NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

CONFIGURER LES MÉTHODES D'AUTHENTIFICATION DE TYPE "GUEST"

Produits concernés : SNS 3.x, SNS 4.x

Date : 09 décembre 2019

Référence : sns-fr-configurer_les_methodes_guests_note_technique

Table des matières

Avant de commencer

Pour permettre aux utilisateurs externes d'une entreprise d'accéder à des ressources réseau ciblées (accès Internet par exemple), la version 3 de firmware SNS propose 3 méthodes d'authentification :

- La méthode "Invités" (mode déclaratif) : cette méthode est basée sur l'acceptation d'un panneau présentant les conditions d'accès à Internet (*disclaimer*). Elle est particulièrement adaptée pour proposer un accès Internet public dans un lieu de passage comme un restaurant, une gare, un office de tourisme ...
- Les comptes temporaires : il est possible de créer des comptes à durée limitée dans le temps. La durée de validité de ces comptes est paramétrable pour chaque compte. Cette méthode est par exemple destinée aux infrastructures hôtelières souhaitant proposer un accès Internet limité à la durée de séjour des clients.
- La méthode "Parrainage" : depuis le portail captif, l'utilisateur renseigne ses noms et prénoms ainsi que l'adresse e-mail d'un correspondant interne. Ce correspondant, s'il est habilité et explicitement déclaré dans le firewall comme étant autorisé à parrainer des utilisateurs, valide la demande, autorisant ainsi immédiatement l'accès aux ressources Web pour le demandeur. Cette méthode peut, par exemple, être utilisée au sein d'une entreprise pour offrir un accès Internet à ses visiteurs prestataires.

Configurer la méthode "Invités" (mode déclaratif)

Ce mode consiste en une identification sans authentification. Lors de sa première connexion à Internet, l'utilisateur est redirigé vers le portail captif. Les conditions d'utilisation de l'accès à Internet lui sont alors présentées, et il doit les valider pour accéder au site Web demandé. Il peut ensuite accéder, selon la politique de filtrage d'URL mise en place, aux ressources web.
L'affichage des conditions d'accès à Internet intervient de manière régulière; cette fréquence est paramétrable. La durée de connexion d'un utilisateur invité est de 4 heures.

Il est possible d'inclure 1 à 3 champs complémentaires (Nom, Prénom, E-mail...) que l'utilisateur invité pourra remplir avant d'accepter les conditions d'accès. Ces informations complémentaires sont reportées dans les fichiers de traces du firewall. Il est également possible de définir plusieurs profils d'authentification pour le portail captif. Chaque profil pouvant être associé à une ou plusieurs interfaces réseau du firewall, il est ainsi possible de configurer plusieurs accès à Internet via la méthode « Invités » mais présentant des paramètres distincts (champs complémentaires) selon l'interface par laquelle l'utilisateur se présente.

Activer la méthode "Invités"

1. Dans l'onglet *Méthodes disponibles* du module **Configuration** > **Utilisateurs** > **Authentification**, déroulez le menu **Ajouter une méthode** et cliquez sur **Invités**.
2. Dans le panneau de droite, réglez la fréquence d'affichage des Conditions d'utilisation de l'accès à Internet. Cette fréquence peut être exprimée en minutes, heures ou jours. La valeur proposée par défaut est de 1440 minutes (18 heures).

Créer une règle dans la politique d'authentification

1. Dans l'onglet *Politique d'authentification* du module **Configuration** > **Utilisateurs** > **Authentification**, déroulez le menu **Nouvelle règle** et cliquez sur **Règle Invités**.
2. Cliquez sur **Ajouter une interface** et sélectionnez la ou les interface(s) par laquelle peuvent se présenter les comptes invités.
3. Cliquez sur **Ajouter un objet** pour sélectionner (ou créer puis sélectionner) le réseau ou les machines depuis lesquels les invités vont se connecter.
4. Validez en cliquant sur **Terminer**
5. Double cliquez sur l'état de cette règle afin de l'activer.
6. Cliquez sur le bouton **Appliquer**.

Personnaliser un profil de portail captif pour cette méthode

Dans l'onglet *Profils du portail captif* du module **Configuration** > **Utilisateurs** > **Authentification**, sélectionnez le profil *"Guest"*. Ce profil implémente automatiquement les paramètres nécessaires au fonctionnement de cette méthode :

Authentification

- **Méthode ou annuaire par défaut :** *"Invités (guest_users.local.domain)"*.

Conditions d'utilisation de l'accès à Internet

- **Activer l'affichage des conditions d'utilisation d'accès à Internet**. La fréquence d'affichage de des conditions est fixée à 18 heures.

> **NOTE**
> Le texte des conditions d'accès est personnalisable dans l'onglet *Portail captif*.

Champs personnalisés du portail captif

- **Champ n°1** : E-mail
- **Champ n°2** : Vide
- **Champ n°3** : Vide

> **NOTE**
> La saisie de ces champs est optionnelle pour valider les conditions d'accès à Internet.

Configuration avancée

- **Activer le portail captif**.
- **Expiration du 'cookie' HTTP** : *"A la fin de la période d'authentification"*.

En cas de modification de l'un de ces paramètres (exemple : champs personnalisés du portail captif), cliquez sur **Appliquer** pour enregistrer la configuration.

Associer le profil du portail captif et les interfaces réseau concernées

Sélectionnez l'onglet *Portail captif* du module **Configuration** > **Utilisateurs** > **Authentification**. La grille **Correspondance entre profil d'authentification et interface** est vide. Cliquez sur le bouton **Ajouter** pour sélectionner l'interface souhaitée et affectez-lui le profil *Guest*. La méthode et l'annuaire associés à ce profil sont automatiquement renseignés dans la colonne *Méthode ou annuaire par défaut*.

Adapter la politique de filtrage pour les utilisateurs invités

La politique de filtrage décrite ci-dessous permet aux utilisateurs invités d'accéder aux sites Internet en HTTP et HTTPS avec du filtrage d'URL.

Créer une règle d'inspection SSL

L'assistant permet de créer deux règles : l'une destinée à déchiffrer les flux HTTPS, l'autre pour les diriger vers le proxy SSL afin de les soumettre au filtrage d'URL et aux traitements de prévention d'intrusion.

1. Dans l'onglet *Filtrage* du module **Configuration** > **Politique de sécurité** > **Filtrage et NAT**, cliquez sur le bouton **Nouvelle règle** et sélectionnez **Règle d'inspection SSL.**
2. Renseignez les réseaux ou machines sources (colonne **Depuis** - *guests_network* dans l'exemple), la destination (colonne **Vers** - *Internet* dans l'exemple) et le port destination (HTTPS dans l'exemple). Validez en cliquant sur **Terminer**.
3. Faites un double-clic sur la source de la règle de redirection vers le proxy SSL. Dans le champ **Utilisateur**, sélectionnez Any user@guest_users.local.domain.

4. Dans l'onglet *Configuration avancée*, sélectionnez *Invité* comme **Méthode d'authentification**.
5. Dans la section **Port / Protocole**, sélectionnez la valeur *Protocole applicatif* pour le champ **Type de protocole**, puis *HTTP* pour le **Protocole applicatif**.
6. Dans la section **Inspection**, sélectionnez le profil de filtrage d'URL à appliquer (*URLFilter_00* dans l'exemple).
7. Validez en cliquant sur **OK**.

Créer une règle de redirection vers le portail captif

1. Dans l'onglet *Filtrage* du module **Configuration** > **Politique de sécurité** > **Filtrage et NAT**, cliquez sur le bouton **Nouvelle règle** et sélectionnez **Règle d'authentification**.
2. Dans l'assistant de création, renseignez les réseaux ou machines sources (champ **Depuis** - *guests_network* dans l'exemple) et la destination (champ **Vers** - *Internet* dans l'exemple) pour lesquels les utilisateurs non authentifiés seront redirigés vers le portail captif.
3. Validez en cliquant sur le bouton **Terminer**. Cette règle sélectionne le port HTTP comme port destination par défaut.
4. Pour y ajouter le port HTTPS, double-cliquez sur le champ **Port dest** de cette règle. Dans le champ **Port destination** de la fenêtre d'édition de la règle, ajoutez le port HTTPS. Validez en cliquant sur **OK**.
5. A l'aides des flèches **Monter** et **Descendre**, placez cette règle entre la règle de déchiffrement SSL et la règle de redirection vers le proxy SSL.

Ajouter la règles de filtrage des flux HTTP pour les utilisateurs invités

1. Dans l'onglet *Filtrage* du module **Configuration** > **Politique de sécurité** > **Filtrage et NAT**, cliquez sur le bouton **Nouvelle règle** et sélectionnez **Règle simple**.
2. Dans la colonne Status, double-cliquez sur *Off* pour activer la règle (l'état de la règle passe à *On*).
3. Dans la colonne **Action**, double-cliquez sur *bloquer* puis choisissez la valeur *passer* pour le champ **Action**. Sélectionnez le niveau de traces souhaité pour les connexions correspondant à cette règle; *tracer (journal de filtrage)* permet de visualiser les événements liés aux connexions des utilisateurs invités dans les journaux de connexion par exemple.
4. Dans la section **Source** située sur la gauche de la fenêtre d'édition de la règle, affectez les valeurs suivantes aux différents champs :

Onglet général

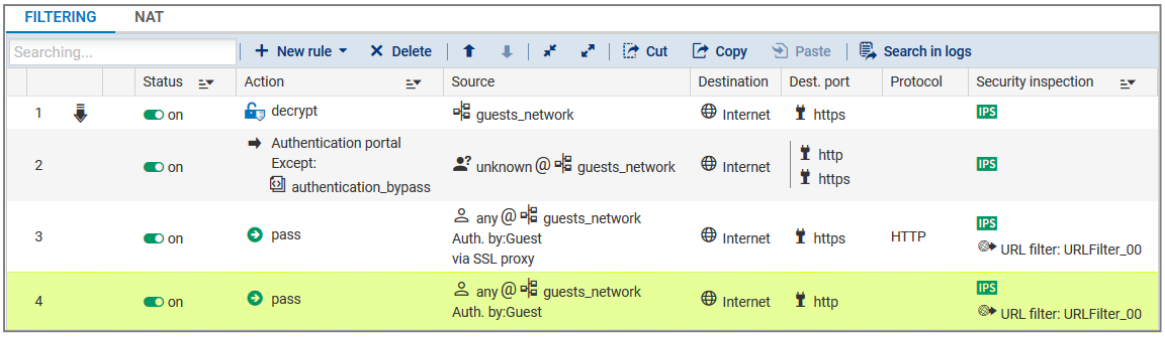
- **Utilisateur** : sélectionnez *Any user@guest_users.local.domain.*
- **Machines sources** : sélectionnez le réseau des utilisateurs invités.

Onglet configuration avancée

- **Méthode d'authentification** : sélectionnez la méthode *Invité*.

5. Dans la section **Destination**, sélectionnez l'objet *Internet* pour le champ **Machines destinations.**
6. Dans la section **Port - Protocole**, sélectionnez l'objet HTTP pour le champ **Port destination**.
7. Dans la section **Inspection**, laissez le mode IPS proposé par défaut et sélectionnez le profil de filtrage d'URL à appliquer (*URLFilter_00* dans l'exemple). Ce profil pourra être personnalisé dans le module **Configuration** > **Politique de sécurité** > **Filtrage URL**.

La politique de filtrage concernant les utilisateurs invités prend ainsi la forme suivante :



Consulter les journaux de traces

Dans la méthode Invités, les utilisateurs ne sont pas enregistrés dans une annuaire LDAP. Ils sont associés à des comptes générés automatiquement par le firewall et dont la durée de vie correspond à la durée d'authentification des utilisateurs invités.

Ces comptes prennent la forme d'une chaîne aléatoire de caractères préfixée par "*guest_*".

Si des champs personnalisés de type Nom, Prénom, E-mail,... ont été définis dans le profil d'authentification, les valeurs renseignées dans ces champs peuvent permettre d'associer l'utilisateur réel à l'utilisateur virtuel.

Associer le compte virtuel et les informations complémentaires

Depuis l'interface d'administration Web du Firewall, accédez aux journaux de traces (**Utilisateurs**, **Trafic réseau**, **Filtrage**) et aux rapports afin de vérifier le fonctionnement de la configuration mise en place.

Le journal Utilisateurs indique le nom *guest_xxxx* attribué par le firewall (colonne **Utilisateur**), l'adresse IP source de la machine, la méthode ("Invité") et la valeur des éventuels champs additionnels s'ils ont été remplis par l'utilisateur (colonne **Message**).

Configurer la méthode "Comptes temporaires"

Cette méthode permet de créer des comptes à durée limitée dans le temps. Ces comptes sont composés au minimum d'un nom et d'un prénom qui forment l'identifiant du compte, ainsi que d'un mot de passe généré automatiquement. La durée de validité de ces comptes est paramétrable pour chaque compte. Cette méthode est par exemple destinée aux infrastructures hôtelières souhaitant proposer un accès Internet limité à la durée de séjour des clients.

Il est possible de déléguer la création des comptes temporaires à un utilisateur qui bénéficiera d'un accès limité exclusivement au module permettant de créer ce type de comptes.

Activer la méthode "Comptes temporaires"

1. Vous pouvez régler une durée de validité par défaut pour la création d'un nouveau compte. Cette durée est exprimée en jours. Elle sera proposée par défaut à chaque création de nouveau compte et pourra être remplacée par une durée personnalisée.
2. Appliquez les modifications. La méthode "Comptes Temporaires" est alors automatiquement ajoutée à la liste des méthodes d'authentification disponibles.

Ajouter un utilisateur délégué à la création des comptes temporaires

Si vous souhaitez déléguer la création des comptes temporaires à un ou plusieurs utilisateur (s), il est nécessaire de définir des "administrateur de comptes temporaires". Lorsqu'ils se connectent à l'interface d'administration du firewall, ces utilisateurs particuliers ont uniquement accès au module de gestion des comptes temporaires.

1. Dans le module **Configuration** > **Système** > **Administrateurs**, déroulez le menu **Ajouter un administrateur** et sélectionnez **Administrateur de comptes temporaires**.
2. Sélectionnez un utilisateur existant. Cet utilisateur est obligatoirement issu de l'annuaire LDAP interne du firewall.
3. Validez la création en cliquant sur le bouton **Appliquer**.

Créer une règle dans la politique d'authentification

1. Dans l'onglet *Politique d'authentification* du module **Configuration** > **Utilisateurs** > **Authentification**, déroulez le menu **Nouvelle règle** et cliquez sur **Règle Comptes temporaires**.
2. Dans le menu **Source**, cliquez sur **Ajouter une interface** et sélectionnez l'interface réseau par laquelle peuvent se présenter les comptes invités.
3. Cliquez sur **Ajouter un objet** pour sélectionner (ou créer puis sélectionner) le réseau ou les machines depuis lesquels les invités vont se connecter.
4. Validez en cliquant sur **Terminer**
5. Double cliquez sur l'état de cette règle afin de l'activer.
6. Cliquez sur le bouton **Appliquer**.

Personnaliser un profil de portail captif pour cette méthode

Dans l'onglet *Profils du portail captif* du module **Configuration** > **Utilisateurs** > **Authentification**, sélectionnez le profil *"Voucher"*. Ce profil implémente automatiquement les paramètres nécessaires au fonctionnement de cette méthode :

Authentification

- **Méthode ou annuaire par défaut :** *"Comptes temporaires(voucher_users.local.domain)"*.

Durées d'authentification autorisées

- **Durée minimale** : elle peut être réglée de 1 minute à 24 heures (valeur proposée par défaut : 15 minutes).
- **Durée maximale** : elle peut être réglée de 1 minute à 24 heures (valeur proposée par défaut : 4 heures).

Configuration avancée

- **Activer le portail captif**.
- **Expiration du 'cookie' HTTP** : *"A la fin de la période d'authentification"*.

Paramètres complémentaires :

Conditions d'utilisation de l'accès à Internet

Vous pouvez cocher la case **Activer l'affichage des conditions d'utilisation d'accès à Internet** si vous souhaitez que ces conditions d'accès soient affichées lors de la connexion d'un utilisateur. Elles seront également affichées à intervalle régulier (valeur proposée par défaut : 18 heures).

NOTE
Le texte des conditions d'accès est personnalisable dans l'onglet *Portail captif*.

En cas de modification de l'un de ces paramètres (exemple : durées d'authentification), cliquez sur **Appliquer** pour enregistrer la configuration.

Associer le profil du portail captif et les interfaces réseau concernées

Sélectionnez l'onglet *Portail captif* du module **Configuration** > **Utilisateurs** > **Authentification**. La grille **Correspondance entre profil d'authentification et interface** est vide. Cliquez sur le bouton **Ajouter** pour sélectionner l'interface souhaitée et affectez-lui le profil *Voucher*. La méthode et l'annuaire associés à ce profil sont automatiquement renseignés dans la colonne *Méthode ou annuaire par défaut*.

Adapter la politique de filtrage pour les comptes temporaires

La politique de filtrage décrite ci-dessous permet aux utilisateurs bénéficiant de comptes temporaires d'accéder aux sites Internet en HTTP et HTTPS avec du filtrage d'URL.

Créer une règle d'inspection SSL

L'assistant permet de créer deux règles : l'une destinée à déchiffrer les flux HTTPS, l'autre pour les diriger vers le proxy SSL afin de les soumettre au filtrage d'URL et aux traitements de prévention d'intrusion.

1. Dans l'onglet *Filtrage* du module **Configuration** > **Politique de sécurité** > **Filtrage et NAT**, cliquez sur le bouton **Nouvelle règle** et sélectionnez **Règle d'inspection SSL.**

2. Renseignez les réseaux ou machines sources (colonne **Depuis** - *temporary_accounts_network* dans l'exemple), la destination (colonne **Vers** - *Internet* dans l'exemple) et le port destination (HTTPS dans l'exemple). Validez en cliquant sur **Terminer**.
3. Faites un double-clic sur la source de la règle de redirection vers le proxy SSL. Dans le champ **Utilisateur**, sélectionnez Any user@voucher_users.local.domain.
4. Dans l'onglet *Configuration avancée*, sélectionnez *Comptes temporaires* comme **Méthode d'authentification**.
5. Dans la section **Port / Protocole**, sélectionnez la valeur *Protocole applicatif* pour le champ **Type de protocole**, puis *HTTP* pour le **Protocole applicatif**.
6. Dans la section **Inspection**, sélectionnez le profil de filtrage d'URL à appliquer (*URLFilter_00* dans l'exemple).
7. Validez en cliquant sur **OK**.

Créer une règle de redirection vers le portail captif

1. Dans l'onglet *Filtrage* du module **Configuration** > **Politique de sécurité** > **Filtrage et NAT**, cliquez sur le bouton **Nouvelle règle** et sélectionnez **Règle d'authentification**.
2. Dans l'assistant de création, renseignez les réseaux ou machines sources (champ **Depuis** - *temporary_accounts_network* dans l'exemple) et la destination (champ **Vers** - *Internet* dans l'exemple) pour lesquels les utilisateurs non authentifiés seront redirigés vers le portail captif.
3. Validez en cliquant sur le bouton **Terminer**. Cette règle sélectionne le port HTTP comme port destination par défaut.
4. Pour y ajouter le port HTTPS, double-cliquez sur le champ **Port dest.** de cette règle. Dans le champ **Port destination** de la fenêtre d'édition de la règle, ajoutez le port HTTPS. Validez en cliquant sur **OK**.
5. A l'aides des flèches **Monter** et **Descendre**, placez cette règle entre la règle de déchiffrement SSL et la règle de redirection vers le proxy SSL.

Ajouter la règles de filtrage des flux HTTP pour les comptes temporaires

1. Dans l'onglet *Filtrage* du module **Configuration** > **Politique de sécurité** > **Filtrage et NAT**, cliquez sur le bouton **Nouvelle règle** et sélectionnez **Règle simple**.
2. Dans la colonne Status, double-cliquez sur *Off* pour activer la règle (l'état de la règle passe à *On*).
3. Dans la colonne **Action**, double-cliquez sur *bloquer* puis choisissez la valeur *passer* pour le champ **Action**. Sélectionnez le niveau de traces souhaité pour les connexions correspondant à cette règle; *tracer (journal de filtrage)* permet de visualiser les événements liés aux connexions des comptes temporaires dans les journaux de connexion par exemple.
4. Dans la section **Source** située sur la gauche de la fenêtre d'édition de la règle, affectez les valeurs suivantes aux différents champs :

Onglet général

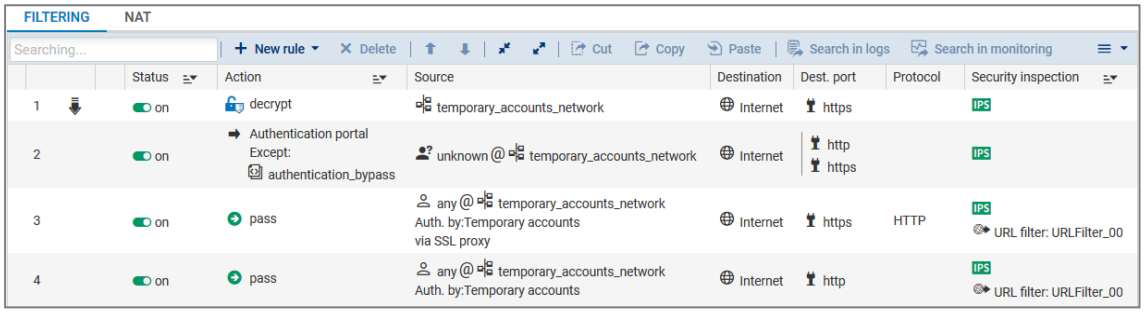
- **Utilisateur** : sélectionnez *Any user@voucher_users.local.domain.*
- **Machines sources** : sélectionnez le réseau des comptes temporaires.

Onglet configuration avancée

- **Méthode d'authentification** : sélectionnez la méthode *Comptes temporaires*.

5. Dans la section **Destination**, sélectionnez l'objet *Internet* pour le champ **Machines destinations.**
6. Dans la section **Port / Protocole**, sélectionnez l'objet HTTP pour le champ **Port destination**.
7. Dans la section **Inspection**, laissez le mode IPS proposé par défaut et sélectionnez le profil de filtrage d'URL à appliquer (*URLFilter_00* dans l'exemple). Ce profil pourra être personnalisé dans le menu **Politique de sécurité** > **Filtrage URL**.

La politique de filtrage concernant les comptes temporaires prend ainsi la forme suivante :



Consulter les journaux de traces

Depuis l'interface d'administration Web du Firewall, accédez aux journaux de traces (**Utilisateurs**, **Trafic réseau**, **Filtrage**) et aux rapports afin de vérifier le fonctionnement de la configuration mise en place.

Configurer la méthode "Parrainage"

Ce mode permet, par exemple, d'offrir un accès partagé à Internet aux visiteurs prestataires de l'entreprise. Lors de sa première connexion à Internet, l'utilisateur est redirigé vers le portail captif sur lequel il effectue sa demande de parrainage en renseignant ses noms et prénoms ainsi que l'adresse e-mail d'un correspondant interne. Ce correspondant, s'il est habilité et explicitement déclaré dans le firewall comme étant autorisé à parrainer des utilisateurs, valide la demande, autorisant ainsi immédiatement l'accès aux ressources Web pour le demandeur.

Les conditions d'utilisation de l'accès à Internet lui sont alors présentées, et il doit les valider pour accéder au site Web demandé. Il peut ensuite accéder, selon la politique de filtrage d'URL mise en place, aux ressources Web. L'affichage des conditions d'accès à Internet intervient de manière régulière; cette fréquence est paramétrable. La durée de connexion d'un utilisateur invité est de 4 heures. Au delà de cette durée, le panneau des conditions d'accès à Internet sera automatiquement affiché.

Configurer l'envoi d'e-mails de parrainage

Définir le serveur de messagerie

1. Dans l'onglet *Configuration* du module **Configuration** > **Notifications** > **Alertes e-mails**, cochez la case **Activer les notifications par e-mail**.
2. Champ **Serveur** : sélectionnez ou créez l'objet réseau de type machine correspondant au serveur de messagerie.
3. Champ **Port** : sélectionnez le port d'écoute du serveur de messagerie (généralement SMTP ou SMTPS).
4. Si la connexion au serveur de messagerie requiert une authentification, remplissez les champs **Identifiant** et **Mot de passe**.
5. Champ **Domaine DNS** : saisissez le nom du domaine de messagerie. Il sera accolé au nom du firewall afin de former une adresse e-mail d'expéditeur valide.
6. Validez en cliquant sur le bouton **Appliquer**.

Personnaliser l'e-mail de parrainage (facultatif)

1. Dans l'onglet *Modèles* du module **Configuration** > **Notifications** > **Alertes e-mails**, sélectionnez l'e-mail **Demande de Parrainage** (section **Parrainage**).
2. Cliquez sur le bouton **Modifier** si vous souhaitez personnaliser l'e-mail envoyé lors d'une requête de parrainage puis sauvegardez vos modifications.

Activer la méthode "Parrainage"

1. Dans l'onglet *Méthodes disponibles* du module **Configuration** > **Utilisateurs** > **Authentification**, déroulez le menu **Ajouter une méthode** et cliquez sur **Parrainage**.
2. Dans le panneau de droite, réglez les durées minimale et maximale d'authentification. Les valeurs respectives proposées par défaut sont de 15 minutes et 4 heures.

Autoriser un utilisateur à valider les demandes de parrainage

Définissez un utilisateur ou un groupe d'utilisateurs autorisés à valider les demandes de parrainage reçues par mail.

1. Sélectionnez l'onglet *Accès détaillé* du module **Configuration** > **Utilisateurs** > **Droits d'accès**.
2. Cliquez sur le bouton **Ajouter** afin d'ajouter une nouvelle ligne à la grille de droits (aucun droit n'est attribué).
3. Cliquez sur le champ **Utilisateur - groupe d'utilisateurs** et sélectionnez un utilisateur ou un groupe existant. Cet utilisateur ou ce groupe sont obligatoirement issus de l'annuaire LDAP interne du firewall.
4. Cliquez sur le champ **Parrainage** et choisissez la valeur *Autoriser*.
5. Faites un double clic sur la colonne **Etat** afin d'activer cette règle de droits.
6. Validez la création en cliquant sur le bouton **Appliquer**.

Créer une règle dans la politique d'authentification

1. Dans l'onglet *Politique d'authentification* du module **Configuration** > **Utilisateurs** > **Authentification**, déroulez le menu **Nouvelle règle** et cliquez sur **Règle Parrainage**.
2. Cliquez sur **Ajouter une interface** pour sélectionner l'interface réseau par laquelle peuvent se présenter les requêtes de parrainage.
3. Cliquez sur **Ajouter un objet** pour sélectionner (ou créer puis sélectionner) le réseau ou les machines depuis lesquels les invités vont se connecter.
4. Validez en cliquant sur **Terminer**.
5. Double cliquez sur l'état de cette règle afin de l'activer.
6. Cliquez sur le bouton **Appliquer**.

Personnaliser un profil de portail captif pour cette méthode

Dans l'onglet *Profils du portail captif* du module **Configuration** > **Utilisateurs** > **Authentification**, sélectionnez le profil *"Sponsor"*. Ce profil implémente directement les paramètres suivants :

Authentification

- **Méthode ou annuaire par défaut :** *"Parrainage (sponsored_users.local.domain)"*.

Durées d'authentification autorisées

- **Durée minimale** : elle peut être réglée de 1 minute à 24 heures (valeur proposée par défaut : 15 minutes).
- **Durée maximale** : elle peut être réglée de 1 minute à 24 heures (valeur proposée par défaut : 4 heures).

Configuration avancée

- **Activer le portail captif**.
- **Expiration du 'cookie' HTTP:** "**None**".

> **IMPORTANT**
>
> Le paramètre d'expiration du cookie ne doit surtout pas être modifié pour la méthode Parrainage.

D'autre part, le fait de ne pas utiliser de cookie interdit l'utilisation d'objets multi-utilisateurs (serveurs TSE par exemple) comme machines sources pour cette méthode.

Paramètres complémentaires :

Conditions d'utilisation de l'accès à Internet

Vous pouvez cocher la case **Activer l'affichage des conditions d'utilisation d'accès à Internet** si vous souhaitez que ces conditions d'accès soient affichées lors de la connexion d'un utilisateur. Elles seront également affichées à intervalle régulier (valeur proposée par défaut : 18 heures).

NOTE
Le texte des conditions d'accès est personnalisable dans l'onglet *Portail captif*.

En cas de modification de l'un de ces paramètres (exemple : durées d'authentification), cliquez sur **Appliquer** pour enregistrer la configuration.

Associer le profil du portail captif et les interfaces réseau concernées

Sélectionnez l'onglet *Portail captif* du module **Configuration** > **Utilisateurs** > **Authentification.** La grille **Correspondance entre profil d'authentification et interface** est vide. Cliquez sur le bouton **Ajouter** pour sélectionner l'interface souhaitée et affectez-lui le profil *Sponsor*. La méthode et l'annuaire associés à ce profil sont automatiquement renseignés dans la colonne *Méthode ou annuaire par défaut*.

Adapter la politique de filtrage pour les comptes temporaires

La politique de filtrage décrite ci-dessous permet aux utilisateurs parrainés d'accéder aux sites Internet en HTTP et HTTPS avec du filtrage d'URL.

Créer une règle d'inspection SSL

L'assistant permet de créer deux règles : l'une destinée à déchiffrer les flux HTTPS, l'autre pour les rediriger vers le proxy SSL afin de les soumettre au filtrage d'URL et aux traitements de prévention d'intrusion.

1. Dans l'onglet *Filtrage* du module **Configuration** > **Politique de sécurité** > **Filtrage et NAT**, cliquez sur le bouton **Nouvelle règle** et sélectionnez **Règle d'inspection SSL.**
2. Renseignez les réseaux ou machines sources (colonne **Depuis** - *sponsorship_network* dans l'exemple), la destination (colonne **Vers** - *Internet* dans l'exemple) et le port destination (HTTPS dans l'exemple). Validez en cliquant sur **Terminer**.
3. Faites un double-clic sur la source de la règle de redirection vers le proxy SSL. Dans le champ **Utilisateur**, sélectionnez Any user@sponsored_users.local.domain.
4. Dans l'onglet *Configuration avancée*, sélectionnez *Parrainage* comme **Méthode d'authentification**.
5. Dans la section **Port / Protocole**, sélectionnez la valeur *Protocole applicatif* pour le champ **Type de protocole**, puis *HTTP* pour le **Protocole applicatif**.
6. Dans la section **Inspection**, sélectionnez le profil de filtrage d'URL à appliquer (*URLFilter_00* dans l'exemple).
7. Validez en cliquant sur **OK**.

Créer une règle de redirection vers le portail captif

1. Dans l'onglet *Filtrage* du module **Configuration** > **Politique de sécurité** > **Filtrage et NAT**, cliquez sur le bouton **Nouvelle règle** et sélectionnez **Règle d'authentification**.
2. Dans l'assistant de création, renseignez les réseaux ou machines sources (champ **Depuis** - *sponsorship_network* dans l'exemple) et la destination (champ **Vers** - *Internet* dans l'exemple) pour lesquels les utilisateurs non authentifiés seront redirigés vers le portail captif.
3. Validez en cliquant sur le bouton **Terminer**. Cette règle sélectionne le port HTTP comme port destination par défaut.
4. Pour y ajouter le port HTTPS, double-cliquez sur le champ **Port dest**. de cette règle. Dans le champ **Port destination** de la fenêtre d'édition de la règle, ajoutez le port HTTPS. Validez en cliquant sur **OK**.
5. A l'aides des flèches **Monter** et **Descendre**, placez cette règle entre la règle de déchiffrement SSL et la règle de redirection vers le proxy SSL.

Ajouter la règles de filtrage des flux HTTP pour les utilisateurs parrainés

1. Dans l'onglet *Filtrage* du module **Configuration** > **Politique de sécurité** > **Filtrage et NAT**, cliquez sur le bouton **Nouvelle règle** et sélectionnez **Règle simple**.
2. Dans la colonne Status, double-cliquez sur *Off* pour activer la règle (l'état de la règle passe à *On*).
3. Dans la colonne **Action**, double-cliquez sur *bloquer* puis choisissez la valeur *passer* pour le champ **Action**. Sélectionnez le niveau de traces souhaité pour les connexions correspondant à cette règle; *tracer (journal de filtrage)* permet de visualiser les événements liés aux connexions des utilisateurs parrainés dans les journaux de connexion par exemple.
4. Dans la section **Source** située sur la gauche de la fenêtre d'édition de la règle, affectez les valeurs suivantes aux différents champs :

Onglet général

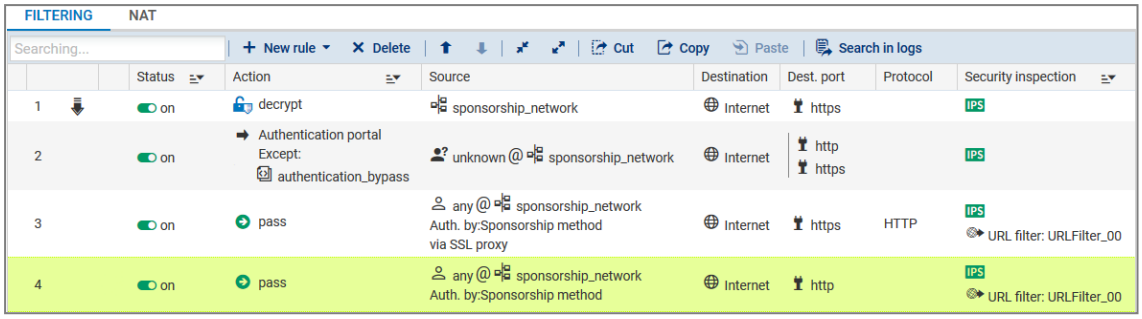
- **Utilisateur** : sélectionnez *Any user@sponsored_users.local.domain.*
- **Machines sources** : sélectionnez le réseau des comptes parrainés.

Onglet configuration avancée

- **Méthode d'authentification** : sélectionnez la méthode *Comptes temporaires*.

5. Dans la section **Destination**, sélectionnez l'objet *Internet* pour le champ **Machines destinations.**
6. Dans la section **Port / Protocole**, sélectionnez l'objet HTTP pour le champ **Port destination**.
7. Dans la section **Inspection**, laissez le mode IPS proposé par défaut et sélectionnez le profil de filtrage d'URL à appliquer (*URLFilter_00* dans l'exemple). Ce profil pourra être personnalisé dans le menu **Politique de sécurité** > **Filtrage URL**..

La politique de filtrage concernant les utilisateurs parrainés prend ainsi la forme suivante :



Consulter les journaux de traces

Depuis l'interface d'administration Web du Firewall, accédez aux journaux de traces (**Utilisateurs**, **Trafic réseau**, **Filtrage**) et aux rapports afin de vérifier le fonctionnement de la configuration mise en place.

documentation@stormshield.eu