**一、设备扫描**

功能：扫描指定局域网网段内的被保护设备及防火墙设备信息（包括设备IP地址，MAC地址以及被保护设备的设备类型），必须提前知道被保护设备的IP地址。根据扫描结果建立拓扑结构。

**二、规则配置**

1、深度包检测规则

a、ModbusTCP（数据包中目的和源IP地址、端口、寄存器地址、功能码及寄存器传值）；

b、OPC

c、DNP3（目的和源IP地址、端口）；

2、应用层协议控制（APC）

可配置允许通过或者禁止通过某应用层协议（http,ftp,smtp,pop3,telnet,ssh）；

3、连接数控制（CNC）

控制IP最大并发会话数

4、NAT映射（源地址映射和目的地址映射）

5、策略路由（PRT）

默认路由，到主机的路由，到网络的路由

6、状态检测（STD）

<http://blog.chinaunix.net/uid-127037-id-2919355.html>

iptables的状态检测机制： http://blog.chinaunix.net/uid-7387830-id-118921.html

**三、IP配置**

可将防火墙设置为无IP模式，同时提供重设IP地址操作。

**四、白名单**

设置能通过的用户（主机IP地址）

**五、日志**

配置规则后防火墙产生的iptables日志发送给客户端后存入客户端主机的数据库中