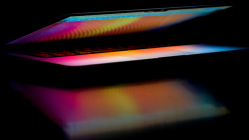


Data Sheet

WANUP 4.0



Mise à jour 7 Janvier 2026

A propos

SAYSE est l'alternative **française** en SD-WAN & SASE

Depuis 2014, SAYSE est éditeur de logiciel basé sur la connectivité et la cybersécurité des entreprises avec WANUP, une solution 100% française, conçue pour offrir simplicité, performance et sécurité. Contrairement aux solutions américaines complexes, coûteuses et dépendantes du Cloud Act, SAYSE propose une approche simple et souveraine :

SD-WAN & SASE unifiés : des équipements autonomes installés sur site, pilotés via une gestion centralisée dans un cloud français.

Cybersécurité intégrée : ZTNA, Firewall, IPS/IDS, filtrage avancé... tout est natif et inclus, sans surcoût.

Performances optimisées : WANUP exploite la sortie Internet locale et le routage intelligent pour un réseau plus rapide et plus fiable.

Notre approche

La solution WANUP intègre une plateforme SaaS de gestion centralisée et simplifiée des réseaux d'entreprise et de sécurité informatique.

Elle est également constituée d'équipements SD-WAN (disponibles sous forme physique ou virtuelle) et offre une protection complète contre les cyber-menaces grâce à sa technologie avancée de détection et de prévention des intrusions.

Elle permet aux entreprises de travailler en toute sécurité et de se concentrer sur leur cœur de métier.

Agréments



United Nations
Global Compact

Gamme d'équipements

	W-G6	W-G4X2	Machine Virtuelle
Processeur	Intel Core i3-8145U - 2,10 GHz	Intel Core i5-1245U - 4,4 GHz	-
Cache	4 Mo	12 Mo	-
Coeurs	2 cores 4 threads	10 cores 12 threads	-
vCPU	-	-	4 recommandés
Ram	4 Go SO-DIMM DDR4	8 Go SO-DIMM DDR5	4 Go recommandés
Disque	SSD 64 Go	SSD 128 Go	10 Go minimum
Interfaces réseau	6 RJ45 x 1Gbps	4 RJ45 x1Gbps + 2 SFP+ x 10Gbps	De 1 à 4
Module optique	Non concerné	Non fourni	Non concerné
Alimentation	DC 12V 5A	DC 12V 8A	-
Poids	2 Kg	2 Kg	-
Format	-	-	x86 64bit image
Hyperviseurs	-	-	VMware - Hyper V - KVM
Dimension	210 x 160 x 60 mm	160 x 140 x 60 mm	-
CE	Oui	Oui	-

W-G6



W-G4X2



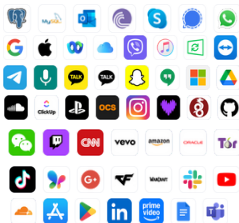
Compatibilité Cloud



Intégration



+ de 200 Apps reconnues



Fonctionnalités clés

Routages avancés - Fail Over

Le Failover WANUP assure une connexion ininterrompue en basculant automatiquement sur une liaison de secours en cas de panne. Il surveille en temps réel l'état des connexions et détecte toute anomalie en quelques secondes. Lorsqu'une liaison est dégradée ou hors service, le trafic est immédiatement redirigé vers la meilleure connexion disponible. Une fois la connexion principale rétablie, le retour se fait automatiquement sans intervention manuelle. Cette haute disponibilité garantit un accès stable et sécurisé aux services cloud et aux applications critiques. WANUP optimise les performances en réduisant l'impact des interruptions sur l'activité. Il est compatible avec les infrastructures multi-opérateurs et multi-technologies comme la fibre, la 4G, la 5G ou le satellite. Sa gestion avancée du Failover assure une continuité de service même en environnement hétérogène. Avec WANUP, bénéficiez d'un réseau résilient, fiable et performant.

Routages avancés - Load balancing

Le Load Balancing WANUP répartit intelligemment le trafic entre plusieurs liaisons Internet de même technologie et débit. Il évite les engorgements, améliore la réactivité du réseau et garantit une connectivité fluide, même en période de forte demande. Chaque connexion entrante est analysée et orientée vers la liaison la plus performante en temps réel. Grâce à des algorithmes avancés, le trafic est équilibré selon la capacité et la disponibilité des liens. Cette gestion dynamique optimise l'utilisation des ressources et évite les goulots d'étranglement. La haute disponibilité assure un accès constant aux services cloud et aux applications critiques. WANUP adapte automatiquement le routage du trafic pour une stabilité et une performance maximales. Cette solution est idéale pour les entreprises disposant de plusieurs liaisons homogènes. Avec WANUP, bénéficiez d'un réseau performant, fluide et résilient.

Qos Applicative

Le service de QoS applicative WANUP optimise le trafic en classant et priorisant automatiquement les flux selon leur importance métier. Il reconnaît plus de 200 applications et assure une gestion fluide même en cas de congestion. Les services critiques comme la voix et la visioconférence bénéficient d'une priorité maximale pour garantir une expérience utilisateur optimale. Chaque paquet est analysé, marqué et traité dynamiquement en fonction de sa classe de service. WANUP intègre une base enrichie de protocoles et applications, avec la possibilité de personnaliser les règles en fonction des IP, ports et domaines spécifiques. La configuration est flexible, s'appliquant par interface WAN ou globalement sur l'Appliance SD-WAN. Grâce à une reconnaissance avancée des protocoles, le trafic est géré de manière précise et performante. Avec WANUP, maîtrisez votre réseau pour une connectivité fluide et sécurisée.

Firewall As A Service

Le Firewall as a Service (FWaaS) WANUP offre une protection réseau robuste et flexible grâce à son intégration native dans notre UTM (Unified Threat Management). Il contrôle le trafic, détecte les intrusions, filtre le web et sécurise les applications contre les menaces. La gestion est centralisée, permettant un déploiement rapide des politiques de sécurité via un système de modèles. Toute modification est appliquée instantanément à l'ensemble des équipements SD-WAN, garantissant une mise à jour continue et uniforme. Contrairement aux solutions cloud, le traitement de sécurité est effectué localement, assurant une réactivité optimale. La surveillance en temps réel bloque immédiatement toute activité suspecte sans installation supplémentaire. WANUP simplifie la sécurité en l'intégrant directement dans son infrastructure, garantissant une protection efficace et évolutive.

IPS/IDS

Le système IDS/IPS WANUP protège votre réseau en détectant et bloquant les tentatives d'intrusion en temps réel. Il analyse le trafic via une détection par signatures et une analyse comportementale, permettant d'identifier les menaces connues et les activités suspectes. Une surveillance continue repère les anomalies avant qu'elles ne compromettent votre infrastructure. La gestion centralisée offre un suivi détaillé et une personnalisation des règles de sécurité. Les alertes sont classées par niveau de gravité et transmises via plusieurs canaux pour une réactivité immédiate. WANUP garantit une protection avancée et évolutive, capable d'anticiper et de neutraliser les cybermenaces avant qu'elles n'impactent votre activité.

Secure Web Gateway

Le Secure Web Gateway (SWG) WANUP sécurise l'accès à Internet en bloquant les sites malveillants et en filtrant le trafic en temps réel. Il empêche l'accès aux sites non sécurisés, réduisant les risques liés aux cyberattaques et au phishing. Grâce à une base de données enrichie et mise à jour régulièrement, il identifie et neutralise les menaces avant qu'elles n'atteignent les utilisateurs. Le moteur de filtrage catégorise précisément les sites pour appliquer des restrictions adaptées aux politiques de l'entreprise. WANUP filtre également les connexions HTTPS via le SNI, garantissant un contrôle strict sans altérer la confidentialité. Cette solution assure un usage sécurisé et conforme du web, que les utilisateurs soient au bureau ou en mobilité. Avec WANUP, la navigation est fluide, protégée et totalement maîtrisée.

VPN Remote

Le client VPN WANUP, basé sur WireGuard, offre une connexion sécurisée et chiffrée pour les télétravailleurs et les utilisateurs mobiles. Il garantit une latence réduite et des performances optimales, tout en assurant un haut niveau de protection des communications. L'installation est rapide sur Mac et Windows, avec une gestion centralisée simplifiant le déploiement des politiques de sécurité. Grâce à la fonction "Always On", l'utilisateur est protégé dès son authentification. Avec WANUP, la connexion est fluide, fiable et totalement sécurisée, quel que soit l'endroit où vous travaillez.

IP Toxiques

Le module Toxic IPs WANUP bloque les connexions avec des adresses IP malveillantes, identifiées via des bases de données mises à jour en temps réel. Il analyse le trafic entrant et sortant pour détecter toute communication suspecte et alerter les administrateurs. Chaque entreprise peut ajuster sa politique de filtrage : surveillance passive, blocage préventif ou rejet strict des IPs classées dangereuses. Les règles peuvent être personnalisées selon le contexte métier, permettant par exemple d'exclure certains pays ou d'autoriser des flux spécifiques. Cette fonctionnalité complète l'IDS/IPS en empêchant les menaces connues d'accéder au réseau. Avec WANUP, la protection est dynamique, évolutive et sans impact sur les performances.

Fonctionnalités

	P1 SOWAN	P2 CYBER+	P3 SASE
Services IP & Routage			
Aggrégations (Bond / Bridge)	✓	-	✓
DHCP client/serveur/relai	✓	✓	✓
IP par nom de domaine (FQDN)	✓	✓	✓
IP Statique/Dynamique	✓	✓	✓
Policy Based Routing	✓	-	✓
PPPoE	✓	✓	✓
QoS par application (+200)	✓	-	✓
QoS personnalisée (IP/Port)	✓	-	✓
Routage dynamique (BGP/OSPF)*	✓	-	✓
Routage statique	✓	✓	✓
Table ARP	✓	✓	✓
Test de bande passante par WAN	✓	✓	✓
vLAN (802.1q)	✓	✓	✓
Vpn & Accès distants			
Authentification VPN nomade par LDAP	✓	✓	✓
Authentification VPN nomade par Radius	✓	✓	✓
Authentification VPN nomade par SSO*	✓	✓	✓
AlwaysOn / VPN auto-reconnect	✓	✓	✓
Client VPN Smartphone*	✓	✓	✓
Client VPN (Mac/PC)	✓	✓	✓
Interconnexions SD-WAN	✓	-	✓
IPSec	✓	✓	✓

*Disponibilité en fin d'année

Fonctionnalités

	P1 SDWAN	P2 CYBER+	P3 SASE
Haute disponibilité			
Compatibilité multi-opérateurs	✓	✓	✓
Compatibilité multi-technologies	✓	✓	✓
Cluster Actif / Passif (Fonction HA)*	Option NA	Option NA	Option NA
Fail Over	✓	✓	✓
Load Balancing	✓	✓	✓
Rapports			
Bande passante	✓	✓	✓
Gigue	✓	✓	✓
Latence	✓	✓	✓
Etat des équipements	✓	✓	✓
Logs (3 mois en ligne et 12 mois hors ligne)	✓	✓	✓
Perte de paquets	✓	✓	✓
QoS	✓	-	✓
Règles de Firewall	-	✓	✓
SNMP v1/v2c	✓	✓	✓
Traffic détaillé	✓	✓	✓
Sécurité			
Filtrage Web	-	✓	✓
Firewall Standard	✓	✓	✓
Firewall avancé (L3/L4/L7 - NAT/PAT)	-	✓	✓
IPs toxiques	-	✓	✓
IPS / IDS	-	✓	✓

Fonctionnalités

	P1 SDWAN	P2 CYBER+	P3 SASE
Management			
Accès à la console de gestion	✓	✓	✓
Accès ligne de commande	✓	✓	✓
Accès multifactoriel (2FA)	✓	✓	✓
API	✓	✓	✓
Gestion des accès à Internet	✓	✓	✓
Gestion des autorisations	✓	✓	✓
Gestion des équipements	✓	✓	✓
Gestion des stocks matériels	✓	✓	✓
Gestion des comptes utilisateurs	✓	✓	✓
Gestion Firewall et Filtrage web par modèle	-	✓	✓
Gestions des objets	✓	✓	✓
Notifications avancées des incidents	✓	✓	✓
Rapport de connexions à l'interface	✓	✓	✓
Rapport de connexions Vpn	✓	✓	✓
"Roll Back" des actions sur l'interface	✓	✓	✓
"Super validation" des actions	✓	✓	✓

sayse

Prêt à vous sécuriser ?

