如何配置 FSSO 认证

版本	1.0
时间	2011 年 9 月
作者	胡丹丹(ddhu@fortinet.com)
支持的版本	FortiOS v4.3.1
状态	草稿

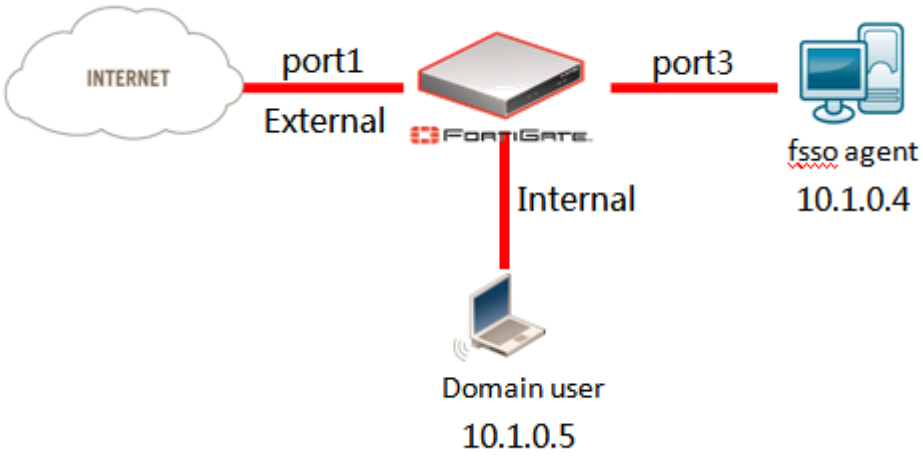
目录

1.目的

本文档针对 Fortinet 的 FSSO，即防火墙结合 Windows 活动目录的策略认证配置进行说明。

2.环境介绍

本文使用 FortiGateVM,Windows2003,windows xp 做演示。本文支持的系统版本为 FortiOS v4.0MR3 Patch 1 及更高,FSSO 的软件版本为 3.5.068。



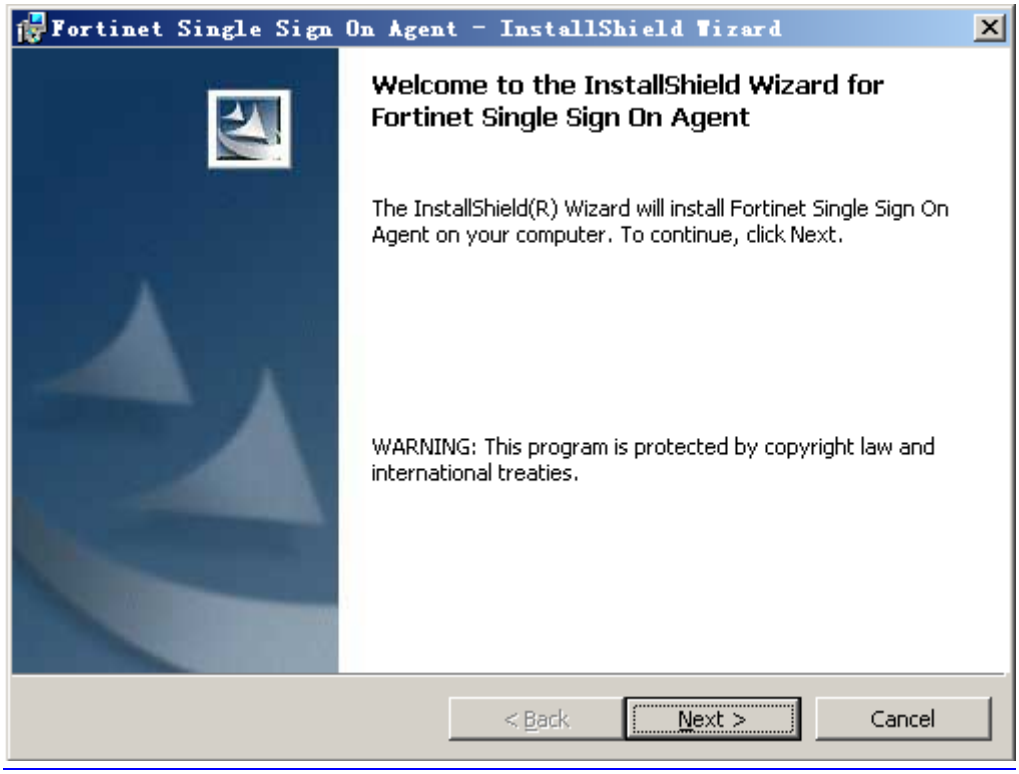
3.在域控中安装 FSSO

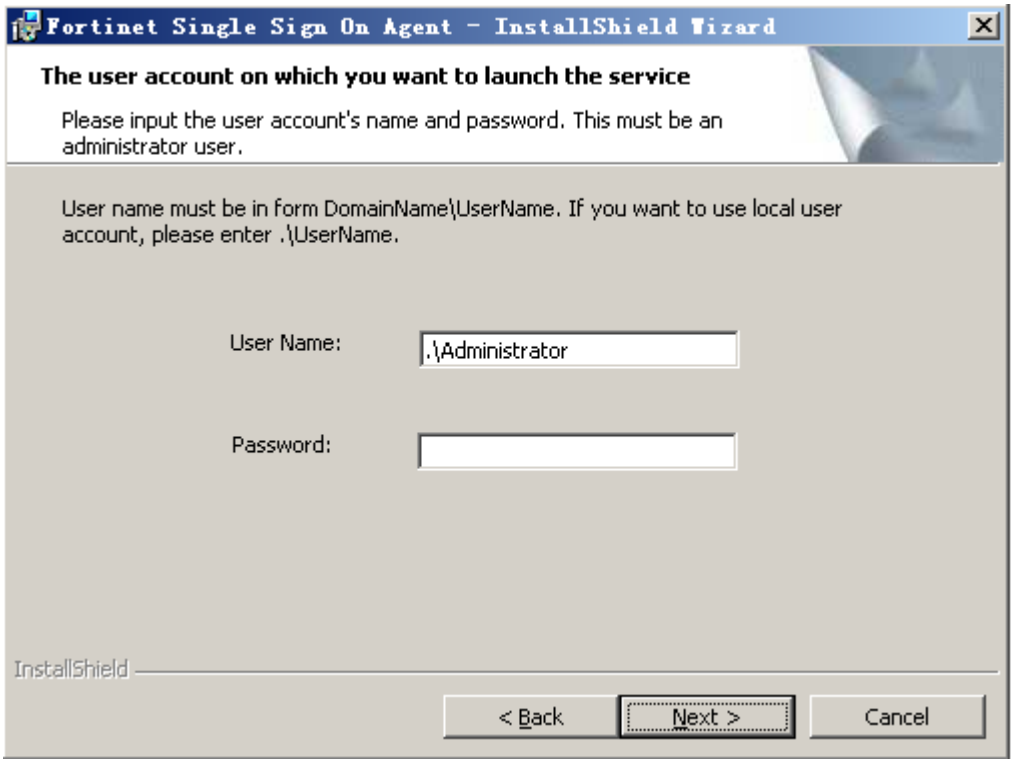
3.1. 下载 FSSO 安装软件

通过账号登陆 Support.fortinet.com 进去 Firmware 菜单 4.0MR3 Patch1 FSSO 目录中获取 FSSO 软件，

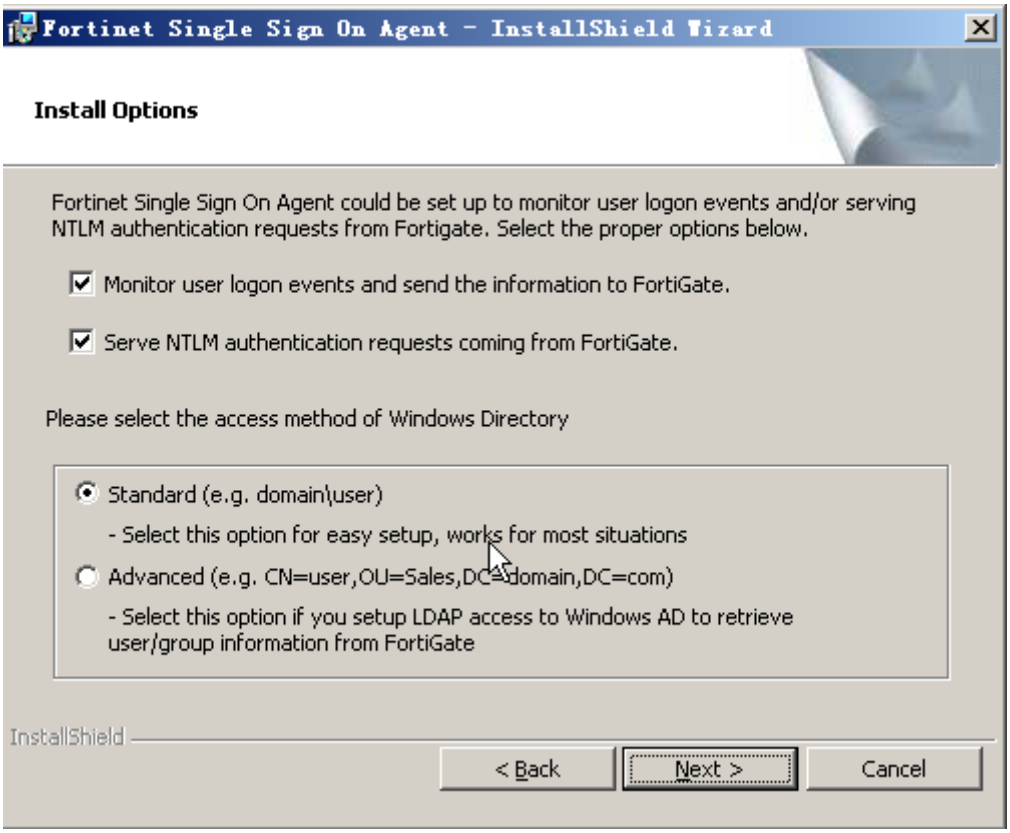
3.2. 安装 FSSO

运行 FSSO 安装文件

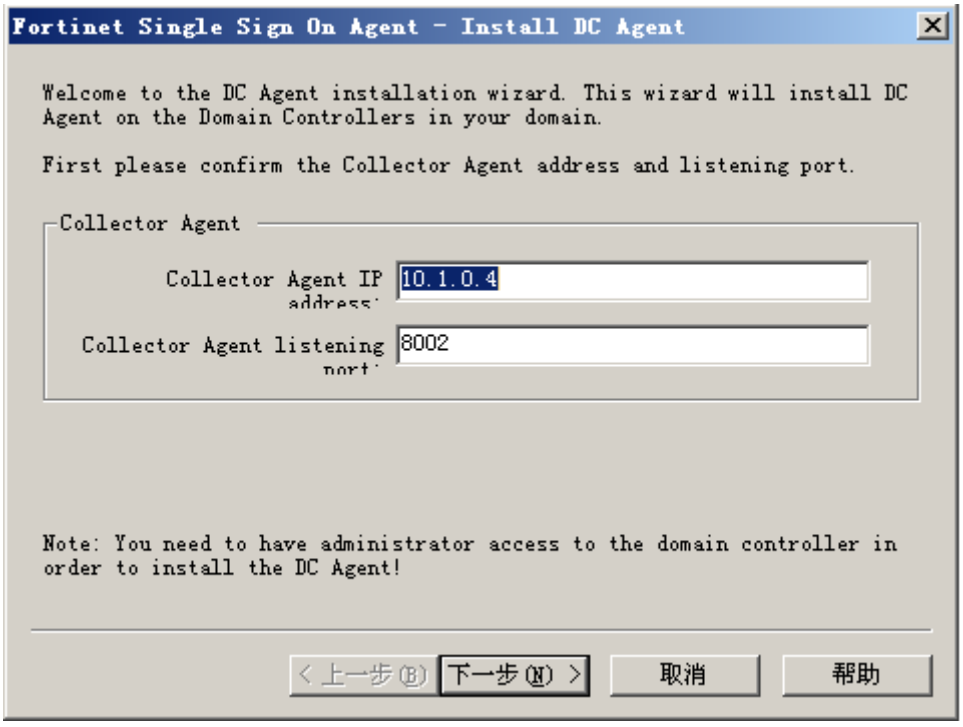

Fortinet Single Sign On Agent - InstallShield Wizard
Welcome to the InstallShield Wizard for Fortinet Single Sign On Agent
The InstallShield(R) Wizard will install Fortinet Single Sign On Agent on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel


Fortinet Single Sign On Agent - InstallShield Wizard
The user account on which you want to launch the service
Please input the user account's name and password. This must be an administrator user.
User name must be in form DomainName\UserName. If you want to use local user account, please enter .\UserName.
User Name:
.\Administrator
Password:
InstallShield
< Back
Next >
Cancel

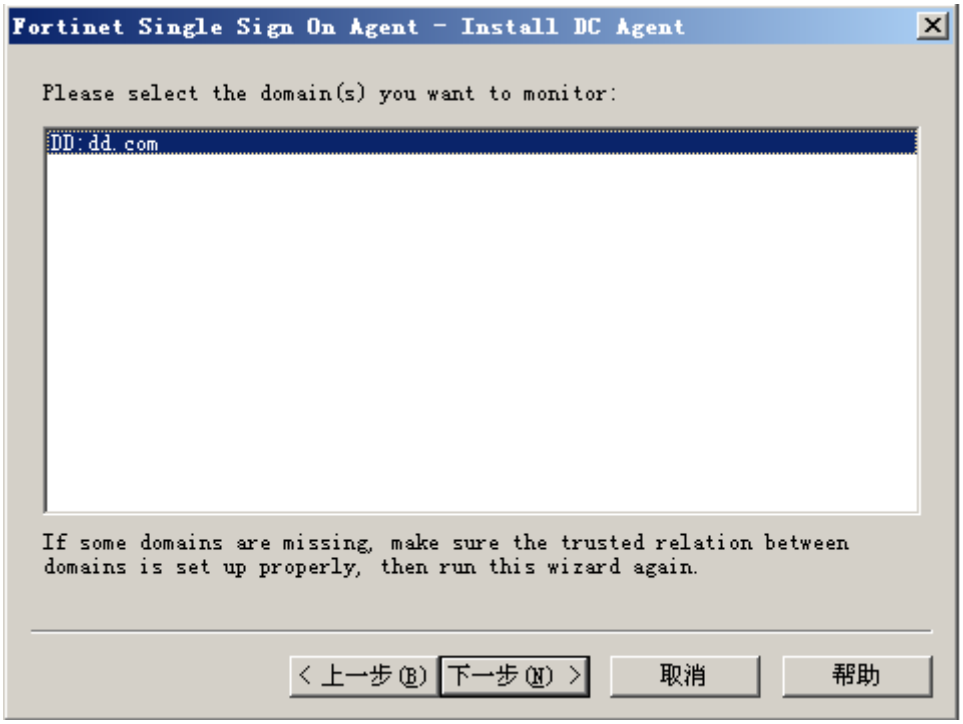
可以根据实际情况选择标准模式或者高级模式，标准适用于大部分场景。



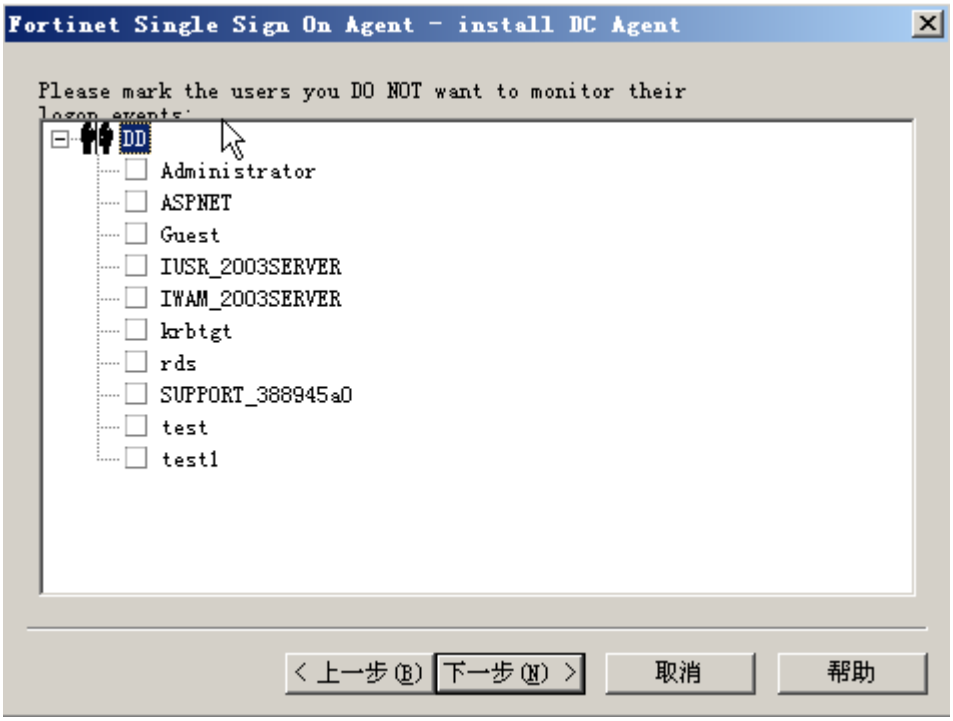
填入 FSSO 代理的认证的地址(通常为 windows AD 服务器地址)和监听端口



选择需要认证的域，此例的域名为 dd.com



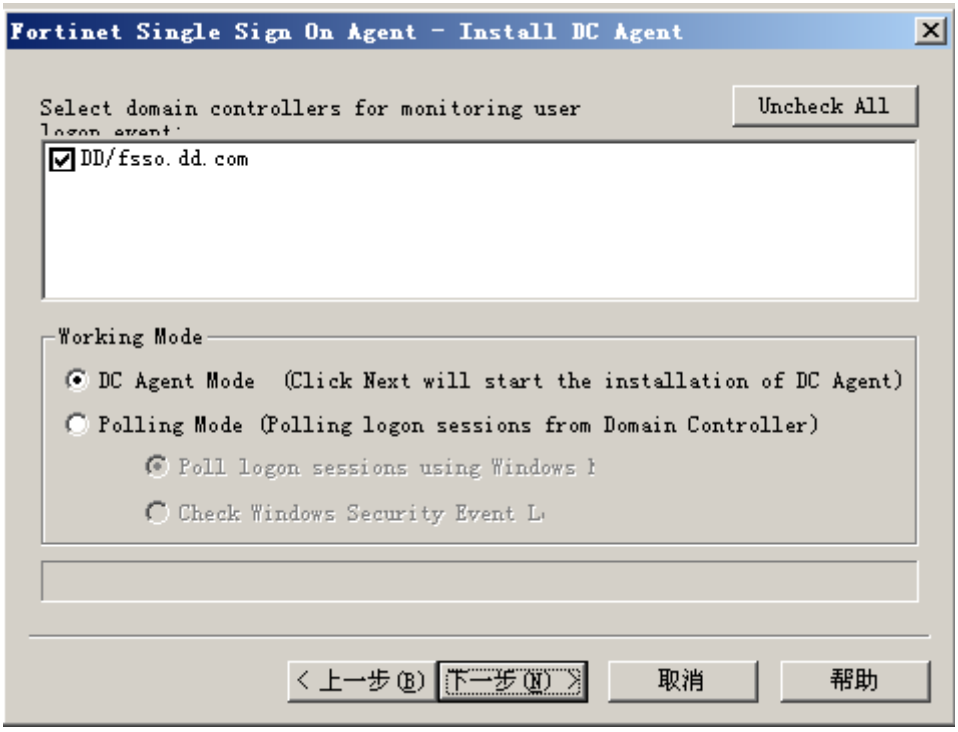
FSSO agent 模式通过监控 AD 的用户登陆事件实现认证，此处选择用户表示对此用户的登陆事件不进行监控，该用户将无法通过认证。



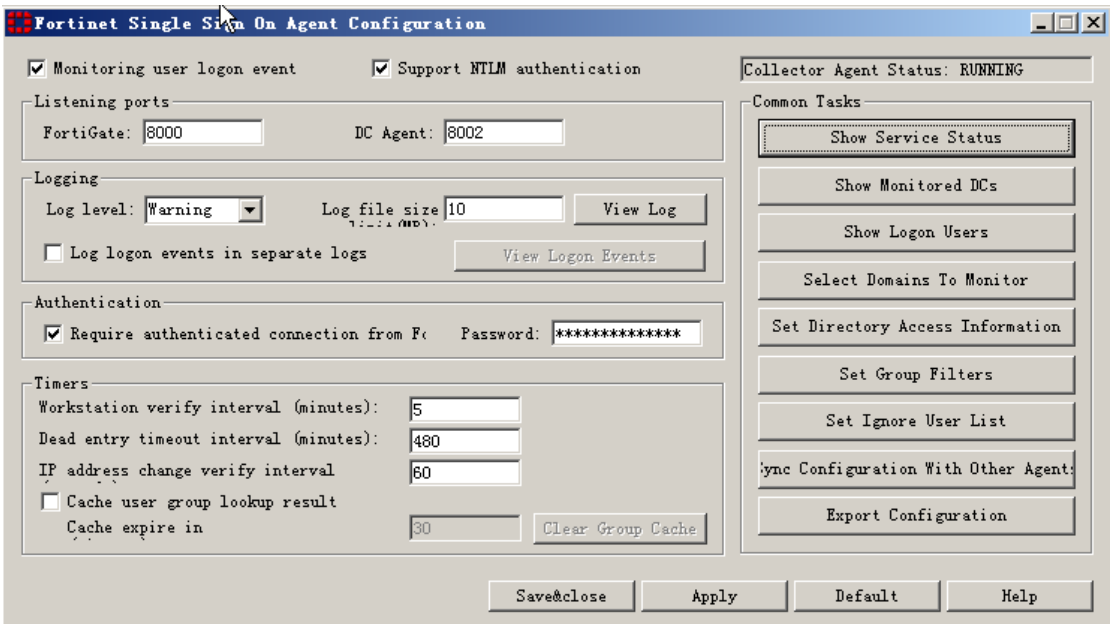
FSSO 可以工作在 DC Agent 模式，Polling 模式。DC Agent 与 Polling 的区别如下:

DC Agent 通过监控 Windows 的登陆事件来完成认证，在实现域中多台域控服务器认证时，需要在每台域控中安装 FSSO Agent 以实现最大精度的监控；

Polling 模式:FSSO 每 10 秒使用轮询方式获取所有域服务器中的用户的登陆信息，在大型部署或异地认证时不适用此模式。

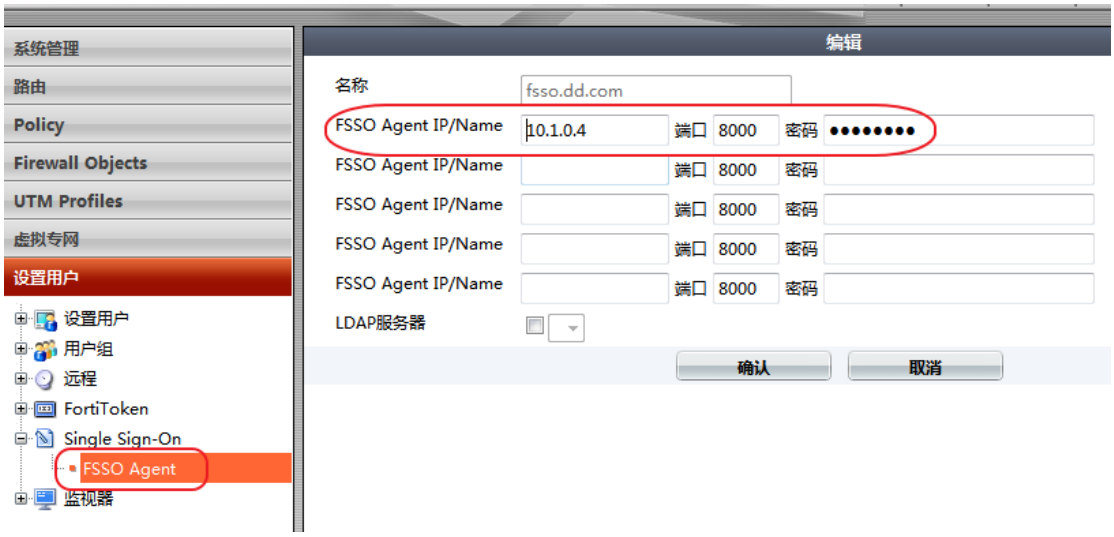


运行 Configure Fortinet Single sign on Agent



3.3. 设置 FortiGate 用户及用户组

在设置用户中新增 fsso agent 填入 agent 地址和密码，该密码须与 fsso 设置认证密码一致。



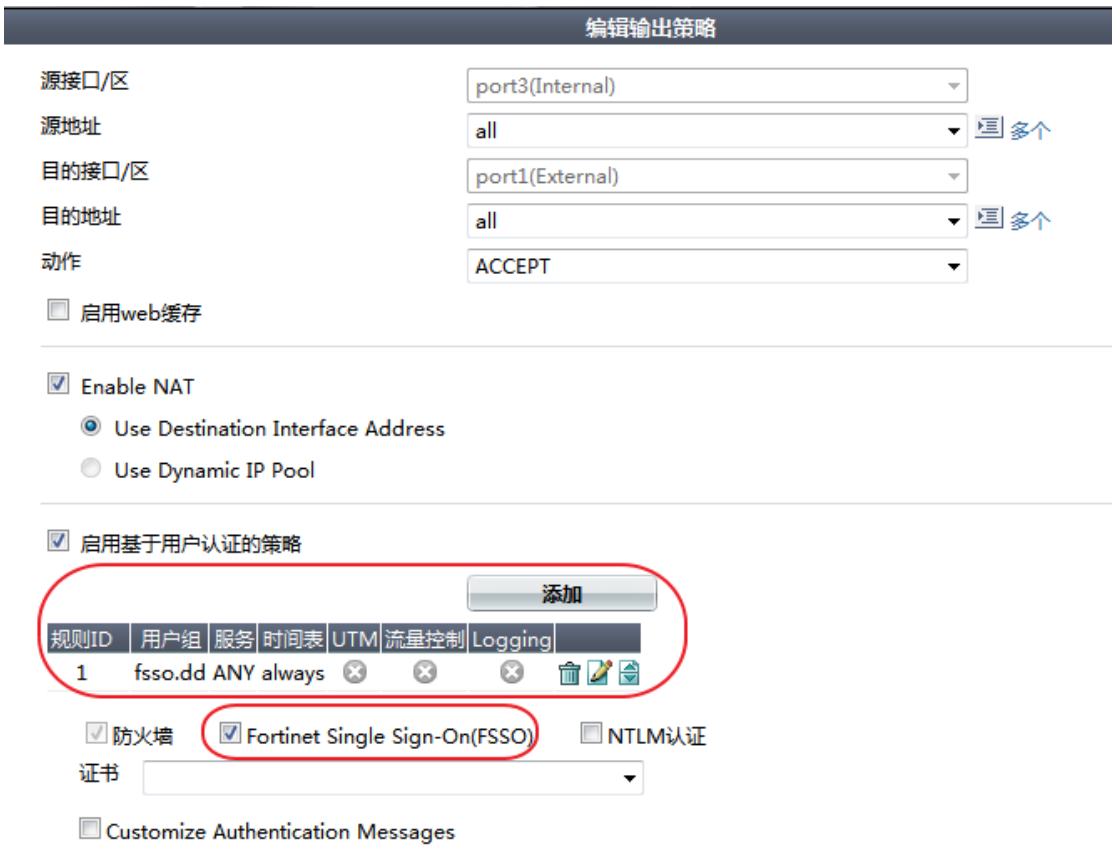
确认完成后，选择该 agent 刷新后会出现域控中的组

继续建立用户组，此例我们以 USERS 作为认证用户组，如果实际环境涉及到所有用户实现域认证，需要将所有用户组选中。

该文中我们使用域中的 fsso 用户作为测试用户

3.4. 建立域认证策略

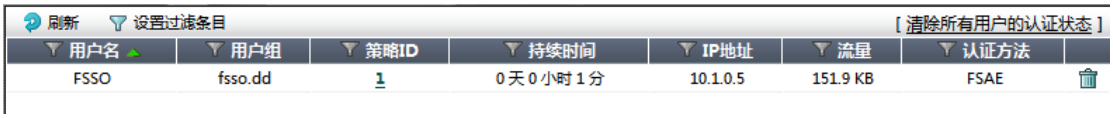
进入防火墙-->策略，新建一条防火墙策略，源接口是内网接口，目的接口是外网接口，然后添加 FSSO 认证组，选择之前建立的 FSSO 用户组即可，并勾选 FSSO 认证选项，具体如下图显示：



3.5. 验证及调试信息

使用域中用户登陆

通过访问 Internet 激活策略中的认证，那么在防火墙的设置用户中的监视器可以查看到通过 FSSO 认证的用户信息。



在防火墙 CLI 的相关命令：

dia debug enable　　显示 debug 信息

dia debug application authd -1　　显示认证信息

通过验证输出信息:

Fortigate-VM # _event_read[fsso.dd.com]: received heartbeat 100240
message_loop: checking timeouts
authd_admin.c:541 authd_admin_read: called
authd_admin.c:572 proto=6 src=10.1.0.5:1217 dst=117.79.130.24:80
authd_admin.c:420 fsae_add_policy: called
_find_policy: **found cached policy (id=1)**
fsae_add_policy:449: **1 group(s) found for user FSSO(DD/USERS) IP 10.1.0.5 on policy 1**
fsae_add_policy:465: new policy 10.1.0.5 timeout=3000 policy_id=1groups=(4)

diagnose debug authd fsae list　　显示在域上的用户

输出信息:

Fortigate-VM # diagnose debug authd　fsso list
----FSSO logons----
IP: 10.1.0.5　User: FSSO　Groups: DD/DOMAIN USERS+DD/USERS
Total number of logons listed: 1, filtered: 0
----end of FSSO logons----

未通过验证输出信息:

authd_admin.c:541 authd_admin_read: called
authd_admin.c:572 proto=6 src=10.1.0.5:1269 dst=222.88.93.170:80
authd_admin.c:420 fsae_add_policy: called
_find_policy: found cached policy (id=1)
fsae_add_policy:441: **no group found for user FSSO group DD/DOMAIN USERS+DD/USERS IP 10.1.0.5 (policy id 1)**

4.FSSO 参数设定说明

在 AD 服务器上 FSAE 软件的参数:

Listening ports 监听端口: 默认用 TCP8000 端口与 FortiGate 通讯，用 UDP 8002 端口与 DC 代理通讯

Timers 时间设置:

工作站检查时间:FSAE 会定时检查登陆的用户是不是还在域上，默认为 5 分钟

不可达主机超时时间(Not verify 状态):对于登陆到域的主机，但 FSAE 无法与该主机通讯 默认 480 分钟后会将改主机从登陆用户中删除（解决办法请参考 FSAE 用户列表中“Not verified”解决办法)

IP 地址更换检查时间:FSAE 会每 60 秒（默认）检查在域上的主机ＩＰ，对于更改 IP 的主机，FSAE 会及时地通知 FortiGate

Common Tasks 常用工具:

Show Service Status:显示 FSAE 与 FortiGate 的通讯状态，正常为 RUNNING

Show Logon Users:显示 FSAE 收集到的在域上用户信息