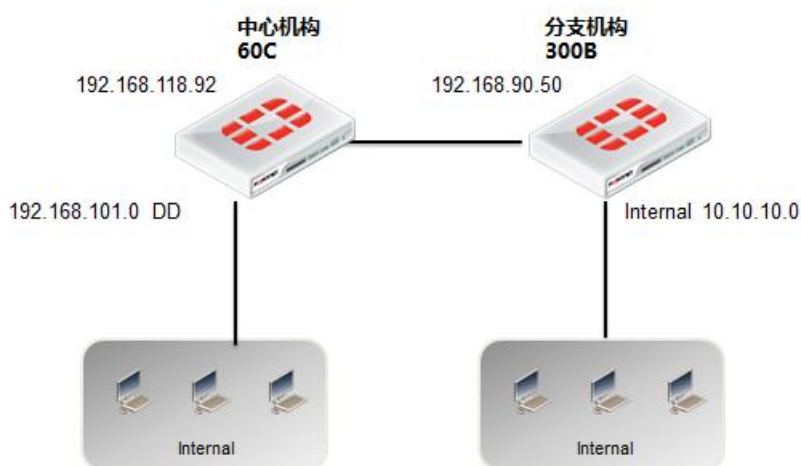


## 5.0 功能概要 auto-ipsec

版本	1.0
时间	2013 年 1 月
作者	(support_cn@fortinet.com)
支持的版本	FortiOS v5.0.1 build147
状态	草稿

5.0 新增 auto-ipsec 功能 ,该功能提供 ipsec 两端及其简易的 ipsec 配置功能 ,使普通用户无需配置 IKE ,可以在一分钟之内仅通过一条策略配置即可实现 ipsec 配置下发至对端 ,实现 ipsec 联通。以下为该功能的简要介绍。此功能仅针对低端产品可用 ,中高端可以通过 FortiManager 实现 VPN 策略的下发。

本文使用 1 台 FortiWifi 60C(中心)与 1 台 FortiGate310B(分支)进行说明, 本文使用的系统版本为 FortiOS v5.01 build 147。该功能仅支持 site to site 模式 ,不支持 dialup vpn。



1. 在分支 310 B 机构命令行的接口中的管理服务启用 auto-ipsec 功能。

```
config system interface
  edit "port1"
    set vdom "root"
    set ip 192.168.90.50 255.255.255.0
    set allowaccess ping https ssh http telnet auto-ipsec
    set type physical
  next
end
```

2. 在中心机构 60C 配置策略 ,需注意 ,在策略配置中必须使用明确的源目标 IP 地址段 ,并且在配置完 IPSEC 相关配置后 ,通过保存并告知来实现配置下发。

新建输出策略

---

策略类型  防火墙  VPN

策略子类型  IPSEC  SSL-VPN

本地接口

本地被保护网络

流出VPN接口

远程被保护网络

时间表

服务

记录允许流量

必须使用明确的源目标IP地址段

---

VPN隧道

新建  使用现有

Site-to-Site  拨号

名称

远端FortiGate IP

预共享密钥

允许从远端站点发起流量

---

UTM安全配置

反病毒

网页过滤

应用控制

IPS

邮件过滤

DLP传感器

VoIP

ICAP

SSL Inspection

流量控制

标签

已应用的标签

添加标签

注释

---

保存并告知发送请求到远端FortiGate

使用保存并告知，通知FG下发相关配置给分支机构。

确认 保存并告知 取消

此处完成后，再次编辑该策略将无法看见“保存并告知”按键。

3. 配置完成后分支机构可以通过命令行输入以下命令接受该部分配置

```
diag vpn auto-ipsec bootstrap accept 123456
```

今后版本将改为从 web 界面弹出接受请求框。

完成后分支机构将自动建立策略以及 IKE phase1，如下



IKE 中仅包含 Phase1，但不影响联通。

顺序号	源	目的	源地址	目的地址	时间表	服务	认证	动作	UTM配置
1	port4	port1	_autogw0_srcgrp_	_autogw0_dstgrp_	always	ALL		IPSEC	
2	port2	port3	all	all	always	ALL		接受	
3	port2	port3	SSLVPN_TUNNEL_ADDR1	all	always	ALL		接受	
4	port2	port3	SSLVPN_TUNNEL_ADDR1	all	always	ALL		接受	
5	port5	port7	all	all	always	ALL		接受	
6	port9	port2	all	all	always	ALL		接受	
7	port5	port6	all	all	always	ALL		接受	
8	port1	port2	all	SSLVPN_TUNNEL_ADDR1	always	ALL		SSL-VPN	
9	any	any	any	any	always	ALL		拒绝	

策略为系统自动建立。

4. 中心机构此时也已经完成 IKE 的自动建立。



IKE 仅包含 Phase1

5. 隧道在策略完成后自动建立

名称	类型	远程网关	远程端口	用户名	超时	Proxy ID源	Proxy ID目的	状态	流入数据	流出数据	持续时间
a1	静态IP或DNS	192.168.90.50	4500		1500	0.0.0.0/0	0.0.0.0/0	打开	160 B	84 B	5531 秒

系统管理

- 路由
- 策略
- 防火墙对象
- UTM安全配置
- 虚拟专网
  - IPsec
    - 自动交换密钥(IKE)
    - 手动模式
    - 集中器
  - SSL
    - 监视器
      - IPsec监测
      - SSL-VPN监测