Procédure de résolution VPN SAML

Procédure de résolution VPN SAML

1. Procédure Technique de Résolution (Post-Mortem)

Voici la séquence exacte qui a permis de résoudre l'incident et de rétablir les connexions utilisateurs.

Étape 1 : Préparation et Import du Certificat

L'utilisation d'un certificat au format **PFX (PKCS#12)** est requise car il embarque de manière sécurisée la clé privée, la clé publique (certificat) ainsi que la chaîne d'autorité (CA).

1. Depuis l'interface web du FortiGate, naviguez dans **System** > **Certificates**.
2. Cliquez sur **Create/Import** > **Certificate** et choisissez **Import Certificate**.
3. Sélectionnez le type **PKCS12 Certificate**, téléversez le fichier .pfx et saisissez le mot de passe associé.

Étape 2 : Assignation du Certificat dans la configuration SAML (via l'interface graphique)

Une fois le certificat importé, il doit être associé à la configuration du Service Provider (SP) SAML.

1. Dans l'interface d'administration du FortiGate, naviguez vers **User & Authentication** > **Single Sign-On** (si le menu n'est pas visible, assurez-vous que la fonctionnalité est activée dans **System** > **Feature Visibility**).
2. Modifiez le profil SAML existant correspondant à votre tunnel (ex : **sp-tunnel**).
3. **Localisez la section "Service Provider Configuration" (et non la section de configuration de l'IdP / Identity Provider).**
4. Repérez-y le champ **Certificate** (ou *Certificat de l'entité*) et sélectionnez votre certificat fraîchement importé ([votre_certificat]) dans la liste déroulante.
5. Cliquez sur **OK** ou **Apply** pour enregistrer et appliquer les modifications.

Étape 3 : Extraction du XML de Métadonnées complet

Pour récupérer le fichier XML brut nécessaire à LemonLDAP::NG sans dépendre d'un accès par navigateur web externe (souvent bloqué par des politiques de flux), la commande de diagnostic dédiée suivante a été exécutée sur le FortiGate :

diag vpn ssl saml-metadata sp-tunnel

Cette commande génère et affiche l'intégralité du schéma XML directement dans la console CLI, incluant les balises de signature et la clé publique du certificat de chiffrement/signature.

Étape 4 : Alignement côté IdP (LemonLDAP::NG)

Le flux XML récupéré à l'étape précédente a été copié puis importé dans l'interface d'administration de LemonLDAP::NG en naviguant dans **Fournisseurs de services SAML** > **[votre_profil_SP]** (ex : sp-fortinet) > **Métadonnées**, rétablissant ainsi immédiatement la confiance mutuelle (*Trust relationship*) et le fonctionnement du VPN SSL.

2. Recommandation Majeure : Politique de Rotation des Certificats

? **Objectif : Ne pas perdre l'habitude et maintenir la maîtrise technique de la plateforme.**

L'un des principaux pièges des liaisons SAML/SSO est la longue durée de vie des certificats (souvent 3, 5 voire 10 ans pour les certificats d'IdP). Lorsqu'ils expirent, les équipes techniques ont souvent perdu l'historique et la procédure de renouvellement, transformant une tâche simple en coupure de production stressante.

Préconisations :

1. **Fréquence de rotation recommandée :** Mettre en œuvre un renouvellement systématique du certificat SAML **tous les 1 à 2 ans**.
2. **Entraînement des équipes :** Cette récurrence courte permet d'ancre le geste technique (génération du CSR, export PFX, modification FortiGate, extraction du XML via diag, import IdP) dans les tâches courantes d'exploitation.
3. **Mise en place d'alertes d'expiration :**
   - Configurez des alertes de supervision (via SNMP ou API) sur le FortiGate pour notifier l'équipe 30 jours avant l'expiration du certificat.
   - Utilisez les fonctions d'alerting natives de LemonLDAP::NG concernant la validité des certificats des SP enregistrés.
4. **Maintien de la documentation :** Tenez à jour cette procédure dans le wiki technique de l'équipe réseau/sécurité.