ASA IPsec和IKE调试（IKEv1主动模式）故障排除技术说明

目录

简介

本文档介绍在同时使用主动模式和预共享密钥(PSK)时在思科自适应安全设备(ASA)上进行的调试。还将讨论将某些调试行转换为配置。思科建议您对IPsec和互联网密钥交换(IKE)有基本的了解。

本文档不讨论隧道建立后传递的流量。

核心问题

IKE和IPsec调试有时很晦涩，但您可以使用它们来了解IPsec VPN隧道建立问题。

场景

主动模式通常用于软件（Cisco VPN客户端）和硬件客户端（Cisco ASA 5505自适应安全设备或Cisco IOS）的Easy VPN(EzVPN)?软件路由器)，但仅当使用预共享密钥时。与主模式不同，主动模式包含三条消息。

调试来自运行软件版本8.3.2并充当EzVPN服务器的ASA。EzVPN客户端是软件客户端。

debug命令

以下是本文档中使用的debug命令：

```
debug crypto isakmp 127
debug crypto ipsec 127
```

ASA 配置

本例中的ASA配置应严格为基本配置；不使用外部服务器。

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.48.67.14 255.255.254.0

crypto ipsec transform-set TRA esp-aes esp-sha-hmac

crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000

crypto dynamic-map DYN 10 set transform-set TRA
crypto dynamic-map DYN 10 set reverse-route

crypto map MAP 65000 ipsec-isakmp dynamic DYN
crypto map MAP interface outside
crypto isakmp enable outside

crypto isakmp policy 10
 authentication pre-share
 encryption aes
 hash sha
 group 2
lifetime 86400

username cisco password  cisco
username cisco attributes
vpn-framed-ip-address 192.168.1.100 255.255.255.0

tunnel-group EZ type remote-access
tunnel-group EZ general-attributes
 default-group-policy EZ
tunnel-group EZ ipsec-attributes
 pre-shared-key *****

group-policy EZ internal
group-policy EZ attributes
 password-storage enable
 dns-server value 192.168.1.99
 vpn-tunnel-protocol ikev1
 split-tunnel-policy tunnelall
 split-tunnel-network-list value split
 default-domain value jyoungta-labdomain.cisco.com
```

调试

注意：使用 **debug 命令之前，请参阅**有关 Debug 命令的重要信息。

服务器消息说明

从客户端接收AM1。

处理AM1。将收到的提议和转换与已配置用于匹配的提议和转换进行比较。
相关配置：
接口上启用了ISAKMP，并且至少定义了一个与客户端发送的内容匹配的策略：

```
crypto isakmp enable
outside
crypto isakmp policy
10
authentication pre-
share
encryption aes
hash sha
group 2
lifetime 86400
```

与身份名称匹配的隧道组存在：

```
tunnel-group EZ type
remote-access
tunnel-group EZ
general-attributes
default-group-policy
EZ
tunnel-group EZ ipsec-
attributes
pre-shared-key cisco
```

构建AM2。此过程包括：
— 选择的策略
- Diffie-Hellman(DH)
— 响应方ID
-auth
— 网络地址转换(NAT)检测负载

发送AM2。

从客户端接收AM3。

进程AM 3.确认NAT穿越(NAT-T)的使用。现在，两端都已准备好开始流量加密。

启动第1.5阶段(XAUTH)并请求用户凭证。

接收用户凭证。

处理用户凭证。验证凭证并生成模式配置负载。
相关配置：

```
username cisco
password cisco
```

发送xuath结果。

接收并处理ACK;服务器没有响应。

接收mode-config请求。

进程模式配置请求。
其中许多值通常在组策略中配置。但是，由于本示例中的服务器具有非常基本的配置，因此您在此处看不到

使用所有已配置的值构造模式配置响应。
相关配置：
请注意，在这种情况下，始终为用户分配相同的IP。

```
username cisco
attributes
vpn-framed-ip-
address 192.168.1.100
255.255.255.0
group-policy EZ
internal
group-policy EZ
attributes
password-storage
enabledns-server value
192.168.1.129
vpn-tunnel-protocol
ikev1
split-tunnel-policy
tunnelall
split-tunnel-network-
list value split default-
domain value
jyoungta-
labdomain.cisco.com
```

发送模式配置响应。

第1阶段在服务器上完成。启动快速模式(QM)流程。

为客户端构造并发送DPD。

接收QM1。

进程QM1。

相关配置：

```
crypto dynamic-map
DYN 10 set transform-
set TRA
```

构建QM2。

相关配置：

```
tunnel-group EZ
type remote-access !
(tunnel type ra = tunnel
type remote-access)
crypto ipsec transform-
set TRA esp-aes esp-
sha-hmac
crypto ipsec security-
association lifetime
seconds 28800
crypto ipsec security-
association lifetime
kilobytes 4608000
crypto dynamic-map
```

```
DYN 10 set transform-
set TRA
crypto map MAP 65000
ipsec-isakmp dynamic
DYN
crypto map MAP
interface outside
```

发送QM2。

接收QM3。

处理QM3。创建入站和出站安全参数索引(SPI)。 为主机添加静态路由。

相关配置：

```
crypto ipsec transform-
set TRA esp-aes esp-
sha-hmac
crypto ipsec security-
association lifetime
seconds 28800
crypto ipsec security-
association lifetime
kilobytes 4608000
crypto dynamic-map
DYN 10 set transform-
set TRA
crypto dynamic-map
DYN 10 set reverse-
route
```

第2阶段完成。双方现在都在加密和解密。

对于硬件客户端，在客户端发送有关自身信息的位置接收另一条消息。如果仔细查看，您应该找到EzVPN

隧道验证

ISAKMP

sh cry isa sa det**命令的输**出为：

```
 Active SA: 1
 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1 IKE Peer: 10.48.66.23
 Type : user Role : responder
 Rekey : no State : AM_ACTIVE
 Encrypt : aes Hash : SHA
 Auth : preshared Lifetime: 86400
 Lifetime Remaining: 86387
 AM_ACTIVE - aggressive mode is active.
```

IPsec

由于Internet控制消息协议(ICMP)用于触发隧道，因此只有一个IPsec SA处于启用状态。协议1是ICMP。请注意，SPI值与调试中协商的值不同。实际上，这是第2阶段重新生成密钥后的同一隧道。

sh crypto ipsec sa命令的输出为：

```
interface: outside
 Crypto map tag: DYN, seq num: 10, local addr: 10.48.67.14

 local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
 remote ident (addr/mask/prot/port): (192.168.1.100/255.255.255.255/0/0)
 current_peer: 10.48.66.23, username: cisco
 dynamic allocated peer ip: 192.168.1.100

 #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
 #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
 #pkts compressed: 0, #pkts decompressed: 0
 #pkts not compressed: 5, #pkts comp failed: 0, #pkts decomp failed: 0
 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
 #send errors: 0, #recv errors: 0

 local crypto endpt.: 10.48.67.14/0, remote crypto endpt.: 10.48.66.23/0
 path mtu 1500, ipsec overhead 74, media mtu 1500
 current outbound spi: C4B9A77C
 current inbound spi : EA2B6B15

 inbound esp sas:
 spi: 0xEA2B6B15 (3928714005)
 transform: esp-aes esp-sha-hmac no compression
 in use settings ={RA, Tunnel, }
 slot: 0, conn_id: 425984, crypto-map: DYN
 sa timing: remaining key lifetime (sec): 28714
 IV size: 16 bytes
 replay detection support: Y
 Anti replay bitmap:
 0x00000000 0x0000003F
 outbound esp sas:
 spi: 0xC4B9A77C (3300501372)
 transform: esp-aes esp-sha-hmac no compression
 in use settings ={RA, Tunnel, }
 slot: 0, conn_id: 425984, crypto-map: DYN
 sa timing: remaining key lifetime (sec): 28714
 IV size: 16 bytes
 replay detection support: Y
 Anti replay bitmap:
 0x00000000 0x00000001
```

相关信息

- 关于IPsec的维基百科文章
- IPSec故障排除：了解和使用debug命令
- 技术支持和文档 - Cisco Systems