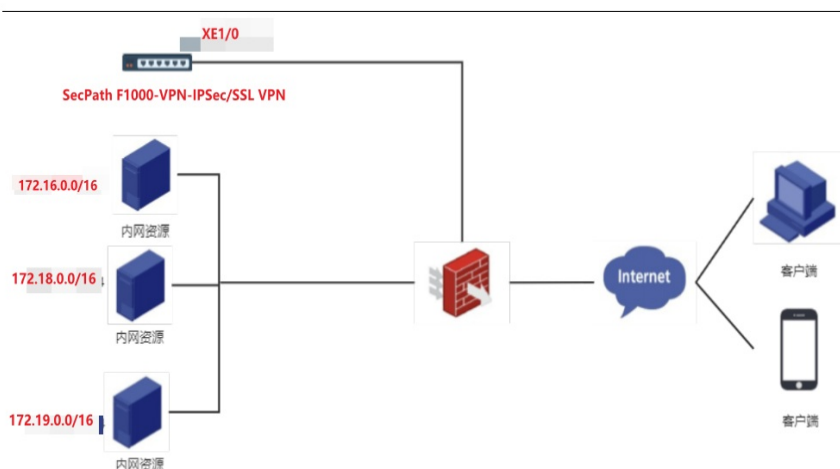


知 SecPath F1000-VPN-IPSec/SSL VPN拨号成功后访问资源失败

SSL VPN 曾招维 2024-06-29 发表

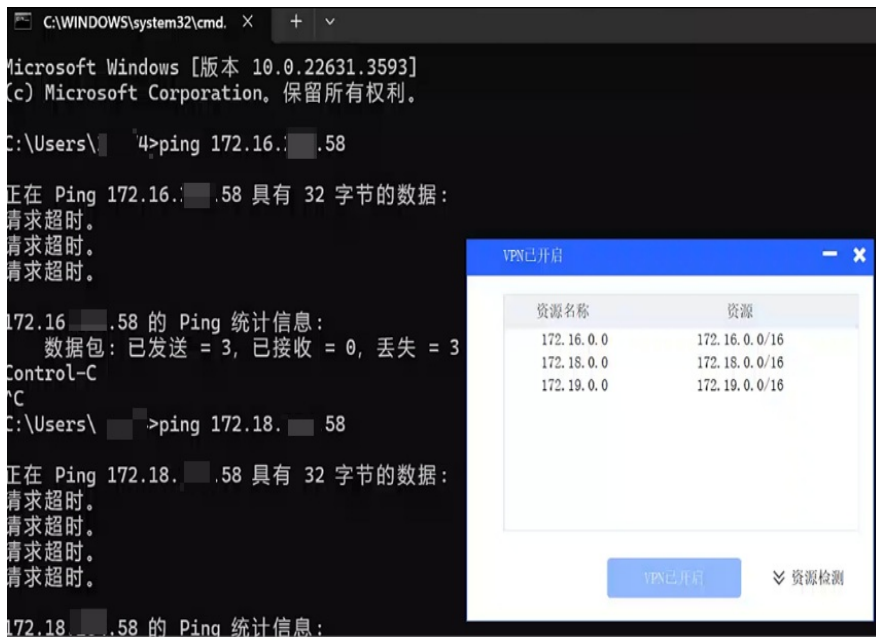
组网及说明

SecPath F1000-VPN-IPSec/SSL VPN旁挂组网部署



问题描述

存在于公用网络的pc或者安卓手机通过防火墙的SSL VPN功能访问被隔离于内网的网络资源，业务运行一段时间后，发现安装了SLINK客户端的Windows终端拨号成功，但是访问资源异常。



过程分析

1、检查vpn到资源通: 通信正常，说明内网侧路由正常、服务器可用。



2、SSLVPN 设置 > 资源管理，默认资源组中确认已方通相关资源：正常，资源已放行。



3、SSLVPN 设置 > 映射配置，确认旁挂口正常映射到tunnel口：正常。



4、防火墙策略检查：有放通所有的策略。

系统设置 > 系统配置 > 网络配置

默认策略: ACCEPT DROP

注: 当前的默认策略为 DROP, 运行白名单模式。

显示 10 项结果

序号	端口	策略	协议	源地址/CIDR	目标地址/CIDR	端口号/CMP类型	统计(pkts-bytes)	是否正常
1	any	ACCEPT	tcp	192.168.0.198	0.0.0.0/0	22	0-0	正常
2	lo	ACCEPT	all	0.0.0.0/0	0.0.0.0/0	*	14M-1158M	正常
3	any	ACCEPT	tcp	0.0.0.0/0	0.0.0.0/0	8181,8445,9080,9494,8000,9000,8443,18443,38443,18500,18800	866M-974G	正常
4	any	ACCEPT	udp	0.0.0.0/0	0.0.0.0/0	123,500,4500	2-112	正常
5	any	ACCEPT	esp	0.0.0.0/0	0.0.0.0/0	*	0-0	正常
6	any	ACCEPT	icmp	0.0.0.0/0	0.0.0.0/0	*	2333-469K	正常
7	any	ACCEPT	vrrp	0.0.0.0/0	0.0.0.0/0	*	0-0	正常
8	any	ACCEPT	tcp	127.0.0.1	0.0.0.0/0	8080	0-0	正常
9	any	ACCEPT	89	0.0.0.0/0	0.0.0.0/0	*	0-0	正常
10	any	ACCEPT	gre	0.0.0.0/0	0.0.0.0/0	*	0-0	正常

5. 虚卡配置检查, tun3的虚卡IP有做更改: **异常**, 虚卡ip网段和业务ip有冲突影响业务转发。

编辑 虚卡生效

虚卡名称	虚卡ip	子网掩码
tun0	10.0.0.1	255.255.255.0
tun1	11.0.0.1	255.255.255.0
tun2	12.0.0.1	255.255.255.0
tun3	172.16.X.X	255.255.255.0

显示 10 项结果 上页 1 下页

解决方法

修改回缺省配置后, 访问正常。

编辑 虚卡生效

虚卡名称	虚卡ip	子网掩码
tun0	10.0.0.1	255.255.255.0
tun1	11.0.0.1	255.255.255.0
tun2	12.0.0.1	255.255.255.0
tun3	13.0.0.1	255.255.255.0

显示 10 项结果 上页 1 下页