















Tableau explicatif – Politiques DoS

 Nom (FR / EN)	 Description	 Exemple	 Utilité	 Recommandation
ip_src_session (Sessions source IP)	Limite le nombre de sessions ouvertes depuis une même IP source, tous protocoles confondus.	Une IP infectée tente d'ouvrir 500 connexions TCP, UDP et ICMP vers un serveur.	Bloque les attaques multi-protocole d'un seul client.	 Activer avec un seuil modéré (ex: 20-50).
ip_dst_session (Sessions destination IP)	Limite les connexions vers une IP cible.	Plusieurs attaquants envoient des requêtes vers une même IP publique.	Protection anti-DDoS vers un serveur critique.	 Activer pour surveiller une IP sensible (Web, Mail, etc.)
tcp_syn_flood	Détecte un SYN Flood (demande de connexions TCP sans finaliser).	Attaque en masse de paquets TCP SYN vers un port 80.	Empêche de saturer la pile TCP du serveur.	 Recommandé avec un seuil > 50/s
tcp_port_scan	Détecte le scan de ports TCP.	Utilisation de nmap -sT ou masscan sur une cible.	Empêche la reconnaissance avant attaque.	 Activer si trafic sensible ou serveur exposé
tcp_src_session	Limite les sessions par IP source via TCP uniquement.	Une IP établit trop de connexions HTTP rapidement.	Complément à ip_src_session mais plus précis.	 Activer (ex: 10-20)
tcp_dst_session	Limite les sessions TCP vers une IP cible.	Plusieurs IP ciblent un serveur Web simultanément.	Protection du service ciblé.	 Recommandé pour serveur Web
udp_flood	Détecte un flood UDP (paquets massifs vers un port).	Attaque sur le port DNS (53) ou VoIP.	Préserve les ressources de la cible.	 Activer avec seuil 50-100/s
udp_scan	Détecte un scan de ports UDP.	nmap -sU vers un hôte.	Empêche les reconnaissances réseau.	 Activer si services UDP utilisés
udp_src_session	Limite les	Un client	Précision sur	 Activer si

	sessions UDP par IP source.	envoie beaucoup de requêtes DNS/VoIP.	abuse UDP d'un client.	usage UDP prévu
udp_dst_session	Limite les sessions UDP vers une cible.	DDoS VoIP ou DNS d'un serveur.	Contrôle le nombre de sessions entrantes.	✅ Recommandé pour serveurs UDP
icmp_flood	Détecte un flood ICMP (ping flood).	ping -f ou script ICMP flood.	Bloque les saturations de bande passante (L3).	✅ Fortement recommandé
icmp_sweep	Détecte un balayage ICMP (ping vers plusieurs hôtes).	nmap -sn 192.168.1.0/24	Empêche les découvertes réseau.	✅ Recommandé en environnement fermé
icmp_src_session	Limite ICMP par IP source.	Une machine envoie 100 pings/sec.	Affine les seuils d'abus ICMP.	✅ Utile avec icmp_flood
icmp_dst_session	Limite ICMP vers IP cible.	Plusieurs IPs attaquent un serveur avec ping flood.	Défend un hôte contre attaque ICMP distribuée.	✅ Recommandé pour IP publique
sctp_flood	Détecte un flood SCTP (rare, protocoles télécom).	Attaque SCTP sur port de signalisation.	Spécifique à certains réseaux (5G, télécom).	♦ Facultatif si SCTP n'est pas utilisé
sctp_scan	Scan de ports via SCTP.	Scanner télécom spécialisé.	Comme port_scan mais pour SCTP.	♦ À activer en environnement télécom
sctp_src_session	Limite SCTP depuis une IP source.	Voir ci-dessus.	Contrôle de l'usage SCTP.	♦ Réservé aux environnements télécom
sctp_dst_session	Limite SCTP vers une cible.	Voir ci-dessus.	Protection de serveurs SCTP.	♦ Idem