Comprendre les contextes IPS : HEADER vs BODY dans FortiGate

1. Qu'est-ce qu'un header ?

Le header (ou entête) est la partie supérieure d'un message réseau (comme HTTP, SMTP, FTP...), contenant des informations de contrôle, de routage ou de session. Il ne contient pas les données utiles, mais des instructions utilisées par les navigateurs, serveurs ou proxies.

Exemples courants dans un header HTTP :

- - User-Agent
  - Host
  - Content-Type
  - Authorization
  - WWW-Authenticate

Exemple :

GET /index.html HTTP/1.1
Host: example.com
User-Agent: Mozilla/5.0
Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==

2. Qu'est-ce que le body ?

Le body (ou corps) est la partie inférieure du message, contenant les données utiles. Cela inclut les contenus HTML, les fichiers transmis, les données POST, etc.

Exemple :

POST /login HTTP/1.1
Host: example.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 27

username=admin&password=123

3. Comment identifier le header ou le body dans Wireshark ?

Étapes :

- - Lancez Wireshark
  - Appliquez un filtre HTTP : http
  - Cliquez sur un paquet, ouvrez l'onglet "Hypertext Transfer Protocol"
  - Repérez les lignes : celles avant la ligne vide sont le header, celles après sont le body

4. Contextes IPS FortiGate

Principaux contextes :

- - header : analyse des entêtes
  - body : analyse des données utiles
  - uri : analyse des chemins HTTP
  - raw : analyse complète du paquet
  - filename : analyse des noms de fichiers transmis

5. Bonnes pratiques

À respecter lors de la création d'une signature personnalisée IPS :

- - Toujours ajouter --no_case sauf si la casse est importante
  - Copier exactement les motifs vus dans Wireshark
  - Choisir le bon contexte selon la position du motif
  - Rédiger une description claire pour les logs
  - Adapter la sévérité selon le risque

Résumé pédagogique

• Le header contient les informations de contrôle (avant la ligne vide)
• Le body contient les données utiles (après la ligne vide)
• Dans Wireshark, utilisez les filtres HTTP pour repérer header et body
• Le bon contexte IPS est essentiel pour détecter les menaces
• Une analyse précise précède toujours une signature efficace