EzVPN登陆失败

目录

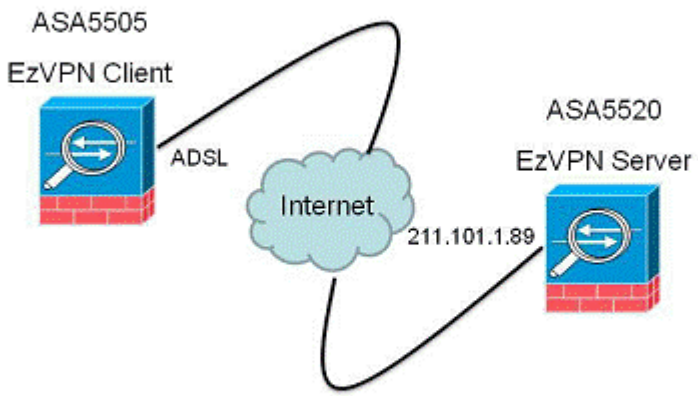
故障描述

客户有三个分支点EzVPN 工作一直正常, 最近客户增加了新的分公司.虽然EzVPN客户端的配置和其它分公司一样,但是VPN总是登陆不成功。

网络拓扑

ASA5505 OS version :8.3(1)

ASA5520 OS version :7.0(7)



网络设备配置

1. ASA5505配置

```
ASA Version 8.3(1)
!
```

```
hostname asa5505
domain-name cisco.com
enable password
```

2. ASA5520 配置

```
ASA Version 7.0(7)
!
interface Ethernet0/0
nameif outside
security-level 0
ip address 211.101.1.89 255.255.255.0
!
interface Ethernet0/1
nameif inside
security-level 100
ip address 192.168.5.1 255.255.255.0
!
access-list ADSL extended permit ip 192.168.5.0 255.255.255.0
192.168.101.0 255.255.255.0
group-policy tunnel internal
group-policy tunnel attributes
split-tunnel-policy tunnelspecified
split-tunnel-network-list value ADSL
nem enable
username cisco password xWh.sOL10ki7Ia5G encrypted
!
crypto ipsec transform-set myset esp-3des esp-sha-hmac
crypto dynamic-map ezvpn 30 set transform-set myset
crypto map outside_map 65535 ipsec-isakmp dynamic ezvpn
crypto map outside_map interface outside
isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
tunnel-group mytunnel type ipsec-ra
tunnel-group mytunnel general-attributes
default-group-policy tunnel
tunnel-group mytunnel ipsec-attributes
pre-shared-key *
-Omitted-
```

故障排除

1. EzVPN client 失败登陆的输出

```
ciscoasa# show vpnclient

LOCAL CONFIGURATION
vpnclient server 211.101.1.89
vpnclient mode network-extension-mode
vpnclient nem-st-autoconnect
vpnclient vpngroup mytunnel password *****
vpnclient username cisco password *****
vpnclient enable

MISCELLANEOUS INFORMATION
- Key exchange is based on Pre-Shared Key
- Connection attempt will be automatically initiated
```

2. 收集EzVPN server 段系统日志

通常我们一旦确认配置无误后,首先要从EzVPN server 端的系统日志入手.

将日志级别调成informational 级别:

```
Logging on
Logging buffered informational
```

从Syslog message 输出我们可以得到如下信息

```
%ASA-6-113013: AAA unable to complete the request Error : reason = Simultaneous
logins exceeded for user : user = Cisco
```

该日志信息表明用户名为 "cisco" 的VPN并发连接数超过了最大限制.

此时我们基本可以找到问题根源是同一vpn 用户的并发登陆数量被限制了.

通过 " show vpn-sessiondb remote | include cisco" 我们可以看到有3个用户 "cisco"成功登陆.

```
ciscoasa(config)# show vpn-sessiondb remote | include cisco
Username : cisco
Username : cisco
Username : cisco
```

此时我们就已经得到了问题的答案,在ASA IPSEC Remote VPN 中同一用户允许同时登陆的默认数量为3个, 所以我们将这个默认数值更改就可以解决此问题

3. 解决问题

我们将此默认并发值设为4个,修改命令如下:

```
group-policy tunnel internal
group-policy tunnel attributes
vpn-simultaneous-logins 4
```

此时再次验证EzVPN client 登陆情况:

```
ciscoasa# show vpnclient

LOCAL CONFIGURATION
vpnclient server 10.75.61.179
vpnclient mode network-extension-mode
vpnclient nem-st-autoconnect
vpnclient vpngroup mytunnel password *****
vpnclient username cisco password *****
vpnclient enable

DOWNLOADED DYNAMIC POLICY
Current Server : 211.101.1.89
PFS Enabled : No
Secure Unit Authentication Enabled : No
User Authentication Enabled : No
Split Tunnel Networks : 192.168.5.0/255.255.255.0
Backup Servers : None
```

此时我们发现EzVPN登陆成功.