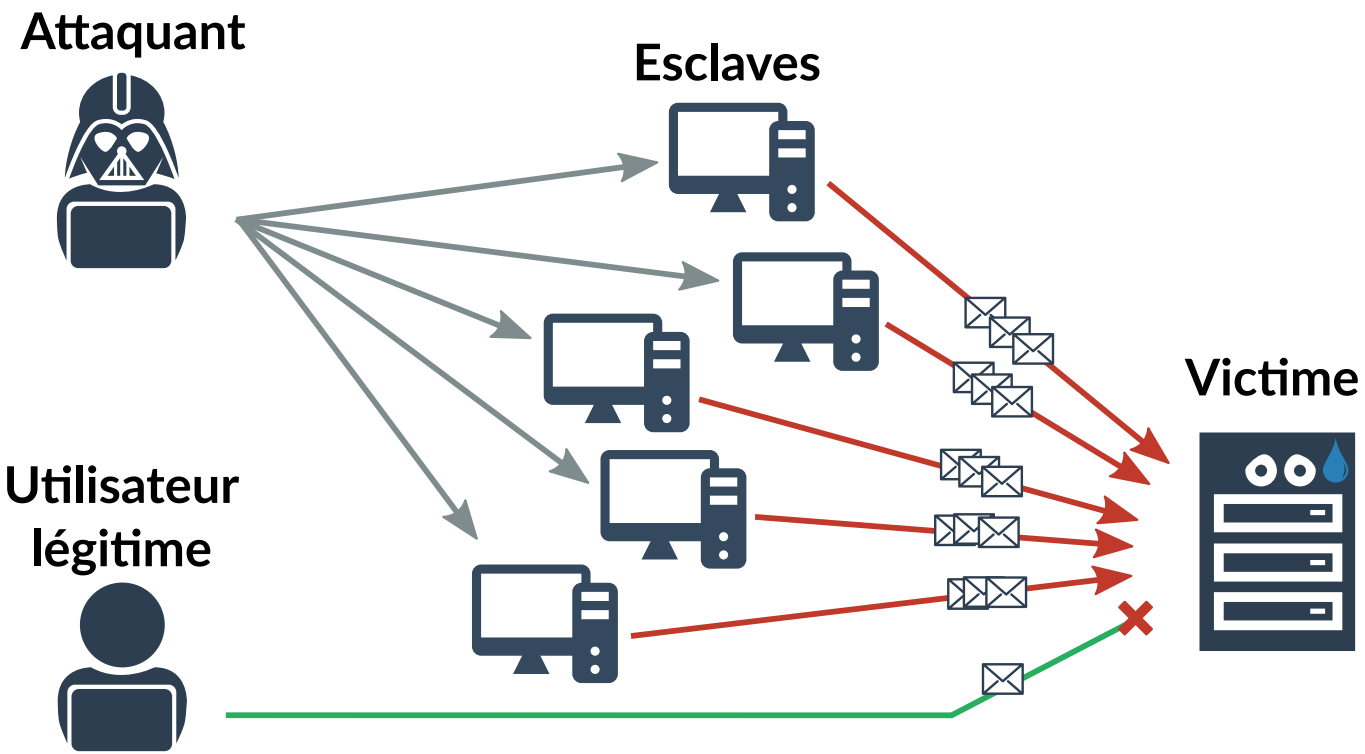
Détection d'attaques DDoS dans les réseaux

Gilles Roudière
gilles.roudiere@laas.fr

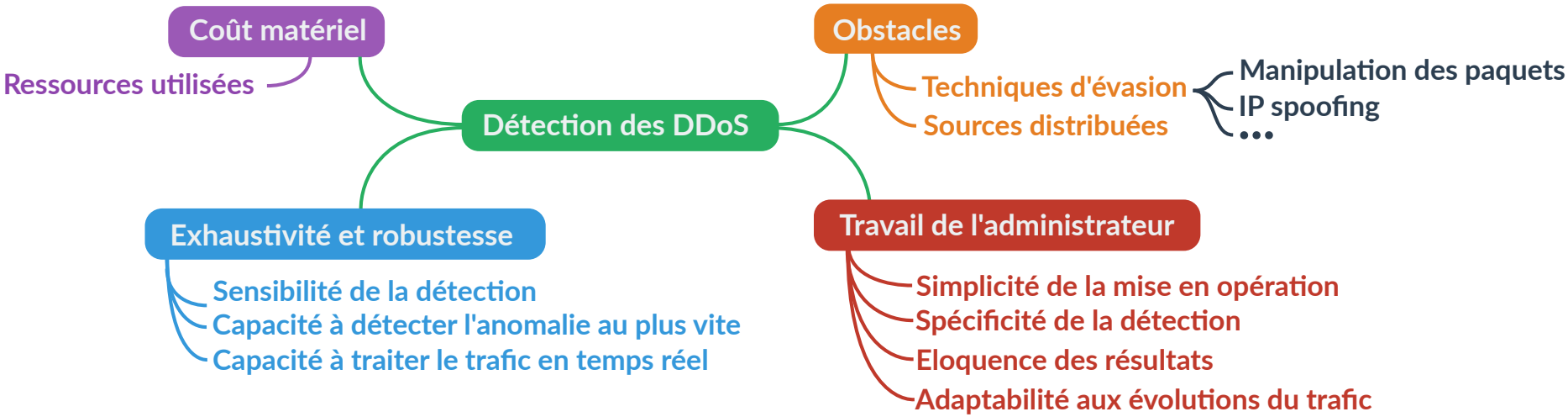
15 Septembre 2017

Contexte

Attaques par déni de service distribuées (DDoS) :



Problématique



Problématique

- Capacités de calcul restantes limitées,
- Détection au point d'entrée de l'entreprise (côté cible),
- Détection au niveau réseau

Problématique

- Capacités de calcul restantes limitées,
- Détection au point d'entrée de l'entreprise (côté cible),
- Détection au niveau réseau

Problématique

- Capacités de calcul restantes limitées,
- Détection au point d'entrée de l'entreprise (côté cible),
- Détection au niveau réseau

Détection à base de signatures

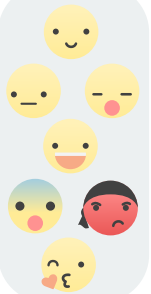
Base d'attaques

Attaques connues

Oreilles pointues et bouche ouverte = *attaque 1*

Cagoule = *attaque 2*

Cache oeil = *attaque 3*



Tout le reste
= *normal*

Détection à base de signatures

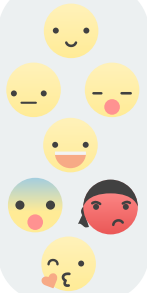
Base d'attaques

Attaques connues

Oreilles pointues et bouche ouverte = *attaque 1*

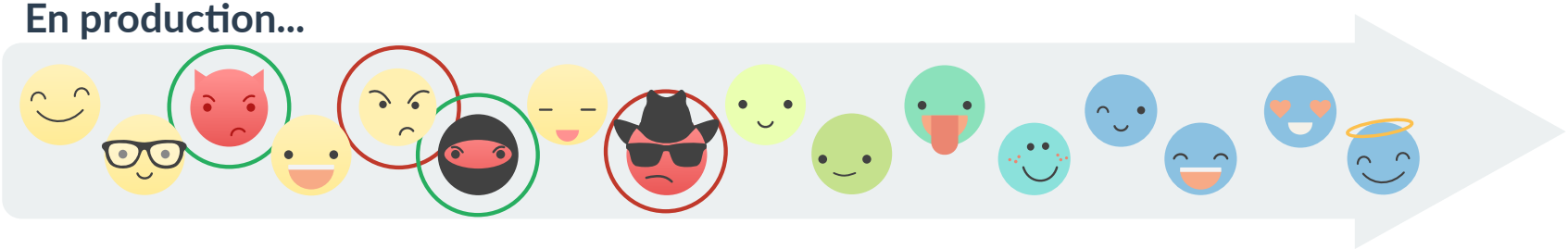
Cagoule = *attaque 2*

Cache oeil = *attaque 3*



Tout le reste
= *normal*

En production...



Détection à base de signatures

- ✓ Détection efficace des attaques connues,
- ✓ Nécessite relativement peu de ressources de calcul,
- ✗ Les signatures sont difficiles à créer,
- ✗ Ne détecte pas les attaques inconnues.

Détection à base de signatures

- ✓ Détection efficace des attaques connues,
- ✓ Nécessite relativement peu de ressources de calcul,
- ✗ Les signatures sont difficiles à créer,
- ✗ Ne détecte pas les attaques inconnues.

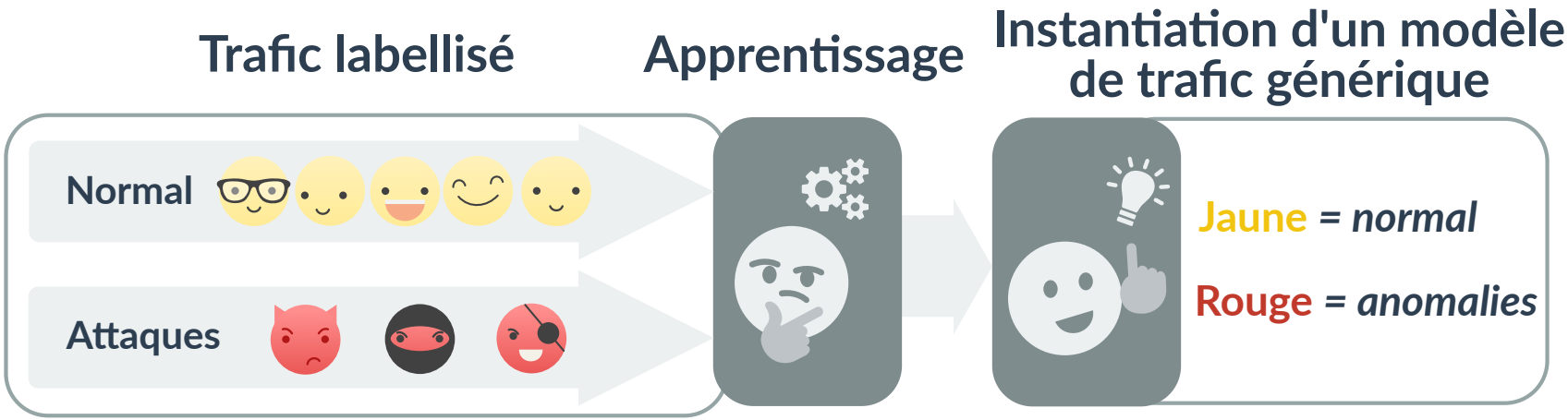
Détection à base de signatures

- ✓ Détection efficace des attaques connues,
- ✓ Nécessite relativement peu de ressources de calcul,
- ✗ Les signatures sont difficiles à créer,
- ✗ Ne détecte pas les attaques inconnues.

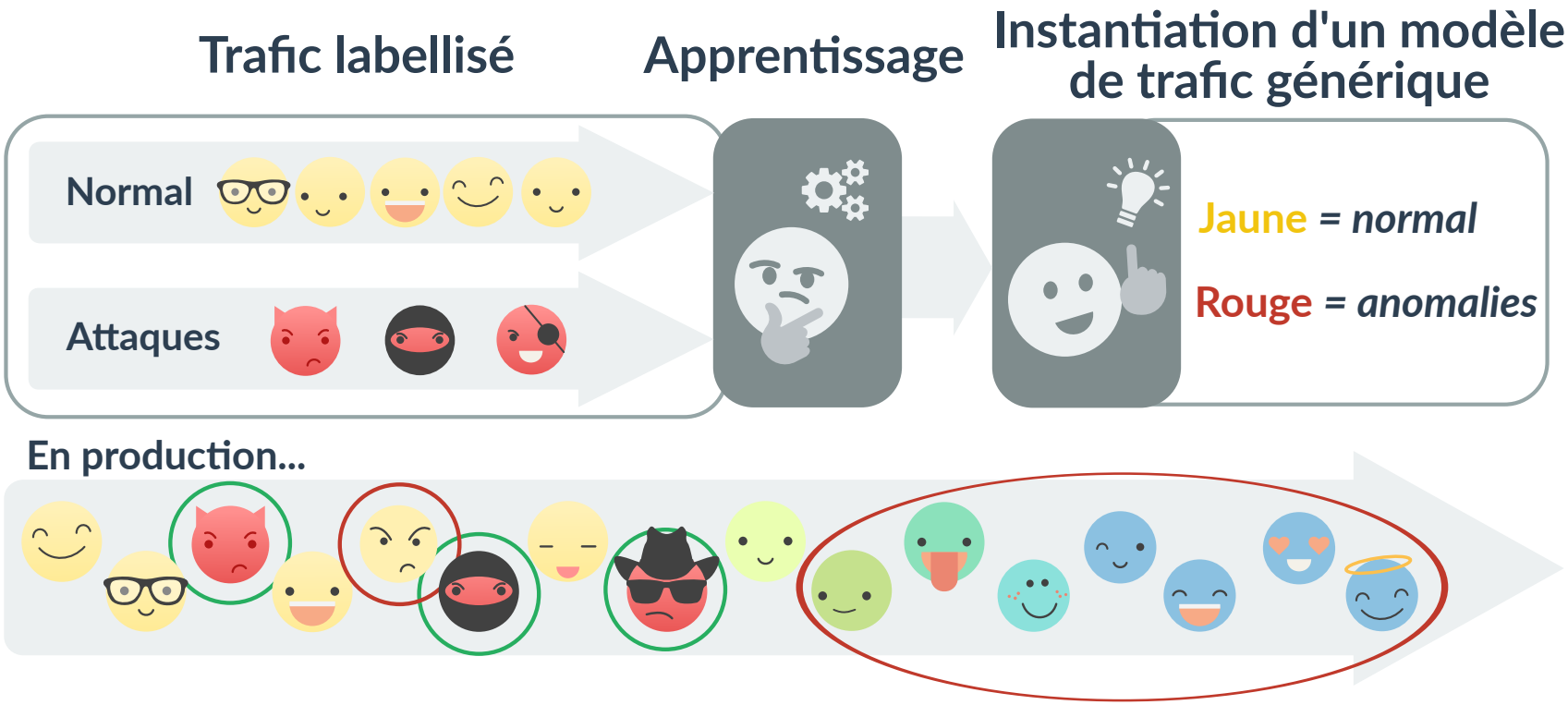
Détection à base de signatures

- ✓ Détection efficace des attaques connues,
- ✓ Nécessite relativement peu de ressources de calcul,
- ✗ Les signatures sont difficiles à créer,
- ✗ Ne détecte pas les attaques inconnues.

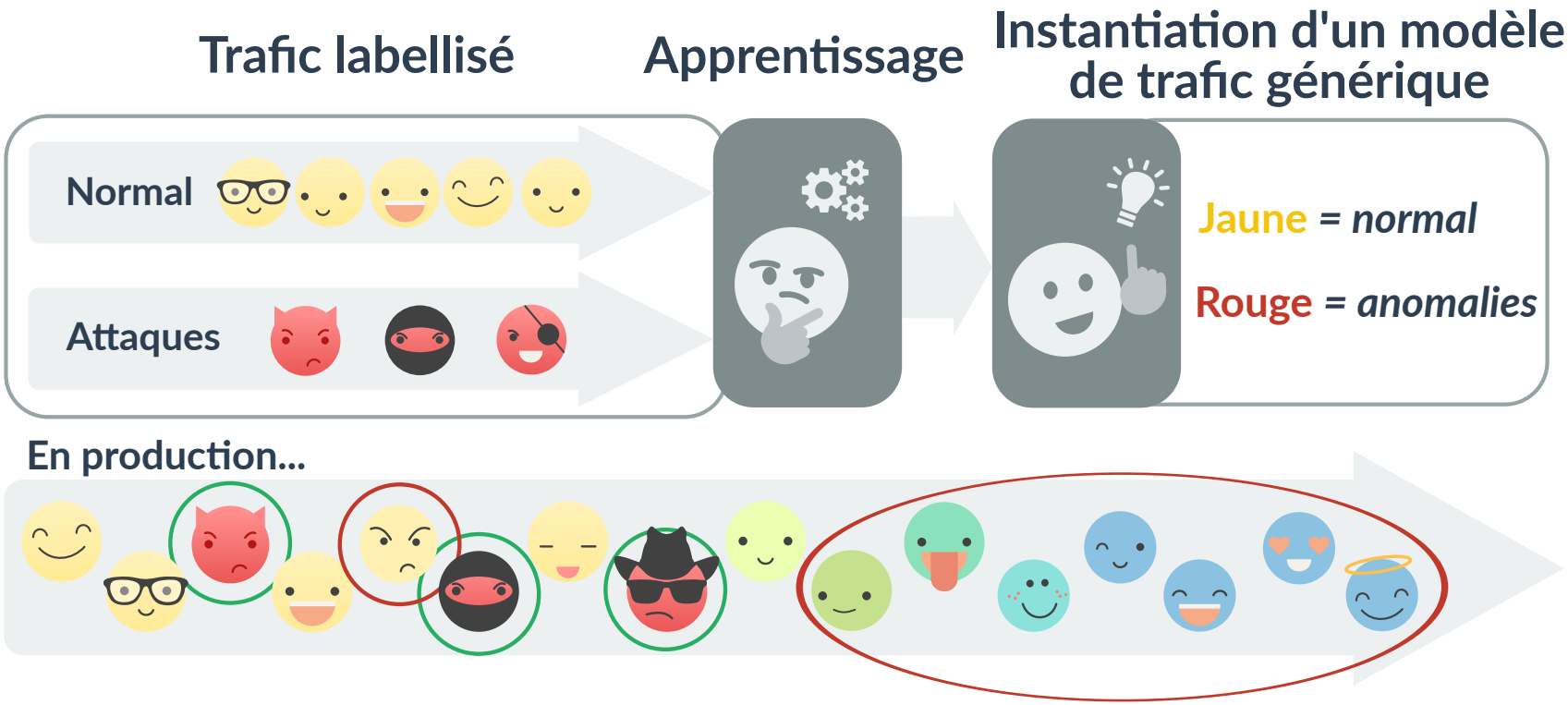
Détection supervisée



Détection supervisée

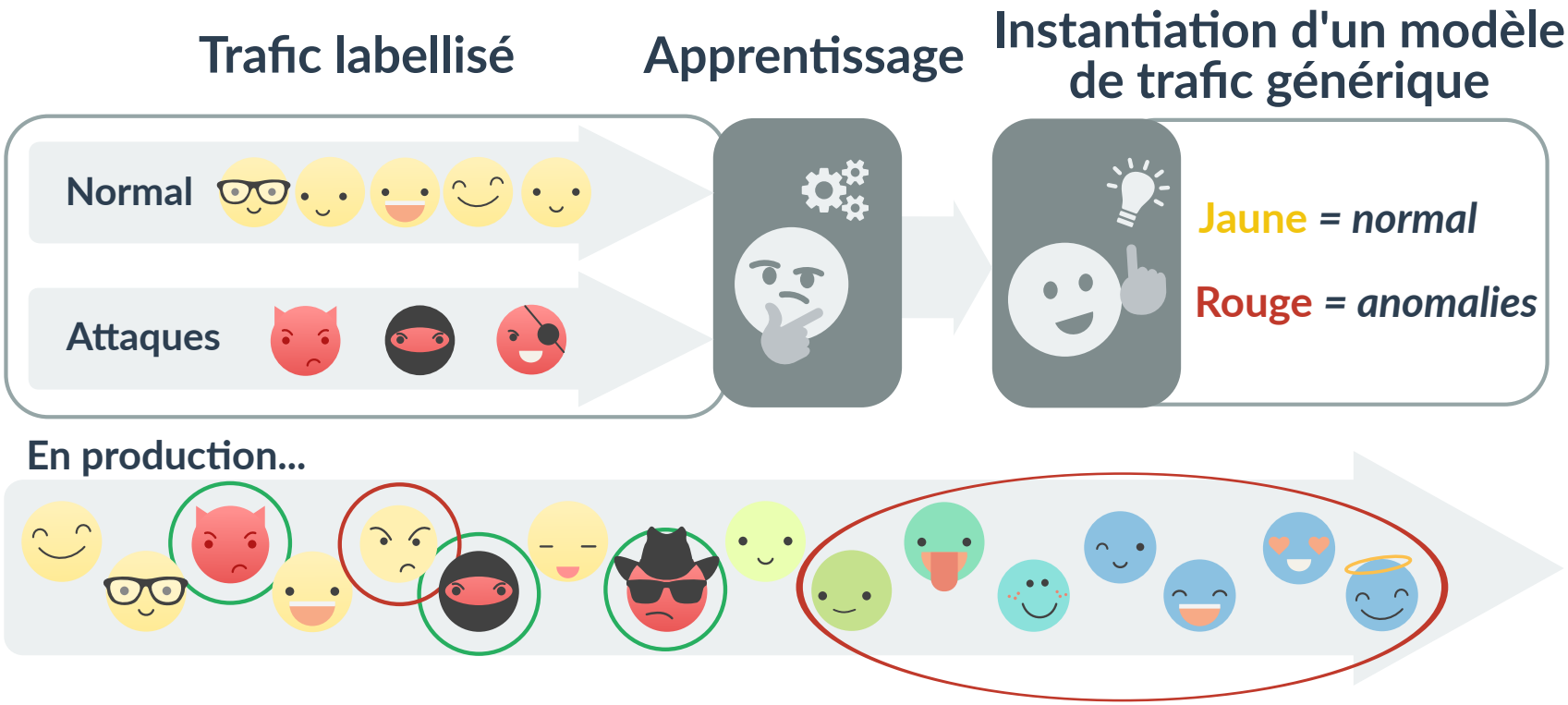


Détection supervisée



- ✓ Peut détecter des anomalies inconnues,
- ✓ Peut être entraîné à nouveau si le trafic évolue,
- ✗ Construire un modèle du trafic est complexe,
- ✗ Nécessite un jeu de données labellisé représentatif...
- ✗ ...qui doit être reconstruit à chaque fois que le trafic évolue.

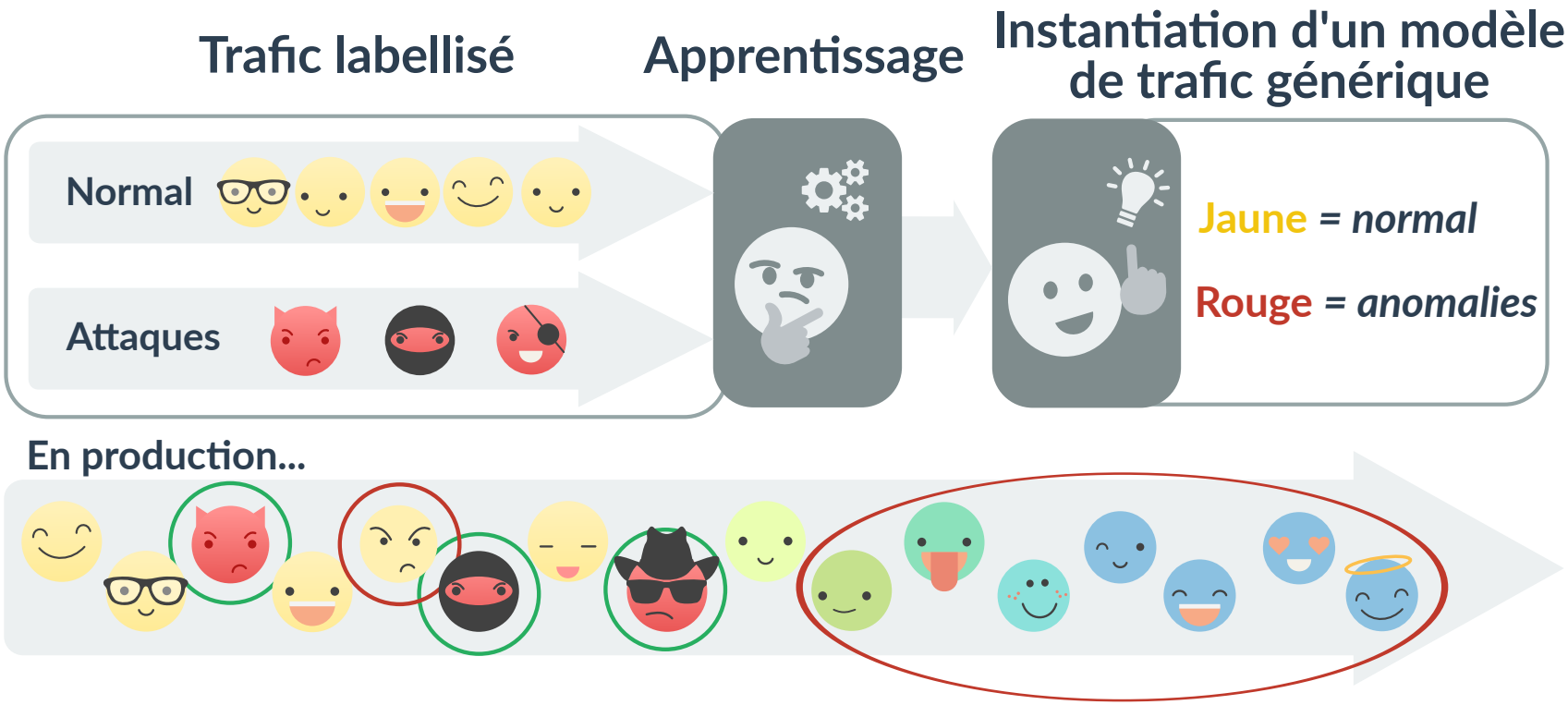
Détection supervisée



- ✓ Peut détecter des anomalies inconnues,
- ✓ Peut être entraîné à nouveau si le trafic évolue,

- ✗ Construire un modèle du trafic est complexe,
- ✗ Nécessite un jeu de données labellisé représentatif...
- ✗ ...qui doit être reconstruit à chaque fois que le trafic évolue.

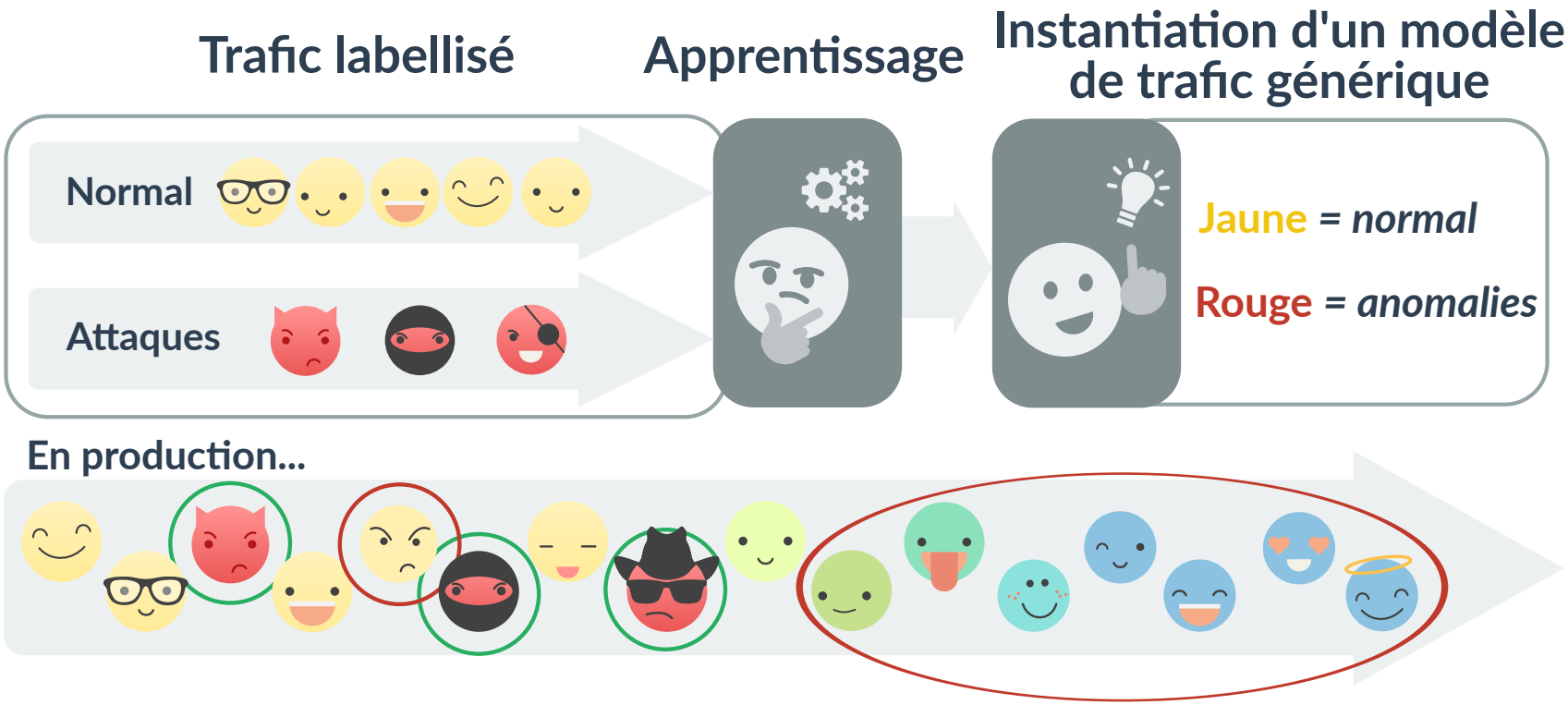
Détection supervisée



- ✓ Peut détecter des anomalies inconnues,
- ✓ Peut être entraîné à nouveau si le trafic évolue,

- ✗ Construire un modèle du trafic est complexe,
- ✗ Nécessite un jeu de données labellisé représentatif...
- ✗ ...qui doit être reconstruit à chaque fois que le trafic évolue.

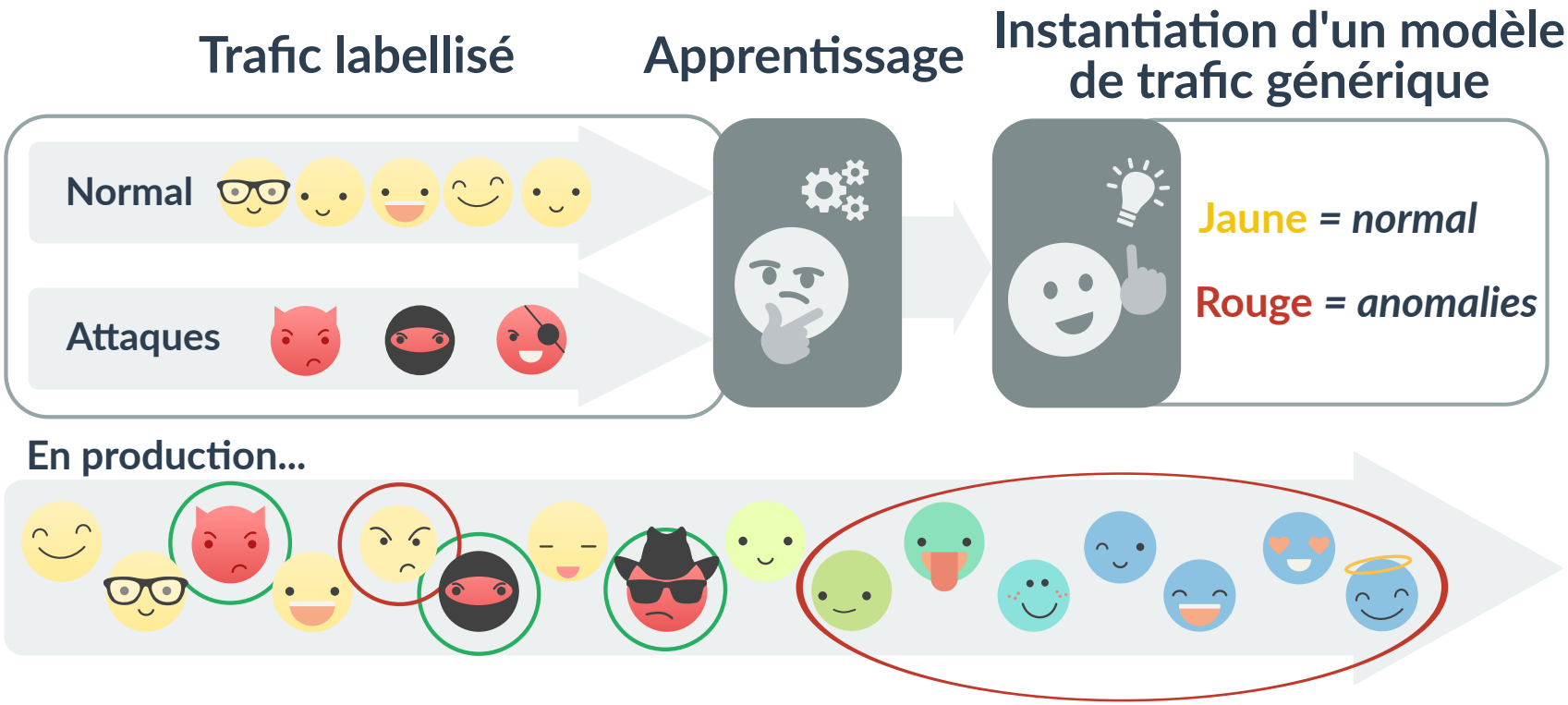
Détection supervisée



- ✓ Peut détecter des anomalies inconnues,
- ✓ Peut être entraîné à nouveau si le trafic évolue,

- ✗ Construire un modèle du trafic est complexe,
- ✗ Nécessite un jeu de données labellisé représentatif...
- ✗ ...qui doit être reconstruit à chaque fois que le trafic évolue.

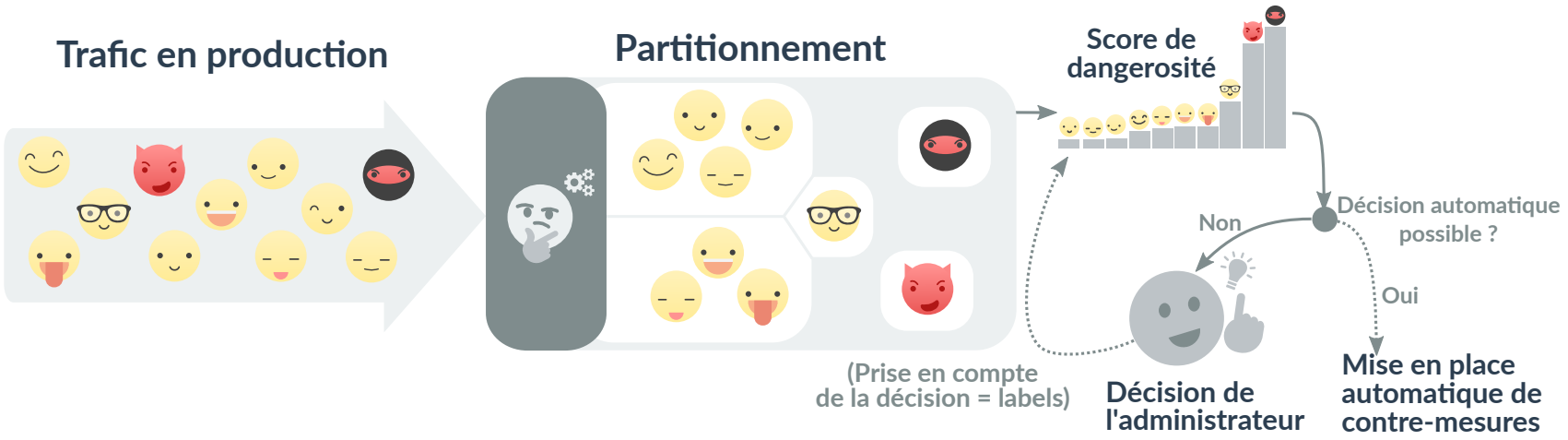
Détection supervisée



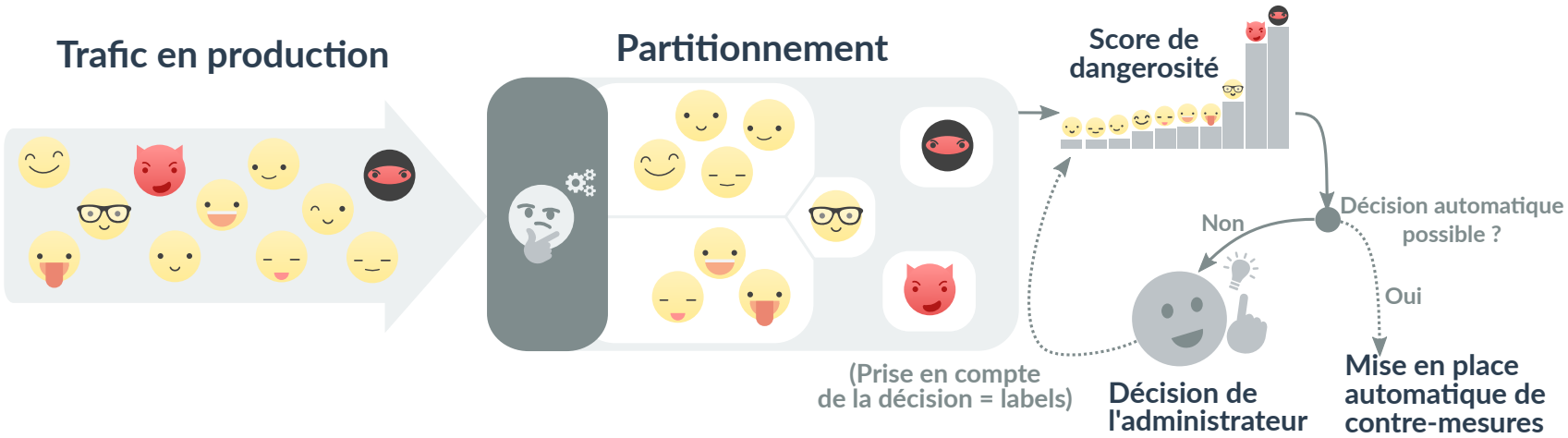
- ✓ Peut détecter des anomalies inconnues,
- ✓ Peut être entraîné à nouveau si le trafic évolue,

- ✗ Construire un modèle du trafic est complexe,
- ✗ Nécessite un jeu de données labellisé représentatif...
- ✗ ...qui doit être reconstruit à chaque fois que le trafic évolue.

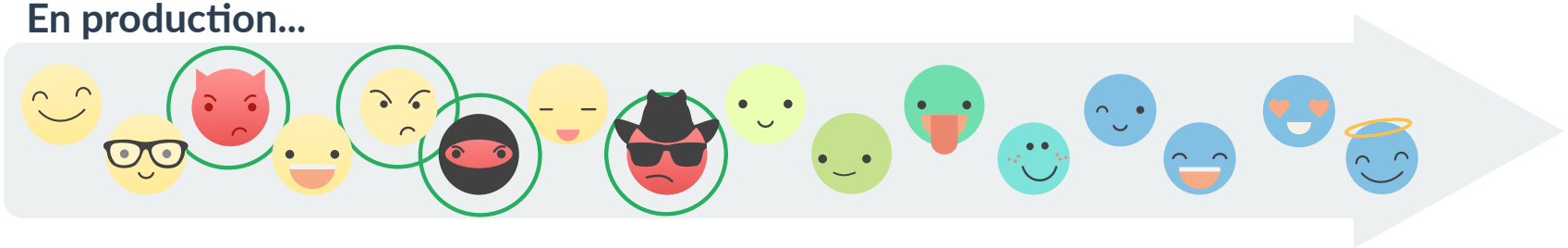
Détection non supervisée



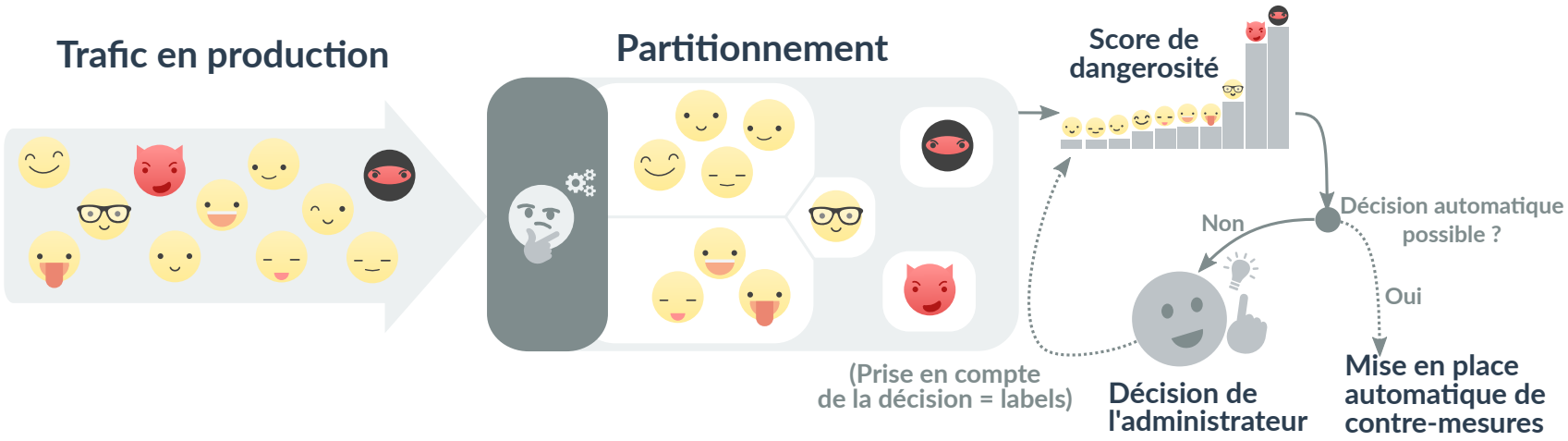
Détection non supervisée

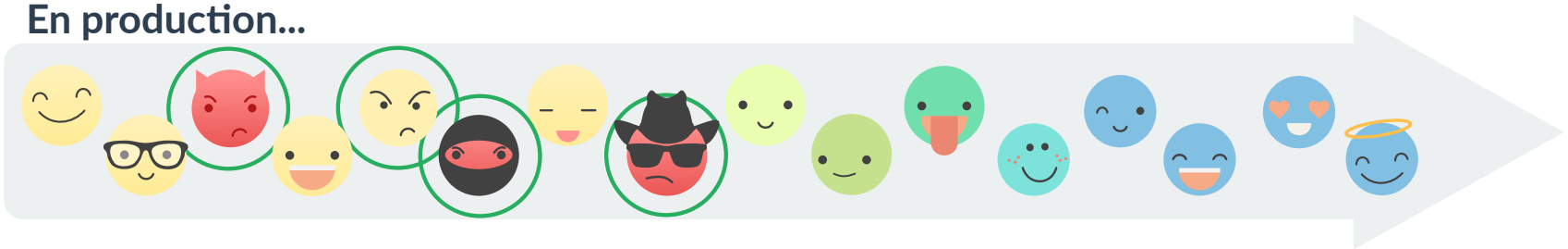


En production...



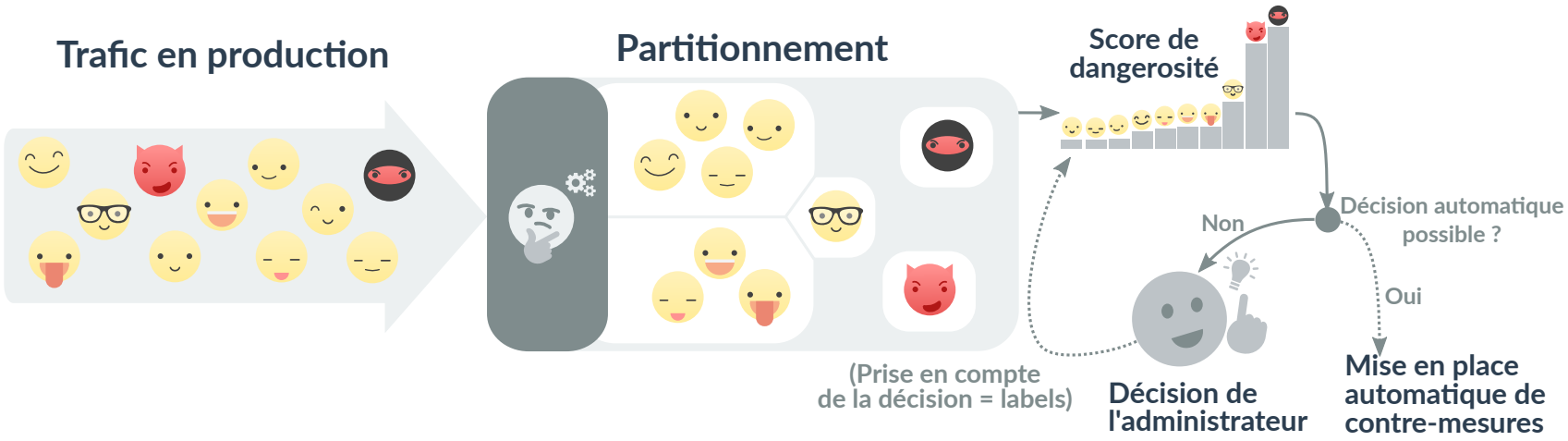
Détection non supervisée

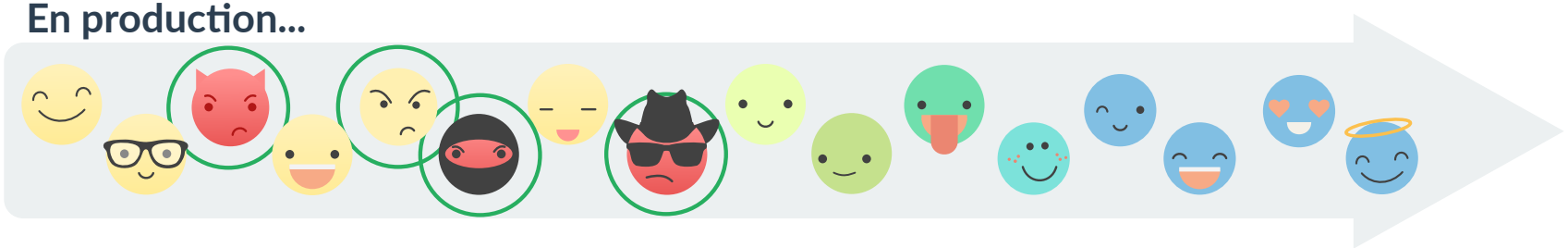




- ✓ Nécessite peu ou pas d'intervention de l'administrateur, autonome dans la plupart des cas,
- ✓ Peut détecter des anomalies inconnues,
- ✓ Extrait automatiquement les caractéristiques de chaque classe de trafic ⇒ Peut produire automatiquement des règles de filtrage,
- ✗ Peut être gourmande en ressources de calcul, suivant l'algorithme utilisé et les données d'entrée.

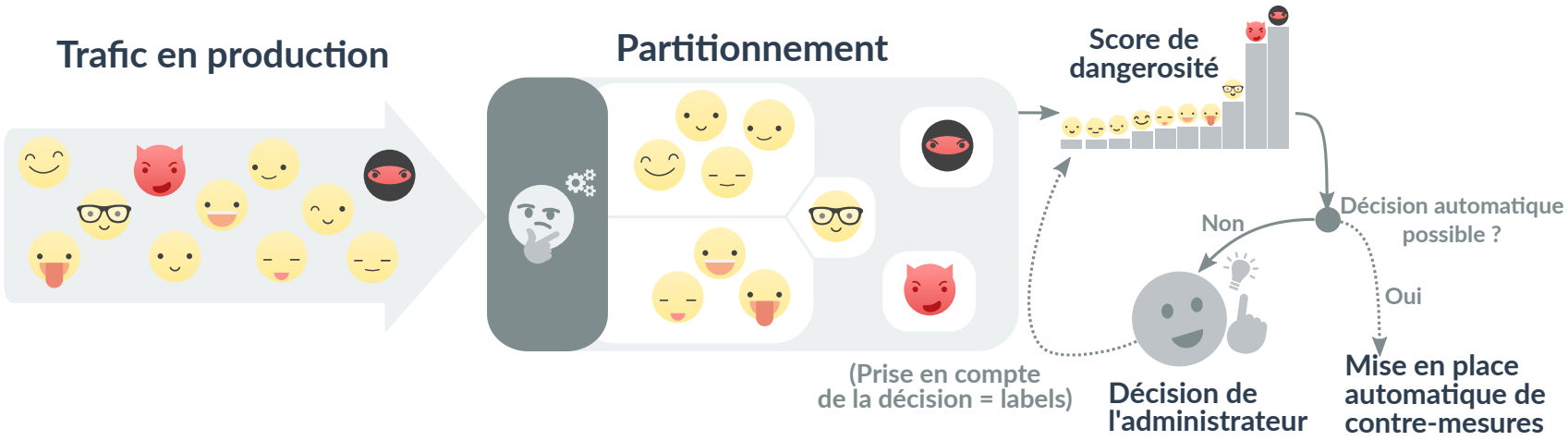
Détection non supervisée

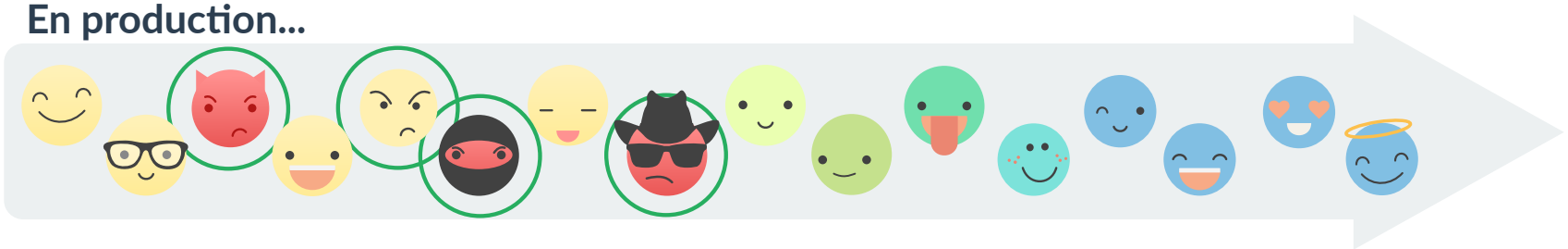




- ✓ Nécessite peu ou pas d'intervention de l'administrateur, autonome dans la plupart des cas,
- ✓ Peut détecter des anomalies inconnues,
- ✓ Extrait automatiquement les caractéristiques de chaque classe de trafic ⇒ Peut produire automatiquement des règles de filtrage,
- ✗ Peut être gourmande en ressources de calcul, suivant l'algorithme utilisé et les données d'entrée.

Détection non supervisée

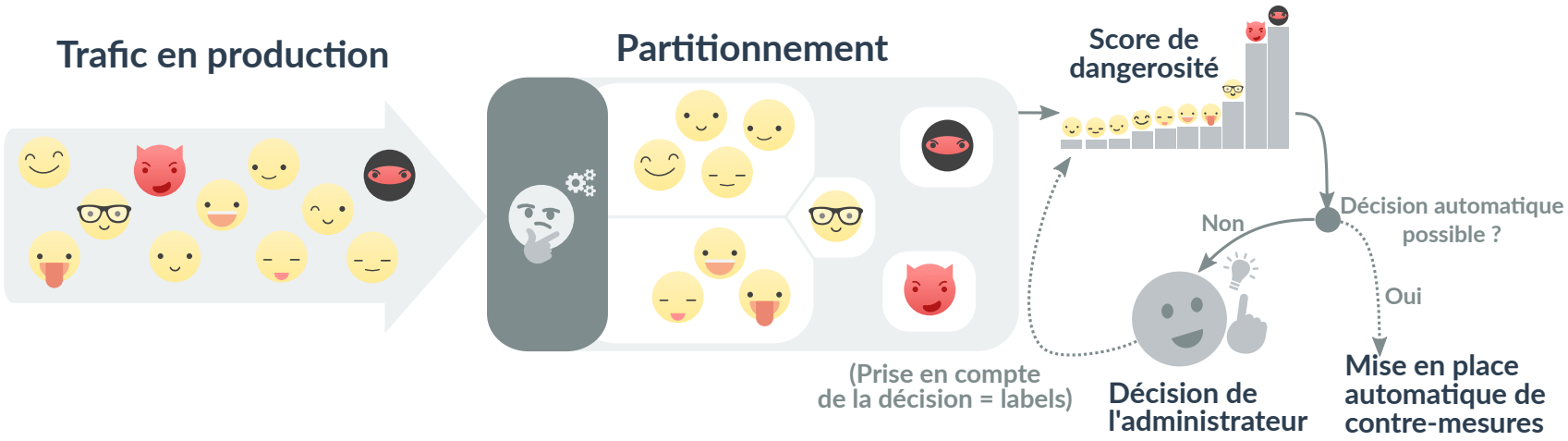


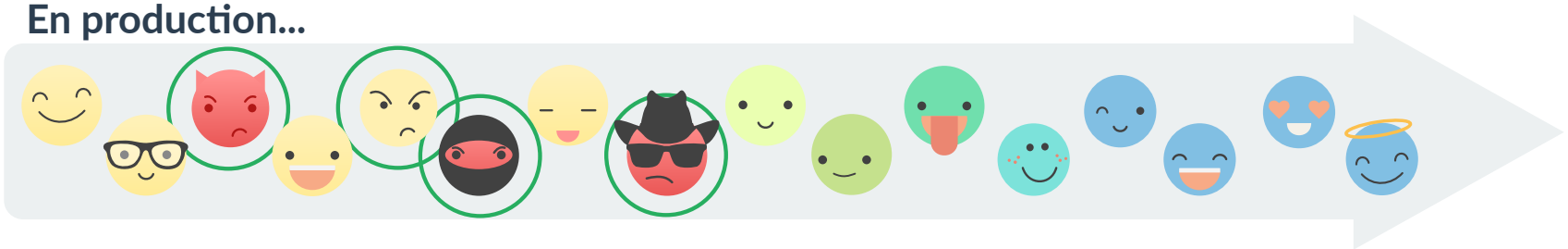


- ✓ Nécessite peu ou pas d'intervention de l'administrateur, autonome dans la plupart des cas,
- ✓ Peut détecter des anomalies inconnues,
- ✓ Extrait automatiquement les caractéristiques de chaque classe de trafic ⇒ Peut produire automatiquement des règles de filtrage,

- ✗ Peut être gourmande en ressources de calcul, suivant l'algorithme utilisé et les données d'entrée.

Détection non supervisée

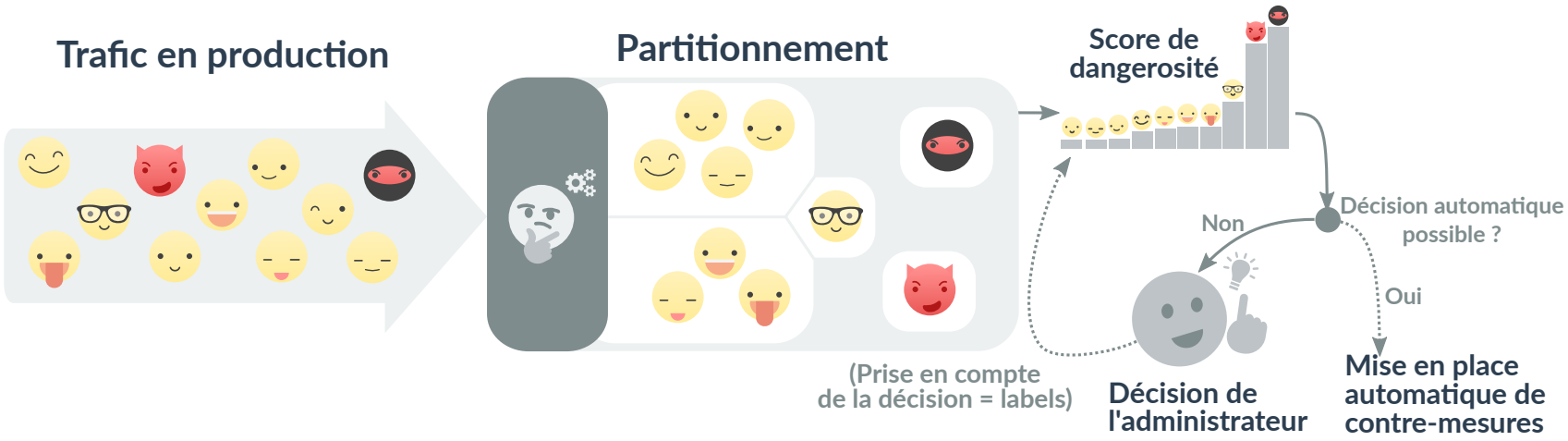


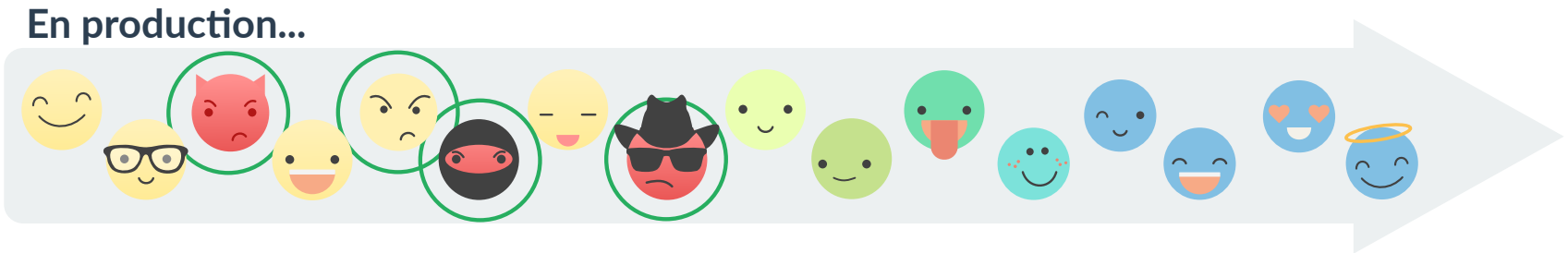


- ✓ Nécessite peu ou pas d'intervention de l'administrateur, autonome dans la plupart des cas,
- ✓ Peut détecter des anomalies inconnues,
- ✓ Extrait automatiquement les caractéristiques de chaque classe de trafic ⇒ Peut produire automatiquement des règles de filtrage,

- ✗ Peut être gourmande en ressources de calcul, suivant l'algorithme utilisé et les données d'entrée.

Détection non supervisée



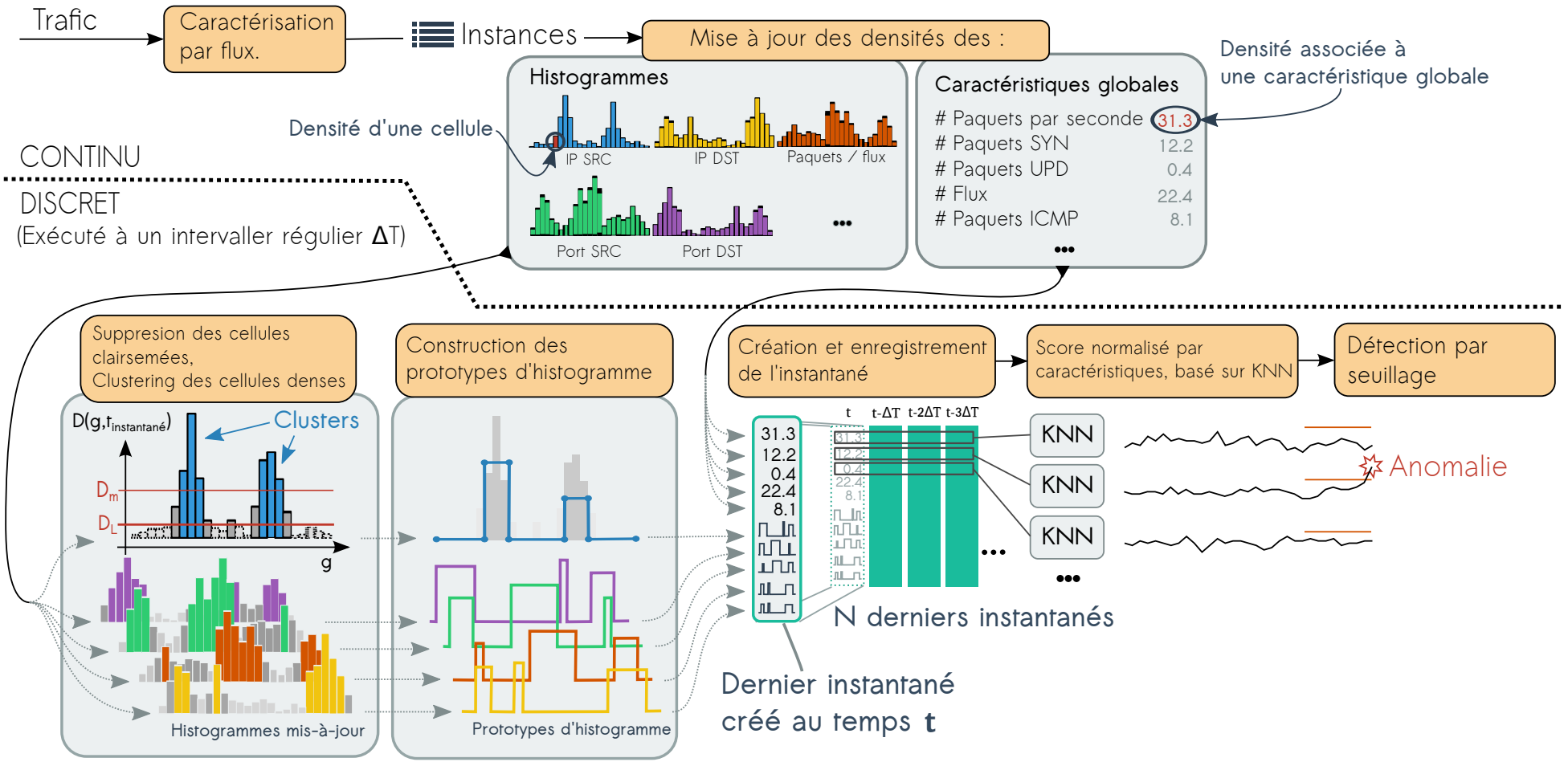


- ✓ Nécessite peu ou pas d'intervention de l'administrateur, autonome dans la plupart des cas,
- ✓ Peut détecter des anomalies inconnues,
- ✓ Extrait automatiquement les caractéristiques de chaque classe de trafic ⇒ Peut produire automatiquement des règles de filtrage,
- ✗ Peut être gourmande en ressources de calcul, suivant l'algorithme utilisé et les données d'entrée.

Objectifs de l'algorithme AATAC

- Une détection autonome (donc non supervisée),
- Nécessitant peu de ressources de calcul,
- Produisant des résultats simples à intepréter.

L'algorithme AATAC



Video

Evaluation : Banc de test

- Implémention en C,
- Extraction des flux par lots de 1 seconde, basée sur *libpcap*,
  $\Longrightarrow$ *Notement pour travailler sur des traces hors ligne*
- 3.00GHz Intel Xeon CPU (E5-2623 v3).
  8 cœurs (16 avec l'hyper-threading)
- Traitement discret parallélisé, par caractéristique du trafic analysée.

Evaluation : deux jeux de données

SynthONTS :

- Traces réelles sans la charge utile, 3Gb/s en moyenne,
- Un ensemble complet d'anomalies générées,
- Plusieurs type de DDoS.

Evaluation : deux jeux de données

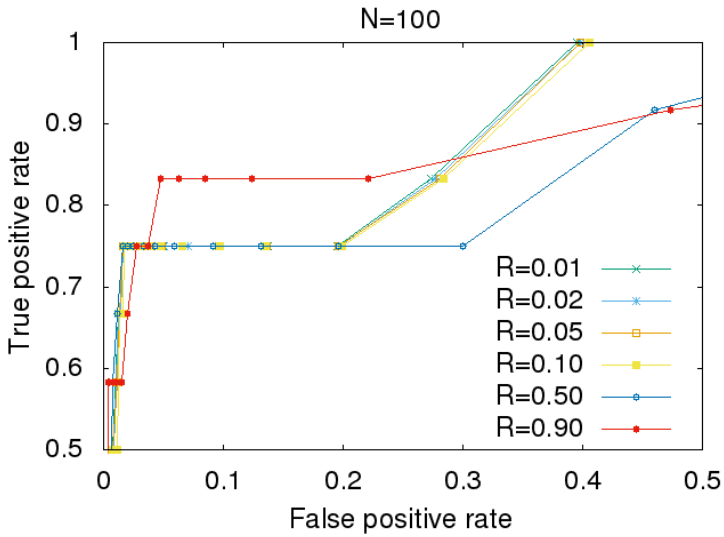
SynthONTS :

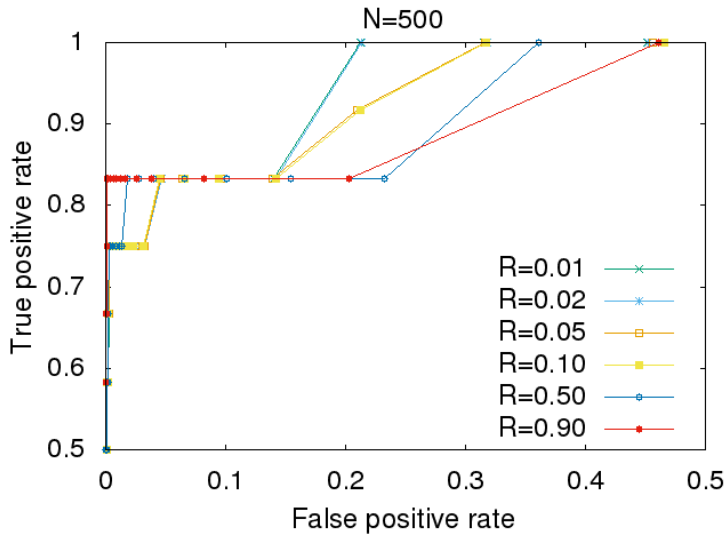
- Traces réelles sans la charge utile, 3Gb/s en moyenne,
- Un ensemble complet d'anomalies générées,
- Plusieurs type de DDoS.

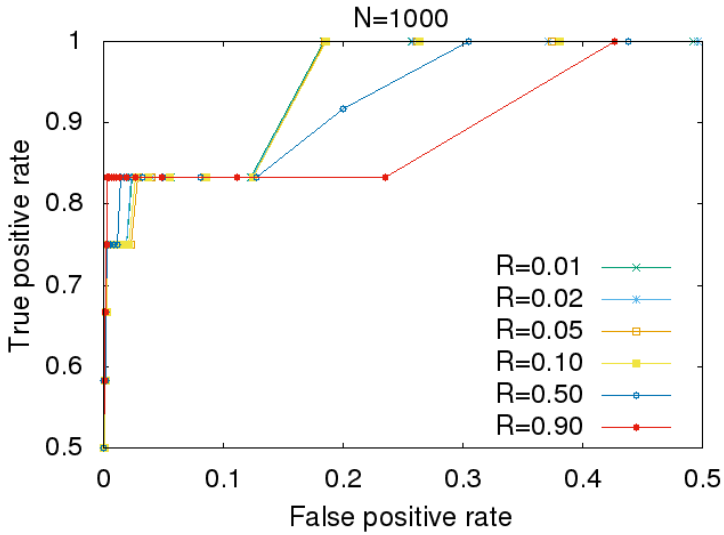
Kering :

- Traces réelles sans la charge utile, 3Gb/s en moyenne,
- Essentiellement du trafic web,
- Plusieurs jours de traces, contenant une attaque DDoS atténuée.

Evaluation : courbes ROC







Résultats dans la meilleure configuration :

Taux de vrais positifs : 0.83

Taux de faux positifs : 0.0013

Evaluation

Temps réel :

0.20s pour traiter 1s de trafic

Evaluation

Temps réel :

0.20s pour traiter 1s de trafic

Comparaison avec d'autres outils :

	Type	Temps réel	Détection
FastNetMon	Signatures	3× plus lent	6 / 13 et 1 FP
ORUNADA	Non-supervisé	10× plus lent	13 / 13

Conclusion et travaux futurs

Une détection :

- Efficace,
- Robuste et temps réel,
- Autonome,
- Produisant des signatures automatiquement, ou à défaut, des résultats simples à interpréter,
- Avec un algorithme public et publié.

Conclusion et travaux futurs

Une détection :

- Efficace,
- Robuste et temps réel,
- Autonome,
- Produisant des signatures automatiquement, ou à défaut, des résultats simples à interpréter,
- Avec un algorithme public et publié.

Conclusion et travaux futurs

Une détection :

- Efficace,
- Robuste et temps réel,
- Autonome,
- Produisant des signatures automatiquement, ou à défaut, des résultats simples à interpréter,
- Avec un algorithme public et publié.

Conclusion et travaux futurs

Une détection :

- Efficace,
- Robuste et temps réel,
- Autonome,
- Produisant des signatures automatiquement, ou à défaut, des résultats simples à interpréter,
- Avec un algorithme public et publié.

Conclusion et travaux futurs

Une détection :

- Efficace,
- Robuste et temps réel,
- Autonome,
- Produisant des signatures automatiquement, ou à défaut, des résultats simples à interpréter,
- Avec un algorithme public et publié.

Conclusion et travaux futurs

Une détection :

- Efficace,
- Robuste et temps réel,
- Autonome,
- Produisant des signatures automatiquement, ou à défaut, des résultats simples à interpréter,
- Avec un algorithme public et publié.

Conclusion et travaux futurs

Une détection :

- Efficace,
- Robuste et temps réel,
- Autonome,
- Produisant des signatures automatiquement, ou à défaut, des résultats simples à interpréter,
- Avec un algorithme public et publié.

Pour le futur :

- Evaluer AATAC sur du trafic échantillonné,
- Rédiger et soutenir ma thèse.

Conclusion et travaux futurs

Une détection :

- Efficace,
- Robuste et temps réel,
- Autonome,
- Produisant des signatures automatiquement, ou à défaut, des résultats simples à interpréter,
- Avec un algorithme public et publié.

Pour le futur :

- Evaluer AATAC sur du trafic échantillonné,
- Rédiger et soutenir ma thèse.

Conclusion et travaux futurs

Une détection :

- Efficace,
- Robuste et temps réel,
- Autonome,
- Produisant des signatures automatiquement, ou à défaut, des résultats simples à interpréter,
- Avec un algorithme public et publié.

Pour le futur :

- Evaluer AATAC sur du trafic échantillonné,
- Rédiger et soutenir ma thèse.

Questions ?