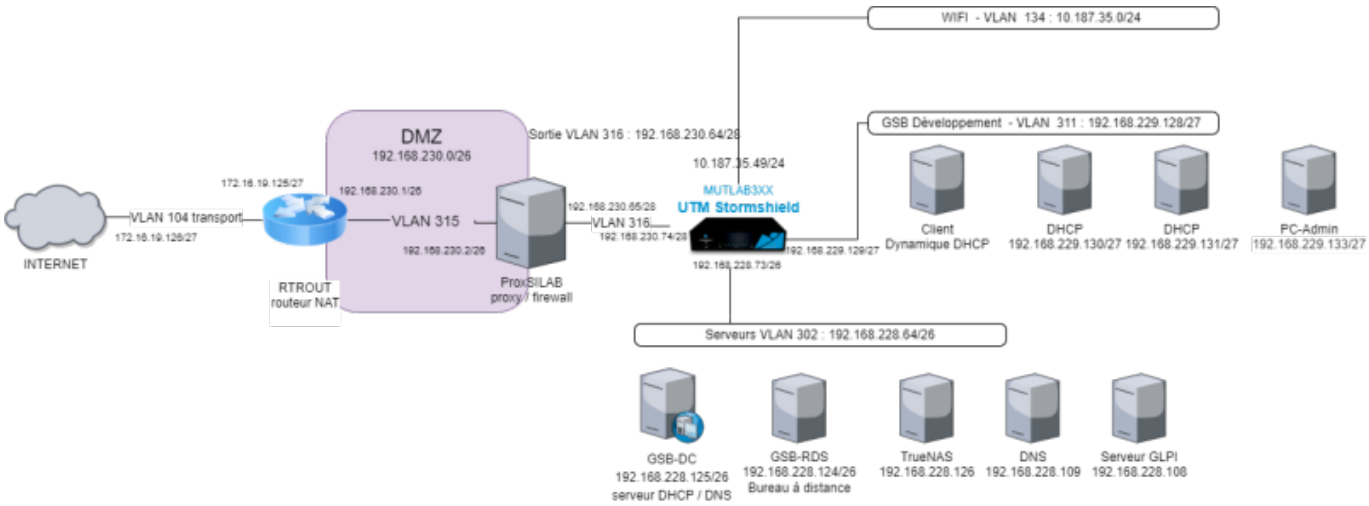
Documentation technique

Schéma d'adressage:



Plan d'adressage pour le VLAN 311 Développement 192.168.229.128/27:

Service(s)	**Adressage IP**
Passerelle (IN SNS)	192.168.229.129/27
DHCP 1	192.168.229.130/27
DHCP 2	192.168.229.131/27
PC-Admin	192.168.229.133/27
Serveur FreeRadius	192.168.229.134/27
Serveur Centreon)	192.168.229.135/27
Serveur Linux (NAS)	192.168.229.136/27
Plage d'adresses DHCP	192.168.229.140/27 - 192.168.229.150/27
Cluster Web	192.168.229.151/27
Serveur Web2	192.168.229.152/27

Plan d'adressage pour le VLAN 302 Serveur 192.168.228.192/26:

Service(s)	**Adressage IP**
Passerelle (DMZ1 SNS)	192.168.228.73/26
Serveur Web1 / GLPI	192.168.228.108/26
DNS	192.168.228.109/26
Contrôleur de domaine	192.168.228.110/26

Configuration Switch :

Accès telnet depuis le réseau wifi:

```
telnet 10.187.35.33
```

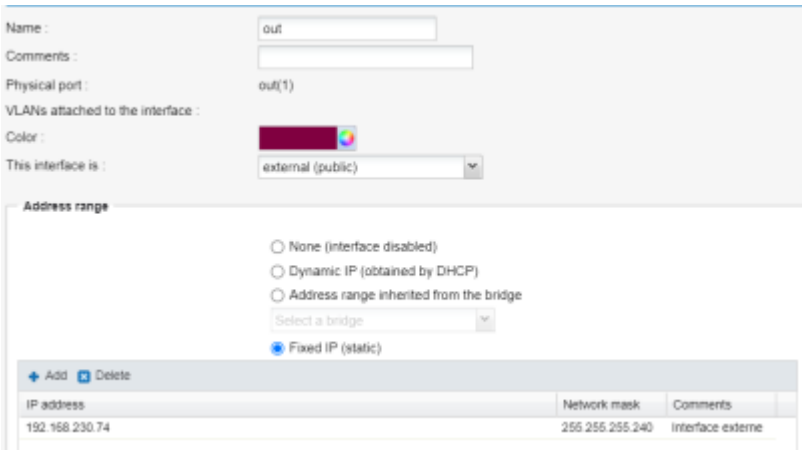
Interface	Type	ID	Commentaire
interface FastEthernet0/1	VLAN	316	Sortie
interface FastEthernet0/2	VLAN	311	Utilisateurs
interface FastEthernet0/3	VLAN	302	Serveurs
interface FastEthernet0/4	VLAN	134	Wifi-Byod
interface FastEthernet0/5	VLAN	352	BTS SIO
interface FastEthernet0/6	VLAN	311	Utilisateurs
interface FastEthernet0/7	VLAN		1
interface FastEthernet0/8	VLAN		1
interface GigabitEthernet0/1	Trunk	-	Trunk pour les cinq VLAN Sortie, Utilisateur, Serveurs, Wifi-BYOD, BTS SIO

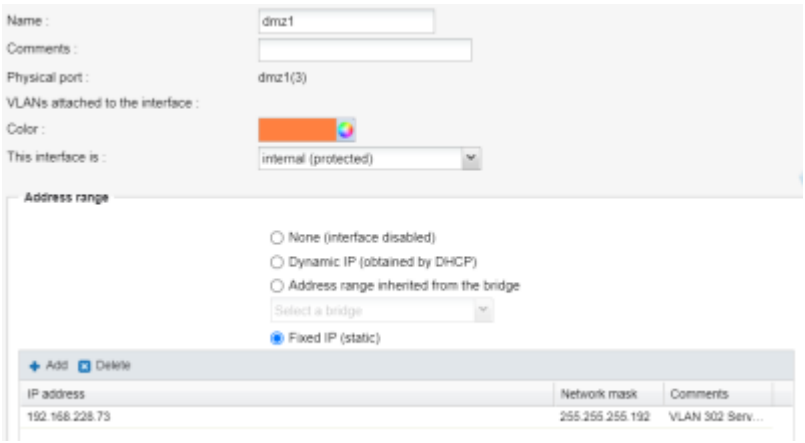
Voir Fichier Texte Configuration Switch

Configuration Pare-Feu StormShield:

Adressage des interfaces du Pare-Feu:

Interface	VLAN	Adresse
interface OUT	316 Sortie	192.168.230.74/28
interface IN	311 Développement	192.168.229.129/27
interface DMZ1	302 Serveurs	192.168.228.73/26
interface DMZ2	134 Wifi	10.187.35.49/24
interface DMZ3	Bridge	10.0.0.0/16
interface DMZ4	Bridge	10.0.0.0/16
interface DMZ5	Bridge	10.0.0.0/16
interface DMZ6	Bridge	10.0.0.0/16



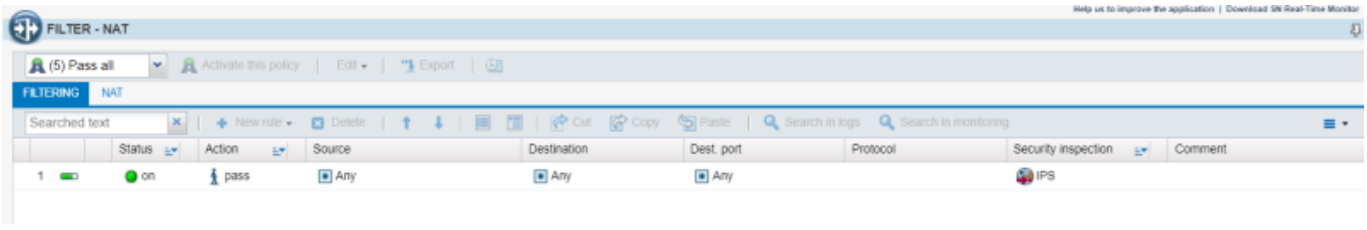


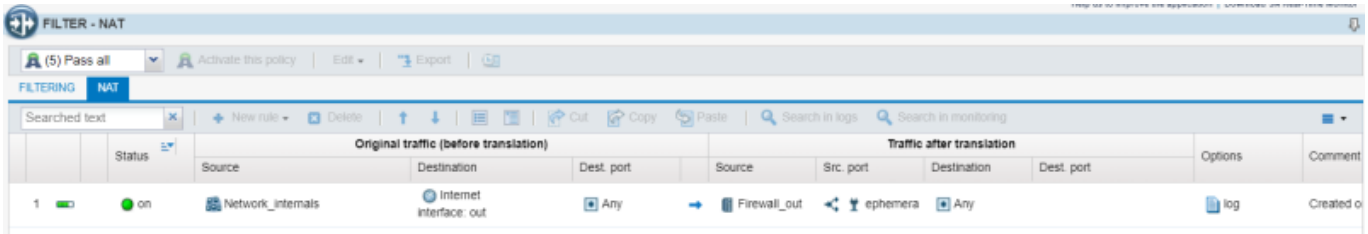
config_pare-feu_03.10.22.rar

config_pare-feu_17.10.22.rar

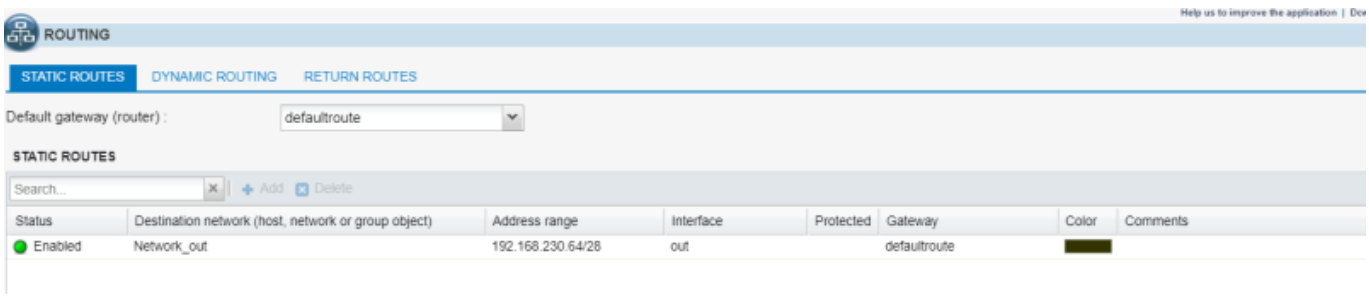
vmsnsx09k0639a9_2022-11-18.rar

Filtre et NAT/PAT





Route par défaut



Règles de filtrage :

Section 1 – Règles d'autorisation à destination du pare-feu

1: Autoriser SSH et HTTPS pour le panneau de configuration web du pare-feu sur vlan Développement pour le PC Admin

Section 2 – Règles de protection du pare-feu

2: Bloquer tous les paquets en destination des interfaces du routeur pour le sécuriser

Section 3 – Règles d'autorisation des flux métiers

3: Autoriser les paquets HTTP et HTTPS protocole TCP pour le vlan Développement

Section 4 – Règles d'autorisation pour la DMZ

4: Autoriser les paquets HTTP et HTTPS protocole TCP pour le vlan Serveur

5: Autoriser les paquets DNS protocole UDP vers le Serveur DNS

6: Autoriser les paquets DNS protocole TCP/UDP venants du Serveur DNS

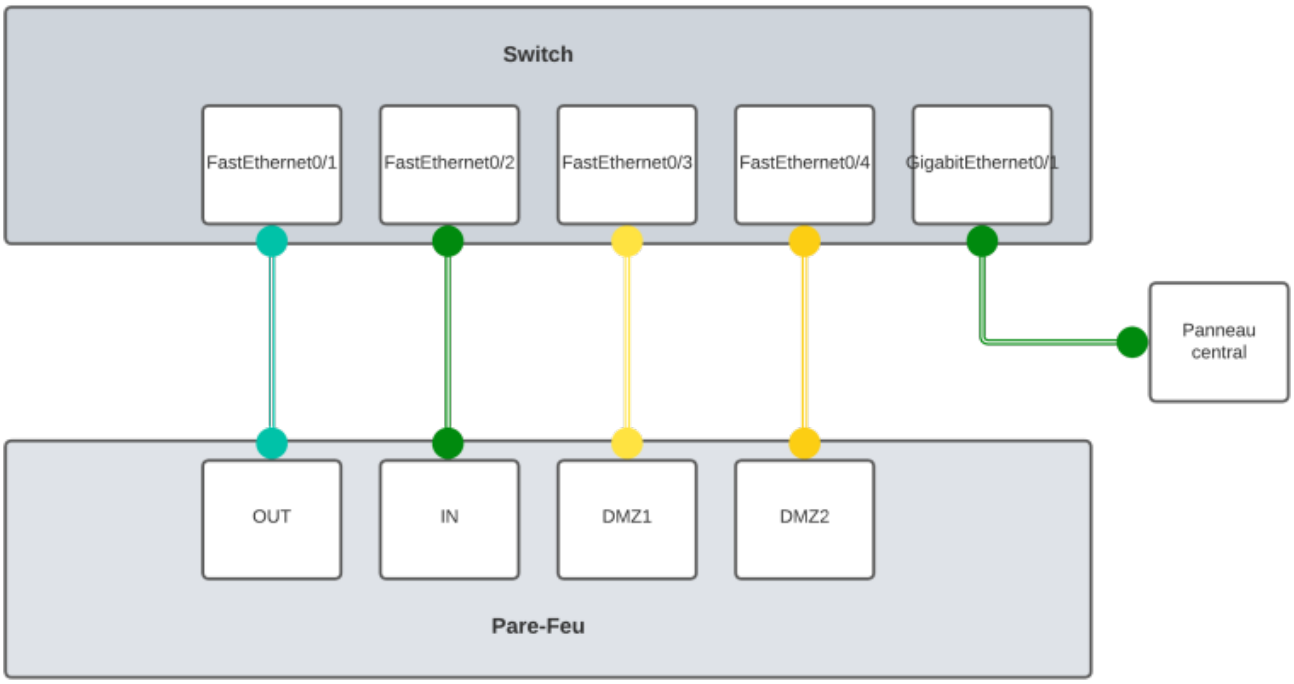
Section 5 – Règle d'interdiction finale

7: Bloquer tous les paquets

N°	Adresse IP Source	Port Source	Adresse IP Destination	Port Destination	Proto(cole)	Action
Section 1 – Règles d'autorisation à destination du pare-feu						
1	192.168.229.133	>1023	192.168.229.129	22, 443	*	Autoriser
2	*	*	192.168.230.74	80, 443	*	Autoriser
Section 2 – Règles de protection du pare-feu						

N°	Adresse IP Source	Port Source	Adresse IP Destination	Port Destination	Proto(cole)	Action
3	*	*	192.168.229.129, 192.168.228.73, 192.168.230.74, 10.187.35.49	*	*	Bloquer
Section 3 – Règles d'autorisation des flux métiers						
4	192.168.229.128/27	>1023	*	80, 443	TCP	Autoriser
5	192.168.229.128/27	>1023	192.168.228.109/27	53	TCP/UDP	Autoriser
Section 4 – Règles d'autorisation pour la DMZ						
6	192.168.228.64/28	*	*	80, 443	TCP	Autoriser
7	192.168.228.109/27	*	*	*	TCP/UDP	Autoriser
Section 5 – Règle d'interdiction finale						
8	*	*	*	*	*	Bloquer

Brassage



Câblage et brassage du Switch et du SNS :

Serveurs DHCP :

Haute disponibilité du service DHCP grâce à une configuration du service DHCP en Failover/Load-balancing

Serveur DHCP primaire : 192.168.229.130/27

Serveur DHCP secondaire : 192.168.229.131/27

Installation du service DHCP :

```
apt install isc-dhcp-server
```

Redémarrer le service DHCP :

```
service isc-dhcp-server restart
```

Contenu du fichier de configuration du service DHCP du serveur primaire /etc/dhcp/dhcpd.conf :

```
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#
# Declaration du FAILOVER DHCP pour le serveur primaire#
failover peer "GSB" {
        primary;
```

```
        address 192.168.229.130;
        port 647;
        peer address 192.168.229.131;
        peer port 847;
        max-response-delay 60;
        max-unacked-updates 10;
        mclt 3;
        split 128;
        load balance max seconds 3;
}
#failover peer "GSB" state {
#    my state partner-down;
#}
option domain-name "developpement.gsb.local";
option domain-name-servers 192.168.229.132;
default-lease-time 600;
max-lease-time 7200;
ddns-update-style none;
authoritative;
log-facility local7;
subnet 192.168.229.128 netmask 255.255.255.224 {
  pool {
       failover peer "GSB";
     range 192.168.229.140 192.168.229.150;
       }
  #option domain-name-servers 8.8.8.8;
  #option domain-name "GSB.LOCAL";
  option routers 192.168.229.129;
  option broadcast-address 192.168.229.159;
  #default-lease-time 600;
  #max-lease-time 7200;
}
```

Contenu du fichier de configuration du service DHCP du serveur secondaire /etc/dhcp/dhcpd.conf :

```
# dhcpd.conf
#
# Sample configuration file for ISC dhcpd
#
# Declaration du FAILOVER DHCP pour le serveur secondaire#
failover peer "GSB" {
        secondary;
        address 192.168.229.131;
        port 847;
        peer address 192.168.229.130;
        peer port 647;
        max-response-delay 60;
        max-unacked-updates 10;
        load balance max seconds 3;
}
#failover peer "GSB" state {
```

```
#    my state partner-down;
#}
# option definitions common to all supported networks...
option domain-name "developpement.gsb.local";
option domain-name-servers 192.168.228.109;
default-lease-time 600;
max-lease-time 7200;
ddns-update-style none;
#authoritative;
log-facility local7;
subnet 192.168.229.128 netmask 255.255.255.224 {
  pool {
       failover peer "GSB";
    range 192.168.229.140 192.168.229.150;
       }
  #option domain-name-servers 8.8.8.8;
  #option domain-name "GSB.LOCAL";
  option routers 192.168.229.129;
  option broadcast-address 192.168.229.159;
  #default-lease-time 600;
  #max-lease-time 7200;
}
```

Commandes de test:

Renouveler une configuration IP DHCP:

Sur Linux:

```
systemctl restart networking
```

```
ifdown eth0
ifup eth0
```

Sur Windows:

```
ipconfig /release
ipconfig /renew
```

Procédure pour synchroniser les deux serveurs DHCP

1) Lancer les serveurs DHCP sans activer le service DHCP

```
update-rc.d isc-dhcp-server remove
reboot
```

2) Décommenter ces trois lignes sur les deux serveurs DHCP DHCP1 et DHCP2.

```
failover peer "GSB" state {
    my state partner-down;
}
```

3) Lancer le service DHCP sur le serveur primaire DHCP1 seulement.

```
systemctl start isc-dhcp-server
```

5) Démarrer le serveur secondaire DHCP2.

```
systemctl start isc-dhcp-server
```

6) Arrêter le serveur primaire DHCP1.

```
systemctl stop isc-dhcp-server
```

7) Commenter les lignes sur le serveur primaire DHCP1.

```
#failover peer "GSB" state {
#    my state partner-down;
#}
```

8) Démarrer le serveur primaire DHCP1.

```
systemctl start isc-dhcp-server
```

9) Arrêter le serveur secondaire DHCP2.

```
systemctl stop isc-dhcp-server
```

10) Commenter les lignes sur le serveur secondaire DHCP2.

```
#failover peer "GSB" state {
#    my state partner-down;
#}
```

11) Démarrer le serveur secondaire DHCP2.

```
systemctl start isc-dhcp-server
```

Serveur DNS :

Nom de domaine à utiliser : developpements.gsb.fr

Adresse IP du serveur DNS : 192.168.228.109/26

Config à insérer à chaque postes ou DHCP :

```
domain developpement.gsb.fr
search developpement.gsb.fr
nameserver 192.168.228.109
```

Installation de Bind9:

```
apt -y install bind9 dnsutils
```

Le fichier /etc/bind/named.conf.local contient:

```
zone "developpement.gsb.fr" {
    type master;
    file "/etc/bind/db.developpement.gsb.fr";
};
zone "168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.developpement.gsb.inv";
};
```

Le fichier /etc/bind/db.developpement.gsb.fr contient :

```
$ORIGIN developpement.gsb.fr.
$TTL 1D
@       IN      SOA     DNS-Equipe9.developpement.gsb.fr.
root.developpement.gsb.fr. (
        2006031201      ; serial
        28800           ; refresh
        14400           ; retry
        3600000         ; expire
        86400 )         ; minimum
       NS      DNS-Equipe9.developpement.gsb.fr.
DNS-Equipe9    A       192.168.228.109
dhcp1          A       192.168.229.130
dhcp2          A       192.168.229.131
```

Le fichier /etc/bind/db.developpement.gsb.inv contient :

```
$TTL 3D
@ IN SOA DNS-Equipe9.developpement.gsb.fr. root.developpement.gsb.fr. (
        2006031201      ; serial
        28800           ; refresh
        14400           ; retry
        3600000         ; expire
        86400 )         ; minimum
    NS DNS-Equipe9.developpement.gsb.fr.
109 PTR DNS-Equipe9.developpement.gsb.fr.
130 PTR dhcp1.developpement.gsb.fr.
131 PTR dhcp2.developpement.gsb.fr.
```

Le fichier /etc/bind/named.conf.options contient :

```
options {
        directory "/var/cache/bind";
        allow-recursion { any; };
        dnssec-validation no;
        listen-on-v6 { any; };
        forwarders {
                8.8.8.8;
         };
};
```

Commandes de test

```
nslookup google.com
```

```
root@client-test:~# nslookup google.com
Server:         192.168.228.109
Address:        192.168.228.109#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.200.206
```

```
ping google.com
```

```
root@DNS-Equipe9:~# ping google.com
PING google.com (142.250.201.46) 56(84) bytes of data.
64 bytes from 142.250.201.46: icmp_seq=1 ttl=110 time=21.8 ms
64 bytes from 142.250.201.46: icmp_seq=2 ttl=110 time=19.9 ms
64 bytes from 142.250.201.46: icmp_seq=3 ttl=110 time=20.4 ms
64 bytes from 142.250.201.46: icmp_seq=5 ttl=110 time=19.2 ms
64 bytes from 142.250.201.46: icmp_seq=6 ttl=110 time=19.6 ms
64 bytes from 142.250.201.46: icmp_seq=7 ttl=110 time=19.1 ms
64 bytes from 142.250.201.46: icmp_seq=8 ttl=110 time=22.4 ms
64 bytes from 142.250.201.46: icmp_seq=9 ttl=110 time=21.2 ms
64 bytes from 142.250.201.46: icmp_seq=10 ttl=110 time=19.7 ms
64 bytes from 142.250.201.46: icmp_seq=11 ttl=110 time=19.2 ms
64 bytes from 142.250.201.46: icmp_seq=12 ttl=110 time=19.9 ms
64 bytes from 142.250.201.46: icmp_seq=13 ttl=110 time=19.6 ms
```

```
dig google.com
```

```
root@DNS-Equipe9:~# dig google.com

; <<>> DiG 9.16.33-Debian <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39740
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 7a50566ad4ac48dc0100000063529e60e4f2c99141272750 (good)
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             141     IN      A       142.250.201.46

;; Query time: 28 msec
;; SERVER: 192.168.228.109#53(192.168.228.109)
;; WHEN: Fri Oct 21 13:28:00 UTC 2022
;; MSG SIZE  rcvd: 83
```

Contrôleur de domaine :

IP : 192.168.208.110/26

OS : Windows Server 2019

UrBackup

Téléchargement et installation via :
https://hndl.urbackup.org/Server/2.4.14/UrBackup%20Server%202.4.14%28x64%29.msi

Configuration via : http://localhost:55414

FreeRadius :

Sur le serveur Radius

Installation des paquets:

```
apt install freeradius
```

Ajout des clients dans /etc/FreeRadius/3.0/clients.conf :

```
client Serveur-linux {
ipaddr = @IP-de-votre-serveur-linux 192.168.27.165
secret = BTS-SIO-Secret # secret partagé entre ce client et le serveur
Radius
}
```

Ajout des utilisateurs dans /etc/FreeRadius/3.0/users :

```
admin Cleartext-Password := "azerty123"
```

Sur le serveur client Radius

Installation des paquets:

```
apt install libpam-radius-auth freeradius-utils
```

Ajout de l'authentification dans /etc/pam_radius_auth.conf :

```
192.168.229.134 BTS-SIO-Secret 5
```

Création de l'utilisateur Radius “Admin” :

```
adduser admin --disabled-password --quiet --gecos ""
```

Test

Commande de test :

```
radtest admin azerty123 192.168.229.134 0 BTS-SIO-Secret
```

La commande retourne : Received Access-Accept

```
root@Serveur-Linux-NAS:~# radtest admin azerty123 192.168.229.134 0 BTS-SIO-Secret
Sent Access-Request Id 244 from 0.0.0.0:36103 to 192.168.229.134:1812 length 75
        User-Name = "admin"
        User-Password = "azerty123"
        NAS-IP-Address = 192.168.229.135
        NAS-Port = 0
        Message-Authenticator = 0x00
        Cleartext-Password = "azerty123"
Received Access-Accept Id 244 from 192.168.229.134:1812 to 192.168.229.135:36103 length 20
```

Sur le serveur client Radius

Modification du fichier de configuration /etc/pam.d/sshd en ajoutant:

```
auth sufficient pam_radius_auth.so debug
```

Puis mettre en commentaire tous les autres paramètres

Ajout au fichier /etc/pam.d/sudo :

```
auth sufficient pam_radius_auth.so
```

Ajout au fichier /etc/pam.d/su :

```
auth sufficient pam_radius_auth.so
```

Fichier Configuration Switch :

config_switch_gsb.rar

```
Current configuration : 3341 bytes
!
! Last configuration change at 00:51:23 UTC Mon Mar 1 1993
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname 2960SI-AP-06
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$LANj$eyEG/JGRtrL7P3tEn60R80
!
username btssio password 7 03064F1815062E
no aaa new-model
system mtu routing 1500
!
!
ip domain-name 0970019y.lan
!
!
crypto pki trustpoint TP-self-signed-660967168
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-660967168
 revocation-check none
 rsakeypair TP-self-signed-660967168
!
!
```

```
crypto pki certificate chain TP-self-signed-660967168
 certificate self-signed 01
  3082024F 308201B8 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 36363039 36373136 38301E17 0D393330 33303130 30303130
  335A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3636 30393637
  31363830 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
  AD6DE301 0ADC2435 2422D199 4A913E6F 72943198 3F9F7420 77CDA0E7 9FAA129C
  C08FCCA9 7E0AFEE3 9E698301 C2884294 7FF769BF 4C0C57B4 5EBAAACD 3DA1578E
  FCD25C0C 058E829B BA6BB75C CC39B685 4B13FE68 A6CA57D9 7B7D7E95 976346F6
  5E61FFA5 A7B80461 7391BD31 3A0BD5ED 079C91B5 630F106E 5886A67A 28F5CECF
  02030100 01A37930 77300F06 03551D13 0101FF04 05300301 01FF3024 0603551D
  11041D30 1B821932 39363053 492D4150 2D30362E 30393730 30313979 2E6C616E
  301F0603 551D2304 18301680 14451204 6475FD7F F6510853 14EFAC57 1847D2F9
  91301D06 03551D0E 04160414 45120464 75FD7FF6 51085314 EFAC5718 47D2F991
  300D0609 2A864886 F70D0101 04050003 81810021 DC76417D 792F1AB9 BBB4A6ED
  9D551544 E496A954 E588863A 1CA96DF3 7C2C1493 DF2EB896 28FF7EDD 61776964
  1A1F2255 2491209E 25567907 60AB37FE 397CE470 DB691E92 D2304E58 1E05A999
  10712A15 805720F1 313622FA FDF81269 40B940F1 041519E0 96F51B4B E11540E1
  996EE71E 6097846C FE9A2D12 46A87C49 2B5077
        quit
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip ssh time-out 50
ip ssh version 2
!
!
!
!
interface FastEthernet0/1
 switchport access vlan 316
 switchport trunk allowed vlan 314
 switchport mode access
!
interface FastEthernet0/2
 switchport access vlan 311
 switchport trunk allowed vlan 316
 switchport mode access
!
interface FastEthernet0/3
 switchport access vlan 302
 switchport trunk allowed vlan 352
 switchport mode access
!
```

```
interface FastEthernet0/4
 switchport access vlan 134
 switchport trunk allowed vlan 302
 switchport mode access
!
interface FastEthernet0/5
 switchport access vlan 352
 switchport mode access
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface GigabitEthernet0/1
 switchport mode trunk
!
interface Vlan1
 no ip address
 no ip route-cache
!
interface Vlan134
 ip address 10.187.35.33 255.255.255.0
 no ip route-cache
!
ip default-gateway 10.187.35.254
ip http server
ip http secure-server
logging esm config
!
line con 0
 password 7 110B0D16041B04
 login
line vty 0 4
 password 7 03064F1815062E
 logging synchronous
 login
 transport input telnet
line vty 5 15
 password 7 110B0D16041B04
 login
!
end
```

```
hostname 2960SI-AP-06
ip domain-name 0970019y.lan
interface FastEthernet0/1
 switchport access vlan 316
 switchport trunk allowed vlan 314
```

```
 switchport mode access
interface FastEthernet0/2
 switchport access vlan 311
 switchport trunk allowed vlan 316
 switchport mode access
interface FastEthernet0/3
 switchport access vlan 302
 switchport trunk allowed vlan 352
 switchport mode access
interface FastEthernet0/4
 switchport access vlan 134
 switchport trunk allowed vlan 302
 switchport mode access
interface FastEthernet0/5
 switchport access vlan 352
 switchport mode access
interface GigabitEthernet0/1
 switchport mode trunk
interface Vlan1
 no ip address
 no ip route-cache
interface Vlan134
 ip address 10.187.35.33 255.255.255.0
 no ip route-cache
ip default-gateway 10.187.35.254
end
```

Identifiants

SNS : admin labarde2003

admin centreon : Yaya@chalet79

DC : yaya@chalet79

Comptes AD :

Administrateur@lan.developpement.gsb.fr yaya@chalet79

jasmin@lan.developpement.gsb.fr yaya@chalet79