

Documentation Infrastructure Réseau LAB Security

Sécurisation d'une infrastructure réseau

Objectif :

- Étude conceptuelle et mise en place d'un réseau avec élaboration d'un plan d'adressage optimisé et d'un plan de sécurité réseau

Table des matières

Table des matières

Introduction

Topologie et plan d'adressage du réseau

Topologie du réseau

Adressage IP et VLSM

Plan d'Adressage

Infrastructure des agences

Modèles routeurs et switch utilisés

Câblage

Réseau FAI

Analyse des besoins de sécurité

Définition de la sécurisation d'un réseau

Disponibilité

Protocole OSPF

Redondance via HSRP

Serveur de sauvegarde (**TFTP**)

VLAN

Configuration des Syslogs

Intégrité

ACL

Confidentialité

Mot de passe sur les équipements Cisco:

Tunnel VPN IPSEC

NAT

Port sécurisé sur les switch

Introduction

L'infrastructure réseau déployée repose sur une conception soigneusement élaborée pour répondre aux exigences spécifiques de connectivité, de redondance, et de sécurité au sein de notre organisation. Cette documentation vise à fournir un aperçu détaillé de l'architecture réseau, mettant en évidence des éléments clés tels que la redondance du service DHCP avec HSRP, l'utilisation du protocole OSPF pour un routage dynamique efficace, ainsi que la sécurisation et la mise en place du NAT pour l'accès à internet.

Notre approche repose sur une allocation judicieuse des adresses IP en utilisant la technique VLSM, garantissant une utilisation optimale des ressources tout en prévoyant l'évolutivité future. Pour chaque agence ont attribut une plage d'adresses IP distincte, avec une segmentation des réseaux locaux (LAN) pour une gestion efficace du trafic.

La présence de serveurs DHCP au sein de chaque LAN assure une attribution dynamique des adresses IP, tandis que la redondance est assurée par le protocole HSRP, garantissant la continuité du service même en cas de défaillance d'un routeur.

Le protocole OSPF est déployé pour permettre un routage dynamique, assurant une connectivité optimale entre les différentes agences. La liaison Internet est sécurisée via la translation d'adresse réseau (NAT), permettant aux agences d'accéder à Internet tout en maintenant une séparation claire entre les réseaux internes et externes.

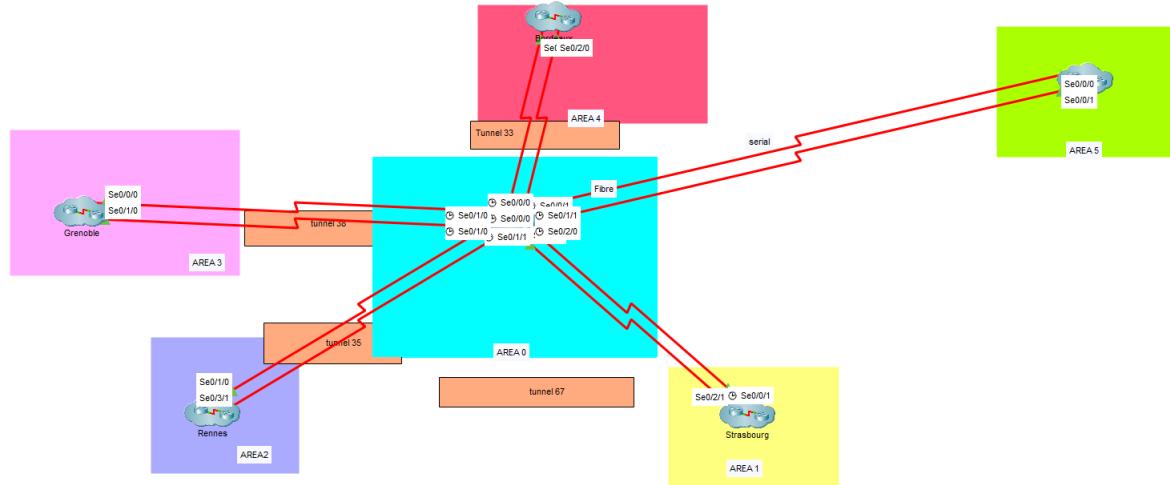
Cette documentation détaillée offre une vue approfondie de notre infrastructure réseau, allant des fondations; l'adressage IP à la mise en œuvre de protocoles de routage dynamique et de mécanismes de redondance. Elle servira de référence cruciale pour la gestion, la maintenance, et l'évolution continue de notre réseau, tout en répondant aux normes élevées de performance et de sécurité de notre organisation.

Topologie et plan d'adressage du réseau

Topologie du réseau

Le réseau est conçu avec une architecture intégrant quatre agences distinctes, à savoir Rennes, Strasbourg, Grenoble, et Bordeaux, toutes reliées à un routeur central basé au siège de la société, situé à Paris. Cette configuration spécifique vise à assurer une connectivité efficace tout en limitant les communications directes entre les agences. Chaque agence se voit attribuer une plage d'adresses IP unique, établissant ainsi une structure logique et ordonnée pour le réseau.

Le réseau du fournisseur d'accès à Internet (FAI) est intégré à la conception globale, se connectant au routeur central à Paris. Pour assurer une connectivité Internet sécurisée, la plage d'adresses IP 20.6.4.0/30 et 20.6.3.0/30 est réservée à cette liaison.



Adressage IP et VLSM

Notre réseau est conçu selon l'architecture d'adressage IP basée sur la méthode de VLSM (Variable Length Subnet Mask). Cette approche permet une utilisation efficace des adresses IPv4 en attribuant des plages de tailles variables à différents sous-réseaux. Cette stratégie nous permet de répondre de manière spécifique aux besoins de chaque agence tout en préservant une gestion rationnelle de l'espace d'adressage. En adoptant une approche VLSM, nous nous assurons également de faire preuve d'économie d'adresses IP en adaptant la taille des sous-réseaux en fonction du nombre réel d'hôtes nécessaires. Ainsi, notre réseau s'ajuste dynamiquement pour optimiser l'utilisation des adresses IP, garantissant une allocation efficiente des ressources tout en répondant de manière précise aux exigences spécifiques de chaque segment du réseau.

Plan d'Adressage

AGENCE	NOMBRE D'HÔTES REQUIS TOTAL	LAN1	HÔTES DISPO1	LAN2	HÔTES DISPONIBLE	HÔTES DISPONIBLE TOTAL
Rennes	320	172.16.4.0/24	254	172.16.3.0/25	126	380
Strasbourg	527	172.16.0.0/23	510	172.16.2.0/27	30	557
Grenoble	160	172.16.8.0/25	126	172.16.9.0/25	126	252
Bordeaux	560	172.16.7.0/26	62	172.16.5.0/23	510	572
Paris		172.16.10.0/24 172.16.11.0/24 172.16.12.0/24 172.16.13.0/24 172.16.14.0/24				
FAI		20.6.4.0/30 20.6.3.0/30		20.6.4.0/30		

LAN DE PARIS	Adresses IP	HÔTES DISPONIBLE TOTAL
COM	172.16.11.0/24	254
RH	172.16.10.0/24	254

INFORMATIQUE	172.16.14.0/24	254
COMPTA	172.16.12.0/24	254
PATRIMOINE IMMO	172.16.13.0/24	254

La conception du réseau implique également la création de sous-réseaux spécifiques à partir du réseau 172.16.0.0/8 pour les réseaux locaux (LAN) de chaque agence, garantissant ainsi une segmentation efficace des réseaux internes. En favorisant une connectivité centralisée entre les agences par le biais du routeur à Paris, cette architecture offre une gestion optimisée du trafic tout en répondant aux exigences de sécurité et d'efficacité propres à l'organisation. Ce modèle assure également une flexibilité pour une expansion future tout en maintenant une structure de réseau organisée et documentée.

Infrastructure des agences

Modèles routeurs et switch utilisés

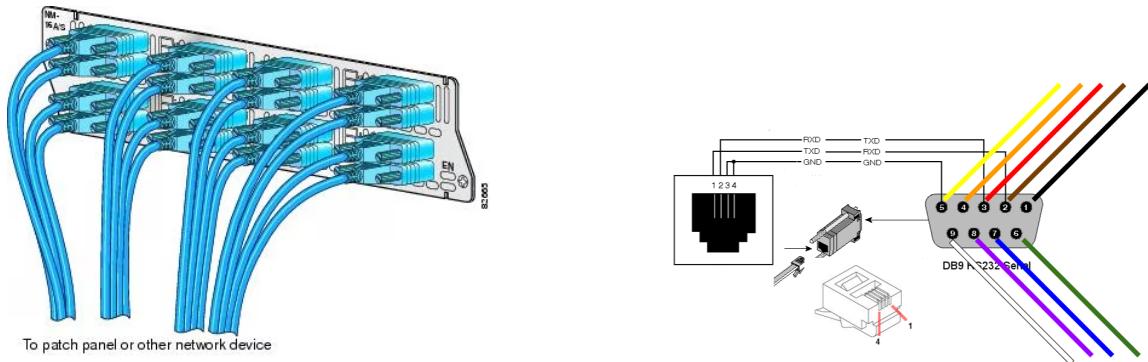
Pour cette infrastructure nous allons utiliser les 10 routeurs (sans compter le FAI) 2911 et 19 switch (sans compter le FAI) 2960-24TT.



Câblage

Dans notre projet, nous avons mis en place une infrastructure réseau robuste en utilisant des câbles croisés pour relier les switchs entre eux et les routeurs entre eux. Les liaisons directes entre les switchs et les PC, ainsi qu'entre les switchs et les routeurs, sont établies à l'aide de câbles droits.

En outre, pour assurer la connectivité entre chaque site distant et Paris, ainsi que la liaison entre Paris et le fournisseur d'accès Internet (FAI), nous avons déployé des connexions Serial DCE. Cette approche diversifiée garantit une gestion optimale des flux de données, assurant une performance et une fiabilité accrues dans l'ensemble du réseau.



Le protocole DHCP (Dynamic Host Configuration Protocol) est essentiel au sein de notre infrastructure réseau pour la gestion dynamique des adresses IP attribuées aux dispositifs connectés, offrant une solution automatisée et évolutive. Les serveurs DHCP jouent un rôle central dans ce processus, facilitant la configuration réseau des clients de manière efficace. Les serveurs DHCP, configurés dans chaque agence, répondent aux requêtes des clients en attribuant de manière dynamique des adresses IP, simplifiant ainsi la configuration réseau.

PARIS Master :

```

ip dhcp pool VLAN_SERVEUR
network 172.16.14.0 255.255.255.0
default-router 172.16.14.254
dns-server 10.10.10.4

ip dhcp pool PARTIMOINE_IMMO
network 172.16.13.0 255.255.255.0
default-router 172.16.13.254
dns-server 10.10.10.4

ip dhcp pool COM
network 172.16.11.0 255.255.255.0
default-router 172.16.11.254
dns-server 10.10.10.4

ip dhcp pool RH
network 172.16.10.0 255.255.255.0
default-router 172.16.10.254
dns-server 10.10.10.4

ip dhcp pool COMPTA
network 172.16.12.0 255.255.255.0
default-router 172.16.12.254
dns-server 10.10.10.4

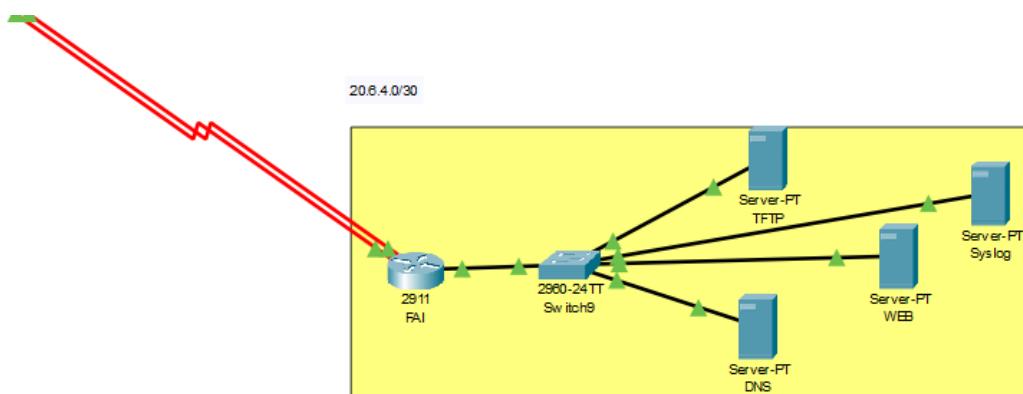
```

Réseau FAI

Dans le cadre de notre infrastructure, nous avons déployé plusieurs serveurs essentiels pour simuler le réseau Internet. Ces serveurs, incluant DNS, WEB, et TFTP, qui sont soigneusement configurés au sein du réseau du fournisseur d'accès Internet (FAI) avec une plage d'adresses IP définie comme "20.6.4.0/30" et "20.6.3.0/30".

Notre serveur WEB particulier, dédié à l'hébergement d'un site intitulé "LAB Security", est attribué avec l'adresse IP "20.6.4.1". Pour garantir la résolution DNS de manière réaliste, ce serveur est associé à un nom de domaine fourni par notre serveur DNS, dont l'adresse IP est "20.6.4.2". En parallèle, notre serveur TFTP, qui facilite le transfert de fichiers, à l'adresse IP "20.6.4.3".

Cette configuration permet de reproduire un environnement réseau authentique, nous permettant de simuler des services cruciaux tels que la résolution DNS, l'hébergement web, et le transfert de fichiers via TFTP. Ces choix tactiques d'adresses IP et de noms de domaine contribuent à établir une structure réseau cohérente et efficace pour nos besoins de simulation.



Analyse des besoins de sécurité

Définition de la sécurisation d'un réseau

- Disponibilité :** La disponibilité dans le contexte de la sécurisation informatique implique la mise en place de mesures pour garantir un accès constant et fiable aux ressources informatiques. Cela peut être réalisé grâce à la mise en place de systèmes de sauvegarde, de redondance de serveurs, et de mécanismes de gestion de la charge. L'objectif est d'assurer que les utilisateurs autorisés peuvent accéder aux applications, aux systèmes ou aux données sans interruption, même en cas de défaillance d'un composant.
- Confidentialité :** La confidentialité vise à protéger l'information contre un accès non autorisé. Cela implique souvent le chiffrement des données sensibles, la mise en place de contrôles d'accès stricts et la surveillance constante pour détecter toute tentative d'accès non autorisé. L'objectif est de s'assurer que seules les personnes ayant les autorisations nécessaires peuvent accéder à des informations sensibles, préservant ainsi la confidentialité et évitant les fuites d'informations.
- Intégrité :** L'intégrité concerne la protection contre toute altération non autorisée des données. Cela peut être réalisé par le biais de techniques telles que le hachage et la signature numérique. Le hachage est utilisé pour vérifier l'intégrité des données en générant une empreinte unique pour un ensemble de données, tandis que la signature numérique utilise des clés cryptographiques pour garantir l'authenticité et l'intégrité des données pendant la transmission. L'objectif est de s'assurer que les données ne sont pas modifiées de manière non autorisée, que ce soit lors de leur transit à travers le réseau ou lors de leur stockage.

En combinant ces trois aspects, les professionnels de la sécurité informatique cherchent à créer un environnement où les utilisateurs autorisés ont un accès fiable aux données confidentielles et peuvent être assurés que ces données n'ont pas été altérées de manière non autorisée. Cela contribue à maintenir la confiance dans l'utilisation des systèmes informatiques et des réseaux.

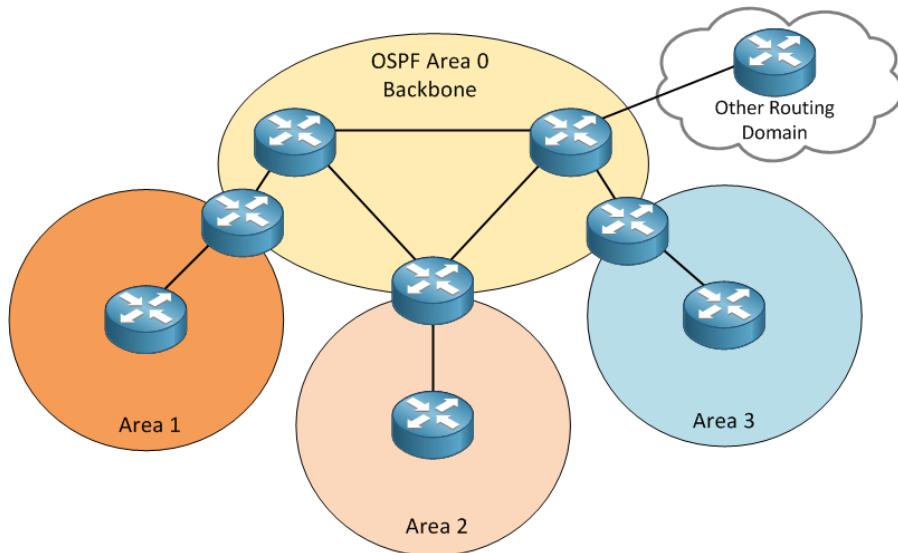


Disponibilité

Protocole OSPF

La mise en œuvre du protocole OSPF (Open Shortest Path First) au sein de notre infrastructure réseau constitue un élément essentiel pour garantir un routage dynamique efficace. OSPF, en tant que protocole de routage à état de lien, offre une convergence rapide en ajustant dynamiquement les chemins en fonction de la topologie réseau. Chaque routeur OSPF partage des informations sur les liaisons avec ses pairs, permettant la construction d'une table de routage actualisée. Cette approche dynamique favorise une utilisation optimale des chemins disponibles, améliorant la résilience du réseau face aux changements de topologie. La hiérarchisation des zones OSPF permet de segmenter logiquement le réseau, facilitant la gestion et réduisant la charge de calcul liée au routage. De plus, OSPF offre des mécanismes d'authentification pour sécuriser les échanges entre routeurs. Dans l'ensemble, l'implémentation d'OSPF contribue à une connectivité robuste et adaptative au sein de notre infrastructure, répondant aux besoins de scalabilité, d'efficacité, et de sécurité du réseau.

Pour renforcer la sécurité de notre réseau nous avons mis en place l'authentification avec un mot de passe. Cela permettra d'exiger une authentification entre les routeurs avant qu'ils ne partagent des informations de routage.



PARIS Master :

```
router ospf 10
log adjacency-changes
area 0 authentication message-digest
network 172.16.38.0 0.0.0.7 area 0
network 20.6.4.0 0.0.0.7 area 0
network 172.16.33.0 0.0.0.7 area 0
network 172.16.35.0 0.0.0.7 area 0
network 172.16.67.0 0.0.0.7 area 0
network 172.16.10.0 0.0.0.255 area 0
network 172.16.11.0 0.0.0.255 area 0
network 172.16.12.0 0.0.0.255 area 0
network 172.16.13.0 0.0.0.255 area 0
network 172.16.14.0 0.0.0.255 area 0
```

Rennes Backup :

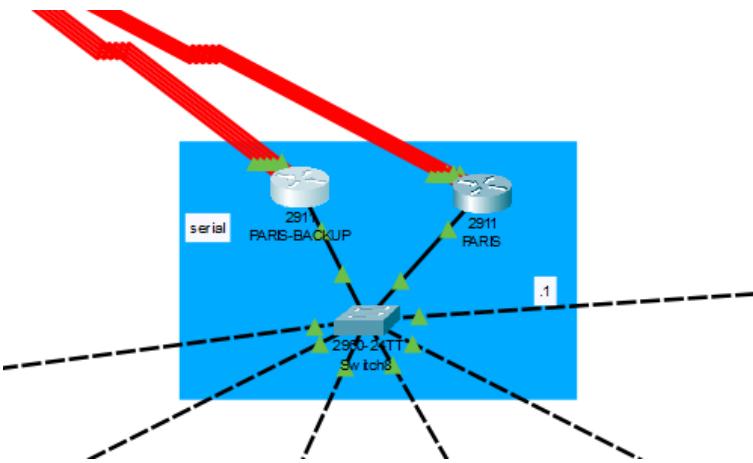
```
router ospf 4
log adjacency-changes
network 172.16.4.0 0.0.0.255 area 2
network 172.16.3.0 0.0.0.127 area 2
network 172.16.35.0 0.0.0.7 area 0
```

Redondance via HSRP

HSRP (Hot Standby Router Protocol) est un protocole de premier hop de redondance (FHRP) utilisé pour assurer la redondance et la haute disponibilité en créant une adresse IP virtuelle qui sera la passerelle par défaut. Dans notre infrastructure, nous avons un routeur principal (Master) et un routeur de secours (backup). Ces deux routeurs sont configurés avec une adresse IP virtuelle que nous avons créée. Par la suite, le routeur de secours envoie des requêtes au routeur principal. Si celui-ci ne répond pas, le routeur de secours devient le routeur principal. Par ailleurs, pour cette configuration, nous avons défini une priorité de 105 pour les routeurs principaux et de 100 pour les routeurs

de secours (priorité par défaut). Enfin, nous avons configuré dans le service DHCP les adresses IP virtuelles comme "Default Gateway".

Enfin nos deux routeurs ont exactement la même configuration pour que en cas de bascule la disponibilité reste intacte.



PARIS Master:

```
standby 10 ip 172.16.10.254
standby 10 priority 105
standby 10 preempt
standby 10 track GigabitEthernet0/0
```

PARIS Backup:

```
standby 10 ip 172.16.10.254
standby 10 preempt
standby 10 track GigabitEthernet0/0
```

Serveur de sauvegarde (TFTP)

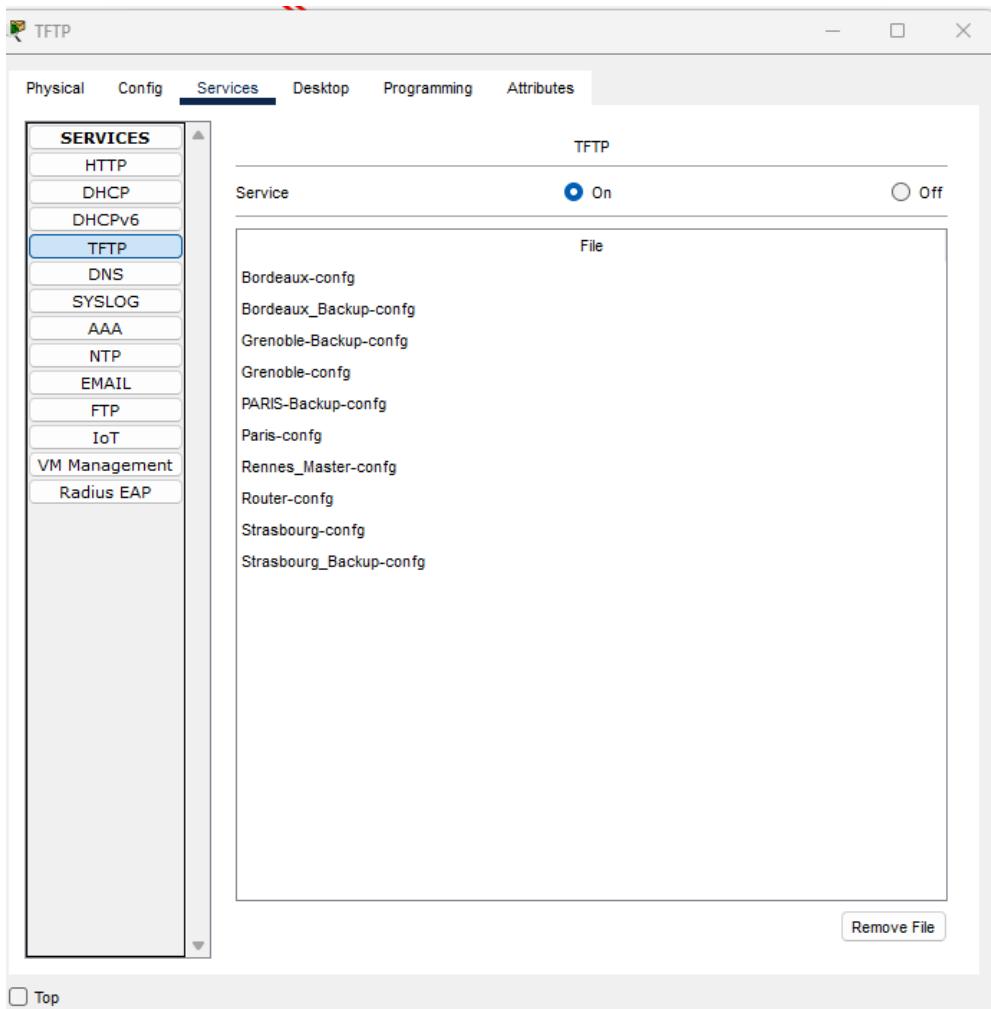
Le Trivial File Transfer Protocol nous donne la possibilité de transférer nos configurations réseaux (switch et routeurs) vers un serveur. Notre serveur TFTP est situé dans le FAI protégeant nos données d'une corruption réseau potentiel au siège (Paris).

TFTP utilisant le protocole UDP, il nécessite moins de mémoire et de programmation que le FTP.

Cette configuration nous permet d'assurer une disponibilité de la configuration Switch et Routeur.

Il est important de posséder un système de sauvegarde pour protégé la configuration réseau de l'entreprise.

Si un routeur tombe en panne par exemple, nous pourrons récupérer toute la configuration sur le serveur et faciliter la configuration d'une nouvelle machine.



VLAN

Un Virtual Local Area Network, est une technique de segmentation d'un réseau. Il permet de diviser un réseau local en plusieurs segments logiques, même s'ils sont physiquement connectés au même réseau. Chaque VLAN, agit comme s'il était un réseau distinct.

Dans notre infrastructure nous avons créer plusieurs VLAN à PARIS pour segmenté les Métiers : VLAN COM, RH, SERVEUR, COMPTA, PATRIMOINE_IMMO.

Les VLAN porte le numéro de leur sous réseau, exemple VLAN COMPTA = VLAN
12 car 172.16.12.0/24.

Par conséquent pour les interfaces virtuelles sur les routeurs la logique reste la même.

```
interface GigabitEthernet0/0.12
encapsulation dot1Q 12
ip address 172.16.12.1 255.255.255.0
```

Pour des raisons de sécurité, seules les interfaces en directions des routeurs (Switch → Routeur) sont en mode Trunk (seuls les vlan 10 à 14 sont autorisés) le reste est en mode access.

SWITCH dans le VLAN COMPTA:

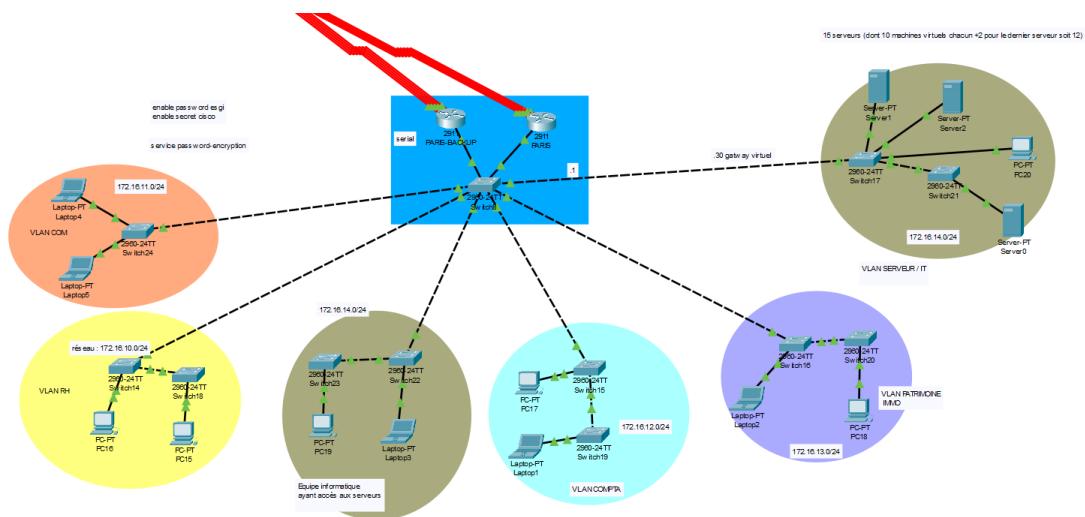
```
interface FastEthernet0/1
switchport access vlan 12
switchport mode access
```

SWITCH entre les ROUTEUR:

```
interface GigabitEthernet0/1
switchport trunk allowed vlan 10-14
switchport mode trunk

interface GigabitEthernet0/2
switchport trunk allowed vlan 10-14
switchport mode trunk

interface FastEthernet0/1
switchport access vlan 10
switchport mode access
```



Configuration des Syslogs

Les syslog sont des messages de journalisation qui contiennent des informations sur divers événements, activités, erreurs et états de fonctionnement des composants du système. Cela permet de maintenir la disponibilité grâce aux informations importantes que renferment les syslog, facilitant ainsi la surveillance, la détection d'incidents et la réponse aux événements de sécurité. Dans notre configuration, tout comme pour les sauvegardes TFTP, nos syslog sont envoyés à un serveur dédié dans notre réseau FAI (Fournisseur d'Accès Internet).

Enfin il est important de configurer des syslog pour pouvoir comprendre et résoudre des problèmes liés au réseau plus rapidement.

Syslog

Physical Config Services Desktop Programming Attributes

Syslog			
Service		On	Off
	Time	HostName	Message
1	03.01.1993 12:00:37.473 AM	20.6.3.2	%HSRP-6-STATECHANGE: ...
2	03.01.1993 12:00:39.582 AM	172.16.35.2	%HSRP-6-STATECHANGE: ...
3	03.01.1993 12:00:39.663 AM	20.6.3.2	%HSRP-6-STATECHANGE: ...
4	03.01.1993 12:00:40.490 AM	172.16.35.2	00:00:40: %OSPF-5-ADJCH...
5	03.01.1993 12:00:40.516 AM	172.16.35.1	00:00:40: %OSPF-5-ADJCH...
6	03.01.1993 12:00:40.525 AM	20.6.4.2	00:00:40: %OSPF-5-ADJCH...
7	03.01.1993 12:00:40.525 AM	20.6.3.2	00:00:40: %OSPF-5-ADJCH...
8	03.01.1993 12:00:40.991 AM	20.6.3.2	%HSRP-6-STATECHANGE: ...
9	03.01.1993 12:00:41.067 AM	172.16.35.2	%HSRP-6-STATECHANGE: ...
10	03.01.1993 12:00:41.068 AM	20.6.3.2	%HSRP-6-STATECHANGE: ...
11	03.01.1993 12:00:45.007 AM	20.6.4.2	00:00:45: %OSPF-5-ADJCH...
12	03.01.1993 12:00:45.034 AM	20.6.3.2	00:00:45: %OSPF-5-ADJCH...
13	03.01.1993 12:00:45.093 AM	20.6.4.2	00:00:45: %OSPF-5-ADJCH...
14	03.01.1993 12:00:45.115 AM	20.6.3.2	00:00:45: %OSPF-5-ADJCH...
15	03.01.1993 12:00:45.435 AM	20.6.4.2	00:00:45: %OSPF-5-ADJCH...
16	03.01.1993 12:00:45.445 AM	20.6.3.2	00:00:45: %OSPF-5-ADJCH...

Top

```
Routeur(config)# logging on
Routeur(config)# logging trap debug
Routeur(config)# logging hst 10.10.10.5
```

Intégrité

ACL

Une "access list étendue" (ACL étendue) est une liste de contrôle d'accès qui offre des fonctionnalités de filtrage plus avancées par rapport aux ACL standard (ne liste de contrôle d'accès utilisée pour filtrer le trafic réseau en fonction des adresses IP sources). Les ACL étendues permettent de spécifier des critères plus détaillés pour filtrer le trafic en fonction d'une variété de paramètres tels que les adresses IP source et destination, les numéros de port, les protocoles, etc.

Les access list étendue mise en place dans notre infrastructure, permettent d'autoriser seulement les ports : 443, 80, 69 et 21 sur les serveurs 172.16.14.3-5.

Seuls les employés dans le domaine de l'IT (VLAN SERVEUR -172.16.14.0/24) peuvent avoir un accès complet aux serveurs. Ce choix consiste à maintenir l'intégrité du réseau en protégeant nos serveurs d'une intrusion ou les autres attaques potentiels. Il serait facile par exemple de changer les prix depuis nos serveurs WEB sans ces restrictions. Il est important de noter qu'une access list bloque tout par défaut, nous avons donc créer des règles "permit" pour autoriser les machines à communiquer entre elles. Autrement dit le réseau 172.16.13 peut communiquer avec le réseau 172.16.11, cependant ils ne peuvent toujours pas communiquer avec 172.16.14.3 en SSH (port 22).

Enfin les access list sont appliquées sur toutes les interfaces en "in".

PARIS Master :

```
access-list 101 deny tcp any host 172.16.14.3 eq 22
access-list 101 deny icmp any host 172.16.14.3
access-list 101 deny tcp any host 172.16.14.4 eq 22
access-list 101 deny icmp any host 172.16.14.4
access-list 101 deny tcp any host 172.16.14.5 eq 22
access-list 101 deny icmp any host 172.16.14.5
access-list 101 permit ip 172.16.14.0 0.0.0.255 172.16.14.0 0.0.0.255
access-list 101 permit ip any any
```

Confidentialité

Mot de passe sur les équipements Cisco:

Afin de nous protéger de toutes personnes malveillante, nous avons configuré un mot de passe sur nos équipement (switch et routeurs). Ce mot de passe est demandé lorsque l'on rentre dans le mode EXE privilégié, donc aucune configuration n'est possible sans. Le mot de passe permet aussi de rallonger la possibilité d'un hacker de s'introduire au sein de notre infrastructure. De plus les mots de passes sont stockés sous forme de HASH (chiffrement en MD5 et 7 qui utilise un algorithme d'obfuscation).

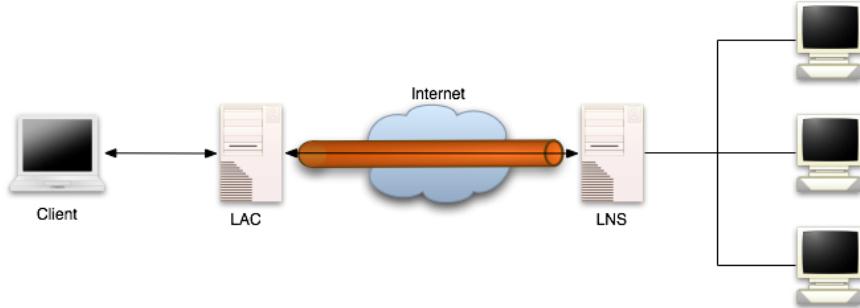
PARIS Master :

```
enable secret 5 <Hash_password>
enable password 7 08245F4900
```

Tunnel VPN IPSEC

L'IPSec, ou Internet Protocol Security, est une technologie de sécurisation des communications réseau opérant à la couche 3 du modèle OSI, compatible avec IPv4 et IPv6. Fondamental pour la sécurité des datagrammes IP, il intègre l'authenticité, l'authentification, et le chiffrement des données. En position basse du modèle OSI, il sécurise diverses applications et protocoles basés sur IP, avec une utilisation répandue pour déployer des réseaux VPN à grande échelle via Internet. Les aspects techniques de l'IPSec reposent sur les mécanismes AH (Authentication header) et ESP (Encapsulating Security Payload), permettant des configurations personnalisées en termes d'algorithme de hachage et de chiffrement. La gestion des flux IPSec s'effectue à travers les bases de données SPD et SAD, avec une approche unidirectionnelle et une distinction entre Security Policy (SP) et Security Association (SA). Deux modes d'utilisation, Transport et Tunnel, offrent des options flexibles pour sécuriser les connexions point à point ou créer des

tunnels entre réseaux distants. En parallèle, le protocole ISAKMP facilite la négociation des associations de sécurité, permettant ainsi l'établissement sécurisé de connexions IPSec.

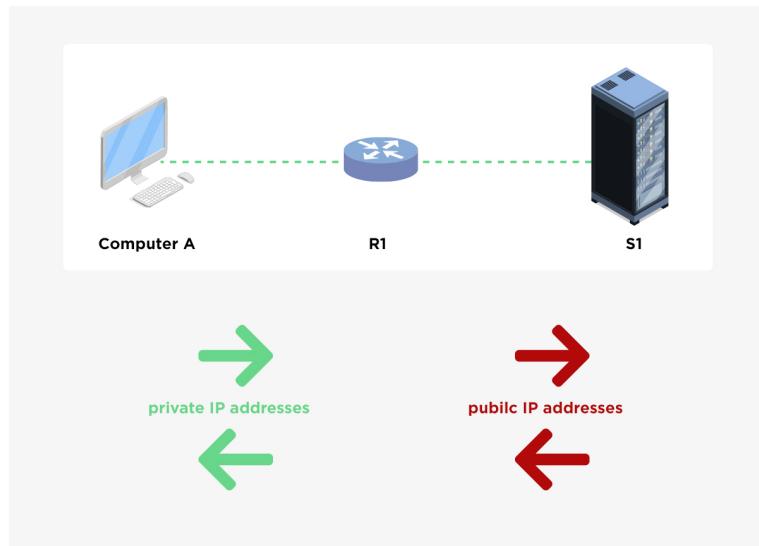


```
Grenoble (config)#crypto isakmp enable
Grenoble (config)#crypto isakmp policy 10
Grenoble(config-isakmp)# encr aes
Grenoble(config-isakmp)# authentication pre-share
Grenoble(config-isakmp)# group 2
Grenoble (config)# crypto isakmp key cisco address 172.16.38.4
```

Notre infrastructure est composé de plusieurs sites distants mais possède plusieurs interconnexions. nous avons donc décidé d'utilisé des tunnels VPN (type de VPN ?) entre nos différents sites ce qui nous permet un chiffrement des données et d'éviter les attaques comme le man in the middle. (cette attaque permet à un hacker de récupéré les paquets et alors d'écouter la communication entre l'envoi et la réception. Ce même hacker se fait passer pour le destinataire ou expéditeur pour paraître indétectable.)

NAT

Le Network Address Translation est une technique fréquemment utilisée en réseaux pour reconfigurer les adresses IP des appareils au sein d'un réseau privé de manière à ce qu'ils soient associés à une seule adresse IP publique. Dans notre infrastructure, nous avons mis en place une configuration NAT spécifique pour le réseau Lab-security, attribuant les plages d'adresses IP 20.6.4.0/30 et 20.6.3.0/30 pour les communications sortantes, puis les mapper vers notre FAI. Par ailleurs, nous avons également effectué une redirection de ports (443, 53 et 69) afin de permettre aux machines du réseau interne d'accéder aux services spécifiques hébergés sur les serveurs du FAI.
le NAT est généralement utilisé pour masquer les adresses IP internes, fournissant ainsi une couche de confidentialité en modifiant les adresses IP lorsqu'elles traversent nos routeurs vers Internet.



```

ip nat inside source static tcp 10.10.10.3 443 20.6.4.1 443
ip nat inside source static tcp 10.10.10.3 443 20.6.3.1 443
ip nat inside source static udp 10.10.10.4 53 20.6.4.1 53
ip nat inside source static udp 10.10.10.4 53 20.6.3.1 53
ip nat inside source static udp 10.10.10.2 69 20.6.3.1 69
ip nat inside source static udp 10.10.10.2 69 20.6.4.1 69

interface Serial 0/0/0
ip nat outside

interface Gigethernet 0/0
ip nat inside

```

Port sécurisé sur les switch

La sécurisation de Port est mis à part car elle concerne les trois piliers de la sécurité.

- **Intégrité** : La fonction Port Security assure l'intégrité des adresses MAC autorisées sur un port spécifique. Elle permet de restreindre l'accès aux adresses MAC définies, évitant ainsi des changements non autorisés.
- **Disponibilité** : En restreignant l'accès aux adresses MAC autorisées, Port Security contribue à maintenir la disponibilité du réseau en évitant les interférences et les atteintes à la sécurité qui pourraient résulter de l'accès non autorisé.
- **Confidentialité** : Bien que la principale fonction de Port Security soit liée à l'intégrité, elle peut également contribuer à la confidentialité en restreignant l'accès aux adresses MAC spécifiques autorisées, empêchant ainsi l'accès non autorisé à certaines parties du réseau.

Dans notre cas le « port-security » a été activé au sein de notre Vlan Serveur, il vise à sécuriser nos ports sur lesquels sont branché nos machines / serveurs sensibles, afin de limiter à UNE seul adresse MAC par port ce qui permet en cas de « spoofing » de port de shutdown les interfaces associés.

SWITCH VLAN 14 à PARIS:

```
interface FastEthernet0/5
switchport access vlan 14
switchport mode access
switchport port-security
switchport port-security mac-address 0004.9A82.592B
```