WebSaaS

Contrôle et Optimisation de la navigation Internet d'entreprise

Présenté par Benoît DOLEZ
Willy TARREAU
Sylvain CHOISNARD

EXOSEC
*Architecte de sérénité

Qui sommes nous ?

- Exosec SAS, société Française indépendante
- Fondée en 2002 et financée par les fondateurs

- Conseil, audit et intégration des infrastructures réseau ;
- Supervision et Services managés ;
- Expertise en Logiciel Libres.

- Membre de l'APRIL
- Participe au pôle de compétitivité SYSTEMATIC
- Contribue au monde Open Source :

  maintenance du noyau Linux 2.4, Formilux, HAProxy, ARP Alert, OpenPOM

EXOSEC*
*Architecte de sérénité

Compétences thématiques

LAN / WAN	Infrastructure	Sécurité	Optimisation	Supervision
VLAN	Point de Cloisonnement	Authentification	Répartition de charge	Métrologie
VPN (IPSEC / SSL)	Clusters Linux	Chiffrement	QoS des flux	Supervision de disponibilité
DNS / DHCP	Haute Disponibilité	Filtrage d'accès	Troubleshooting réseau	Supervision de la bande passante
Redondance de Liens / Sites	Répartition de charge	Filtrage applicatif	Accélération de flux	Supervision des performances
Agrégation de Liens	Optimisation de flux / QoS	Contrôle d'activité	Benchmarks	Gestion des logs

EXOSEC
*Architecte de sérénité

Les offres packagées d'Exosec

Solutions

- POM : Plateforme Opensource de Monitoring
- Instant Audit : audit de troubleshooting réseau avec engagement de résultat
- WebSaaS : contrôle des flux de navigation sortant en mode SaaS

Appliances

- Sentineo : Appliances Réseaux et Sécurité (Vpn, IPSec, SSL)
- ALOHA : Appliances de Load Balancing Web

Services

- Serenity : offre de Services Managés (Supervision – MCO – Télégestion 24/7)
- HAProxy Services : assistance, support, formation sur HAProxy

WebSaaS – plan de la présentation

- Étude de l'existant
- Solution proposée
- Composants
- Évolutions

EXOSEC*
*Architecte de sérénité

Nos clients

- PME de 100 à 500 personnes
- Collectivités locales de 200 à 2000 personnes
- Souvent multi-sites
- Tous secteurs d'activités confondus
- Compétences internes peu disponibles
- Budgets informatiques limités
- Navigation sur Internet souvent accessoire

EXOSEC*
*Architecte de sérénité

Composants mis en œuvre

- Proxy cache : Squid
- Anti-virus : HAVP + clamav / IWSS
- Filtrage : Squidguard / Olfeo / Websense
- Haute disponibilité : keepalived / heartbeat
- Authentification : auth_ntlm
- Efficacité : 2 000 users par machine (<1k€)

Administration / Exploitation

- Développement d'interfaces spécifiques
- Reporting avec des logiciels libres
- Extraits/recherches de logs manuels
- Mises à jour peu pratiquées
- Peu de personnalisation demandée
- Supervision non triviale
- Support et assistance externes

Limites des plateformes dédiées

- Coût d'exploitation
- Complexité de mise à jour
- Liberté d'administration
- Concentration des accès réseaux (WAN)
- Besoin de spécialistes

Ressenti client

- Fonctionnement convaincant
- Bonne efficacité
- Bonne stabilité
- Compromis coût WAN / coût d'exploitation

**Ne pas réinventer la roue,
mais rendre l'existant
plus facile et peu onéreux.**

EXOSEC
*Architecte de sérénité

Besoins clients

- Décentralisation pour les coûts WAN
- Limiter les composants
- Limiter l'exploitation
- Conserver les logs !
- Rapport succinct pour les directions
- Assistance

EXOSEC
*Architecte de sérénité

WebSaaS – plan de la présentation

- Étude de l'existant
- Solution proposée
- Composants
- Évolutions

EXOSEC
*Architecte de sérénité

Solution proposée

- Basée sur des logiciels éprouvés
- Externalisée sur des datacenters
- Haute disponibilité
- Interface de gestion et de reporting simplifiée
- Plateforme dédiée ou mutualisée
- Infogérée
- Gestion de droits simplifiée par groupe d'utilisateurs
- Coût à l'utilisation et non à la déclaration

EXOSEC*
*Architecte de sérénité

Fonctionnement macroscopique

1. Configuration par proxy.pac
2. Requête vers le proxy, authentification
3. Filtrage anti-malware
4. Filtrage blacklist puis whitelist puis catégories
5. Cache
6. Récupération sur le site d'origine
7. Analyse anti-virus

Configuration du navigateur

- Configuration générique : transparente pour l'utilisateur
- Configuration spécifique : URL dans les options du navigateur Web
- Choix du proxy :

    - Résolution de noms pour les sites internes

    - Ferme de proxies pour les sites externes

Accès sortant

- Un seul port nécessaire (au choix)
- Liste d'adresses officielles pour les firewalls
- Aiguillage des services réalisé sur la plateforme hébergée
  - Distribution de configuration
  - Pages de blocages
  - Proxy Cache

WebSaaS – plan de la présentation

- Étude de l'existant
- Solution proposée
- Composants
- Évolutions

EXOSEC*
*Architecte de sérénité

Authentification

- Identifier l'utilisateur
- Déduire ses droits et ses options via le groupe
- Le retrouver dans les stats et les logs
- Utiliser la console d'administration

Authentification : Comptes

- Base d'authentification
- Base des autorisations
- Alimentation par la console Web

Authentification explicite

- HTTP Basic (sécurisation du stockage)
- HTTP Digest (sécurisation du transport)
- Identification de l'utilisateur au lancement du navigateur
- Base de comptes locale
- Compatible avec une utilisation nomade

Authentification par cookie

- A venir courant 2011
- Authentification 1 seule fois
- Cookie assigné et conservé sur le poste

\+ authentification unique

– fortes contraintes navigateur

– support limité des POST

– nombreux aller-retours

Authentification transparente NTLM

- Lien complexe entre serveur d'authentification et client
- Authentification couplée à la session utilisateur
- Communication permanente entre le proxy et le serveur d'authentification
- Pas de base de compte sur le proxy

➡ Requiert l'utilisation d'un proxy chez le client

Solution Anti-malware

Malware-Control de Lexsi

www.malware-control.com

- Produit Commercial
- Empêche les malwares de communiquer avec les serveurs de C&C.

Listes des serveurs de C&C :

- Base d'URL fournie et maintenue par la société française Lexsi
- Base qualifiée sur une étude comportementale de malwares collectés

EXOSEC
*Architecte de sérénité

Solution Anti-malware

Malware-Control de Lexsi

www.malware-control.com

+ 0% de faux positifs sur le premier million de sites les plus populaires
+ Mise à jour tous les ¼ d'heure
+ Utile : 1 hit sur 50k cible un site de C&C.

EXOSEC
*Architecte de sérénité

Filtrage d'URL par catégorisation

Olfeo

www.olfeo.com

- Produit Commercial.
- Catégorise les URL et autorise ou non selon des droits définis pour un groupe d'utilisateurs.

Constitution de la liste d'URL :

- Distribuée par la société française Olfeo
- Collecte d'URL de clients volontaires
- Qualification automatique et manuelle

EXOSEC

*Architecte de sérénité

Filtrage d'URL par catégorisation

Olfeo
www.olfeo.com

+ Sites visités par des sociétés françaises

+ Architecture modulaire
  + Un serveur autonome avec MySQL
  + Un « redirecteur » SQUID client du serveur
  – Le serveur ne sait pas restreindre ses adresses d'écoute

EXOSEC
*Architecte de sérénité

Anti-Virus : HAVP + ClamAV

HAVP + ClamAV

www.server-side.de — www.clamav.net

- Logiciels Libres
- HAVP agit en cache parent après SQUID.

Provenances des données:

- Base communautaire
- Mise à jour quotidienne
- 800k signatures

EXOSEC
*Architecte de sérénité

Anti-Virus : HAVP

HAVP

www.server-side.de

+ Analyse en mode flux
+ Utilisé avec ClamAV
+ Évolutif vers les principaux anti-virus du marché
+ Appliqué aux contenus non cachés
– Limite la durée de rétention

Cas du filtrage HTTPS

- Supporte le filtrage d'URL par domaine
- Filtrage de contenu non demandé
  - Impactant pour l'utilisateur final
  - Présente des risques potentiels de sécurité
  - Perte de confidentialité ressentie

Journalisation

- Archivage quotidien sur machines dédiées sur FS chiffré
- Logs (J-1) récupérables par le client depuis l'interface de gestion
- Logs indexés pour consultation partielle (tableau de bord)
- Anonymisation des logs à venir

Infrastructure

- Nœuds normalisés et indifférenciés, faciles à installer
- Forte scalabilité
- Distribution Linux CentOS 5
- Machines physiques ou virtuelles
- 4 machines réparties chez 2 opérateurs en France

Scalabilité

- Scalabilité du nombre de serveurs par site
- Scalabilité du nombre de sites
- RR DNS détermine un site et un serveur

Haute-Disponibilité

- Perte d'un site gérée par le proxy.pac, qui liste des sites de repli
- Adresses IP de service mutuellement redondées sur chaque site
- Les composants de chaque machine sont redondés par ceux des autres machines du même site

Interface de gestion

- Interface Web *user-friendly*
- Fonctionnalités :
  - Gérer sa consommation
  - Gérer les utilisateurs / groupes
  - Gérer la politique de filtrage
  - Accéder aux logs / statistiques

Relation utilisateur / groupe

- Un utilisateur fait partie d'un seul groupe
- La politique de filtrage est appliquée au groupe.
- Un utilisateur peut être désactivé
- Pas de limite sur le nombre d'utilisateurs ni de groupes.

Délégation de droits

- 3 rôles possibles pour les utilisateurs :
  - Simple utilisateur du proxy
  - Gestionnaire de groupes
  - Gestionnaire du compte

➡ Possibilité de déléguer à une direction/site la politique d'accès Internet de sa branche

Facturation à l'utilisateur actif

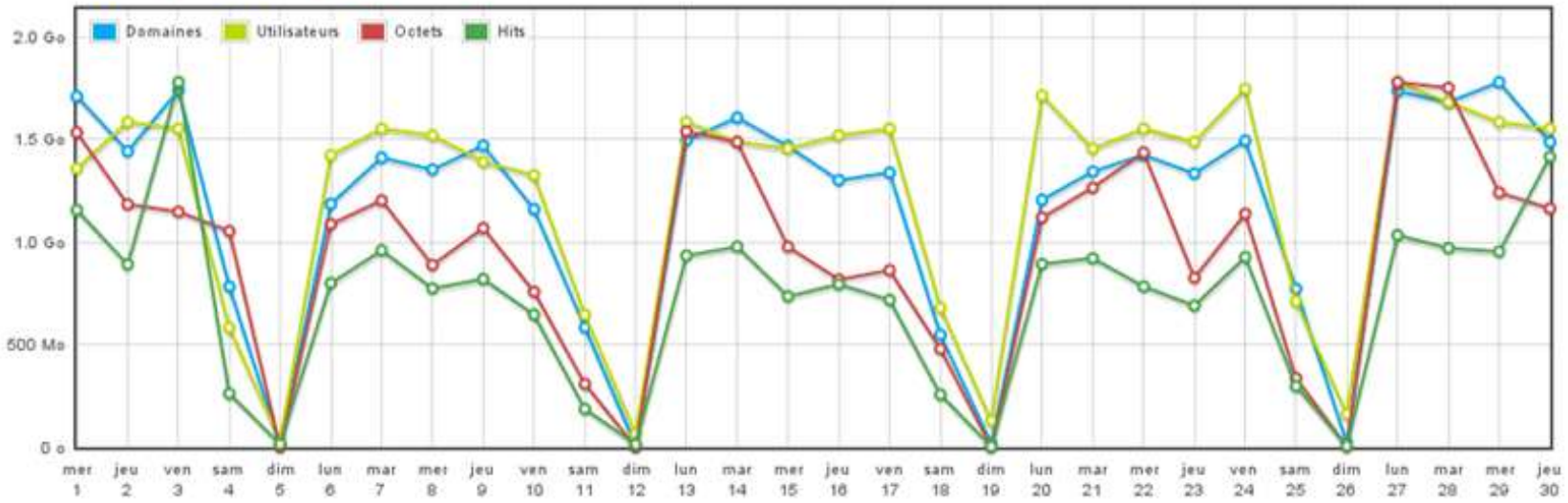
- Comptage mensuel par utilisateur actif et non par utilisateur déclaré
- Analyse des logs pour déduire l'activité liée à chaque fonction
- Les CGU définissent les règles d'abus

Commercialisation de l'offre

- mode FLEX : mensuel sans engagement
- mode CLASSIC : forfait avec engagement 12, 24 ou 36 mois
- marque blanche : plateforme dédiée personnalisée pour partenaires/revendeurs (opérée par Exosec).

Statistiques septembre 2010

septembre 2010



Top 10 Domaines

Domaines	BP Consommée (octets)	Hits
fbcdn.net	1 295 523 086	135 308
apple.com	1 002 201 878	2 309
youtube.com	907 624 361	2 650
facebook.com	764 060 505	58 333
jquery.com	741 640 608	86 065
infopro49.fr	668 724 630	5 810
umu.se	605 857 690	10
google.com	602 391 920	58 378
orange.fr	583 669 314	61 797
dailymotion.com	577 409 794	4 073

Top 10 Utilisateurs

Utilisateurs	BP Consommée (octets)	Hits
benoit.dolez@exosec	2 242 861 835	299 351
sylvain.choisnard@exosec	2 089 482 147	188 648
willy.tarreau@exosec	1 876 247 585	114 051
celine.harrand@exosec	1 754 332 875	29 759
bertrand.jacquin@exosec	1 655 640 761	199 774
julien.thomas@exosec	1 615 947 889	62 648
emeric.brun@exosec	1 448 555 961	302 642
henri.laurent@exosec	1 238 293 782	100 789
herve.commowick@exosec	1 212 050 864	135 043
alexandre.bray@exosec	945 900 385	99 112

WebSaaS – plan de la présentation

- Étude de l'existant
- Solution proposée
- Composants
- Évolutions

EXOSEC*
*Architecte de sérénité

Evolutions - utilisateur

- Charte d'utilisation :
  - Disponible dans les pages de blocage et d'authentification
  - Gérée par l'administrateur
- Pages d'erreurs personnalisables

Evolutions - infrastructure

- Masquage des identifiants dans les logs
- Authentification Kerberos « Negociate » en évolution du NTLM
- Compression du flux

À l'étude

- Proxy FTP
- Proxy SOCKS
- Authentification par cookies
- IPSec (Opportunistic Encryption)
- Agent sur le poste

Pour en savoir plus

- Benoît DOLEZ — bdolez@exosec.fr
- Willy TARREAU — wtarreau@exosec.fr
- Sylvain CHOISNARD — schoisnard@exosec.fr