e-securIT

[Evaluation de solutions de proxy-cache]

http://securit.free.fr

[securIT@free.fr]

TABLE DES MATIÈRES

1. PRÉSENTATION GÉNÉRALE

1.1. DÉFINITIONS

Quelques définitions préalables son essentielles pour permettre la compréhension des différents concepts et critère abordés par la suite :

- **Proxy-cache :** on dénomme proxy-cache (plus souvent nommé proxy par abus de langage) toute solution (logicielle ou matérielle) permettant d'assurer deux rôles essentiels :
  - La fonction de relais (proxy) : il s'agit d'une fonction de sécurité généralement effectuée par des firewalls. Elle permet de masquer l'origine d'une requête vers un serveur et d'effectuer un certain nombre de contrôles sur les flux (contrôle d'accès, filtrage, journalisation…).
  - La fonction de cache : la fonction de cache n'assure pas de service de sécurité mais permet le stockage local des données les plus demandées afin de fournir directement aux clients ces données sans réaliser de nouvelles requêtes vers le serveur distant. Elle permet de diminuer les temps de réponse et la consommation de la bande passante.
- **Proxy générique :** un proxy générique permet de relayer des flux marginaux pour lesquels on ne dispose pas de relais standards. Le protocole Socks (version 5) traite de cette problématique et permet la définition et le relayage de flux atypiques (http://www.socks.nec.com/). Cependant, il ne permet pas de réaliser de cache.
- **Reverse proxy (relais inverse) :** un reverse proxy est un mode de fonctionnement particulier d'un proxy-cache. Il s'agit d'une utilisation "à l'envers". Un reverse proxy sert classiquement à protéger une batterie de serveurs Web. Le reverse-proxy se fait passer pour le serveur Web, intercepte les requêtes en provenance des clients, et les retransmet vers le serveur Web adéquat en ouvrant une nouvelle connexion. Le reverse-proxy joue aussi le rôle de cache, de sorte que lorsqu'il dispose déjà d'une page demandée par un client, il n'émet pas de requête vers le serveur Web et renvoie directement la page en cache. Un reverse proxy peut également assurer des fonctions de sécurité fondamentales : l'authentification et le chiffrement. On décharge ainsi les serveurs Web de ces fonctionnalités. Le reverse proxy peut également effectuer du partage de charge en répartissant, suivant des algorithmes particuliers (ex.: round trip, round robin...), les requêtes clientes vers différents serveurs Web.
- **Chaînage de proxies :** il arrive, pour optimiser la bande passante et gérer la sécurité au plus près de l'utilisateur, de relier en série plusieurs proxies-cache. On nomme cela une chaîne de proxies.
- **ICP :** Internet Cache Protocol (RFC 2186 et 2187 pour ICP v2). Le protocole ICP permet de réaliser du routage dynamique entre proxies et de l'interrogation de caches voisins.
- **CARP :** Cache Array Routing Protocol. Le protocole CARP utilise un algorithme déterministe pour répartir les requêtes des clients sur différents proxies.

1.2. CAS D'USAGE D'UN PROXY-CACHE

De nombreuses entreprises s'appuient sur la technologie proxy-cache afin de fournir un moyen d'accès à l'Internet pour les utilisateurs de leur système d'information. Ceci vise à subvenir à deux grands besoins :

- Économie de bande passante : fonction de cache.
- Contrôle des accès : authentification des utilisateurs, journalisation de l'activité et de l'usage du service, filtrage.

Cependant (et hélas), rares sont les entreprises qui mettent en oeuvre des proxy-cache pour assurer une fonction de relais inverse.

1.3. PRÉSENTATION DES PRODUITS DU MARCHÉ

Les principaux produits du marché sont divisés en deux catégories :

- Les produits type « boites noires » (hardware) pouvant supporter des charges importantes et destinés, en priorité, aux fournisseurs d'accès Internet (ISP).
  Parmi les plus importants, citons :
  - Cache Engine de la société Cisco Systems - http://www.cisco.com.
  - CacheFlow de la société du même nom - http://www.cacheflow.com.
  - Cobalt Qube de la société Cobalt Networks - http://www.cobaltnet.com.
  - DynaCache 200 de la société InfoLibria - http://www.inforlibria.com.
  - NetCache de la société Network Appliance - http://www.netapp.com.
  - WebSpeed de la société PacketStorm - http://www.packetstorm.on.ca.
- Les proxies logiciels standards. Les principaux produits sont :
  - Computer Software Manufaktur Proxy de la société CSM - http://www.csm-usa.com/product/proxy.
  - Netscape Proxy Server édité par iPlanet - http://www.iplanet.com/products/iplanet_proxy/home_2_1_1ae.html.
  - Microsoft Proxy Server v2.0 de la société Microsoft - http://www.microsoft.com/proxy/default.asp.
  - Internet Security and Accelerator Serveur 2000 (ISA Server 2000) de la société Microsoft - http://www.microsoft.com/isaserver.
  - Squid, sous licence GNU - http://squid.nlanr.net.
  - Websense (standalone), de la société Websense Inc - http://www.websense.com/products/integrations/Proxy-WS.cfm.

Remarque : la plupart des firewalls du marché fournissent des fonctions de proxy HTTP/FTP, mais n'assure pas le service de cache. Ils ne sont donc pas mentionnés ci-dessus.

1.4. SOLUTIONS ÉTUDIÉES

Les solutions détaillées dans ce document sont les produits majoritaires sur le marché :

- Netscape Proxy Server v.3.5.
- Microsoft Proxy Server v.2.0.
- Microsoft ISA Server 2000.
- Squid v.2.3.

2. NETSCAPE PROXY SERVER V.3.5

2.1. CARACTÉRISTIQUES TECHNIQUES

- Systèmes d'exploitation supportés : Unix, HP-UX, AIX, IRIX, Solaris, Windows NT 3.51/4.0.
- Netscape Proxy Server est indépendant de tout serveur Web.
- Protocoles supportés :
  - HTTP, HTTPS, FTP et Gopher par défaut.
  - L'administrateur peut également définir et spécifier les protocoles particuliers qu'il souhaite relayer ou filtrer.
  - Support de SOCKS version 5 pour la définition et la mise en œuvre de proxies génériques.
  - Netscape Proxy Server sait fonctionner en relais pour le protocole SSL.
- Modes d'authentification :
  - Utilisateurs déclarés localement (couple login/mot de passe).
  - Interfaçage avec un annuaire LDAP. Netscape Proxy Server permet l'interrogation de tout type d'annuaires compatibles avec le standard LDAP.
    Remarque : Netscape Proxy Server ne permet pas l'authentification en mode NTLM (challenge/response) d'utilisateurs d'un domaine Windows NT. Cependant, il est possible d'utiliser l'annuaire LDAP de Netscape (Netscape Directory Server) pour importer et synchroniser des bases de compte NT. Cet annuaire est alors interrogeable par Netscape Proxy Server.
  - Netscape Proxy Server ne sait pas relayer les paquets d'authentification à un serveur en amont.
- Critères de filtrage. Netscape Proxy Server dispose d'une grande granularité de filtrage, il est ainsi possible :
  - De filtrer la source d'une requête en fonction de l'adresse IP, du nom DNS, du nom de domaine.
  - De filtrer les destinations en fonction :
    - Du protocole spécifié.
    - De l'URL. *Remarque :* Netscape Proxy Server peut également s'appuyer sur des produits tiers fournissant des listes de destinations interdites ou autorisées, tels que :
      - Websense - http://www.websense.com.
      - Smartfilter - http://www.smartfilter.com.
      - SurfControl - http://www.surfcontrol.com…
  - De supprimer les entêtes en sortie afin de conserver anonyme la topologie du réseau interne.

- De filtrer le contenu des flux :
  - Moteur antivirus intégré (nécessite la présence d'un antivirus tiers).
  - Blocage des contenus indésirables (Java, scripts, extensions MIME, tags HTML, ActiveX..).
  - Filtrage de commandes : GET, PUT…

➢ Netscape Proxy Server ne fournit pas de service pour la traduction d'adresse (Network Address Translation).

➢ Netscape Proxy Server supporte :

- La fonction de reverse proxy.
- Le protocole ICP.

2.2. ADMINISTRATION

L'administration de Netscape Proxy Server s'effectue via une interface Web, par l'intermédiaire de n'importe quel navigateur standard (Netscape Navigator recommandé !). En outre, les communications entre les postes d'administration distante et le serveur sont chiffrées à l'aide du protocole SSL.

L'interface d'administration permet la gestion centralisée et unitaire d'un ensemble de serveurs Netscape Proxy.

L'administration est également réalisable en modifiant directement les fichiers de configuration.

En outre, la granularité des paramètres de configuration est très importante et permet un réglage excessivement fin.

Netscape Proxy Server permet à un administrateur de personnaliser les fichiers de logs (et leur contenu) générés. Cependant, ces données ne sont pas exportables dans une base SQL ou via l'interface ODBC.

Netscape Proxy Server peut être surveillé en utilisant le protocole SNMP.

2.3. PERFORMANCES

Netscape Proxy Server supporte le protocole CARP.

En outre, un ensemble de proxies Netscape peut être configuré en grappe.

Le chaînage de proxies multiples permet le partage de charge et la tolérance aux pannes.

3. MICROSOFT PROXY SERVER V.2.0

3.1. CARACTÉRISTIQUES TECHNIQUES

- Système d'exploitation supporté : Windows NT 4.0 (Service Pack 1).
- Nécessité d'installer préalablement Internet Information Server v.2.0 (Proxy Server est un filtre ISAPI de IIS).
- Protocoles implémentés :
  - Le proxy Web supporte HTTP (v.1.1), HTTPS, FTP et Gopher.
  - Le proxy WinSock inclut : AlphaWorld, AOL, Archie, Echo, Enliven, IMAP4, IRC, Microsoft NetShow, MSN, NNTP, POP3, RealAudio, SMTP, Telnet et VDOLive.
  - Le service SOCKS Proxy permet de supporter un nombre infini de services non listés ci-dessus. Il joue le rôle de proxy générique.
  - Microsoft Proxy Server sait fonctionner en relais pour le protocole SSL.
- Modes d'authentification :
  - Utilisateurs déclarés localement : authentification basique (login/mot de passe en clair).
  - Utilisateurs de domaine Windows NT : authentification en mode NTLM (challenge/response).
    Remarque : Microsoft Proxy Server v.2.0 ne dispose pas d'interface LDAP pour l'interrogation d'un annuaire compatible avec ce standard.
  - Microsoft Proxy Server ne sait pas relayer les paquets d'authentification à un serveur en amont.
- Critères de filtrage. Microsoft Proxy Server filtre au niveau du service (HTTP, HTTPS, FTP ou Gopher) et de l'adresse source (IP, nom de domaine, nom Wins) de la machine cliente.
  Remarque : Microsoft Proxy v.2.0 ne permet pas, en standard, de réaliser un filtrage basé sur l'adresse destination (URL, adresse IP). Cette fonction est réalisée par l'ajout d'un outil tiers s'appuyant sur l'interface ISAPI (ex. : Websense, Smartfilter…). Il en est de même pour le blocage des codes mobiles (Java, ActiveX, types MIME…).
- Microsoft Proxy Server fournit un service de traduction d'adresse et d'anti-spoofing reposant sur la technologie Microsoft Local Address Translation.
- Microsoft Proxy Server supporte la fonction de reverse proxy.
- Microsoft Proxy Server ne supporte pas le protocole ICP.
- Enfin, Microsoft Proxy Server peut assurer la fonction de passerelle IP/IPX.

3.2. ADMINISTRATION

L'administration de Microsoft Proxy Server s'effectue à l'aide de la console d'administration Microsoft (MMC) disposant d'un snap-in dédié à IIS et Proxy Server.

Une solution d'administration en mode Web (via un navigateur) est également disponible. Il est cependant conseillé d'utiliser la console de management pour réaliser les tâches d'administration et d'exploitation.

L'administration centralisée des droits de plusieurs proxies est réalisable par le biais des tableaux (arrays). Cependant, il est nécessaire d'administrer le serveur IIS en plus du serveur proxy.

Microsoft Proxy Server fournit des journaux d'événements moyennement complets et non personnalisables, mais permet l'exportation des éléments de suivi vers des bases de données SQL et au format ODBC.

Enfin, Microsoft Proxy Server peut être surveillé en utilisant le protocole SNMP.

3.3. PERFORMANCES

Microsoft Proxy Server dispose de fonctions de tableaux permettant d'administrer un pool de serveurs proxies de manière unitaire, comme s'il s'agissait d'une seule machine logique. On dispose ainsi de fonctions de partage de charge, tolérance aux pannes et déploiement progressif.

4. MICROSOFT ISA SERVER 2000

4.1. CARACTÉRISTIQUES TECHNIQUES

- Système d'exploitation supporté : Windows 2000.
- Pas de nécessité d'installer préalablement Internet Information Server.
- Protocoles implémentés :
  - Protocoles standards : HTTP, FTP, Internet Relay Chat (IRC), H.323, Transparent HTTP, Windows Media technologies, RealAudio, RealVideo, SMTP, NNTP.
  - D'autres protocoles peuvent être spécifiés (port, TCP/UDP).
  - Support de Socks v.4.3.
  - ISA Server sait fonctionner en relais pour le protocole SSL.
- Modes d'authentification :
  - Authentification basique (mot de passe en clair).
  - Pour les utilisateurs du domaine Windows 2000 :
    - Authentification par fonction de hachage (digest).
    - Support des modes d'authentification intégrés à Windows 2000 : Kerberos et NTLM (challenge/response).
  - Authentification par certificats X.509 v.3.
  - ISA Server sait relayer les paquets d'authentification à un serveur en amont.
- Critères de filtrage. ISA Server 2000 se veut être plus un firewall qu'un proxy-cache. De sorte qu'il dispose de nombreuses fonctionnalités évoluées de filtrage :
  - Filtrage IP dynamique (avec état des connexions).
  - Filtres pré-installés : HTTP, FTP, SMTP, Socks, RPC, H.323, Streaming media, POP et DNS.
  - Définition possible de filtres d'URLs.
  - Priorisation possible des flux pour la gestion de la bande passante.
- ISA Server fournit un service de traduction d'adresse et d'anti-spoofing reposant sur la technologie SecureNAT.
- ISA Server supporte la fonction de reverse proxy.
- ISA Server ne supporte pas le protocole ICP.

4.2. ADMINISTRATION

ISA Server s'administre par un snap-in de la console de management Microsoft (MMC). Un groupe de proxies ISA Server peuvent ainsi être administrés de manière centralisée.

L'outil d'administration permet de configurer les règles de cache, de contrôle d'accès, d'alerte et de monitoring.

Les possibilités natives de reporting de l'activité des utilisateurs sont intéressantes.

4.3. PERFORMANCES

ISA Server supporte le protocole CARP.

En outre, un ensemble de proxies ISA Server peut être configuré en grappe et effectuer du partage de charge à l'aide du service Network Load Balancing (NLB) de Windows 2000.

ISA Server permet le chaînage de proxies multiples.

5. SQUID

5.1. CARACTÉRISTIQUES TECHNIQUES

- Systèmes d'exploitation supportés : AIX, Digital Unix, FreeBSD, HP-UX, Irix, Linux, NetBSD, Nextstep, SCO, Solaris, Windows NT.
  Remarque : Squid a été optimisé pour des plates-formes de type Unix (ou dérivées). Ainsi, bien qu'une version soit compilable sous Windows NT, il n'est pas recommandé, pour des considérations de performance, de déployer Squid sur ce système d'exploitation.
- Squid est indépendant de tout serveur Web.
- Protocoles implémentés :
  - En natif, Squid fournit des solutions évoluées de proxy-cache pour les protocoles HTTP, FTP, SSL.
  - Un administrateur peut définir et spécifier des protocoles particuliers qu'il souhaite relayer ou filtrer.
  - En outre, Squid fournit des fonctions spécifiques de cache tels que, à titre d'exemple, le cache des interrogations DNS (DNS lookups).
  - Squid sait fonctionner en relais pour le protocole SSL.
- Modes d'authentification :
  - L'authentification ne peut être réalisée, en natif, que sur des bases d'utilisateurs déclarés localement (à l'image de la déclaration des utilisateurs d'un système Unix dans le fichier /etc/passwd).
  - Un patch est disponible pour permettre l'interfaçage avec un annuaire LDAP (ex. : OpenLDAP - http://www.openldap.org).
  - Squid ne fournit pas de possibilité d'interrogation de base d'utilisateurs de domaine Windows NT en mode NTLM (défi/réponse).
  - Squid ne sait pas relayer les paquets d'authentification à un serveur en amont.
- Critères de filtrage.
  Squid permet d'effectuer tout type de filtres sur la source et la destination de chacune des requêtes. Il est ainsi possible d'implémenter des listes de contrôle d'accès (Access Control Lists) pour effectuer :
  - Du filtrage d'URLs à partir de fichiers plats contenant les URLs autorisées ou interdites.
  - Du filtrage sur le contenu des flux. Un exemple particulier concerne le traitement des cookies.
  - Du filtrage au niveau client (machine et utilisateur) et protocoles.
  - De la suppression d'entêtes (Anonymize_headers).
  - …
- Squid ne fournit pas de service de traduction d'adresse.

- Squid supporte les protocoles :
  - ICP.
  - HTCP (Hyper Text Caching Protocol, RFC 2756). Protocole de découverte de caches HTTP et de données en cache, de gestion et surveillance de caches HTTP.
  - CARP.
  - Cache Digests.

5.2. ADMINISTRATION

Squid s'administre :

- En mode commande en ligne et par fichiers plats. Squid peut s'administrer à distance par le biais de r-commandes ou d'accès telnet au serveur hébergeant le proxy.
- Par l'intermédiaire d'interfaces en mode Web.

L'administration de Squid nécessite de réelles compétences Unix, mais permet un niveau de granularité maximum dans la configuration du filtrage et du contrôle des requêtes soumises au serveur.

Squid peut être surveillé en utilisant le protocole SNMP.

5.3. PERFORMANCES

Squid est le proxy-cache le plus utilisé au monde du fait de sa compatibilité avec de nombreux standards et son implémentation de protocoles de gestion de caches hiérarchiques et de partage de charge (ICP, HTCP, CARP).

Il est en particulier largement déployé chez les fournisseurs de services Internet (ISP) dont le besoin en terme de cache est énorme.

Squid constitue l'une des meilleures solutions du marché, performante, évolutive et extensible.