

## Nginx + Tomcat + HTTPS 配置原来不需要在 Tomcat 上启用 SSL 支持

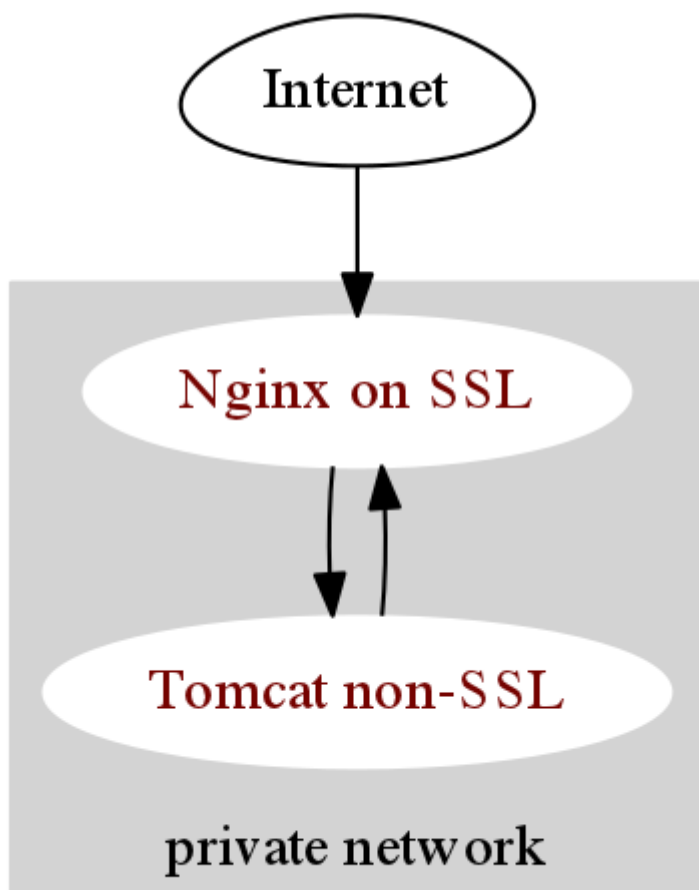
OSC厦门源创会，报名倒计时！>>>

HOT

9

收藏(133)

之前在网上搜索到的很多文章在描述 Nginx + Tomcat 启用 HTTPS 支持的时候，都必须在 Nginx 和 Tomcat 两边同时配置 SSL 支持。但我一直在想为什么就不能按照下面的方式来配置呢？就是 Nginx 上启用了 HTTPS，而 Nginx 和 Tomcat 之间走的却是普通的 HTTP 连接。但是搜索很多没有解决办法，最后还是老老实实的 Nginx 和 Tomcat 同时配置的 SSL 支持。



最近给 OSChina 买了个新的支持 \*.oschina.net 泛域名的证书，然后我又开始偷懒的想为什么 Tomcat 一定要配 HTTPS 呢？没道理啊。然后潜心搜索终于找到了解决方案。原来却是如此的简单。

最终配置的方案是浏览器和 Nginx 之间走的 HTTPS 通讯，而 Nginx 到 Tomcat 通过 proxy\_pass 走的是普通 HTTP 连接。

下面是详细的配置（Nginx 端口 80/443，Tomcat 的端口 8080）：

Nginx 这一侧的配置没什么特别的：

```
upstream tomcat {
    server 127.0.0.1:8080 fail_timeout=0;
}

# HTTPS server
server {
    listen 443 ssl;
    server_name localhost;

    ssl_certificate /Users/winterlau/Desktop/SSL/oschina.bundle.crt;
    ssl_certificate_key /Users/winterlau/Desktop/SSL/oschina.key;
```

```

ssl_session_cache    shared:SSL:1m;
ssl_session_timeout  5m;

ssl_ciphers HIGH:!aNULL:!MD5;
ssl_prefer_server_ciphers on;

location / {
    proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
    proxy_set_header Host $http_host;
    proxy_set_header X-Forwarded-Proto https;
    proxy_redirect off;
    proxy_connect_timeout    240;
    proxy_send_timeout       240;
    proxy_read_timeout       240;
    # note, there is not SSL here! plain HTTP is used
    proxy_pass http://tomcat;
}

```

其中最为关键的就是 `ssl_certificate` 和 `ssl_certificate_key` 这两项配置，其他的按正常配置。不过多了一个 `proxy_set_header X-Forwarded-Proto https;` 配置。最主要的配置来自 Tomcat，下面是我测试环境中的完整 `server.xml`：

```

<?xml version='1.0' encoding='utf-8'?>
<Server port="8005" shutdown="SHUTDOWN">
  <Service name="Catalina">
    <Connector port="8080" protocol="HTTP/1.1"
      connectionTimeout="20000"
      redirectPort="443"
      proxyPort="443"/>

    <Engine name="Catalina" defaultHost="localhost">

      <Host name="localhost" appBase="webapps"
        unpackWARs="true" autoDeploy="true">
        <Valve className="org.apache.catalina.valves.RemoteIpValve"
          remoteIpHeader="x-forwarded-for"
          remoteIpProxiesHeader="x-forwarded-by"
          protocolHeader="x-forwarded-proto"
        />
        <Context path="" docBase="/oschina/webapp" reloadable="false"/>
      </Host>
    </Engine>
  </Service>
</Server>

```

上述的配置中没有什么特别的，但是特别特别注意的是必须有 **`proxyPort="443"`**，这是整篇文章的关键，当然 `redirectPort` 也必须是 443。同时 **<Value>** 节点的配置也非常重要，否则你在 Tomcat 中的应用在读取 `getScheme()` 方法以及在 `web.xml` 中配置的一些安全策略会不起作用。

怎么样，简单到一塌糊涂吧！！！！



Tomcat

红薯



举报 分享

发贴于2年前 32回/13K+阅