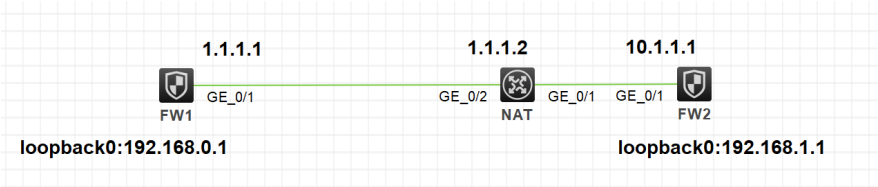
ikev2协商方式建立ipsec协商失败

IPSec VPN IKE 王树岭 2022-02-23 发表

组网及说明

如图



问题描述

某局点用我司F1000系列防火墙和第三方设备对接ikev2建立ipsec隧道，对端涉及NAT穿越
用loopback0口代替内网用户；相关配置略

FW1主动带源ping触发，发现本端没有ikev2 sa，对端有ikev2 sa；
debug ikev2 all后报错为：
*Feb 23 14:55:26:019 2022 H3C IKEV2/7/ERROR: -COntext=1; vrf = 0, src = 1.1.1.1, dst = 1.1.1.2/500 Check match item failed for Peer's identity in profile 1, peer's policy verify failed.
*Feb 23 14:55:26:019 2022 H3C IKEV2/7/ERROR: -COntext=1; vrf = 0, src = 1.1.1.1, dst = 1.1.1.2/500 Authentication failed.
*Feb 23 14:55:26:019 2022 H3C IKEV2/7/PACKET: -COntext=1; vrf = 0, src = 1.1.1.1, dst = 1.1.1.2/500 Processed response with message id 1, requests can be sent from (2 ~ 2).
*Feb 23 14:55:26:020 2022 H3C IKEV2/7/FSM: -COntext=1; vrf = 0, src = 1.1.1.1, dst = 1.1.1.2/500 Child SA(Msg ID 1) deleted.
*Feb 23 14:55:26:020 2022 H3C IKEV2/7/FSM: -COntext=1; vrf = 0, src = 1.1.1.1, dst = 1.1.1.2/500 (Tunnel ID 7): IKE SA deleted.

过程分析

根据对端提供的配置，本端配置相同的协商参数
根据debug报错，是对端的身份标识有问题。
查看配置手册的说明
(3)　配置本端身份信息。
identity local { address { ipv4-address | ipv6 ipv6-address } | dn | email email-string | fqdn fqdn-name | key-id key-id-string }
缺省情况下，未配置本端身份信息。此时使用IP地址标识本端的身份，该IP地址为IPsec安全策略应用的接口的IP地址。

本端FW1中关于对端的身份标识配置成了NAT后的公网地址，导致收到对端的交互报文时身份识别出现错误，匹配不了ikev2 profile

解决方法

将FW1中关于对端的身份信息相关的配置修改成对端的ipsec接口地址，或者是手动配置的identity address地址，本例中为10.1.1.1

ikev2 keychain中peer的identity配置和ikev2 profile中match remote的identity配置修改后，隧道能正常建立