防火墙SSL VPN短信认证原理

SSL VPN 胡伟 2021-06-30 发表

问题描述

防火墙SSL VPN短信认证原理

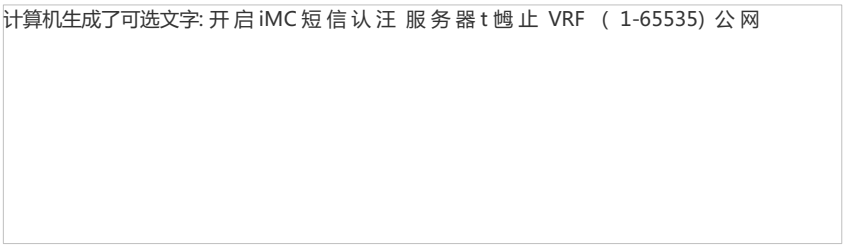
解决方法

三种方式：

1. radius认证，使用我司iMC做radius服务器，iMC和短信平台对接，支持的短信平台种类和厂商，与iMC的规格有关，请与业软确认。【最常见】

组网：PC —— SSLVPN ——radius服务器 —— 短信平台

SSL VPN访问实例context需要做如下配置：



2. radius认证，支持radius挑战模式进行二次认证，radius挑战为标准radius协议，第三方radius厂商如果支持即可进行短信认证，由radius对接短信平台，与radius服务器的支持情况有关。

组网：PC —— SSLVPN ——radius服务器 —— 短信平台

使用radius协议challenge实现，完整流程如下：

1. VPN ——> radius server Access-Request报文，提交密码，2号标准属性
2. Radius server ——> VPN Access-Challenge报文
3. VPN ——>radius server Access-Request报文，提交短信码，2号标准属性
4. Radius server ——> VPN Access-Accept报文，认证成功

3.FW直接对接短信网关，目前只支持亿美软通短信网关，不受限于AAA的认证方式，本地，radius，ldap均可。（D060SP分支支持）

组网：PC —— SSLVPN ——认证服务器

|

亿美软通短信网关

SMS简介

SMS（Short Message Service，短信服务）是一种发送短信服务，该服务通过SMS网关来实现。设备作为SMS网关时，首先与第三方短信平台对接，然后通过HTTP协议将短信数据发送给第三方短信平台，由第三方短信平台将短信发送至用户手机。

1.2 SMS配置限制和指导

目前仅支持对接亿美软通第三方短信平台。

1.3 SMS配置步骤

(1) 进入系统视图。

system-view

(2) 创建短信网关，并进入短信网关视图。

sms-gateway gateway-name

(3) 配置短信网关发送短信的平台。

sms-platform emay

缺省情况下，未配置短信网关发送短信的平台。

(4) 配置第三方短信平台的标识。

app-id app-id

缺省情况下，未配置第三方短信平台的标识。

(5) 配置用于加密短信数据的密钥。

secret-key { **cipher** | simple } string

缺省情况下，未配置用于加密短信数据的密钥。

(6) （可选）配置向测试手机号码发送短信。

sms-send test-mobile number

(7) （可选）配置短信网关关联的VPN实例。

vpn-instance vpn-instance-name

缺省情况下，短信网关属于公网。

1.8.8 配置短信网关认证功能

1. 配置准备

短信网关的具体配置，请参见“安全配置指导”中的“SMS”。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入SSL VPN访问实例视图。

sslvpn context *context-name*