Fortinet FortiGate 产品安装及快速配置

— FortiGate-90D-PoE 产品为例

Fortinet 公司是全球网络安全行业领导者，FortiGate 正是这家公司的旗舰产品。FortiGate 拥有强大的网络和安全功能，服务于全球数万家客户，产品型号也是业界覆盖最广的，从几十兆产品到几百 G 产品，能够满足不同规模用户的使用需求。对于大企业和运营商客户来说，IT 人员能力强，资源多，对于设备的配置自然不在话下。但是对于规模不大的中小企业来说，IT 人员的运维能力可能就没有那么强了。

大家印象中传统的企业级设备配置安装都比较麻烦，友好性远不如家用路由器。因此很多用户也希望他们购买的企业级产品能够像家用级设备一样简单配置。FortiGate 就是一款这样的产品。

视频版本：http://edu.51cto.com/course/course_id-1118.html

FortiGate 设备开箱及配件说明

我们以 FortiGate-90D-POE 设备为演示，来为大家介绍一下 FortiGate 产品的安装、配置。后续我们还会有设备功能的使用介绍。

图 1：FortiGate-90D-POE 包装

图 2：FortiGate-90D-POE 和配件

如上图所示，FortiGate-90D-POE 内置了电源，光盘，手册，RJ45 网线和一根 USB 管理数据线。PC 可以通过 USB 管理数据线，使用 FortiExplorer 软件实现设备的快速配置。稍后我们会有讲解。

图 3：FortiGate-90D-POE 前面板和后面板

如图 3，前面板的左侧接口是用于调试的 console 口，中间四个灯为电源，状态等指示灯，右侧的双排指示灯是 WAN 口和交换口的状态指示灯，红色的 ABCD 四个灯标示了 POE 供电的四个接口。后面板的左侧为电源接口，螺丝钉为固定地线用，避免在漏电的情况下用户触电。螺丝钉下面的接口为 USB2.0 小接口，用于手机连接设备进行配置。再往右两个为 USB 管理口。后面板上的 16 个接口中，最右面两个为 WAN 口，其余 14 个为交换接口，红色标示的 ABCD 接口为 POE 供电口。

FortiGate 管理方式

图 4：接口示意图

FortiGate 系列产品默认在 internal 或者 mgmt1 口上有 IP 地址：https://192.168.1.99。用户名为：admin 密码为空。对于这款设备，随意插到任何一个接口都可以进行 web 登陆，因为默认在交换接口上已经启用了 DHCP 功能。所以只需让 PC 自动获得 IP 地址，即可通过访问上面的管理地址来进行 web 页面的登陆。结果如下图所示：

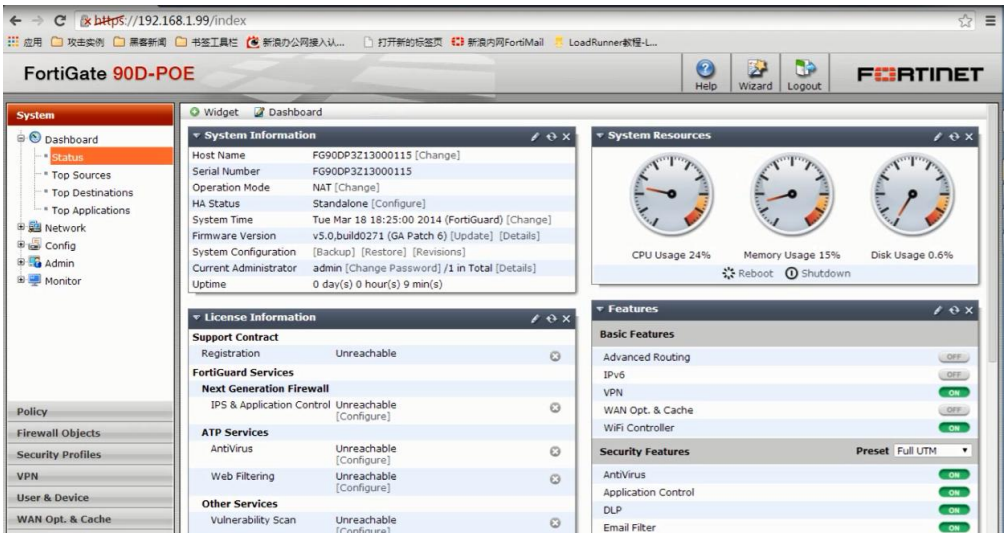

图 5 ：Web 界面

Fortinet 为用户提供了简单易用的管理软件 FortiExplorer 来进行初始化配置。下面我们就来介绍下如何使用 FortiExplorer 管理 FortiGate。

FortiExplorer 下载地址：
http://www.fortinet.com/resource_center/product_downloads.html

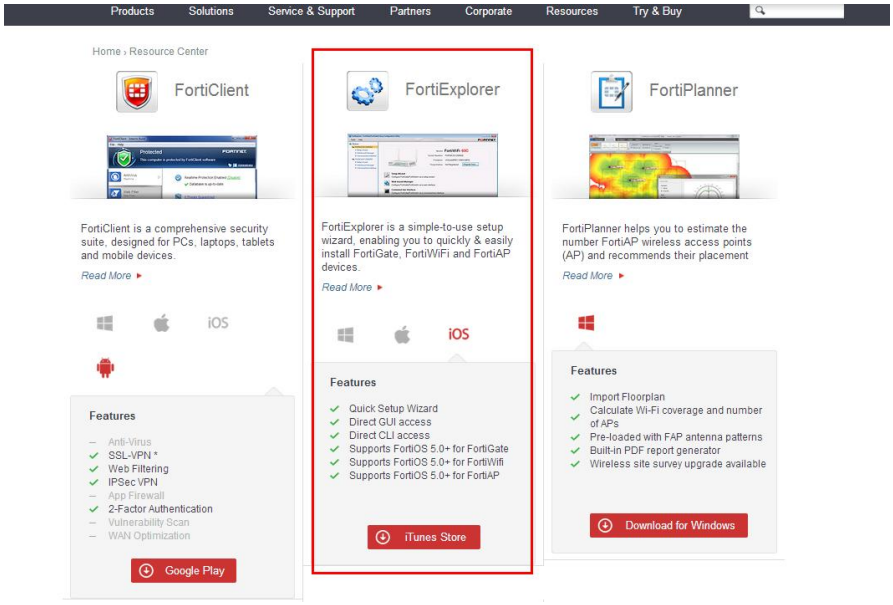

图 6：下载界面

可以看出 FortiExplorer 支持 windows，macOS 以及 iOS 三种操作系统，也就是说我们不仅可以通过 PC 和 MAC 来进行配置，还可以使用 iPhone。下面我们先来看看如何用 PC 版 FortiExplorer 来配置设备。

图 7：FortiExplorer PC 版连接方式

图 7 中使用的数据线就是设备包装中自带的 USB2.0 数据线。小口插到 FortiGate 上，大口插在 PC 端。

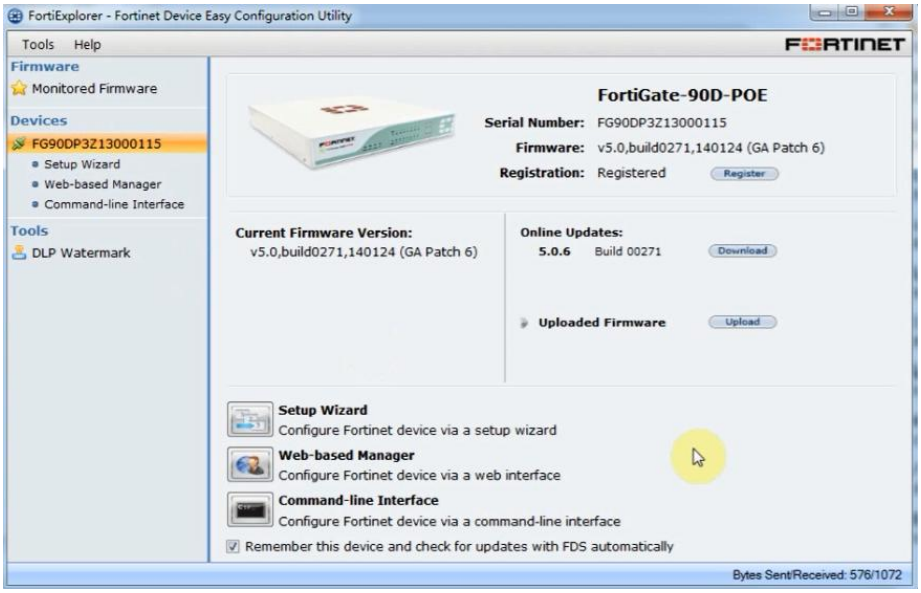

图 8：FortiExplorer 界面

连接上之后界面上就会自动显示出设备的产品图，序列号，系统版本，注册情况等等。跟常用的 PC 端手机管理软件很像。黄色高亮的内容就是这台 FortiGate 设备的名字，默认为设备序列号。用户可以使用这个软件来进行快速配置，基于 web 和命令行模式的管理。

有人可能会问，既然可以用浏览器进行 web 管理，在这个软件中还提供 web 模式管理不是多此一举吗？

非也！有的用户可能时间长了不登陆忘记了管理 ip，通过这个软件可以直接通过 USB 线连接到设备上，在软件中运行友好的 web 模式来查看接口信息等等。是不是想的很周到呢！

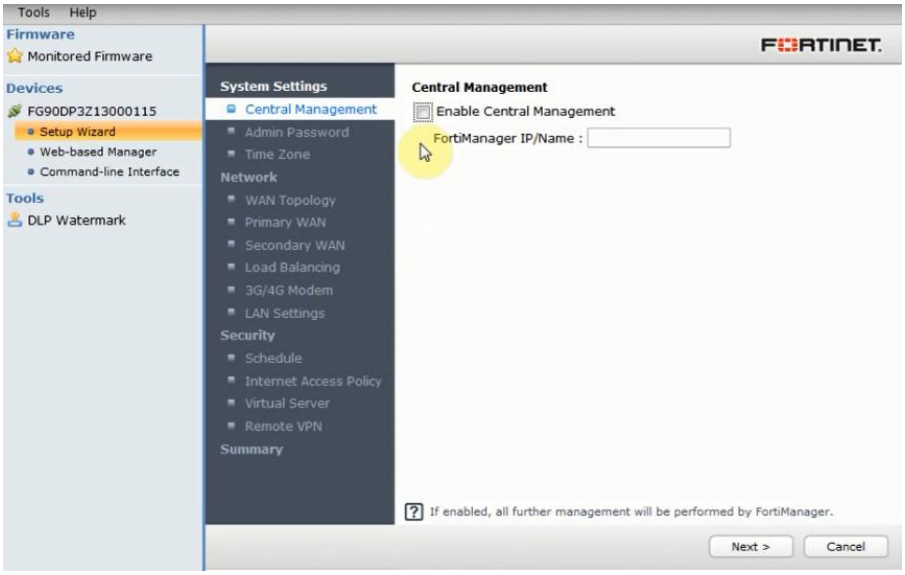

图 9： 通过 FortiExplorer 进行初始化配置

用户可以按照深蓝色的部分来依次配置，以完成设备的初始化配置。当然，虽然列表项很多，但是可以快速跳过某些项，比如 3G/4GModem，负载均衡等等。

刚才我们介绍了，我们可以通过 iPhone 配置和管理 FortiGate 设备，只需要通过一根数据线和 FortiExplorer 应用就可以了。那么该如何使用呢？

图 10： iPhone 连接 FortiGate 设备

将手机上的 fortiexplorer 打开，在将手机连接到设备上，就会自动进行初始化。过程中，您需要在如图 11 中所示的那样，选择设备类型，比如我们使用的是 FortiGate-90D-PoE，在 app 中就选择 FortiGate 90DP，然后选择添加，之后就会看到图 11 右侧的界面，用户名处输入 admin，密码留空，点击 login，就通过手机登陆到设备上了。

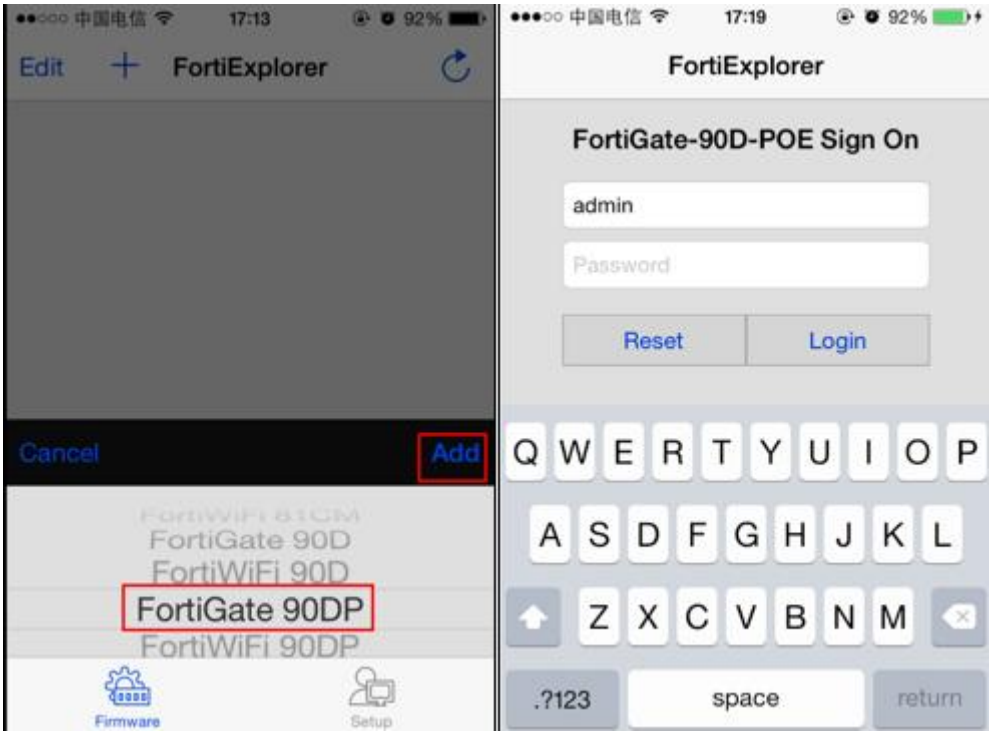

图 11：手机连接初始化

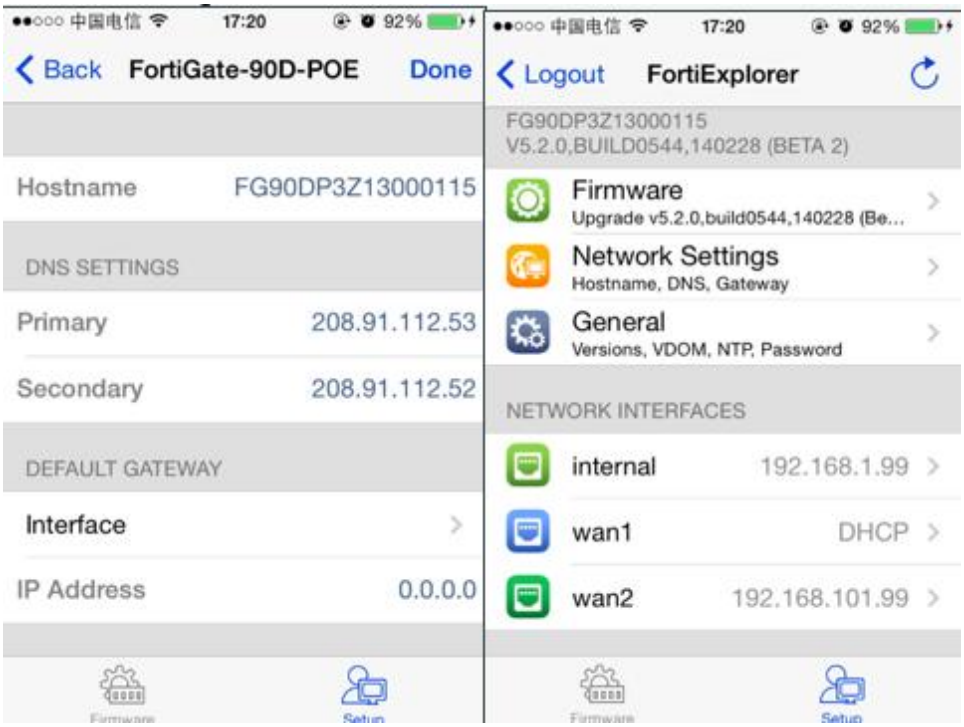

图 12：手机连接后 fortigate 状态显示

用手机登陆之后，就能看到如图 12 所示的内容了。设备名称，默认 DNS，初始 IP 地址，还有设备的版本信息，接口信息等等。

介绍完使用 fortiexplorer 进行设备初始化配置和管理之后，我们现在来介绍对一般用户来说难度较高的初始配置方法，也是我们后期真正做调试的过程中用的比较多的一种方法，就是使用 Console 口来进行配置。

图 13： console 线连接示意

线接好之后，我们使用的是 SecureCRT 来创建连接。

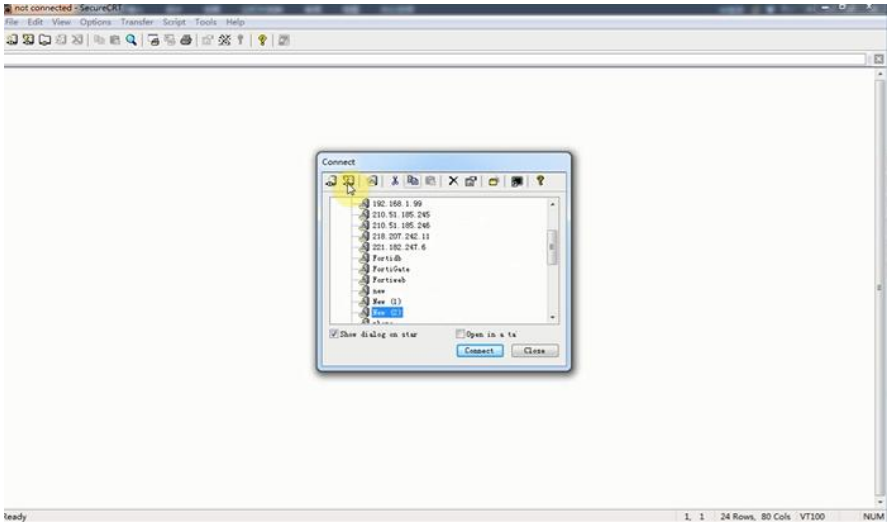

图 14：SecureCRT 界面

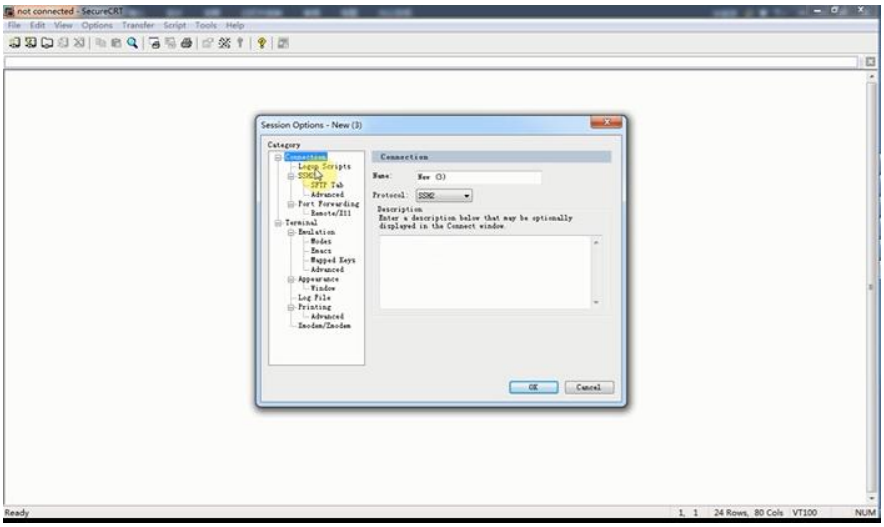

图 13：SecureCRT 新建连接

我们需要在连接到设备之前新建一个连接，协议选择的地方选择串口协议。选完协议后会被要求选择接口，具体是 COM1/COM2/COM3。。。我们就要到计算机的设备管理器中查看了，看一下端口（COM 和 LPT）这一项下面虚拟出来的 COM 口是几，我们的计算机显示为 COM3，就回到 SecureCRT 中选择 COM3 接口，然后波特率选择 9600

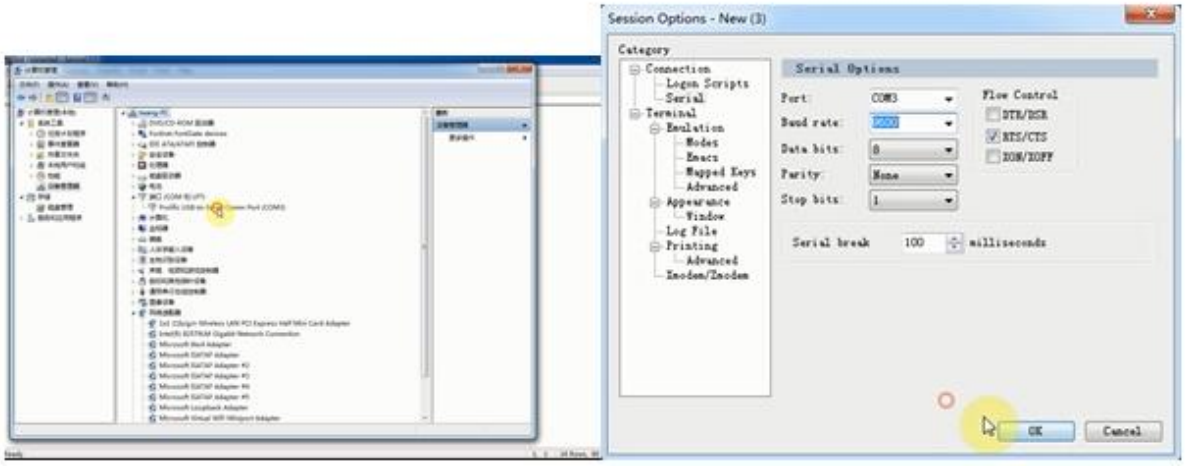

图 14：初始化连接建立配置

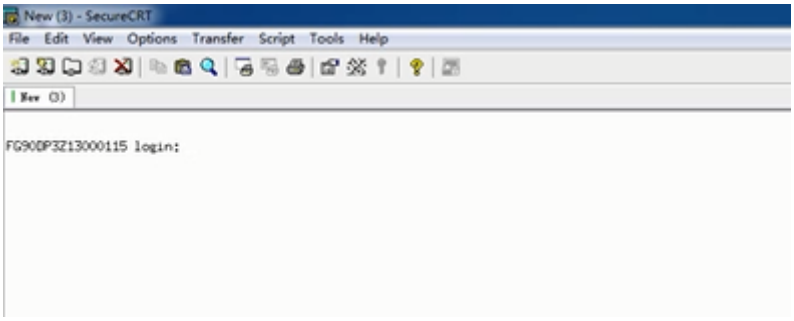

图 15：连接建立成功

FortiGate 界面操作

刚才介绍了几种不同的连接方式，我们已经能够成功地连接到设备上了。那么一开始基本的操作都有哪些呢？让我们来一起看一看。

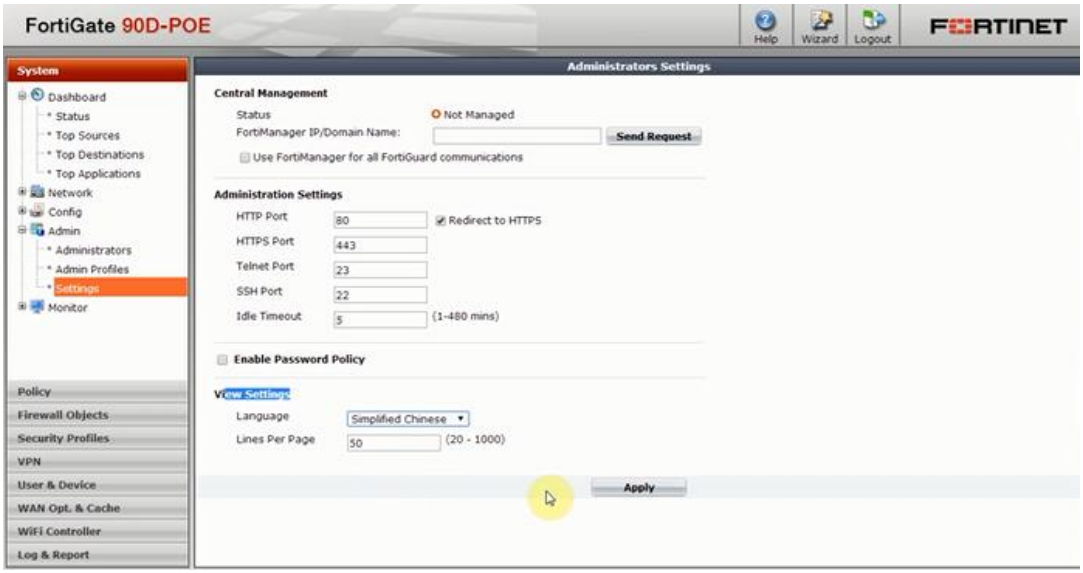

图 16：修改英文界面到中文界面

FortiGate 设备的 web 界面默认是英文的，但是管理员可能需要中文界面才能更好的操作，这样的话只需要在 System-Admin-Settings 中最下面找到 Language，选择 simplified Chinese（简体中文），然后点击 Apply。我们的 web 界面就会切换到中文模式了。

图 17：配置向导

配置向导中第一项就是集中管理，我们可以从图 17 中看到，可以选择是否启用集中管理，需要 FortiManager IP 等信息。FortiManager 是 fortinet 一款集中管理平台，可以管理分布在不同地区的上百台 FortiGate 设备，进行集中策略部署，下发，更新等等。这里我们由于没有 FortiManager 需要连接，所以直接点击下一步。

图 18：修改密码

第二项就是 Admin 密码，如果修改密码的话可以点击修改密码。不需要修改密码则只需点击下一步即可到下一项来设置时区。FortiGate 默认时区是 GMT-8，我们可以改为+8 北京时间。设置完之后再点击下一步，我们就来到了网络配置部分。

图 19：网络设置

由于这款设备支持双 WAN 接入，因此在图 19 中您可以看到有单以太网和双以太网两个，而且还支持 3G/4G 接入，可以将上网卡插到设备的 USB 接口上。由于我们演示环境只有单线接入，因此我们选择单以太网，然后点击下一步。

图 20：主 WAN 连接选择

设备提供 3 种主 WAN 网络接入类型，DHCP 类型，静态 IP 类型，和 PPPoE 拨号类型。PPPoE 就像是 ADSL 接入，设置方法和家用无线路由器一样，将 ADSL 账号和密码输入就好了。图 20 所示为静态 IP 的配置情况，填写好就可以了。我们演示环境是 DHCP，也是大多数企业场景。

图 21：LAN 设置

其实选择了 DHCP 之后，到 LAN 配置的界面上，设备自动生成了默认的一套配置。可以看到 internal 接口默认启用 DHCP，接口 ip 为 192.168.1.99，24 位掩码。地址池为 110-210。到这里网络方面的配置就已经结束了。按照向导，我们要进行安全策略方面的配置。

图 22：安全策略配置-时间表

这是要控制允许设备如何上外网，是否是允许设备总是通过设备上外网。或者在固定的时间段内可以上外网。比如有的公司要求某些部门的员工在 9 点到 12 点，14 点到 18 点是禁止上外网的，就会用到这样的策略。在这里我们选择总是允许来进行下一步的配置。

图 23：网络接入策略

内网设备要上外网必须要有从私网地址到公网地址的转换，因此 NAT 是默认开启的，其余的安全功能比如 UTM 功能，用户行为限制等等也是默认开启的。用户为了快速上线可以先不考虑，把界面上的勾点掉。后续有需求的时候可以再自行根据需求来开启相应的功能并且配置策略。

图 24：配置虚拟服务器

这一步就来到了是否要配置虚拟服务器。有些诸如 FTP 服务器的需要对外开放，因此要做服务器的虚拟地址映射。关于这部分内容和 VPN 连接我们后期会有详细的介绍。这里就不开启虚拟服务器了，并且跳过 VPN 配置，直接保存现有配置。

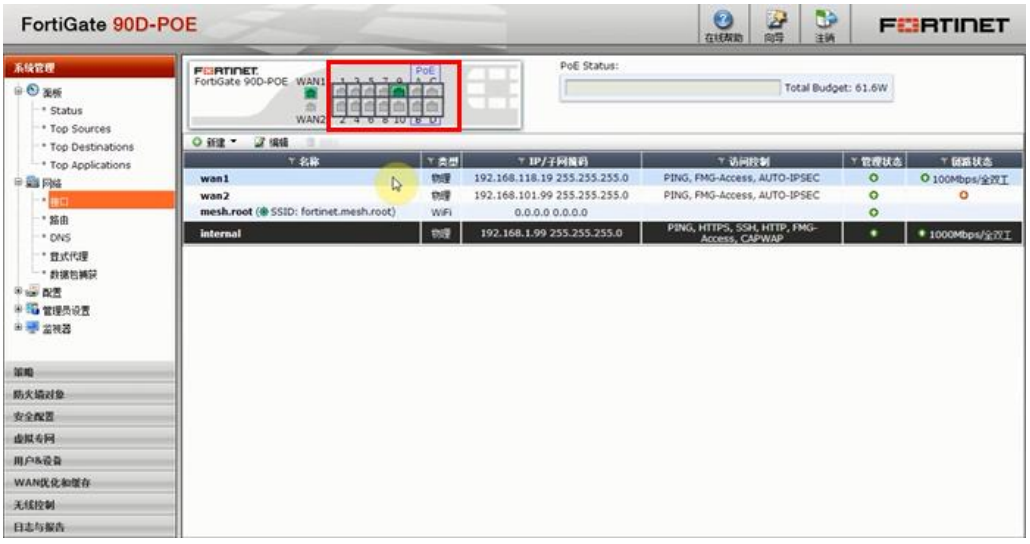

图 25：Web 界面确认配置

我们可以再系统管理-网络-接口中查看接口状态。FortiGate 的 web 界面作的比较友好的一点就是当您选择了 internal 接口后，图 25 中红色圈出来的地方能看到灰色的格子，可以对比没有高亮的 WAN 口，这样很直观地告诉用户哪些口是属于您选择的这个类型的接口。

之前我们已经通过向导正常配置设备。包括向导中也自动生成了一条策略。始终允许内网所有接口到 WAN 口的流量通行。

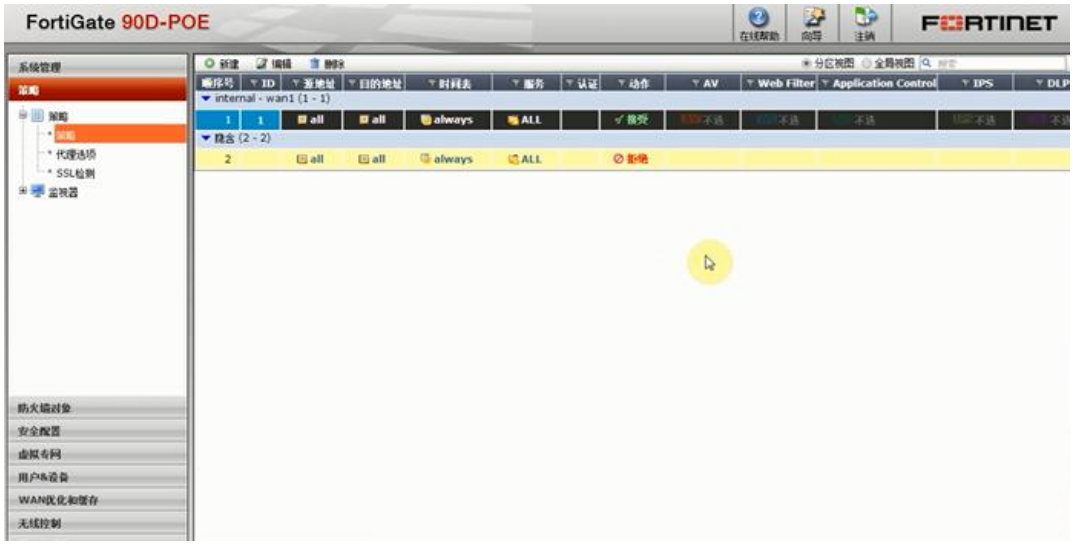

图 26：策略示意

至此为止我们已经建立好了网络。下一步就是需要对设备进行注册。当然您也可以选择不注册。注册地址为 support.fortinet.com。

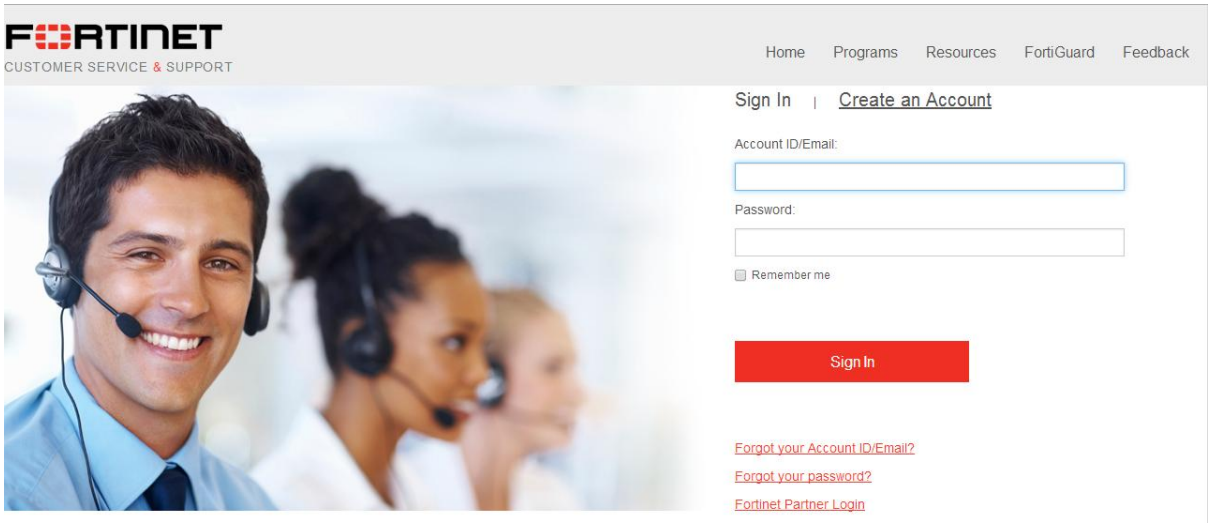

图 27：注册网站

（ https://support.fortinet.com/login/UserLogin.aspx ）

注册 FortiGate 设备

如果您已经注册过这个网站，那么可以直接选择登陆，如果是第一次使用 Fortinet 的产品，则需要先创建一个账号。点击创建账号之后完成个人信息的填写。保存之后您会收到一份确认注册成功的邮件。

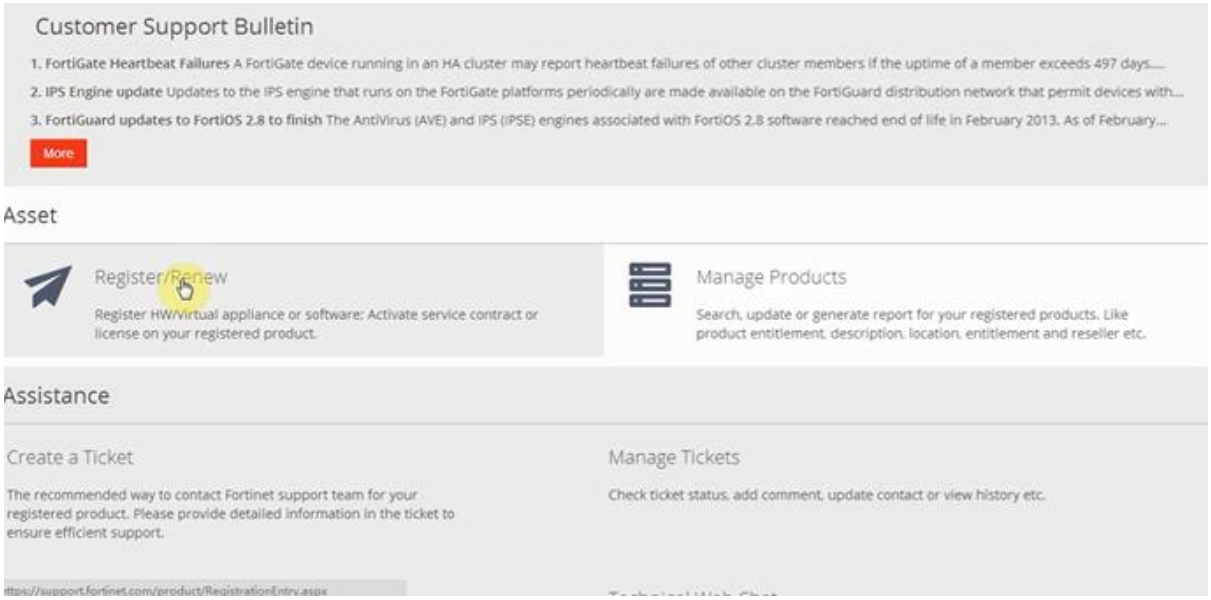

图 28：注册设备

我们点击图 28 黄色部分，开始将设备注册到您之前注册的账号中。将设备的序列号填写到表格中，点击下一步。会显示您设备所包含的服务。比如病毒库，IPS 特征库，安全服务等等。

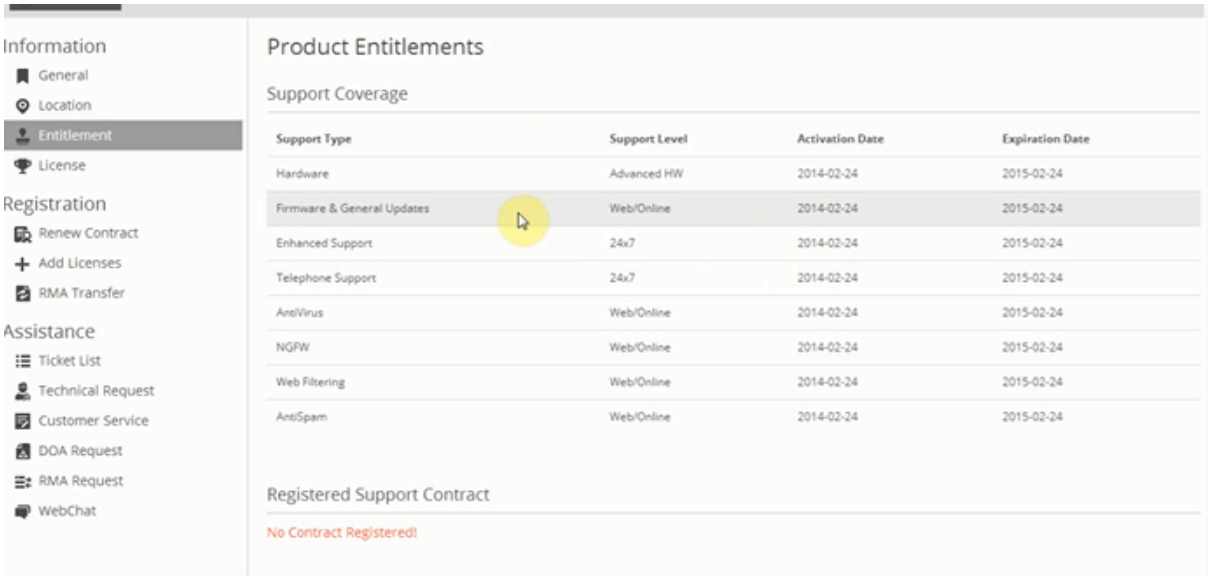

图 29：服务列表

图 29 显示了我们演示的这台设备的服务内容。

图 30：设备管理界面显示服务状态

若是已经注册成功，在图 30 所示的设备管理界面中蓝色高亮出来的部分会显示服务到期的日期，和是否生效的信息。由于我们的服务信息是通过云网络同步的，可能会有几分钟的延迟。如果几分钟之后还没有更新，您可以在下方的命令行中输入命令 exec update-now 来强制同步服务信息。

图 31：手动更新服务

至此为止，我们产品安装及快速配置部分就为您介绍完毕了。后续我们还会针对重点功能来进行细致的讲解。