

**Mise en place**

# Structure des signatures Suricata

Les signatures Suricata peuvent sembler complexes au premier abord, mais une fois que l’on comprend comment elles sont structurées et comment Suricata les traite, on est en mesure de créer ses propres règles en fonction des exigences de on réseau.

À un niveau élevé, les signatures Suricata se composent de trois parties …

* **Action** ;
* **En-tête** ;
* **Options**.

Une **action** qui spécifie ce que la règle effectue lorsque le trafic correspond à la règle.

Un **en-tête** qui décrit …

* les hôtes ;
* les adresses IP ;
* les ports ;
* les protocoles   
  et la direction du trafic (entrant ou sortant)

Les **options** qui spécifient des éléments tels que …

* l'ID de signature (sid) ;
* le message de journal ;
* les expressions régulières qui correspondent au contenu des paquets ;
* le type de classification   
  et
* d'autres modificateurs qui peuvent aider à affiner l'identification du trafic légitime et suspect.

La structure générale d'une signature est la suivante …  
**<Action> <Entête> <Options>  
<*Action*> <*Header*> <*Options*>**

Les parties d'en-tête et d'options d'une signature comportent plusieurs sections.   
Comme exemple … la règle avec le sid 2100498  
**alert ip any any -> any any (msg:"GPL ATTACK\_RESPONSE id check returned root"; content:"uid=0|28|root|29|"; classtype:bad-unknown; sid:2100498; rev:7; metadata:created\_at 2010\_09\_23, updated\_at 2010\_09\_23;)**

* **alert**  
  Action de la signature ;
* **ip any any -> any any**   
  En-tête de la signature ;
* **(msg:"GPL ATTACK\_RESPONSE …**Options de la signature.

# Actions

La première partie de la signature sid:2100498 est l'action ; dans l’exemple précédent **alert**.   
Cette partie d'une signature spécifie l'action à entreprendre lorsqu'un paquet correspond à la règle.

Une action peut être l'une des suivantes selon que Suricata fonctionne en mode IDS ou IPS …

* **pass**  
  Suricata arrêtera d'analyser le paquet et l'autorisera, sans générer d'alerte ;
* **drop**  
  Lors du travail en mode IPS, Suricata arrête immédiatement de traiter le paquet et génère une alerte.   
  Si la connexion qui a généré le paquet utilise TCP, elle va se fermer (expirer) ;
* **reject**Lors du travail en mode IPS, un paquet de réinitialisation TCP sera envoyé et Suricata supprimera le paquet correspondant ;
* **alert**   
  Suricata génére une alerte et l'enregistre pour une analyse ultérieure plus approfondie.

# En-têtes

Chaque signature Suricata possède une section d'en-tête qui décrit le protocole réseau, les adresses IP source et de destination, les ports et la direction du trafic.

Le format général de la section d'en-tête d'une règle est …  
**<Protocole> <Adresse IP source> <Port source> -> <Adresse IP destination> <Port de destination>**

Le protocole peut être …

* TCP ;
* UDP ;
* ICMP ;
* IP ;
* Autres protocoles de la couche Application.

Les champs **<Source>** et **<Destination>** peuvent être des adresses IP ou des étendues réseau.  
La valeur spéciale **any** correspond à toutes les adresses IP et tous les réseaux.   
La flèche … -> … indique le sens de la circulation.

**Remarque** …  
Les signatures peuvent aussi utiliser un marqueur non directionnel … <> … qui correspond au trafic dans les deux sens. Toutefois, le marqueur directionnel … -> … est dans la majorité des cas utilisé.

Si on veut produire des alertes sur le trafic sortant malveillant (c'est-à-dire le trafic quittant le réseau), le champ **<Source>** est alors l'adresse IP ou l’étendue réseau de son système.   
La destination peut être l'adresse IP ou le réseau d'un système distant, ou la valeur spéciale any.

Inversement, si on veut générer une alerte pour le trafic entrant malveillant, le champ **<Source>** pourrait être défini sur **any**, et le champ **<Destination>** sur l'adresse IP ou l’étendue réseau de son système.

On peut également spécifier le port TCP ou UDP à examiner à l'aide des champs **<Port>**.   
Généralement, le trafic provenant d'un système se voit attribuer un port aléatoire, de sorte que la valeur any est appropriée pour le côté gauche de l'indicateur … ->.   
Le port de destination peut également être any si on prévoie examiner le contenu de chaque paquet entrant, ou on peut limiter une signature pour analyser uniquement les paquets sur des ports individuels, comme 22 pour le trafic SSH ou 443 pour HTTPS.

L'en-tête **ip any any -> any any** de la règle sid:2100498 est un en-tête générique qui correspondra à tout le trafic, quel que soit le protocole, les adresses IP source ou de destination ou les ports.   
Ce type d'en-tête générique est utile afin de s’assurer que le trafic entrant et sortant est contrôlé pour détecter tout contenu suspect.

**Remarque** …  
Les champs Source, Destination et Port peuvent également utiliser l'opérateur de négation spécial !, qui traitera le trafic qui ne correspond pas à la valeur du champ.

Par exemple, la signature suivante ferait de Suricata une alerte sur tous les paquets SSH entrants du réseau any qui sont destinés au réseau local (représenté par le bloc IP 192.168.1.0/24), qui ne sont pas destinés au port 22 …  
**alert ssh any any -> 192.168.1.0/24 !22 (sid:1000000;)**

Cette alerte ne serait pas très utile, car elle ne contient aucun message concernant le paquet, ni type de classification. Pour ajouter des informations supplémentaires à une alerte, ainsi qu'une correspondance sur des critères plus spécifiques, les règles Suricata possèdent une section **<Options>** dans laquelle il est possible de spécifier un certain nombre de paramètres supplémentaires pour une signature.

# Options

Les arguments entre parenthèses (. . .) dans une signature Suricata contiennent diverses options et modificateurs de mots clés que l’on peut utiliser afin de …

* faire correspondre des parties spécifiques d'un paquet ;
* classer une règle   
  ou
* consigner des messages personnalisés.

Alors que les arguments d'en-tête d'une règle fonctionnent sur les en-têtes de paquet au niveau de l'adresse IP, du port et du protocole, les options correspondent aux données contenues dans un paquet.

Les options d'une règle Suricata doivent être séparées par un point-virgule (;) et utilisent généralement un format clé:valeur.   
Certaines options n'ont pas de paramètres et seul le nom doit être spécifié dans une règle.

Considérant la règle suivante …  
**alert ssh any any -> 192.168.1.0/24 !22 (sid:1000000;)**

On peut ajouter l'option msg avec une valeur d'explication SSH traffic detected on non-SSH port de l'objet de l'alerte …  
**alert ssh any any -> 192.168.1.0./24 !22 (msg:"SSH TRAFFIC on non-SSH port"; sid:1000000;)**

Il existe certaines options de base comme le mot-clé content et divers mots-clés Meta qui sont utilisés dans la plupart des signatures.

### Mot-clé Content

L'une des options les plus importantes pour toute règle est le mot-clé content.

Considérant la règle suivante …  
**alert ip any any -> any any (msg:"GPL ATTACK\_RESPONSE id check returned root"; content:"uid=0|28|root|29|"; classtype:bad-unknown; sid:2100498; rev:7; metadata:created\_at 2010\_09\_23, updated\_at 2010\_09\_23;)**

La partie en surbrillance **content:"uid=0|28|root|29|"**; contient le mot-clé content et la valeur que Suricata recherchera dans un paquet.   
Dans ce cas, tous les paquets provenant de n'importe quelle adresse IP sur n'importe quel port seront vérifiés pour s'assurer qu'ils ne contiennent pas la valeur de chaîne **uid=0|28|root|29|**(indiquant un hôte compromis).

Le mot-clé content peut être utilisé avec la plupart des autres mots-clés de Suricata.   
Il est possible de créer des signatures très spécifiques à l'aide de combinaisons d'en-têtes et d'options qui ciblent des protocoles d'application spécifiques, pour la suite vérifier le contenu des paquets pour des octets individuels, des chaînes ou des correspondances à l'aide d'expressions régulières.

Comme exemple, la signature qui suit examine le trafic DNS à la recherche de tout paquet avec le contenu tux.info afin de générer une alerte …  
**alert dns any any -> any any (msg:"DNS LOOKUP for tux.info"; dns.query; content:"TUX.INFO"; sid:1000001;)**

Toutefois, cette règle ne correspond pas si la requête DNS utilisait le domaine TUX.INFO, puisque Suricata utilise par défaut la correspondance de contenu sensible à la casse.

Pour rendre les correspondances de contenu insensibles à la casse, on doit ajouter le mot clé nocase; à la règle …  
**alert dns any any -> any any (msg:"DNS LOOKUP for your\_domain.com"; dns.query; content:"your\_domain.com"; nocase; sid:1000001;)**

Désormais, toute combinaison de lettres minuscules ou majuscules correspondra toujours au mot-clé content.

### Mot-clé msg

Bien que l'option msg ne soit pas obligatoire, si elle est vide, il est difficile de comprendre pourquoi une alerte ou une action de suppression s'est produite lors de l'examen des journaux de Suricata.

L’option msg est une description textuelle consultable d'une alerte.   
Ce message doit être descriptif et ajouter des informations afin de comprendre le pourquoi qu’une alerte a été déclenchée.   
Cela facilite grandement l’analyse des différents journaux.

### Mots-clés sid et rev

Chaque signature Suricata nécessite un ID de signature unique (sid).   
Si deux règles ont le même sid, Suricata ne pourra démarrer et va générer une erreur similaire à celle-ci …  
. . .  
**19/11/2022 -- 01:17:40 - <Error> - [ERRCODE: SC\_ERR\_DUPLICATE\_SIG(176)] - Duplicate signature "drop ssh any any -> 127.0.0.0/8 !22 (msg:"blocked invalid ssh"; sid:10000000;)"  
. . .**

Lors de la création de ses propres signatures, l’étendue 1000000 - 1999999 est réservée aux règles personnalisées.   
Les règles intégrées de Suricata sont comprises entre 2200000 et 2299999.

L'option sid est généralement la dernière partie d'une règle Suricata.   
Toutefois, s'il existe plusieurs versions d'une signature avec des modifications au fil du temps, une option rev est utilisée afin de spécifier la version d'une règle.

Comme exemple, l'alerte SSH précédente peut être modifiée pour analyser uniquement le trafic SSH sur le port 2022 …  
**alert ssh any any -> 192.168.1.0/24 2022 (msg:"SSH TRAFFIC on non-SSH port"; sid:1000000; rev:2;)**

La signature mise à jour inclut désormais l'option rev:2 indiquant qu'elle a été mise à jour à partir d'une version précédente.

### Mot-clé reference

Le mot-clé reference est utilisé dans les signatures pour décrire où trouver plus d'informations sur l'attaque ou le problème qu'une règle est censée détecter.

Par exemple, si une signature est conçue pour détecter un nouveau type d'exploit ou de méthode d'attaque, le champ de référence peut être utilisé pour créer un lien vers un site spécialisé en sécurité ou le site Web d'une entreprise qui documente le problème.

La vulnérabilité Heartbleed dans OpenSSL est un exemple de bogue largement médiatisé et recherché.   
Suricata est livré avec une signature conçue afin vérifier les paquets TLS incorrects et inclut une référence de l'entrée principale CVE Heartbleed dans le fichier /etc/suricata/rules/tls-events.rules …  
**alert tls any any -> any any (msg:"SURICATA TLS invalid heartbeat encountered, possible exploit attempt (heartbleed)"; flow:established; app-layer-event:tls.invalid\_heartbeat\_message; flowint:tls.anomaly.count,+,1; classtype:protocol-command-decode; reference:cve,2014-0160; sid:2230013; rev:1;)**

Cette option indique, lors de l’examen des alertes de Suricata, où trouver plus d'informations sur un problème particulier.

L'option de référence peut utiliser n'importe lequel des préfixes du fichier /etc/suricata/reference.config.   
Par exemple, url pourrait être utilisé à la place de cve, avec un lien direct vers le site Heartbleed à la place de l'idntifiant CVE 2014-0160.

### Mot clé classtype

Suricata peut classer le trafic selon un ensemble préconfiguré de catégories qui sont incluses lors de l’installation du paquet Suricata.

Le fichier de classification par défaut est /etc/suricata/classification.config.  
Il contient des entrées similaires celles-ci …  
  
Une image contenant texte

Description générée automatiquement  
**Cette sortie a été tronquée.**

Comme l'indique l'en-tête du fichier, chaque entrée de classification comporte trois champs …

* Un nom court lisible par hôte  
  (not-suspicious, unknown et bad-unknown) ;
* La description d'une classification à utiliser avec les alertes  
  (Not Suspicious Traffic) ;
* Un champ prioritaire, qui détermine l'ordre dans lequel une signature sera traitée par Suricata.  
  La priorité la plus élevée est la valeur 1.  
  Les signatures qui utilisent un classificateur avec une priorité plus élevée seront vérifiées en premier lorsque Suricata traitera un paquet.

Comme exemple pour la signature sid:2100498, le type de classe est classtype:bad-unknown; …  
**alert ip any any -> any any (msg:"GPL ATTACK\_RESPONSE id check returned root"; content:"uid=0|28|root|29|"; classtype:bad-unknown; sid:2100498; rev:7; metadata:created\_at 2010\_09\_23, updated\_at 2010\_09\_23;)**

La priorité implicite de la signature est 2, car il s'agit de la valeur attribuée au type de classe **bad-unknown** dans le fichier /etc/suricata/classification.config.   
Si on souhaite remplacer la priorité par défaut d'un type de classe, il est possible ajouter une option **priority:n** à une signature, où **n** est une valeur comprise entre 1 et 255.

### Mot-clé target

Une autre option utile dans les signatures Suricata est l'option target.   
Elle peut être définie sur l'une des deux valeurs suivantes …

* src\_ip   
  et
* dest\_ip.

Le but de cette option est d'identifier correctement les hôtes source et destination (*target*) dans les journaux d'alertes de Suricata.

Comme exemple, la signature SSH qui suit peut être améliorée avec l' option target:dest\_ip; …  
**alert ssh any any -> 203.0.113.0/24 2022 (msg:"SSH TRAFFIC on non-SSH port"; target:dest\_ip; sid:1000000; rev:3;)**

Cet exemple utilise dest\_ip parce que la règle est conçue pour vérifier le trafic SSH entrant dans le réseau, c'est donc la destination.   
L'ajout de l'option target à une règle entraînera les champs supplémentaires suivants dans la partie alert d'une entrée eve.json de journal.

Une image contenant texte

Description générée automatiquement  
**Cette sortie a été tronquée.**

Avec ces entrées dans les journaux de Suricata, elles peuvent être envoyées à un outil de gestion des informations et des événements de sécurité (SIEM ou *Security Information and Event Management*) afin de faciliter la recherche d'alertes pouvant provenir d'un hôte commun ou d'attaques dirigées vers une cible spécifique sur le réseau.

**Référence** …  
https://www.digitalocean.com/community/tutorials/understanding-suricata-signatures