目次

概要

このドキュメントでは、HTTP を使用するか、SSL を使用するかに関係なく、クライアントを同じサーバに固定するための CSS 11xxx 製品および Web アプリケーションの設定例を紹介します。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- HTTP および SSL の基本を理解して下さい。
- CSS 11xxx 製品および Webアプリケーションについてのナレッジを持って下さい。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco WebNS ソフトウェアリリース 5.00 およびそれ以降
- すべての Cisco CSS 11xxx シリーズ コンテンツ サービス スイッチ

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

多くの Webサイトはクライアントに Hypertext Transfer Protocol （ HTTP ） ポート 80 の助けによってサイトを入力してもらいますがクライアントに安全なトランザクションのためのセッションの間に Secure Socket Layer （ SSL ） プロトコルに移行してほしいです。 HTTP か SSL を使用するかどうかクライアントを同じサーバに接続しておく方法はここにあります。

クライアントは、宛先が Virtual IP (VIP; 仮想 IP) である HTTP トラフィックを要求します。 スイッチは、ロード バランシングの決定を行います。 この資料では、トラフィックはサーバ s1 に行きます。 クライアントはスティッキsrip、sticky-srcip-dstport およびクッキーのようなアドバンス バランス メソッドの 1 つに、基づいてサーバ s1 にそれから接続されます。 詳細についてはコンテンツルールのためのスティッキー パラメータの設定を参照して下さい。

クライアントのセッションの間に、SSL ポート 443 への遷移はクライアントが https にリダイレクトするページのリンクを選択するときなされます。 これにより新しいコンテンツ ルールがヒットし、クライアントが別のサーバにロード バランスされる場合があります。 このときトラフィックが暗号化された https （ SSL/TLS ）であるので、CSS は情報が CSS を渡すとき要求が暗号化されるのでクッキー、URL 等をレイヤ4 （ TCPポート番号 ）の上でチェックできません。 この問題の発生を防ぐために、ここに示されているように同じサーバ パブリックアドレスで https に戻って、ない VIP アドレス、指すために各サーバのリダイレクト HREF を設定して下さい:

サーバがプライベートアドレス空間にある場合、SSL コンテンツルール VIP に各サーバの HREF で各サーバのための SSL コンテンツルールをそのポイント設定して下さい。

また保護されたサーバ s1 および s2 で Webアプリケーションのコンフィギュレーションへのいくつかの修正を行う必要がある場合もあります。

また、スティッキ設定が advanced-balance cookies に設定されているコンテンツ ルールでは、すべてのクライアントがブラウザのクッキーを有効にしている必要があります。

設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool （登録ユーザ専用 ）を使用してください。

設定

このドキュメントでは次の設定を使用しています。

- WebNS 5.00 およびそれ以降の CSS11XXX -実行コンフィギュレーション

WebNS 5.00 およびそれ以降の CSS11XXX -実行コンフィギュレーション

```
!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>
```

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- Cisco CSS 11000 シリーズ製品に関するサポートページ
- コンテンツ ルールのためのスティッキ パラメータの設定
- テクニカルサポートとドキュメント - Cisco Systems