Institut supérieur d'informatique

Projet d'intégration II

Conception et design d'un réseau informatique

Présenté par :

Yvan florent Moukouo

Didoungou junyor

CONTEXTE

Dans le cadre de la mise en place du réseau informatique il nous a été demandé de mettre en place une solution de déploiement.

Pour cela nous avons procédé de la manière suivante:
-Recenser les solutions existantes

-Justifier le choix d'une solution

-Mettre en œuvre la solution choisie

1. ***Présentation globale de la solution (infrastructure reseau***

Selon les besoins de l'entreprise notre équipe a décidé de monter le réseau suivant:

-Pour la conception générale de la structure réseau nous avons décidé de segmenter notre réseau en 3 parties (LAN, DMZ, WAN):

-LAN: Un local area network (LAN) défini comme étant un groupe d'ordinateurs et de périphériques qui partagent une ligne de communication commune ou un lien sans fil ou avec fil avec un ou plusieurs serveurs dans une zone géographique distincte. Dans notre cas le réseau LAN va nous permettre de gérer le flux du réseau interne de l'entreprise (clients et serveurs internes)

-DMZ: Un réseau DMZ est un réseau de périmètre qui protège et ajoute une couche de sécurité supplémentaire au réseau local interne d'une organisation contre le trafic non approuvé. Une DMZ commune est un sous-réseau situé entre l'Internet public (WAN) et les réseaux privés (LAN).

-WAN : est un réseau informatique ou un réseau de télécommunications couvrant une grande zone géographique, typiquement à l'échelle d'un pays, d'un continent, ou de la planète entière. Le plus grand WAN est le réseau Internet.

Nous allons aussi utiliser un firewall checkpoint. Le firewall est un appareil de sécurité réseau qui surveille le trafic réseau entrant et sortant et autorise ou bloque les paquets de donnés en se basant sur un ensemble de règles de sécurité. Il est chargé de dresser une barrière entre votre réseau interne et le trafic entrant provenant de sources externes (comme Internet) afin de bloquer le trafic malveillant des virus et des pirates.

Le firewall logiciel va nous permettre directement de configurer la détection des failles informatiques, l'antivirus, le proxy et mettre en place un ids/ips.

Pour tous les services, les serveurs, les VM des utiliseurs que nous allons utiliser pour le bon fonctionnement de l'entreprise nous allons opter pour les esxi. ESXi est un hyperviseur de type 1, ce qui signifie qu'il s'exécute directement sur le matériel du système sans avoir besoin d'un système d'exploitation. Les hyperviseurs de type 1 sont également appelés hyperviseurs bare metal car ils s'exécutent directement sur le matériel. Les hyperviseurs permettent d'exécuter efficacement plusieurs machines virtuelles sur un serveur physique. Ces machines virtuelles auront tous les services nécessaires.

2. ***Critère de l'entreprise et solution***

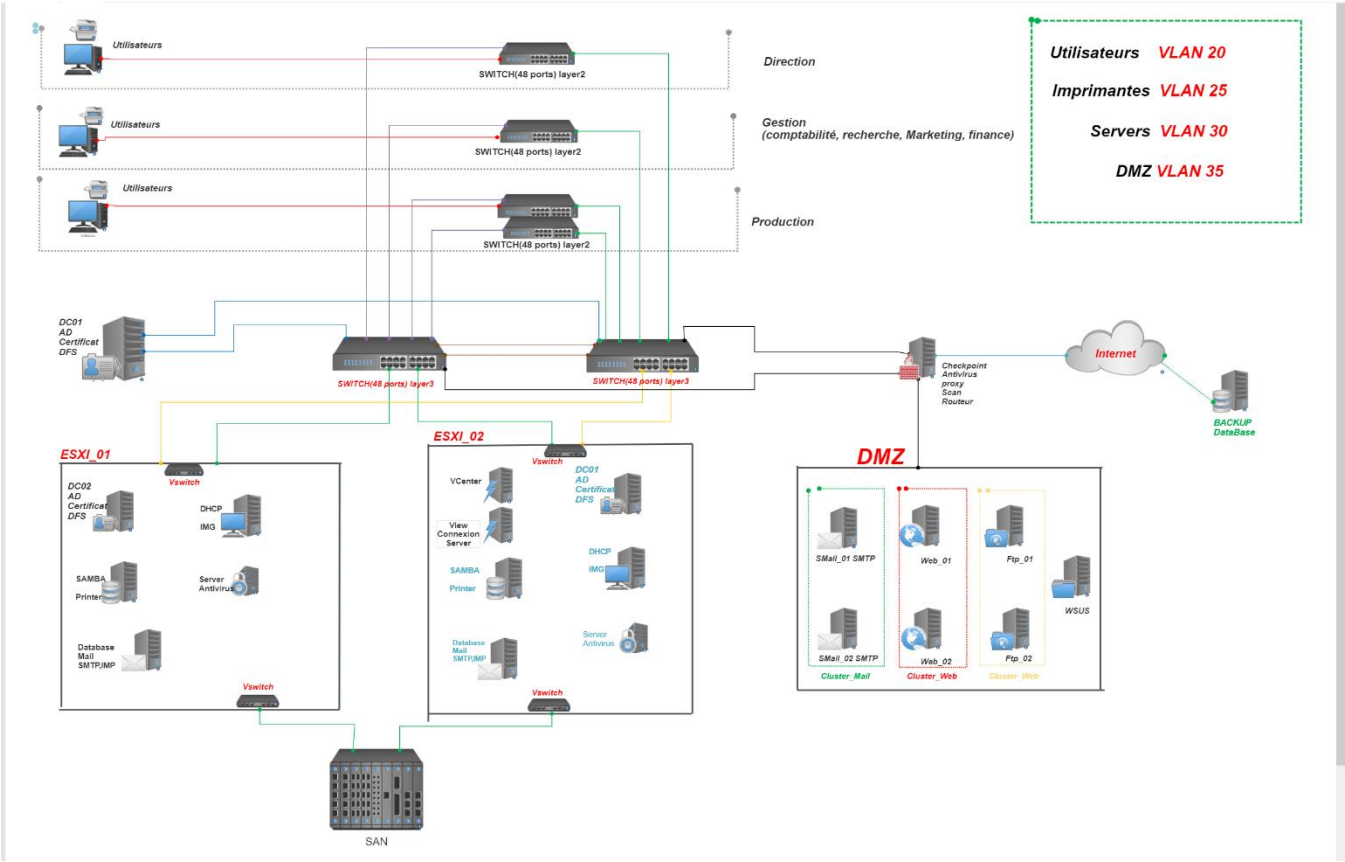
Pour le bon fonctionnement de son entreprise, le client a proposé les besoins suivants:

L'entreprise doit être équipé d'un pare-feu (pfsense ou opensense), une administration centralisées des utilisateurs et de leur mots de passe, avoir une tolérance de panne au niveau des serveurs fondamentaux, tous les serveurs doivent être accessibles via rdp à l'interne et à l'externe, obliger tous les utilisateurs à changer leur mot de passe tous les 30 jours, chaque utilisateurs possède un répertoire personnel U, reteindre tous les ordinateurs/utilisateurs du réseau Microsoft store, avoir un serveur d'antivirus centralisé, serveur linux avec l'installation d'un site web, un certificat ssl pour le site web et un IPS/IDP(snort)

Pour la présentation de notre infrastructure, nous avons opter pour 2 différents réseaux. Le premier sera le réseau que nous allons présenter à l'entreprise avec tous le matérielles nécessaire et le second sera celui que nous allons implanter en classes avec le matérielles physique mis à notre disposition à cet effet.

a) **Première solution**

La première solution représente le réseau physique et virtuel mais que nous n'allons pas implanter à défaut de manque de matériel mais:



Nous allons mettre en place 2 esxi, le esxi va nous permettre de créer différentes machines virtuelles avec différents services. Les deux esxi seront administré par un VCenter qui va nous permettre la gestion centralisée de nos différentes machines et démarrer les différents servers dans l'un des deux esxi en fonction des ressources CPU et RAM.

Dans le premier esxi nous aurons comme server:

- Un server DC02 qui fera office de backup de tous les objets de l'active directory principal
- Un serveur DHCP pour fournir les adresse ip aux clients
- Un server samba pour faire l'impression et la partage des données entres les utilisateurs
- Un serveur d'antivirus
- Un serveur qui fera office de base de données pour le mail

Dans le deuxième esxi nous allons utiliser comme server:

- Un serveur VCenter qui va nous permettre la gestion centralisée de nos différentes machines présentes sur les esxi et permettre en cas de panne d'un esxi ou de problème lies avec les ressources du esxi cpu ram de le démarrer la ou les serveurs virtuels dans le second esxi2
- Un serveur view connexion qui va nous permettre la gestion des postes de travail et d'application à distance

Les 2 esxi vont être relier directement à un serveur **SAN** Un réseau de stockage ou SAN (Storage Area Network) est un réseau spécifiquement dédié à l'interconnexion de ressources de stockage en mode bloc avec des serveurs. Il permet à un serveur d'accéder à des ressources de stockage distantes comme s'il s'agissait d'un disque dur local. Lorsqu'un hôte désire accéder à des données sur une baie de stockage SAN, il lui suffit d'envoyer la commande SCSI appropriée et les informations lui seront retournées via le réseau. L'intérêt majeur des SAN est qu'ils ont permis de mutualiser une ressource coûteuse, le stockage, entre de multiples serveurs, tout en simplifiant l'administration du stockage via des politiques définies et appliquées de façon centralisée (gestion des ressources, gestion des droits d'accès, qualité de service, sauvegarde…).

Pour tous les services qui seront directement exposé à internet nous allons utiliser une dmz, la DMZ zone démilitarisée, est le sous-réseau physique qui sépare un réseau local (LAN) des autres réseaux non approuvés généralement l'Internet public. Tout service fourni aux utilisateurs sur l'internet public devrait être placé dans le réseau DMZ. Les serveurs, ressources et services externes s'y trouvent généralement. Certains des plus courants de ces services comprennent le Web, la messagerie électronique, et le protocole de transfert

de fichiers Les serveurs et les ressources de la DMZ sont accessibles depuis Internet, mais le reste du réseau local interne reste inaccessible. Cette approche fournit une couche de sécurité supplémentaire au réseau local car elle limite la capacité d'un pirate à accéder directement aux serveurs internes et aux données à partir d'Internet. Plus d'information

Les pirates et les cybercriminels peuvent accéder aux systèmes exécutant des services sur des serveurs DMZ. Ces serveurs doivent être renforcés pour résister à des attaques constantes. Le terme *DMZ* vient de la zone tampon géographique qui a été mise en place entre la Corée du Nord et la Corée du Sud à la fin de la guerre de Corée.

Dans cette zone dmz nous aurons 2 serveurs web, 2 serveurs mail, 2 serveurs ftp et un serveur wsus

- Le serveur web va nous permettre d'héberger le site web, nous allons utiliser le cms WordPress
- Le serveur mail va nous permettre d'envoyer des mails de l'interne depuis l'externe
- Le serveur ftp va nous permettre de transférer les fichier interne depuis internet

Tous les serveurs en double seront dans le même cluster, le cluster va nous permettre d'avoir une redondance au niveau des services dans le cas où une machine tombe en panne.

Toutes les ressources de la san sont copiée chez un hébergeur à partir cloud en cas de panne général.

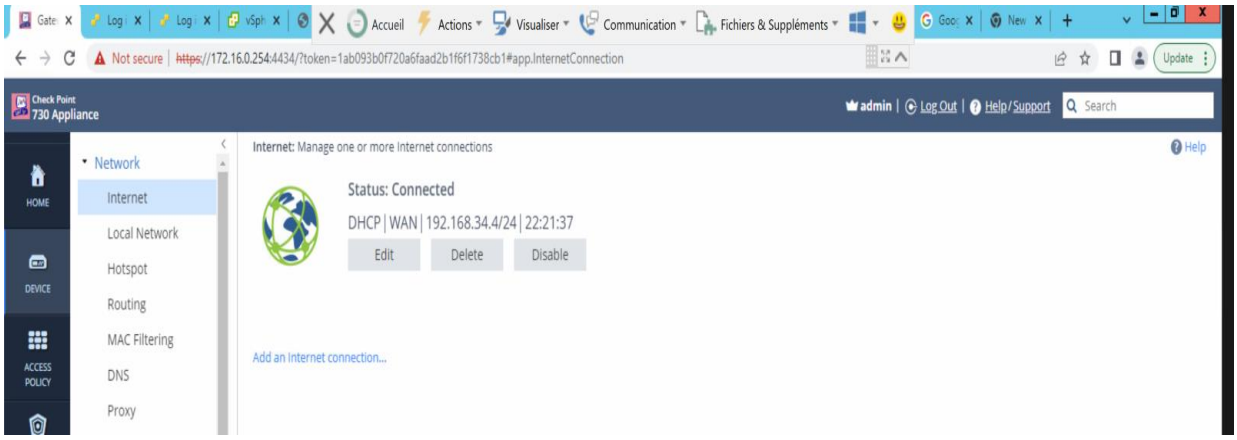
b) Deuxième solution

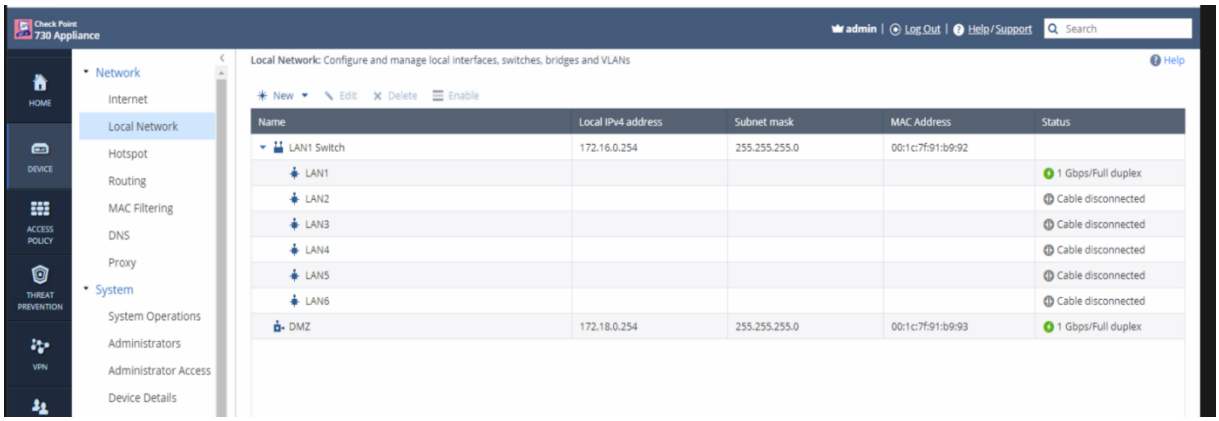
Nous allons apporter des solutions directes aux critères voulus par l'entreprise et plusieurs autres solutions que nous trouvons pertinent et idéal pour l'entreprise. Ici nous utiliserons aussi les esxi pour les services et aussi le ftp et le serveur web dans la dmz.

- **L'entreprise doit être équipé d'un pare-feu:**

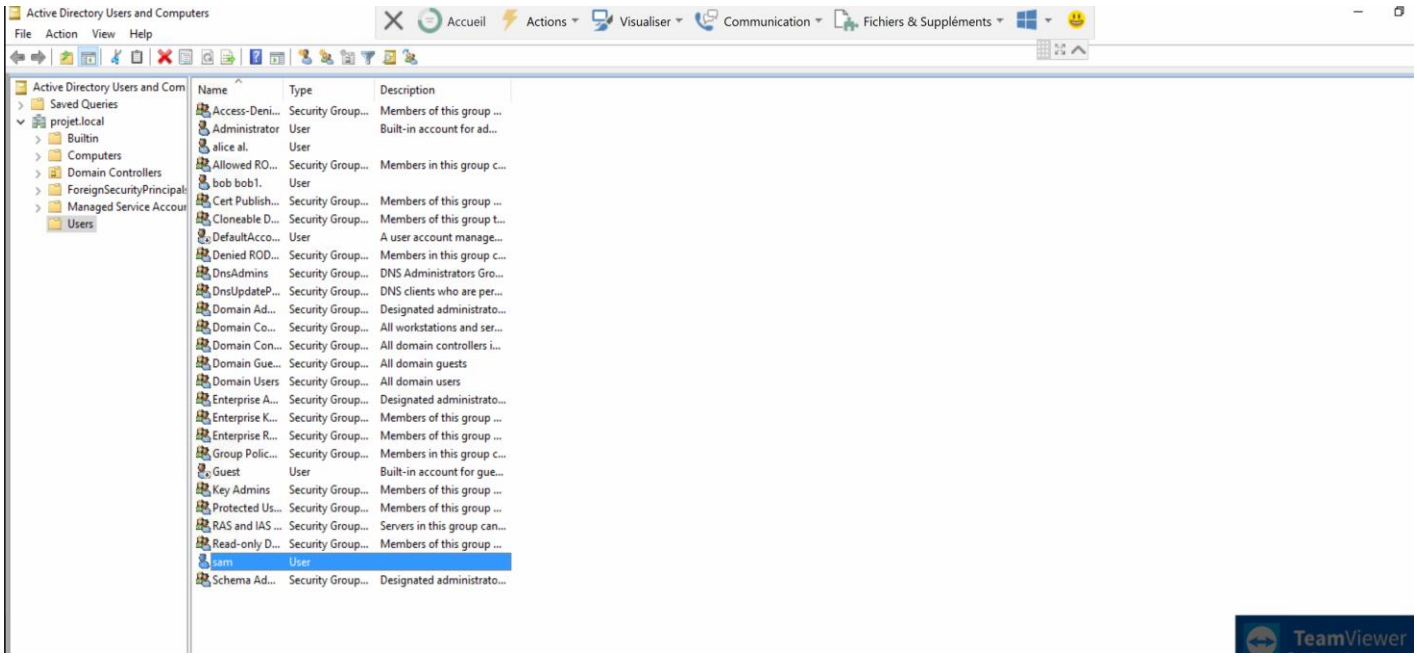
Un firewall physique est un équipement installé entre votre réseau et la passerelle d'accès. le firewall à filtrage de paquets, le type le plus courant, examinent les paquets et leur interdisent de passer s'ils ne correspondent pas à un ensemble de règles de sécurité établies. Ce type de firewall vérifie les adresses IP source et destination du paquet. Si les paquets correspondent à ceux d'une règle "autorisée" sur le firewall, alors on lui fait confiance pour entrer sur le réseau.

ici nous avons utilisé le firewall physique de checkpoint.

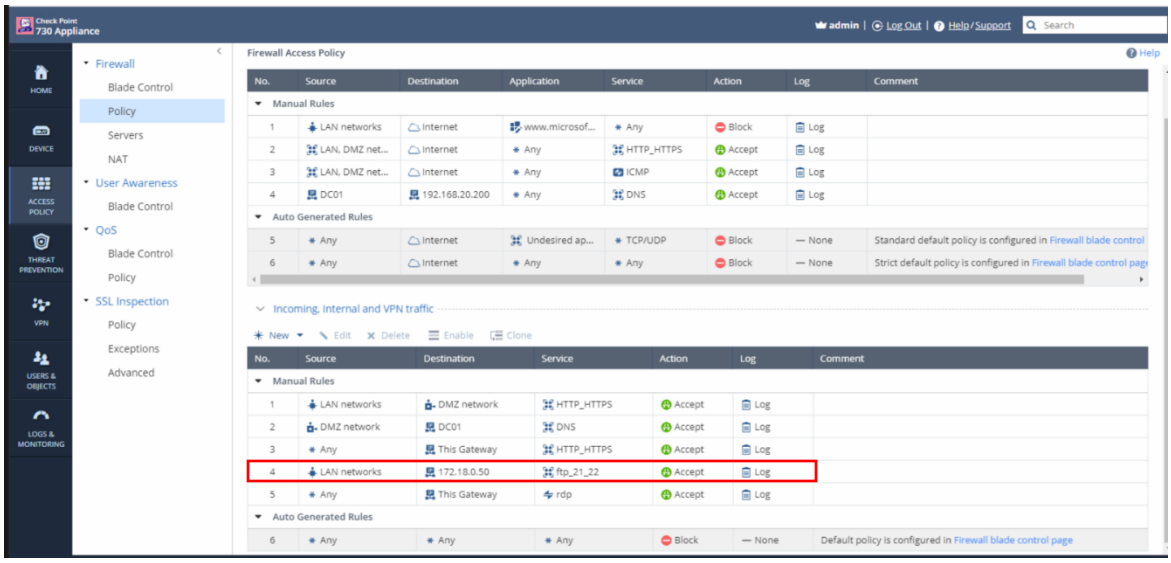


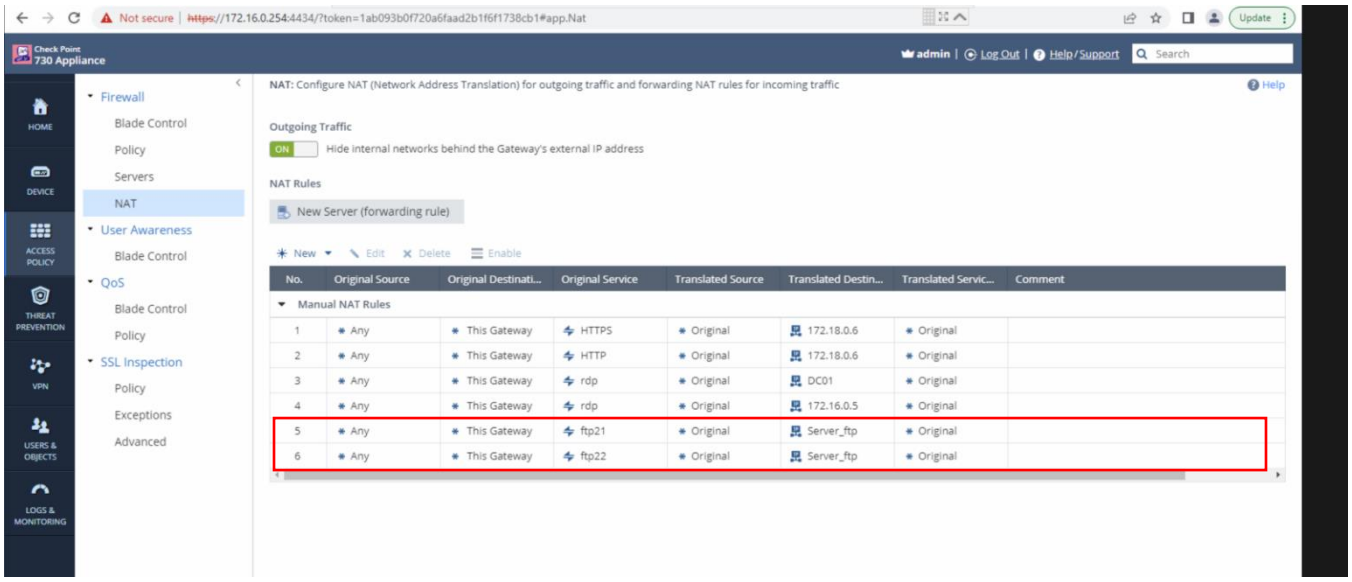


- **Une administration centralisée des utilisateurs et de leur mot de passe:** pour cela nous allons utiliser active directory

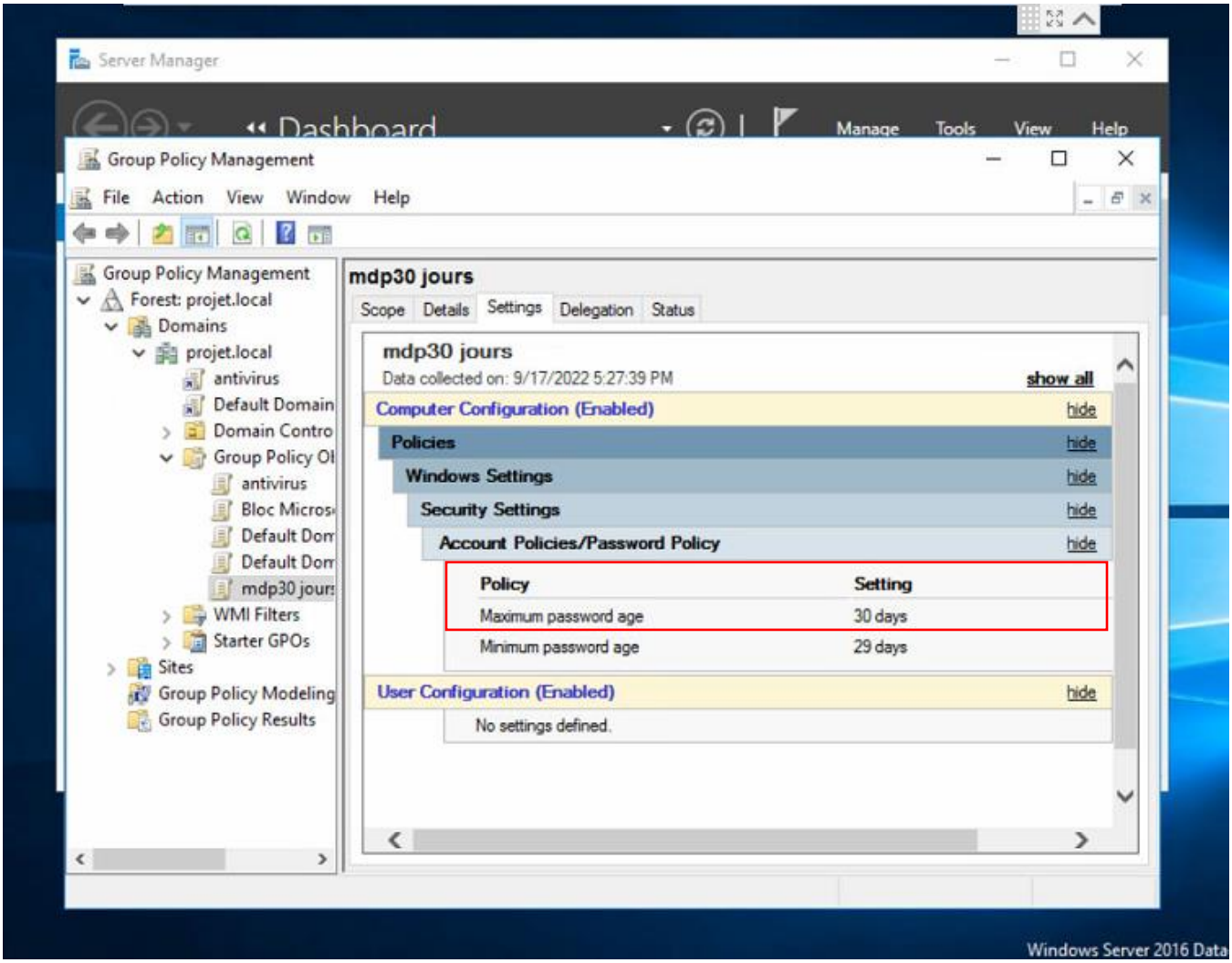


- **Tous les serveurs doivent être accessibles via rdp à l'interne et à l'externe:** ici nous avons configurer des règles dans le firewall pour autoriser ce Traffic

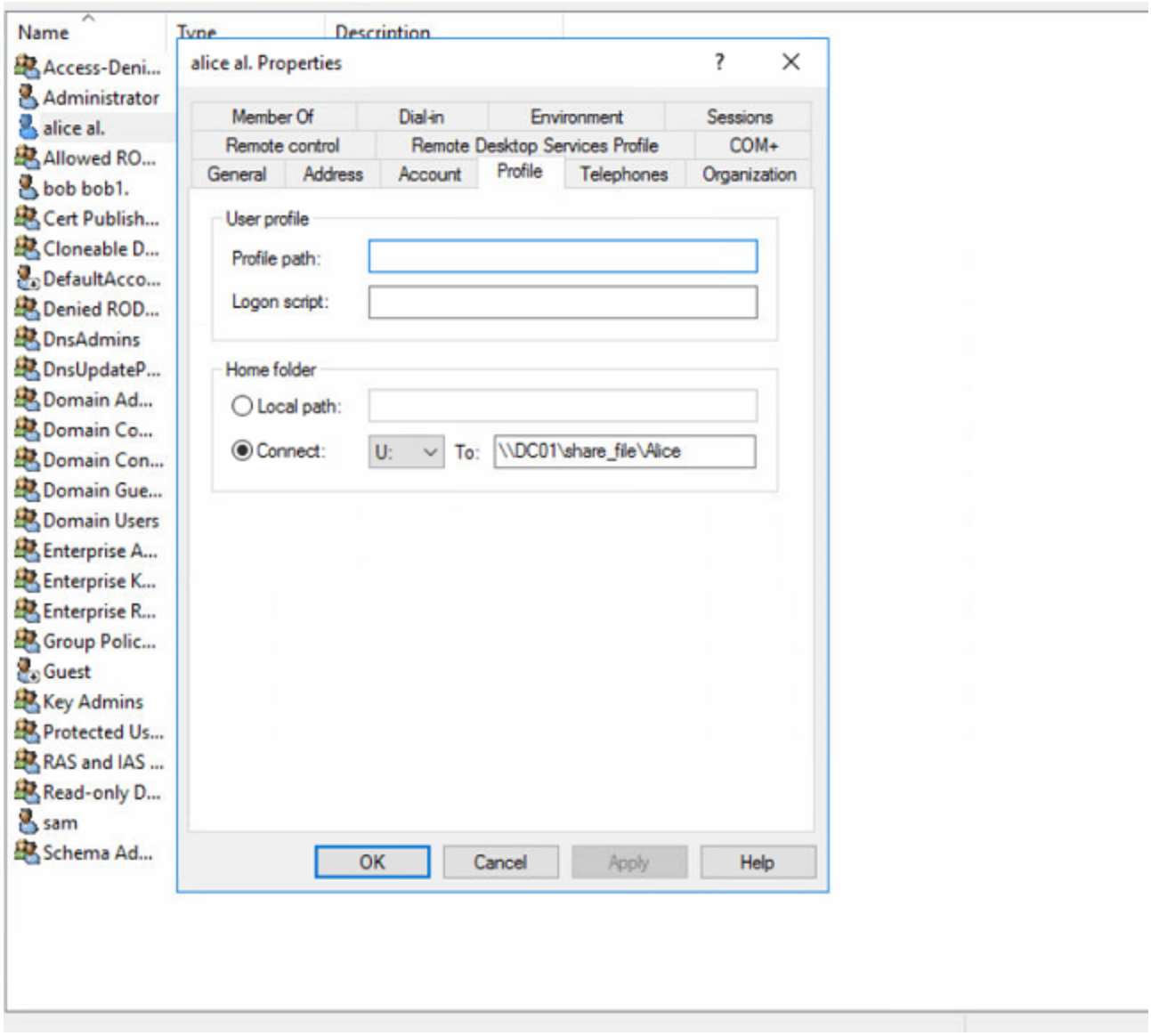

Check Point
730 Appliance
admin | Log Out | Help/Support
Search
HOME
DEVICE
ACCESS POLICY
THREAT PREVENTION
VPN
USERS & OBJECTS
LOGS & MONITORING
Firewall
Blade Control
Policy
Servers
NAT
User Awareness
Blade Control
QoS
Blade Control
Policy
SSL Inspection
Policy
Exceptions
Advanced
Firewall Access Policy
Help
No. Source Destination Application Service Action Log Comment
Manual Rules
1 LAN networks Internet www.microsof... Any Block Log
2 LAN, DMZ net... Internet Any HTTP_HTTPS Accept Log
3 LAN, DMZ net... Internet Any ICMP Accept Log
4 DC01 192.168.20.200 Any DNS Accept Log
Auto Generated Rules
5 Any Internet Undesired ap... TCP/UDP Block None Standard default policy is configured in Firewall blade control
6 Any Internet Any Any Block None Strict default policy is configured in Firewall blade control page
Incoming, Internal and VPN traffic
New Edit Delete Enable Clone
No. Source Destination Service Action Log Comment
Manual Rules
1 LAN networks DMZ network HTTP_HTTPS Accept Log
2 DMZ network DC01 DNS Accept Log
3 Any This Gateway HTTP_HTTPS Accept Log
4 LAN networks 172.18.0.50 ftp_21_22 Accept Log
5 Any This Gateway rdp Accept Log
Auto Generated Rules
6 Any Any Any Block None Default policy is configured in Firewall blade control page



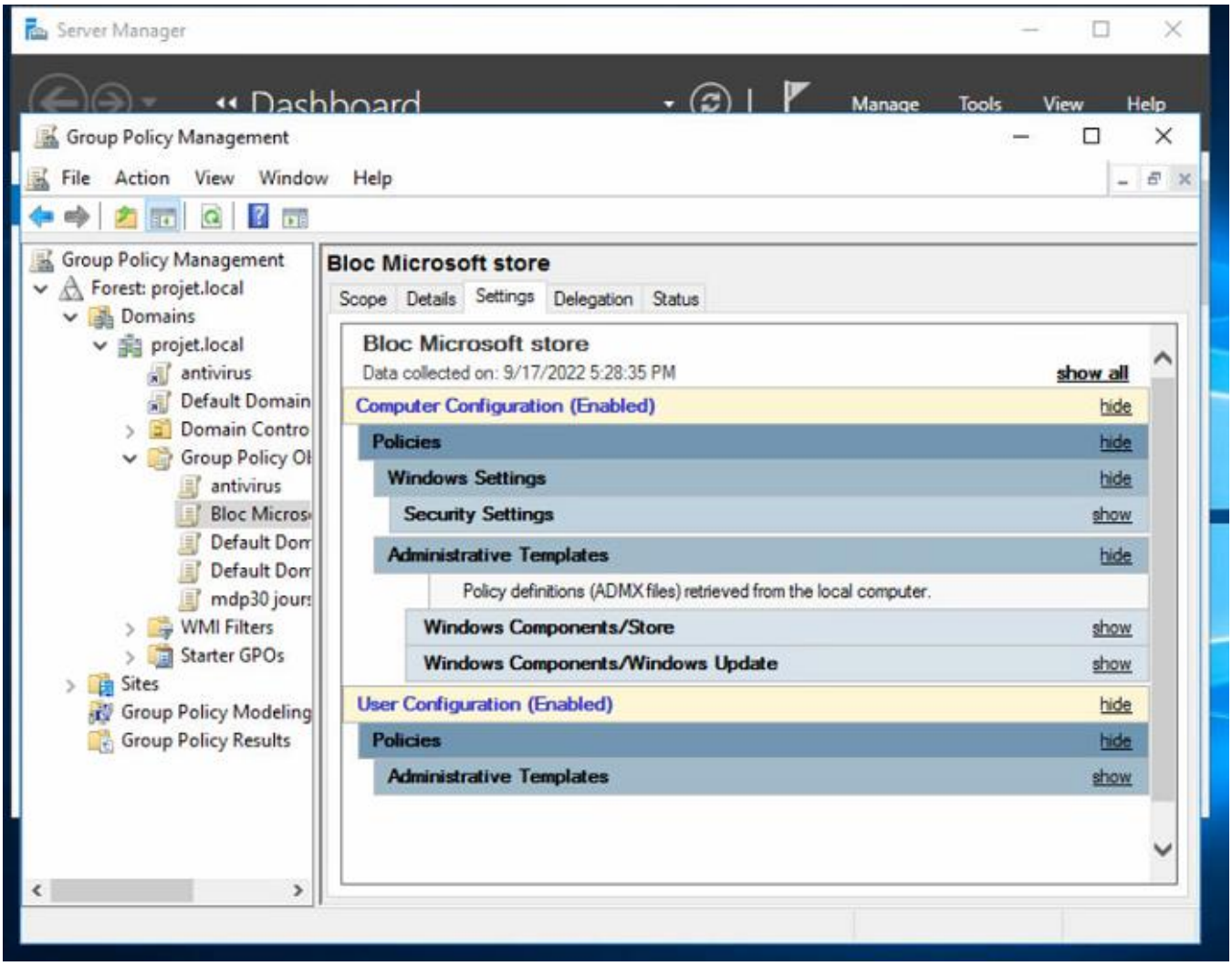
- **obliger tous les utilisateurs à changer leur mot de passe tous les 30 jours :** ici nous allons utiliser les GPO

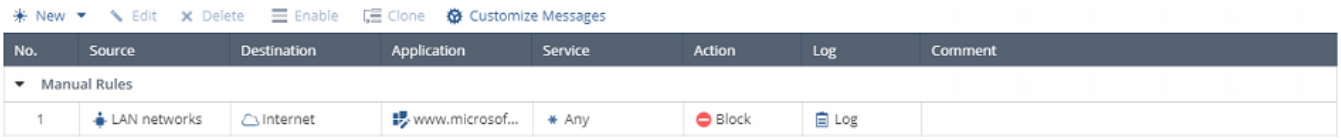


- **Chaque utilisateur possède un répertoire personnel U :**

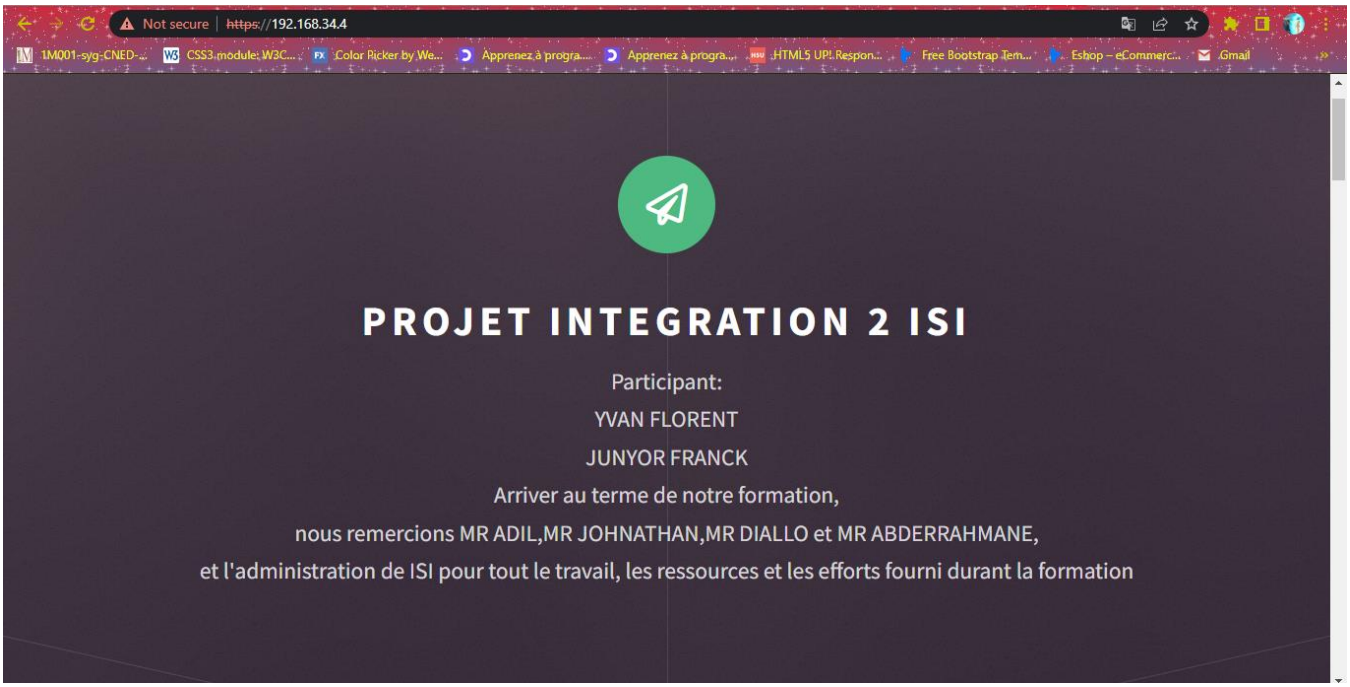

Name
Type
Description
Access-Deni...
Administrator
alice al.
Allowed RO...
bob bob1.
Cert Publish...
Cloneable D...
DefaultAcco...
Denied ROD...
DnsAdmins
DnsUpdateP...
Domain Ad...
Domain Co...
Domain Con...
Domain Gue...
Domain Users
Enterprise A...
Enterprise K...
Enterprise R...
Group Polic...
Guest
Key Admins
Protected Us...
RAS and IAS ...
Read-only D...
sam
Schema Ad...
alice al. Properties
?
Member Of
Dial-in
Environment
Sessions
Remote control
Remote Desktop Services Profile
COM+
General
Address
Account
Profile
Telephones
Organization
User profile
Profile path:
Logon script:
Home folder
Local path:
Connect:
U:
To:
\\DC01\share_file\Alice
OK
Cancel
Apply
Help

- **Restreindre tous les ordinateurs/utilisateurs du réseau Microsoft store :** ici on peut le faire soit par gpo ou par règles dans le firewall





- **Serveur linux avec l'installation d'un site web :**



- **Un certificat ssl pour le site site web :**

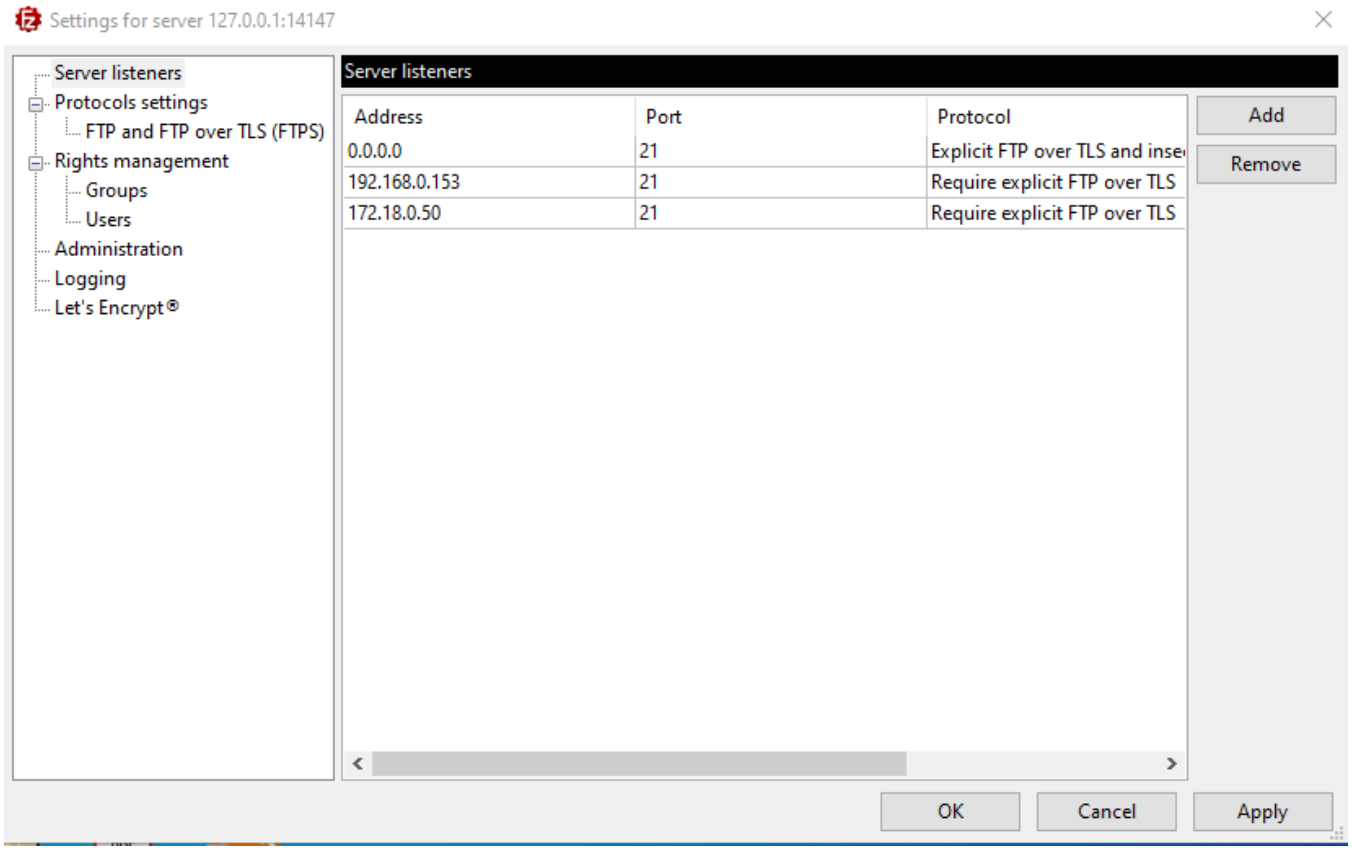
Nous avons utiliser des certificats des certificat Auto signé (SLEF-SIGNED ssl certificat) raison pour la quelle le site affiche Not secure

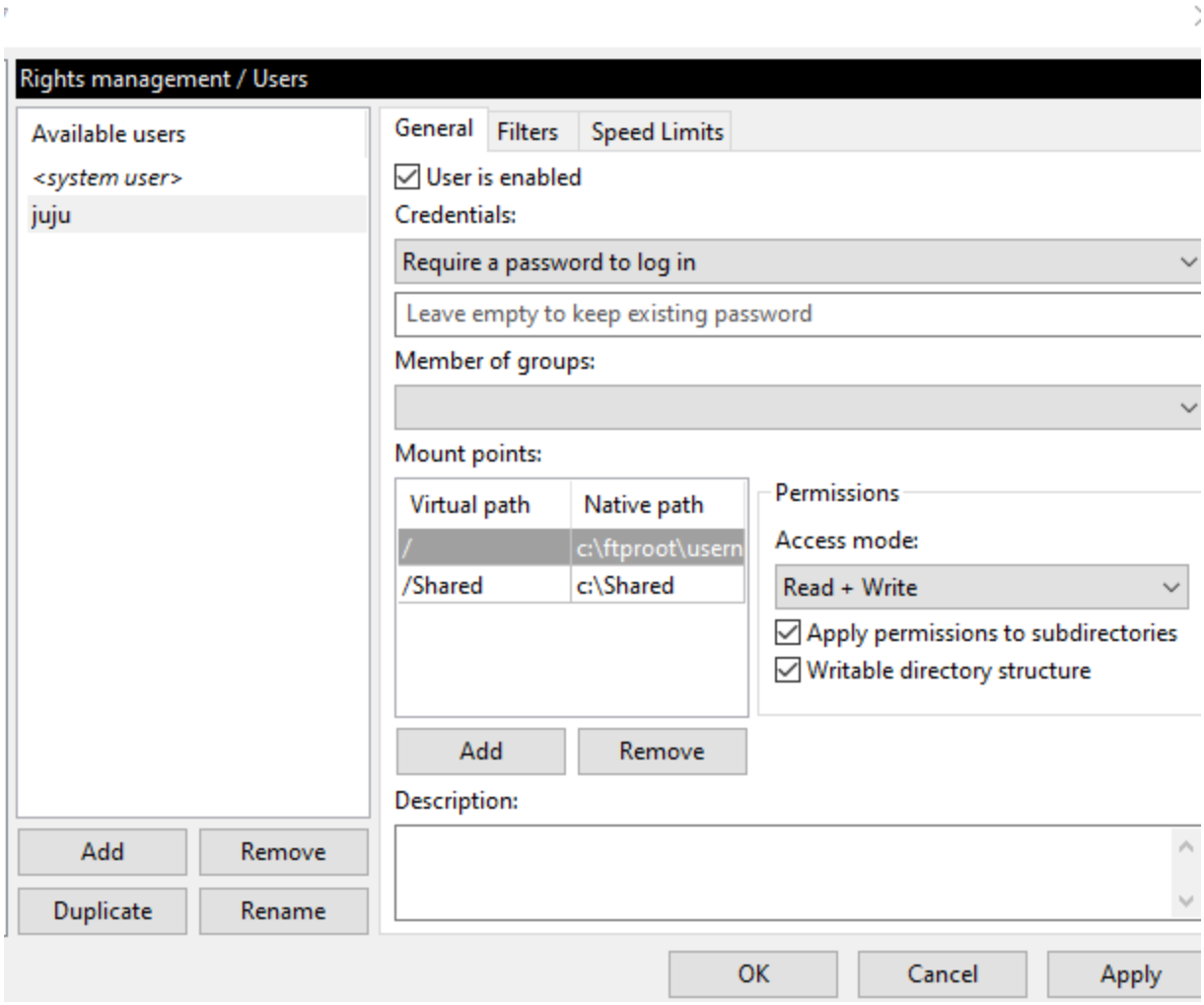
- **Et enfin avoir un ids/ips :** notre firewall checkpoint a déjà un service ids/ips activé et en fonction.

En dehors des critères voulus par l'entreprise nous avons aussi configurée :

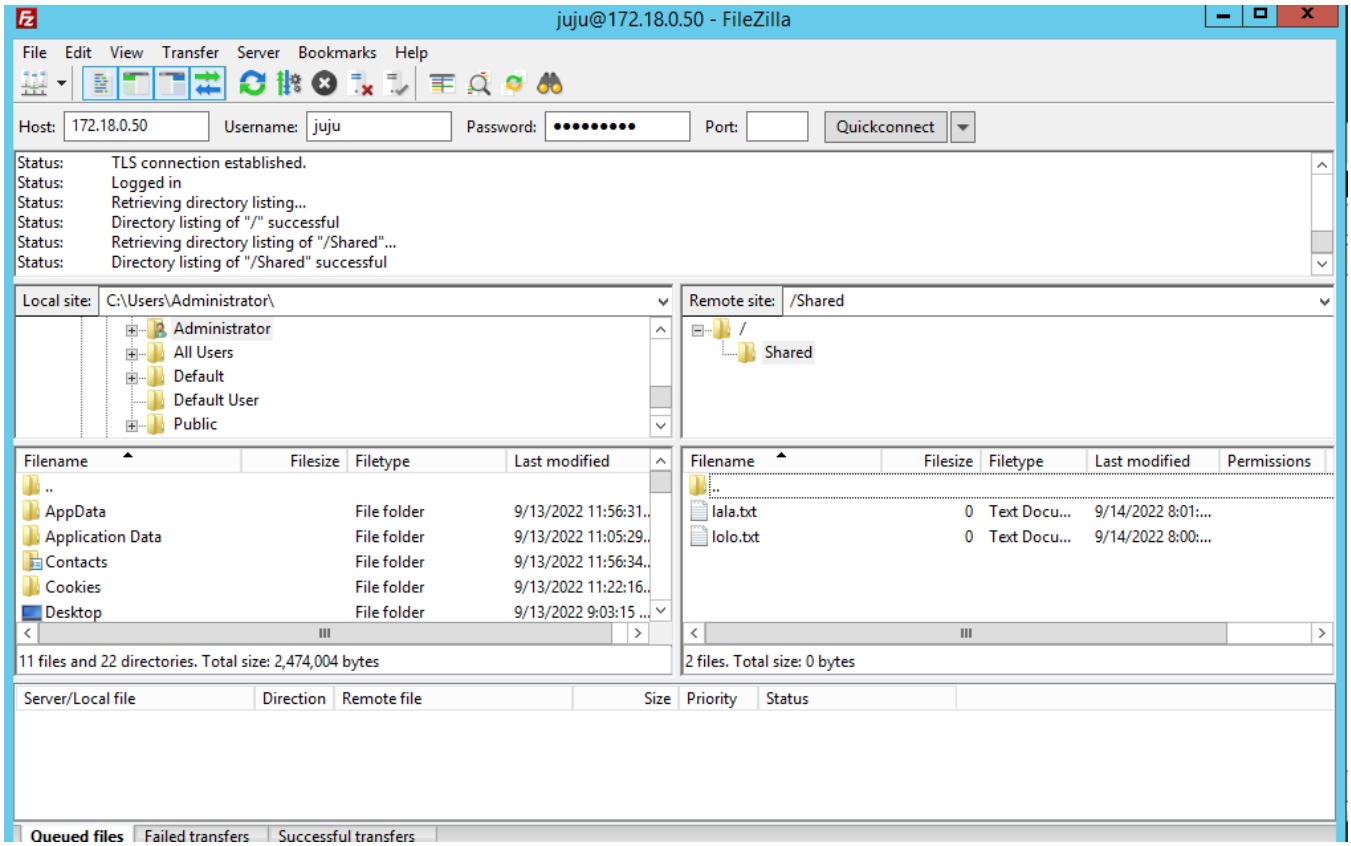
Un serveur ftp

Configuration cotes serveurs

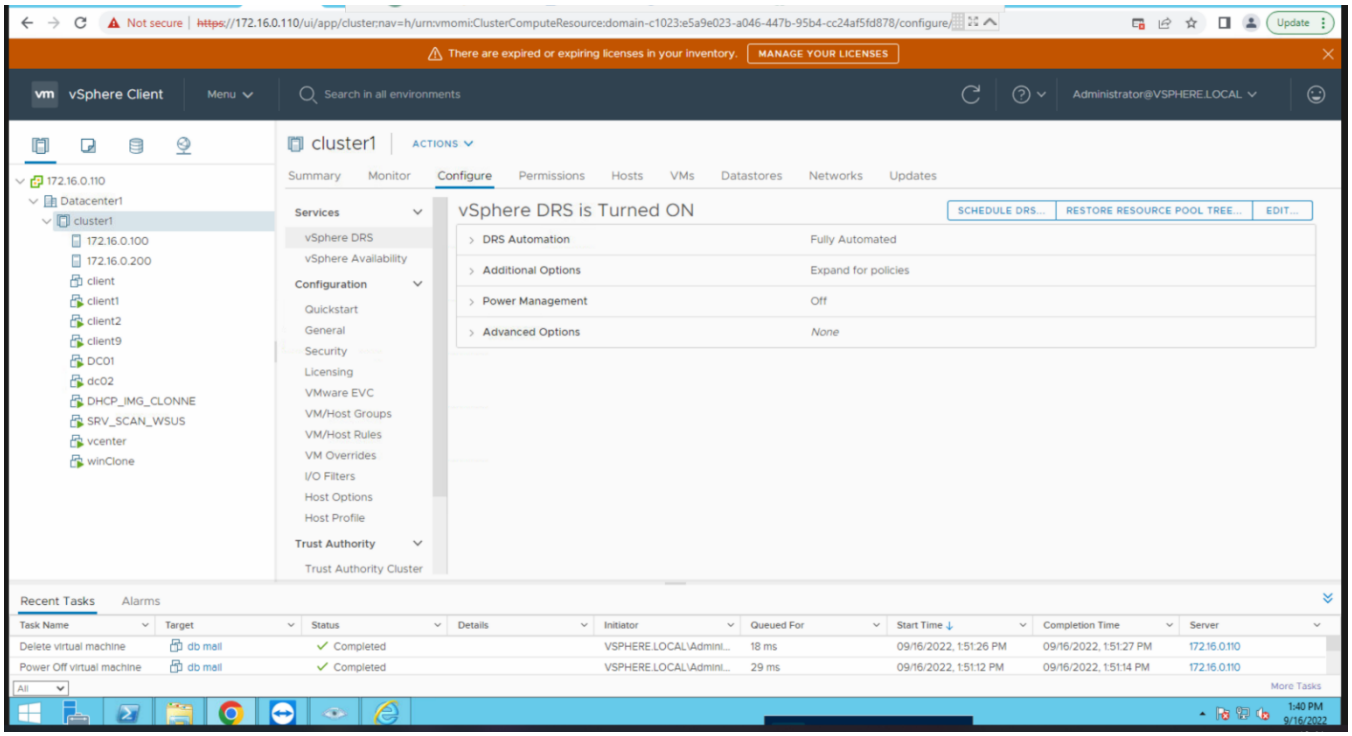

Settings for server 127.0.0.1:14147
Server listeners
Protocols settings
FTP and FTP over TLS (FTPS)
Rights management
Groups
Users
Administration
Logging
Let's Encrypt®
Server listeners
Address
Port
Protocol
0.0.0.0
21
Explicit FTP over TLS and inse
192.168.0.153
21
Require explicit FTP over TLS
172.18.0.50
21
Require explicit FTP over TLS
Add
Remove
OK
Cancel
Apply

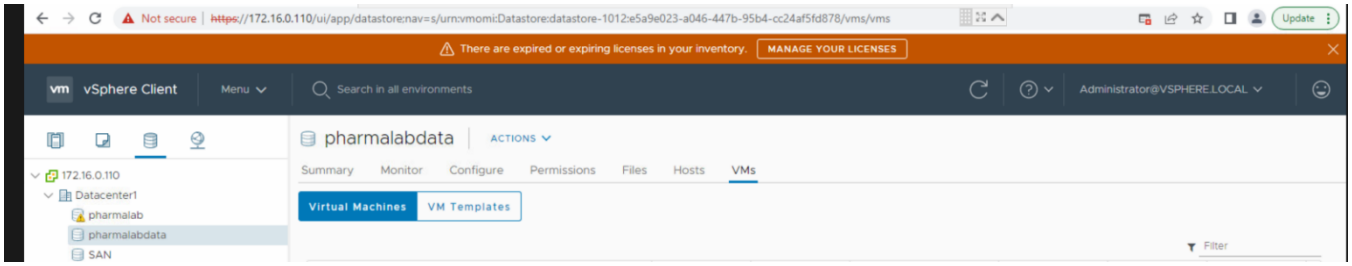

Rights management / Users
Available users
<system user>
juju
Add
Remove
Duplicate
Rename
General
Filters
Speed Limits
User is enabled
Credentials:
Require a password to log in
Leave empty to keep existing password
Member of groups:
Mount points:
Virtual path
Native path
/
c:\ftproot\usern
/Shared
c:\Shared
Add
Remove
Permissions
Access mode:
Read + Write
Apply permissions to subdirectories
Writable directory structure
Description:
OK
Cancel
Apply

client

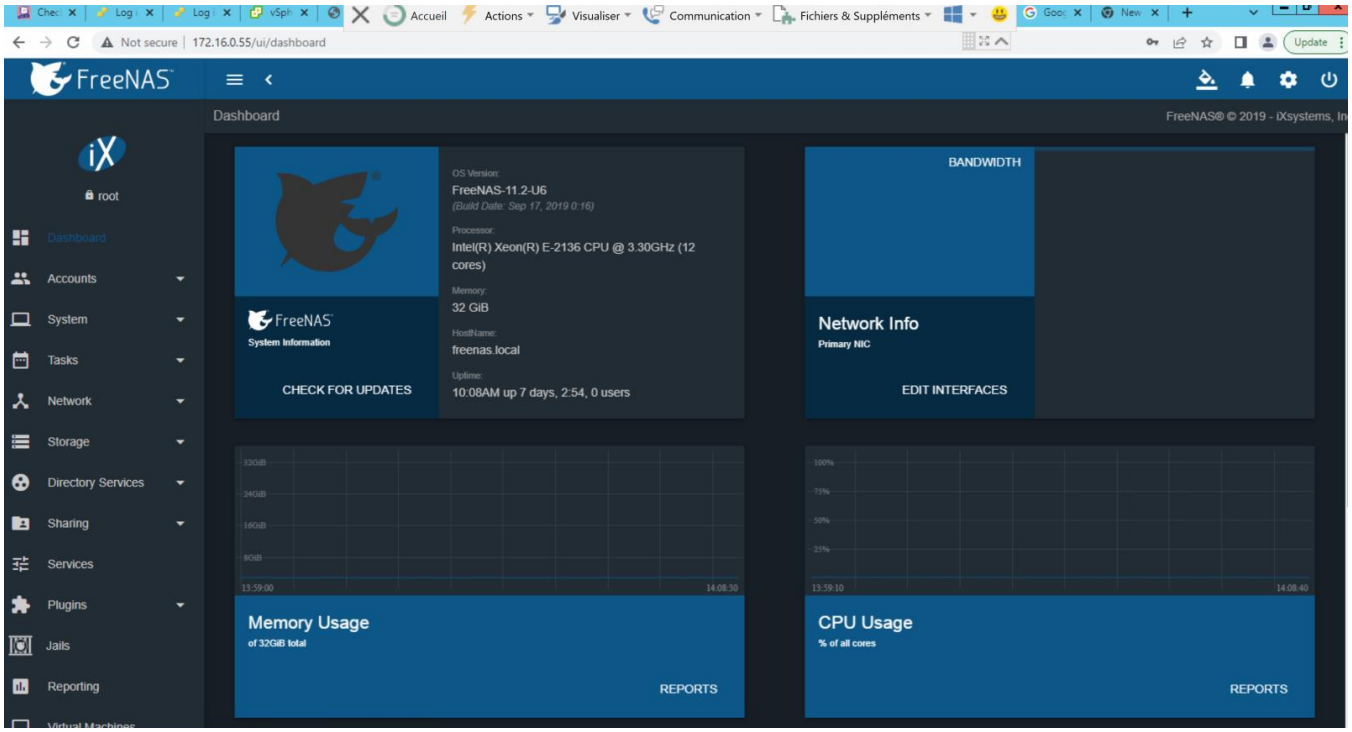

juju@172.18.0.50 - FileZilla
File Edit View Transfer Server Bookmarks Help
Host: 172.18.0.50 Username: juju Password: ••••••••• Port: Quickconnect
Status: TLS connection established.
Status: Logged in
Status: Retrieving directory listing...
Status: Directory listing of "/" successful
Status: Retrieving directory listing of "/Shared"...
Status: Directory listing of "/Shared" successful
Local site: C:\Users\Administrator\
Administrator
All Users
Default
Default User
Public
Remote site: /Shared
/
Shared
Filename Filesize Filetype Last modified
..
AppData File folder 9/13/2022 11:56:31..
Application Data File folder 9/13/2022 11:05:29..
Contacts File folder 9/13/2022 11:56:34..
Cookies File folder 9/13/2022 11:22:16..
Desktop File folder 9/13/2022 9:03:15 ...
11 files and 22 directories. Total size: 2,474,004 bytes
Filename Filesize Filetype Last modified Permissions
..
lala.txt 0 Text Docu... 9/14/2022 8:01:...
lolo.txt 0 Text Docu... 9/14/2022 8:00:...
2 files. Total size: 0 bytes
Server/Local file Direction Remote file Size Priority Status
Queued files Failed transfers Successful transfers

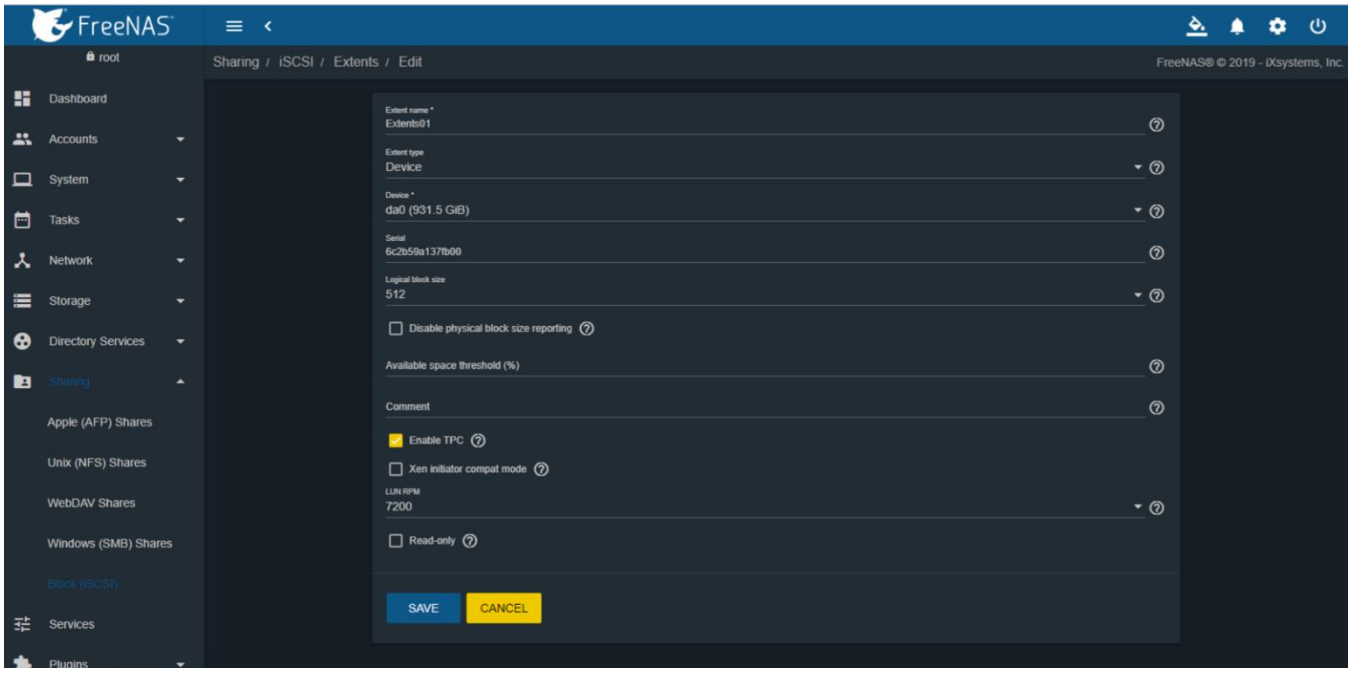
Vsphere pour une gestion centralisée des esxi

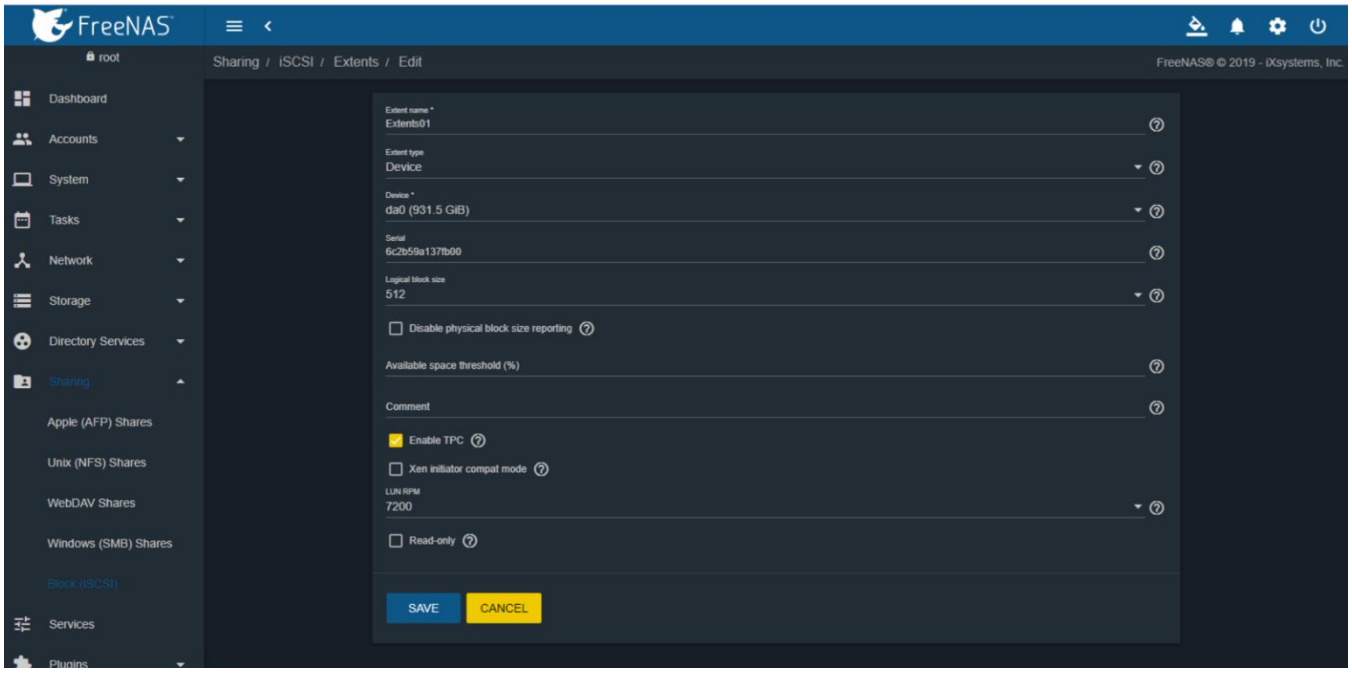


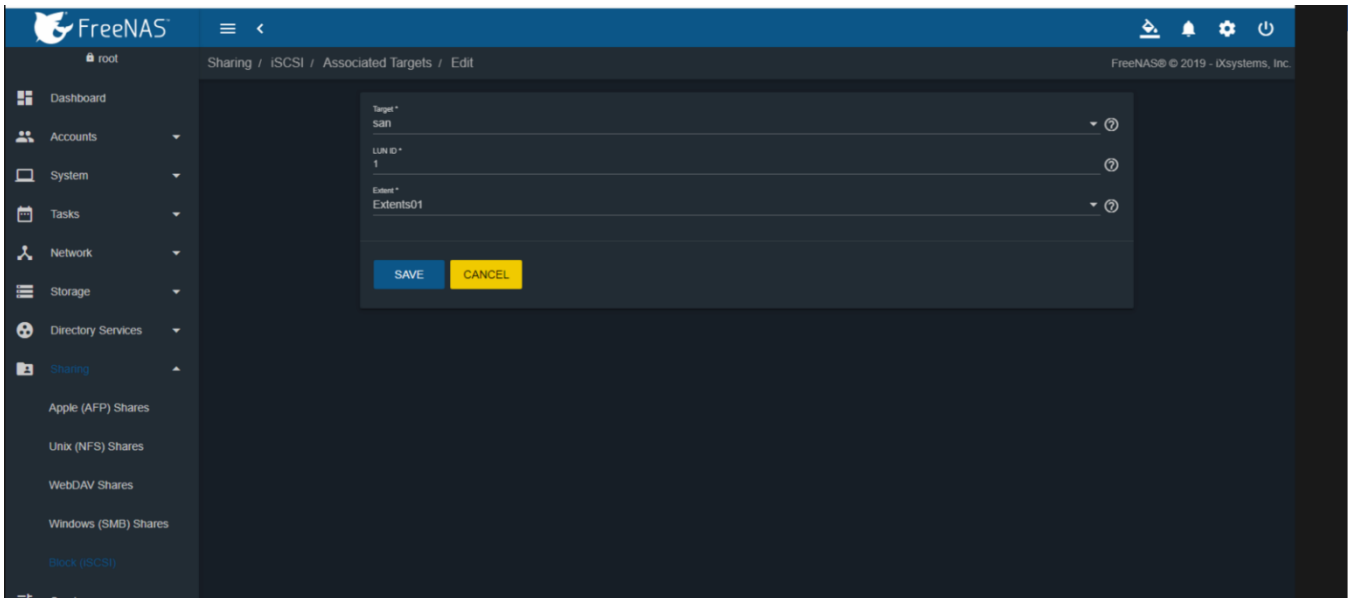


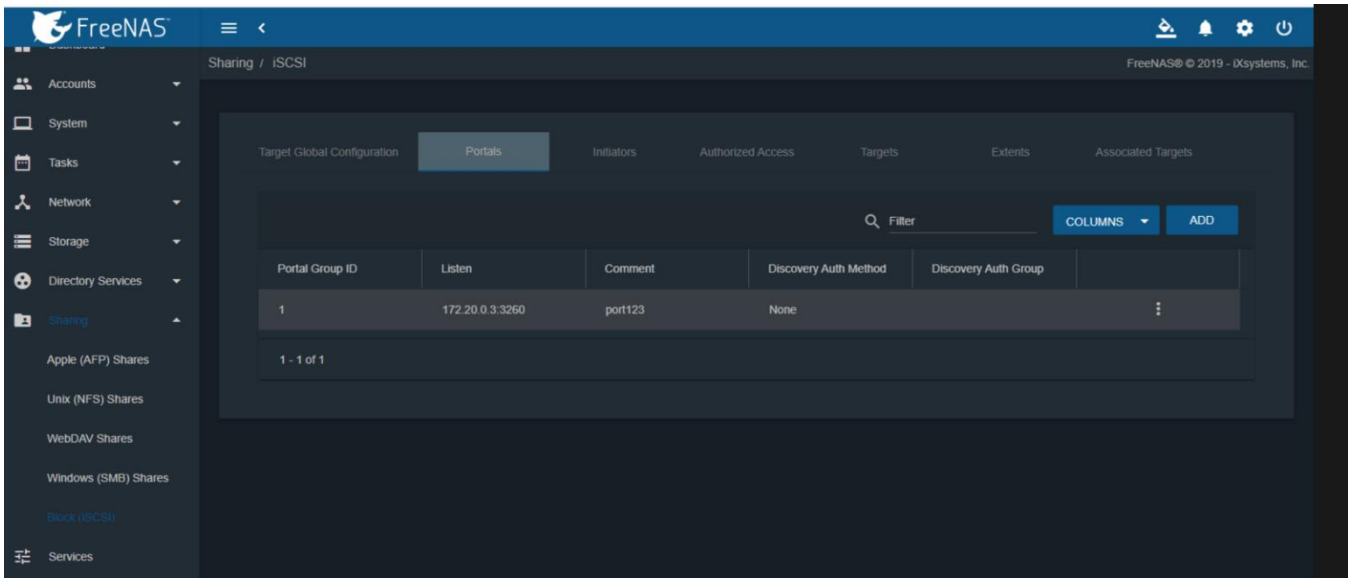
Freenas : pour la configuration de la san



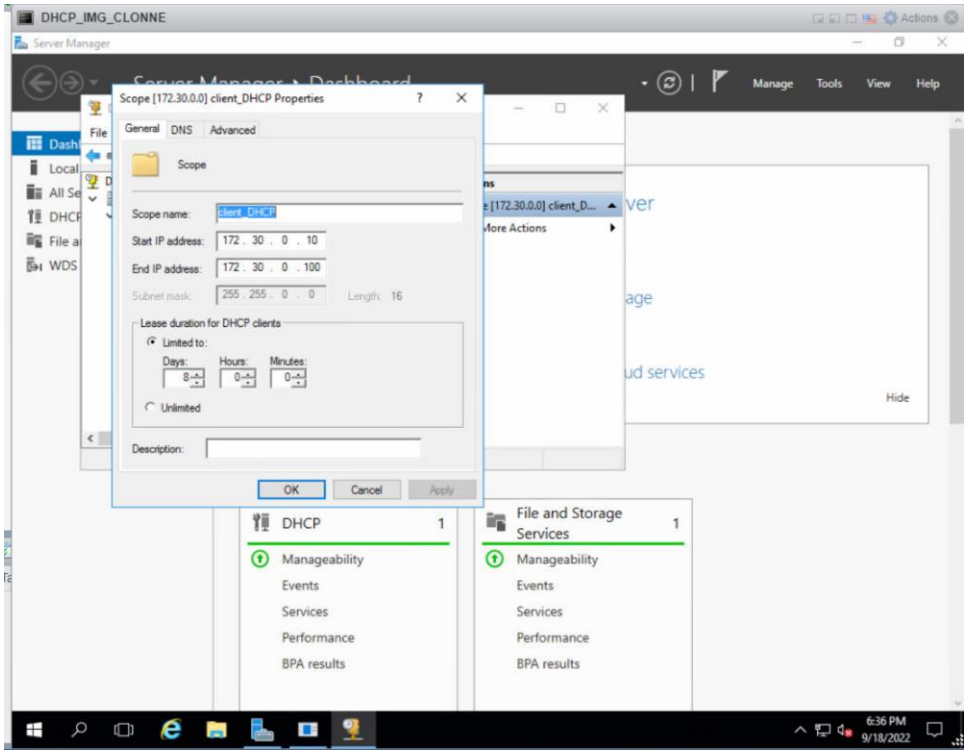



FreeNAS
root
Dashboard
Accounts
System
Tasks
Network
Storage
Directory Services
Sharing
Apple (AFP) Shares
Unix (NFS) Shares
WebDAV Shares
Windows (SMB) Shares
Block (iSCSI)
Services
Plugins
Sharing / iSCSI / Extents / Edit
FreeNAS® © 2019 - iXsystems, Inc.
Extent name *
Extents01
Extent type
Device
Device *
da0 (931.5 GiB)
Serial
6c2b59a137fb00
Logical block size
512
Disable physical block size reporting
Available space threshold (%)
Comment
Enable TPC
Xen initiator compat mode
LUN RPM
7200
Read-only
SAVE
CANCEL

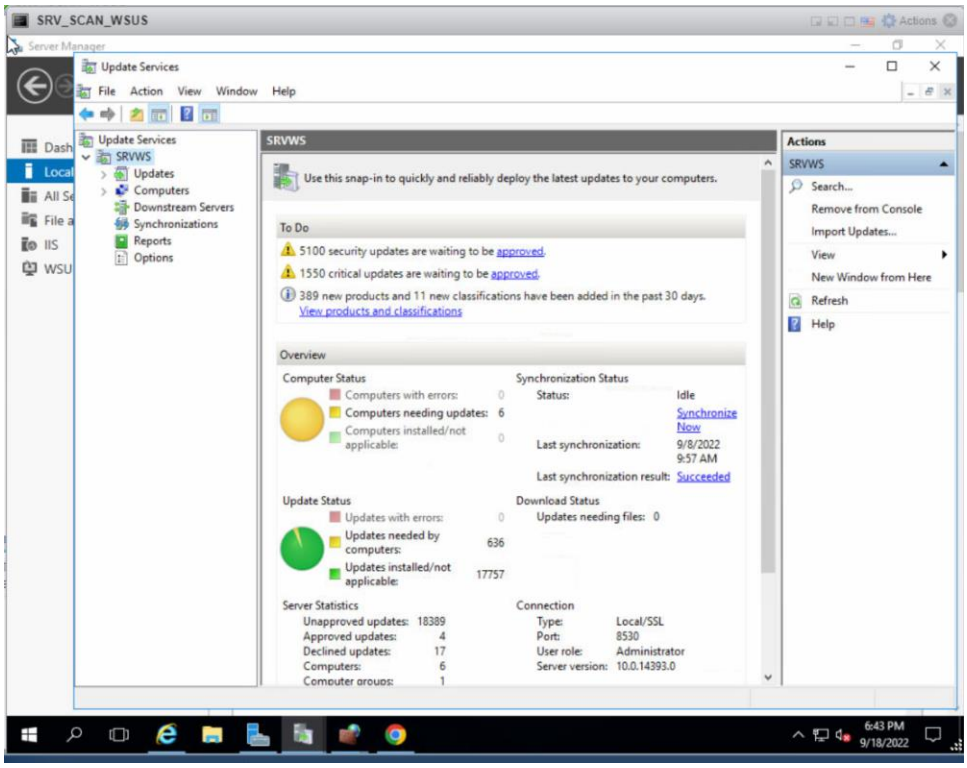

FreeNAS
root
Dashboard
Accounts
System
Tasks
Network
Storage
Directory Services
Sharing
Apple (AFP) Shares
Unix (NFS) Shares
WebDAV Shares
Windows (SMB) Shares
Block (iSCSI)
Sharing / iSCSI / Associated Targets / Edit
FreeNAS® © 2019 - iXsystems, Inc.
Target *
san
LUN ID *
1
Extent *
Extents01
SAVE
CANCEL



Serveur DHCP pour les utilisateurs :



Serveur WSUS pour la mise a jour des ordinateurs de facon centralisé



Plan et adressage IP

Il nous a été demandé de réfléchir à un découpage possible du réseau de la société.

Adressage des PC

N° adresse	Adresse réseaux PC	1 ère Adresse PC	Département
1	172.30.0.0	172.30.0.1	production
2	172.30.0.0	172.30.0.2	Gestion (finance
3	172.30.0.0	172.30.0.3	direction

Adressage des imprimantes

N° adresse	Adresse réseaux imprimante	1 ère Adresse imprimante	Département
1	172.40.2.0	172.40.2.1	production
2	172.40.2.0	172.40.2.2	Gestion (finance

3	172.40.2.0	172.40.2.3	direction

Adressage des Serveurs

N° adresse	Adresse Serveur	Nom Serveur
1	172.16.0.2	DC01
2	172.16.0.4	DC02
3	172.16.0.5	SRV-DHCP-IMG
4	172.16.0.6	SRV-SMB
5	172.16.0.7	SRV-DBM
6	172.16.0.8	SRV-ANTI
7	172.16.0.9	vcenter
8	172.16.0.10	View Connecxion Server

Adressage des Serveurs de la DMZ

N° adresse	Adresse Serveur	Nom Serveur
1	172.18.0.2	Smail_01
2	172.18.0.3	Smail_02
3	172.18.0.4	Web_01
4	172.18.0.5	Web_02
5	172.18.0.50	Ftp_01
6	172.18.0.7	Ftp_02