目录

简介

本文为CSS 11xxx产品和Web应用程序提供一配置示例为了保持客户端被滞留对同一个服务器，您是否使用HTTP或SSL。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 了解HTTP和SSL基础。
- 有关于CSS 11xxx产品和Web应用程序的知识。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco WebNS软件版本5.00和以上
- 所有Cisco CSS 11xxx系列内容服务交换机

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

在加密套接字层的，会话期间许多网站让客户端在超文本传输协议(HTTP)端口80帮助下进入他们的站点，但是希望客户端过渡到安全套接字层SSL协议。这是方式保持客户端被滞留对同一个服务器，您是否使用HTTP或SSL。

客户端要求HTTP数据流被注定对Virtual IP (VIP)。交换机做出一个负载平衡决策。在本文中，流量去服务器s1。客户端然后被滞留到根据其中一个s1的服务器高级平衡方法，例如sticky-srip，sticky-srcip-dstport和Cookie。参考配置内容规则的粘性参数欲知更多信息。

在客户端的会话期间，转换被使得到SSL端口443，当客户端选择在重定向对https的页时的一条链路。这导致一个新的内容规则点击，并且客户端可能负载平衡到另一个服务器。因为流量当前是加密的https (SSL/TLS)， CSS不能在第4层(TCP端口号)上检查Cookie， URL等，因为请求加密，当信息通过CSS时。为了防止此问题出现，请配置在每个服务器的重定向的HREF指向回到https同一服务器公共地址，不是VIP地址，如显示此处：

如果您的服务器在专用地址空间，请配置每个服务器的SSL内容规则有在每个服务器的一HREF的对SSL内容规则VIP的该点。

您在安全服务器s1和s2可能也需要做对Web应用程序的配置的一些修改。

并且一个内容规则粘性配置设置为高级平衡小段信息要求所有客户端启用在他们的浏览器的Cookie。

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

配置

本文档使用以下配置：

- CSS11XXX用WebNS 5.00及以后-运行的配置

CSS11XXX用WebNS 5.00及以后-运行的配置

```
!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>
```

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- Cisco CSS 11000系列产品支持页
- 配置内容规则的粘性参数
- 技术支持和文档 - Cisco Systems