通过Tracert了解Secpath1800F状态防火墙包过滤机制

郭晓翔 2006-02-21 发表

通过Tracert了解Secpath1800F状态防火墙包过滤机制

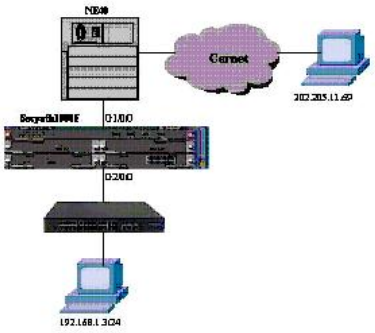
【问题描述】

某学校将我司Secpath1800F放置与内部核心交换机Passport8610与出口路由器NE40之间做透明模式防火墙。替换原有联想防火墙，承担高达700M并发流量的校园网出口负荷，一直稳定运行，并对我司防火墙的ASPF应用状态检测非常满意。近期该校网管反应网络中心网段（192.168.1.0/24）用户无法trace外网来排除故障，trace 在1800F及以后的逐跳全部不显示，但最后一跳可以正常显示目标可达。而且ping是可以正常通的：

比如内网地址192.168.1.3/24 *trust区域。 外网被trace地址：202.205.11.69/24 *untrust区域

1800F中的配置：interzone trust untrust 的outbound放开了整个192.168.1.0/24 IP网段。inbound只允许了外网可以访问部分服务器。

【组网拓扑】



【相关配置】

```
#
 sysname ScuSecpath1800F
#
acl number 3000
description Trust to Untrust,permit access free ip,permit access internet by cernet,permit access inter
net by TeleComm
rule 801 permit ip source 192.168.1.0  0.0.0.255
……..
#
acl number 3200
description UntrustToTrust_permitAccessPublicServer
……..
#
 firewall packet-filter default permit interzone local trust direction inbound
 firewall packet-filter default permit interzone local trust direction outbound
 firewall packet-filter default permit intleerzone DMZ untrust direction outbound
#
 firewall mode transparent
#
vlan 2
#
interface Vlanif2
 ip address 202.115.32.251 255.255.255.0
#
interface GigabitEthernet1/0/0
 port default vlan 2
#
interface GigabitEthernet2/0/0
 port default vlan 2
#
interface GigabitEthernet4/0/0
 port default vlan 2
#
firewall zone local
```

```
 set priority 100
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet1/0/0
#
firewall zone untrust
 set priority 5
 add interface GigabitEthernet2/0/0
#
firewall interzone local trust
#
firewall interzone local untrust
#
firewall interzone local DMZ
#
firewall interzone trust untrust
  packet-filter 3200 inbound
packet-filter 3000 outbound
detect ftp
 detect h323
 detect sip
 detect pptp
 detect hwcc
 detect http
 detect netbios
 detect rtsp
 detect qq
 detect msn
#
firewall interzone trust DMZ
packet-filter 3400 outbound
#
firewall interzone DMZ untrust
 packet-filter 3300 inbound
#
ip route-static 202.115.36.0 255.255.255.0 202.115.32.254
#
```

【解决方案】

在interzone trust untrust的inbound ACL 3200中加一条rule 5 permit icmp icmp-type ttl-exceeded 后问题解决。