# 5.0 功能概要-FSSO 增强

| | |
|---|---|
| 版本 | 1.0 |
| 时间 | 2013 年 1 月 |
| 作者 | Fortinet 技术中心(support_cn@fortinet.com) |
| 支持的版本 | FortiOS v5.0 build 147 |
| 状态 | 已审核 |

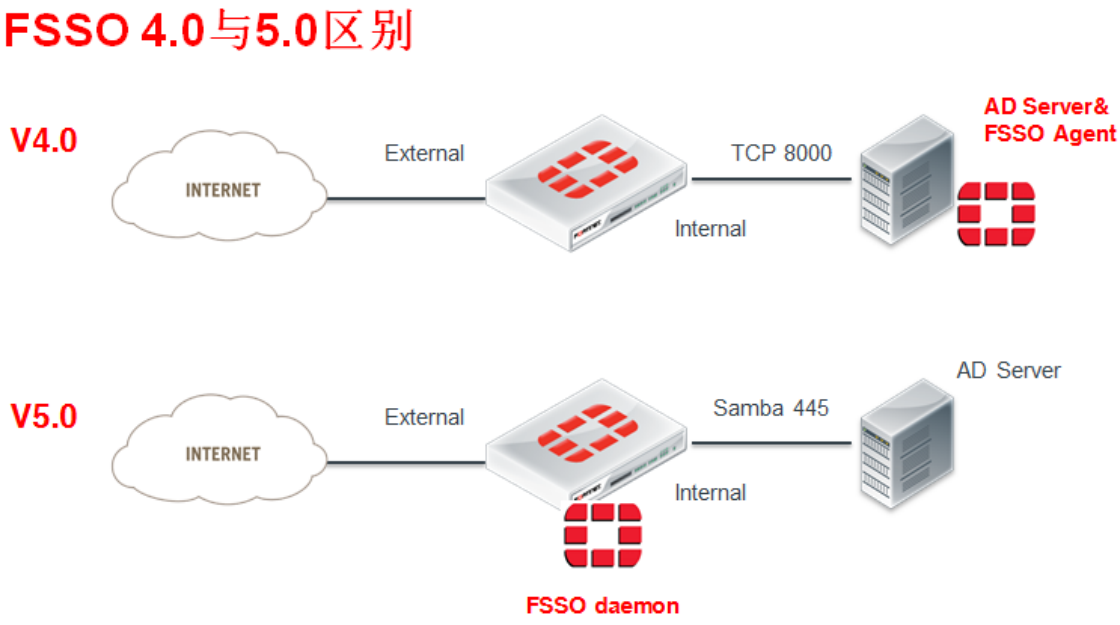
# 目录

# 1.目的

FOS 5.0 之前的 FSSO 支持 Agent 模式及 polling 模式 ,需要在 AD 服务器上安装 Collector agent 或者 DC agent。FOS5.0 起支持无需在 AD 服务器中安装任何插件实现 FSSO 的工作模式。本文就 FOS5.0 的 FSSO 部分增强进行说明。

# 2.环境介绍

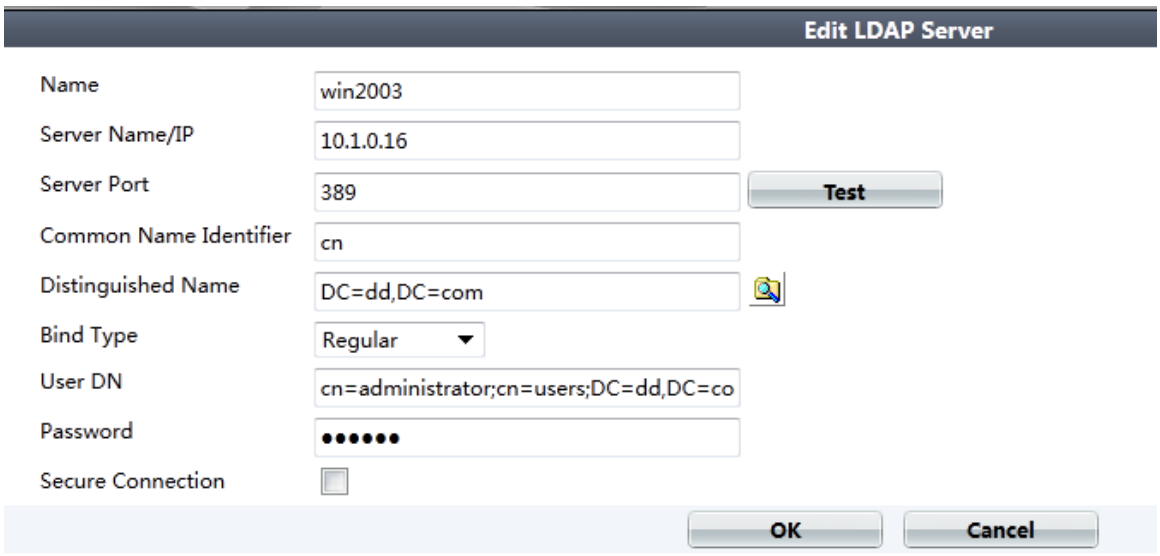
本文使用 FortiGate VM，本文使用 FOS5.0 build 147 进行说明。FSSO 在 4.0 的模式中需要安装 Agent，FortiGate 通过 TCP 8000 端口与 AD 进行交换，5.0 中 FortiGate 自身将会有进程专门负责原来 AD agent 的工作，通过 LDAP 以及 445 端口获取用户登陆信息。以下为 4.0 及 5.0 工作模式示意，对于 4.0 下的 FSSO 配置可以参考 [如何配置 FSSO 认证 4.3]。



# 3.配置

## 3.1 配置 LDAP

在用户认证中配置 LDAP 用于获取用户信息




## 3.2 配置单点登录(SSO)

FOS5.0 中支持以下三种单点登录 SSO 方式。此例着重说明无需代理安装情况。

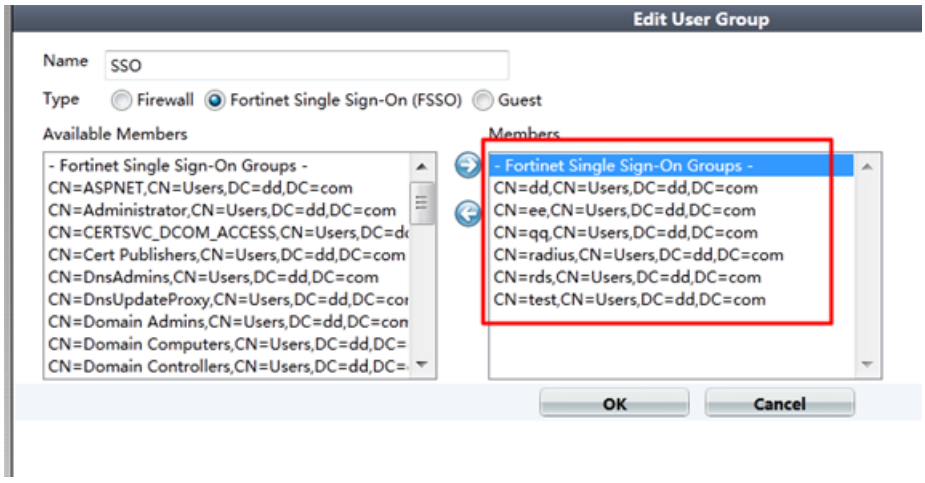
1.活动目录服务器(无需代理安装)

2.Fortinet 单点登录代理(4.0 需要安装代理)

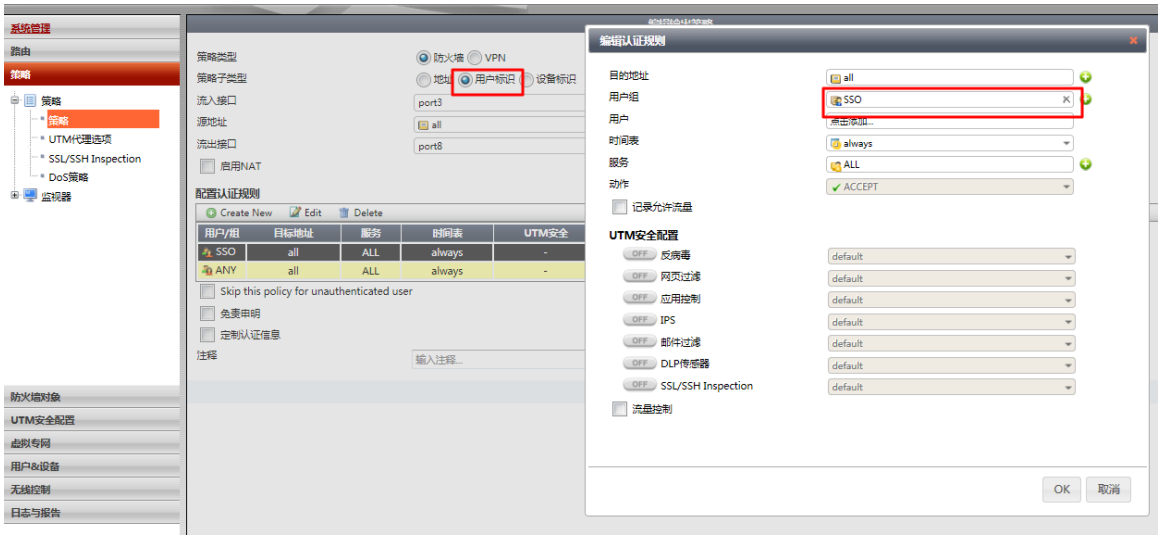
3.Radius SSO (结合 radius 服务实现单点登录)

配置 LDAP server 后，如果通讯正常，则可以继续选择相应的用户组


添加用户组




## 3.3 配置单点登录策略




## 3.4 测试验证

连接后可以查看相应的状态


ForiGate 将周期的从 ldap 获取 event log。

```
1 0.000000   10.1.0.16   10.1.0.1    SMB      250 Session Setup AndX Response
2 0.000737   10.1.0.1    10.1.0.16   SMB      152 Tree Connect AndX Request, Path: \\10.1.0.16\IPC$
3 0.003284   10.1.0.16   10.1.0.1    SMB      126 Tree Connect AndX Response
4 0.003628   10.1.0.1    10.1.0.16   SMB      174 NT Create AndX Request, FID: 0x800e, Path: \eventlog
5 0.004104   10.1.0.16   10.1.0.1    SMB      173 NT Create AndX Response, FID: 0x800e
6 0.004903   10.1.0.1    10.1.0.16   DCERPC   224 Bind: call_id: 1 Fragment: Single EVENTLOG V0.0
7 0.005424   10.1.0.16   10.1.0.1    DCERPC   194 Bind_ack: call_id: 1 Fragment: Single accept max_xmit: 4280 max_
```

# 4.诊断及调试相关

以下为相关的诊断及调试命令

FortiGate-VM # **diag debug en**

FortiGate-VM # **diag debug authd fsso**　需要开启 debug 以下命令才有输出

clear-logons　clear logon information

filter　filters used for list or clear logons

list　list current logons　#当前已登录用户

refresh-groups　refresh group mappings

refresh-logons　resync logon database

server-status　show FSSO agent connection status　#Agent 连接状态

summary　summary of current logons

FortiGate-VM # **di de fsso-polling　/ di de fsso**

client　Show FSSO AD Server Clients

detail　Show FSSO AD Server Detail　#FSSO samba 连接信息

group　Show FSSO AD Server Groups

refresh-group　Refresh FSSO AD Server Groups

refresh-user　Refresh FSSO AD Server users

summary　Show FSSO AD Server Summary

user　Show FSSO AD Server users

查看 fssod 进程 debug 信息

FortiGate-VM #

FortiGate-VM # di de en

FortiGate-VM # di de app fssod -1　#查看 fssod 进程 debug 信息

FortiGate-VM # [fsso_svr.c:ldap_get_grp:855] failed to get ldap entries for dn=null at ldap server(win2008, 10.1.0.18, user(cn=administrator;cn=users;DC=DAN,DC=com))

[fsso_svr.c:ldap_get_grp:855] failed to get ldap entries for dn=null at ldap ser ver(win2008, 10.1.0.18, user(cn=administrator;cn=users;DC=DAN,DC=com)) com))