Содержание

Введение

Этот документ предоставляет пример конфигурации для CSS 11xxx продукты и Web - приложения для хранения, клиент придерживался того же сервера, используете ли вы HTTP или SSL.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Поймите основы HTTP и SSL.
- Ознакомьтесь о CSS 11xxx продукты и Web - приложения.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Выпуск 5.00 Программного обеспечения webns Cisco и позже
- Весь CSS Cisco 11xxx коммутаторы служб содержимого серии

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Общие сведения

Много веб-сайтов сделали, чтобы клиенты ввели свой узел с помощью порта 80 Протокола HTTP, но хотели клиентов к переходу к Протоколу SSL во время сеанса для безопасных транзакций. Вот способ поддержать, клиент придерживался того же сервера, используете ли вы HTTP или SSL.

Трафик HTTP запросов клиента, предназначенный к Виртуальному IP (VIP). Коммутатор принимает решение о распределении нагрузки. В этом документе трафик переходит к s1 сервера. Клиент тогда застревает к s1 сервера на основе одного из балансировочных методов усовершенствования, таких как sticky-srip, Sticky-srcip-dstport и cookie. См. Постоянные параметры Настройки для Правил содержимого для получения дополнительной информации.

Во время сеанса клиента переход сделан к порту 443 SSL, когда клиент выбирает ссылку на странице, которая перенаправляет к https. Это вызывает новое правило содержимого для обращения, пользователь может быть перемещен на другой сервер для выравнивания нагрузки. Поскольку трафик является теперь зашифрованным https (SSL/TLS), CSS не в состоянии проверить выше уровня 4 (номер порта TCP) для cookie, URL и т.д., потому что запросы зашифрованы, когда информация передает CSS. Для предотвращения возникновения этой проблемы настройте HREF перенаправления на каждом сервере для обращения назад к https в том же общем адресе серверов, не адресу VIP, как показано здесь:

Если ваши серверы находятся в частном пространстве адресов, настраивают SSL правила содержимого для каждого сервера с HREF на каждом сервере, который указывает к VIP Правил содержимого SSL.

Вы, возможно, также должны сделать некоторые модификации к конфигурациям web - приложений на защищенном s1 серверов и s2.

Также правило содержимого с набором конфигурации сообщений на экране к файлам cookie с расширенными возможностями балансировки требует, чтобы все клиенты включили cookie на своем браузере.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Конфигурации

В данном документе используется следующая конфигурация:

- CSS11XXX с WEBNS 5.00 и позже - Рабочая конфигурация

CSS11XXX с WEBNS 5.00 и позже - Рабочая конфигурация

```
!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>
```

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Страница поддержки Cisco CSS 11000
- Настройка Sticky-параметров для правил контента

- Cisco Systems – техническая поддержка и документация