NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

SN SSO AGENT POUR LINUX - INSTALLATION ET DÉPLOIEMENT

Produits concernés : SNS 3.10, 3.11 LTSB, SSO Agent 2.1 pour Linux

Dernière mise à jour du document : 17 janvier 2022

Référence : sns-fr-sso_agent_linux_note technique-v3

Table des matières

Avant de commencer

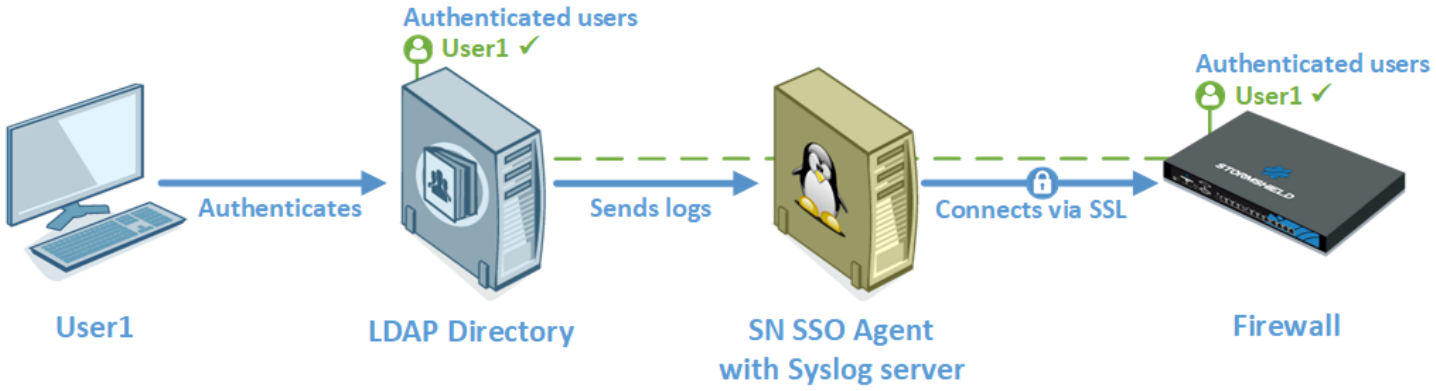
SN SSO Agent pour Linux permet aux firewalls SN de bénéficier de l'authentification sur un annuaire LDAP non Microsoft (par exemple Samba 4) de manière transparente.

A l'ouverture d'une session, c'est-à-dire lorsqu'un utilisateur se connecte au domaine d'authentification, celui-ci est automatiquement authentifié sur le firewall.

Principe

La méthode SSO (*Single Sign-On* ou *Authentification Unique*) permet à un utilisateur de ne procéder qu'à une seule authentification pour accéder à plusieurs services.

A l'ouverture d'une session, un utilisateur est authentifié sur le domaine d'authentification, générant ainsi des logs. Ces derniers sont transmis au format Syslog au SN SSO Agent, équipé d'un serveur Syslog qui filtre les logs qu'il reçoit selon des expressions régulières. SN SSO Agent relaie ensuite ces informations via une connexion SSL au firewall, qui met à jour sa table des utilisateurs authentifiés.



Pré-requis

Les pré-requis pour utiliser SN SSO Agent sont les suivants :

- Une machine sous Ubuntu 18.04 LTS pour héberger SN SSO Agent,
- Un firewall SNS et SN SSO Agent pour Linux dans une version compatible :

SN SSO Agent pour Linux	Versions SNS compatibles
2.1	3.10, 3.11 LTSB et 4.1

Préconisations

Sécurisation des échanges avec le serveur Syslog

Les échanges entre l'annuaire LDAP et le serveur Syslog du SN SSO Agent doivent s'effectuer en UDP. Ce protocole n'offrant aucune garantie de confidentialité ni d'intégrité, nous vous recommandons de sécuriser ces échanges afin d'écarter un risque potentiel de sécurité.

Ceci peut se réaliser par le biais d'une segmentation du réseau physique ou par VLAN, via un tunnel IPsec, SSH ou SSL, ou encore en positionnant en relai un serveur Syslog TLS entre les deux machines concernées.

Même si SN SSO Agent et l'annuaire LDAP peuvent être installés sur la même machine, nous vous recommandons de réaliser leur installation sur deux équipements différents.

Limitation du service

Après avoir verrouillé une première session sans la fermer, une seconde session ouverte remplace la précédente. En cas de reconnexion sur la première session, celle-ci restera identifiée avec les privilèges de la seconde session.

En conséquence, il est conseillé de fermer toute session et non de la verrouiller en cas de changement d'utilisateur sur une même machine.

Configurer l'annuaire LDAP

Pour cette notre technique, nous utilisons l'annuaire LDAP non Microsoft Samba 4 qui est installé sur une machine avec le système d'exploitation Ubuntu 18.04 LTS.

Configurer pour tracer les événements d'authentification

Éditez le fichier de configuration de l'annuaire LDAP Samba 4 selon le contexte d'utilisation adapté à votre situation. Le chemin vers ce fichier peut être différent selon votre installation.

Dans notre exemple, le fichier se situe à l'emplacement */usr/local/samba/etc/smb.conf* et contient la configuration suivante :

```
log level = 3
vfs object = full_audit
full_audit:success = connect
full_audit:failure = disconnect
full_audit:prefix = %u %I | %S
full_audit:facility = local5
```

Paramètre	Détail
log level	Permet de définir les événements à tracer. Le niveau "3" permet notamment de conserver des logs des événements d'authentification.
vfs object	Correspond au module VFS utilisé par Samba. Dans notre exemple, nous avons besoin d'utiliser le module "full_audit".
full_audit:success	Permet d'établir la liste des opérations VFS qui doivent être tracées si elles réussissent. Dans notre cas, nous ajoutons "connect" pour tracer les opérations de connexion. Le phénomène inverse existe pour les opérations qui échouent avec le paramètre "full_audit:failure".
full_audit:prefix	Permet de définir le format utilisé pour générer les logs. Personnalisez-le avec des variables qui font référence à des éléments précis, comme "%u" qui correspond au nom d'utilisateur utilisé. Ces logs étant transmis au serveur Syslog du SN SSO Agent qui les analyse grâce à des expressions régulières, définissez leur format en accord avec les éléments que vous souhaitez transmettre.
full_audit:facility	Permet d'associer à un système applicatif les logs que nous souhaitons envoyer au serveur Syslog du SN SSO Agent.

Pour plus d'informations, reportez-vous à la documentation officielle pour configurer Samba ainsi qu'à la documentation officielle du module VFS "full_audit" de Samba.

Une fois la configuration modifiée, exécutez cette commande pour que le démon recharge sa configuration et l'applique :

```
smbcontrol all reload-config
```

Configurer l'envoi des logs

L'annuaire LDAP Samba 4 s'appuie sur un client Syslog lui permettant d'envoyer des logs au format Syslog vers le serveur Syslog du SN SSO Agent.

Dans le répertoire */etc/rsyslog.d/*, créez un fichier portant le nom "00-samba.conf". Ajoutez-y la configuration souhaitée en respectant le format suivant :

```
facility.syslogseverity @ip:port
```

Dans notre exemple, nous utilisons la configuration suivante :

```
local5.notice @172.30.227.74:3514
```

Paramètre	Détail
facility	Permet de définir le système applicatif pour lequel le client Syslog récupère les logs. Dans notre exemple, il correspond au paramètre "full_audit:facility" renseigné dans la configuration de l'annuaire LDAP Samba 4.
syslogseverity	Correspond au niveau de criticité des logs Syslog. Avec le système applicatif (facility) renseigné, ceci détermine les logs qui sont transmis au serveur Syslog du SN SSO Agent.
@	Spécifie l'utilisation du mode UDP pour l'envoi des logs. Les échanges avec le serveur Syslog du SN SSO Agent doivent s'effectuer en UDP.
ip:port	Correspond à l'adresse IP du SN SSO Agent vers lequel les logs sont envoyés, ainsi que le numéro de port sur lequel son serveur Syslog écoute. Nous recommandons d'utiliser un port supérieur ou égal à 1024. Pour utiliser un port inférieur à 1024, SN SSO Agent doit être démarré avec des droits administrateur (sudo).

Pour plus d'informations, reportez-vous à la documentation officielle Syslog.

Une fois le fichier de configuration ajouté, exécutez cette commande pour redémarrer le démon rsyslog :

```
sudo service rsyslog restart
```

Installer SN SSO Agent

Télécharger SN SSO Agent

1. Connectez-vous à votre espace personnel MyStormshield,
2. Rendez-vous dans la partie **Téléchargements**,
3. Dans **Stormshield Network Security** > **SSO Agent**, téléchargez l'archive SN SSO Agent pour Linux et copiez-la sur la machine où vous souhaitez l'installer.

Configurer SN SSO Agent

1. Sur la machine concernée, décompressez l'archive dans le répertoire de votre choix. Par sécurité, ce répertoire doit avoir des droits limités.
2. Ouvrez le fichier de configuration du SN SSO Agent, "config.ini".
3. Éditez les paramètres suivants :

Paramètre	Détail
VerboseLevel	Définit la quantité d'information tracée. Renseignez "low" pour une utilisation en production. Utilisez le niveau "high" pour une utilisation en phase d'installation.
SSLKey	Définit le mot de passe permettant au SN SSO Agent de communiquer avec votre firewall. Pour garantir sa complexité, il est conseillé d'utiliser des majuscules, des caractères spéciaux, ainsi qu'une longueur minimale suffisante. Gardez en tête ce mot de passe, il doit être également renseigné dans la configuration de votre firewall.

Démarrer SN SSO Agent

Utilisez la commande suivante pour démarrer SN SSO Agent :

```
./stormshieldssoagent
```

Adaptez la manipulation pour démarrer SN SSO Agent avec des droits administrateur (sudo) s'il doit utiliser un port Syslog inférieur à 1024.

Vous pouvez également configurer sur la machine un démarrage automatique du SN SSO Agent. Pour cela, nous vous recommandons de créer un service spécifique permettant de lancer automatiquement SN SSO Agent lors du processus de démarrage. Plusieurs solutions existent, par exemple via "Systemd" ou via "/etc/init.d". Pour plus d'informations, reportez-vous à la documentation du site Wiki ubuntu-fr "Les services système".

Configurer le firewall SN

Plusieurs manipulations sont nécessaires pour configurer le firewall :

- Créer des objets réseau,
- Ajouter l'annuaire LDAP,
- Ajouter une méthode d'authentification,
- Définir une politique d'authentification.

Créer des objets réseau

Vous devez créer plusieurs objets réseau :

- Un objet "Machine" pour l'équipement hébergeant l'annuaire LDAP,
- Un objet "Machine" pour l'équipement hébergeant SN SSO Agent,
- Un objet "Port" représentant le port d'écoute du serveur Syslog du SN SSO Agent, sauf dans le cas où vous utilisez le port par défaut (514 en UDP) pour lequel un objet existe déjà.

Créer les objets "Machine"

1. Connectez-vous à l'interface d'administration du firewall à l'adresse : https://*adresseIP_du_firewall*/admin.
2. Rendez-vous dans le module **Configuration** > **Objets** > **Objets réseau**.
3. Cliquez sur **Ajouter**.
4. Dans l'assistant, assurez-vous d'être positionné sur l'onglet **Machine**.
5. Entrez le nom du SN SSO Agent ou de l'annuaire LDAP dans le champ **Nom de l'objet**.
6. Renseignez l'adresse IPv4 de la machine concernée. Pour sa résolution DNS, nous recommandons une utilisation **statique** (adresse IP fixe). Il est cependant possible, selon votre configuration, d'utiliser une résolution dynamique (DHCP changeant l'adresse IP à chaque connexion).
7. L'adresse MAC de la machine n'est pas requise. Renseignez-la seulement si cela est nécessaire à votre configuration.

Si vous disposez de plusieurs SN SSO Agent ou de plusieurs annuaires LDAP, créez des objets "Machine" pour chacun d'entre eux.

Créer l'objet "Port"

1. Connectez-vous à l'interface d'administration du firewall à l'adresse : https://*adresseIP_du_firewall*/admin.
2. Rendez-vous dans le module **Configuration** > **Objets** > **Objets réseau**.
3. Cliquez sur **Ajouter**.
4. Dans l'assistant, positionnez-vous sur l'onglet **Port**.
5. Définissez un nom à l'objet.
6. Renseignez le numéro de port sur lequel le serveur Syslog concerné écoute.
7. Sélectionnez le protocole "UDP".

Si vous disposez de plusieurs SN SSO Agent, et donc de plusieurs serveur Syslog, créez un objet "Port" pour chaque port d'écoute nécessaire à votre configuration.

Ajouter l'annuaire LDAP

Ajouter votre annuaire LDAP permet notamment d'accéder à la recherche de ses utilisateurs et groupes depuis votre firewall. Vous pourrez ainsi y définir une politique d'authentification basée sur les utilisateurs et groupes de votre annuaire LDAP.

Pour ajouter l'annuaire LDAP sur le firewall :

1. Connectez-vous à l'interface d'administration du firewall à l'adresse : https://*adresseIP_du_firewall*/admin.
2. Rendez-vous dans le module **Configuration** > **Utilisateurs** > **Configuration des annuaires**.
3. Si vous n'avez pas encore configuré un annuaire sur le firewall, l'assistant de création s'affiche automatiquement. Si ce n'est pas le cas, cliquez sur **Ajouter un annuaire**.
4. Dans l'assistant, sélectionnez le type "Connexion à un annuaire LDAP externe".
5. Renseignez les informations d'accès à l'annuaire. Pour plus d'informations, reportez-vous au manuel utilisateur SNS.

Répétez ces étapes pour ajouter plusieurs annuaires. Vous pouvez configurer jusqu'à 4 annuaires LDAP non Microsoft et/ou annuaire Active Directory en plus de l'annuaire interne.

Ajouter une méthode d'authentification

Vous devez configurer sur votre firewall la méthode d'authentification "Agent SSO" pour permettre aux utilisateurs du domaine d'authentification concerné de s'authentifier. Vous avez la possibilité de configurer jusqu'à 5 méthodes d'authentification "Agent SSO".

1. Connectez-vous à l'interface d'administration du firewall à l'adresse : https://*adresseIP_du_firewall*/admin.
2. Rendez-vous dans le module **Configuration** > **Utilisateurs** > **Authentification**, onglet *Méthodes disponibles*.
3. Cliquez sur **Ajouter une méthode** et sélectionnez **Agent SSO** dans le menu déroulant.
4. Dans la partie de droite, pour le champ **Nom de domaine**, sélectionnez dans la liste déroulante le domaine d'authentification concerné.
5. Poursuivez ensuite la configuration zone par zone selon les éléments ci-dessous.

Zone "Agent SSO"

Renseignez les informations du SN SSO Agent principal :

Champ	Détail
Adresse IP	Sélectionnez dans la liste l'objet "Machine" correspondant au SN SSO Agent créé précédemment.
Port	Laissez l'objet "agent_ad" sélectionné par défaut.
Clé pré-partagée	Renseignez la clé (SSLKey) définie lors de l'installation du SN SSO Agent. Cette clé est utilisée pour le chiffrement en SSL des échanges entre SN SSO Agent et le firewall. La force de la clé pré-partagée indique le niveau de sécurité du mot de passe.

Zone "Contrôleur de domaine"

Ajoutez tous les annuaires LDAP qui régissent le domaine d'authentification concerné. Ceux-ci doivent au préalable être enregistrés dans la base **Objets réseau** du firewall. Pour plus d'informations, reportez-vous à la section Créer des objets réseau.

Zone "Configuration avancée"

Mode : SN SSO Agent étant installé sur une machine Linux, sélectionnez **Mode serveur Syslog**.

Configuration du serveur Syslog :

Champ	Détail
Adresse IP d'écoute	Choisissez dans la liste l'objet "Machine" associé à la machine hébergeant SN SSO Agent et son serveur Syslog.
Port d'écoute	Sélectionnez dans la liste l'objet "Port" représentant le port d'écoute du serveur Syslog. L'objet "syslog" y est proposé par défaut (514 en UDP).
Recherche d'adresse IP	Expression régulière destinée à rechercher les adresses IP dans les logs hébergés par le serveur Syslog. Pour cette note technique, nous utilisons : `([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})\s`
Recherche d'utilisateur	Expression régulière destinée à rechercher les noms d'utilisateurs dans les logs hébergés par le serveur Syslog. Pour cette note technique, nous utilisons : `NOMDEDOMAINE\\([a-zA-Z0-9\.]*)\s` Remplacez "NOMDEDOMAINE" par le domaine d'authentification utilisé. Pensez également à protéger les caractères spéciaux utilisés.
Recherche de message	Expression régulière destinée à rechercher les messages de connexion dans les logs hébergés par le serveur Syslog. Pour cette note technique, nous utilisons : `connect|ok` Prenez soin de formater correctement cette expression régulière pour éviter d'inclure dans la recherche de message des résultats non souhaités.

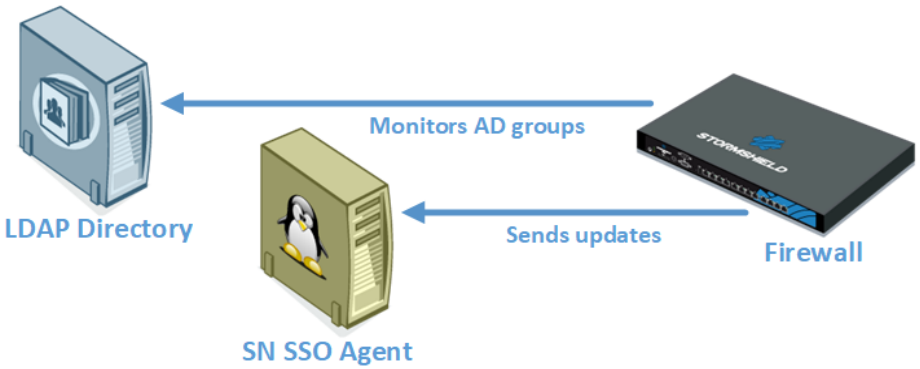
Pour plus d'informations sur ces éléments, reportez-vous au manuel utilisateur SNS.

Durée maximum d'authentification : définissez la durée maximale de session d'un utilisateur authentifié. Passé ce délai, le firewall supprime l'utilisateur associé à cette adresse IP de sa table d'utilisateurs authentifiés, déconnectant l'utilisateur du firewall.

Ce seuil est à définir en minutes ou heures et est fixé par défaut à 10 heures.

Délai de mises à jour des groupes d'utilisateurs : pour chaque annuaire LDAP configuré sur le firewall, ce dernier consulte les éventuelles modifications apportées aux **groupes de l'annuaire LDAP**. Le firewall met à jour la configuration de son annuaire, puis renvoie ces informations au SN SSO Agent.

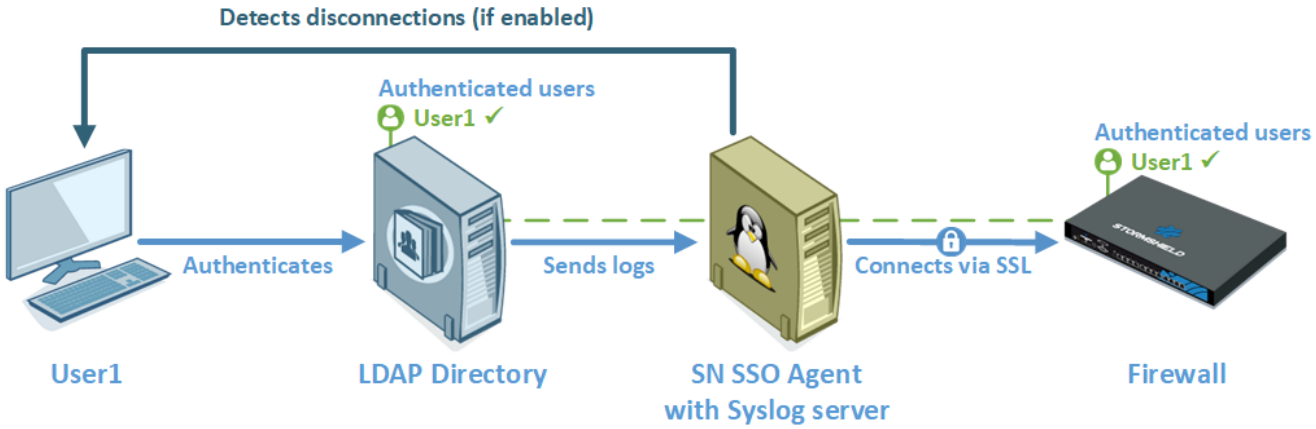
Ce seuil est à définir en minutes ou heures et est fixé par défaut à 1 heure.



Détection des déconnexions : activez la méthode de déconnexion pour supprimer les utilisateurs authentifiés lors d'une déconnexion de la machine ou d'une fermeture de session. Sans l'activation de cette méthode, l'utilisateur sera désauthentifié une fois la durée maximale d'authentification fixée atteinte, même en cas de fermeture de session.

SN SSO Agent teste l'accessibilité des machines authentifiées sur le firewall toutes les 60 secondes par le biais d'un test de PING. Pour que ce test fonctionne, il est indispensable :

- Que les machines du domaine d'authentification autorisent les réponses au test de PING (requêtes ICMP). Le pare-feu Windows peut par exemple bloquer ces requêtes.
- Qu'une règle dans la politique de filtrage du firewall autorise SN SSO Agent à tester les machines du domaine d'authentification si celui-ci doit passer au travers du firewall pour y accéder.



Considérer comme déconnecté après : si une machine ne répond pas pendant une durée définie au test de "Détection des déconnexions" réalisé toutes les 60 secondes, SN SSO Agent considère cette machine comme déconnectée. Il envoie alors une demande de déconnexion au firewall qui supprime l'utilisateur concerné de sa table d'utilisateurs authentifiés, le déconnectant du firewall.

Cette durée est déterminée en secondes ou minutes et est fixée par défaut à 5 minutes.

Activer la vérification DNS des machines : activez ce paramètre si les machines connectées au firewall ont plusieurs adresses IP ou en changent régulièrement. Par exemple, ce paramètre peut être intéressant si vos utilisateurs passent souvent d'une connexion en Ethernet à une connexion en WIFI.

Pour cette vérification, SN SSO Agent effectue périodiquement une requête DNS (PTR) pour vérifier que les machines n'ont pas changé d'IP. En cas de nouvelle adresse IP, l'information est envoyée au firewall. Pour que ce test fonctionne, il est indispensable :

- Qu'une **Zone de recherche inversée** ou **Reverse lookup zone** (clic droit sur le dossier) soit ajoutée dans les paramètres du serveur DNS des machines du domaine d'authentification,
- Qu'une règle dans la politique de filtrage du firewall autorise SN SSO Agent à tester les machines du domaine d'authentification si celui-ci doit passer au travers du firewall pour y accéder.

Comptes d'Administration ignorés : dans la configuration d'usine du firewall, il existe une liste d'utilisateurs dont l'authentification est ignorée. Cette liste comporte les identifiants usuels dédiés à l'administrateur (*Administrator* et *Administrateur* par défaut).

Ce mécanisme a été mis en place car le lancement d'un service ou d'une application (fonction *Exécuter en tant qu'administrateur*, par exemple) est vu par l'annuaire LDAP comme une authentification. SN SSO Agent restreignant à une authentification par adresse IP, ce type d'authentification pourrait remplacer l'authentification de l'utilisateur ayant ouvert une session.

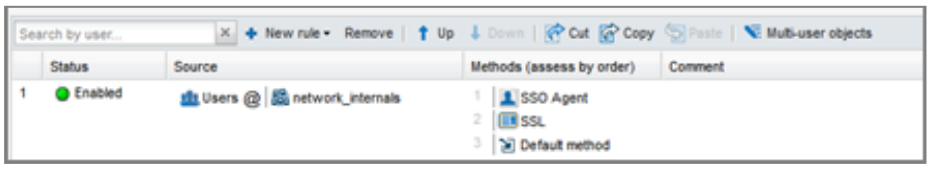
Cette liste préétablie de "Comptes Administrateur ignorés" permet au SN SSO Agent de ne pas prendre en compte leur authentification. Modifiez-la si nécessaire.

Définir une politique d'authentification

Pour autoriser le trafic dédié à la méthode d'authentification "Agent SSO" configurée, vous devez définir une ou plusieurs règles dans la politique d'authentification.

1. Connectez-vous à l'interface d'administration du firewall à l'adresse : https://*adresseIP_du_firewall*/admin.
2. Rendez-vous dans le module **Configuration** > **Utilisateurs** > **Authentification**, onglet *Politique d'authentification*.
3. Cliquez sur **Nouvelle règle** et sélectionnez **Règle standard** pour lancer l'assistant de création.
4. Dans l'onglet **Utilisateur**, champ **Utilisateur ou groupe**, sélectionnez l'utilisateur ou le groupe concerné, ou laissez la valeur par défaut *Any_user@domaine*.
5. Dans l'onglet **Source**, cliquez sur **Ajouter un objet** et sélectionnez l'origine du trafic concernée par la règle. Cela peut être l'objet correspondant aux réseaux internes (*network_internals*).
   Une interface ne peut pas être appliquée comme critère pour la méthode d'authentification "Agent SSO" qui se base sur les événements d'authentification collectés par les annuaires LDAP. Ceux-ci n'indiquant pas l'origine du trafic, la politique d'authentification ne peut pas être spécifiée avec des interfaces.
6. Dans l'onglet **Méthodes d'authentification**, cliquez sur **Autoriser une méthode** et sélectionnez dans la liste déroulante les méthodes d'authentification à appliquer au trafic concerné par la règle. **Elles sont évaluées dans l'ordre de la liste**, du haut vers le bas. La méthode "Agent SSO" étant transparente, elle est par définition toujours appliquée en priorité.
   La méthode par défaut peut être modifiée en dessous du tableau des règles de la politique d'authentification.
7. Cliquez sur **OK** puis sur **Appliquer**.

Répétez les étapes ci-dessus pour ajouter plusieurs règles.

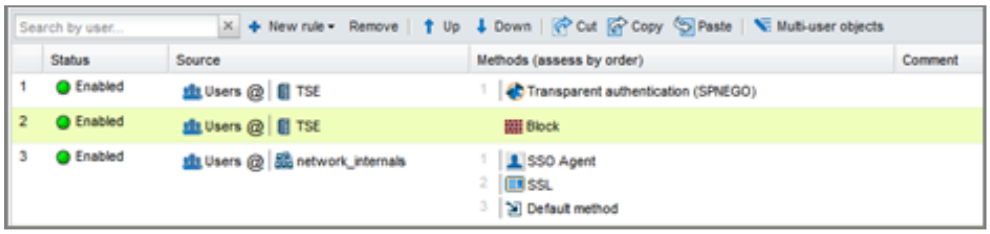


La méthode "Agent SSO" ne supporte pas les objets multi-utilisateur (plusieurs utilisateurs authentifiés sur une même adresse IP). Or, un objet de ce type peut être contenu dans un réseau, une plage ou un groupe défini comme source d'une règle faisant appel à la méthode d'authentification "Agent SSO".

Pour éviter d'avoir des logs de rejet du SN SSO Agent pour les utilisateurs sur une adresse déclarée comme multi-utilisateur, il est conseillé d'ajouter deux règles dédiées à ce type d'objet, précédant celles utilisant la méthode d'authentification "Agent SSO" :

- La première règle précise la méthode d'authentification employée par l'objet multi-utilisateur,
- La suivante précise d'"interdire" pour l'objet multi-utilisateur toute autre méthode d'authentification.

Dans l'exemple ci-dessous, la machine TSE est déclarée comme objet multi-utilisateur et appartient au réseau interne (network_internals) :



Vérifier le fonctionnement

Vérifier le fonctionnement du service vous permet notamment de vous assurer que SN SSO Agent est correctement installé et configuré, et que le firewall est correctement paramétré.

Plusieurs manipulations sont possibles pour vérifier le fonctionnement du service :

- Consulter les logs du SN SSO Agent,
- Consulter les logs sur l'interface d'administration du firewall.

Consulter les logs du SN SSO Agent

Les logs enregistrent les communications entre SN SSO Agent et votre firewall. Ils peuvent contenir les informations suivantes :

- La connexion du SN SSO Agent au firewall. Si elle échoue, un message d'erreur est retourné.
- Les règles de la politique d'authentification appliquées aux utilisateurs.
- Les ouvertures de session des utilisateurs (date et heure de la session, nom de l'utilisateur concerné, adresse IP de la machine utilisée).
- Les déconnexions des machines associées aux utilisateurs.

Pour accéder aux logs, identifiez le répertoire où est installé SN SSO Agent sur la machine, puis consultez les fichiers dans le répertoire */log/*, par exemple "stormshieldssoagent.log".

La taille maximale d'un fichier est de 1 Mo. Le dossier peut contenir un maximum de 100 Mo. Quand le dossier atteint la limite, le fichier de logs le plus ancien est supprimé. Ces fichiers permettent le dépannage du service et sont nécessaires lors d'une assistance technique auprès de notre Technical Assistance Center.

L'image ci-dessous affiche un extrait d'un fichier de logs contenant une information de connexion au firewall.

Consulter les logs sur le firewall

Sur le firewall où est configurée la méthode d'authentification "Agent SSO", vous pouvez consulter les logs des utilisateurs qui s'authentifient ainsi que les connexions entre SN SSO Agent et le firewall.

Authentification des utilisateurs

1. Connectez-vous à l'interface d'administration du firewall à l'adresse : https://*adresseIP_du_firewall*/admin.
2. Rendez-vous dans le module **Supervision** > **Utilisateurs**.
3. Filtrez les résultats par méthode d'authentification.

Pour plus d'informations, reportez-vous au manuel utilisateur SNS ainsi que sur la note technique Se conformer aux règlements sur les données personnelles.

Connexion entre SN SSO Agent et le firewall

1. Connectez-vous à l'interface d'administration du firewall à l'adresse : https://*adresseIP_du_firewall*/admin.
2. Rendez-vous dans le module **Logs - Journaux d'audit** > **Événements système**.
3. Dans la fenêtre, affichez les données selon la période de temps souhaitée.

Pour plus d'informations, reportez-vous au manuel utilisateur SNS.

Cas spécifiques

Cette section aborde des cas différents que celui mettant en œuvre un firewall unique dans un seul domaine d'authentification, avec un seul SN SSO Agent.

Firewalls multiples gérant le même domaine d'authentification

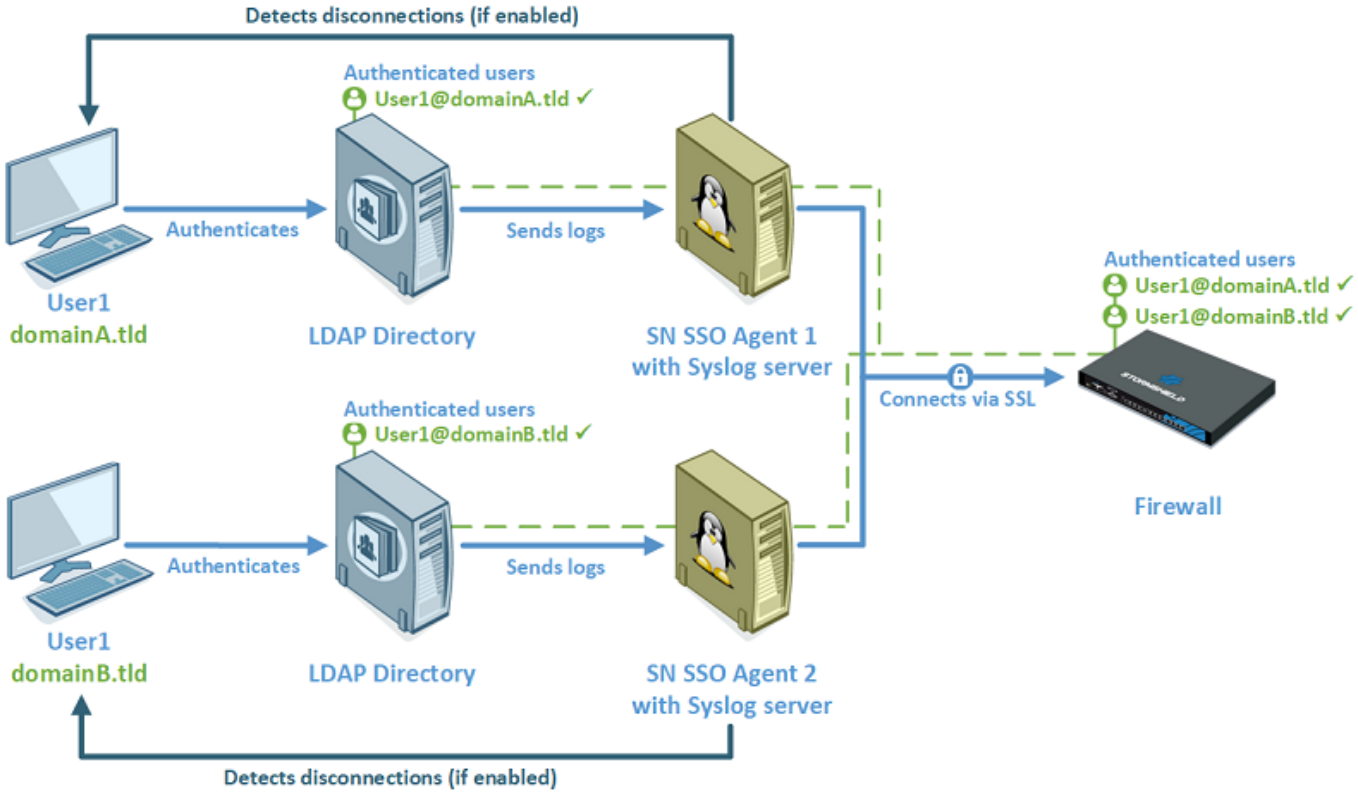
Plusieurs firewalls gérant le même domaine d'authentification peuvent se connecter au même SN SSO Agent.

Firewall unique gérant plusieurs domaines d'authentification

Lorsqu'un firewall gère plusieurs domaines d'authentification, qu'ils soient de type annuaire LDAP non Microsoft et/ou annuaire Active Directory, il est impératif de dédier à chacun d'entre eux un SN SSO Agent. Un firewall peut gérer jusqu'à 5 SN SSO Agent et donc gérer jusqu'à 5 domaines d'authentification différents.

Pour plus d'informations concernant l'installation à réaliser avec un domaine d'authentification de type annuaire Active Directory (Microsoft), reportez-vous à la note technique "Stormshield Network SSO Agent pour Windows".

L'exemple suivant montre un firewall gérant deux domaines d'authentification de type annuaire LDAP non Microsoft.



Résoudre les problèmes

La vérification des éléments ci-dessous peut aider à la résolution d'un dysfonctionnement.

SN SSO Agent ne peut pas se connecter au firewall

- Vérifiez la **clé de chiffrement SSL** (SSLKey), dite **clé pré-partagée**.
  Elle est renseignée dans la configuration du SN SSO Agent (fichier config.ini) ainsi que dans la configuration de la méthode d'authentification "Agent SSO".
- Assurez-vous que le **port 1301**, ou celui que vous avez personnalisé, ne soit pas bloqué par un firewall ou sur la machine hébergeant SN SSO Agent.
  Pour cette dernière, vérifiez que les messages transitent correctement par ce port avec la commande :
  ```
  tcpdump port 1301
  ```
- Vérifiez les logs depuis l'interface d'administration du firewall dans le module **Logs - Journaux d'audit** > **Événements système**.

Aucun utilisateur ne s'authentifie sur le firewall

- Vérifiez les logs depuis l'interface d'administration du firewall dans le module **Logs - Journaux d'audit** > **Authentification**.
- Assurez-vous qu'aucune règle de la politique d'authentification ne bloque les utilisateurs qui essayent de s'authentifier.
  Tentez d'ajouter en premier (tout en haut) dans votre politique d'authentification une règle utilisant les éléments suivants :
  - Pour le champ **Utilisateur** : "Tous",
  - Pour le champ **Source** : "Any",
  - Pour le champ **Méthodes d'authentification** : la méthode "Agent SSO" concernée.
- Vérifiez grâce à la commande suivante que les messages envoyés par le serveur Syslog du SN SSO Agent au firewall transitent correctement par le port défini dans sa configuration.
  ```
  tcpdump port 3514
  ```
- Assurez-vous que les informations du serveur Syslog soient correctement renseignées dans la méthode d'authentification "Agent SSO" configurée sur le firewall.
- Assurez-vous que les expressions régulières configurées dans votre firewall et utilisées par le serveur Syslog du SN SSO Agent permettent de récupérer les événements d'authentification nécessaires au bon fonctionnement du service. Aidez-vous d'un site vous permettant de vérifier vos expressions régulières (*RegEx*) si besoin.

Le serveur Syslog du SN SSO Agent ne récupère pas les événements de l'annuaire LDAP

- Assurez-vous que la configuration de votre annuaire LDAP soit correcte. Pour plus d'informations, reportez-vous à la section Configurer l'annuaire LDAP.

- Vérifiez que l'annuaire LDAP trace correctement les événements d'authentification. Dans notre exemple, nous utilisons la commande suivante pour le vérifier sur un serveur Samba 4. Le chemin d'accès peut avoir été modifié dans la configuration du serveur (fichier smb.conf).

```
tail -f /var/log/messages.log
```

- Vérifiez la configuration du client Syslog installé sur la même machine de votre annualre LDAP (fichier 00-samba.conf). Tentez de modifier sa configuration pour qu'il transmette tous les logs qu'importe le niveau de criticité et le système applicatif lié. Respectez le format suivant en conservant "*.*" :

```
*.* @ip:port
```

documentation@stormshield.eu