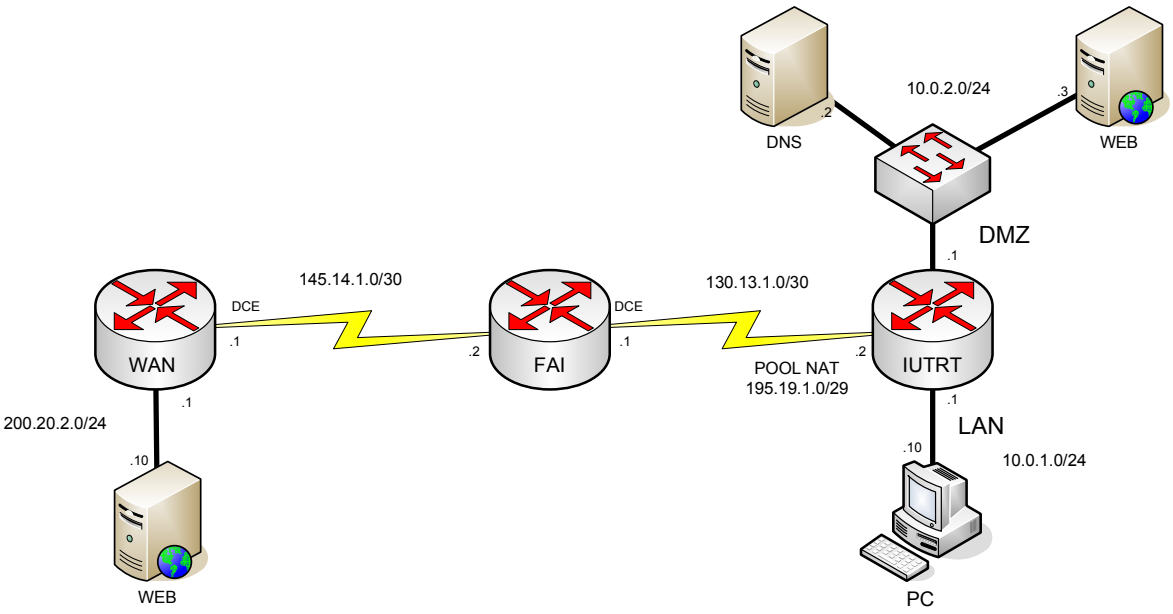
TD ACL

Le TD ci-dessous met en place une solution de type DMZ (de l'anglais demilitarized zone) pour l'établissement d'un réseau sécurisé. Il ne constitue en aucun cas une solution complète qui nécessiterait l'utilisation d'équipements réseaux dédiés comme par exemple des pare-feux, des serveurs proxy, etc.

1. Topologie de travail

En réseau, une DMZ est un sous-réseau séparé du réseau local de l'entreprise, et qui contient des machines (dans notre cas serveurs WEB et DNS) susceptibles d'être atteints depuis Internet ou du réseau local, mais qui en cas de compromission ne devront pas permettre au pirate de lancer une attaque sur le réseau local ou internet.

Dans le cadre de ce TD, nous utiliserons la topologie classique suivante :



où le routeur IUTRT assure la sécurité des réseaux LAN et DMZ au moyen d'un mécanisme de traduction d'adresses et d'ACLs.

Les interfaces des routeurs respectent le plan d'adressage ci-dessous :

Nom de Interface	WAN	FAI	IUTRT
fa0/0	200.20.2.1/24		10.0.1.1/24
fa0/1			10.0.2.1/24
S0/1/0	145.14.1.1/30	145.14.1.2/30	130.13.1.2/30
s0/1/1		130.13.1.1/30	

Et les interfaces des PCs suivent le plan d'adressage ci-dessous, avec une distinction dans le cas où ils sont visibles directement dans le réseau ou au travers d'une traduction d'adresses :

	PC LAN	DNS du WAN	WEB du WAN	DNS de la DMZ	WEB de la DMZ
@public	195.19.1.1/29	200.20.2.2/24	200.20.2.3/24	195.19.1.2/29	195.19.1.3/29
@privée	10.0.1.10/24			10.0.2.2 /24	10.0.2.3 /24

2. Mise en place générale

Toutes les interfaces de vos routeurs ainsi que celles des PCs sont configurées.

Mettez en place le routage en respectant les consignes suivantes :

- EIGRP est utilisé entre WAN et FAI ; FAI n'annoncera pas le réseau 130.13.1.0/30 et redistribuera sa route statique vers le réseau 195.19.1.0/29 ;
- une route par défaut sera placée sur IUTRT.

A ce stade-là du TD, votre score doit-être de 31% et la table de routage du routeur WAN est la suivante :

145.14.0.0/16 is variably subnetted, 2 subnets, 2 masks
D 145.14.0.0/16 is a summary, 03:15:11, Null0
C 145.14.1.0/30 is directly connected, Serial0/1/0
195.19.1.0/29 is subnetted, 1 subnets
D EX 195.19.1.0 [170/7289856] via 145.14.1.2, 03:15:11, Serial0/1/0
C 200.20.2.0/24 is directly connected, FastEthernet0/0

Mettez en place maintenant la traduction d'adresses sur le routeur IUTRT selon les consignes suivantes :

1) pour que le site web de l'entreprise puisse être consulté de l'extérieur, l'adresse 10.0.2.3 en tcp sur le port 80 sera traduite statiquement en 195.19.1.3 sur le port 8080 ;
2) pour permettre les échanges entre les serveurs DNS, l'adresse 10.0.2.2 sera traduite statiquement en 195.19.1.2[1] ;
3) pour permettre aux machines du réseau local de sortir sur internet, les adresses du réseau local 10.0.1.0/24 seront toutes traduites sur l'adresse 195.19.1.1 . Pour cela vous définirez un pool de traduction **POOL_LAN** ne contenant que l'adresse 195.19.1.1, et mettrez en place une surcharge de port sur ce pool. L'acces-list capturant le trafic à traduire sera une ACL nommée standard appelée **PAT_LAN**.

A l'issue de la mise en place de la traduction d'adresses, votre score doit-être de 68% (ou 57% si vous inversez les consignes 1 et 2).

Pour un trafic initié depuis le LAN, vérifiez que vous obtenez les résultats attendus aux tests suivants:

N° Test	Protocole	Source	Destination	Résultat attendu
1	ICMP	10.0.1.10	10.0.2.2	oui
2	ICMP	10.0.1.10	10.0.2.3	oui

[1] Cette solution n'est pas la meilleure, mais compte tenu de vos connaissances et de l'utilisation de Packet Tracer, il n'est pas possible de faire autrement.

3	ICMP	10.0.1.10	200.20.2.3	oui
4	HTTP	10.0.1.10	10.0.2.2	oui
5	HTTP	10.0.1.10	10.0.2.3	oui
6	HTTP	10.0.1.10	webrt	oui
7	HTTP	10.0.1.10	200.20.2.3	oui
8	HTTP	10.0.1.10	web.wan.fr	oui

Pour un trafic initié depuis la DMZ, vérifiez que vous obtenez les résultats attendus aux tests suivants :

N° Test	Protocole	Source	Destination	Résultat attendu
9	ICMP	10.0.2.2	10.0.1.10	oui
10	ICMP	10.0.2.2	200.20.2.3	oui
11	HTTP	10.0.2.2	200.20.2.3	oui
12	HTTP	10.0.2.2	web.wan.fr	oui
13	ICMP	10.0.2.3	10.0.1.10	oui
14	ICMP	10.0.2.3	200.20.2.3	non
15	HTTP	10.0.2.3	200.20.2.3	non

Pour un trafic initié depuis le WAN, vérifiez que vous obtenez les résultats attendus aux tests suivants:

N° Test	Protocole	Source	Destination	Résultat attendu
16	ICMP	200.20.2.3	195.19.1.2	oui
17	ICMP	200.20.2.3	195.19.1.3	non
18	HTTP	200.20.2.3	195.19.1.3:8080	oui
19	HTTP	200.20.2.3	web.rt.fr:8080	oui
20	HTTP	200.20.2.3	195.19.1.2	oui
21	TFTP	Routeur WAN	195.19.1.2	oui

Pourquoi est-il normal que les tests 14, 15 et 17 échouent ?
Pourquoi est-il normal que le test 21 fonctionne ?

3. Mise en place de la sécurité

Afin de protéger notre réseau local et notre DMZ, nous allons mettre sur le routeur IUTRT une ACL étendue nommée en entrée de chaque interface.

Ces acls respecteront une politique générale de sécurité qui consistera :

1. à contrôler la source d'un trafic issu du réseau LAN ou DMZ ;
2. qu'un trafic revenant correspond bien à la réponse d'un trafic initié depuis le réseau LAN ou DMZ ;
3. à empêcher par défaut que tout rentre (ce qui est le comportement classique d'une ACL).

3.1 Protection du réseau d'entreprise

La plupart des attaques réseaux étant dues à des pirates internes, il faut se garantir que seul le trafic du réseau `10.0.0.0` puisse entrer dans le routeur par l'interface `fa0/0`.

De plus, il a été décidé que les utilisateurs du réseau local ne pourront faire que du web, utiliser le protocole `ICMP` pour vérifier qu'une machine est connectée, et interroger uniquement le DNS situé dans la DMZ.

Ecrire une access-list **LAN** nommée étendue correspondant au tableau ci-dessous :

N° règle	Action	Protocole	Source	Port Source	Destination	Port destination
10	autorise	udp	10.0.1.0/24	> 1023	10.0.2.2	53
20	refuse	ip	10.0.1.0/24		10.0.2.2	
30	autorise	tcp	10.0.1.0/24	> 1023	n'importe où	80
40	autorise	icmp	10.0.1.0/24		n'importe où	

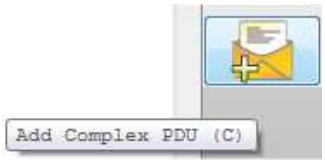
Dans la règle 10, pourquoi est-il indiqué que le port source est supérieur à 1023 ?
Pourquoi la règle n°20 est-elle nécessaire dans cette ACL ?

Contrôlez que l'ACL fonctionne bien en vous assurant de retrouver les résultats attendus aux tests suivants :

N° Test	Protocole	Source	Destination	Résultat attendu
1	ICMP	10.0.1.10	10.0.2.2	**non**
4	HTTP	10.0.1.10	10.0.2.2	**non**
6	HTTP	10.0.1.10	webrt	**Toujours oui**
8	HTTP	10.0.1.10	web.wan.fr	**Toujours oui**

Si vous souhaitez contrôler également que cette ACL filtre bien la source du trafic, vous pouvez utiliser une fonctionnalité intéressante du mode Simulation de Packet Tracer

Ainsi, après être passé en mode simulation, cliquez sur l'enveloppe permettant de créer un PDU complexe. Choisissez votre protocole, indiquez une adresse source bidon, remplissez les paramètres du protocole et au moyen du bouton `Capture Forward` vérifiez que le trafic est bien bloqué. **N'oubliez pas de quitter le mode Simulation !**



3.2 Protection de la DMZ

La protection de la DMZ est plus complexe. Comme pour le réseau local, il faudra s'assurer que :

- le trafic entrant par l'interface `fa0/1` possède bien une adresse source en `10.0.2.X/24`, mais qu'en plus pour les flux `HTTP`, `DNS` et `ICMP`, il est bien la réponse à un trafic initié depuis le réseau local ou le WAN ;
- le serveur DNS de la DMZ puisse interroger le serveur DNS du WAN lorsqu'une requête concernera le domaine `wan.fr`.

Traduisez l'ensemble de cette politique de sécurité en écrivant une access-list **DMZ** nommée étendue correspondant au tableau ci-dessous :

N° règle	Action	Protocole	Source	Port Source	Destination	Port destination
10	autorise	tcp établi	10.0.2.3	80	n'importe où	> 1023
20	autorise	udp	10.0.2.2	53	10.0.1.0/24	> 1023
30	autorise	udp	10.0.2.2	53	200.20.2.2	> 1023
40	autorise	echo-reply	10.0.2.0/24		10.0.1.0/24	
50	autorise	udp	10.0.2.2	> 1023	200.20.2.2	53

Contrôlez que l'ACL fonctionne bien en vous assurant de retrouver les résultats attendus aux tests suivants :

N° Test	Protocole	Source	Destination	Résultat attendu
6	HTTP	10.0.1.10	webrt	**Toujours oui**
9	ICMP	10.0.2.2	10.0.1.10	**non**
10	ICMP	10.0.2.2	200.20.2.3	**non**
11	HTTP	10.0.2.2	200.20.2.3	**non**
13	ICMP	10.0.2.3	10.0.1.10	**non**
16	ICMP	200.20.2.3	195.19.1.2	**non**
19	HTTP	200.20.2.3	web.rt.fr:8080	**Toujours oui**
20	HTTP	200.20.2.3	195.19.1.2	**non**
21	TFTP	Routeur WAN	195.19.1.2	**non**

Le résultat du test 16 "délai d'attente dépassé" implique que l'`echo-request` a été traduit mais que l'`echo-reply` a été bloqué par notre ACL (le résultat du test 20 indique le même problème). Cette situation n'est qu'à demi satisfaisante et nous allons maintenant y remédier.

3.3 Contrôle du trafic en provenance du WAN

Pour finir, nous allons filtrer le trafic qui rentre sur l'interface du routeur IUT qui est connecté au wan.

Tout d'abord nous allons nous protéger d'une méthode classique d'attaque des réseaux qui consiste à tenter d'usurper une adresse IP source interne valide (on parle de "spoofing). Dans notre cas, les trois types d'adresse IP source qu'un pirate pourrait usurper sont les adresses du réseau `10.0.0.0`, les adresses réservées aux essais en mode bouclé `127.x.x.x`, et les adresses de multicast `224.x.x.x – 239.x.x.x`.

Ensuite, nous nous assurerons que le trafic entrant correspond bien à un trafic établi (par exemple, la réponse à un trafic que nous avons initié depuis une machine du réseau LAN). Pour ce faire, nous ne laisserons entrer que les `echo-reply`, le trafic `TCP` venant de n'importe où depuis le port 80 et à destination de notre adresse de surcharge, et la réponse du DNS situé dans le WAN à une demande du DNS situé dans la DMZ.

Enfin, nous nous assurerons que le seul autre trafic pouvant rentrer correspond à une requête d'interrogation destinés aux serveurs DNS et WEB.

Traduisez l'ensemble de cette politique de sécurité en écrivant une access-list **WAN** nommée étendue correspondant au tableau ci-dessous :

N° règle	Action	Protocole	Source	Port Source	Destination	Port destination
10	refuse	ip	10.0.0.0/8		n'importe où	
20	refuse	ip	224.0.0.0/4		n'importe où	
30	autorise	echo-reply	n'importe où		195.19.1.1	
40	autorise	tcp établi	n'importe où	80	195.19.1.1	> 1023
50	autorise	tcp	n'importe où	> 1023	195.19.1.3	8080
60	autorise	udp	n'importe où	> 1023	195.19.1.2	53
70	autorise	udp	n'importe où	53	195.19.1.2	> 1023

Contrôlez que l'ACL fonctionne bien en vous assurant de retrouver les résultats attendus aux tests suivants :

N° Test	Protocole	Source	Destination	Résultat attendu
3	ICMP	10.0.1.10	200.20.2.3	**Toujours oui**
8	HTTP	10.0.1.10	web.wan.fr	**Toujours oui**
16	ICMP	200.20.2.3	195.19.1.2	**Toujours non**
19	HTTP	200.20.2.3	web.rt.fr:8080	**Toujours oui**

Le résultat du test 16 est maintenant "hôte injoignable" ce qui indique que l'`echo-request` a bien été bloqué

Voici un récapitulatif de tous les tests dont on a changé le comportement

N° Test	Protocole	Source	Destination	Résultat initial	Résultat final
1	ICMP	10.0.1.10	10.0.2.2	oui	**non**
4	HTTP	10.0.1.10	10.0.2.2	oui	**non**
9	ICMP	10.0.2.2	10.0.1.10	oui	**non**
10	ICMP	10.0.2.2	200.20.2.3	oui	**non**
11	HTTP	10.0.2.2	200.20.2.3	oui	**non**
12	HTTP	10.0.2.2	web.wan.fr	oui	**non**
13	ICMP	10.0.2.3	10.0.1.10	oui	**non**
14	ICMP	10.0.2.3	200.20.2.3	non	**non**
15	HTTP	10.0.2.3	200.20.2.3	non	**non**
16	ICMP	200.20.2.3	195.19.1.2	oui	**non**
17	ICMP	200.20.2.3	195.19.1.3	non	**non**
20	HTTP	200.20.2.3	195.19.1.2	oui	**non**
21	TFTP	Routeur WAN	195.19.1.2	oui	**non**