NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

# SIGNATURES DE PROTECTION CONTEXTUELLE PERSONNALISÉES

**Produit concerné :** SNS 3 et versions supérieures

**Version du document :** 1.0

**Référence :** sns-fr-signatures_protection_personnalisées_note_technique

# Table des matières

# Avant de commencer

Les signatures de protection contextuelle personnalisées sont destinées à l'analyse par le firewall d'applications développées au sein de l'entreprise ou en complément des signatures développées par Stormshield.

Elles sont basées sur des expressions régulières (appelées "variantes") permettant de retrouver des chaînes de caractères dans les données des paquets réseaux échangés. Les alarmes associées peuvent alors bloquer ou laisser passer le flux détecté, selon le paramétrage réalisé au sein de la signature personnalisée (ce paramétrage peut par la suite être modifié sur chaque firewall au sein du module **Protection applicative** > **Applications et protections**).

L'exemple présenté dans cette note technique consiste à détecter la chaîne "perdu.org" dans une requête TCP ou UDP et à déployer automatiquement cette signature sur un parc de firewalls. Il met en œuvre quatre catégories d'équipements : un poste de développement, un firewall de recette des signatures de protection contextuelle personnalisées, un serveur Active Update pour la distribution automatisée des signatures, et des firewalls clients.

Bien que l'écriture du fichier de définition des signatures personnalisées puisse être réalisé directement sur le firewall de recette, l'un des avantages du poste de développement consiste en la disponibilité de nombreux outils de validation d'expressions régulières, en ligne, ou à installer localement.

Dans la suite de ce document, les signatures de protection contextuelle personnalisées seront appelées signatures personnalisées.

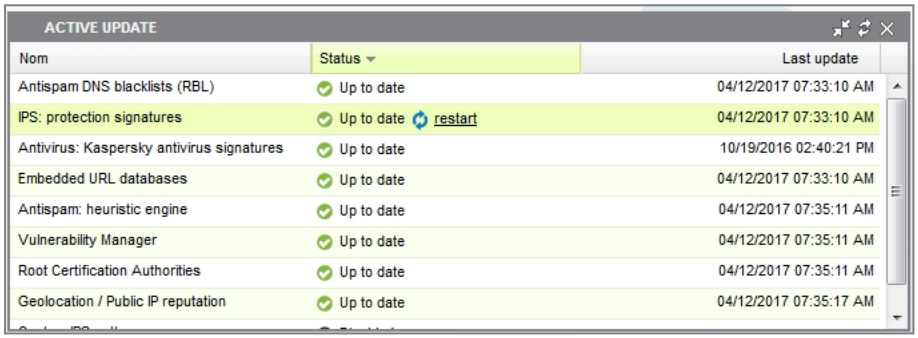
Notez bien que les signatures personnalisées peuvent révéler des informations habituellement masquées dans les journaux de traces du firewall.

# Prérequis

## Sur le firewall de recette uniquement

### Vérifier que les signatures Stormshield sont présentes et à jour

Dans l'interface Web administration du firewall de recette, vérifiez à l'aide du **Tableau de bord** (composant **Active Update**) que les signatures de protection contextuelle Stormshield ont bien été téléchargées :




Dans le cas contraire, lancez manuellement leur téléchargement en cliquant sur le menu contextuel **Redémarrer**.

### Vérifier que les signatures personnalisées sont exclues du mécanisme Auto Update

Dans le module **Système** > **Active Update** > **Mises à jour automatiques**, vérifiez que la ligne "IPS : signatures de protection contextuelles personnalisées" est désactivée afin d'éviter que les signatures personnalisées en cours de modifications ne soient écrasées par celles récupérées depuis le serveur Active Update.

## Sur le firewall de recette et sur les firewalls clients

### Activer l'utilisation de signatures personnalisées

Dans le menu **Système** > **Console CLI** , saisissez les deux commandes suivantes :

```
CONFIG SECURITYINSPECTION COMMON INIT CustomPatternsMatching=1
CONFIG SECURITYINSPECTION ACTIVATE
```

## Sur les firewalls clients

### Définir le serveur Active Update

1. Dans le menu **Système** > **Active Update**, dépliez le panneau **Configuration avancée**.
2. Dans le tableau **Serveurs de mise à jour des signatures de protection contextuelles personnalisées**, cliquez sur le bouton **Ajouter** et saisissez l'URL de votre serveur (exemple : http://my_active_update_server/ActiveUpdate/). Vous pouvez indiquer jusqu'à 8 sites de mise

à jour des signatures personnalisées.

3. Appliquez la modification.

Pour plus de détails concernant l'installation d'un serveur personnalisé Active Update, veuillez vous référer à la base de connaissances du support utilisateur Stormshield. Notez qu'une authentification est nécessaire pour accéder à ce document.

### Activer la récupération des signatures personnalisées via Active Update

Dans le module **Système** > **Active Update** > **Mises à jour automatiques**, faites un double clic sur l'état de la ligne "IPS : signatures de protection contextuelles personnalisées puis validez.

# Structure d'un fichier de signatures personnalisées

Une signature personnalisée est caractérisée par :

- Un contexte (exemple: tcpudp:hostname, smtp:client, dcerpc:request:data ...),
- Un identifiant unique pour un contexte donné.

## Remarques et contraintes

- Une signature personnalisée est exclusivement de type *asq* (cf. la section Contenu d'un fichier de signatures contextuelles). C'est une signature simple, destinée à déclencher une stratégie de sécurité et à lever une alarme associée,
- Les contextes *probe*, *mix* et ceux commençant par *http:javascript* ne sont pas autorisés. La commande `enpattern -l | grep -Ev "(mix|probe)"` permet de lister les contextes utilisables,
- L'identifiant de signature est obligatoirement supérieur à 4096,
- Un contexte donné accepte un maximum de 2048 signatures,
- Une signature ne peut pas contenir plus de 256 expressions régulières (*variantes*),
- L'ensemble des contextes regroupant des définitions de signatures personnalisées est regroupé dans un fichier unique (nommé *CustomPatterns.in* dans l'exemple).

**IMPORTANT**

Une signature contextuelle peut être très consommatrice de ressources processeur et mémoire, notamment lorsque les expressions régulières qu'elle contient n'imposent pas une limite en nombre de caractères pour une recherche donnée.

## Contenu d'un fichier de signatures contextuelles

La structure minimale du fichier de définition de signatures contextuelles personnalisées est la suivante :

- Une section "[contexte.global]", unique pour chaque contexte, dans laquelle la révision des signatures est précisée :

| Nom du champ | Description | Valeurs possibles (signification) |
|---|---|---|
| **Revision=** | Numéro de révision des signatures. | Valeur entière.<br><br>**Exemple**<br>1,2, ... |

- Pour chaque signature contextuelle personnalisée, une section "[contexte.identifiant]" reprenant les champs obligatoires suivants (l'ordre des champs dans la section est libre) :

| Nom du champ | Description | Valeurs possibles (signification) |
|---|---|---|
| **type=** | Précise le champ d'application de la signature | asq |
| **classification=** | Catégorisation de la signature.<br><br>Dans l'Interface Web d'Administration (module **Applications et protections** > **Vue par profil d'inspection**), ce champ permet :<br>• d'associer l'icône adéquate,<br>• de filtrer les signatures en fonction de cette valeur à l'aide des boutons disponibles. | 0 (Protections)<br>1 (Applications)<br>2 (Malware) |
| **action_fw=** | Action appliquée par l'alarme associée à la signature personnalisée.<br><br>Ce champ est composé de 4 valeurs, séparées par une virgule, sans espace, correspondant aux 4 modèles prédéfinis de sécurité : Internet, Basse, Moyenne et Haute. | pass<br>block<br><br>**Exemple**<br>pass,pass,pass,pass<br>pass,pass,block,block |
| **level_fw=** | Niveau affecté à l'alarme associée.<br><br>Ce champ est composé de 4 valeurs, séparées par une virgule, sans espace, correspondant aux 4 modèles prédéfinis de sécurité : Internet, Basse, Moyenne et Haute. | ignore<br>minor<br>major<br><br>**Exemple**<br>ignore,minor,major,major<br>major,major,major,major |
| **description=** | Description courte de la signature rédigée en anglais. Ce texte est affiché dans la colonne **Message** du module **Applications et protection**. | Texte libre encadré par des guillemets.<br><br>**Exemple**<br>"Access to perdu.org site" |
| **ldescr=** | Complément d'information sur la signature, rédigé en anglais. Ce texte est affiché dans une infobulle, lors du survol du descriptif de l'alarme (colonne **Message** du module **Applications et protection**). | Texte libre encadré par des guillemets.<br><br>**Exemple**<br>"This custom signature is able to detect when a computer tries to connect to the website perdu.org" |
| **1=** | Première expression régulière utilisée dans la signature | Expression régulière encadrée par des guillemets |

Cette section peut également contenir les champs optionnels suivants :

| Nom du champ | Description | Valeurs possibles (signification) |
|---|---|---|

| | | |
|---|---|---|
| **severity=** | Niveau de sévérité affecté à la menace détectée par la signature personnalisée. | 0 (Information)<br>1 (Faible)<br>2 (Modéré)<br>3 (Elevé)<br>4 (Critique) |
| **resource=** | Ce champ permet d'attribuer à la signature l'icône de l'application concernée. Cette icône est placée à droite de l'icône de classification. | Texte libre<br><br>**Exemple**<br>Facebook<br>Googleplus<br>Twitter |
| **description_fr=** | Description courte de la signature rédigée en français. Ce texte est affiché dans la colonne **Message** du module **Applications et protection**. | Texte libre encadré par des guillemets.<br><br>**Exemple**<br>"Accès au site perdu.org" |
| **ldescr_fr** | Complément d'information sur la signature, rédigé en français. Ce texte est affiché dans une infobulle, lors du survol du descriptif de l'alarme (colonne **Message** du module **Applications et protection**). | Texte libre encadré par des guillemets.<br><br>**Exemple**<br>"Cette signature personnalisée est capable de détecter lorsqu'un poste tente d'accéder au site perdu.org" |
| **reference=** | Pour les signatures personnalisées, ce champ est indicatif. Il complète éventuellement la description de la signature dans le fichier *CustomPatterns.in*. | url,http://www.xxx.yz<br><br>**Exemple**<br>url,http://documentation.stormshield.eu |
| **2=**<br>**3=**<br>**4=**<br>**....** | Expressions régulières additionnelles (*variantes*). Lorsque plusieurs variantes sont définies, leurs numéros d'identifiants sont obligatoirement consécutifs.<br>**Exemple de liste invalide de variantes** :<br>1="blue"<br>3="red"<br>4="green"<br>6="yellow" | Expression régulière encadrée par des guillemets |
| **Fromasqversion=** | Version minimale de firmware SNS prenant en charge la signature. | Numéro de version.<br><br>**Exemple**<br>1.0.0 |
| **Uptoasqversion=** | Version maximale de firmware SNS prenant en charge la signature. | Numéro de version.<br><br>**Exemple**<br>8.0.0 |

# Définir des signatures personnalisées

## Définir une signature utilisant uniquement les champs obligatoires

L'objet de cet exemple de signature étant de détecter la connexion au site Web http://*perdu.org* dans une requête TCP ou UDP, le contexte choisi sera `tcpudp:hostname`. La valeur choisie pour l'identifiant de signature est 4101.

Sur le poste de développement :

1. Créez un fichier *CustomPatterns.in*,
2. Éditez ce fichier et insérez la section "[tcpudp:hostname.global]" contenant la révision de la signature, suivie de la section " [tcpudp:hostname.4101]" incluant les paramètres obligatoires :

```
[tcpudp:hostname.global]
Revision=1
[tcpudp:hostname.4101]
type=asq
classification=1
action_fw=pass,pass,block,block
level_fw=minor,minor,major,major
description="Access to perdu.org site"
ldescr="This custom signature is able to detect when a computer tries to connect
to the website perdu.org"
1="^(.+\.)?(?i)perdu\.org(?-i)$"
```

3. Insérez autant de sections "[contexte.identifiant]" que vous souhaitez définir de signatures personnalisés dans le contexte considéré (dans la limite des 2048 signatures possibles par contexte).

## Signification des différents champs de cet exemple

Champ **Revision**

Le numéro de révision des signatures personnalisées du contexte *tcpudp:hostname* est 1 .

Champ **type**

La signature est obligatoirement du type *asq* : elle est destinée à déclencher une stratégie de sécurité et à lever une alarme.

Champ **classification**

La signature appartient à la catégorie *Applications*.

Champ **action_fw**

Lorsqu'une connexion au site perdu.org est détectée, l'action associée à l'alarme déclenchée est :

- *Passer* pour les modèles prédéfinis de sécurité "Internet" et "Basse",
- *Bloquer* pour les modèles prédéfinis de sécurité "Moyenne" et "Haute".

Champ **level_fw**

Cette alarme a un niveau :

- *Mineur* pour les modèles prédéfinis de sécurité "Internet" et "Basse",
- *Majeur* pour les modèles prédéfinis de sécurité "Moyenne" et "Haute".

Champ **description**

Le message associé à la signature et apparaissant dans l'interface Web d'Administration est "Accès to perdu.org site".

Champ **ldescr**

L'info-bulle affichée en survolant le message indique : "This custom signature is able to detect when a computer tries to connect to the website perdu.org".

Champ **1**

L'expression régulière utilisée pour détecter une connexion à perdu.org est :

```
^(.+\.)?(?i)perdu\.org(?-i)$
```

### Exemple de champs additionnels pouvant être ajoutés à cette définition

```
severity=2
resource=perdu
reference=url,http://perdu.org
description_fr="Accès au site perdu.org"
ldescr_fr="Cette signature personnalisée détecte la tentative de connexion d'une
machine au site Web perdu.org"
Fromasqversion=1.0.0
Uptoasqversion=8.0.0
```

# Mettre en oeuvre les signatures personnalisées sur le firewall de recette

## Transférer le fichier de signatures personnalisées sur le firewall de recette

Copiez via SCP (en ligne de commande où à l'aide d'un utilitaire de type WinSCP) le fichier CustomPatterns.in dans le répertoire /usr/Firewall/ConfigFiles du firewall de recette.

## Vérifier la validité du fichier de définition des signatures personnalisées

Lancez la commande :

```
enpattern -t /usr/Firewall/ConfigFiles/CustomPatterns.in
```

Si le fichier de définition des signatures est invalide, un ou plusieurs messages sont affichés indiquant le type d'erreurs détectées.

## Compiler les signatures personnalisées

Après avoir corrigé les éventuelles anomalies détectées dans le fichier de définition des signatures personnalisées, lancez la commande :

```
enpattern -fav
```

Cette commande lance la compilation de l'ensemble des signatures (options -f et -a). L'option -v active le mode verbeux de la commande.

Le répertoire /usr/Firewall/Data/CustomPatterns/Download contient alors un fichier par contexte, contenant l'ensemble des signatures propres à ce contexte (exemple : *tcpudp_hostname*).

## Activer les signatures personnalisées dans le moteur de prévention d'intrusion

Sur le firewall de recette, lancez la commande :

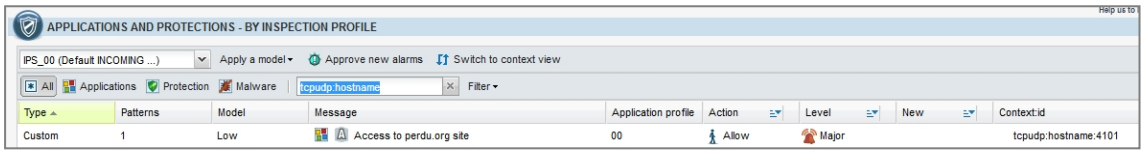
```
enasq
```

Cette commande impose au moteur de prévention d'intrusion de prendre en compte les signatures personnalisées précédemment compilées.

# Tester une signature personnalisée

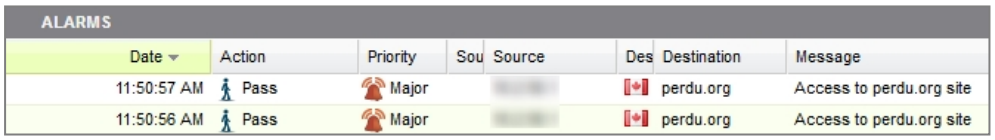
## Vérifier dans l'Interface Web d'Administration la présence de la signature personnalisée

1. Dans le module **Protection Applicative** > **Applications et protections**, affichez la colonne **Type.**
2. Cliquez une fois sur l'intitulé de cette colonne pour afficher les signatures personnalisées en premier :




## Tester la signature personnalisée

1. Depuis un poste traversant le firewall de recette, générez des flux correspondant à la signature personnalisée.
2. Dans le tableau de bord du firewall de recette (composant **Alarmes**), l'alarme levée par cette signature doit être présente :




3. Cette alarme peut également être visualisée dans le module **Journaux d'Audit** > **Journaux** > **Alarmes** :


# Déployer les signatures sur le serveur Active Update

Sur le firewall de validation, générez l'archive contenant l'ensemble des signatures personnalisées à l'aide de la commande :

```
enpattern -favz
```

Cette commande lance la compilation de l'ensemble des signatures (options -f et -a) ainsi que la création de l'archive regroupant ces signatures (option -z) et destinée à être mise à disposition sur le serveur Active Update. L'option -v active le mode verbeux de la commande.

Le répertoire /usr/Firewall/Data/CustomPatterns/Download contient le résultat de cette commande :

- L'archive nommée *custom_patterns_active_update.tgz,*
- Un fichier par contexte, contenant l'ensemble des signatures propres à ce contexte (exemple : *tcpudp_hostname*).

Transférez l'archive custom_patterns_active_update.tgz à la racine du site Web hébergé sur votre serveur Active Update puis décompressez la.

Le contenu de cette archive est le suivant :

- Un fichier CustomPatterns- vX.index comprenant la liste des contextes de signatures personnalisées et de leur numéro de révision,
- Un fichier CustomPatterns-vX.md5 permettant de vérifier l'intégrité du fichier d'index,
- Une arborescence regroupant les signatures personnalisées.

La signature personnalisée est prête à être déployée sur le parc de firewalls clients.

# Télécharger la signature personnalisée sur les firewalls clients

Chaque firewall client reçoit la signature personnalisée :

- Lors d'une synchronisation automatique avec son serveur Active Update (programmée toutes les 3 heures),
- Via le composant **Active Update** du tableau de bord, en cliquant sur le menu **Redémarrer** situé à côté de l'entrée "IPS : signatures de protection contextuelle personnalisées".

La mise à jour des signatures personnalisées sur un firewall est réalisée selon le mécanisme suivant :

1. Le firewall télécharge sur le serveur Active Update le fichier CustomPatterns-vX.md5 du sous-système ActiveUpdate des Signatures personnalisées.
2. Lorsque celui- ci diffère de son fichier .md5 local situé dans le répertoire /usr/Firewall/Data/CustomPatterns/Download/, le firewall télécharge le fichier CustomPatterns-vX.index depuis le serveur afin de comparer les révisions de chacun des contextes :
    - Si le contexte n'existe pas sur le firewall ou si la révision du contexte présent sur le serveur est supérieure à celle de son fichier local, le firewall télécharge le fichier de contexte du serveur. Celui-ci est ensuite compilé puis ajouté aux signatures du firewall.
    - Si le fichier de contexte existe sur le firewall mais qu'il mais il n'est pas ou plus présent sur le serveur Active Update, alors ce fichier de contexte est supprimé du firewall. Les signatures rattachées à ce contexte sont également supprimées du firewall.
    - Si la révision du contexte sur le firewall est égale ou supérieure à celle du fichier présent sur le serveur Active Update, alors le fichier n'est pas modifié et c'est cette version locale du contexte qui est prise en compte sur le firewall.

# Supprimer une signature personnalisée

La suppression d'une signature personnalisée nécessite les étapes suivantes :

## Sur le poste de développement

1. Dans le fichier *CustomPatterns.in* :
   - Supprimez la section définissant la signature,
   - Incrémentez le champ **Révision** du contexte correspondant.
1. Transférez ce fichier sur le firewall de recette.

## Sur le firewall de recette

1. Supprimez le fichier unitaire correspondant à ce contexte dans le répertoire */usr/Firewall/Data/CustomPatterns/Download* (exemple : tcpudp_hostname).
2. Validez le fichier de signatures personnalisées.
3. Lancez la compilation des signatures.
4. Vérifiez dans le module **Protection applicative** > **Applications et protections** que cette signature a bien été supprimée.

## Sur le serveur Active Update

Déployez la nouvelle archive de signatures personnalisées sur votre serveur Active Update.