Les points portent, en générale sur les explications. Une simple réponse "oui" ou "non" à une question ne rapportera aucun point.

Exercice 1 TLS

Question 1 MIM

Expliquez ce qu'est une attaque ManIntheMiddle (MIM) et en quoi TLS permet de s'en protéger.

Question 2 MIM et ssh

Comment se comporte ssh vis à vis des attaques MiM (Man In the Middle) ?

Question 3 certificat

Alice a mis en place un serveur WeB accessible en https. Elle demande à Bob ce qu'il pense de la sécurité de son serveur. Bob lui annonce fièrement qu'en utilisant un outil de pentest profond récupérer sur le darkweb via le protocole Tor, il a réussit à récupérer le certificat du site d'Alice et donc que la sécurité de son serveur et de ses utilisateurs est compromise.

Alice lui rit au nez.

Que pensez-vous de la situation et de la position des deux amis ? (pas d'explications, pas de points)

Question 4 TOR

Bob explique à Alice qu'il utilise TOR pour se connecter sur le site http://supersite.com/ et

- qu'ainsi, la communication est chiffrée
- que personne ne peut espionner sa communication
- que le serveur destination ne sait même pas qui il est et l'IP de son poste
- que c'est bien mieux que https

Que pensez-vous des affirmations de Bob ?

Exercice 2 supervision

Question 1 supervision

Définissez et expliquez les différences entre supervision et métrologie. Nagios fait-il de la supervision ou de la métrologie ou les 2 ? (cette dernière question sur Nagios ne rapportera de points que si vous avez défini les 2 notions "métrologie" et "supervision").

Question 2 NRPE/NSCA

On se place dans le cadre de nagios. Expliquez les contextes d'usage et la différence entre NRPE et NCSA.

Exercice 3 IPv6

Question 1 adresses IPv6

Ipv6 supporte plusieurs modes de récupération dynamique d'adresses Ipv6. Citez 2 méthodes permettant de fournir des adresses Ipv6 à des machines d'un réseau local et expliquez dans quel contexte on utilise l'un plutôt que l'autre.

Question 2 adresses Ipv6 et vie privée

On dit parfois qu'Ipv6 posera des soucis en matière de vie privée. Expliquez ce que l'on entend par là et ce qui est prévu pour palier ce problème.

Exercice 4 Ipv6 NAT64/DNS64: Intégration d'IPv6 dans le réseau d'entreprise du cabinet 6-4-2

Cet exercice est plus que largement inspiré de l'évaluation du MOOC Objectif Ipv6 session 3.

Le cabinet 6-4-2 est une société de conseil, de formation et d'assistance à maîtrise d'ouvrage (AMOA) sur les infrastructures numériques. Le réseau du cabinet (voir la figure 1) est cloisonné en plusieurs domaines de diffusion (VLAN). Une zone démilitarisée (DMZ) héberge les serveurs publics (DNS, web, serveur mail...) accessibles depuis l'Internet, sous le contrôle d'un routeur firewall. Les autres zones hébergent les postes utilisateurs. L'espace WiFi supporte les postes nomades ainsi que les postes invités.

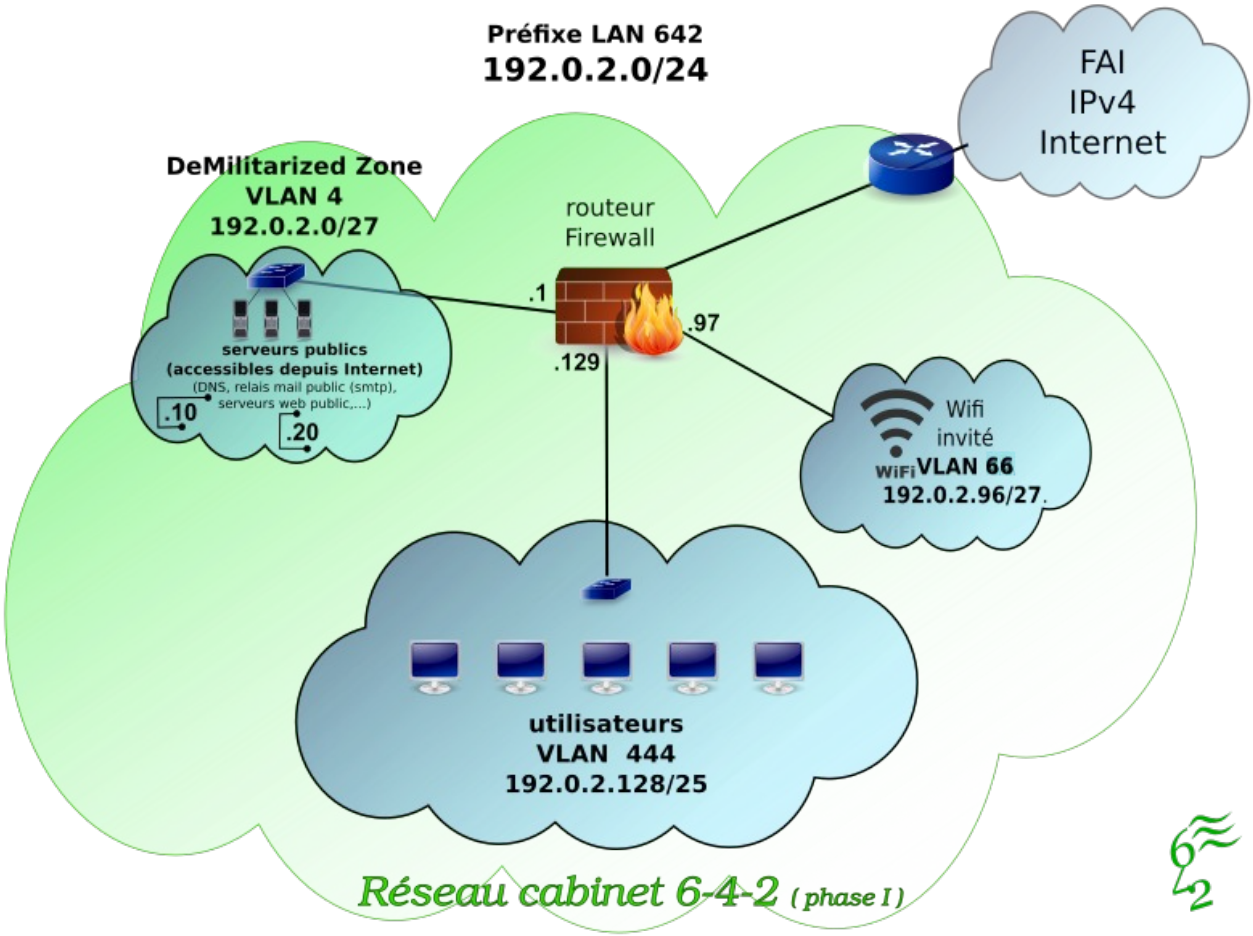


Figure 1 : Ancienne infrastructure du réseau du cabinet 6-4-2.

Pour faire face à sa croissance, le cabinet emménage dans de nouveaux locaux localisés dans une zone d'activité tertiaire localisée à Villeneuve d'Ascq dans les Hauts de France. Le fournisseur d'accès Internet du cabinet 6-4-2 fournit maintenant l'accès natif à IPv6 en plus de l'accès IPv4. Le cabinet prend la décision d'étendre son réseau en intégrant IPv6 pour les nouveaux projets et les postes des nouveaux collaborateurs. Les nouveaux noeuds du réseau seront uniquement IPv6. Seuls les serveurs de la nouvelle DMZ et les relais de cohabitation v4-v6 (DNS64, NAT64) seront configurés en double pile. La figure 2 illustre l'infrastructure du réseau déployé dans les nouveaux locaux.

Après avoir observé l'organisation de l'adressage de cette infrastructure, vous répondrez à

différentes questions relatives aux flux IP en vous appuyant sur les indications de la figure 2.

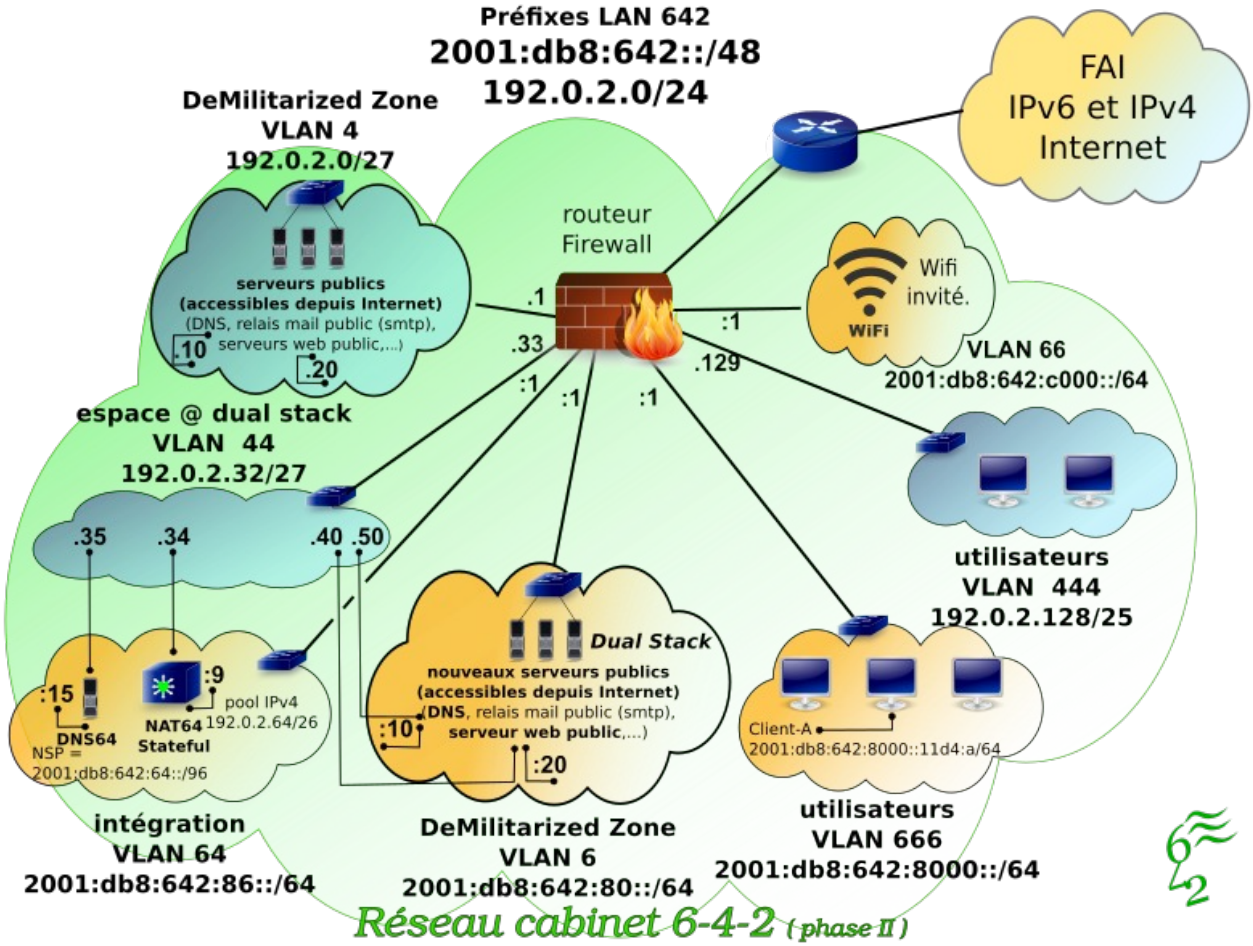
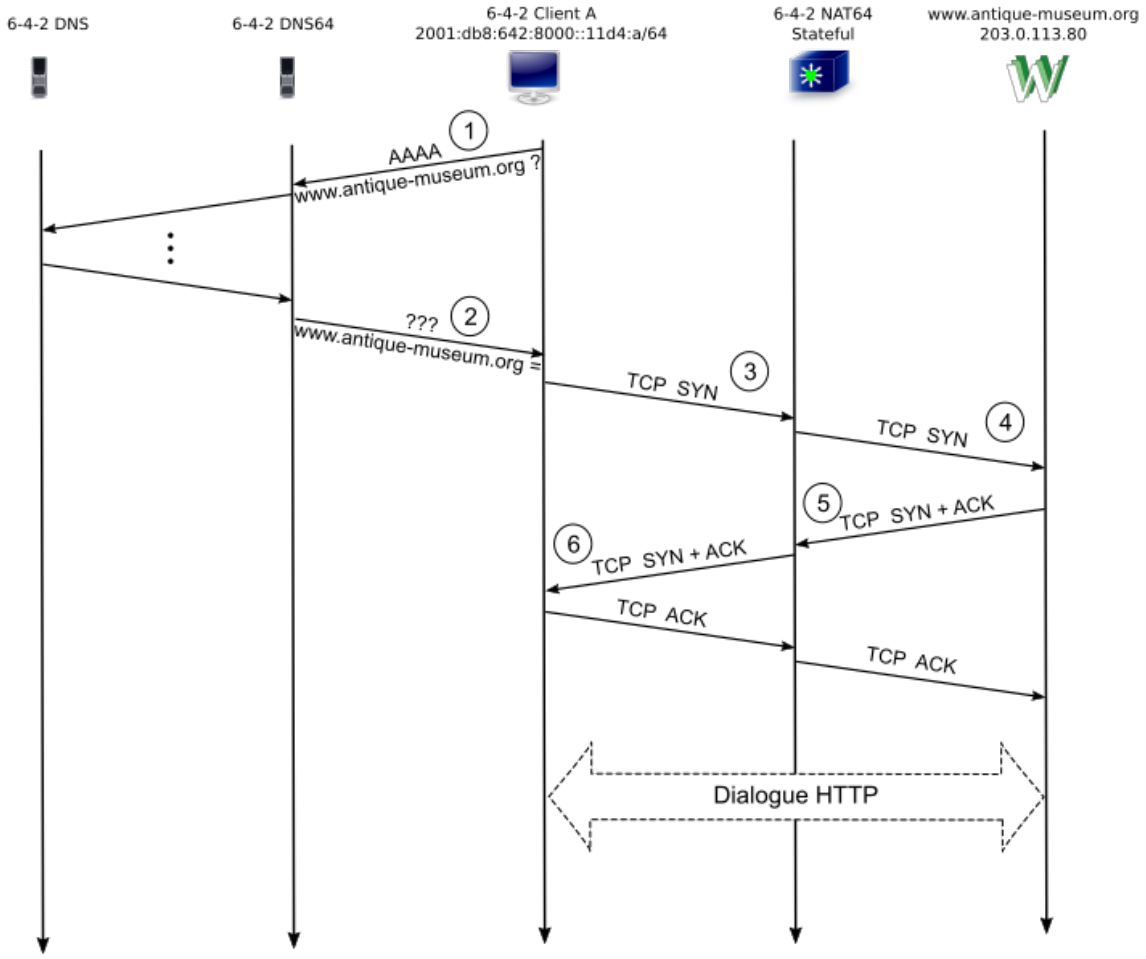


Figure 2 : Infrastructure du réseau du cabinet 6-4-2.

Le chronogramme de la figure 3 décrit les échanges réseau de l'établissement de la connexion TCP (succession des messages SYN, SYN+ACK, ACK) lors de l'ouverture d'une session web entre '"client-A"', du VLAN 666 "utilisateurs" du cabinet 6-4-2, et le serveur web "www.antique-museum.org", localisé sur l'Internet v4.



Question 1 Étape "repère 1" : requête DNS. L'adresse IP de destination du datagramme portant la requête DNS de résolution du nom de domaine "www.antique-museum.org" émis par "client-A" est : (**entourez la bonne réponse**)

192.0.2.34	192.0.2.35	192.0.2.10	203.0.113.80
2001:db8:642:86::9	2001:db8:642:86::15	2001:db8:642:80::10	
2001:db8:642:8000::11d4:a		2001:db8:642:64::c000:223	
2001:db8:642:64::cb00:7150			

Question 2 Étape "repère 2" : Le type du "Resource Record DNS" de la réponse est (**entourez la bonne réponse**)

PTR	A	AAAA	A6
CNMAME	MX	SRV6	
192.0.2.131	2001:db8:642:64::c000:223		

Question 3 Étape "repère 3" : L'adresse destination du datagramme repéré "3" portant le message SYN d'ouverture de connexion TCP est : (**entourez la bonne réponse**)

192.0.2.34 192.0.2.35 192.0.2.10 203.0.113.80

2001:db8:642:86::9 2001:db8:642:86::15 2001:db8:642:80::10

2001:db8:642:8000::11d4:a 2001:db8:642:64::c000:223

2001:db8:642:64::cb00:7150

Question 4 Étape "repère 4" : L'adresse destination du datagramme repéré "4" portant le message SYN d'ouverture de connexion TCP est : (**entourez la bonne réponse**)

192.0.2.34 192.0.2.35 192.0.2.10 203.0.113.80

2001:db8:642:86::9 2001:db8:642:86::15 2001:db8:642:80::10

2001:db8:642:8000::11d4:a 2001:db8:642:64::c000:223

2001:db8:642:64::cb00:7150

Question 5 Étape "repère 5" : "Le préfixe" de l'adresse destination du datagramme repéré "6" portant le message SYN+ACK d'ouverture de connexion TCP est : (**entourez la bonne réponse**)

192.0.2.0/27 192.0.2.32/27 192.0.2.64/26

2001:db8:642:c000::/64 2001:db8:642:8000::/64

2001:db8:642:80::/64 2001:db8:642:64::/64

2001:db8:642:86::/96

Question 6 Étape "repère 6" : "Le préfixe" de l'adresse destination du datagramme repéré "6" portant le message SYN+ACK d'ouverture de connexion TCP est : (**entourez la bonne réponse**)

192.0.2.0/27 192.0.2.32/27 192.0.2.64/26

2001:db8:642:c000::/64 2001:db8:642:8000::/64

2001:db8:642:80::/64 2001:db8:642:64::/64

2001:db8:642:86::/96