

GSS 4492R Appliance DNS et Global Server Load Balancing

Introduction

Le produit ACE GSS (Global Site Selector) de la série 4400 représente la nouvelle génération d'appliance DNS. Le dernier modèle 4492R fait partie de la gamme ACE de Cisco. Il permet entre autres d'offrir quatre grands types de services :

- Le GSS remplace tout type de serveur DNS. Il permet d'optimiser l'accès aux applicatifs sur Internet ou l'intranet de l'entreprise. Le GSS4492R permet de répondre jusqu'à 7.000 requêtes DNS clientes par seconde par appliance.
- Il permet de distribuer intelligemment les clients sur plusieurs sites géographiques – c'est un service de « Global server load Balancing ». Dans ce mode, le GSS traite jusqu'à 30.000 requêtes DNS/s par appliance.
- Il offre une sécurité accrue aux attaques de type distributed-denial-of-service DDoS. Le GSS n'a pas à être mis à jour régulièrement, comme tout serveur de type BIND.
- Le GSS4492R est capable de travailler en parallèle avec plusieurs autres GSS, distribuant la charge et offrant une redondance totale pour héberger ces services DNS

Appliance DNS

Le GSS permet de gérer jusqu'à 2000 noms de domaines différents. Pouvant gérer en mode DNS jusqu'à 7000 requêtes DNS/s, il remplace de façon efficace tout serveur DNS. Il communique avec sept autres GSS pour offrir un cluster de huit équipements, managé à partir d'un point central. Le management se fait via une interface HTTPS interactive.

Le GSS offre des fonctions avancées de répartition de charges entre serveurs, avec monitoring des serveurs ce qu'un serveur DNS traditionnel ne fait pas.

Protection DDoS

Le GSS offre en option une protection comme les attaques de type Distributed Denial of Service attacks.

Ce type d'attaque a déjà été utilisé maintes fois sur des intranets et sur internet, arrivant à bloquer l'infrastructure réseau des entreprises.

La protection DDoS se base sur les mécanismes suivants

- Anti Spoofing
- Rate limiting
- Mitigation checks contre des attaques de type Reflector
- Peacetime learning

L'anti spoofing est réalisé sur chaque requête DNS sur le port 53. En cas d'attaques, la machine source est automatiquement bloquée. La fonction de rate limiting est également réalisée sur chaque requête DNS. On pourra activer la fonction Peacetime Learning afin de permettre au GSS de calculer les paramètres pour la fonction de rate Limiting.

Global server load Balancing

Cisco offre un grand choix de technologies dans le monde du Content Routing. Le but de ces technologies est de prendre des décisions intelligentes pour la redirection d'utilisateurs vers des Data Centers particuliers.

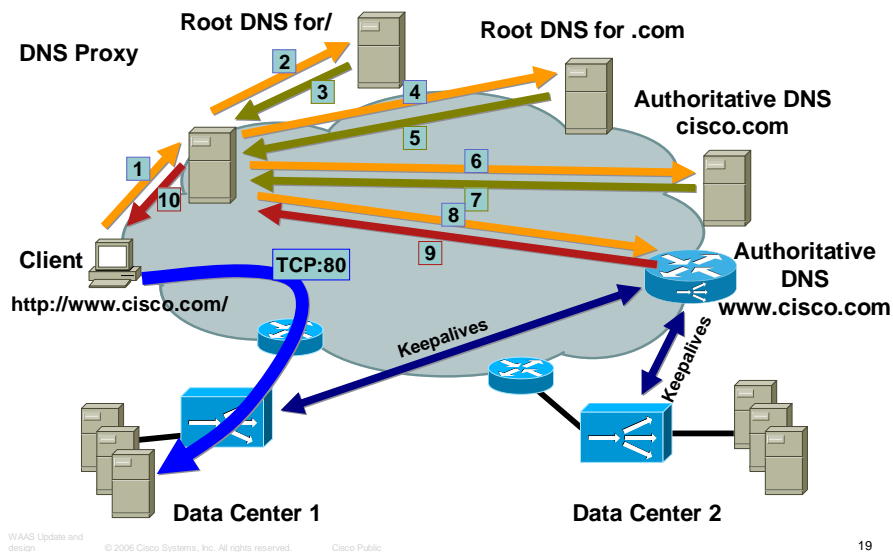
On distingue à ce jour trois grands types de technologies basées sur :

- le HTTP redirect
- l'Injection de Routes (Route Health Injection)
- le DNS

Nous allons couvrir rapidement le mode de fonctionnement DNS offert par le GSS 4492R.

Le mode DNS

Quand un utilisateur recherche un site comme www.cisco.com, la requête est envoyée à son serveur DNS local encore nommé DNS-Proxy ou D-proxy. Ce dernier cherche à résoudre par des requêtes itératives l'adresse IP du site demandé. L'utilisateur final ne voit jamais ce processus de résolution. Egalement, le serveur authoritative DNS ne voit pas les adresses IP des utilisateurs finaux.



DNS-BSED Site Selection

Le GSS 4492R

En s'insérant dans ce mécanisme de résolution DNS, le GSS 4492R va remplacer le serveur authoritative DNS. Il décide du meilleur site à utiliser pour la réponse et peut choisir de rediriger une population particulière vers un site en fonction de paramètres basés sur

- la charge des sites
- la disponibilité des sites
- la latence entre les différents DCs et les D-proxies des utilisateurs finaux
- la présence de contenus
- l'adresse IP des DNS-proxies effectuant des requêtes...

En détectant rapidement des problèmes sur les Data Centers, puis en routant les requêtes vers des sites alternatifs, le GSS garantit que des applications critiques sont toujours disponibles. Il est capable de surveiller plusieurs centaines de sites, d'équipements SLB et de serveurs, tout en offrant un management centralisé.

Le GSS optimise le processus de résolution DNS en soulageant les serveurs DNS des tâches répétitives redondantes. Le GSS 4492R peut répondre jusqu'à 30.000 requêtes DNS/s.

Le GSS supporte de nombreux mécanismes de partage de charge. En effet, les algorithmes suivants sont disponibles : Round Robin, Weighted Round Robin, Least loaded, Hashing sur les noms de domaines demandés, Hashing sur les adresses des D-proxies, partage en fonction de la latence calculée dynamiquement entre les différents Data Centers et les clients...

Management

Il est possible de configurer le GSS via telnet ou via une interface web sécurisée (Https). Dans ce cas, on se connecte sur le GSS Master (GSSM) qui fonctionne en coordination avec un maximum de sept GSSs esclaves. La configuration mise en place sur le GSSM est automatiquement positionnée sur les GSSs esclaves.

Il est également possible de partager une table de stickiness entre les différents équipements. Ceci permet de rediriger une certaine population d'utilisateurs vers un site dédié pendant une durée fixée à l'avance.

Keepalives

Le GSS dispose d'une bibliothèque de keepalives standards afin de vérifier la disponibilité des différents Data Centers. Il dispose de mécanismes basés sur des paquets ICMP, requêtes TCP, requêtes HTTP. Entre autres, le mécanisme KAL-AP permet de récupérer via une simple requête à un équipement de partage de charge Cisco l'intégralité des données relatives au SLB : charge et disponibilité des différentes fermes. KAL-AP est disponible sur les SLBs standalone CSS, sur la carte CSM et bientôt sur ACE.

Règles avancées

L'administrateur du GSS peut très facilement mettre en place des règles sophistiquées. Par exemple, il est possible de mettre en place des règles comme ceci :

- 1) utilise le mécanisme de Round Robin entre les sites de Paris et de New York. Si les deux sites sont chargés à plus de 75%, applique la règle suivante :
- 2) utilise le mécanisme de Least Connections entre les sites de Tokyo et de Washington. Si les deux sites sont chargés à plus de 61%, applique la règle suivante :
- 3) utilise finalement le site de Paris.

Pour chaque règle, l'administrateur pourra également définir le nombre de réponses et leur TTL respectif (Time To live).

Implémentation

Le GSS peut être aussi bien positionné sur un intranet que sur un extranet. En interne, on l'utilisera comme serveur DNS ultra-performant. En externe, il fonctionnera comme Authoritative DNS. Cet équipement très puissant résout jusqu'à 30.000 requêtes DNS par seconde.



Contactez-nous :

www.cisco.fr

0800 907 375

Siège social Mondial

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Etats-Unis

www.cisco.com

Tél. : 408 526-4000
800 553 NETS (6387)
Fax : 408 526-4100

Siège social France

Cisco Systems France
11 rue Camille Desmoulins
92782 Issy Les Moulineaux
Cedex 9
France

www.cisco.fr

Tél. : 33 1 58 04 6000
Fax : 33 1 58 04 6100

Siège social Amérique

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Etats-Unis

www.cisco.com

Tél. : 408 526-7660
Fax : 408 527-0883

Siège social Asie Pacifique

Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapour 068912

www.cisco.com

Tél. : +65 317 7777
Fax : +65 317 7799

Cisco Systems possède plus de 200 bureaux dans les pays et les régions suivantes. Vous trouverez les adresses, les numéros de téléphone et de télécopie à l'adresse suivante :

www.cisco.com/go/offices

Afrique du Sud • Allemagne • Arabie saoudite • Argentine • Australie • Autriche • Belgique • Brésil • Bulgarie • Canada • Chili • Colombie • Corée • Costa Rica • Croatie • Danemark • Dubaï, Emirats arabes unis • Ecosse • Espagne • Etats-Unis • Finlande • France Grèce • Hong Kong SAR Hongrie • Inde • Indonésie • Irlande • Israël • Italie • Japon • Luxembourg • Malaisie • Mexique • Nouvelle Zélande • Norvège • Pays-Bas • Pérou Philippines • Pologne • Portugal • Porto Rico • République tchèque • Roumanie • Royaume-Uni • République populaire de Chine • Russie Singapour • Slovaquie • Slovénie • Suède • Suisse • Taiwan • Thaïlande • Turquie • Ukraine • Venezuela • Vietnam • Zimbabwe



Copyright © 2008 Cisco Systems, Inc. Tous droits réservés. CCSP, CCVP, le logo Cisco Square Bridge, Follow Me Browsing et StackWise sont des marques de Cisco Systems, Inc. ; Changing the Way We Work, Live, Play, and Learn, et iQuick Study sont des marques de service de Cisco Systems, Inc. ; et Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, le logo Cisco Certified Internetwork Expert, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, le logo Cisco Systems, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, le logo iQ, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, le logo Networkers, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient et TransPath sont des marques déposées de Cisco Systems, Inc. et/ou de ses filiales aux États-Unis et dans d'autres pays.

Toutes les autres marques mentionnées dans ce document ou sur le site Web appartiennent à leurs propriétaires respectifs. L'emploi du mot partenaire n'implique pas nécessairement une relation de partenariat entre Cisco et une autre société. (0502R)

205534.E_ETMG_JD_05/08