2024

Mise en réseau et paramétrages d'un nas synology, nas Qnap, camera D-Link, Firewall



Brieuc le Faucheur SC-Micro 5/31/2024 Durant ce TP, nous allons mettre en place le fonctionnement et la mise en réseau. Il faudra également sécuriser les différents périphériques, un schéma réseau sera présent dans cette doc.

Voici la liste et détails de ce que nous avons :

- Nas Synology

Créer un RAID1 avec 2 disques durs de 2 TO Mettre en applications les fondamentaux de sécurité

- NAS QNAP

Créer un RAID 5 avec les disques durs de 3TO Mettre en applications les fondamentaux de sécurité

- Caméra D-LINKC DGS-5222L

Compte D-LINK si besoin donné. Caméra lié au Wi-Fi suivant : Bbox-SCMG IP caméra : ?

- FIREWALL Fortigate 60-C

A mettre en fonction. Assistant Wizard + Recherche de fonctionnement de règles Premier démarrage sur : 192.168.1.99 Login : ****** / mdp : *******

- Switch ZyXel GS1200-8

A mettre en fonction. Produit Reset. Trouver les identifiants par défauts. (Google DORKS)

- BOX INTERNET : Bbox

Nous allons commencer ce TP par le Nas Synology.

Une fois tous les branchements fait allumons le, ensuite nous allons lancer l'application Synology Assistance qui vas nous permettre de voir les Nas synology branché sur le réseau, comme le montre la capture d'écran ci-dessous on peut apercevoir le nôtre :

Synology Assist	ant				—		
Gestion	ériphérique d'imp	ression			Sj	no logy	
Recherche	La Connecter 🔤	<mark>∄</mark> Mapper un	lecteur	Configurer WOL	1	🔅 😧 🚯)
Nom de serveur	Adresse IP	Statut IP	Statut	Adresse MAC	Version	Modèle	
SynologyNAS	192.168.119.10	DHCP	<u>Non installé</u>	90:09:D0:54:40:F1	7.1.1-42962 update 4	DS224+	2
SynologyNAS	192.168.119.10	DHCP	<u>Non installé</u>	90:09:D0:54:40:F1	7.1.1-42962 update 4	DS224+	2

Si votre périphérique n'est pas répertorié, reportez-vous à ces astuces. 1 serveur(s) Synology trouvé(s) au total.

Une fois cela fait, nous pouvons nous rendre sur l'adresse <u>http://192.168.119.10:5000/web_index.html</u> pour contrôler notre nas. On lance l'installation de celui-ci.

Une fois être arrivé sur l'interface de configuration, nous devons aller dans gestionnaire de stockage, c'est ici que l'on vas créer le stockage et le volume En suivant les instructions et en choisissant nos besoins voici ce que au final cela donne :

Assistant de création de	Assistant de création de stockage				
Confirmer les pa	aramètres				
∧ Groupe de stocka	age				
Type de RAID		RAID 1			
Type de disque		SATA HDD			
Disque sélectionr	né	Disque 1, Disque 2			
Capacité estimée	3	1852 Go			
∧ Volume					
Capacité allouée		1852 Go			
Système de fichi	ers	Btrfs			

Retour

Appliquer

Une fois cela fait, optionnellement, nous allons créer un dossier partagé, il se nomme partage, un utilisateur nommé marc a été créer, l'administrateur « control » et l'utilisateur « marc » on des droits de lecture et écriture sur celui-ci. Une fois cela fait nous allons mettre en place les fondamentaux de sécurité. Pour commencer nous allons

Pour commencer on va s'occuper du pare-feu, par défaut, le pare-feu n'est pas activé, et donc tous les accès sont permis. L'idée générale est d'autoriser les accès depuis le réseau local, et de le fermer aux accès distants. Pour configurer le pare-feu, il faut

cocher Activer le pare-feu.

Sécurité	Compte	Pare-feu	Protection	Certificat	Avancé	КМІР	
Général							
 Active 	r le pare-fe	eu					
 Active 	r les notific	ations du pa	are-feu				
M'aver	rtir quand d	les applis ou	services sont	bloqués par	le pare-feu	et fournir l'option de débloquer ce	service ou cette appli.
Profil du p	oare-feu						
Personnalis	sez votre p	rofil de pare	-feu.				
Profil du pa	are-feu :	defa	ault			•	Modifier les règles

Ensuite on vas cliquer sur créer :

lom du profil i	parfou inter	face		
vom du prom :	parieu-interi	ace		
Règles du pare-feu				
Créer Modifier	Supprimer		(LAN 1
Activé Ports	3	Protocole	IP source	Toutes les interfaces
				LAN 1
				LAN 2
				PPPoE
				VPN
		Aucun élément		
				0 élément
aucune règle n'est rem	plie : 💿 Autorise	r l'accès 🔵 Refuser a	accès	
marque : Vous pouvez priorité.	faire glisser les rè	gles pour réarranger le	ur ordre. Les rè	ègles au dessus prennent la

On va tout d'abord ajouter quatre règles garantissant un accès local complet à votre NAS :

Règles	du pare-fe	eu				
Créer	Modifier	Supprimer			LAN 1	-
	Activé	Ports	Protocole	IP source		Action
	\checkmark	Tous	Tous	192.168.0	0.0/255.255.255.0	Autoriser
		Tous	Tous	172.16.0.	0/255.240.0.0	Autoriser
		Tous	Tous	10.0.0.0/	255.0.0.0	Autoriser
		Tous	Tous	fe80::/10		Autoriser

Dernier point, <u>mais le plus important</u>, on choisit Refuser l'accès comme comportement du pare-feu en cas de requête non déclenchée par les règles précédemment ajoutées :

Si aucune règle n'est remplie : 🔵	Autoriser l'accès 💽	Refuser accès

Ensuite, nous allons voire les services de fichiers,

On va dans Panneau de configuration -> Services de fichiers SMB (ou Samba dans sa déclinaison Linux) est le protocole utilisé par Windows lorsqu'on monte un lecteur réseau dans l'explorateur de fichiers. Mais même sous Linux, il est le protocole à privilégier lorsqu'on se connecte à un NAS.

^	Par	ramètres SMB			
	Ac	tiver le service SMB			
	Gro	oupe de travail :	WORKGRO	OUP	
		Refuser l'accès aux	versions pr	écédentes	
	✓	Masquer les dossiers	s partagés	pour les utilisateurs	ne disposant pas d'autorisation
	<	Activer le journal de	s transfert	S	
		Paramètres de jou	ırnal Af	fficher les journaux	
	F	Paramètres avancés			
	Rei	marque :			
	• ' • !	Vous pouvez activer l Une fois les dossiers i l'Explorateur de fichier	a corbeille s ndexés dan rs Windows	sur la page d'édition s <u>Liste des dossiers</u> pour rechercher de	de <u>Dossier partagé</u> . <u>indexés</u> , vous pouvez utiliser Mac Finder ou s fichiers et leur contenu.
		Saisissez les adresss réseau local :	ci-dessous	pour accéder aux c	lossiers partagés à l'aide d'un ordinateur sur votre
		PC (Windows Explo	rer):	\\Nas-Brieuc	
		Mac (Finder) :		smb://Nas-Brieu	IC

- 1. Dans Paramètres SMB, cochez Activez le journal des transferts
- 2. On coche Masquer les dossiers partagés pour les utilisateurs ne disposant pas d'autorisation

3. Dans WS-Discovery, on coche Activer la découverte de réseau Windows pour autoriser l'accès aux fichiers via SMB

∧ WS-Discovery
Les périphériques réseaux locaux peuvent utiliser la découverte de réseaux Windows pour accéder à des fichiers sur votre DiskStation.
Activer la découverte de réseaux Windows pour autoriser l'accès aux fichiers via SMB

4. On clique sur **Paramètres avancés** et on définit le protocole SMB minimum sur **SMB2 et Large MTU**, SMB1 a de nombreuses failles de sécurité et n'est plus nativement par défaut activé dans DSM :

Paramètres avancés			×
Général macOS Autres			
Serveur WINS :			
Protocole SMB maximum :	SMB3	•	
Protocole SMB minimum :	SMB2 et Large MTU	•	
Plage SMB :	SMB2 et Large MTU,SMB3	3	
Mode de chiffrement du transport :	Défini par le client	•	
Activer la signature serveur :	Désactiver	•	
Activer Opportunistic Locking			
Activer le bail SMB2			
Activer les handles durables de SM fichiers sera désactivé.)	1B (Le verrouillage inter-p	rotocole de	2S
Vider le cache SMB			

Ensuite on va dans « Autre » et On coche les 3 options suivantes :

✓	Permettre les liens symboliques au sein de dossiers partagés
	Autoriser les liens symboliques entre différents dossiers partagés
	Désactiver les connexions multiples à partir de la même adresse IP
	Collecter des journaux de déboggage
	Application des permissions UNIX par défaut
	Ne pas réserver d'espace disque lors de la création de fichiers
	Activer l'authentification NTLMv1
	Activer la lecture asynchrone
~	Contrôle des modifications apportées à tous les sous-dossiers du répertoire e cours

Utilisateur et groupe

Lors du passage à DSM 7, ou lors d'une nouvelle installation, vous êtes invités à créer un nouveau compte administrateur si votre seul compte administrateur est le compte "admin".

Cela permet d'avoir un compte administrateur avec des accès plus robustes (voir Politique de mot de passe), et de désactiver le compte "admin" par défaut, sur lequel vous ne pourrez plus vous connecter.

Utilisateur	Groupe	Avancé				
Créer 🝷	Modifier	Supprimer	Exporter +	Déléguer -		
Nom +		Courrier é	lectronique	Description	État de 2FA	Statut
			@gmail.cor	n	Activé	Normal
admin				System default user	Désactivé	Désactivé

Configuration du mot de passe

On se dirige vers l'onglet Avancé -> Configuration du mot de passe :

Utilisateur Groupe Avancé
∧ Configuration du mot de passe
✓ Autoriser les utilisateurs non-administrateur à réinitialiser les mots de passe oubliés via email
Obliger les utilisateurs à modifier leur mot de passe une fois que l'administrateur l'a réinitialisé
✓ Appliquer les règles de force de mot de passe
Veuillez consulter <u>cet article</u> pour plus d'informations sur la manière de renforcer un mot de passe.
Exclure du mot de passe le nom et la description de l'utilisateur
✓ Inclure le mélange majuscule/minuscule
✓ Inclure les caractères numériques
Inclure les caractères spéciaux
Exclure un mot de passe faible
✓ Longueur minimale du mot de passe 10
Historique des mots de passe (fois)

Espace personnel de l'utilisateur

Au bas du menu **Avancé** on coche **Activer le service d'accueil de l'utilisateur**, afin que chaque utilisateur dispose de son propre dossier personnel dans homes (homes n'est visible que des membres du groupe administrateurs).

Réseau

Dans l'onglet Général de la catégorie Réseau :

- Dans Paramètres avancés :
 - Cochez Répondre à la demande ARP si l'adresse IP cible est identique à une adresse locale configurée sur l'interface entrante, cela permet de faire en sorte que les données sortent par leurs interfaces respectives.
 - Cochez Activer la détection des conflits IP, vous aurez des notifications dans DSM si votre NAS rencontre des problèmes de conflit d'IP.

Connectivité

Cochez Activer HTTP/2

Sécurité

Protection du compte

Cochez Activez la protection du compte :

 Protection du co 	mpte							
Activez cette option po	Activez cette option pour protéger vos comptes des attaques par des clients non fiables.							
 Activer la protection 	Activer la protection du compte							
	- · ·							
Clients non fiat	bles							
Une protection d	e compte sera déclenché	ée si un client non fiable ne parvient pas à s						
Tentatives de cor	nnexion :	5						
Sous (minutes) :		1						
La protection de	La protection de compte sera annulée après une période prédéterminée.							
Annuler la protec	tion du compte	30						
(minutes plus tar	rd) :							
Gérer les comp	otes protégés							
Clients fiables								
Un client fiable s	era bloqué s'il ne parvie	nt pas à se connecter à de trop nombreuses						
Tentatives de cor	nexion :	10						
Sous (minutes) :		1						
Définir une pério	Définir une période après laquelle les clients seront débloqués.							
Débloquer (minu	tes plus tard) :	30						
Gérer les client	ts fiables							

Cliquez ensuite sur **Autoriser/Bloquer la liste**, sélectionnez **Créer -> Ajouter une adresse IP**, choisissez Sous-réseau et ajouter les deux entrées suivantes :

Ajouter une adresse IP	×
🔵 Hôte unique 💿 Sou	ıs-réseau
Adresse IP/Nom de domaine :	192.168.0.0
Masque de sous réseau/Longueur du prefix :	16
Ajouter une adresse IP	×
Ajouter une adresse IP Hôte unique Sou	X Is-réseau
Ajouter une adresse IP Hôte unique Adresse IP/Nom de domaine :	X Is-réseau fe80::

Enfin, cochez également Activer la protection DoS.

Portail de connexion

DSM

Vous pouvez cocher la case **Rediriger automatiquement les connexions HTTP vers HTTPS** pour le bureau DSM pour vous connecter automatiquement en HTTPS même si l'adresse entrée commence par HTTP. Il est préférable d'avoir mis en place un certificat avant d'activer cette option pour éviter les avertissements de sécurité du navigateur.

REMARQUE : Ne pas activer cette option si vous utiliser un proxy inversé pour accéder à vos services DSM.

E Panneau de configuration									
DSM Applications Avanc	é								
∧ Style de connexion									
	Modifier								
∧ Services Web									
Port DSM (HTTP) :	5000								
Port DSM (HTTPS) :	5001								
✓ Rediriger automatiquemen	t les connexions HTTP vers HT	TPS pour le bureau DSM							
Remarque : Vous pouvez impo	rter des certificats sur la page	e <u>Certificat</u> .							
∧ Domaine									
Vous pouvez faire pointer un r	nom de domaine enregistré ver	s votre Synology NAS.							
Domaine personnalisé :	nas-brieuc	i							
✓ L'activation de HSTS force les navigateurs à utiliser les connexions sécurisées.									

Réinitialiser Sauvegarder

Parfait, maintenant que nous avons appliqués quelques bases de sécurité pour le nas Synology. Nous pouvons désormais passer au NAS QNAP

Lançons l'applications Qfinder

											QG) 🛡 🌐
	Ţ		$\overline{\mathbf{O}}$	\odot		Δ	~	æ	<u>ි</u>			2
(onnexion	Lecteurs réseau	Téléchargement de photo					Localiser cet appareil				
Signet	Nom	Adresse IP	Туре	Nom de l'appa	areil myQNAPclou	Catégorie	Modèle	Systèm	e d'exploital \	/ersion	Adresse MAC	Statut
ŵ	NAS25A057	169. <mark>254</mark> .7	.130			NAS	TS-451+	QTS	5	5.1.7.2770	24-5E-BE-25-A0-57	?

On observe donc ici notre NAS qui est à l'adresse IP 169.254.7.130

Il nous suffit donc d'aller à l'adresse <u>http://169.254.7.130:8080</u>, lors de la première installation, il suffit de suivre les indications, c'est-à-dire créer directement le compte admin, comment nommer le serveur etc...



Normalement une fois toute les étapes faites nous arrivons sur le nas (connecté en tant que admin)

2/ CRÉATION D'UN UTILISATEUR

Pour commencer nous allons d'abord créer un utilisateur, dans cette exemple, nous allons l'appeler « Marc » . Pour se faire, il suffit simplement d'aller dans le panneau de configuration --> utilisateur --> Créer --> Créer un utilisateur

Panneau de c	configuration					- 🗆 🗙
← (ControlPanel					Q ()
ૼૢૼ	🙎 Utilisateurs	Créer - Supprimer Paramèt	res avancés •	U	Itilisateur locaux	• Q
Système	🧟 Groupes d'utilisateurs	Créer un utilisateur	Description	Quota	État	Action
0	😽 Dossiers partagés	Créer plusieurs utilisateurs	administrator	-	Désactivé	
ے۔ Privilège	🟮 Quota	Importer/Exporter des utilisateurs		-	Activer	? Ø&2 ::
	💼 Sécurité du domaine					
Réseau et services de	🛕 Contrôleur de domaine					
Applications		KK ⊲ Page 1 /1 ► >> 4	3	Élém	ients affichés: 1-2, Total: 2	Afficher 10 ▼ Eléments

Il ne nous reste plus qu'à remplir les informations.

3/CRÉATION DE VOLUME ET MISE EN PLACE RAID 5

D'abord, voyons plus précisément ce qu'est un système RAID 5. Le RAID 5 est une **matrice d'au moins trois disques durs**. Elle agit comme un lecteur logique et l'emporte clairement sur les autres supports de données individuels pour ce qui est de la résilience et de la vitesse de lecture. Les systèmes RAID 5 s'appuient sur deux méthodes actives, utilisées ensemble, pour offrir ces avantages : d'une part, la matrice **répartit** les fichiers à enregistrer **de manière uniforme** sur tous les disques liés entre eux. Cette technique est également connue sous le nom de « *striping* ».

D'autre part, un système RAID 5 calcule les **informations de parité** correspondant à toutes les données utilisateur stockées, et celles-ci sont également réparties sur les différents supports de stockage. À l'aide d'un **lien XOR**, le système de stockage permet ensuite de restaurer tout bloc de données perdu ou endommagé.

Présentation rapide des avantages et inconvénients du système RAID 5 :

- Bon rapport qualité prix
- Redondance générée de manière efficace
- Solution économique pour l'amélioration de la vitesse de lecture
- Une bonne résilience
- Vitesse d'écriture réduite par rapport aux disques uniques
- Capacité de stockage des disques durs individuels limitée dans une certaine mesure

Une fois toutes ces informations réunis concernant ce qu'est le « RAID 5 » nous pouvons commencer.

Pour se faire nous allons nous diriger dans **Stockage et Snapshot -->** dérouler le menu roulant **Stockage** et sélectionner **Stockage et Snapshot**,



cette manipulation nous donne cette interface :

Nous allons cliquer sur le petit logo au milieu, ce qui nous permettra de créer le stockage et le raid 5.

🗖 Assista	nt Créer un	pool de	stockage	2					>	
	on 🖴 Se	électionner di	isque(s)	Configu	rer 🥝	Résumé				
Sélectionnez et configurez des disques :										
Unité du boî	tier [total : 1 unité(s)] : NAS H	Hôte [disques d	isponibles : 4/4]	*					
Créer un	pool de stockage sé	curisé SED (😤 <u>Qu'est-ce qu'un</u>	pool de stocka	<u>ge sécurisé SED ?</u>		
✓ Disq	ue	État F	Fabricant	Modèle	Туре	Type de bus	Capacité	Type de SED		
Disqu	ue 1	Bon T	TOSHIBA	DT01ACA3	HDD	SATA	2.73 To	-		
Disqu	ue 2	Bon S	Seagate	ST3000VX	HDD	SATA	2.73 To	-		
🗹 Disqu	ue 3	Bon S	Seagate	ST3000VN	HDD	SATA	2.73 To	-		
Disqu	ue 4	Bon V	WDC	WD30EFRX	HDD	SATA	2.73 To	-		
Sélectionné	: 4						Capacité é	valuée: 8.16 To		
Type RAID:	RAID 5	•				Disque de rechange:	Aucun	• 0		
	Seul									
	JBOD									
	RAID 0									
	HAID 1									
Annuler	RAID 5						Précédent	Suivant		
	RAID 10									

Il est évidemment important de sélectionner le type de RAID, en l'occurrence ici nous souhaitons le 5, alors, prenons le TYPE 5. Enfin cela nous donne ceci :

🗖 Assistant Créer un pool de stockage								
Introduction 🖉 Sélectionner disqu	ue(s) III Configurer 🔗 Résumé							
Créer: Nouveau pool de stockage								
Configuration du disque:								
A disque(s)	à NAS Hôte, RAID 5, 8.16 To: Disque 4, Disque 3, Disque 2, Disque 1							
Configurer:								
Surprovisionnement:	Indisponible							
Espace de snapshot garanti:	835.58 Go (10%)							
Seuil d'alerte:	Activé (80%)							
Résumé:								
Estimation de la capacité totale disponible :	8.16 To							
Estimation de l'espace réservé :	985.74 Go 🚺							
Estimation de l'espace non alloué :	7.20 То							
📕 Réservé: 11.80% 📃 Non alloué : 88.20	0%							
Annuler	Précédent Créer							

Lors du lancement de la procédure, cela peut durer quelques minutes.

Maintenant, créons nos dossiers partagés, un pour Direction (accès pour control) et un pour PARTAGE (accès pour control/Marc)

Stockage et snapshots	•					- • ×
Stockage et snapshots				📟 Pé	riphérique de stockage externe 🔹	<u>\$</u> 0 \$
Vue d'ensemble	Espace de stockage	Pool de stockage: 1,	Volume: 0, LUN: 0		Créer • Snapshot •	Gérer 🖯
	Nom/Alias	État	Туре	Snapshot R	Nouveau pool de stockage	e utilisé
	∧ Pool de stockage 1	🔮 Prêt (Synchro	D		Nouveau volume	
Stockage/Spanshote					LUN basé sur un nouveau bloc	
					Créer un JBOD virtuel	
Stockare externe						
Disque Distant						
Topologie						
I Sourcegardo de enone						
Snapshot						
Snapshot Replica						
Germannel Germann						
🛆 HybridMount 🛛 🖄						
🔤 Outil de profilage SSD 🗹						
(†1)						

On fait nouveau volume et on le paramètres suivant nos besoins.

Une fois le volume crée, on peut maintenant créer nos dossiers partagés.

Il est important de bien Activer le dénombrement basé sur l'accès (ABE) et de Permettre le dénombrement des actions en fonction de l'accès (ABSE) (surtout sur le dossier direction) car en faisant cela, tous les utilisateurs n'ayant pas les droits à ce dossier ne le verront tout simplement pas, par exemple l'utilisateur marc n'a pas accès au dossier direction, il ne le vois donc pas grâce à ces deux paramètres (activer ceci lors de la création du dossier partagé) l'image ci-dessous nous sommes connecté en tant que « control », on a bien accès au partage et direction



Maintenant, appliquons les fondamentaux de sécurité Avec les règles de bases on doit évidemment désactiver le compte par défaut de QTS. Il s'appelle « admin », de même pour les utilisateurs que vous n'utilisez pas, désactiver les au minimum, pas besoin de les supprimer.

Panneau ue	conligur	auon					
÷	Con	trol Panel					Q (?)
ŝ	2	Utilisateurs	Créer - Supprimer Paramètres	avancés -	Utilis	ateurs locaux	• Q
Système	2	Groupes d'utilisateurs	Nom d'utilisateur	Description	Quota	État	Action
~		Administration déléguée	admin	administrator	-	Désactivé	
ĕ	-	Dossiers partagés	control ≓ 🗊		-	Activer	?283:
Privilège			Marc		-	Activer	?223:
(\mathcal{A})		Quota					
Réseau et		Sécurité du domaine					
services de	<u> </u>	Contrôleur de domaine					
Applications							

On voit sur le screen du dessus que on a désactivé le compte admin, qui est le compte de base, mais on a créé un autre nommé « control », qui lui a tous les droits d'admin.

Ensuite, Dans le Control Panel, dans Système puis Sécurité, on a pas mal d'options, dont la configuration d'une politique de mots de passe, on vas cocher toutes les cases.

~ (Control Panel							Q (?)				
දරූ	🙀 Paramètres généraux	Liste des autorisations/refus	Protection d'accès des IP	Protection d'accès aux comptes	Certificat SSL et clé privée	Politique de mot de passe	Vérification en deux étapes					
Système	5tockage et snapshots							^				
0	🔒 Sécurité	Force du mot de passe										
C Privilège	Matériel	Appliquer les critères suivants po	ur renforcer la sécurité du mo	t de passe.								
	Alimentation Inclut les caractères suivants :											
C)	Centre de notifications	💟 Lettres de l'alphabet angl	ais : Au moins 1 majuscul	e et 1 miniscule 🔹								
services de	🧵 Mise à jour du firmware	Chiffres										
	Sauvegarde/Restauration	Ne doit pas inclure des caract	Volaracieres specialux									
Applications	Appareil externe	Ne doit pas être identique au	nom d'utilisateur associé, ou a	au nom d'utilisateur inversé								
	💻 État du système	✓ Longueur minimale : 8										
	🤶 QuLog Center											
	Moniteur de ressources											
	Centre de licences	Changer le mot de passe										
		Obliger les utilisateurs à chan	ger régulièrement de mots de	passe								
		Ancienneté maximale des mo	ots de passe (jours) 30									
	Envoyer un e-mail de notification une semaine avant l'expiration de leur mot de passe 1											
		Appliquer										

On va même faire en sorte que les utilisateurs, change leurs mots de passe, tous les trente jours.

QTS propose d'autres fonctionnalités intéressantes comme le blocage d'adresse IP automatique après x tentatives de connexions échouées. Cela marche pour la page de connexion mais on peut également le configurer

pour les accès SSH, FTP, Samba, etc.

Panneau d	le configura	ation								-	+ ×
←	Cont	t rol Panel								Q,	?
ŝ	i d	Paramètres généraux	Liste des auto	orisations/refus	Protection	d'accès des IP	Protection d'accès aux comptes	Certificat SSL et clé privée	Politique des mots de passe		
Système	ò	Stockage et snapshots	Désactiver auto	matiquement les cor	nptes s'ils	échouent à tro	op de tentatives de connexion dans une	période spécifiée. Vous pou	vez afficher les comptes désactivé	s dans	
õ	A	Sécurité	Utilisateurs.								
Privilège		Matériel	Utilisateurs :	Tous les utilisateurs	non dans	s le groupe 💌					
	۲	Alimentation	SSH	Intervalle de temp	5: 5	minute(s)	Nombre de tentatives de connexion a	ayant échoué: 5			
Déseau el	2	Centre de notifications									
services d	• 🧵	Mise à jour du micrologi	Telnet	Intervalle de temp	5	minute(s)	Nombre de tentatives de connexion a	ayant échoué: 5			
Application	15	Sauvegarde/Restauration	HTTP(S)	Intervalle de temp	5	minute(s)	Nombre de tentatives de connexion a	ayant échoué: 5			
		Dispositif externe									
	-	État du système	FTP	Intervalle de temp	5: 5	minute(s)	Nombre de tentatives de connexion a	ayant échoué: 5			
		QuLog Center		Intervalle de temp	5	minute(s)	Nombre de tentatives de connexion a	avant échoué: 5			
	M	Moniteur de ressources		interfaile de temp		- minacc(o)		ajun conouc.			
		License Center	AFP	Intervalle de temp	5	minute(s)	Nombre de tentatives de connexion a	ayant échoué: 5			
			Applique	er -							

Dans ce cas, on va cocher toutes les cases, pour un maximum de sécurité.

Pour maximiser un maximum nos comptes, on vas activer la double authentifications, la double authentifications permet que au moment où l'on se connecte, on doit confirmer avec un code reçu par email pour se connecter, ce qui veux dire que si un hacker tente de se connecter avec des logs admin, si il n'a pas accès au mail, il ne pourra pas se connecter.

Voici comment procéder :

Il faut en premier lieu ajouter une adresse mail dans les paramètres du profil de l'utilisateur, ici, on vas faire pour le compte administrateur qui est « control », lors de la prochaine connexion, le nas demandera a activer la double authentification, il faut ensuite suivre le processus, la méthode utilisé dans ce TP est la totp



Comme on peut le voir su le screen du dessus, il ne nous reste plus qu'à aller dans notre applications qnap authenticator et mettre le code.

Une fois les nas fait, on vas maintenant s'occuper de la caméra IP, je lance donc un IP scanner en « 192.168.1.1-254 »

Image: 192.168.1.112192.168.1.112D-Link International28:10:7B:1B:B8:88une fois que on a l'IP de la caméra on peut aller sur son interface web.

Quand on est dessus cela nous demande des logs, les logs par défaut son juste admin et pas de mots de passe, nous somme sur l'interface :



on vas tout de suite aller dans la partie maintenance au milieu.

microprogramme Fermeture de session	et l'heure pour la vidéo en direct et les enregistrements.	recommande de changer le mot de passe de votre compte	
	CONFIGURATION DU MOT DE PASSE ADMINISTRATEUR	administrateur. Veillez à écrire le nouveau mot	
	Ancien mot de passe maximum	30 caractères au	de passe pour éviter de devoir réinitialiser la caméra en cas d'oubli.
	Nouveau mot de passe mæxmum Confirmer le nouveau mot de passe Enregistrer	30 caractères au	Compte utilisateur Le compte d'utilisateur donne à un utilisateur le droit de se connecter à la page Vidéo en direct et d'utiliser les fonctions de la page.
	AJOUTER UN COMPTE UTILISATEUR Nom d'utilisateur maximum	30 caractères au	Authentification RTSP Activez la validation des utilisateurs pour la
	Nouveau mot de passe maximum Confirmer le nouveau mot de passe Ajouter 20 utilisateurs maximum	30 caractères au	diffusion RTSP. Authentification HTTP Activez la validation des utilisateurs pour la diffusion HTTP.
	LISTE DES UTILISATEURS	Authentification de l'URL de l'instantané	

Dans cette partie on va donc rajouter un mot de passe.

Par la suite on va aller dans la partie **Du produit** qui vas nous permettre par exemple de changer l'adresse IP de la caméra, étant donné qu'elle est en 192.168.1.112, on va la mettre sur notre petit réseau en 192.168.119.20



On peut prendre accès a la caméra en installant l'application IP caméra



Maintenant, occupons-nous du firewall, on va brancher un câble Ethernet sur le port Lan 1 et le brancher au switch, une fois cela fait uns e connecte au wifi avec notre ordinateur de configuration et on va sur l'IP qui nous est donné : « 192.168.1.99 », on arrive sur l'interface de connexion, on rentre les logs qui nous sont données. On va faire l'assistant wizzard en haut à droite

FORTINET	FortiGate 60C	Witzard, Video Alde en li Decon
Système	🔿 Widget 🥃 Tableau de bord	
🖶 🕙 Dashboard	v Etat	⊕ x v Ressources / ⊕ x
 Etat FortiView Réseau Configuration Admin Moniteur 	Etat HA Autonome [Configure] Nom d'hôte FG160CS10018678 [Changer] Numério de série FG160CS10018678 Mode d'operation NAT [Changer] Heure système Tus Jun 4 00:45148 2024 (FortiGuard) [Changer] Version de code VS.2.2.build542 (GA) (Mise à jour) Configuration système [Sauvegarder] [Restauru] [Revisione] Administration generation and [Changer] (Lin Tudi [Changer]	CPU Usage: 1% Memory Usage: 58% Disk Usage: 1%
	Actif depuis 0 (jours) 23 (heures) 10 (minutes) Thformation de licence	Sessions: New Sessions per Second: 0
	Support Contract • Registration ② Unreachable IPS & Application Control ③ Unreachable Config FortiGuard • AntiVrus ③ Unreachable © Config Web Filtering ④ Unreachable © Config	
	Forticloud Account Account Registered / Allowed 10 O of Dets Enter II	VPN Corr wAN Opt. & Cache Corr sis WFi Controller december 2 Preset NGFW + ATP v
Policy & Objects	FortiClient Installers	ArtiVirus (M) Application Control (M) DP
Security Profiles	Console CLI Détacher	Email Filter OFF
User & Device Journaux/Alertes	Cliquez ici pour vous connecter	Explicit Proxy OFF Intrusion Protection ON

Cet assistant nous demande de configurer quelques détails et activer les fonctionnalités du nas en premier les **paramètres systèmes** qui nous permet de de configurer le mot de passe administrations et le fuseau horaires



Ensuite on a la partie **réseau** qui nous permet de configurer le Wan et la partie Lan.



Le paramètres suivant est important, il concerne la **sécurité**, il nous permet de planifier les accès à internet, et de faire du filtrage de site sur internet :



Et autoriser des vpn distant.

On a donc un récapitulatif de ce que nous avons paramétrer :

FURTINET.

Paramètres systèmes	Résumé	
Mot de passe d'administration Fuseau Horaire Réseau Internet Connection Paramètres LAN Security Planification Politique d'acces à l'internet VPN Distant	Admin Password Fuseau Horaire Internet Connection Paramètres LAN Planification Politique d'acces à l'internet	non modifié (GMT-8:00)Pacific Time(US&Canada) 31 / 255.255.255.0 192.168.1.99 / 255.255.255.0 Toujours Enable NAT Block Malicious Content Allow Access to G and Lower Sites Enable Application Control Innactivé
Configuration Résumé FortiCloud		
< retour Configurer]	Annuler

Dans le Dashboard, on pense à activer tous les programmes de sécurité :

▼ Features	<i>ℓ</i> ↔ ×
Basic Features	
Advanced Routing	OFF
IPv6	OFF
VPN	ON
WAN Opt. & Cache	OFF
WiFi Controller	OFF
Security Features	Preset Full UTM v
AntiVirus	
Application Control	ON
DLP	ON
Email Filter	ON
Endpoint Control	ON
Explicit Proxy	ON
Intrusion Protection	ON
Web Filter	ON
	Appliquer
🔻 Console de message d'alerte	50 ℓ ↔ X
Pas de messages d'alerte.	

Full UTM

Voici le schéma réseau :

