académie Bordeaux

Direction des Systèmes d'Information

RÉGION ACADÉMIQUE
NOUVELLE-AQUITAINE

MINISTÈRE
DE L'ÉDUCATION NATIONALE,
DE L'ENSEIGNEMENT SUPÉRIEUR
ET DE LA RECHERCHE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Référentiel académique d'exigences de sécurité applicable dans les établissements scolaires

Version 2017.1 / Février 2017

SOMMAIRE

Statut du document

Date	Auteur	N° version	Description des modifications
23/12/2016	RSSI	V.0.1	Version initiale
20/01/2017	RSSI	V.0.2	Version corrigée par le directeur des affaires juridiques
31/01/2017	RSSI	V.0.3	Modification de la page 9
06/02/2017	RSSI	V.0.4	Modification de la page 24
14/02/2017	RSSI	V.2017 .1	Validation par l'AQSSI

Contexte et cadre réglementaire

Le présent référentiel d'exigences de sécurité est établi par l'autorité qualifiée pour la sécurité des systèmes d'information en la personne du recteur d'académie en vue de procurer aux collectivités territoriales de l'académie de Bordeaux un cadre de référence leur permettant d'opérer les choix d'architecture technique des établissements scolaires au regard de la loi d'orientation et de programmation pour la refondation de l'école de la République du 8 juillet 2013, en garantissant la sécurité des systèmes d'information et la protection des mineurs.

La politique de sécurité du système d'information académique repose sur l'ensemble juridique suivant:

- Loi informatique et liberté loi 78-17 du 6 janvier 1978 modifiée
- Loi n° 2004-575 du 21 juin 2004 – article 6-I 1
- les lois dites « anti-terroristes » n°2006-64 du 23 janvier 2006 et n° 2008-1245 du 1er décembre 2008 et décret n°2006-358 du 24 mars 2006
- Loi HADOPI - Article de référence : code de la propriété intellectuelle L.336-3.
- le Référentiel Général de Sécurité (RGS), défini dans le cadre de l'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et de ses évolutions ultérieures
- le décret n°2010-112 du 2 février 2010,
- l'arrêté du premier ministre du 13 juin 2014 portant approbation du RGS ;
- la circulaire du premier ministre en date du 17 juillet 2014 fixant la PSSI de l'Etat
- les recommandations de la Commission Nationale de l'Informatique et des Libertés
- les recommandations de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

Le présent document est révisé annuellement en comité de sécurité des systèmes d'information. Il peut toutefois faire l'objet d'avenants ponctuels en cas d'urgence à tout moment sur décision de l'AQSSI.
La version numérique à jour est disponible en ligne : http://ssi.ac-bordeaux.fr

Responsabilités des acteurs

La loi n° 2013-595 du 8 juillet 2013 d'orientation et de programmation pour la refondation de l'école de la République s'est attachée, en ses articles 19, 21 et 23, à clarifier, sans la modifier, la répartition des compétences entre l'Etat et les collectivités territoriales en matière d'équipement informatique des établissements scolaires du second degré, et notamment en matière d'acquisition et de maintenance de ces équipements, telle qu'elle résulte des premières lois de décentralisation, bien avant le développement et la banalisation des outils numériques dans la vie courante des établissements scolaires.

Ainsi, au titre de l'équipement et du fonctionnement des collèges, qui relèvent de sa compétence depuis 1983 en vertu de l'article L. 213-2 du code de l'éducation, le Département a la charge de l'ensemble des dépenses informatiques, matérielles ou logicielles, qui sont nécessaires au fonctionnement régulier de l'établissement et au bon déroulement de la scolarité des élèves, y compris de la maintenance de ces matériels et logiciels, laquelle est d'ailleurs fréquemment intégrée dans les marchés passés en vue de leur acquisition.

Ainsi, au titre de l'équipement et du fonctionnement des lycées, qui relèvent de sa compétence depuis 1983 en vertu de l'article L. 214-6 du code de l'éducation, la région a la charge de l'ensemble des dépenses informatiques, matérielles ou logicielles, qui sont nécessaires au fonctionnement régulier de l'établissement et au bon déroulement de la scolarité des élèves, y compris de la maintenance de ces matériels et logiciels, laquelle est d'ailleurs fréquemment intégrée dans les marchés passés en vue de leur acquisition.

A cet égard, les espaces numériques de travail (ENT) font partie des « matériels informatiques et logiciels (..) nécessaires (..) aux échanges entre les membres de la communauté éducative », que mentionne les articles L. 213-2 et L. 214-6 du code de l'éducation, et comptent ainsi parmi les dépenses à la charge des départements et des régions.

Dans ce cadre, les charges relevant de la collectivité ne concernent que les infrastructures propres des établissements. Les applications « nationales », c'est-à-dire les applications informatiques mises à disposition de l'ensemble des établissements par le ministère (par exemple pour les actes de gestion financière ou de ressources humaines) ne rentrent pas dans ce cadre.

Les charges relevant de la collectivité portent sur tous les aspects des infrastructures : équipements actifs réseaux, matériels de sécurité, serveurs de données, terminaux. Les matériels et dispositifs de sécurité en font partie, puisqu'ils sont indispensables au bon fonctionnement des infrastructures et équipements.

La collaboration entre l'académie et les collectivités territoriales est essentielle en matière de sécurité, dans la mesure où la politique de sécurité des systèmes d'information doit prendre en compte les exigences et contraintes de tous les utilisateurs dans les différents secteurs intéressant la vie de l'établissement : pédagogie, gestion, échanges entre les membres de la communauté éducative.

A cet égard, il convient de rappeler que, dans les collèges et les lycées, le chef d'établissement, en qualité de représentant de l'État, « prend toutes dispositions, en liaison avec les autorités administratives compétentes, pour assurer la sécurité des personnes et des biens, l'hygiène et la salubrité de l'établissement », conformément aux dispositions du 3° de l'article R. 421-10 du code de l'éducation. Il est chargé, à ce titre, de prendre des mesures générales de prévention et d'organisation du service public de l'éducation garantissant la sécurité, y compris en matière informatique. Les dispositions qui précèdent ont été affirmées à travers l'éclairage juridique de la DAJ du ministère à plusieurs reprises.

L’autorité hiérarchique qualifiée en Responsable de la Sécurité des Systèmes d’Information (RSSI) est juridiquement responsable de la sécurité des systèmes d’information de ses entités et du respect des réglementations. Dans l'établissement scolaire, le chef d'établissement est la personne juridiquement responsable, il agit sous l’autorité du recteur, dénommé Autorité Qualifiée de la Sécurité des Systèmes d’Information (AQSSI).

Lorsque la collectivité assure pleinement la charge de mise en service et de maintenance des organes de sécurité de l'établissement, elle doit mettre à disposition de chaque chef d'établissement et de l’AQSSI un outillage leur permettant de vérifier librement par des audits ponctuels que les règles édictées ci-dessous sont effectivement mises en œuvre.

Chaîne d'alerte

Au niveau académique la chaîne des acteurs de la Sécurité des Systèmes d'Information se décline suivant les préconisations nationales.

Le recteur (AQSSI), conseillé par le Responsable de la Sécurité des Systèmes d'Information (RSSI), arbitre la stratégie SSI et identifie les moyens associés.

Le RSSI est nommé et mandaté par l'autorité qualifiée pour définir et veiller à la bonne réalisation de la politique de sécurité. Son rattachement direct auprès de l'AQSSI lui confère toute sa légitimité et lui permet d'assurer pleinement sa mission. Il s'appuie lui même sur une chaîne de correspondants de sécurité (CR) qu'il organise et dont il est le référent.

Le correspondant de sécurité est chargé de la mise en œuvre de la sécurité sur l'infrastructure technique (équipements de sécurité, versions logicielles, carnets d'exploitation des serveurs) et sur les dispositifs spécifiques de sécurité (filtres, sondes de détection, antivirus, …). Son domaine d'intervention couvre les établissements scolaires (gestion des fonctions et équipements de sécurité des EPLE).

La collectivité doit désigner des correspondants de sécurité et doit communiquer leurs coordonnées au RSSI lorsque intervient une nomination. En cas d'alerte signalée par le RSSI académique, les correspondants de sécurité mettent tout en œuvre pour revenir à une situation conforme aux exigences de sécurité et rendent compte de leur action à la collectivité et au RSSI simultanément.

Tout incident ou toute alerte de sécurité ou tout action conduite par un correspondant de sécurité doit faire l'objet d'un signalement sans délai par courrier électronique à l'adresse :

l.rssi@ac-bordeaux.fr

Informations des utilisateurs et chartes

Informations des utilisateurs

Il importe que les utilisateurs aient connaissance des dispositifs de traitement des informations relatives à la supervision des flux de données et des usages ainsi qu'aux restrictions d'accès à certains services du fait de contraintes de sécurité mis en place dans l'établissement scolaire.
A ce titre la collectivité produit un document explicatif à destination des chefs d'établissement destiné à être communiqué à l'ensemble de la communauté éducative (élèves, parents et personnels). Les chefs d'établissement intègrent ce document au règlement intérieur et le soumettent notamment à la signature des parents.

En complément de cette information, des chartes précisant les obligations des usagers doivent être mises en place. Elles permettent de définir les droits et les obligations des membre de la communauté éducative concernant l'utilisation des services numériques de l'établissement. Les chartes visent principalement à prévenir ou limiter d'éventuels usages abusifs et servent de référence en cas de litige porté devant la juridiction compétente.

Les chartes proposées ci-après sont à intégrer ou à annexer au règlement intérieur de l'établissement (liste non exhaustive) pour disposer d'une valeur réglementaire et être opposable aux usagers.

Charte d'usage des TIC intégrée au règlement intérieur de l'EPLE

La charte des systèmes d'information d'un établissement a pour vocation d'encadrer l'utilisation des outils et services numériques mis à disposition des utilisateurs. À ce titre, elle définit les conditions d'utilisation, les droits et les obligations des utilisateurs. C'est un document qui a une valeur juridique et qui engage l'établissement et ses utilisateurs dès lors qu'il est intégré au règlement intérieur de l'établissement.

http://eduscol.education.fr/cid57095/guide-d-elaboration-des-chartes-d-usage.html

Charte académique régissant l'usage des TIC par les personnels

La charte régissant l'usage des TIC par les personnels de l'académie est disponible sur le site Sécurité des Systèmes d'Information du rectorat de Bordeaux.

http://ssi.ac-bordeaux.fr/fileadmin/TIC-CharteDesPersonnels-19052010.pdf

Charte de l'administrateur réseau

La charte administrateur détermine les droits et devoirs des administrateurs du réseau ou des applications en ligne. Elle prend en compte le respect des obligations légales, par exemple en matière de conservation des traces, de protection de la vie privée et des données à caractère personnel. Elle fixe également un cadre déontologique qui expose clairement la distinction entre ce que l'administrateur a la possibilité de réaliser du point de vue technique, ce qu'il est autorisé à faire dans le cadre de ses missions ordinaires et ce qu'il peut être amené à faire dans des circonstances exceptionnelles. La CNIL insiste sur le fait que ce document doit rappeler l'existence et l'importance du secret professionnel applicable aux administrateurs.

http://ssi.ac-bordeaux.fr/fileadmin/charte_administrateur.rtf

Charte de responsable de site RACINE-AGRIATES

Cette charte définit les rôles et responsabilités du chef d'établissement en tant que responsable de site RACINE-AGRIATES.

http://ssi.ac-bordeaux.fr/fileadmin/charte_racine.pdf

Charte déontologique régissant l'usage du réseau RENATER

Cette charte concerne tous les organismes de la communauté "éducation-recherche" connectés au réseau RENATER. L'ensemble des lycées et EREA de l'académie, les collèges de Dordogne, des Landes et des Pyrénées utilisent RENATER comme accès à Internet.

https://www.renater.fr/IMG/pdf/charte_fr.pdf

Charte RACINE-API (Accès Poste Isolé)

Cette charte fixe les conditions d'accès distant au système d'information de l'Education nationale via le réseau RACINE par l'utilisation de clés d'authentification forte.

http://ssi.ac-bordeaux.fr/fileadmin/charte_racine_api.pdf

Réseaux virtuels privés de l'Education nationale

Les réseaux RACINE (Réseau d'Accès et de Consolidation des Intranets de l'Education) sont des réseaux privés virtuels qui offrent et garantissent un environnement d'accès sécurisés aux systèmes d'information de l'Education nationale pour toute communauté d'utilisateurs « ayants droit » quel que soit le lieu où ces utilisateurs exercent leurs activités professionnelles.

Les réseaux RACINE sont indépendants de toute infrastructure de transport. Ces accès deviennent par la même, indépendant du niveau de sécurité de chacune des infrastructures externes de réseaux traversées.

Ils se basent sur :

- une organisation en zone de confiance avec des niveaux d'habilitation
- un plan d'adressage IP respectant les standards de l'Internet et commun à l'ensemble des services
- un réseau privé virtuel sécurisé interconnectant l'ensemble des services
- une autorité de certification

Les zones de confiance sont :

- Le réseau RACINE pour la fourniture d'un support sécurisé pour les échanges d'informations entre le réseau de l'administration centrale et les services académiques.

- Le réseau RACINE-AGRIATES (Accès Généralisé aux Réseaux Intranet Académiques et Territoriaux pour les établissements Scolaires) pour la fourniture d'un support sécurisé pour les échanges d'informations entre le réseau de l'administration des établissements et le rectorat.

- Le réseau RACINE-ADRIATIC (Accès des Départements et des Régions aux Intranet Académiques et aux TICs) pour la fourniture d'un support sécurisé pour les échanges d'informations entre le réseau Internet du rectorat et les collectivités.

- Le réseau RACINE-API (Accès Postes Isolés) pour la fourniture d'un support sécurisé permettant l'accès des postes isolés des utilisateurs « ayants droit » aux services des ressources nécessaires au bon exercice de leurs fonctions ou missions.

Ces réseaux reposent sur un VPN IPsec (site à site ou client à site) nécessitant l'utilisation de mécanismes cryptographiques. Les suites cryptographiques doivent être pleinement compatibles avec les exigences du RGS.

L'usage de certificats de type SHA2 délivrés par la Plate-forme Nationale de Confiance Numérique (PNCN), autorité de certification du ministère, qui garantit la confiance globale du réseau, est exigé. Une délégation de droit d'usage du domaine de la collectivité doit être accordée par celle-ci au RSSI académique pour l'obtention des certificats afin de rendre possible leur implémentation sur les

équipements de sécurité des EPLE raccrochés à ce domaine par la collectivité. Un modèle de délégation figure en annexe.

Toutefois, le recours à des réseaux de type MPLS peut être accepté. Il est alors préconisé de garantir la confidentialité des données par convention avec l'opérateur tiers assurant la liaison. De plus, la collectivité devra acquérir, mettre en place, maintenir, exploiter et assurer la continuité de service de l'ensemble des équipements permettant cette liaison y compris le point de collecte positionné dans les locaux du rectorat.

Le plan d'adressage ADRIATIC

10.64.1.0 /24	ADRIATIC-CRA-ADMIN
10.64.2.0 /24	ADRIATIC-CG24-ADMIN
10.64.3.0 /24	ADRIATIC-CG33-ADMIN
10.64.4.0 /24	ADRIATIC-CG40-ADMIN
10.64.11.0 /24	ADRIATIC-CRA-PEDA
10.64.12.0 /24	ADRIATIC-CG24-PEDA
10.64.13.0 /24	ADRIATIC-CG33-PEDA
10.64.14.0 /24	ADRIATIC-CG40-PEDA
10.64.23.0 /24	ADRIATIC-CG33-PEDA
10.64.24.0 /24	ADRIATIC-ALPI40

Flux de données des établissements

Le système d'information de l'établissement scolaire met en œuvre des flux de données qui transitent à partir et en direction de différentes zones relevant de différents niveaux de confiance telles que définies ci-dessous :

DEFINITION DES ZONES DE CONFIANCE	
Zone administrative	Ensemble des points d'accès au réseau de l'établissement pour les personnels administratifs
Zone pédagogique	Ensemble des points d'accès au réseau de l'établissement pour des personnels pédagogiques et les élèves
Zones de services informatiques locaux (DMZ privées)	Ensemble des points d'accès au réseau de l'établissement dédiés à l'hébergement des équipements et services informatiques locaux. La création de plusieurs zones différenciées vise à respecter le principe de cloisonnement réseau exigé par la PSSIE (serveurs de fichiers et d'authentification, GTB, ToIP, interfaces d'administration des équipements informatiques ...)
Zone de services informatiques pour le public (DMZ publique)	Ensemble des points d'accès au réseau de l'établissement dédiés à l'hébergement des équipements et services informatiques accessibles depuis le réseau public
Zone d'accès wifi local	Ensemble des points d'accès au réseau de l'établissement pour les équipements mobiles sans-fil avec accès possibles à Internet et aux ressources locales pédagogiques
Zone d'accès wifi de type invité	Ensemble des points d'accès au réseau de l'établissement pour les équipements mobiles sans-fil avec accès possibles à Internet
Zone externe publique (Internet)	services informatiques Internet, hors établissement, incluant par exemple les services de vie scolaire centralisés, les ENT, les prestataires externes, les DSI de la CT et du Rectorat ...

La matrice ci-après décrit les possibilités d'échanges de données que le dispositif technique de l'établissement doit respecter obligatoirement.

DE \ VERS		ZONES DE CONFIANCE LOCALES						
		Zone administrative	Zone pédagogique	Zones de services informatiques locaux (DMZ privées)	Zone de services informatiques pour le public (DMZ publique)	Zone d'accès wifi local	Zone d'accès wifi de type invité	Zone externe publique (Internet)
ZONES DE CONFIANCE LOCALES	Zone administrative		A	A	A	I	I	A*
	Zone pédagogique	I		A	A	I	I	A*
	Zones de services informatiques locaux (DMZ privées)	I	A		I	I	I	P
	Zone de services informatiques pour le public (DMZ publique)	I	I	I		I	I	P
	Zone d'accès wifi local	I	A	A	A		I	A*
	Zone d'accès wifi de type invité	I	I	I	A	I		A*
Zone externe publique (Internet)		P	P	P	P	P	P	

A : les flux sont ADMIS par défaut

A* : les flux sont ADMIS par défaut et des mécanismes assurant la disponibilité et la confidentialité d'accès à des ressources spécifiques sont déployés après validation par le RSSI

I : les flux sont INTERDITS

P : les flux sont INTERDITS par défaut et POSSIBLES après validation par le RSSI académique

Réseaux Wi-Fi

Le déploiement de réseaux sans fil doit faire l'objet d'une analyse de risques spécifique.
Dans tous les cas, le raccordement d'un point d'accès Wifi à la zone administrative est interdit. Pour les autres besoins de raccordement, les niveaux de protection intrinsèques à cette technologie étant insuffisants, des mesures complémentaires doivent être prises, reposant sur les principes de la défense en profondeur.
Une segmentation du réseau doit être mise en place de façon à limiter à un périmètre déterminé les conséquences d'une intrusion depuis la voie radio. Il est obligatoire d'assurer un cloisonnement du réseau Wifi du reste du réseau de l'établissement : l'interconnexion au réseau principal doit se faire au travers d'une passerelle maîtrisée permettant de tracer les accès et de restreindre les échanges aux seuls flux nécessaires.
À défaut de mise en œuvre de ces mesures spécifiques, le déploiement de réseaux sans fil est proscrit.

Dans tous les cas d'usages, il convient de respecter les exigences suivantes :

1) Avant la mise en œuvre :

a) mener une étude préalable au déploiement :

- décrire la zone de couverture et ses spécificités (interférences, obstacles),
- optimiser l'emplacement des bornes et régler la puissance d'émission au minimum nécessaire
- décrire les données et fonctions utilisées sur le réseau en fonction de la finalité envisagée pour l'utilisation du WiFi :
  - extension d'un réseau local
  - accès à des services
  - interconnexion de bâtiments distants au sein d'un même établissement

b) déterminer les objectifs de sécurité en termes de :

- disponibilité,
- intégrité, confidentialité,
- qualité des preuves techniques d'accès aux services et aux actions.

2) Principes d'exploitation à respecter :

- Contrôler les accès physiques aux équipements
- Modifier l'identifiant réseau des bornes (SSID) par défaut (« Désactiver la diffusion de SSID » ne peut être considéré comme une mesure de sécurité efficace)
- Changer les mots de passe par défaut d'accès aux équipements et les modifier régulièrement
- Désactiver les services non utilisés (DHCP, SNMP, telnet,…).
- Procéder à la mise à jour régulière du « firmware » (logiciel d'exploitation) des bornes
- Activer la conservation des traces des sessions sur 12 mois glissants
- Proscrire l'usage du mode « ad-hoc » sur les postes de travail
- Auditer régulièrement le réseau sans fil pour s'assurer qu'il ne couvre pas des zones non désirées et pour contrôler qu'il n'existe pas de réseau sans fil non désiré dans le périmètre à sécuriser (bornes sauvages ou bornes de voisins).

3) La mise en production d'un réseau Wi-fi dans l'établissement doit faire l'objet d'une homologation par l'autorité académique selon la procédure décrite au chapitre « homologation ».

La matrice ci-dessous présente les possibilités de déploiement de réseaux Wifi selon les zones de confiance internes à l'établissement scolaire :

Zone de confiance / Méthode de chiffrement / authentification	Zone administrative	Autres zones	Interconnexion de bâtiments au sein d'un même établissement
Cryptage WEP	**Réseau WiFi interdits**	**insuffisant**	**insuffisant**
Cryptage WPA-TKIP		**insuffisant**	**insuffisant**
Cryptage WPA2 (AES) / authentification basique (identifiant et mot de passe avec validation du certificat serveur)		**admis sous conditions**	**insuffisant**
Cryptage WPA2 (AES) / authentification forte par certificat (avec validation du certificat serveur)		**préconisé**	**admis sous conditions**
Cryptage WPA2 (AES) / authentification forte par certificat avec clef privée non copiable (avec validation du certificat serveur)		**inutile**	**préconisé**
Cryptage WPA2 (AES) / authentification forte par clef OTP (avec validation du certificat serveur)		**inutile**	sans objet

Règles de filtrage

Le filtrage des accès est obligatoire pour répondre aux lois sur la propriété intellectuelle, sur l'usage de l'internet (cf extraits ci-dessous) pour la protection des utilisateurs et en particulier les mineurs. Il permet aussi de régir les flux entre les zones de confiance d'un établissement et l'internet comme décrit dans la matrice de flux, protégeant ainsi les systèmes de l'établissement.

- L'article L. 336-3 alinéa 1 du Code de la propriété intellectuelle issue de la loi dite Hadopi, qui dispose que « La personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise. Le manquement de la personne titulaire de l'accès à l'obligation définitive au premier alinéa n'a pas pour effet d'engager la responsabilité pénale de l'intéressé sous réserve des articles L 335-7 et L 335-7-1 du Code de la propriété intellectuelle.

- La circulaire 2004-035 relative à l'usage de l'Internet dans le cadre pédagogique et de la protection des mineurs du 18 février 2004 prévoyant « la mise en œuvre d'outils de filtrage dans les établissements ou écoles » et la mise en place d'une chaîne d'alerte qui doit être utilisée en cas d'incidents liés à l'usage des TIC dans le cadre pédagogique.

Dès lors que le dispositif de filtrage engendre une collecte de données à caractère personnel, un document doit être rédigé pour informer les usagers individuellement et collectivement de sa mise en place.

Les règles de filtrage ci-dessous représentent la traduction de la matrice des flux entre les zones de confiance de l'établissement et internet comme défini dans le chapitre «Flux de données des établissements». Elles constituent également les règles de sécurité pour prévenir des usages illicites et protéger les données et les équipements connectés de l'établissement.

Règles qui traduisent la matrice des flux

Règle	Exemple iptables à titre indicatif
Autoriser le réseau administratif à accéder au réseau pédagogique	ACCEPT all -- anywhere anywhere
Autoriser le réseau administratif à accéder à la DMZ publique	ACCEPT all -- anywhere anywhere
Autoriser le réseau administratif à accéder à la DMZ privée	ACCEPT all – anywhere anywhere
Interdire au réseau administratif d'aller sur les réseaux wifi	DROP all -- anywhere anywhere
Autoriser le réseau administratif à aller sur internet	ACCEPT all -- 10.33.55.0/24 anywhere ACCEPT all -- anywhere anywhere
Interdire l'accès au réseau administratif depuis le réseau pédagogique	DROP all -- anywhere anywhere
Interdire l'accès au réseau administratif depuis la DMZ publique	DROP all -- anywhere anywhere
Interdire l'accès au réseau administratif depuis la DMZ privée	DROP all -- anywhere anywhere
Interdire l'accès au réseau administratif depuis les réseaux wifi	DROP all -- anywhere anywhere
Interdire l'accès au réseau administratif depuis internet par défaut (autorisation possible si validation RSSI)	DROP all -- anywhere anywhere
Autoriser le réseau pédagogique à aller sur internet	ACCEPT all -- anywhere anywhere
Autoriser le réseau pédagogique à aller sur la DMZ	ACCEPT all -- anywhere anywhere
Interdire au réseau pédagogique d'aller sur les réseaux wifi	ACCEPT all -- anywhere anywhere
Autoriser la DMZ privé à accéder au réseau pédagogique	ACCEPT all -- anywhere anywhere
Interdire l'accès à la DMZ publique depuis la DMZ privée	DROP all -- anywhere anywhere
Interdire l'accès au réseaux wifi depuis le DMZ privée	DROP all -- anywhere anywhere
Interdire l'accès à la DMZ privée depuis internet par défaut (autorisation possible si validation RSSI)	DROP all -- anywhere anywhere
Interdire la DMZ publique à aller sur internet par défaut (autorisation possible si validation RSSI)	DROP all -- anywhere anywhere

Interdire la DMZ publique d'aller sur le réseau pédagogique	DROP all -- anywhere anywhere
Interdire la DMZ publique d'aller sur la DMZ privée	DROP all -- anywhere anywhere
Interdire la DMZ publique d'aller sur les réseaux wifi	DROP all -- anywhere anywhere
Interdire la DMZ publique à aller sur internet par défaut (autorisation possible si validation RSSI)	DROP all -- anywhere anywhere
Interdire par défaut les accès depuis internet sur tous les réseaux de l'établissement (autorisation possible si validation RSSI)	DROP all -- anywhere anywhere

Règles de routage des réseaux et translations d'adresses

Règle	Réseaux	Exemple iptables à titre indicatif
Paquets entrants (INPUT)		
Accepter les requêtes à destination des réseaux du rectorat depuis le réseau administratif en passant par le tunnel sécurisé (IPSEC)	10.0.0.0/9 192.168.0.0/17 172.24.0.0/13 161.48.0.0/19 10.192.0.0/10	ACCEPT all -- 10.0.0.0/9 anywhere state RELATED,ESTABLISHED policy match dir in pol ipsec proto esp ACCEPT all -- 10.0.0.0/9 anywhere state NEW policy match dir in pol ipsec proto esp
Autoriser les requêtes ICMP sur les différents réseaux		icmp-acc icmp -- anywhere anywhere
Paquets réorientés (FORWARD)		
Autoriser les échanges entre les réseaux de l'établissement (admin, pédagogique et DMZ) avec les réseaux du rectorat par le tunnel sécurisé (IPSEC)	10.0.0.0/9 192.168.0.0/17 172.24.0.0/13 161.48.0.0/19 10.192.0.0/10	ACCEPT all--10.0.0.0/9 10.33.118.0/24 state RELATED,ESTABLISHED policy match dir in pol ipsec proto esp ACCEPT all -- 10.0.0.0/9 10.33.118.0/24 state NEW policy match dir in pol ipsec proto esp ACCEPT all -- 10.33.118.0/24 10.0.0.0/9 state RELATED,ESTABLISHED policy match dir out pol ipsec proto esp ACCEPT all -- 10.33.118.0/24 10.0.0.0/9
Bloquer et tracer les requêtes vers les sites sur les listes noires (base liste de Toulouse + ajouts rectorat)		LOG all -- anywhere anywhere set BlacklistDmz dst LOG level info prefix `BlacklistDmz ' DROP all -- anywhere anywhere set BlacklistDmz dst LOG all -- anywhere anywhere set BlacklistPeda dst LOG level info prefix `BlacklistPeda ' DROP all -- anywhere anywhere set BlacklistPeda dst LOG all -- anywhere anywhere set BlacklistAdmin dst LOG level info prefix `BlacklistAdmin ' DROP all -- anywhere anywhere set BlacklistAdmin dst
Paquets sortants (OUTPUT)		
Accepter les requêtes des réseaux établissement vers les réseaux du rectorat suivants en passant par un tunnel sécurisé (IPSEC):	10.0.0.0/9 192.168.0.0/17 172.24.0.0/13 161.48.0.0/19 10.192.0.0/10	ACCEPT all -- anywhere 10.0.0.0/9 state RELATED,ESTABLISHED policy match dir out pol ipsec proto esp ACCEPT all -- anywhere 10.0.0.0/9 state NEW policy match dir out pol ipsec proto esp
Remplacer les adresses privées des réseaux administratif et pédagogique internes par l'adresse du pare-feu	Adresse publique du pare-feu	SNAT all -- 172.22.84.0/23 anywhere to:212.234.77.130
Remplacer les adresses privées des serveurs sur la DMZ autorisés à sortir sur internet par l'adresse du pare-feu (sauf cas particulier où on leur attribue une adresse publique spécifique)	Postes en 231, 233, 246, 247 ou 248	SNAT all -- 10.133.166.231 anywhere to:212.234.77.130
Réorienter les requêtes de différents ports arrivant sur les adresses publiques libres vers un serveur particulier de la DMZ quand il est présent (les ports dépendent des services sur le serveur)	Exemple: tcp 49400, 49600, x11, www, https, 3128	DNAT tcp -- anywhere 217.109.172.179 tcp dpt:49600 flags:SYN,RST,ACK/SYN to:10.133.118.246 DNAT tcp -- anywhere 217.109.172.179 tcp dpt:x11 flags:SYN,RST,ACK/SYN to:10.133.118.246

Règles concernant certains services techniques

Règle	Ports	Réseaux	Exemple iptables à titre indicatif
DNS			
Autoriser le service DNS sur l'administration	tcp/udp 53		ACCEPT udp -- anywhere admin.0333134c.in.ac-bordeaux.fr state NEW udp dpt:domain ACCEPT tcp -- anywhere admin.0333134c.in.ac-bordeaux.fr state NEW tcp dpt:domain flags:SYN,RST,ACK/SYN
Autoriser le service DNS sur la pédagogie	tcp/udp 53		ACCEPT udp -- anywhere pedago.estay.clg state NEW udp dpt:domain ACCEPT tcp -- anywhere pedago.estay.clg state NEW tcp dpt:domain flags:SYN,RST,ACK/SYN
Autoriser services DNS sur la DMZ	tcp/udp 53		ACCEPT udp -- anywhere dmz.estay.clg state NEW udp dpt:domain ACCEPT tcp -- anywhere dmz.estay.clg state NEW tcp dpt:domain flags:SYN,RST,ACK/SYN
Bloquer les services DNS extérieurs	udp 53		DROP udp -- anywhere !admin.0333134c.in.ac-bordeaux.fr udp dpt:domain DROP udp -- anywhere !pedago.estay.clg udp dpt:domain

NTP			
Autoriser serveur de temps (NTP)	Udp 123		ACCEPT udp -- anywhere anywhere udp spt:ntp ACCEPT udp -- anywhere anywhere udp dpt:ntp
Netbios			
Interdire les requêtes Netbios de partage et d'accès distant depuis internet	Tcp/udp 135,137,138,139, 445		DROP tcp -- anywhere anywhere tcp dpt:loc-srv DROP udp -- anywhere anywhere udp dpt:loc-srv DROP tcp -- anywhere anywhere tcp dpts:netbios-ns:netbios-ssn DROP udp -- anywhere anywhere udp dpts:netbios-ns:netbios-ssn DROP tcp -- anywhere anywhere tcp dpt:microsoft-ds DROP udp -- anywhere anywhere udp dpt:microsoft-ds
SMTP			
Autoriser serveurs SMTP rectorat	tcp 25	194.199.33.0/255.255.255.0 10.24.128.0/255.255.255.0 192.168.54.0/255.255.255.0	ACCEPT tcp -- anywhere 192.168.54.0/24 tcp dpt:smtp ACCEPT tcp -- anywhere 10.24.128.0/24 tcp dpt:smtp ACCEPT tcp -- anywhere 194.199.33.0/24 tcp dpt:smtp
Interdire les SMTP extérieurs	tcp 25	Sur les réseaux administratifs et pédagogiques	DROP tcp -- anywhere anywhere tcp dpt:smtp
Proxy			
Tracer toutes les requêtes vers internet (web et https)	Tcp 80, 443, 8080		LOG tcp -- anywhere anywhere tcp dpt:webcache LOG level info prefix ` ***SERVICE 8080 ETH2*** ' LOG tcp -- anywhere anywhere tcp dpt:webcache LOG level info prefix ` ***SERVICE 8080 ETH1*** ' LOG tcp -- anywhere anywhere tcp dpt:https LOG level info prefix ` ***SERVICE HTTPS ETH2*** ' LOG tcp -- anywhere anywhere tcp dpt:https LOG level info prefix ` ***SERVICE HTTPS ETH1***
Forcer l'utilisation du proxy pour les accès web en dehors des requêtes vers l'intranet du rectorat	tcp 80	réseaux concernés : 10.0.0.0/8; 10.192.0.0/10; 161.48.0.0/19; 192.168.0.0/16; 172.16.0.0/12; 172.24.0.0/13	REDIRECT tcp -- anywhere anywhere tcp dpt:www flags:SYN,RST,ACK/SYN ! set intranetbordeaux dst redir ports 3128
Forcer l'utilisation du proxy pour les accès web sécurisés HTTPS quand l'authentification est mise en place sur Amon	tcp 443, 3128		Commande pour l'implémenter: /sbin/iptables -t nat -A PREROUTING -p tcp --dport 443 --tcp-flags SYN,RST,ACK SYN -i eth2 -s 0/0 -d 0/0 -j REDIRECT --to-ports 3128
SNMP			
Autoriser la supervision des équipements réseaux et serveurs	Udp 161, 162	Réseaux du rectorat et de la collectivité	ACCEPT udp -- 10.33.118.0/24 admin.0332246m.in.ac-bordeaux.fr state NEW udp dpt:snmp

Règles nécessaires uniquement dans le cas de serveurs encore administrés par l'académie

Règle	Ports	Réseaux	Exemple iptables
Autoriser l'administration du Amon depuis le rectorat	tcp 22,81,443,4200,4203,7070,8090,8443 udp 161,162 icmp	IP pour le rectorat: 194.199.33.21 194.199.33.89	ACCEPT tcp -- eole.ac-bordeaux.fr amon-ng.0332246m.in.ac-bordeaux.fr state NEW tcp dpt:8090 flags:SYN,RST,ACK/SYN ACCEPT tcp -- proxy1-carayon.ac-bordeaux.fr amon-ng.0332246m.in.ac-bordeaux.fr state NEW tcp dpt:8090
Autoriser l'administration du Amon depuis le réseau administratif	Tcp 22, 81, 443, 4200, 4203, 7070, 8090, 8443 udp 161, 162 icmp		ACCEPT tcp -- 10.33.118.0/24 admin.0332246m.in.ac-bordeaux.fr state NEW tcp dpt:8090 flags:SYN,RST,ACK/SYN ACCEPT tcp -- 10.33.118.0/24 admin.0332246m.in.ac-bordeaux.fr state NEW tcp dpt:4200 flags:SYN,RST,ACK/SYN
Autoriser l'accès à l'administration du Amon depuis un poste identifié sur le réseau pédagogique et les serveurs pédagogiques	tcp 22, 81, 4200, 8090, 8443 udp 161 , 162 icmp	Adresses serveurs 231 ou 232 Adresse poste référencé 240	ACCEPT tcp -- 172.22.33.240 pedago.chambery.clg state NEW tcp dpt:8090 flags:SYN,RST,ACK/SYN ACCEPT tcp -- serveur1.chambery.clg pedago.chambery.clg state NEW tcp dpt:8090 flags:SYN,RST,ACK/SYN
Autoriser l'administration web sur le parefeu Amon depuis la DMZ	Tcp 8443		ACCEPT tcp -- anywhere dmz.chambery.clg state NEW tcp dpt:8443 flags:SYN,RST,ACK/SYN
Autoriser les requêtes provenant sur serveur administratif Horus			ACCEPT all -- horus.0332246m.in.ac-bordeaux.fr anywhere
Autoriser serveur scribe installé sur la DMZ à sortir sur internet avec une des ip publiques		Adresse généralement retenue 231	ACCEPT all -- 10.133.118.231 anywhere
Autoriser le serveur scribe installé en DMZ à se connecter au réseau pédagogique	Udp 65535 tcp/udp 137 à 139, 7725 tcp 445, 515, 5800, 5900, 8788, 9100,	Adresse généralement retenue pour le scribe: 231	ACCEPT tcp -- 10.133.118.231 anywhere state NEW tcp dpt:8788 flags:SYN,RST,ACK/SYN

	59982		
Autoriser le serveur antivirus/Wsus installé sur la DMZ à sortir sur internet		Adresse généralement retenue 233	ACCEPT all -- 10.133.118.233 anywhere
Autoriser le serveur web et/ou pronote.net installé sur la DMZ à sortir sur internet avec une des ip publiques		Adresse généralement retenue 246, 247 ou 248	ACCEPT all -- 10.133.118.246 anywhere ACCEPT all -- 10.133.118.247 anywhere ACCEPT all -- 10.133.118.248 anywhere
Autoriser le serveur pronote.net installé en DMZ à se connecter au serveur pédagogique ou se trouve la base pronote	tcp 49300, 49500	Adresse généralement retenue pour pronote.net sur la DMZ 246, 247 ou 248 Adresse généralement retenue pour le serveur sur le réseau pédagogique 231	ACCEPT tcp -- 10.133.118.246 serveur1.chambery.clg state NEW tcp dpt:49300 flags:SYN,RST,ACK/SYN ACCEPT tcp -- 10.133.118.246 serveur1.chambery.clg state NEW tcp dpt:49500 flags:SYN,RST,ACK/SYN
Ouvrir les ports spécifiques aux serveurs web (ex: nginx) depuis internet vers le parefeu	tcp 443,4203,7070,8443		ACCEPT tcp -- anywhere amon-ng.0332246m.in.ac-bordeaux.fr state NEW tcp dpt:https flags:SYN,RST,ACK/SYN ACCEPT tcp -- anywhere amon-ng.0332246m.in.ac-bordeaux.fr state NEW tcp dpt:7070 flags:SYN,RST,ACK/SYN ACCEPT tcp -- anywhere amon-ng.0332246m.in.ac-bordeaux.fr state NEW tcp dpt:4203 flags:SYN,RST,ACK/SYN ACCEPT tcp -- anywhere amon-ng.0332246m.in.ac-bordeaux.fr state NEW tcp dpt:8443 flags:SYN,RST,ACK/SYN

Règles de sécurité pour bloquer certaines applications dangereuses

Règle	Ports	Réseaux	Exemple iptables
Blocage Openvpn	Tcp/udp 1194	Réseau pédagogique et équipements réseaux du réseau administratif (adresses hautes)	DROP udp -- !172.22.33.0/24 anywhere udp dpt:openvpn DROP tcp -- !172.22.33.0/24 anywhere tcp dpt:openvpn DROP udp -- !10.33.118.192/26 anywhere udp dpt:openvpn DROP tcp -- !10.33.118.192/26 anywhere tcp dpt:openvpn
Blocage réseau UTORENT	tcp/udp 6881		DROP udp -- anywhere anywhere udp dpt:6881 DROP tcp -- anywhere anywhere tcp dpt:6881
Blocage réseau TOR	tcp/udp 9001		DROP udp -- anywhere anywhere udp dpt:9001 DROP tcp -- anywhere anywhere tcp dpt:9001
Blocage Teamviewer	tcp/udp 5938	sur serveurs, les imprimantes et équipements réseaux du réseau pédagogique	DROP udp -- !172.22.33.128/25 anywhere udp dpt:5938 DROP tcp -- !172.22.33.128/25 anywhere tcp dpt:5938

Règles répondant à des configurations spécifiques ou à des accès particuliers liés aux besoins des établissements

Règle	Ports	Réseaux	Exemple iptables
Collèges du 40: Autoriser serveurs SMTP CD40	Tcp 25	193.52.2.220/255.255.255.255 195.101.65.134/255.255.255.255	ACCEPT tcp -- anywhere rsmtp.landes.org tcp dpt:smtp
Collèges du 47: Autoriser serveur SMTP ADITU	Tcp 25	85.31.144.28/255.255.255.255	ACCEPT tcp -- anywhere 85.31.144.28 tcp dpt:smtp
Collèges du 64: Autoriser serveurs SMTP HELIANTIS	Tcp 25	83.173.64.0/255.255.240.0	ACCEPT tcp -- anywhere 83.173.64.0/20 tcp dpt:smtp
Service FTP	tcp 20:21	sur serveurs et équipements réseaux du réseau pédagogique	ACCEPT tcp -- 172.22.33.128/25 anywhere state NEW tcp dpts:ftp-data:ftp flags:SYN,RST,ACK/SYN
ESIDOC: ports à ouvrir sur le réseau pédagogique	Tcp 990, 1024:1028		ACCEPT tcp -- anywhere anywhere multiport dports ftps,1024:1028
Serveur WSUS académique: liaison du serveur local avec le serveur académique	tcp 8530		ACCEPT tcp -- anywhere anywhere tcp dpt:8530
Portail captif Amonet: accès HTTPS autorisé vers internet et openvpn	tcp 443	Adresse généralement retenue pour Amonet: 234	ACCEPT udp -- amonet.chambery.clg anywhere udp dpt:openvpn

Accès distant et authentification

Mode accès en poste isolé (API)

L'accès distant au réseau de l'établissement depuis un poste isolé doit faire l'objet d'une demande d'autorisation signée par le chef d'établissement et validée par le RSSI. Celui-ci ne pourra se faire que par le biais d'une solution sécurisée de type VPN permettant le cryptage des données, l'authentification nominative forte et la journalisation des accès.
Pour les besoins des personnels administratifs de l'établissement, une solution par clé OTP et, selon les cas, la mise en œuvre d'un tunnel chiffré IPSEC depuis le rectorat est préconisée.

Télé-assistance

Indépendamment de tout contexte et de toute solution de prise de main à distance pour les opérations de télé-assistance, les 12 recommandations suivantes s'appliquent. Lorsque les solutions utilisées le permettent, ces recommandations doivent être imposées techniquement.

- L'opération de télé-assistance doit s'effectuer dans le contexte de l'utilisateur, avec ses droits, et sans que son mot de passe ne soit communiqué au télé-assistant.
- La télé-assistance du poste de travail doit s'effectuer de manière visuelle par affichage partagé entre l'utilisateur et le télé-assistant. L'utilisateur doit être en mesure de voir les opérations effectuées par le télé-assistant.
- L'opération de télé-assistance sur le poste de travail de l'utilisateur doit respecter le consentement de ce dernier. Elle ne doit être possible que suite à l'acceptation explicite de l'utilisateur. Toute connexion arbitraire à un poste de travail utilisateur par un télé-assistant doit être impossible.
- L'authentification des télé-assistants sur les postes distants doit idéalement être réalisée à l'aide de certificats individuels délivrés par une IGC de confiance. Lorsque seul un usage de mots de passe est possible, il convient de s'assurer que celui-ci respecte les recommandations de sécurité sur les mots de passe. Des méthodes d'authentification alternatives par jetons ou mots de passe d'accès unique (OTP) peuvent également être suffisantes.
- L'offre d'assistance, lorsqu'elle est utilisée, ne doit être possible que par des télé-assistants dûment autorisés par l'utilisateur. Cette restriction peut par exemple consister en une liste blanche de groupes ou de comptes utilisateurs autorisés à offrir une télé-assistance.
- Dans le cadre d'une offre d'assistance, l'utilisateur télé-assisté doit être en mesure de vérifier l'identité du télé-assistant qui lui est présentée préalablement à toute acceptation. L'identité de ce dernier peut être prouvée par exemple par la présentation d'un certificat X509 ou du compte Active-Directory utilisé.
- La solution de télé-assistance doit se présenter sous la forme d'une application pouvant être démarrée par l'utilisateur plutôt qu'un service lancé automatiquement au démarrage du poste de travail.
- La solution de télé-assistance doit être à jour de ses correctifs de sécurité en permanence, et mise à jour sans délai dès lors qu'une version plus sécurisée est disponible. Une vulnérabilité impactant une solution de prise en main à distance peut en effet permettre l'élévation de privilèges rapide par une personne malveillante.
- Les postes de télé-assistance doivent être dédiés à ces opérations, isolés d'Internet et, en permanence à jour de leurs correctifs de sécurité.
- La solution de télé-assistance doit reposer sur des protocoles sécurisés. Les mécanismes de sécurité implémentés doivent permettre :
  - une authentification mutuelle entre les postes de télé-assistant et télé-assisté ;

- un échange de clés de sessions éphémères à la manière de TLS ;
- une protection contre le rejeu ou les attaques de type "man in the middle".

Pour satisfaire cette recommandation, un tunnel chiffré (IPSEC) mis en œuvre préalablement à l'aide d'une solution tierce ayant fait l'objet d'une qualification de sécurité par l'ANSSI, a minima d'une certification de sécurité de premier niveau, pourra s'avérer nécessaire.

- La télé-assistance ne doit pouvoir être opérée que depuis des adresses IP sources bien identifiées comme étant celles des postes des télé-assistants. Des mesures de sécurité au niveau réseau doivent donc être mises en œuvre : l'établissement d'un tunnel IPSEC dans le respect des recommandations faites par l'ANSSI, comme évoqué précédemment, est une bonne solution.
- L'ensemble des opérations de télé-assistance effectuées doivent être « journalisées », idéalement en les distinguant de toute autre action effectuée sur le poste de travail. Il doit être a minima possible de savoir quelle personne s'est connectée à quel poste de travail pour une opération de télé-assistance, quand et pendant combien de temps.

Dans le cas de télé-assistance sur des postes administratifs, l'accès doit se faire uniquement depuis des réseaux ou postes identifiés et il doit être sécurisé par l'établissement d'un tunnel IPSEC dans le respect des recommandations faites par l'ANSSI.

Télé-administration

L'administration des serveurs doit se faire depuis des postes physiques réservés à ces tâches. Ces postes doivent être distincts de ceux permettant d'accéder aux ressources bureautiques conventionnelles accessibles sur le système d'information de l'entité (ressources métier, messagerie interne, gestion documentaire, Internet, etc.).
Si les flux d'administration doivent circuler à travers un autre système d'information qui servirait de réseau de transport, les flux d'administration doivent y être chiffrés et authentifiés de bout en bout jusqu'à atteindre un autre SI d'administration ou une ressource à administrer.

Plan d'adressage

Le réseau RACINE

Le réseau se base sur une architecture sécuritaire définissant des "zones de confiance" et un schéma d'interconnexion national qui ne peut être mis en œuvre qu'en respectant, de façon aussi rigoureuse que possible, les concepts d'adressage communs aux différents partenaires.

Pouvant apparaître contraignants ou complexes, ces concepts constituent le fondement de RACINE. Ils contribuent au succès de sa mise en œuvre et à sa robustesse depuis son ouverture le 13 mars 2001.

Un plan d'adressage cohérent établi à l'échelle académique et qui concerne les réseaux administratifs des EPLE, est nécessaire pour les échanges internes à l'académie mais également pour les échanges inter-académiques notamment pour garantir l'accès à des ressources applicatives distribuées sur l'ensemble du réseau national, telles que les applications de gestion du système éducatif.

Il doit donc être scrupuleusement respecté par les collectivités. En cas d'une incompatibilité avec les plans d'adressage existants au sein du système d'information d'une collectivité, une dérogation peut être envisagée. Dans ce cas, un mécanisme de translation d'adresses devra être mis en place sous le contrôle de l'Ingénieur de Sécurité Racine .

Les applications métier de l'Education nationale GFC et Presto, lorsqu'elles sont installées en réseau, ne peuvent l'être que sur un serveur Linux Horus de la suite Eole. L'assistance et la maintenance de ces applications étant assurées par l'académie, le serveur Horus doit être joignable depuis le rectorat (télémaintenance, ssh, http et https). Si le serveur n'est pas sur le plan d'adressage de la zone administrative, une translation d'adresse doit être mise en place vers une adresse d'un réseau RACINE fournie par le rectorat pour ces besoins.

Le plan d'adressage est défini en annexe pour chaque réseau administratif des établissements de l'académie.

Certains établissements dans des cités scolaires peuvent partager le même réseau administratif (les établissements concernés sont spécifiés sous les plans d'adressage de chaque collectivité).

La collectivité devra transmettre une demande auprès du rectorat pour qu'une nouvelle plage d'adresses IP soit attribuée pour le réseau administratif, dans les cas suivants :

- évolution de la situation d'établissements en cité scolaire
- création d'un nouvel établissement
- création d'une annexe à un établissement existant (avec des besoins administratifs)

De même en cas de fermeture d'un établissement, la demande de libération de la plage d'adresses IP doit être faite par la collectivité au rectorat.

En ce qui concerne les annexes d'établissements, une solution de type MPLS peut être mise en place par la collectivité entre les sites afin de partager le même plan d'adressage et de permettre aux utilisateurs d'accéder à des ressources communes déployées sur l'un des sites (cf . p 11).

Les autres réseaux de l'EPLE

Le plan d'adressage des réseaux pédagogiques, de gestion technique des bâtiments, du WIFI, d'administration des équipements actifs, de la DMZ, etc est laissé libre à la collectivité territoriale.

Protection des mineurs

Conformément à la circulaire N°2004-035 DU 18-2-2004 relative à l'usage de l'internet dans le cadre pédagogique et à la protection des mineurs, afin de rendre possible le travail en autonomie, un contrôle automatique des pages consultées doit être mis en place. Deux modes de contrôle, complémentaires, sont possibles, modulables selon les situations rencontrées (selon l'équipement des établissements et le niveau d'enseignement) :

- un contrôle a priori des informations recherchées, en interdisant l'accès à un ensemble de sites reconnus comme inappropriés (sites au contenu pornographique, raciste, violent...) par l'intermédiaire de "listes noires". Il doit également être possible, pour des situations pédagogiques particulières, de limiter la consultation à un ensemble connu de sites, à partir de "listes blanches" ;

- un contrôle a posteriori, par examen de la liste des sites consultés.

Ces dispositifs s'appuient en règle générale sur la liste noire gérée par l'université de Toulouse, reconnue comme une référence nationale en matière de filtrage des requêtes « http » qui n'est cependant pas suffisante pour traiter les requêtes « https ».

L'architecture exigée doit reposer sur un dispositif adapté de type serveur proxy filtrant ou boîtier dédié capable de traiter les requêtes « http » et « https ». Ce dispositif est le passage obligé de toute connexion. Il n'y a donc pas de contournement possible, toutes les pages et tous les contenus doivent être analysés par le dispositif avant affichage.

Afin de pouvoir gérer d'éventuels incidents, de garantir l'efficacité du dispositif de filtrage et de pouvoir perfectionner les listes noires disponibles, il est indispensable de conserver les informations de connexion (« logs ») des usagers. (cf Journalisation).

Les traces pourront être analysées à l'aide de programmes de type scripts, afin de systématiser et d'améliorer l'efficacité de cette analyse. Des scripts d'analyse peuvent par exemple être trouvés sur la page http://download.savannah.gnu.org/releases/pornfind/, afin de détecter les pages inappropriées non filtrées par la liste noire.

Protection des systèmes

La protection des systèmes est de la responsabilité de la collectivité explicitée qui en assure la charge. Une série de bonnes pratiques qui doivent être mises en œuvre est rappelée ci-après :

Les bonnes pratiques à respecter sur les postes de travail :

- tous les accès en écriture au paramétrage du BIOS (activation/désactivation de fonctions, ordre de démarrage des périphériques, heure système, etc.) doivent être protégés par un mot de passe ;
- déployer systématiquement des techniques d'identification pour l'accès aux postes de travail ;
- les mots de passe doivent dans la mesure du possible être choisis en tenant compte des recommandations de la note technique « Recommandations de sécurité relatives aux mots de passe » disponible sur le site de l'ANSSI ;
- lorsque cela est possible, en application du principe de minimisation, les composants non requis au bon fonctionnement du système doivent être désactivés. Cette désactivation peut porter sur la configuration de connecteurs externes (port(s) série, contrôleurs USB, interfaces de disques externes comme eSATA ou Thunderbolt, etc.) et éventuellement certains périphériques internes ou sans-fil comme des contrôleurs disques, des cartes Wifi/Bluetooth ou multimédias intégrées ;
- mettre en œuvre des techniques de sécurité conforme à l'état de l'art (antivirus, anti-malwares, mises à jour de sécurité des postes ...)

Les bonnes pratiques pour les équipements systèmes et réseaux :

- désactiver les services inutiles ;
- changer les identifiants et les mots de passe par défaut des équipements ;
- utiliser des mots de passe complexes et les renouveler régulièrement ;
- filtrer les connexions aux interfaces d'administration ;
- sur les équipements supportés, activer le démarrage sécurisé (Secure Boot) ;
- « journaliser » les événements.

Il convient de maîtriser les équipements réseaux exploités, notamment le système d'exploitation installé sur ces équipements :

- il doit provenir directement du constructeur, pas d'un réseau pair-à-pair ou d'un site non officiel ;
- leur intégrité doit être vérifiée, avant l'installation et périodiquement après, selon le guide du constructeur ;
- les modifications de leur configuration doivent être maîtrisées et contrôlées ;
- les mises à jour de sécurité doivent être appliquées dans les meilleurs délais après publication.

Il est nécessaire de prévoir un plan de reprise d'activité en ce qui concerne les différents éléments sensibles du réseau.

Politique autour des mots de passe :

- Imposer le renouvellement des mots de passe avec une fréquence raisonnable
- Imposer l'utilisation de mots de passe robustes
- Forcer le changement des mots de passe communiqués sur un canal non confidentiel dès la première connexion

Journalisation du trafic

Il convient de conserver différents types de journaux (logs) et d'en informer les utilisateurs (l'article 6 I. – 1° de la loi 20046575 du 21 juin 2004 (LCEN)). Ces mesures sont prises afin de s'assurer de la sécurité et de la performance des solutions mises en place, gérer des éventuels incidents et répondre aux réquisitions judiciaires transmises par le RSSI académique ou directement par un officier de police judiciaire.

Voici une liste non exhaustive des types de journaux qu'il est recommandé de collecter :

- les événements relatifs à la politique de filtrage (paquets rejetés, etc.) ;
- les connexions réseaux ;
- les éléments relatifs aux VPN IPsec (mise en place et destruction de tunnels, etc.) ;
- les événements d'authentification (tentatives avortées, réussites, échecs, etc.) ;
- les événements d'administration (connexion d'administrateurs, modification de configurations) ;
- les statistiques ;
- les événements systèmes ;
- les alarmes.

Les informations extraites de ces fichiers, par exemple lors d'incident ou d'accès à des contenus inappropriés doivent être transmises, via la chaîne de remontée des incidents, au RSSI qui est le référent unique en matière de sécurité et de filtrage au niveau académique à l'adresse :

l.rssi@ac-bordeaux.fr

D'autre part, la collectivité territoriale, étant titulaire des lignes internet, elle a obligation en sa qualité d'opérateur de communication électronique :

- de surveiller les accès (article L.336-3 du Code de la propriété intellectuelle - issu de la loi DAVSI) : « La personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise ».

- de conserver les **données de trafic** répondant aux " *besoins de la recherche, de la constatation et de la poursuite des infractions pénales* " et destinées aux autorités légalement habilitées **pendant 1 an à compter du jour de leur enregistrement (en application des dispositions de l'article 1 du décret 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques)**. A savoir :

  a) Les informations permettant d'identifier l'utilisateur ;
  b) Les données relatives aux équipements terminaux de communication utilisés ;
  c) Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;
  d) Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;
  e) Les données permettant d'identifier le ou les destinataires de la communication.

La conservation et le traitement de ces données de journalisation s'effectuent dans le respect des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Quel que soit le mode de conservation, l'accès à tous les journaux de connexion (logs) est garanti en permanence aux chefs d'établissement et à l'AQSSI pour l'exercice de leurs prérogatives en matière de sécurité des systèmes d'information et de protection des mineurs.

De plus afin de pouvoir répondre en urgence à toute réquisition d'un officier de police judiciaire, la collectivité communique au chef d'établissement et au RSSI académique les coordonnées téléphoniques directes du technicien de support et veille à actualiser cette information. Dans pareil cas, ce technicien doit répondre sans délai à la sollicitation du chef d'établissement ou du RSSI.

Homologation

Autorité d'homologation

L'autorité d'homologation est désignée par le recteur d'académie. Son rôle est de prendre les décisions d'homologation des applications informatiques et des systèmes d'information mis en place dans l'académie de Bordeaux.

Procédure d'homologation

La mise en place d'une application ou d'un composant du système d'information au sein de l'établissement scolaire ou interconnecté avec le réseau RACINE doit obligatoirement faire l'objet d'une homologation préalable délivrée par l'autorité académique. La procédure se fait au moyen d'un formulaire disponible sur le site SSI de l'académie.

https://ssi.ac-bordeaux.fr/homologation

Suivi de la sécurité

Le suivi de la sécurité s'opère de manière continue par l'AQSSI et les chefs d'établissement grâce à l'outillage mis à disposition par la collectivité territoriale qui permet la supervision de l'ensemble des règles éditées dans le présent référentiel.

ANNEXES :

Annexe 1 - plan d'adressage des réseaux administratifs

Collèges de Dordogne

0240962R	CLG	PIERRE FANLAC	BELVES	10.233.163.0	255.255.255.0
0240004Z	CLG	HENRI IV	BERGERAC	10.234.115.0	255.255.255.0
0240004Z	CLG	HENRI IV (Annexe)	BERGERAC	10.234.181.0	255.255.255.0
0240119Z	CLG	EUGENE LE ROY	BERGERAC	10.233.205.0	255.255.255.0
0240996C	CLG	JACQUES PREVERT	BERGERAC	10.233.164.0	255.255.255.0
0240010F	CLG	ALIENOR D'AQUITAINE	BRANTOME	10.233.152.0	255.255.255.0
0240047W	CLG	JEAN MOULIN	COULOUNIEIX CHAMIERS	10.234.124.0	255.255.255.0
0241007P	CLG	GIRAUT DE BORNEIL	EXCIDEUIL	10.234.179.0	255.255.255.0
0240014K	CLG	G. ET MARIE BOUSQUET	EYMET	10.234.119.0	255.255.255.0
0240045U	CLG	CHARLES DE GAULLE	LA COQUILLE	10.234.123.0	255.255.255.0
0240053C	CLG	MAX BRAMERIE	LA FORCE	10.234.126.0	255.255.255.0
0240158S	CLG	JEAN MONNET	LALINDE	10.233.199.0	255.255.255.0
0240015L	CLG	PLAISANCE	LANOUAILLE	10.233.153.0	255.255.255.0
0240011G	CLG	LEROI-GOURHAN	LE BUGUE	10.234.117.0	255.255.255.0
0240016M	CLG	ARNAULT DE MAREUIL	MAREUIL	10.233.154.0	255.255.255.0
0240927C	CLG	YVON DELBOS	MONTIGNAC	10.234.135.0	255.255.255.0
0240117X	CLG	JEAN ROSTAND	MONTPON MENESTEROL	10.234.132.0	255.255.255.0
0240961P	CLG	LES CHATENADES	MUSSIDAN	10.234.136.0	255.255.255.0
0240044T	CLG	HENRI BRETIN	NEUVIC	10.234.122.0	255.255.255.0
0241041B	CLG	ALCIDE DUSOLIER	NONTRON	10.233.255.0	255.255.255.0
0240029B	CLG	CLOS CHASSAING	PERIGUEUX	10.234.120.0	255.255.255.0
0240030C	CLG	MICHEL DE MONTAIGNE	PERIGUEUX	10.233.157.0	255.255.255.0
0240052B	CLG	ANNE FRANK	PERIGUEUX	10.233.161.0	255.255.255.0
0241042C	CLG	BERTRAN DE BORN	PERIGUEUX	10.233.238.0	255.255.255.0
0241043D	CLG	LAURE GATET	PERIGUEUX	10.234.31.0	255.255.255.0
0240043S	CLG	PIEGUT PLUVIERS	PIEGUT PLUVIERS	10.233.206.0	255.255.255.0
0241011U	CLG	CITE SC. A. DANIEL	RIBERAC	10.234.139.0	255.255.255.0
0240121B	CLG	LA BOETIE	SARLAT	10.234.133.0	255.255.255.0
0240650B	CLG	ARTHUR RIMBAUD	ST ASTIER	10.234.134.0	255.255.255.0
0240055E	CLG	DRONNE-DOUBLE	ST AULAYE	10.234.127.0	255.255.255.0
0240065R	CLG	JEAN LADIGNAC	ST CYPRIEN	10.234.128.0	255.255.255.0
0240037K	CLG	JULES FERRY	TERRASSON	10.233.159.0	255.255.255.0
0240066S	CLG	SUZANNE LACORE	THENON	10.233.162.0	255.255.255.0
0240040N	CLG	LEONCE BOURLIAGUET	THIVIERS	10.233.160.0	255.255.255.0
0240073Z	CLG	TOCANE ST APRE	TOCANE ST APRE	10.234.129.0	255.255.255.0
0240106K	CLG	OLYMPE DE GOUGES	VELINES	10.234.130.0	255.255.255.0
0240056F	CLG	DES TROIS VALLEES	VERGT	10.233.166.0	255.255.255.0

Collèges de Gironde

RNE	Type	Nom	Ville	IP Admin	Masque Admin
0331617D	CLG	CLAUDE MASSE	AMBARES ET LAGRAVE	10.33.71.0	255.255.255.0
0331890A	CLG	ANDRE LAHAYE	ANDERNOS LES BAINS	10.33.100.0	255.255.255.0
0330167C	CLG	MARIE BARTETTE	ARCACHON	10.33.63.0	255.255.255.0
0332704K	CLG	PANCHON	ARSAC	10.33.138.0	255.255.255.0
0332085M	CLG	JEAN AURIAC	ARVEYRES	10.33.106.0	255.255.255.0
0330008E	CLG	JEAN VERDIER	AUDENGE	10.33.3.0	255.255.255.0
0331884U	CLG	MANON CORMIER	BASSENS	10.33.97.0	255.255.255.0
0332288H	CLG	AUSONE	BAZAS	10.33.122.0	255.255.255.0
0331752A	CLG	BERTHELOT	BEGLES	10.33.88.0	255.255.255.0
0331880P	CLG	PABLO NERUDA	BEGLES	10.33.95.0	255.255.255.0
0330017P	CLG	JEAN ZAY	BIGANOS	10.33.6.0	255.255.255.0
0331754C	CLG	EMMANUEL DUPATY	BLANQUEFORT	10.33.90.0	255.255.255.0
0332347X	CLG	SEBASTIEN VAUBAN	BLAYE	10.33.130.0	255.255.255.0
0330065S	CLG	MONSEJOUR	BORDEAUX	10.33.24.0	255.255.255.0
0330066T	CLG	SAINT ANDRE	BORDEAUX	10.33.25.0	255.255.255.0
0330140Y	CLG	DU GRAND PARC	BORDEAUX	10.33.57.0	255.255.255.0
0331461J	CLG	CASSIGNOL	BORDEAUX	10.33.68.0	255.255.255.0
0331461J	CLG	CASSIGNOL (Annexe)	BORDEAUX	10.33.251.0	255.255.255.0
0331462K	CLG	FRANCISCO GOYA	BORDEAUX	10.33.69.0	255.255.255.0
0331618E	CLG	LEONARD LENOIR	BORDEAUX	10.33.72.0	255.255.255.0
0331662C	CLG	ALAIN FOURNIER	BORDEAUX	10.33.79.0	255.255.255.0
0331663D	CLG	CHEVERUS	BORDEAUX	10.33.80.0	255.255.255.0
0331663D	CLG	CHEVERUS (Annexe)	BORDEAUX	10.233.148.0	255.255.255.0
0331753B	CLG	BLANQUI	BORDEAUX	10.33.89.0	255.255.255.0
0332082J	CLG	EDOUARD VAILLANT	BORDEAUX	10.33.104.0	255.255.255.0
0332285E	CLG	JACQUES ELLUL	BORDEAUX	10.33.121.0	255.255.255.0
0332746F	CLG	EMILE COMBES	BORDEAUX	10.33.147.0	255.255.255.0
0332768E	CLG	ALIENOR D'AQUITAINE	BORDEAUX	10.33.149.0	255.255.255.0
0332341R	CLG	JACQUES PREVERT	BOURG SUR GIRONDE	10.33.124.0	255.255.255.0
0330058J	CLG	Paul Emile VICTOR	BRANNE	10.33.19.0	255.255.255.0
0333274E	CLG	ROSA BONHEUR	BRUGES	10.233.208.0	255.255.255.0
0333133B	CLG	OLYMPE DE GOUGES	CADAUJAC	10.33.38.0	255.255.255.0
0330059K	CLG	ANATOLE FRANCE	CADILLAC	10.33.20.0	255.255.255.0
0333132A	CLG	CARBON BLANC	CARBON BLANC	10.33.32.0	255.255.255.0
0330062N	CLG	CANTERANE	CASTELNAU DE MEDOC	10.33.22.0	255.255.255.0
0330064R	CLG	ALIENOR D'AQUITAINE	CASTILLON L.BATAILLE	10.33.23.0	255.255.255.0
0331464M	CLG	JEAN ZAY (Z.U.P)	CENON	10.33.70.0	255.255.255.0
0331885V	CLG	JEAN JAURES	CENON	10.33.98.0	255.255.255.0
0332342S	CLG	CANTELANDE	CESTAS	10.33.125.0	255.255.255.0
0331621H	CLG	HENRI DE NAVARRE	COUTRAS	10.33.75.0	255.255.255.0
0332283C	CLG	FRANCOIS MITTERRAND	CREON	10.33.120.0	255.255.255.0
0332084L	CLG	ALBERT CAMUS	EYSINES	10.33.105.0	255.255.255.0
0331419N	CLG	GEORGES RAYET	FLOIRAC	10.33.64.0	255.255.255.0
0332189A	CLG	NELSON MANDELA	FLOIRAC	10.33.110.0	255.255.255.0
0331622J	CLG	FONTAINES DE MONJOUS	GRADIGNAN	10.33.76.0	255.255.255.0
0332190B	CLG	ALFRED MAUGUIN	GRADIGNAN	10.33.111.0	255.255.255.0
0330138W	CLG	JEAN AVIOTTE	GUITRES	10.33.56.0	255.255.255.0
0331759H	CLG	CHANTE CIGALE	GUJAN MESTRAS	10.33.93.0	255.255.255.0
0330081J	CLG	JULES CHAMBRELENT	HOURTIN	10.33.28.0	255.255.255.0
0332343T	CLG	MONTESQUIEU	LA BREDE	10.33.126.0	255.255.255.0
0332248P	CLG	PAUL ESQUINANCE	LA REOLE	10.33.119.0	255.255.255.0
0330129L	CLG	HENRI DHEURLE	LA TESTE	10.33.53.0	255.255.255.0
0333287U	CLG	LACANAU	LACANAU	10.233.229.0	255.255.255.0

RNE	Type	Nom	Ville	IP Admin	Masque Admin
0330083L	CLG	JULES FERRY	LANGON	10.33.30.0	255.255.255.0
0330084M	CLG	TOULOUSE LAUTREC	LANGON	10.33.31.0	255.255.255.0
0331620G	CLG	CAMILLE CLAUDEL	LATRESNE	10.33.74.0	255.255.255.0
0331669K	CLG	AUSONE	LE BOUSCAT	10.33.86.0	255.255.255.0
0333108Z	CLG	JEAN MOULIN	LE BOUSCAT	10.33.186.0	255.255.255.0
0332437V	CLG	EMILE ZOLA	LE HAILLAN	10.33.131.0	255.255.255.0
0332934K	CLG	PIAN SUR GARONNE	LE PIAN SUR GARONNE	10.33.135.0	255.255.255.0
0332982M	CLG	VAL DES PINS	LE TEICH	10.33.45.0	255.255.255.0
0332657J	CLG	LEGE CAP FERRET	LEGE CAP FERRET	10.33.137.0	255.255.255.0
0332244K	CLG	FRANCOIS MAURIAC	LEOGNAN	10.33.117.0	255.255.255.0
0331891B	CLG	LES LESQUES	LESPARRE MEDOC	10.33.101.0	255.255.255.0
0330091V	CLG	LES DAGUEYS	LIBOURNE	10.33.35.0	255.255.255.0
0330162X	CLG	EUGENE ATGET	LIBOURNE	10.33.61.0	255.255.255.0
0333213N	CLG	M DURAS	LIBOURNE	10.33.51.0	255.255.255.0
0331619F	CLG	GEORGES LAPIERRE	LORMONT	10.33.73.0	255.255.255.0
0331895F	CLG	MONTAIGNE	LORMONT	10.33.102.0	255.255.255.0
0330093X	CLG	LUSSAC	LUSSAC	10.33.36.0	255.255.255.0
0333121N	CLG	GASTON FLAMENT	MARCHEPRIME	10.33.163.0	255.255.255.0
0332743C	CLG	ALIENOR D'AQUITAINE	MARTIGNAS SUR JALLE	10.33.144.0	255.255.255.0
0330145D	CLG	CAPEYRON	MERIGNAC	10.33.59.0	255.255.255.0
0330146E	CLG	JULES FERRY	MERIGNAC	10.33.60.0	255.255.255.0
0331435F	CLG	LES EYQUEMS	MERIGNAC	10.33.66.0	255.255.255.0
0332090T	CLG	BOURRAN	MERIGNAC	10.33.108.0	255.255.255.0
0333329P	CLG	MIOS	MIOS	10.33.34.0	255.255.255.0
0330100E	CLG	ELEONORE DE PROVENCE	MONSEGUR	10.33.37.0	255.255.255.0
0332569N	CLG	PORTE DU MEDOC	PAREMPUYRE	10.33.136.0	255.255.255.0
0330103H	CLG	PIERRE DE BELLEYME	PAUILLAC	10.33.39.0	255.255.255.0
0330105K	CLG	CHAMP D'EYMET	PELLEGRUE	10.33.40.0	255.255.255.0
0330106L	CLG	FRANCOIS MITTERRAND	PESSAC	10.33.41.0	255.255.255.0
0331623K	CLG	ALOUETTE	PESSAC	10.33.77.0	255.255.255.0
0331758G	CLG	NOES	PESSAC	10.33.92.0	255.255.255.0
0332191C	CLG	GERARD PHILIPPE	PESSAC	10.33.112.0	255.255.255.0
0332723F	CLG	EMILE DURKHEIM	PEUJARD	10.33.142.0	255.255.255.0
0330108N	CLG	G. BRASSENS	PODENSAC	10.33.42.0	255.255.255.0
0331433D	CLG	PIERRE MARTIN	RAUZAN	10.33.65.0	255.255.255.0
0331666G	CLG	ALIENOR D'AQUITAINE	SALLES	10.33.83.0	255.255.255.0
0331667H	CLG	ROBERT BARRIERE	SAUVETERRE GUYENNE	10.33.84.0	255.255.255.0
0330125G	CLG	GEORGES MANDEL	SOULAC SUR MER	10.33.49.0	255.255.255.0
0331757F	CLG	LA GAROSSE	ST ANDRE DE CUBZAC	10.33.91.0	255.255.255.0
0333093H	CLG	LEONARD DE VINCY	ST AUBIN DU MEDOC	10.33.162.0	255.255.255.0
0330113U	CLG	JEAN MONNET	ST CIERS SUR GIRONDE	10.33.44.0	255.255.255.0
0333134C	CLG	de l'ESTEY	ST JEAN D'ILLAC	10.33.151.0	255.255.255.0
0332340P	CLG	MAX LINDER	ST LOUBES	10.33.123.0	255.255.255.0
0331664E	CLG	FRANCOIS MAURIAC	ST MEDARD EN JALLES	10.33.81.0	255.255.255.0
0332187Y	CLG	HASTIGNAN	ST MEDARD EN JALLES	10.33.109.0	255.255.255.0
0330122D	CLG	FRANCOIS MAURIAC	ST SYMPHORIEN	10.33.48.0	255.255.255.0
0331888Y	CLG	DU VAL DE SAYE	ST YZAN DE SOUDIAC	10.33.99.0	255.255.255.0
0332705L	CLG	FRANCOIS MAURIAC	STE EULALIE	10.33.139.0	255.255.255.0
0330163Y	CLG	ELIE FAURE	STE FOY LA GRANDE	10.33.62.0	255.255.255.0
0330128K	CLG	HENRI BRISSON	TALENCE	10.33.52.0	255.255.255.0
0332195G	CLG	VICTOR LOUIS	TALENCE	10.33.115.0	255.255.255.0
0332706M	CLG	LEO DROUYN	VERAC	10.33.140.0	255.255.255.0
0330132P	CLG	PONT DE LA MAYE	VILLENAVE ORNON	10.33.54.0	255.255.255.0
0332246M	CLG	CHAMBERY	VILLENAVE ORNON	10.33.152.0	255.255.255.0

Collèges des Landes

RNE	Type	Nom	Ville	IP Admin	Masque Admin
0400090F	CLG	GASTON CRAMPE	AIRE SUR ADOUR	10.233.227.0	255.255.255.0
0400003L	CLG	DU PAYS DES LUYS	AMOU	10.234.39.0	255.255.255.0
0400092H	CLG	JEAN MERMOZ	BISCARROSSE	10.234.57.0	255.255.255.0
0401048X	CLG	NELSON MANDELA	BISCARROSSE	10.233.146.0	255.255.255.0
0400005N	CLG	JEAN ROSTAND	CAPBRETON	10.234.40.0	255.255.255.0
0400729A	CLG	L. DUSSARAT dit LEON DES LANDES	DAX	10.234.66.0	255.255.255.0
0400740M	CLG	D'ALBRET	DAX	10.234.67.0	255.255.255.0
0400010U	CLG	JULES FERRY	GABARRET	10.234.41.0	255.255.255.0
0400011V	CLG	PIERRE DE CASTELNAU	GEAUNE	10.234.42.0	255.255.255.0
0400012W	CLG	VAL D ADOUR	GRENADE SUR L'ADOUR	10.234.43.0	255.255.255.0
0400727Y	CLG	JEAN MARIE LONNE	HAGETMAU	10.234.64.0	255.255.255.0
0401014K	CLG	LABENNE	LABENNE	10.233.147.0	255.255.255.0
0400014Y	CLG	FELIX ARNAUDIN	LABOUHEYRE	10.234.44.0	255.255.255.0
0401077D	CLG	LABRIT	LABRIT	10.234.183.0	255.255.255.0
0401015L	CLG	LUCIE AUBRAC	LINXE	10.233.145.0	255.255.255.0
0400105X	CLG	JACQUES PREVERT	MIMIZAN	10.234.63.0	255.255.255.0
0400648M	CLG	VICTOR DURUY	MONT DE MARSAN	10.233.228.0	255.255.255.0
0400774Z	CLG	CEL LE GAUCHER	MONT DE MARSAN	10.233.172.0	255.255.255.0
0400779E	CLG	JEAN ROSTAND	MONT DE MARSAN	10.233.173.0	255.255.255.0
0400023H	CLG	SERGE BARRANX	MONTFORT EN CHALOSSE	10.233.167.0	255.255.255.0
0400093J	CLG	H. SCOGNAMIGLIO	MORCENX	10.234.58.0	255.255.255.0
0400025K	CLG	RENE SOUBAIGNE	MUGRON	10.234.47.0	255.255.255.0
0400026L	CLG	SAINT EXUPERY	PARENTIS EN BORN	10.233.226.0	255.255.255.0
0400028N	CLG	DU PAYS D'ORTHE	PEYREHORADE	10.234.48.0	255.255.255.0
0400032T	CLG	ROSA PARKS	POUILLON	10.234.49.0	255.255.255.0
0400033U	CLG	MARIE CURIE	RION DES LANDES	10.233.175.0	255.255.255.0
0400034V	CLG	GEORGE SAND	ROQUEFORT	10.234.50.0	255.255.255.0
0400728Z	CLG	F. MITTERRAND	SOUSTONS	10.234.65.0	255.255.255.0
0401070W	CLG	AIME CESAIRE	ST GEOURS DE MAREMNE	10.234.113.0	255.255.255.0
0400874H	CLG	FRANCOIS TRUFFAUT	ST MARTIN DE SEIGNANX	10.234.68.0	255.255.255.0
0400096M	CLG	JEAN MOULIN	ST PAUL LES DAX	10.234.60.0	255.255.255.0
0401066S	CLG	DANIELLE MITTERRAND	St Paul les Dax	10.234.177.0	255.255.255.0
0400103V	CLG	LUBET BARBON	ST PIERRE DU MONT	10.234.62.0	255.255.255.0
0400038Z	CLG	CAP DE GASCOGNE	ST SEVER	10.234.51.0	255.255.255.0
0400039A	CLG	JEAN-CLAUDE SESCOUSSE	ST VINCENT DE TYROSSE	10.234.52.0	255.255.255.0
0400091G	CLG	LANGEVIN WALLON	TARNOS	10.234.56.0	255.255.255.0
0400042D	CLG	JEAN ROSTAND	TARTAS	10.233.169.0	255.255.255.0
0400043E	CLG	PIERRE BLANQUIE	VILLENEUVE DE MARSAN	10.233.170.0	255.255.255.0

Collèges du Lot-et-Garonne*

RNE	Type	Nom	Ville	IP Admin	Masque Admin
0470005A	CLG	JASMIN LES ILES	AGEN	10.233.176.0	255.255.255.0
0470008D	CLG	PAUL DANGLA	AGEN	10.233.177.0	255.255.255.0
0470677F	CLG	DUCOS DU HAURON	AGEN	10.234.98.0	255.255.255.0
0470777P	CLG	JOSEPH CHAUMIE	AGEN	10.234.103.0	255.255.255.0
0470720C	CLG	LA ROCAL	BON ENCONTRE	10.234.99.0	255.255.255.0
0470011G	CLG	GASTON CARRERE	CASSENEUIL	10.234.79.0	255.255.255.0
0470012H	CLG	JEAN ROSTAND	CASTELJALOUX	10.234.80.0	255.255.255.0
0470732R	CLG	LUCIE AUBRAC	CASTELMORON SUR LOT	10.234.100.0	255.255.255.0
0470014K	CLG	JEAN BOUCHERON	CASTILLONNES	10.234.81.0	255.255.255.0
0470017N	CLG	LUCIEN SIGALA	DURAS	10.234.83.0	255.255.255.0
0470046V	CLG	JEAN MONNET	FUMEL	10.234.84.0	255.255.255.0
0470775M	CLG	LA PLAINE	LAVARDAC	10.234.102.0	255.255.255.0
0470043S	CLG	DANIEL CASTAING	LE MAS D AGENAIS	10.234.92.0	255.255.255.0
0470105J	CLG	THEOPHILE DE VIAU	LE PASSAGE	10.234.97.0	255.255.255.0
0470103G	CLG	JEAN MOULIN	MARMANDE	10.233.183.0	255.255.255.0
0470023V	CLG	ARMAND FALLIERE	MEZIN	10.234.85.0	255.255.255.0
0470024W	CLG	DIDIER LAMOULIE	MIRAMONT DE GUYENNE	10.234.86.0	255.255.255.0
0470026Y	CLG	Joseph KESSE	MONFLANQUIN	10.234.87.0	255.255.255.0
0470048X	CLG	KLEBER THOUEILLES	MONSEMPRON LIBOS	10.234.94.0	255.255.255.0
0470031D	CLG	DAMIRA ASPERTI	PENNE D AGENAIS	10.234.89.0	255.255.255.0
0470032E	CLG	J.PH. DELMAS DE GRAMMONT	PORT STE MARIE	10.234.90.0	255.255.255.0
0470102F	CLG	PAUL FROMENT	STE LIVRADE SUR LOT	10.234.96.0	255.255.255.0
0470104H	CLG	GERMILLAC	TONNEINS	10.233.200.0	255.255.255.0
0470049Y	CLG	ANATOLE FRANCE	VILLENEUVE SUR LOT	10.234.95.0	255.255.255.0
0470678G	CLG	ANDRE CROCHEPIERRE	VILLENEUVE SUR LOT	10.233.181.0	255.255.255.0

** 3 collèges sont inclus dans des cités scolaires et ont leur administration sur le même réseau que celui d'un des autres établissements qui les composent:*

- 0470774L Collège Stendhal à Aiguillon

- 0470776N Collège Henri de Navarre à Nérac

- 0470733S Collège Val de Garonne à Marmande

Collèges des Pyrénées-Atlantiques

RNE	Type	Nom	Ville	IP Admin	Masque Admin
0640003F	CLG	ENDARRA	ANGLET	10.233.110.0	255.255.255.0
0640004G	CLG	DE BARETOUS	ARETTE	10.234.141.0	255.255.255.0
0640005H	CLG	CORISANDE D ANDOINS	ARTHEZ DE BEARN	10.233.111.0	255.255.255.0
0640231D	CLG	JEAN MOULIN	ARTIX	10.234.152.0	255.255.255.0
0640007K	CLG	D'OSSAU	ARUDY	10.234.142.0	255.255.255.0
0640008L	CLG	ARZACQ	ARZACQ ARRAZIGUET	10.233.184.0	255.255.255.0
0640212H	CLG	MARRACQ	BAYONNE	10.233.132.0	255.255.255.0
0640609P	CLG	ALBERT CAMUS	BAYONNE	10.233.136.0	255.255.255.0
0640016V	CLG	D'ASPE	BEDOUS	10.233.185.0	255.255.255.0
0640078M	CLG	VILLA FAL	BIARRITZ	10.233.130.0	255.255.255.0
0641414P	CLG	JEAN ROSTAND	BIARRITZ	10.233.140.0	255.255.255.0
0640019Y	CLG	DU PAYS DE BIDACHE	BIDACHE	10.233.116.0	255.255.255.0
0640606L	CLG	DU BOIS D'AMOUR	BILLERE	10.234.153.0	255.255.255.0
0641413N	CLG	DES LAVANDIERES	BIZANOS	10.234.158.0	255.255.255.0
0640023C	CLG	HENRI BARBUSSE	BOUCAU	10.233.117.0	255.255.255.0
0641392R	CLG	ERROBI	CAMBO LES BAINS	10.233.138.0	255.255.255.0
0640025E	CLG	JOSEPH PEYRE	GARLIN	10.233.186.0	255.255.255.0
0641393S	CLG	ELHUYAR	HASPARREN	10.233.139.0	255.255.255.0
0640228A	CLG	IRANDATZ	HENDAYE	10.233.134.0	255.255.255.0
0641411L	CLG	ERNEST GABARD	JURANCON	10.234.156.0	255.255.255.0
0640035R	CLG	LES CINQ MONTS	LARUNS	10.233.188.0	255.255.255.0
0640036S	CLG	PIERRE JELIOTE	LASSEUBE	10.234.143.0	255.255.255.0
0640037T	CLG	DU VIC-BILH	LEMBEYE	10.234.144.0	255.255.255.0
0641391P	CLG	SIMIN PALAY	LESCAR	10.233.198.0	255.255.255.0
0640039V	CLG	ARGIA	MAULEON SOULE	10.233.119.0	255.255.255.0
0640041X	CLG	RECTEUR J. SARRAILH	MONEIN	10.234.145.0	255.255.255.0
0641412M	CLG	LA HOURQUIE	MORLAAS	10.234.157.0	255.255.255.0
0641561Z	CLG	ALBERT CAMUS	MOURENX	10.234.107.0	255.255.255.0
0640045B	CLG	DES REMPARTS	NAVARRENX	10.233.190.0	255.255.255.0
0641509T	CLG	HENRI IV	NAY BOURDETTES	10.234.159.0	255.255.255.0
0640048E	CLG	DES CORDELIERS	OLORON STE MARIE	10.233.193.0	255.255.255.0
0640211G	CLG	TRISTAN DEREME	OLORON STE MARIE	10.233.246.0	255.255.255.0
0640214K	CLG	DANIEL ARGOTE	ORTHEZ	10.233.133.0	255.255.255.0
0641560Y	CLG	GASTON FEBUS	ORTHEZ	10.234.203.0	255.255.255.0
0640227Z	CLG	JEANNE D'ALBRET	PAU	10.233.196.0	255.255.255.0
0640607M	CLG	MARGUERITE DE NAVARRE	PAU	10.234.154.0	255.255.255.0
0640608N	CLG	CLERMONT	PAU	10.233.197.0	255.255.255.0
0642095E	CLG	INNOVANT PIERRE EMMANUEL	PAU	10.234.155.0	255.255.255.0
0640062V	CLG	JEAN BOUZET	PONTACQ	10.233.195.0	255.255.255.0
0640071E	CLG	FELIX PECAUT	SALIES DE BEARN	10.233.127.0	255.255.255.0
0640073G	CLG	REINE SANCIE	SAUVETERRE DE BEARN	10.233.128.0	255.255.255.0
0641780M	CLG	RENE FORGUES	SERRES CASTET	10.234.161.0	255.255.255.0
0640064X	CLG	JEAN PUJO	ST ETIENNE BAIGORRY	10.233.123.0	255.255.255.0
0640229B	CLG	CHANTACO	ST JEAN DE LUZ	10.233.135.0	255.255.255.0
0641559X	CLG	MAURICE RAVEL	ST JEAN DE LUZ	10.234.206.0	255.255.255.0
0640069C	CLG	LA CITADELLE	ST JEAN PIED DE PORT	10.233.126.0	255.255.255.0
0641232S	CLG	LEON BERARD	ST PALAIS	10.233.137.0	255.255.255.0
0642038T	CLG	ATURRI	ST PIERRE D'IRUBE	10.233.144.0	255.255.255.0
0640074H	CLG	DR PIERRE JAUREGUY	TARDETS SORHOLUS	10.233.129.0	255.255.255.0

Lycées et EREA*

RNE	Type	Nom	Dept	Ville	IP Admin	Masque Admin
0240005A	LGT	MAINE DE BIRAN	24	BERGERAC	10.233.150.0	255.255.255.0
0240006B	LP	DE L'ALBA	24	BERGERAC	10.234.116.0	255.255.255.0
0240007C	LP	JEAN CAPELLE	24	BERGERAC	10.233.151.0	255.255.255.0
0240012H	LP	METIERS DU BATIMENT	24	COULAURES	10.233.165.0	255.255.255.0
0240013J	LG	GIRAUT DE BORNEIL	24	EXCIDEUIL	10.234.118.0	255.255.255.0
0240021T	LPO	ALCIDE DUSOLIER	24	NONTRON	10.233.155.0	255.255.255.0
0240024W	LG	BERTRAN DE BORN	24	PERIGUEUX	10.234.16.0	255.255.255.0
0240025X	LGT	LAURE GATET	24	PERIGUEUX	10.233.203.0	255.255.255.0
0241137F	LGT	JAY DE BEAUFORT	24	PERIGUEUX	10.234.14.0	255.255.255.0
0240028A	LP	PABLO PICASSO	24	PERIGUEUX	10.233.156.0	255.255.255.0
0240984P	LP	LEONARD DE VINCY	24	PERIGUEUX	10.234.137.0	255.255.255.0
0240026Y	LPO	ALBERT CLAVEILLE	24	PERIGUEUX	10.233.207.0	255.255.255.0
0240032E	LGT	CITE SCOL. A. DANIEL	24	RIBERAC	10.234.121.0	255.255.255.0
0240035H	LGT	PRE DE CORDY	24	SARLAT	10.233.158.0	255.255.255.0
0240048X	LP	PRE DE CORDY	24	SARLAT	10.234.182.0	255.255.255.0
0241125T	LPO	ANTOINE ST EXUPERY	24	TERRASSON	10.234.140.0	255.255.255.0
0240039M	LP	PORTE D'AQUITAINE	24	THIVIERS	10.233.204.0	255.255.255.0
0240112S	EREA	JOEL JEANNOT	24	TRELISSAC	10.234.131.0	255.255.255.0
0332724G	LG	NORD BASSIN	33	ANDERNOS LES BAINS	10.33.143.0	255.255.255.0
0330003Z	LGT	GRAND AIR	33	ARCACHON	10.233.252.0	255.255.255.0
0332194F	LP	CONDORCET	33	ARCACHON	10.33.114.0	255.255.255.0
0330010G	LGT	ANATOLE DE MONZIE	33	BAZAS	10.33.4.0	255.255.255.0
0331882S	LP	EMILE COMBES	33	BEGLES	10.33.96.0	255.255.255.0
0333273D	LPO	VACLAV HAVEL	33	BEGLES	10.233.209.0	255.255.255.0
0332745E	LG	JEAN MONNET	33	BLANQUEFORT	10.234.10.0	255.255.255.0
0330018R	LP	BLANQUEFORT	33	BLANQUEFORT	10.33.7.0	255.255.255.0
0330020T	LGT	JAUFRE RUDEL	33	BLAYE	10.233.253.0	255.255.255.0
0332781U	LP	DE L'ESTUAIRE	33	BLAYE	10.33.150.0	255.255.255.0
0330021U	LG	MICHEL MONTAIGNE	33	BORDEAUX	10.33.9.0	255.255.255.0
0330022V	LG	MONTESQUIEU	33	BORDEAUX	10.233.254.0	255.255.255.0
0330022V	LG	MONTESQUIEU (Annexe)	33	BORDEAUX	10.33.134.0	255.255.255.0
0330026Z	LG	FRANCOIS MAGENDIE	33	BORDEAUX	10.233.251.0	255.255.255.0
0330023W	LGT	CAMILLE JULLIAN	33	BORDEAUX	10.234.1.0	255.255.255.0
0330027A	LGT	FRANCOIS MAURIAC	33	BORDEAUX	10.234.3.0	255.255.255.0
0332747G	LGT	JEAN CONDORCET (Annexe)	33	BORDEAUX	10.33.78.0	255.255.255.0
0332747G	LGT	JEAN CONDORCET	33	BORDEAUX	10.233.250.0	255.255.255.0
0330031E	LP	TOULOUSE LAUTREC	33	BORDEAUX	10.33.16.0	255.255.255.0
0330032F	LP	NICOLAS BREMONTIER	33	BORDEAUX	10.234.108.0	255.255.255.0
0330033G	LP	DES MENUTS	33	BORDEAUX	10.33.18.0	255.255.255.0
0330142A	LP	TREGEY	33	BORDEAUX	10.33.58.0	255.255.255.0
0331460H	LP	LES CHARTRONS	33	BORDEAUX	10.33.67.0	255.255.255.0
0332445D	LP	A. BEAU DE ROCHAS	33	BORDEAUX	10.234.15.0	255.255.255.0
0330028B	LPO	GUSTAVE EIFFEL	33	BORDEAUX	10.233.242.0	255.255.255.0
0330029C	LT	NICOLAS BREMONTIER	33	BORDEAUX	10.233.243.0	255.255.255.0
0332468D	LT	SAINT LOUIS	33	BORDEAUX	10.233.248.0	255.255.255.0
0330060L	LP	FLORA TRISTAN	33	CAMBLANES ET MEYNAC	10.33.21.0	255.255.255.0
0330069W	LP	LA MORLETTE	33	CENON	10.33.26.0	255.255.255.0

RNE	Type	Nom	Dept	Ville	IP Admin	Masque Admin
0331739L	EREA	DE LA PLAINE	33	EYSINES	10.33.87.0	255.255.255.0
0330076D	LP	CHARLES PEGUY	33	EYSINES	10.33.27.0	255.255.255.0
0332846P	LG	DES GRAVES	33	GRADIGNAN	10.234.12.0	255.255.255.0
0332870R	LPO	DE LA MER (Annexe de Biganos)	33	GUJAN MESTRAS	10.233.237.0	255.255.255.0
0332870R	LPO	DE LA MER	33	GUJAN MESTRAS	10.233.245.0	255.255.255.0
0330109P	LPO	JEAN RENOU	33	LA REOLE	10.33.43.0	255.255.255.0
0331636Z	LG	JEAN MOULIN	33	LANGON	10.234.6.0	255.255.255.0
0330082K	LP	DES METIERS SUD GIRONDE	33	LANGON	10.33.29.0	255.255.255.0
0332831Y	LG	SUD MEDOC	33	LE TAILLAN MEDOC	10.234.11.0	255.255.255.0
0330088S	LGT	MAX LINDER	33	LIBOURNE	10.234.4.0	255.255.255.0
0330089T	LP	IND-HOT. J. MONNET	33	LIBOURNE	10.33.33.0	255.255.255.0
0332344U	LP	HENRI BRULLE	33	LIBOURNE	10.33.127.0	255.255.255.0
0332744D	LGT	ELIE FAURE	33	LORMONT	10.234.9.0	255.255.255.0
0332441Z	LP	JACQUES BREL	33	LORMONT	10.33.132.0	255.255.255.0
0332832Z	LT	LES IRIS	33	LORMONT	10.233.249.0	255.255.255.0
0331760J	LGT	FERNAND DAGUIN	33	MERIGNAC	10.234.8.0	255.255.255.0
0331668J	LP	MARCEL DASSAULT	33	MERIGNAC	10.33.85.0	255.255.255.0
0332081H	LGT	ODILON REDON	33	PAUILLAC	10.234.109.0	255.255.255.0
0332081H	LGT	ODILON REDON (Annexe Lesparre)	33	PAUILLAC	10.33.94.0	255.255.255.0
0330102G	LP	ODILON REDON	33	PAUILLAC	10.234.7.0	255.255.255.0
0332198K	EREA	LE CORBUSIER	33	PESSAC	10.33.116.0	255.255.255.0
0332722E	LGT	PAPE CLEMENT	33	PESSAC	10.33.141.0	255.255.255.0
0332345V	LP	PHILADELPHE DE GERDE	33	PESSAC	10.33.128.0	255.255.255.0
0332346W	LP	PHILIPPE COUSTEAU	33	ST ANDRE DE CUBZAC	10.33.129.0	255.255.255.0
0330119A	LP	JEHAN DUPERIER	33	ST MEDARD EN JALLES	10.33.47.0	255.255.255.0
0330115W	LG	RECLUS	33	STE FOY LA GRANDE	10.33.46.0	255.255.255.0
0330126H	LPO	VICTOR LOUIS	33	TALENCE	10.234.5.0	255.255.255.0
0330135T	LPO	ALFRED KASTLER	33	TALENCE	10.233.244.0	255.255.255.0
0332192D	LPO	HOTELIER TOURISME	33	TALENCE	10.33.113.0	255.255.255.0
0400047J	LP	JEAN D ARCET	40	AIRE SUR ADOUR	10.234.54.0	255.255.255.0
0400002K	LPO	GASTON CRAMPE	40	AIRE SUR ADOUR	10.234.25.0	255.255.255.0
0400004M	LP	LOUIS DARMANTE	40	CAPBRETON	10.233.202.0	255.255.255.0
0400007R	LPO	DE BORDA	40	DAX	10.234.17.0	255.255.255.0
0400017B	LGT	VICTOR DURUY	40	MONT DE MARSAN	10.234.18.0	255.255.255.0
0400018C	LGT	CHARLES DESPIAU	40	MONT DE MARSAN	10.234.24.0	255.255.255.0
0400019D	LP	FREDERIC ESTEVE	40	MONT DE MARSAN	10.234.45.0	255.255.255.0
0400020E	LP	ROBERT WLERICK	40	MONT DE MARSAN	10.234.46.0	255.255.255.0
0400097N	LP	JEAN GARNIER	40	MORCENX	10.234.61.0	255.255.255.0
0400046H	LG	SAINT EXUPERY	40	PARENTIS EN BORN	10.234.53.0	255.255.255.0
0400057V	LP	SAINT EXUPERY	40	PARENTIS EN BORN	10.234.55.0	255.255.255.0
0400027M	LP	JEAN TARIS	40	PEYREHORADE	10.233.168.0	255.255.255.0
0401002X	LPO	HAROUN TAZIEFF	40	ST PAUL LES DAX	10.233.174.0	255.255.255.0
0400094K	EREA	NICOLAS BREMONTIER	40	ST PIERRE DU MONT	10.234.59.0	255.255.255.0
0400933X	LGT	SUD DES LANDES	40	ST VINCENT DE TYROSSE	10.234.69.0	255.255.255.0
0400049L	LP	AMBROISE CROIZAT	40	TARNOS	10.233.171.0	255.255.255.0
0470004Z	LP	ANTOINE LOMET	47	AGEN	10.234.78.0	255.255.255.0
0470003Y	LT	JEAN BAPT. DE BAUDRE	47	AGEN	10.234.26.0	255.255.255.0
0470001W	LGT	BERNARD PALISSY	47	AGEN CEDEX	10.233.182.0	255.255.255.0
0470009E	LG	STENDHAL	47	AIGUILLON	10.233.178.0	255.255.255.0
0470015L	LP	DES METIERS PORTE DU LOT	47	CLAIRAC	10.234.82.0	255.255.255.0
0470782V	LP	JEAN MONNET	47	FOULAYRONNES	10.234.104.0	255.255.255.0
0470641S	LP	BENOIT D'AZY	47	FUMEL	10.234.21.0	255.255.255.0
0470020S	LGT	VAL DE GARONNE	47	MARMANDE	10.234.20.0	255.255.255.0
0470028A	LG	GEORGE SAND	47	NERAC	10.233.179.0	255.255.255.0
0470029B	LP	JACQUES DE ROMAS	47	NERAC	10.234.88.0	255.255.255.0

RNE	Type	Nom	Dept	Ville	IP Admin	Masque Admin
0470753N	EREA	MARIE-CLAUDE LERICHE	47	VILLENEUVE SUR LOT	10.234.101.0	255.255.255.0
0470040N	LP	LOUIS COUFFIGNAL	47	VILLENEUVE SUR LOT	10.234.91.0	255.255.255.0
0470038L	LPO	GEORGES LEYGUES	47	VILLENEUVE SUR LOT	10.233.180.0	255.255.255.0
0640001D	LPO	DES METIERS CANTAU	64	ANGLET	10.233.109.0	255.255.255.0
0640010N	LG	RENE CASSIN	64	BAYONNE	10.233.112.0	255.255.255.0
0640010N	LG	RENE CASSIN (Annexe Biarritz)	64	BAYONNE	10.233.241.0	255.255.255.0
0640011P	LGT	LOUIS DE FOIX	64	BAYONNE	10.233.113.0	255.255.255.0
0640013S	LP	PAUL BERT	64	BAYONNE	10.233.114.0	255.255.255.0
0640017W	LG	EXPERIMENTAL MALRAUX	64	BIARRITZ	10.234.205.0	255.255.255.0
0641823J	LPO	HOTELIER	64	BIARRITZ	10.233.142.0	255.255.255.0
0641779L	LGT	DU PAYS DE SOULE	64	CHERAUTE	10.233.141.0	255.255.255.0
0640098J	LP	GABRIEL HAURE PLACE	64	COARRAZE	10.234.151.0	255.255.255.0
0640026F	LP	DES METIERS DE L'HABITAT	64	GELOS	10.233.187.0	255.255.255.0
0640028H	LP	AIZPURDI	64	HENDAYE	10.233.118.0	255.255.255.0
0640031L	LP	ANDRE CAMPA	64	JURANCON	10.233.201.0	255.255.255.0
0641839B	LGT	JACQUES MONOD	64	LESCAR	10.234.162.0	255.255.255.0
0640040W	LP	JEAN-PIERRE CHAMPO	64	MAULEON SOULE	10.233.120.0	255.255.255.0
0640042Y	LP	DES METIERS HAUTE VUE	64	MORLAAS	10.233.189.0	255.255.255.0
0640044A	LG	ALBERT CAMUS	64	MOURENX	10.234.146.0	255.255.255.0
0640046C	LG	PAUL REY	64	NAY BOURDETTES	10.233.191.0	255.255.255.0
0640047D	LG	JULES SUPERVIELLE	64	OLORON STE MARIE	10.233.192.0	255.255.255.0
0640049F	LP	GUYNEMER	64	OLORON STE MARIE	10.234.147.0	255.255.255.0
0640050G	LP	IV SEPTEMBRE	64	OLORON STE MARIE	10.233.194.0	255.255.255.0
0640052J	LGT	GASTON FEBUS	64	ORTHEZ	10.233.121.0	255.255.255.0
0640053K	LP	FRANCIS JAMMES	64	ORTHEZ	10.233.122.0	255.255.255.0
0640080P	LP	MOLIERE	64	ORTHEZ	10.233.131.0	255.255.255.0
0640055M	LG	LOUIS BARTHOU	64	PAU	10.234.148.0	255.255.255.0
0641732K	LGT	SAINT-JOHN PERSE	64	PAU	10.234.160.0	255.255.255.0
0640058R	LP	HONORE BARADAT	64	PAU	10.234.150.0	255.255.255.0
0641815A	LP	Saint-Cricq Nitot	64	PAU	10.234.187.0	255.255.255.0
0640057P	LPO	SAINT CRICQ	64	PAU	10.234.149.0	255.255.255.0
0640065Y	LG	MAURICE RAVEL	64	ST JEAN DE LUZ	10.233.124.0	255.255.255.0
0640066Z	LP	RAMIRO ARRUE	64	ST JEAN DE LUZ	10.233.125.0	255.255.255.0
0641844G	LGT	DE NAVARRE	64	ST JEAN PIED DE PORT	10.233.143.0	255.255.255.0

**7 lycées sont inclus dans des cités scolaires et ont leur administration sur le même réseau que celui d'un des autres établissements qui les composent:*

- 0240050Z LP Arnaud Daniel à Riberac

- 0330011H LP Anatole de Monzie à Bazas

- 0330114V LP Paul Broca à Ste Foy la Grande

- 0332835C LGT Philippe Cousteau à St André de Cubzac

- 0470018P LGT Marguerite Filhol à Fumel

- 0640012R LP Louis de Foix à Bayonne

- 0640079N LP Pierre et Marie Curie à Mourenx

Annexe 2 - modèle de délégation d'usage de nom de domaine

Logo
Intitulé de la collectivité

Direction
Service

Réf :
Dossier suivi par :

Monsieur le Recteur de la région académique Nouvelle-Aqu
Recteur de l'académie de Bordeaux
Chancelier des Universités
5 Rue Joseph de Carayon Latour
CS 81499
33060 BORDEAUX Cedex

le

Monsieur le Recteur,

En tant que représentant du conseil *****, titulaire auprès de l'AFNIC du nom de domaine ***.fr, je délègue ou subdélègue ma responsabilité portant sur le nom de domaine suivant :

*****.fr**

au bénéfice du Ministère de l'Education nationale, de l'Enseignement supérieur et de la Recherche, représenté en ce domaine par :

- **M. Patrick BENAZET**, RSSI de l'académie de Bordeaux,
- **M. Fabrice FLAUSS,** ISR (ingénieur de sécurité RACINE) au rectorat de l'Académie de Bordeaux

Ces personnes sont autorisées à valider la ou les demandes d'utilisation du nom de domaine précité aux fins de gérer tous les aspects d'enregistrement des certificats électroniques délivrés par la plate-forme nationale de confiance numérique (PNCN) de Toulouse.

Je vous prie de croire, Monsieur le Recteur, à l'assurance de ma considération distinguée.

Adresse
Tél :
Fax :
Mél :