【MVS】华为防火墙如何查看IPSEC IKE交互失败的信息?

VPN技术 **胡伟** 2024-06-24 发表

问题描述

【MVS】华为防火墙如何查看IPSEC IKE交互失败的信息?

解决方法

不同于其他厂商防火墙，华为防火墙可以使用下面的命令对IPSEC IKE交互过程的错误进行打印显示。

> **display ike error-info**命令用来查看IKE协商IPSec隧道失败的信息。

命令格式

display ike error-info [**verbose**] [**peer** *remote-address*] [**slot** *slot-id* **cpu** *cpu-id*]

参数说明

参数	参数说明	取值
verbose	显示IKE协商IPSec隧道失败的详细信息。	-
peer *remote-address*	显示指定对端地址的IKE协商IPSec隧道失败的信息。	IPv4地址：点分十进制格式；IPv6地址：冒号十六进制格式。
slot *slot-id* **cpu** *cpu-id*	显示指定槽位号和CPU号的IKE协商IPSec隧道失败的信息。	*slot-id*和*cpu-id*均为整数形式，根据设备实际配置情况选取。

查看IKE协商IPSec隧道失败的详细信息。

```
<sysname> display ike error-info verbose


  current info Num :1
  Ike error information:
  current ike Error-info number :1
  ------------------------------------------------------------------------

  Peer       : 10.1.1.1
  Port       : 500
  version    : v1
  Reason     : phase1 proposal mismatch
  Detail     : phase1 proposal mismatch
  Error-time : 2013-08-26 12:02:37
  ------------------------------------------------------------------------
```

表1 display ike error-info命令输出信息描述

项目	描述
current info Num	目前信息数目。
Ike error information	IKE协商IPSec隧道失败的信息。
current ike Error-info number	目前IKE协商IPSec隧道失败的信息数目。
peer或Peer	对端IP地址。
port或Port	对端UDP端口号。

项目	描述
error-reason或Reason	IKE协商IPSec隧道失败的常见原因，包括： • phase1 proposal mismatch：两端IKE安全提议参数不匹配。 • phase2 proposal or pfs mismatch：两端IPSec安全提议参数、PFS算法或Security ACL不匹配。 • responder dh mismatch：响应方的DH算法不匹配。 • initiator dh mismatch：发起方的DH算法不匹配。 • encapsulation mode mismatch：封装模式不匹配。 • flow or peer mismatch：两端Security ACL或IKE Peer地址不匹配。 • version mismatch：两端IKE版本号不匹配。 • peer address mismatch：两端的IKE Peer地址不匹配。 • config ID mismatch：根据ID未找到匹配的IKE Peer。 • exchange mode mismatch：两端的协商模式不匹配。 • authentication fail：身份认证失败。 • construct local ID fail：构造本端ID失败。 • rekey no find old sa：重协商时找不到旧的SA。 • rekey fail：重协商时旧的SA正在下线。 • first packet limited：首包限速。 • unsupported version：不支持的IKE版本号。 • malformed message：畸形消息。 • malformed payload：畸形载荷。 • critical drop：未识别的critical载荷。 • COOKIE mismatch：COOKIE不匹配。 • invalid COOKIE：无效COOKIE。 • invalid length：报文长度非法。 • unknown exchange type：未知的协商模式。 • uncritical drop：未识别的非critical载荷。 • route limit：路由注入的数目达到规格。 • ip assigned fail：IP地址分配失败。 • eap authentication timeout：EAP认证超时。 • eap authentication fail：EAP认证失败。 • xauth authentication fail：XAUTH认证失败。 • xauth authentication timeout：XAUTH认证超时。 • license or specification limited：License限制。 • local address mismatch：IKE协商时的本端IP地址和接口IP地址不匹配。 • dynamic peers number reaches limitation：IKE对等体数达到规格。 • ipsec tunnel number reaches limitation：IPSec隧道数达到规格。 • netmask mismatch：开启IPSec掩码过滤功能后，掩码不匹配。 • flow confict：数据流冲突。 • proposal mismatch or use sm in ikev2：IPSec安全提议不匹配或者IKEv2使用SM算法。 • ikev2 not support sm in ipsec proposal ikev2：IKEv2不支持IPSec安全提议的SM算法。 • no policy applied on interface：没有策略应用到接口上。 • nat detection fail：NAT探测失败。 • fragment packet limit：分片报文超规格。 • fragment packet reassemble timeout：分片报文重组超时。
version	IKE版本。
Error-time/error-time	IKE协商IPSec隧道失败的时间。
Detail	IKE协商IPSec隧道失败的详细信息。 • phase1 proposal mismatch：两端IKE安全提议参数不匹配。 • phase2 proposal or pfs mismatch：两端IPSec安全提议参数、PFS算法或Security ACL不匹配。 • responder dh mismatch：响应方的DH算法不匹配。 • initiator dh mismatch：发起方的DH算法不匹配。 • encapsulation mode mismatch：封装模式不匹配。 • flow or peer mismatch：两端Security ACL或IKE Peer地址不匹配。 • version mismatch：两端IKE版本号不匹配。 • peer address mismatch：两端的IKE Peer地址不匹配。 • config ID mismatch：根据ID未找到匹配的IKE Peer。 • exchange mode mismatch：两端的协商模式不匹配。 • authentication fail：身份认证失败。 • construct local ID fail：构造本端ID失败。 • rekey no find old sa：重协商时找不到旧的SA。 • rekey fail：重协商时旧的SA正在下线。 • first packet limited：首包限速。 • unsupported version：不支持的IKE版本号。 • malformed message：畸形消息。 • malformed payload：畸形载荷。 • critical drop：未识别的critical载荷。 • COOKIE mismatch：COOKIE不匹配。 • invalid COOKIE：无效COOKIE。 • invalid length：报文长度非法。 • unknown exchange type：未知的协商模式。 • uncritical drop：未识别的非critical载荷。 • route limit：路由注入的数目达到规格。 • ip assigned fail：IP地址分配失败。 • eap authentication timeout：EAP认证超时。 • eap authentication fail：EAP认证失败。 • xauth authentication fail：XAUTH认证失败。 • xauth authentication timeout：XAUTH认证超时。 • license or specification limited：License限制。 • local address mismatch：IKE协商时的本端IP地址和接口IP地址不匹配。 • dynamic peers number reaches limitation：IKE对等体数达到规格。 • ipsec tunnel number reaches limitation：IPSec隧道数达到规格。 • netmask mismatch：开启IPSec掩码过滤功能后，掩码不匹配。

项目	描述
	• flow conflict：数据流冲突。 • proposal mismatch or use sm in ikev2：IPSec安全提议不匹配或者IKEv2使用SM算法。 • ikev2 not support sm in ipsec proposal ikev2：IKEv2不支持IPSec安全提议的SM算法。 • no policy applied on interface：没有策略应用到接口上。 • nat detection fail：NAT探测失败。 • fragment packet limit：分片报文超规格。 • fragment packet reassemble timeout：分片报文重组超时。 • receive phase1 proposal mismatch：收到的IKE安全提议参数不匹配。 • receive phase2 proposal mismatch：收到的IPSec安全提议参数不匹配。 • phase2 proposal mismatch：两端IPSec安全提议参数不匹配。 • receive flow or peer mismatch：收到的Security ACL或IKE Peer地址不匹配。 • (peer local or tunnel local or interface) address mismatch：对端的本端IP地址、隧道本端IP地址或接口IP地址不匹配。 • remote auth method mismatch：对端认证方法不匹配。 • proc cert fail or inband cert validate fail：处理证书或证书校验失败。 • outband cert validate fail(rsa-signature)：RSA签名认证时证书校验失败。 • hash value not equal(pre-share-key)：预共享密钥认证时Hash值不相等。 • hash value not equal(digital-envelope)：数字签名认证时Hash值不相等。 • verify sig data fail(rsa-signature)：签名校验失败。 • proc auth payload fail(pre-share-key)：预共享密钥认证时处理认证载荷失败。 • proc auth payload fail(rsa-signature)：RSA签名认证时处理认证载荷失败。 • proc auth payload fail(eap)：IKEv2 EAP认证时处理认证载荷失败。 • recv peer auth fail notification：收到对端认证失败通知消息。 • recv peer auth fail notification(pre-share-key)：预共享密钥认证时收到对端认证失败通知消息。 • recv peer auth fail notification(rsa-signature)：RSA签名认证时收到对端认证失败通知消息。 • recv peer auth fail notification(digital-envelope)：数字签名认证时收到对端认证失败通知消息。 • recv peer auth fail notification(eap)：IKEv2 EAP认证时收到对端认证失败通知消息。 • proc and auth ID payload fail(pre-share-key)：预共享密钥认证时对端ID认证失败。 • proc and auth ID payload fail(rsa-signature)：RSA签名认证时对端ID认证失败。 • proc and auth ID payload fail(eap)：IKEv2 EAP认证时对端ID认证失败。 • can not find key by cert：获取证书对应的密钥对失败。 • the cert is not valid：证书无效。 • cert revoked by CRL：证书被CRL吊销。 • unable to get issuer cert：找不到颁发者。 • ocsp valid fail：证书在线检验失败。 • cert filter check mismatch：证书过滤校验不匹配。 • no corresponding CRL：没有对应的CRL。 • inband cert validate fail：证书验证失败。 • cert PKI whitelist valid fail：PKI证书白名单校验失败。 • receive proposal mismatch or use sm in ikev2：收到的IPSec安全提议不匹配或者IKEv2使用SM算法。