

BUT R&T - Semestre 3

Parcours Cybersécurité

SAÉ3.Cyber.03

« Concevoir un réseau informatique sécurisé multi-sites »

1,5h CM (présentation du projet + visite s408)

4,5h CM (Cryptographie et VPN)

3h TP (ASA) + 3h TP (téléphonie IP-SIP et QoS)

6h TP (évaluation pratique des compétences)

- présentation collective organisation du projet
- niveau d'attente des objectifs / points d'étape
- fourniture plan d'@IP complet, identifiants
- démonstration injection des configurations
- évaluation technique individuelle
- réaction à plusieurs niveaux de pannes

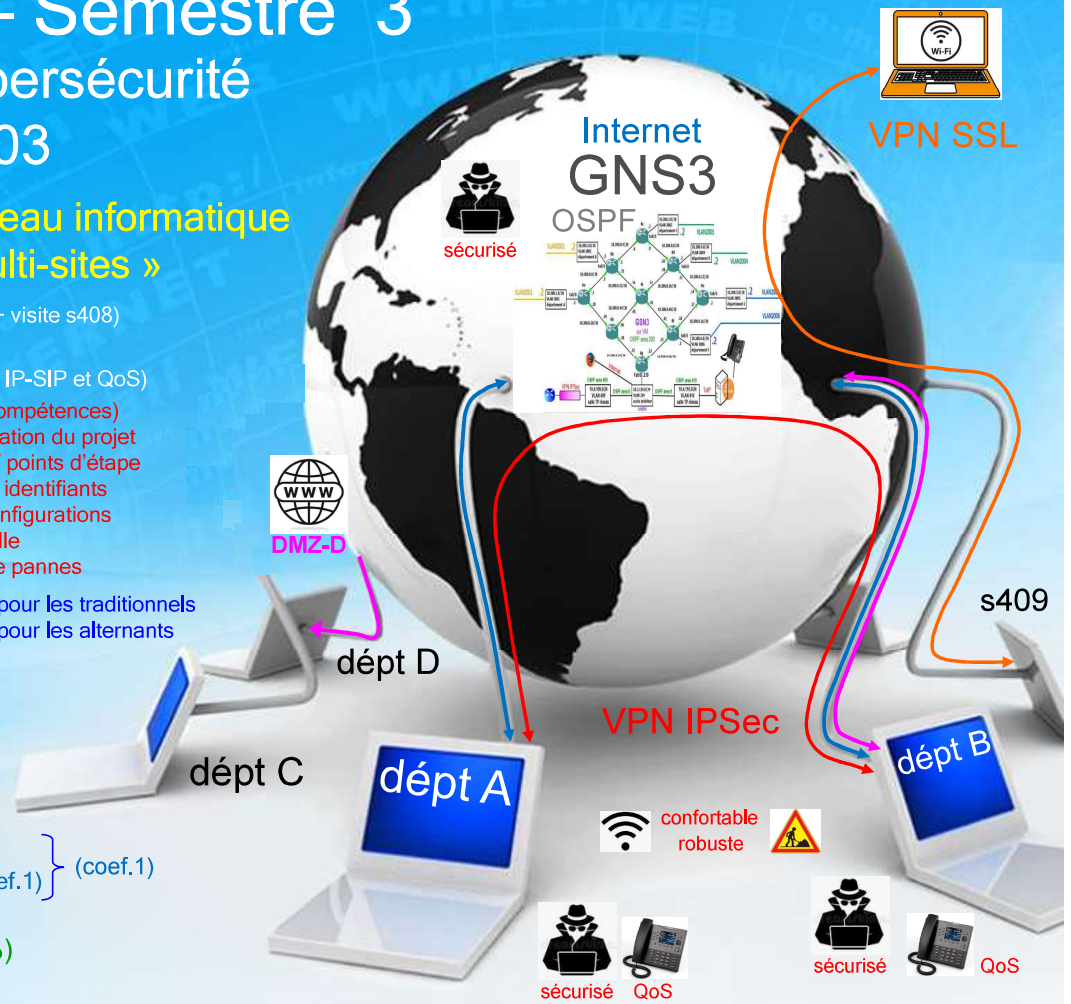
30h projet en autonomie planifié pour les traditionnels

21h projet en autonomie planifié pour les alternants

trois notes :

TP Parefeu ASA5505 (coef.1)
TP ToIP avec VPN IPSec (coef.1) } (coef.1)
Évaluation projet (coef.3)

coefficient : 47/300 (~16%)



Sommaire :

- 1-Objectifs : de la connaissance aux compétences
- 2-Contraintes imposés dans l'architecture proposée
- 3-Architecture réseau proposée : simulation à production
- 4-Connexion sur les équipements réels depuis l'extérieur
- 5-Pistes de réflexions dans les choix techniques
- 6-Organisation de la situation d'apprentissage
- 7-Évaluation de la situation d'apprentissage
- 8-Démonstration simulation et production département E
- 9-Visite des installations et échanges



1.a-Objectif :

Compétences ciblées :

- administrer et sécuriser un système d'information multisite
- connecter les sites de l'entreprise et les usagers de manière sécurisée
- comprendre un cahier des charges, faire des choix techniques

Problématique professionnelle :

- justifier les solutions apportées à partir d'un cahier des charges
- mettre en œuvre les méthodes de test garantissant le fonctionnement
- évaluer les vulnérabilités potentielles et connues face aux menaces



Connaissances mobilisées : ● BUT1 ● BUT2 ● BUT3

- à partir d'un cahier des charges exprimant les besoins de l'entreprise
- découpage en sous-réseaux d'une adresse IPv4 : [ressource R2.01](#)
- configuration de VLAN et routage inter-VLAN : [ressource R1.03](#)
- redondance du réseau local STP/RSTP : [ressource R1.03](#)
- routage statique et routage dynamique OSPF : [ressource R2.01](#)
- redondance de la liaison d'extrémité HSRP : [ressource R2.01](#)
- accès via un tunnel sécurisé : [ressource R.201](#) et cours/TP VPN-Crypto
- services DHCP, DNS, T/FTP, NTP : [ressources R2.01 / R2.03 / R3.03](#)
- sécurisation et accès par une translation d'adresses NAT : [ressource R2.01](#)
- sécurisation des accès : SSH et ACL : [ressource R1.03](#) et [ressource R2.01](#)
- sécurisation des réseaux LAN : [ressource R4.Cyber.09](#)
- sécurisation des services réseaux : [ressource R4.Cyber.11](#)
- sauvegarde des configurations : [ressource R1.03](#)
- intégration d'un réseau WiFi : [ressource R3.01](#) et [ressource R5.01](#)
- téléphonie : [ressource R2.04](#) et TP ToIP avec VPN IPSec
- recherche de vulnérabilités PENTESTING : [R3.Cyber.16](#) et [SAE3.Cyber.04](#)



1.b-Compétences évaluées :

Compétences techniques mobilisées : savoir-faire



Packet Tracer
OSPF avec priorité selon VLAN
HSRP sur routeur ou switch
Subnetting imposé selon site
Continuité des flux SW vers RT
Service DHCP avec options ToIP
AAA avec MD5 et accès SSH
Sécurité LAN, ports shut
ASA avec VPN SSL
ASA avec VPN IPSec
IPBX et DHCP spécifique ToIP
ASA avec NAT et ACL
Injection sans erreur < 15 min

- savoir utiliser la simulation pour valider son étude avant la phase de production
- mettre en œuvre une redondance de niveau 2 avec équilibrage des charges
- mettre en œuvre une redondance de niveau 3 sur le cœur de réseau
- savoir effectuer un découpage pertinent en sous-réseaux
- savoir optimiser les chemins empruntés par les flux
- savoir identifier le besoin en services réseaux, les configurer si besoin
- mettre en œuvre une sécurité d'accès local et distant des équipements actifs
- mettre en œuvre une sécurité du réseau local de chacun des sites
- mettre en œuvre un accès nomade sécurisé
- mettre en œuvre une liaison sécurisée entre les sites de l'entreprise
- savoir intégrer de la téléphonie sur IP basée sur l'IPBX Asterisk
- savoir intégrer la dmz avec ressources accessibles depuis l'extérieur
- savoir injecter rapidement des configurations sauvegardées



Compétences personnelles mobilisées : savoir-être

Mobiliser ses connaissances
S'adapter au contexte
Interpréter et réactivité
Faculté d'autonomie
Imposer sa place dans l'équipe
Justifier ses choix, S'organiser
Faculté d'auto-apprentissage
Force participative dans l'équipe

- savoir mobiliser les connaissances issues des enseignements réseaux en R&T
- savoir appréhender des matériels réels hétérogènes (hardware et IOS)
- savoir interpréter les différents types de messages lors des configurations
- savoir s'adapter et rechercher une alternative aux problèmes qui se posent
- savoir gérer un projet en équipe afin de garantir l'atteinte des objectifs fixés
- savoir se positionner techniquement et temporellement
- savoir mettre à niveau ses connaissances/compétences censées être acquises
- être à l'écoute et force de proposition au sein de son équipe, rendre compte

2-Contraintes imposées :

Contexte :

- sites interconnectés vers le monde extérieur de manière sécurisée
- architecture robuste (**résistante aux pannes** et **résistante aux attaques**)
- équilibrage de charge au sein de la topologie (HSRP/STP/VLAN)
- confort des utilisateurs au niveau de la mobilité et des services proposés
- **transparence des configurations pour les usagers :**

DHCP	–	obtention des paramètres IP de manière automatique
VLAN	–	accès aux ressources qui lui sont destinées
RSTP, PortFast	–	permanence de la connexion locale et reconfiguration rapide
HSRP	–	permanence de la connexion au monde extérieur
STP+HSRP+VLAN	–	équilibrage de charge par une orientation des flux internes
ASA+NAT	–	masquer les adresses IP locales depuis l'extérieur (NAT)
SSH/AAA+VPN	–	accéder en sécurité aux équipements actifs en interne et depuis l'extérieur
VPN SSL + DMZ	–	prendre en compte les besoins en mobilité au sein de l'entreprise
IPBX+DHCP ToIP	–	prendre en compte les besoins en ToIP intra et inter départements



A B C D E F

Quelques données imposées : Z = 8, 16, 24, 32, 40, 48 selon le département

- trois réseaux internes affectés : 192.168.[Z].0/21 – 172.16.[Z].0/27 – 10.10.[Z].0/28
- réseau extérieur en 10.200.x.0/30 avec x = numéro du site de 1 à 6
- sur le réseau virtuel GSN3 depuis l'ASA 5505 « outside » vers 10.200.x.2
- **OSPF si routage dynamique envisagé et sans inondation du monde extérieur !**
- organisation des flux selon quatre VLAN :
 - **VLAN 2** : connexion filaire des collaborateurs (ports 1 à 10 des commutateurs)
 - **VLAN 3** : connexion filaire de l'administration (ports 11 à 20 des commutateurs)
 - **VLAN 4** : connexion téléphonie sur IP (port 21 des commutateurs)
 - **VLAN 7** : destiné à la gestion des équipements actifs

R11

gestion
des flux

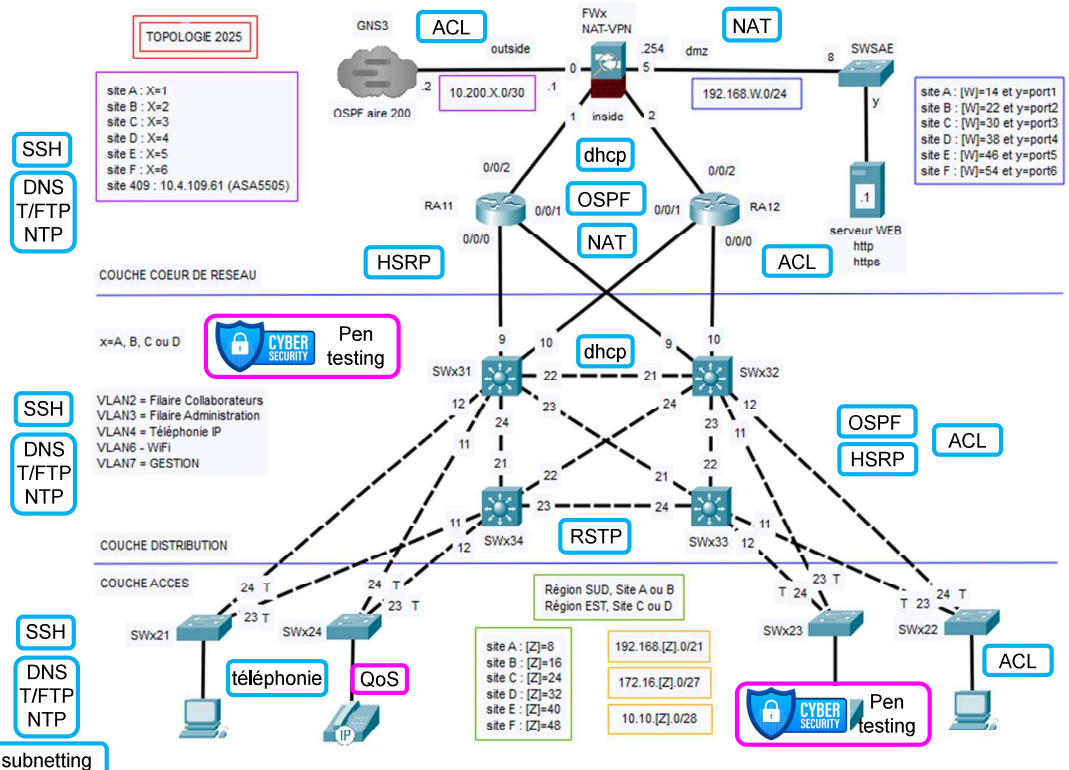
R12



Synthèse :

● BUT1 ● BUT2 ● BUT3

- une topologie globale englobant de nombreuses notions
 - beaucoup de ces notions ont été étudiées en BUT1 R&T
 - investissement initial à considérer
 - organisation dans le temps
 - répartition des tâches dans l'équipe
 - des notions acquises au cours du BUT2 R&T : à implémenter
- Garantir la finalisation du projet**



- plan d'adressage IP complet
- décomposition en sous-réseaux
- gestion des différents VLAN
- accès équipements par VLAN
- commutation-routage
- inter-VLAN



A vertical image featuring a globe at the bottom, connected by thin white wires to two small, silver laptop computers. The background is a light blue gradient with a repeating pattern of text in various shades of blue and white, including 'WWW', 'INTERNET', 'e-mail', 'http', and 'information'. The text is arranged in a way that suggests a global network or the internet.

sites **B** ou **D**

3-Architecture proposée :

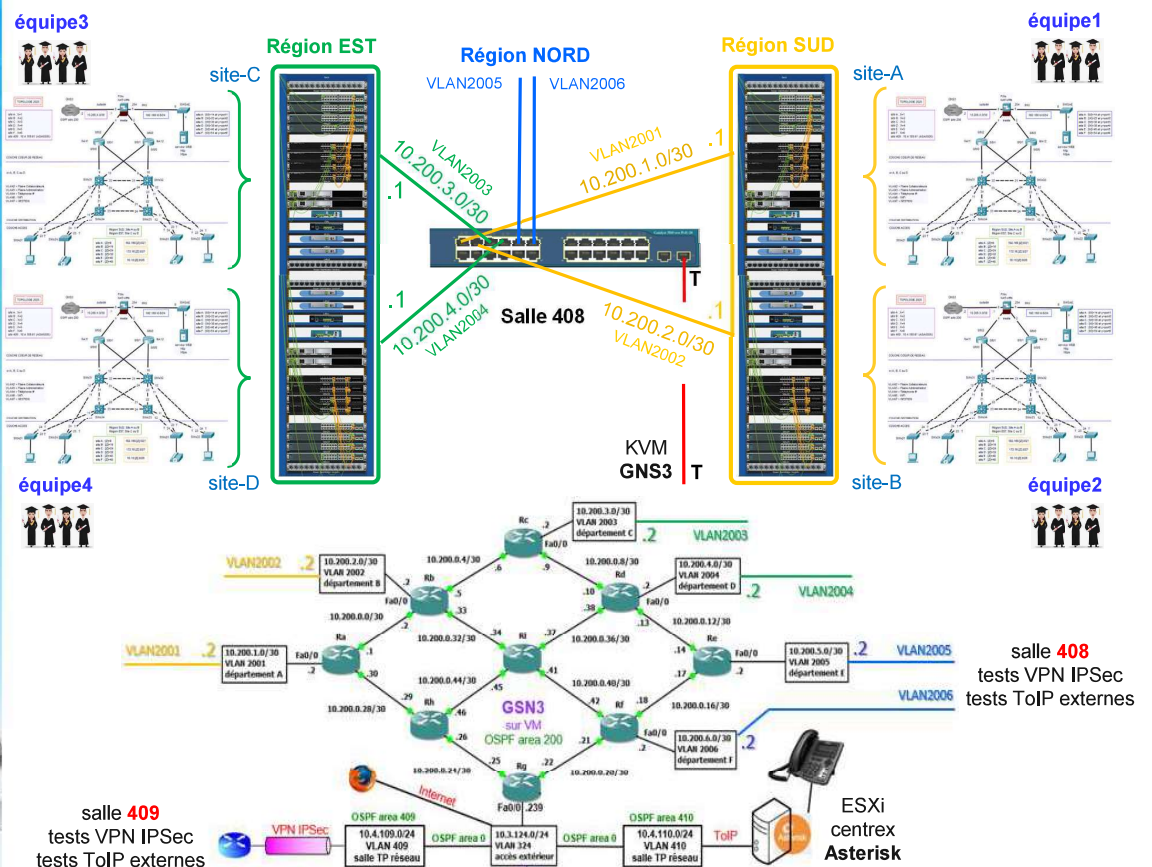
b) Phase de production sur les équipements réels :

- équipements hétérogènes testés par le responsable SAÉ : opérationnels
 - région SUD, site A entièrement configuré selon une stratégie : 20% du choix étudiant
 - région EST, site C entièrement configuré selon autre stratégie : 80% du choix étudiant
 - région NORD, département E et F : configuration permanente d'études (laboratoire test)
 - Paillasse 6 salle 409 (enseignant) : Pare-feu configuré outside 10.4.109.61, Lan 192.168.100.0/24
- adapter fichiers de configuration aux caractéristiques des équipements
 - version d'IOS plus, ou moins limitée que Packet Tracer : sécurité, commandes spécifiques
 - nomenclature, débits, nombre d'interfaces différentes : adaptation des fichiers de configuration
 - utilisation de SFP non compatibles : service unsupported-transceiver, no errdisable detect cause gbic
 - utilisation d'anciennes cartes réseaux : vérification du mode de communication full-duplex
 - gestion des mots de passe : en MD5 et les laisser en clair dans le fichier de configuration ...
 - sécurité niveau 2 : beaucoup plus de possibilités sur les équipements réels !
 - activation des interfaces : « no shutdown » à ajouter aux fichiers
 - vérification de la pertinence des configurations : show cdp neighbors, sh ip interfaces brief
- méthodologie de validation des configurations injectées et de tests
 - injection des fichiers : aucune erreur, pas de blocage par attente de réponse, réaction interfaces !
 - connectivité interne sur Vlan de gestion : tous commutateurs et routeurs joignables entre eux
 - service dhcp : activation service dhcp sur vlan des commutateurs de la couche d'accès
 - connectivité inter-VLAN : tous commutateurs sur tous les VLAN gérés
 - routage du cœur de réseau : connaissance de tous les réseaux internes jusqu'au Firewall
- éprouver la topologie face aux pannes (niveau de robustesse)
 - redondance commutation : désactivation plusieurs interfaces et tests de connectivité
 - redondance routage : désactivation plusieurs interfaces et tests de connectivité, réaction HSRP
 - équilibrage des charges : vérification convergence RSTP selon VLAN d'appartenance
- sécurisation vers le monde extérieur et depuis l'extérieur
 - configuration pertinente du Pare-feu : connectivité avec le réseau interne et vers réseaux externes
 - connexion vers un autre site : vérification connexion VPN IPSec (réseau 192.168.100.254 en s409)
 - connexion depuis l'extérieur : vérification connexion VPN SSL depuis connexion salle R&T
 - gestion de la sécurité : autorisation des connexions entrantes juste nécessaires
 - gestion de la dmz : autorisation des accès depuis Internet et vers le réseau local de site
- intégration de la ToIP : IPBX, DHCP, serveur TFTP, ...

si le reste fonctionne

3-Architecture proposée :

b) Phase de production : tests connectivité et redondance



3-Architecture proposée :

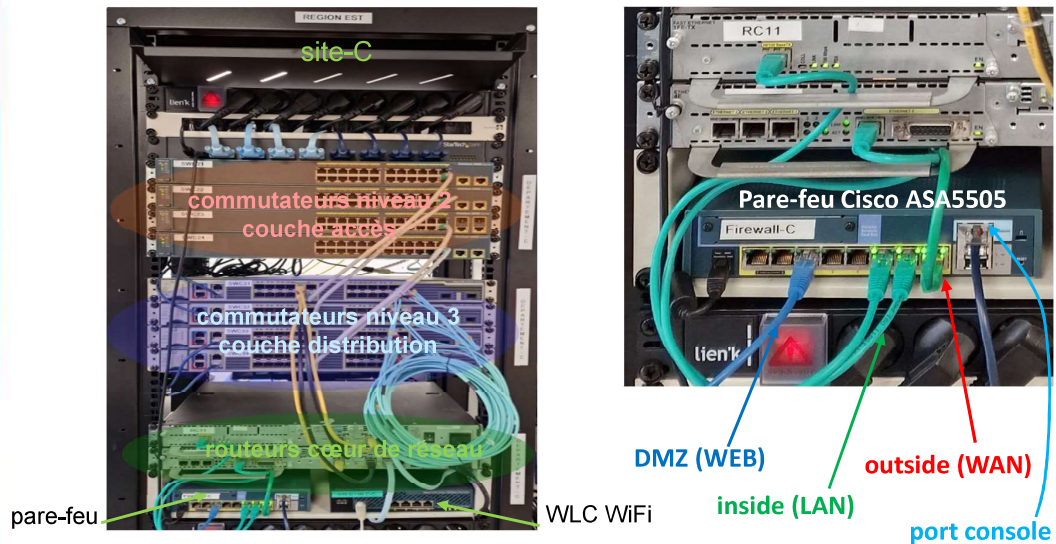
si le reste fonctionne

c) Phase d'enrichissement : ToIP

- uniquement si la phase production est opérationnelle :
- intégration de la ToIP : **port 21 – Vlan4 de la couche d'accès**
 - mise en place d'un IPBX local sous Linux ASTERISK
 - configuration d'un DHCP spécifique ToIP avec options et serveur TFTP selon téléphone
 - configuration pare-feu pour permettre les accès TFTP, SIP et RTP liés à la téléphonie
 - **DHCP en 192.168.8x.0/24 (x étant le numéro du département)** pour le VLAN ToIP
 - finalisation des configurations des téléphones IP, tests communications internes et externes

– Transmission de toutes les configurations au plus tard **début décembre**

– Si configurations pertinentes, test sur matériels réels possible jusqu'aux vacances de Noël



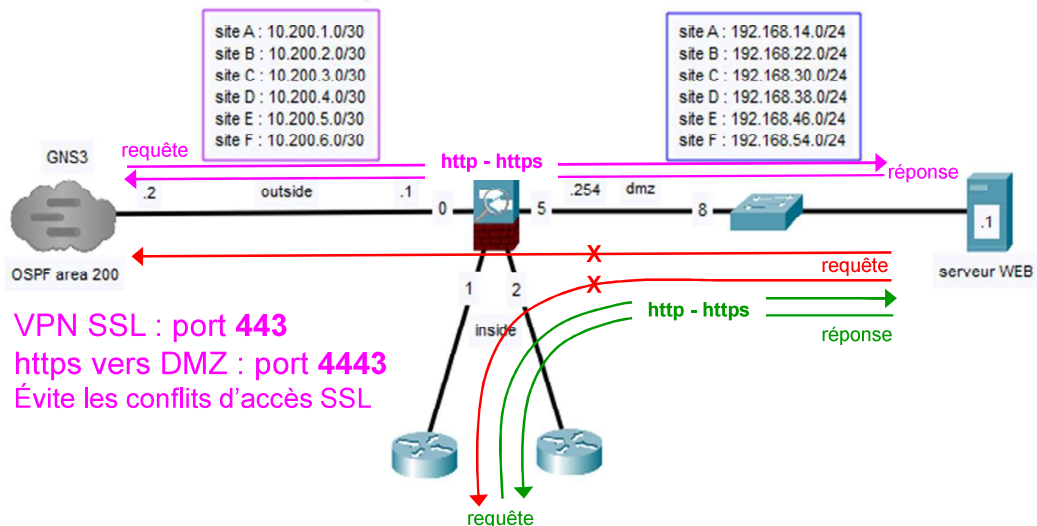
3-Architecture proposée :

si le reste fonctionne

c) Phase d'enrichissement : DMZ

- uniquement si la phase production est opérationnelle :
- intégration de l'accès aux ressources WEB dans la DMZ :
 - DMZ accessible depuis Internet en http, https, ftp, tftp, dns, icmp
 - réseau local d'un site accède à sa DMZ sans restriction
 - le serveur Web sur la DMZ ne répond qu'aux sollicitations et ne peut initier une requête
 - Les adresses sources provenant d'Internet sont masquées sur le réseau DMZ
 - adresses des DMZ selon les sites :

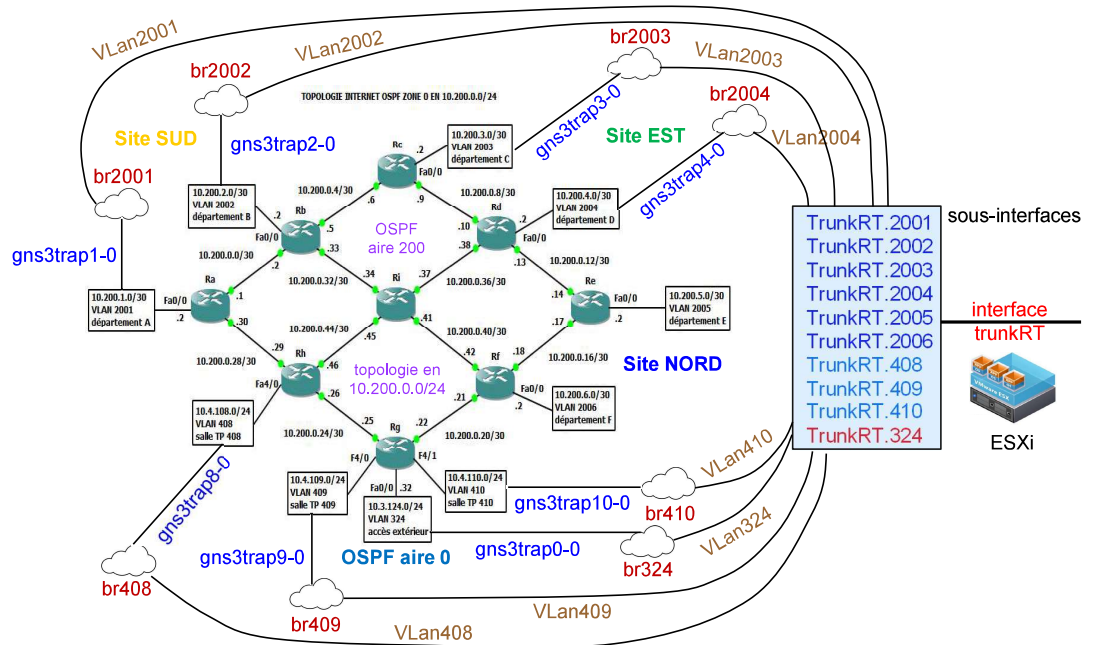
site A : 192.168.14.0/24 avec interface ASA-dmz en .254
 site B : 192.168.22.0/24 avec interface ASA-dmz en .254
 site C : 192.168.30.0/24 avec interface ASA-dmz en .254
 site D : 192.168.38.0/24 avec interface ASA-dmz en .254
 site E : 192.168.46.0/24 avec interface ASA-dmz en .254
 site F : 192.168.54.0/24 avec interface ASA-dmz en .254



3-Architecture proposée :

d) Interconnexion des sites par routage sous GNS3

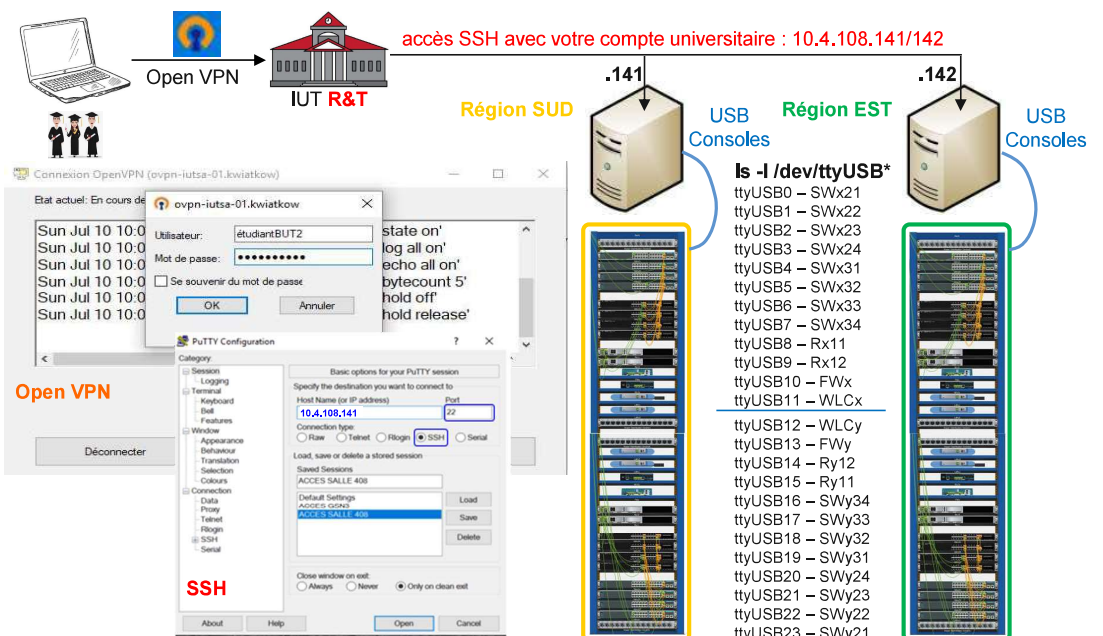
- solution choisie : utilisation de la topologie de routage OSPF sous GNS3
 - réalisation de la topologie GNS3 localement et fonctionnelle : 9 routeurs
 - respect de l'utilisation de l'@IP : 10.200.0.0/24 pour la topologie GSN3
 - interfaces d'extrémité respectant les @IP : 10.200.x.2/24, x = site
 - routage entre département dynamique en OSPF aire 200 vers l'aire 0
 - interface de connexion extérieure reliée au Vlan 324 via l'aire 0
 - interface de connexion extérieure respectant l'@IP : 10.3.124.239/24
 - création des interfaces br200(x) et br324 et création sous-interfaces TrunkRT.?



4-Connexion depuis l'extérieur :

a) Répartition des régions et départements

- un groupe de TP = 3 à 4 équipes responsables d'un département chacun
 - connexion réseau R&T directement sur place ou par OpenVPN depuis l'extérieur
 - accès SSH avec compte étudiant sur le serveur gérant le département X
 - serveurs Debian = 10.4.108.141 (région SUD), 10.4.108.142 (région EST)
 - accès aux ports USB connectés sur les ports console des équipements (0 à 23)
 - 12 équipements connectés par département (2xRT, 4xSWL2, 4xSWL3, FW, WLC)
 - créneaux de 3h par équipe et par groupe de TP : configuration usine en partant !
 - se reporter aux photos des matériels par site pour s'approprier l'architecture



4-Connexion depuis l'extérieur :

b) Connexion sur port console des équipements actifs

- \$minicom -D /dev/ttyUSB?
- minicom -D /dev/ttyUSB0à3 ou 23à20 (SWx21à24 site-x ou SWy21à24 site-y)
- minicom -D /dev/ttyUSB4à7 ou 19à16 (SWx31à34 site-x ou SWy31à34 site-y)
- minicom -D /dev/ttyUSB8à9 ou 15à14 (Rx11à12 site-x ou Ry11à12 site-y)
- minicom -D /dev/ttyUSB10 ou 13 (FWx site-x ou FWy site-y)
- minicom -D /dev/ttyUSB11 ou 12 (WLCx site-x ou WLCy site-y) **non concerné !**

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Jul 9 14:45:20 2022 from 172.23.136.5
rt@rt408p159:~$ minicom -D /dev/ttyUSB9

Bienvenue dans minicom 2.8

OPTIONS: I18n
Port /dev/ttyUSB9

Tapez CTRL-A Z pour voir l'aide concernant les touches spéciales

CTRL-A Z for help 9600 8N1 NOR Minicom 2.8 VT102 Déconnecté tyUSB9
```

connexion via le VPN

lancement session série ciblant le port console du commutateur RB12 du site B sur la région SUD

débit de l'interface série

état

device

- visualisation identique à un port console via PuTTY ou HyperTerminal

```
Switch>
Switch>en
Switch>sh run
Building configuration...

Current configuration : 1185 bytes
!
version 12.1
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
```

Configuration vierge :

- à partir du port console : configuration en temps réel
- à partir du port console : copie d'une configuration existante
- pas de téléversement/téléchargement à partir d'un serveur TFTP
- un site peut être entièrement opérationnel en moins de 10 minutes !

Déconfiguration usine :

- #delete vlan.dat - #write erase - reload
- Would you like to enter the initial configuration dialog ? [yes/no]
- laisser en l'état, sinon recommencer ...

4-Connexion depuis l'extérieur :

c) Paramétrage et conflit d'accès

- CTRL-A et P : accès au paramétrage du port série :
 - permet de sélectionner le débit du port série en 9600 bauds : C
 - permet de sélectionner le débit du port série en 115200 bauds : E
 - permet de paramétrer le port série classiquement 8-N-1 : Q (ou 8-L-1)
 - les paramètres sont pris en compte en temps réel !

débit de l'interface série

```
----[Paramètres de communication]----
Actuelle: 9600 8N1
Vitesse Parité Données
A: <suiv> L: Aucune S: 5
B: <prev> M: Paire T: 6
C: 9600 N: Impaire U: 7
D: 4800 O: Marque V: 8
E: 115200 P: Espace

Bits de stop
W: 1 Q: 8-N-1
X: 2 R: 7-E-1

Choix ou <Entrée> pour sortir ?
```

contrôle de parité

paramètres présélectionnés

- conflit d'accès à une session série :
 - perte de la connexion SSH vers le poste Linux en salle 408
 - perte de la connexion VPN entre votre poste de travail et le département R&T
 - équipement ciblé en train d'être configuré par un collègue de l'équipe
 - 95% des cas - déconnexion brutale de la part d'un autre étudiant d'une équipe précédente
 - connexion série /dev/ttyUSBx toujours active et non accessible par un tiers

numéro processus

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Jul 10 10:09:33 2022 from 172.23.0.14
rt@rt408p159:~$ ps ax | grep minicom
14945 pts/0 S+ 0:00 minicom -D /dev/ttyUSB15
14961 pts/1 S+ 0:00 grep minicom
rt@rt408p159:~$
```

après connexion sur le poste Linux listez les processus de liaison série
\$ps ax | grep minicom
parmi la liste des processus affichés Mettez fin au processus ciblant l'USB x
\$kill -9 14945

- mettre fin à une session série : CTRL-A et Q
tuer la fenêtre sans se déconnecter au préalable = **incompétence !**

Quitter sans remettre à zéro ?
Oui Non

4-Connexion depuis l'extérieur :

d) Synthèse du câblage des ports console

Pare-feu = Cisco ASA 5505

WLC = Cisco Wireless Lan Controller 2504



- Attribution des ports USB via la machine Linux : 10.4.108.**141/142/143**

Région SUD

```
/dev/ttyUSB0 dépt-A: SWA21
/dev/ttyUSB1 dépt-A: SWA22
/dev/ttyUSB2 dépt-A: SWA23
/dev/ttyUSB3 dépt-A: SWA24
/dev/ttyUSB4 dépt-A: SWA31
/dev/ttyUSB5 dépt-A: SWA32
/dev/ttyUSB6 dépt-A: SWA33
/dev/ttyUSB7 dépt-A: SWA34
/dev/ttyUSB8 dépt-B: RA11
/dev/ttyUSB9 dépt-B: RA12
/dev/ttyUSB10 dépt-A: FWA
/dev/ttyUSB11 dépt-A: WLCA
/dev/ttyUSB12 dépt-B: WLCB
/dev/ttyUSB13 dépt-B: FWB
/dev/ttyUSB14 dépt-B: RB12
/dev/ttyUSB15 dépt-B: RB11
/dev/ttyUSB16 dépt-B: SWB21
/dev/ttyUSB17 dépt-B: SWB22
/dev/ttyUSB18 dépt-B: SWB23
/dev/ttyUSB19 dépt-B: SWB24
/dev/ttyUSB20 dépt-B: SWB31
/dev/ttyUSB21 dépt-B: SWB32
/dev/ttyUSB22 dépt-B: SWB33
/dev/ttyUSB23 dépt-B: SWB34
```

Région NORD

```
/dev/ttyUSB0 dépt-E: SWE21
/dev/ttyUSB1 dépt-E: SWE22
/dev/ttyUSB2 dépt-E: SWE23
/dev/ttyUSB3 dépt-E: SWE24
/dev/ttyUSB4 dépt-E: SWE31
/dev/ttyUSB5 dépt-E: SWE32
/dev/ttyUSB6 dépt-E: SWE33
/dev/ttyUSB7 dépt-E: SWE34
/dev/ttyUSB8 dépt-E: RE11
/dev/ttyUSB9 dépt-E: RE12
/dev/ttyUSB10 dépt-E: FWE
/dev/ttyUSB11 dépt-E: WLCE
/dev/ttyUSB12 dépt-F: WLCF
/dev/ttyUSB13 dépt-F: FWF
/dev/ttyUSB14 dépt-F: RF12
/dev/ttyUSB15 dépt-F: RF11
/dev/ttyUSB16 dépt-F: SWF21
/dev/ttyUSB17 dépt-F: SWF22
/dev/ttyUSB18 dépt-F: SWF23
/dev/ttyUSB19 dépt-F: SWF24
/dev/ttyUSB20 dépt-F: SWF31
/dev/ttyUSB21 dépt-F: SWF32
/dev/ttyUSB22 dépt-F: SWF33
/dev/ttyUSB23 dépt-F: SWF34
```

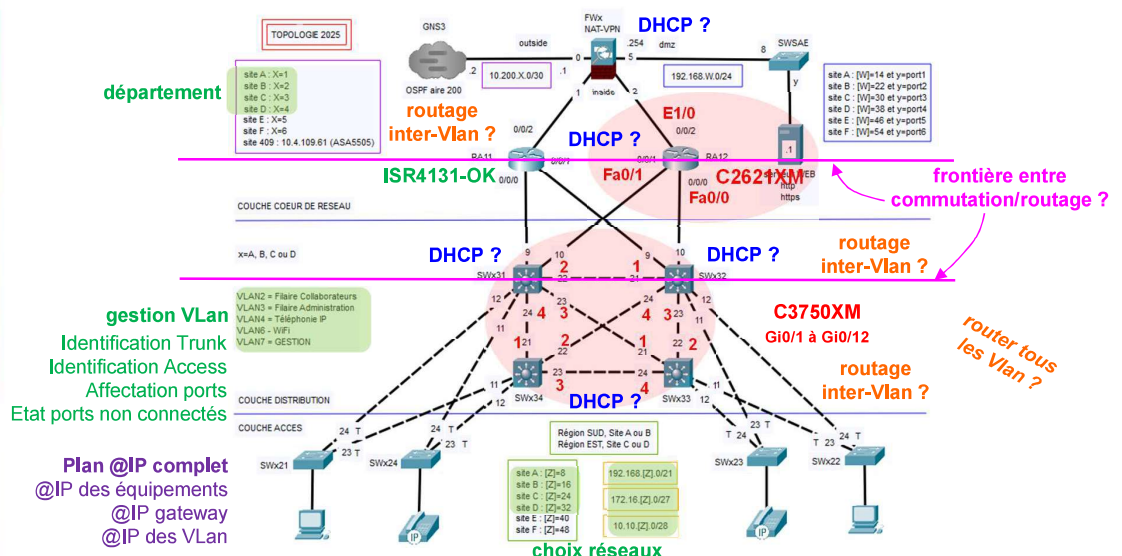
Région EST

```
/dev/ttyUSB0 dépt-C: SWC21
/dev/ttyUSB1 dépt-C: SWC22
/dev/ttyUSB2 dépt-C: SWC23
/dev/ttyUSB3 dépt-C: SWC24
/dev/ttyUSB4 dépt-C: SWC31
/dev/ttyUSB5 dépt-C: SWC32
/dev/ttyUSB6 dépt-C: SWC33
/dev/ttyUSB7 dépt-C: SWC34
/dev/ttyUSB8 dépt-C: RC11
/dev/ttyUSB9 dépt-C: RC12
/dev/ttyUSB10 dépt-C: FWC
/dev/ttyUSB11 dépt-C: WLCC
/dev/ttyUSB12 dépt-D: WLCD
/dev/ttyUSB13 dépt-D: FWD
/dev/ttyUSB14 dépt-D: RD12
/dev/ttyUSB15 dépt-D: RD11
/dev/ttyUSB16 dépt-D: SWD21
/dev/ttyUSB17 dépt-D: SWD22
/dev/ttyUSB18 dépt-D: SWD23
/dev/ttyUSB19 dépt-D: SWD24
/dev/ttyUSB20 dépt-D: SWD31
/dev/ttyUSB21 dépt-D: SWD32
/dev/ttyUSB22 dépt-D: SWD33
/dev/ttyUSB23 dépt-D: SWD34
```

5-Pistes de réflexions :

a) Réflexions n°1 : adaptation, premiers choix techniques

- adaptation Packet Tracer aux équipements réels :
 - type d'équipement réels présent dans Packet Tracer : ASA, WLC, RT, SW
 - ports connectés sur les équipements réels à reproduire sur Packet Tracer
 - au besoin, ajouter des interfaces ou partir d'un équipement générique
 - topologie Packet Tracer la plus proche de l'architecture de production**
- premiers choix techniques : établissement du plan d'@IP complet
 - emplacement du service DHCP, sur un ou plusieurs équipements ?, relais DHCP ?
 - à quel niveau se situe le routage inter-Vlan : SWL3 ou RT ?
 - placement de la frontière entre le monde commuté et le monde routé ?
 - choix des adresses réseau selon le département affecté et subnetting
 - création Vlan, affectation des ports, **plan d'adressage IP complet de la topologie**



- TOPOLOGIE 2025**

sie A : X=1
sie B : X=2
sie C : X=3
sie D : X=4
sie E : X=5
sie F : X=6
sie 409 : 10.109.61 (ASA5505)

GNS3
OSPF are 200

FWX NAT-VPN
outside
inside

SWSAE

RA11
RA12

serveur WEB
http
https

VLAN 2,7 ?

Vlan 3-4 ?

STP
pont racine
état des ports
influence des chemins
équilibrage de charges

Robustesse
mises en œuvre pannes
réaction topologie
convergence STP
tests de connectivité

Attques
Vlan spoofing
Vlan hopping
BPDU storm
DHCP starvation
DHCP spoofing

Couche Coeur de Réseau

x=A, B, C ou D

VLAN2 = Faire Collaborateurs
VLAN3 = Faire Administration
VLAN4 = Téléphone P.
VLAN5 = WIFI
VLAN7 = GESTION

Couche Distribution

Couche Accès

Région SUD, Site A ou B
Région EST, Site C ou D

sie A : [Z]=8
sie B : [Z]=16
sie C : [Z]=24
sie D : [Z]=32
sie E : [Z]=40
sie F : [Z]=48

192.168.[Z]/0/21
172.16.[Z].0/27
10.10.[Z].0/28

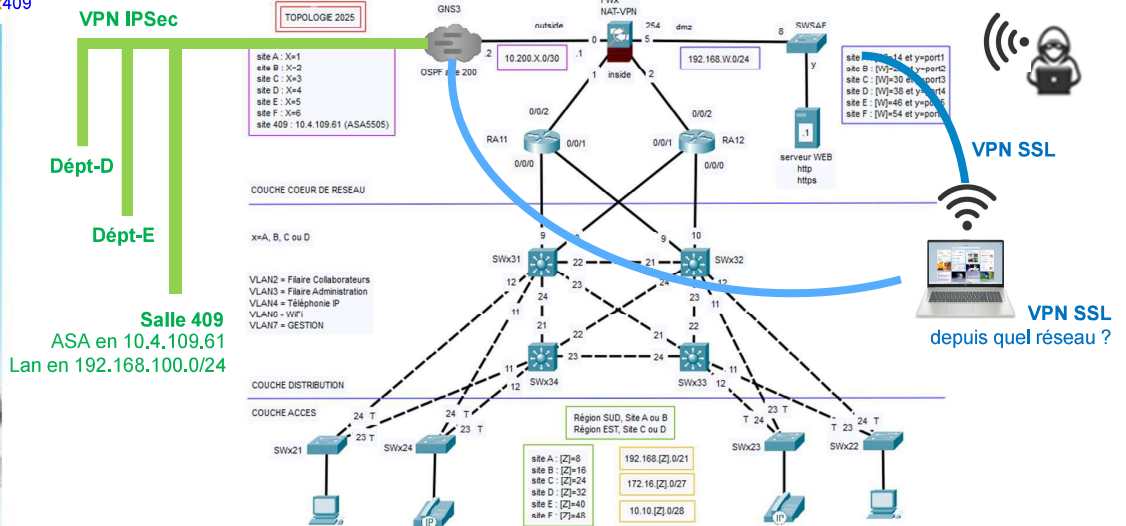
-
- The diagram illustrates a multi-tier network architecture, showing the transition from static routing to dynamic routing (OSPF) and the implementation of HSRP for redundancy and load balancing.
- COUCHE CŒUR DE RESEAU (Core Network Layer):**
- RA11 and RA12:** Core routers connected via their 0/0/0 and 0/0/1 interfaces. They are configured with OSPF.
 - SWx31 and SWx32:** Core switches connected to RA11 and RA12. They are configured with OSPF.
 - SWx33 and SWx34:** Core switches connected to SWx31 and SWx32. They are configured with OSPF.
- COUCHE DISTRIBUTION (Distribution Layer):**
- SWx21 and SWx24:** Distribution switches connected to SWx31 and SWx34. They are configured with OSPF.
 - SWx23 and SWx22:** Distribution switches connected to SWx32 and SWx33. They are configured with OSPF.
- COUCHE ACCES (Access Layer):**
- SWx21 and SWx24:** Access switches connected to SWx21 and SWx24. They are configured with OSPF.
 - SWx23 and SWx22:** Access switches connected to SWx23 and SWx22. They are configured with OSPF.
- External Connections and Services:**
- GNS3:** Connected to the network via an outside interface (10.200.X.0/30) and an inside interface (192.168.X.0/24).
 - FWx NAT-VPN:** Connected to the network via an outside interface (10.200.X.0/30) and an inside interface (192.168.X.0/24).
 - SWSAE:** Connected to the network via an outside interface (10.200.X.0/30) and an inside interface (192.168.X.0/24).
 - serveur WEB:** Connected to the network via an outside interface (10.200.X.0/30) and an inside interface (192.168.X.0/24).
- Static vs. Dynamic Routing:**
- routeur statique ?** (Static router?)
 - OSPF ?** (OSPF?)
- HSRP (Hot Standby Router Protocol):**
- équilibrage de charges** (Load balancing)
 - frontière entre commutation/routage ?** (Boundary between switching/routing?)
- IP Addressing and Subnets:**
- 192.168. [Z] 0/21**
 - 172.16. [Z] 0/27**
 - 10.10. [Z] 0/28**
- Site Information:**
- site A:** [Z]=8
 - site B:** [Z]=16
 - site C:** [Z]=24
 - site D:** [Z]=32
 - site E:** [Z]=40
 - site F:** [Z]=48
- Other Information:**
- OSPF are 200**
 - COUCHE CŒUR DE RESEAU**
 - COUCHE DISTRIBUTION**
 - COUCHE ACCES**
 - Region SUD, Site A ou B**
 - Region EST, Site C ou D**

5-Pistes de réflexions :

d) Réflexions n°4 : prise en compte Pare-feu

- fonctionnalités limitées sous Packet Tracer : équipement réel
 - SAÉ BUT1 abordant l'ASA5505 sous Packet Tracer
 - TP ASA5505 réel BUT2 dans le cadre de la SAÉ3.cyber.03 } **compétences pare-feu ASA = votre investissement !**
 - sécuriser la connexion entre son département et D – E – salle 409 (VPN IPSec)
 - sécuriser la connexion d'un collaborateur nomade extérieur (VPN SSL)
 - comment vérifier le fonctionnement du VPN IPSec et vers quels réseaux ?
 - comment vérifier le fonctionnement du VPN SSL depuis quel réseau ?
- uniquement si les connexions VPN fonctionnent :
 - comment permettre les connexions WiFi depuis la DMZ (droits, DHCP) ?
 - comment accéder au VLAN de gestion depuis l'extérieur sans risque ?
 - non pris en compte si VPN non opérationnels !**

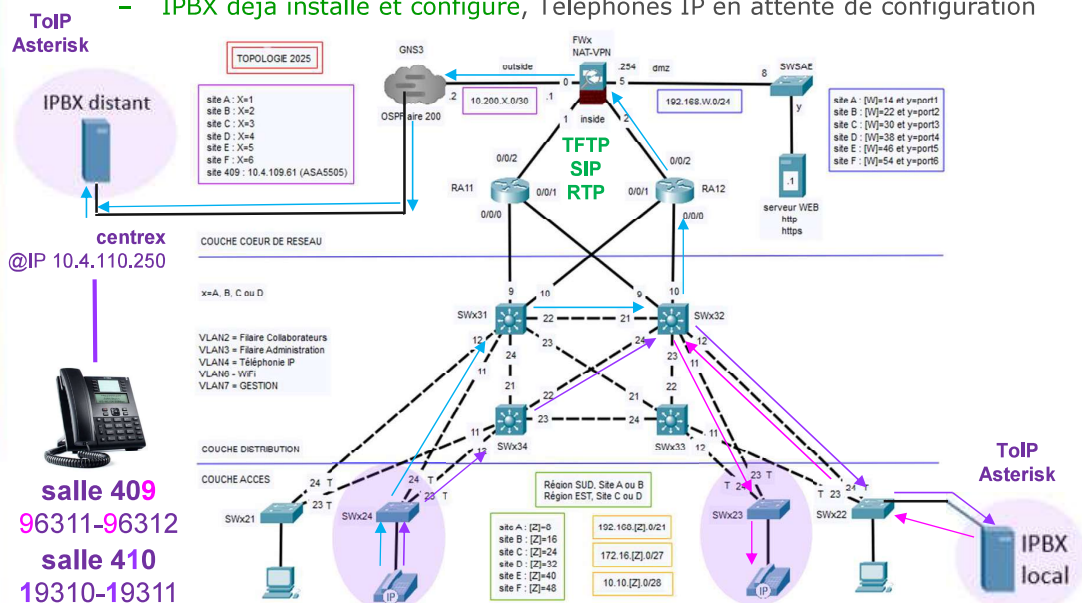
```
object network LAN-E
subnet 192.168.40.0 255.255.248.0
description reseau local dept-E
object network LAN-F
subnet 192.168.48.0 255.255.248.0
description reseau local dept-F
object network LAN-409
subnet 192.168.100.0 255.255.255.0
description paillasse prof salle 409
!
tunnel-group 10.200.5/6.1 type ipsec-l2l
tunnel-group 10.200.5/6.1 ipsec-attributes
ikev1 pre-shared-key SAEdept-xE/F
tunnel-group 10.4.109.166 type ipsec-l2l
tunnel-group 10.4.109.166 ipsec-attributes
ikev1 pre-shared-key SAEdept-x409
```



5-Pistes de réflexions :

e) Réflexions n°5 : intégration de la téléphonie IP

- prise en compte uniquement si les VPN sont opérationnels :
 - plusieurs Travaux pratiques sur téléphonie IP en BUT1
 - TP ToIP réel BUT2 dans le cadre de la SAÉ3.cyber.03 } **compétences Téléphonie IP = votre investissement !**
 - prendre en compte les aspects ToIP avec un IPBX Debian Asterisk
 - gérer les accès aux services distants : DHCP, DNS, NTP, TFTP (options dhcp)
 - comment communiquer avec « centrex » (IPBX distant) à travers le pare-feu ?
 - quel est le plan de numérotation des téléphones de l'ensemble des régions ?
- en pratique : essais en salle 408 après validation configurations
 - transmission des configurations IPBX et autres services à l'enseignant
 - IPBX déjà installé et configuré, Téléphones IP en attente de configuration



ToIP Asterisk

IPBX distant

centrex
@IP 10.4.110.250

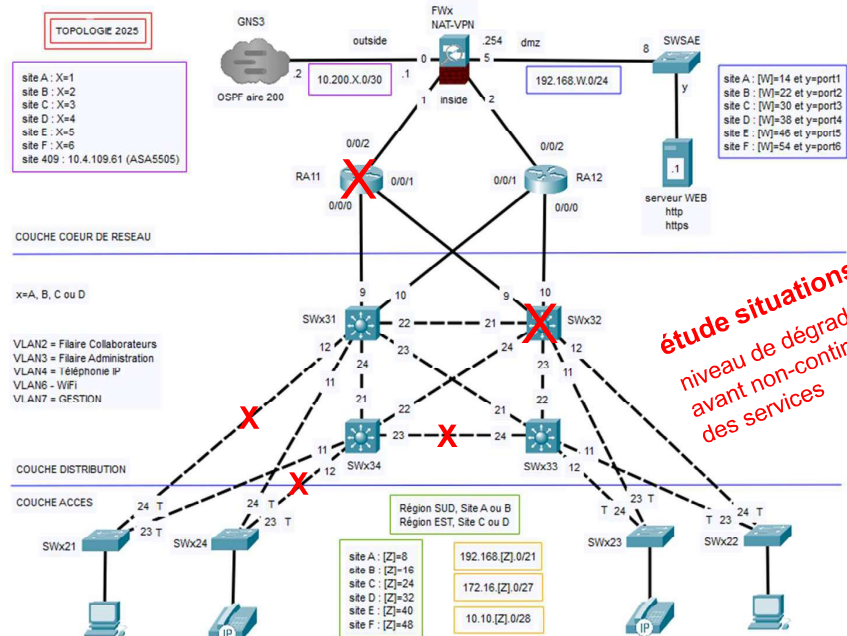
salle 409
96311-96312

salle 410
19310-19311

5-Pistes de réflexions :

f) Réflexions n°6 : robustesse de l'architecture

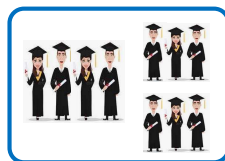
- test de l'efficacité de la redondance configurée :
 - connaissance des chemins empruntés par défaut par les différents flux
 - réaction de la convergence RSTP face aux **pannes**
 - réaction du routage interne et externe face aux **pannes**
 - conséquence sur l'équilibrage de charges initialement attendu
 - conséquence sur la disponibilité des services : DHCP, NTP, TFTP
 - quel est le niveau de dégradation maximum tolérable pour l'architecture ?
 - existante de pannes critiques ? Vers un déploiement de SNMP ?



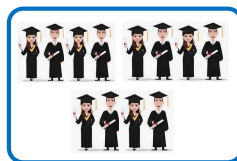
6-Organisation :

Contexte :

- seconde année BUTR&T avec 1 groupe TRAD et 1 groupe ALT
- groupe TRAD : jusqu'à 28 étudiants, soit deux groupes de TP
- groupe ALT : jusqu'à 28 étudiants, soit deux groupes de TP
- projet selon une répartition par équipe de 3 à 4 étudiants
- équipiers = obligation de se trouver dans le même groupe de TP



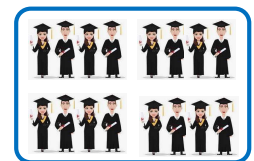
TP à 10 étudiants : 4-3-3



TP à 12 étudiants : 4-4-4



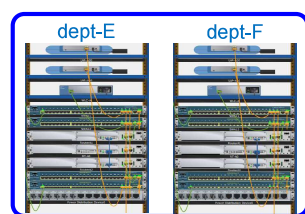
TP à 14 étudiants : 4-4-3-3



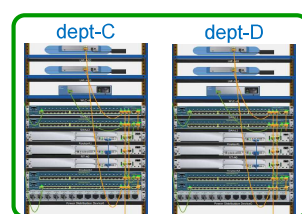
TP à 16 étudiants : 4-4-4-4

Répartition :

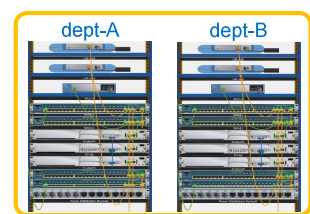
- au choix du responsable de la SAÉ dans le groupe de TP
- montrer sa capacité d'inclusion et d'enrichissement mutuel
- si problème d'assiduité en BUT1 = **interdiction d'intégrer une équipe de 3**
- savoir-être aussi important que le savoir-faire au sein d'une équipe
- affectation d'un site en gestion aux équipes par le responsable de la SAÉ
- jusqu'à **4 équipes présentes** simultanément dans l'entreprise



Région NORD = sites TESTS



Région EST : 3 x 2 équipes



Région SUD : 3x 2 équipes

Calendrier prévisionnel, objectifs intermédiaires :

séances encadrées

- s36 présentation de la SAÉ
- s37 complément cours
- s38 complément TP1 - ASA
- s39 complément TP2 - ToIP

s40 point d'étape n°1

Topologie Packet Tracer éprouvée et complètement opérationnelle !

s46 point d'étape n°2

point d'étape =
sur déclenchement de l'équipe
avancement et discussion
Négatif si non effectué !

s49 point d'étape n°3

1 janvier :
blocage des comptes
évaluation des connaissances
et des compétences

travail en autonomie et 21h à 30h planifiées selon groupe TP

- séance planifiée n°1
- séance planifiée n°2
- séance planifiée n°3
- séance planifiée n°4
- séance planifiée n°5
- séance planifiée n°6
- séance planifiée n°7
- séance planifiée n°8
- séance planifiée n°9
- séance planifiée n°10

brainstorming

PT~réalité

phase

étude

fichiers
configurations
épurés

fichiers
configurations
adaptés

phase

production

tests
fiabilité/sécurité
accès site distant

phase

enrichissement

plan d'@IP complet
fichiers configurations de tous équipements
fichier login/mot de passe utilisés
projet complet .pkt étude simulation

délivrables :
avant le 31 décembre

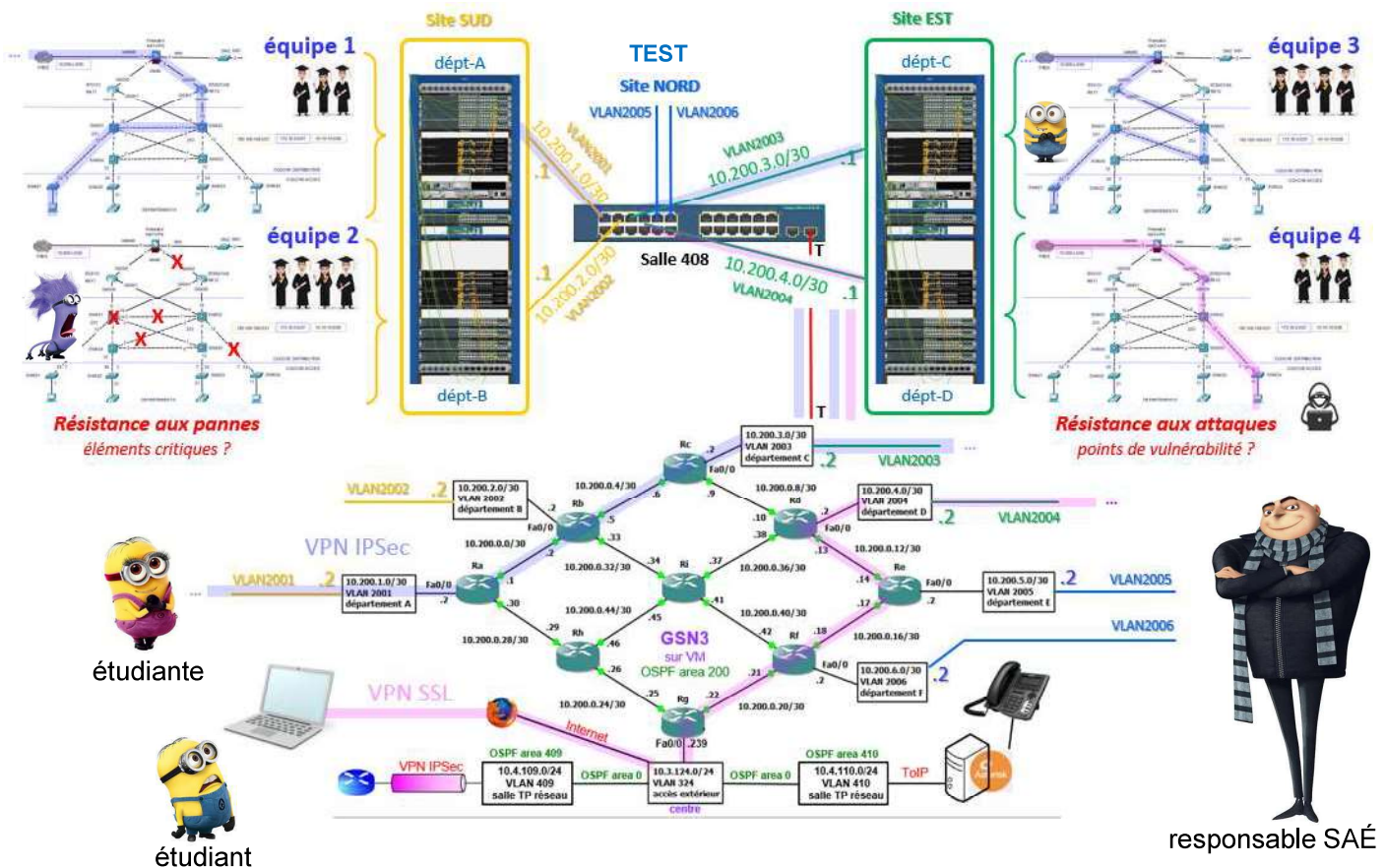
tests préalables :
accès depuis salles infos R&T
répartition injections config
présentation avec vidéoprojecteur
tous les fichiers sur compte UCA

**effet majeur avant
la Toussaint**



6-Organisation :

Résultats minimums attendus en production :

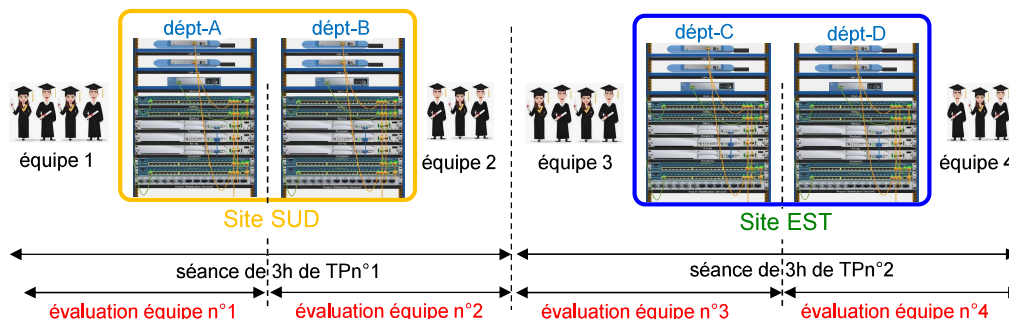


7-Evaluation :



Contexte : de l'équipe à l'individu dans la finalité d'un projet !

- évaluer la **motivation** d'un **travail de groupe** afin de finaliser le projet
- évaluer la **participation individuelle** à un projet collectif
- évaluer l'**appropriation** individuelle des **compétences techniques**
- évaluer le **degré d'autonomie individuelle** au sein de l'équipe
- Évaluer la **maîtrise individuelle de l'architecture multisite sécurisée**
- 6h d'évaluation par groupe de TP



Critères :

1/degre de finalisation du projet : 5 points (pas de dépannage !)

5 points :

site parfaitement fonctionnel, robuste et sécurisé, connexions VPN IPSec/SSL fonctionnelles, intégration de la ToIP et/ou accès DMZ.

3 points :

site parfaitement fonctionnel, robuste et sécurisé, connexions VPN IPSec, VPN SSL non fonctionnel.

1 point :

site partiellement fonctionnel, robuste et sécurisé, **Redondance non fonctionnelle.**

4 points :

site parfaitement fonctionnel, robuste et sécurisé, connexions VPN IPSec/SSL fonctionnelles, pas d'intégration de la ToIP et/ou accès DMZ.

2 points :

site parfaitement fonctionnel, robuste et sécurisé. Pas de VPN et/ou Redondance non fonctionnelle.

0 point :

site non fonctionnel ou non robuste ou non sécurisé ne respectant donc pas le CdC.

7-Evaluation :

-4pts

à fournir par l'équipe : avant 31 décembre

- fichier d'étude finalisée Packet Tracer
- plan d'adressage IP complet
- fichiers de configuration des équipements
- identifiant/mdp d'accès aux équipements

Critères :

2/évaluation de l'équipe : 7 points

- savoir se connecter sur sa topologie vierge ou non
- savoir réinitialiser, injecter ses configurations et tester en **-15 minutes**
- savoir présenter ses choix techniques (robuste, sécurité) en **10 minutes**
- savoir argumenter la gestion inclusive du projet en **5 minutes**



modulée par
motivation constatée
en points d'étape

3/évaluation individuelle : 8 points

- démontrer la maîtrise des notions techniques (réponses aux questions)
- démontrer sa connaissance globale de l'architecture réseau
- démontrer son aisance dans la configuration de l'architecture réseau
- réagir face à une panne au sein de l'architecture (méthodologie et alternative)
- évaluation du degré de participation de chacun au projet



7-Evaluation :

Principaux défauts des promotions précédentes

- non-respect des consignes données lors de la présentation :
 - un **investissement de départ** très en-dessous des consignes (effet majeur)
 - un **investissement qui débute à la Toussaint** (perte d'un mois et demi !)
 - utilisation d'**adresses IP non affectées** au département en gestion
 - **frontière commutation/routage** floue entraînant des erreurs de configuration
 - **approche ToIP ou WiFi** alors qu'**architecture** de production **non fonctionnelle**
 - **approche ASA** avec couches accès, distribution et cœur non fonctionnelles
 - pas de redondance du service DHCP
 - **pont racine** du RSTP **non pertinent** ou **identique pour tous les VLAN**
 - pas d'**influence des flux** au niveau RSTP pour **équilibre des charges**
 - pas de redondance fonctionnelle au niveau routage (**HSRP non fonctionnel**)
 - **tests de connectivité non fonctionnels** entre équipements sur **VLAN de gestion**
 - **tests de connectivité inter-VLAN non effectué** (routage inter-VLAN non testé)
 - **fichiers** configuration **perfectibles** (no shutdown, problème mdp crypté, clé SSH)
 - pas de test en **mode dégradé** de l'architecture afin de tester sa robustesse
 - des **points d'étape boudés** par bon nombre d'équipes (tant pis pour elles !)
- en pratique : lors de l'évaluation
 - tests d'injection depuis une salle informatique non évident pour tous
 - injection des configurations perfectibles (il reste des erreurs à traiter)
 - manque de coordination au sein de l'équipe (qui s'occupe de quel équipement)
 - présentation des choix techniques à l'image de la fonctionnalité de l'architecture
 - connaissance faible du fonctionnement de STP et de HSRP : **inadmissible** !
 - réponses aux pannes perfectibles montrant une architecture non éprouvée !
 - une répartition des rôles dans l'équipe pauvrement argumentée
 - manque d'un leader affirmé dans certaines équipes pour le succès du projet
 - un diagramme de Gantt qui ne garantit pas les délais et l'atteinte des objectifs
- comportement : après l'évaluation
 - **frustration** devant **sentiment d'effort** alors que compétences BUT1 non acquises
 - **sentiment d'être le meilleur** de l'équipe et de mériter plus que les autres

L'évaluation reflète un **travail d'équipe** ET la **capacité individuelle** à convaincre !

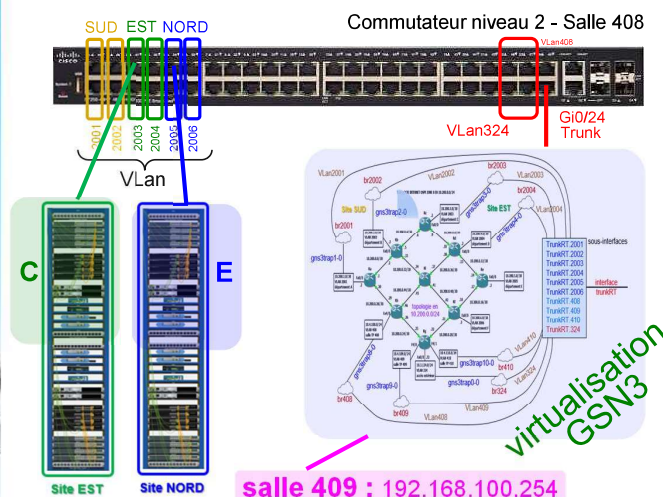
8-Démonstration :

Objectifs : étude puis production sur le site E

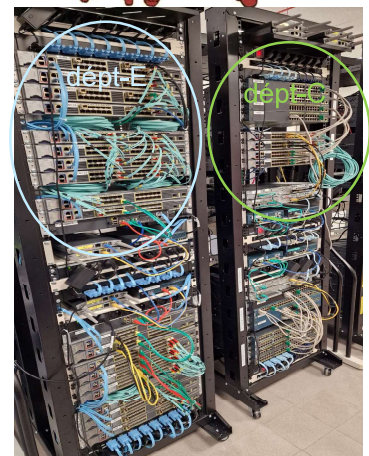
- configuration et tests sur Packet Tracer : **validation du fonctionnement**
- générer des fichiers de configuration simu sans erreur au chargement
- intégrer les différences entre équipements PT et équipements réels
- générer des fichiers de configuration réelle sans erreur au chargement
- configuration des équipements actifs réels sur le département E
- tester la connexion entre sites et l'accès SSH à tous les équipements
- connexion VPN vers site E et test VPN IPSec vers site F via GNS3

Contexte :

- région NORD, site-E, 6 VLAN à gérer
- @privées utilisateurs = 192.168.40.0/21
- @publics=10.200.5.0/30, Internet : .2



Un jeu d'enfant



9-Visite et questions :

Organisation pratique :

- visite des installations en salle 408 (niveau 4 R&T)
- groupe de 14 à 16 étudiants au maximum (sécurité des accès)
- **aucun bavardage, attitude sérieuse, conditions d'entreprise !**
- possibilité de prendre des photos sans flash
- **interdiction de toucher aux équipements actifs et aux câblages présents**
- **10 minutes par groupe**

Questions/échanges :

- durant la visite
- pertinentes et non redondantes
- prendre des notes

une situation d'apprentissage et d'évaluation



compétences

NON ACQUISES

ACQUISES

