



**FortiGate-60/60M/ADSL,
FortiWiFi-60,
FortiGate-100A
V3.0 MR1 设备安装手册**

FORTINET™

www.fortinet.com

V3.0 MR1 FortiGate-60系列以及FortiGate-100 A 设备安装手册

2006年4月10日

01- 30001-0266-20060410

© Copyright 2006 美国飞塔有限公司版权所有。

本手册中所包含的任何文字、例子、图表和插图，未经美国飞塔有限公司的许可，不得因任何用途以电子、机械、人工、光学或其它任何手段翻印、传播或发布。

注册商标

动态威胁防御系统（DTPS），APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate, FortiGate 统一威胁管理系统, FortiGuard, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiManager, Fortinet, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP 和 FortiWiFi 均是飞塔有限公司的注册商标（包括在美国和在其他国家的飞塔有限公司）。

本手册中提及的公司和产品由他们各自的所有者拥有其商标或注册商标。

服从规范

FCC Class A Part 15 CSA/CUS



注意：如果您安装的电池型号有误，可能会导致爆炸。请根据使用说明中的规定处理废旧电池。

目录

简介.....	6
Fortinet 产品家族.....	6
FortiGuard服务订制.....	6
FortiClient.....	7
FortiMail.....	7
FortiAnalyzer.....	7
FortiReporter.....	7
FortiBridge.....	7
FortiManager.....	7
关于FortiGate设备.....	8
FortiGate-60/60M/ADSL.....	8
FortiWiFi-60.....	8
FortiGate-100A.....	8
关于本手册.....	8
该手册中的注释.....	9
排版说明.....	9
FortiGate技术文档.....	10
Fortinet 知识库.....	11
Fortinet 技术文档的建议与意见.....	11
客服与技术支持.....	11
FortiGate设备安装.....	12
设备包装.....	12
FortiGate-60/60M/ADSL.....	12
FortiWiFi-60.....	13
FortiGate-100A.....	13
启动FortiGate设备.....	14
启动FortiGate设备.....	14
连接FortiGate设备.....	15
基于web的管理器.....	15
命令行接口（CLI）.....	15
连接到基于web的管理器.....	16
连接到CLI（命令行接口）.....	18
使用出厂默认设置快速启动FortiGate设备.....	19
出厂默认设置.....	21
出厂默认的DHCP服务器配置.....	21
出厂默认的NAT/ 路由模式的网络配置.....	21
出厂默认的透明模式的网络配置.....	23
出厂默认防火墙设置.....	23
出厂默认的防火墙保护内容设置.....	23
恢复出厂默认设置.....	24

使用基于web的管理器恢复默认的出厂设置	24
使用CLI恢复默认的出厂设置	25
在网络中配置FortiGate设备	26
规划FortiGate配置	26
NAT/路由模式安装	26
设置公共FortiGate接口对Ping命令请求不作出响应	29
NAT/路由模式安装	30
配置FortiGate设备的NAT/路由模式准备	30
配置使用DHCP或PPPoE	31
使用基于web的管理器	31
使用命令行接口 (CLI)	33
将FortiGate设备连接到网络中	35
配置网络	36
透明模式安装	36
配置透明模式的准备	37
使用基于web的管理器	37
使用命令行接口 (CLI)	38
将FortiGate设备连接到网络	39
下一步	40
设置系统日期与时间	40
FortiGate设备注册	40
更新病毒防护与IPS特征	41
配置modem接口	44
设置modem接口模式	44
冗余模式配置	44
单机模式配置	45
对FortiGate-60 与FortiWiFi-60 设备配置modem	47
对Modem连接添加防火墙策略	50
配置ADSL接口	51
使用web管理器配置ADSL接口	51
配置基本ADSL设置	51
配置ADSL接口使用DHCP	52
配置接口使用PPPoE或PPPoA	52
使用CLI配置ADSL接口	54
对ADSL连接添加防火墙策略	58
无线网络的使用	59
建立无线网络	59
AP定位	59
无线电频率对接	60
使用多个访问点	60

无线安全	61
无线等效协议 (WEP)	61
WPA	61
其它的无线网络安全方式	62
MAC地址过滤	62
服务设置标识符 (SSID)	62
FortiWiFi-60 设备操作模式	62
访问点 (AP) 模式	62
用户模式	63
在网络中配置FortiWiFi-60 设备作为访问点 (AP)	64
配置DHCP设置	64
设置安全选项	64
配置防火墙策略	65
FortiGate固件	66
升级为新的固件版本	66
恢复为旧的固件版本	67
使用CLI在系统重启过程中安装固件镜像	70
FortiUSB 密钥	72
安装固件之前测试新的固件镜像	74
安装并使用备份固件镜像	76
安装备份固件镜像	76

简介

欢迎选购Fortinet产品构筑实时网络防护。

FortiGate™ 统一威胁管理系统增强了网络的安全性，避免了网络资源的误用和滥用，帮助您更有效的使用通讯资源的同时不会降低网络的性能。FortiGate病毒防火墙获得了ICSA 防火墙认证，IP 安全认证和防病毒服务认证。

FortiGate统一威胁管理系统是致力于网络安全的，易于管理的安全设备。其功能齐备，包括：

- 应用层服务，例如病毒防护和内容过滤，
- 网络层服务，例如防火墙、入侵检测、VPN以及流量控制等。

FortiGate统一威胁管理系统采用了先进的行为加速（Accelerated Behavior）和内容分析系统技术（ABACASTM），具有芯片设计、网络通信、安全防御及内容分析等方面诸多技术优势。独特的基于ASIC上的网络安全构架能实时进行网络内容和状态分析，并及时启动部署在网络边界的防护关键应用程序，随时对您的网络进行最有效的安全保护。

Fortinet 产品家族

Fortinet 的产品家族涵盖了完备的网络安全解决方案包括邮件，日志，报告，网络管理，安全性管理以及FortiGate 统一安全性威胁管理系统的既有软件也有硬件设备的产品。

更多Fortinet产品信息，详见 www.fortinet.com/products .

FortiGuard服务订制

FortiGuard 服务定制是全球Fortinet安全专家团队建立,更新并管理的安全服务。Fortinet安全专家们确保最新的攻击在对您的资源损害或感染终端用户使用设备之前就能够被检测到并阻止。FortiGuard服务均以最新的安全技术构建，以最低的运行成本考虑设计。

FortiGuard 服务订制包括：

- FortiGuard 反病毒服务
- FortiGuard 入侵防护（IPS）服务
- FortiGuard 网页过滤服务
- FortiGuard 垃圾邮件过滤服务
- FortiGuard Premier伙伴服务

并可获得在线病毒扫描与病毒信息查看服务。

FortiClient

FortiClient™ 主机安全软件为使用微软操作系统的桌面与便携电脑用户提供了安全的网络环境。FortiClient的功能包括：

- 建立与远程网络的VPN连接
- 病毒实时防护
- 防止修改Windows注册表
- 病毒扫描

FortiClient还提供了无人值守的安装模式，管理员能够有效的将预先配置的FortiClient分配到几个用户的计算机。

FortiMail

FortiMail™安全信息平台针对邮件流量提供了强大且灵活的启发式扫描与报告功能。FortiMail单元在检测与屏蔽恶意附件例如DCC（Distributed Checksum Clearinghouse）与Bayesian扫描方面具有可靠的高性能。在Fortinet卓越的FortiOS与FortiASIC技术的支持下，FortiMail反病毒技术深入扩展到全部的内容检测功能，能够检测到最新的邮件威胁。

FortiAnalyzer

FortiAnalyzer™ 为网络管理员提供了有关网络防护与安全性的信息，避免网络受到攻击与漏洞威胁。FortiAnalyzer具有以下功能：

- 从FortiGate与syslog设备收集并存储日志。
- 创建日志用于收集日志数据。
- 扫描与报告漏洞。
- 存储FortiGate设备隔离的文件。

FortiAnalyzer也可以配置作为网络分析器用来在使用了防火网的网络区域捕捉实时的网络流量。您也可以将FortiAnalyzer用作存储设备，用户可以访问并共享存储在FortiAnalyzer硬盘的报告与日志。

FortiReporter

FortiReporter™安全性分析软件生成简洁明的报告并可以从任何的FortiGate设备收集日志。FortiReporter可以暴露网络滥用情况，管理带宽，监控网络使用情况，并确保员工能够较好的使用公司的网络。FortiReporter还允许IT管理员能够识别并对攻击作出响应，包括在安全威胁发生之前先发性的确定保护网络安全的方法。

FortiBridge

FortiBridge™产品是设计应用于当停电或是FortiGate系统故障时，提供给企业用户持续的网络流量。FortiBridge绕过FortiGate设备，确保网络能够继续进行流量处理。FortiBridge产品使用简单，部署方便；您可以设置在电源或者FortiGate系统故障发生的时FortiBridge设备所应采取的操作。

FortiManager

FortiManager™系统设计用来满足负责在许多分散的FortiGate安装区域建立与维护安全策略的大型企业（包括管理安全服务的提供商）的

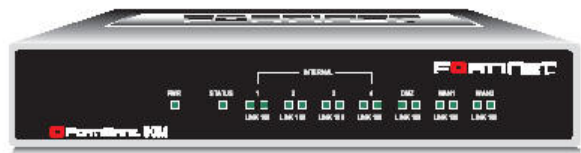
需要。拥有该系统，您可以配置多个FortiGate并监控其状态。您还能够查看FortiGate设备的实时与历史日志，包括管理FortiGate更新的固件镜像。FortiManager 系统注重操作的简便性包括与其他第三方系统简易的整合。

关于FortiGate设备

FortiGate-60系列以及FortiGate-100A设备是应用于小型企业级别的（包括远程工作用户），集基于网络的反病毒、内容过滤、防火墙、VPN以及基于网络的入侵检测与防护为一体的FortiGate系统模块。FortiGate-60系列以及FortiGate-100A设备支持高可靠性（HA）性能。

FortiGate-60/60M/ADSL

FortiGate-60设备设计应用于远程工作用户以及零售店操作用户。FortiGate-60设备中含有一个外部调制解调器接口，可以作为备用



接口或作为与单机连接接入到互联网，该设备中还拥有一个内部调制解调器也能够作为一个到互联网的备份或单机连接。FortiGate-60ADSL中包括一个内部ADSL调制解调器。

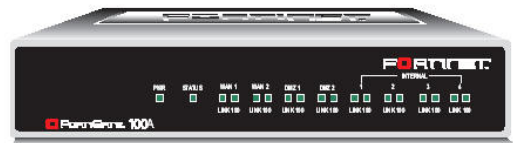
FortiWiFi-60

FortiWiFi-60设备能够提供一个安全，无线的LAN解决方案。FortiWiFi病毒防火墙功能集移动性与灵活性，并且能够升级到将来应用的无线通信技术。FortiWiFi-60可以作为无线与有线网络的连接点或一个单独的无线网络的中心点。



FortiGate-100A

FortiGate-100A是应用于小型办公、soho以及一些公司机构的分支部门的，易于管理员部署的网络防护设备。



FortiGate -100A设备支持一些高级的功能例如802.1Q VLAN、虚拟域以及RIP与OSPF路由协议。

关于本手册

该文档就如何安装FortiGate设备，在网络中配置设备，以及如何安装

与升级固件进行了说明。

该手册包含以下章节：

- [安装FortiGate设备](#) — 安装并启动FortiGate设备。
- [出厂默认设置](#) — FortiGate设备出厂默认设置信息。
- [在网络中配置FortiGate设备](#) — FortiGate设备的操作模式说明以及如何将FortiGate设备集成到网络中。
- [配置Modem接口](#) — 如何配置以及使用FortiGate-60系列设备的Modem。
- [使用无线网络](#) — 无线网络的使用注意事项以及使用步骤，使无线网络的使用更为高效。
- [FortiGate固件](#) — 描述了如何安装，升级，恢复与测试FortiGate设备的固件。



注意：本手册中所述的信息涉及到五个设备FortiGate-60/60M、FortiWiFi-60以及FortiGate-100A。其中大部分的内容适用于所有的设备，针对对具体某个模块所做的说明与描述内容，将使用以下的图标作为描述提示。



该手册中的注释

以下是该手册中的注释：

- 在所举的例子中，私人IP地址既可以用做私人也可以是公共IP地址。
- 注意与警告标识中的提示较为重要的信息。



注意：突出另外其它的有用信息。



警告：对可能造成意外的不良的结果包括数据丢失或者设备损害等命令或程序发出警告提示。

排版说明

以下是该安装手册中使用的排版说明：

排版说明	举例
键盘输入	在网关名称字段，键入远程VPN或用户（例如，Central_office_1）
命令举例	Config sys global Set ips-open enable end
CLI命令句法模式	Config firewall policy edit id_integer set http_retry_count <retry_interer>

	set natip <address_ipv4mask> end
文档名称	<i>FortiGate 管理员使用手册</i>
菜单命令	进入 VPN>IPSEC>阶段1并点击“新建”。
程序输出	Welcome !
变量	<address_ipv4>

FortiGate技术文档

您可以从Fortinet技术文档网站<http://kc.forticare.com>，获得最新发布的Fortinet技术文档。

公开以下Fortinet产品技术手册：

• *FortiGate 快速启动指南*

提供关于连接与安装Fortinet设备的信息。

• *FortiGate 设备安装手册*

提供有关如何安装FortiGate设备的信息。包括硬件信息,默认配置信息,安装操作,连接操作以及基本的配置操作。请查看产品型号选择不同的安装手册。

• *FortiGate 管理员使用手册*

有关如何配置FortiGate设备的基本信息,包括如何定义FortiGate病毒防护与防火墙策略;如何应用入侵保护,病毒防护,网页内容过滤以及垃圾邮件过滤服务与配置VPN。

• *FortiGate 在线帮助*

在线帮助是对FortiGate管理员手册的HTML格式上下文有关的检索与查询。您可以通过基于web的管理其访问在线帮助。

• *FortiGate CLI 参考手册*

有关如何使用FortiGate CLI (命令行接口) 以及所以FortiGateCLI命令的参考。

• *日志信息参考手册*

访问Fortinet公司网站的Fortinet知识库板块, FortiGate 日志信息参考对FortiGate日志信息的结构与FortiGate设备所生成的日志信息有关内容做了描述。

• *FortiGate HA 用户使用指南*

深入介绍了FortiGate 高可用性的性能与FortiGate群集协议的信息。

• *FortiGate IPS 用户使用指南*

对如何配置FortiGate设备的入侵检测功能以及IPS是如何处理普通的攻击做出了描述。

• *FortiGate IPSec VPN 用户指南*

对使用基于web的管理器如何配置IPSec VPN进行了逐步详细的说明。

• *FortiGateSSL VPN 用户使用指南*

对FortiGate IPSec VPN与FortiGate SSL VPN 技术进行比较,并对通过基于web的管理器,远程用户怎样配置只适用于网络模式与通道模式SSL VPN访问做了描述。

• *FortiGate PPTP VPN 用户使用指南*

使用基于web的管理器如何配置PPTP VPN。

- *FortiGate Certificate Management User Guide 证书管理用户指南*
管理电子证书的程序包括生成电子证书的请求，安装签发的证书，引入CA根权威证书与证书撤销名单，以及备份与存储安装的证书信息与私人密钥。

- *FortiGate VLAN and VDOM 用户使用指南*
在NAT/路由与透明模式下如何配置VLAN与VDOM。

Fortinet 知识库

其它有关 Fortinet 技术手册信息都可以从 Fortinet 公司网站（www.fortinet.com）中的知识库板块获得。知识库涵盖涉及fortinet产品故障排除与解释说明性的文章，FAQ，技术说明等。

Fortinet 技术文档的建议与意见

如果您在本文档或任何Fortinet 技术文档中发现了错误或疏漏之处，欢迎您将有关信息发送到 techdoc@fortinet.com 。

客服与技术支持

Fortinet 技术支持将确保您的Fortinet系统在您的网络中能够快速启动，轻松配置并能够可靠运行。

敬请访问Fortinet技术支持网站<http://support.fortinet.com> 获知更多Fortinet所提供的技术支持服务。

FortiGate设备安装

本章节就如何安装以及在网络中配置FortiGate设备进行了详细说明。

具体包括：

- [设备包装](#)
- [空气流通](#)
- [机械性负荷](#)
- [启动FortiGate设备](#)
- [连接FortiGate设备](#)

设备包装

请检查FortiGate设备包装盒所有部件。

FortiGate-60/60M/ADSL

FortiGate-60/60M/ADSL设备包装盒中部件：

- FortiGate防火墙设备
- 一根橙色以太网交叉线缆（Fortinet 部件号：CC300248）
- 一根灰色以太网普通线缆（Fortinet 部件号：CC300249）
- 一根RJ-45到DB-9串连线缆（Fortinet 部件号：CC300247）
- 一根RJ-11电话线（FortiGate -60M专用）
- 一根电源线以及一个AC适配器
- FortiGate-60快速启动指南册页、FortiGate-60M设备快速启动指南册页或FortiGate-60ADSL设备快速启动指南册页
- Fortinet技术手册CD一张

图1：FortiGate-60/60M设备部件

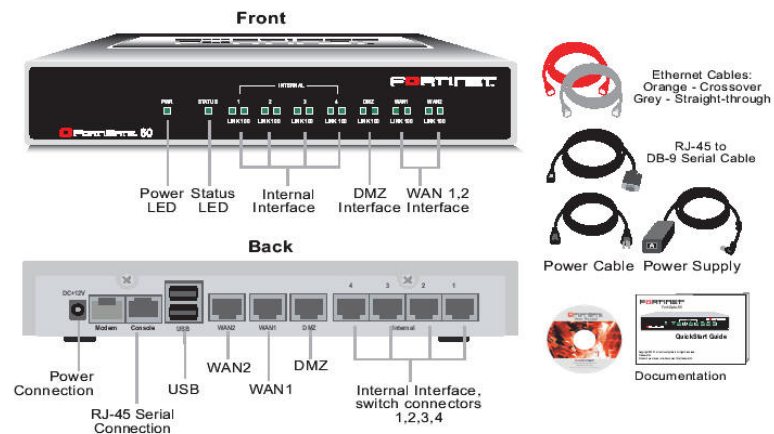


表1：技术参数

尺寸	8.63×6.13×1.38英尺（21.9×15.6×3.5厘米）
重量	1.5磅（0.68千克）
工作需求	DC输入电压：100至240VAC DC输入电流：1.6A

工作环境	工作温度：32至104华氏度（0至40摄氏度）
	放置温度：-13至158华氏度（-25至70摄氏度）
	湿度：5至95%（非冷凝）

FortiWiFi-60

FortiWiFi-60设备包装盒中部件：

- FortiWiFi-60防火墙设备
- 一根橙色以太网交叉线缆（Fortinet 部件号：CC300248）
- 一根灰色以太网普通线缆（Fortinet 部件号：CC300249）
- 一根RJ-45到DB-9串连线缆（Fortinet 部件号：CC300247）
- 一根电源线以及一个AC适配器
- FortiWiFi-60快速启动指南册页
- Fortinet技术手册CD一张

图2：FortiWiFi-60设备部件

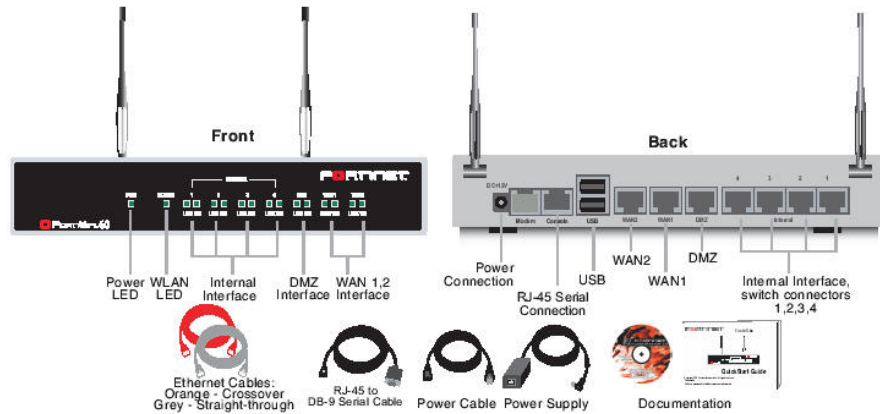


表2：技术参数

尺寸	8.63×6.13×1.38英尺（21.9×15.6×3.5厘米）
重量	1.5磅（0.68千克）
工作需求	DC输入电压：12V DC输入电流：3A
无线连接	工作温度：32至104华氏度（0至40摄氏度） 天线型号：外部固定双天线 天线范围：802.11 b/g: 2.4GHz 天线增益：5dBi
工作环境	操作温度：32到104 华氏度（0到40摄氏度） 放置温度：-13至158华氏度（-25至70摄氏度） 湿度：5至95%（非冷凝）

FortiGate-100A

FortiGate-100A设备包装盒中部件：

- FortiGate-100A防火墙设备
- 一根橙色以太网交叉线缆（Fortinet 部件号：CC300248）

- 一根灰色以太网普通线缆（Fortinet 部件号：CC300249）
- 一根RJ-45到DB-9串连线缆（Fortinet 部件号：CC300302）
- 一根电源线以及一个AC适配器
- FortiGate-100A快速启动指南册页
- Fortinet技术手册CD一张

图3: FortiGate-100A设备部件

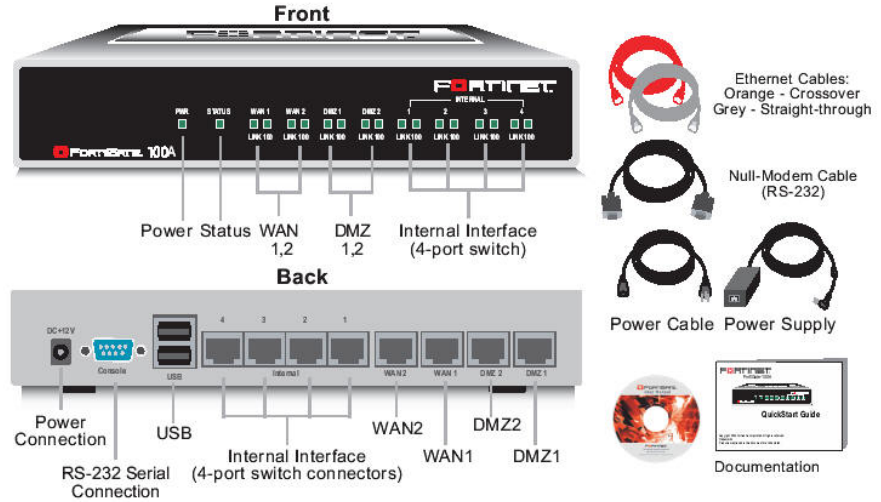


表3: 技术参数

尺寸	10.25×6.13×17.5英尺（26×15.6×34.5厘米）
重量	1.5磅（0.68千克）
工作要求	DC输入电压：12V DC输入电流：5A
工作环境	工作温度：32至104华氏度（0至40摄氏度） 放置温度：-13至158华氏度（-25至70摄氏度） 湿度：5至95%（非冷凝）

安装

FortiGate设备可以安装在任何稳固且水平的表面。请保持设备安装相隔至少1.5英寸（3.75厘米）的距离，便于通风与冷却。

启动FortiGate设备

FortiGate设备中没有ON/OFF开关。

启动FortiGate设备

1. 将AC适配器与设备背后的电源接口连接。
2. 将AC适配器与电源线连接。
3. 将电源线连接到电源插座。

FortiGate设备启动，电源与LED状态显示灯亮起。FortiGate设备启动过程中LED状态指示灯闪烁并在设备启动后保持亮着状态。

表4: LED显示

LED	状态	描述
Power	绿色	FortiGate设备启动。
	熄灭	FortiGate设备断电。
状态	绿色	连接线使用正确，连接的设备已启动。
	绿色闪烁	FortiGate设备正在启动。
	熄灭	设备已断电。
链接 (内部(Internal), DMZ1 DMZ2 WAN1 WAN2)	绿色	连接线使用正确，连接的设备已启动。
	绿色闪烁	此接口有网络活动。
	熄灭	没有建立链接。
DMZ1 DMZ2 WAN1 WAN2	绿色	接口达到速率为100Mbps的连接。

关闭FortiGate设备

请在闭合电源开关之前，关掉FortiGate操作系统，以免造成硬件损伤。

关闭FortiGate设备

1. 访问基于web的管理器，进入系统> 状态> 系统状态，选择关闭系统，然后点击“确认”关闭系统；或者在命令行接口（CLI）中，输入
`execute shutdown`
2. 关闭电源开关。

连接FortiGate设备

有二种方法连接并配置基本FortiGate设置：

- 基于web的管理器
- 命令行接口（CLI）

基于web的管理器

您可以通过任何运行微软Internet Explorer 6.0或其他最近版本的浏览器的计算机，使用HTTP或一个安全的HTTPS连接配置并管理FortiGate设备。基于web的管理器支持多种语言。

您可以使用基于web管理器配置大多数FortiGate设置并监控FortiGate设备的状态。

命令行接口（CLI）

您可以通过连接到一个管理计算机串行端口进入FortiGate串行Console连接器，访问FortiGate命令行接口。您也可以从任何连接FortiGate设备的网络包括内部网，使用Telnet或一个安全的SSH连接接入到CLI。

连接到基于web的管理器

根据以下操作步骤建立与基于web管理器的初次链接。在基于web的管理器中所做的配置修改，无需重新设置防火墙或中断运行便可生效。

连接到基于web的管理器，您需要：

- 一台能够连接以太网的计算机
- 微软6.0版本的浏览器或以上的版本，或任何现行的web浏览器
- 一根交叉的以太网网线或一个以太网网络集线器（hub）与两根以太网网线。



注意：启动IE之前（或其他现行版本的网页浏览器），ping FortiGate设备，检测计算机与FortiGate设备之间是否连接正常。

连接到基于web的管理器

1. 设置计算机与以太网连接的IP地址为静态IP地址192.168.1.2，掩码为255.255.255.0。



您可以配置管理计算机使用DHCP自动获取IP地址。FortiGate DHCP服务器将对管理计算机分配范围为192.168.1.1到192.168.1.254之间的IP地址。

2. 使用交叉线或以太网集线器（hub）与线缆将FortiGate设备的内部接口与您的光纤网络接口连接。
3. 启动IE浏览器，浏览地址为 <https://192.168.1.99> 的页面（请注意是https://）。

为了支持安全的HTTPS识别程序，FortiGate设备引入一个自签订的安全认证，每当远程用户对FortiGate设备发起一个HTTPS连接时，该安全认证便会弹出。当您进行连接时，FortiGate设备在浏览器中显示两个安全警告。

第一个警告信息提示您接受并安装FortiGate设备的自签安全证书。如您不接收认证，FortiGate设备将拒绝连接。如您接收认证，将转入FortiGate登录页面。输入用户名与密码验证信息登录。如您选择永久接受认证，警告信息不再弹出。

在FortiGate登录页面显示之前，第二个警告信息告知您FortiGate认证与原始请求的区别。该信息弹出是因为FortiGate设备试图进行再次连接。是一条报告性信息。点击“OK”键确认，继续登录页。

图4: FortiGate登录页面



4. 输入名称字段输入admin登录。

系统操作面板

登录到基于web的管理器后，页面显示系统操作面板。面板显示所有的系统状态信息。

图5: FortiGate-60M系统面板



面板中包括以下信息:

- 端口状态—面板中显示有FortiGate设备的正面镜像图。包括FortiAnalyzer连接状态—X表示没有连接，当检测标志中没有标注X时，说明存在连接。滑动鼠标到每个端口，可以查看端口信息，如IP地址与掩码，速率，以及接收或发送的数据包信息。当端口使用中时，其状态显示呈绿色。
- 系统信息—操作系统信息的显示包括设备串行数量与固件版本。在该区域，可以进行固件升级，设置系统时间或更改操作模式。

- 系统资源—显示系统资源使用情况。
- 许可证信息—显示FortiGate设备中当前的病毒防护与安全性升级的情况。
- 报警信息Console—显示最近FortiGate设备发出的警告日志信息。
- 统计表—提供FortiGate设备的实时流量与攻击信息。

连接到CLI（命令行接口）

将管理计算机的串口与FortiGate设备的控制台连接器连接并可以访问FortiGate设备命令行接口。您也可以在任何网络（包括互联网）中使用Telnet或一个安全的SSH连接访问FortiGate设备也可以连接到CLI。

CLI（命令行接口）支持与基于web的管理器相同的配置与功能。另外，您还可以使用CLI配置一些web管理器不能配置的更高级的选项。本手册中包含一些基本的以及某些高级的CLI命令信息。有关连接到FortiGate设备使用CLI的详细信息，参见*FortiGate设备CLI使用参考手册*。

连接到CLI

除了使用基于web的管理器，您也可以使用CLI安装与配置FortiGate设备。无需重新设置防火墙或中断设备运行，CLI所进行的配置更改便可以生效。

连接到CLI，您需要：

- 一台有通信端口的计算机
- FortiGate设备包装中带有的RJ-45到DB-9的串口线缆。
- 终端模拟软件，如Microsoft Windows的HyperTerminal。

连接到CLI

1. 使用RJ-45到DB-9的串口线将您计算机的通信端口与FortiGate console端口连接。
2. 启动HyperTerminal，键入连接的名称，点击OK确认。
3. 配置将HyperTerminal与您计算机的通信端口直接连接并点击OK键确认。
4. 输入以下端口设置并点击OK确认。
5. 按回车连接到FortiGate CLI。

```
Bit per second 9600
Bata bits      8
Partity       None
Stop bits     1
Flow control   None
```

5. 按Enter键，建立与FortiGate CLI的连接。
弹出登录页。
6. 键入admin的名称并按Enter键两次
显示如下提示信息；
Welcome！

键入？列出可用的命令。有关如何使用CLI（命令行接口）的详细信息，参见 *FortiGate 设备CLI使用参考手册*。

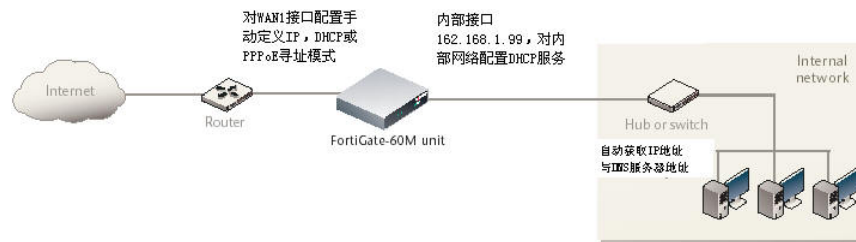
使用出厂默认设置快速启动FortiGate设备



使用基于web的管理器与出厂默认的FortiGate设备配置，您可以快速在soho情况下配置启用FortiGate-60系列设备。您所要做的只是配置您网络中的计算机使用DHCP自动获取IP地址以及DNS服务器IP地址，并访问基于web的管理器对WAN1接口配置所需的设置。如需要，您也可以配置FortiGate DNS服务器并添加默认的路由。

FortiGate内部接口可以配置作为一个DHCP服务器在内部网络中自动对计算机设备（最多可达100台）自动分配地址范围为192.168.1.110到192.168.1.210之间的IP地址。

图6：适用默认设置快速配置设备



FortiGate DHCP服务器也可以对内部网络中的每台计算机分配DNS服务器IP地址为192.168.1.99。那么，FortiGate设备内部接口将作为内部网络中的一个DNS服务器。使用DNS转发，FortiGate设备将从内部网络获取的DNS请求转发到DNS服务器IP地址添加在FortiGate设备配置中并将查询结果返回到内部网络中。

有关DHCP服务器的详细信息，参见“出厂默认DHCP服务器配置”。

以下操作是有关如何配置您的内部网络与FortiGate设备使用FortiGate设备默认的设置：

1. 将FortiGate设备连接在内部网络与互联网之间，并启动设备。
2. 设置网络计算机的TCP/IP属性使用DHCP自动获取IP地址与DNS服务器IP地址。
3. 使用管理计算机，浏览：<https://192.168.1.99>。
登录到FortiGate设备基于web管理器页面。
4. 进入系统>网络>接口，点击外部接口的“编辑”图标。
5. 选择以下一种寻址模式：
 - 手动模式：输入静态IP地址与掩码，点击OK并进入步骤6。
 - DHCP模式：点击选择DHCP，从ISP获取IP地址，并进入步骤9。

- PPPoE模式：点击选择PPPoE，从ISP获取IP地址，并进入步骤9。
6. 进入系统>网络>选项。
 7. 选择以下一种DNS设置：
 - 自动获取DNS服务器地址：设置从ISP自动获取DNS地址，点击“应用”。
 - 使用以下DNS服务器地址：输入ISP给的DNS地址并点击“OK”。
 8. 进入路由>静态，编辑路由#1并将网关更改为默认的网关IP地址并点击OK。
 9. 如果ISP支持服务器或代理内部DNS选项，点击获取默认的网关并点击OK确认后继续执行“下一步”。
- 如果您没有设置这些选项，进入步骤6。

出厂默认设置

FortiGate设备有出厂默认设置。该默认设置允许您连接到FortiGate设备并能够使用FortiGate基于web的管理器在网络中配置FortiGate设备。在网络中配置FortiGate，您需要添加管理员密码，更改网络接口IP地址与DNS服务器的IP地址，如有必要，可以配置基本的路由。

如果您打算以透明模式运行FortiGate设备，可以从出厂默认配置中切换到透明模式，并根据您的网络结构与情况配置透明模式下的FortiGate设备。

完成网络配置后，您还可以进行其他的配置操作，如设置系统时间，配置病毒及攻击的定义更新，注册FortiGate设备等。

出厂时默认的防火墙配置包括单一网络地址转换（NAT）策略，该策略允许您内部网络的用户连接到外部网络，同时阻止外部网络中的用户连接到内部网络。您可以添加更多其它的策略，对通过FortiGate设备的流量进行更多的控制。

出厂时默认的内容配置文件可以用来快速地在防火墙策略中设置不同级别的防病毒保护、网页内容过滤、垃圾邮件过滤，以便控制网络通讯。

本章包括以下内容：

- [出厂默认的DHCP服务器配置](#)
- [出厂默认的NAT/路由模式的网络配置](#)
- [出厂默认的透明模式的网络设置](#)
- [出厂默认的防火墙配置](#)
- [恢复默认配置](#)

出厂默认的DHCP服务器配置

使用出厂默认的DHCP服务器设置，您可以快速配置内部网络以及FortiGate设备。参见“使用出厂默认设置快速安装”。

表5：出厂默认DHCP服务器配置

名称	Internal_dhcp_server
接口	internal
默认网关	192.168.1.99
IP范围	192.168.1.110-192.168.1.210
网络掩码	255.255.255.0
租期	7天
DNS服务器1	192.168.1.99

出厂默认的NAT/ 路由模式的网络配置

FortiGate设备首次启动时，它运行于NAT/路由模式，表6所列是该工作模式下的基本网络配置。该配置允许您连接到FortiGate设备的基于web的管理器，并建立FortiGate设备连接到网络所需的配置。表6中，HTTPS管理访问表示您可以通过该接口的HTTPS协议连接到基于web的管理器。Ping管理访问表示该接口对ping这一命令可以做出响应。

表6：出厂默认的NAT/路由模式的网络配置

管理员账号	用户名： 密码：	Admin (无)
内部接口(internal接口)	IP： 子网掩码： 管理访问：	192.168.1.99 255.255.255.0 Ping HTTP, HTTPS
WAN1接口	IP： 子网掩码： 管理访问：	192.168.100.99 255.255.255.0 Ping
WAN2接口	IP： 子网掩码： 管理访问：	192.168.100.99 255.255.255.0. Ping
DMZ接口 DMZ1 (FortiGate-100A)	IP： 子网掩码： 管理访问：	10.10.10.1 255.255.255.0 HTTP, Ping
DMZ2接口 (FortiGate-100A)	IP： 子网掩码： 管理访问：	10.10.10.1 255.255.255.0 HTTP, Ping
Modem接口	IP： 子网掩码： 管理访问：	0.0.0.0. 0.0.0.0
ADSL Modem接口	IP： 子网掩码： 管理访问：	0.0.0.0. 0.0.0.0
WLAN	IP： 子网掩码： 管理访问：	10.10.80.1 255.255.255.0 Ping
网络设置	默认网关(默认路由)	192.168.100.1
	接口连接到外部网络 (默认的路由)	external
	默认路由 默认的路由由一个默认的网关与连接到外部网络 (通常是互联网)接口的名称组成。 默认的网关将所有非本地的通讯集中到该接口与外部网络。	
	一级DNS:	65.39.139.53
	二级DNS:	65.39.139.63

出厂默认的透明模式的网络配置

表7是透明模式下，FortiGate设备默认的网络配置。

表7：出厂默认的透明模式网络配置

管理员帐户	用户名： 密码：	Admin (无)
管理IP	IP： 子网掩码：	0.0.0.0. 0.0.0.0.
DNS	一级DNS服务器 二级DNS服务器	65.39.139.53 65.39.139.63
管理访问	Internal DMZ DMZ1 DMZ2 WAN1 WAN2 WLAN	HTTPS, ping HTTPS, ping HTTPS, Ping Ping Ping Ping Ping

出厂默认防火墙设置

FortiGate防火墙策略是有关FortiGate设备对所有通讯流量的控制。除非添加了防火墙策略，否则没有流量通讯能够被FortiGate设备接收或经过FortiGate设备。您可以添加防火墙策略允许网络流量通过FortiGate设备。有关添加防火墙策略，参见*FortiGate 设备管理员使用手册*。

以下是默认的防火墙配置中的策略配置设置：

表8：出厂默认防火墙配置

配置设置	名称	描述
防火墙地址	所有	防火墙地址与任何数据包的源目标地址匹配。
预先定义的服务	50多条预先定义的服务	从50多条预先定义的服务中选择控制通过FortiGate流量的服务。
循环任务时间表	总是	任何时间，循环任务计划都是有效的。
防火墙保护	Stict, Scan, Web, Unfiltered	控制防火墙设备是怎样启用病毒扫描，网页内容过滤，垃圾邮件过滤与IPS。

NAT/路由模式与透明模式下防火墙配置的出厂默认设置是相同的。

出厂默认的防火墙保护内容设置

使用防火墙保护设置对防火墙策略控制的流量进行不同的防护设置。

- 给HTTP, FTP, IMAP, POP3与SMTP防火墙策略配置防病毒保护。
- 给HTTP防火墙策略配置网页过滤。
- 给HTTP策略配置网页类别过滤。
- 给IMAP, POP3与SMTP防火墙策略配置垃圾邮件过滤。
- 对所有的服务启动入侵防护系统 (IPS)。
- 对HTTP, FTP, IMAP, POP3与SMTP防火墙策略启动内容日志

通过内容保护列表, 您可以构建适用与不同类型防火墙策略的保护配置。并允许您针对不同防火墙策略定制不同类型与级别的防护。

例如, 内部与外部地址之间的流量可能需要比较严格的防护, 而内部地址之间的流量可能需要中等一般的防护。您可以针对不同的流量使用相同或不同的保护设置配置防火墙策略。

NAT/路由模式与透明模式的防火墙策略也可以添加保护设置。

FortiGate设备可以预先配置四种保护设置。

Strict (严格型) 适用于对HTTP, FTP, IMAP, POP3与SMTP流量应用最大限度的保护。一般情况下, 不必使用Strict (严格型) 的保护设置, 发现病毒攻击, 需要扫描检测时, 可以启用Strict (严格型) 保护。

Scan (扫描型) 针对HTTP, FTP, IMAP, POP3, 与SMTP内容流量采用病毒扫描与文件隔离。

Web (网页内容控制型) 针对HTTP内容流量采取病毒扫描与网页内容屏蔽。您可以在防火墙策略中添加该保护设置来控制HTTP流量。

Unfiltered (无过滤型) 如果对于内容流量不愿意采用内容防护, 您可以使用无过滤型保护。您可以在不需要内容保护的高可信与安全性较高的网络连接区域, 在防火墙的策略中添加该保护设置。

恢复出厂默认设置

如果您误更改了网络设置, 并无法恢复, 您可以先恢复到出厂默认设置然后重新启动。



警告: 该操作将删除您对FortiGate做的所有配置更改, 并将系统退回至原始配置包括重新设置接口地址。

使用基于web的管理器恢复默认的出厂设置

恢复默认的设置

- 1.进入系统>状态>系统操作。
- 2.点击“恢复为出厂默认设置”。
- 3.点击“确认”。

使用CLI恢复默认的出厂设置

键入如下命令恢复为出厂默认设置：

```
execute factoryreset
```

在网络中配置FortiGate设备

本章是FortiGate设备的操作模式说明。开始配置FortiGate设备之前，先要考虑怎样将FortiGate设备集成到网络中。针对不同的操作模式，NAT/路由模式或透明模式，进行对应的配置。

该章节包括以下内容：

- [规划FortiGate配置](#)
- [设置公共FortiGate接口对Ping命令请求不作出响应](#)
- [NAT/路由模式安装](#)
- [透明模式安装](#)
- [下一步](#)

规划FortiGate配置

配置FortiGate设备之前，先要考虑怎样把FortiGate设备集成在网络中。至于其它问题，如还需要决定FortiGate设备是否在网络中可见，需要配置哪些防火墙功能，与怎样控制接口间的流量。

您所选择的FortiGate设备的操作模式是配置的依据。FortiGate设备有两个模式，分别为：NAT/路由模式（出厂默认）与透明模式。

您也可以在出厂默认的操作模式设置即NAT/路由模式下，在网络中配置FortiGate设备。

NAT/路由模式安装

NA/路由模式下，FortiGate设备在网络中是可见的类似一个路由器，设备的所有接口在不同的子网中。在NA/路由模式下，以下接口是可用的。

表9：NAT/路由模式下接口

FortiGate设备	内部接口	外部接口	其他
FortiGate-60	内部接口(Internal 1, 2, 3, 4)	WAN1 WAN2	DMZ
FortiGate-60M	内部接口(Internal)	WAN1 WAN2	DMZ
FortiWiFi-60	内部接口(Internal)	WLAN	DMZ WAN1 WAN2
FortiGate-60ADSL	内部接口(Internal)	WAN1 WAN2	DMZ
FortiGate-100A	内部接口(Internal)	WAN1 WAN2	DMZ1 DMZ2

您可以添加防火墙策略控制NAT/路由模式下的FortiGate设备是否有通信流量通过。防火墙策略根据源地址、目标地址与每个数据包的服

务来控制数据流量。 NAT模式下， FortiGate设备发送数据包到目标网络之前， 先执行网络地址转换。 路由模式操作没有地址转换。

NAT/路由模式下的FortiGate设备的典型的应用是作为私网与公网之间的网关。 该配置中， 您可以建立NAT模式防火墙策略控制内部网、 私网与外部网， 公网（通常指互联网）之间的数据流量。


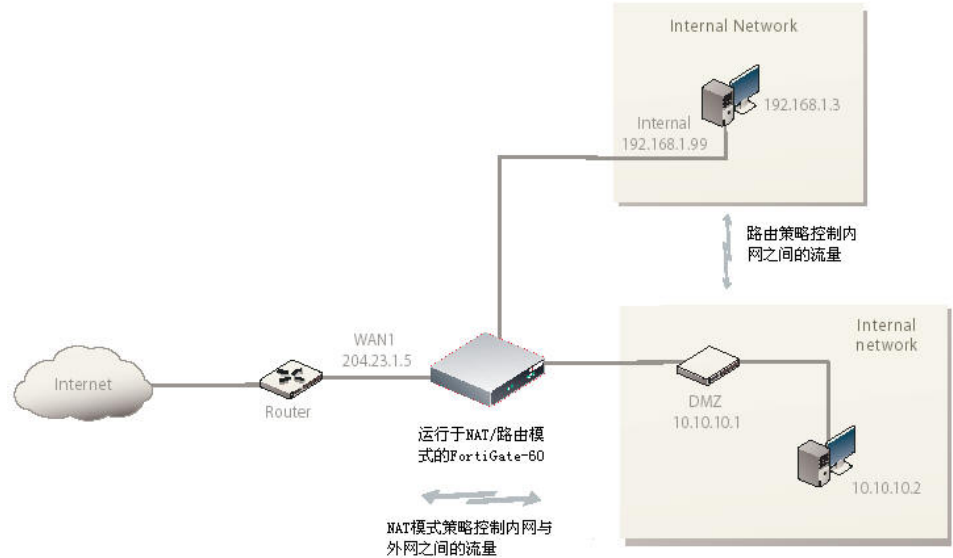
 **注意：**如果是多重内部网络连接， 例如内部网之外的DMZ网络、 私网； 您可以建立路由模式下的防火墙策略控制这些多重网络之间的流量。

图7： FortiGate-60设备NAT/路由模式下的网络配置举例



具有多个外部网络连接的NAT/路由模式

NAT/路由模式下， 您可以配置FortiGate设备具有多个冗余连接， 连接到外部网络（通常指互联网）。

例如， 您可以创建以下配置：

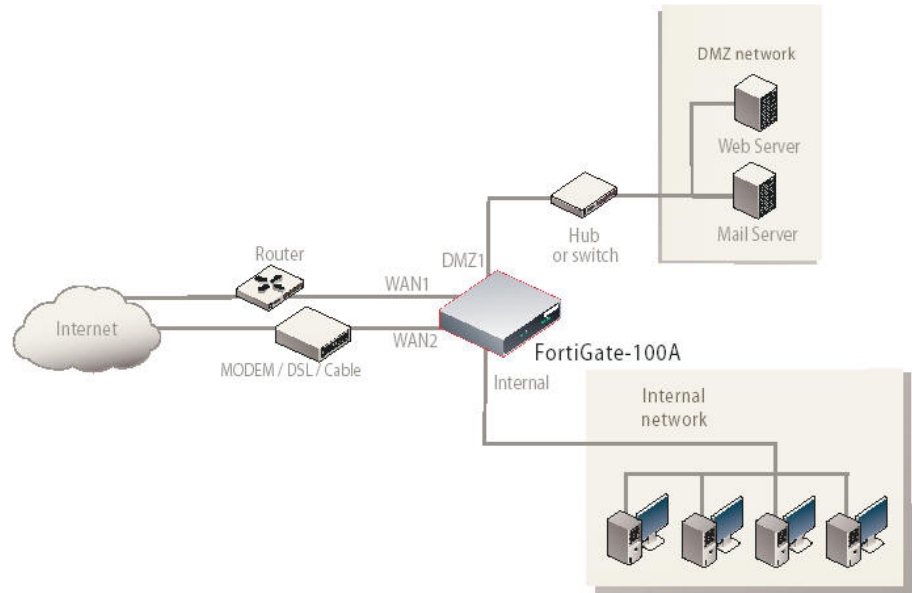
- WAN1是连接到外部网络（通常指互联网）的默认接口。
- Modem是FortiGate-60系列设备连接到外部网络的冗余接口。
- DMZ是FortiGate-100A设备中连接到外部网络的冗余接口。
- Internal是连接到内部网络的接口。

您必须配置路由支持冗余的网络连接。 如果到外部网络的连接失败， 路由可以从接口自动重新定向改连接。

另外， 安全策略配置类似于单项互联网连接下的NAT/路由模式配置。 您可以创建NAT模式防火墙策略控制内网、 死亡以及外网、 公共网络

(通常指互联网) 之间的流量。

图8: FortiGate-100A设备NAT/路由模式下多重internet (互联网) 连接配置举例



透明模式

透明模式下，FortiGate设备在网络中是透明的。类似于网络桥梁，所有的FortiGate接口都在同一个子网中。您只需配置一个管理IP地址便可以进行配置更改。管理IP地址也可用来配置病毒及攻击的定义更新。

透明模式下的FortiGate设备的典型应用位于当前的防火墙或路由器之后。FortiGate设备具有防火墙、IPsecVPN、病毒扫描、IPS、网页过滤与垃圾邮件过滤功能。

根据不同型号的FortiGate设备，您最多可以将4个网段连接到FortiGate设备上，以控制这些网段之间的数据流量。

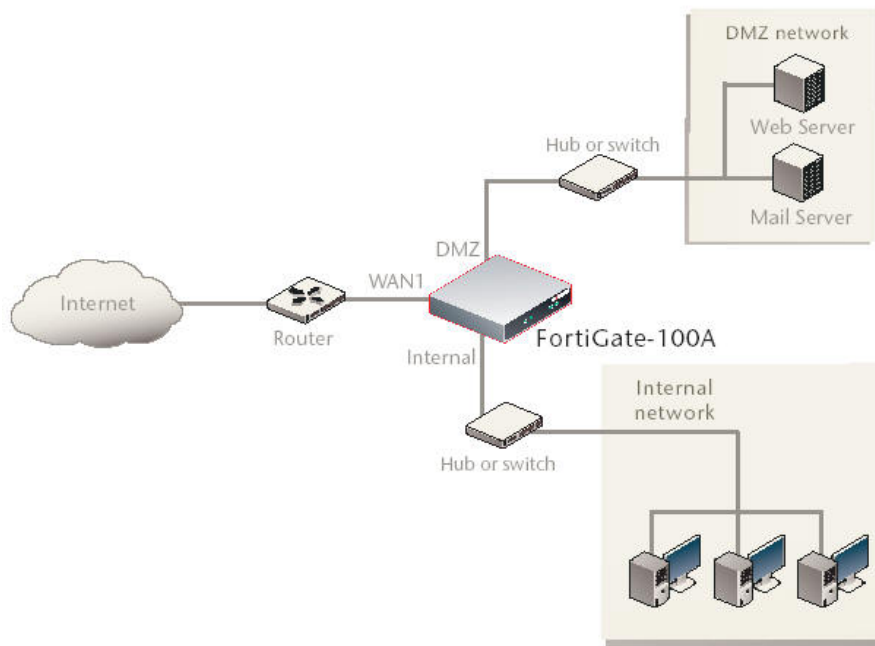
表10: 透明模式下的网络分段

FortiGate设备	内部接口	外部接口	其他
FortiGate-60	Internal (1, 2, 3, 4)	WAN1	WAN2 DMZ
FortiGate-60M	Internal	WAN1 WAN2	DMZ
FortiWiFi-60	Internal	WLAN	DMZ WAN1 WAN2
FortiGate-60ADSL	Internal	WAN1	WAN2 DMZ
FortiGate-100A	Internal	WAN1	WAN2

			DMZ1 DMZ2
--	--	--	--------------

 注意：透明模式下，FortiGate-60M中modem接口不可用。

图9：FortiGate-100A设备透明模式下的网络配置举例



设置公共FortiGate接口对Ping命令请求不作出响应

出厂默认的FortiGate设备允许默认的公共接口对ping请求作出响应。默认的工作接口也称为默认的外部接口，该接口是通常用于连接到互联网的接口。

出于安全操作着想，您应该更改外部接口的配置，对外部的ping请求不作出响应。配置对外部的ping请求不作出响应增强了网络的安全性，增加网络中可能的攻击对FortiGate设备的探测。

根据FortiGate设备不同的型号，默认的外部接口可以是external接口或WLAN1接口。

如果对接口启动了ping管理访问设置，那么FortiGate设备将对ping请求作出响应。您可以使用以下操作步骤撤消对FortiGate设备外部接口的ping访问。同样的操作适用于任何操作模式下的设备接口。

使用基于web的管理器撤消ping管理访问

1. 登录基于web的管理器。
2. 进入系统>网络>接口。
3. 选择外部接口并点击对应的“编辑”。

4. 撤消Ping 管理访问功能。
5. 点击OK保存该配置更改。

使用CLI撤消ping管理访问

1. 登录FortiGate CLI。
2. 输入以下命令，撤消对外部接口的管理访问：

```
config system interface
  edit external
    unset allowaccess
end
```

NAT/路由模式安装

以下是有关如何在NAT/路由模式下安装Fortigate设备。包括以下内容：

- [配置FortiGate设备的NAT/路由模式准备](#)
- [配置DHCP或PPPoE](#)
- [使用基于web的管理器](#)
- [使用命令行接口（CLI）](#)
- [将FortiGate设备配置到网络中](#)
- [配置网络](#)

配置FortiGate设备的NAT/路由模式准备

参考表11中的信息，您可以定制NAT/路由模式设置。您可以使用以下几种方法配置FortiGate设备：

- 通过基于web的管理器的用户界面可以配置设备的大部分设置。参见“[使用基于web的管理器](#)”。
- 使用命令行接口（CLI）可以配置设备的全部设置。参见“[使用命令行接口（CLI）](#)”。

根据配置，访问与设备组合的复杂性与您惯用的接口类型选择合适的配置方法。

表11： NAT/路由模式设置

管理员密码		
Internal (内部)	IP: 子网掩码:	_____._____._____ _____._____._____
WAN1	IP: 子网掩码:	_____._____._____ _____._____._____
WAN2	IP: 子网掩码:	_____._____._____ _____._____._____
DMZ	IP: 子网掩码:	_____._____._____ _____._____._____
DMZ1	IP:	_____._____._____

(Fortigate-100A)	子网掩码:	_____ : _____ : _____
DMZ2 (Fortigate-100A)	IP: 子网掩码:	_____ : _____ : _____ _____ : _____ : _____
ADSL (Fortigate-60ADSL)	IP: 子网掩码	_____ : _____ : _____ _____ : _____ : _____
WAN	IP: 子网掩码:	_____ : _____ : _____ _____ : _____ : _____
网络设置	默认网关: (与外部网络连接的接口)	_____ : _____ : _____
	默认路由由默认的网关与连接到外部网络(通常指互联网)的接口组成。默认的网关将所有非本地流量集中到该接口与外部网络中。	
	一级DNS服务器: 二级DNS服务器:	_____ : _____ : _____ _____ : _____ : _____

配置使用DHCP或PPPoE

您可以配置任何FortiGate接口从DHCP或PPPoE服务器获得IP地址。您的互联网服务提供商(ISP)便是使用这其中的一项协议提供IP地址的。

使用FortiGate DHCP服务器,您需要配置该服务器的IP地址范围与默认的路由。将接口配置为使用DHCP便不需要做更多的配置了。

配置使用PPPoE需要设置用户名与密码。另外,PPPoE未编号配置要求固定一个IP地址。参考表12记录的信息配置PPPoE。

表12: PPPoE设置

用户名	
密码	

使用基于web的管理器

您可以使用基于web的管理器进行FortiGate设备的初始配置以及所有FortiGate设备的设置。

有关连接到基于web的管理器信息,参见“[连接到基于web的管理器](#)”。

配置基本设置

连接到基于web的管理器后,您可以使用以下操作完成FortiGate设备的基本配置。

添加或更改管理员密码

- 1.进入**系统> 管理员配置> 管理员**。

2. 点击“更改密码”图标更改管理员密码。
3. 输入新密码，再输入一次确认。
4. 点击OK确认。

配置接口

1. 进入**系统> 管理员配置> 管理员**。
2. 点击接口的“编辑”图标。
3. 设置接口的地址模式。
从菜单中选择DHCP或PPPoE。
4. 完成地址配置。
 - 对于手动的地址，输入接口的IP地址与掩码
 - 对于DHCP地址，点击DHCP并进行任何需要的设置
 - 对于PPPoE地址，点击PPPoE后输入用户名与密码有关接口设置的配置，参见FortiGate在线帮助或*FortiGate 设备管理员使用手册*。
6. 点击“OK”确认
重复以上步骤，对每个接口进行配置。



注意：如果您想更改连接接口的IP地址，您必须使用新的地址通过网页浏览器重新连接。浏览<http://>后跟接口新的IP地址。如果接口新的IP地址是不同的子网，您还需将计算机IP地址更改为与该子网相同的IP地址。

配置DNS服务器设置

1. 进入**系统>网络>选项**。
2. 输入一级DNS服务器的IP地址。
3. 输入二级DNS服务器的IP地址。
4. 点击“应用”。

添加默认路由

FortiGate设备发送数据包到外部网络（通常指互联网）时，需要配置添加默认的路由。添加默认的路由也需要定义哪个接口连接到外部网络。如果与外部网络连接的接口配置使用了DHCP或PPPoE，则不需要添加默认的路由。

添加默认路由

1. 进入**路由>静态路由**。
2. 如果静态路由表格中有默认的路由设置（IP与掩码设置为0.0.0.0），点击“删除”图标删除该路由。
3. 点击“新建”。
4. 设置目标IP地址为0.0.0.0。
5. 设置掩码为0.0.0.0。

- 6.设置网关为默认的网关IP地址
- 7.设置连接到外部网络接口的驱动。
- 8.点击OK确认。

校验基于web管理器配置

校验访问设置，进入所校验的接口并点击编辑图标。管理访问字段有检验标识可以确认是否执行了校验。

校验连接

使用以下步骤校验连接：

- 访问www.fortinet.com
- 从您的邮件帐户收发电子邮件

如果您不能浏览fortinet网站或收发电子邮件，请检查以上步骤确保所输入的信息正确，再试一次。

使用命令行接口（CLI）

您可以使用命令行接口（CLI）对FortiGate设备进行配置。有关连接到CLI的详细信息，参见“[连接到CLI](#)”。

配置FortiGate设备运行于NAT/路由模式

参考表11中所采集的信息完成以下步骤。

添加或更改管理员命令

- 1.登录到CLI（命令行接口）
- 2.更改管理员密码。输入：

```
config system admin
  edit admin
    set password <psswr>
  end
```

配置接口

- 1.登录到CLI（命令行接口）
 - 2.设置内部接口的IP地址与掩码为表11中所记录的内部IP地址与掩码。
- 输入：

```
config system interface
  edit internal
    set mode static
    set ip <address_ip> <netmask>
  end
```

举例

```
config system interface
  edit internal
    set mode static
    set ip 192.168.120.99 255.255.255.0
```

end

3. 设置外部接口的IP地址与掩码为表11中所记录的外部IP地址与掩码。输入：

```
config system external
  edit wan1
    set mode static
    set ip <address_ip> <netmask>
  end
```

举例

```
config system external
  edit wan1
    set mode static
    set ip 204.28.1.5 255.255.255.0
  end
```

设置外部接口使用DHCP

```
config system interface
  edit wan1
    set mode dhcp
  end
```

设置外部接口使用PPPoE

```
config system interface
  edit wan1
    set mode pppoe
    set connection enable
    set username <name_str>
    set password <psswr>
  end
```

4. 根据需要使用命令句法模式配置每个接口的IP地址。

5. 确认输入的地址是正确的。输入：

```
get system interface
```

CLI命令行接口列出了每个FortiGate接口的IP地址、掩码、与其他设置。

配置DNS服务器设置

设置一级与二级DNS服务器的IP地址。输入：

```
config system dns
  set primary <address_ip>
  set secondary <address_ip>
  end
```

举例

```
config system dns
  set primary 293.44.75.21
  set secondary 293.44.75.22
  end
```

添加默认的路由

FortiGate设备发送数据包到外部网络（通常指互联网）时，需要配置添加默认的路由。添加默认的路由也需要定义哪个接口连接到外部网络。如果与外部网络连接的接口配置使用了DHCP或PPPoE，则不需要

默认的路由。

添加默认的路由

设置默认网关IP地址的路由。输入：

```
config router static
  edit 1
    set dst 0.0.0.0 0.0.0.0
    set gateway <gateway_IP>
    set device <interface>
  end
```

举例

如果默认的网关IP地址是204.23.1.2，该网关连接到端口1：

```
config router static
  edit 1
    set dst 0.0.0.0 0.0.0.0
    set gateway 204.23.1.2
    set device port1
  end
```

校验连接

使用以下步骤校验连接：

- Ping FortiGate设备。
- 浏览基于web管理器的用户界面。
- 从您的邮件帐户收发电子邮件

如果您不能浏览fortinet网站或从您的帐户收发电子邮件，请检查以上步骤确保所输入的信息正确，再试一次。

至此，FortiGate设备的初始化配置完成。

将FortiGate设备连接到网络中

当您完成Fortigate设备的初始化配置后，便可以在您的内部网与互联网之间连接FortiGate设备了。

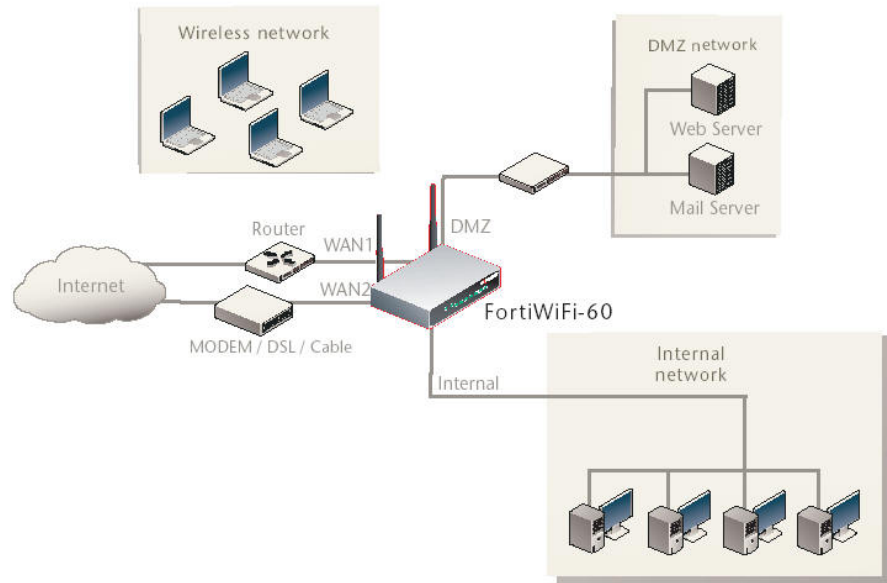
以下是FortiGate设备中可用的网络连接：

- 连接Internal接口，可以连接到内部网络。
- WAN1接口可以连接到互联网。
- WAN是FortiWiFi设备中的无线接口。
- DMZ是连接到DMZ网络的接口。

与FortiGate设备建立连接：

- 1.通过将内部接口连接到hub或交换机，接入内部网络。
- 2.将外部接口（External）与互联网连接。连接到ISP服务商提供的公共交换机或路由器。如果您是DSL或有线网络用户，将WAN1接口与内部网络或您DSL的LAN连接或有线调制解调器连接。
- 3.DMZ接口是连接DMZ网络的可选接口。
通过DMZ网络，无需在您的内部网络安装服务器，便可以进行从互联网到网络服务器或其他服务器的访问。

图10: FortiWiFi-60 NAT/路由模式连接



配置网络

如果FortiGate设备运行于NAT/路由模式，您需要给网络配置路由，使所有的网络流量都能够流向与网络连接的接口。

- 对于内部网络，更改与内部网络直接连接的所有计算机与路由器默认的网关地址为FortiGate内部接口的IP地址。
- 对于DMZ网络，更改与您的DMZ网络直接连接的所有计算机与路由器默认的网关地址为FortiGate设备DMZ接口的IP地址。
- 对于WAN网络，更改与您的WAN网络直接连接的所有计算机与路由器默认的网关地址为FortiGate设备WAN接口的IP地址。
- 对于处于WLAN网络中的FortiWiFi-60/60M设备，更改与您的WAN网络直接连接的所有计算机与路由器默认的网关地址为FortiGate设备WAN接口的IP地址。

如果您将FortiGate设备作为内部网络中的DHCP服务器使用，需要配置内部网络的计算机使用DHCP。

通过内部网络的计算机连接到互联网，确定连接的FortiGate设备工作正常。您应该可以连接到任何互联网地址。

透明模式安装

本章介绍了如何安装透明模式下安装FortiGate设备。包括以下内容：

- [配置透明模式的准备](#)
- [使用基于web管理程序](#)
- [使用命令行接口\(CLI\)](#)
- [将FortiGate设备连接到网络中](#)



注意：ADSL接口只有在使用FortiGate-60ADSL设备运行于NAT/路由模式时才有效。将模式切换为透明模式后改接口不生效。

配置透明模式的准备

参考表13的信息定制透明模式设置。

以下三种方法均可配置透明模式：

- 基于web管理程序的GUI
- 命令行接口（CLI）

根据配置，访问与设备的复杂性与您惯用的接口类型选择配置透明模式的方法。

表13：透明模式设置

管理员密码：		_____
管理IP	IP：	_____ : _____ : _____ : _____
	掩码：	_____ : _____ : _____ : _____
	默认网关：	_____ : _____ : _____ : _____
管理IP地址与掩码对于您所管理的FortiGate设备来讲必须是有效的网络地址。如果FortiGate设备需要连接到路由器后才能到达管理计算机，那么需要添加默认的网关。		
DNS设置	一级DNS服务器：	_____ : _____ : _____ : _____
	二级DNS服务器：	_____ : _____ : _____ : _____

使用基于web的管理器

您可以使用基于web的管理器完成FortiGate设备初始化配置以及设置功能选项。

有关连接到基于web的管理器信息，参见“[连接到基于web的管理器](#)”。初次连接到FortiGate设备时，默认操作模式是NAT/路由模式。

使用基于 web 的管理器切换到透明模式

- 1.进入系统>状态。
- 2.点击“操作模式”选项旁边的的“更改”。
- 3.在操作模式列表中选择透明（Transparent）模式。
4. 输入表13中收集的管理IP/掩码地址与默认网关地址。
- 5.点击应用。

无需与基于web的管理器重建建立连接。点击应用后，配置更改即可生效，您可以进入系统面板对更改为透明模式下的FortiGate设备进行校验。

配置DNS服务器设置

- 1.进入系统>网络>选项。
- 2.输入一级DNS服务器的IP地址

- 3.输入二级DNS服务器的IP地址
- 4.点击应用。

使用命令行接口（CLI）

除了使用基于web的管理器，您也可以使用命令行接口（CLI）对FortiGate设备进行初始化配置，参见“[连接到命令行接口（CLI）](#)”说明。表13中的收集的信息，可以协助完成以下操作。

使用CLI更改为透明模式

- 1.登录到CLI
- 2.切换到透明模式。输入：

```
config system settings
    set opmode transparent
    set manageip <address_ip> <netmask>
    set gateway <address_gateway>
end
```

几秒后，显示以下信息：

Changing to TP mode

- 3.登录页弹出时，输入以下命令：

```
get system settings
```

CLI显示FortiGate设备的状态包括管理IP地址与掩码：

```
opmode : transparent
```

```
manageip : <address_ip><netmask>
```

您需要校验DNS服务器设置的正确性。DNS设置是沿用NAT/路由模式的，对于透明模式可能并不正确。使用表13信息配置DNS服务器设置。

校验DNS服务器设置

输入以下命令检验FortiGate设备的DNS服务器设置：

```
show system dns
```

键入上述CLI命令后显示如下DNS服务器设置信息：

```
config system dns
    set primary 293.44.75.21
    set secondary 293.44.75.22
    set fwdintf internal
end
```

配置DNS服务器设置

设置一级与二级DNS服务器IP地址。输入命令：

```
config system dns
    set primary <address_ip>
    set secondary <address_ip>
end
```

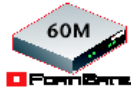
重新连接到基于web的管理器

当FortiGate设备切换到透明模式后，您可以使用新的IP地址重新连接

到基于web的管理器。键入HTTP://加新的IP地址。如果您通过一个路由器连接到管理接口，请确认是否在管理IP默认的网关字段添加了路由连接的网关。

将FortiGate设备连接到网络

完成设备初始化配置，便可以将FortiGate连接到您的内部网络与互联网之间，或是通过DMZ接口连接到其它网络中。



运行于透明模式下FortiGate-60M以及FortiGate-60ADSL设备的Modem连接不可用。

与透明模式运行下的FortiGate设备连接

- 1.将内部端口与连接到内部网络的网络集线器（hub）或交换机连接。
- 2.将外部端口与连接到您外部网络的网络集线器（hub）或交换机连接。连接到ISP服务商的公共交换机或路由器。
- 3.根据需要，将DMZ接口连接到hub或交换机。

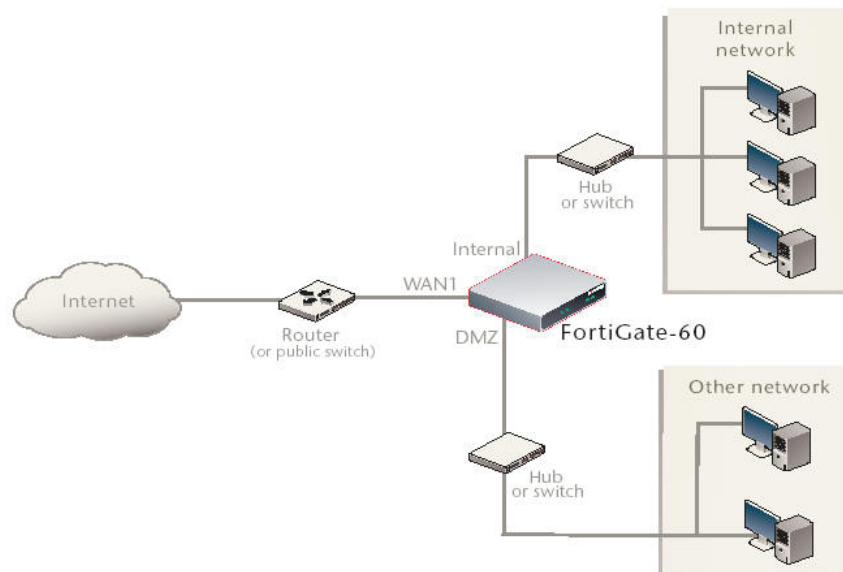
校验连接

使用以下操作校验连接：

- Ping FortiGate设备
- 登录到基于web的管理器
- 从您的邮件帐户收发电子邮件

如果您不能够正常浏览网站或收发电子邮件，检查以上步骤确定输入的信息正确，然后再试一次。

图11：FortiGate-60透明模式连接



下一步

以下是关于配置FortiGate系统时间、FortiGate设备注册以及配置病毒与攻击定义的更新的内容说明。

参见*FortiGate 管理员使用手册*有关FortiGate设备的配置，监控与维护信息。

设置系统日期与时间

为了便于部署与记录日志，需要准确设置FortiGate设备的系统时间与日期。您可以手动设置系统时间与日期，或通过与网络时间协议(NTP)服务器同步自动校准时间。

设置日期与时间

- 1.进入**系统>状态**。
- 2.**系统信息>系统时间**菜单选项下，点击“更改”。
- 3.点击“刷新”显示当前的FortiGate系统日期与时间。
- 4.从时区（Time Zone）列表中选择时区。
- 5.可选择“自动”选项自动调整夏令时。
- 6.点击“设置时间”，设置FortiGate系统日期与时间。
- 7.设置时，分，秒，月，日，年。
- 8.点击OK确认。



注意：如果您选择了根据夏令时自动调整时间，系统的时间必须在夏令时结束后手动重新调整。

使用NTP设置FortiGate设备的日期与时间

- 1.进入**系统管理>状态**。
- 2.**系统信息>系统时间**选项下，点击更改。
- 3.选择“与NTP服务器保持同步”，配置FortiGate使用NTP自动设置系统时间与日期。
- 4.输入NTP服务器的IP地址与域名，便于FortiGate设备自动设置时间与日期。
- 5.注明FortiGate设备与NTP服务保持时间日期同步校准的频率。
- 6.点击OK确认。

FortiGate设备注册

FortiGate设备安装完成后，访问<http://support.fortinet.com>并点击“产品注册”进行设备注册。

输入您的联系方式与所购买的FortiGate设备序列号进行注册。您可以在注册栏中对所购买的全部设备进行同时注册，而无需重复输入联系信息。

通过FortiGate设备注册，您将接收到Fortinet公司发布的病毒与入侵检测等的更新并确保您能够访问Fortinet技术支持。

更新病毒防护与IPS特征

您可以配置FortiGate设备连接到FortiGuard Distribution Network进行病毒防护升级，反垃圾邮件与IPS攻击的定义更新。

FDN是遍及全世界范围的FDS服务器网络。当FortiGate设备连接到FDN，根据就近原则，所有的FortiGate设备根据设备配置中的时区中相隔位于最近时区的FDN进行划分。

通过基于web的管理器或CLI，您可以更新病毒保护与IPS特征。设备在接收更新之前，需要先登录Fortinet网站进行注册。有关FortiGate设备注册的详细信息，参见“[FortiGate设备注册](#)”。

FortiGate设备注册后，校验是否能够与FDN连接：

- 检查FortiGate设备的系统时间是否正确。
- 登录基于web管理程序，在FortiGuard Center选项中点击“刷新”。

如果您不能连接到FDN，检查注册FortiGate设备步骤是否正确后，再试一次连接；或参见“[添加替代的FDN服务器](#)”。

使用基于web的管理器更新病毒防护与IPS特征

FortiGate设备注册完成后，您可以使用基于web的管理器更新病毒防护与IPS特征。FortiGuard Center将发送推进式更新，您需要设置接收更新的IP地址，以及指定更新的时间频率如每日、每周或隔小时。

更新病毒防护定义与IPS特征

1.进入**系统管理>维护> FortiGuard中心**。

2.点击“立即更新”，进行病毒防护更新。

如果与FDN连接良好，基于web的管理器显示类似以下的信息：

Your update request has been sent. Your database will be updated in a few minutes. Please check your update page for the status of the update.（您的更新请求已被发送，数据库将尽快进行更新。请浏览更新页面查看更新情况。）

几分钟后，如果有可获得的更新，FortiGuard Center系统页面列出新版本的病毒定义信息。系统状态页面也同样显示病毒防护定义的更新日期与版本号。该消息将被记录到时间日志中，标明更新是否成功。



注意：病毒定义更新时会导致流量的暂时性中断或干扰，您可以设置在通过设备流量低峰的时候更新病毒定义，例如夜间时间，将中断流量的可能性降到最低。



注意：AV与IPS特征需要经常定期进行更新。如果不定期更新AV与IPS特征，FortiGate设备容易受到新病毒的攻击。

使用CLI更新IPS特征



注意：您也可以从基于web管理器更新病毒定义。

使用CLI接口更新IPS特征。使用以下步骤更新IPS特征：

使用CLI更新IPS特征

1.登录到CLI

2.键入以下CLI命令：

```
configure system autoupdate ips
    set accept-recommended-settings enable
end
```

制定病毒防护与IPS更新时间

使用基于web的管理器或CLI制定定期、自动更新病毒防护与IPS特征。

使用基于web的管理器制定更新时间

1.进入**系统管理>维护> FortiGuard 中心**。

2.点击“制定更新”的功能框。

3.选择以下的更新时间之一并下载更新

Every（每天）24小时之间。选择每次更新间隔的时间。

Daily（每天）您可以指定每天检查更新的时间。

Weekly（每周）您可以指定每周检查更新的时间。

4.点击应用。

FortiGate设备将根据新指定的更新时间执行接下来的更新。

只要FortiGate设备执行所制定时间进行更新，更新事件均将被记录都事件日志中。

使用CLI制定更新时间

1.登录CLI。

2.键入以下命令：

```
config system autoupdate schedule
    set day
    set frequency
    set status
    set time
end
```

举例

```
config system autoupdate schedule
    set update every Sunday
    set frequency weekly
    set status enable
    set time 16:45
end
```

添加替代的FDN服务器

如果您不能连接到FDN，或您的公司使用自己的FortiGuard服务器提供更新，使用以下操作步骤在基于web的管理器或CLI中添加替代FDN服务器的IP地址。

使用基于web的管理器添加替代的FDN服务器

- 1.进入**系统管理>维护> FortiGuard中心**。
- 2.选中“使用替代FDN服务器地址”的功能框。
- 3.键入有效的FortiGuard 服务器域名或IP地址
- 4.点击应用。

FortiGate设备检测与代理FDN服务器的连接。

如果FDN设置更改为“连接”状态，说明FortiGate设备与替代FDN服务器建立了连接。

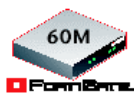
如果FDN保持“无法连接”状态，说明FortiGate设备不能与替代FDN建立连接。请检查是否是FortiGate配置或网络配置设置阻碍了FortiGate设备与替代FDN服务器的连接。

使用CLI添加替代FDN服务器

- 1.登录CLI。
- 2.键入以下命令：

```
config system autoupdate override
    set address
    set status
end
```

配置modem接口



除了FortiGate-60ADSL设备其余FortiGate-60系列设备中的modem接口都是可用的。

以下是基于web管理器，如何配置FortiGate-60M设备的modem接口，以及通过CLI配置FortiGate-60以及FortiWiFi-60 modem接口。

FortiGate-60系列设备在NAT/路由模式下支持冗余或单机modem接口。

- 冗余模式下，当Ethernet接口不可用的情况下，modem接口自动从所选的Ethernet接口承接连接。
 - 单机模式下，modem接口是FortiGate设备到互联网之间的连接。
- 以上两种配置模式下连接ISP时，modem接口可以自动对三个帐户进行拨号直到其中一个连接到ISP。

本章包括以下内容：

- 设置modem接口模式
- 配置modem设置
- 单机模式下，连接与断开与modem的连接
- 配置FortiGate-60以及FortiWiFi-60的modem设置
- 添加ping服务器
- 对modem连接添加防护墙策略

设置modem接口模式

Modem接口可以运行于两种模式：

- 冗余模式
- 单机模式

冗余模式配置

冗余modem接口作为Ethernet接口的备用接口，如果Ethernet接口断开与网络的连接，modem接口将自动拨号配置的帐户。当modem与一个拨号帐户连接时，FortiGate设备自动将发送到Ethernet接口的IP数据包发送到modem接口。Modem接口代连接的过程中，设备将不断对Ethernet接口发出ping的命令查看Ethernet接口恢复使用的时间。

当Ethernet接口重新连接到网络中时，FortiGate设备将断开与modem接口的连接，切换回Ethernet接口的连接。

配置FortiGate-60M设备的冗余modem连接

1. 进入系统>网络>modem。
2. 点击启动modem。
3. 选择冗余模式。
4. 在冗余接口列表，选择将Modem作为Ethernet接口的备用接口。
5. 根据需要配置其它modem设置。
6. 对Ethernet接口配置ping服务器。
7. 对通过modem接口的连接配置防护墙策略。

通过CLI配置FortiGate-60与FortiWiFi设备

1. 登录CLI。
2. 输入以下命令配置冗余modem:

```
config system modem
  set status enable
  set status mode redundant
end
```

单机模式配置

单机模式下，您可以手动设置modem连接到拨号帐户。Modem接口将作为与互联网的首选连接。FortiGate设备通过modem接口路由数据包，该接口将成为与拨号帐户的永久连接。

如果到拨号帐户的连接失败，FortiGate设备modem将自动重拨号码。重拨次数可以在配置中设置，或直至连接到该帐户。

单机模式下，modem接口将代替外部Ethernet接口。您必须也需要对modem接口以及其它FortiGate接口之间的连接配置防火墙策略。



注意： 不要对代替Ethernet接口的modem接口添加任何路由。



注意： 不要对代替Ethernet接口的modem接口与其它接口之间的连接添加防火墙策略。

运行于单机模式的FortiGate-60M设备

1. 进入系统>网络>Modem。
2. 根据需要配置其它modem设置。
查看拨号帐户的信息是否正确。
3. 对通过modem接口的连接配置防火墙策略。
4. 点击“拨号连接”。

FortiGate设备依次对每个拨号发起连接直至modem连接到ISP。

使用CLI操作运行于单机模式

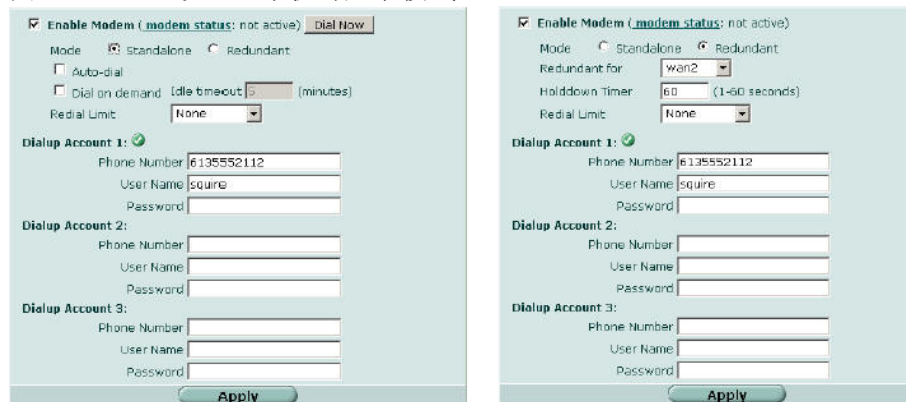
1. 登录CLI。
2. 输入以下命令配置单机模式下modem设置:

```
config system modem
  set status enable
  set status mode standalone
end
3. 输入以下命令配置拨号帐户。
config system modem
  set auto-dail
  set idle-timeout <mintues_interger>
  set passwd1 <phone-number_str>
  set redial <tries_interger>
  set username1 <name_str>
end
```

配置modem设置

配置modem设置，以便FortiGate设备modem连接到ISP拨号帐户。您可以配置modem最多连接三个拨号帐户。您也可以启动或撤消FortiGate设备modem支持，配置modem拨号帐户并选择modem作为设备哪个接口的冗余。

图12: modem设置（单机与冗余模式）



启动Modem Modem状态

选中启动功能框，启动FortiGate设备modem设置。Modem的状态显示：“未激活”，“连接中”，“已连接”，“断开连接”或“挂断”。（只适用于单机模式）

拨号连接/挂断 模式

点击拨号连接，自动连接到一个拨号帐户。如果与modem建立了连接，点击“挂断”断开与modem的连接。选择独立或冗余模式。独立模式下，modem是一个独立的接口。冗余模式下，modem作为在选择以太网接口后的备用设备。

自动拨号

（只适用于独立模式）如果失去连接或FortiGate重新启动，选择自动拨号modem。“请求时拨号”与“自动拨号”不能同时选择。

冗余

（只适用于独立模式）点击以太网接口，modem作为备用。

请求时拨号

（只适用于独立模式）当数据包路由到modem接口时，点击拨号modem。闲置超时时，断开与modem的连接。“请求时拨号”与“自动拨号”不能同时选择。

闲置超时

（只适用于独立模式）输入闲置超时的间隔时间。如果保持在设定的间隔时间内没有连接活动，将断开与modem的连接。

等待时间

（只适用于冗余模式）主接口恢复之后，modem接口将转为主接口，FortiGate设备等待的时间（1到60秒）。缺省的等待时间是1秒。如果发现SecPath F1800-AW设备在主接口与modem接口之间重复装换，设置较高的等待时间值。

重拨次数

与ISP的连接失败后，SecPath F1800-AW设备的modem试图与ISP重新发起连接请求的最大次数。缺省的最多重拨次数是1次。选择“空”不限制重拨请求的次

- 数。
- 拨号帐户** 最多可以配置三个帐户。SecPath F1800-AW设备逐个与每个帐户连接，直到连接已经建立。
- 电话号码** 与拨号帐户连接需要的电话号码。请不要在电话号码的填写之间加空格。根据modem连接到拨号帐户的要求填写。
- 用户名** 发送到ISP的用户名称。（最多可以设置为63个字符长度）
- 密码** 发送到ISP的密码。
- Modem设置只有在NAT/路由模式配置使用使用。

配置modem设置

1. 进入系统>网络>Modem。
2. 选中“启动modem”功能框。
3. 更改拨号连接的设置。
4. 输入拨号帐户1的设置。
5. 如果有多个拨号帐户，输入电话号码、用户名以及帐户2与帐户3的密码。
6. 点击“应用”。

单机模式下，建立以及断开与modem的连接
连接到拨号帐户

1. 进入系统>网络>modem。
2. 选中“启动modem”功能框。
3. 确认拨号帐户中的信息输入正确。
4. 如果更改了设置，点击“应用”。
5. 点击“立即拨号”。

FortiGate设备依次发起对每个帐户的连接，直至与ISP建立连接。

未激活	Modem接口没有连接到ISP。
激活	Modem接口正在试图与ISP连接，或已经连接到ISP。

检验框呈绿色显示表示激活状态下的拨号帐户。

分配到modem接口的IP地址与掩码。进入系统>网络>接口，校验IP地址与掩码。

断开modem连接

使用以下步骤断开modem与拨号帐户的连接。

1. 进入系统>网络>modem。
2. 如果断开与拨号帐户的连接，点击“挂断”。

对FortiGate-60与FortiWiFi-60设备配置modem

通过CLI配置FortiGate-60与FortiWiFi-60设备的modem设置。以下是所使用命令的详细信息。

表12: CLI命令

关键字与命令	描述	缺省值
altmode {enable disable}	启动PPP设置。	enable
auto-dial {enable disable}	如果连接断开,或FortiGate设备重启时启动modem自动拨号。必须将dial-on-demand disable。mode 设置为standalone。	disable
connect_timeout <seconds>	设置连接超时(30到255秒)。	90
dial-on-demand {enable disable}	当数据包路由到modem接口时启动modem拨号。在idle-timer设定的时间之后,断开modem连接。必须disable auto-dial。mode 设置为standalone。	disable
holddown-timer <seconds>	当modem配置作为接口的备份时使用。设置在从modem接口切换到主接口之前,主接口恢复之后,这个过程中FortiGate设备等待的时间(1到60秒)。mode设置为redundant。	60
idle-timer <minutes>	设置在modem连接断开之前的闲置时间。mode设置为standalone。	5
interface <name>	输入modem接口备份(备份配置)或代替(单机模式配置)Ethernet接口的名称。	没有缺省值
mode <mode>	设置模式: ● Standalone Modem接口是从FortiGate设备到Internet网络之间的连接。 ● redundant 当Ethernet接口不可用时,modem接口将自动代替所设定的Ethernet接口。	standalone
passwd1 <password_srt>	输入访问指定拨号帐户的密码。	没有缺省值
passwd2 <password_srt>	输入访问指定拨号帐户的密码。	没有缺省值
passwd3 <password_srt>	输入访问指定拨号帐户的密码。	没有缺省值
peer_modem1 {actiontec ascendTNT generic}	如果与phone1连接的modem是Actiontec或Ascend TNT,点击选择型号,或者保留该栏目为generic。该设置只适用于FortiGate-50AM, FortiGate-60M以	generic

	及FortiWiFi-60M设备。	
peer_modem2 {actiontec ascendTNT generic}	如果与 phone2 连接的 modem 是 Actiontec 或 Ascend TNT，点击选择型号，或者保留该栏目为 generic。该设置只适用于 FortiGate-50AM, FortiGate-60M 以及 FortiWiFi-60M 设备。	generic
peer_modem3 {actiontec ascendTNT generic}	如果与 phone3 连接的 modem 是 Actiontec 或 Ascend TNT，点击选择型号，或者保留该栏目为 generic。该设置只适用于 FortiGate-50AM, FortiGate-60M 以及 FortiWiFi-60M 设备。	generic
phone1 <phone-number>	输入与拨号帐户连接所需的电话号码。号码输入之间不需要加空格。确定适用标准特殊字符来分隔连接拨号帐户时所填写的信息。	没有缺省值
phone2 <phone-number>	输入与拨号帐户连接所需的电话号码。号码输入之间不需要加空格。确定适用标准特殊字符来分隔连接拨号帐户时所填写的信息。	没有缺省值
phone3 <phone-number>	输入与拨号帐户连接所需的电话号码。号码输入之间不需要加空格。确定适用标准特殊字符来分隔连接拨号帐户时所填写的信息。	没有缺省值
redial <tries_interger>	输入 modem 可以重拨帐户的最大次数（1到10次）。 输入 none, modem 可以无限次的拨号帐户。	没有缺省值
status {enable disable}	启动或撤消 modem 支持。	disable
username1 <name_str>	输入访问指定拨号帐户的用户名。	没有缺省值
username2 <name_str>	输入访问指定拨号帐户的用户名。	没有缺省值
username3 <name_str>	输入访问指定拨号帐户的用户名。	没有缺省值

举例说明：

```

config system modem
  set action dial
  set status enable
  set holddown-time 5
  set interface wan1
  set password1 acct1passwd
  set phone1 1234567891
  set redial 10

```

```
set username1 acctluser
end
```

添加 Ping 服务器

Modem在冗余模式下发生路由故障时，需要添加ping服务器。用来确定到Ethernet接口的连接性。

对接口添加ping服务器

1. 进入系统>网络>接口。
2. 选择接口并点击“编辑”。
3. 对与接口连接的网络中的下一个中继路由的IP地址添加ping服务器。
4. 选中“启动”功能框。
5. 点击OK保存设置更改。

失效网关检测

FortiGate设备使用失效网关检测功能发送ping命令到Ping服务器的IP地址查看FortiGate设备是否能够连接到该IP地址。

更改失效网关检测的配置可以控制FortiGate设备是如何确认与添加到接口的ping服务器连接性。有关在接口添加ping服务器的详细信息，参见上文。

修改失效网关检测设置

1. 进入系统>网络>选项。
2. 在“检测间隔”字段，输入FortiGate设备检测与ping目标连接性的频率。
3. 在“失效检测”字段，输入在FortiGate设备认为网关已经不再起作用之前连接检测失效的次数。
4. 点击“应用”。

对Modem连接添加防火墙策略

在modem接口需要添加防火墙地址与策略。您可以在modem接口添加一个或多个防火墙地址。有关地址添加的详细信息，参见***FortiGate 设备管理员使用手册***。在您设置添加地址时，modem接口在策略栏目中出现。

您可以添加防火墙策略控制FortiGate设备modem接口与其它接口之间的数据包流。有关添加防火墙策略的详细信息，参见***FortiGate 设备管理员使用手册***。

配置ADSL接口



只有FortiGate-60ADS设备设置有ADSL modem接口。

本章是有关配置FortiGate-60ADSL设备ADSL接口的内容，尤其是ADSL接口与其它接口之间不同的配置步骤。详细信息，参见*FortiGate设备管理员使用手册*。

FortiGate-60ADSL设备包含一个非对称数字用户线（ADSL）接口。该接口能够提供比标准电话线modem更高的通信速度。



注意：ADSL接口只有在FortiGate设备运行于NAT/路由模式下生效。更改为透明模式将撤消ADSL接口的功能。

使用web管理器配置ADSL接口

以下描述是有关配置ADSL接口与ISP服务商连接的步骤。您需要获得您ADSL ISP的有关信息。

配置基本ADSL设置

ADSL接口与任何其它FortiGate设备物理接口配置类似。根据ISP要求使用的寻址模式提供配置信息。如果设置使用IPOA或EOA的静态寻址模式，需要输入IP地址与掩码。如果使用动态寻址模式，您需要根据“在ADSL接口配置使用DHCP”或“配置ADSL接口使用PPPoE或PPPoA”的配置步骤填写配置信息。

进入系统>网络>接口，点击“新建”或点击现有接口的编辑图标。在寻址模式，点击IPOA或EoA。

Addressing mode

IPoA EoA DHCP PPPoE PPPoA

IP/Netmask:

Gateway:

Connect to Server.

Virtual Circuit Identification VPI: VCI:

MUX Type LLC Encap VC Encap

寻址模式

- IPOA** 点击ISP指定的寻址模式。
- EoA** 基于ATM的IP，输入ISP提供的IP地址与掩码。
- DHCP** 基于ATM的Ethernet，通常也称为桥模式。输入ISP提供的IP地址与掩码。
- PPPoE** 参见“配置ADSL接口使用DHCP”。
- PPPoA** 参见“配置ADSL接口使用PPPoE”。

网关

参见“配置ADSL接口使用PPPoA”。

输入默认的网关。

连接到服务器	启动“连接到服务器”，那么接口可以自动建立连接。如果您配置接口处于离线状态，可以撤消该选项。
虚电路标识	输入ISP提供的VPI与VCI值。
MUX类型	选择MUX类型：LLC Encap或VC Encap。ISP需要提供该信息。

配置ADSL接口使用DHCP

如果您配置接口使用DHCP，FortiGate设备将自动发送一个DHCP请求。

进入系统>网络>接口，点击“新建”或点击现有接口的编辑图标。在寻址模式下，选择“DHCP”。

图13: ADSL接口 DHCP设置



管理距离	输入从DHCP服务器获取默认网关的管理距离。管理距离可以设置为1到255之间的任何整数，表示在有多个路由同时到达同一目的时，相对具有优先性的路由。
从服务器获取默认网关	启动“从服务器自动获取默认”，从DHCP服务器自动获取默认的网关IP地址。默认的网关将被添加到静态路由表中。
代理内部DNS	启动“代理内部DNS”，从DHCP服务器获取DNS地址，而不是从DNS页面获取DNS服务器的IP地址。进入系统>网络>选项，您应该同时启动“获取DNS”，自动获取DNS服务器地址。
连接到服务器	启动“连接到服务器”，接口可以自动连接到一个DHCP服务器。如果您配置接口处于离线状态，需要撤消该选项。

配置接口使用PPPoE或PPPoA

如果您配置接口使用PPPoE，FortiGate设备将自动发送一个PPPoE请求。如果您配置FortiGate设备处于离线状态或FortiGate设备不发送PPPoE请求，您可以撤消“连接到服务器”功能框选项。

FortiGate设备支持许多PPPoE RFC功能（RFC 2516）包括未编号IP、初始发现超时以及PPPoE有效发现终止（PDAT）。

进入系统>网络>接口，点击“新建”或点击现有接口的编辑图标。在寻址模式下，选择“PPPoE或PPPoA”。

图14: ADSL接口 PPPoE或PPPoA设置

输入以下信息，并点击“确认”。

用户名	输入ISP服务商提供的PPPoE或PPPoA帐户用户名。
密码	输入ISP服务商提供的PPPoE或PPPoA帐户密码。
未编号IP	指定接口的IP地址。如果您的ISP服务商分配给您一批IP地址，使用其中的一个。否则，该IP地址可能与其它接口的IP地址相同或作为任何其它IP地址。
初始发现超时	重新开始一个PPPoE有效发现之前的等待时间。设置初始发现的时间为0将在任何时间下都不会终止会话。
初始PADT超时时间	如果闲置的时间超出了设置的时间，PPPoE将被关闭。PADT功能需要ISP服务商的支持。设置初始PADT的时间为0将在任何时间下都不会终止会话。
验证	选择ISP使用的验证方法： PAP,CHAP,MACHAPv1,MSCHAPv2或 Auto。
管理距离	输入默认从PPPoE服务器获取默认网关的管理距离参数。管理距离可以设置未1到255之间的整数，指定在多个路由到相同目的地的情况下选择一条当对较为优先的路由。管理距离越小表示其路由资源越值得信赖。默认网关的管理距离设置为1。
从服务器获取默认网关	启动“获取默认网关”从PPPoE服务器获取默认的网关的IP地址。默认的网关将被添加到静态路由表中。
代理内部DNS	启动“代理内部服务器”（Override internal DNS）使用从DHCP获取的DNS地址代替DNS页面中DNS服务器的IP地址。
连接到服务器	启动“连接到服务器”（Override internal DNS）那么接口将自动试图与DHCP服务器建立连接。如果您配置接口未与网络连接将不能启动该选项。
状态	显示FortiGate设备与DHCP连接的DHCP状态信息以及寻址信息。点击“状态”刷新寻址模式状态信息。
	初始连接 没有网络活动。
	正在连接 接口试图与DHCP服务器建立连接。
	完成连接 接口从DHCP服务器获取了IP地址，掩码以及其它设置。
	连接失败 接口不能从DHCP服务器获取了IP地址以及

其它信息。

使用CLI配置ADSL接口

ADSL接口与任何其它FortiGate设备物理接口配置类似。根据ISP要求使用的寻址模式提供配置信息。

本节所示设置，是配置ADSL接口所特有的，在其它FortiGate技术文件中没有描述。许多适用于一般接口的设置也适用于ADSL接口。这里只对您需要配置与ISP建立通信的设置信息进行了说明。有关接口设置的全部列表，参见**FortiGate 设备CLI使用参考手册**。

命令句法

```
config system interface
  edit adsl
  set ip 10.10.10.1 255.255.255.0
  set mux_type vc-encaps
  .....
end
```

这些关键字与变量是ADSL接口配置特有的。 而且这些变量也只有在edit adsl命令下可用。		
关键字与变量	描述	
pppoe-mtu <mtu_bytes>	设置ADSL接口PPPoE会话的最大传输单元（MTU）。最理想的MTU值应该与该FortiGate设备与目标数据包地址之间的所有网络传输的最小MTU。 范围：576到1492。	
gwaddr<gw_ipv4>	网关地址。只有在mode是ipoa or eoa。	
mux_type { 11c-encap vc-encaps }	输入虚拟电路的Mux模式。	
vci	输入您的ISP提供的VCI。	35
vpi	输入您的ISP提供的VPI。	0
适用于ADSL接口的常规关键字与变量。 联系您的ISP获得有关配置这些设置的信息。		
关键字与变量	描述	默认值
auth-type <ppp_auth_method>	选择 PPPOE， PPPoA 或 DHCP的验证方法。 <ul style="list-style-type: none">● 输入auto设置为自动。● 输入chap表示CHAP。● 输入 ms-chapv1 表示 Microsoft CHAP v1。● 输入 ms-chapv2 表示 Microsoft CHAP v2。● 输入pap表示PAP。	auto

	只有mode设置为pppoe时，auth-type可用。	
connection {enable disable}	启动或撤消与一个PPPoE或PPPoA服务器连接对接口配置使用PPPoE或PPPoA。只有当设备运行于NAT/路由模式，并且mode是dhcp，pppoe或pppoa时，该功能才可用。	disable
defaultgw {enable disable}	启动或撤消接口作为默认网关。	disable
disc-retry-timeout <pppoe_retry_seconds>	设置初始发现超时。重新启动一个PPPoE发现之前等待的时间。将disc-retry-timeout设备为0，表示撤消该功能。只有当设备运行于NAT/路由模式，并且mode是pppoe时，该功能才可用。	
dns-server-override {enable disable}	启动允许接口通过使用DHCP或PPPoE获取使用DNS服务器地址。mode必须设置为dhcp或pppoe。	disable
edit <interface_name>	编辑现有的接口或建立一个新的VLAN接口。	None
gwdetect {enable disable}	启动或撤消与服务器在detectserver IP地址上的连接性。FortiGate设备检测连接性的频率是通过system global命令中failtime与interval关键字设置的。详细信息，参见 FortiGate 设备 CLI 使用参考手册 。该功能只有在NAT/路由模式下可用。	disable
idle-timeout <pppoe_timeout_seconds>	如果PPPoE或PPPoA连接超过设置的闲置时间，将被断开。该功能只有在mode设置为dhcp或pppoe时可用。	0
ip <interface_ip4mask>	输入接口IP地址与掩码。只有当设备运行于NAT/路由模式，并且mode是pppoe时，该功能才可用。IP地址不能与其它任何接口处于相同的子网。	

<p>Ipunnumbered <unnumbered_ipv4></p>	<p>对PPPoE或PPPoA启动IP未编号模式。注明从接口借用的IP地址。该IP地址可以与其它接口的地址相同，或是其它任何地址。未编号的地址可以用于设置了PPPoE或PPPoA的接口，在这样的接口中不没有唯一性的本地地址。如果您的ISP提供了一个IP地址段，您可以将这些地址中的任意一个添加在未编号IP中。</p>	<p>没有默认值</p>
<p>mode <interface_mode></p>	<p>对接口配置连接模式。只有当设备运行于NAT/路由模式，该功能才可用。</p> <p>dhcp</p> <ul style="list-style-type: none"> ● 配置接口从DHCP服务器获取IP地址。 <p>pppoe</p> <ul style="list-style-type: none"> ● 配置接口从PPPoE服务器获取IP地址。 <p>pppoa</p> <ul style="list-style-type: none"> ● 配置接口从PPPoA服务器获取IP地址。 <p>eoaa</p> <ul style="list-style-type: none"> ● 在ADSL EoA桥模式下，对接口配置静态IP地址。 <p>ipoaa</p> <ul style="list-style-type: none"> ● 在ADSL IPoA路由模式下，对接口配置静态IP地址。 	<p>eoaa</p>
<p>mtu<mtu_bytes></p>	<p>设置ADSL接口PPPoE会话的最大传输单元（MTU）。最理想的MTU值应该与该FortiGate设备与目标数据包地址之间的所有网络传输的最小MTU。</p> <p>对于static模式，<mtu_bytes>设置范围为576到1500比特。</p> <p>对于dhcp模式，<mtu_bytes>设置范围为576到1500比特。</p> <p>对于pppoe模式，<mtu_bytes>设置范围为576到1492比特。</p> <p>透明模式下，如果您更改接口的MTU值，您必须相应对</p>	<p>1500</p>

	所有接口的MTU值更改以匹配新的MTU值。 该功能只有在mtu-override启动后才可以生效。	
mtu-override {enable disable}	启动使用用户定义MTU值功能，而不是默认的MTU值（1500）。	disable
padt-retry-timeout <padt_retry_seconds>	初始PDAT超时时间。该设置可以在PPPoE会话超过规定的闲置时间后自动切断会话。您的ISP必须支持PADT功能。将PDAT超时设置为0表示使用默认值。只有当设备运行于NAT/路由模式，并且mode是pppoe时，该功能才可用。	
password <pppoe_password>	输入连接到PPPoE或PPPoA服务器的密码。	
status {down up}	启动或停止接口的功能，如果接口被停止通信，将不接收或发送任何数据包。如果您撤消物理接口的功能，与该接口相应的VLAN接口的功能也将停止。	up（VLAN接口显示down）
username <pppoe_username>	输入与PPPoE或PPPoA服务器连接的用户名。只有当设备运行于NAT/路由模式，并且mode是pppoe时，该功能才可用。	没有默认值。

IPOA或EOA举例

以下举例中说明在IPOA模式下IP地址为10.10.10.1，掩码为255.255.255.0使用PPPoE定义VPI与VCI设置。如果将mode更改为eoa，该例子同时适用。

```
config system interface
edit adsl
set mode ipoa
set ip 10.10.10.1 255.255.255.0
set vpi 1
set vci 34
set mux-type 11c-encaps
set connection enable
end
end
```

DHCP举例

以下是使用默认的VCI与VPI设置在DHCP配置下与ISP连接所需的设

置。

```
config system interface
  edit adsl
    set mode dhcp
    set mux-type 11c-encaps
    set connection enable
  end
end
```

PPPoE或PPPoA举例

以下是使用默认的VCI与VPI设置与ISP连接所需设置举例。如果您将mode关键字更改为pppoa，该例子同样适用于PPPoA设置。

```
config system interface
  edit adsl
    set mode pppoe
    set username user1
    set password hard_to_guess
    set suth-type pap
    set mux-type pap
    set connection enable
  end
end
```

对ADSL连接添加防火墙策略

ADSL接口需要添加防火墙地址与策略。您可以在ADSL接口添加一个或多个地址。有关添加地址的详细信息，参见***FortiGate 设备管理员使用手册***。对ADSL接口添加地址时，ADSL接口将出现在策略栏中。

对FortiGate设备ADSL接口与其它接口之间的连接添加防火墙策略可以控制其数据包流量。有关添加防火墙策略的详细信息，参见***FortiGate 设备管理员使用手册***。

无线网络的使用



本章是针对FortiWiFi-60设备的说明。

有线网络中，计算机设备是通过线缆联接传输信息的。而无线网络中是通过无线电波来传输信息。无线电波在空气中的数据传输受很多因素的影响，在搭建无线网络时需要将这些因素考虑在内。

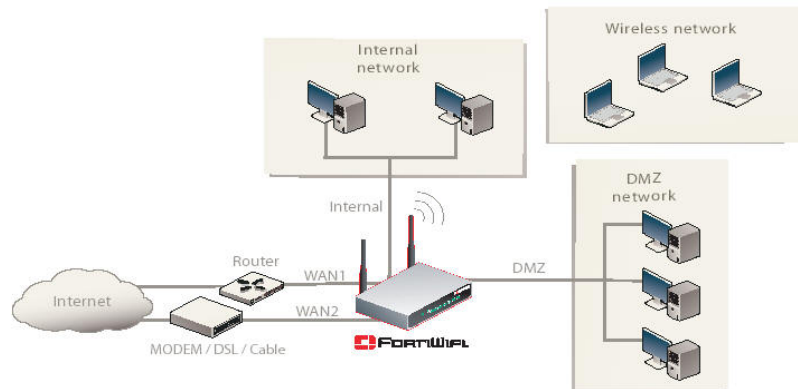
本章包括以下内容：

- 建立无线网络
- 无线网络安全
- FortiWiFi-60的操作模式
- 设置FortiWiFi-60作为访问点

建立无线网络

无线网络的终极简单的形式是，一个无线网络是一个无线设备与一个访问点之间的通信。一个访问点（AP, access point）是能够在无线网络中提供通讯集点的设备。AP与无线设备使用相同的无线频率。FortiWiFi-60作为一个AP，将所有的无线用户集中在同一个子网，通过使用恰当的防火墙策略与路由，无线用户可以与内网或外网（例如互联网）中的用户通信。

图15：FortiWiFi-60设备作为一个连接点（AP）



AP定位

当FortiWiFi-60设备放置在网络中AP，最主要的考虑因素是如果对所有的用户提供稳定强烈的信号。强的信号可以保证较快的连接速度与高效的数据传输。信号弱意味着数据传输出错的几率较大，并且需要重复发送信息，数据传输的速度也就慢。

以下是配置FortiWiFi-60设备作为AP需要考虑的几方面：

- 物理障碍物可以阻挡无线电信号的传播。固体例如墙壁、家具或人可以吸收消弱无线电信号。所以，注意办公室内的物理屏障可以减弱信息。如果有交叉的物理隔断，会有一些死角接收不到信

- 号。
- 将FortiWiFi-60作为访问点，放置在空间中中心且突出的位置，避免放置在拐角。
 - 建筑物或大厦使用的建筑材料也可以削弱无线电信号。混凝土或金属建筑的墙壁也影响信息的强弱。

无线电频率对接

802.11标准使用的频率是2.4到2.483GHz。当其它设备正常运行时使用的频率与FortiWiFi-60作为访问点发送的频率相同时，就会发生无线电频率干涉。无线电装置例如2.4GHz无线电话、微波炉与蓝牙设备干扰无限网络中的数据包传输。

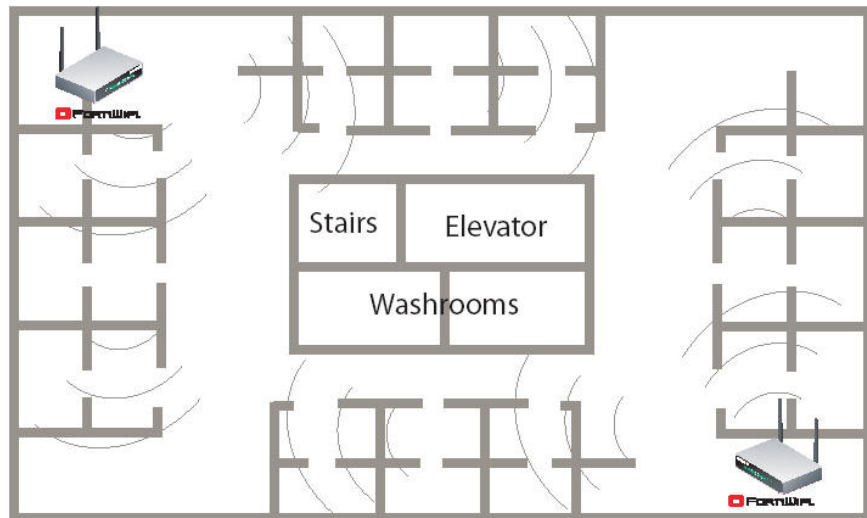
避免无线电频率干涉的方法：

- 将这些设备从用户使用的无线网络区域移开。一个如果蓝牙启动的鼠标可能会导致数据传输的中断。
- 将FortiWiFi-60 AP与无线设备同诸如微波炉与无线电话这样工具保持至少10英尺的距离。
- 如果您必须使用无线电话，选择一个频率不在2.4GHz频率范围内的。
- 多考虑FortiWiFi-60作为访问点的位置，加强信号的传播。较弱的信号，与较慢的数据传输是FortiWiFi设备与其它无线设备竞争信号导致的。
- 设置用户与FortiWiFi-60 AP使用特定的频道，可以加强信号的质量。

使用多个访问点

如果由于办公间的布局或建筑材料不能避免上述可能发生导致信号弱传输慢的结果，您可以应用多个FortiWiFi-60作为访问点加强信号的传播。图16所示怎样在一个固定形状的办公室空间部署FortiWiFi-60设备传播信号。

图16：使用多个AP提供连续稳定的信号



以上办公室的结构图，洗手间、楼梯间与电梯间处于建筑物中心，这样使用一台FortiWiFi-60作为AP很难实现高效的稳定的信号传播。电梯轴与洗手间的金属隔断削弱了信号。但是，将FortiWiFi-60放置在

办公室拐角相对的位置，可以提供最大的信号覆盖范围。

无线安全

无线电波载无线设备与访问点之间传输提供无线设备与网络服务器之间的链接。无线网络通过无线电传输信息数据，无线电是公共传输介质，所以风险比较大。802.11标准中包括安全选项，防止您的信息被不必要的资源所截取。无线等效协议（WEP）与WPA（WiFi Protected Access）是现行使用的无线加密技术。无线加密只有用字无线设备与访问点之间。在访问点（AP）发送信息之前将其加密。FortiWiFi-60设置对以上两种技术均支持。

无线等效协议（WEP）

WEP安全技术在线设备与AP之间应用加密密钥。对于WEP安全技术，无线设备与AP必须使用相同的加密密钥，而且需要无线用户与管理员手动输入密钥。密钥激活后，无线设备通过加密密钥使用RSA RC4密码对每帧数据加密。

WEP无线安全技术也存在缺陷。WEP密钥是静态的，必须在无线设备与AP中手动定期更改密钥。在一个小型的公司，或者拥有很少用户与AP的网络中，定期更改WEP密钥还不算什么问题。但是，在一个多用户与AP的网络，定期更改WEP密钥在网络管理中成为一项负担，而且潜在的引发错误。那么这样下去，密钥更改可能几个月甚至几年发生一次，给黑客很多大量的时间获取密钥访问网络。

在小型无线网络环境中，激活WEP安全密钥将会减少外部入侵进入您网络的机会。但是，如果能够定期更改WEP密钥，至少每星期或每月，无线网络将更加安全。

WPA

WPA的发展将要代替WEP标准，提供更高层次的无线网络数据保护。WPA能够提供两种认证方法，通过802.1X验证或预先共享密钥。

802.1X通过一个EAP服务器验证用户，例如一个RADIUS服务器在用户连接到网络之前对该用户进行验证。加密密钥不定期的更改减少了黑客利用密钥入侵网络的机会。

在网络搭建时，RADIUS服务器不是一个可行的选项，WPA也能够提供使用暂时密钥集成协议（TKIP）利用预共享密钥验证用户。使用TKIP，加密密钥在用户连接到无线网络时对其实行再加密。这样，对每个数据包就建立了一个唯一的密钥。能够更进一步确保数据的完整性，一个数据完整性代码（MIC: Message Integrity Code）将在每个数据包中合并。8位数据完整性代码通过从每帧数据中的MAC地址与数据加密并提供更安全的数据包传输。

WPA能够提供在线设备与AP之间更安全的数据传输保护。FortiWiFi-60设备支持WPA两种用户验证的方法。

其它的无线网络安全方式

FortiWiFi-60设备具有其它措施保障无线网络的安全。您可以屏蔽一些不必要的用户对您无线网络的访问。通过设置几项额外的配置，确保您的网络以及信息的安全。

MAC地址过滤

为了加强无线网络的安全，在FortiWiFi-60设备中可以启动MAC地址过滤。通过启动该功能，您可以定义无线设备使用系统MAC地址访问网络。当一个用户试图访问无线网络时，FortiWiFi-60设备根据您建立的MAC地址列表查看用户的用户的MAC地址。如果列表中没有用户地址的记录，用户对无线网络的访问将被拒绝。MAC地址过滤功能对黑客使用随便的MAC地址访问网络或骗取MAC地址访问网络的机率。

服务设置标识符（SSID）

服务设置标识符（SSID）是无线网络中所有用户共享的网络名称。无线用户应该设置其计算机设备与播放其网络名称的网络连接。为了网络安全，不要将默认的“fortinet”作为网络名称。

网络名称播放可以使无线用户找到使用网络。FortiWiFi-60设备中的功能选项可以设置不播放SSID。这提供了额外的安全保护。如果您配置所有的无线用户使用正确的SSID，则不需要启动SSID播放。

撤消SSID

1. 进入系统>无线>设置。
2. 在SSID选项中选中“撤消”功能框。
3. 点击OK确认。

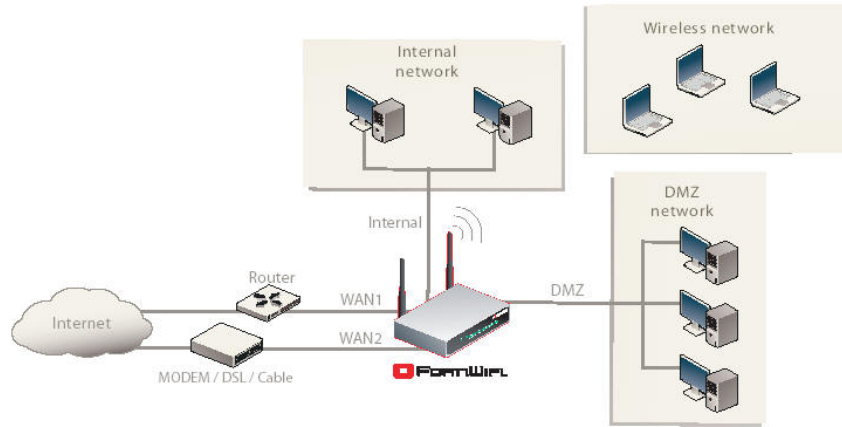
FortiWiFi-60设备操作模式

FortiWiFi-60设备在无线网络中具有两种操作模式：访问点（AP）与用户（Client）。

访问点（AP）模式

FortiWiFi-60设备运行于AP模式时，作为一个无线用户能够连接到的访问点，通过该访问点无线用户发送与接收信息。该模式下，多个无线网络用户在与FortiWiFi-60没有建立物理连接的情况下访问网络。FortiWiFi-60能够连接到内部网络并作为防火墙设备在网络中生效。AP模式是设备默认的模式。

图17：运行于AP模式的FortiWiFi设备

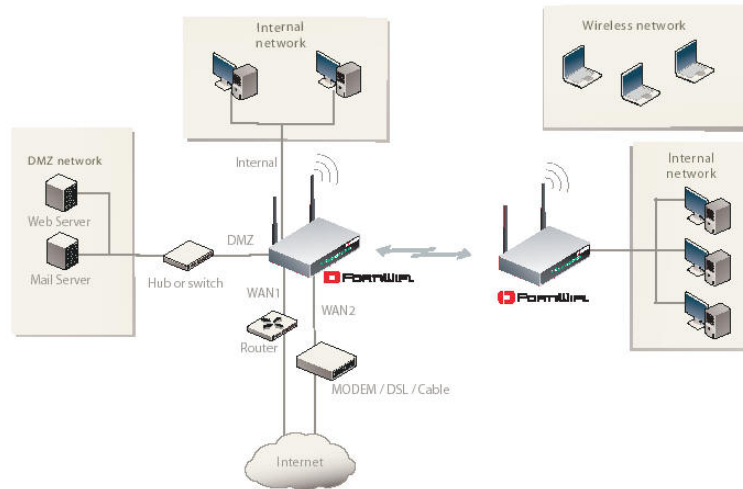


用户模式

FortiWiFi-60设备运行于用户模式时，作为一个数据接收设备从其它访问点接收数据。该设置可以使您利用无线网络协议从没有有线设施的位置连接到远程用户。

举例说明，仓库中，货物的发送与接收分别在库中对角的位置，仓库中的环境不适合搭建有线。这个时候，FortiWiFi-60设备可以支持有线用户使用四个Ethernet接口，连接到其它无线网络中的访问点（AP）。该连接可以使用802.11无线标准作为主干网与有线网络中的用户连接。

图18：运行于用户模式的FortiWiFi-60/60M设备



更改操作模式

1. 进入系统>无线>设置。
2. 在操作模式中，点击“更改”。
3. 选择操作模式，并点击“更改”。

在网络中配置FortiWiFi-60设备作为访问点（AP）

本节是有关如何快速配置FortiWiFi-60作为一个AP，允许处于同一个无线LAN网络中的作为无线工作站的设备对网络的访问。以及如何配置防火墙策略以及无线安全防护提供安全的无线网络环境。在初始建立时，使用内网中一个桌面计算机将TCP/IP设置为一个DHCP用户。

包括以下配置步骤：

- 配置DHCP设置
- 设置安全选项
- 配置防火墙策略

配置DHCP设置

对FortiWiFi-60设备的WLAN接口配置一个DHCP服务器。作为一个DHCP服务器，接口可以自动对与WLAN接口连接的主机分配地址。

配置FortiWiFi-60/60M作为一个DHCP服务器

1. 进入系统>DHCP>服务。
2. 点击蓝色三角扩展WLAN选项。
3. 配置DHCP服务器设置：

名称：	输入DHCP服务器的名称。例如，DHCPserver_1。
启动：	选中DHCP服务器选项。
类型：	除非您配置了远程用户端对WLAN接口使用IPSec VPN连接，设置为regular（常规）。
IP范围：	输入WLAN网络的IP地址范围。例如10.10.80.1到10.10.80.20。
掩码：	输入您在表9中设置的掩码。
域名：	设置域名，例如： www.fortinet.com 。
租期	IP地址过期时间。该选项说明地址是无限时或有限时使用。
高级选项	用于对接口设置几个DNS服务器（包括WIN服务器）。

4. 点击OK确认。



注意：IP地址范围必须与子网中接收到的DHCP服务器请求的地址相匹配。

设置安全选项

设置FortiWiFi-60设备的安全选项，确保对网络的安全进行保护。

设置数据安全

1. 进入系统>无线>设置。
2. 输入SSID。
3. 设置启动或撤消“SSID播放”。
4. 选择“安全模式”。
5. 根据所选择的“安全模式”，输入密钥或预先共享密钥。
6. 点击“MAC过滤”栏目。
7. 启动“MAC过滤”。
8. 输入MAC地址并对每个地址设置无线网络“允许”该地址通过，或“拒绝”该地址的访问。



注意：步骤2与5的设置，同样需要无线网络中的用户作同样的设置，才能够连接到无线网络。



注意：强烈建议请不要将这些设置项保留为空，这样容易给黑客造成攻击的机会。

配置防火墙策略

FortiWiFi-60设备中带有到互联网连接的WAN接口。通过该接口，您可以配置内网中有线网络和/或外网中的DMZ接口与无线网络与互联网连接。

您可以创建防火墙策略控制从WLAN接口到WAN1或WAN2接口的流量，对无线用户提供安全的互联网访问。

以下是对无线用户（WLAN接口）到互联网（WAN1 接口）之间的流量创建了防火墙策略，控制网络流量、防火墙验证以及默认的“严格型”内容过滤。

创建防火墙策略

1. 进入防火墙>策略。
2. 点击WLAN到WAN1的蓝色箭头。
3. 点击“新建”。

配置以下设置：

接口/区域源地址	WLAN
接口/区域目标地址	WAN1
地址名称源地址	全部
地址名称目标地址	全部
时间表	总是
服务	任何
动作	接受
NAT	启动
保护内容表	严格

4. 点击“高级选项”。
5. 点击“流量控制”。
6. 根据需要，配置带宽以及流量优先级设置。
7. 点击“OK”。

FortiGate固件

Fortinet公司定期更新Fortigate设备固件加强其性能与锁定问题并诊断的功能。FortiGate设备注册完成后，便可以从fortinet网站的技术支持中心<http://support.fortinet.com> 下载FortiGate设备固件。只有具有对系统模块读和写权限的管理员与设备admin用户可以更改FortiGate设备固件。

本章包括以下内容：

- [升级为新的固件版本](#)
- [恢复为旧的固件版本](#)
- [使用CLI在系统重启过程中安装固件镜像](#)
- FortiUSB密钥
- [在安装前检测新的固件镜像](#)
- [安装并使用备份的固件镜像（只适用于FortiGate-100A）](#)



注意：如果FortiGate设备中的固件是较老的版本，例如FortiOS v.2.50版，在升级到FortiOS v.3.0版之前请先升级到v.2.80。

升级为新的固件版本

使用基于web的管理器或CLI升级为新的FortiOS固件版本或者同一固件版本的较新的子版本。



注意：安装固件替代您现行的防病毒与攻击定义。安装固件后，确保防病毒与攻击定义已经更新。。

详细信息，参见*FortiGate 设备管理员使用手册*。



注意：执行以下步骤之前，确认您可以登录使用管理员帐户，或拥有系统配置读写权限的管理员帐户。

使用基于web的管理器升级固件

- 1.将固件镜像文件拷贝到您的管理计算机
 - 2.登录基于web的管理器页面
 - 3.进入**系统管理>状态**。
 - 4.**系统选项>固件版本**选项下，点击“升级”。
 - 5.输入固件镜像文件的路径与文件名，或点击“浏览”查找文件的位置。
 - 6.点击OK确认。
- FortiGate设备上传固件镜像文件、升级到新的固件版本、重新启动并显示FortiGate登录页面。该操作过程将花费几分钟的时间。
- 7.登录基于web的管理器。
 - 8.进入**系统管理>系统状态**，并检查固件版本确认新固件升级成功
 - 9.升级防病毒与攻击定义。有关升级防病毒与攻击定义的详细信息，参见*FortiGate 设备管理员使用手册*。

使用CLI升级固件

使用以下步骤时，您须配备一台FortiGate设备能够连接到的TFTP服务器。



注意：新的固件安装后将替代您现行的防病毒与攻击定义。因此，新的固件安装完成后，请进行更新防病毒与攻击定义。您也可以使用CLI命令`execute update-now`进行防病毒与攻击定义的更新。详细信息，参见*FortiGate 设备管理员使用手册*。



注意：执行以下步骤，您必须使用管理员帐户，或拥有系统配置读写权限的管理员帐户登录设备。

使用CLI升级固件

- 1.确定TFTP服务器已运行。
- 2.将新的固件镜像拷贝到TFTP服务器的根目录。
- 3.登录CLI。

4.确定FortiGate设备能够连接到TFTP服务器。

您可以ping一下FortiGate设备是否连接到TFTP服务器。例如，如果TFTP服务器的IP地址是192.168.1.168，那么执行以下命令：

```
execute ping 192.168.1.168
```

5.输入以下命令将固件镜像从TFTP服务器拷贝到FortiGate设备：

```
execute restore image <name_str> <tftp_ip4>
```

<name_str>输入固件镜像名称，<tftp_ip>输入TFTP服务器的IP地址。

例如：如果固件镜像文件名称是FGT_3000-v3.0-build183-FORTINET.out，TFTP服务器的IP地址是192.168.1.168，那么输入：

```
execute restore image FGT_3000-v3.0-build183-FORTINET.out  
192.168.1.168
```

FortiGate设备显示以下信息：

```
This operation will replace the current firmware version!
```

```
Do you want to continue? (y/n)
```

6.键入y（是）。

FortiGate设备上传固件镜像文件，升级到新的固件版本并重新启动。该操作过程将花费几分钟时间。

7.重新连接到CLI。

8.确认固件镜像安装成功，输入

```
get system status
```

9.升级防病毒与攻击定义（参见*FortiGate 设备管理员使用手册*）或进入CLI输入：

```
execute update-now
```

恢复为旧的固件版本

以下操作可以将FortiGate设备固件恢复到旧的版本。

使用基于web的管理器或CLI操作可以恢复为旧的固件版本。该操作将

FortiGate设备恢复为出厂默认配置。
使用基于web的管理器恢复为旧的固件版本

以下操作将FortiGate设备恢复为出厂默认的配置并删除IPS自定义特征、网页内容列表、邮件过滤列表以及对替换信息所作的修改。
执行该操作之前，建议您：

- 备份FortiGate设备配置。
 - 备份IPS自定义特征。
 - 备份网页内容与邮件过滤列表。
- 详细信息，参见*FortiGate 设备管理员使用手册*。
恢复为旧的FortiOS版本（例如，从FortiOSv3.0恢复到FortiOSv2.80版本），从备份的配置文件中，不能恢复旧版本的配置。



注意：新的固件安装后将替代设备现运行的防病毒与攻击定义。新的固件安装成功后，请下载更新防病毒与攻击定义。
详细信息，参见*FortiGate 设备管理员使用手册*。



注意：执行以下步骤，您必须先登录使用管理员帐户，或拥有系统配置读写权限的管理员帐户。

使用基于web的管理器恢复为旧的固件版本

1. 拷贝固件镜像到管理计算机
2. 登录到FortiGate基于web的管理器
3. 进入**系统管理>状态**。
4. 在**系统信息>固件版本**菜单项下，点击“升级”。
5. 键入固件镜像文件的路径与文件名，或点击“浏览”查找文件。
6. 点击OK确认。

FortiGate设备上传固件镜像文件，恢复为旧的固件版本，重新设置配置并重新启动，同时显示FortiGate登录页面。该操作过程将花费几分钟时间实现。

7. 登录基于web的管理器。
8. 进入**系统管理>系统状态**并检查固件版本，确认固件安装成功。
9. 恢复配置。

有关恢复配置的详细信息，参见*FortiGate 设备管理员使用手册*。

10. 更新防病毒与攻击定义。
有关防病毒与攻击定义更新的详细信息，参见*FortiGate 设备管理员使用手册*。

使用CLI恢复为旧的固件版本

该操作将FortiGate设备恢复为出厂默认的配置，并删除IPS自定义特征，网页内容列表，邮件过滤列表以及对替换信息所作的修改。
执行该操作之前，建议您：

- 使用命令execute backup config备份FortiGate设备系统配置
- 使用命令execute backupipsuserdefsig备份FortiGate设备系统配置
- 备份网页内容与邮件过滤列表

详细信息，参见*FortiGate 设备管理员使用手册*。

恢复为旧的FortiOS版本（例如，从FortiOSv3.0恢复到FortiOSv2.80版本），从备份的配置文件中，不能恢复旧版本的配置。



注意：安装固件替代您现行的防病毒与攻击定义。安装您的固件后，确保防病毒与攻击定义已经更新。您也可以使用CLI命令execute update-now进行防病毒与攻击定义的更新。

详细信息，参见*FortiGate 设备管理员使用手册*。



注意：执行以下步骤，您必须先登录使用管理员帐户，或拥有系统配置读写权限的管理员帐户。

执行以下操作，您须配备一台FortiGate设备可以连接到的TFTP服务器。

使用CLI恢复为旧的固件版本

- 1.确定TFTP服务器已运行。
- 2.拷贝固件镜像文件到TFTP服务器的根目录。
- 3.登录到CLI。
- 4.确定FortiGate设备能够连接到TFTP服务器。

您可以ping一下FortiGate设备是否连接到TFTP服务器。

例如，如果TFTP服务器的IP地址是192.168.1.168，那么执行以下命令：

```
execute ping 192.168.1.168
```

- 5.输入以下命令将固件镜像从TFTP服务器拷贝到FortiGate设备：

```
execute restore image <name_str> <tftp_ip4>
```

<name_str>输入固件镜像名称，<tftp_ip>输入TFTP服务器的IP地址。

例如：如果固件镜像文件名称是FGT_3000-v3.0-build183-FORTINET.out，TFTP服务器的IP地址是192.168.1.168，那么输入：

```
execute restore image FGT_3000-v3.0-build183-FORTINET.out  
192.168.1.168
```

FortiGate设备显示以下提示信息：

```
This operation will replace the current firmware version!
```

```
Do you want to continue? (y/n)
```

- 6.键入y。

FortiGate设备上传固件镜像文件。文件上传之后，类似以下的提示信息显示：

```
Get image from tftp server OK.
```

```
Check image OK.
```

```
This operation will downgrade the current firmware version!
```

```
Do you want to continue? (y/n)
```

- 7.键入y。

FortiGate设备恢复到旧的固件版本、恢复为出厂默认设置并重新启动。该操作过程将花费几分钟时间。

- 8.重新连接到CLI。

9. 输入命令get system status，确认新的固件镜像已经安装。

- 10.如需要，使用命令execute restore config <name_str> <tftp_ip4>恢复

为以前配置。

11.更新防病毒与攻击定义

详细信息，参见*FortiGate 设备管理员使用手册*，或在CLI中输入execute update-now。

使用CLI在系统重启过程中安装固件镜像

该操作可以安装指定的固件镜像并将FortiGate设备恢复为默认的设置。您可以使用该操作升级为新的固件版本、恢复为旧的固件版本或重新安装现运行的固件版本。如要执行以上所述操作，您须使用FortiGate console端口与交叉线连接到CLI。该操作将FortiGate设备恢复为出厂默认的配置。



注意：不同的版本的FortiGate BIOS中这一操作略有不同。这些不同将在向牵涉的步骤中说明。重启FortiGate设备时，BIOS版本号会在Console连接的命令行中显示。

执行该操作时，您需要：

- 使用RJ-45到DB-9线连接到FortiGate console控制台接口，访问CLI。
- 安装一台您能够从FortiGate内部接口连接到的TFTP服务器。TFTP服务器应与内部接口处于同一子网中。

执行该操作前，建议您：

- 备份FortiGate设备配置
- 备份IPS自定义特征
- 备份网页内容与邮件过滤

详细信息，参见*FortiGate 设备管理员使用手册*。

恢复为旧的FortiOS版本（例如，从FortiOSv3.0恢复到FortiOSv2.80版本），从备份的配置文件中，不能恢复旧版本的配置。

系统重新启动过程中安装固件

- 1.使用RJ-45到DB-9线与FortiGate console端口连接到CLI。
- 2.确定TFTP服务器已经运行。
- 3.新的固件镜像文件拷贝到TFTP服务器的根目录。
- 4.确定内部接口与TFTP服务器连接的是同一网络。
- 5.使用以下操作ping FortiGate设备是否连接到TFTP服务器。例如，如果TFTP服务器的IP地址是192.168.1.168，执行命令：

```
execute ping 192.168.1.168
```

- 6.输入execute reboot命令重新启动FortiGate设备，FortiGate设备显示以下提示信息：

```
This operation will reboot the system!
```

```
Do you want to continue? (y/n)
```

- 7.键入y

FortiGate设备启动时，显示一系列的启动信息。当以下信息之一出现时：

- 运行v2.xBIOS的FortiGate设备

```
Press Any Key To Download Boot Image....
```

- 运行v3.xBIOS的FortiGate设备

Press any key to display configuration menu.....

按任意键中断系统启动。



注意： 3秒内按任意键。如果您没有按下任意键，FortiGate设备继续重启过程，您须重新登录CLI并重复输入execute reboot命令。

如果您成功中断了重启过程，将显示以下信息之一：

·运行v2.xBIOS的FortiGate设备

Enter TFTP Server Address [192.168.1.168]:

转入步骤 9

·运行v3.xBIOS版本的FortiGate设备

[G]: Get firmware image from TFTP server.

[F]: Format boot device.

[Q]: Quit menu and continue to boot with default firmware.

[H]: Display this list of options.

输入 G, F, Q, 或 H:

8.键入G从TFTP服务器进入新的固件镜像

显示以下信息：

Enter TFTP server address [192.168.1.168]:

9.键入TFTP服务器的IP地址并按Enter键：

显示如下信息：

Enter Local Address [192.168.1.188]:

10.键入FortiGate设备用来连接到TFTP服务器的IP地址。该IP地址可以是与该网络接口连接的任何有效的地址。确定您没有误输入该网络中其他设备的IP地址。

显示一下信息：

Enter File Name [image.out]:

11.输入固件镜像文件名并按Enter键。

TFTP服务器上上传固件镜像到FortiGate设备并显示信息：

·运行v2.xBIOS的FortiGate设备

Do You Want To Save The Image? [Y/n]

键入Y

·运行v3.xBIOS版本的FortiGate设备

Save as Default firmware/Run image without saving:[D/R]

或

Save as Default firmware/Backup firmware/Run image without saving: [D/B/R]

12.键入D

设备安装新的固件镜像并重启启动。安装过程需要持续几分钟时间。

恢复新的固件安装之前的配置

如需要，可以更改内部接口地址。您可以在CLI中执行以下命令：

```
config system interface
  edit internal
    set ip <address_ip4mask>
```




```
set allowaccess { ping https ssh telnet http }
end
```

更改接口地址后，您可以通过基于web的管理器访问FortiGate设备并恢复配置。

详细信息，参见*FortiGate 设备管理员使用手册*。

恢复为旧的FortiOS版本（例如，从FortiOSv3.0恢复到FortiOSv2.80版本），从备份的配置文件中，不能恢复旧版本的配置。

FortiUSB 密钥

FortiUSB 密钥在备份配置文件或着安装新的固件镜像方面提供了较高的灵活性与可操作性。

FortiUSB具有自动安装功能，可以系统重新启动过程中自动安装配置文件与镜像文件。USB自动安装功能使用存储在FortiUSB密钥中的配置文件与固件镜像，在系统重新启动时查找并确定是否需要安装这些文件。如需要，FortiGate设备从FortiUSB中直接将配置文件与固件镜像文件安装在系统中。



注意： FortiUSB需单独购买。FortiGate设备只支持Fortinet公司售出的FortiUSB。

从FortiGate设备上插拔FortiUSB

使用以下步骤操作插拔FortiUSB，使FortiGate设备能够识别FortiUSB。按照操作从FortiGate设备移除FortiUSB，确保USB中存储的文件不被损坏或非正常性丢失。



注意： 如果安插了FortiUSB，FortiGate设备从闪存中启动。如果启动了USB自动安装功能，设备将检查是否有不同的镜像或配置文件需要安装。

正确安插FortiUSB密钥

1. 用CLI命令关闭FortiGate设备。
2. 显示以下信息后，将设备断电：
The system is halted
3. 将FortiUSB插入USB接口。
4. 将FortiGate设备接电，重新启动系统。

FortiUSB插入FortiGate设备中。

正确移除FortiUSB密钥

1. 用CLI命令关闭FortiGate设备。
2. 显示以下信息后，将设备断电：
The system is halted
3. 将FortiUSB拔出。
4. 将FortiGate设备接电，重新启动系统。

使用FortiUSB备份与恢复固件镜像

您可以使用FortiUSB密钥备份现运行的固件镜像或是恢复使用以前的镜像。您也可以加密备份在您PC机或FortiUSB的配置文件。执行以上操作时，确保FortiUSB已经插入到FortiGate设备的USB接口。请在拔出FortiUSB密钥之前，确认FortiGate设备已经关闭。该操作是确定系

统识别FortiUSB从FortiGate设备中拔出。



注意：如果加密固件文件，您只可以保存VPN证书。确保启动了配置加密程序，那样您可以将VPN证书与配置文件一起保存。

使用基于web的管理器备份FortiGate设备配置

- 1.进入系统>维护>备份与恢复。
- 2.将所要备份的配置文件加入USB磁盘列表中。
- 3.点击“备份”。

如果需要加密配置文件，点击“加密”并输入密码后点击“备份”。该密码在恢复文件时使用。

使用基于web的管理器恢复FortiGate设备配置

- 1.进入系统>维护>备份与恢复。
- 2.从USB磁盘中选出所要恢复的配置文件
- 3.从列表中选择已经备份的配置文件
如果对配置文件进行了加密，输入密码。
- 4.点击恢复“恢复”

使用CLI备份配置文件

- 1.登录到CLI
- 2.输入以下命令备份配置文件：
`exec back config usb<filename>`
3. 输入以下命令查看配置文件是否备份到了密钥中
`Exec usb-disk list`

使用CLI恢复配置文件

- 1.登录到CLI
- 2.输入以下命令恢复配置文件
`exec restore image usb<filename>`

FortiGate系统回馈以下信息：

This operation will replace the current firewear version!

Do you want to continue?(y/n)

- 3.输入y


使用USB自动安装功能

您可以FortiUSB自动安装功能在系统重启的时候自动升级FortiGate配置文件与镜像。该功能可以在一个系统模块重新启动或关闭时运行现行的设置。

配置自动安装功能之前，您需要执行以下操作：

- 关闭FortiGate设备。
- 安装FortiUSB
- 启动FortiGate设备

以下步骤既可以通过使用基于web的管理器也通过CLI执行。建议使用CLI命令，在安装完成之前显示CLI登录信息时进入。如果安装了固件镜像或配置文件，FortiGate设备可能要重启两次。

 **注意：** 该功能需要用到不加密的配置文件，配置文件image.out与fgt_system.conf必须在根目录下。

 **注意：** 安装之前，请确定FortiGate设备已经安装了FortiOS v.30 MR 1。

使用基于web的管理器配置USB自动安装功能

- 1.进入系统>维护>备份与恢复。
- 2.点击蓝色箭头扩展“高级选项”。
- 3.选中以下信息：
 - 如果USB磁盘中有默认的配置文件名，在系统重启时自动升级FortiGate配置文件。
 - 如果USB磁盘中有默认的镜像，在系统重启时自动升级FortiGate固件镜像。
- 4.输入配置与镜像的文件名或使用默认的配置文件名（system.conf）与默认的镜像名称（image.out）。
- 5.点击应用“应用”。

使用CLI配置使用USB自动安装功能

- 1.登录CLI
- 2.输入以下命令：

```
config system auto-install
    set default-config-file <filename>
    set auto-insatll-config <enable/diable>


    set default-image-file<filename>
    set auto-install-image<enable/diable>
end
```
- 3.输入以下命令查看新的固件安装设置：

```
get system statue
```

配置FortiUSB密钥的其它CLI命令

当您要从FortiUSB密钥中删除文件，或列出密钥中存储的文件，包括格式化密钥或重命名文件时，可以使用以下CLI命令：

- exec usb-disk list
- exec usb-disk delete <filename>
- exec usb-disk format
- exec usb-disk rename <filename1><filename2>

 **注意：** 如果您试图通过CLI命令行接口删除配置文件，以及在所命名的文件名中包含空格时，在您删除FortiUSB密钥中的文件前您需要先将文件名加上引号扩展为CLI可以解析的命令。

安装固件之前测试新的固件镜像

在系统重启过程中安装固件镜像的时候可以检测新的镜像并将其保存在系统内存中。完成该操作后，FortiGate设备以当前配置运行使用新的镜像。新的镜像不是永久性的安装，下次FortiGate设备重启时，将

以当前的配置运行使用最初安装的固件镜像。如果新的镜像运行良好，您可以使用的“[升级为新的固件版本](#)”操作，永久安装使用该镜像。安装新镜像之前，使用以下操作测试新的固件镜像。执行该操作时，您需要使用FortiGate console接口与一根交叉线连接到CLI。该操作使用当前的配置，暂时性的安装新的固件镜像。

执行该操作时，您需要：

- 使用RJ-45到DB-9线与FortiGate console端口连接，访问CLI。
- 安装一台您可以通过FortiGate内部接口连接的TFTP服务器。TFTP服务器应与内部接口处于同一子网。

检测新的固件镜像

1.使用RJ-45到DB-9线与FortiGate console端口连接到CLI。

2.确定TFTP服务器运行。

3.将新的固件镜像拷贝到TFTP服务器的根目录。

4.确认内部接口与TFTP服务器连接的同一网段。

Ping一下FortiGate设备是否连接到TFTP服务器。例如，如果TFTP服务器的IP地址是192.168.1.168，执行命令：

```
execute ping 192.168.1.168
```

5.输入以下命令重新启动FortiGate设备：

```
execute reboot
```

6.FortiGate设备重启时，按任意键中断系统启动。FortiGate设备重启时，显示一系列的启动信息：

·运行v2.x BIOS的FortiGate设备

```
Press Any Key To Download Boot Image.
```

·运行v3.x BIOS的FortiGate设备

```
Press any key to display configuration menu.
```

7. 按任意键立即中断系统启动。



注意： 3秒内按任意键将中断设备重新启动。如果您没有按下任意键，FortiGate设备继续重启过程，您须重新登录CLI并重新输入execute reboot命令。

如果您成功中断启动过程，将显示以下信息之一：

·运行v2.x BIOS的FortiGate设备

```
enter TFTP Server Address: [192.168.1.168]:
```

转入步骤 9

·运行v3.x BIOS的FortiGate设备

```
[G]: Get firmware image from TFTP server.
```

```
[F]: Format boot device.
```

```
[Q]: Quit menu and continue to boot with default firmware.
```

```
[H]: Display this list of options.
```

输入 G, F, Q, 或 H:

8.键入G从TFTP服务器获得新的固件镜像，显示以下信息：

```
Enter TFTP server address [192.168.1.168]:
```

9.输入TFTP服务器的IP地址并按Enter键：

显示如下信息：

```
Enter Local Address [192.168.1.188]:
```

10.键入一个FortiGate设备用以连接TFTP服务器的IP地址。

该IP地址须是与TFTP服务器处于同一网段的地址。查看该IP地址，确

认没有误输入网络中其他设备的IP地址。

显示以下信息：

Enter File Name [image.out]:

11. 输入固件镜像文件名并按Enter键。

TFTP服务器上上传固件镜像到FortiGate设备并显示信息：

·运行v2.x BIOS的FortiGate设备

Do You Want To Save The Image? [Y/n]

键入n

·运行v3.x BIOS的FortiGate设备

Save as Default firmware/Run image without saving: [D/R]

或



Save as Default firmware/Backup firmware/Run image without saving: [D/B/R]

12. 键入R

FortiGate镜像安装在系统内存中，FortiGate设备以当前的配置启动运行新的固件镜像。

13. 您可以使用任何管理帐户登录到CLI或基于web的管理器。

14. 在CLI中键入get system status确认新的固件镜像已经安装。

如需要，您可以检测新的固件镜像。

安装并使用备份固件镜像



以下步骤只适用于 FortiGate-100A。

如果设备运行于BIOS 3.X版本，您可以安装一个备份固件镜像。安装了备份固件镜像后，您可以在需要时切换到备份镜像。

安装备份固件镜像

执行该操作之前，您需要：

- 使用RJ-45到DB-9线与FortiGate console端口连接到CLI。
- 安装一个您可以从FortiGate设备可以连接到的TFTP服务器。

安装备份固件镜像

1. 使用RJ-45到DB-9线与FortiGate console端口连接到CLI。
2. 确定TFTP服务器已运行。
3. 拷贝一份附件镜像文件到您TFTP服务器的根目录。
4. 确定FortiGate设备能够连接到TFTP服务器，使用以下命令去Ping运行TFTP服务器的设备。例如，如果TFTP服务器的IP地址是192.168.1.168。那么执行以下命令：
execute ping 192.168.1.168
5. 输入以下命令重新启动FortiGate设备。
execute reboot
设备重新启动，显示一系列的启动信息，在其中一条显示为：
press any key to enter configuration menu.....
6. 此时按任意键中断系统重启。



注意：您只有三秒钟按下任意键的时间。如果您不能尽快按任意

键中断系统重启，您必须重新登录并再一次输入execute reboot命令。

[G]: Get firmware image from TFTP server.

[F]: Format boot device.

[Q]: Quit menu and continue to boot with default firmware.

[H]: Display this list of options.

输入 G, F, Q, 或 H:

7.键入G从TFTP服务器获得新的固件镜像，显示以下信息：

Enter TFTP server address [192.168.1.168]:

8.输入TFTP服务器的IP地址并按Enter键：

显示如下信息：

Enter Local Address [192.168.1.188]:

9.键入一个FortiGate设备用以连接TFTP服务器的IP地址。

该IP地址须是与TFTP服务器处于同一网段的地址。查看该IP地址，确认没有误输入网络中其他设备的IP地址。

显示以下信息：

Enter File Name [image.out]:

10. 输入固件镜像文件名称，并按Enter键。

TFTP服务器上传固件镜像到FortiGate设备，并显示以下信息：

Save as Default firmware/Backup firmware/Run image without saving:
[D/B/R]

11. 键入B。

FortiGate设备保存备份固件镜像并重新启动。FortiGate设备重新启动并运行先前安装的固件版本。