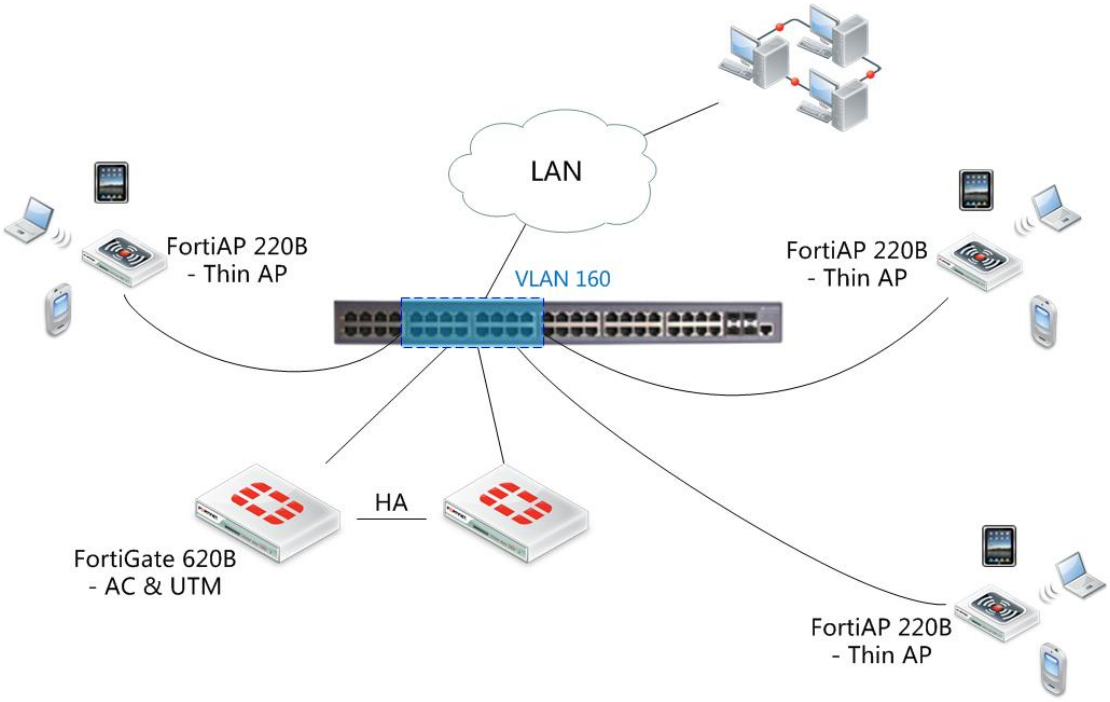
Fortinet 无线网络安全实施方案

版本	1.0
时间	2011 年 9 月
作者	谭杰(jtan@fortinet.com)
支持的版本	FortiGate v4.2.x,v4.3.x
状态	草稿

目录

1、部署拓扑示意图



2、概述

Fortinet 的无线网络接入及安全方案由 AP（无线接入点）和 AC（无线接入控制器）两部分组成。

FortiAP 是可管理的瘦 AP（以下简称 AP）。FortiAP 配备最新的 IEEE 802.1n 的无线芯片以提供高性能的无线接入，在每个无线波段集成监控和多个虚拟 AP 功能。AP 产品与一系列丰富的 FortiGate 控制器（以下简称 AC）产品给用户提供了增强的无线空间。无线运行模式、通道设定、传输功率强弱等，都由 AC 集中控制，以更方便安装和管理。

每个 AP 都把流量引入到集成在 FortiGate 平台的 AC，该流量经过身份识别、UTM（统一威胁管理）引擎检查，仅授权的无线数据流量被转发。除从一个控制台控制网络访问、快速方便的更新策略和监控外，FortiGate 的深度检查

引擎还能提供防火墙、VPN、防病毒、IPS 等网络层和应用层安全防御手段，建立在 Fortinet 多年的网络安全经验基础之上，为客户提供安全的无线网络接入。

FortiAP（AP）和 FortiGate（AC）的无线控制功能提供超强的安全解决方案：

身份验证：强大的身份验证功能，支持 WPA2、802.1x 等。

安全防御：为无线网络提供业绩顶级的 UTM 安全保护。

高性价比：灵活的安装，多功能安全与无线接入的整合，实现较低的总体拥有成本。

本方案选择的 AC 型号为 FortiGate-620B，AP 型号为 FortiAP-220B。

FortiGate-620B

FortiAP-220B

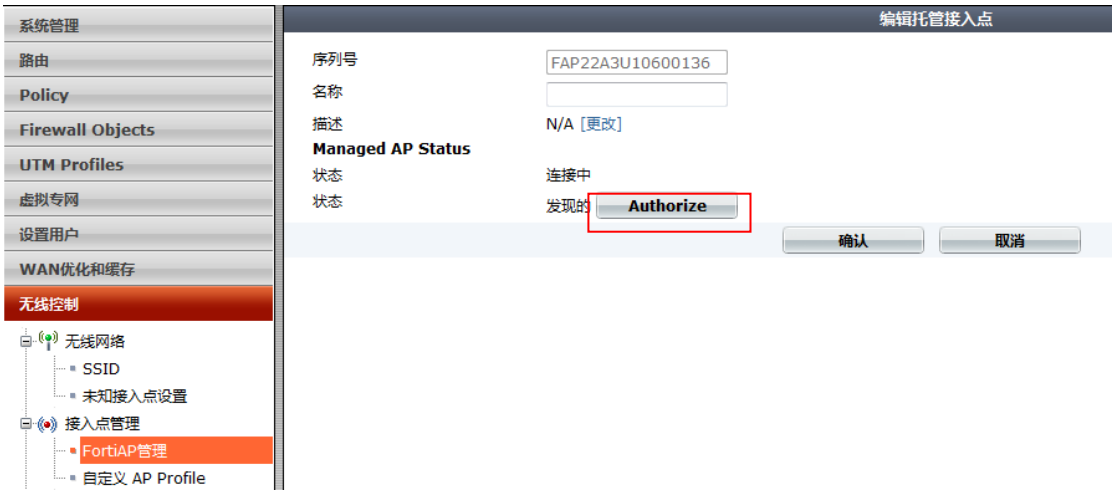
3、部署方式

3.1 AP 与 AC 的连接

在内网交换机上划分一个 VLAN（例如：VLAN 160），专门用于 AP 和 AC 的连接。

AP 和 AC 各使用一个接口连接至 VLAN 160，IP 地址设置为同一地址段。例如：AC 的 Port19 接口地址设置为 10.160.1.230/24，并配置默认路由指向 10.160.1.254，使之能访问内部有线网络的其它部分。AP 的 Eth 接口地址分别设置为 10.160.1.1-10.160.1.200，并将 AC 地址指向 10.160.1.230。AP 的 IP 地址和 AC 地址既可以通过 console 手工设置，也可以通过在 AC 上配置 DHCP 服务动态获取（此时无需对 AP 进行任何配置）。

AP 自动连接到 AC 后，需要管理员手动进行授权，才能接入网络，防止非法 AP 接入的发生。如下图：

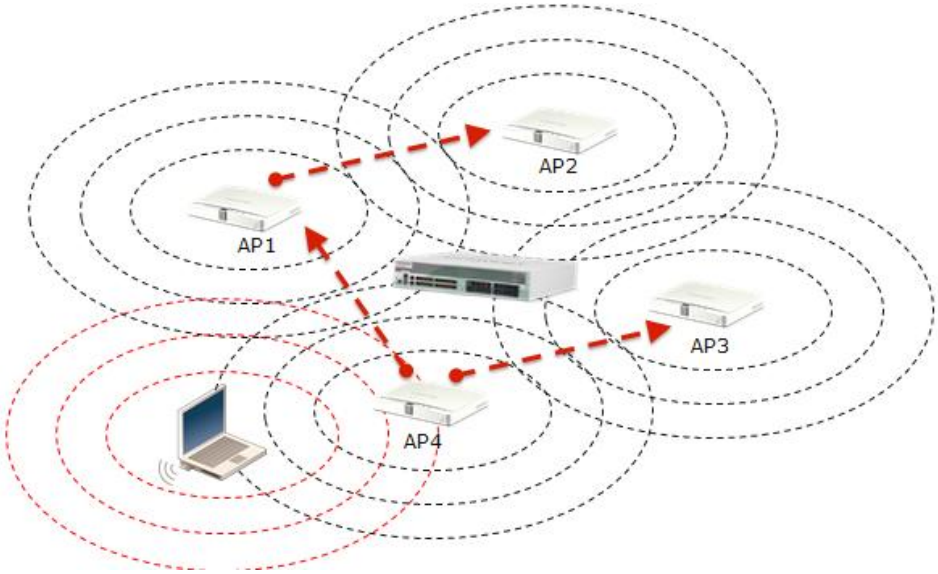


AP 和 AC 之间支持多种连接环境，包括直连、交换环境、路由环境，以及跨广域网的远程环境，AP 与 AC 可以工作在相同或不同 IP 网段，可以在同一局域网或广域网的不同地区，只要 IP 可达，即可正常工作。

AP 和 AC 之间使用标准的 CAPWAP 协议（无线接入点控制与配置协议），AP 仅作为一个无线信号接入点，不处理任何数据，透明地将无线设备(PC、PAD、手机等)的流量通过 CAPWAP 隧道传输到 AC，由 AC 统一处理，并由 AC 负责进行网络层及应用层的安全过滤(包括防火墙访问控制、用户身份认证、入侵防御、病毒过滤、上网行为管理、内容过滤等)。

CAPWAP 协议的控制流量和数据流量均可以使用 DTLS 加密，保证通信内容不被窃取。(目前 Fortinet 仅对控制流量使用 DTLS 加密)

一台 AC 可以同时接入管理多台 AP，AC 可以把相同的 SSID 分发到所有 AP，使无线用户在不同 AP 的覆盖范围内无缝漫游。

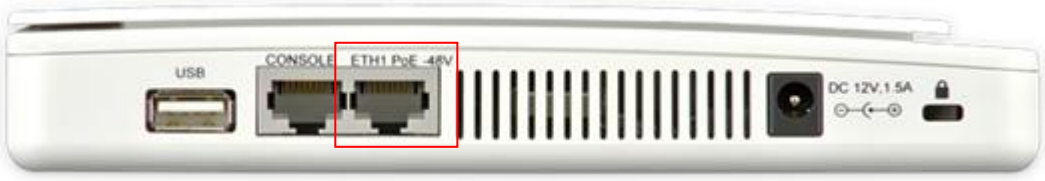


本次选择的 FortiGate-620B，配合 FortiOS V4.0MR3 版本软件，可以同时接入管理 512 台 FortiAP。

3.2 AP 的部署和供电

为保证型号覆盖及传输质量，应该将 AP 按照不超过 20 米的间隔进行蜂窝状部署，并考虑各种墙体对信号的屏蔽作用。

FortiAP-220B 支持 PoE 供电，只要将其与支持 PoE 的交换机或网络设备相连，便可直接通过网线供电，无需连接外置电源。



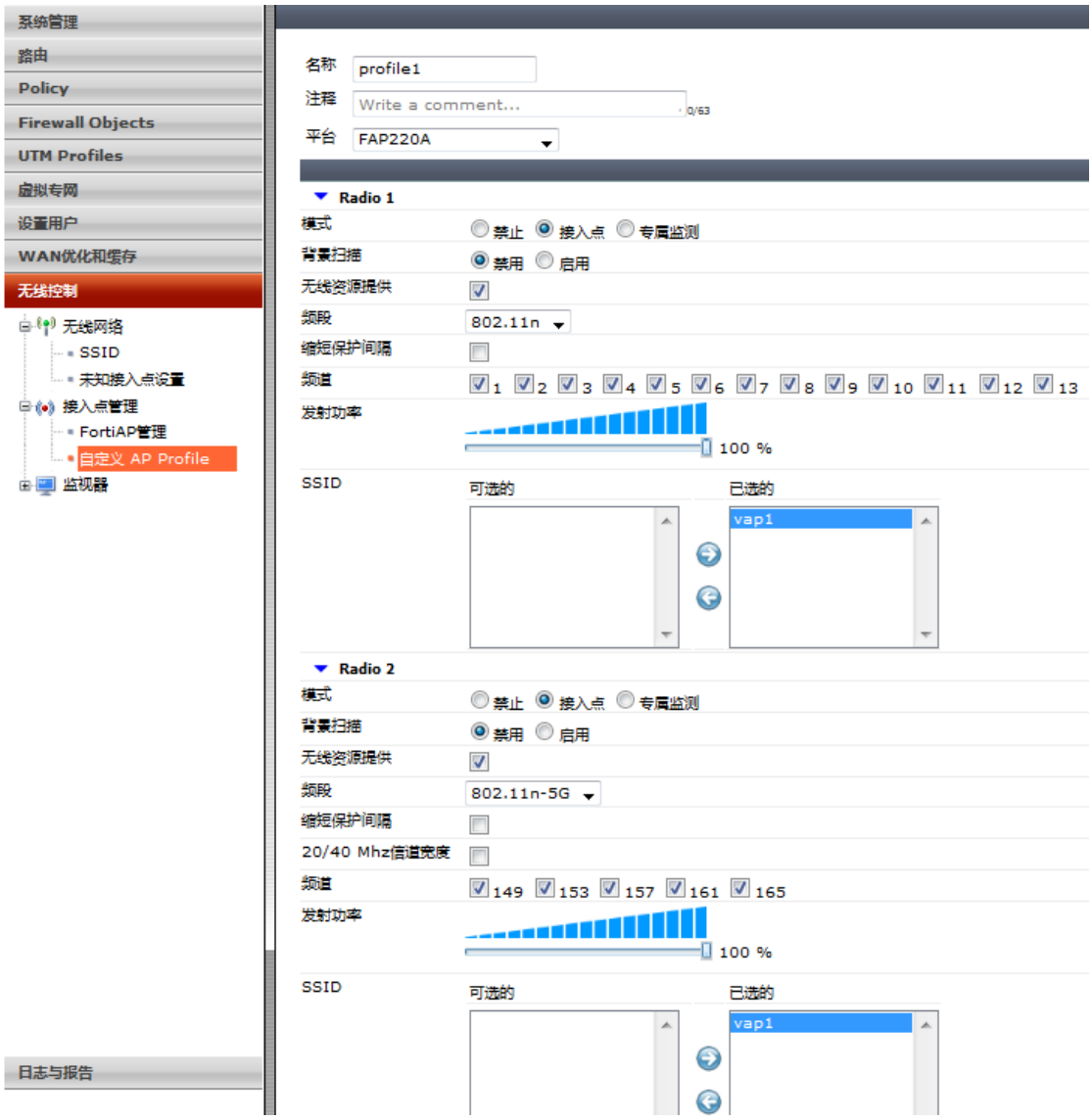
3.3 无线用户与 AP 的连接

无线上网用户（PC、PAD、手机等）使用标准的 802.11 无线协议族连接到 AP，从而接入无线网络。

FortiAP 支持以下 WIFI 协议：

- IEEE 802.11a (5-GHz Band)
- IEEE 802.11b (2.4-GHz Band)
- IEEE 802.11g (2.4-GHz Band)
- IEEE 802.11n (5-GHz & 2.4-GHz Band)

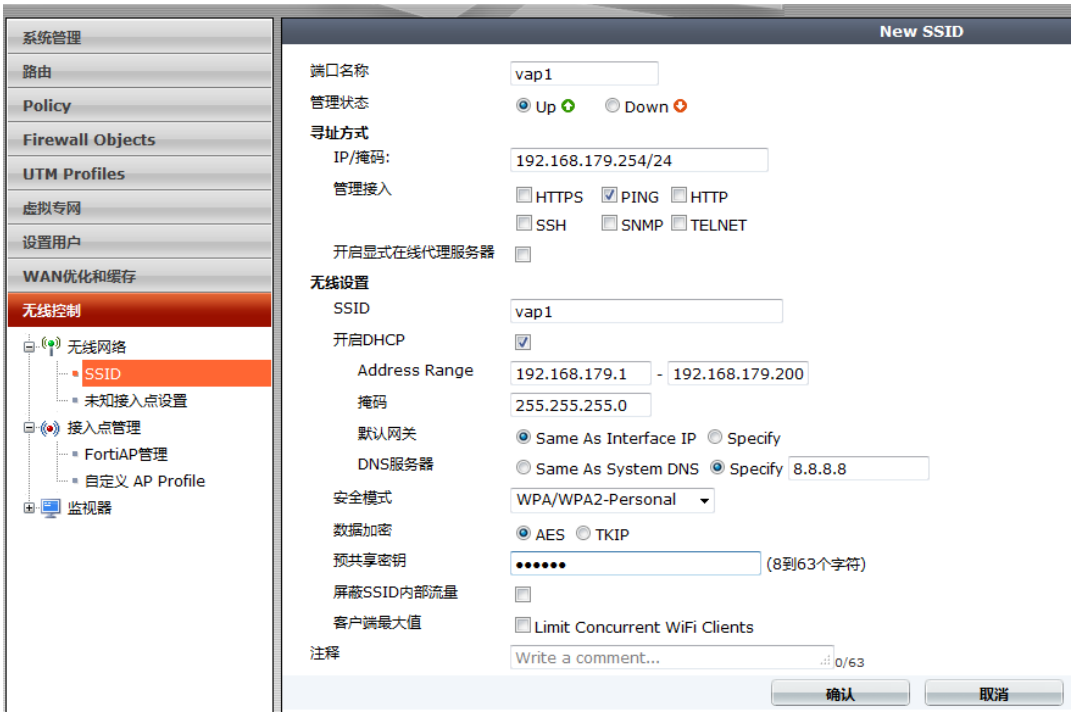
FortiAP-220B 内置 4 个天线，支持两个 Radio 同时工作，例如一个 Radio 处理 5-GHz 802.11n，另一个 Radio 处理 2.4-GHz 802.11n。



Fortinet 的无线方案支持 ARRP（自动无线资源管理）功能，所有 AP 都会

自动周期性地检查无线网络环境，选择最佳频道进行通信，减少网络干扰，获得最佳通信质量。

AP 可以使用 DHCP 为无线上网终端分配 IP 地址、掩码、网关、DNS 等网络设置，减少终端配置量。



3.4 无线通信的安全保护

3.4.1 通信加密

Fortinet 无线方案支持多种无线加密方式，包括：

- 开放模式（不加密，不建议使用）；
- WEP（64bit 或 128bit RC4 加密）；
- WPA（256bit TKIP 或 AES 加密）；
- WPA2（256bit TKIP 或 AES 加密，在 WPA 的基础上支持 802.11i 标准的安全要求）；

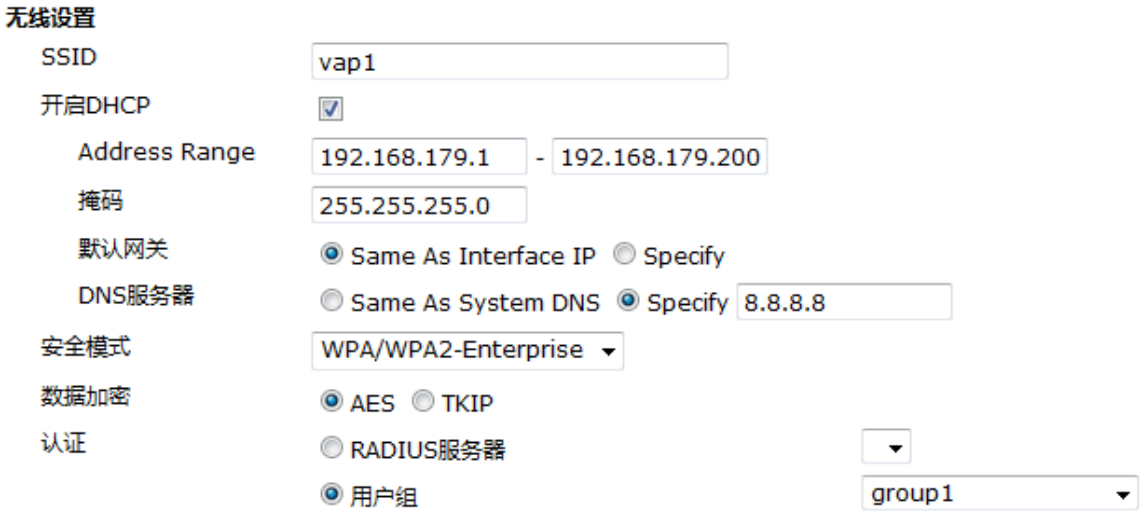
从安全角度考虑，建议使用 WPA2 和 AES 加密方式。

3.4.2 无线准入控制

为防止非法用户对无线网络的滥用以及可能产生的安全威胁，Fortinet 无线方案可以使用如下几种方式对无线用户的接入进行控制：

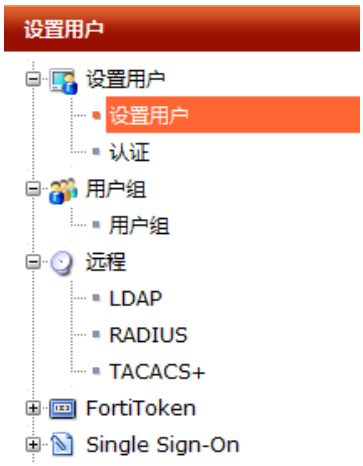
- 关闭 SSID 广播——其它无线用户无法扫描到 SSID，降低安全风险。
- 控制发射功率——减少不必要的覆盖，例如办公区域以外。

- MAC 地址过滤——建立 MAC 地址白名单，不在名单内的终端无法接入网络。
- 无线接入用户认证——支持强制 Web 认证页、WEP 预共享密钥、WPA/WPA2 预共享密钥、802.1x、动态令牌等。用户认证数据库既可以在 FortiGate 本地建立，也可以使用第三方认证服务器，包括 Radius、LDAP、TACACS+、Windows AD 等。



- 访问控制用户认证——在无线用户访问网络的防火墙策略中，也可以启

用用户认证功能，包括静态口令、动态令牌、数字证书等。用户认证数据库既可以在 FortiGate 本地建立，也可以使用第三方认证服务器，包括 Radius、LDAP、TACACS+、Windows AD 等。访问控制用户认证支持自动超时（超过管理员设定的超时时间，如 5 分钟，就自动退出登录）和保持认证状态（用户手动退出登录）两种方式。

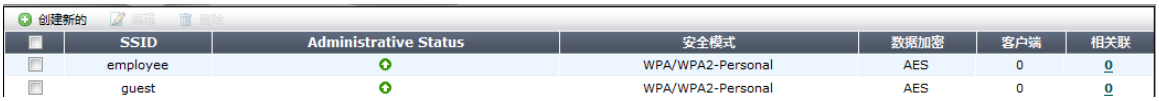


3.4.3 访问控制

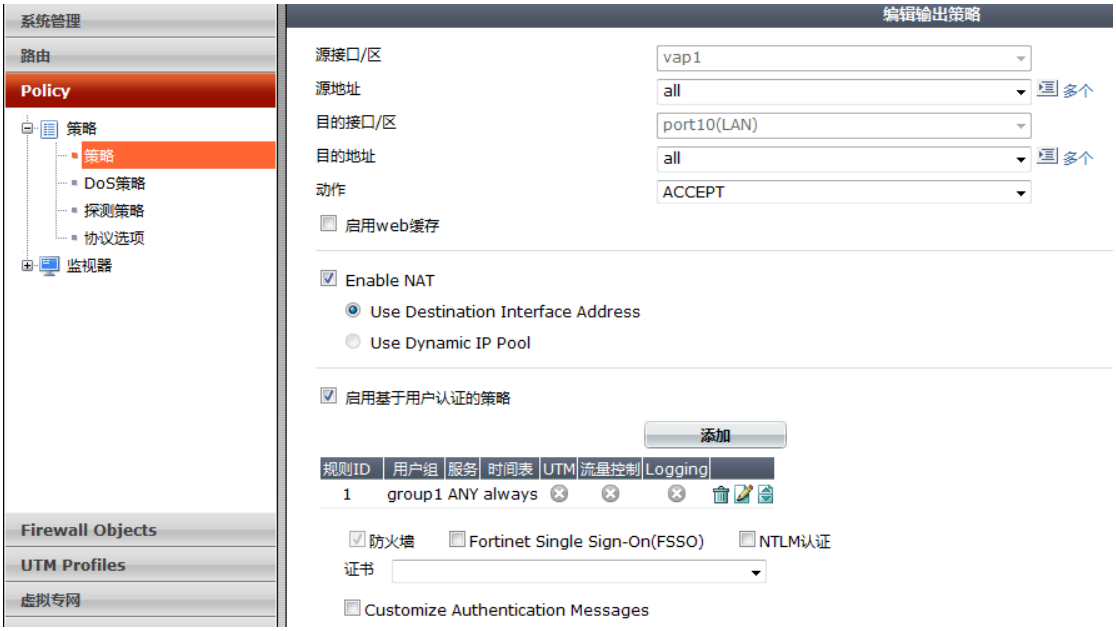
Fortinet 无线方案能对无线用户接入网络后的访问权限进行控制，包括以下几种方式：

- 使用不同的 SSID 将用户分组。例如内部员工使用 employee SSID，来宾使用 guest SSID。这两个 SSID 使用不同的 IP 地址段，不能直接互访，必须经过 FortiGate 安全设备的过滤。本次部署的方案支持最多 14 个接入用的 SSID。

  还可以为不同的 AP 分配不同的属性（AP profile），实现不同的部署。例如：AP1 部署在会议室等公共区域，启用 employee 和 guest 两个 SSID；AP2 部署在办公区域，只启用 employee 一个 SSID。

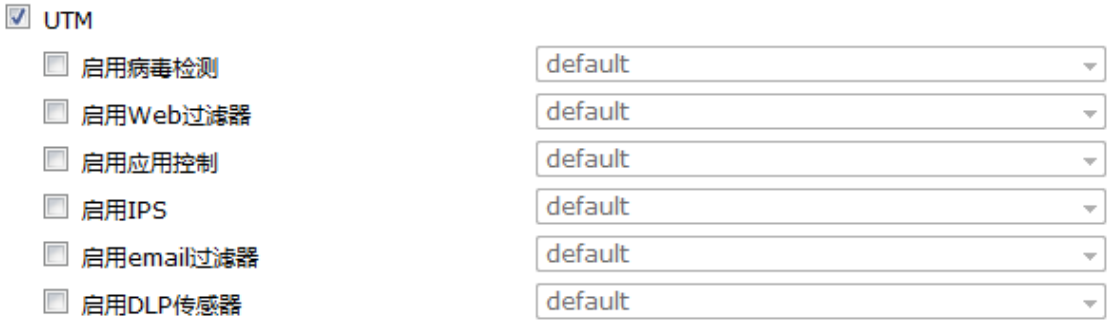


- 防火墙访问控制。各组用户通过不同 SSID 接入无线网络后，无论互访还是访问网络其它区域（如生产网、办公网等），都要经过防火墙策略的控制。FortiGate 可以对源/目的接口、源/目的 IP 地址、源/目的端口、时间、用户等进行过滤，从而使每一个无线用户都仅能访问他可以访问的资源。



3.4.4 应用安全功能

Fortinet 无线安全方案无缝集成了 Fortinet 公司领先业界的 UTM（统一威胁管理）安全解决方案，除防火墙外，还可以直接使用 VPN、入侵防御、网关防病毒、Web 内容过滤、应用控制、Email 过滤、数据泄漏防护等网络层及应用层安全功能，对无线用户的网络访问进行全面的安全防护，使整个无线网络达到一个很高的安全水平。



3.5 AC 的冗余保护

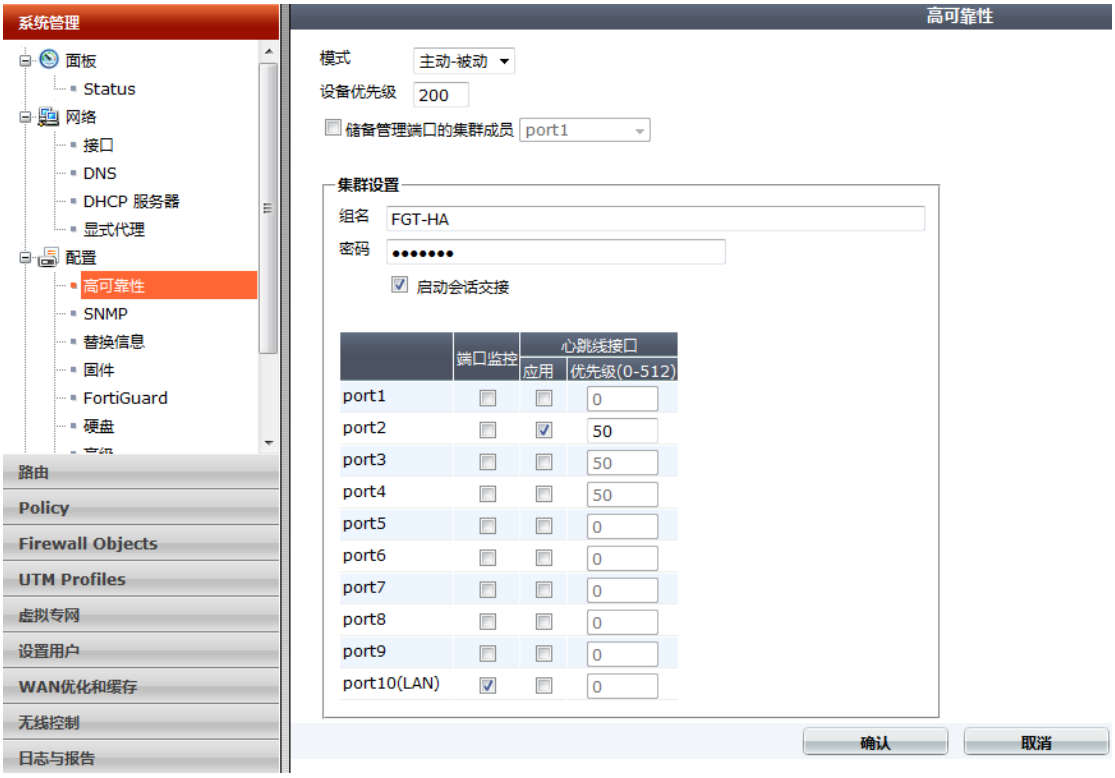
根据上文中的部署拓扑示意图所述，使用 2 台 FortiGate-620B，使用相同的接口连接到 AP、AC 所在的 VLAN，2 台 FortiGate-620B 配置成 A-P（主动-被动）HA 模式。

FortiGate HA 集群中的设备根据设备优先级的大小协商产生主机和备机，优先级高的设备成为 HA 组中的主机，优先级低的设备成为 HA 组中的备机。主机和备机具有完全相同的接口地址、完全相同的配置。

主机和备机的配置通过心跳线实时同步，管理员的配置针对整个 HA 集群，无需单独配置每一台设备。

主机和备机的相应接口具有完全相同的 IP 地址，并使用同一个虚拟 MAC 地址，在发生故障切换时不会产生 IP 或 ARP 问题。

当主机的任意接口或设备本身发生故障时，产生 HA 设备切换，主机变为 standby 状态，备机变为 work 状态，自动接替主机工作。由于会话状态均在主备机之间同步，因此所有访问自动切换到备机上进行，所有已建立会话无需重新连接。


系统管理
面板
Status
网络
接口
DNS
DHCP 服务器
显式代理
配置
高可靠性
SNMP
替换信息
固件
FortiGuard
硬盘
路由
Policy
Firewall Objects
UTM Profiles
虚拟专网
设置用户
WAN优化和缓存
无线控制
日志与报告
高可靠性
模式
主动-被动
设备优先级
200
储备管理端口的集群成员
port1
集群设置
组名
FGT-HA
密码
启动会话交接
端口监控
心跳线接口
应用
优先级(0-512)
port1
port2
port3
port4
port5
port6
port7
port8
port9
port10(LAN)
确认
取消