积极模式)排除故障技术说明的ASA IPsec和IKE调试(IKEv1

目录

简介

本文描述在思科可适应安全工具(ASA)的调试，当使用积极模式和预先共享密钥(PSK)时。某些调试线路的转换到配置里也讨论。思科推荐您有IPsec和Internet Key Exchange (IKE)基础知识。

在通道设立了后，本文不讨论通过流量。

核心问题

IKE和IPsec调试有时隐秘，但是您能使用他们为了了解与IPSec VPN隧道建立的问题。

方案

积极模式在Easy VPN (ezvpn)的情况下典型地使用与软件(Cisco VPN Client)和硬件客户端(思科ASA 5505可适应安全工具或Cisco IOS ? 软件路由器)，但是，只有当使用预先共享密钥。不同于主模式，积极模式包括三个消息。

调试是从运行软件版本8.3.2并且作为EzVPN服务器的ASA。EzVPN客户端是软件客户端。

使用的调试指令

这些是用于本文的调试指令：

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

ASA 配置

在本例中的ASA配置被认为严格基本;没有使用外部服务器。

```
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

从客户端的接收AM1。

处理AM1。compare接收建议和转换与为匹配已经配置的那些。

相关配置：

ISAKMP在接口启用，并且匹配至少的一项策略定义什么客户端发送：

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

匹配标识名称存在的隧道群：

```
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。此进程包括：
-选择的策略
- Diffie-Hellman (DH)
-响应方ID
-验证
-网络地址转换(NAT)检测有效负载

发送AM2。

从客户端的接收AM3。

进程AM 3.确认NAT横越(NAT-T)使用。两边当前准备开始数据流加密。

启动相位1.5 (XAUTH)，并且请求用户凭证。

接收用户凭证。

进程用户凭证。验证凭证，并且生成模式配置有效负载。
相关配置：

```
username cisco
password cisco
```

发送xuath结果。

接收和进程ACK;从服务器的无响应。

接收模式设置请求。

处理模式设置请求。
许多这些值在组政策通常配置。然而，因为在本例中的服务器有一个非常基本配置，您看不到他们此处。

修建与配置的所有值的模式设置答复。
相关配置：
注释在这种情况下，用户总是分配同样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
```

发送模式设置答复。

阶段1在服务器完成。启动快速模式进程。

客户端的构建和发送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。

进程QM3。创建入站和出站安全参数索引(斯皮)。添加主机的静态路由。

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
```

完整的第2阶段。两边是当前加密和解密。

对于硬件客户端，一个消息还接收客户端发送关于本身的地方信息。如果仔细查找，您应该查找在客户端

通道验证

ISAKMP

从**嘘啼声sa isa det**命令的输出是：

```
 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

因为互联网控制消息协议(ICMP)用于触发通道，只有一IPsec SA是UP。协议1是ICMP。注意SPI值与在调试协商的那个有所不同。在第2阶段重新生成密钥后，这是，实际上，同一个通道。

从**嘘crypto sa ipsec**命令输出是：

```
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

- 在IPsec的维基百科条款
- IPSec故障排除：了解和使用调试指令
- 技术支持和文档 - Cisco Systems