Mutualisation d'un service d'accès à distance sécurisé VPN

Laurence Moindrot, Jean Benoit

Mutualisation d'un service d'accès à distance sécurisé VPN

Laurence Moindrot
Centre Réseau Communication, Université Louis Pasteur
7 rue René Descartes F-67084 Strasbourg
Laurence.Moindrot@crc.u-strasbg.fr

Jean Benoit
Centre Réseau Communication, Université Louis Pasteur
7 rue René Descartes F-67084 Strasbourg
Jean.Benoit@crc.u-strasbg.fr

Résumé

Le Centre Réseau Communication, gestionnaire du réseau métropolitain Osiris pour le compte de 16 établissements strasbourgeois, offre de nombreux services mutualisés à l'ensemble des utilisateurs de la communauté de l'enseignement et de la recherche.

En 2004, le CRC a mis en œuvre un service d'accès distant sécurisé VPN pouvant répondre aux attentes des différentes composantes (établissement, laboratoire, service, etc). La prise en charge de l'hétérogénéité de la population d'utilisateurs (incluant des novices en informatique), de leur système d'exploitation, des ressources auxquelles ils souhaitent accéder, ainsi que de la politique de sécurité de leur composante faisait partie des principales contraintes.

Le CRC offre aujourd'hui des solutions d'accès nomade personnalisées ; la plus avancée d'entre elles permet à un utilisateur d'avoir virtuellement une prise Ethernet dans son réseau de composante. De plus, le support d'IPv6 et de la haute disponibilité en fait une solution de qualité.

Cet article explique le choix de la solution, les avantages de la mutualisation, ainsi que le mode opératoire de mise en œuvre d'un serveur VPN virtuel pour une composante.

Mots clefs

Nomadisme, VPN, mutualisation, haute disponibilité, IPv6, service.

1 Introduction

Aujourd'hui, beaucoup d'organismes de l'enseignement et de la recherche s'équipent d'un serveur VPN pour offrir des accès distants sécurisés et permettre à leurs utilisateurs d'accéder aux ressources internes de leur organisation.

Le Centre Réseau Communication (CRC) a décidé de mettre en place une solution mutualisée afin de proposer à toute la communauté *Osiris* un service de qualité à moindre coût répondant aux attentes du plus grand nombre. Le service proposé permet à chaque composante (établissement, laboratoire, service, etc.) de disposer d'un serveur VPN virtuel et d'offrir à ses utilisateurs une solution personnalisée.

Après avoir présenté le contexte de déploiement du service, nous mettrons en avant les avantages d'une solution mutualisée et présenterons l'offre du CRC. Nous ferons ensuite un rappel des diverses technologies VPN existantes et expliquerons notre choix. Avant de présenter le bilan d'exploitation, nous présenterons les fonctionnalités mises en œuvre ainsi que le mode opératoire nécessaire à l'activation d'un serveur VPN virtuel dans un sous réseau d'*Osiris*.

2 Contexte

Le réseau *Osiris* est le réseau métropolitain regroupant la quasi-totalité des établissements de l'enseignement supérieur et de la recherche implantés sur le territoire de la Communauté Urbaine de Strasbourg (CUS). Au total, 16 établissements sont connectés, ce qui représente 20 sites, 120 bâtiments, plus de 26 000 machines déclarées dans le DNS et 50 000 utilisateurs.

L'infrastructure du réseau *Osiris* est composée de cinq sites de concentration maillés et connectés avec des liens multiGigabit. Chaque réseau de composante est relié au site de concentration le plus proche au travers de liaisons à haut débit en utilisant majoritairement des fibres optiques privatives. Le routage IPv4 et IPv6 est effectué sur les sites de concentration.

Le réseau *Osiris* est opéré par le CRC, service commun de l'Université Louis Pasteur (ULP), pour le compte de l'ensemble des établissements membres d'*Osiris*.

La séparation du niveau de responsabilité entre le cœur de réseau *Osiris* et les réseaux de composantes se fait au niveau des ports Ethernet du commutateur d'entrée de bâtiment.

Les interlocuteurs privilégiés des réseaux de composantes sont les « correspondants réseau » qui s'occupent entre autre des politiques de sécurité locales, de la gestion des plages d'adresses IP qui leur sont confiées, ainsi que du support de premier niveau de leurs utilisateurs.

Hormis la gestion du réseau de transport *Osiris*, le CRC propose de très nombreux services mutualisés aux utilisateurs de l'ensemble des établissements membres : hébergement de boîtes aux lettres, relais de messagerie, synchronisation de temps (NTP), service de nommage

(DNS), transfert de fichiers (FTP), listes de diffusion, accès au réseau sans fil (WiFi) et depuis 2005 service d'accès distant sécurisé VPN.

La généralisation de la mise en place des annuaires d'établissements ainsi que des Environnements Numériques de Travail (E.N.T.) a contribué à la création de l'infrastructure d'authentification du CRC [1] sur laquelle reposent tous les services proposés.

3 Avantages de la mutualisation

L'implémentation d'une solution de service d'accès distant sécurisé VPN est une tâche lourde et complexe en raison de l'ingénierie à mettre en œuvre, de l'exploitation quotidienne et du support aux utilisateurs.

Le déploiement d'un service VPN nécessite une connaissance approfondie des technologies IP, de sécurité, de tunneling, de chiffrement, et d'authentification. L'installation d'un service VPN sans connaissance minimum et sans suivi régulier peut très vite devenir une faille de sécurité.

Les diverses opérations de configuration, d'installation et d'administration du service sont très lourdes. Parmi ces opérations, on peut citer la mise à jour matérielle et logicielle des serveurs, le suivi des incidents, la mise à jour et la validation des logiciels clients, la supervision du service, ou encore la gestion des accès. Si l'on souhaite un service de qualité, ce travail prend beaucoup de temps.

La gestion des utilisateurs est également très dense. La particularité de ce service est que les utilisateurs se connectent peu pendant les heures de bureau. De plus, certains ne maîtrisent pas toujours les outils informatiques. Afin de répondre au mieux à leurs attentes, il faut pouvoir fournir une documentation précise, à jour, simplifiée mais complète.

Au vu de ces nombreuses tâches, il semble évident qu'une solution mutualisée permet d'offrir un service de qualité tout en déchargeant les administrateurs locaux de contraintes importantes.

La solution du CRC répond à toutes ces attentes.

Toute l'administration du service (maintenance matérielle et logicielle, configuration et supervision) est réalisée par le CRC. Le CRC apporte également un service à valeur ajoutée d'assistance et de support technique, de formation et de conseil personnalisé.

L'accès utilisateur est simplifié au maximum. Les identifiants sont ceux de l'annuaire d'établissement. Les logiciels clients sont pré-configurés avec des paramètres identiques pour tous. Toutes les données nécessaires à la configuration du poste de travail (adressage IP, serveur de nom, routage spécifique) sont fournies par l'infrastructure d'authentification du CRC.

Étant donnée la diversité des utilisateurs et des systèmes d'exploitation des postes de travail, deux logiciels clients (le client libre VPNC [2] et le client VPN CISCO) ont été mis à disposition des utilisateurs. Les systèmes d'exploitation validés et supportés sont : Windows, Linux, MAC OS X, et les systèmes *BSD.

Pour simplifier l'installation du coté de l'utilisateur et également l'administration du coté du CRC, la configuration des logiciels clients est téléchargeable (client VPNC [2]) ou pré-configurée (client VPN CISCO). Les logiciels clients sont financièrement pris en charge par le CRC et ne sont donc pas à la charge de l'utilisateur. Ces logiciels sont validés, mis à jour régulièrement et mis à la disposition des utilisateurs via un accès Web authentifié. Les procédures d'installation ainsi qu'une FAQ[1] sont également maintenues et mises à disposition des utilisateurs sur le site.

Compte-tenu de la taille de la communauté, il était impératif de mettre en place une solution robuste, efficace et facile à gérer. La solution répond également aux contraintes de disponibilité de 99,9% [3] fixées par les instances politiques du CRC. Le service est donc entièrement redondant et configuré en mode haute disponibilité de type actif/passif.

Chaque composante peut accéder aux avantages de cette solution qui allie facilité de mise en œuvre et fonctionnalités avancées (haute disponibilité, IPv6, clients multi plate-forme, accès haut débit, accès direct au réseau de composante). La création d'un serveur VPN virtuel est réalisée en collaboration avec les correspondants réseau des composantes en fonction des besoins de leurs utilisateurs et surtout de la politique de sécurité locale.

4 L'offre VPN du CRC

Les diverses composantes connectées sur *Osiris* ont des politiques de sécurité spécifiques et des ressources internes sécurisées très diversifiées. Chaque composante a donc des besoins différents en terme d'accès distant. Ceci nous a amené à décliner le service sous 3 formes.

4.1 L'accès « VPN standard »

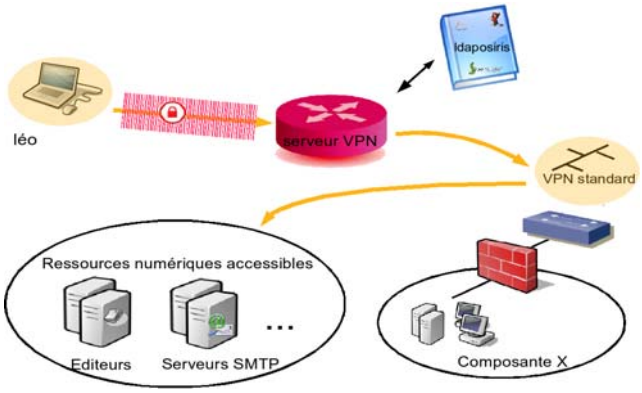

Figure 1: *l'offre VPN standard*

[1] http://www-crc.u-strasbg.fr/osiris/services/vpn/faq.html

L'accès « VPN standard » est le service offert par défaut à tous les utilisateurs d'*Osiris.*

Il permet aux utilisateurs nomades d'arriver dans un sous-réseau commun et d'accéder aux ressources partagées en accès restreint sur *Osiris*, comme par exemple les publications mises à disposition par le SICD (Service Inter-établissement de Coopération Documentaire), ou encore les serveurs SMTP ou tout autre ressource commune à l'ensemble d'*Osiris* (cf. Figure 1).

4.2 L'accès « VPN-Lab »

L'accès VPN-Lab, permet aux utilisateurs nomades d'arriver dans un sous-réseau dédié à leur composante.

Une plage d'adresses IP étant réservée à ses utilisateurs, l'administrateur système et réseau de la composante peut autoriser l'accès depuis cette plage d'adresses IP à des ressources internes, comme des serveurs de fichiers (cf. Figure 2).

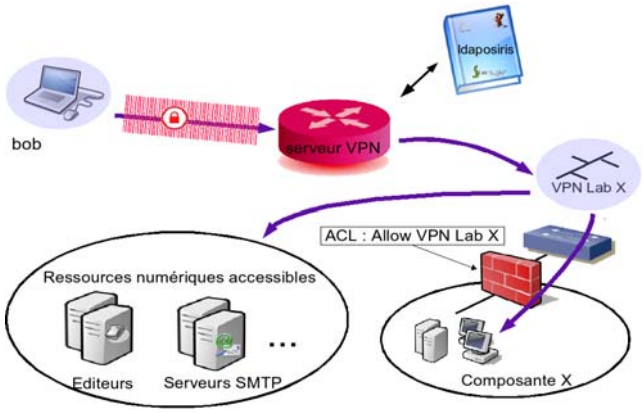

Figure 2: *l'offre VPN-Lab*

4.3 L'accès « VPN-Lab+ »

L'accès VPN-Lab+ est la solution la plus intégrée : elle permet aux utilisateurs nomades d'arriver directement dans le sous-réseau de leur composante.

La différence par rapport à l'accès « VPN-Lab » est que le trafic des postes nomades est amené par le CRC via un Vlan dédié au commutateur d'entrée du bâtiment de la composante. Ceci permet à l'administrateur système et réseau de la composante de connecter les domaines de diffusion Ethernet du réseau principal et du réseau nomade. Il peut également mettre un pare-feu bridgé pour implémenter une politique de sécurité plus fine.

L'utilisateur nomade bénéficie de la protection de la politique de sécurité locale et de l'accès aux fonctionnalités nécessitant la diffusion Ethernet (par exemple les partages Windows).

Pour l'administrateur système et réseau, la politique de sécurité est aussi simplifiée car le réseau des utilisateurs nomades est distingué sur une interface particulière s'il le souhaite (cf. Figure 3).

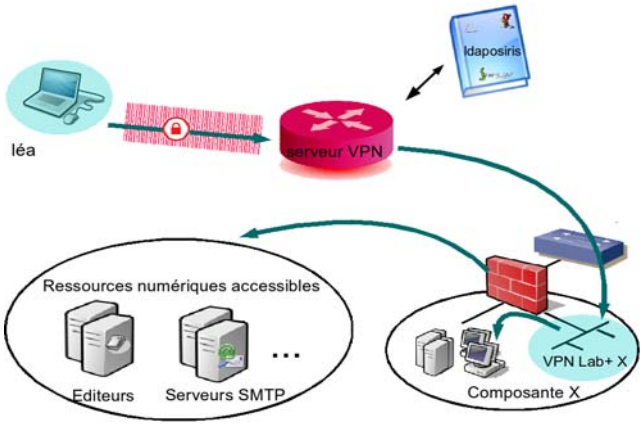

Figure 3: *l'offre VPN-Lab+*

5 Choix techniques

Pour comprendre le type de solution technique retenue, rappelons que la responsabilité du CRC s'arrête à l'entrée des bâtiments. La position du CRC est celle d'un opérateur réseau : nous n'avons aucune maîtrise sur les applications et sur la politique de sécurité de la composante. Il s'agit simplement de fournir un accès réseau de niveau 2 (couche liaison) ou de niveau 3 (couche réseau) aux clients VPN.

Il existe deux grandes familles de technologies VPN [4] [5] : IPsec et SSL.

Au moment du choix, seuls les VPN IPsec présentaient une richesse fonctionnelle et une maturité suffisantes. Les VPN SSL permettaient essentiellement un accès applicatif aux ressources de l'intranet. Ce n'est que récemment que les VPN SSL proposent un accès complet au niveau réseau.

Pour mémoire, IPsec est un protocole de sécurisation des échanges au niveau de la couche IP. Il propose entre autre, des services de chiffrement et du respect de l'intégrité des communications. Le fonctionnement d'IPsec repose sur la négociation et la création d'associations de sécurité (SA). Ces SA sont gérées par le protocole IKE qui se charge de la phase d'authentification. À l'origine, IKE n'authentifiait pas les utilisateurs mais simplement les machines. Dans notre cas, un autre protocole, XAUTH, seconde IKE pour authentifier les utilisateurs.

Les solutions supportant ces protocoles vont du logiciel libre aux boîtiers dédiés. Nous avons choisi une solution intermédiaire sous la forme d'un routeur Cisco. Contrairement aux boîtiers dédiés, souvent moins flexibles, cette solution était capable d'apporter toutes les fonctionnalités requises : IPv6, routage sur adresse source, proxy ARP, XAUTH, haute disponibilité etc. En ce qui concerne la haute disponibilité, les serveurs VPN libres ne supportent que depuis peu la reprise à chaud des SA. De plus, la solution choisie inclut des clients pour toutes les plates-formes. Elle est même compatible avec le client libre VPNC [2].

6 Infrastructure d'authentification

Pour faire face à l'usage massif de services authentifiés (WiFi, messagerie, VPN), le CRC a mis en place un annuaire LDAP [1] contenant plus de 50 000 comptes. Il est alimenté par les annuaires des différents établissements.

Les accès VPN sont authentifiés via un serveur Radius qui puise ses informations dans cet annuaire. Outre les attributs standards (login/mot de passe pour l'authentification), le schéma de l'annuaire contient les définitions nécessaires pour la configuration du client.

Ces informations sont stockées dans l'attribut privé radiusProfileVPN : il y a notamment la plage d'adresses IP du réseau de composante, le masque IP du réseau, le nom de domaine, et les serveurs de noms. Par exemple :

ipsec:addr-pool=Plage_ad_IP_VPN_Composante_X
ipsec:netmask=255.255.255.0
ipsec:default-domain=u-strasbg.fr
ipsec:dns-servers=130.79.200.1 130.79.200.3

La gestion des comptes est possible via l'interface Web « Authiris » [1] développée par le CRC. Cette interface permet de déléguer aux correspondants réseau la gestion des utilisateurs pour la messagerie électronique, le réseau sans fil et le VPN. Les correspondants peuvent notamment ré-initialiser les mots de passe ou éditer les profils VPN.

7 Principes réseaux mis en œuvre

7.1 Architecture

Le fonctionnement du service est assuré par deux routeurs « Cisco 3845 Security Bundle ». Ces routeurs sont redondants et configurés en mode actif/passif.

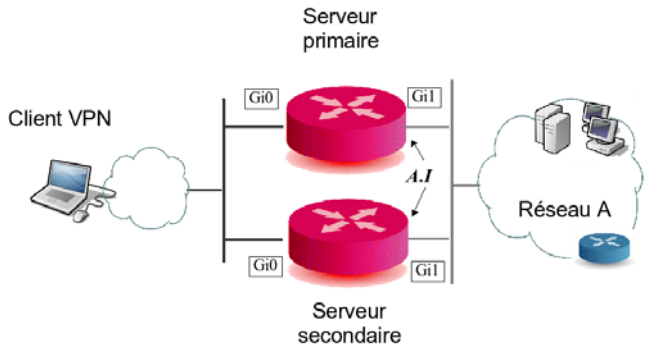

Figure 4: *Architecture générale*

Les serveurs possèdent deux interfaces Ethernet à 1Gb/s. La première interface (Gi0) est l'interface externe du serveur VPN. Les postes clients se connectent via cette interface. La seconde interface (Gi1) est l'interface interne du serveur VPN. Cette interface est découpée en sous-interfaces logiques (protocole 802.1Q). Chaque sous-interface logique correspond à un Vlan et possède une adresse IP ***A.I*** dans un sous-réseau ***A***.

Lorsqu'un utilisateur nomade se connecte au serveur VPN, il obtient une adresse IP ***A.N*** dans le réseau ***A*** défini dans son profil de connexion.

Un tunnel chiffré est créé entre le poste client et le serveur VPN. Par défaut, tout le trafic réseau du poste client est envoyé vers le serveur VPN à travers le tunnel chiffré.

Le serveur VPN aiguille le trafic du poste client en fonction de son adresse IP source ***A.N*** :

– si le trafic est à destination du réseau ***A,*** le trafic est directement transmis sur l'interface ***A.I*** en utilisant le mécanisme de routage traditionnel (routage direct Figure 5) ;

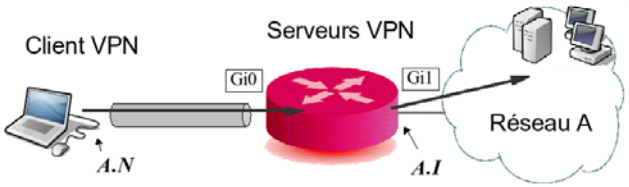

Figure 5: *Routage direct*

– sinon, le serveur VPN aiguille le trafic vers le routeur par défaut ***A.R*** du réseau ***A***. Cet aiguillage est réalisé par le mécanisme de Policy Routing basé sur l'adresse IP source (Figure 6).

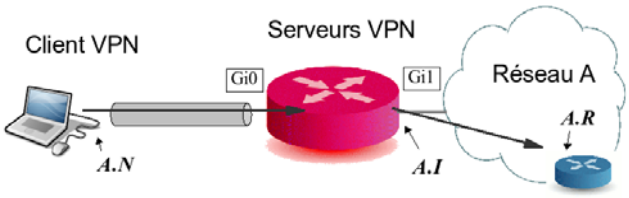

Figure 6: *Mécanisme de Policy Routing*

Pour permettre le retour des paquets du réseau A vers le client VPN, on utilise le mécanisme de Proxy ARP. Le serveur répond à la place du client aux requêtes ARP venant du réseau A. Ainsi, les paquets à destination du client VPN sont captés par le serveur et retransmis au client via le tunnel IPsec.

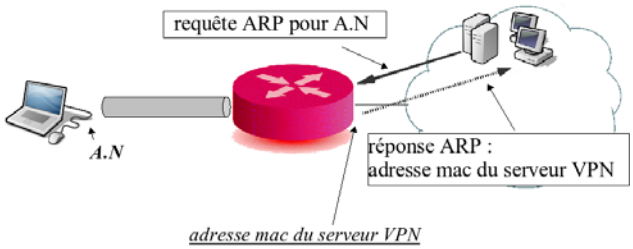

Figure 7: *Mécanisme de Proxy ARP*

7.2 Fonctionnalités avancées

7.2.1 Disponibilité du service en IPv6

Depuis 2001, le CRC a initié un déploiement à grande échelle du protocole IPv6 [6]. Dans cette démarche, le CRC s'est fixé comme objectif de rendre disponible en IPv6 chacun des services réseau qu'il propose.

Les clients VPN disponibles n'implémentant pas nativement IPv6, nous avons mis en place une solution consistant à monter un deuxième tunnel de type ISATAP [7] dans le premier tunnel IPsec. Le serveur VPN permet ainsi aux utilisateurs qui le souhaitent d'obtenir un adresse IPv6 dans le réseau *Osiris*. Nous avons développé à destination des utilisateurs avertis des scripts (Windows, Linux, FreeBSD) fournis sur demande.

7.2.2 Haute disponibilité

Les instances politiques ayant fixé un objectif de disponibilité de 99,9% au CRC [3], nous avons déployé deux serveurs VPN redondants en mode actif/passif.

Les serveurs sont déployés sur deux sites distincts et possèdent une double alimentation électrique. Si le serveur primaire subit une panne ou un arrêt volontaire (maintenance matérielle ou logicielle), les connexions en cours ou à venir sont automatiquement basculées sur le serveur secondaire de façon totalement transparente pour les utilisateurs en moins de 3 secondes.

La solution mise en œuvre actuellement repose sur les fonctionnalités de « statefull failover IPsec » de Cisco [8] qui utilise les protocoles Hot Standby Routing Protocol (HSRP) et Stateful SwitchOver (SSO). HSRP permet à N routeurs de partager une adresse IP virtuelle et ainsi d'assurer la redondance d'équipements. SSO, quant à lui est un protocole qui permet notamment de synchroniser les sessions VPN en cours.

Nous réalisons des exercices de bascule toutes les semaines pour valider le bon fonctionnement de la solution.

7.2.3 Les aspects sécurité de la solution

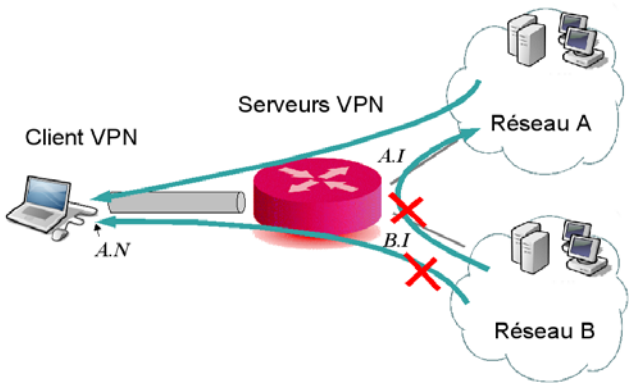

Figure 8: *sécurisation des échanges*

Les utilisateurs du service d'accès distant sécurisé doivent bien évidemment respecter la « Charte[2] de bon usage de l'informatique et du réseau Osiris » lorsqu'ils utilisent le service.

Afin de protéger les utilisateurs qui se connectent via le VPN, des ACL ont été ajoutées pour protéger les postes clients. Seul le trafic en provenance du réseau de la composante est transmis aux postes clients.

Des filtres ont également été ajoutés pour garantir l'étanchéité des différents réseaux de composante connectés sur le serveur VPN (cf Figure 8).

7.2.4 Journaux de connexion

Les journaux de connexion sont centralisés au CRC. Les informations sont extraites toutes les nuits des serveurs VPN et Radius ; elles sont disponibles pendant un mois avant d'être archivées. Une option de l'application Web « Authiris » permet aux correspondants réseau de visualiser ces journaux pour les utilisateurs dont ils ont la charge. L'interface permet de sélectionner par profil VPN, par utilisateur ou par adresse IP.

8 Mode opératoire de création d'un serveur VPN virtuel

La méthode de déploiement d'un serveur VPN virtuel au CRC se fait en collaboration étroite avec les correspondants réseau de la composante.

Avant tout, nous leur expliquons la solution mise en œuvre au CRC, les choix possibles (VPN standard, VPN-Lab, VPN-Lab+) et les avantages et inconvénients de chaque solution.

Il est ensuite nécessaire de connaître l'architecture réseau de la composante : y a-t-il plusieurs Vlans, plusieurs réseaux IP, quels sont les équipements réseaux (commutateurs, routeurs) et les pare-feux (bridgés, routés) mis en place ?

Il faut également identifier les besoins des utilisateurs : à quelles ressources veulent-ils accéder ? Combien d'utilisateurs peuvent se connecter simultanément au réseau ?

Pour finir, il faut déterminer les risques que la solution comporte et la politique de sécurité à associer.

Les bases de la solution étant choisies, il faut passer aux définitions et à la mise en œuvre.

Si les besoins de la composante se restreignent à l'utilisation d'un VPN standard, aucune définition n'est nécessaire : tous les utilisateurs d'Osiris accèdent par défaut à cette solution. Ils obtiennent une adresse IP dans une plage d'adresse commune qui ne permet pas de distinction utilisateur/adresse IP.

[2] http://www-crc.u-strasbg.fr/securite/charte-osiris.html

Si les besoins de la composante se portent sur un VPN-Lab, le CRC réserve dans son espace d'adressage IP, une plage dédiée à la composante. Tous les paramètres réseaux (nom de domaine, masque et serveurs de noms) sont imposés.

Le correspondant réseau doit, de son côté, configurer le pare-feu de la composante pour laisser passer le trafic depuis cette plage d'adresses vers les ressources à accéder.

La mise en place d'un VPN-Lab+ demande plus d'implication de la part du correspondant réseau.

Il doit définir la plage d'adresses IP utilisée, la dimensionner correctement et l'allouer. Le nom de domaine, le masque IP et les serveurs de noms sont ceux utilisés dans le réseau de composante.

Le trafic du VPN-Lab+ est amené par le CRC sur un port spécifique du commutateur d'entrée de bâtiment. Le correspondant doit alors déterminer, en fonction de l'architecture de son réseau et de sa politique de sécurité, où il raccordera ce Vlan.

Il devra également, si cela est nécessaire, mettre en place les règles de filtrage appropriées. Pour finir, il devra sensibiliser ses utilisateurs aux problèmes de sécurité (ils devront au minimum posséder un système sécurisé et à jour).

Nos recommandations sont de mettre en place un pare-feu bridgé et de ne laisser passer que les protocoles nécessaires.

9 Bilan et exemple d'utilisation

La mise en place du service et son « industrialisation » a nécessité un an de travail et son exploitation mobilise un ingénieur à mi-temps.

Le service est aujourd'hui adopté par plus de 1 300 utilisateurs. De plus, 46 composantes ont installé un VPN-Lab ou Lab+.

En moyenne, le serveur accueille une centaine d'utilisateurs différents par jour qui restent connectés 90 minutes. Plus de cinq cents utilisateurs différents se connectent dix fois par mois (Figure 9).

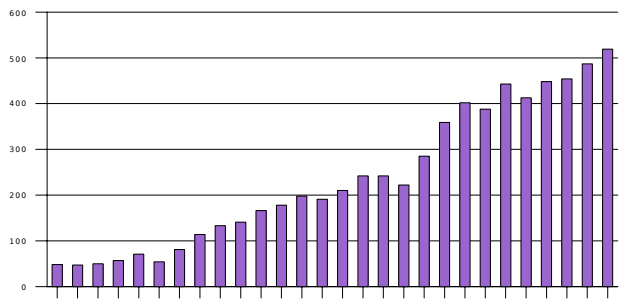

Figure 9: *Nombre mensuel d'utilisateurs différents depuis le démarrage du service en 2005*

Le CRC est le premier utilisateur de ses services. Cela nous permet de nous rendre compte des conditions d'utilisation, des performances et d'éventuels dysfonctionnements.

Nous avons déployé une solution d'accès VPN-Lab+ pour l'ensemble de nos équipes (cf Figure 10).

Le CRC regroupe schématiquement trois types d'utilisateurs :

- les utilisateurs Windows, pour qui cette solution permet de retrouver l'environnement de travail avec notamment l'accès au serveur SAMBA ;
- les membres de l'équipe téléphone, qui utilisent le service pour accéder aux applications de gestion du réseau de PABX lorsqu'ils sont en déplacement ou depuis chez eux ;
- les « accros » de la messagerie électronique, qui peuvent utiliser les serveurs SMTP *Osiris* depuis n'importe où.

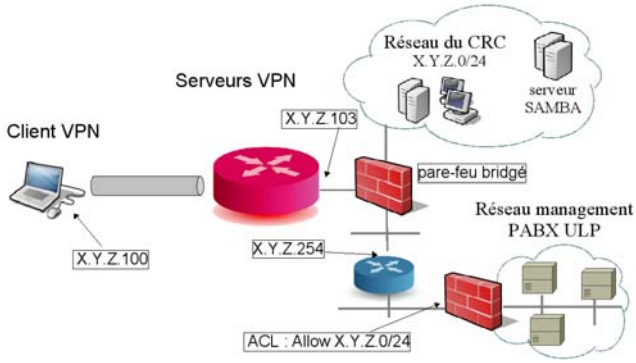

Figure 10: *Exemple d'utilisation*

10 Conclusion

Le CRC offre aujourd'hui un service mutualisé qui permet à chaque composante de bénéficier d'un serveur VPN virtuel.

Le service a remporté un franc succès. Plutôt que de déployer leur propre solution, quarante six composantes ont choisi de faire confiance au CRC. Les utilisateurs nous font régulièrement savoir leur satisfaction quant à la stabilité et la robustesse du VPN.

Le développement de l'annuaire *Osiris* a permis d'intégrer l'ensemble des personnels et des étudiants et de fédérer tous les services autour d'une authentification unique. Il a ainsi joué un rôle critique dans le déploiement à grande échelle et l'adoption rapide du VPN par les utilisateurs.

Cette solution a répondu à la grande majorité des attentes de nos utilisateurs jusqu'à aujourd'hui. Cependant de nouveaux besoins apparaissent :

- un contrôle de la conformité des postes nomades à la politique de sécurité de la composante avant l'accès au réseau ;

– un accès au code source pour avoir une meilleure maîtrise de la solution ;
– un vrai service de niveau 2 pour bénéficier nativement d'IPv6 et du multicast.

Ces nouveaux besoins font apparaître les limites de la solution en place. C'est pourquoi le CRC envisage de faire évoluer le service.

D'une part, pour répondre à la demande récurrente d'intégration du contrôle d'accès dans le VPN, nous allons évaluer différentes solutions de contrôle de la conformité des postes avant l'accès au réseau. Le choix de la solution devra être compatible avec l'architecture du réseau sans fil. En effet, les utilisateurs WiFi peuvent d'ores et déjà accéder directement à leur réseau de composante grâce à un nouveau dispositif, le « Vlaniseur » [9].

D'autre part, le CRC envisage de mettre en œuvre une nouvelle architecture VPN. Celle-ci devra répondre aux nouvelles contraintes que nous nous sommes fixées tout en maintenant les fonctionnalités en place et la qualité de service offerte. Les solutions libres, comme OpenVPN, semblent aujourd'hui répondre à toutes nos attentes.

Bibliographie

[1] A. Zamboni, P. David et J. Benoit, Des services authentifiés pour une communauté de 50 000 utilisateurs dans 17 établissements. Dans *Actes du congrès JRES2005*, Marseille, Décembre 2005.

[2] G. Keating et M. Massar, A VPN client compatible with Cisco's EasyVPN equipment, www.unix-ag.uni-kl.de/~massar/vpnc/

[3] P. Gris et P. David, Osiris 2, objectif 99,9% Un réseau fiable à très haut débit. Dans *Actes du congrès JRES2005*, Marseille, Décembre 2005.

[4] B. Dexheimer, R. Dirlewanger et F. Morris, Tutoriel VPN, *JRES2003*, Lille, Novembre 2003.

[5] M.C. Quidoz, Accès distants sécurisés : un essai de bilan des solutions possibles, Dans *Actes du congrès JRES2001*, Lyon, Décembre 2001.

[6] P. Pegon, Un exemple de généralisation opérationnelle à grande échelle d'IPv6 sur un réseau métropolitain. Dans *Actes du congrès JRES2005*, Marseille, Décembre 2005.

[7] RFC 4214 : Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), http://www.ietf.org/rfc/rfc4214.txt

[8] Cisco System Inc., Cisco IOS Security Configuration Guide, Release 12.4 Part 4.

[9] S. Boggia, Accès aux ressources locales dans un réseau sans-fil de 400 bornes, *Actes du congrès JRES2007*, Strasbourg, Novembre 2007.