SSLVPN 隧道模式下使用书签

版本	1.0
时间	2014 年 12 月
支持的版本	FortiOS v4.3.x, v5.0.x
审核	已通过
反馈	support_cn@fortinet.com

目　录

目的

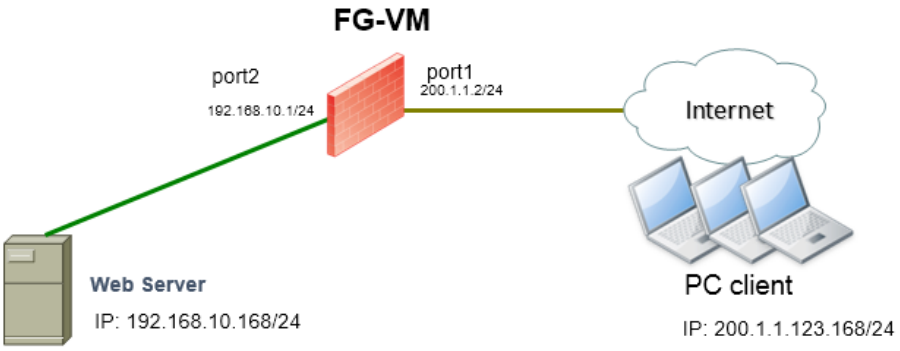
1. 解决 SSLVPN 代理模式的兼容性问题

由于用户 Web 服务器的网页代码不规范，常常与 SSLVPN 代理模式不兼容，导致无法正常访问。

2. 解决 SSLVPN 代理模式已有书签功能受限问题

SSLVPN 代理模式(proxy mode)已经支持书签功能，但由于防火墙本身存储容量及扩展性受限，用户定制书签时不能任意设计书签，局限性比较大。

拓扑



组件

FortiGate VM, FortiOS v5.0.9 build0292

内网 WEB 服务器：

定制的书签在内网 WEB 服务器上运行

方法

客户通过浏览器登陆 SSLVPN 后，先后执行两个行为：

1. 登陆后利用 SSLVPN 代理模式的 url 链接重定向功能，重定向到内网的书签网页。
2. 自动启用 SSLVPN 隧道模式，以便后续书签页的访问流量都走 SSLVPN 隧道

注意：

a) 重新编码书签网页的在线工具 http://htmlobfuscator.com/

b) 在浏览器上要允许对 SSLVPN 站点弹出窗口，否则不能打开这个重定向的书签页面。

配置步骤

FortiGate 配置

FortiGate 上 SSLVPN 配置主要启用隧道模式，**在命令行配置 redir-url**。


```
config vpn ssl web portal
    edit "full-access"
    next
    edit "Intranet_Sites"
        set allow-access web
        set redir-url "http://192.168.10.168"    #重定向到内网的服务器书签页面
        set heading "MySSLVPN"
        set allow-user-bookmark disable
        set auto-prompt-mobile-user-download disable
            config widget
                edit 1
                    set name "Please enable PopUps for this site"
                    set type tunnel
                    set ipv6-split-tunneling disable
                    set ip-pools "ssl-pool"
                next
            end
    next
end
```

SSLVPN 认证策略

SSL 隧道策略

其他配置与常规的 SSLVPN 配置一样。

书签网页重新编码

访问网站 http://htmlobfuscator.com/。书签网页需要重新编码，以便 SSLVPN 代理模式不再在书签链接前加上代理头，这样后续的流量就能走隧道模式了。

粘貼的源代碼:

```
<html style="height:100%">
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=UTF-8">
<TITLE>My Book Marker</TITLE>
<body>
        <DL>
        <DT><A HREF="ftp://192.168.10.168" target="_blank">FTP server</A>
        <DT><A HREF="http://192.168.10.168/mySearch.html" target="_blank">Web Server</A>
        </DL>
        <DT><A HREF="https://home.eease.com"  target="_blank">Fortinet HR</A>
</body>
</html>
```

原始书签网页代码

加密 | 復位 | 區別

來源類型: ○JavaScript ◉HTML 注意区别

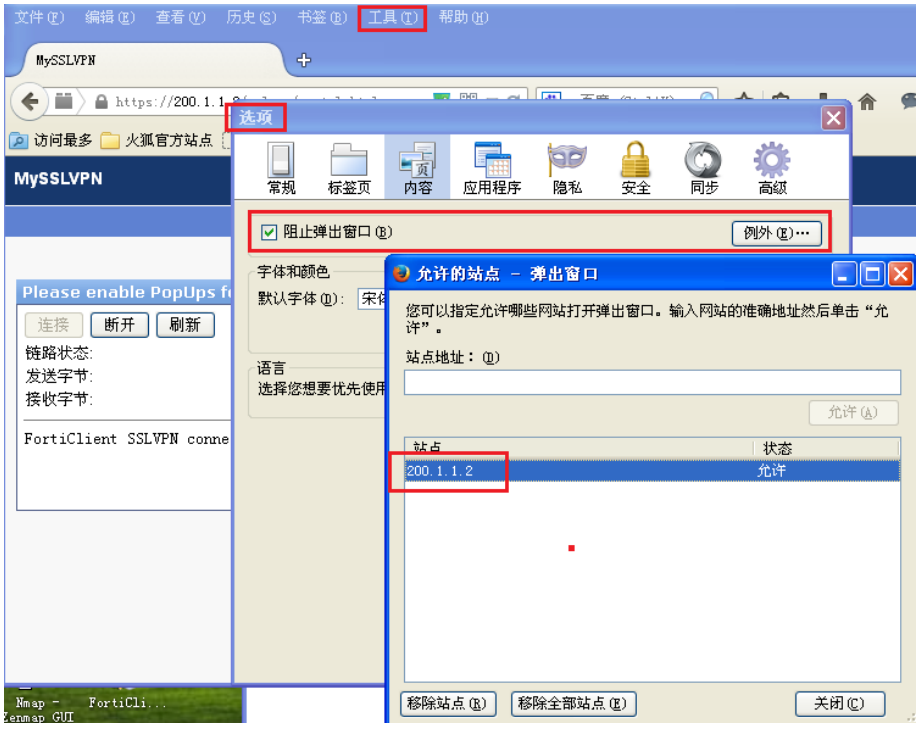
加密代码:

编码后书签网页代码

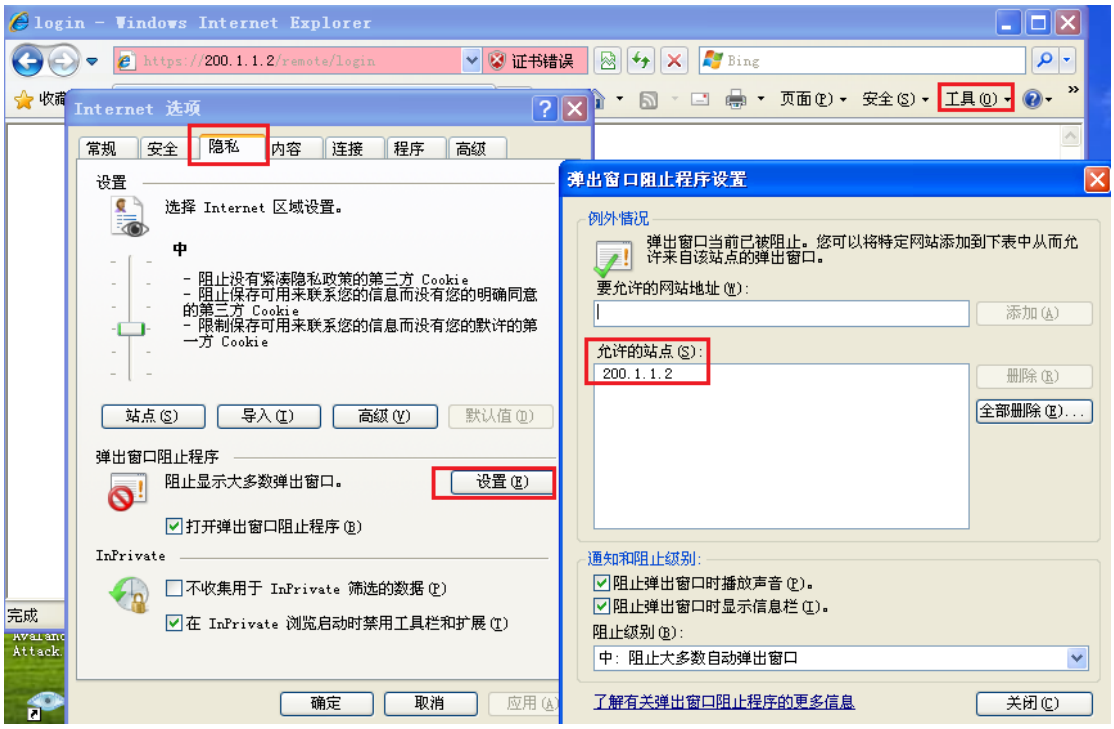
```
<script language="javascript" type="text/javascript">var
lOO='KkSKpcCfngCdpxGcz5yJlNXYlVGfShEMywHZslGaDRmblBHchxHdl5Wa0J3bGV0M8JXZ2JXZTBjM8lHZvJGf
05WZtVGbFVGdhVmcjxHTExXZ0lmc3xnZlJHfsJXd8JXZyJXZmVmc812bjxXZtFmTnFGV5J0c05WZtVGbFRXZnxXZw
F2YzVmb1xHTSVFfkFWZoxHdodWalhmMywnVJVVUFxHVOVEVO90QwIDfpBXY5JXZ1Fna8NmczRXZnxHc0RHa8VWbvh
GfzBHd0hmMywncltmch1EMywHd4VGdyIDfvZmbpxHduVGdu92QyIDf0V2cyFGajBjM8h2YyFWZTlXb8lXTFNDfFxE
VJR1Qzw3avxnRUVFRzwXZwlHV8VGb5R3cwIDfs1GdoN0M8xHf8xHfwATMBNDfiV2VFNDfxAzT8xERDNDfr92bCBjM
8BHdmJjM8JXZ2JXZzBjM8FEVF10QzwHUUZURzwHdwlmcjNHfr5WYsJ2XyIDfwRHdoJjM8lHZvJ2QzwXQDNDfyFmd8
ZURShEMywHN3EDfUR0QzwXZwF2YzV2X8Rnbl52bw12bDlkUVVGZvNmblxHdldmchRHMywHbtRHa8VETUlEV8Rnbl1
Wdj9GZ8FEM8BDO8BFVUhEMyw3YyNHfsFTS8xHf5ADf4YTM8JTOxwnM2wHc4V0ZlJFflR2bDJXYoNUbvJnZ8RXasB3
c8dmbpJHdT9Gd8RnbJV2cyFGc8dXZuxHbhZXZ8ZWa8dmbpJHdTxXZjFGbwVmc8VGbph2d85mc1RXZyxnbvlGdj5Wd
mxHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8xHf8
```

浏览器允许弹出窗口

FireFox

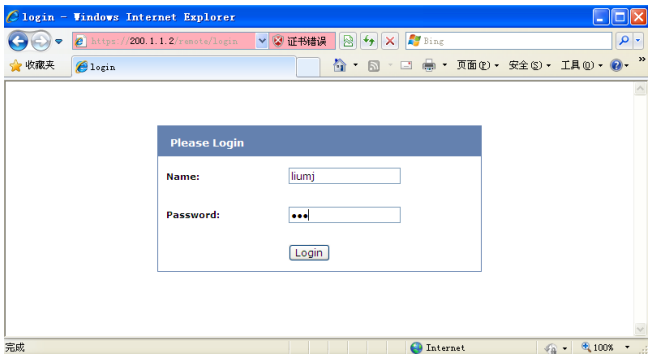


IE 浏览器

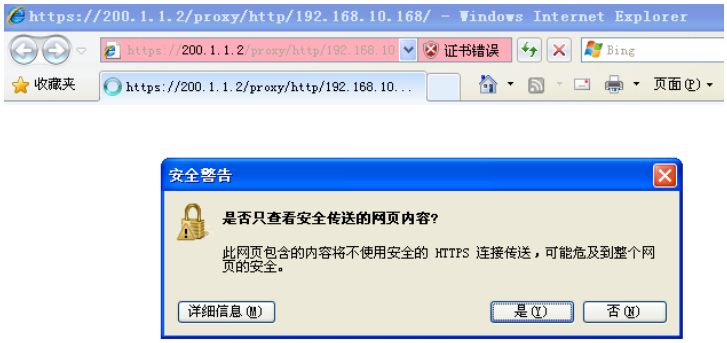


测试效果

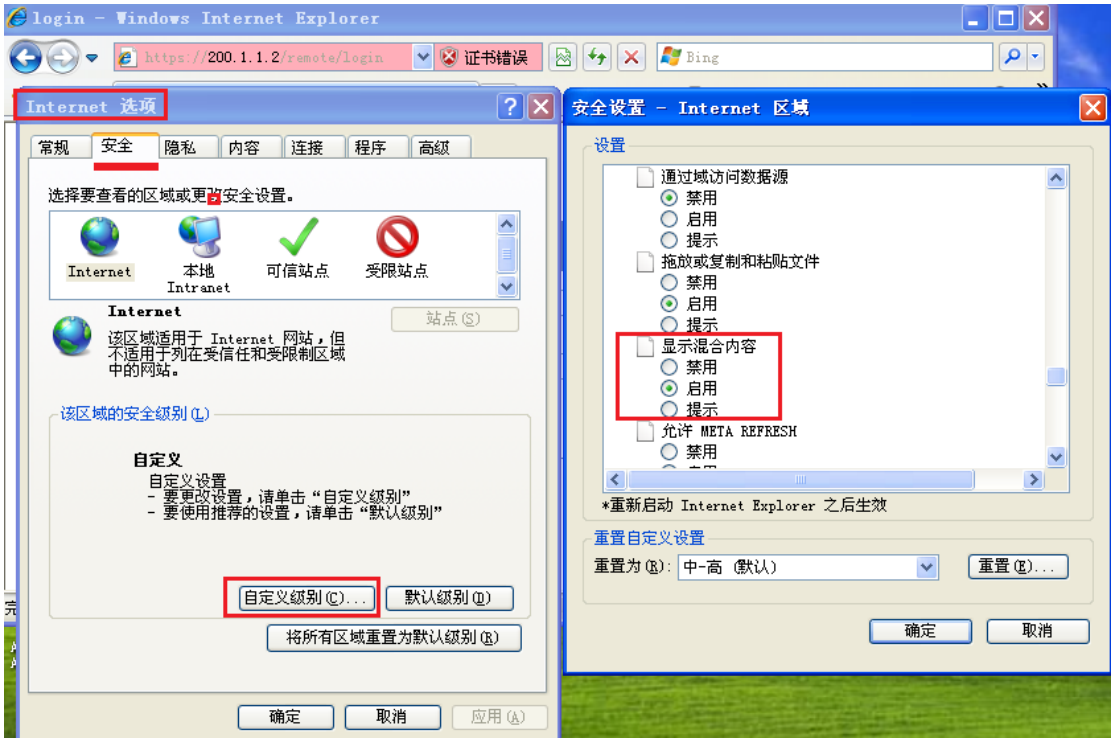
用 IE 登录 SSL 登录



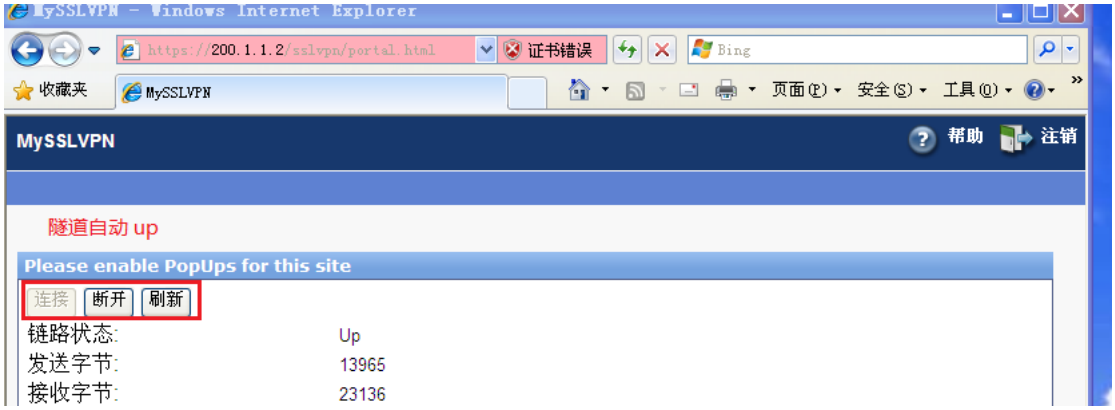
弹出的书签页面有安全告警提示，选择 否



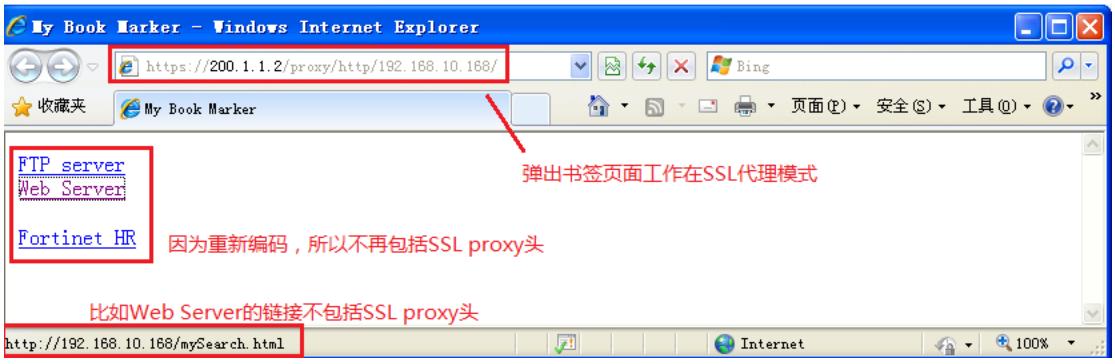
避免提示的设置



隧道自动 UP



弹出不包括 SSL proxy 头的书签链接



FireFox 的测试过程没有弹出安全警告，简单直接。