

Authentification

- 802.1x : transparente pour l'utilisateur après paramétrage
- Portail Captif : zero configuration
- Annuaire Interne ou Externe (LDAP / Actif Directory)
- Authentification Unique (SSO) : ENT
- Portail Entièrement paramétrable (composants opensource)

Sécurisation

- Filtrage d'URL
 - Catégories (Université Toulouse 1)
 - Listes Noires / Liste blanches
- Antivirus de flux (clamav)
- Filtrage de protocoles
- Contrôles des ressources réseau
 - Routage Inter VLAN

Consultation

- Données de communication légales (journaux)
 - Cryptées
 - Archivage local ou cloud
- Statistiques de volumetrie
 - Utilisateur / Site / protocole / date

Optimisation

- Gestion des ressources disponibles
 - par utilisateur / groupe d'utilisateur (enseignant, classe ..)
 - par type de ressource
 - par créneau horaire (gestion de l'emploi du temps)
- Limitation de la bande passante
 - instantanée (montante et descendante)
cumulée (par session)

Intégration

- Déploiement
 - Cloud (gestion centralisée multi-site)
 - Serveur Physique ou virtuel
- Intégration Solution Wifi
 - Cisco WLC
 - Cisco Meraki
 - Ubiquiti Unifi
- Applications tierces (SSO / LDAP)



OPTIGATE
SÉCURISER - OPTIMISER - PARTAGER

**Passerelle Filtrante
d'authentification, d'imputation
des accès et de partage des
ressources**

CONTACT

projet@avantgarde-dom.com
www.avantgarde-dom.com

UNE SOLUTION



 **AVANT GARDE**
au service de l'outre mer

Authentifier et contrôler les connexions

Optigate est positionné en coupure entre le réseau de consultation et Internet afin d'en interdire l'accès pour les usagers non authentifiés (identifiant + mot de passe). Il se comporte comme un sas d'accès pour l'ensemble des services Internet.

finement, par créneau horaire les ressources accessibles par profil d'utilisateur. Le paramétrage des ressources accessible peut également prendre en compte le lieu de consultation de l'utilisateur.



Le contrôle des connexions permet, par exemple, de définir des usagers et des groupes d'usagers autorisés à se connecter. Pour chaque usager ou groupe d'usagers, il est possible de définir des dates de fin de validité, des créneaux de connexion hebdomadaire ainsi que des durées maximales de connexion, des débits ou des volumes maximum de données téléchargeables. Il est possible de gérer



Sécurité des Systèmes d'Information

- Ce site a été mis en place pour assurer réglementairement la traçabilité, l'inséparabilité et la non-répudiation des connexions.
- Les données enregistrées ne pourront être exploitées que par une autorité judiciaire dans le cadre d'une enquête.
- Votre activité sur le réseau est enregistrée conformément au respect de la vie privée.
- Ces données seront automatiquement supprimées au bout d'un an.
- Cliquez sur le bouton pour changer votre mot de passe ou pour intégrer le certificat de sécurité à votre navigateur.

Tracer et imputer tout en protégeant la vie privée

Optigate permet aux responsables d'organismes de répondre aux exigences des politiques d'accès et d'utilisation des réseaux de consultation Internet. En France, il permet de décliner l'obligation légale de tracer et d'imputer les connexions. Ces exigences consistent à authentifier les usagers du réseau de consultation lorsqu'ils décident de se connecter sur Internet et à produire, pour chacun d'eux, une trace précise de toutes les activités réalisées (consultation, téléchargement, écoute multimédia, courriel, discussion, blog, connexions chiffrées, etc.). Les données peuvent être archivées sur support externe ou sur notre plateforme cloud. Dans le cadre de la cybersurveillance et pour répondre aux exigences de la CNIL, la production de ces traces est cryptée afin d'en assurer la non-répudiation et afin de garantir la protection de la vie privée.

Sécuriser le réseau de consultation

Optigate intègre un pare-feu et un antivirus de flux WEB afin de protéger les équipements du réseau de consultation des menaces externes directes. Il comporte également un module permettant d'éviter l'usurpation d'adresses MAC et d'adresses IP afin de protéger les usagers authentifiés des tentatives d'un utilisateur interne cherchant à usurper leurs sessions.

Les mises à jour de sécurité des équipements de consultation (antivirus mises à jours systèmes) sont automatisables.

Protéger les usagers

Afin de protéger les usagers authentifiés, Optigate met en œuvre plusieurs dispositifs de filtrage qui ont entre autre surtout été élaborés pour les organismes susceptibles d'accueillir un jeune public :

- Le premier permet de bloquer l'accès aux sites dont le contenu est jugé répréhensible ou non-conforme (liste noire). Il est entièrement paramétrable (activation, désactivation, ajout ou retrait de sites, etc.) par catégorie de sites et par profil d'utilisateur.
- Le deuxième active la fonction 'safesearch' des principaux moteurs de recherche. Cette fonction permet d'exclure du résultat des recherches le contenu réservé aux adultes.
- Le troisième permet de bloquer tout trafic autre que le trafic WEB et de n'activer que les services réseau désirés (Web sécurisé « HTTPS », courriel « SMTP/POP », etc.).

Optimiser l'utilisation de la bande passante disponible

Optigate dispose de plusieurs mécanismes permettant d'optimiser l'utilisation de la bande passante afin que la bande passante disponible soit utilisée aux mieux par tous.

Définition des ressources disponibles par profil : il est possible de bloquer les contenus fort consommateurs de bande passante (video, contenus multimédias) ou ayant peu d'utilité professionnelle ou pédagogique (réseau sociaux ...) et de réserver leur usage à des groupes d'utilisateurs ayant réellement besoins de ces contenus.

Définition des ressources disponibles par plage horaire : Optigate permet d'octroyer ponctuellement ou suivant un calendrier prédéfinis des droits d'accès supplémentaires pour chaque groupe d'utilisateurs.

Par exemple :

- N'autoriser certains sites que pendant la pause de midi.
- Bloquer les contenus multimédia pendant les heures de pointes sauf le mercredi ...

Une solution unique et packagée regroupant l'ensemble des besoins matériels, logiciels et services pour un réseau wifi sécurisé et à haute disponibilité.