Mutualisation d'un service d'accès distants sécurisés VPN

JRES 2007

Laurence MOINDROT – Jean BENOIT

Centre Réseau Communication

- Opérateur du réseau strasbourgeois Osiris
- Service inter-établissement
  - 16 établissements
  - 120 bâtiments
  - 50 000 utilisateurs
- Offre de services mutualisés
  - Messagerie, DNS, WiFi, VPN ...
- Limite de responsabilité
  - 120 commutateurs d'entrée de bâtiment
  - ~ 100 correspondants réseau

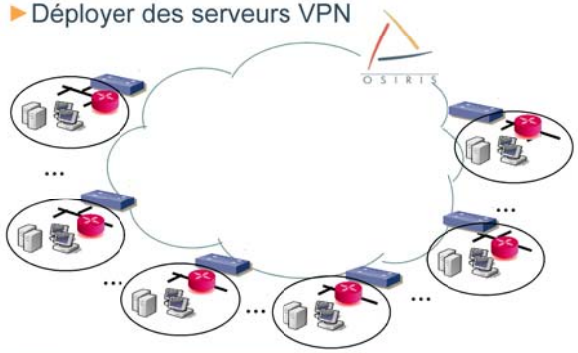
Plan

Besoins

- Accéder aux serveurs de publications
- Accéder aux ressources locales à distance
  - Pour l'utilisateur novice
  - Accès aux partages Windows
  - Intranet de composante (laboratoire, service...)
  - Envoi de mail via les relayeurs Osiris
- Identifier les utilisateurs qui accèdent aux ressources

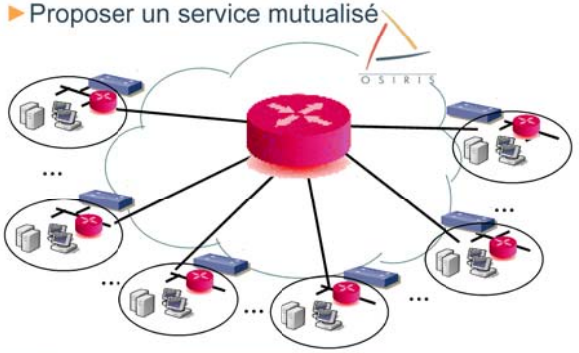
Besoins

- Déployer des serveurs VPN



Objectifs

- Proposer un service mutualisé



Plan

Avantages de la mutualisation (1/2)

- Centralisation des tâches d'administration
  - Maintenance matérielle / logicielle et supervision
  - Configuration
- Fonctionnalités avancées
  - Haute disponibilité, IPv6, clients multi plate-formes
- Facilité de mise en œuvre pour les composantes
  - Intégration de la solution par le CRC
- Garantie de la sécurité des réseaux de composante

Avantages de la mutualisation (2/2)

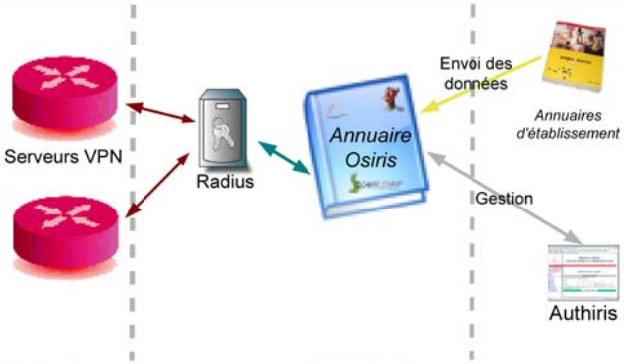
- Accès simplifié pour les utilisateurs
  - Identifiants de l'annuaire d'établissement
  - Logiciels clients pré-configurés et multi plate-formes
- Documentation et assistance utilisateur
  - Principes / FAQ
  - Procédures d'installation
  - http://www-crc.u-strasbg.fr/osiris/services/vpn
  - email : vpn@crc.u-strasbg.fr
- Effort de grande ampleur : 50% d'un ingénieur
- Hors de portée de la plupart des composantes

Plan

Infrastructure d'authentification

- Basée sur l'annuaire LDAP Osiris
  - Créé pour faire face à l'usage massif des services authentifiés
- Annuaire centralisé
  - Utilisé par tous les services du CRC
    - Messagerie, WiFi, VPN, liste de diffusion ...
  - Identifiant unique pour tous les services
- Alimentation
  - Automatiquement par les annuaires d'établissement
  - Manuellement par l'application Web « Authiris »

Infrastructure d'authentification



Infrastructure d'authentification

- Attributs standards et privés nécessaires au VPN

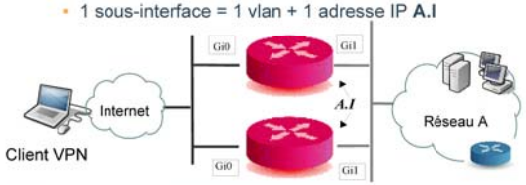
uid: bob
userPassword: GarY
cn: sponge bob
radiusProfileVpn: uid=vpn-composante-bleue,ou=profilsVpn

objectClass: radiusprofile
uid: vpn-composante-bleue
radiusReplyItem: Cisco-AVPair := "ipsec:addr-pool=**composante-bleue-ippool**"
radiusReplyItem: Cisco-AVPair += "ipsec:netmask=255.255.255.0"
radiusReplyItem: Cisco-AVPair += "ipsec:default-domain=u-strasbg.fr"
radiusReplyItem: Cisco-AVPair += "ipsec:include-local-lan=1"
radiusReplyItem: Cisco-AVPair += "ipsec:dns-servers=130.79.200.1"

Plan

Les serveurs VPN

- 2 routeurs Cisco 3845 security bundle
  - Redondants et configurés en mode actif / passif
- Configuration des interfaces
  - Gi0 = interface externe de connexion des clients
  - Gi1 = interface interne découpée en sous-interfaces
    - 1 sous-interface = 1 vlan + 1 adresse IP **A.I**

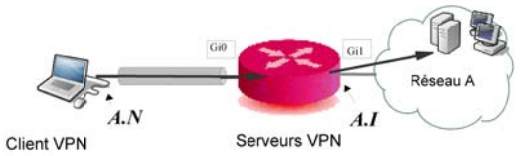


Les clients VPN

- Configuration des postes
  - Création d'un tunnel IPSEC
  - Obtention adresse IP ***A.N*** dans le réseau A
  - Routage de tout le trafic vers le serveur VPN

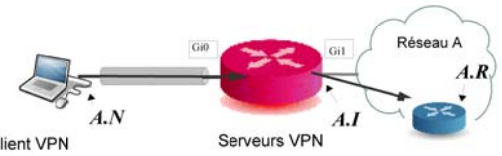
Routage du trafic sur le serveur

- Aiguillage du trafic client en fonction de ***A.N***
  - Mécanisme de Policy Routing basé sur l'adresse source
  - Si destination dans réseau A
    - Routage direct, envoi trafic sur interface ***A.I***



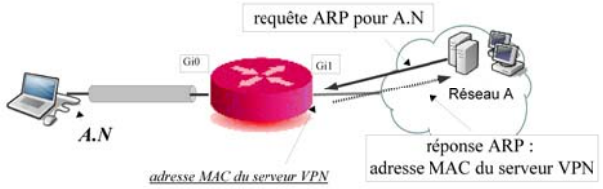
Routage du trafic sur le serveur

- Aiguillage du trafic client en fonction de ***A.N***
  - Mécanisme de Policy Routing basé sur l'adresse source
  - Si destination différente du réseau A
    - Envoi du trafic vers routeur par défaut ***A.R*** du réseau ***A***



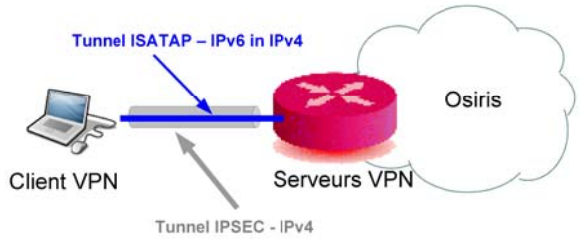
Mécanisme de Proxy ARP

- Retour des paquets du réseau A vers client ***A.N***
- Le serveur VPN répond aux requêtes ARP de ***A.N***



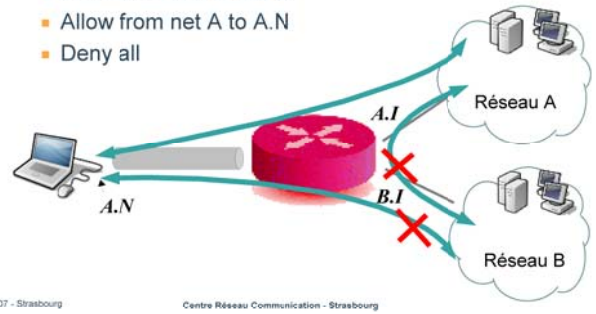
Accès IPv6

- Pas d'IPv6 natif
- Tunnel ISATAP (préfixe Osiris)



Sécurité

- Mise en place de règles de filtrage
  - Allow from A.N to net A
  - Allow from net A to A.N
  - Deny all



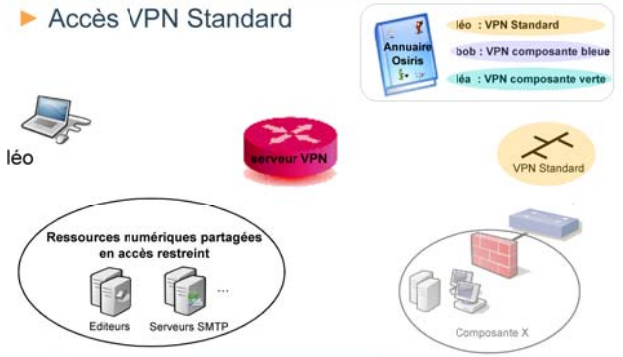
Plan

L'offre VPN du CRC

- Intégration aux architectures des composantes
- Déclinaison du service sous 3 formes
  - Accès « VPN Standard »
    - Accès à un sous-réseau commun
  - Accès « VPN Lab »
    - Accès à un sous-réseau dédié à une composante
  - Accès « VPN Lab+ »
    - Accès au sous-réseau propre de la composante

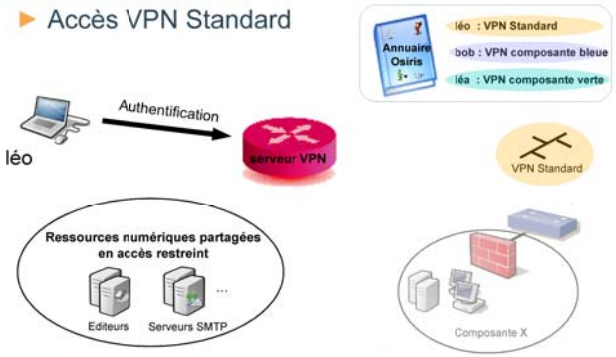
L'offre VPN du CRC

- Accès VPN Standard



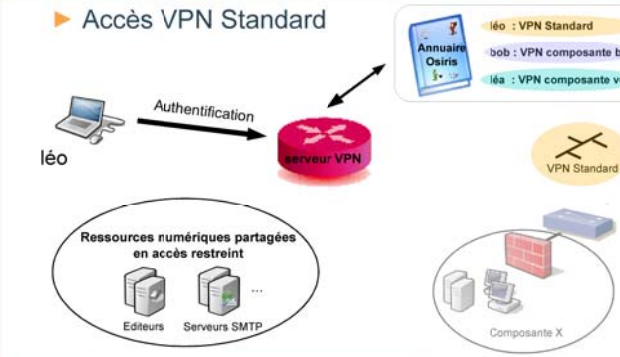
L'offre VPN du CRC

Accès VPN Standard



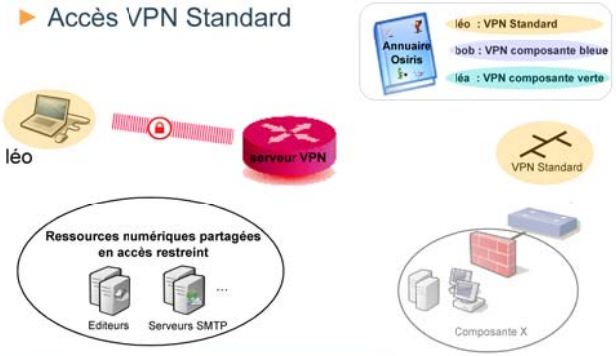
L'offre VPN du CRC

Accès VPN Standard



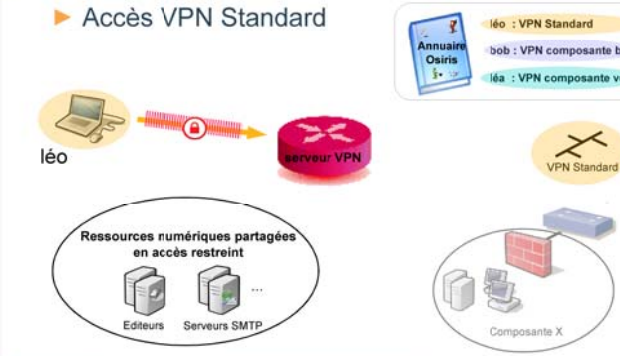
L'offre VPN du CRC

Accès VPN Standard



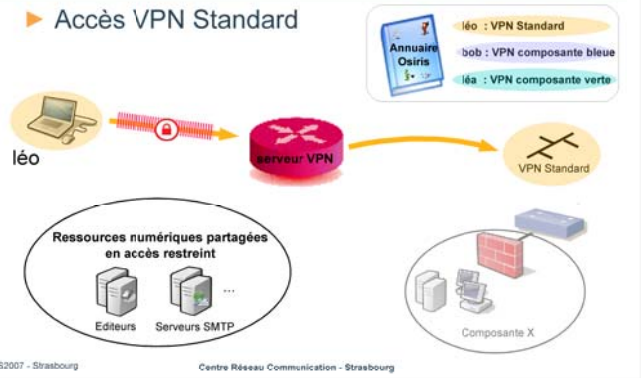
L'offre VPN du CRC

Accès VPN Standard



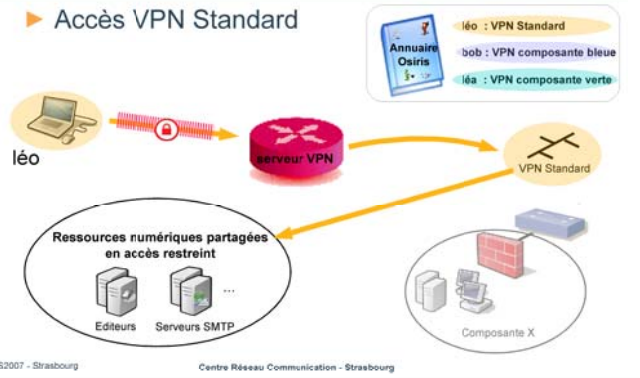
L'offre VPN du CRC

Accès VPN Standard



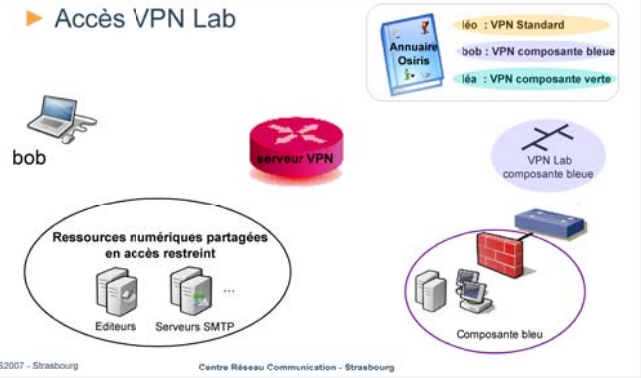
L'offre VPN du CRC

Accès VPN Standard



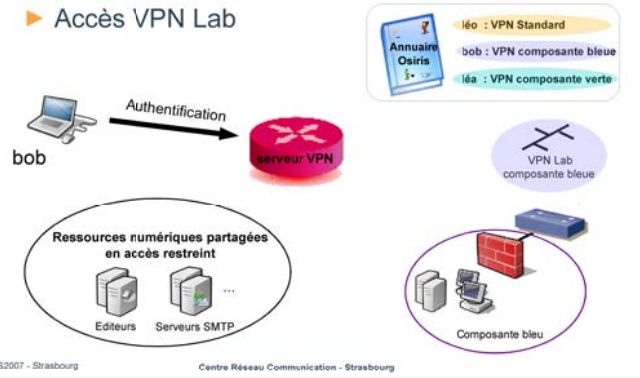
L'offre VPN du CRC

Accès VPN Lab



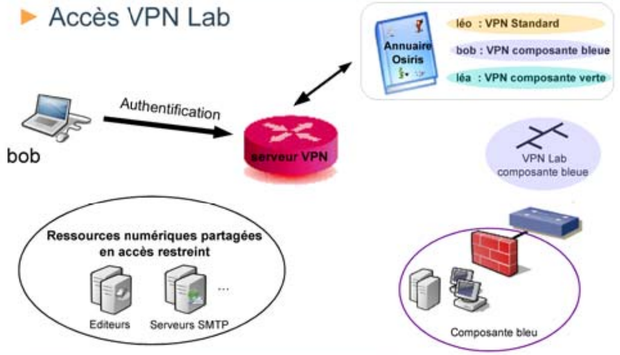
L'offre VPN du CRC

Accès VPN Lab



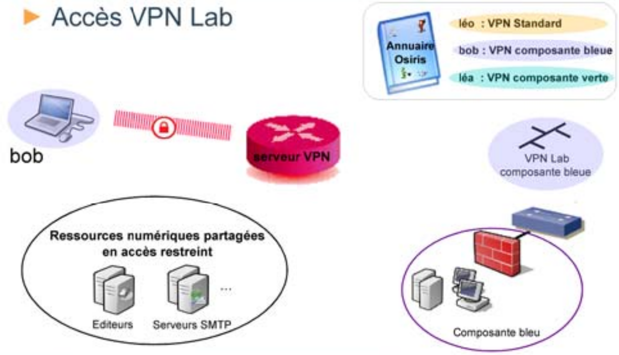
L'offre VPN du CRC

- Accès VPN Lab



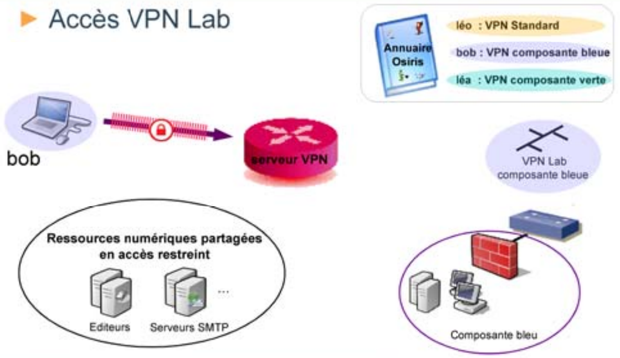
L'offre VPN du CRC

- Accès VPN Lab



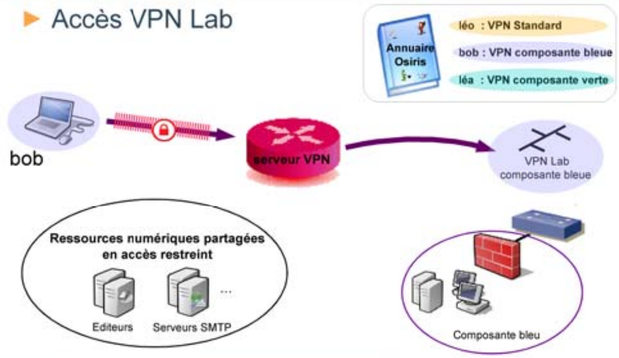
L'offre VPN du CRC

- Accès VPN Lab



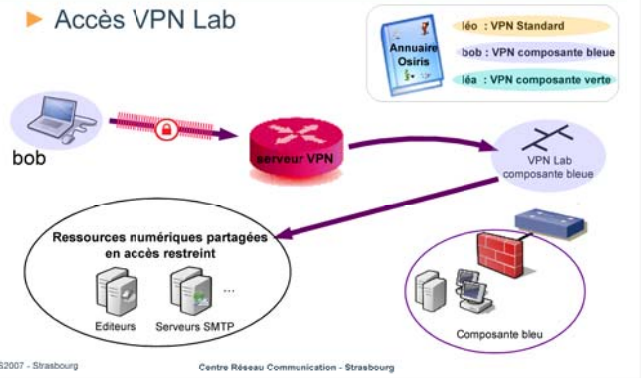
L'offre VPN du CRC

- Accès VPN Lab



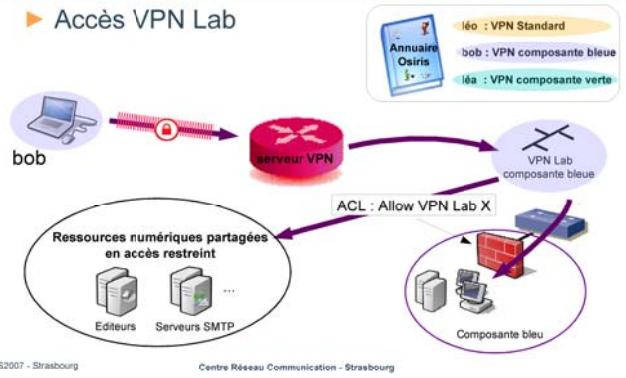
L'offre VPN du CRC

- Accès VPN Lab



L'offre VPN du CRC

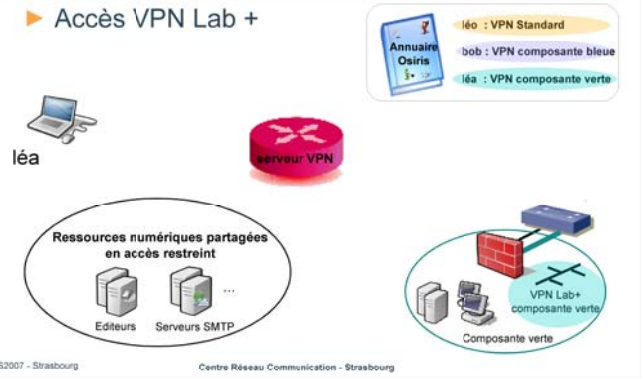
- Accès VPN Lab



JRES2007 - Strasbourg
Centre Réseau Communication - Strasbourg

L'offre VPN du CRC

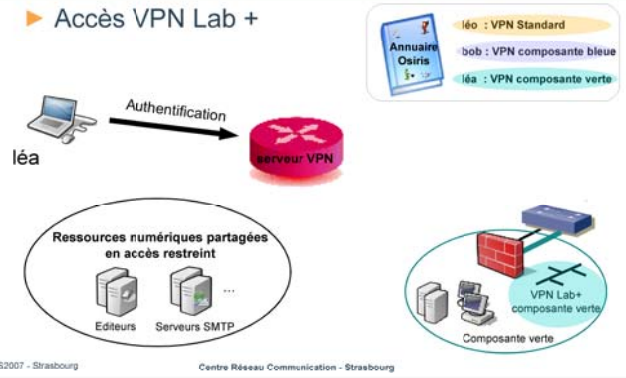
- Accès VPN Lab +



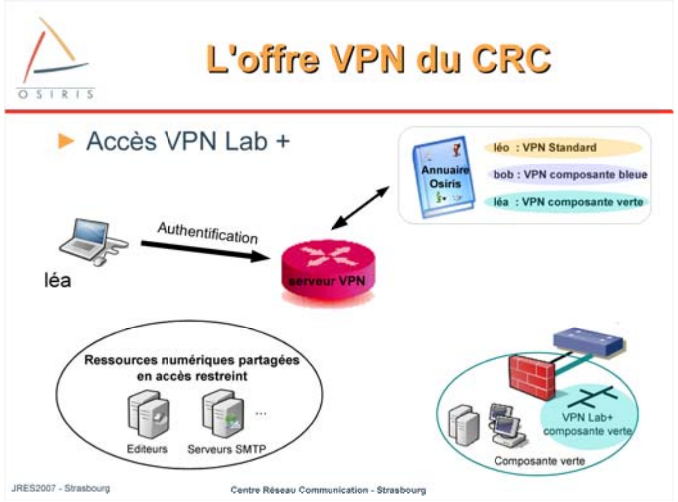
JRES2007 - Strasbourg
Centre Réseau Communication - Strasbourg

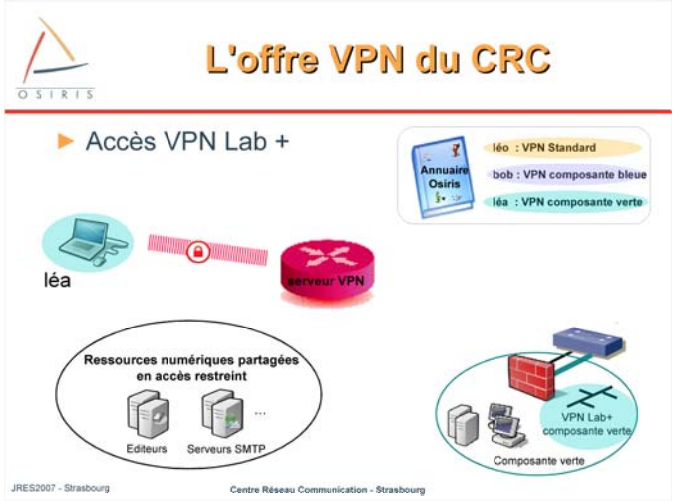
L'offre VPN du CRC

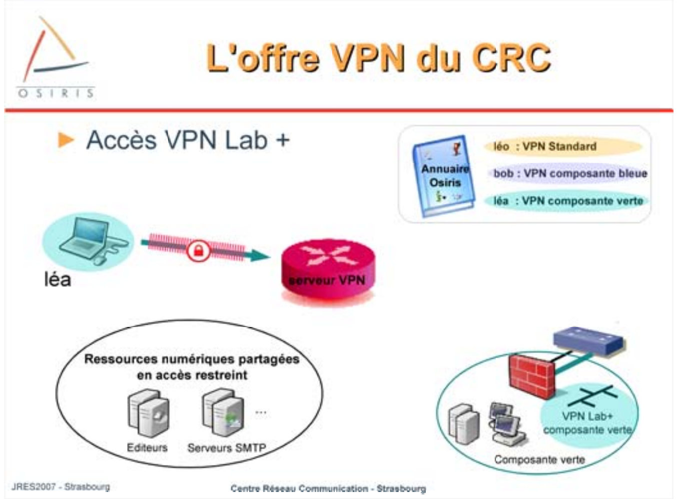
- Accès VPN Lab +

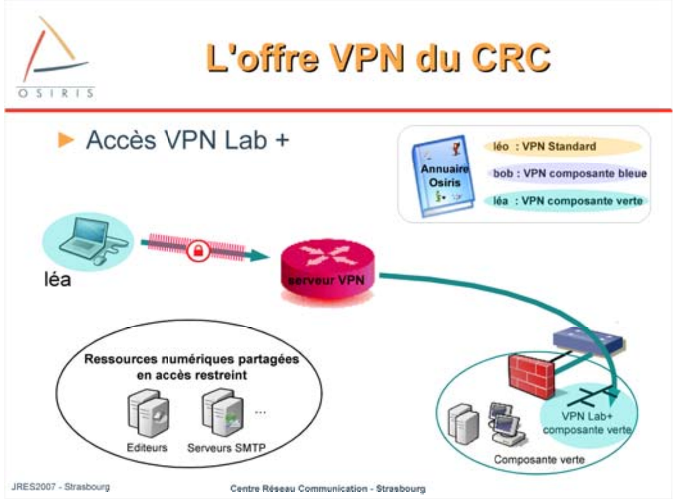


JRES2007 - Strasbourg
Centre Réseau Communication - Strasbourg


OSIRIS
L'offre VPN du CRC
Accès VPN Lab +
Annuaire Osiris
léo : VPN Standard
bob : VPN composante bleue
léa : VPN composante verte
Authentification
léa
serveur VPN
Ressources numériques partagées en accès restreint
Editeurs
Serveurs SMTP
VPN Lab+ composante verte
Composante verte
JRES2007 - Strasbourg
Centre Réseau Communication - Strasbourg

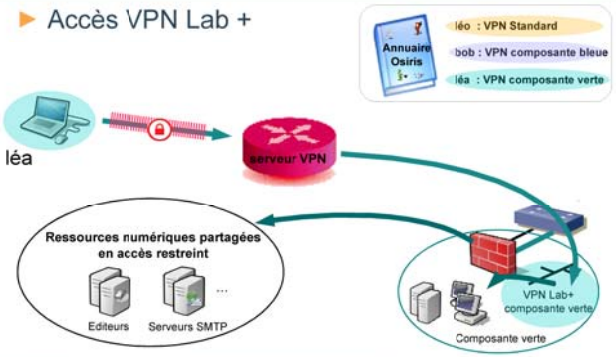

OSIRIS
L'offre VPN du CRC
Accès VPN Lab +
Annuaire Osiris
léo : VPN Standard
bob : VPN composante bleue
léa : VPN composante verte
léa
serveur VPN
Ressources numériques partagées en accès restreint
Editeurs
Serveurs SMTP
VPN Lab+ composante verte
Composante verte
JRES2007 - Strasbourg
Centre Réseau Communication - Strasbourg


OSIRIS
L'offre VPN du CRC
Accès VPN Lab +
Annuaire Osiris
léo : VPN Standard
bob : VPN composante bleue
léa : VPN composante verte
léa
serveur VPN
Ressources numériques partagées en accès restreint
Editeurs
Serveurs SMTP
VPN Lab+ composante verte
Composante verte
JRES2007 - Strasbourg
Centre Réseau Communication - Strasbourg


OSIRIS
L'offre VPN du CRC
Accès VPN Lab +
Annuaire Osiris
léo : VPN Standard
bob : VPN composante bleue
léa : VPN composante verte
léa
serveur VPN
Ressources numériques partagées en accès restreint
Editeurs
Serveurs SMTP
VPN Lab+ composante verte
Composante verte
JRES2007 - Strasbourg
Centre Réseau Communication - Strasbourg

L'offre VPN du CRC

- Accès VPN Lab +



Mode opératoire de création d'un serveur VPN virtuel

- Travail effectué en collaboration avec le correspondant réseau de la composante
  - Comprendre l'architecture réseau de la composante
    - Vlans, réseaux IP, équipements réseaux, pare-feux
  - Identifier les besoins utilisateurs
    - A quelles ressources souhaitent-ils accéder ?
    - Combien d'utilisateurs sont concernés ?
  - Aider à définir la politique de sécurité
  - Choisir la solution VPN à mettre en œuvre

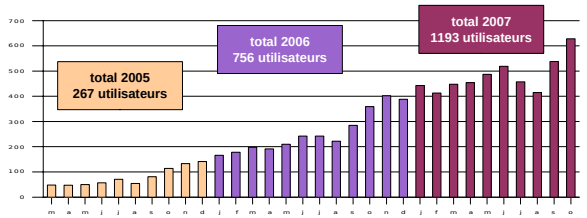
Mode opératoire de création d'un serveur VPN Lab+

- Rôle du CRC :
  - Configurer le serveur VPN et le profil de connexion
  - Propager le Vlan jusqu'au commutateur d'entrée de bâtiment de la composante sur un port spécifique
- Rôle de la composante :
  - Définir la plage d'adresses IP utilisée
    - Dimensionnement, allocation
  - Raccorder le nouveau Vlan dans l'architecture réseau
  - Mettre en place les nouvelles règles de filtrage
    - Nouveau pare-feu, nouvelle interface
  - Affecter le profil VPN Lab+ à ses utilisateurs

Plan

Bilan d'exploitation

- Franc succès
  - 45 composantes ont déployé un serveur VPN virtuel
  - Répond à la grande majorité des attentes
  - Nombre d'utilisateurs différents mensuel en hausse



Perspectives

- Les évolutions :
  - Contrôler la conformité des postes nomades à la politique de sécurité des composantes
  - Offrir un vrai service de niveau 2 pour bénéficier nativement d'IPv6 et du multicast
  - Accéder au code source pour avoir une meilleure maîtrise de la solution
- Nouvelle architecture

Questions