🎓 Formation Udemy – Différences entre IPS et DoS Policy dans FortiGate (SSH Brute Force)

Dans cette section de la formation, nous allons comparer deux mécanismes de protection dans FortiGate pour contrer les attaques par force brute SSH : le système de prévention d'intrusion (IPS) et la politique de déni de service (DoS Policy). Chacun a ses forces et ses limites, et une utilisation combinée offre une défense optimale.

📊 Tableau comparatif IPS vs DoS Policy (Brute Force SSH)

Critère	IPS (Prévention d'intrusion)	DoS Policy (Détection d'anomalies réseau)
Couche OSI	L4–L7 (comprend SSH)	L3–L4 (trafic réseau brut)
Détection lente	✅ Oui (via rate-count, signatures)	❌ Non
Détection rapide	✅ Oui	✅ Oui
Inspection du contenu	✅ Oui, comprend les échanges SSH	❌ Non
Signature spécifique SSH	✅ ssh.brute.force	❌ Aucune, seulement TCP/UDP générique
Réaction contextualisée	✅ Action, log, quarantaine	❌ Blocage basique uniquement
Support quarantaine IP	✅ Oui (via IPS sensor)	✅ Oui (via DoS + expiry)
Complexité de config	Moyenne à élevée	Faible
Cas typique	Hydra, Ncrack, Medusa (brute force ciblé)	SYN Flood, scan de ports rapide
Utilisation recommandée	🎯 Détection précise SSH	🛡 Filet de sécurité volume

☑ Recommandation pédagogique

Dans un scénario de test ou en production, il est recommandé de :
- Activer un capteur IPS avec signature `ssh.brute.force` bien configurée (rate-count, log, reset/quarantine)
- Compléter par une DoS Policy ciblée sur le port SSH avec seuil bas (ex: 5 SYN/s) et quarantaine automatique

En combinant les deux, vous couvrez à la fois les attaques furtives lentes (via IPS) et les agressions massives (via DoS).