SANGFOR_SSLVPN7.1_RADIUS认证

测试指导

深信服科技有限公司

文档编号	SSL_CONF_14_05	审核	
修订记录			
版本	时间	修订内容	
1.0	2016年7月		

目 录

1 介绍.....3
1.1 总体说明.....3
1.2 文档目的.....3
1.3 缩写和约定.....3
2 需求背景.....3
3 实现方式.....3
4 测试环境.....3
4.1 测试拓扑.....3
4.2 测试条件.....3
4.3 预期测试效果.....3
5 测试过程.....4
6 测试效果.....7

1 介绍

1.1 总体说明

完成该文档的过程中，不可删除文档结构，但撰写本文档时，可以自行进行内容和结构的扩展。无内容可写的章节，请保持现有斜体字描述。模板中现有的**黑体字、非斜体字务必予以保留**。

1.2 文档目的

为了方便快速达到功能测试效果，减少现场测试出现问题机率。

1.3 缩写和约定

2 需求背景

2.1. 客户有自己的RADIUS认证服务器，希望SSLVPN用户直接到他们RADIUS服务器上进行认证，而不用在本地添加用户，实现SSLVPN和RADIUS服务器的认证结合。

3 实现方式

4 测试环境

4.1 测试拓扑

SSLVPN单臂或者网关部署，保证SSLVPN与RADIUS服务器RADIUS服务端口正常通信，默认是UDP1812端口

4.2 测试前准备

4.2.1 准备一台RADIUS服务器，搭建好RADIUS服务，RADIUS服务器与SSLVPN正常通信。

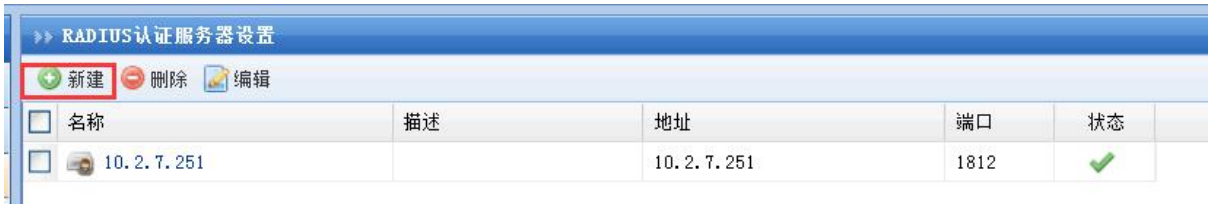
4.3 预期测试效果

4.3.1 RADIUS服务器存在用户test，本地不存在用户庄洋，用户庄洋通过RADIUS认证登录到SSLVPN

5 测试过程

5.1 RADIUS认证设置基础配置

(1)添加LDAP服务器



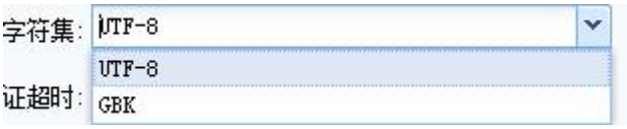
(2)RADIUS服务器基本属性配置

RADOIS服务器基本属性主要有上图标注的四点：

①RADIUS服务器的IP地址和端口，端口默认1812，可根据实际情况调整。

②与RADIUS服务器认证协议的选择，默认是PAP认证协议，可根据实际情况选择，支持以下认证协议

③字符集的设置，默认是UTF-8,可根据实际情况进行选择，支持UTF-8和GBK



④认证超时的设置，根据客户需求选择启用还是禁用，根据客户需求配置超时时间，默认5s

(3)RADIUS服务器扩展属性配置

Radius扩展属性主要应用于radius用户需要绑定手机号码或者虚拟IP的时候的设置，如果没有这个需求可以不进行配置。

Radius用户绑定手机号码或者虚拟IP，需要客户RADIUS服务器设置好相应的ID字段及子属性值绑定这些信息，SSLVPN上RADIUS认证配置好对应的属性ID，在用户认证的时候会通过SSLVPN上RADIUS认证配置好的属性ID去RADIUS服务器查询对应的值，即手机号码或者虚拟IP。

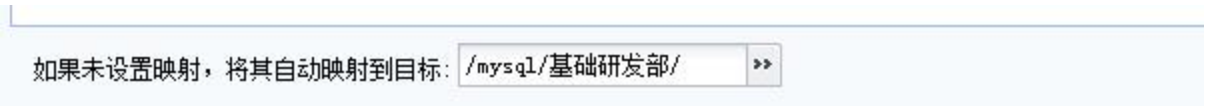
(3)RADIUS用户组映射设置

RADIUS用户组映射的设置主要应用于客户需要针对RADIUS上的用户的分组授权不同的资源，这种情况下就可以将radius上的不同的用户组映射到本地不同的用户组。

这里的字段是指RADIUS服务器上用户分组的字段名称，然后配置映射到本地哪个用户组，比如RADIUS服务器上的字段1对应本地的学生组，字段0对应本地的老师组。

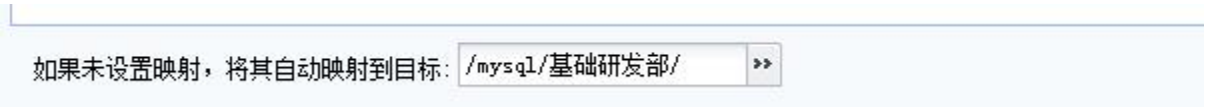
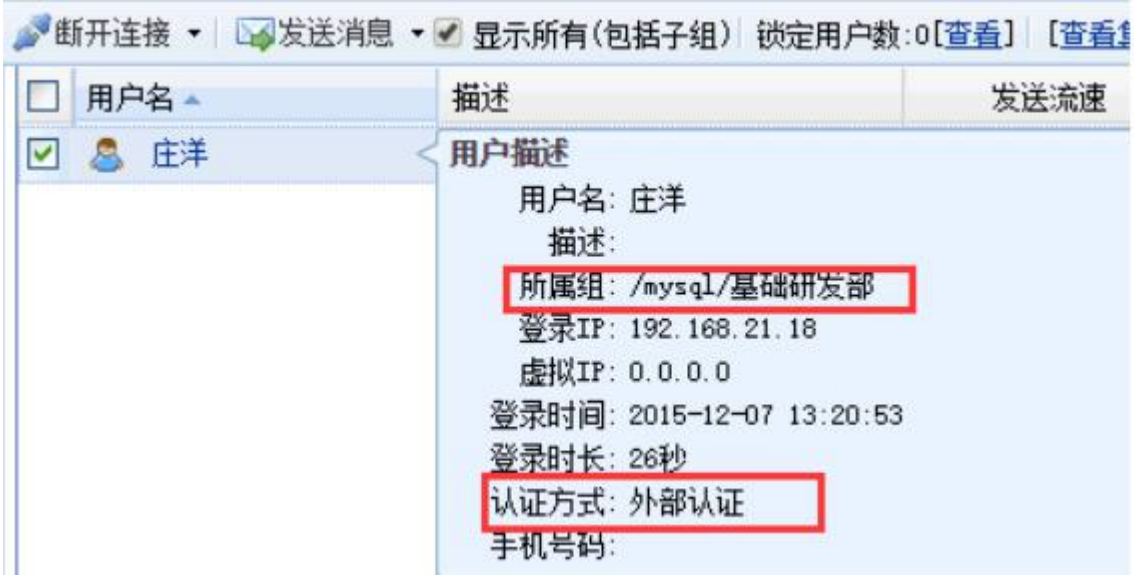
【注意】设置RADIUS组映射的时候，RADIUS分组信息必须由CLASS属性25携带，这样SSLVPN才能识别，进行组映射

在没有配置特定的组映射的时候，RADIUS的用户会匹配默认的组映射规则，匹配到对应的用户组的权限，这个默认映射的用户组可以自己设置，然后授权需要给RADIUS用户访问的资源



6 测试效果

本地用户不存在庄洋，庄洋这个用户在RADIUS服务器上，RADIUS认证默认映射到用户组/mysql/基础研发部



在用户庄洋登录后，可在在线用户里看到他匹配到了/mysql/基础研发部这个用户组