NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

IDENTIFIER LES COMMANDES DE PROTOCOLES INDUSTRIELS TRAVERSANT LE FIREWALL

Produits concernés : SNS 3 et versions supérieures

Date : 3 Octobre 2018

Référence : sns-fr-identifier_commandes_protocoles_industriels_note_technique

Table des matières

Introduction

Les protocoles industriels ont dans la majorité des cas été conçus dans un objectif fonctionnel, sans prendre en considération la notion de sécurité.

Ils permettent en général à une machine cliente de solliciter l'action d'un automate (PLC - Programmable Logic Controller), attendant en retour l'exécution de cette action. Un poste client peut ainsi demander au PLC l'écriture en mémoire de données, ou tout simplement lui ordonner de s'arrêter.

Cette demande d'action est définie dans un champ particulier du protocole nommé « code fonction ». Les protocoles industriels ne comportant aucun mécanisme de sécurité comme la vérification de l'identité de l'émetteur du message, toute machine présente sur le réseau est donc susceptible de solliciter une action du PLC.

L'objectif de ce document est de présenter une méthode permettant d'identifier les différents codes de fonction d'un protocole échangés sur le réseau industriel de l'entreprise. Suite à cette capture, l'administrateur sera en mesure de construire une politique de sécurité adaptée aux codes de fonction à autoriser ou interdire pour chaque machine présente sur le réseau.

Ainsi une machine suspicieuse située sur le réseau ne pourra pas envoyer de messages au PLC car ceux-ci seront filtrés par le Firewall Stormshield Network.

Prérequis

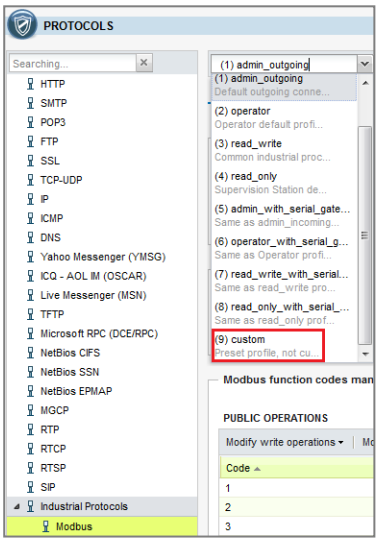
Firewall SNS en version 2.3.4 ou supérieure.

Créer un profil d'inspection personnalisé

Créez un profil d'inspection personnalisé pour le protocole industriel sélectionné (Modbus dans l'exemple). Dans ce profil, tous les codes de fonctions seront configurés pour générer une alarme permettant d'identifier les codes transitant sur le réseau. Ce profil d'inspection sera ensuite utilisé au sein de la politique de filtrage.

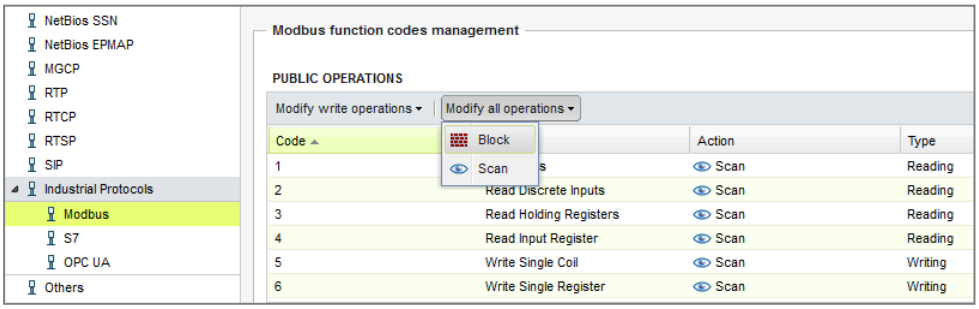
Sélectionner le profil protocolaire de Modbus

1. Dans le menu **Configuration** > **Protection applicative** > **Protocoles**, sélectionnez le protocole Modbus (section *Protocoles industriels*):
2. Choisissez le profil protocolaire **(9) custom** :



Interdire l'ensemble des opérations publiques Modbus

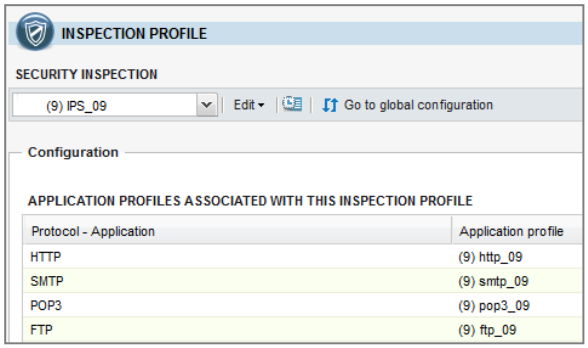
1. Dans la grille listant les opérations Modbus publiques, parcourez le menu **Modifier toutes les opérations**, et sélectionnez **Bloquer**. Cette action aura pour effet de déclencher une alarme à chaque détection d'un code de fonction Modbus :



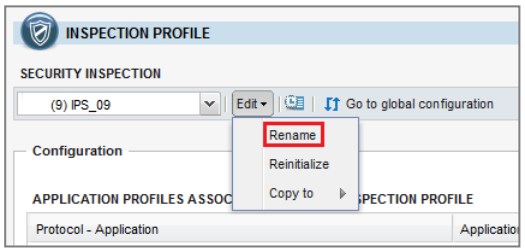
2. Validez en cliquant sur le bouton **Appliquer**.

Personnaliser le profil d'inspection applicative

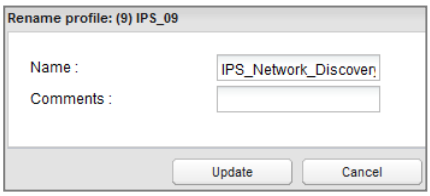
1. Dans le menu **Configuration** > **Protection applicative** > **Profils d'inspection**, cliquez sur **Accéder aux profils**.
2. Sélectionnez le profil **(9) IPS_09** (ce profil d'inspection utilise par défaut les profils protocolaires n°9) :



3. Déroulez le menu **Editer** et sélectionner **Renommer** afin de personnaliser le nom de ce profil d'inspection :

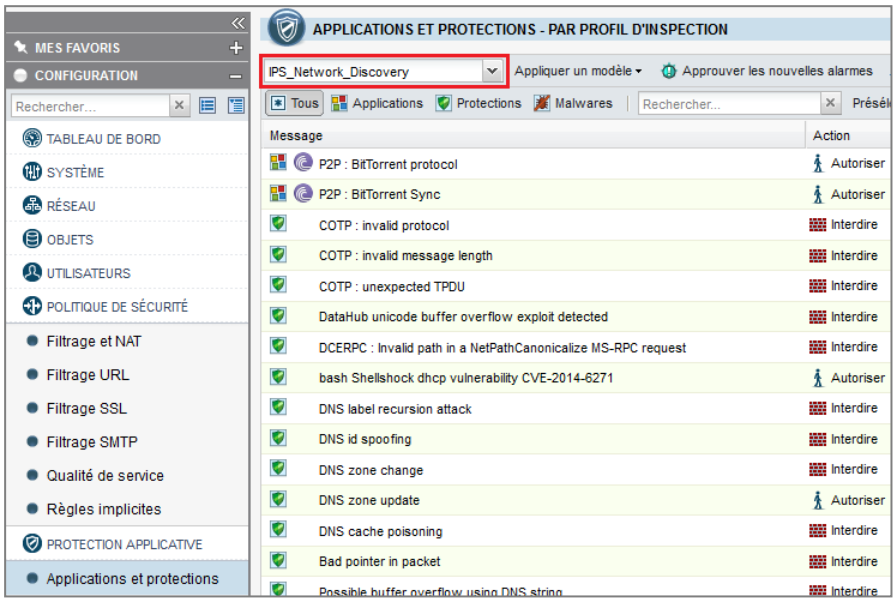


4. Choisissez un nom représentatif (*IPS_Network_Discovery* dans l'exemple) et validez la modification en cliquant sur le bouton **Mettre à jour** :

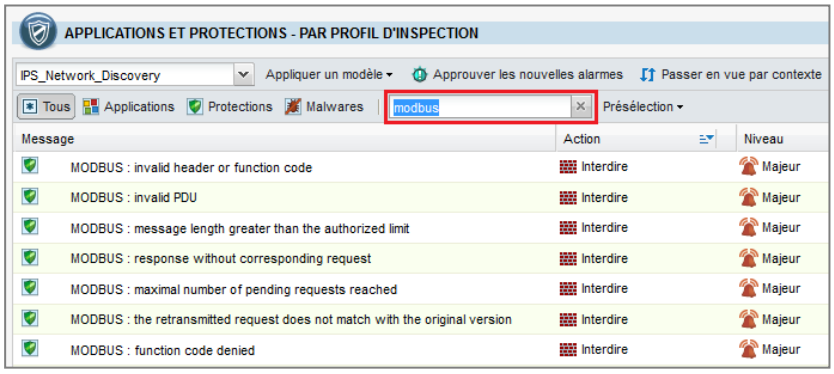


Modifier l'action de l'alarme "Function code denied"

1. Dans le menu **Configuration** > **Protection applicative** > **Applications et protections**, sélectionnez le profil d'inspection personnalisé précédemment créé :



2. Entrez le nom du protocole industriel à filtrer dans le champ de recherche. L'ensemble des alarmes liées à ce protocole s'affiche :



3. Identifiez l'alarme "function code denied" et modifiez son action en double-cliquant sur *Interdire*. Sélectionnez la valeur *Autoriser* :

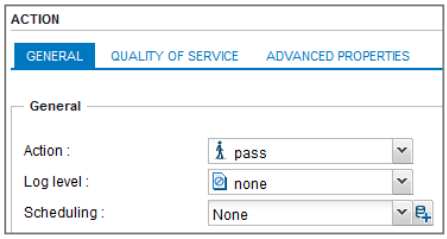
4. Validez la modification en cliquant sur le bouton **Appliquer**.

Créer une règle de filtrage exploitant le profil d'inspection personnalisé

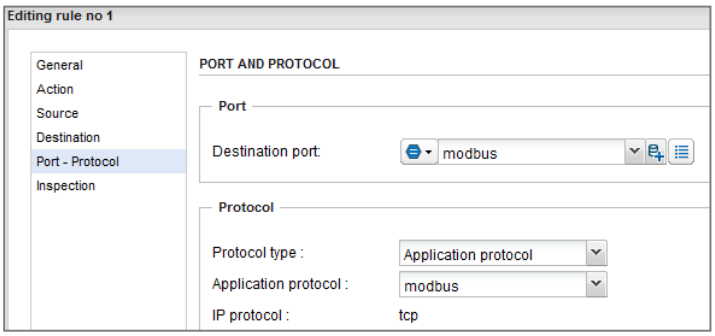
L'objectif de cette règle est de laisser passer tous les codes de fonctions du protocole industriel choisi (Modbus dans ce document) mais en générant systématiquement une alarme afin de les identifier dans les traces du firewall.

NOTE
Cette règle, temporaire, est à placer en première position de la politique de filtrage active.

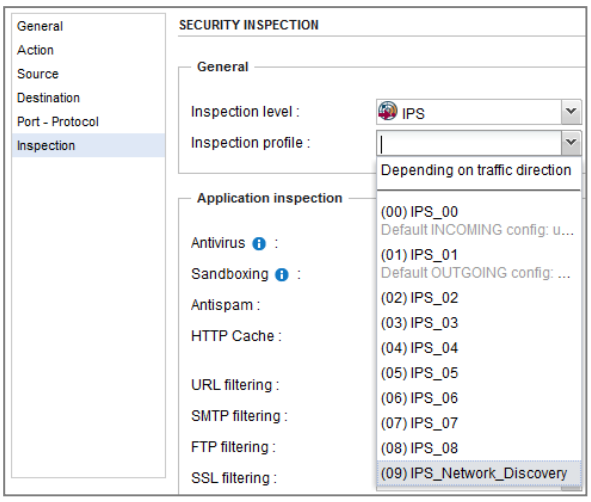
1. Dans le menu **Configuration** > **Politique de Sécurité** > **Filtrage et NAT**, sélectionnez le slot de filtrage actif (slot [9] Filter 09 dans l'exemple), puis cliquez sur le bouton **Nouvelle règle** et sélectionnez **Règle simple.**
2. Dans la colonne Status, double-cliquez sur **Off** pour activer 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** :



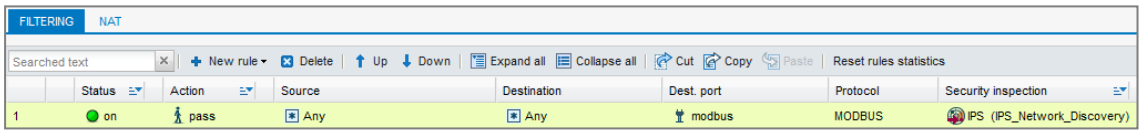
4. Dans la section **Port - Protocole** située sur la gauche de la fenêtre d'édition de la règle, affectez les valeurs suivantes aux différents champs :
   - **Port destination** : modbus,
   - **Type de protocole** : Protocole applicatif,
   - **Protocole applicatif** : modbus.



5. Dans la section **Inspection**, sélectionnez le profil d'inspection précédemment renommé (*(9)IPS_Network_Discovery* dans l'exemple) :



6. Validez les modifications en cliquant sur le bouton **OK**. La règle de filtrage prend donc la forme suivante :

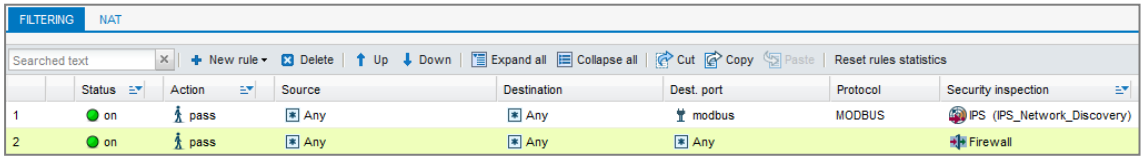


IMPORTANT

Si aucune politique de sécurité n'était active sur le firewall, il est impératif de créer une seconde règle de filtrage assurant de ne bloquer aucun flux en dehors du protocole Modbus. Cette règle sera placée en dernière position du slot de filtrage et prendra les valeurs suivantes :

- **Status** : On,
- **Action** : passer,
- **Source** : Any,
- **Destination** : Any,
- **Port destination** : Any,
- **Protocole** : laissez le champ vide,
- **Inspection de sécurité** : sélectionnez le mode *Firewall*.

La politique de filtrage devient alors :

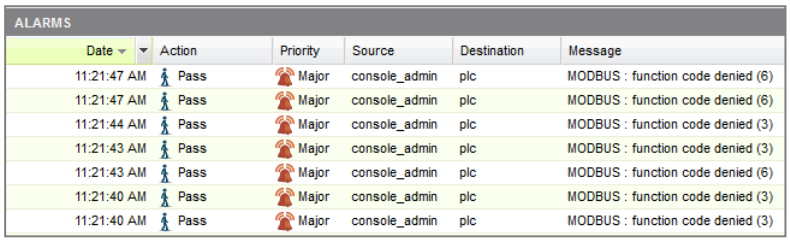


7. Activez la politique de filtrage en cliquant sur le bouton **Sauvegarder et activer**.

Visualiser les alarmes générées

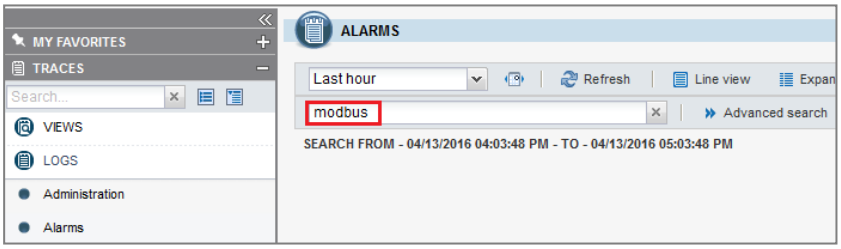
Visualiser les alarmes dans le tableau de bord

Dans le menu **Tableau de bord**, la fenêtre **Alarmes** affiche en temps réel les alarmes levées lorsque des paquets réseaux issus du protocole industriel traversent le firewall :



Visualiser les alarmes dans l'application des journaux et rapports d'activités

Visualisez les alarmes générées par le firewall (menu **Logs - Journaux** > **Alarmes**) en filtrant sur le nom du protocole industriel :



Construire une politique de sécurité personnalisée

Après avoir mis en évidence les codes de fonctions du protocole industriel circulant sur votre réseau, il vous est désormais possible d'implémenter une politique de sécurité adaptée. Les différentes étapes à respecter sont les suivantes:

1. Choisir un profil d'inspection protocolaire prédéfini, ou construire un profil personnalisé pour le protocole industriel considéré.
2. Associer ce profil protocolaire à un profil d'inspection applicative.
3. Modifier l'action associée à l'alerte "*function code denied*" pour la rendre bloquante.
4. Modifier la règle de filtrage dédiée au protocole industriel pour appeler ce profil d'inspection applicative.

Sélectionner le profil d'inspection protocolaire

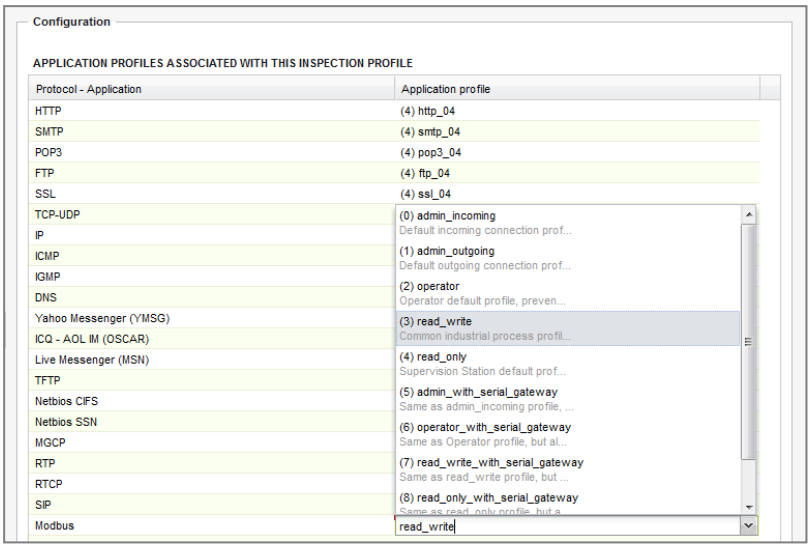
1. Dans le menu **Protection applicative** > **Protocoles** > **Protocoles Industriels**, cliquez sur le protocole industriel à paramétrer (*Modbus* dans l'exemple). Le menu de sélection des profils protocolaires propose 9 profils prédéfinis (numérotés de 0 à 8) et un profil personnalisé (9),
2. En cliquant sur chacun de ces profils, visualisez les opérations publiques interdites ou autorisées et repérez le profil correspondant à la configuration que vous souhaitez mettre en place.
3. Si les profil prédéfinis ne correspondent pas à vos besoins, privilégiez le profil "(9)" utilisé lors de la phase d'analyse. Choisissez l'action *Analyser* pour chacune des opérations publiques à autoriser. Cliquez sur le bouton **Appliquer**.

Utiliser ce profil dans le profil d'inspection applicative

1. Dans le menu **Configuration** > **Protection applicative** > **Profils d'inspection**, cliquez sur **Accéder aux profils**.
2. Pour une configuration plus aisée à lire, sélectionnez le profil IPS portant le même numéro que le profil protocolaire sélectionné. Par exemple, si pour le protocole industriel considéré (Modbus dans l'exemple) vous avez choisi d'appliquer le profil protocolaire intitulé "Read_write" (profil N°3), sélectionnez le profil IPS nommé "(3) IPS_03" qui applique par défaut ce profil protocolaire.

NOTE

Si ce profil n'est pas disponible, sélectionnez un profil IPS non utilisé, puis double-cliquez sur le profil applicatif appliqué par défaut pour le protocole industriel, et sélectionnez le profil à utiliser :



3. Vous pouvez renommer ce profil pour lui donner un nom plus représentatif (menu **Editer** > **Renommer**). **Exemple**: *"IPS_Modbus_Protocol"*.

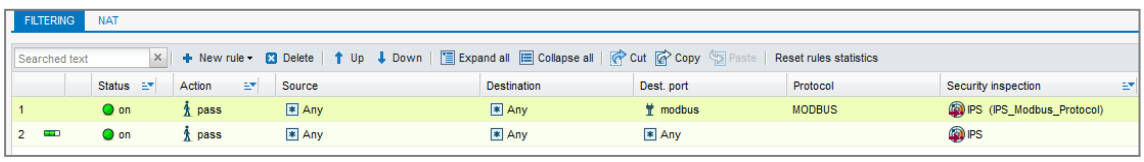
Modifier l'action de l'alarme "Function code denied"

1. Dans le menu **Configuration** > **Protection applicative** > **Applications et protections,** sélectionnez le profil d'inspection personnalisé utilisé dans la règle de filtrage (*IPS_Modbus_Protocol* dans l'exemple.).
2. Entrez le nom du protocole industriel à filtrer dans le champ de recherche. L'ensemble des alarmes liées à ce protocole s'affiche.
3. Identifiez l'alarme "function code denied" et modifiez son action en double-cliquant sur *Autoriser*. Sélectionnez la valeur *Interdire*.
4. Cliquez sur le bouton **Appliquer**.

Modifier la règle de filtrage dédiée au protocole industriel

1. Dans le menu **Configuration** > **Politique de Sécurité** > **Filtrage et NAT**, sélectionnez la règle de filtrage créée pour la découverte des flux industriels transitant sur le réseau.
2. Double-cliquez sur le profil d'inspection (colonne *Inspection de sécurité*) et choisissez le profil sélectionné pour l'analyse du protocole industriel (*IPS_Modbus_Protocol* dans l'exemple).
3. Cliquez sur le bouton **Sauvegarder et activer**.

La règle de filtrage prend donc la forme suivante :



documentation@stormshield.eu