Etapes de la configuration du VPN-SSL sur les FORGATE

Définition d'une plage d'adresse des postes distants, qui leur sera attribuée dynamiquement - VPN-SPOOL-xxxx

Définition du/des réseau(x) « SPLIT » qui seront joignables depuis le client par le tunnel. Le mode SPLIT consiste à ne faire passer que les trames à destinations des réseaux « internes » par le tunnel, les autres flux transiteront par l'interface par défaut du poste client - VPN-SPLIT-xxxx,

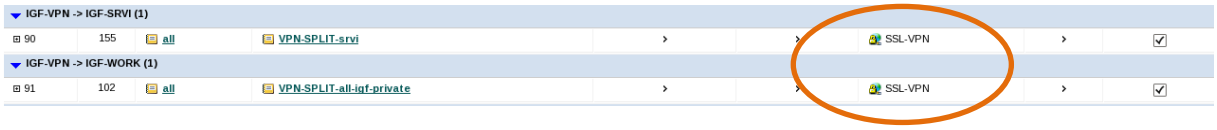
☐	VPN-ADMIN-POOL	10.21.30.0/255.255.255.0	Any	Subnet		12
☐	VPN-IPAM-POOL	10.21.32.0/255.255.255.0	Any	Subnet		2
☐	VPN-SPLIT-SRVX	195.220.10.0/255.255.255.224	Any	Subnet		2
☐	VPN-SPLIT-all-igf-private	10.7.0.0/255.255.0.0	Any	Subnet		3
☐	VPN-SPLIT-srvi	10.7.0.0/255.255.255.0	Any	Subnet		2
☐	VPN-SPLIT-work	10.7.16.0/255.255.240.0	Any	Subnet		0
☐	VPN-USER-POOL	10.21.31.0/255.255.255.0	Any	Subnet		11

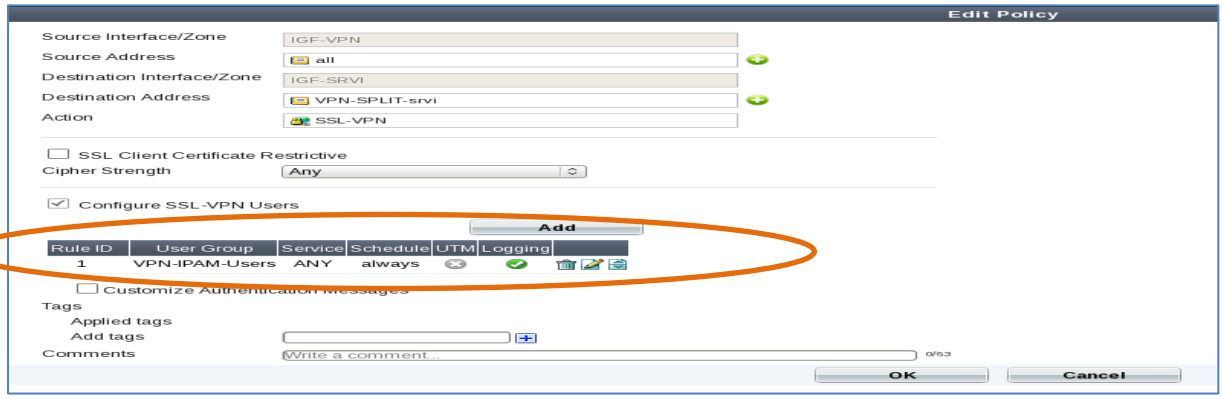
Définition d'un portail VPN SSL
- Liste éventuelle des protocoles autorisés
- Mise en place éventuelle du mécanisme de SPLIT et des adresses autorisées par le tunnel, VPN-SPLIT-xxxx
- Association à la plage d'adresse des postes utilisateurs distants, VPN-SPOOL-xxxx

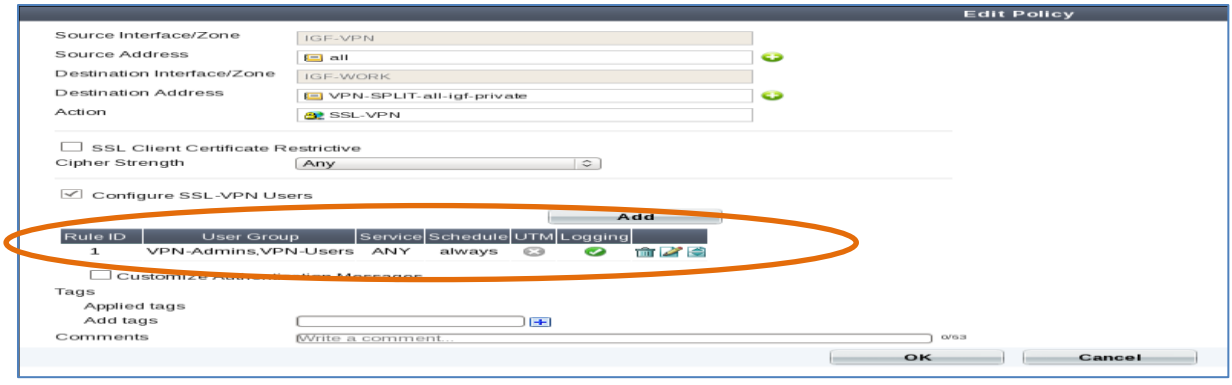
Définition d'une source d'authentification des utilisateurs
- Utilisateurs locaux
- Utilisateurs déclarés dans un annuaire LDAP
- Utilisateurs déclarés dans un annuaire AD

Définition d'une population d'utilisateur, un groupe d'utilisateur
- Association d'une source d'authentification
- Association d'un portail VPN SSL

Mise en place de règle de FW depuis l'interface physique VPN vers le réseau ciblé
- Soit depuis une interface dédiée type LABO-VPN par exemple
- Soit depuis l'interface « EXTRA » ou « WAN » coté extérieur
- Vers les interfaces des réseaux ciblés, exemple IGF-SRVI
- Par une ACTION de **type SSL-VPN** (ACTION, pas SERVICE)
- Associer un/des groupe(s) d'utilisateur (valider et choisir SSL-USERS)
- Possibilité de filtrer les adresses IP publiques des postes distants cherchant à ouvrir le VPN SSL

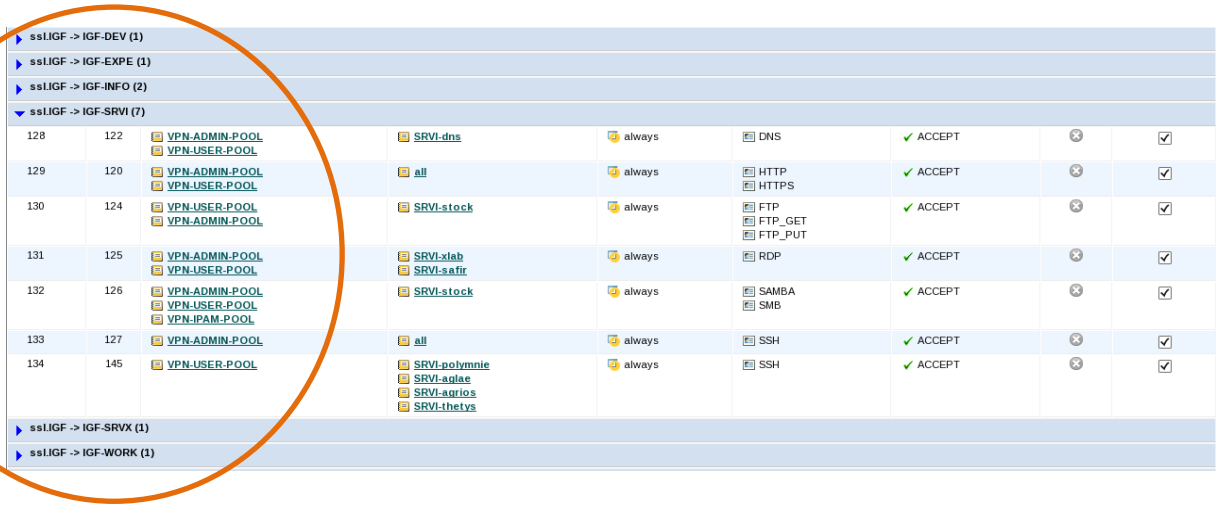






Mise en place de règle de FW depuis l'interface ssl vers le réseau ciblé

- Soit depuis ssl.root si pas de VDOM
- Soit depuis ssl.IGF si par exemple VDOM IGF
- Depuis les adresses VPN-SPOOL-xxxx
- Vers le réseau ciblé
- Pour les services autorisés



Ajout d'une route statique pour joindre le réseau des postes clients VPN-SPOOL-xxxx

- Destination le réseau VPN-SPOOL-xxxx
- Par l'interface (Device) ssl.IGF si VDOM ssl.root sinon.

Configuration d'une source de type annuaire **LDAP**

- `set cnid "uid"`
  Permet de préciser l'attribut qui sera utilisé pour rechercher le nom de l'utilisateur lorsque ce n'est pas cn (common name)
- `set dn "ou=Users,dc=igf,dc=cnrs,dc=fr"`
  Précise le début de l'arborescence de recherche dans l'annuaire. Attention ce point d'origine ne peut pas varier par la suite. Toutes les recherches, quelque soit le groupe d'utilisateur, se feront forcément à partir de ce point.
  Par exemple, il ne peut pas y avoir un dn de cette valeur, et un groupe d'utilisateur dont la racine serait "ou=ipam-ext,dc=igf,dc=cnrs,dc=fr". Dans ce cas, soit il faut définir un dn à "dc=igf,dc=cnrs,dc=fr" et jouer avec un set filter pour filtrer un certain type de fiche de l'annuaire, soit il faut définir une seconde source de type annuaire, même si elle a la même adress ip, avec le dn ciblé.
- `set member-attr "dialupAccess"`
  Parcourt l'arborescence à partir du dn pour trouver la fiche dont le champ cnid vaut le nom d'utilisateur, et évalue la valeur du champ dialupAccess pour un classement par groupe ultérieur.
- `set filter (objectClass=posixAccount)`
  Limite l'évaluation à certaines fiches, ici celles de type posixAccount.

```
FW-IGH-IGF-2 (IGF) # show user ldap IGF-ldap-master
config user ldap
    edit "IGF-ldap-master"
        set server "10.7.0.20"
        set cnid "uid"
        set dn "ou=Users,dc=igf,dc=cnrs,dc=fr"
        set type regular
        set username "cn=Fortinet,ou=Users,dc=igf,dc=cnrs,dc=fr"
        set password ENC
IXiAEA0U3iXGIimtF36cibo11P8qxySi1nij23hdsIMQ5iczgzJNElrfUhSBg/1/bKY/MKrcQtE3uFaQGpnrwiK
73vphIGGN6WqyblbV3xqkUpvc
        set member-attr "dialupAccess"
    next
end

FW-IGH-IGF-2 (IGF) # show user ldap IGF-ldap-ipam
config user ldap
    edit "IGF-ldap-ipam"
        set server "10.7.0.20"
        set cnid "uid"
        set dn "ou=ipam-ext,dc=igf,dc=cnrs,dc=fr"
        set type regular
        set username "cn=Fortinet,ou=Users,dc=igf,dc=cnrs,dc=fr"
        set password ENC
IXiAEA0U3iXGIimtF36cibo11P8qxySi1nij23hdsIMQ5iczgzJNElrfUhSBg/1/bKY/MKrcQtE3uFaQGpnrwiK
73vphIGGN6WqyblbV3xqkUpvc
        set member-attr "dialupAccess"
```

```
    next
end
```

Le member-attr permet de définir des groupes d'utilisateur, chacun correspondant à un portail donné, donc à une source de machines clientes spécifiques :

- dans le premier cas, les utilisateurs définis dans l'annuaire IGF-ldap-master, ayant le champ dialupAccess positionné à la valeur admin, utiliseront le portail VPN-ADMIN, et donc les droits/restrictions associées
- Dans le second cas, les utilisateurs définis dans l'annuaire IGF-ldap-master ayant le champs dialupAccess positionné à la valeur user, utiliseront le portail VPN-USER, droits et réglés associés
- Dans le dernier cas, les utilisateurs définis dans l'annuaire IGF-ldap-ipam, ayant le champ dialupAccess positionné à la valeur user, utiliseront le portail VPN-IPAM

```
FW-IGH-IGF-2 (IGF) # show user group VPN-Admins
config user group
    edit "VPN-Admins"
        set sslvpn-portal "VPN-ADMIN"
            set member "IGF-ldap-master" "olivier.durant" "eric.mauger"
            config match
                edit 1
                    set server-name "IGF-ldap-master"
                    set group-name "admin"
                next
            end
    next
end

FW-IGH-IGF-2 (IGF) # show user group VPN-Users
config user group
    edit "VPN-Users"
        set sslvpn-portal "VPN-USER"
            set member "IGF-ldap-master"
            config match
                edit 1
                    set server-name "IGF-ldap-master"
                    set group-name "user"
                next
            end
    next
end

FW-IGH-IGF-2 (IGF) # show user group VPN-IPAM-Users
config user group
    edit "VPN-IPAM-Users"
        set sslvpn-portal "VPN-IPAM"
            set member "IGF-ldap-ipam"
            config match
                edit 1
                    set server-name "IGF-ldap-ipam"
                    set group-name "user"
                next
            end
    next
end
```

Configuration du VPN-SSL de L'IGF

```
FW-IGH-IGF-2 (IGF) # sh user ldap
config user ldap
    edit "IGF-ldap-master"
        set server "10.7.0.20"
        set cnid "uid"
        set dn "ou=Users,dc=igf,dc=cnrs,dc=fr"
        set type regular
        set username "cn=Fortinet,ou=Users,dc=igf,dc=cnrs,dc=fr"
        set password ENC
IXiAEA0U3iXGIimtF36cibo11P8qxySi1nij23hdsIMQ5iczgzJNElrfUhSBg/1/bKY/MKrcQtE3uFaQGpnrwiK
73vphIGGN6Wqyblbv3xqkUpvc
        set member-attr "dialupAccess"
    next
    edit "IGF-ldap-ipam"
        set server "10.7.0.20"
        set cnid "uid"
```

```
        set dn "ou=ipam-ext,dc=igf,dc=cnrs,dc=fr"
        set type regular
        set username "cn=Fortinet,ou=Users,dc=igf,dc=cnrs,dc=fr"
        set password ENC
IXiAEA0U3iXGIimtF36cibo11P8qxySi1nij23hdsIMQ5iczgzJNElrfUhSBg/1/bKY/MKrcQtE3uFaQGpnrwiK
73vphIGGN6Wqyblbv3xqkUpvc
        set member-attr "dialupAccess"
    next
end


FW-IGH-IGF-2 (IGF) # sh user group
config user group
    edit "FSSO_Guest_Users"
        set group-type fsso-service
    next
    edit "VPN-Users"
        set sslvpn-portal "VPN-USER"
            set member "IGF-ldap-master"
            config match
                edit 1
                    set server-name "IGF-ldap-master"
                    set group-name "user"
                next
            end
    next
    edit "VPN-Admins"
        set sslvpn-portal "VPN-ADMIN"
            set member "IGF-ldap-master" "eric.mauger" "olivier.durant"
            config match
                edit 1
                    set server-name "IGF-ldap-master"
                    set group-name "admin"
                next
            end
    next
    edit "VPN-IPAM-Users"
        set sslvpn-portal "VPN-IPAM"
            set member "IGF-ldap-ipam"
            config match
                edit 1
                    set server-name "IGF-ldap-ipam"
                    set group-name "user"
                next
            end
    next
end


FW-IGH-IGF-2 (IGF) # sh vpn ssl settings
config vpn ssl settings
    set dns-server1 10.7.0.2
    set dns-server2 193.49.132.10
    set port 443
end


FW-IGH-IGF-2 (IGF) # show vpn ssl web portal
config vpn ssl web portal
    edit "VPN-ADMIN"
        set allow-access web ftp smb telnet ssh vnc rdp ping
        set heading "VPN Admins"
        set page-layout double-column
        set allow-user-bookmark disable
            config widget
                edit 4
                    set name "Session Information"
                    set type info
                next
                edit 1
                    set name "Bookmarks"
                    set allow-apps web
                next
                edit 2
                    set name "Connection Tool"
                    set type tool
                    set column two
```

```
                    set allow-apps web ftp smb telnet ssh vnc rdp
                next
                edit 3
                    set name "Tunnel Mode"
                    set type tunnel
                    set column two
                    set tunnel-status enable
                    set split-tunneling enable
                    set ip-mode usrgrp
                        set ip-pools "VPN-ADMIN-POOL"
                        set split-tunneling-routing-address "VPN-SPLIT-SRVX" "VPN-
SPLIT-all-igf-private"
                next
            end
    next
    edit "VPN-USER"
        set theme gray
        set heading "VPN Utilisateurs"
        set page-layout double-column
        set allow-user-bookmark disable
            config widget
                edit 3
                    set name "Tunnel Mode"
                    set type tunnel
                    set tunnel-status enable
                    set split-tunneling enable
                        set ip-pools "VPN-USER-POOL"
                        set split-tunneling-routing-address "VPN-SPLIT-all-igf-private"
"VPN-SPLIT-SRVX"
                next
                edit 4
                    set name "Session Information"
                    set type info
                next
                edit 2
                    set name "Connection Tool"
                    set type tool
                    set column two
                    set allow-apps web ftp smb telnet ssh vnc rdp
                next
                edit 1
                    set name "Bookmarks"
                    set column two
                    set allow-apps web
                next
            end
    next
    edit "VPN-IPAM"
        set theme orange
        set heading "VPN-SSL IGF pour IPAM"
        set page-layout double-column
        set allow-user-bookmark disable
            config widget
                edit 4
                    set name "Session Information"
                    set type info
                next
                edit 3
                    set name "CONNEXION"
                    set type tunnel
                    set column two
                    set tunnel-status enable
                    set split-tunneling enable
                    set ip-mode usrgrp
                        set ip-pools "VPN-IPAM-POOL"
                        set split-tunneling-routing-address "VPN-SPLIT-srvi"
                next
            end
    next
end
```

```
FW-IGH-IGF-2 (IGH) # show user ldap
config user ldap
    edit "cesar.igh.cnrs.fr"
        set server "193.50.6.43"
        set cnid "sAMAccountName"
        set dn "DC=igh,DC=cnrs,DC=fr"
        set type regular
        set username "CN=annuaireigh,OU=S-Info,OU=Utilisateurs,DC=igh,DC=cnrs,DC=fr"
        set password ENC
NoY3JrKhDtC9iseTK7yHtJN+A67mqcI4eSRqZnoFM3uHJLpntOHCWIjI2CQaguWojehQs5ny1un0do+pmgwi5Ns
LjWSGmnbBU7bJUS7p5y4WS4Vs
    next
end

FW-IGH-IGF-2 (IGH) # show user group
config user group
    edit "VPN-Admins"
        set sslvpn-portal "VPN-ADMIN"
            set member "cesar.igh.cnrs.fr"
            config match
                edit 1
                    set server-name "cesar.igh.cnrs.fr"
                    set group-name "CN=gg-vpn-admins,OU=Groupes,DC=igh,DC=cnrs,DC=fr"
                next
            end
    next
    edit "VPN-Users"
        set sslvpn-portal "VPN-USER"
            set member "cesar.igh.cnrs.fr" "jgarnier"
            config match
                edit 1
                    set server-name "cesar.igh.cnrs.fr"
                    set group-name "cn=gg-vpn-users,ou=Groupes,DC=igh,DC=cnrs,DC=fr"
                next
            end
    next
end

FW-IGH-IGF-2 (IGH) # sh vpn ssl settings
config vpn ssl settings
    set dns-server1 193.49.132.10
    set dns-server2 194.57.118.10
        set tunnel-ip-pools "VPN-USER-POOL" "VPN-ADMIN-POOL"
    set port 443
end


FW-IGH-IGF-2 (IGH) # sh vpn ssl web portal
config vpn ssl web portal
    edit "VPN-ADMIN"
        set allow-access web ftp smb telnet ssh vnc rdp ping
        set heading "VPN Admins"
        set page-layout double-column
        set allow-user-bookmark disable
            config widget
                edit 4
                    set name "Session Information"
                    set type info
                next
                edit 1
                    set name "Bookmarks"
                    set allow-apps web
                next
                edit 2
                    set name "Connection Tool"
                    set type tool
                    set column two
                    set allow-apps web ftp smb telnet ssh vnc rdp
                next
                edit 3
                    set name "Tunnel Mode"
                    set type tunnel
                    set column two
                    set tunnel-status enable
                    set ip-mode usrgrp
                        set ip-pools "VPN-ADMIN-POOL"
                next
```

```
            end
    next
    edit "VPN-USER"
        set allow-access web smb rdp
        set theme gray
        set heading "VPN Utilisateurs"
        set page-layout double-column
        set allow-user-bookmark disable
            config widget
                edit 3
                    set name "Tunnel Mode"
                    set type tunnel
                    set tunnel-status enable
                    set ip-mode usrgrp
                        set ip-pools "VPN-USER-POOL"
                next
                edit 4
                    set name "Session Information"
                    set type info
                next
                edit 2
                    set name "Connection Tool"
                    set type tool
                    set column two
                    set allow-apps web ftp smb telnet ssh vnc rdp
                next
                edit 1
                    set name "Bookmarks"
                    set column two
                    set allow-apps web
                next
            end
    next
end
```

Configuration CEFE

```
FW-CEFE_MRI-1 (CEFE) # show user ldap
config user ldap
    edit "AD1"
        set server "193.49.134.113"
        set cnid "sAMAccountName"
        set dn "DC=newcefe,DC=newage,DC=FR"
        set type regular
        set username "CN=LDAPWIFI,DC=newcefe,DC=newage,DC=FR"
        set password ENC
hb4ca2a4ApfXR9zGTssAmrxCBCJIYHGG/kyImP91rWmW8QueKOG9lWtNFWmJXT/9VcfCVHVvXzRlma3qaGpmAQS
A5C/TbOthf/bZ/eoGToChwovD
    next
    edit "AD2"
        set server "193.49.134.36"
        set cnid "sAMAccountName"
        set dn "DC=newcefe,DC=newage,DC=FR"
        set type regular
        set username "CN=LDAPWIFI,DC=newcefe,DC=newage,DC=FR"
        set password ENC
myPyaL3gb9m/ODx5ze40Fc7R/5EUWGOGRe/Xgp2dYUFWLeaujoeAs5tYkZh5mtggPV56iEsBMgfqwQ7Omt1wCfT
85eIvRfmiILZFgpIgdrJ7fLYg
    next
end

FW-CEFE_MRI-1 (CEFE) # show user group
config user group
    edit "VPN-Admins"
        set sslvpn-portal "VPN-ADMIN"
            set member "AD1" "AD2" "jgarnier"
            config match
                edit 1
                    set server-name "AD1"
                    set group-name "CN=VPN-
ADMINS,OU=UoCAMPUS,OU=uoINCEFE,OU=uoCEFE,DC=newcefe,DC=newage,DC=fr"
                next
                edit 2
                    set server-name "AD2"
```

```
                    set group-name "CN=VPN-
ADMINS,OU=UoCAMPUS,OU=uoINCEFE,OU=uoCEFE,DC=newcefe,DC=newage,DC=fr"
                next
            end
    next
    edit "VPN-Users"
        set sslvpn-portal "VPN-USER"
            set member "AD1" "AD2"
            config match
                edit 1
                    set server-name "AD1"
                    set group-name "CN=VPN-
USERS,OU=UoCAMPUS,OU=uoINCEFE,OU=uoCEFE,DC=newcefe,DC=newage,DC=fr"
                next
                edit 2
                    set server-name "AD2"
                    set group-name "CN=VPN-
USERS,OU=UoCAMPUS,OU=uoINCEFE,OU=uoCEFE,DC=newcefe,DC=newage,DC=fr"
                next
            end
    next
end

FW-CEFE_MRI-1 (CEFE) # sh vpn ssl settings
config vpn ssl settings
    set dns-server1 193.49.134.113
    set dns-server2 193.49.134.36
    set wins-server1 193.49.134.36
    set port 443
end

FW-CEFE_MRI-1 (CEFE) # sh vpn ssl web portal
config vpn ssl web portal
    edit "VPN-ADMIN"
        set allow-access web ftp smb telnet ssh vnc rdp ping
        set heading "VPN Admins"
        set page-layout double-column
        set allow-user-bookmark disable
            config widget
                edit 4
                    set name "Session Information"
                    set type info
                next
                edit 1
                    set name "Bookmarks"
                    set allow-apps web
                        config bookmarks
                            edit "FireWall"
                                set description "Acces vers le firewall"
                                set url "https://10.8.0.1:4443"
                            next
                        end
                next
                edit 2
                    set name "Connection Tool"
                    set type tool
                    set column two
                    set allow-apps web ftp smb telnet ssh vnc rdp
                next
                edit 3
                    set name "Tunnel Mode"
                    set type tunnel
                    set column two
                    set tunnel-status enable
                    set split-tunneling enable
                    set ip-mode usrgrp
                        set ip-pools "VPN-ADMIN-POOL"
                        set split-tunneling-routing-address "VPN-Split-private" "VPN-
Split-SRV"
                next
            end
    next
    edit "VPN-USER"
        set theme gray
        set heading "VPN Utilisateurs"
        set page-layout double-column
        set allow-user-bookmark disable
```

```
            config widget
                edit 3
                    set name "Tunnel Mode"
                    set type tunnel
                    set tunnel-status enable
                    set split-tunneling enable
                    set ip-mode usrgrp
                        set ip-pools "VPN-USER-POOL"
                        set split-tunneling-routing-address "VPN-Split-private" "VPN-
Split-SRV"
                next
                edit 4
                    set name "Session Information"
                    set type info
                next
                edit 2
                    set name "Connection Tool"
                    set type tool
                    set column two
                    set allow-apps web ftp smb telnet ssh vnc rdp
                next
                edit 1
                    set name "Bookmarks"
                    set column two
                    set allow-apps web
                next
            end
    next
end
```

Configuration MRI

```
FW-CEFE_MRI-1 (MRI) # sh user ldap

FW-CEFE_MRI-1 (MRI) # sh user group VPN-Admins
config user group
    edit "VPN-Admins"
        set sslvpn-portal "VPN-ADMIN"
            set member "jgarnier" "o.miquel"
    next
end

FW-CEFE_MRI-1 (MRI) # sh user group VPN-Users
config user group
    edit "VPN-Users"
        set sslvpn-portal "VPN-USER"
    next
end


FW-CEFE_MRI-1 (MRI) # sh vpn ssl settings
config vpn ssl settings
    set port 443
end

FW-CEFE_MRI-1 (MRI) # sh vpn ssl web portal VPN-ADMIN
config vpn ssl web portal
    edit "VPN-ADMIN"
        set allow-access web ftp smb telnet ssh vnc rdp ping
        set heading "VPN Admins"
        set page-layout double-column
        set allow-user-bookmark disable
            config widget
                edit 4
                    set name "Session Information"
                    set type info
                next
                edit 1
                    set name "Bookmarks"
                    set allow-apps web
                        config bookmarks
                            edit "FireWall"
                                set description "Acces vers le firewall"
                                set url "https://10.5.0.1:4443"
                            next
```

```
                        end
                next
                edit 2
                    set name "Connection Tool"
                    set type tool
                    set column two
                    set allow-apps web ftp smb telnet ssh vnc rdp
                next
                edit 3
                    set name "Tunnel Mode"
                    set type tunnel
                    set column two
                    set tunnel-status enable
                    set split-tunneling enable
                    set ip-mode usrgrp
                        set ip-pools "VPN-ADMIN-POOL"
                        set split-tunneling-routing-address "VPN-Split-private" "VPN-
Split-SRV"
                next
            end
    next
end

FW-CEFE_MRI-1 (MRI) # sh vpn ssl web portal VPN-USER
config vpn ssl web portal
    edit "VPN-USER"
        set theme gray
        set heading "VPN Utilisateurs"
        set page-layout double-column
        set allow-user-bookmark disable
            config widget
                edit 3
                    set name "Tunnel Mode"
                    set type tunnel
                    set tunnel-status enable
                    set split-tunneling enable
                    set ip-mode usrgrp
                        set ip-pools "VPN-USER-POOL"
                        set split-tunneling-routing-address "VPN-Split-private"
                next
                edit 4
                    set name "Session Information"
                    set type info
                next
                edit 2
                    set name "Connection Tool"
                    set type tool
                    set column two
                    set allow-apps web ftp smb telnet ssh vnc rdp
                next
                edit 1
                    set name "Bookmarks"
                    set column two
                    set allow-apps web
                next
            end
    next
end

FW-CEFE_MRI-1 (MRI) # sh vpn ssl web portal WIFI
config vpn ssl web portal
    edit "WIFI"
        set theme orange
        set heading "Welcome to WIFI Service"
        set allow-user-bookmark disable
            config widget
                edit 3
                    set name "Session Information"
                    set type info
                next
            end
    next
end
```

```
FW-SIC-1 (SIC) # sh user ldap
config user ldap
    edit "alkaid2.sic.int"
        set server "10.4.2.32"
        set cnid "cn"
        set dn "ou=people,dc=sic,dc=montp,dc=cnrs,dc=fr"
        set type regular
        set username "cn=fforti,ou=people,dc=sic,dc=montp,dc=cnrs,dc=fr"
        set password ENC
AAAEAIP5NoOdSYw2SRjFEqBWAYZBtWNED+lIIGEquVKfHlSsyr1pSuxQ6t8HhnQTQyZ91ffJppG2OIQ80cBzjJg
owoSce1iX2xeKAYZdGAZo7YpJ
        set member-attr "pager"
    next
    edit "alkaid.sic.int"
        set server "10.4.2.31"
        set cnid "cn"
        set dn "ou=people,dc=sic,dc=montp,dc=cnrs,dc=fr"
        set type regular
        set username "cn=fforti,ou=people,dc=sic,dc=montp,dc=cnrs,dc=fr"
        set password ENC
AAAEAIP5NoOdSYw2SRjFEqBWAYZBtWNED+lIIGEquVKfHlSsyr1pSuxQ6t8HhnQTQyZ91ffJppG2OIQ80cBzjJg
owoSce1iX2xeKAYZdGAZo7YpJ
        set member-attr "pager"
    next
    edit "opale.sic.int"
        set server "194.57.116.90"
        set cnid "cn"
        set dn "ou=people,dc=sic,dc=montp,dc=cnrs,dc=fr"
        set type regular
        set username "cn=fforti,ou=people,dc=sic,dc=montp,dc=cnrs,dc=fr"
        set password ENC
AAAEAIP5NoOdSYw2SRjFEqBWAYZBtWNED+lIIGEquVKfHlSsyr1pSuxQ6t8HhnQTQyZ91ffJppG2OIQ80cBzjJg
owoSce1iX2xeKAYZdGAZo7YpJ
        set member-attr "pager"
    next
end

FW-SIC-1 (SIC) # sh user group
config user group
    edit "VPN-Admins"
        set sslvpn-portal "VPN-ADMIN"
            set member "alkaid2.sic.int" "alkaid.sic.int" "opale.sic.int"
            config match
                edit 1
                    set server-name "alkaid2.sic.int"
                    set group-name "admin"
                next
                edit 2
                    set server-name "alkaid.sic.int"
                    set group-name "admin"
                next
                edit 3
                    set server-name "opale.sic.int"
                    set group-name "admin"
                next
            end
    next
    edit "VPN-Users"
        set sslvpn-portal "VPN-USER"
            set member "alkaid2.sic.int" "alkaid.sic.int" "opale.sic.int"
            config match
                edit 1
                    set server-name "alkaid2.sic.int"
                    set group-name "user"
                next
                edit 2
                    set server-name "alkaid.sic.int"
                    set group-name "user"
                next
                edit 3
                    set server-name "opale.sic.int"
                    set group-name "user"
                next
            end
    next
end
```

```
FW-SIC-1 (SIC) # sh vpn ssl settings
config vpn ssl settings
    set dns-server1 10.4.2.33
    set dns-server2 10.4.2.34
    set servercert "cerbere"
    set idle-timeout 3600
    set port 443
end

FW-SIC-1 (SIC) # sh vpn ssl web portal
config vpn ssl web portal
    edit "VPN-ADMIN"
        set allow-access web ftp smb telnet ssh vnc rdp ping
        set heading "VPN Admins"
        set page-layout double-column
        set allow-user-bookmark disable
            config widget
                edit 4
                    set name "Session Information"
                    set type info
                next
                edit 1
                    set name "Bookmarks"
                    set allow-apps web
                next
                edit 2
                    set name "Connection Tool"
                    set type tool
                    set column two
                    set allow-apps web ftp smb telnet ssh vnc rdp
                next
                edit 3
                    set name "Tunnel Mode"
                    set type tunnel
                    set column two
                    set tunnel-status enable
                    set split-tunneling enable
                    set ip-mode usrgrp
                        set ip-pools "VPN-ADMIN-POOL"
                        set split-tunneling-routing-address "VPN-Split-private" "VPN-
Split-MZ"
                next
            end
    next
    edit "VPN-USER"
        set theme gray
        set heading "VPN Utilisateurs"
        set page-layout double-column
        set allow-user-bookmark disable
            config widget
                edit 3
                    set name "Tunnel Mode"
                    set type tunnel
                    set tunnel-status enable
                    set split-tunneling enable
                    set ip-mode usrgrp
                        set ip-pools "VPN-USER-POOL"
                        set split-tunneling-routing-address "VPN-Split-private" "VPN-
Split-DMZ"
                next
                edit 4
                    set name "Session Information"
                    set type info
                next
                edit 2
                    set name "Connection Tool"
                    set type tool
                    set column two
                    set allow-apps web ftp smb telnet ssh vnc rdp
                next
                edit 1
                    set name "Bookmarks"
                    set column two
                    set allow-apps web
                next
```

```
            end
    next
end
```

Configuration DR13

```
FW-DR13-1 # sh user ldap
config user ldap
    edit "AD2008"
        set server "193.49.133.208"
        set cnid "sAMAccountName"
        set dn "OU=DR13,DC=ad,DC=dr13,DC=cnrs,DC=fr"
        set port 636
        set type regular
        set username "CN=fortigate
fortigate,OU=divers,OU=Utilisateurs,OU=DR13,DC=ad,DC=dr13,DC=cnrs,DC=fr"
        set password ENC
RkmKYqUDJ2uvoKDWJfXMibmBll93oj9rpINGMKxVVYbJ5M03bHedMfMdkGrQF+p7SY0hdozecta52/giG7HsO+Q
3KxVfhhzVlqvpOkCHm2+7bVWK
        set secure ldaps
        set ca-cert "CA_Cert_1"
    next

    edit "SQL"
        set server "193.49.133.119"
        set cnid "sAMAccountName"
        set dn "OU=DR13,DC=ad,DC=dr13,DC=cnrs,DC=fr"
        set port 636
        set type regular
        set username "CN=fortigate
fortigate,OU=divers,OU=Utilisateurs,OU=DR13,DC=ad,DC=dr13,DC=cnrs,DC=fr"
        set password ENC
AAAEAN6EoLcH8fXrfZeCYSWOvL6UslqvnRQXovWFJaf/7Fu3xVertA+E8u9+L9VA2BGEb8QPllAU93RrHe+Et0U
jKpIoA3A1L7GuOmRyO6NfHDXd
        set secure ldaps
        set ca-cert "CA_Cert_1"
    next
end

FW-DR13-1 # sh user group
config user group
    edit "VPN-Admins"
        set sslvpn-portal "Admins"
            set member "AD2008"
            config match
                edit 1
                    set server-name "AD2008"
                    set group-name "CN=VPN-
Admins,OU=groupes,OU=Utilisateurs,OU=DR13,DC=ad,DC=dr13,DC=cnrs,DC=fr"
                next
            end
    next
    edit "VPN-Utilisateurs"
        set sslvpn-portal "Users"
            set member "AD2008" "kerlidou" "juju"
            config match
                edit 1
                    set server-name "AD2008"
                    set group-name "CN=VPN-
Users,OU=groupes,OU=Utilisateurs,OU=DR13,DC=ad,DC=dr13,DC=cnrs,DC=fr"
                next
            end
    next
end


FW-DR13-1 # sh vpn ssl settings
config vpn ssl settings
    set dns-server1 193.49.133.208
    set dns-server2 193.49.133.119
    set servercert "VPN2.tcs"
    set algorithm low
    set port 443
end
```

```
FW-DR13-1 # sh vpn ssl web portal
config vpn ssl web portal
    edit "Admins"
        set allow-access web ftp smb telnet ssh vnc rdp ping
        set host-check av
        set cache-cleaner enable
        set theme gray
        set heading "Serveur VPN Administration"
        set page-layout double-column
            config widget
                edit 1
                    set name "Mode tunnel"
                    set type tunnel
                    set tunnel-status enable
                    set split-tunneling enable
                        set ip-pools "SSLVPN_TUNNEL_Admins"
                        set split-tunneling-routing-address "split-DR13" "split-Imp"
"split-adm" "split-SRVI"
                next
                edit 4
                    set name "Informations"
                    set type info
                next
                edit 3
                    set name "Outils de connexion"
                    set type tool
                    set column two
                    set allow-apps web ftp smb telnet ssh vnc rdp
                next
                edit 2
                    set name "Raccourcis"
                    set column two
                    set allow-apps web ftp smb telnet ssh vnc rdp
                next
            end
    next
    edit "Users"
        set allow-access web smb rdp ping
        set heading "Bienvenue sur le VPN de la DR13"
        set allow-user-bookmark disable
            config widget
                edit 3
                    set name "Connexion"
                    set type tunnel
                    set tunnel-status enable
                    set split-tunneling enable
                    set ip-mode usrgrp
                        set ip-pools "SSLVPN_TUNNEL_Users"
                        set split-tunneling-routing-address "split-DR13" "split-Imp"
                next
                edit 1
                    set name "Session Information"
                    set type info
                next
                edit 2
                    set name "Raccourcis"
                    set allow-apps web smb rdp
                    config bookmarks
                            edit "Mes fichiers sur Mars"
                                set apptype smb
                                set folder "\\mars"
                            next
                        end
                next
                edit 4
                    set type tool
                    set allow-apps web ftp smb ping
                next
            end
    next
end
```

Très intéressant car beaucoup de portail, choisi en fonction de l'utilisateur de tel groupe, et dont l'accès est limité à certaines adresses ip publiques.
Des groupes depuis un AD, ou de comptes locaux.

```
Forti-Ecotron # sh user ldap
config user ldap
    edit "VPN-Admins"
        set server "10.4.0.40"
        set cnid "sAMAccountName"
        set dn "OU=UoEcotron,DC=intraecotron,DC=fr"
        set type regular
        set username "CN=fortigate,CN=Users,DC=intraecotron,DC=fr"
        set password ENC
AAAApM7Sy2PQjGYVyVTaId5jVlvgcF5kVIF6e+GXv3rvTJ3b797+cTWu8TUlwpb+w5LNODXRadjgz6v0g6LEPwB
bHsc+P2qaaxR9gkl9CekYjepY
    next
    edit "VPN-Automates"
        set server "10.4.0.40"
        set cnid "sAMAccountName"
        set dn "OU=UoEcotron,DC=intraecotron,DC=fr"
        set type regular
        set username "CN=fortigate,CN=Users,DC=intraecotron,DC=fr"
        set password ENC
bamycCvPoKu6EtkfvgasbldMiRa19wKMNFwMqcg8YtbPzrpw+pKJYTScGEVjMXvjDLa4x3nbMNMnOWe6z/WuB7k
o4WSRoDN9yBYY9Fd9NxV2z8ZF
    next
    edit "Ecotron"
        set server "10.4.0.40"
        set cnid "cn"
        set dn "OU=UoEcotron,DC=intraecotron,DC=fr"
        set type regular
        set username "CN=fortigate,CN=Users,DC=intraecotron,DC=fr"
        set password ENC
C7ZcRyBT2XRF/EP5RSmJKkQDoxkYcFAgx7F3E8riONS+5/KnggWsA0qTYGBg5lP817jRZO/IMlIn18VpQYWOK9j
remQ0PZBZ92xwt3oy+KISl3JY
    next
end


Forti-Ecotron # sh user group
config user group
    edit "admin"
        set sslvpn-portal "Admin PC"
            set member "VPN-Admins"
            config match
                edit 1
                    set server-name "VPN-Admins"
                    set group-name "cn=VPN-
Admins,OU=AdminEcotron,OU=UoEcotron,DC=intraecotron,DC=fr"
                next
            end
    next
    edit "Telemaintenance"
        set sslvpn-portal "Telemaintenance S.Te.P"
            set member "step" "jgarnier"
    next
    edit "Astreinte"
        set sslvpn-portal "Automates astreinte"
            set member "VPN-Automates" "landais"
            config match
                edit 1
                    set server-name "VPN-Automates"
                    set group-name "cn=VPN-
Automates,OU=AdminEcotron,OU=UoEcotron,DC=intraecotron,DC=fr"
                next
            end
    next
    edit "SRC"
        set sslvpn-portal "SRC"
            set member "jgarnier"
    next
    edit "PRESTATAIRE-ASA"
        set sslvpn-portal "Prestataire-Asa"
            set member "V.Bouquet" "V.Bosquier"
    next
    edit "PRESTATAIRE-FELIX"
        set sslvpn-portal "Prestataire-Felix"
```

```
            set member "felix-f.vernadal" "felix-j.lanterno" "felix-j.thevenart"
"felix-l.cassin" "olivier.durant"
    next
end


Forti-Ecotron # sh vpn ssl settings
config vpn ssl settings
    set dns-server1 10.4.0.40
    set dns-server2 193.49.132.10
    set servercert "vpn.2012"
    set port 443
end


Forti-Ecotron # sh vpn ssl web portal
config vpn ssl web portal
    edit "Admin PC"
        set allow-access web ftp smb telnet ssh vnc rdp
        set cache-cleaner enable
        set theme orange
        set heading "Administration Ecotron"
        set page-layout double-column
            config widget
                edit 4
                    set name "Session Information"
                    set type info
                next
                edit 2
                    set name "Raccourcis"
                    set allow-apps web ftp smb telnet ssh vnc rdp
                        config bookmarks
                            edit "Exchange"
                                set apptype rdp
                                set host "10.4.0.50"
                                set screen-height 0
                                set screen-width 0
                                set keyboard-layout fr
                            next
                            edit "Controleur de domaine"
                                set apptype rdp
                                set host "10.4.0.40"
                                set screen-height 0
                                set screen-width 0
                                set keyboard-layout fr
                            next
                            edit "host 1"
                                set apptype rdp
                                set host "10.4.0.11"
                            next
                            edit "host 2"
                                set apptype rdp
                                set host "10.4.0.21"
                                set screen-height 0
                                set screen-width 0
                                set keyboard-layout fr
                            next
                            edit "Sharepoint"
                                set apptype rdp
                                set host "10.4.0.60"
                                set screen-height 0
                                set screen-width 0
                                set keyboard-layout fr
                            next
                            edit "Imprimante"
                                set url "10.4.0.81"
                            next
                            edit "Serveur Divers"
                                set apptype rdp
                                set host "10.4.0.70"
                            next
                        end
                next
                edit 3
                    set name "Connection Tool"
                    set type tool
                    set column two
```

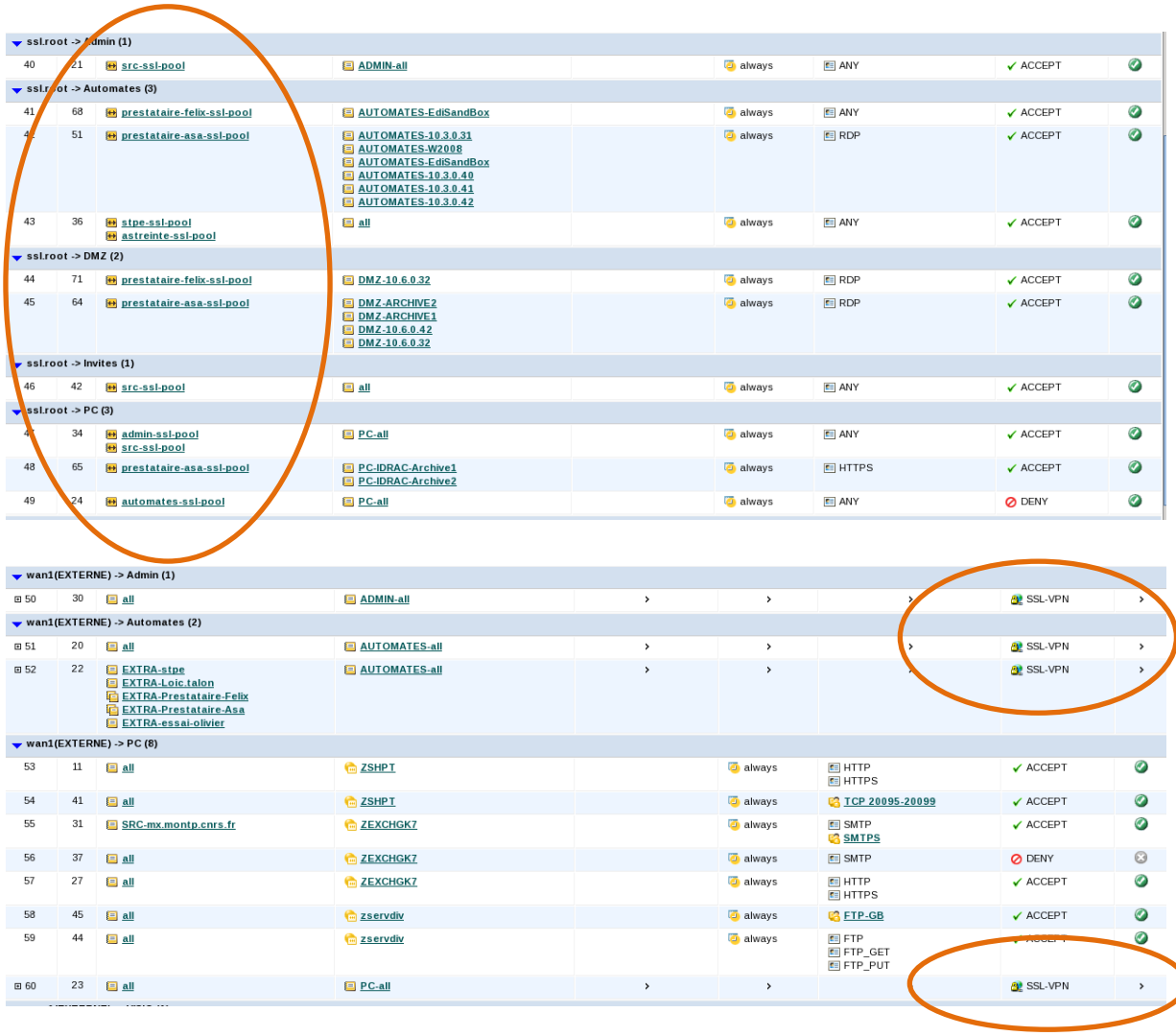
```
                set allow-apps web ftp smb telnet ssh vnc rdp
            next
            edit 1
                set name "Tunnel Mode"
                set type tunnel
                set column two
                set tunnel-status enable
                set split-tunneling enable
                    set ip-pools "admin-ssl-pool"
                    set split-tunneling-routing-address "split-PC-Subnet"
            next
        end
    next
    edit "Telemaintenance S.Te.P"
        set allow-access web ftp smb telnet ssh vnc rdp ping
        set host-check av
        set cache-cleaner enable
        set heading "Telemaintenance S.Te.P"
        set page-layout double-column
        set allow-user-bookmark disable
            config widget
                edit 3
                    set name "Connection Tool"
                    set type tool
                    set allow-apps web ftp smb telnet ssh vnc rdp ping
                next
                edit 1
                    set name "Raccourcis"
                    set allow-apps web smb ssh vnc rdp
                        config bookmarks
                            edit "Supervision 2"
                                set apptype rdp
                                set host "10.3.0.18"
                                set screen-height 0
                                set screen-width 0
                                set keyboard-layout fr
                            next
                            edit "Supervision CO2"
                                set apptype rdp
                                set host "10.3.0.25"
                                set screen-height 0
                                set screen-width 0
                                set keyboard-layout fr
                            next
                            edit "Serveur 2008"
                                set apptype rdp
                                set host "10.3.0.30"
                                set screen-height 0
                                set screen-width 0
                                set keyboard-layout fr
                            next
                            edit "Base de donnees"
                                set apptype rdp
                                set host "10.3.0.31"
                                set screen-height 0
                                set screen-width 0
                                set keyboard-layout fr
                            next
                            edit "vDSC2"
                                set apptype rdp
                                set host "10.3.0.41"
                                set screen-height 0
                                set screen-width 0
                                set keyboard-layout fr
                            next
                            edit "vMYSQL2"
                                set apptype rdp
                                set host "10.3.0.42"
                                set screen-height 0
                                set screen-width 0
                                set keyboard-layout fr
                            next
                        end
                next
                edit 2
                    set name "Tunnel Mode"
                    set type tunnel
```

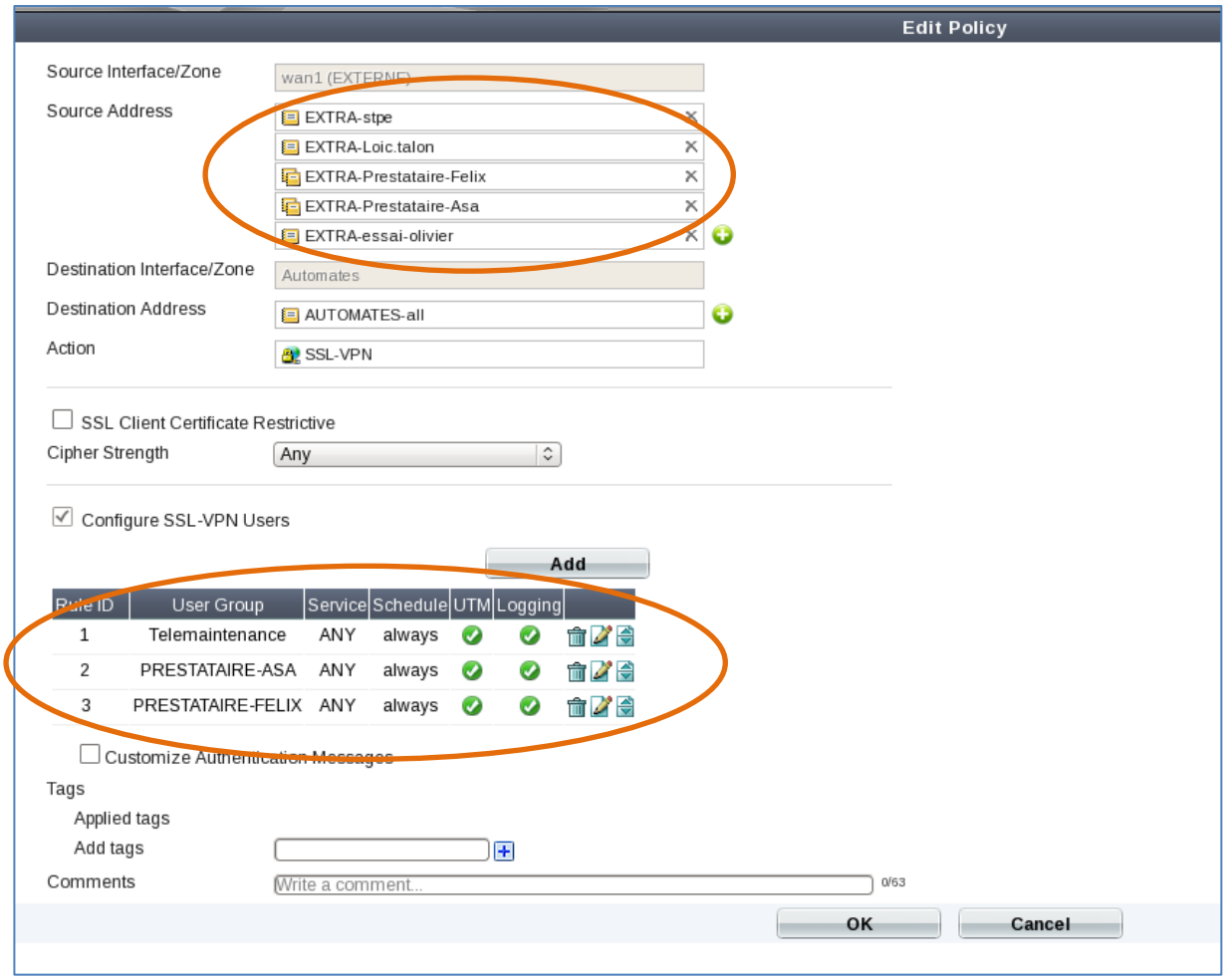
```
                    set column two
                    set tunnel-status enable
                    set split-tunneling enable
                        set ip-pools "stpe-ssl-pool"
                next
                edit 4
                    set name "Session Information"
                    set type info
                    set column two
                next
            end
    next
    edit "Automates astreinte"
        set allow-access web ftp smb telnet ssh vnc rdp ping
        set theme gray
        set heading "Accès aux automates"
        set page-layout double-column
        set allow-user-bookmark disable
            config widget
                edit 3
                    set name "Tunnel Mode"
                    set type tunnel
                    set tunnel-status enable
                    set split-tunneling enable
                    set ip-mode usrgrp
                        set ip-pools "astreinte-ssl-pool"
                        set split-tunneling-routing-address "split-AUTOMATES-subnet"
                next
                edit 1
                    set name "Bookmarks"
                    set allow-apps web vnc rdp
                        config bookmarks
                            edit "Supervision 2"
                                set apptype rdp
                                set host "10.3.0.18"
                                set screen-height 0
                                set screen-width 0
                                set keyboard-layout fr
                            next
                            edit "Supervision CO2"
                                set apptype rdp
                                set host "10.3.0.25"
                                set screen-height 0
                                set screen-width 0
                                set keyboard-layout fr
                            next
                            edit "passerelle ecotron"
                                set apptype rdp
                                set description "Serveur DSC, ne pas arrêter
l'application. Accès réservé."
                                set host "10.3.0.19"
                                set screen-height 0
                                set screen-width 0
                                set keyboard-layout fr
                            next
                            edit "Serveur 2008"
                                set apptype rdp
                                set host "10.3.0.30"
                                set screen-height 0
                                set screen-width 0
                                set keyboard-layout fr
                            next
                            edit "Base de donnees"
                                set apptype rdp
                                set host "10.3.0.31"
                                set screen-height 0
                                set screen-width 0
                                set keyboard-layout fr
                            next
                            edit "Supervision Microsomes"
                                set apptype rdp
                                set description "Supervision des Microsomes"
                                set host "10.3.0.90"
                                set full-screen-mode enable
                                set screen-height 0
                                set screen-width 0
                                set keyboard-layout fr
```

```
                            next
                            edit "vDSC2"
                                set apptype rdp
                                set host "10.3.0.41"
                                set screen-height 0
                                set screen-width 0
                                set keyboard-layout fr
                            next
                            edit "vMYSQL2"
                                set apptype rdp
                                set host "10.3.0.42"
                                set screen-height 0
                                set screen-width 0
                                set keyboard-layout fr
                            next
                        end
                next
                edit 2
                    set name "Outil de connexion"
                    set type tool
                    set column two
                    set allow-apps vnc rdp ping
                next
            end
    next
    edit "automates Full"
        set allow-access web ftp smb telnet ssh vnc rdp ping
        set theme gray
        set heading "Acces automates COMPLET"
        set page-layout double-column
        set allow-user-bookmark disable
            config widget
                edit 4
                    set name "Session Information"
                    set type info
                next
                edit 1
                    set name "Bookmarks"
                    set allow-apps web
                next
                edit 2
                    set name "Connection Tool"
                    set type tool
                    set column two
                    set allow-apps web ftp smb telnet ssh vnc rdp
                next
                edit 3
                    set name "Tunnel Mode"
                    set type tunnel
                    set column two
                    set tunnel-status enable
                        set ip-pools "automates-ssl-pool"
                next
            end
    next
    edit "SRC"
        set allow-access web ftp smb telnet ssh vnc ping
        set host-check av
        set cache-cleaner enable
        set theme orange
        set heading "Welcome to SSL VPN SRC"
        set page-layout double-column
        set allow-user-bookmark disable
            config widget
                edit 4
                    set name "Information de session"
                    set type info
                next
                edit 1
                    set name "Bookmarks"
                    set allow-apps web ssh
                        config bookmarks
                            edit "FIrewall"
                                set url "10.2.0.1"
                            next
                            edit "SWITCH 1"
                                set apptype ssh
```

```
                                set host "10.2.0.10"
                            next
                            edit "SWITCH 2"
                                set apptype ssh
                                set host "10.2.0.2"
                            next
                            edit "SWITCH 3"
                                set apptype ssh
                                set host "10.2.0.3"
                            next
                            edit "SWITCH 4"
                                set apptype ssh
                                set host "10.2.0.4"
                            next
                        end
                next
                edit 2
                    set name "Connection Tool"
                    set type tool
                    set column two
                    set allow-apps web ftp smb telnet ssh vnc rdp
                next
                edit 3
                    set name "Mode tunnel"
                    set type tunnel
                    set column two
                    set tunnel-status enable
                    set split-tunneling enable
                        set ip-pools "src-ssl-pool"
                        set split-tunneling-routing-address "split-ADMIN-subnet"
                next
            end
    next
    edit "Admin"
            config widget
                edit 2
                    set name "Tunnel Mode"
                    set type tunnel
                    set tunnel-status enable
                    set split-tunneling enable
                        set ip-pools "admin-ssl-pool"
                        set split-tunneling-routing-address "split-AUTOMATES-subnet"
"split-PC-Subnet" "split-ADMIN-subnet"
                next
                edit 3
                    set type tool
                    set allow-apps web smb telnet ssh rdp ping
                next
            end
    next
    edit "Prestataire-Felix"
        set heading "SSLVPN - Prestataire FELIX"
        set page-layout double-column
            config widget
                edit 4
                    set name "Session Information"
                    set type info
                next
                edit 3
                    set name "CONNEXION"
                    set type tunnel
                    set column two
                    set tunnel-status enable
                    set split-tunneling enable
                        set ip-pools "prestataire-felix-ssl-pool"
                        set split-tunneling-routing-address "split-AUTOMATES-subnet"
"split-DMZ-Subnet"
                next
            end
    next
    edit "Prestataire-Asa"
        set heading "VPNSSL - Prestataire ASA"
        set page-layout double-column
        set allow-user-bookmark disable
            config widget
                edit 4
                    set name "Session Information"
```

```
                    set type info
                next
                edit 3
                    set name "Tunnel Mode"
                    set type tunnel
                    set column two
                    set tunnel-status enable
                    set split-tunneling enable
                        set ip-pools "prestataire-asa-ssl-pool"
                        set split-tunneling-routing-address "split-AUTOMATES-subnet"
"split-PC-Subnet" "split-DMZ-Subnet"
                next
            end
    next
end
```




Edit Policy
Source Interface/Zone
wan1 (EXTERNE)
Source Address
EXTRA-stpe
EXTRA-Loic.talon
EXTRA-Prestataire-Felix
EXTRA-Prestataire-Asa
EXTRA-essai-olivier
Destination Interface/Zone
Automates
Destination Address
AUTOMATES-all
Action
SSL-VPN
SSL Client Certificate Restrictive
Cipher Strength
Any
Configure SSL-VPN Users
Add
Rule ID
User Group
Service
Schedule
UTM
Logging
1
Telemaintenance
ANY
always
2
PRESTATAIRE-ASA
ANY
always
3
PRESTATAIRE-FELIX
ANY
always
Customize Authentication Messages
Tags
Applied tags
Add tags
Comments
Write a comment...
0/63
OK
Cancel

.