






FortiGate IPS – Actions, Status et Logging

Ce tableau présente les paramètres clés d'une entrée IPS dans un capteur FortiGate : action, statut et logging.



Paramètre : action

 Valeur	 Signification	 Comportement FortiGate
block	Bloque la session immédiatement	Session abandonnée sans réponse
reset	Réinitialise la connexion avec un RST	Fermeture brutale, visible côté attaquant
monitor	Journalise uniquement, sans bloquer	Utilisé pour l'audit ou test de règle
quarantine	Ajoute l'IP source en quarantaine	Requiert la quarantaine active globalement
default	Utilise l'action par défaut de la signature	Basé sur FortiGuard : pass, block, reset...

Paramètre : status

 Valeur	 Signification
enable	Active la signature (inspecte et logue)
disable	Ignore la signature (aucune inspection ni log)
default	Utilise le statut recommandé par FortiGuard (souvent enabled)

Paramètre : log-packet

 Valeur	 Signification
enable	Capture le paquet déclencheur (téléchargeable dans les logs)
disable	Pas de capture, uniquement les logs d'événement