Contenu

Introduction

Ce document fournit une configuration d'échantillon pour les Produits et des applications Web CSS 11xxx afin de maintenir un client coincé au même serveur, si vous utilisez le HTTP ou le SSL.

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Comprenez les fondements du HTTP et du SSL.
- Ayez la connaissance au sujet des Produits et des applications Web CSS 11xxx.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version de logiciel 5.00 et ultérieures de Cisco WebNS
- Tous les Commutateurs de services satisfaits de gamme 11xxx de Cisco CSS

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à

Conventions relatives aux conseils techniques Cisco.

Informations générales

Beaucoup de sites Web font entrer dans à des clients leur site avec l'aide du port 80 de Protocole HTTP (Hypertext Transfer Protocol), mais veulent les clients à la transition au protocole de Protocole SSL (Secure Socket Layer) pendant la session pour des transactions sécurisé. Voici une manière de maintenir un client coincé au même serveur, si vous utilisez le HTTP ou le SSL.

Le client demande le trafic http destiné à l'IP virtuel (VIP). Le commutateur prend une décision d'équilibrer la charge. Dans ce document, le trafic va au serveur S1. Le client est alors coincé au serveur S1 basé sur une des méthodes d'avance-équilibre, telles que Rémanent-srip, Rémanent-srcip-dstport, et des Témoins. Référez-vous à configurer des paramètres Rémanents pour le pour en savoir plus de règles de contenu.

Pendant la session du client, la transition est faite au port 443 SSL quand le client sélectionne un lien à la page cette des https de redirect to. Ceci entraîne une nouvelle règle de contenu d'être frappé et le client peut être chargement-équilibré à un autre serveur. Car le trafic est maintenant les https chiffrés (SSL/TLS), le CSS ne peut pas vérifier au-dessus de la couche 4 (le nombre de port TCP) pour les Témoins, l'URLs etc., parce que les demandes sont chiffrées quand les informations passent le CSS. Afin d'empêcher l'occurrence de cette question, configurez le HREF de réorientation sur chaque serveur pour redésigner des https à la même annonce publique de serveurs, pas l'adresse de VIP, comme affiché ici :

Si vos serveurs sont dans un espace d'adressage privé, configurez les règles de contenu SSL pour chaque serveur avec un HREF sur chaque serveur ces points au VIP de règles de contenu SSL.

Vous pouvez également devoir apporter quelques modifications aux configurations des applications Web sur les serveurs sécurisés S1 et s2.

Également une règle de contenu avec les Témoins Rémanents d'un avancé-équilibre de définition de configuration exige de tous les clients d'activer des Témoins sur leur navigateur.

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Configurations

Ce document utilise la configuration suivante :

- CSS11XXX avec WebNS 5.00 et plus tard - Configuration en cours

CSS11XXX avec WebNS 5.00 et plus tard - Configuration en cours
`!Generated on 10/10/2001 18:12:17 !Active version:`

```
ap0500015s  configure !*************************
SERVICE************************   service s1     ip
address 10.10.1.101     active  service s2     ip
address 10.10.1.102     active
!*************************
OWNER************************  owner cookie-ssl
content layer5cookie        vip address 10.10.1.66
protocol tcp        port 80        url "/*"
advanced-balance arrowpoint-cookie        !--- Specify a
port in the content rule to use this option. !--- Port
80 traffic is used here. !--- All clients must enable
cookies on their browser.         add service s1
add service s2        active      content s1-ssl
vip address 10.10.1.88        protocol tcp        port
443        application ssl        add service s1
active     content s2-ssl        vip address 10.10.1.99
protocol tcp        port 443                application
ssl        add service s2        active !--- Use this
HREF on server S1 where switching from http to https:
<A HREF="https://10.10.1.101/applicationpath1/"> secure
site s1 </A> !--- Use this HREF on server S2 where
switching from http to https: <A
HREF="https://10.10.1.102/applicationpath2"> secure site
s2 </A> !--- In the example, the addresses for servers
s1 and s2 must be !--- reachable from the client. If
this is not the case, you must add a !--- content rule
for each server with a unique publicly routable VIP !---
address and one service for each SSL server, as shown
here: content s1-ssl vip address 10.10.1.88 protocol tcp
port 443 application ssl add service s1 active content
s2-ssl vip address 10.10.1.99 protocol tcp port 443
application ssl add service s2 active!--- Use this HREF
on server s1 where the switch from http to https occurs:
<A HREF=https://10.10.1.88/applicationpath1/> secure
site s1 </A>  !--- Use this HREF on server s2 where the
switch from http to https occurs: <A
HREF=https://10.10.1.99/applicationpath2> secure site s2
</A>
```

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Page de support produit de gamme 11000 de Cisco CSS
- Configurer des paramètres Rémanents pour des règles de contenu
- Support et documentation techniques - Cisco Systems