Préprocesseurs SCADA

Les rubriques suivantes expliquent les préprocesseurs pour les protocoles de contrôle de supervision et d'acquisition de données (SCADA) et comment les configurer :

Introduction aux préprocesseurs SCADA

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Les protocoles de supervision, de contrôle et d'acquisition de données (SCADA) surveillent, contrôlent et acquièrent des données des processus industriels, des processus d'infrastructure et d'installation tels que la fabrication, la production, le traitement de l'eau, la distribution d'énergie électrique, les systèmes aéroportuaires et d'expédition, et ainsi de suite. Le système Firepower fournit des préprocesseurs pour les protocoles Modbus, DNP3), CIP (Common Industrial Protocol) et S7Commplus SCADA qui que vous pouvez configurer dans le cadre de votre politique d'analyse de réseau.

Si le, DNP3, CIP ou S7Commplus est désactivé et que vous activez et déployez une règle de prévention des intrusions qui nécessite l'un de ces préprocesseurs, le système utilise automatiquement le préprocesseur requis, avec ses paramètres actuels, bien que le préprocesseur reste désactivé dans l'interface Web pour la politique d'analyse de réseau correspondante.

Exigences de licences pour les préprocesseurs SCADA

Licence de défense contre les menaces

IPS

Licence traditionnelle

Protection

Exigences et conditions préalables pour les préprocesseurs SCADA

Prise en charge des modèles

Tout.

Domaines pris en charge

N'importe quel

Rôles utilisateur

- Admin
- Administrateur d'intrusion

Le préprocesseur Modbus

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le protocole Modbus, qui a été publié pour la première fois en1979 par Modicon, est un protocole de SCADA très utilisé. Le préprocesseur Modbus détecte les anomalies dans le trafic Modbus et décode le protocole Modbus pour le traitement par le moteur de règles, qui utilise des mots-clés Modbus pour accéder à certains champs de protocole.

Une seule option de configuration vous permet de modifier le paramètre par défaut du port que le préprocesseur inspecte pour le trafic Modbus.

Sujets connexes

Mots-clés SCADA

Option de ports pour le préprocesseur Modbus

Ports

Spécifie les ports que le préprocesseur inspecte pour le trafic Modbus. Séparez les valeurs de ports multiples par des virgules.

Configuration du préprocesseur Modbus

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Vous ne devez pas activer ce préprocesseur dans une politique d'analyse de réseau que vous appliquez au trafic si votre réseau ne contient aucun périphérique compatible Modbus.

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si **la configuration Modbus** est désactivée sous **préprocesseurs SCADA**, cliquez sur **Enabled** (Activé).

Étape 6 Cliquez sur **Edit** (✎) à côté de **Configuration Modbus**.

Étape 7 Saisissez une valeur dans le champ **Ports**.

Séparez les valeurs multiples par des virgules

Étape 8 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez utiliser générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, activez les règles de préprocesseur Modbus (GID 144). Pour plus de renseignements, consultez les sections Définition des états des règles d'intrusion et Règles du préprocesseur Modbus, à la page 4.
- Déployer les changements de configuration.

Sujets connexes

Gestion des couches

Conflits et modifications : analyse de réseau et politiques de prévention des intrusions

Règles du préprocesseur Modbus

Vous devez activer les règles de préprocesseur Modbus dans le tableau suivant si vous souhaitez que ces règles générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés.

Tableau 1 : Règles du préprocesseur Modbus

GID de la règle de préprocesseur : SID	Description
144:1	Génère un événement lorsque la longueur indiquée dans l'en-tête Modbus ne correspond pas à la longueur requise par le code de fonction Modbus. Chaque fonction Modbus a un format attendu pour les requêtes et les réponses. Si la longueur du message ne correspond pas au format attendu, cet événement est généré.
144:2	Génère un événement lorsque l'ID de protocole Modbus est différent de zéro. Le champ Protocol ID (ID de protocole) est utilisé pour multiplexer d'autres protocoles avec Modbus. Comme le préprocesseur ne traite pas ces autres protocoles, cet événement est généré à la place.
144:3	Génère un événement lorsque le préprocesseur détecte un code de fonction Modbus réservé.

Le préprocesseur DNP3

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le Distributed Network Protocol (DNP3) est un protocole SCADA qui a été développé à l'origine pour assurer une communication cohérente entre les postes électriques. DNP3 est également devenu très utilisé dans les secteurs de l'eau, des orteils, des transports et de nombreuses autres.

Le préprocesseur DNP3 détecte les anomalies dans le trafic DNP3 et décode le protocole DNP3 pour le traitement par le moteur de règles, qui utilise des mots-clés DNP3 pour accéder à certains champs de protocole.

Sujets connexes

Mots-clés DNP3

Options du préprocesseur DNP3

Ports

Active l'inspection du trafic DNP3 sur chaque port spécifié. Vous pouvez spécifier un port unique ou une liste de ports séparés par des virgules.

Consigner les CRC incorrects

Valide les sommes de contrôle contenues dans les trames de la couche de liaison DNP3. Les trames avec des sommes de contrôle non valides sont ignorées.

Vous pouvez activer la règle 145:1 à générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés lorsque des sommes de contrôle non valides sont détectées.

Configuration du préprocesseur DNP3

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Vous ne devez pas activer ce préprocesseur dans une politique d'analyse de réseau que vous appliquez au trafic si votre réseau ne contient aucun périphérique compatible avec DNP3.

Dans un déploiement multidomaine, le système affiche les politiques créées dans le domaine actuel, que vous pouvez modifier. Il affiche également les politiques créées dans les domaines ancêtres, que vous ne pouvez pas modifier. Pour afficher et modifier les politiques créées dans un domaine inférieur, basculez vers ce domaine.

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si **la configuration DNP3** sous **préprocesseurs SCADA** est désactivée, cliquez sur **Enabled** (Activer).

Étape 6 Cliquez sur **Edit** (✎) à côté de **DNP3 Configuration** (Configuration DNP3).

Étape 7 Saisissez une valeur pour le champ **Ports**.

Séparez les valeurs multiples par des virgules

Étape 8 Cochez ou décochez la case **Log bad CRC** (Journaliser les CRC incorrects).

Étape 9 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, activez les règles de préprocesseur DNP3 (GID 145). Pour plus de renseignements, consultez les sections Définition des états des règles d'intrusion, Options du préprocesseur DNP3, à la page 5 et Règles de préprocesseur DNP3, à la page 6.
- Déployer les changements de configuration.

Sujets connexes

Gestion des couches
Conflits et modifications : analyse de réseau et politiques de prévention des intrusions

Règles de préprocesseur DNP3

Vous devez activer les règles de préprocesseur DNP3 dans le tableau suivant si vous souhaitez que ces règles générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés.

Tableau 2 : Règles de préprocesseur DNP3

GID de la règle de préprocesseur : SID	Description
145:1	Lorsque **Log bad CRC** (journaliser la CRC incorrecte) est activé, génère un événement lorsque le préprocesseur détecte une trame de couche de liaison avec une somme de contrôle non valide.
145:2	Génère un événement et bloque le paquet lorsque le préprocesseur détecte une trame de couche de liaison DNP3 avec une longueur non valide.

GID de la règle de préprocesseur : SID	Description
145:3	Génère un événement et bloque le paquet pendant le réassemblage lorsque le préprocesseur détecte un segment de la couche de transport avec un numéro de séquence non valide.
145:4	Génère un événement lorsque la mémoire tampon de réassemblage DNP3 est effacée avant qu'un fragment complet puisse être réassemblé. Cela se produit lorsqu'un segment portant l'indicateur FIR apparaît après que d'autres segments ont été mis en file d'attente.
145:5	Génère un événement lorsque le préprocesseur détecte une trame de couche de liaison DNP3 qui utilise une adresse réservée.
145:6	Génère un événement lorsque le préprocesseur détecte une requête ou une réponse DNP3 qui utilise un code de fonction réservée.

Le préprocesseur CIP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le Common Industrial Protocol (CIP) est un protocole d'application très utilisé qui prend en charge les applications d'automatisation industrielle. EtherNet/IP (ENIP) est une implémentation de CIP utilisée sur les réseaux Ethernet.

Le préprocesseur CIP détecte le trafic CIP et ENIP s'exécutant sur TCP ou UDP et l'envoie au moteur de règles de prévention des intrusions. Vous pouvez utiliser les mots-clés CIP et ENIP dans les règles de prévention des intrusions personnalisées pour détecter les attaques dans le trafic CIP et ENIP. Reportez -vous à la section Mots-clés CIP et ENIP. En outre, vous pouvez contrôler le trafic en spécifiant les conditions d'application CIP et ENIP dans les règles de contrôle d'accès. Consultez Configuration des conditions d'application et des filtres.

Options du préprocesseur CIP

Ports

Spécifie les ports à inspecter pour le trafic CIP et ENIP. Vous pouvez spécifier un nombre entier entre 0 et 65 535. Séparez les valeurs de ports multiples par des virgules

Remarque Vous devez ajouter le port de détection CIP par défaut 44818 et tout autre port que vous répertoriez à la liste de flux TCP **Effectuer le réassemblage des flux sur les deux ports**. Consultez Options de prétraitement du flux TCP et Création d'une politique d'analyse de réseau personnalisée.

Délai d'expiration par défaut de la déconnexion (secondes)

Lorsqu'un message de demande CIP ne contient pas de valeur d'expiration spécifique au protocole et que le **Nombre maximal de demandes non connectées simultanées par connexion TCP** est atteint, le système rythme le message pour le nombre de secondes spécifié par cette option. À l'expiration de la temporisation, le message est supprimé pour libérer de l'espace pour les demandes futures. Vous pouvez spécifier un entier entre 0 et 360. Lorsque vous spécifiez 0, tout le trafic qui n'a pas de délai d'expiration spécifique au protocole expire en premier.

Nombre maximal de demandes simultanées non connectées par connexion TCP

Le nombre de demandes simultanées qui peuvent rester sans réponse avant que le système ne ferme la connexion. Vous pouvez spécifier un entier entre 1 et 10 000.

Nombre maximal de connexions CIP par connexion TCP

Le nombre maximal de connexions CIP simultanées autorisées par le système, par connexion TCP. Vous pouvez spécifier un entier entre 1 et 10 000.

Événements CIP

De par leur conception, les détecteurs d'applications détectent et les visualiseurs d'événements affichent la même application une fois par session. Une session CIP peut inclure plusieurs applications dans différents paquets, et un seul paquet CIP peut contenir plusieurs applications. Le préprocesseur CIP gère tout le trafic CIP et ENIP selon la règle de prévention des intrusions correspondante.

Le tableau suivant présente les valeurs CIP affichées dans les vues des événements.

Tableau 3 : Valeurs du champ d'événement CIP

Champ d'événement	Valeur affichée
Protocole d'application	CIP ou ENIP
Client	Client CIP ou client ENIP
Application Web	L'application spécifique détectée, à savoir : • Pour les règles de contrôle d'accès qui autorisent ou surveillent le trafic, le dernier pro détecté dans la session. Les règles de contrôle d'accès que vous configurez pour journaliser les connexion générer d'événements pour des applications CIP spécifiées, et les règles de contrô ne configurez pas pour journaliser des connexions peuvent générer des événements p CIP. • Pour les règles de contrôle d'accès qui bloquent le trafic, le protocole d'applicatio blocage. Lorsqu'une règle de contrôle d'accès bloque une liste d'applications CIP, les visuali affichent la première application détectée.

Règles de préprocesseur CIP

Si vous souhaitez que les règles de préprocesseur CIP répertoriées dans le tableau suivant génèrent des événements, vous devez les activer. Consultez Définition des états des règles d'intrusion pour en savoir plus sur l'activation des règles.

Tableau 4 : Règles de préprocesseur CIP

GID:SID	Message de règle
148:1	CIP_MALFORMED
148:2	CIP_NON_CONFORMING
148:3	CIP_CONNECTION_LIMIT
148:4	CIP_REQUEST_LIMIT

Lignes directrices pour la configuration du préprocesseur CIP

Tenez compte des éléments suivants lors de la configuration du préprocesseur CIP :

- Vous devez ajouter le port de détection CIP par défaut 44818 et tous les autres **ports** CIP que vous indiquez à la liste **Exécuter le réassemblage du flux TCP sur les deux ports**. Consultez les sections Options du préprocesseur CIP, à la page 7, Création d'une politique d'analyse de réseau personnalisée et Options de prétraitement du flux TCP.
- Les visionneuses d'événements offrent un traitement spécial aux applications CIP. Consultez Événements CIP, à la page 8.
- Nous vous recommandons d'utiliser une action de prévention des intrusions comme action par défaut de votre politique de contrôle d'accès.
- Le préprocesseur CIP ne prend pas en charge une action de politique de contrôle d'accès par défaut **Access Control: Trust All Traffic**(contrôle d'accès : confiance dans tout le trafic), ce qui peut entraîner un comportement indésirable, notamment ne pas abandonner le trafic déclenché par les applications CIP spécifiées dans les règles de prévention des intrusions et les règles de contrôle d'accès.
- Le préprocesseur CIP ne prend pas en charge une action de contrôle d'accès par défaut **Access Control: Block All Traffic**(contrôle d'accès : blocage de tout le trafic), ce qui peut entraîner un comportement indésirable, notamment le blocage d'applications CIP qui ne devraient pas être bloquées.
- Le préprocesseur CIP ne prend pas en charge la visibilité des applications pour les applications CIP, y compris la découverte de réseau.
- Pour détecter les applications CIP et ENIP et les utiliser dans les règles de contrôle d'accès, les règles de prévention des intrusions, etc., vous devez activer manuellement le préprocesseur CIP dans la politique d'analyse de réseau personnalisée correspondante. Consultez Création d'une politique d'analyse de réseau personnalisée, Définir la politique d'analyse de réseau par défaut et Configuration des règles d'analyse du réseau.
- Pour abandonner le trafic qui déclenche les règles de préprocesseur CIP et les règles de prévention des intrusions CIP, assurez-vous que **Drop when inline** (Abandonner quand en ligne) est activée dans la

politique de prévention des intrusions correspondante. Reportez-vous à la section Définition du comportement d'abandon dans un déploiement en ligne.

- Pour bloquer le trafic des applications CIP ou ENIP à l'aide des règles de contrôle d'accès, vérifiez que le préprocesseur de normalisation en ligne et son option de **mode en ligne** sont activés (le paramètre par défaut) dans la politique d'analyse de réseau correspondante. Consultez Création d'une politique d'analyse de réseau personnalisée, Définir la politique d'analyse de réseau par défaut et Modification du trafic de préprocesseur dans les déploiements en ligne.

Configuration du préprocesseur CIP

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Avant de commencer

- Vous devez ajouter le port de détection CIP par défaut 44818 et tout autre port que vous indiquez comme **ports** CIP à la liste TCP **Perform Stream Reassembly on Both Ports** (Effectuer le réassemblage des flux sur les deux ports). Consultez les sections Options du préprocesseur CIP, à la page 7, Création d'une politique d'analyse de réseau personnalisée et Options de prétraitement du flux TCP.
- Familiarisez-vous avec Lignes directrices pour la configuration du préprocesseur CIP, à la page 9.
- Le préprocesseur CIP n'est pas pris en charge par les périphériques défense contre les menaces .

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** (✎) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** (👁) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si **la configuration CIP** est désactivée sous les **préprocesseurs SCADA**, cliquez sur **Enabled** (Activée).

Étape 6 Vous pouvez modifier n'importe quelle option décrite dans Options du préprocesseur CIP, à la page 7.

Étape 7 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez générer des événements et, dans un déploiement en ligne, supprimer les paquets incriminés, activez les règles de prévention des intrusions CIP et, éventuellement, les règles de préprocesseur CIP (GID 148). Pour plus de renseignements, consultez les sections Définition des états des règles d'intrusion, Règles de préprocesseur CIP, à la page 9 et Événements CIP, à la page 8.
- Déployer les changements de configuration.

Le préprocesseur S7Commplus

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le préprocesseur S7Commplus détecte le trafic S7Commplus. Vous pouvez utiliser des mots-clés S7Commplus dans les règles de prévention des intrusions personnalisées pour détecter des attaques dans le trafic S7Commplus. Consultez Mots-clés S7Commplus.

Configuration du préprocesseur S7Commplus

Remarque Cette section s'applique aux préprocesseurs Snort 2. Pour en savoir plus sur les inspecteurs Snort 3, consultez https://www.cisco.com/go/snort3-inspectors.

Le préprocesseur S7Commplus est pris en charge sur tous les périphériques défense contre les menaces .

Procédure

Étape 1 Choisissez **Politiques** > **Contrôle d'accès**, puis cliquez sur **Politique d'analyse des réseaux** ou **Policies (politiques)** > **Access Control (contrôle d'accès)** > **Intrusion**, puis cliquez sur **Network Analysis Policies (Politiques d'analyse de réseau)**.

Remarque Si votre rôle d'utilisateur personnalisé restreint l'accès au premier chemin répertorié ici, utilisez le deuxième chemin pour accéder à la politique.

Étape 2 Cliquez sur **Snort 2 Version** à côté de la politique que vous souhaitez modifier.

Étape 3 Cliquez sur **Edit** ( ) (Modifier) à côté de la politique que vous souhaitez modifier.

Si **Afficher** ( ) apparaît plutôt, la configuration est héritée d'une politique ancêtre ou encore, vous n'êtes pas autorisé à modifier la configuration.

Étape 4 Cliquez sur **Settings** (paramètres) dans le panneau de navigation.

Étape 5 Si **la configuration de S7Commplus** est désactivée sous **préprocesseurs SCADA**, cliquez sur **Enabled** (Activée).

Étape 6 Vous pouvez également cliquer sur **Edit** ( ) à côté de **Configuration S7Commplus** et modifier **s7commplus_ports** pour identifier les ports que le préprocesseur inspecte pour le trafic S7Commplus. Séparez les valeurs de ports multiples par des virgules.

Étape 7 Pour enregistrer les modifications que vous avez apportées à cette politique depuis la dernière validation de politique, cliquez sur **Policy Information** (informations de politique), puis cliquez sur **Commit Changes** (valider les modifications).

Si vous quittez la politique sans valider les modifications, les changements présents dans le cache apportés depuis la dernière validation sont annulés si vous modifiez une autre politique.

Prochaine étape

- Si vous souhaitez générer des incidents d'intrusion, activez les règles de préprocesseur S7Commplus (GID 149). Pour en savoir plus, consultez Définition des états des règles d’intrusion
- Déployer les changements de configuration.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.