FortiWeb 部署模式介绍

版本	1.1
时间	2016 年 12 月
支持的版本	FortiWeb -v5.0.x 以上
作者	李威峰
状态	草稿
反馈	support_cn@fortinet.com

目录

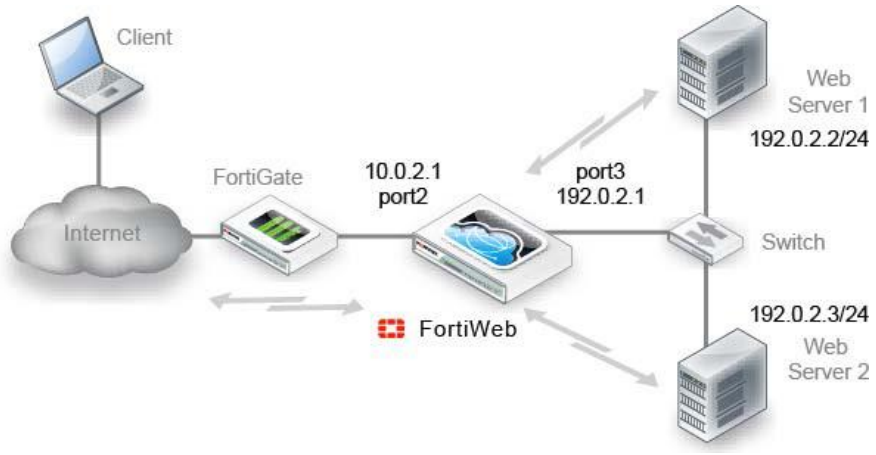
简介.....3
在线模式.....3
拓扑.....3
数据流.....3
纯粹透明代理模式.....5
拓扑.....5
数据流.....5
透明模式.....6
拓扑.....6
数据流.....6
离线保护模式.....7
拓扑.....7
数据流.....7
WCCP 模式.....8
拓扑.....8
数据流.....8
部署模式选择.....9
各种工作模式下的功能对比.....10

简介

FortWeb 有五种工作模式，分别为“在线保护”/“纯粹透明代理”/“透明模式”/“离线模式”“WCCP”模式， 经常有工程师在部署 FortiWeb 的时候会问到，有什么区别，应该如何选择，本文详细介绍这部分。如果需要了解各种模式的配置过程和细节，请参考其它文档。

在线模式

拓扑



为了与其它模式有明显的区别，使用了以上拓扑来表达在线模式，
实际中往往是单臂部署，而不是串在网络中。

数据流

Client----FortiWeb（VIP）-----FortiWeb（Src-IP）----WebServer

1.客户端访问 FortiWeb 发布的 VIP（不能直接访问物理 IP）

2.FortiWeb 把 VIP 转换成 Web-Server 物理 IP。

3.FortiWeb 检测安全策略。

4.FortiWeb 以距离物理 Web-Server 最近的接口访问物理服务器。源地址为

FortiWeb 出接口 IP。

5.物理 Web—Server 返回报文给 FortiWeb-IP

6.FortiWeb 转换源物理 IP 为 VIP，源 IP 为 VIP 返回给客户端。

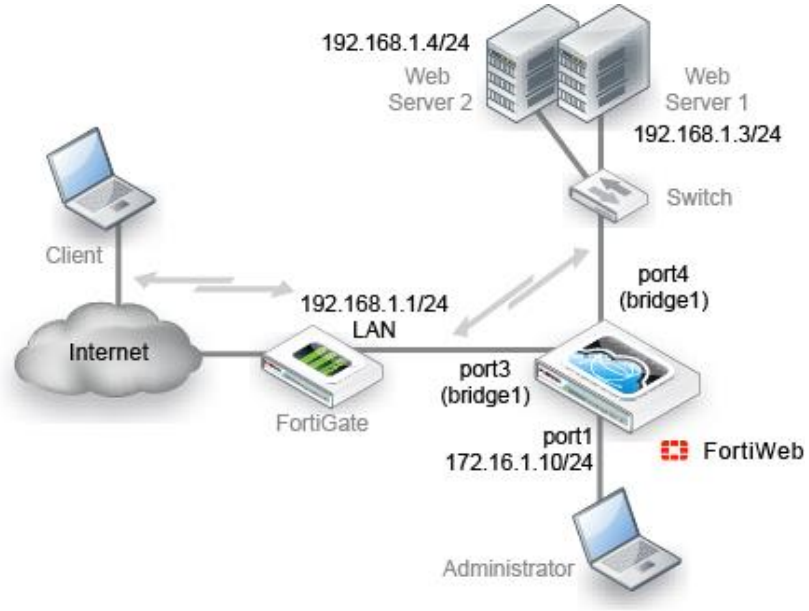
注意事项：

1. 在物理 Web_Server 上，看到的 HTTP 客户端的 IP 全部为 FortiWeb 的 IP
2. 如果需要在 Web_Server 上看到真实客户端的 IP，需要启用 FortiWeb 的 X-forwarded-for 特性，插入到 HTTP 的 header 中。

配置如下：

纯粹透明代理模式

拓扑



数据流

Client----FortiWeb(透明代理)------WebServer

1.客户端访问物理 Web-Server。

2.FortiWeb 代理这个请求（冒充 Web-Server）。

3.FortiWeb 检测安全策略。

4.FortiWeb 冒充客户端发起到 Web-Server 的访问。

5.物理 Web—Server 返回报文给 FortiWeb-代理。

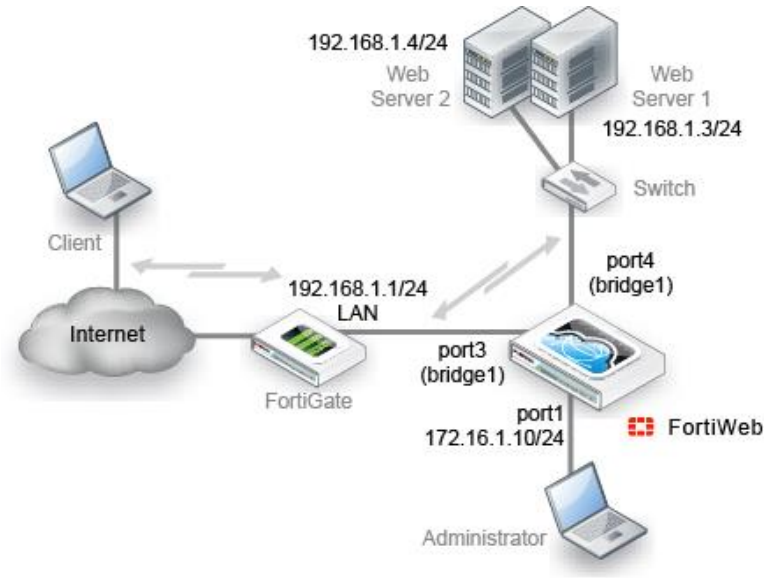
6.FortiWeb 代理返回给客户端。

注意事项：

1. FortiWeb 打断三层通讯，即对网络层“透明”。
2. 在 Web—Server 上看到的为真实客户端的 IP。

透明模式

拓扑



数据流

Client----------WebServer

1.客户端访问物理 Web-Server。

2.FortiWeb”看”这个请求。

3.FortiWeb 检测安全策略。如果发现请求有问题，发 TCP-Reset 报文给 Server 和 Client。

4.客户端访问 WebServer。

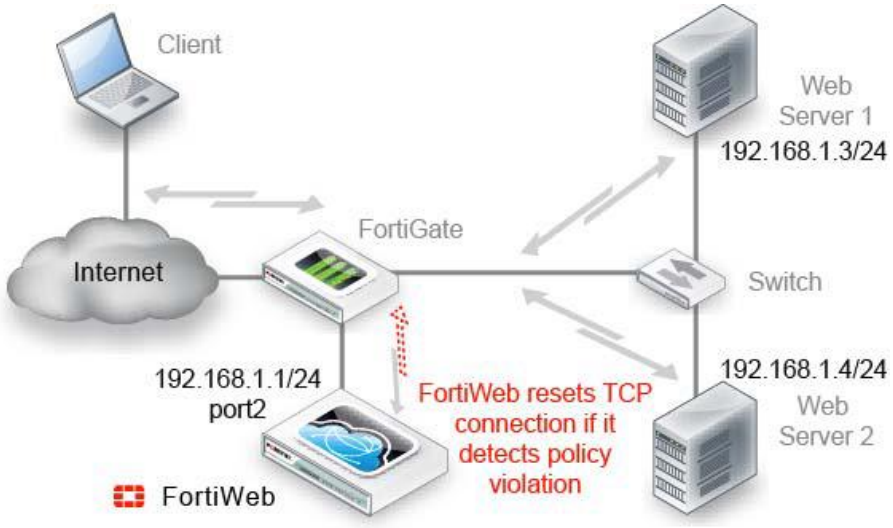
注意事项：

1.FortWeb 不打断三层通讯，即对网络层真正透明。

2.在 Web—Server 上看到的为真实客户端的 IP。

离线保护模式

拓扑



数据流

Client---------WebServer

1.客户端访问物理 Web-Server。

2.其它网络设备镜像流量给 FortiWeb。

3.客户端访问 WebServer。

4.FortiWeb 分析 Copy 过来的流量并检测安全策略。如果发现请求有问题，发 TCP-Reset 报文给 Server 和 Client。

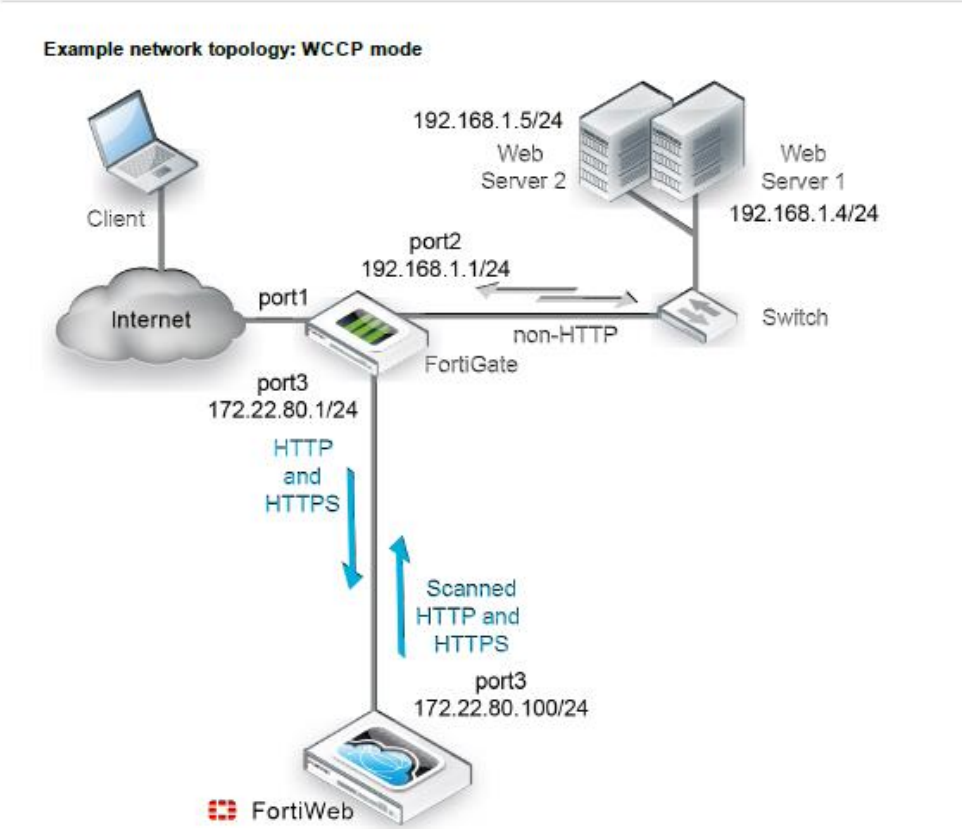
注意事项：

1.FortWeb 不打断三层通信，即对网络层真正透明。

2.在 Web—Server 上看到的为真实客户端的 IP。

WCCP 模式

拓扑



为了与其它模式有明显的区别，使用了以上拓扑来表达在线模式，

实际中往往是单臂部署，而不是串在网络中。

数据流

Client---------FortiWeb（Src-IP）----WebServer

1.客户端访问能直接访问物理 IP。

2.FortiWeb 检测安全策略。

3.FortiWeb 以距离物理 Web-Server 最近的接口访问物理服务器。源地址为 FortiWeb 出接口 IP。

4.物理 Web—Server 返回报文给 FortiWeb-IP。

5.FortiWeb 转换源物理 IP 为 VIP，源 IP 为 VIP 返回给客户端。

注意事项：

1.在物理 Web_Server 上，看到的 HTTP 客户端的 IP 全部为 FortiWeb 的 IP

2.如果需要在 Web_Server 上看到真实客户端的 IP，需要启用 FortiWeb 的 X-forwarded-for 特性，插入到 HTTP 的 header 中。

配置如下：

部署模式选择

FortiWeb 工作模式可以简单的理解为：

- 在线模式和纯粹透明代理，WCCP 模式本质上是一种模式，都是使用的代理方式，**支持所有 HTTP 应用层的功能**，要打断三层 TCP 会话，所以支持的功能比较多。
- 透明模式和离线模式为一种模式，使用的技术类似 IPS 和 IDS 的抓包技术，不打断三层 TCP 会话，所以支持的功能比较少。

在物理网络上，可以分为是旁挂和串两种方式。

其中，在线模式和 WCCP 模式：物理上使用旁挂，逻辑上是串接，对网络不透明。

纯粹透明代理：物理上串接，逻辑上是透明代理。

透明模式： 物理上串接，逻辑上是 IPS/IDS 模式。

离线模式：物理上是旁挂，逻辑上是 IDS(sniffer)模式。

在实际部署中，根据功能需求和客户的网络结构特点进行选择：

1.用户希望不改变网络拓扑，而且 Web 服务器比较集中，所以，纯粹透明代理模式比较常见。

2.在服务器比较分散的没有办法串接到网络中，使用在线模式（反向代理）。

3.WCCP 模式场景，可以使用 WCCP 协议或者用户通过做策略路由把 HTTP 流量送个 FortiWeb，FortiWeb 把流量处理完后以 FortiWeb 地址送给 Web 服务器。

透明模式和离线模式 因为对阻断效果有限，在实际中部署中并不常见。

各种工作模式下的功能对比

以下列举了常见的，详细对比见手册。

特性	工作模式			
	在线（In_Line）	纯粹透明代理（TTP）	透明模式（TI）	离线模式（Off_line）
桥/vzone	NO	Yes	Yes	No
缓存	Yes	Yes	No	No
服务器负载均衡	Yes	No	No	No
客户端证书校验	Yes	Yes	No	No
配置同步（不是 HA）	Yes（部分配置同步）	Yes	Yes	Yes
HA 模式	Yes	Yes	Yes	No
Cookies 保护	Yes	Yes	No	No
Dos 保护	Yes	Yes	No（仅支持 TCP-Flood）	No
错误页面自定义	Yes	Yes	No	No
Bypass	NO	Yes	Yes	No
文件压缩	Yes	Yes	Yes	No
信息泄露	Yes	Yes	No（仅仅 alart 报警）	Yes
页面访问顺序	Yes	Yes	No	No

页面重写/页面重定向	Yes	Yes	Yes	No
启始页面强制	Yes	Yes	No	No
X-forwarded-for	Yes	Yes	No	No