防火墙国密ipsec隧道建立失败

IPSec VPN　彭钦　2024-02-20 发表

组网及说明

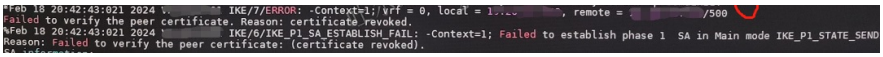
不涉及

告警信息

不涉及

问题描述

国密ipsec隧道建立失败，display ike sa显示为unkown状态，debug显示Failed to vertify the peer certificate.Reason:certificate revoked.



过程分析

现场配置带有revocation-check method crl none，会先进行CRL检查，然后发现对端证书被吊销了导致建立失败。undo crl check enable------关闭crl检查，就可以正常建立了。

pki domain vpndomain11
certificate request entity vpncer11
public-key sm2 signature name xxxx encryption name yyyyy
pkcs7-encryption-algorithm sm4-cbc
crl url ldap://xxxxxxxxx
revocation-check method crl none
crl update-period 719

revocation-check method命令用来指定证书吊销情况检查的方法。
undo revocation-check method命令用来恢复缺省情况。

【命令】

revocation-check method *method1* [*method2*]
undo revocation-check method

【缺省情况】

使用CRL方法检查证书吊销情况。

【视图】

PKI域视图

【缺省用户角色】

network-admin
context-admin

【参数】

method1 [*method2*]：指定证书吊销情况检查的方法。*method*取值为：

- **crl**：指定证书吊销时进行CRL检查。
- **none**：忽略证书吊销检查。

如果*method1*指定为**none**，则*method2*不能再指定**crl**。

【使用指导】

指定了**crl**方法，必须保证CRL检查功能处于开启状态（通过**crl check enable**命令配置）。如果CRL检查功能处于关闭状态，则不进行CRL检查，认为所有证书可信。
指定了**none**方法，则忽略检查认为所有证书可信，**crl check enable**命令不生效。
如果同时指定了**crl**和**none**方法，则先进行CRL检查，检查证书是否可信；如果从CRL发布点所在的服务器上获取不到CRL，则使用**none**方式，忽略检查认为所有证书可信。

【举例】

#配置使用CRL方式检查证书吊销情况。

```
<Sysname> system
[Sysname] pki domain abc
[Sysname-pki-domain-abc] revocation-check method crl
```

解决方法

undo crl check enable------关闭crl检查