FortiOS 升级手册

www.fortinet.com

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

介绍

FortiNet 公司在研发与更新其 FortiGate 防火墙设置的同时，一直注重开发、测试与优化 FortiGate 设备的操作系统。FortiOS 3.0 是基于之前的系统之上，更高效可靠的操作信息，对网络实现更好的屏蔽与监控功能。

升级说明中对 FortiOS3.0 操作系统以及升级后可能对当前配置造成的问题。FortiOS3.0 中新增加的功能，以及对现有系统功能的改进，您需要了解升级到 FortiOS 可能对当前的配置产生的影响。本手册还对备份当前配置以及在 FortiGate 设备中安装 FortiOS3.0 系统进行了说明。

本手册还包括 FortiOS 固件发布的信息。

关于本手册

本手册包括以下章节：

- 升级说明--- FortiOS 系统中对之前系统中一些功能的更改以及新增加的功能说明。
- 新增功能与功能的更改----基于 FortiOSv2.80MR11，升级到 FortiOS3.0 后功能性的更改与加强。
- 更改固件版本---- 对如何安装 FortiOS 系统以及将系统恢复到 FortiOS2.80MR11 的操作进行了说明，包括有关 FortiOS3.0 系统的说明、如何备份当前配置设置、升级后重新建立连接以及升级成功后的校验。
- 有关 FortiOS 3.0MR2 ---- FortiOS 3.0MR2 中新增的功能以及功能的更改。
- 有关 FortiOS 3.0MR3 ---- FortiOS 3.0MR3 中新增的功能以及功能的更改。
- 有关 FortiOS 3.0MR4 ---- FortiOS 3.0MR4 中新增的功能以及功能的更改。

Fortinet 公司技术文档

有关Fortinet公司产品最新的消息发布以及产品手册使用说明，可以访问Fortinet公司技术支持网站http://kc.forticare.com.

技术文档 CD

有关Fortinet公司产品最新的消息发布以及产品手册使用说明，可以访问Fortinet 公司技术支持网站 http://kc.forticare.com. 访问 http://docs.forticare.com/fgt5k.html.获得有关FortiGate-5000 系列文档。

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.forttinet.com）中的知识库获得。知识库涉及 fortinet 产品故障排除与解释

说明性的文章，FAQ，技术说明等。

FortiGate 设备日志信息参考只能够从 Fortinet 知识库中获得。日志信息参考就有关 FortiGate 设备生成的日志信息的结构，以及所生成日志所说明的信息。

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 。

客户服务与技术支持

Fortinet 技术支持将确保您的Fortinet产品在您设置的网络中能够快速启动，轻松配置并可靠运行。

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

设备注册

通过 FortiGate 设备注册，您可以接收例如产品更新以及技术支持这样的用户服务。只有通过产品注册才可以获得 FortiGuard 服务，如反病毒与入侵保护升级、web 过滤与反垃圾邮件服务。

安装新的FortiGate设备后，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。您可以在注册栏中同时注册购买的 FortiGate 系列设备，而无需重复输入联系信息。

升级说明

下载 3.0 版的 FortiOS 操作系统之前，建议您参看本章节的内容说明，了解新版操作系统的新功能、对现有系统的改进以及与现有系统比较操作上的不同。

新增加的与修改的 CLI 命令，请查看 *FortiGate 设备 CLI 使用参考手册*以及 *FortiGate 设备管理员操作手册*。

本章包括以下内容：

- 配置文件备份
- 安装向导
- FortiLog 设备名称的更改
- LCD 显示信息更改
- 基于 web 的管理器更改
- 基于 web 管理器功能的变化
- CLI 命令更改
- FortiUSB
- 公知信息

配置文件备份

您可以备份未加密或加密的配置文件。对于备份未加密的文件，FortiGate 设备将以明文格式保存文件，选择加密的设置后，保存 VPN 证书。

安装向导

不设置安装向导提示。

FortiLog 设备名称的更改

FortiLog 设备在 FortiOS3.0 中更名为 FortiAnalyzer。FortiAnalyzer 设备名更能诠释设备的用途，即强劲的报告与日志记录与分析功能。

LCD 显示信息更改

升级为 FortiOS 3.0 后，FortiGate 设备 LCD 中显示的主菜单信息更改如下：

图 1：NAT/路由模式下主菜单 LCD 显示信息

图 2：透明模式下主菜单 LCD 显示信息

基于 web 管理器更改

FortiOS 系统面板功能进行了加强，各种系统信息进行了集成归类并增加了新的功能以便能够好的监控 FortiGate 设备。

图 3：FortiGate-60 设备中基于 web 的管理器显示面板

系统信息		
	序列号	FortiGate 设备序列号。
	运行时间	FortiGate 设备已经运行的时间。
	系统时间	根据时区设置，系统显示的当前时间。
	设备名称	FortiGate 设备名称。点击“更新”可以更改设备名称。
	固件版本	当前使用的固件版本。点击“更新”可以安装新的固件。
	操作模式	设备运行的模式。点击“更新”可以切换设备的操作模式。
系统资源		

	CPU 使用率	CPU 的使用率。
	内存使用率	内存使用率。
	FortiAnalyzer 设备使用率	FortiGate 设备与 FortiAnalyzer 设备连接时，FortiAnalyzer 设备中可用的报告与日志存储的空间。
	以上所述系统资源使用的历史记录可以点击“系统资源”区域中右上角中“历史记录”查看。	
许可证信息		
	支持合同	支持合同的版本号与过期时间。
	FortiGuard 服务注册	FortiGate 设备注册申请的 FortiGuard 服务，以及是否需要升级或是否已经过期。
报警信息	显示系统报警信息，包括固件升级或降级，以及系统重启信息。控制台也显示如果反病毒引擎在具体的时间段内存较低的报警信息。	
统计表	显示内容存档以及攻击日志的详细信息。	

基于 web 管理器主页面中右上角显示有 FortiGate 设备的映像，以及设备端口设置的状态。当您将鼠标停留在设备端口时，显示端口名称、IP/掩码地址、链接状态、速度以及发送与接收的数据包数量。如果端口没有连接，呈灰色显示；连接状态下，显示为绿色。当 FortiGate 设备没有连接到 FortiAnalyzer 设备时，FortiAnalyzer 设备映像显示为灰色。

基于 web 管理器的功能变化

FortiOS 3.0 中，几项功能与其他一些功能进行了合并。参见“新增的功能与功能更改”。

如果您需要查看这些新功能的详细信息，参见“*FortiGate 设备管理员使用手册*”。

CLI 命令的更改

命令行接口中的使用命令进行了更改，并添加了新的命令。参见 FortiGate 设备 CLI 参考手册获得更详细的信息。

FortiOS 2.8 版本中一些基于 web 管理器的功能转移到了 FortiOS 3.0 版本中使用 CLI 命令来实现。

FortiUSB 支持

FortiOS 3.0 支持 USB 的使用。使用 FortiUSB 密钥（单独购买）可以备份与恢复配置文件。以及配置 FortiGate 设备自动安装新的固件镜像，以及在设备重新启动时使用 USB 密钥恢复配置设置。

详细信息，参见您所使用的 FortiGate 设备型号对应的安装手册。

以下型号的 FortiGate 设备支持使用 FortiUSB 密钥：

- FortiGate-60/60M
- FortiWiFi-60
- FortiWiFi-60A/60AM
- FortiGate-100A
- FortiGate-200A
- FortiGate-300A
- FortiGate-400A
- FortiGate-500A
- FortiGate-800/800F
- FortiGate-5001SX
- FortiGate-5001FA2
- FortiGate-5002FB2

注意：FortiGate 设备只支持 Fortinet 公司生产的 FortiUSB 密钥。

公知信息

以下是一些您应该注意的公知信息，既不包括在以上所述的内容中以及“新增功能与功能更改”。除非另有说明，这些公知的信息将延续到其他 FortiOS 固件的版本中适用。

系统设置

以下信息说明，涉及基于 web 管理器与 CLI 管理工具中配置系统设置的操作。

- 日历显示为年月日（YYYY-MM-DD）格式。
- 进入“系统设置>状态>许可证信息>支持合同”，点击 FDS 注册链接。
- 只有 CLI 中可以链接到“提交 Bug 报告到 Fortinet”。
- 当夏令时在凌晨 2 点结束时，系统不能够自动调整时间。只有在一个小时后 3 点时系统才能够调整自动调整时间。当夏令时结束后，您应该人工重新设置系统时间。
- CLI 命令 execute backup log <ip><string>在没有安装硬盘的 FortiGate 设备中也可以使用。
- 当使用 TFTP 将 FortiOS 镜像上传到闪存中时，DHCP 租期数据库将保留在安装硬盘的 FortiGate 设备中。没有安装有硬盘的 FortiGate 设备不保留数据库。
- 当在非 root 虚拟域中启动 DNS 转发时，FortiGate 设备不转发 DNS 请求。
- 在备份与恢复页面中使用“导入 CLI”功能导入 CLI 命令时，不管导入是否成功，基于 web 管理器页面都显示为“成功导入”。
- FortiGate-1000A 与 FortiGate-5001FA2 设备中使用 diagnose hardware deviceinfo nic <FA2 ports>命令时，将产生 16 进制的输出。
- 替换因病毒感染需要屏蔽或隔离的文件信息时，替换信息中出现的 FortiLog 改为 FortiAnalyzer。
- 如果基于 web 管理器中管理语言设置为简体中文，会话过滤不能成功实现。

- 对虚拟域中 VLAN 接口的管理访问不在基于 web 的管理器中显示。CLI 中使用 get system interface <VLAN>命令可以实现该功能。
- FortiGate 设备不能兼容使用生成的 SSH 公共密钥。
- 如果 FortiGate 设备配置使用 FSAE，而后断开与 FSAE 的连接时，设备会发生内存泄露。
- 当您配置第二分区“上传并重启”时，在系统设置>维护选项下，FortiGate 设备不能实现上传第二镜像。设备重启时覆盖分区 1 中正在使用的镜像。CLI 中，输入 get system status 与 diagnose sys flash list 命令将显示冲突信息。
- FortiUSB 初始插入后，FortiGate 设备不能够自动配置与停止 FortiUSB 的活动。如果 FortiUSB 被停止或重新插入使用时，CLI 中将显示目录文件的列表；CLI 命令 execute backup usb <file>在没有安装 FortiUSB 的情况下是不能够报错的。
- 如果 WLAN 升级不成功，可能是无线后台程序关闭为了保存内存。
- 访问系统设置>无线>设置，当安全模式 WEP64 或 WEB128 设置为“无（None）”时，显示数据加密标签，而不是下拉菜单。当安全模式设置为 WPA 预先共享密钥或 WPA RADIUS，数据加密标签与下拉菜单同时可见。以上所述只适用于 FortiWiFi-60A/AM 设备。
- 对于 FortiOS 3.0MR1 或更高的版本，透明模式下的多播转发与 NAT/路由模式稍有不同。透明模式下，多播转发在默认情况下是启动的，可以通过 CLI 添加多播转发策略。详细信息访问 Fortinet 公司网站知识库中 “FortiOS 透明模式下的多播转发”与“增强的多播策略支持”的技术文章说明。
- 当配置 FortiGate 设备使用 PPPoE 连接 ISP 时，用户不能够访问某些网站。这种情况的发生是因为相比较标准以太网的 1500MTU，PPPoE 帧额外需要 8 个字节。当服务器发送较大的数据包，DF 位设置为 1 时，ADSL 服务商的路由器既不能发送“需要 ICMP 片段”的大数据包，或者数据包在沿着到 web 服务器的路径过程中被丢弃。这两种情况下，web 服务器根本不知道片段文件要到达用户端。

  CLI 中，在防火墙策略配置选项中使用 tcp-mss-sender 可以配置用户访问所有的网站。详细信息，参见 Fortinet 公司网站知识库中有关“使用 PPPoE 不能访问一些网站的问题说明”。
- 某些 IPS 组设置不能在升级后自动保持配置，您需要在升级后手工配置这些设置。在 FortiOS MR1 发布说明中附件 A，有关“IPS 组设置升级”的内容。
- FortiOS 2.8MR11 中的列表不能在FortiOS3.0 中恢复。请在升级前存档这些列表文件。如果使用基于web的管理器升级，这些列表文件将被保存。使用基于web的管理器升级后，通过web管理器或CLI都可以校验这些列表文件是否被保存。参见附件B---将FortiOS 2.80 中web过滤与垃圾邮件过滤列表影射到FortiOS CLI命令。查看Fortinet公司网站www.fortinet.com 知识库版块中“使用CLI命令选项导入 2.80 版本列表文件”将FortiOS 2.80 中的列表文件导入FortiOS 3.0。

防火墙

防火墙的设置的有关信息涉及到基于 web 的管理器与 CLI 这两个管理工具中应用的配置。

- 当具有相同外部 IP 地址的 VIP 已经存在时，在基于 web 的管理器中不能建立端口转发 VIP。
- CLI 命令 conf user adgrp 是配置 FortiGate 设备在 AD 服务器发送 AD 组到配置文件时，添加发送的 AD 组。如果一个 AD 服务器没有发送 AD 组，您手工添加条目时，基于 web 管理器中将不显示 Windows AD 页面。删除条目时，显示 Windows AD 页面。FortiGate 设备中一个 AD 不需要手工增加到 AD 组。
- 配置动态 IP 池后，防火墙>策略页面的下拉框中显示 ANY。ANY 并不是所支持的特性。
- 使用基于 web 的管理器不能够更改防火墙地址组的名称。

高可用性（HA）

高可用性，涉及在基于 web 管理器与 CLI 中的操作。

- 当 HA 群集运行于透明模式下的主动-主动模式下时，不同通过 VLAN 接口实现负载平衡。通过 HA 群集中主设备通信会话能够顺利进行，但是通过从属设备的会话将不能够连接。
- 如果一个端口作为聚合端口，FortiOS 允许选择这些端口中的一个作为 HA 心跳设备（hbdev）端口。该操作将中断 HA 连接。
- 当一台 FortiGate 设备作为 HA 群集中的从属设备，并运行于主动-主动模式时，邮件内容日志不能发送到 FortiAnalyzer 设备。
- 当 HA 群集中主设备的序列号在排列顺序上高于从属设备的序列号时，基于 web 的管理器不能够显示运行于 HA 模式下 HA 的统计数据。
- 当一个运行于主动-主动模式的 HA 群集发生故障时，新的主设备不能将日志邮件内容发送到 FortiAnalyzer 设备。
- 当一对冗余接口在从首要连接到备份连接失败时，备份连接将获得一个不同于之前首要连接使用的 MAC 地址。这种情况只发生在 HA 模式，并会导致 ARP 请求失败。
- 运行于主动-主动模式的从属设备不能发送邮件内容。
- 如果 FortiGuard 本地分类在 HA 群集配置之前，那么本地分类不能在 HA 群集设备之间同步。
- 在同一个虚拟群集中，通过不同物理接口形成的不同 VLAN 使用相同的虚拟 MAC 地址。
- 一个 HA 群集恢复配置时会丢失从属设备的名称、HA 优先级设置以及优越性设置。
- 使用基于 web 的管理器更改主设备的主机名称或优先级，偶尔这些设置的更改不能同步反映到从属设备。通过 CLI 更改主设备与从属设备的主机名称与优先级设置。
- 用户定义的 IPS 特征上传到主设备时，不能在从属设备中同步。必须重启从属设备以同步用户定义的 IPS 特征。
- 序列号为 FGT100A2905500001 的 FortiGate-100A 设备，与序列号为 FGT200A2905500001 的 FortiGate-200A 设备不能够加入其它序列号的 FortiGate-100A 与 FortiGate-200A 的设备组成的 HA 群集。举例说明，序列号为 FGT100A2905500001 的 FortiGate-100A 设备加入由序列号 FGT100A28704400001 组成的 HA 群集时，将不能够与 HA 群集设备建立连

接。

反病毒

反病毒设置，涉及在基于 web 管理器与 CLI 中的操作。

- 当一个 MSN 的用户通过 msn 发送受感染的病毒文件时，FortiGate 设备不发送配置的替代信息返回到用户。
- 反病毒监控需要在 CLI 中配置。
- 反病毒扫描、屏蔽与隔离在即时通信工具 AIM，MSN，Yahoo massager 与 ICQ 中进行文件传输时可用。

反垃圾邮件

以下所述是有关在 FortiOS2.8MR12 包括 FortiOS 3.0MR1 或更高版本的系统中反垃圾邮件列表顺序问题。

对于 SMTP：

- IP 地址 BWL 查看最后一跳 IP。
- RBL 与 ORDBL 查看最后一跳 IP。FortiGuard 反垃圾邮件查看最后一跳 IP HELO DNS 查询。
- MIME 报头检索，电子邮件地址 BWL 检索。
- 邮件主题的禁忌词汇检索。
- IP 地址 BWL 检索（从“已接收邮件”的报头中获取 IP 地址）。
- 在邮件正文中查看禁忌词汇。
- 退回的邮件进行 DNS 检索。FortiGuard 反垃圾邮件从报头获取公共 IP 地址进行 RBL 与 ORDBL 检索。

对于 POP3 与 IMAP：

- MIME 报头检索，邮件地址 BWL 检索。
- 对邮件主题进行禁忌词汇检索。
- IP 地址 BWL 检索。
- 对邮件正文进行禁忌词汇检索。
- 对回复邮件进行 DNS 检索。FortiGuard 反垃圾邮件从报头获取公共 IP 地址。进行 RBL 与 ORDBL 检索。

Fortinet 知识库中有关于反垃圾邮件过滤顺序技术文本的说明。

VPN

- 在基于 web 的管理器中，用户点击 VPN 显示图标时，VPN 通道并不亮起。
- SSL VPN 通道模式下，FortiGate 设备不能将 DDNS 主机名称表达为 IP 地址。
- FortiOS 2.8 中的 PING 发生器在 FortiOS3.0MR1 中以自动协商设置代替。
- 访问“VPN>IPSEC>监控器”，用于加亮显示拨号通道的图标并不能发亮显示 IPsec 拨号通道，但使用 CLI 命令 diagnose vpn tunnel flush 可以实现该功能。
- 标签条目被编辑后，将显示重新定向 URL 窗口。

- 当拨号服务器中 IPSec 阶段 1 对等 ID 改变后，没有任何 ISAKMP 删除通知发送到拨号用户端，以告知用户删除旧的 SA。当拨号用户端的对等 ID 更改时，发送 ISAKMP 删除通知。当阶段 1 对等 ID 更改后，对现有的拨号通道执行 diagnose vpn tunnel flush 命令。
- 对 IPSec 进行 Internet 浏览需要两个策略。

即时消息通信

即时通讯的公知信息只涉及到在基于 web 管理器中的操作。

- FortiGate 设备不能够屏蔽即时通讯用户之间 webcam/视频流量。即使启动了音频屏蔽功能，用户仍然能够发送与接收 webcam/视频信息。
- 运行于主动-主动模式的 HA 成员设备之间的即时通讯不能同步。这是因为 IM 用户之间的行为以及会话传输需要跨越多个 HA 主动-主动模式下的成员设备。根据 IM 的功能来讲，例如病毒扫描与登录屏蔽将不能实现。
- 以下所述情况在 FortiOS3.0MR1 支持的每个 IM 工具中都存在。

受影响的 即时工具用户	版本	描述
AIM	5.9.3797	● 用户使用非加密或加密 AIM 版本时，不能够与其它 AIM 用户进行视频连接。 ● 应用 AIM 加密时，不能实现到 AIM 对等用户的连接。这样的情况在所有 AIM 非加密与加密的用户中都存在。 ● 当一个 AIM 用户从另一个 AIM 用户接收文件时，FortiGate 文件数目统计将不增加。这样的情况在所有 AIM 非加密与加密的用户中都存在。
AIM	5.9.3861	● NetMeeting 使用 H.323 不能建立连接。这样的情况在所有 AIM 非加密与加密的用户中都存在。
AIM ICQ	5.9.3861 5.04	● 当 ICQ/AIM 使用其它端口（非 5190 端口）登录，登录被屏蔽的事件将不被记录在 FortiGate 设备的日志中。 ● 包含的日文的 IM 系统替换信息不能正常显示。 ● 用户文本信息内容在文本格式的即时消息内容日志中不显示。
ICQ	5.04	● 在 NAT 模式 FortiGate 设备之后的 ICQ 用户之间不能建立视频与音频会话。 ● 当用户建立聊天会话时，FortiGate 按协议区分的聊天会话统计并不增加。 ● FortiGate 设备之后的用户不能够与多个不同的防火墙产品后的 ICQ 用户进行多用户聊天连接。
MSN	7.0/7.5	● MSN 用户之间进行文件传输时，会发生意外超时现象。
MSN	7.5	● MSN 7.5 版本中，不能建立视频/音频通信。

Yahoo！Messenger	6.0.0.1922	● 当用户通过 FortiGate 设备对其它 MSN 用户发送消息时，会话统计计数不正确。
Yahoo！Messenger	7.0.2.120	● Yahoo!7.0 版本中，不能屏蔽音频通信。 ● 内容存档中，当用户使用 P2P 传输即时消息时，laddr 与 raddr 是错误的。

P2P

P2P 有关的问题，只涉及使用基于 web 管理器的操作。

- 在防火墙中配置的传输限值不能对 Gnutella 兼容。如果用户是 Gnutella 用户端，下载速度不能超过传输速率限值中规定的速度。
- FortiGate 设备不能在延长的期限过后，或者屏蔽 Skype 用户超过一天。
- 当 IPS Kazaa 特征设置为“丢弃”或“丢弃会话”，IPS 引擎将屏蔽 Kazza 流量，但是只限于很短的一段时间。所以持续试图通过防火墙连接到 Kazza 网络的用户也将在短时间内建立连接。
- 以下是 FortiOS 3.0MR1 所支持的 P2P 协议中发现的问题。

P2P 用户	版本	描述
Gnuleus/Limewire/Swapper.NET	2.2.0.0/4.9.3.7 4.6	配置 FortiGate 屏蔽具体使用某些协议传输的文件时，P2P 用户端仍然能够接收到部分下载的文件。
Xolox	2.0	配置 FortiGate 屏蔽文件传输后，等待 10 到 30 分钟后，P2P 用户仍然可以下载文件。

网页过滤

网页过滤涉及到基于 web 管理器与 CLI 中的操作。

- 当用户使用基于 web 的管理器更改用户组 web 跳过属性时，防火墙不能够马上实施该设置更改。
- 配置了禁忌词汇与禁忌词汇免除条目后，二者之间的事件日志会不同。
- 在一个非根 VDOM 中，使用基于 web 的管理器不能够在保护文件中启动 FortiGuard 服务中的 web 跳过功能，功能框总是呈现灰色显示。但是使用 CLI 可以实现以上的操作。
- 对于 FortiGate-800 设备以及该型号以上的设备中，web 过滤/反垃圾邮件列表需要在每个保护内容文件中配置。

FortiFuard web 过滤

以下是关于 FortiGuard web 过滤中出现的问题描述。

- 如果使用微软 IE 浏览器，FortiGuard 网页跳过功能在验证成功后不能够自动重新定向到一个网页。必须在验证成功后重新在浏览器中输入 URL。

虚拟域

使用基于 web 的管理器与 CLI 在配置虚拟域中出现的问题。

- 访问“VPN>IPSEC>监控器”，VDOM 的显示中，除了根 VDOM，其它 VPN 均显示为不工作。使用 CLI 命令 diagnose vpn tunnel list 显示 VPN 的状态。
- 使用基于 web 的管理器，进入“系统>维护>许可证”输入新的 VDOM 许可证时，FortiGate 设备不接受。该操作可以使用 CLI 命令 execute upd-vd-license<license key>实现。
- 如果一个物理接口属于 VDOM_A，并且物理接口上的 VLAN 接口属于 VDOM_B， VDOM_A 管理员将不能恢复 VDOM_A 配置文件。
- VDOM_A 的管理员不能更改属于 VDOM_A 的 VLAN 接口配置。接口设置必须由物理接口的 VDOM 管理员更改。

日志与报告

使用基于 web 的管理器与 CLI 在配置日志与报告中出现的问题。

- FortiGate-100A，FortiGate-60，FortiGate-50A 与 FortiWiFi-60 设备不能够完全存档邮件。设置 FortiGate 将邮件存档到 FortiAnalyzer 设备需要以下两个步骤：
  1. 进入“反病毒>隔离>配置”，选中 FortiAnalyzer 功能框。
  2. 进入“防火墙>内容保护列表”，选择一个保护项并点击“内容存档”将邮件日志存档至 FortiAnalyzer。
- IMAP 邮件不能够存档。只能使用 IMAP APPEND 命令，而不是 IMAP FETCH 命令执行完整的邮件内容存档。SMTP 不存在内容存档问题。
- 当使用 POP3 或 IMAP 下载复合邮件时，FortiGate 设备不能存档邮件内容。SMTP 不存在这样的问题。

新增功能与功能的更改

FortiOS3.0 增加了几项新的功能，以及对原有功能修改。以下将做详细说明。在将系统升级到 FortiOS 3.0 之前，建议阅读本技术文档以及以下所列技术文档，熟悉增加的新功能以及一些功能的更改。

- FortiGate 设备管理员使用手册
- FortiGate 设备 CLI 使用参考

本章包括以下内容：

- 系统设置
- 防火墙
- VPN
- 用户
- 反病毒
- 入侵防护（之前名为 IPS）
- 反垃圾邮件（之前名为垃圾邮件过滤）
- IM/P2P（新加设置项）
- 日志与报告
- HA
- SNMP MIB 与陷阱更改

注意：除了另行注明，以下菜单中的设置配置均没有改变。

系统设置

系统设置菜单包括以下配置项：

- 状态
- 网络
- 配置
- 管理员
- 维护
- 虚拟域

注意：从 FortiOS2.80MR11 后 DHCP 菜单便没有更改，所以系统设置菜单中不包括 DHCP。

状态

状态页面显示系统面板。系统面板经过整合，新添加五个功能条目：

- CPU 与内存使用率的历史记录
- FortiGuard 订购服务与许可证信息
- FortiGate 设备端口状态设置的镜像
- FortiAnalyzer 设备镜像，以及与 FortiGate 设备的连接状态

- AV/IPS 内容统计概述列表

系统面板同样显示有一个登录监控器，以显示登录管理员的数量。该功能提供了对系统配置具有写的权限的管理员在必要时断开与其它管理员用户的连接。通过该页面，您可以刷新系统面板以及关闭 FortiGate 设备。

会话

进入系统设置>状态>统计表，查看会话信息。

网络

系统菜单里显示网络设置选项。FortiGate-60，FortiWiFi-60 与 FortiGate-50A 的 Moderm 的设置只有通过 CLI 进行配置。

选项中添加了失效网关检测，之前需要进入“ 系统>配置>选项”中查看。

配置

配置菜单中的几项信息栏转移到了其它菜单项。时间显示信息栏需要访问“系统>状态>系统信息>系统时间”。

选项栏放到了系统>管理员>设置。该选项栏包括虚拟域配置、web 管理员端口以及 web 管理设置选项。Web 管理现称为“语言设置”。

HA，SNMP v1/v2c 以及替换信息栏目仍然在配置菜单中。

操作模式可以在该菜单中进行切换，同样也可以进入“系统>系统信息>操作模式”实现模式切换的操作。

FortiManager 选项栏转移到了管理员菜单。

管理员

管理员菜单中除了以上所述栏目，还包括管理员与访问控制列表项。

在管理员栏目，在设置新的管理员时可以对应设置其访问权限。

FortiManager 选项栏转移到了管理员菜单，也是增加在管理员菜单中的新选项。

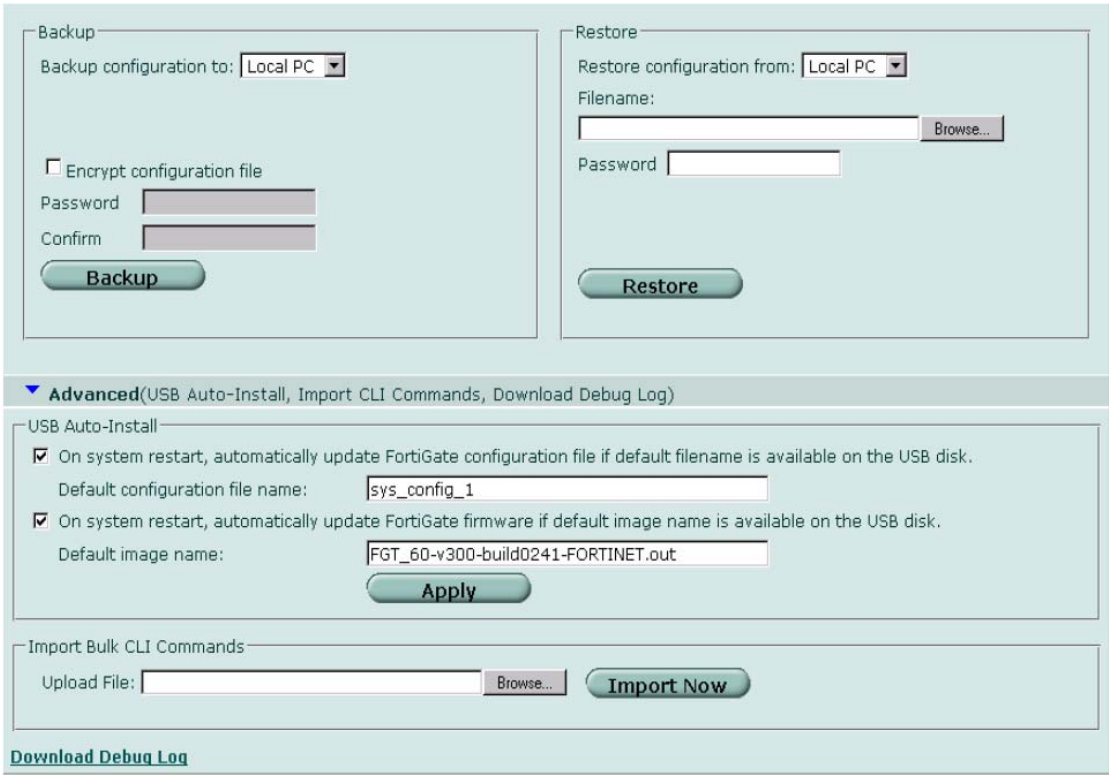
维护

维护菜单中现在只有两个选项栏，分别是备份与恢复，FortiGuard 服务中心。

备份与恢复栏目增加了几项新的选项用于配置备份与恢复配置文件设置。通过备份与恢复栏您可以备份、恢复配置文件，以及加密配置文件。如果 FortiGate 设备型号支持 FortiUSB KEY，可以选择本地 PC 或 FortiUSB KEY 备份或恢复配置文件。备份与恢复栏目还设有高级选项，可以设置在系统重新启动时自动启用 FortiUSB KEY 安装配置文件或镜像文件。通过高级选项也可以导入 CLI 命令。

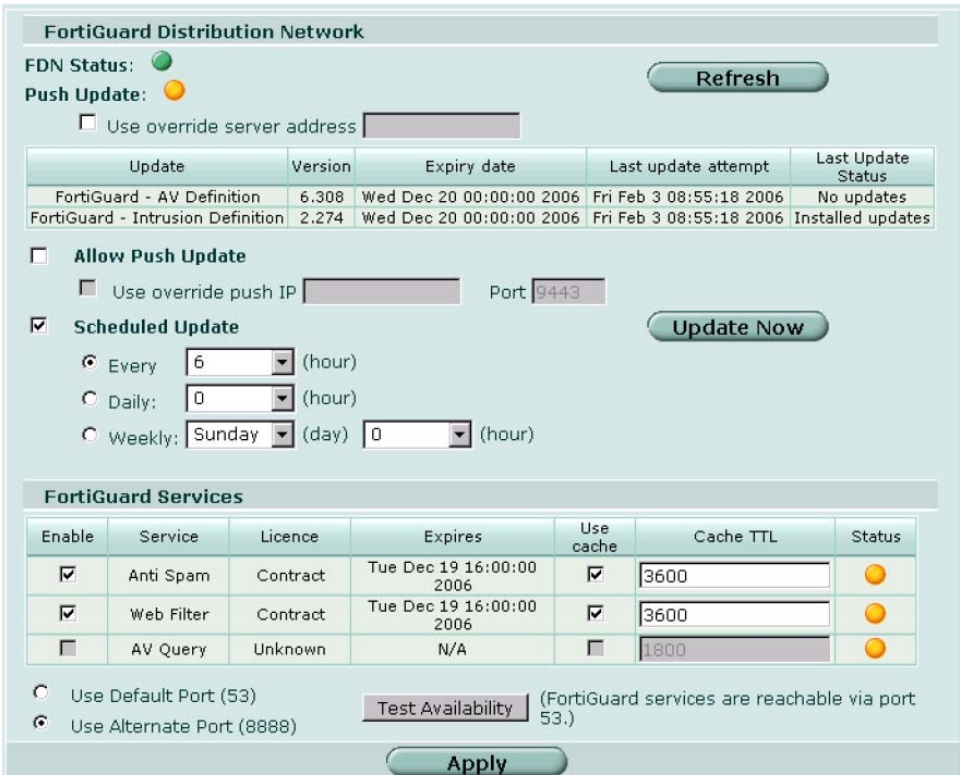
高级选项中还设置有下载调试日志项。您可以下载加密调试日志并已文件形式将其发送到 Fortinet 技术支持协助诊断 FortiGate 设备的问题。

图 4：备份与恢复页面



FortiGuard 服务中心，之前名为“更新中心”，包括可以启动 FortiGate 设备连接到 Fortinet Distribution Network（FDN）、更新反病毒与攻击定义的选项。在该页面中，您也可以测试 FortiGuard 服务的可用性。

图 5：FortiGuard 服务中心



以下是维护菜单中去掉的选项栏：

- 支持栏不可用。
- 关闭设备栏设置在访问系统>状态>系统操作项下。

虚拟域

该菜单显示是“系统>管理员>设置”中的选项。当您配置启动该选项时，需要退回到 web 管理起页面先配置 VDOM 设置。基于 web 管理与 CLI 管理工具中虚拟域配置的选项都发生了改变：

- 全局配置与每个 VDOM 配置分离。
- 只有 admin 管理员账户可以查看与配置全局配置选项。
- Admin 管理员可以配置所有的 VDOM。
- Admin 管理员账户可以通过根 VDOM 中的任何接口连接。
- Admin 管理员账户可以通过任何常规管理员账户管理的 VDOM 的任何接口连接。
- 常规管理员只能配置对其分配的 VDOM 并访问属于这些所管理的 VDOM 的接口。
- 常规管理员能够在其所管理的 VDOM 中的物理接口创建 VLAN 子接口。
- 您可以对管理员账户设置访问权限。
- Admin 管理员可以配置所有的 VDOM，即使某个 VDOM 是分配到某个常规管理员进行管理。

路由表

路由表菜单中包括以下选项：

- 静态路由
- 动态路由
- 路由监控

静态路由

静态路由中包括两个选项：策略路由与静态路由。策略路由以前在路由菜单中是一个单独选项栏。

动态路由

动态路由是新添的菜单，包括四个配置选项，分别可以配置 RIP，OSPF，BGP 与多播协议。

启动动态路由协议配置可以自动与邻居路由共享路由信息，包括邻居路由器发送的路由与网络信息。

- RIP 协议是距离向量路由协议，用于小型网络或类似网络。
- OSPF 稍有不同，是链路状态路由协议，用于大型网络中在同一个自主区域内的路由器之间共享网络信息。
- BGP 是互联网路由协议，典型的被 ISP 用于在不同 ISP 网络之间交换路由信息。例如，BGP 设置可以对在自主系统内使用 RIP 和/或 OSPF 路由数据报的 ISP 与自主系统之间共享网络路径信息。
- 多播设置可以使用 FortiGate 设备作为独立组播协议（PIM）版本 2 的路由器在根虚拟域中操作。PIM 路由器通过网络确保只有一个数据包被转发，直到数据包到达终端目的地，并在只有当需要将信息发送到多播用户应用程序时拷贝数据包，将流量发送到多播地址。

注意：以下设置需要使用 CLI 进行配置：

- 分布列表
- 偏移列表
- 前缀列表
- 路由映射
- 密钥链
- 访问控制列表

监控器

路由监控显示设备路由表的条目，您可以应用过滤器根据具体的路有协议搜索并显示路由。

防火墙

防火墙菜单包括以下配置选项：

- 策略
- 地址
- 服务
- 虚拟 IP
- 内容保护列表

策略

策略菜单与 FortiOS 2.80MR11 中的策略菜单相似，在您建立新的策略时没有高级选项。其它两个额外选项，内容保护列表与日志允许流量中含有验证与流量控制功能框。

当您选中“流量控制”功能，您可以设置“保证带宽”“最大带宽”与“流量优先级”。

地址

地址菜单中设置有您要创建地址类型的选项。地址类型可以设置为“子网/IP 范围”或“完整的限定域名（FQDN）”。

注意：FQDN 存在安全隐患，请小心使用。

服务

服务菜单中用户定义栏目显示进行了更新。用户定义地址栏目中，您可以添加任意多用户服务所需要的 TCP/UDP 协议。

虚拟 IP

虚拟 IP 地址还有其它选项，IP 池菜单包括在该选项中。

内容包括列表

内容保护列表中新增了两个选项：IM/P2P 与日志。

VPN

VPN 菜单中包括以下设置项：

- IPSec

- SSL
- 证书

FortiOS3.0.VPN配置中对VPN菜单进行了更改。建议您查看FortiOS 3.0MR1发布说明中有关VPN配置更改的问题。

注意：当您设备系统升级到FortiOS 3.0. VPN后，需要重新配置VPN设置。升级过程中，IPSec阶段2设置的源与目标端口重置归零。

注意：CLI命令auto-negotiate代替了Ping发生器的功能。默认情况下，auto-negotiate是没有启动的，该功能在IPSec阶段2配置中的IPSec通道中可用。

IPSec

更改了IPSec菜单显示的配置VPN界面。阶段1与阶段2功能栏与新增的AutoKey（IKE）功能栏结合。Ping发生器的功能可以使用CLI命令实现，详细信息参见*FortiGate 设备 CLI 使用参考手册*。

SSL

SSL菜单在FortiOS 3.0中是新增的。含有两个栏目选项，分别为配置与监控，您可以使用这两个选项配置SSL VPN与监控器。

SSL应用使用两个密钥，分别为公共密钥与私有密钥加密数据的加密系统。如果您需要SSL版本2加密与老版本的浏览器兼容，您可以使用CLI启动该协议。参见FortiGate设备CLI设备参考手册有关SSL的详细信息。对于验证远程用户，同样可以使用电子证书。

证书

证书菜单新增了栏目选项：证书恢复列表（CRL）。FortiGate设备使用CRL确保属于CA与远程用户端的证书是有效的。

从CRL选项栏，您也可以导入这些证书的类型。这对于定期从CA网站获取证书恢复列表，使用撤消证书的用户不能建立与FortiGate设备连接的用户很重要。

注意：从CA网站下载CRL以后，需要将下载文件保存在可以访问FortiGate设备的管理计算机中。

用户

用户菜单包括以下选项：

- LDAP
- Windows AD
- 用户组

注意：不包括本地菜单与RADIUS菜单，这两个选项菜单从FortiOS 2.8MR11中就没有更改过。

LDAP

进入 LDAP 菜单，可以访问“普通名称标识符”，“著名名称”与“服务器端口”进行配置。“服务器保密字段”现在需要使用 CLI 命令配置，详细信息参见 FortiGate 设备 CLI 命令参考手册中用户章节。

Windows AD

FortiOS 3.0 中，Windows AD 菜单是新增的，可是在 Windows Active Directory（AD）网络配置 FortiGate 设备，使其能够在查看用户的用户名与密码的情况下验证用户。

通过 Windows AD 菜单，您可以创建新的 Windows AD 以及删除、编辑或刷新服务器。

注意：Fortinet 技术文档的 CD 或访问技术支持网站 http:\\support.fortinet.com 中包括有关 Fortinet 服务器验证扩展（FSAE）的说明。

用户组

在用户组菜单栏，您可以配置用户组的类型：

- 防火墙
- Active Directory
- SSL VPN

在用户组页面，您可以选择“FortiGuard 网页过滤跳过”选项，以便 FortiGate 设备能够实现 FortiGuard 网页过滤跳过配置。

反病毒防护

反病毒菜单在 FortiOS 3.0 中位于用户菜单之下，包括以下菜单项：

- 文件模式
- 隔离
- 配置

文件模式

“文件模式”菜单进行了更改。文件模式页面中的栏目为：模式，动作与启动。当您点击“新建”时，可以选择选择创建的文件模式，所采取的动作是屏蔽或允许，以及是否启动或撤消新的文件模式。

隔离

隔离菜单是反病毒菜单中新增的设置项，包括两个栏目，分别为“隔离文件”

与“配置”。“已隔离文件”显示每个文件的信息，包括文件被隔离的原因。您可以可以根据文件名、日期、服务、状态与状态描述过滤并查找文件。

“配置”显示 FortiGate 设备所屏蔽的当前病毒文件列表，您可以配置隔离文件与电子邮件的大小限制，包括灰色软件屏蔽。

注意：在配置文件与电子邮件的大小限制，包括灰色软件的屏蔽时，FortiGate 设备应该与 FortiAnalyzer 设备建立了连接。

配置

“配置”菜单包括“病毒列表”与“灰色软件”两个设置栏。“配置”栏现在位于 CLI 中的反病毒服务项下，详细信息参见 FortiGate 设备 CLI 使用参考手册。

入侵防护（IPS）

入侵防护菜单包括以下设置项：

- 特征
- 异常
- 协议解码器

注意：升级到 FortiOS 3.0 之前，保存所有 FortiOS 2.80 IPS 组设置，因为某些 IPS 组设置不能留存到 FortiOS 3.0，必须手工配置。详细信息参见 FortiOS 3.0 MR1 发布说明中附件-A。

特征

“特征”菜单中，您可以查看预先定义特征与用户定义特征的严重级别设置。如果您想更改预先定义的特征，您可以将特征设置重置归为默认设置，然后进行更改。

创建信息的用户定义特征时，您可以对用户定义特征设置严重性级别。

异常

异常特征检测是指检测并识别试图利用已知漏洞的网络流量。

当您创建信息的异常特征时，可以设置特征的严重级别。“日志记录”选项的名称改为“数据包日志”。“参数”栏被取消了。

协议解码器

协议解码器菜单，FortiOS 3.0 中新增的选项，对协议异常可以进行日志记录。您可以启动或撤消对协议异常的日志记录功能，以及配置当检测到异常时所采取

的 IPS 动作。如果您需要恢复到默认的设置，可以点击“重置”图标。

您可以使用 CLI 命令根据源与目标地址配置会话控制。当固件镜像升级后，协议异常列表也相应更新。

Web 过滤

Web 过滤菜单在入侵防护主菜单之下，包括以下选项。

- 内容屏蔽
- URL 过滤
- FortiGuard-web 过滤

注意：如果使用基于 web 的管理器升级，您在 FortiOS 2.80 中配置的列表将会留存在 FortiOS 中。保存这些列表以便在升级之后进行校验。详细信息参见 FortiOS 3.0MR1 发布说明。

内容屏蔽

内容屏蔽菜单在 FortiOS3.0 中增加了新的选项“web 内容屏蔽豁免”。

URL 过滤

“URL 过滤”功能可以允许或屏蔽对具体 URL 的访问。您也可以添加模式或表达式以允许或屏蔽 URL。“URL 过滤”菜单包括两个选项，分别为“网页 URL 屏蔽”与“网页模式屏蔽”。

FortiOS 2.80MR11 中，“URL 过滤”用于屏蔽 URL。FortiOS 3.0 中 web 过滤与 URL 过滤合并。

Web 过滤

FortiGuard-web 过滤菜单，之前在 web 过滤>类型屏蔽>配置选项下，FortiOS3.0 中，web 过滤成为独立的菜单项。

FortiGuard-web 过滤是 Fortinet 公司提供的可管理的 web 过滤解决方案，将数百万计的网页根据其内容分类，用户可以根据类型对网页采取“允许”、“屏蔽”与“监控”的动作。

FortiGuard-web 过滤菜单包括“跳过”、“本地类别”与“本地分类”栏目。对于带有硬盘的 FortiGate 设备，您可以使用“报告”选项创建报告。

“跳过”选项给管理员在屏蔽网页时提供了更多的灵活性与控制力。管理员可以配置“跳过”规则，在必要时允许用户访问被屏蔽的网页。管理员也创建用户定义的网页类型，允许用户基于每项用户内容屏蔽 URL 组。

“本地分类 ”选项中，您可以配置本地分类以指定本地分类是否与 FortiGate 分类结果，或用于设置 URL“跳过”。“本地类别”选项允许您指定用户定义的类别，并指定一些 URL 属于该类别。

反垃圾邮件（之前名为“垃圾邮件过滤”）

反垃圾邮件包括以下设置项：

- 禁忌词汇
- 黑/白名单

您可以对 FortiGate-800 设备以及更高端的设备，配置其他功能。例如，在“禁忌词汇”列表中，您可以：

- 创建信息的反垃圾邮件禁忌词汇列表
- 查看反垃圾邮件禁忌词汇目录

同样，对于 FortiGate-800 设备以及更高端的设备，您也可以对黑/白名单列表进行配置：

- 添加多个电子邮件地址列表
- 创建新的反垃圾邮件地址列表
- 创建新的反垃圾邮件 ip 地址列表
- 查看反垃圾邮件 IP 地址列表目录

FortiOS 2.80 MR11 中基于 web 管理器可用有关反垃圾邮件的选项，包括 FortiGuard 反垃圾邮件服务、IP 地址、DNSBL、ORDBL、MIME 报头与邮件地址，在 FortiOS 3.0 中转移到使用 CLI 配置。详细信息参见 FortiGate 设备 CLI 使用参考手册。

如果使用基于 web 的管理器对 POP3、IMAP 或 SMTP 启动了 MIME 报头检测，并且使用基于 web 的管理器对内容保护文件进行了修改，如 IP 地址检测、禁忌词汇检测或记录超大文件日志，那么 MIME 检测将撤消。

电子邮件中对于垃圾邮件所采取的“清除”动作，FortiOS 升级后，使用 CLI 支持该功能。在配置禁忌词汇时，避免使用“清除”动作，因为在 FortiOS 3.0 中这个动作不再是有效的动作。

注意：黑/白名单不是分离的。升级到 FortiOS 3.0 后，您可能需要重新启动 MIME 报头。

禁忌词汇

“禁忌词汇”设置通过屏蔽邮件中包含的具体词汇或模式来检测与控制垃圾邮件。“禁忌词汇”菜单所能设置的动作栏“计数”，在创建新的禁忌词汇时会出现该设置项。

“计数”是应用于禁忌词汇的计算出现次数的设置项，如果“计数”所得高于内容保护文件列表中设定的构成垃圾邮件的限值，程序将根据对邮件流量类型所采取的动作继续进行，例如，对于 smtp3-spamaction，内容保护文件列表中设置的动作为“通过”或“标签”。在一个 web 页面中，即使一条禁忌词汇出现多次，但“计数”中只计为一次。

黑/白名单

在内容保护列表中启动了“黑/白名单”设置后，可以过滤进入的邮件。

FortiGate 设备使用 IP 地址列表与邮件列表进行过滤。

FortiGate 设备将邮件发件人的 IP 地址与 IP 地址列表逐个检测，如果发现匹配，将采取对应的动作，没有发现匹配，通过邮件进行下一项垃圾邮件过滤选项。“邮件列表”的操作方法与“IP 地址”一样。

IM/P2P

IM/P2P 菜单包括以下选项：

- 统计表
- 用户

随着即时通信与 P2P 网络流量的增加，FortiOS3.0 中是新增 IM/P2P 菜单。您可以对 P2P 分配带宽限制。

使用 CLI，还可以对 IM/P2P 配置扩展的功能。使用 config imp2p old-version 命令启动旧版本的 IM 协议。这些 IM 的老版本可以绕过文件屏蔽功能，因为一些文件的类型无法识别。该命令对于终止这些旧版本的 IM 协议提供了选择。

所支持的即时通信协议包括：

- MSN 6.0 以及更高版本
- ICQ4.0 以及更高版本
- AIM5.0 以及更高版本
- Yahoo6.0 以及更高版本

注意：FortiGate 设备不能够屏蔽 Skype 用户。即使启动了音频屏蔽功能，即时信息的用户仍然可以发送/接收 webcam/video 信息流量。

统计表

管理员可以查看“统计表”中即时通信与点到点通信数据，以便了解这些即时通信协议在网络中的使用情况。

“总述”提供了所有 IM/P2P 协议使用的详细信息。“协议”栏显示从最近一次重启后当前的用户、屏蔽的用户信息。

用户

“用户”菜单显示连接着的哪些即时通信工具的用户。网络管理员可以分析列表并决定屏蔽或允许的用户。

管理员可以使用“配置”栏，配置对未知用户采取的动作。

日志与报告

“日志与报告”是新增的菜单，包括以下设置项：

- 日志配置
- 日志访问

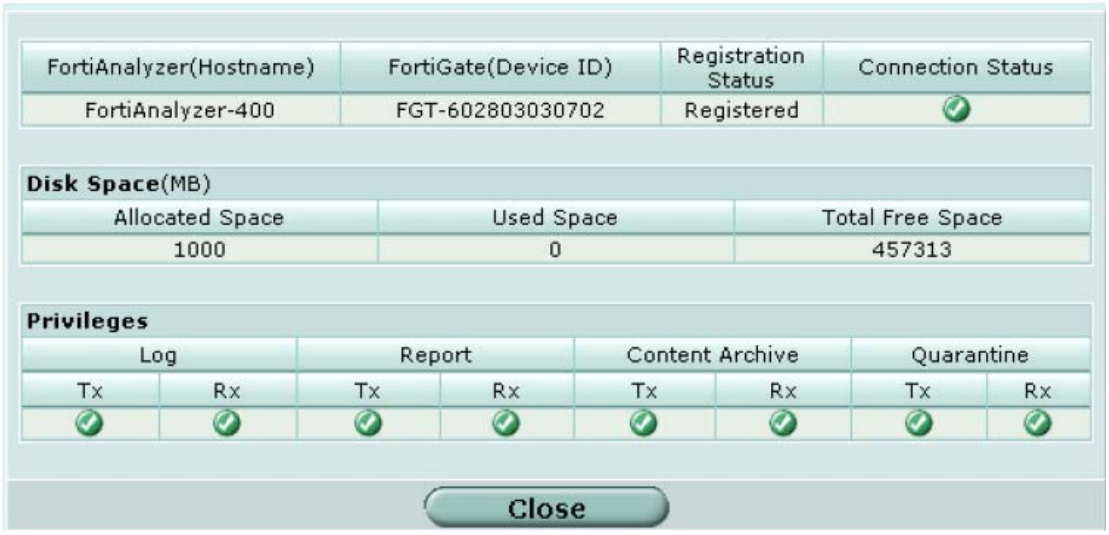
- 报告

日志配置

“事件日志”是日志配置菜单中新添的栏目。“事件日志”中您可以选择需要日志记录的事件。“事件日志”栏目中还包括“报警邮件”，其功能与 FortiOS 2.80MR11 中相同，当 FortiGate 设备发生情况时，如设备故障或网络攻击时提供即时的告知。

“日志设置”中，您可以测试 FortiGate 设备与 FortiAnalyzer 设备的连接性，以查看连接状态。

图 6：日志与报告菜单中“测试连接性”的功能



FortiOS 3.0 中新增了选项栏“FortiDiscovery”，自动检测 FortiGate 设备并将其连接在同一子网中的本地 FortiAnalyzer 设备。“FortiDiscovery”使用在同一子网中的本地 FortiAnalyzer 设备发送 HELLO 数据包的功能实现与 FortiAnalyzer 设备的连接。

Web 趋势选项与流量过滤，CLI 中可以进行配置使用。详细信息参见 FortiGate 设备 CLI 使用参考手册。

对于各种协议与流量的日志记录，可以在“内容保护列表”中进行配置。

注意：“日志过滤”功能需要进入防火墙>内容保护列表>日志中进行配置使用，您也可以使用 CLI 启动该功能。“流量过滤”使用 CLI 也可以配置。详细信息参见 FortiGate 设备 CLI 使用参考手册。

日志访问

“日志访问”有两个设置栏，“内存”栏显示记录到内存的事件日志类型。“FortiAnalyzer 设备”栏显示记录在 FortiAnalyzer 设备的日志类型。

其它栏目表示如果 FortiGate 设备带有硬盘则显示“硬盘”标记。使用下拉菜单选择不同的日志类型。

报告

“报告”菜单提供从 FortiAnalyzer 设备记录的所有不同范围报告的访问，该功能只有在 FortiGate 设备与 FortiAnalyzer 设备连接时才能够实现。

您可以选择“基本流量”报告或“访问任何类型的 FortiAnalyzer 报告”以显示日志。“基本流量”包括是存储在 FortiGate 设备内存中的日志信息，在“日志访问”页面以两种类型的条形图显示信息。

您可以从很多 FortiAnalyzer 报告中查找日志数据，或为您的 FortiGate 设备定制默认的报告生成。这些包括从新闻组到 VoIP 收集的数据信息。

HA

FortiOS3.0 中对配置 HA 有很大的更改，包括增加了新的功能。对于 HA 最大的改变是对单个虚拟域配置 HA 中涉及的虚拟群集。虚拟群集涉及到两台 FortiGate 中每个虚拟群集的操作。

FortiGate 设备 HA 概述中提供了对现有功能更改的其它信息，以及 FortiOS3.0 中新增的功能。有关 FortiOS 3.0 的详细信息，参见 FortiGate 设备管理员配置手册（系统配置章节中 HA 部分）、FortiGate 设备 CLI 使用参考手册以及在线帮助。

系统菜单中，进入系统>配置>HA，配置 HA。 从该配置栏中，您也可以配置 HA 设置。“替代主设备”在默认情况下是启动的。

注意：配置一个 HA 群集时，保证所有的 FortiGate-100A 与 FortiGate-200A 设备具有相同的序列号。

升级 HA 群集

以下步骤帮助您将 FortiOS 2.80HA 群集升级到 FortiOS3.0。
您可以使用基于 web 的管理器或执行 CLI 命令 execute restore image 以及一台 TFTP 服务器升级群集。

升级群集

1. 备份主设备的配置。
2. 在主设备上安装固件镜像。

该操作需要持续几分钟的时间，因为主设备同样需要升级从属设备。群集中的 FortiGate 设备在升级过程中将重新启动一次或两次。

注意：如果在升级前没有启动“HA 替代”功能，主从设备的地位可能会发生变化。

SNMP MIB 与陷阱

FortiOS3.0 中，陷阱文件结合在 MIB 文件中。只有一个 MIB 文件可下载安装在您的 SNMP 管理系统中。

之前 SNMP 陷阱与参数使用连字符表示，如 xxx-yyy，现在去掉了连字符，并大写第二个条目，如 xxxYyy。

FortiOS 3.0 的 MIB 文件同样有更深入的描述以及所支持的型号。联系 Fortinet 公司技术支持获得 MIB 文件。

SNMP 陷阱

以下叙述有关 FortiOS3.0 中 SNMP 陷阱更改的有关信息。

FortiOS3.0 陷阱名称/状态	FortiOS2.8 陷阱名称/状态
fnFMTrapIfChange	新增
fnFMTrapConChange	新增
不再可用	fnTrapHaStateChange
不再可用	fnTrapIdsPortScan
不再可用	fnTrapImTableFull

MIB 文件名称

下表显示陷阱名称的梗概，包括 FortiOS 3.0 中其它陷阱名称。

位置	FortiOS3.0 陷阱名称/状态	FortiOS 2.8 陷阱名称/状态
系统	fnSysDiskCapacity	新增
	fnSysDiskUsage	新增
	fnSysMemCapacity	新增
HA	fnHaLBSchedule	fnHaSchedule
	fnHaGroupID	fnHaGroupID
	fnHaPriority	不可用
	fnHaAutoSync	不可用
	fnHaOverride	不可用
选项	fnOptAuthTimeout	新增
	fnOptionLanguage	新增
	fnOptLcdProtection	新增
管理	fnManSysSerial	新增
	fnManIfName	新增
	fnManIfIp	新增
	fnManIfMask	新增
管理员帐户	fnAdminTable	
	perm	不可用

FortiOS 3.0 MR2

FortiOS 3.0MR2 中提供了更多的功能以及对现有功能的改进。该版本的操作系统中支持从 FortiUSB 密钥中安装固件，以及使用基于 web 的管理器配置 FortiAnalyzer 报告，包括直接从 FortiUSB 密钥安装固件镜像。

本章包括以下内容：

- 升级说明
- 新的功能与功能更改
- 公知信息

Fortinet 公司建议有关 FortiOS 3.0 MR2 中新增加的功能，以及一些功能的更改，参见以下文件：

- FortiGate 设备管理员使用手册
- FortiGate 设备 CLI 使用参考手册
- FortiGate 设备 HA 概述

注意：有关 FortiOS 3.0MR1 中已经解决的技术问题，参见 FortiOS 3.0MR2 发布说明中“已解决的公知问题”章节。

升级说明

本章是有关 FortiOS 3.0 MR2 发布的一些常规信息说明。其中包括 FortiOS 3.0MR2 中公知的信息以及其它在 “新的功能与功能更改”章节中没提到的信息。

LCD 显示更改

升级到 FortiOS MR2 后，FortiGate 设备的 LCD 显示如下：

图 7：NAT/路由模式下的主菜单设置显示

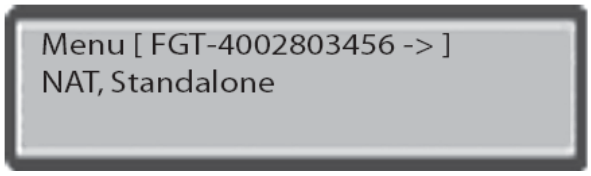
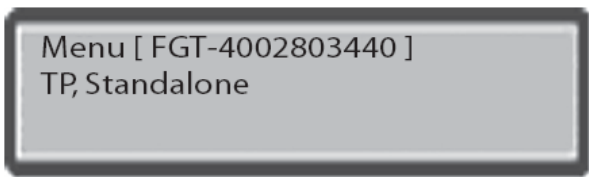


图 8：透明模式下的主菜单设置显示



FortiGuard 状态显示图标

FortiOS 3.0MR2 中，FortiGuard 状态图标显示状态说明：

最近一次试图连接到 FDN 成功，对应的许可证信息正确。

最近一次试图连接到 FDN 成功，但是对应的许可证过期或设备未注册。

最近一次试图连接到 FDN 没有成功。

FortiUSB 支持

FortiUSB 密钥支持 FortiGate 设备从密钥直接安装固件镜像。FortiUSB 密钥可以自动升级固件并通过 USB 的自动安装功能下载存储在 FortiUSB 中的配置文件。

FortiGate 设备只支持 Fortinet 公司出品的 FortiUSB Key。

新增功能与功能的更改

本章只对 FortiOS3.0MR2 中涉及到新功能以及部分功能更改的菜单进行说明。

系统设置

系统设置菜单增加了几项新的功能，如验证存活的方法。举例说明，当一个用户登录设备后，在当用户打开新的浏览器点击一个链接页面，并定向到所请求的页面时，对用户将出现一个验证存活的提示。

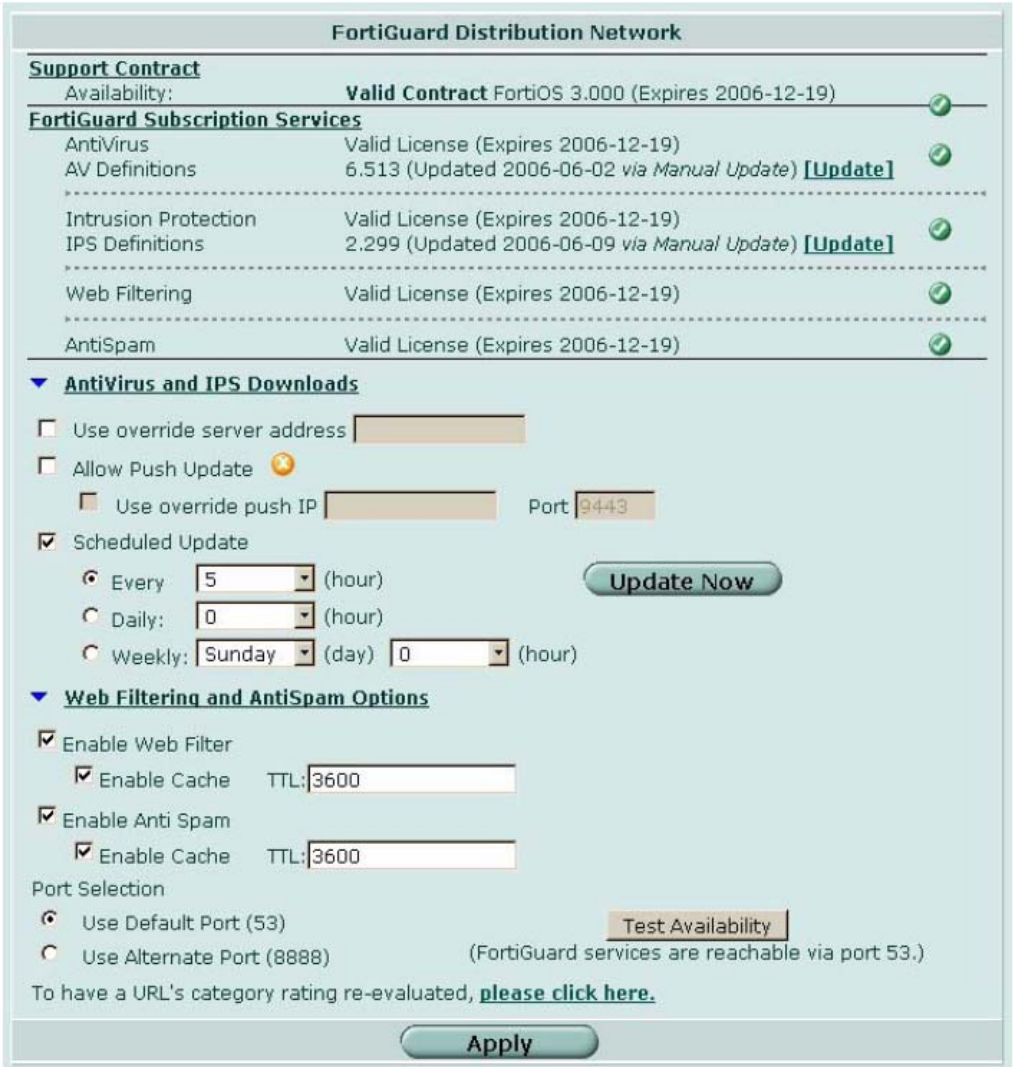
FortiOS 3.0MR2 中，管理员可以在不保存对配置文件更改的情况下，试运行一个配置文件并观察其运行情况。该功能只能在 CLI 中实践。

您可以在 FortiOS 3.0MR2 的配置文件中添加 ARP 条目。该功能只有在 NAT 模式下使用 CLI 来实现，并是基于每个 VDOM 的。

虚拟域是基于 HA 模式下配置的，但是主动-主动（A-A）的 HA 模式并不支持虚拟群集。VDOM/VLAN 技术允许用户可以独立配置多个被管理的域。

加强了 FortiGuard 中心页面的服务状态显示，以及提供了更高效配置 AV/IPS 下载以及 web 过滤选项的方法。

图 9：FortiOS 3.0MR2 中 FortiGuard 中心显示页面



路由

路由菜单中含有等效多路径路由（ECMP），以及在 DHCP 与 PPPoE 模式下对接口配置静态路由。

FortiOS 3.0MR2 中，新增加 ECMP 的应用，提供了 FortiGate 设备使用相同成本下的两条路由转发数据包。这些路由通过配置或通过路由协议获知，并且对每条协议的开销是相同的。您需要创建 ECMP 运行到相同目标地址下具有相同具体的几条静态路由以及优先级设置。这同样适用于 OSPF。

静态路由是对 DHCP 或 PPPoE 模式下的接口配置的。当 DHCP 或 PPPoE 接口需要路由但是在动态接口出现之前没有已知的网关时，以上对接口的静态路由配置是比较有用的。当建立、断开以及重新建立到接口的连接，并且启动了动态网关时，所有有关的静态路由都将更新。动态接口上的 Ping 服务器是启动的。

CLI 中增加了新的命令 ospf-interface cost 提供了与 FortiGate 设备不同接口速率连接情况下计算路由开销的方法。命令 ospf-interface 中 cost 字段在默认情况下设置为 0，auto-cost-ref-band-width 的值在默认情况下设置为 1000。这些默认值将自动执行。

那么，就是对设备设置强制提供静态路由。如果在 FortiOS 2.80 中没有对设备配置静态路由，升级到 FortiOS 3.0 时，静态路由设置不能续载入到 3.0 的 FortiOS 中。

路由菜单中还包括对 OSPF 的自动开销计算。

防火墙

进入“防火墙>策略”，您可以定制查看策略的字段顺序。您可以使用栏目设置图标定义显示策略。使用鼠标可以拖动策略条目在整个策略列表中排列的顺序。

FortiOS 3.0MR2 中，您可以对一项防火墙策略创建并添加多个 IP 池。使用 CLI，配置多个 IP 池。

CLI 命令 config user adgrp 是只读命令。只有在 Windows AD 服务器上 FSAE 软件没有对 FortiGate 设备发送组时可用。建议在升级到 FortiOS3.0MR2 之前备份这些条目，以防在升级后丢失。

预先定义的防火墙服务只在基于 web 的管理器中显示。

防火墙菜单提供 RADIUS 计算。FortiGate 设备通过发送以下 RADIUS 属性计算开始/结束信息。

- Acc-Session-ID
- NAS-标识符（FortiGate 设备主机名称）
- Fortinet-VSA（建立与用户连接的 IP 地址）
- Acct-Output-Octet
- User-Name（用户名称）
- Framed IP Address（用户 IP 地址）
- Acct-Input-Octet

下表是所支持验证事件的描述以及发送的 RADIUS 的属性：

属性							
验证方式	1	2	3	4	5	6	7
Web	×	×	×		×		
IPSec 的 XAuth （没有配置 DHCP）	×	×	×		×		
IPSec 的 XAuth（配置了 DHCP）	×	×	×	×	×		
PPTP/L2TP（PPP 中）	×	×	×	×	×	×	×
SSLVPN	×	×	×		×		

FortiGate RADIUS 计算同时支持提供商指定属性（VSA）。

防火墙菜单还包括几项新的验证属性。LDAP 用户配置中有可选用户字段。用户字段启动后，LDAP 验证在具备成功验证条件时校验所验证的用户是否是 LDAP 服务器中设置的组的成员。用户字段在 CLI 中使用命令 config user ldap 启动。

验证选项中，FortiNet 厂商定制 RADIUS 属性也是新增的。该属性被定义为 Fortinet 组名称，可以通过 RADIUS 服务器发送访问-接收回应中返回到该属性。启动该属性后，FortiGate 设备在具备成功验证的条件下校验与用户组匹配的属性。

SSL-VPN 的验证支持 RSA 安全 ID 所需的质询。

VPN

VPN 菜单中，当 SSL VPN 应用于通道模式时支持通道分割。举例说明，支持通道分割的情况下，允许到达网络 A 的流量通过 SSL VPN，同时到达网络 B 的流量通过常规接口。通道分割可以在用户组页面中 SSL-VPN 用户组选项下启动。

用户

用户菜单下，LDAP 浏览器功能是可用的。当管理员进入“用户>LADP >新建”中，添写了服务器名称/IP 字段并点击浏览图标后，FortiGate 设备查询 LDAP 服务器并自动将查询结果反映到字段中。

Web 过滤

Web 过滤>URL 过滤项下，您可以使用鼠标在 URL 列表中拖动 URL 项，使其处于任何您拖动到的位置，实现 URL 的重新排列。

当FortiGate设备位于HTTP代理服务器之后时，FortiGuard web过滤验证绕过不能返回到绕过页面。您可以在web浏览应用程序前添加*.8008并放入应该绕过服务器的URL中。8008是端口验证的默认端口号。

日志与报告

升级到FortiOS3.0MR2，日志与报告模块下增加了新的功能，以及一些功能的更改。日志与报告菜单中额外添加了两个子菜单“报告配置”与“报告访问”。“报告配置”与“报告访问”提供了通过FortiGate设备基于web的管理器访问FortiAnalyzer设备中存储的报告的可达性。从这两个菜单中您也可以配置、编辑或打印FortiAnalyzer报告。

FortiOS3.0MR2版本中同时对外部日志记录设备例如FortiAnlyzer设备增加了设备名称字段进行明确的定义。

“报警邮件”提供两种类型的警报邮件。报警邮件根据所记录的事件或记录日志的严重级别发送。

如果设置了HA群集，将不能够FortiGate HA从属防火墙中访问与查看日志与报告。

如果在一批FortiGate设备与FortiAnlyzer设备之间使用了NAT设备，将只有一台FortiGate设备具有访问FortiAnalyzer浏览器的功能。

注意：内容存档菜单将在未来发布的版本中支持。您可以在统计模块下状态页面查看当前的内容存档。

报告配置

报告配置页面的顶端，显示配置到FortiAnalyzer设备报告的信息，包括FortiAnalyzer引擎的状态，并且当生成一个设定的报告时，或当前情况下生成的报告。您也可以点击“编辑”图标，对这些报告进行编辑。

报告访问

报告访问菜单包括两个状态栏，FortiAnalyzer栏与内存栏。内存栏还包括您可以配置从FortiGate设备内存的基本流量报告。FortiAnalyzer栏中，您可以操作从FortiAnalyzer设备中查看与打印所有有关FortiGate设备的报告。

HA

访问“系统>状态”，显示HA状态。HA状态以及FortiGate设备与FortiAnalyzer设备的连接状态是通过状态页面中右上角中FortiGate设备图标显示的。群集名称与群集成员显示在状态页面的系统信息栏中。

从属设备可能发出从FDS获得的AV更新没有安装成功这样的报告。您可以登录CLI，使用命令diagnose sys autoupdate version校验每台从属设备AV更新的情况。

FortiOS 3.0MR2中增加了在不中断服务同时升级HA群集的功能。该功能同样在CLI中使用以下命令来实现：

```
config sys ha
set uninterruptible-upgrade<enable|disable>
end
```

SNMP MIB 与陷阱更改

SNMP OID中硬盘容量（fnSysDiskCapacity）与硬盘使用率（fnSysDisk）是以兆字节显示的。

公知信息

FortiOS 3.0MR1版本中列数的公知信息，同样存在于FortiOS 3.0MR2中，除非另有注明。

基于 web 的管理器

基于web的管理器中存在的公知信息关系到所有使用web管理器能够配置的所有功能：

- 报告页面中定期显示不正确的时间。

- 有关最近检测到的攻击生成的报告被缩短了。
- 具有写的权限的管理员不能够在基于web的管理器中备份配置，但是可以在CLI中实现。
- 默认的网关在从DHCP服务器接收并显示IP地址时，在IP地址前显示有大于号。但是，这并不影响设备的功能性。
- 不显示环回接口。
- 当用户以一个VDOM管理员登录时，基于web的管理器不显示报告访问页面。
- 在事件日志页面，即使启动了事件选项，事件选项的功能框显示也是未选中的，事件日志不能被记录的状态。报警邮件界面，如果启动了一些类型，将不被发送出去。

系统设置

- 当DNS转发在非根虚拟域启动时，FortiGate设备不转发DNS请求。
- 数据加密标签在“设置”页面中显示，但当安全模式设置为“无”“WEP64”或“WEP128”时，下拉菜单中不显示数据加密标签。只有当安全模式设置为“预共享密钥”或“WPA RADIUS”时，数据加密标签与下拉菜单是可见的。
- FortiGate-60在启动过程中不能发送冷启动SNMP陷阱。
- 在无线接口设置中可以更改传输功率级别，但是应用diagnose sys wireless cmd wlan命令时仍就显示更改之前的功率。
- 如果“安全模式设置”设置为WPA-PSK，并且接口设置为“闭合”状态，用户仍然可以建立连接。
- VDOM管理用户或非VDOM管理用户不能使用基于web的管理器备份配置文件。
- 如果服务器配置用在HA群集中，DHCP服务器不能自动分配IP地址。

系统设置（FortiWiFi-60A/AM）

以下系统设置有关的问题，只涉及到FortiWiFi-60A/AM设备：

- 运行Windows 2000的PC，如果“无线安全设置”设置为WEP标准时，不能连接到FortiWiFi-60A/AM设备。
- 运行Windows 2000的PC，如果FortiWiFi设备使用WEP与扩展无线接口时，不能连接到FortiWiFi-60A/AM设备。
- 如果FortiWiFi-60AM设备的“安全模式”设置为WPA预共享密钥时，在用户模式下不能启动无线连接。
- 应用于HA群集中的从属设备的LCD不能正确报告群集连接状态中ZERO。Zero被群集中主设备使用。从属设备的指示从1开始。
- FortiWiFi-60A/AM设备上的VDOM启动后，无线接口属于非管理VDOM，同时安全模式字段设备为WPA-RADIUS， RADIUS服务器字段在下拉菜单中显示RADIUS组。

防火墙

防火墙的设置的有关信息涉及到基于 web 的管理器与 CLI 这两个管理工具中应用的配置。

- 当具有相同外部IP地址的VIP已经存在时，在基于web的管理器中部能建立端口转发VIP。
- CLI命令conf user adgrp是只读命令。它用于配置FortiGate设备在AD服务器中的FSAE发送AD组到配置文件时，添加发送的AD组。如果该命令下有很多条目，在从FortiOS 3.0MR1升级到FortiOS 3.0MR2时，这些条目都将丢失。这并不影响FortiGate设备或FSAE的功能性，因为在升级完成之后，AD组都已经发送到FortiGate设备，并且恢复了连接。
- 在配置config sys global 命令中set ip-src-port-range<start>-<end>的IP范围时，FortiGate设备不能够对端口实现使用设定IP地址范围内的地址。
- 预先定义的防火墙服务在通过CLI命令访问时不能在VDOM中显示。
- 当一项防火墙策略配置使用预定义的防火墙服务FTP-Get时，FortiGate设备在FTP活动模式下不能屏蔽FTP-Get命令。同样的行为也在使用FTP-Put预定义防火墙服务时发生。
- LDAP用户名称中包含的特殊字符可能会导致验证失败，这些特殊字符包括：字符串开始或结束的空格键、#、+、逗号（,）、斜划线（\）、左引号（“）、小于号（<）、大于号（>）、分号（;）。
- 当在PPPoE接口添加一个VIP时，FortiGate设备不能将数据包流量从VIP地址转发到目标地址。

高可用性（HA）

高可用性，涉及在基于 web 管理器与 CLI 中的操作。

- 当HA群集运行于透明模式下的主动-主动模式下时，不同通过VLAN接口实现负载平衡。通过HA群集中主设备通信会话能够顺利进行，但是通过从属设备的会话将不能够连接。
- 如果一个端口作为聚合端口，FortiOS允许选择这些端口中的一个作为HA心跳设备端口。这将中断HA连接。
- 当FortiGate设备一个HA群集中的从属设备，并运行于主动-主动模式时，邮件内容日志不能发送到FortiAnalyzer设备。
- 在一个HA群集恢复配置时，从属设备的主机名称、HA优先级别或跳过设置都将丢失。
- 从属设备可能会报告从FDS获得升级不能安装。
- FortiGate设备不能阻止在心跳设备上分配聚合与冗余接口，那么这样将导致HA群集的中断。

VPN

- SSL-VPN web模式下，在FTP服务器创建目录的时间与系统时间不符。

FortiGate设备在发生目录条目复制或不创建条目时都不能发出警告。

- 如果从其它两台FortiGate设备上终止到另一台FortiGate设备之间的IPSec通道，并且浏览器只对IPSec通道启动，这两台设备还是可以连接到互联网。
- 对PPTP地址范围配置多个C-class网络不再可用。

即时信息与 P2P

以下公知信息只涉及到P2P：

- P2P统计表不能升级，除非内容保护文件中启动了P2P速率限制。

IPS

入侵保护有关的公知信息涉及到基于web的管理器与CLI中的操作：

- 当用户访问“日志与报告>日志访问>磁盘>攻击日志”，在弹出的“打包日志”的窗口中选择“保存”时，FortiGate设备并不能保存IPS数据包。
- “入侵防护>特征>用户定义特征”下，撤消选定的用户定义的功能框时，并不能撤消用户定义特征的应用。
- 在攻击去往关闭的端口或者没有启动的服务时，攻击日志信息并不记录这些操作。例如，对一个接口的Telnet管理访问并没有启动，那么对TCP端口23发生的攻击并不生成日志信息。
- 从IPS 2.214定义版本开始，对以下特征所采取的默认动作更改如下：

特征	IPS版本<2.214中默认的动作	IPS版本>=2.214中默认的动作
icmp_floog	清除会话	未启动
ping_death	丢弃会话	未启动
large_icmp	无	未启动
udp_flood	丢弃会话	未启动

Web 过滤

- 当FortiGate设备位于HTTP代理服务器之后时，FortiGuard web过滤验证绕过功能并不能返回到绕过页面。

虚拟域

- VDOM中，除了根VDOM，其它的VPN在进入VPN>IPsec>监控器查看时，都显示关闭状态。
- VDOM管理员不能从一个虚拟HA群集中恢复VDOM配置，如果该VDOM并不是设置为所恢复VDOM配置。
- 如果使用基于web的管理器不能执行一个VDOM管理用户或非VDOM用户备份配置文件的操作，那么可以使用CLI显示这样的备份操作。

- 当配置一个虚拟HA群集，并VDOM管理员恢复其VDOM配置时，如果管理VDOM并没有设置到配置文件被恢复的VDOM，那么虚拟群集不能同步。

反垃圾邮件

有关公知信息中，只涉及到反垃圾邮件功能项：

- FortiOS 3.0删除了在基于web的管理器中对电子邮件中出现的禁忌词汇采取的动作“清除”。该功能仍然在CLI中是可用并支持升级。在使用基于web的管理器添加条目，并且使用CLI将动作更改为“清除”，条目将从基于web的管理器中消失，但是在CLI仍然是存在的，所有包含禁忌词汇的邮件都将被屏蔽。在CLI中，将条目更改回“垃圾邮件”，那么被禁词汇条目重新在基于web的管理器中出现。在FortiOS3.0中，反垃圾邮件的“清除”动作并不是有效的动作，那么就不应该使用CLI更改对禁忌词汇所采取动作。

日志与报告

有关日志与报告中的公知信息关系到基于web的管理器与CLI中的操作：

- 防火墙不能对IMAP邮件进行内容存档。只有通过IMAP APPEND命令，而不是IMAP FETCH命令执行全部的邮件内容存档。SMTP不涉及到内容存档。
- 被HA群集中从属设备隔离的文件不能发送到FortiAnalyzer设备。
- 从FortiOS2.80升级到3.0之前，使用基于web的管理器备份日志文件。FortiOS 3.0将有关VDOM的日志信息拆分为每个VDOM具有其自身的日志文件与目录。升级后创建的任何信息都可以从基于web的管理器中可以查看。在FortiAnalyzer设备中访问日志浏览页面，点击“导入”。
- 设定上传的日志在配置的时间下不能将日志上传到FTP服务器。
- 基于web的管理器
- FortiGate-100A不能将攻击、反病毒与web过滤事件记录到系统内存。

FortiOS 3.0MR3

FortiOS 3.0MR3的更新是继以上两个版本，对设备功能性与管理性的改进与升级。MR3支持内容存档，日志文件中清晰的说明了日志类型、日志来源设备、VDOM日志记录以及日志记录时间。CLI中对系统面板的操作有些更改。系统面板中包括内嵌的CLI控制台窗口。

以下章节中的信息是对MR3版本的说明：

- 新增功能与更改的功能
- 公知信息

Fortinet 公司建议有关 FortiOS 3.0 MR3 中新增加的功能，以及一些功能的更改，参见以下文件：

- FortiGate 设备管理员使用手册

- FortiGate 设备 CLI 使用参考手册
- FortiGate 设备 HA 概述

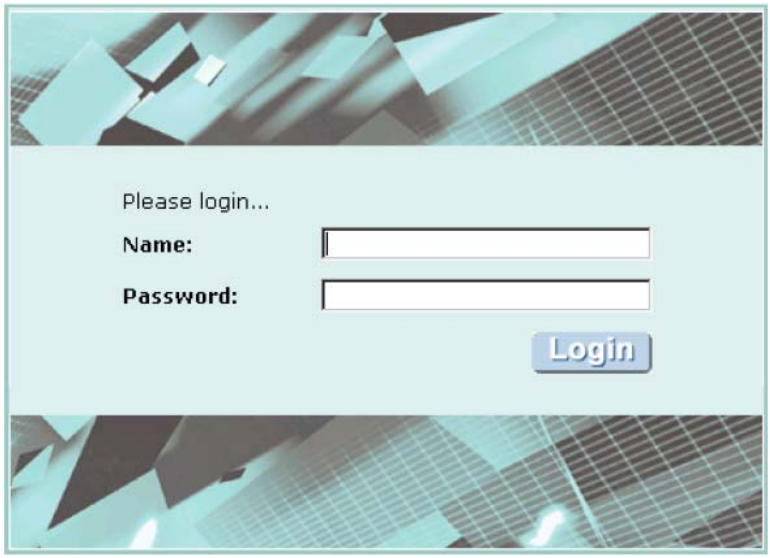
注意：有关 FortiOS 3.0MR1 中已经解决的技术问题，参见 FortiOS 3.0MR2 发布说明中“已解决的公知问题”章节。

新增功能与更改的功能

以下信息只涉及新增加的功能与一些功能的更改。当出现具体的应用时同时说明程序性信息。

升级到FortiOS 3.0MR3后，基于web的管理器登录页面显示如下：

图10：FortiOS 3.0MR3登录页面



FortiOS3.0MR3 中 CLI 操作的更改

CLI命令get,show与clear在MR3中的功能性得到了增强。

- get --- get命令现在可以显示动态系统信息。
- show --- show命令包括新的选项full-configuration，显示所有的关键字值，与与执行get命令的效果一样。
- clear --- 新的命令，执行execute clear命令可以清除或重设动态计算器与数据库。

系统设置

系统面板中增加了嵌入的CLI控制台以及HA群集成员、HA群集名称以及登录基于web管理器和/或CLI的管理员人数。

图11：FortiGate-60设备的系统面板显示

系统信息		
	序列号	FortiGate设备的序列号。
	运行时间	设备运行的具体时间。
	系统时间	系统在特定的时区中的时间显示。
	HA状态	设备在HA群集中运行的状态。点击“配置”配置群集中的FortiGate设备。
	群集名称	FortiGate设备所在HA群集的名称。该名称只在FortiGate设备加入群集时显示。
	群集成员	属于当前HA群集的群集成员。该信息只在只在FortiGate设备加入群集时显示。
	主机名称	FortiGate设备的主机名称。点击“更改”可以更改FortiGate设备的名称。
	固件版本	当前固件的版本。点击“更新”安装新的固件版本或降级到之前的固件版本。
	操作模式	FortiGate设备运行的操作模式。点击“更改”更改操作模式。
	虚拟域	显示是否启动了虚拟域。点击“更改”启动或撤消使用虚拟域。
	当前管理员	基于web管理器和/或CLI中当前登录的管理员数量。当您选择“详情”时会弹出一个窗口显示每个管理员信息，包括管理员登录的IP地址，您可以点击“断开连接”断开一个管理员与设备的连接。

许可证信息			
	支持合同	支持合同的版本与过期时间。	
	FortiGuard服务订购	您为FortiGate设备所购买的FortiGuard服务。显示这些服务是否是当前的，是否需要更新或服务过期的时间。	
	虚拟域		
		允许的虚拟域	FortiGate 设备允许设定的最大虚拟域数量。
CLI控制台	MR3中，CLI操作窗口是新增的。在基于web管理器的应用下您可以控制台您可以输入CLI命令。		
系统资源			
	CPU使用率	CPU使用率的百分比。	
	内存使用率	内存使用率的百分比。	
	FortiAnalyzer使用率	FortiAnalyzer使用率的百分比。	
报警信息	显示系统报警信息。这些信息中包括如果系统重启后固件升级或降级的信息。如果在具体一个时间段内反病毒引擎在内存中较低，也会显示报警信息。		
统计表	显示内容存档与攻击日志的详细统计信息。		

访问“系统设置>管理员”，新增一个可用的访问内容表，名为超级管理员（super_admin）。超级管理员账户创建了新的admin管理员，与默认的admin管理器员具有同样的读写权限。您可以设置多个超级管理员（super_admin），如需要您可以编辑或删除超级管理员账户。CLI中实现该功能的命令是is-admin。

使用CLI恢复固件镜像时，您可以使用FTP协议。以下是FTP的CLI语法：
execute restore image ftp <image name> <server IP> <ftp_user> <ftp_pwd>

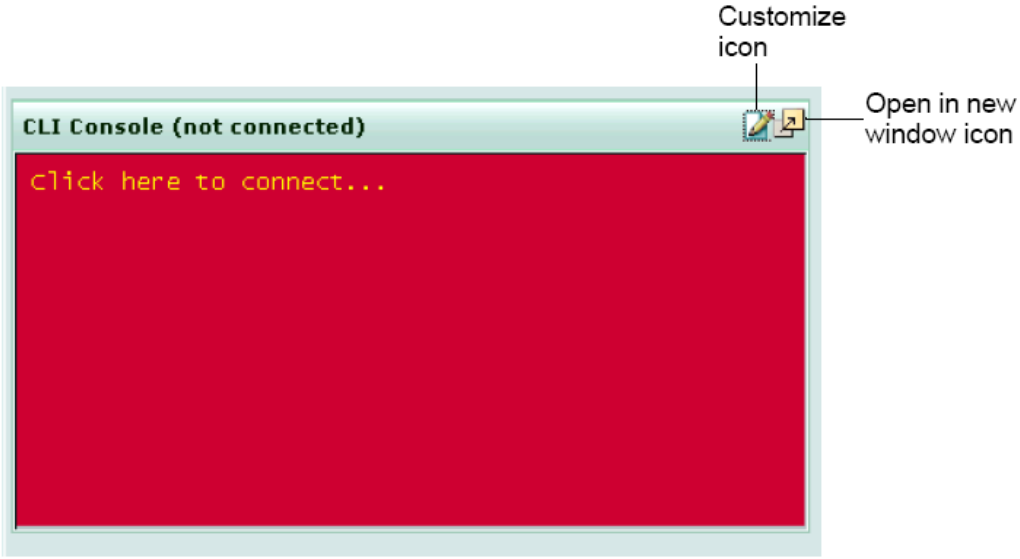
以下管理端口的性能得到增强，能够提供更有效灵活的管理：

- 对于TELNET与SSH的非标准端口
- SSHv1支持
- 两个新的CLI命令可以显示管理性登录状态，分别是get system admin status与get system admin ssh status。

CLI 控制台

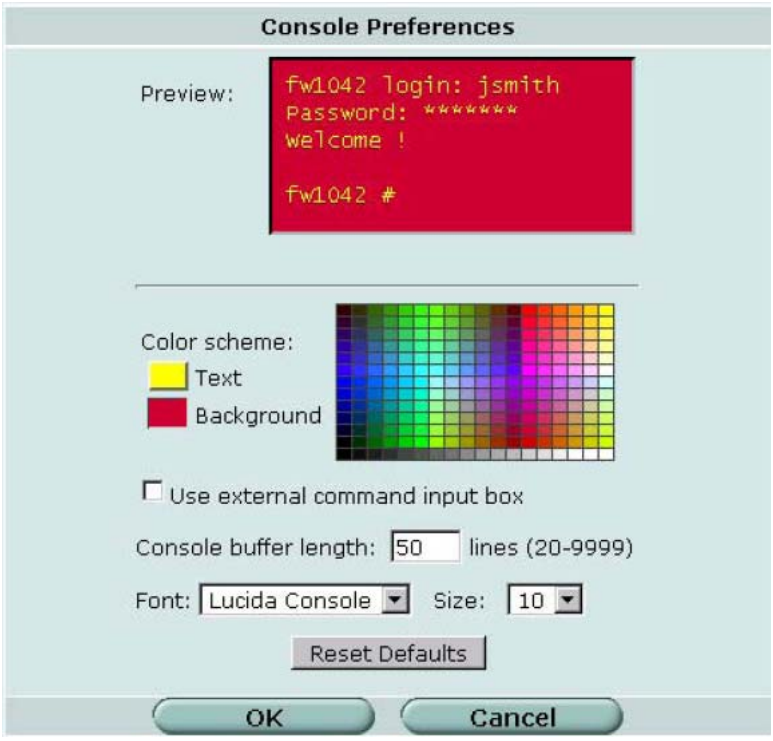
FortiOS 3.0MR3中，您可以在基于web的管理器的系统设置面板中CLI控制台显示板块查看并输入CLI命令。您可以可以点击嵌入的CLI控制台的显示背景连接到CLI。

图12：设置了背景色的CLI控制台



CLI控制台中，您可以编辑设置CLI控制台显示的背景色或在新的窗口打开控制台。如图12所示，您可以订制CLI控制台的显示窗口，包括控制台显示命令的行数。

图13：CLI控制台自定义窗口



CLI可以使用SSH登录远程系统，举例说明，一台FortiManager设备与FortiGate设备的CLI连接，使用CLI命令execute ssh<IPaddress@host>，可以使您直接连接到另外一台Fortinet产品设备的CLI。

注意：您可以利用使用终端模拟软件程序如HyperTerminal中应用exit命令退出CLI的方法同样可以退出基于web的管理器系统面板中的CLI窗口。

在 FortiOS 3.0MR3 中创建列表

在创建例如URL过滤列表或黑白列表时需要在添加列表条目之前输入配置真实列表的名称和/或注释。有关配置列表的详细信息，参见*FortiGate设备管理员手册*。

注意：FortiOS MR3对多数从FortiOS 3.0MR2升级后的列表创建了默认的名称。如需要您可以更改默认的列表名称。

FortiGate-5050 与 FortiGate-5140 设备的机架管理

FortiOS 3.0MR3中，您可以使用基于web的管理器与CLI管理FortiGate-5050与FortiGate-5140设备的机框状态。机框监控提供包括机框管理器在内的刀片的状态、温度与电压状态信息。

FortiGate-5000刀片SNMP代理可以配置在刀片温度或电压超过操作规定的阀值时发送陷阱信息。

FortiGate-5000刀片的base背板接口可以通过FortiGate-5000机框背板提供数据通信功能。Base背板接口可以使用基于web的管理器或CLI启动。也可以对base背板接口配置防火墙策略进行流量控制。

防火墙

防火墙菜单中新增了一项“虚拟IP”菜单，您可以通过该菜单管理VIP。

创建防火墙策略时，点击“新建”选项旁边的向下箭头显示新建选项与选项名称。点击“新建”创建新的防火墙策略。点击“区域名称”可以在一项防火墙策略项下创建指定名称的一行，例如指定名称为：internal->wan1，那么与这条防火墙策略有关的这些策略都将包括在新的区域中。

创建“区域名称”

1. 进入防火墙>策略，点击向下箭头的“新建”。
2. 显示“区域名称”。
3. 在“名称字段”输入名称。
4. 在开始策略ID字段输入开始策略的编号，也就是防火墙策略号。
5. 点击“OK”确认。

根据您在起始策略ID字段输入的防火墙策略ID，与该“区域名称”有关的可以是一项防火墙策略或许多防火墙策略。

通过策略菜单，您可以对每项防火墙策略添加多个地址、组或服务。

图14：在一项防火墙策略中的多个地址与服务

FortiGate设备对每个防火墙策略支持多个地址、组与服务。举例说明，如果您想设置在一项防火墙策略中具有多个地址，点击策略页面中“地址名称”旁边的“新增”。

NTML是一个微软验证协议，FSAE B015支持NTML功能。

支持基于每一用户组的验证超时。但只能使用CLI来实现。

config user group
edit localgroup
set authtimeout < (0-480 minutes)
end

如果您将authtimeout值设置为0，配置用户组使用全局超时值应该在config system global选项下配置。

策略

FortiOS 3.0MR3中，FortiGate设备处理透明模式与NAT模式下的多播流量略有不同。

透明模式下，多播转发在默认的情况下是启动的，但是必须添加具体的多播防火墙策略。可以使用CLI配置多播防火墙策略。

config firewall multicast-policy
edit 1
set srcintf source interface name
set srcaddr source address
set dstintf destination interface name
set dstaddr destination address
set nat source nat address
set action {accept|deny}
end

NAT模式下，多播转发在默认情况下是没有启动的，需要在配置具体的多播策略之前启动，类似透明模式下的操作。

config system global
set multicast-forwading enable
end

内容保护列表

在每项保护列表中，您可以存档元信息并通过选择“无”,“摘要”或“完整”设定传输的文件。只有HTTP具有“无”与“摘要”选项。

FortiClient 检测防火墙策略

FortiOS 3.0MR3中，FortiGate-1000A与FortiGate-1000AF2对FortiClient用户在防火墙策略中增加了新的限制。当这些策略启动后，通过FortiGate设备对FortiClient3.0MR2的访问限制是基于：

- 没有安装FortiClient
- 没有取得许可证的FortiClient安装
- AV或IPS数据库过期
- 没有启动AV
- 没有启动web过滤选项

如果FortiClient用户是由于以上的情况被限制访问，您可以将用户重新定向到一个能够下载FortiClient的网页。进入“系统设置>维护>备份与恢复”，如果PC被限制访问，您可以下载存储一份FortiClient 3.0MR2 固件镜像。

RADIUS

FortiOS 3.0MR3支持一级与二级RADIUS服务器。一级与二级RADIUS服务器的操作方法与一级与二级DNS服务器一样。该功能只能够使用CLI来实现。一级RADIUS服务器需要在配置二级RADIUS之前进行配置。

举例说明，输入以下CLI命令可以建立一级与二级RADIUS服务器：

```
config user radius
  edit radiusserver
    set server [IP address or FQDN]
    set secret [pre-shared key for primary RADIUS server]
    set secondary-server [IP address or FQDN]
    set secret [pre-shared key for secondary RADIUS server]
    end
```

RADIUS设置在3.0中的改进还包括:

- RADIUS请求的新属性:
  1. NAS-IP地址
  2. NAS-端口
  3. Called-Station-ID
  4. Fortinet-Vdom名称
  5. NAS标示符
  6. Acct-Session-ID
  7. Connet_Info
- RADIUS请求中对RADIUS服务器配置的IP地址选项。

- 在CLI中使用RADIUS组属性选择保护文件：

```
config user radius
   set user-group-for-profile [enable | disable]
```

- 在CLI中，使用选项对管理VDOM发送RADIUS请求：

```
config user radius
   set user-management-vdom [enable | disable]
```

VPN

FortiOS 3.0MR3中，相同的接口即可以用于SSL-VPN也可以用于HTTPS访问的管理员，即时管理员并不运行于相同的接口和/或IP地址。

一个管理员通常建立防火墙的方法如下：

- 一个专门的端口用于管理，如管理接口。
- 在内部接口启动HTTPS管理访问，允许到外部端口的SSL-VPN连接。
- 允许到各处的HTTPS管理访问，但是会配置SSL-VPN与HTTPS对不同的端口进行侦听。

SSL-VPN

FortiOS 3.0MR3中，对SSL-VPN的设置进行如下改进：

- 对下载的适当的用户机类型、Java或ActiveX进行浏览器类别的SSL-VPN检测。
- VNC Java client
- 对微软Windows中的Firefox进行主机检测
- 对微软Windows中的Firefox采用通道模式用户
- 对通道模式与web模式进行主机检测
- 对最近的AV特征进行主机检测

反病毒

反病毒远程校验查询允许对通过FortiGate设备的文件进行远程扫描。在FortiGate设备生成MD5校验和然后发送到FortiGuard数据库与已知的恶意软件进行匹配。这种情况下，FortiGate设备就能够扫描比本地FortiGate数据库更大型的FortiGuard数据库。本地的FortiGate数据库因为闪存的容量而有存储有限。进行以下配置启动AV查询：

- 进入“系统>维护>FortiGuard中心>web过滤与反垃圾邮件”选项，启动到FortiGuard服务的连接。
- 使用以下CLI命令配置AV查询：

```
config firewall profile
   edit myProfile
      set <http| ftp | pop3| smtp| imap| im| nntp|>
      avquery
```

SNMP陷阱现在包括超大文件、分片邮件与文件名屏蔽模式。

NNTP也是能够支持的。使用基于web的管理器或CLI都可以配置NNTP。通过NNTP传输文件的内容存档在该固件发布中不可用。

反垃圾邮件

在反垃圾邮件菜单中，被识别为垃圾邮件的邮件，支持使用邮件协议IMAP、POP3与SMTP，可以存档到FortiAnalyzer设备。默认情况下，该功能没有启动。

IM/P2P

IM/P2P菜单下，微软Live Messenger 8.0与Yahoo！8.0 IM用户可以设定聊天会话形式并可以将会话内容存档。

日志与报告

您可以从日志与报告菜单下查看内容存档日志。FortiAnalyzer设备存储内容存档日志。

日志文件名称定义具有非常明确的命名格式，清晰的定义了日志类型、FortiGate设备序列号、VDOM以及日志存储的日期与时间。例如名为tlog.FG500A2904123456.vdom2—NAT.20060810235959。只有在升级到FortiOS 3.0MR3后建立的日志文件具有这样新的命名语法。

使用CLI命令execute backup memory可以启动将FortiGate设备中备份的日志文件存储到一个远程服务器。

进入“日志与报告>日志配置”，您可以在FortiAnalyzer报告中添加P2P活动报告。CLI中可以反映出这样的设置添加。

每项IPS特征与异常都设定了相应的严重性级别。可以在攻击日志文件或alog.log中查看到这样的信息。这些日志文件现在具有新的日志文件名称。

内容存档

从内容存档菜单，您可以查看存储在FortiAnalyzer设备的内容存档。内容存档菜单在相对的项目栏中显示有关FTP、Email以及IM内容存档日志。如果您要查看邮件内容存档日志，您可以电机主题栏中相应的链接，可以独立的窗口查看邮件。

HA

FortiOS 3.0MR3中，从属设备将被其隔离的文件发送到主设备，主设备接收到隔离文件后传输到FortiAnalyzer设备。

FortiOS 3.0MR3可以同步HA从属设备中用于验证的本地、LDAP、FASE与

NTLM的策略。使用IPSec的防火墙策略现在也可以同步到从属设备。

公知信息

FortiOSMR2中有关的公知信息继续存在于FortiOS3.0MR3中。其它信息将在下文中说明。

FortiWiFi-60A/AM设备支持WPA2，增强了无线安装性。

基于 web 的管理器

涉及到所有需要使用基于web管理器进行的操作。

- 当启动DVOM模式时，FortiGate设备不能够自动退出与控制台连接的管理员。
- 一个只具有读的权限的管理员（即使只启动了一些访问）不能够使用面板上的内嵌CLI控制台。
- 状态页面中弹出的当前管理员窗口可能显示大于实际登录数量的管理员信息。
- 升级到FortiOS 3.0MR3时，所有在MR2中创建的列表都具有默认的名称。FortiOS 3.0MR3 要求多数的列表具有名称和/或注释。举例说明，当URL过滤列表升级到MR3.0后，被重新命名为“已定义url过滤”。如需要，点击“编辑”图标，您可以重新命名默认的名称。

虚拟域

- 当启动VDOM后，状态页面中的“内容存档”与“攻击日志”统计表数据不会更新。这是因为这些数据均是在全局设置维护的，并不是基于每个VDOM的。

路由

该操作只涉及到在路由菜单中的操作：

- 当一个静态寻址模式接口配置静态缺省路由更改为DHCP后返回到静态缺省路由时，FortiGate设备不能形成路由表。使用CLI命令execute restart router重新启动路由程序。

防火墙

防火墙的操作涉及到使用基于web管理器与CLI。

- FortiGate设备不能执行在RADIUS服务器配置的硬性超时设置值。
- SSL-VPN策略中“用户验证方式”在被选的用户组或验证方式下不能生效。
- FortiOS 3.0MR3加强了内容存档功能，提供了三项显示内容存档的方式，分

别为“无”“摘要”与“全部”，详细信息参见FortiOS3.0 MR3的发布说明。

- 在内容包含列表中“内容存档”栏，存档被识别为垃圾邮件的邮件时，您需要选择“全部”。只有“全部”选项可以将被识别为垃圾邮件的邮件备份存储到FortiAnalyzer设备。

即时消息

即时消息的操作只涉及到基于web的管理器的使用。

- 当编码后Yahoo！流量通过端口80将不服从于IM后台程序的处理。通过端口80传输的文件将被屏蔽。
- 下表信息是有关MR3支持的每项IM协议的有关信息：

IM 用户	版本	描述
AIM Classic	5.9.3861	● 用户使用非加密或加密 AIM 版本时，不能够与其它 AIM 用户进行视频连接。 ● NetMeeting 使用 H.323 不能建立连接。这样的情况在所有 AIM 非加密与加密的用户中都存在。
AIM Triton	1.2.80.1	● 当受感染的文件被屏蔽时，FortiGate 设备不能显示替换信息。 ● 用户使用非加密或加密 AIM 版本时，不能够与其它 AIM 用户进行视频连接。 ● 当一个 AIM 用户从另一个 AIM 用户接收文件时，FortiGate 文件数目统计将不增加。这样的情况在所有 AIM 非加密与加密的用户中都存在。 ● 用户文本信息内容以及文本格式信息将在即时信息内容日志中显示。 ● NetMeeting 使用 H.323 不能建立连接。这样的情况在所有 AIM 非加密与加密的用户中都存在。
AIM	5.9.3861	● 使用了到 AIM 加密的直接连接。所有的连接请求都将失败，除非取消 AIM 加密的使用。这样的情况在所有 AIM 非加密与加密的用户中都存在。 ● 当 ICQ/AIM 使用其它端口（非 5190 端口）登录，登录被屏蔽的事件将不被记录在 FortiGate 设备的日志中。 ● 包含的日文的 IM 系统替换信息不能正常显示。 ● 用户文本信息内容在文本格式的即时消息内容日志中不显示。
ICQ	5.10	● 在 NAT 模式 FortiGate 设备之后的 ICQ 用户之间不能建立视频与音频会话。 ● 当用户建立聊天会话时，FortiGate 按协议区分的聊天会话统计并不增加。 ● FortiGate 设备之后的用户不能够与多个不同的防火墙产品后的 ICQ 用户进行多用户聊天连接。 ● 用户文本信息内容以及文本格式信息将在即时信息

		内容日志中显示。 ● 当 ICQ/AIM 使用其它端口（非 5190 端口）登录，登录被屏蔽的事件将不被记录在 FortiGate 设备的日志中。 ● 包含的日文的 IM 系统替换信息不能正常显示。
MSN	7.5	● MSN 7.5 版本中，不能建立视频/音频通信。
Yahoo！Messenger	8.0.0.701	● 当用户通过 FortiGate 设备对其它 MSN 用户发送消息时，会话统计计数不正确。 ● Yahoo!7.0 版本中，不能屏蔽音频通信。

- FortiGate设备可以从IM用户登录时就对其采取屏蔽动作，但是不能控制如果IM用户使用HTTP通道进行的通信流量。这里的IM用户涵盖所有的IM即时通信协议使用用户。
- 如果“IM屏幕名称”是以敏感字符编辑的，那么FortiGate设备不能屏蔽用户列表中的IM用户。这里的IM用户涵盖所有的IM即时通信协议使用用户。

P2P

有关P2P的操作只涉及到基于web的管理器。

- 下表信息是有关MR3支持的每项P2P协议的有关信息：

P2P用户	版本	描述
Azurenus/BitTorrent	2.5	FortiGate设备不能够屏蔽AzurenusP2P用户。
Phex/Gnutella	2.8.10.98	FortiGate设备不能够屏蔽PhexP2P用户。
Winny	2.0b7.28	FortiGate设备不能够屏蔽WinnyP2P用户。但是这一版本除外。
Skype	2.5	FortiGate设备不能够屏蔽SkypeP2P用户。

IPS

- 用户定义IPS特征在恢复到出厂默认设置以及恢复保存的之前的用户定义IPS特征后仍然能够保留。CLI中，在恢复用户定义IPS特征之前使用config ips custom下的清除命令。

日志与报告

日志与报告涉及到使用基于web的管理器与CLI的操作。

- 当FortiGate设备获得FortiAnalyzer设备的IP地址后，点击“测试连接”避免发生错误报告故障。如果FortiGate设备与FortiAnalyzer设备配置使用FDP获取并建立连接，会有将近10秒钟的延迟。
- FortiOS3.0 MR3 中对过滤日至文件的日志搜索功能进行了修改。流量日志中一些日志数据因为这样的更改而不能进行过滤，这些流量包括：

流量日志：

- 序号
- 源地址名称
- 目标地址名称
- SentReceived
- SentPacket
- 接收到的数据包
- 源端口
- 组
- Dir显示
- Tran显示

只有“精确匹配”或“前缀匹配”时才被支持。

- 当一个文件模式在被允许列表中时，通过POP3、SMTP、IMAP与NNTP协议下载文件带来.exe扩展名的文件均不能进行日志记录。HTTP与FTP不受影响。
- Syslog 日志文件以CVS文件格式存储，在“日期”与“时间”字段之间没有逗点分隔。在“vd”与“用户”字段之间以分号（;）分隔，而不是逗号（,）。
- FortiGate设备不能够正确进行事件日志记录，当它实际被删除时会添加访问权限内容。
- 在过滤攻击日志时，在点击攻击日志页面中过滤图标时，弹出窗口不显示。您可以在栏目设置链接中删除“攻击ID”条目，然后点击漏斗形图标执行过滤操作。

解决方法

以下提供了一些方法解决升级后某些公知信息中提到的问题。

- 使用CLI命令可以查看在基于web管理器中不能显示的回环接口。
- 当FortiGate设备不能使用CLI命令config sys global指定源端口范围中的端口时，重新启动防火墙。
- 使用CLI命令不能访问VDOM中预定义的防火墙服务时，可以使用基于web的管理器实现该操作。

FortiOS 3.0MR4

FortiOS3.0 MR4在MR3的基础上增加的新的功能以及对原有功能进行了改进。新的功能包括对每个接口增加二级IP地址，提供显示配置拓扑结构图以及对VoIP电话进行日志记录并可以进行查看。

FortiOS3.0MR4中对以下方面功能进行了改进与增强，包括VDOM、路由与VIP负载均衡。

本章包括以下内容：

- 新增功能与功能更改
- 公知信息

FortiOS3.0MR4 增加了几项新的功能，以及对原有功能修改。以下将做详细说明。

在将系统升级到 FortiOS 3.0MR4 之前，建议阅读本技术文档以及以下所列技术文档，熟悉增加的新功能以及一些功能的更改。

- FortiGate 设备管理员使用手册
- FortiGate 设备 CLI 使用参考
- FortiGate 设备 HA 概述

警告：建议升级到 FortiOS 3.0MR4 补丁。MR4 补丁解决了 FortiOS 3.0 中影响关键功能的几项公知信息。已解决的公知信息包括：

- Windows 更新需要花费较长的时间来完成。
- FortiGate-3600A 允许在一些端口中通过一项拒绝策略进行某些会话分割。
- 对于 FortiOS 3.0MR4，不能修改 IPS 特征的严重性级别。
- 简化基于 web 管理服务器负载均衡
- 实现基于每项策略的流量计数

注意：参见 FortiOS 3.0MR4 发布说明中有关“已解决的公知信息”章节，获得更详细的信息。有关 FortiOS3.0MR4 升级的信息，参见“更改固件版本”中的叙述。

新增功能与功能更改

以下信息只涉及新增加的功能与一些功能的更改。当出现具体的应用时同时说明程序性信息。

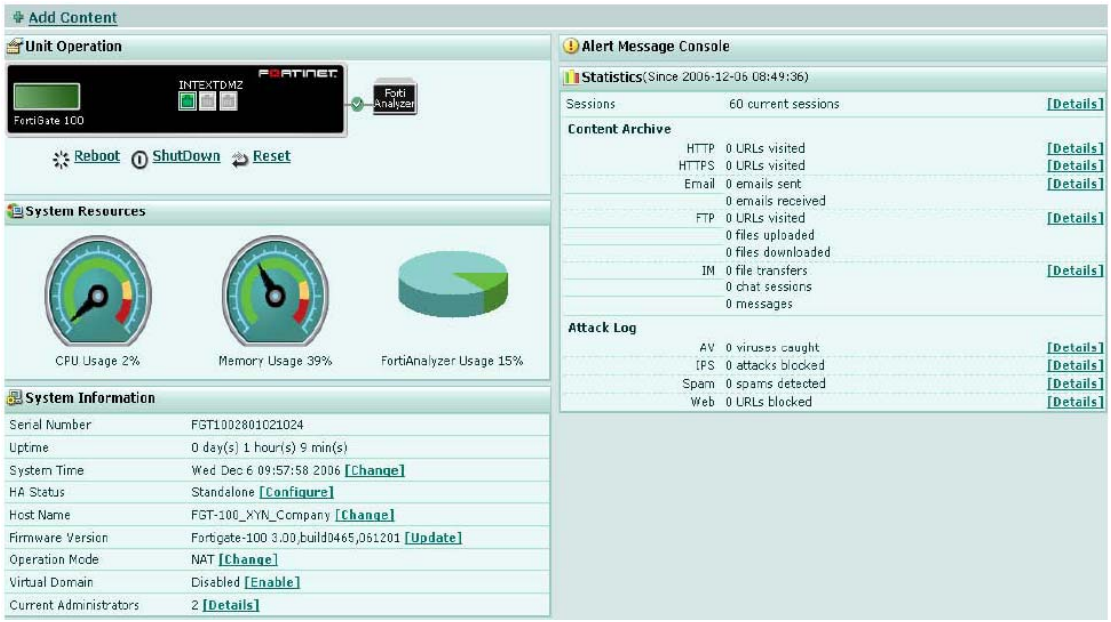
系统设置

MR4 增强了系统面板的功能。您可以在面板中移动各功能区域。类似于FortiOS3.0MR2 中的防火墙策略，您可以拖动策略移动到面板中的任何位置。将鼠标移动到面板中任何一显示板块名称的旁边，点击出现的箭头，可以折叠或

扩展板块，类似其它菜单中的蓝色箭头功能。您也可以点击每个板块类型右上角中显示的 X 型，隐藏板块。您也可以点击面板上方“添加内容”将隐藏的板块返回到面板中。图 15 显示将板块类型系统的系统面板。

您可以点击面板上方的刷新图标刷新面板。

图 15：FortiGate-100 设备的系统面板，其中隐藏了 CLI 控制台与许可证信息显示板块



“重启系统”、“关闭系统”、“重新设置”这些选项都设置在“设备操作”板块中。当您点击其中任何一个选项，将会弹出可以窗口需要您输入“重新设置 FortiGate 设备”、“关闭设备”以及“重新启动设备”的原因。这些原因的描述信息都将记录到日志信息，例如以下信息中的黑体字显示：

2006-12-09 15:09:06 log_id=0104032138 type=event subtype=admin pri=critical vd=root user= “admin” ui-GUI (142.50.140.1) action=reboot msg=“User admin rebooted the device from GUI (142.50.140.1). **The FortiGate unit was rebooted for testing purpose.**”

注意：退出基于 web 的管理器之前进行对面板显示板块的重新排列不能够保存。调整后面板显示将在每次退出/登录基于 web 的管理器后显示。

网络接口

进入系统>网络接口，您可以对每个接口配置二级 IP 地址，最多可以配置 32 个二级地址。一级与二级 IP 地址可以共享同一个 ping 发生器。

在对接口配置二级 IP 地址前，您需要：

- 配置一级 IP 地址
- 启动“手工寻址”模式
- 如果允许系统子网重叠，使用 config system global 命令

默认情况下，IP 地址不能是相同子网的一部分。您需要允许系统子网交叠。您可以使用 system global 命令配置系统子网交叠。详细信息，参见 FortiGate 设备 CLI 使用参考手册。

访问控制列表

对管理员配置访问控制列表时，您可以选择在防火墙配置中只允许对某些防火墙策略配置的访问。当您点击蓝色箭头扩展防火墙策略配置选项时，您可以选择设置允许管理员对以下配置之一或全部进行访问：

- 策略配置
- 地址配置
- 服务配置
- 时间表配置
- 内容保护文件配置
- 其它配置

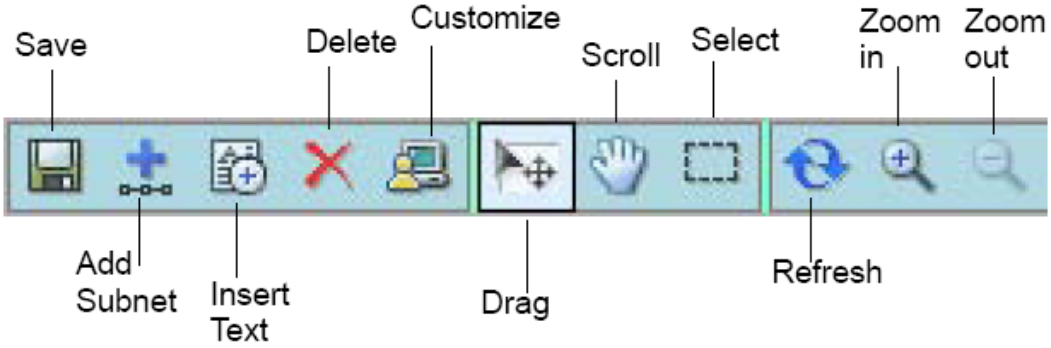
拓扑结构

“拓扑结构”是状态菜单中新增的功能。在拓扑功能栏，您可以图表结构的网络配置。以图表显示的网络结构下，您可以快速查看每个接口的连接情况，和/或 FortiGate 设备到 FortiAnalyzer 设备或到 FortiManager 设备的连接；也可以编辑和/或配置网络配置。

注意：只有对防火墙具有读写权限的管理员或对系统具有读写权限的管理员才可以配置与编辑拓扑结构图。FortiGate 设备需要有 256MB 的 RAM 维持拓扑酮能的操作。

您点击“编辑”图标后，可以编辑或配置拓扑结构图。

图 16：拓扑结构图的编辑/查看图标



保存(Save)	点击保存拓扑结构图。当您对拓扑结构进行修改后，点击“保存”及时存储配置更改。
添加子网 (Add subnet)	点击图标对接口添加防火墙策略。这些连接称为子网。

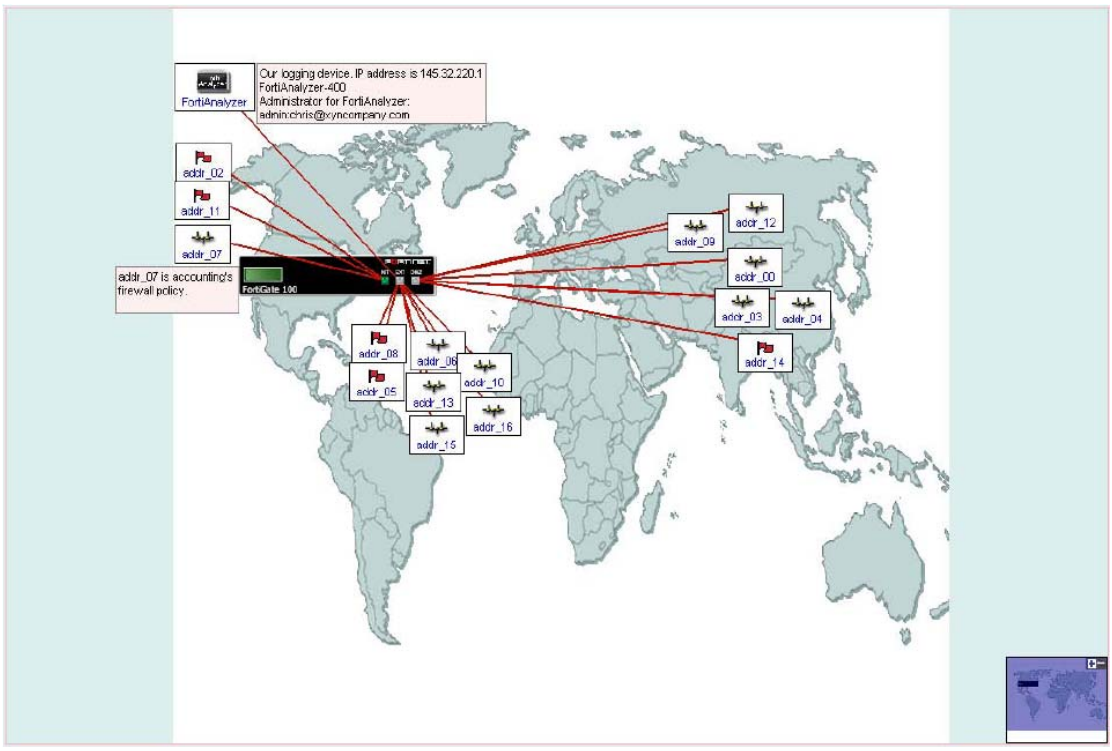
插入注释 (Insert Text)	点击图标对子网添加注释或描述。
删除(Delete)	点击图标删除子网连接。
用户定制 (Customize)	点击图标定义拓扑结构显示背景、线条颜色以及显示图像大小。您可以选择使用美国地图或世界地图作为背景或自选图像。图 17 为使用世界地图的背景。
拖动(Drag)	点击拖动结构图中的图示，将其放置在拓扑结构中任何选定的位置。
手形工具 (Scroll)	点击固定拓扑结构图显示比例查看图表。
选择(Select)	选定查看拓扑结构图。
刷新(Refresh)	点击刷新拓扑结构图页面。只有在查看或编辑和/或配置拓扑结构图时，该图标是可见的。
放大(Zoom in)	点击放大显示拓扑结构图。只有在查看或编辑和/或配置拓扑结构图时，该图标是可见的。
缩小(Zoom out)	点击缩小显示拓扑结构图。只有在查看或编辑和/或配置拓扑结构图时，该图标是可见的。

网络配置的复杂性决定拓扑结构图的显示。如图 17 所示，网络管理员配置 FortiGate 设备连接到一台 FortiAnalyzer 设备，并对网络拓扑结构图中的某些连接添加了注释。

图 17 右下方是缩小版的结构图显示。您可以不在使用结构图页面上方图标的情况下放大或缩小或查看结构图的不同区域。

如果您在 VDOM 配置下，拓扑结构图功能不可用。有关 FortiOS3.0MR4 中 VDOM 的详细信息，参见 FortiGate 设备管理员手册。

图 17：FortiGate-100 的拓扑结构图



多个 DHCP 服务器的 IP-MAC 绑定

对多个 DHCP 服务器 IP-MAC 绑定功能可用。FortiOS3.0MR4 在配置两个不同的 DHCP 服务器时也支持 IP-MAC 绑定功能。如果一个 DHCP 用户是多功能型，需要在所有的 DHCP 用户接口设定 IP-MAC 绑定。您可以在 DHCP 用户要求每次获得一个具体 IP 地址时应用 IP-MAC 绑定功能。

硬盘健康状态监控（HDD）

硬盘健康状态监控（HDD）功能以自身监控分析与报告（SMART）系统诊断潜在的硬盘故障。SMART 是针对计算机设备硬盘，检测与报告可靠性指标并进行预警的开放标准监控系统。

通过程序性的查询SMART诊断程序，可以对潜在的硬盘故障发出较早的警告。当第一个故障发生后，生成一个报警控制信息，并在每次故障发生后生成一个危急日志。

diagnostic解释命令包括两个新的HDD命令：

diagnose sys logdisk smart

diagnose sye logdisk usage

命令行接口

使用CLI，您可以备份全部的配置以及每次设置时全部默认的设置值。您可以将配置文件保存到FortiUSB或一个TFTP服务器。

execute backup full-config<tftp|usb> filename ip [password]

不均衡的路由现在是基于每个VDOM设置，使用system settings命令可以显示。

PPTP地址范围中的起始与结束IP必须是相同级别的子网的地址。以下所示的PPTP地址起止范围是无效的：

```
config vpn pptp
  set status enable
  set usrgrp test-group
  set sip 192.168.10.1
  set eip 19.168.11.250
  end
```

FortiGuard-web 过滤与反垃圾邮件服务

FortiGuard-web过滤与反垃圾邮件服务结合对改善URL的提交包括反垃圾误报的正确性的提交。

FortiGuard-web过滤URL提交页面现在需要输入您的名字、公司与邮件地址才可以接受进行URL的查看。建议您在发送提交内容之前查看所填写信息的准确性。

FortiGuard-web过滤URL提交页面也包含CAPTCHA（Completely Automated

Public Turing）测试，对发送URL提供了更好的安全性。

反垃圾邮件误报特征提交页面输入邮箱地址，但是姓名与公司并不是必添项。您也必须确认所提交的垃圾邮件特征是垃圾邮件或干净邮件，提高了提交的正确性。反垃圾邮件误报特征提交页面与URL提交服务器是由同一个服务器托管，总是可用的。

VDOM

进入系统设置>状态，启动VDOM。当您在系统信息中点击“启动”时，基于web的管理器将自动将您退出登录状态。您再次登录到基于web的管理器后，VDOM便启动了，并且进入系统设置>VDOM便可以对VDOM进行配置。VDOM菜单只有在启动VDOM后出现。

VDOM菜单下，您可以实现配置、编辑、删除以及切换VDOM的操作。如需要，您可以对每个配置的VDOM配置管理访问权限。

启动VDOM后，某些VDOM只允许对FortiGate设备一部分功能的访问。建议在您所处的VDOM校验是否能够对您需要配置的FortiGate设备的功能进行访问。

路由

路由功能中包括IETF标准化双向转发检测协议（IETF standardized Bi-directional Forwarding Detection）。BFD是高速单机HELLO协议，类似于其它路由协议如OSPF。这些协议可以应用于接口、通道、路由或其他网络转发设备。

BFD需要通过OSPF与BGP来实现。BFD先要进行协议配置，路由协议是根据配置分配的。协议配置是基于每个VDOM的。对于每个VDOM有一个全局设置，可以对VDOM的所有接口启动BFD，以及全局计时数值。在每个接口，全局设置可以被接口中的BFD设置覆盖。BFD通过CLI进行配置，参见FortiGate设备CLI使用参考手册获得详细信息。

路由功能的加强还体现在路由重启。路由重启可以使用FortiGate设备重新启动路由后台程序时将对流量的影响将到最小化。该功能应用在HA中，当群集中主设备故障，需要从属设备接替主设备的情况下。该重启功能只可以使用CLI来实现，详细信息参见FortiGate设备CLI使用参考手册。

注意：MR4 中BGP路由协议具有MD5密码验证，只在CLI中可用。

防火墙

防火墙菜单增加新的功能，基于协议的验证，并加强了VIP负载平衡功能。进入防火墙>策略，您可以查看通过防火墙策略的数据包量。

基于每项协议验证可以使管理员控制使用用于验证的协议，如HTTP、HTTPS与Telnet。举例说明，如果对FTP启动了验证，FortiGate设备收到用户发来的FTP请求后会要求输入用户名与密码。对于接下来从同一个用户发送的消息，不管使用任何传输协议都被允许通过。例如，如果只启动HTTP，那么意味着撤消了

HTTPS、FTP与Telnet，也就是说用户试图发送Telnet连接时，FortiGate设备不会要求用户输入用户名与密码，只有使用HTTP时才会要求进行验证。对于HTTP验证的另外一项功能是在不断发送的请求可以被重新定向使用HTTPS，该功能可以在基于web的管理器中进入“用户>验证”，以及在CLI命令global shell命令下实现。

MR4加强了VIP负载平衡功能。FortiGate设备可以在VIP配置下设置多个不连续应射IP地址。设置了VIP负载平衡，FortiGate设备也可以Ping服务器以此来判断该服务器是否在使用中。VIP负载平衡设置只能使用CLI实现。

在MR4中，当设置匹配的策略时，建议考虑以下因素，因为SSL VPN策略将对SSL通道模式检索主机IP地址：

- 需要验证的策略必须添加到策略列表中不匹配策略之前。否则，不需要验证的策略将优先被选。
- IPSec VPN通道模式策略必须添加在策略列表中匹配接受或拒绝策略之前。
- SSL VPN策略必须添加在策略列表中匹配接受或拒绝策略之前。

策略

防火墙策略列表页面包括与每项防火墙策略对应的会话计数。每项防火墙策略的计数栏显示次数以及防火墙策略匹配的字节数。计数栏只有在被选中后才生效。

在一个数据包到达防火墙并与策略相匹配是将创建议一条新的策略会话。这条匹配防火墙策略的第一数据包将记录在新的策略会话计数中。后续的数据包将不予考虑。

当FortiGate防火墙策略重新启动时，以及重新配置或删除防火墙，计数器也需要重新设置。默认的情况下将启动新的策略会话计数。

VPN

VPN菜单增加的新的功能，一级与二级IPSec阶段1接口；并增强了公共秘钥架构（PKI）功能。

相对FortiOS3.0MR4，建议先升级到FortiOS3.0MR4补丁版。如果您升级到FortiOS3.0MR4，所有的SSL VPN通道都将崩溃。MR4补丁可以保持在升级时所有的SSL VPN通道都是正常的。

一级与二级IPSec阶段1是对IPSec接口定义的。该功能允许定义一个VPN，在一级接口中断时，二级接口可以进行接替；并且在一级接口恢复时，二级接口自动关闭。上述情况通常发生在当二级接口通过设置调制解调器作于一级IPSec接口的冗余。一级与二级IPSec阶段1接口的功能只可以使用CLI来实现。

加强管理访问IPSec、SSL VPN的基于证书验证与基于web的验证在MR4中很重要。以下是MR4中PKI功能增强的体现：

- 所有有效的用户验证必须是没有过期且由CA签发的证书。
- 用户证书有效期可以包括从CRI或从在线证书状态协议（OCSP）服务器获得的证书撤销状态中的一个或者全部。
- 支持从LDAP或HTTP服务器进行自动的CRL升级。

- 在用户证书中可以使用普通名称（CN）执行活动目录（Active Directory）查询，以判断用户的访问权限。例如，LDAP查询识别是否 CN是在正确的设置组，并是该组成员之一。
- 支持较大的CRL文件。
- 支持SCEP发送证书请求到一个CA服务器并且获得CA签发的证书，从CA服务器获取CA证书，或从CA证书获取CRL证书。

导入CA与CRL证书时，您可以指定导入证书的地址。您可以指定将CRL证书导入四个地址，指定CA证书导入两个地址。

对于SSL VPN功能，“RDP到主机”选项web模式可以在用户连接到一个服务器时接受键盘布局设置作为参数。在“RDP到主机”字段，包括以下信息：
<IP地址或服务器的FQDN>-m<语言>
<语言>可以是以下任何一种：

ar-阿拉伯语	fi-芬兰语	it-立陶宛语	pt-br-巴西语
da-丹麦语	fr-法语	lv-拉脱维亚语	ru-俄语
de-德语	fr-比利时式法语	mk-马其顿语	sl-斯洛文尼亚语
en-bg-英语	hr-克罗地亚语	no-挪威语	sv-色当语
en-美式英语	it-意大利语	pl-波兰语	tk-土库曼语
es-西班牙语	ja-日语	pt-葡萄牙语	tr-土耳其语

“用户”菜单中增加了新的栏目，分别为PKI与验证。

“验证”功能之前在“系统设置>管理员>设置”项下进行配置，现在设在“用户”菜单中，并可以选择您需要验证的协议，包括：HTTP、FTP、HTTPS与Telnet。您也可以启动“将HTTP重新到HTTPS”，这之前，您需要先启动HTTPS。PKI菜单中，您可以创建与编辑PKI用户。详细信息，参见FortiGate设备管理员手册有关用户菜单中PKI章节。

入侵防护

FortiGate设备能够将IPS信息以邮件形式发送到FortiGuard服务器以检测IPS特征。该功能可以进入“系统设置>维护>FortiGuard中心”或使用CLI命令ips global启动。FortiGate设备发送以下信息：

- 序列号
- 事件日期与时间
- 报告持续时间
- 网络协议源IP地址与端口，目标IP地址与端口
- 漏洞ID与特征ID
- 在报告持续的时间段内入侵发生的次数
- 匹配的规则的版本ID
- IPS特征发布版本与引擎版本

MR4中对基于web管理器中的IPS菜单进行了更改。以下是菜单中涉及的更改信息：

- 访问所有预先定义的特征，需要进入“入侵防火>特征>预先定义”。
- 在协议解码器页面，只能对端口数量进行更改。在“预定义页面”您可以配置并启动数据包日志的动作。
- 预先定义特征的严重性级别设置是建议设置的级别，不能进行更改。

- 预定义页面中许多栏目中增加了过滤选项。除了名称字段，所有的字段都是大小写敏感的。在以后发布的版本中，所有的字段都将支持大小写敏感。
- IP主机地址与子网地址免于限制于IPS预先定义的特征。例如，如果您想排除主机IP地址172.16.100.100作为源与目标地址，您可以输入172.16.100.100设置免除。

Web 过滤

MR4中，加强了FortiGuard web过滤跳过功能，新增了“FASE组”，该功能只在防火墙用户组中可用。

IM、P2P 与 VoIP

从IM/P2P菜单，您可以查看并对VoIP通话设置日志记录。VoIP的应用，可是实现通过互联网进行电话般的通话，使用IP代替传输的电路传输发送语音数据包。

您可以查看丢弃的VoIP以及连接失败的VoIP通话，使用VoIP连接成功的通话以及当前VoIP通话总数。您也可以查看活动的VoIP会话，如连接的通话等等。在内容保护文件中，可以启动对VoIP通话进行日志记录。详细信息，参见FortiGate设备管理员手册。

日志与报告

日志与报告菜单中，包括新的日志设备，分别为FortiGuard日志与分析服务。该日志设备类似于Syslog服务器或Web Trends服务器，从FortiGate设备设置将日志提交到FortiGuard日志与分析服务。该功能是基于请求的。

FortiGuard日志与分析订购服务只在FortiGate-100或该型号以下的FortiGate设备中可用。

如果您的网络配置使用了VoIP，您可以对VoIP通话设置日志记录。VoIP日志文件是plog。plog文件记录违规，但不包括已经记录到IM日志文件(ilog)里的简单协议违规。所有的日志信息，由被允许的VoIP流量产生并发送到内容日志（clog）。VoIP日志也存储在FortiGate设备的系统内存中。

下表显示与每项VoIP日志文件类型有关的日志信息类型。

信息类型	日志文件
SIP发起通话	clog
SIP结束通话	clog
SIP被屏蔽	plog
SCCP电话注册	clog
SCCP通话信息	clog
SCCP被屏蔽	plog
SIMPLE日志信息	clog
SIMPLE屏蔽信息	ilog

报告配置

报告配置菜单包括一个新的CLI命令multi-report，用于配置多个FortiAnalyzer报告。升级到MR4后，报告配置页面，在multi-report命令还没有启动时，对FortiGate设备显示默认的FortiAnalyzer报告。如果启动multi-report命令，报告配置显示的信息与升级到MR4之前的一样。

当启动“多个报告”后，您可以配置FortiAnalyzer报告、查看引擎状态或任何生成的报告，以及什么时候生成设置的下个阶段的报告。

报告配置菜单包括从日志数据信息选择的类别显示，按照以下顺序：

属性	点击可以自定义页眉与页脚，包括公司名称。该选项是可选的。属性类别之前命名为“用户化”。
报告范围	点击选择报告中需要包含的信息项目。
报告类型	点击报告所包括的类型。
报告格式	使用变量处理主机名称或报告排列的顺序。
输出	点击选择报告的文件格式。您也可以配置将生成报告发送到的邮件地址和/或设置上传报告到FTP服务器、SFTP服务器或SCP服务器。
时间表	设置FortiAnalyzer设备生成报告的时间频率，如每周或每月。
摘要版面	从26可选不同的图示显示中选择报告显示的格式。您也可以选择显示这些摘要的栏目数或编辑和/或移出列表。

高可用性（**HA**）

FortiOS 3.0MR4固件可以使用FA2加速加强主动-主动HA模式的负载平衡。FA2加速功能只有在设有FA2接口的FortiGate设备中可用，如FortiGate-1000AFA2，5001FA2与5005FA2。

HA群集中主设备的功能会受到主动-主动模式的负载平衡的影响。主设备英国有必需的CPU周期以及总线带宽来接收并发送数据包到从属设备。在一个较繁忙的主动-主动模式HA群集中，主设备可能不能赶得上处理中的负载。那么，这就可能导致丢包以及主设备发送心跳数据包延迟。

FortiOS MR4主动-主动HA模式使FA2设备将在FA2接口接到的数据包发送到从属设备。这种情况下，每个新的会话的第一个数据包仍然由主设备接收，并且主设备使用其负载平衡时间表来决定群集设备处理话该会话。有关所有会话的信息将由从属设备处理并发送到FA2设备。然后，所有的设备在不使用主设备CPU或总线的情况下直接发送到从属设备。这样设置的结果减小了主设备的负担，并能维持一个快速稳定的主动-主动HA群集。

FA2 FortiGate设备组成群集应用于主动-主动模式，利用FA2加速连接到最繁忙的网络。连接非加速的网络到相对不很繁忙的网络。不需要特殊的FortiOS配置。主动-主动HA负载平衡中FA2加速对任何主动-主动HA配置均支持。

公知信息

FortiOS3.0MR3中的公知信息将延续在FortiOS3.0MR4中，除非另有注明。建议升级到FortiOS3.0MR4补丁，补丁的发布解决了Forti3.0MR4中影响主要功能的几项公知信息。

基于 web 的管理器

- FortiGate-100A与FortiGate-200A改版1中基于web的管理器不时地会显示“切换模式”按钮。“切换模式”功能在序列号以FG100A2905或FG200A2905起始的FortiGate-100A与FortiGate-200A改版2中可用，点击该按钮，显示切换模式的管理页面，但是任何设置更改都不被保存。只有FortiGate-100A与FortiGate-200A受影响。
- 启动VDOM模式将导致自动退出管理员对console控制台的登录。
- 状态页面中，当前管理员窗口现在能够正确显示登录管理员数量。
- 对服务器负载平衡简化基于web的管理器。升级使用FortiOSMR4补丁版本可以解决该问题。

系统设置

系统设置涉及到使用基于web管理器与CLI的操作：

- FortiGate-60在电源周期开关周期不能发送冷启动SNMP。
- VDOM启动后，当选择一个超级管理员访问权限时，出现虚拟域字段。对于一个虚拟域来讲没必要设置超级管理员。
- PKI管理用户如果将证书安装在本地PC或将CA证书安装在FortiGate设备，那么即时退出基于web的管理器，还可能会在web管理器中显示。当PKI用户使用HTTPS登录基于web的管理器然后退出时，web管理器页面仍然显示PKI用户。
- 当您在Windows2000或WindowsXP中点击“开始>Windows更新”时，Windows更新功能不能正常工作。您需要升级到FortiOS3.0MR4补丁解决该问题。

虚拟域

虚拟域涉及到使用基于web管理器与CLI的操作：

- 当VDOM启动后，状态页面中内容存档与攻击日志统计信息将不进行更新。这些统计信息不是基于每个VDOM的。对VDOM配置保持的统计信息是针对管理虚拟域的。
- FortiGate设备不能从虚拟群集配置中的非管理器VDOM发送报警邮件，在该虚拟域中群集中的主设备与第一虚拟群集具有不同的主机的情况下。

高可用性（HA）

高可用性涉及到使用基于web管理器与CLI的操作：

- FortiGate-100A与FortiGate-200A（改版2）设备使用了比改版1更高级的芯片。该芯片可以使您配置四个内部接口作为一个第四接口或四个独立的接口。使用改版2与改版1FortiGate-100A或FortiGate-200A不能形成一个HA群集。改版2的设备序列号是从FG100A2905或FG200A2905开始。
- HA中route-ttl命令的默认值是10。

防火墙

防火墙涉及到使用基于web管理器与CLI的操作：

- 防火墙时间表不支持web模式或通道模式SSL-VPN。升级使用FortiOS3.0MR4可以解决该问题。
- 预先定义的防火墙服务，如果使用CLI访问，将不在VDOM中显示。使用基于web的管理器查看预先定义的防火墙服务。
- 对于动态DNS设置vavic.com的协议更改，Fortinet公司正在与服务商协商解决该问题。
- 当FortiClient查看的“声明”启动后，用户将被重新定向到下载页面。当验证与FortiClient查看同时启动时，FortiClient查看功能不能生效。
- 当使用带有web验证的Konqueror3.6.4-12fc6web浏览器，验证不能成功。
- FortiGate-3600A在一些端口允许某些会话摆脱拒绝策略的控制。您需要升级到FortiOS3.0MR4补丁解决该问题。

VPN

VPN涉及到使用基于web管理器与CLI的操作：

- FortiGate设备不支持使用MMS协议通过web模式SSL-VPN通道分配视频数据流的显示。
- 基于web的管理器中删除了VPN闪烁图标，原因是该图标不能生效。
- 编辑标签中的条目时，将显示重新定向URL窗口。
- 对于具有超线程或双核的PC中SSL-VPN可能会中断流量。

反病毒

反病毒涉及到使用基于web管理器与CLI的操作：

- 在NNTP发布操作中AV扫描不能进行。
- 反病毒>隔离>配置的选项中“硬盘空间不足”不可用，只有在设置了“隔离到FortiAnalyzer设备”功能框后，可用的选项才可以被更改。

IPS

入侵防护检测涉及到使用基于web管理器与CLI的操作：

- 当FortiGate设备位于HTTP代理服务器之后时，FortiGuard web过滤验证绕过不能返回到绕过页面。您可以在web浏览应用程序前添加*.8008并放入应该绕过服务器的URL中。8008是端口验证的默认端口号。
- 使用基于web的管理器，可以在内容保护列表中启动FortiGuard跳过功能。
- FortiGate设备现在可以屏蔽Skype用户，即使过了延长的时间段。
- MR4中，用户不能修改IPS严重性规则。您需要升级到FortiOS3.0MR4补丁解决该问题。

Web 过滤

Web过滤涉及到使用基于web管理器与CLI的操作：

- Web过滤禁忌词汇功能不能够屏蔽以SHIFT JIS编码的网页。
- 以http:\\www.fortinet.com格式的本地分类在从FortiOS 3.0MR2升级到FortiOS3.0 MR3后不能被删除。您可以使用CLI命令purge实现条目的删除操作。

即时消息（IM）

- FortiGate设备能够屏蔽所有的即时消息程序的登录，但是如果即时消息用户HTTP通道时不能控制即时消息流量。
- 发生以下情况，不能作为系统bug：
  1. FortiGate设备不能检测与控制使用MSN8.0的IM用户之间的语音聊天流量，因为这些数据流是加密的。
  2. 通过端口80Yahoo！流量是经过编码的，不应用于IM程序处理，所以通过端口80传输的文件被屏蔽。
- 下表信息是有关MR4支持的每项IM协议的有关信息：

IM 用户	版本	描述
AIM Classic	5.9.6089	● 用户使用非加密或加密 AIM 版本时，不能够与其它 AIM 用户进行视频连接。 ● 应用 AIM 加密后，不能进行到 AIM 对等用户的直接连接。如果不使用 AIM 加密，所有的尝试连接均不成功。这样的情况在所有 AIM 非加密与加密的用户中都存在。 ● 当一个 AIM 用户从另一个 AIM 用户接收文件时，FortiGate 文件数目统计将不增加。这样的情况在所有 AIM 非加密与加密的用户中都存在。 ● NetMeeting 使用 H.323 不能建立连接。这样的情况在所有 AIM 非加密与加密的用户中都存在。 ● 包含的日文的 IM 系统替换信息不能正常显示。

		● 用户文本信息内容以及文本格式信息将在即时信息内容日志中显示
AIM Triton	6.028.1	● 当两个 AIM 用户均使用 6.0.28.1 版本进行通信时，FortiGate 设备将音频事件记录到 FortiAnalyzer 设备。
ICQ	5.10	● NetMeeting 使用 H.323 不能建立连接。这样的情况在所有 AIM 非加密与加密的用户中都存在。 ● 包含的日文的 IM 系统替换信息不能正常显示。
Yahoo！Messenger	8.1.0.195	● 当用户通过 FortiGate 设备对其它 MSN 用户发送消息时，会话统计计数不正确。 ● Yahoo!7.0 版本中，不能屏蔽音频通信。

P2P

P2P只涉及到基于web管理器中的操作：

- FortiGate设备不能屏蔽使用Azureus/BitTorrent 2.50版本的P2P用户。
- AIM5.9、AIM6.0或ICQ 5使用非标准端口或应用了IPS2.334版本或更早版本的特征，FortiGate设备不能检测到AIM5.9、AIM6.0或ICQ 5用户。对一些P2P用户的检测需要在内容保护列表中使用CLI命令set ips-signature low。使用IPS2.335版本或更高版本的特征能够保证FortiGate设备检测到AIM5.9、AIM6.0或ICQ 5。

日志与报告

日志与报告的操作涉及到基于web的管理器与CLI的使用：

- FortiGate设备不能正确发送有关是否web过滤事件被屏蔽或被允许这样的报警邮件，即使只在“被屏蔽的web访问”配置发送报警邮件。
- 即使一个SMTP日志信息中包含不止一个接收人，FortiGate设备在记录日志信息中也只记录一个接收人。
- FortiGate设备支持的每项IM程序（MSN，Yahoo!， AIM与 ICQ）的聊天信息编码均不同。这些信息在传输到FortiAnalyzer设备进行日志记录或内容存档之前都将被转换，并且因为这样的转换，IM程序都将以编码后的格式显示。MSN用户以UTF-8，Yahoo用户以UFT-8，AIM使用纯文本或HTML，ICQ使用DTF。

更改固件版本

升级到FortiOS3.0之前，建议阅读本章以便您能全面考虑升级到FortiOS3.0的操作步骤。本章包括所有FortiOS3.0固件版本升级操作内容以及恢复到旧的固件版本FortiOS2.8MR11或所有的FortiOS3.0固件版本的操作。
本章包括以下内容：

- 备份配置
- 升级FortiGate设备
- 返回到FortiOS2.80MR11
- 备份FortiOS3.0配置
- 使用web管理器恢复到FortiOS 2.80MR11
- 恢复配置
- 从FortiOS3.0MR1升级到FortiOS3.0MR2
- 返回到FortiOS3.0MR1
- 有关FortiOS2.80MR11的升级
- 有关FortiOS3.0MR2的升级
- 有关FortiOS3.0MR3的升级
- 有关FortiOS3.0MR4的升级

注意：如果您的网络配置需要在FortiGate设备在透明模式下执行NAT的功能这样特殊的情况，您可以配置FortiGate应用于这种情况。详细信息，参见FortiOS3.0MR1发布说明。

备份配置

Fortinet公司建议在升级到FortiOS3.0之前，备份FortiGate设备中的全部配置设置。这样能够保证如果您需要降级到FortiOS2.8MR11并需要恢复这些配置设置时，所有的配置设置才不会丢失。

警告：在升级/降级到当前固件版本或恢复到出厂默认配置之前总要备份配置。

使用基于 web 的管理器备份配置

以下是使用基于web管理器备份当前配置的操作步骤：

1. 进入“系统设置>维护>备份与恢复”。
2. 选择所有配置文件，点击“备份”图标。
3. 点击“OK”。
4. 保存文件。

注意：备份文件时可以输入密码加密备份的备份文件。

使用 CLI 备份配置文件

以下是使用CLI备份配置文件的步骤：

备份配置文件，输入：

execute backup allconfig <filename><address_ip>

这将花费几分钟的时间。

使用基于web管理器或CLI备份配置文件成功后，您可以执行升级到FortiOS3.0。

升级 FortiGate 设备

如果升级成功，您的FortiGate设备便具有了硬盘驱动，便可以使用备份与恢复页面中“启动固件方法”选项。该选项提供您两种固件镜像的选择，如FortiOS2.80MR11与FortiOS3.0，用于下载/升级。参见Fortinet知识库中“2.80MR11到3.0MR1升级/降级/双重启动”一文中的说明，配置FortiGate设备或配置双重启动。

如果没有成功升级到FortiOS3.0，参见“返回到FortiOS2.80MR11”章节降级到FortiOS2.80MR11。

在FortiOS3.0中，您可能需要重新配置一些设置。参见“有关FortiOS2.80MR11的升级”章节，或“Forti3.0MR1发布说明”获得详细信息。

注意：请在升级到FortiOS3.0之前确定已安装了FortiOS2.80MR11。

升级到 FortiOS3.0

以下是使用基于web的管理器或CLI升级到FortiOS3.0的内容信息。

使用基于 web 的管理器升级

以下是使用基于web管理器升级到FortiOS3.0的操作步骤。建议使用CLI进行升级。TFTP升级会将所有当前的防火墙配置恢复到出厂默认的设置。

警告：在升级/降级到当前固件版本或恢复到出厂默认配置之前要备份配置。

使用基于web的管理器升级到FortiOS3.0

1. 拷贝固件镜像文件到您的管理器计算机。
2. 登录基于web的管理器。
3. 进入“系统设置>状态>设备信息”。
4. 在“设备信息”选项下，点击“升级”。
5. 输入存储固件镜像文件的路径并命名文件，或点击“浏览”查看固件镜像文件存放的位置。

6. 点击“OK”确定。

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后，显示FortiGate登录页面。该操作需要花费几分钟时间完成。

升级成功后：

- Ping FortiGate设备检验是否还存在连接。
- 清除浏览器的缓存并登录到基于web的管理器。

登录返回到基于web的管理器后，您应该保存将要延续使用的配置设置。FortiOS2.80MR11中的一些设置可能会延续到升级的系统，而例如某些IPS组设置将不能延续到升级的系统。进入“系统设置>维护>备份与恢复”保存将延续到升级后系统的配置设置文件。

注意：升级到FortiOS3.0后，执行“立即升级”从FDN获取最新的AV/NID特征，因为固件中这些特征文件可能要比FDN中当前可用特征的版本要旧。

使用 CLI 升级

使用CLI升级到FortiOS3.0与TFTP服务器。

使用CLI升级到FortiOS3.0

1. 将新的固件镜像文件拷贝到TFTP服务器的根目录。
2. 启动TFTP服务器。
3. 登录到CLI。
4. 输入以下命令ping运行TFTP服务器的计算机。该操作保证FortiGate设备与TFTP服务器连接。例如，如果TFTP服务器的IP地址为：192.168.1.168。
   execute ping 192.168.1.168
5. 输入以下命令将固件文件从TFTP服务器拷贝到FortiGate设备。

execute restore image<name_str><tftp_ip4>

<name_str>中输入固件镜像文件的名称，<tftp_ip4>中输入TFTP服务器的IP地址。例如固件镜像文件名为image.out，TFTP服务器的IP地址为192.168.1.168，那么输入：

execute restore image.out 192.168.1.168

FortiGate设备对于以上信息作出类似以下的回应：

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，省级到新的版本并重新启动设备。该操作需要发费几分钟时间。

7. 重新连接到CLI。
8. 输入以下命令确认固件安装成功。

get system status

9. 更新反病毒与攻击定义（参见FortiGate设备管理员使用手册），或在CLI中输入：

execute update-now

校验升级

再次登录基于web的管理器后，大部分FortiOS2.80MR11配置设置将延续到升级后的系统。例如，进入“系统设置>网络>选项”，您可以看到从FortiOS2.80MR11配置设置延续的DNS设置。

您应该校验延续到升级后系统的配置设置。校验配置设置可以使您熟悉FortiOS3.0中的新功能与功能更改。

您可以通过以下方法校验配置设置：

- 使用基于web的管理器检查每个菜单与栏目
- 使用CLI shell 命令show

确定配置到FortiGate设备的管理访问设置也同样延续到升级后的系统。

返回到 FortiOS2.80MR11

如果升级没有成功，您需要返回到之前的固件版本。以下内容将帮助您备份当前的FortiOS3.0配置，恢复到FortiOS2.80MR11以及FortiOS2.80MR11的配置。包括以下内容：

- 备份FortiOS3.0配置
- 使用基于web的管理器恢复到FortiOS2.80MR11
- 使用CLI恢复到FortiOS2.80MR11
- 恢复配置

备份 FortiOS3.0 配置

如果您在FortiOS3.0中配置了其它设置，建议您在恢复到FortiOS2.80MR11之前备份这些设置。这样能够保证您决定升级时，具有FortiOS3.0的当前配置文件。

将配置备份到 PC

1. 进入“系统设置>维护>备份与恢复”。
2. 选择“备份到本地PC”。
3. 点击“应用”。

如果您想加密配置文件以保存VPN证书，选定“加密配置文件”功能框并输入密码，重新输入密码以确认。

备份到 FortiUSB Key

您也可以将配置文件备份到FortiUSB密钥。执行备份操作之前，请先确定FortiUSB是否已经安装在FortiGate设备上。

注意：如果FortiGate设备已安装FortiOS3.0MR1，在您安插FortiUSB之前，请先确定已关闭FortiGate设备。

将配置文件备份到FortiUSB
1. 进入“系统设置>维护>备份与恢复”。
2. 选择“备份到FortiUSB”。
3. 点击“应用”。

如果您想加密配置文件以保存VPN证书，选定“加密配置文件”功能框并输入密码，重新输入密码以确认。

使用基于 web 的管理器恢复到 FortiOS2.80MR11

当您恢复到FortiOS 2.80MR11时，只有以下设置被保留：
- 操作模式
- 接口IP/管理IP
- 静态路由表
- DNS设置
- VDOM设置
- VDOM参数>设置
- 管理员帐户
- 会话帮助
- 系统权限设置

如果您在FortiOS3.0中创建了其它设置，在恢复到FortiOS2.80MR11之前请先备份这些设置。

使用基于 web 的管理器恢复到 FortiOS2.80MR11

1. 进入“系统设置>状态>固件版本”。
2. 点击“更新”。
3. 输入固件存放的位置或点击“浏览”查找固件。
4. 点击“OK”。

FortiGate设备显示如下信息：
The new image does not support CC mode. Do you want to continue to upgrade?
5. 点击“OK”确认。

显示如下信息：
This version will downgrade the current firmware version. Are you sure you want to continue?
6. 点击“OK”确认。

FortiGate设备上传固件镜像文件，恢复到旧的固件版本，恢复配置，系统重新启动后，并显示登录页面。该操作需要花费几分钟的时间。
7. 重新登录基于web的管理器。

进入“系统设置>设备信息”校验更改为FortiOS2.80MR11后的固件版本。

校验恢复

成功恢复到FortiOS2.80MR11后，校验设备连接与设置。如果您不能连接到基于web的管理器，请查看您的管理访问设置与内部网络IP地址是否正确。恢复固件可能将设备的配置设置恢复到出厂默认的设置。

使用 CLI 恢复到 FortiOS2.80MR11

该步骤将使用CLI命令将固件恢复到FortiOS2.80MR11。如果您在FortiOS3.0中创建了其它设置，在恢复到FortiOS2.80MR11之前请先备份这些设置。

使用 CLI 恢复到 FortiOS2.80MR11

1. 将固件镜像文件拷贝到TFTP服务器的根目录。
2. 启动TFTP服务器。
3. 登录CLI。
4. 输入以下命令ping运行TFTP服务器的计算机。该操作保证FortiGate设备与TFTP服务器连接。例如，如果TFTP服务器的IP地址为：192.168.1.168。
   execute ping 192.168.1.168
5. 输入以下命令将固件文件从TFTP服务器拷贝到FortiGate设备。

execute restore image<name_str><tftp_ip4>
<name_str>中输入固件镜像文件的名称，<tftp_ip4>中输入TFTP服务器的IP地址。例如固件镜像文件名为image.out，TFTP服务器的IP地址为192.168.1.168，那么输入：
execute restore image.out 192.168.1.168
FortiGate设备对于以上信息作出类似以下的回应：
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，恢复到旧的版本并重新启动设备。系统显示如下信息：
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设备恢复为旧的固件版本，并恢复为出厂默认设置，重新启动。该操作需要花费几分钟的时间。
FortiGate设备上传固件后，将恢复为默认的设置包括默认的IP地址，您需要重新配置IP地址。

8. 重新连接到CLI。
9. 输入以下命令确定固件已经安装成功：

get system status

恢复配置

当恢复到FortiOS2.80MR11后，配置设置可能并不能随着降级而保留。您需要使用在升级到FortiOS 3.0保存的FortiOS2.80MR11的配置文件来恢复配置设置。

使用基于 web 的管理器恢复配置设置

以下是使用基于web的管理器如何恢复FortiOS2.80MR11的操作。

1. 登录基于web的管理器。
2. 进入“系统设置>维护>备份与恢复”。
3. 选择配置文件，点击“恢复”图标。
4. 如您对保存的配置文件设置了密码，输入密码。
5. 输入配置文件存储的路径，或点击“浏览”查找文件存放的位置。
6. 点击“OK”。

FortiGate设备恢复FortiOS 2.80MR11的配置设置，该过程中FortiGate设备需要重新启动，所以需要几分钟的时间。

您可以登录基于web的管理器，访问各项菜单或条目校验恢复的配置设置。

使用CLI恢复配置设置

以下是使用CLI如何恢复FortiOS2.80MR11的操作。

1. 将备份的配置文件拷贝到TFTP服务器的根目录。
2. 启动TFTP服务器。
3. 登录CLI。
4. 输入以下命令ping运行TFTP服务器的计算机。该操作保证FortiGate设备与TFTP服务器连接。例如，如果TFTP服务器的IP地址为：192.168.1.168。
   execute ping 192.168.1.168
5. 输入以下命令将配置文件从TFTP服务器拷贝到FortiGate设备。

execute restore allconfig <name_str><tftp_ip4><passwrd>
<name_str>中输入备份的配置文件名称，<tftp_ip4>中输入TFTP服务器的IP地址，<passwrd>中输入当您在备份配置文件时设置的密码。例如配置文件名为confall，TFTP服务器的IP地址为192.168.1.168，密码为ghrffdt123：那么输入：
execute restore allconfig confall　192.168.1.168 ghrffdt123
FortiGate设备对于以上信息作出类似以下的回应：
This operation willoverwrite the current setting and the system will reboot!
Do you want to continue? (y/n)

6. 键入“Y”。

FortiGate设备上传备份配置文件，文件上传后，系统显示如下信息：
Getting file confall from tftp server 192.168.1.168
##
Restoring files……

All done. Rebooting….
该操作将花费几分钟的时间。

使用shell 命令show检验恢复的设置，或登录基于web的服务器。

从 FortiOS3.0MR1 升级到 FortiOS3.0MR2

以下是实现从FortiOS3.0MR1升级到FortiOS3.0MR2的信息与操作。同样适用于升级到FortiOS3.0MR3或更高系统版本。

注意：FortiOS3.0MR2支持除了FortiGate-50外的所有设备。如果您使用TFTP服务器升级固件，所有当前防火墙配置都将恢复到出厂默认设置。

注意：从FortiOS2.80MR11升级到FortiOS3.0MR2后，有几箱配置设置是不能延续到升级后的系统的。

备份配置

您可以使用FortiUSB、基于web的管理器或CLI备份当前配置。使用以下步骤之一均可以配置当前配置。

警告：在升级或恢复到当前固件版本，或恢复到出厂默认设置时要备份配置设置。

使用基于 web 的管理器备份当前配置

1. 进入“系统设置>维护>备份与恢复”。
2. 选择“备份到本地PC”。
3. 点击“应用”。

如果您想加密配置文件以保存VPN证书，选定“加密配置文件”功能框并输入密码，重新输入密码以确认。

使用 CLI 备份当前配置

1. 登录CLI。
2. 输入以下CLI命令：

execute backup config tftp <filename><tftp_ipv4>
例如：
execute backup config tftp fgt.conf 192.168.1.23

使用 FortiUSB Key 备份当前配置文件

1. 进入“系统设置>维护>备份与恢复”。
2. 选择“备份到FortiUSB”。

3. 点击“应用”。

如果您想加密配置文件以保存VPN证书，选定“加密配置文件”功能框并输入密码，重新输入密码以确认。

升级到 FortiOS3.0MR2

使用以下任何一种操作的方法均可以升级FortiGate设备。该操作使用TFTP服务器升级到FortiOS3.0MR2。TFTP升级会将所有当前的防火墙配置恢复到出厂默认的设置。

使用基于 web 的管理器升级

1. 拷贝固件镜像文件到您的管理器计算机。
2. 登录基于web的管理器。
3. 进入“系统设置>状态>升级固件”。
4. 点击“升级”。
5. 输入存储固件镜像文件的路径并命名文件，或点击“浏览”查看固件镜像文件存放的位置。
7. 点击“OK”确定。

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后，显示FortiGate登录页面。该操作需要花费几分钟时间完成。

升级成功后：

- Ping FortiGate设备检验是否还存在连接。
- 清除浏览器的缓存并登录到基于web的管理器。

使用 CLI 升级

1. 将新的固件镜像文件拷贝到TFTP服务器的根目录。
2. 启动TFTP服务器。
3. 登录到CLI。
4. 输入以下命令ping运行TFTP服务器的计算机。该操作保证FortiGate设备与TFTP服务器连接。例如，如果TFTP服务器的IP地址为：192.168.1.168。
   execute ping 192.168.1.168

5. 输入以下命令将固件文件从TFTP服务器拷贝到FortiGate设备。

execute restore image<name_str><tftp_ip4>

<name_str>中输入固件镜像文件的名称，<tftp_ip4>中输入TFTP服务器的IP地址。例如固件镜像文件名为image.out，TFTP服务器的IP地址为192.168.1.168，那么输入：

execute restore image.out 192.168.1.168

FortiGate设备对于以上信息作出类似以下的回应：

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，省级到新的版本并重新启动设备。该操作需要发费几分钟时间。

7. 重新连接到CLI。
8. 输入以下命令确认固件安装成功。

get system status

9. 更新反病毒与攻击定义（参见FortiGate设备管理员使用手册），或在CLI中输入：

execute update-now

恢复到 FortiOS3.0MR1

如果升级没有成功，您需要返回到之前的固件版本。您可以使用在设备重新启动时更改固件版本的功能，或使用基于web的管理器或CLI恢复到之前的固件版本。

在设备启动重新启动时更改固件版本的功能只能在安装有硬盘的FortiGate设备中可以实现。也就是说您可以在FortiGate设备的硬盘中备份两个固件镜像文件，用于升级或降级。

警告：在升级/降级到当前固件版本或恢复到出厂默认配置之前要备份配置。

备份配置

您可以将当前配置备份到管理PC或FortiUSB密钥。以下是使用基于web的管理器将当前配置备份到管理PC或FortiUSB密钥的操作步骤。

将 FortiOS3.0MR2 的配置文件备份到 PC

1. 进入“系统设置>维护>备份与恢复”。
2. 选择“备份到本地PC”。
3. 点击“应用”。

如果您想加密配置文件以保存VPN证书，选定“加密配置文件”功能框并输入密码，重新输入密码以确认。

将当前配置备份到 FortiUSB Key

1. 进入“系统设置>维护>备份与恢复”。
2. 选择“备份到FortiUSB”。
3. 点击“应用”。

如果您想加密配置文件以保存VPN证书，选定“加密配置文件”功能框并输入密码，重新输入密码以确认。

恢复到 FortiOS3.0MR1

备份配置后，您可以使用基于web的管理器或CLI将设备恢复FortiOS3.0 MR1。

使用基于 web 的管理器恢复到 FortiOS3.0 MR1

1. 进入“系统设置>状态>固件版本”。
2. 点击“更新”。
3. 输入固件存放的位置或点击“浏览”查找固件。
4. 点击“OK”。

FortiGate设备显示如下信息：

The new image does not support CC mode. Do you want to continue to upgrade?

5. 点击“OK”确认。

显示如下信息：

This version will downgrade the current firmware version. Are you sure you want to continue?

6. 点击“OK”确认。

FortiGate设备上传固件镜像文件，恢复到旧的固件版本，恢复配置，系统重新启动后，并显示登录页面。该操作需要花费几分钟的时间。

7. 重新登录基于web的管理器。
8. 进入“系统设置>设备信息”校验更改为FortiOS3.0MR1固件版本。

使用 CLI 恢复到 FortiOS3.0MR1

1. 将固件镜像文件拷贝到TFTP服务器的根目录。
2. 启动TFTP服务器。
3. 登录CLI。
4. 输入以下命令ping运行TFTP服务器的计算机。该操作保证FortiGate设备与TFTP服务器连接。例如，如果TFTP服务器的IP地址为：192.168.1.168。
   execute ping 192.168.1.168
5. 输入以下命令将固件文件从TFTP服务器拷贝到FortiGate设备。

execute restore image<name_str><tftp_ip4>

<name_str>中输入固件镜像文件的名称，<tftp_ip4>中输入TFTP服务器的IP地址。例如固件镜像文件名为image.out，TFTP服务器的IP地址为192.168.1.168，那么输入：

execute restore image.out 192.168.1.168

FortiGate设备对于以上信息作出类似以下的回应：

This operation will replace the current firmware version!
Do you want to continue? (y/n)

6. 键入“Y”。
7. FortiGate设备上传固件镜像文件，恢复到旧的版本并重新启动设备。系统显示如下信息：

Get image from tftp server OK.
Check image OK.
This operation will downgrade the current firmware version!
Do you want to continue? (y/n)
8. 键入y。

FortiGate设备恢复为旧的固件版本，并恢复为出厂默认设置，重新启动。该操作需要花费几分钟的时间。

FortiGate设备上传固件后，将恢复为默认的设置包括默认的IP地址，您需要重新配置IP地址。

9. 重新连接到CLI。
10. 输入以下命令确定固件已经安装成功：

get system status

恢复 FortiOS3.0MR1 配置

当恢复到FortiOS3.0MR1后，您可以使用基于web的管理器或CLI重新安装FortiOS 3.0MR1的配置设置。

使用基于 web 的管理器恢复配置设置

以下是使用基于web的管理器如何恢复FortiOS3.0MR1的操作。

1. 登录基于web的管理器。
2. 进入“系统设置>维护>备份与恢复”。
3. 选择配置文件，点击“恢复”图标。
4. 如您对保存的配置文件设置了密码，输入密码。
5. 输入配置文件存储的路径，或点击“浏览”查找文件存放的位置。
6. 点击“OK”。

FortiGate设备恢复FortiOS 3.0MR1的配置设置，该过程中FortiGate设备需要重新启动，所以需要几分钟的时间。

您可以登录基于web的管理器，访问各项菜单或条目校验恢复的配置设置。

使用 CLI 恢复 FortiOS 3.0MR1 的配置设置

以下是使用CLI如何恢复FortiOS2.80MR11的操作。

1. 将备份的配置文件拷贝到TFTP服务器的根目录。
2. 启动TFTP服务器。
3. 登录CLI。
4. 输入以下命令ping运行TFTP服务器的计算机。该操作保证FortiGate设备与TFTP服务器连接。例如，如果TFTP服务器的IP地址为：192.168.1.168。

   execute ping 192.168.1.168
5. 输入以下命令将配置文件从TFTP服务器拷贝到FortiGate设备。

execute restore allconfig <name_str><tftp_ip4><passwrd>

<name_str>中输入备份的配置文件名称，<tftp_ip4>中输入TFTP服务器的IP地址，

<passwrd>中输入当您在备份配置文件时设置的密码。例如配置文件名为confall，TFTP服务器的IP地址为192.168.1.168，密码为ghrffdt123：那么输入：
execute restore allconfig confall　192.168.1.168 ghrffdt123
FortiGate设备对于以上信息作出类似以下的回应：
This operation willoverwrite the current setting and the system will reboot!
Do you want to continue? (y/n)
6. 键入“Y”。
7. FortiGate设备上传备份配置文件，文件上传后，系统显示如下信息：
Getting file confall from tftp server 192.168.1.168
##
Restoring files……
This may take a few minutes….
该操作将花费几分钟的时间。
8. 使用shell 命令show检验恢复的设置，或登录基于web的服务器。

使用 FortiUSB 恢复设置

如果您将配置设置保存到 FortiUSB 密钥，您可以使用基于 web 的管理器或 CLI 从 FortiUSB 密钥恢复配置设置。

使用基于web的管理器从FortiUSB密钥恢复配置

1. 进入“系统设置>维护>备份与恢复”。
2. 从“备份配置列表”中选择USB。
3. 点击“OK”。

如果您想加密配置文件以保存VPN证书，选定“加密配置文件”功能框并输入密码，重新输入密码以确认。

使用CLI从FortiUSB密钥恢复配置登录CLI

1. 登录CLI。
2. 输入以下CLI命令：

execute restore config usb <config_name>

3. 显示如下信息：

This operation will overwrite current settings!
Do you want to continue? (y/n)

4. 输入y。

该操作需要花费几分钟时间去实现。

5. 使用导入批量CLI命令恢复列表。

有关 FortiOS2.80MR11 的升级

以下是有关从FortiOS2.80MR11直接升级到FortiOS 3.0或更高版本系统的说明。

从 FortiOS2.80MR11 升级到 FortiOS 3.0MR1

以下是关于升级后一些配置设置不能延续到FortiOS 3.0MR1或与FortiOS 3.0MR1中其它一些设置混合的说明。除了以下注明的信息，其它配置设置都将延续到升级后的系统。

IPS 组

FortiOS2.80中某些IPS组不能延续到升级到的FortiOS3.0MR2。这些IPS组可能会与FortiOS MR2中的IPS组混合或在升级过程中被删除。您需要根据FortiOS3.0MR1发布说明中附件A校验丢失的IPS组，然后对没有能够延续到升级后系统的IPS组手工配置特征设置。使用Fortinet知识库中“使用导入批量CLI命令选项导入2.80列表”中说明将FortiOS 2.80中的列表导入FortiOS3.0。

VPN 防火墙策略

FortiOS 3.0中IPSec阶段1客体是与网络接口绑定的。当在两项防火墙IPSecVPN策略在不同的接口共享相同的阶段1IPSecVPN客体这样特殊情况下升级时，这些防火墙策略是不能延续到升级后的系统。您需要创建一个新的IPSec阶段1客体恢复这些策略，在IPSecVPN防火墙策略使用的相同接口上建立本地接口设置，并创建如VPN通道自动密钥客体这样的另一项新的阶段1客体。

PING 发生器

CLI命令auto-negotiate，默认的情况下没有启动。该CLI命令取代了FortiOS2.80中Ping发生器自动启动两个通道通信的功能。Ping发生器在IPSec2配置下对于IPSec通道与IPSec接口都是可用的。

未被使用的 IPSec VPN

如果FortiOS2.80中存在未被使用的IPSecVPN，并且这些VPN也没有应用在防火墙策略中，那么他们将不能延续到升级后的FortiOS3.0MR1中使用。

FortiGuard web 过滤替代信息字符串

FortiGuard web过滤URL屏蔽功能需要在web过滤替换信息中包括特殊标记字符串。这些特殊标记是用来确保用户定制的替换信息不被覆盖，但是并不是自动进行添加的。系统升级后，您需要手工升级web过滤替换信息，将特殊标记包括在内。以下是需要争取升级的特殊标记字符串：

- 升级后，进入“系统设置>配置>替换信息>FortiGuard web过滤>URL屏蔽信息”。

- 在替换信息<body>与</body>HTML标签之间插入字符串“
%%OVERRIDE%%
”。
- 保存更新的替换字符串并点击“OK”。

Web 过滤与垃圾邮件过滤列表

以下列表存储在FortiOS3.0系统配置中，升级后不能恢复。使用批量CLI命令恢复这些列表：

Web过滤	垃圾邮件过滤
● Web内容屏蔽	● IP地址
● WebURL屏蔽列表	● RBL&ORDBL
● Web URL免除列表	● 电子邮件地址
	● MIME报头
	● 禁忌词汇
	● RBL &ORDBL

Active X, Cookie，与 Java Apple 过滤

如果Active X插件, Cookie，与Java Apple过滤在“web过滤>脚本过滤”项下启动后，那么在每项内容保护文件中是自动启动。当从FortiOS2.80MR11升级时，如果在“web过滤>脚本过滤”项下启动了Active X插件, Cookie，与Java Apple过滤，那么这些设置都将在每项内容保护文件中反映出来。

没有配置“设备设置”的静态路由

FortiOS3.0需要对静态路由配置“设备设置”。FortiOS2.80MR11中任何没有配置“设备设置”的静态路由在升级后均不能延续到FortiOS 3.0。

有关从 FortiOS2.80MR11 升级到 FortiOS 3.0MR2

以下是有关从FortiOS2.80MR11直接升级到FortiOS3.0MR2后发生一些配置设置不能延续到升级后的系统或与升级后的系统中某些设置混合情况的说明。

日志过滤更改

FortiOS3.0中，日志过滤是通过以下两种方法之一进行控制的，分别为基于设备与基于每项内容保护文件的控制。基于设备的过滤控制是否将日志信息发送到设备。基于每项内容保护文件过滤控制是否通过一项内容保护后匹配的流量所产生的日志信息发送到设备。当从FortiOS2.80升级系统时，只有基于设备的日志过滤能够延续到升级后的系统。内容保护文件更改为容纳日志记录，除了命令log-web-ftgd-error。该命令在默认情况下是启动的。系统成功升级到FortiOS3.0

后，查看需要启动日志记录的防火墙策略。

VDOM 许可

升级到系统FortiOS 3.0后，VDOM以及所有有关的配置都将在升级后保留。为了防止返回到出厂默认的设置与配置恢复，FortiGate设备不添加全部的VDOM。如果运行FortiOS2.80的FortiGate设备中设置了超出默认数量的VDOM，升级到FortiOS3.0后需要执行以下操作：

- 备份FortiOS2.80的配置
- 升级到FortiOS3.0MR2
- 备份FortiOS3.0 MR2
- 联系“客户支持”获得配置超出默认设置的其它VDOM的FortiOS 3.0VDOM许可证

  如果您配置运行一个HA群集，您需要获得群集中每台设备的许可证密钥。

VDOM 配置中 IPSec 手工密钥

配置在非根VDOM中IPSec通道使用的手工密钥，在没有被防火墙策略引用时，系统升级后将不能延续到升级后的系统。

报警邮件替代信息

FortiOS 3.0MR2中，“报警邮件”选项经过了修改。FortiGate设备对报警邮件生成新的信息格式。任何修改后的报警邮件替换信息都不能延续到升级后的系统。

报警邮件过滤

报警邮件过滤包括根据类型与阀值发送报警邮件。详细信息参见“日志与报告”章节。

区域中的防火墙策略

防火墙策略并不能延续到升级后的系统，但是如果防火墙策略是配置在启动VDOM的区域中，便可以延续到升级后的系统。

有关从 FortiOS2.80MR11 升级到 FortiOS3.0MR4

以下是有关从FortiOS2.80MR11直接升级到FortiOS3.0MR4后发生一些配置设置不能延续到升级后的系统或与升级后的系统中某些设置混合情况的说明。除

了以下另行的说明，其它以上所述有关升级中存在的情况同样存在。

管理用户

FortiOS2.80中，管理admin用户是全局配置；而在FortiOS3.0MR4中，管理admin用户是基于每个VDOM设置的。升级到FortiOS 3.0MR4后，FortiOS2.80中所有的admin用户在默认情况下都将被分配到根VDOM，所有的管理用户，除了默认的“admin”用户在升级后均不能登录管理VDOM。

策略路由

从FortiOS3.0MR2后，输入设备与输出设备是强制的属性。FortiOS2.80中，输出设备不是强制属性，升级到FortiOS3.0MR4，不配置输出策略的策略路由不能延续到升级后的系统。

WLAN 接口下的 VLAN

配置在WLAN接口下的VLAN不能延续到FortiOS 3.0MR4。FortiOS 3.0MR4不支持WLAN接口下的VLAN的配置。

日志硬盘设置

“日志硬盘设置”配置在系统从FortiOS2.80MR11升级到FortiOS2.80MR12后不能延续到升级后的系统。升级系统后，您需要重新启动并配置该设置。

有关升级到 FortiOS3.0MR2

- FortiOS3.0中需要对静态路由配置“设备设置”，如果静态路由不配置“设备”设置，静态路由将不能延续到升级后的系统。
- 无线设置，如果启动了VDOM，FortiWiFi设备中的无线设置不能延续到升级后的系统，所述无线设置包括SSID、安全模式与广播SSID。

有关 FortiOS3.0MR3 升级

- 以下型号的FortiGate设备中创建的Web过滤列表、反垃圾邮件列表与反病毒文件模式列表存在局限性。

FortiGate-50A、FortiGate-60、FortiGate-100、FortiGate-100A与FortiWiFi-60最多可以创建2个列表。

FortiGate-200与FortiGate-500A最多可以创建4个列表。

有关FortiOS3.0MR4升级

除非另有注明，以下配置在将延续到升级后的系统。

- 以http://www.fortinet.com格式的本地分类在从FortiOS 3.0MR2升级到FortiOS 3.0MR3后不能被删除。只有在CLI中使用purge命令可以删除条目。