

iPhone VPN 与 FortiGate

| | |
|-------|------------------------|
| 版本 | 1.0 |
| 时间 | 2012 年 2 月 |
| 作者 | 胡丹丹(ddhu@fortinet.com) |
| 支持的版本 | FortiOS v4.3.x |
| 状态 | 草稿 |

目录

| | |
|-----------------------|---|
| 1.目的..... | 3 |
| 2.iphone VPN 的支持..... | 3 |
| 3.配置 FortiGate..... | 3 |
| 4.配置手机 VPN..... | 6 |

1.目的

本文档针 FortiGate 对 iphone 手机 VPN 的类型以及 iphone 的 IPsec vpn 进行配置说明。Android 的 vpn 接入请参考 [Android VPN 接入配置 4.2](#)。

本文以 FortiOS v4.0 MR3 的配置进行说明。FortiOS v4.0 MR1 及 MR2 的相关设定请参考 [FortiGate-to-iPhone IPsec VPN configuration guide](#)。

2.iphone VPN 的支持

以下几种 VPN 是 FortiGate 与 iphone 之间的支持信息

IPsec VPN :支持从 iphone 使用 Cisco IPsec VPN Client(unity client)连接 , FortiOS 需要使用 V4.0 MR1 Patch1 以上版本 ;

PPtP: 支持 iphone 使用 pptp 连接 FortiGate ;

SSL VPN 通道模式:不支持 ;

SSL VPN Web 模式: 支持 Apple Safri 1.3(或更高)。

3.配置 FortiGate

本文以 FortiOS v4.0 MR3 的配置进行说明 ,支持使用 iphone 或 ipad 连接 IPsec vpn 至 FortiGate。

该 VPN 配置必须基于路由模式(接口模式)的 VPN ,以下配置测试在 FortiOS v4.0 MR3 测试通过。路由模式的设定方法请参考[站到站 IPsecVPN 设置 4.2](#)。

创建用户、用户组及防火墙地址

```
config user local
```

```
edit "test"
  set status enable
  set type password
  set passwd <password>
next
end

config user group
  edit "apple"
    set group-type firewall
    set member "test"
    set authtimeout 0
  next
end

config firewall address
  edit "LAN"
    set associated-interface "switch"
    set type ipmask
    set subnet 10.1.1.0 255.255.255.0
  next

  edit "iPhoneVPNUsers"
    set associated-interface "Any"
    set comment ""
    set type ipmask
    set subnet 172.16.1.0 255.255.255.0
  next
end
```

添加路由

```
config router static
  edit <route ID>
    set device " iPhoneP1"
    set dst 172.16.1.0 255.255.255.0
  end
```

阶段一设定

```
config vpn ipsec phase1-interface
  edit "iPhoneP1"
    set type dynamic
    set interface "port1"
```

```
set dhgrp 2
set peertype one
set xauthtype auto
set mode aggressive
set mode-cfg enable
set proposal aes256-md5 aes256-sha1
set peerid "iphone"
set authusrgrp "apple"
set ipv4-start-ip 172.16.1.1
set ipv4-end-ip 172.16.1.40
set ipv4-netmask 255.255.255.0
set dns-mode auto
set psksecret "password"
next
end
```

阶段二设定

```
config vpn ipsec phase2-interface
edit "iPhoneP2"
set keylife-type both
set phase1name "iPhoneP1"
set proposal aes256-md5 aes256-sha1
set pfs disable
next
end
```

策略配置

VPN => LAN 方向

```
cconfig firewall policy
edit 1
set srcintf "iPhoneP1"
set dstintf "switch"
set srcaddr "iPhoneVPNUsers"
set dstaddr "LAN"
set action accept
set status enable
set logtraffic enable
set schedule "always"
set service "ANY"
set nat disable
next
```

end

LAN => VPN 方向

```
config firewall policy
```

```
edit 2
```

```
config firewall policy
```

```
edit 1
```

```
set srcintf "switch"
```

```
set dstintf "iPhoneP1"
```

```
set srcaddr "LAN"
```

```
set dstaddr "iPhoneVPNUsers"
```

```
set action accept
```

```
set status enable
```

```
set logtraffic enable
```

```
set schedule "always"
```

```
set service "ANY"
```

```
set nat disable
```

```
next
```

```
end
```

```
next
```

```
end
```

4.配置手机 VPN

Iphone 或 ipad 参数配置如下:

description: FortiGate VPN

server: IP of the FortiGate WAN interface that is configured for VPN (interface : port1 in this case)

account: test (a user account on the FortiGate)

password: test123

Use certificate: off

group name: iphone

secret: Pre-shared key for the tunnel

更多 iphone 设置信息请参考

[iOS: Setting up VPN](#)

[iOS: Supported protocols for VPN](#)

