TLSE | Serveur WEB TLSE | Laptop Paris |
| IP | 192.168.10.2/24 | 192.168.30.1/24 | 172.16.3.10/24 |
| Gateway | 192.168.10.254 | 192.168.30.254 | 172.16.3.254 |
| Sous-réseau | LAN TLSE | DMZ TLSE | LAN Paris |

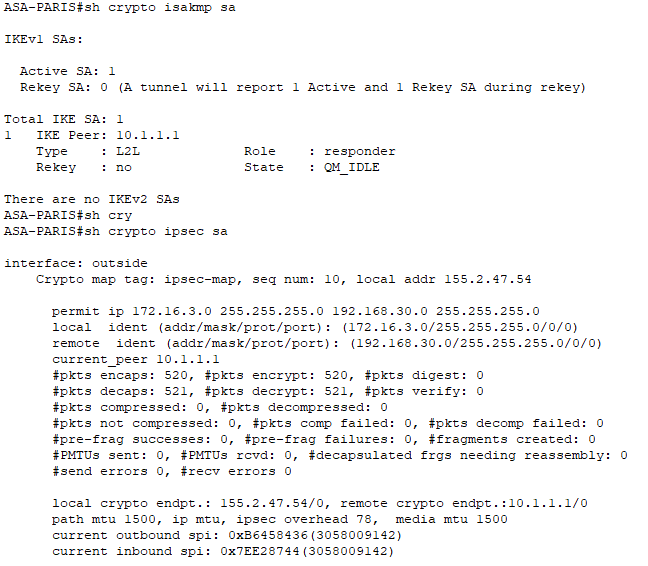
## Validation des tests

Les configurations des routeurs sont disponibles en [**annexe**](#_Configuration_2_ASA_1) ou sur mon github

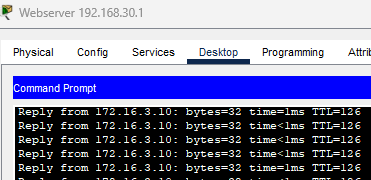
**VPN côté ASA-TLSE**



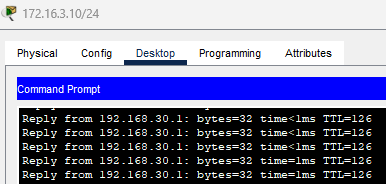
**VPN côté ASA-PARIS**



**Depuis DMZ** (vers LAN PARIS)



**Depuis LAN PARIS** (vers DMZ)



# Annexes

## Configuration 1 ASA

**ASA-TLSE**

|  |
| --- |
| en  conf t  hostname ASA-TLSE  !--Configuration interface outside  int gig1/1  ip addr 10.1.1.1 255.255.255.248  nameif outside  security-level 0  no shut  !--Configuration interface inside  int gig1/2  ip address 192.168.10.254 255.255.255.0  nameif inside  security-level 100  no shut  !--Configuration interface DMZ  int gig1/3  ip address 192.168.30.254 255.255.255.0  nameif dmz  security-level 50  no shut  !--Ajout de la route par défaut  route outside 0.0.0.0 0.0.0.0 10.1.1.2  !---ACL  !--Autorise les flux IP du serveur web vers any  access-list DMZ\_OUTSIDE extended permit ip host 192.168.30.1 any  !--Autorise les flux IP de any vers le serveur web  access-list LAN-DMZ\_OUTSIDE extended permit ip any host 192.168.30.1  !--Autorise ICMP depuis le LAN PARIS vers le LAN TLSE  access-list LAN-DMZ\_OUTSIDE extended permit icmp 172.16.3.0 255.255.255.0 192.168.10.0 255.255.255.0  !--Application des ACL  access-group DMZ\_OUTSIDE in interface dmz  access-group LAN-DMZ\_OUTSIDE in interface outside |

**ISP-TLSE**

|  |
| --- |
| **en**  **conf t**  **hostname ISP-TLSE**  **!--Configuration interface LAN**  **interface gig0/0**  **description link\_to\_ASA\_TLSE**  **ip addr 10.1.1.2 255.255.255.248**  **no shut**  **!--Configuration interface WAN**  **interface gig0/1**  **description link\_to\_ISP-PARIS**  **ip addr 201.122.100.13 255.255.255.252**  **no shut**  **!--Ajout des routes**  **ip route 0.0.0.0 0.0.0.0 201.122.100.14**  **ip route 192.168.10.0 255.255.255.0 10.1.1.1**  **ip route 192.168.30.0 255.255.255.0 10.1.1.1** |

**ISP-PARIS**

|  |
| --- |
| **en**  **conf t**  **hostname ISP-PARIS**  **!--Configuration interface LAN**  **interface gig0/0**  **description link\_to\_LAN-PARIS**  **ip addr 172.16.3.254 255.255.255.0**  **no shut**  **!--Configuration interface WAN**  **interface gig0/1**  **description link\_to\_ISP-TLSE**  **ip addr 201.122.100.14 255.255.255.252**  **no shut**  **!--Ajout des routes**  **ip route 0.0.0.0 0.0.0.0 201.122.100.13** |

## Configuration 2 ASA sans VPN

**ASA-TLSE**

|  |
| --- |
| en  conf t  hostname ASA-TLSE  !--Configuration interface outside  int gig1/1  ip addr 10.1.1.1 255.255.255.248  nameif outside  security-level 0  no shut  !--Configuration interface inside  int gig1/2  ip address 192.168.10.254 255.255.255.0  nameif inside  security-level 100  no shut  !--Configuration interface DMZ  int gig1/3  ip address 192.168.30.254 255.255.255.0  nameif dmz  security-level 50  no shut  !--Ajout de la route par défaut  route outside 0.0.0.0 0.0.0.0 10.1.1.2  !---ACL  !--Autorise les flux IP du serveur web vers any  access-list DMZ\_OUTSIDE extended permit ip host 192.168.30.1 any  !--Autorise les flux IP de any vers le serveur web  access-list LAN-DMZ\_OUTSIDE extended permit ip any host 192.168.30.1  !--Autorise ICMP depuis le LAN PARIS vers le LAN TLSE  access-list LAN-DMZ\_OUTSIDE extended permit icmp 172.16.3.0 255.255.255.0 192.168.10.0 255.255.255.0  !--Application des ACL  access-group DMZ\_OUTSIDE in interface dmz  access-group LAN-DMZ\_OUTSIDE in interface outside |

**ASA-PARIS**

|  |
| --- |
| en  conf t  hostname ASA-PARIS  !--Configuration interface outside  int gig1/1  ip addr 155.2.47.54 255.255.255.252  nameif outside  security-level 0  no shut  !--Configuration interface inside  int gig1/2  ip address 172.16.3.254 255.255.255.0  nameif inside  security-level 100  no shut  !--Ajout de la route par défaut  route outside 0.0.0.0 0.0.0.0 155.2.47.53  !---ACL  !--Autorise ICMP depuis le LAN PARIS vers le LAN TLSE  access-list OUTSIDE\_LAN extended permit icmp 192.168.10.0 255.255.255.0 172.16.3.0 255.255.255.0  !--Autorise ICMP/HTTP depuis le LAN PARIS vers la DMZ  access-list OUTSIDE\_LAN extended permit ip 192.168.30.0 255.255.255.0 172.16.3.0 255.255.255.0  !--Application des ACL  access-group OUTSIDE\_LAN in interface outside |

**ISP-TLSE**

|  |
| --- |
| en  conf t  hostname ISP-TLSE  !--Configuration interface LAN  interface gig0/0  description link\_to\_ASA\_TLSE  ip addr 10.1.1.2 255.255.255.248  no shut  !--Configuration interface WAN  interface gig0/1  description link\_to\_ISP-PARIS  ip addr 201.122.100.13 255.255.255.252  no shut  !--Ajout des routes  ip route 0.0.0.0 0.0.0.0 201.122.100.14  ip route 192.168.10.0 255.255.255.0 10.1.1.1  ip route 192.168.30.0 255.255.255.0 10.1.1.1 |

**ISP-PARIS**

|  |
| --- |
| en  conf t  hostname ISP-PARIS  !--Configuration interface LAN  interface gig0/0  description link\_to\_ASA-PARIS  ip addr 155.2.47.53 255.255.255.252  no shut  !--Configuration interface WAN  interface gig0/1  description link\_to\_ISP-TLSE  ip addr 201.122.100.14 255.255.255.252  no shut  !--Ajout des routes  ip route 0.0.0.0 0.0.0.0 201.122.100.13  ip route 172.16.3.0 255.255.255.0 155.2.47.54 |

## Configuration 2 ASA avec VPN

**ASA-TLSE**

|  |
| --- |
| **!-ASA-TLSE**  **en**  **conf t**  **hostname ASA-TLSE**  **crypto ipsec ikev1 transform-set ipsec-set esp-3des esp-md5-hmac**  **crypto map ipsec-map 10 match address 1**  **crypto map ipsec-map 10 set peer 155.2.47.54**  **crypto map ipsec-map 10 set ikev1 transform-set ipsec-set**  **crypto map ipsec-map interface outside**  **crypto ikev1 enable outside**  **crypto ikev1 policy 1**  **encr 3des**  **authentication pre-share**  **group 2**  **lifetime 43200**  **tunnel-group 155.2.47.54 type ipsec-l2l**  **tunnel-group 155.2.47.54 ipsec-attributes**  **ikev1 pre-shared-key cisco123**  **route outside 0.0.0.0 0.0.0.0 10.1.1.2**  **access-list 1 extended permit ip 192.168.30.0 255.255.255.0 172.16.3.0 255.255.255.0**  **access-list DMZ\_OUTSIDE extended permit ip host 192.168.30.1 any**  **access-list LAN-DMZ\_OUTSIDE extended permit ip any host 192.168.30.1**  **access-list LAN-DMZ\_OUTSIDE extended permit icmp 172.16.3.0 255.255.255.0 192.168.10.0 255.255.255.0**  **access-group DMZ\_OUTSIDE in interface dmz**  **access-group LAN-DMZ\_OUTSIDE in interface outside** |

**ASA-PARIS**

|  |
| --- |
| **!-ASA-PARIS**  **en**  **conf t**  **hostname ASA-PARIS**  **crypto ipsec ikev1 transform-set ipsec-set esp-3des esp-md5-hmac**  **crypto map ipsec-map 10 match address 1**  **crypto map ipsec-map 10 set peer 10.1.1.1**  **crypto map ipsec-map 10 set ikev1 transform-set ipsec-set**  **crypto map ipsec-map interface outside**  **crypto ikev1 enable outside**  **crypto ikev1 policy 1**  **encr 3des**  **authentication pre-share**  **group 2**  **lifetime 43200**  **tunnel-group 10.1.1.1 type ipsec-l2l**  **tunnel-group 10.1.1.1 ipsec-attributes**  **ikev1 pre-shared-key cisco123**  **route outside 0.0.0.0 0.0.0.0 155.2.47.53**  **access-list 1 extended permit ip 172.16.3.0 255.255.255.0 192.168.30.0 255.255.255.0**  **access-list OUTSIDE\_LAN extended permit icmp 192.168.10.0 255.255.255.0 172.16.3.0 255.255.255.0**  **access-list OUTSIDE\_LAN extended permit ip 192.168.30.0 255.255.255.0 172.16.3.0 255.255.255.0**  **access-group OUTSIDE\_LAN in interface outside** |

**ISP-TLSE**

|  |
| --- |
| **en**  **conf t**  **hostname ISP-TLSE**  **!--Configuration interface LAN**  **interface gig0/0**  **description link\_to\_ASA\_TLSE**  **ip addr 10.1.1.2 255.255.255.248**  **no shut**  **!--Configuration interface WAN**  **interface gig0/1**  **description link\_to\_ISP-PARIS**  **ip addr 201.122.100.13 255.255.255.252**  **no shut**  **!--Ajout des routes**  **ip route 0.0.0.0 0.0.0.0 201.122.100.14**  **ip route 192.168.10.0 255.255.255.0 10.1.1.1**  **ip route 192.168.30.0 255.255.255.0 10.1.1.1** |

**ISP-PARIS**

|  |
| --- |
| **en**  **conf t**  **hostname ISP-PARIS**  **!--Configuration interface LAN**  **interface gig0/0**  **description link\_to\_ASA-PARIS**  **ip addr 155.2.47.53 255.255.255.252**  **no shut**  **!--Configuration interface WAN**  **interface gig0/1**  **description link\_to\_ISP-TLSE**  **ip addr 201.122.100.14 255.255.255.252**  **no shut**  **!--Ajout des routes**  **ip route 0.0.0.0 0.0.0.0 201.122.100.13**  **ip route 172.16.3.0 255.255.255.0 155.2.47.54** |