

SAE 401: Sécuriser un système d'information

Introduction:	3
Gestion de projet	4
Trello	4
Configuration minimale du firewall	5
Adressage IP du Firewall	5
Routage du Firewall	5
Configuration du switch Cisco	6
Restriction de l'accès au VLAN 101 que pour l'envoi de logs:	7
Configuration IPv4	7
Mise en place du NAT IPv4	8
Configuration IPv6	9
IPv6 Fixe	10
Autoconf	11
Tests	13
Rôle des machines	14
Serveur DMZ	14
Serveur windows 2016	17
Mise en place de l'AD	17
Mise en place du DHCP	18
Mise en place du DNS	19
Mise en place de l'AD CS	20
Mise en place de Radius	21
Station Windows	24
Mise en place de la centralisation de logs	26
Détection de flooding du firewall par le serveur Graylog	29
Inspections SSL	30
Mise en place d'un VPN	33
Filtre IPS	34
Conclusion:	35

Introduction:

Lors de cette SAE, nous allons avoir une trentaine d'heures pour configurer une infrastructure réseau complète et apporter une vision cybersécurité de cette infrastructure par différents moyens étudiés dans cette SAE. Pour cela, nous allons disposer d'une infrastructure réseau déjà mise en place qui prendra la forme du schéma ci-dessous:

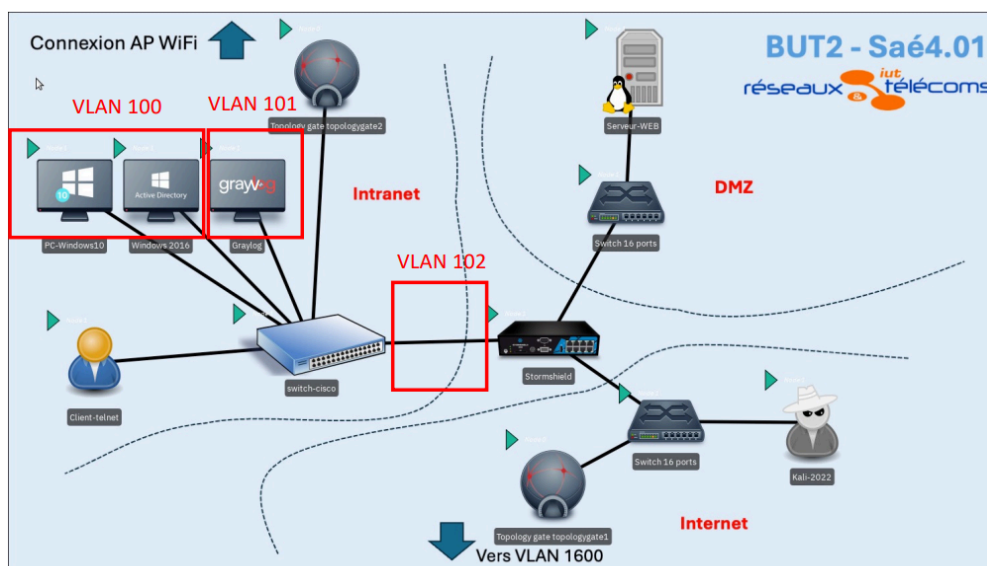


Schéma de l'infrastructure initiale

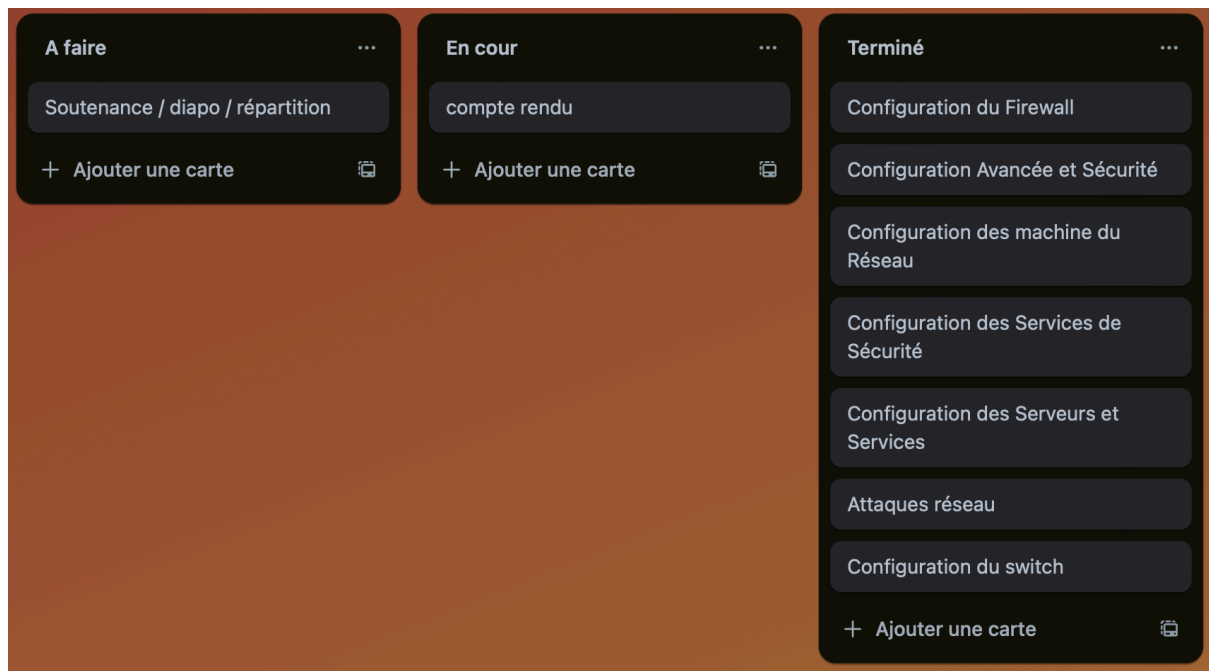
Cette infrastructure dispose d'équipements centraux que sont le firewall Stormshield ainsi qu'un switch Cisco de niveau 3. Cette infrastructure est découpée en 3 par ce firewall en formant l'Intranet, la DMZ et l'Internet. On a dans l'Intranet, tous les serveurs dédiés à l'Intranet tels que le serveur Graylog (Linux), ainsi qu'une Windows serveur 2016 sur laquelle se trouveront l'Active Directory, le DNS, le DHCP et le Radius. Nous disposons aussi d'une Windows cliente pour tester l'accès à tous ces services. Dans la DMZ, nous allons devoir mettre en place un serveur HTTPS qui devra pouvoir être accessible depuis l'Intranet mais aussi depuis l'Internet. Enfin, dans l'Internet, nous pouvons trouver une Kali qui va nous permettre de tester les aspects de sécurité de cette SAE.

La finalité de cette SAE est d'obtenir une infrastructure en double-pile IPv4 et IPv6 complète et qui empêche l'Internet d'accéder à l'Intranet tout en le laissant aller vers la DMZ. Pour cela, nous allons devoir mettre en place une politique de filtrage sur le firewall. Nous allons aussi devoir assurer la remontée de logs et d'alertes du firewall et de la Windows serveur par le serveur Graylog.

Gestion de projet

Trello

Pour maximiser notre efficacité pendant notre SAE, nous avons entamé la liste des tâches à accomplir. Nous avons opté pour l'utilisation de Trello afin de suivre notre progression. Pour ce faire, nous avons structuré les principales composantes de notre SAE afin de mieux comprendre les diverses tâches à réaliser sur chaque machine. Après avoir examiné en détail ces tâches, voici le Trello que nous avons établi :



organisation des tâches avec Trello

Configuration minimale du firewall

Adressage IP du Firewall

Premièrement, nous avons mis en place notre Stormshield. Pour cela, nous avons configuré les adresses IP en respectant le plan d'adressage que nous avons défini précédemment. Pour cela, nous avons directement mis la configuration IP en console du firewall. OUT étant la sortie vers internet, IN pour l'intranet et DMZ comme son nom l'indique vers la DMZ.

```
UINSX0020000A0: FW EVA1 (XL / EUROPE)
Firewall software version 4.3.16 UM-RELEASE

port      name      NS-BSD    state    addressIPv4
  1        out       em0       up       172.16.0.104/16
  2        in        em1       up       192.168.102.254/24
  3        dmz1      em2       up       192.168.103.254/24
```

Configuration IP du firewall

Routage du Firewall

Dans l'onglet Réseau → Routage → Routage statiques IPv4, nous allons d'abord définir la route par défaut correspondant à l'adresse IP du routeur de l'IUT. Ensuite, nous mettrons en place les routes vers les deux VLANs dans le but de permettre la connexion aux équipements dans ces VLANs. Il est à noter que le serveur DMZ ne nécessite pas de route par défaut, car la passerelle du serveur DMZ est déjà le firewall, contrairement aux serveurs Graylog et Windows où la passerelle est l'interface de leur VLAN sur le commutateur.

General

Default gateway (router):

Configuration de la route du firewall vers internet avec l'objet gateway

STATIC ROUTES

Status	Destination network (host, ne...	Interface	Address range	Gateway	Comments
on	Vlan_101	in	192.168.101.0/24	int_vlan_102	
on	Vlan_100	in	192.168.100.0/24	int_vlan_102	

Configuration de la route du firewall vers l'intranet avec les objets vlan 100/101

La configuration des routes est configurée en premier pour accéder au firewall depuis l'intranet.

Configuration du switch Cisco

Chaque interface de vlan à l'adresse 192.168.nb vlan.253 hormis le vlan 900 qui permet la connexion telnet, les vlans ont également une adresse IPv6. Nous avons mis en place une route sur notre Switch, afin qu'il puisse joindre le Firewall pour qu'il puisse avoir accès à la DMZ et/ou à Internet.

Pour ce faire, nous avons ajouté la route en ipv4 et ipv6 ainsi qu'une IP à chaque interface et le mode access pour chaque interface correspondant au vlan. :

```
interface GigabitEthernet0/2
 switchport access vlan 101
 switchport mode access
 media-type rj45
 negotiation auto
!
interface GigabitEthernet0/3
 switchport access vlan 100
 switchport mode access
 media-type rj45
 negotiation auto
!
interface GigabitEthernet1/0
 switchport access vlan 100
 switchport mode access
 media-type rj45
 negotiation auto
!
```

Configuration des interfaces du switch

```
interface Vlan100
 ip address 192.168.100.253 255.255.255.0
 ipv6 address 2001:470:C8F2:104::253/64
!
interface Vlan101
 ip address 192.168.101.253 255.255.255.0
 ipv6 address 2001:470:C8F2:204::253/64
!
interface Vlan102
 ip address 192.168.102.253 255.255.255.0
 ipv6 address 2001:470:C8F2:304::253/64
!
interface Vlan900
 ip address 10.1.1.2 255.255.255.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.102.254
```

Configuration des interfaces des vlans et les routes

Restriction de l'accès au VLAN 101 que pour l'envoi de logs:

Ensuite, on nous a demandé d'accéder au VLAN 101 que pour l'envoi de logs, pour cela, nous mettons en place des access-list comme ceci:

```
interface Vlan101
ip address 192.168.101.253 255.255.255.0
ip access-group logs in
!
interface Vlan102
ip address 192.168.102.253 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.102.254
ip http server
ip http secure-server
!
!
ip access-list extended logs
permit tcp host 192.168.100.2 host 192.168.101.1 eq 6000
permit udp host 192.168.102.254 host 192.168.101.1 eq 7000
deny ip any any
```

ACLs

Ces ACLs permettent au firewall d'envoyer ses logs udp au serveur graylog sur le port 7000 et au windows serveur d'envoyer les siens sur le port 6000 en tcp.

Configuration IPv4

Pour la configuration IPv4, nous avons commencé par mettre en place toutes les adresses IP sur les équipements terminaux. Pour cela, nous avons écrit ces adresses dans le fichier de configuration ainsi que la gateway qui est l'interface du vlan dans le switch et le DNS.

```
iface enp0s3 inet static
address 192.168.103.1
netmask 255.255.255.0
gateway 192.168.103.254
dns-nameservers 192.168.100.2
iface enp0s3 inet6 static
address 2001:470:c8f2:304::1
netmask 64
gateway 2001:470:c8f2:304::254
dns-nameservers 2001:470:c8f2:104::2
```

Mise en place de la configuration IP dans les fichiers de configuration

Pour la configuration des équipements, nous avons d'abord configuré le switch de l'intranet. Pour ce switch, nous avons mis en place tous les vlans nécessaires, mis en place les ip pour chaque interface vlan et le routage inter vlan.

Mise en place du NAT IPv4

Le NAT a été créé dans un premier temps pour accéder à internet et à accéder au site web de la DMZ depuis internet. Les ports seront configurés plus tard. Le NAT translate l'adresse source par l'adresse publique de notre firewall. Nous créons également un NAT pour accéder au site de la dmz. Celui-ci est uniquement mis en place pour accéder au site web depuis l'internet. Pour cela nous allons nous rendre dans l'onglet de l'interface de configuration du firewall Politique de filtrage → Filtrage et NAT → NAT IPv4 et définir les translations suivantes.

FILTERING

IPv4 NAT

Searching...

+ New rule

✕ Delete

↑

↓

↕

↕

✂ Cut

📄 Copy

📄 Paste

🔍 Search in logs

☰

			Sta...	Original traffic (before translation)			Traffic after translation				Protocol
				Source	Destination	Dest. port	Source	Src. port	Destination	Dest. port	
1	<div></div>	<div></div>	<div></div> on	<div></div> Vlan_101	<div></div> Internet interface: out	<div></div> Any	➡	<div></div> Firewall_out		<div></div> Any	
2	<div></div>	<div></div>	<div></div> on	<div></div> Vlan_100	<div></div> Internet interface: out	<div></div> Any	➡	<div></div> Firewall_out		<div></div> Any	
3	<div></div>	<div></div>	<div></div> on	<div></div> serv_dmz	<div></div> Any interface: out	<div></div> Any	➡	<div></div> <div></div> serv_dm			
4	<div></div>	<div></div>	<div></div> on	<div></div> Any interface: out	<div></div> <div></div> serv_c	<div></div> https	➡			<div></div> serv_dmz	

Mise en place du NAT sur le firewall

Pour l'IPv6, il n'y a pas de NAT car il n'existe pas de notion d'adresse publique/privée. Nous n'avons pas mis de NAT pour le vlan 102 puisqu'aucun terminal se trouvant dedans n'a besoin d'aller sur internet.

Configuration IPv6

Dans le contexte actuel de manque d'adresse IPv4 au niveau mondial, nous devons aussi penser à l'avenir en maîtrisant la configuration d'IPv6.

Pour cela, nous devons tout d'abord activer IPv6 sur le firewall en se rendant dans l'espace Système/Configuration et en enclenchant l'interrupteur IPv6.

SYSTÈME / CONFIGURATION

CONFIGURATION GÉNÉRALE ADMINISTRATION DU FIREWALL **PARAMÈTRES RÉSEAUX**

Support IPv6

Le support du protocole IPv6 est activé sur ce Firewall.

Après l'avoir activé, l'interrupteur disparaît l'IPv6 est alors activé.

Nous pouvons alors compléter la configuration IPv4 déjà effectuée en ajoutant une IPv6 à tous les objets créés sur le firewall.

RÉSEAU / INTERFACES

Interface	P...	Type	État	Adresse I...	Adresse IPv6
out		1 Ethernet, ...		172.16.0...	2001:470:c8f2:1::104/64
in		2 Ethernet, ...		192.168.1...	2001:470:c8f2:304::254/64
dmz1		3 Ethernet, ...		192.168.1...	2001:470:c8f2:404::254/64

Nous ajoutons ainsi une IPv6 à toutes les interfaces du firewall dans l'onglet Interfaces.

Nous devons aussi comme pour IPv4 donner un routeur par défaut au firewall ainsi que les routes par défaut vers les différents VLAN de l'intranet.

RÉSEAU / ROUTAGE

< ROUTES STATIQUES IPV4 **ROUTES STATIQUES IPV6** ROUTAGE DYNAMIQUE ROUTAGE DYNAMIQUE

Configuration générale

Passerelle par défaut (routeur):

ROUTES STATIQUES

État	Réseau de destination...	Interface	Plan d'adressage	Passerelle	Cc
on	Vlan_101	in	2001:470:c8f2:204::/64	int_vlan_102	
on	Vlan_100	in	2001:470:c8f2:104::/64	int_vlan_102	

Création des routes par défaut vers les VLANs de l'Intranet.

Romain Noel, Marius Beauchêne, Mathieu Caudan

Sur le commutateur de niveau 3, nous apposons des IPv6 aux différents VLAN, ces interfaces VLAN seront vues depuis les machines comme leur routeur par défaut selon le VLAN auxquelles elles appartiennent. On ajoute aussi une route par défaut pour toutes les adresses que ce switch ne connaît pas vers l'interface entrante du firewall. Pour cela, nous tapons la commande:

ipv6 route ::/0 2001:470:c8f2:304::254

```
!
interface Vlan100
 ip address 192.168.100.253 255.255.255.0
 ipv6 address 2001:470:C8F2:104::253/64
!
interface Vlan101
 ip address 192.168.101.253 255.255.255.0
 ipv6 address 2001:470:C8F2:204::253/64
!
interface Vlan102
 ip address 192.168.102.253 255.255.255.0
 ipv6 address 2001:470:C8F2:304::253/64
!
interface Vlan900
 ip address 10.1.1.2 255.255.255.0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.102.254
!
!
ipv6 route ::/0 2001:470:C8F2:304::254
!
```

Ajout des adresses sur les interfaces VLANs ainsi que la route par défaut.

Nous allons maintenant voir comment configurer l'IPv6 sur les stations clientes de différentes manières et sur différents OS.

IPv6 Fixe

Pour commencer, nous allons voir comment configurer manuellement notre adresse IPv6 sur Linux et sur Windows.

Linux:

Pour Linux, il faut comme souvent passer par le terminal, sur celui-ci, nous devons ajouter une adresse IPv6 ainsi que la traduction IPv6 du routeur.

Pour cela, nous nous plaçons en root et nous tapons la commande ci-dessous.

```
root@graylog:~# ip -6 route add default via 2001:470:c8f2:204::253 dev ens3
RTNETLINK answers: File exists
root@graylog:~# ip -6 route
::1 dev lo proto kernel metric 256 pref medium
2001:470:c8f2:204::/64 dev ens3 proto ra metric 100 pref medium
fe80::/64 dev ens3 proto kernel metric 100 pref medium
default via fe80::201:fcff:fe5a:8065 dev ens3 proto ra metric 100 pref medium
default via 2001:470:c8f2:204::253 dev ens3 metric 1024 pref medium
```

Attribution de la route IPv6

Romain Noel, Marius Beauchêne, Mathieu Caudan

Ajout du routeur IPv6 sur la station Linux.

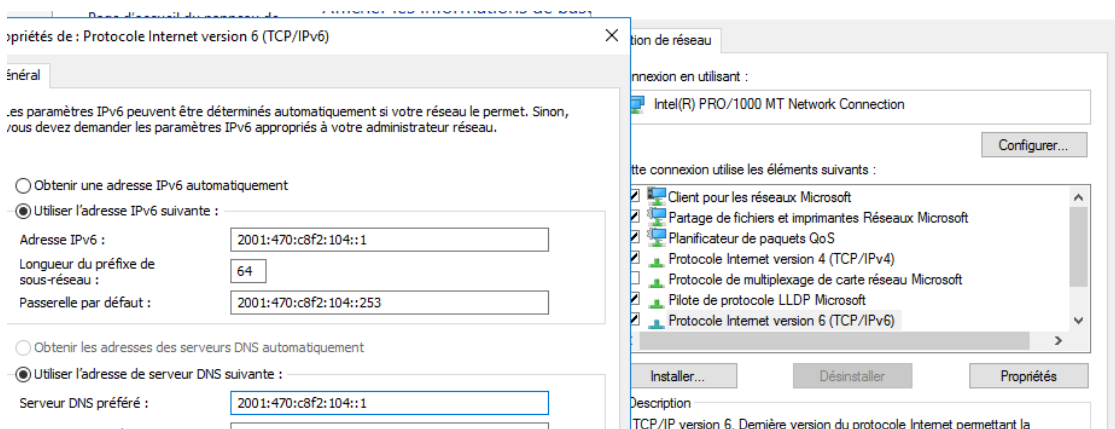
Nous testons ensuite le fonctionnement de la commande en vérifiant que l'entrée du routeur est bien présente.

```
root@graylog:/etc/network# ip -6 addr add 2001:470:c8f2:204::1/64 dev ens3
root@graylog:/etc/network# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether ec:5c:69:5f:80:4e brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    inet6 2001:470:c8f2:204::1/64 scope global
        valid_lft forever preferred_lft forever
    inet6 2001:470:c8f2:204:1f2e:36e0:8c88:blea/64 scope global temporary dynamic
```

Attribution d'une IPv6 fixe

Ensuite pour l'IP du PC, nous tapons la commande ci-dessus et nous vérifions aussi son fonctionnement.

Windows



Attribution d'une IPv6 fixe sur Windows

Du côté de Windows, nous avons choisi de faire notre configuration par l'interface graphique. Dans les propriétés de connexion, nous choisissons IPv6 et nous rentrons notre IP ainsi que notre routeur et DNS.

Autoconf

Un autre avantage d'IPv6 est l'autoconfiguration d'IPv6, propriété que nous allons utiliser dans cette partie.

Linux

Sur Linux, cette auto-configuration est automatique dès que l'on possède un routeur par défaut. Le PC utilise alors le préfixe du routeur et le complète de différentes manières: aléatoires, MAC, lien-local. S'il n'est pas activé par défaut, on peut tout simplement se rendre dans le fichier `/etc/network/interfaces` et ajouter la ligne suivante. Nous avons toujours besoin d'un routeur pour obtenir le préfixe de sous-réseau.

```
GNU nano 7.2 /etc/network/interfaces
# This file describes the network interfaces available on your
# and how to activate them. For more information, see interfac

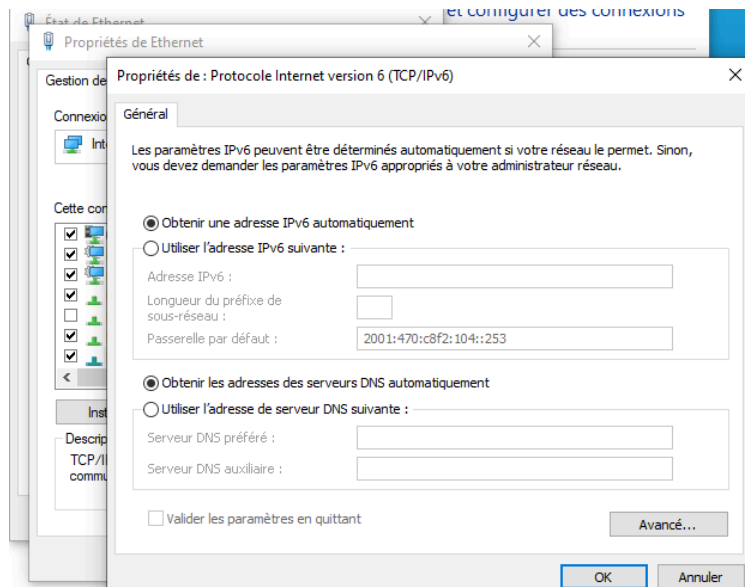
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

allow-hotplug ens3
iface ens3 inet static
    address 172.16.1.104
    netmask 255.255.0.0
    gateway 172.16.255.254
    dns-nameservers 8.8.8.8
iface ens3 inet6 auto
```

IPv6 fixe

Windows:



IPv6 auto sur Windows

Tests

```
C:\Users\user>ping -6 2001:470:c8f2:1::254

Envoi d'une requête 'Ping' 2001:470:c8f2:1::254 avec 32 octets de données :
Réponse de 2001:470:c8f2:1::254 : temps=4 ms
Réponse de 2001:470:c8f2:1::254 : temps=3 ms
Réponse de 2001:470:c8f2:1::254 : temps=6 ms
Réponse de 2001:470:c8f2:1::254 : temps=3 ms

Statistiques Ping pour 2001:470:c8f2:1::254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 3ms, Maximum = 6ms, Moyenne = 4ms
```

Ping concluant vers l'Internet depuis la Windows cliente

```
root@graylog:/home/user# ping6 2001:470:c8f2:1::254
PING 2001:470:c8f2:1::254(2001:470:c8f2:1::254) 56 data bytes
64 bytes from 2001:470:c8f2:1::254: icmp_seq=1 ttl=63 time=3.83 ms
64 bytes from 2001:470:c8f2:1::254: icmp_seq=2 ttl=63 time=4.40 ms
64 bytes from 2001:470:c8f2:1::254: icmp_seq=3 ttl=63 time=4.56 ms
64 bytes from 2001:470:c8f2:1::254: icmp_seq=4 ttl=63 time=5.04 ms
^Z
[27]+  Stoppeé                  ping6 2001:470:c8f2:1::254
```

Ping concluant Graylog→Internet

Finalement après cette configuration d'IPv6, nous possédons une configuration IP complète en IPv4 et IPv6 qui nous permet de joindre tout équipement à l'aide des 2 protocoles. Il nous reste cependant à configurer les serveurs en IPv6 tels que le DNS, le DHCP et le serveur web.

Rôle des machines

Serveur DMZ

Le serveur DMZ est uniquement un serveur qui héberge une page web et doit être disponible depuis internet et l'intranet. Pour ce faire, il faut créer des certificats, le premier qui est une autorité de certification qui va signer les certificat serveur. Ce certificat va être ajouté dans les navigateur à la mains pour simuler le fait que notre certificat ait été signée par une vraie autorité.

```
root@crypto:/etc/certgen# ls
01.pem      ca.csr      conf        dmz.key     index.txt.attr  serial
CA.create   ca.key      dmz.crt     ext         index.txt.old   serial.old
ca.crt      CLIENT.create dmz.csr     index.txt   PURGE           SERVER.create
```

Création des certificats

Pour éviter les alarmes liées aux certificats sur les sites, on a créé une autorité de certification qui a permis de signer notre certificat dmz

Pour améliorer la sécurité, nous avons mis en place ufw permettant le blocage de tous les ports hormis le 443 celui qui permet la connexion HTTPS depuis l'internet. De plus, il fallait qu'apache ne retourne plus son numéro de version. Cela est possible en modifiant le fichier security.conf. Les deux lignes suivantes sont à modifier, ServerTokens qui sert à masquer les informations spécifiques sur la version d'Apache, ne montrant que "Apache" dans l'en-tête de réponse et ServerSignature qui permet de désactiver l'affichage de la signature du serveur dans les pages d'erreur, réduisant ainsi la quantité d'informations divulguées aux utilisateurs.

```
ServerTokens Prod
#ServerTokens Full

#
# Optionally add a line
# name to server-generated
# listings, mod_status
# documents or custom e
# Set to "EMail" to als
# Set to one of: On |
ServerSignature Off
#ServerSignature On
```

Configuration du fichier security d'apache

```

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-21 15:35 CET
Nmap scan report for 172.16.2.105
Host is up (0.0029s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
443/tcp   open  ssl/http Apache httpd
|_ssl-date: TLS randomness does not represent time
|_ssl-cert: Subject: commonName=www.local.lan/organizationName=IUT/stateOrProvinceName=Bretagne/countryName=FR
|_Subject Alternative Name: DNS:client.local.lan, DNS:server.local.lan, DNS:www.local.lan
|_Not valid before: 2024-03-21T13:29:50
|_Not valid after:  2025-03-21T13:29:50
|_http-title: Apache2 Debian Default Page: It works
|_http-server-header: Apache

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.03 seconds
    
```

nmap d'une kali sur le réseau 192.168.103.0/24

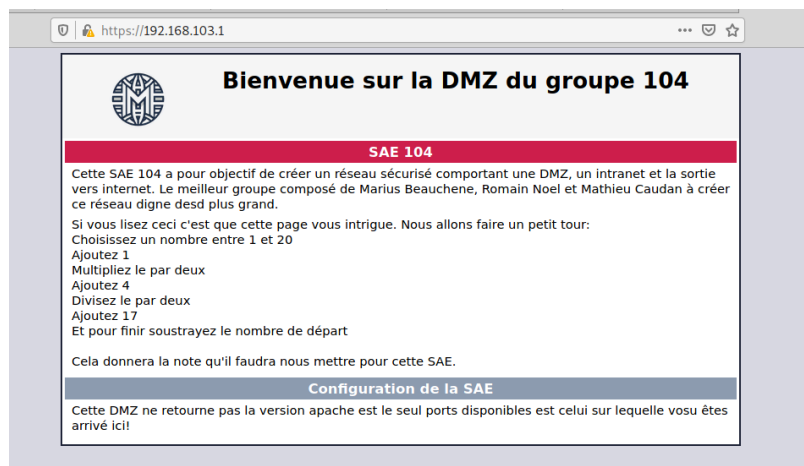
Grâce à la Kali mis sur le réseau, nous avons pu nmap la DMZ et vérifier qu'il n'y a que le port 443 d'ouvert et qu'Apache ne retourne pas le numéro de version.

```

SSLEngine on
SSLCertificateFile /etc/certgen/dmz.crt
SSLCertificateKeyFile /etc/certgen/dmz.key
SSLCACertificateFile /etc/certgen/ca.crt
    
```

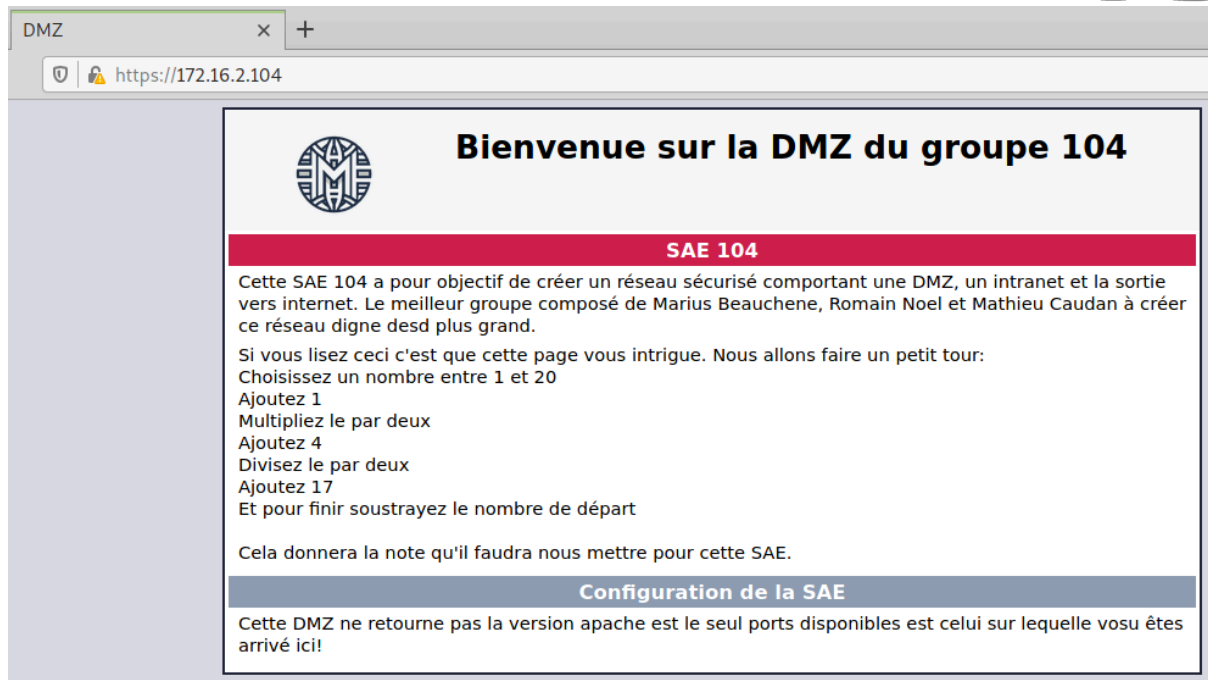
Configuration HTTPS

Pour pouvoir être en https, il faut configurer la fichier de configuration en ajoutant les deux certificats et la clé.



Site de la dmz depuis l'intranet

Romain Noel, Marius Beauchêne, Mathieu Caudan



Site de la dmz depuis l'internet

Serveur windows 2016

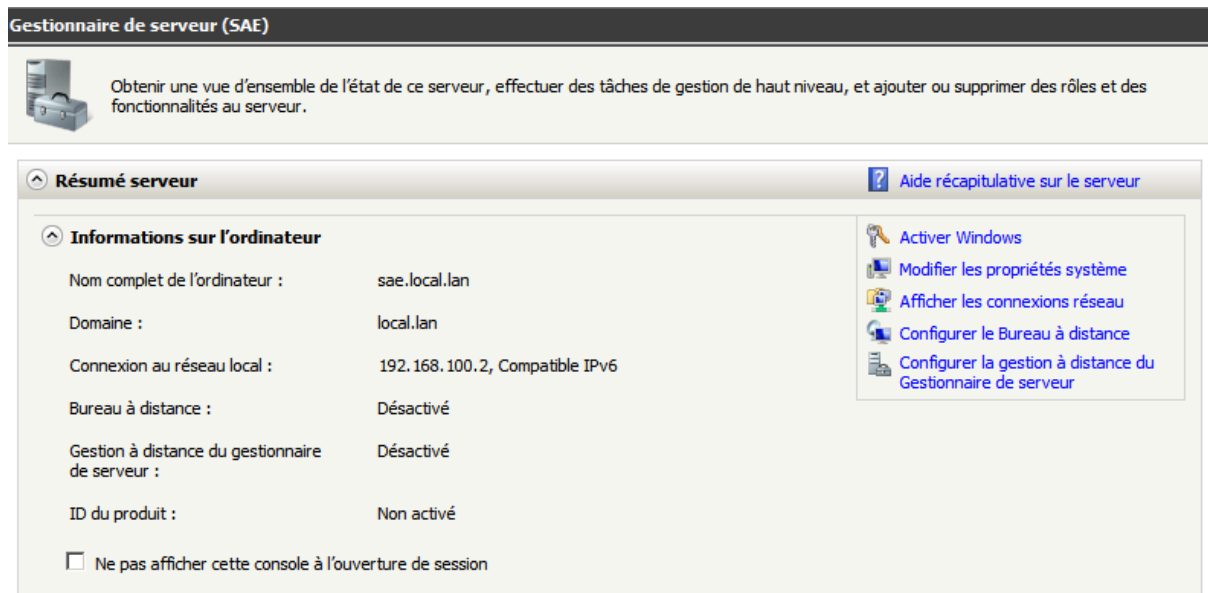
Mise en place de l'AD

Pour configurer Windows 2016, nous avons dû mettre en place un AD Windows.

Un Active Directory (AD) est une solution de gestion d'annuaire qui centralise la gestion des ressources informatiques telles que les utilisateurs, les groupes, les ordinateurs et les applications. Il permet de créer une structure d'arborescence hiérarchique de domaines, où chaque domaine peut établir des relations de confiance avec d'autres domaines. Les objets sont organisés en unités d'organisation, ce qui facilite la délégation des autorisations de gestion aux administrateurs locaux.

Les services AD représentent une architecture géographique de l'annuaire, permettant de regrouper les utilisateurs par entité physique.

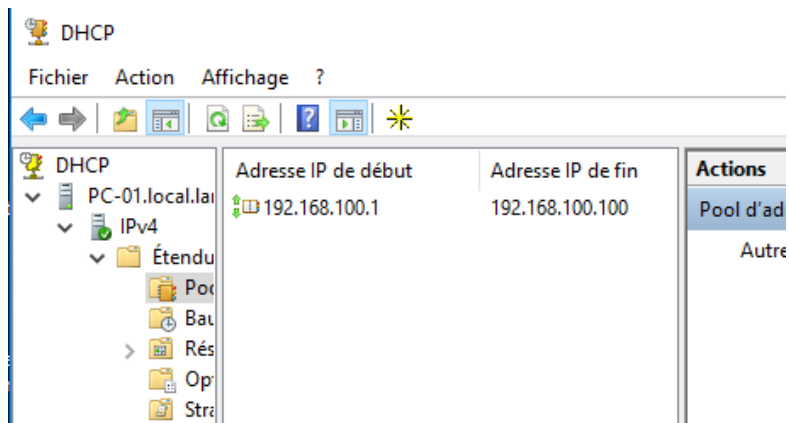
Pour configurer le service AD, nous avons dû accéder au Gestionnaire de serveur et ajouter un rôle. Ensuite, nous avons sélectionné les Services AD DS dans la liste des rôles de serveurs. Une fois cela fait, une notification est apparue dans le Gestionnaire de serveur nous indiquant de promouvoir ce serveur en tant que contrôleur de domaine et d'ajouter une nouvelle forêt. Enfin, nous avons pu vérifier que le serveur est membre du domaine.



Mise en place de l'AD

Mise en place du DHCP

Par la suite nous allons dans l'AD mettre les services dont nous avons besoin pour commencer le DHCP. On va venir renseigner les plages d'adresse IP pour que les prochains pc se connectant à l'AD obtiennent une adresse entre la plage d'@ 192.168.100.1 / 192.168.100.100.



mise en place des plages d'adresses

Mise en place du DNS

Ensuite, nous procéderons à la configuration d'un serveur DNS. Nous installerons un DNS pour la DMZ ainsi que pour l'AD, permettant ainsi la connexion à celui de l'IUT. De plus, nous mettrons en place un DNS pour les résolutions en IPv6, étant donné que notre infrastructure prend en charge à la fois l'IPv4 et l'IPv6. Nous établirons également des zones de recherche inversée pour les adresses IP, nous permettant ainsi de récupérer les informations dans le sens inverse lors de l'utilisation de la commande dig (de l'URL vers l'adresse IP).

DNS	Nom	Type	Données	Horodateur
PC-01.local.lan	_msdcs			
Zones de recherche directes	_sites			
_msdcslan	_tcp			
local.lan	_udp			
Zones de recherche inversées	DomainDnsZones			
100.168.192.in-addr.arpa	ForestDnsZones			
Points d'approbation	(identique au dossier parent)	Source de nom (SOA)	[61], pc-01.local.lan., host...	statique
Redirecteurs conditionnels	(identique au dossier parent)	Serveur de noms (NS)	pc-01.local.lan.	statique
	(identique au dossier parent)	Hôte (A)	192.168.100.2	21/03/2024 10:00:00
	(identique au dossier parent)	Hôte IPv6 (AAAA)	2001:0470:c8f2:0104:0000:0...	21/03/2024 10:00:00
	(identique au dossier parent)	Hôte IPv6 (AAAA)	2001:0470:c8f2:0104:b05d:...	21/03/2024 10:00:00
	dmz	Hôte (A)	192.168.103.1	statique
	dmz	Hôte IPv6 (AAAA)	2001:0470:c8f2:0104:0000:0...	statique
	pc-01	Hôte (A)	192.168.100.2	statique
	pc-01	Hôte IPv6 (AAAA)	2001:0470:c8f2:0104:0000:0...	statique

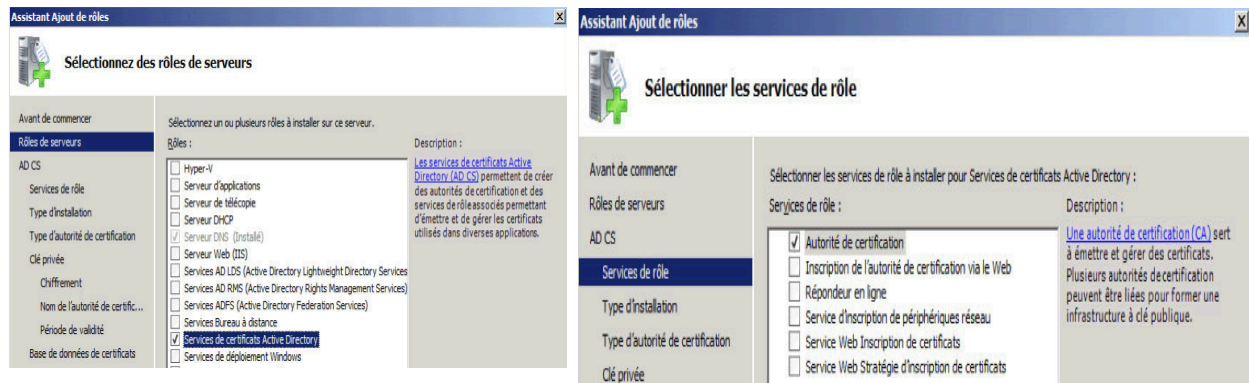
Mise en place des DNS IPv4 et IPv6

Gestionnaire DNS				
Fichier Action Affichage ?				
DNS	Nom	Type	Données	Horodateur
PC-01.local.lan	(identique au dossier parent)	Source de nom (SOA)	[25], pc-01.local.lan., host...	statique
Zones de recherche directes	(identique au dossier parent)	Serveur de noms (NS)	pc-01.local.lan.	statique
_msdcslan	192.168.100.2	Pointeur (PTR)	PC-01.local.lan.	27/03/2024 15:00:00
local.lan				
Zones de recherche inversées				
100.168.192.in-addr.arpa				
Points d'approbation				
Redirecteurs conditionnels				

Mise en place de la zones de recherche inversée

Mise en place de l'AD CS

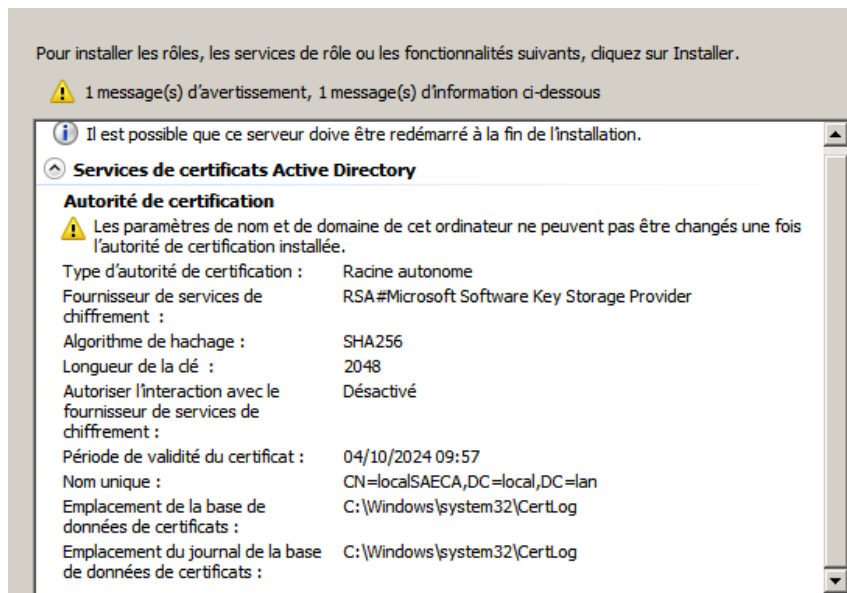
Pour finir, nous allons mettre un certificat afin de nous connecter via un certificat à notre domaine. Pour ce faire, nous allons ajouter un nouveau rôle AD CS.



Mise en place du services AD CS

Nous suivons l'installation étape par étape nous renseignons alors le type Autorité de certification (autonome) et de type racine pour que ce soit le principal. Et on va pouvoir créer une nouvelle clé privée.

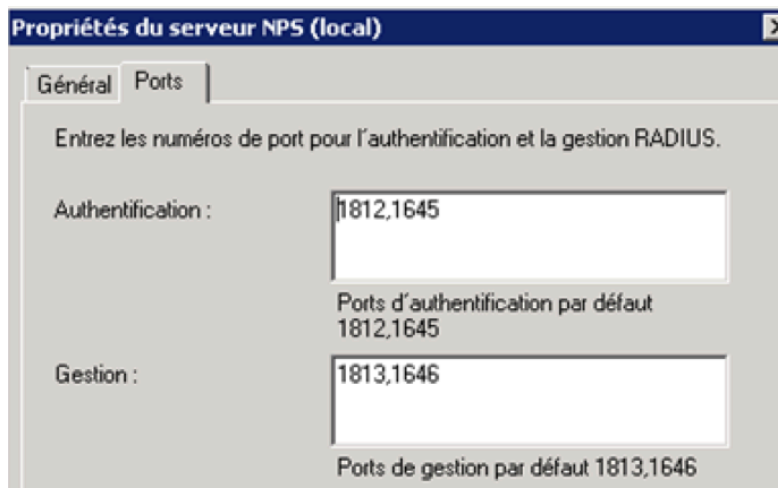
Pour la suite, on va renseigner le chiffrement que nous allons utiliser afin de générer la clé privée. Pour la période du certificat on va mettre celle utilisée dans le monde des réseaux, on va renseigner alors 6 mois puis le certificat sera expiré.



configuration de l'AD CS

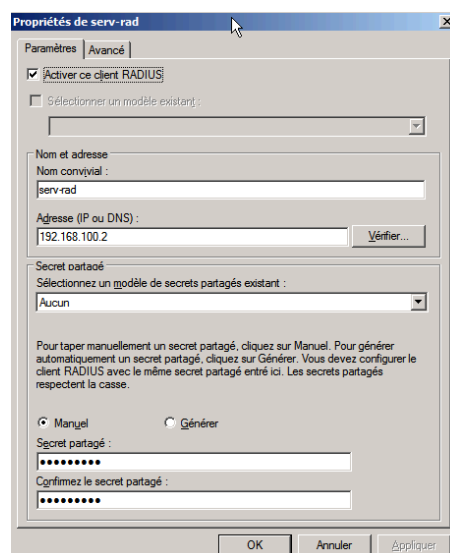
Mise en place de Radius

Nous allons maintenant installer Radius sur notre serveur Windows. Pour ce faire, nous ajouterons le rôle Service de stratégie et d'accès réseau. Après l'installation du rôle, nous pourrons identifier les ports par défaut pour l'authentification et la gestion des connexions à notre service Radius.



Port par défaut

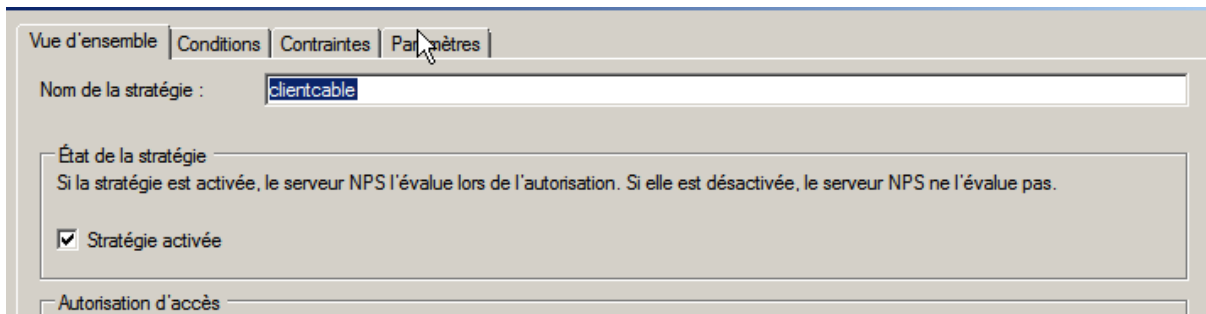
On va déclarer notre client Radius. Dans notre cas, le commutateur est compatible 802.1x. Les éléments à renseigner sont : le nom "convivial" du client-RADIUS, son adresse IP et la chaîne de caractères du "secret partagé" entre le serveur RADIUS et le client RADIUS



Propriété du serveur radius

Nous déclarons une stratégie de demande de connexion pour Ethernet, qui correspond à la connexion physique au serveur. Nous choisissons un nom pour cette stratégie et laissons le type de serveur sur "Unspecified". Nous spécifions ensuite un type de port NAS. Étant donné que toute notre configuration est basée sur une connexion par câble, nous sélectionnons le type de tunnel pour la connexion 802.1x, qui est en Ethernet.

Ensuite, nous déclarons une stratégie réseau. Nous souhaitons mettre en place une stratégie de placement dynamique dans le VLAN 100 pour les membres du groupe d'utilisateurs "Radius.fr". Le commutateur client-RADIUS se chargera lui-même du placement dans un VLAN "guest" des utilisateurs non authentifiés.



Vue d'ensemble | Conditions | Contraintes | Paramètres

Nom de la stratégie : clientcable

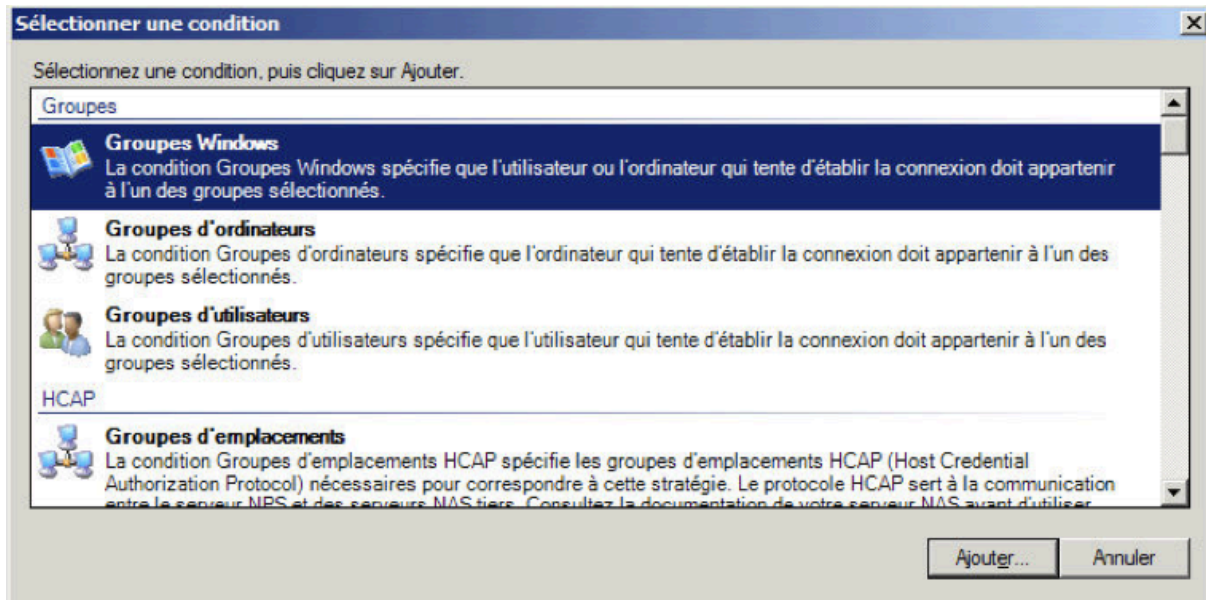
État de la stratégie
Si la stratégie est activée, le serveur NPS l'évalue lors de l'autorisation. Si elle est désactivée, le serveur NPS ne l'évalue pas.

☒ Stratégie activée

Autorisation d'accès

nom de la stratégie mit en place

On ajoute une condition à la validation de la stratégie : que l'utilisateur soit membre d'un groupe AD qui s'appelle "Radius.fr". Pour les membres de ce groupe, on accorde l'accès.



Sélectionner une condition

Sélectionnez une condition, puis cliquez sur Ajouter.

Groupes

- Groupes Windows**
La condition Groupes Windows spécifie que l'utilisateur ou l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.
- Groupes d'ordinateurs**
La condition Groupes d'ordinateurs spécifie que l'ordinateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.
- Groupes d'utilisateurs**
La condition Groupes d'utilisateurs spécifie que l'utilisateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.
- HCAP**
Groupes d'emplacements
La condition Groupes d'emplacements HCAP spécifie les groupes d'emplacements HCAP (Host Credential Authorization Protocol) nécessaires pour correspondre à cette stratégie. Le protocole HCAP sert à la communication entre le serveur NPS et des serveurs NAS tiers. Consultez la documentation de votre serveur NAS avant d'utiliser.

Ajouter... Annuler

mise en place de l'authentification avec la condition d'être dans le groupe radius.fr

On déclare ensuite le type de protocole(PEAP) puis on va venir le type de port NAS en Ethernet.

Pour finir on va ajouter des attributs afin de contrôler le trafic que nous allons avoir.

Attributs :

Nom	Valeur
Framed-Protocol	PPP
Service-Type	Framed
Tunnel-Type	Virtual LANs (VLAN)
Tunnel-Medium-Type	802 (includes all 802 media plus Ethernet canonical for...
Tunnel-Pvt-Group-ID	100

Attribut mit en place

L'installation de notre serveur Windows 2008 est terminée. Nous allons maintenant ajouter les différentes machines à notre réseau. Avant de conclure, nous devons activer le protocole 802.1x sur notre commutateur, car notre serveur Radius est sur notre réseau. Pour ce faire, nous allons exécuter les commandes suivantes :

```
SW-104(config)#aaa new-model
SW-104(config)#aaa authentication dot1x default group radius
SW-104(config)#dot1x system-auth-control
SW-104(config)#radius-server host 192.168.100.2 auth-port 1812 key bonjour
```

activation du contrôle 802.1x

On va attribuer le protocole au port 3 de notre switch. Le port 3 a le VLAN 100 et nous lui attribuons le protocole :

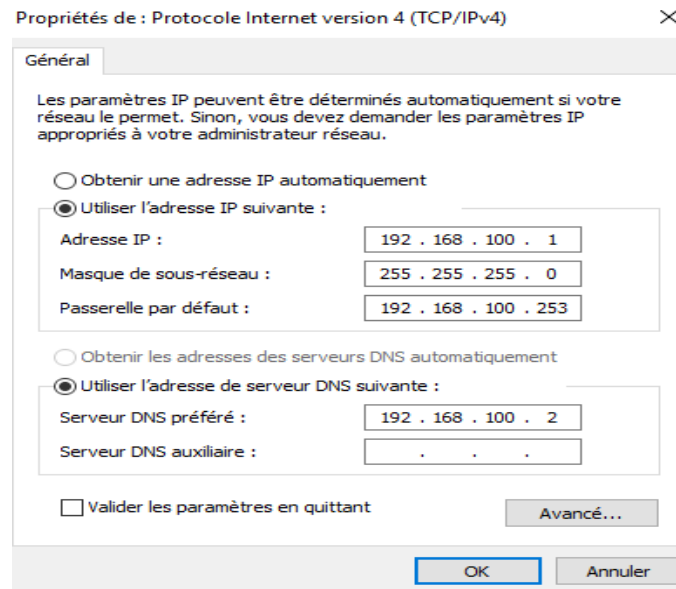
```
interface FastEthernet0/3
 switchport access vlan 100
 switchport mode access
 switchport nonegotiate
 dot1x pae authenticator
```

attribution du protocole au port FA0/3

La configuration de Windows 2008 est terminée. On va maintenant pouvoir configurer notre Windows 10.

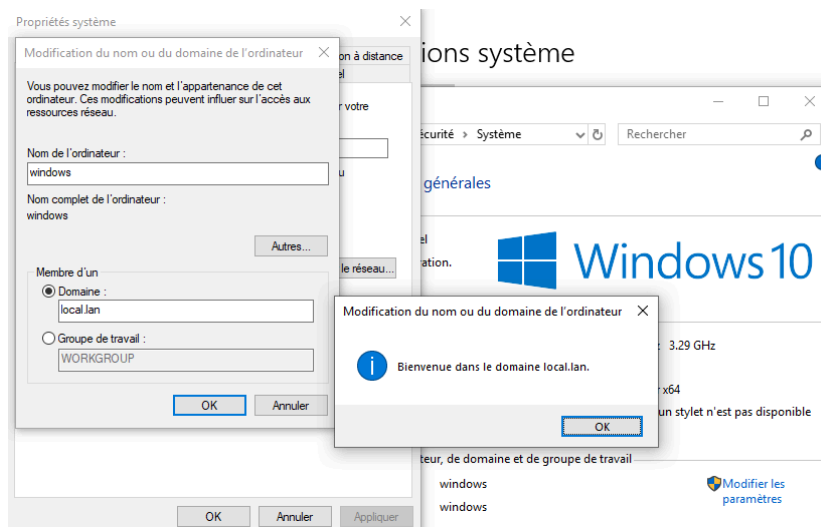
Station Windows

Pour commencer nous attribuons l'adresse IP, la passerelle par défaut ainsi que le DNS à notre machine Windows. Cela va nous servir à se connecter au domaine que nous avons mis en place lors de la configuration de windows serveur.



Adressage de la machine Windows 10

Pour continuer on va se rendre dans les propriétés système afin de pouvoir joindre notre machine windows à notre domaine. Pour se faire on va dans modifier puis on arrive sur la page "modification du nom ou du domaine de l'ordinateur". Nous allons maintenant renseigner le domaine que l'on veut joindre, nous lui donnons alors notre domaine local.lan. On nous demande par la suite de renseigner le nom de l'utilisateur ainsi que son mot de passe. Après avoir entré les différents champs, nous avons un message indiquant que notre ordinateur est dans le domaine local.lan.



connexion au domaine local.lan

Romain Noel, Marius Beauchêne, Mathieu Caudan

On va maintenant vérifier que notre pc est bien dans le domaine voulu. Pour cela on va dans les informations système générales, et nous pouvons voir que notre pc à bien été intégré au domaine.

Informations système générales

Édition Windows

Windows 10 Professionnel
© 2018 Microsoft Corporation.
Tous droits réservés.



Système

Processeur : Intel(R) Core(TM) i5-4590 CPU @ 3.30GHz 3.29 GHz
Mémoire installée (RAM) : 1,98 Go
Type du système : Système d'exploitation 64 bits, processeur x64
Stylet et fonction tactile : La fonctionnalité d'entrée tactile ou avec un stylet n'est pas disponible sur cet écran.

Paramètres de nom d'ordinateur, de domaine et de groupe de travail

Nom de l'ordinateur : windows
Nom complet : windows.local.lan
Description de l'ordinateur :
Domaine : local.lan

[Modifier les paramètres](#)

vérification de l'intégration de notre machine dans le domaine

Mise en place de la centralisation de logs

La centralisation des logs va nous permettre de superviser notre infrastructure réseau en analysant les paquets passant par les équipements centraux de notre réseau. Ainsi nous avons choisi de recevoir dans notre serveur de logs Graylogs, les logs de notre serveur Windows qui regroupe la majorité des serveurs de l'Intranet ainsi que ceux de notre Firewall qui voit tous les paquets entrants et sortants de la DMZ et de l'Intranet.

Pour cela, nous avons dû commencer par lancer notre serveur Graylog et y créer des entrées de logs personnalisés. Pour cela, nous nous rendons sur la VM Graylog qui possède le service graylog et nous éditons le fichier du graylog pour pouvoir accéder à sa console WEB.

```
nano /etc/graylog/server/server.conf
```

On peut observer sur la ligne "http_bind_address" que la console est accessible en tapant 127.0.0.1 avec le port 9000. On peut donc maintenant y accéder depuis la console WEB.

On va alors créer un Input qui recevra les paquets TCP sur le port 6000 comme montré ci-dessous:

TCP firewall

Bind address

0.0.0.0

Address to listen on. For example 0.0.0.0 or 127.0.0.1.

Port

6000

Port to listen on

Configuration d'un input sur le serveur Graylog

L'adresse 0.0.0.0 veut dire que la station Graylog va écouter sur tous ses ports les logs envoyés par les différents équipements.

Après cela, l'entrée Graylog TCP est créée et on peut maintenant s'atteler à l'envoi des logs depuis le firewall et le serveur Windows.

Tout d'abord pour le Firewall, il faut se rendre dans l'onglet syslog et créer un envoi de logs liés à l'input. On précise donc le même port que celui spécifié dans l'input, 6000, l'adresse du serveur Graylog ainsi que le protocole de transport envoyé, ici TCP.

Status	Name
Enabled	firewall_tcp
Disabled	Syslog Profile 1
Disabled	Syslog Profile 2
Disabled	Syslog Profile 3

Details

Name: firewall_tcp

Comments:

Syslog server: serv_graylog

Protocol: TCP

Port: portgraylog

Certification authority:

Server certificate:

Client certificate:

Format: RFC5424

Advanced properties

Configuration de l'envoi de logs depuis le firewall

Enfin on vérifie l'envoi de logs en observant sur les inputs qu'une active connexion a été ajoutée.

TCP firewall Syslog TCP RUNNING

On node ebb25098 / graylog

Show received messages Manage extractors Stop input More actions

```

allow_override_date: true
bind_address: 0.0.0.0
charset_name: UTF-8
expand_structured_data: false
force_rdns: false
max_message_size: 2097152
number_worker_threads: 1
override_source: <empty>
port: 6000
recv_buffer_size: 1048573
store_full_message: false

```

Throughput / Metrics

1 minute average rate: 2 msg/s

Network IO: 0B 0B (total: 90.4KiB 0B)

Active connections: 1 (1 total)

Empty messages discarded: 0

Connexion concluante avec le firewall

On peut ensuite observer les logs envoyés par le firewall, on peut notamment observer des flux http.

Ensuite pour le Windows serveur 2016, nous n'avons pas eu le temps de le faire sur Diateam et ensuite nous avons dû utiliser un Windows serveur 2008, où il n'est pas possible d'installer les applications que l'on souhaite qui nous permettrait d'envoyer nos logs au serveur graylog. En théorie, nous devions installer l'application NXlog sur la window serveur, modifier le fichier de conf de cette application de cette façon :

```
<Extension _gelf>
  Module      xm_gelf
</Extension>

# Snare compatible example configuration
# Collecting event log
<Input in>
  Module      im_msvistalog
</Input>

# Converting events to Snare format and sending them out over TCP syslog
<Output out>
  Module      om_tcp
  Host        192.168.101.1
  Port        6000
  OutputType  GELF
</Output>
#
# Connect input 'in' to output 'out'
<Route 1>
  Path        in => out
</Route>
```

Fichier NXlog permettant l'envoi de logs vers le graylog sur le port 6000

Ensuite normalement, notre serveur graylog reçoit nos logs mais nous n'avons pas pu le prouver comme vu précédemment.

Détection de flooding du firewall par le serveur Graylog

Ensuite, nous avons dû depuis le serveur Graylog détecter les floodings qui saturaient notre firewall depuis l'Internet. Pour cela, nous avons créé un nouvel input UDP sur le serveur Graylog de la même façon que la partie précédente mais cette fois-ci en UDP, nous configurons aussi l'envoi des logs UDP sur le firewall de la même manière dans l'onglet Notifications>Syslog. Enfin sur le Graylog, nous créons un événement flooding qui filtre toutes les alertes reçues.

Filter

Add information to filter the log messages that are relevant for this Event Definition.

Search Query

Search query that Messages should match. You can use the same syntax as in the Search page, including declaring Query Parameters from Lookup Tables by using the `$newParameter$` syntax.

+

Filtrage des trames par le logtype alarm

Enfin nous testons cette configuration par la commande de flooding suivante qui utilise le hping:

```
(root@kali)~# hping3 --flood 172.16.0.104
HPING 172.16.0.104 (eth0 172.16.0.104): NO FLAGS are set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 172.16.0.104 hping statistic ---
1633471 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Attaque test par flooding

On peut ainsi observer les événements flooding dans notre onglet alertes.

Find Events				Q	↺	10
Alerts Events Both						
Description	Key	Type	Event Definition	Timestamp		
Flooding	none	Event	Flooding	2024-04-04 09:47:16		
Flooding	none	Event	Flooding	2024-04-04 09:47:16		
Flooding	none	Event	Flooding	2024-04-04 09:47:13		
Flooding	none	Event	Flooding	2024-04-04 09:47:13		
Flooding	none	Event	Flooding	2024-04-04 09:47:12		
Flooding	none	Event	Flooding	2024-04-04 09:47:12		
Flooding	none	Event	Flooding	2024-04-04 09:47:10		
Flooding	none	Event	Flooding	2024-04-04 09:47:10		
Flooding	none	Event	Flooding	2024-04-04 09:47:06		

Evénements flooding bien reçus et observés

Inspections SSL

L'inspection SSL permet de bloquer des sites afin d'éviter l'accès depuis l'intranet. Pour cela, il a fallu rajouter une règle de filtrage que l'on place en première qui utilise une règle SSL.

FILTERING IPV4 NAT									
Searching...									
+ New rule X Delete ↑ ↓ ↺ ↻ Cut Copy Paste Search in logs									
	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments	
Remote management: Set to system configuration to setup the Web administration application access (does not contain any rules)									
Default policy (contains 8 rules, from 1 to 8)									
1	off	decrypt	Network_in	Internet	ssl_srv		IPS	SSL filter: SSLSFilter_00	Created on 2024-03-27 1...
2	on	pass	Vlan_101	Internet	Any		IPS		Created on 2024-03-25 0...
3	on	pass	Network_in via SSL proxy	Internet	ssl_srv		IPS		Created on 2024-03-27 1...
4	on	pass	Vlan_100	Internet	Any		IPS		Created on 2024-03-25 0...
5	on	pass	Vlan_100	serv_dmz	https		IPS		Created on 2024-03-25 0...
6	on	pass	Vlan_101	serv_dmz	Any		IPS		Created on 2024-03-25 0...
7	on	pass	Firewall_dn	serv_dmz	Any		IPS		Created on 2024-03-25 0...
8	on	block	Any	Any	Any		IPS		Created on 2024-03-25 0...

Mise en place du filtrage SSL

Après avoir mis en place le filtre SSL, nous mettons en place la règle SSL qui bloque une blacklist qui nous avons également créé.

(0) SSLSFilter_00					Edit	URL database provider: Embedded URL database
+ Add X Delete ↑ Up ↓ Down Cut Copy Paste + Add all predefined categories Check URL classification						
Status	Action	URL - CN	Comments			
1 on	Block without decrypting	blacklist	bloque youtube et univ-rennes1			
2 on	Pass without decrypting	proxysl_by...	don't decrypt some specific ssl servers			
3 on	Decrypt	any	default rule (decrypt all)			

Mise en place des règles SSL

Cette blacklist contient la catégorie block_out qui contient les URLs YouTube et de l'ent de l'université.

Romain Noel, Marius Beauchêne, Mathieu Caudan


```

user@crypto:~$ dig dmz.local.lan

; <<>> DiG 9.16.48-Debian <<>> dmz.local.lan
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7559
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
; COOKIE: f1b7f35966c8cde5 (echoed)
;; QUESTION SECTION:
;dmz.local.lan.                IN      A

;; ANSWER SECTION:
dmz.local.lan.                3600    IN      A      192.168.103.1

;; Query time: 4 msec
;; SERVER: 192.168.100.2#53(192.168.100.2)
;; WHEN: Thu Apr 04 11:46:33 CEST 2024
;; MSG SIZE  rcvd: 70

```

```

user@crypto:~$ dig -x 192.168.103.1

; <<>> DiG 9.16.48-Debian <<>> -x 192.168.103.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50951
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
; COOKIE: 240a234ac90bd70e (echoed)
;; QUESTION SECTION:
;1.103.168.192.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
1.103.168.192.in-addr.arpa. 3600    IN      PTR      dmz.local.lan.

;; Query time: 8 msec
;; SERVER: 192.168.100.2#53(192.168.100.2)
;; WHEN: Thu Apr 04 11:49:56 CEST 2024
;; MSG SIZE  rcvd: 95

```



```
user@crypto:~$ dig AAAA dmz.local.lan

; <<>> DiG 9.16.48-Debian <<>> AAAA dmz.local.lan
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6664
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
; COOKIE: f4807f0790c12c6f (echoed)
;; QUESTION SECTION:
;dmz.local.lan.                IN      AAAA

;; ANSWER SECTION:
dmz.local.lan.                3600    IN      AAAA      2001:470:c8f2:104::1

;; Query time: 12 msec
;; SERVER: 192.168.100.2#53(192.168.100.2)
;; WHEN: Thu Apr 04 11:57:27 CEST 2024
;; MSG SIZE  rcvd: 82
```

Mise en place d'un VPN

La mise en place du VPN permet de créer un tunnel IPsec pour connecter dans notre cas un PC de l'internet vers l'intranet.

```
(root@kali)-[~]
# openvpn /home/user/Téléchargements/openvpn_mobile_client.ovpn
2024-04-04 16:36:23 WARNING: Compression for receiving enabled. Compression has
been used in the past to break encryption. Sent packets are not compressed
unless "allow-compression yes" is also set.
Enter Auth Username: vpn
Enter Auth Password: *****
2024-04-04 16:36:33 WARNING: No server certificate verification method has been
enabled. See http://openvpn.net/howto.html#mitm for more info.
```

Commande openvpn pour lancer le tunnel VPN

On voit sur la capture précédente qu'avec la commande openvpn est lié un fichier récupérer dans la configuration sur le Stormshield.

```
(root@kali)-[~]# ping 192.168.101.1
PING: No server certificate verification more info.
PING 192.168.101.1 (192.168.101.1) 56(84) bytes of data.
64 bytes from 192.168.101.1: icmp_seq=1 ttl=63 time=2.66 ms
64 bytes from 192.168.101.1: icmp_seq=2 ttl=63 time=102 ms
^Z
zsh: suspended ping 192.168.101.1
2019-05-04 17:01:15 ERROR: Failed retrieving username or password

(root@kali)-[~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:eb:8d:0a brd ff:ff:ff:ff:ff:ff
    inet 172.16.1.104/16 scope global eth0
        valid_lft forever preferred_lft forever
```

Ping de l'internet vers intranet

Une fois la commande précédente lancée, le tunnel est créé et le ping d'internet vers l'intranet est fonctionnel.

Filtre IPS

on pass Any serv_dmz https IPS (IPS_00)

Afin de limiter le nombre de connexions sur la dmz, il fallait configurer IPS pour éviter tout problème lié aux nombres de connexions trop importantes. Nous avons donc ajouté une règle IPS au NAT qui filtre le nombre de connexions.

Conclusion:

Pour conclure, cette SAE peut-être découpée en deux périodes temporelles, la période virtualisée avec DIATEAM et la période en physique.

La première partie s'est très bien passé, nous avançons rapidement et sûrement et pouvions entrevoir la réussite de notre SAE mais des problèmes techniques sur DIATEAM, nous ont empêché de fournir un travail optimal comme prévu. Cependant, après avoir tout reconfiguré avec les outils que l'on possédait, une Windows serveur 2008, une graylog en ligne de commande, nous avons tout de même accompli une très grande partie de ce projet sans toutefois avoir pu le compléter pleinement. L'utilisation de ce serveur 2008 ne nous a par exemple pas permis de compléter notre configuration de logs par l'envoi de logs depuis la Windows en utilisant NXlog. Cette difficulté nous a par contre forcés à étudier les 2 facettes des réseaux que sont les équipements physiques et virtualisés ce qui pourra nous apporter une polyvalence en entreprise par exemple.

Finalement, nous avons pu appliquer les connaissances que nous avons acquises tout au long de l'année en cyber et en réseaux autour d'un projet complet. Ce projet a finalement été accompli à l'aide des moyens fournis et nous sommes plutôt fiers de ne pas avoir eu à faire d'impasse malgré les déboires de DIATEAM. Cependant, des captures n'ont pas pu être prises sur la plateforme ou en physique car nous avons voulu finir ce projet et pas pris le temps de capturer nos configurations..