PROCEDURE D'INSTALLATION: AJOUT & CONFIGURATION LDAP/AD STORMSHILED

PROJET

CUB

- Assurer la sécurité du réseau via le filtrage du trafic, le chiffrement des communications (VPN), la gestion sécurisée, la surveillance des événements et la sauvegarde des configurations, afin de garantir la confidentialité, l'intégrité et la disponibilité des systèmes.

• Prérequis

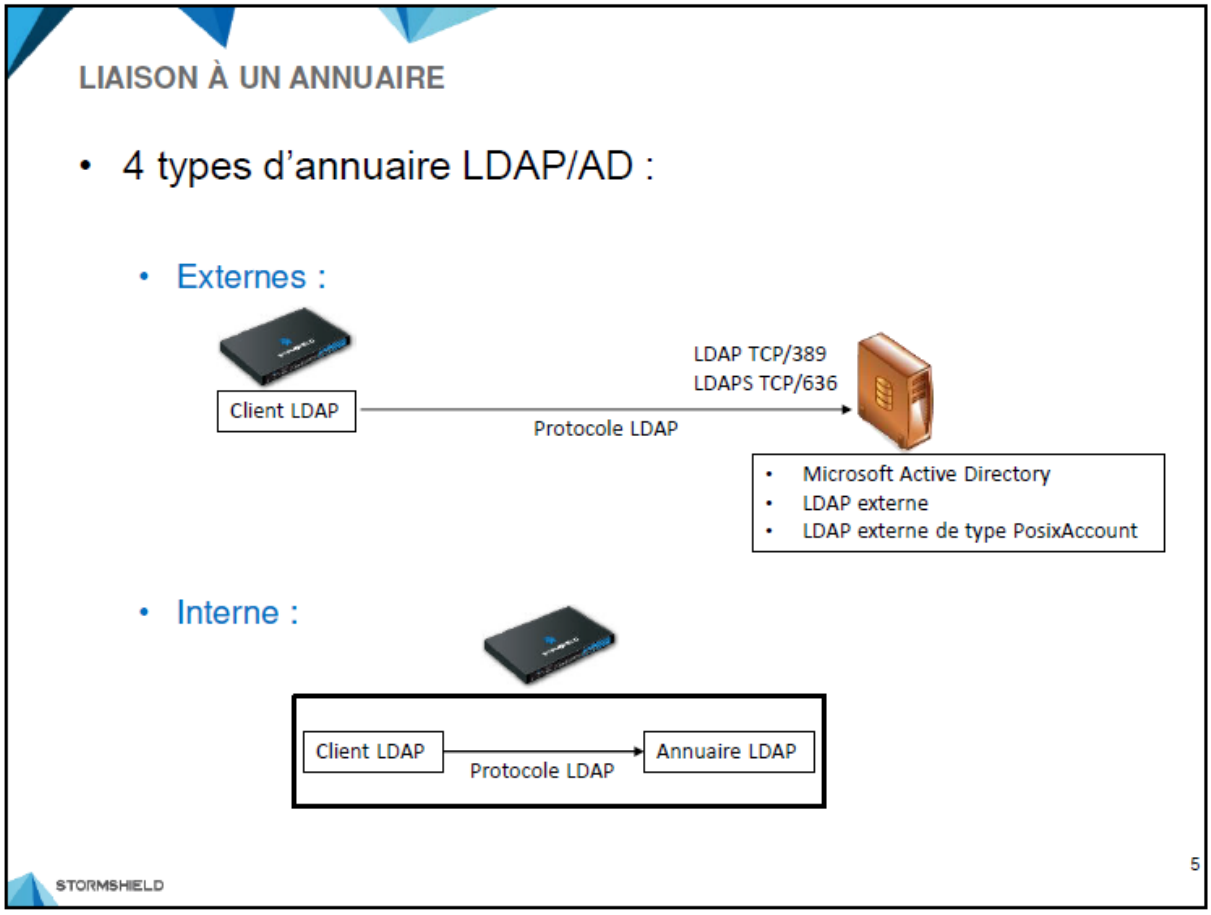
- Système d’exploitation

- OS Stormshield

- Ressources matérielles (minimum recommandé)

- **CPU** : 1 cœurs
- **RAM** : 1 Go
- **Disque** : 32 Go (SSD recommandé)
- **Connexion réseau** : 1 Gbit/s

Liaison a un annuaire



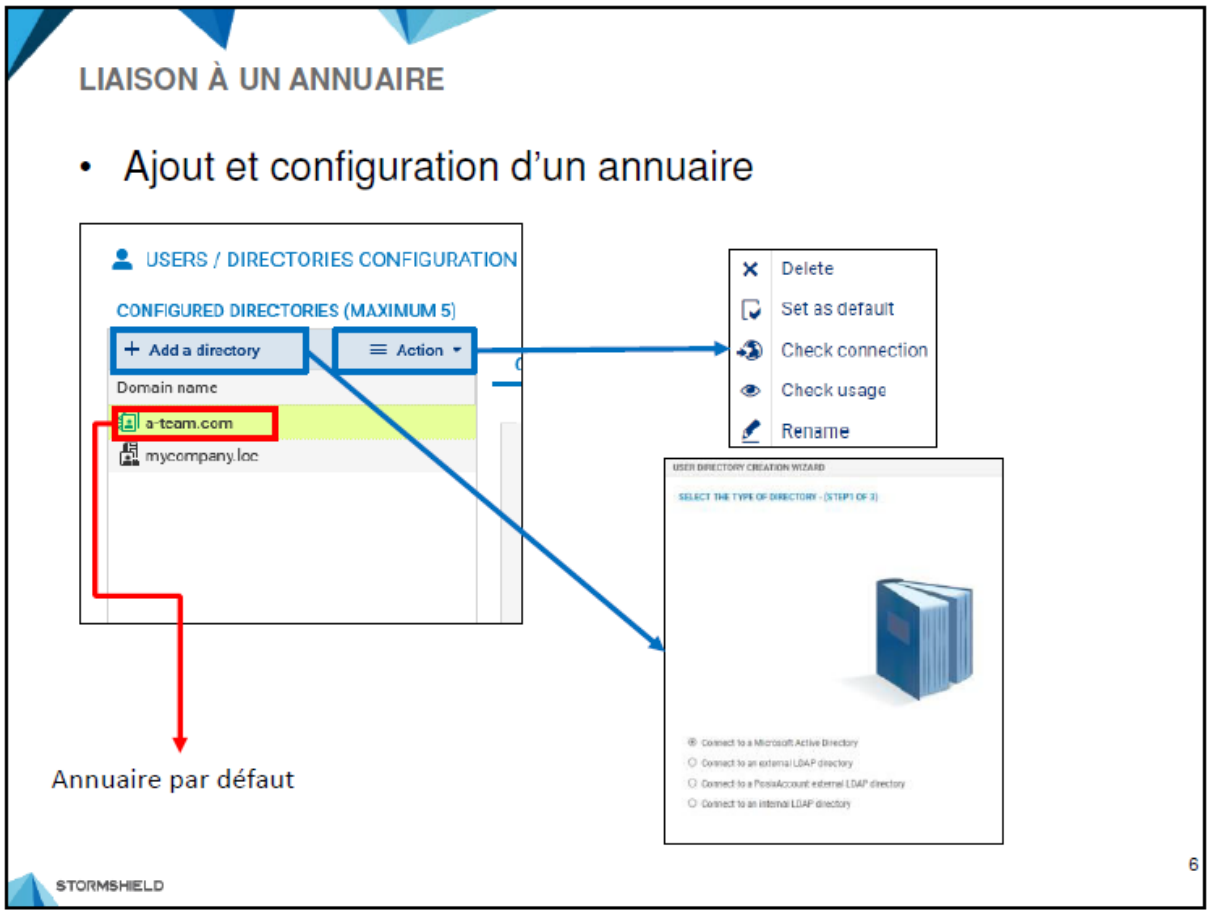
Les firewalls supportent quatre types d'annuaire qui peuvent être classés en deux catégories :

- **LDAP/AD externes** : L'annuaire est stocké sur un serveur externe. Trois types d'annuaire sont supportés :
  - Microsoft Active Directory (AD),
  - LDAP standard,
  - LDAP de type PosixAccount.

- **LDAP interne** : L'annuaire LDAP est créé sur le firewall et héberge les utilisateurs.

Les firewalls peuvent supporter cinq annuaires simultanément : un LDAP interne et quatre LDAP/AD externes, ou cinq LDAP/AD externes. Ce qui signifie que les firewalls peuvent supporter en même temps cinq domaines différents.

Ajout et configuration d’un annuaire



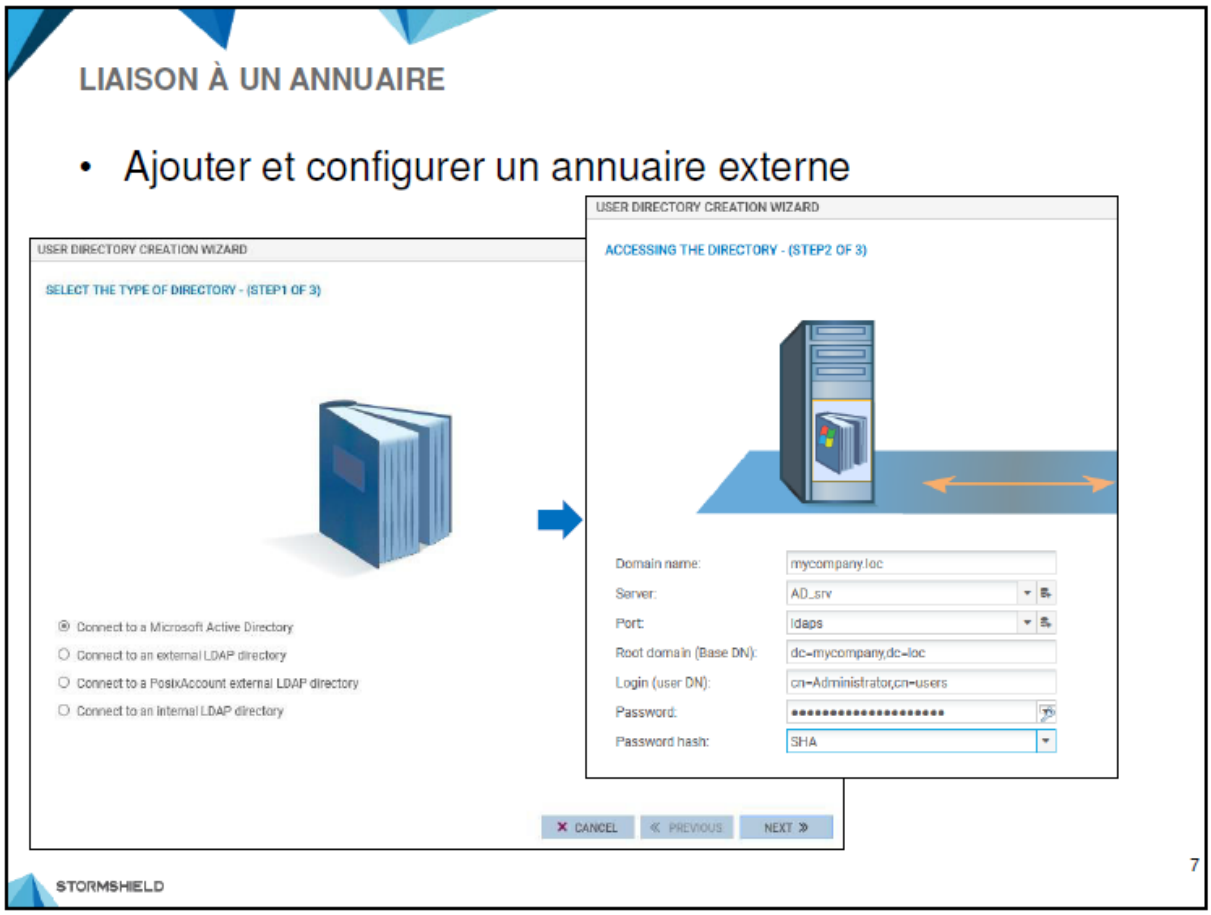
L’ajout et la configuration des annuaires s’effectuent depuis le menu : **CONFIGURATION ⇒ UTILISATEURS ⇒ Configuration de l'annuaire**.

Pour lancer l’assistant d’ajout d’annuaire cliquez sur **Ajouter un annuaire**. Le bouton **Action** permet, quant à lui, d’accéder à plusieurs fonctionnalités :

- Supprimer un annuaire,
- Désigner un annuaire par défaut,
- Vérifier la connexion à l’annuaire,
- Vérifier l’utilisation de l’annuaire,
- Renommer un annuaire.

Le reste du menu liste tous les annuaires ajoutés, parmi lesquels l’annuaire par défaut s’affiche en vert. En cliquant sur un annuaire, ses paramètres s’affichent à droite de la page.

Ajouter et configurer un annuaire externe

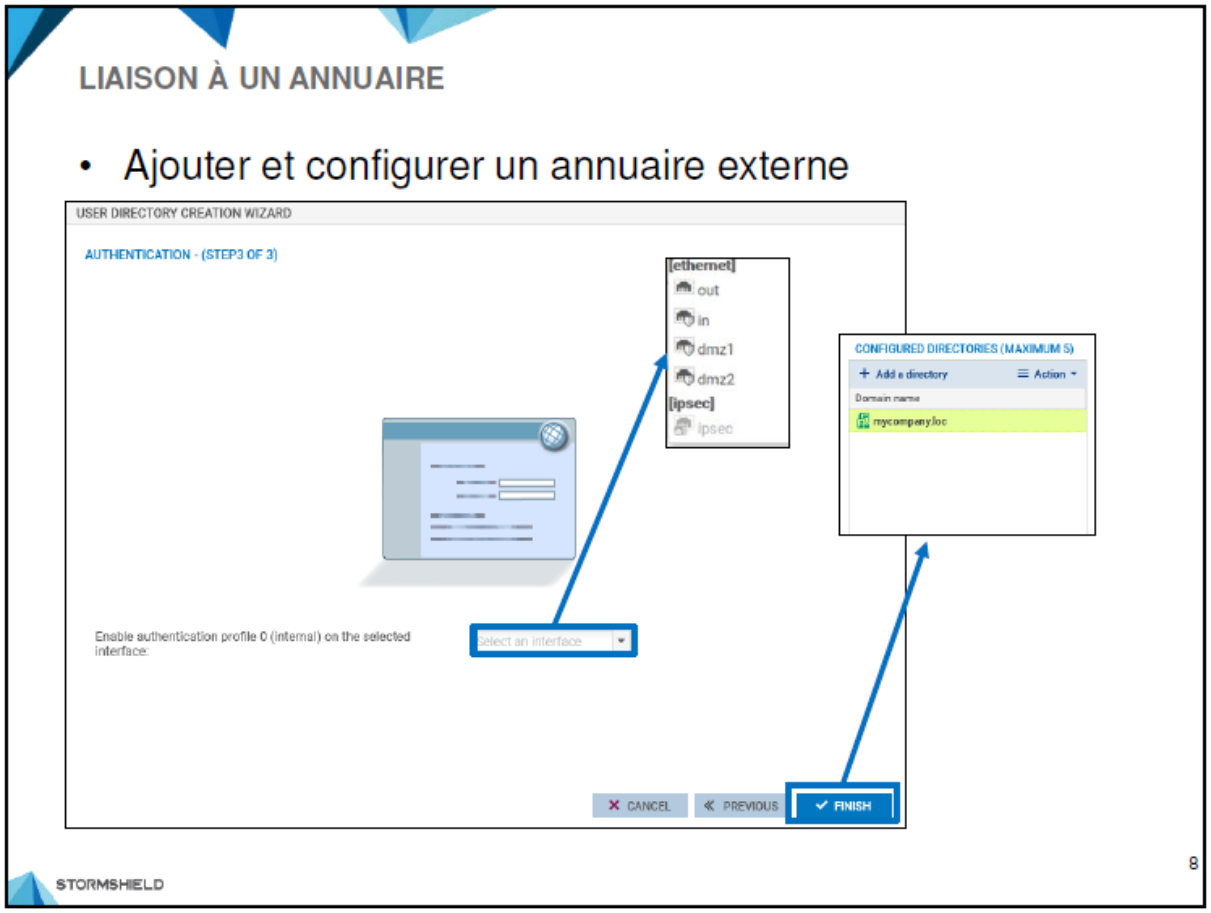


La configuration des annuaires externes (Microsoft Active Directory, LDAP et LDAP de type PosixAccount) est sensiblement identique. L'assistant de configuration vous demande d'abord de renseigner les paramètres du serveur à contacter :

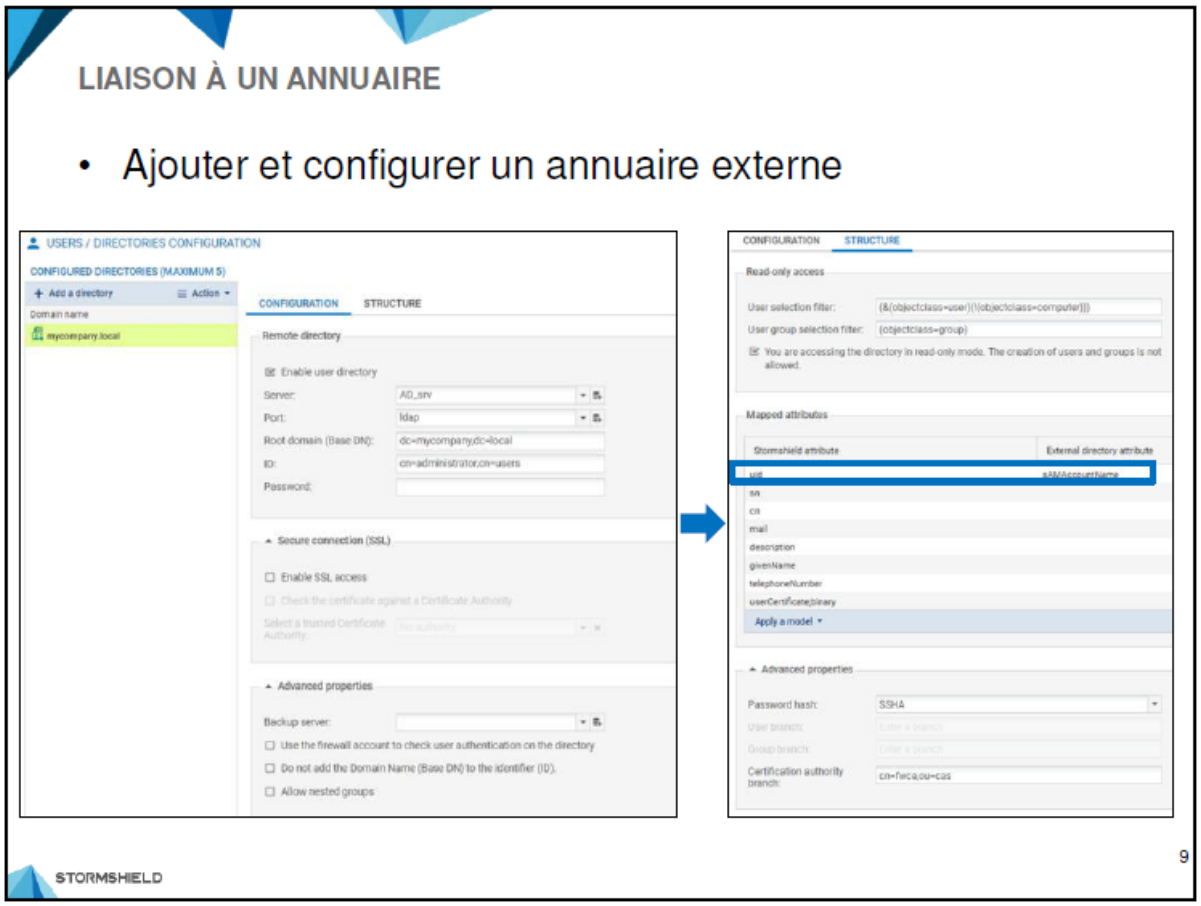
- **Nom du domaine** : Le nom DNS du domaine,
- **Serveur** : L'objet machine qui porte l'adresse IP du serveur qui héberge l'annuaire
- **Port** : Le port d'écoute de votre serveur LDAP. Les ports par défaut sont : 389/TCP pour une authentification en clair (ldap) et 636/TCP pour une authentification en SSL (ldaps),
- **Domaine racine (Base DN)** : Le DN de la racine de votre annuaire (exemple : stormshield.eu ou dc=stormshield,dc=eu),
- **Identifiant (user DN) et le mot de passe** : Un compte administrateur permettant au firewall de se connecter sur votre serveur LDAP et d'effectuer des lectures/écritures sur certains champs. Nous vous recommandons de créer un compte spécifique pour le firewall et de lui attribuer les droits

uniquement sur les champs qui lui sont nécessaires (exemple cn=TrainingAdmin,ou=Training).

- **Haché du mot de passe** : Permet de sélectionner l'algorithme de hachage qui doit être utilisé pour enregistrer les mots de passe des utilisateurs, ce qui évitera de l'enregistrer en clair.



Par la suite, l'assistant vous propose d'activer le profil d'authentification 0 (internal) sur une interface, dans le cas où le profil n'a pas déjà été activé. Si c'est le cas, cette étape ne s'affiche pas.



Les paramètres d'un annuaire externe sont organisés en deux onglets :

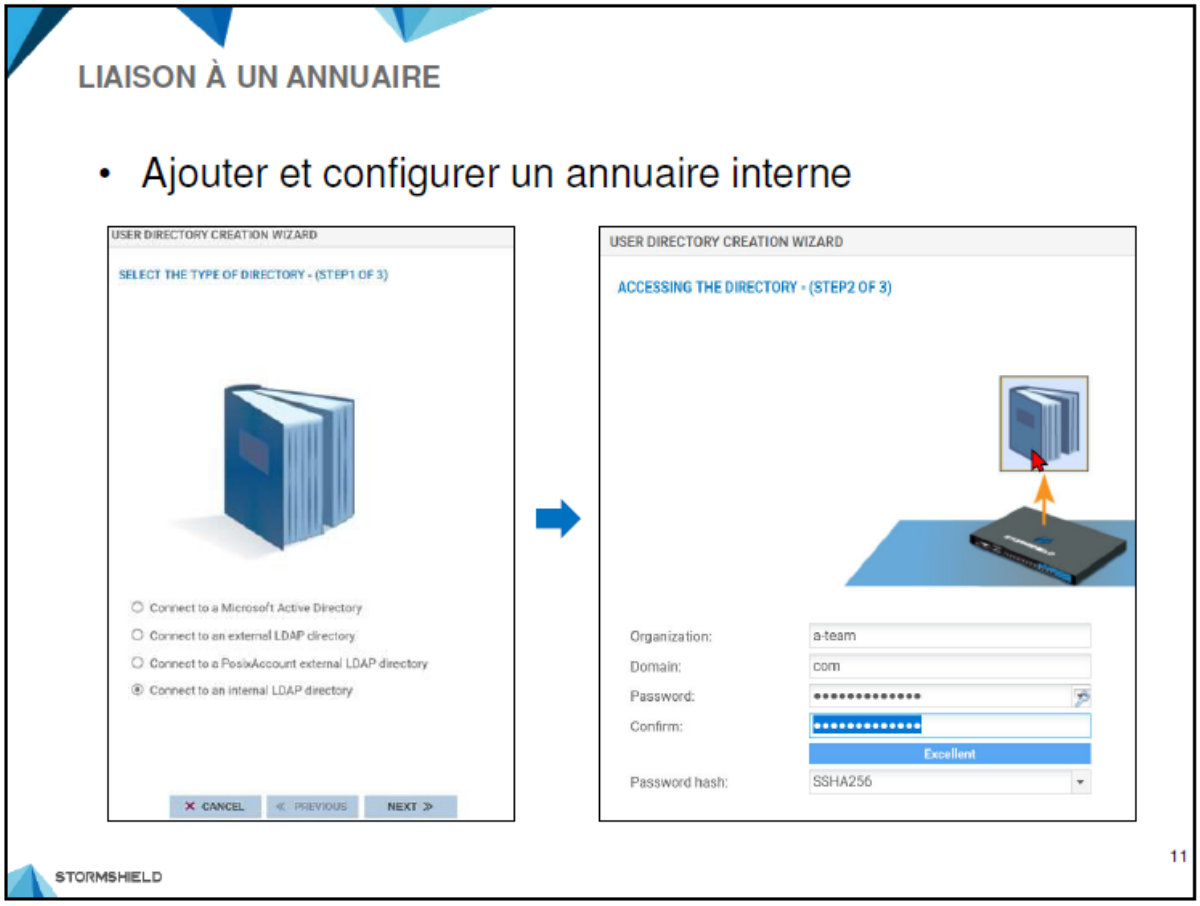
- **CONFIGURATION** : Contient 3 encadrés :
  - **Annuaire distant** : Regroupe les paramètres de connexion à l'annuaire (l'adresse IP du serveur, le numéro de port, le base DN, l'identifiant, etc.).
  - **Connexion sécurisée (SSL)** : Permet d'activer une connexion sécurisée avec l'annuaire en spécifiant l'autorité de certification dont doit être issu le certificat présenté par le serveur d'annuaire.
  - **Configuration avancée** : Permet de définir un serveur de secours, de spécifier l'identifiant (firewall ou utilisateur) utilisé pour se connecter à l'annuaire et d'ajouter ou non le base DN lors de la connexion. Il permet également d'autoriser les groupes imbriqués (un groupe d'utilisateurs contenant d'autres groupes).
- **STRUCTURE** : Contient également 3 encadrés :

- **Accès en lecture** : Permet de définir les filtres pour la sélection des utilisateurs et des groupes dans l'annuaire. Ces filtres dépendent du type d'annuaire et ils sont préconfigurés en conséquence. L'encadré permet également d'indiquer si l'annuaire est accessible en lecture seule ou lecture/écriture.

- **Correspondance d'attributs** : Permet d'indiquer la correspondance entre les attributs utilisés par le firewall et ceux utilisés par l'annuaire externe. Par exemple, avec un annuaire de type Microsoft Active Directory, l'attribut Stormshield *uid* a comme équivalent Active Directory *sAMAccountName*. Des modèles peuvent être appliqués en fonction du type de l'annuaire.

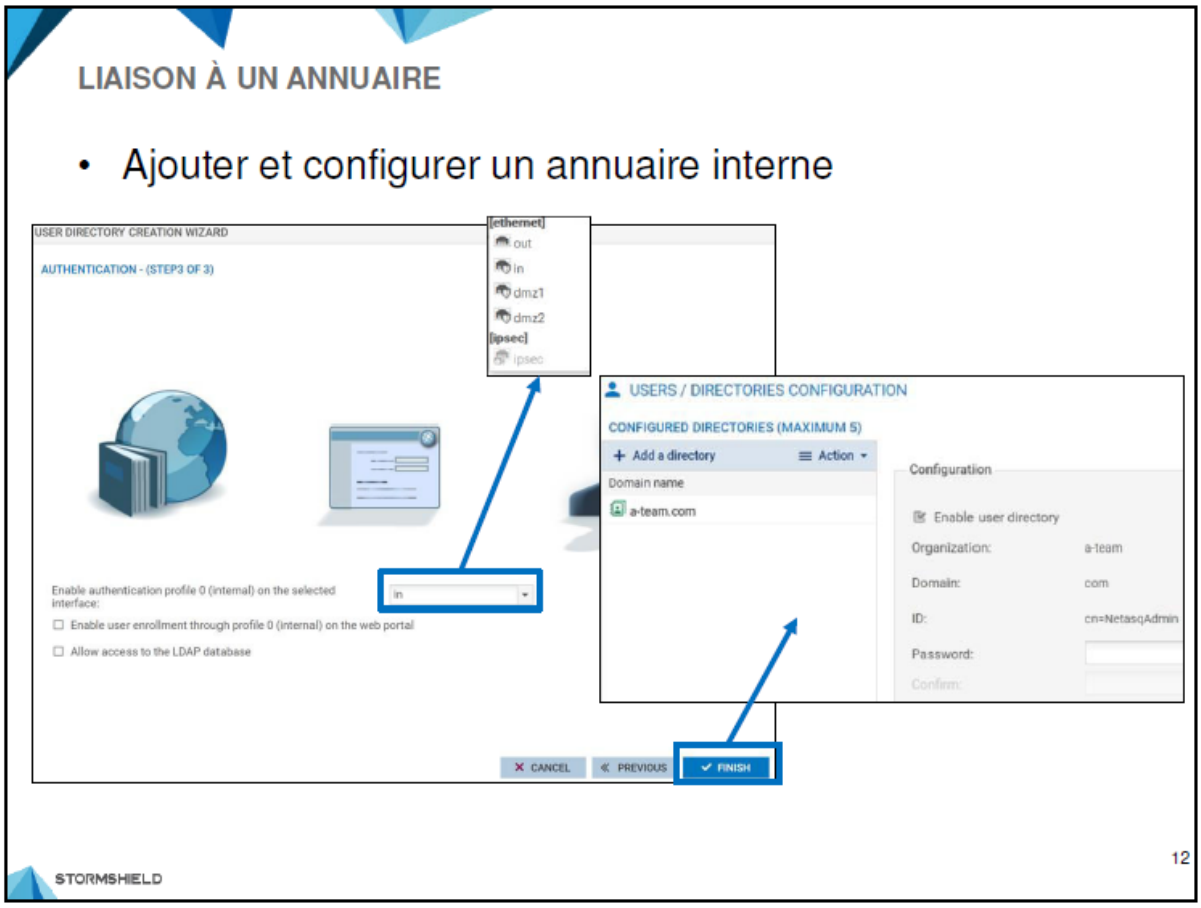
- **Configuration avancée** :
  - **Hachage de mot de passe** : Permet de sélectionner l'algorithme de hachage qui doit être utilisé pour enregistrer les mots de passe des utilisateurs, ce qui évitera de l'enregistrer en clair.
  - **Branche 'utilisateurs'** et **Branche 'groupes'** : À utiliser dans le cas d'un LDAP externe accessible en lecture/écriture. Il permet de renseigner les branches où seront enregistrés les utilisateurs et groupes créés à partir du firewall.
  - **Branche de l'autorité de certification** : Permet de définir l'emplacement de l'autorité de certification présente dans l'annuaire externe. Cet emplacement est notamment utilisé lors de la recherche de la CA utilisée pour la méthode d'authentification SSL.

Ajouter et configurer un annuaire interne



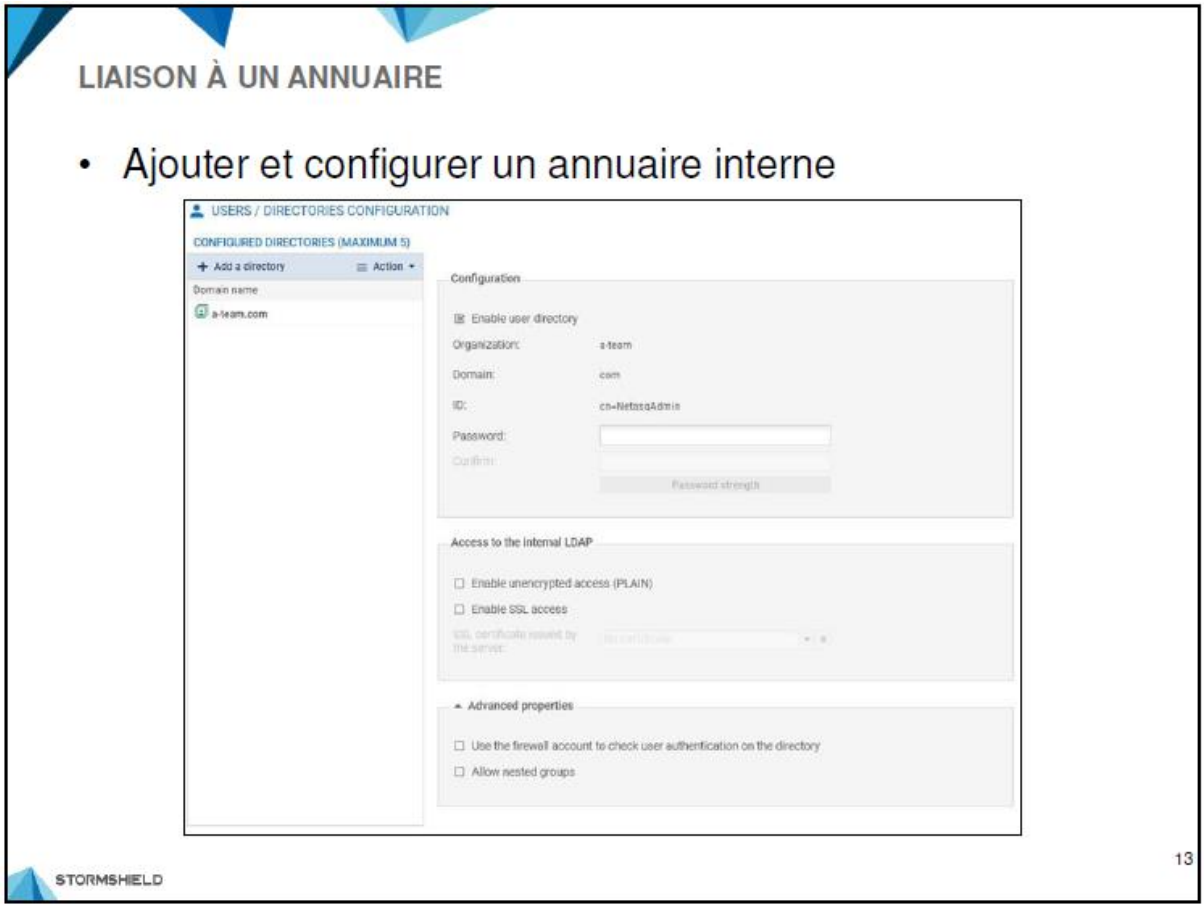
La configuration d'un annuaire interne nécessite le renseignement des informations suivantes :

- **Organisation** : Le nom de l'organisation. Par exemple, Stormshield,
- **Domaine** : Le TLD (Top Level Domain) du domaine. Par exemple, pour le domaine « Stormshield.eu », le TLD est « eu »,
- **Mot de passe** : Un mot de passe permettant de se connecter à l'annuaire LDAP depuis un navigateur LDAP.
- **Haché du mot de passe** : Permet de sélectionner l'algorithme de hachage qui doit être utilisé pour enregistrer les mots de passe des utilisateurs, ce qui évitera de l'enregistrer en clair.



L'étape suivante permet de configurer des paramètres complémentaires :

- **Activer le profil d'authentification 0 (internal) sur une interface :** Dans le cas où le profil n'a pas déjà été activé. Si c'est le cas, cette option sera désactivée (grisée) et un message indique que l'association entre profil d'authentification et interface est déjà réalisée.
- **Activer l'enrôlement des utilisateurs via le profil 0 (interne) du portail Web** : Active le service d'enrôlement sur le profil 0 (interne) permettant aux utilisateurs de remplir un formulaire de création de compte qui sera soumis à l'approbation de l'administrateur.
- **Autoriser l'accès à la base LDAP :** Donne la possibilité d'exposer le service LDAP sur le réseau et d'y accéder depuis un client LDAP. Si cet accès n'est pas nécessaire, il est vivement conseillé de ne pas activer cette option.



Une fois la configuration terminée, il est possible de modifier certains paramètres du LDAP interne :

- **Activer l'utilisation de l'annuaire utilisateur** : Cette option permet de démarrer le service LDAP,
- **Mot de passe** : Le mot de passe permettant de se connecter à l'annuaire, il est possible de le modifier,
- **Activer l'acc□s non chiffré (PLAIN)** : Active l'accès non chiffré à l'annuaire,
- **Activer l'accès SSL** : Active l'accès sécurisé à l'annuaire, il faut alors renseigner le champ certificat SSL présenté par le serveur,
- **Utiliser le compte du firewall pour vérifier l'authentification des utilisateurs sur l'annuaire** : Si cette option n'est pas cochée, l'authentification s'effectue avec le compte de l'utilisateur. Le compte disposant de tous les droits sur l'annuaire est cn=*NetasqAdmin*.