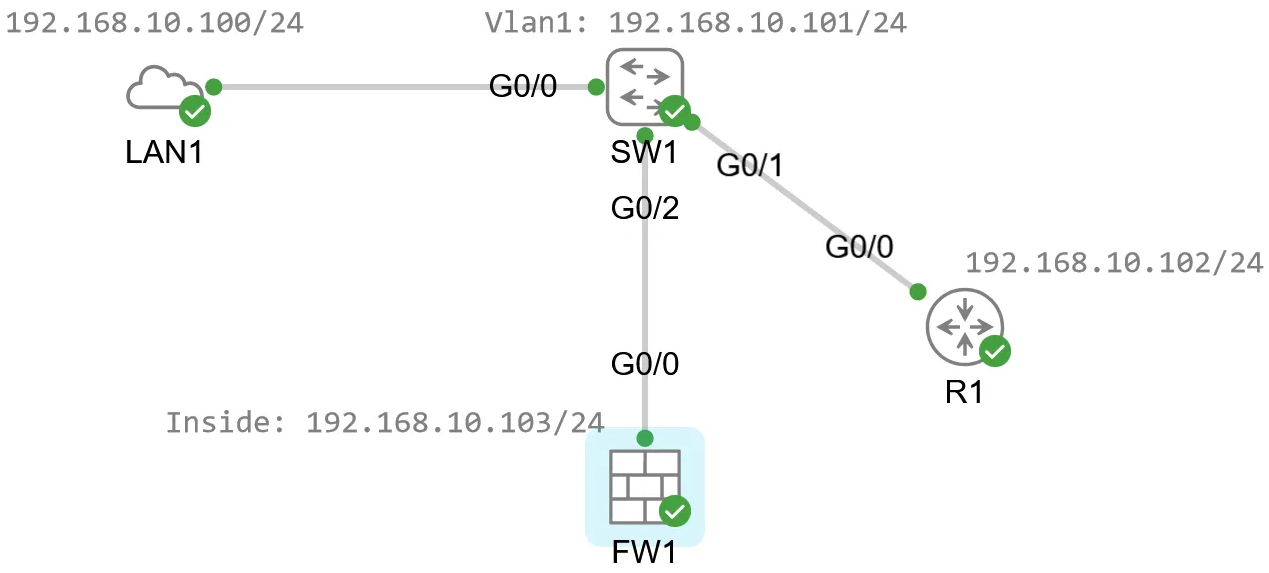
Radius 身份认证专题（ASA/IOS）

一、实验拓扑图



二、Freeradius配置

基本的FreeRADIUS服务器配置指南，适用于Linux环境中的AAA（Authentication, Authorization, Accounting）服务。下面我将对每个步骤进行详细解释：

1. **安装FreeRADIUS**

```bash
apt install freeradius
```

2. **配置客户端**： 编辑 /etc/freeradius/3.0/clients.conf 文件，添加客户端的配置。此配置文件用于指定哪些设备可以与FreeRADIUS服务器通信。

```bash
client 192.168.10.101 {
    secret = cisco
    shortname = SW1
    nas_type = cisco
}
```

3. **配置用户**： 编辑 /etc/freeradius/3.0/users 文件，添加RADIUS用户和相应的权限。

```bash
"user1"    Cleartext-Password := "Skill39!"
            Service-Type = "NAS-Prompt-User",
            Cisco-AVPair = "shell:priv-lvl=15"

"wsi2017"   Cleartext-Password := "Skill39!"
            Service-Type = "NAS-Prompt-User",
            Cisco-AVPair = "shell:priv-lvl=15"
```

4. **重启FreeRADIUS服务**

```bash
systemctl restart freeradius
```

或者使用以下命令停止并以调试模式启动FreeRADIUS：

```bash
systemctl stop freeradius
freeradius -X
```

5. **测试配置**

- **在Linux上测试**： 使用radtest命令来验证FreeRADIUS服务器是否配置正确。

```
Plain Text
1  radtest user1 Skill39! 127.0.0.1 1812 testing123
```

其中，testing123是共享密码。

- **在Cisco设备上测试**： 使用test aaa group命令来测试Cisco设备与RADIUS服务器的连接。

```
Plain Text
1  test aaa group radius user1 Skill39! port 1812 new-code
```

三、Freeradius 详细解释

- **client 192.168.10.101**：定义RADIUS客户端（通常是交换机或路由器）的IP地址。
- **secret = Skill39!**：客户端和RADIUS服务器之间的共享密钥，用于加密RADIUS消息。
- **shortname = SW1**：客户端的简短名称。
- **nas_type = cisco**：指定NAS的类型为Cisco设备。
- **"user1"和"wsi2017"**：用户条目，定义了用户的认证信息和权限。
- **Cleartext-Password := "Skill39!"**：用户的明文密码。
- **Service-Type = "NAS-Prompt-User"**：用户服务类型，通常用于设备管理。
- **Cisco-AVPair = "shell=15"**：Cisco特定的属性值对（AVPair），赋予用户最高的特权级别（15级）。
- **radtest命令**：用于从命令行测试RADIUS认证。参数分别是用户名、密码、RADIUS服务器地址、服务器端口和共享密钥。
- **test aaa group命令**：用于在Cisco设备上测试AAA配置。

这样配置完成后，您可以使用上述命令来测试和验证FreeRADIUS服务器的配置是否正确。如果有任何错误，可以通过freeradius -X命令以调试模式运行FreeRADIUS服务器，从而获取详细的日志信息以便排查问题。

四、IOS网络设备配置

在Cisco IOS设备上配置AAA（认证、授权和记账）以与FreeRADIUS服务器集成的示例配置。下面我将逐行解释这些配置：

1. **启用AAA新模型**

```
aaa new-model
```

启用新的AAA模式以支持RADIUS和TACACS+认证。

2. **配置AAA认证和授权**

```
aaa authentication login Remote-Login group radius local
aaa authorization exec Remote-Exec group radius local
```

- aaa authentication login Remote-Login group radius local：配置登录认证，首先尝试通过RADIUS服务器认证，如果RADIUS服务器不可用，则使用本地认证。
- aaa authorization exec Remote-Exec group radius local：配置exec授权，同样首先尝试通过RADIUS服务器授权，如果RADIUS服务器不可用，则使用本地授权。

3. **配置RADIUS服务器**

```
radius server RADIUS
    address ipv4 192.168.10.100 auth-port 1812 acct-port 1813
    key Skill39!
```

定义RADIUS服务器：

- address ipv4 192.168.10.100 auth-port 1812 acct-port 1813：指定RADIUS服务器的IP地址、认证端口（1812）和记账端口（1813）。
- key Skill39!：指定与RADIUS服务器共享的密钥。

4. **配置SSH**

```
ip domain-name worldskills.org
crypto key generate rsa modulus 2048
ip ssh version 2
```

- ip domain-name worldskills.org：设置设备的域名。
- crypto key generate rsa modulus 2048：生成2048位的RSA密钥对，用于SSH连接。
- ip ssh version 2：启用SSH版本2。

5. **配置VTY线路**

```
line vty 0 15
authorization exec Remote-Exec
login authentication Remote-Login
transport input all
```

- line vty 0 15：选择VTY线路0到15（用于远程登录）。
- authorization exec Remote-Exec：应用之前定义的exec授权方法。
- login authentication Remote-Login：应用之前定义的登录认证方法。
- transport input all：允许所有类型的远程连接（如Telnet和SSH）。

五、ASA网络设备配置

在Cisco防火墙设备上配置AAA，以使用RADIUS服务器进行用户认证和授权的示例配置。以下是逐步配置的详细解释：

1. **配置AAA服务器**

```
aaa-server RADIUS protocol radius
aaa-server RADIUS (Inside) host 192.168.10.100
 key Skill39!
 authentication-port 1812
 accounting-port 1813
```

   - aaa-server RADIUS protocol radius：定义AAA服务器协议为RADIUS。
   - aaa-server RADIUS (Inside) host 192.168.10.100：指定RADIUS服务器的IP地址，并将其分配到Inside接口。
   - key Skill39!：定义与RADIUS服务器共享的密钥。
   - authentication-port 1812 和 accounting-port 1813：指定认证和记账使用的端口号。

2. **配置本地用户**

```
username localadmin password Skill39!
```

   - 定义一个本地用户 localadmin，密码为 Skill39!。

3. **配置AAA认证方法**

```
aaa authentication serial console RADIUS LOCAL
aaa authentication ssh console RADIUS LOCAL
```

- aaa authentication serial console RADIUS LOCAL：配置串行控制台的认证方法，优先使用RADIUS服务器认证，若失败则使用本地认证。
- aaa authentication ssh console RADIUS LOCAL：配置SSH控制台的认证方法，同样优先使用RADIUS服务器认证，若失败则使用本地认证。

4. **配置SSH**

```
crypto key generate rsa modulus 2048
ssh version 2
ssh key-exchange group dh-group14-sha256
ssh 192.168.10.0 255.255.255.0 Inside
```

- crypto key generate rsa modulus 2048：生成2048位的RSA密钥对，用于SSH连接。
- ssh version 2：启用SSH版本2。
- ssh key-exchange group dh-group14-sha256：配置SSH的密钥交换算法。
- ssh 192.168.10.0 255.255.255.0 Inside：允许来自192.168.10.0/24网段的主机通过Inside接口进行SSH访问。

5. **测试AAA服务器认证**

使用以下命令测试RADIUS服务器上的认证配置：

```
test aaa-server authentication RADIUS username user1 password Skill39!
```

测试结果：

```
Server IP Address or name: 192.168.10.100
INFO: Attempting Authentication test to IP address (192.168.10.100) (timeout: 12 seconds)
INFO: Authentication Successful
```

这表明用户 user1 使用密码 Skill39! 成功通过RADIUS服务器认证。