IPsec ASA и отладки IKE (основной режим IKEv1) технические примечания по поиску и устранению проблем

Содержание

[Введение](#)
[Предварительные условия](#)
[Требования](#)
[Используемые компоненты](#)
[Базовая проблема](#)
[Сценарий](#)
[Используемые команды отладки](#)
[Конфигурация ASA](#)
[Отладка](#)
[Дополнительные сведения](#)

Введение

Когда и основной режим и предварительный общий ключ (PSK) используются, этот документ описывает отладки на Устройстве адаптивной защиты (ASA). Также обсуждается превращение определенных отладочных команд в конфигурацию.

Темы, не обсужденные в этом документе, включают проходящий трафик после того, как туннель был установлен и базовые понятия IPsec или Протокола IKE.

Предварительные условия

Требования

Читатели данного документа должны обладать знаниями по следующим темам.

- PSK
- IKE

Используемые компоненты

Сведения в документе приведены на основе данных версий аппаратного и программного обеспечения:

- Cisco ASA 9.3.2
- Маршрутизаторы , которые выполняют Cisco IOS® 12.4T

Базовая проблема

IKE и отладки IPSec являются иногда загадочными, но можно использовать их для понимания, где расположена проблема установления VPN-туннеля IPSec.

Сценарий

Когда сертификаты используются для аутентификации, основной режим, как правило, используется между туннелями между локальными сетями (LAN-to-LAN) или, в случае удаленного доступа (EzVPN).

Отладки от двух ASA, которые работают под управлением ПО версии 9.3.2. Эти два устройства сформируют туннель между локальными сетями (LAN-to-LAN).

Описаны два главных сценария:

- ASA как инициатор для IKE
- ASA как респондент для IKE

Используемые команды отладки

debug crypto ikev1 127

debug crypto ipsec 127

Конфигурация ASA

--- Конфигурация IPSec:

```
crypto ipsec transform-set TRANSFORM esp-aes esp-sha-hmac



crypto map MAP 10 match address VPN
crypto map MAP 10 set peer 10.0.0.2
crypto map MAP 10 set transform-set TRANSFORM
crypto map MAP 10 set reverse-route
crypto map MAP interface outside
crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
tunnel-group 10.0.0.2 type ipsec-l2l
tunnel-group 10.0.0.2 ipsec-attributes
 pre-shared-key cisco
access-list VPN extended permit tcp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
access-list VPN extended permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
```

IP - конфигурация:

```
ciscoasa# show ip
```

```
System IP Addresses:
Interface          Name   IP address    Subnet mask     Method
GigabitEthernet0/0      inside   192.168.1.1     255.255.255.0  manual
GigabitEthernet0/1      outside  10.0.0.1       255.255.255.0  manual
Current IP Addresses:
Interface          Name    IP address    Subnet mask     Method
GigabitEthernet0/0      inside     192.168.1.1     255.255.255.0  manual
GigabitEthernet0/1    outside  10.0.0.1     255.255.255.0  manual
```

Конфигурация статического преобразования сетевых адресов (NAT):

```
object network INSIDE-RANGE
 subnet 192.168.1.0 255.255.255.0 object network FOREIGN_NETWORK
 subnet 192.168.2.0 255.255.255
nat (inside,outside) source static INSIDE-RANGE INSIDE-RANGE destination static
FOREIGN_NETWORK FOREIGN_NETWORK no-proxy-arp route-lookup
```

Отладка

; ,
MM_NO_STATE.
, ASA .

MM1
IKE NAT-T.

MM1.

[IKEv1 DEBUG]: : , spi 0x0
IPSEC (crypto_map_check)-3: , 5 : Prot=1, saddr=192.168.1.2,
sport=2816, daddr=192.168.2.1, dport=2816
IPSEC (crypto_map_check)-3: MAP 10: .
[IKEv1]: IP = 10.0.0.2, IKE: 1, Intf , IKE 10.0.0.2 - 192.168.1.0, -
192.168.2.0, (MAP)
[IKEv1 DEBUG]: IP = 10.0.0.2, **ISAKMP SA** [IKEv1 DEBUG]: IP =
10.0.0.2, VID NAT 02
[IKEv1 DEBUG]: IP = 10.0.0.2, VID NAT 03
[IKEv1 DEBUG]: IP = 10.0.0.2, RFC VID NAT
[IKEv1 DEBUG]: IP = 10.0.0.2, VID +
[IKEv1]: IP = 10.0.0.2, (msgid=0) IKE_DECODE : HDR + SA (1) +
(13) + (13) + (13) + (13) + NONE (0) : 168

========== MM1
==========>

[IKEv1]: IP = 10.0.0.2, IKE_DECODE (msgid=0) : HDR + SA (1) + (13)
+VENDOR (13) + (13) + (13) + NONE (0) : 164

MM1 .

[IKEv1 DEBUG]: IP = 10.0.0.2, SA
[IKEv1 DEBUG]: IP = 10.0.0.2, Oakley
[IKEv1 DEBUG]: IP = 10.0.0.2, VID
[IKEv1 DEBUG]: IP = 10.0.0.2, VID RFC Received NAT-Traversal
[IKEv1 DEBUG]: IP = 10.0.0.2, VID
[IKEv1 DEBUG]: IP = 10.0.0.2, VID
[IKEv1 DEBUG]: IP = 10.0.0.2, NAT 03 VID
[IKEv1 DEBUG]: IP = 10.0.0.2, VID
[IKEv1 DEBUG]: IP = 10.0.0.2, NAT 02 VID
[IKEv1 DEBUG]: IP = 10.0.0.2, IKE SA
[IKEv1 DEBUG]: IP = 10.0.0.2, # 1 IKE SA, # 1 # 2 IKE

MM1.
ISAKMP/IKE .
, NAT-T.
:
crypto isakmp policy 10
authentication pre-share
3des
sha
group 2
86400

[IKEv1 DEBUG]: IP = 10.0.0.2, ISAKMP SA
[IKEv1 DEBUG]: IP = 10.0.0.2, VID NAT 02
[IKEv1 DEBUG]: IP = 10.0.0.2, VID +
[IKEv1]: IP = 10.0.0.2, (msgid=0) IKE_DECODE : HDR + SA (1) +
(13) + (13) + NONE (0) : 128

MM2.
ISAKMP .
NAT-T, .
MM2.

<========== MM2
==========

MM2 .

[IKEv1]: IP = 10.0.0.2, IKE_DECODE (msgid=0) : HDR + SA (1) + (13)
+ NONE (0) : 104
[IKEv1 DEBUG]: IP = 10.0.0.2, SA
[IKEv1 DEBUG]: IP = 10.0.0.2, Oakley
[IKEv1 DEBUG]: IP = 10.0.0.2, VID
[IKEv1 DEBUG]: IP = 10.0.0.2, VID RFC Received NAT-Traversal

MM2.

MM3.

30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2, ke

includesNAT ,
(KE) Diffie-Hellman
(DH) (g, p,), DPD.

MM3.

MM4 .

MM4.
NAT-D , iniator
NAT NAT.

KE DH "B" "s".

```
30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2,
30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2,  VID Cisco Unity
30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2,  xauth V6 VID
30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2,  VID IOS
30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2,  ASA,  IOS (: 1.0.0, : 20000001)
30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2,  VID
30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2,  VID GW Vpn3000/Cisco ASA Altiga/Cisco
30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2,  NAT
30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2,  NAT
30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2,  NAT
30 10:38:29 [IKEv1 DEBUG]: IP = 10.0.0.2,  NAT
[IKEv1]: IP = 10.0.0.2,  (msgid=0)  IKE_DECODE  : HDR + KE (4) +  (10) +  (13) +  (13) +  (13) +  (13) + NAT-D (20) + NAT-D (20) + NONE (0)  : 304
                    ============================== MM3
                                ======================>
[IKEv1]: IP = 10.0.0.2, IKE_DECODE  (msgid=0)  : HDR + KE (4) +  (10) +  (13) +  (13) +  (13) + NAT-D (130) + NAT-D (130) + NONE (0)  : 284
                                                [IKEv1 DEBUG]: IP = 10.0.0.2,  ke
                                                [IKEv1 DEBUG]: IP = 10.0.0.2,  ISA_KE
                                                [IKEv1 DEBUG]: IP = 10.0.0.2,
                                                [IKEv1 DEBUG]: IP = 10.0.0.2,  VID
                                                [IKEv1 DEBUG]: IP = 10.0.0.2,  VID DPD
                                                [IKEv1 DEBUG]: IP = 10.0.0.2,  VID
                                [IKEv1 DEBUG]: IP = 10.0.0.2,  IOS/PIX (: 1.0.0, : 00000f6f)
                                                [IKEv1 DEBUG]: IP = 10.0.0.2,  VID
                                [IKEv1 DEBUG]: IP = 10.0.0.2,  xauth V6 VID
                                                [IKEv1 DEBUG]: IP = 10.0.0.2,  NAT
                                                [IKEv1 DEBUG]: IP = 10.0.0.2,  NAT
                                                [IKEv1 DEBUG]: IP = 10.0.0.2,  NAT
                                                [IKEv1 DEBUG]: IP = 10.0.0.2,  NAT
                                                  [IKEv1 DEBUG]: IP = 10.0.0.2,  ke
                                                    [IKEv1 DEBUG]: IP = 10.0.0.2,
                                [IKEv1 DEBUG]: IP = 10.0.0.2,  VID Cisco Unity
                                [IKEv1 DEBUG]: IP = 10.0.0.2,  xauth V6 VID
                                [IKEv1 DEBUG]: IP = 10.0.0.2,  VID IOS
                [IKEv1 DEBUG]: IP = 10.0.0.2,  ASA,  IOS (: 1.0.0, : 20000001)
                                [IKEv1 DEBUG]: IP = 10.0.0.2,  VID
                [IKEv1 DEBUG]: IP = 10.0.0.2,  VID GW Vpn3000/Cisco ASA Altiga/Cisco
                                                [IKEv1 DEBUG]: IP = 10.0.0.2,  NAT
                                                [IKEv1 DEBUG]: IP = 10.0.0.2,  NAT
                                                [IKEv1 DEBUG]: IP = 10.0.0.2,  NAT
                                                [IKEv1 DEBUG]: IP = 10.0.0.2,  NAT
                                [IKEv1]: IP = 10.0.0.2,  tunnel_group 10.0.0.2
                              [IKEv1 DEBUG]:  = 10.0.0.2, IP = 10.0.0.2,  …
[IKEv1]: IP = 10.0.0.2,  (msgid=0)  IKE_DECODE  : HDR + KE (4) +  (10) +  (13) +  (13) +  (13) +  (13) + NAT-D (130) + NAT-D (130) + NONE (0)  : 304
                                                <============================ MM4
                                                ============================
[IKEv1]: IP = 10.0.0.2, IKE_DECODE  (msgid=0)  : HDR + KE (4) +  (10) +  (13) +  (13) +  (13) +  (13) + NAT-D (20) + NAT-D (20) + NONE (0)  : 304
[IKEv1 DEBUG]: IP = 10.0.0.2,  ike
[IKEv1 DEBUG]: IP = 10.0.0.2,  ISA_KE
[IKEv1 DEBUG]: IP = 10.0.0.2,
[IKEv1 DEBUG]: IP = 10.0.0.2,  VID
[IKEv1 DEBUG]: IP = 10.0.0.2,  VID  Cisco Unity
[IKEv1 DEBUG]: IP = 10.0.0.2,  VID
[IKEv1 DEBUG]: IP = 10.0.0.2,  VID DPD
[IKEv1 DEBUG]: IP = 10.0.0.2,  VID
```

MM3 .

MM3.
NAT-D , NAT
NAT.
KE DH p, g A.

MM4.
NAT, KE DH
"B", "s" ("B"), VID
DPD.

10.0.0.2 L2L,
"s" .

MM4.

[IKEv1 DEBUG]: IP = 10.0.0.2, IOS/PIX (: 1.0.0, : 00000f7f)
[IKEv1 DEBUG]: IP = 10.0.0.2, VID
[IKEv1 DEBUG]: IP = 10.0.0.2, xauth V6 VID
[IKEv1 DEBUG]: IP = 10.0.0.2, NAT
[IKEv1 DEBUG]: IP = 10.0.0.2, NAT
[IKEv1 DEBUG]: IP = 10.0.0.2, NAT
[IKEv1 DEBUG]: IP = 10.0.0.2, NAT

10.0.0.2 L2L, "s" .

[IKEv1]: IP = 10.0.0.2, tunnel_group 10.0.0.2
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, ...
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, ID
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2,
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, ISAKMP
[IKEv1 DEBUG]: IP = 10.0.0.2, IOS: . proposal=32767/32767.
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, dpd vid

MM5.
:
crypto isakmp identity auto

MM5.

[IKEv1]: IP = 10.0.0.2, (msgid=0) IKE_DECODE : HDR + ID (5) + (8) + KEEPALIVE IOS (128) +VENDOR (13) + NONE (0) : 96
========== MM5 ==========>

NAT. NAT-T .

[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, NAT: NAT, NAT

[IKEv1]: IP = 10.0.0.2, IKE_DECODE (msgid=0) : HDR + ID (5) + (8) + NONE (0) : 64

MM5 .
(ID) , .

[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, ID
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR ID 10.0.0.2
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2,
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, ISAKMP
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2,
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, NAT
[IKEv1]: IP = 10.0.0.2, tunnel_group 10.0.0.2
: NAT, NAT
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, ID
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2,
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, ISAKMP
[IKEv1 DEBUG]: IP = 10.0.0.2, IOS: . proposal=32767/32767.
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, dpd vid
[IKEv1]: IP = 10.0.0.2, (msgid=0) IKE_DECODE : HDR + ID (5) + (8) + KEEPALIVE IOS (128) +VENDOR (13) + NONE (0) : 96
<========== MM6 ==========

MM5.
  .
; , .
:
10.0.0.2 ipsec-l2l

NAT-T, .

MM6.

  , .

MM6.

1.
isakmp .
:
crypto isakmp policy 10
 authentication pre-share
 3des
 sha
 group 2
 86400
ciscoasa# sh run
crypto isakmp
crypto isakmp identity auto

[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, 1

MM6 .

[IKEv1]: IP = 10.0.0.2, IKE_DECODE (msgid=0) : HDR + ID (5) + (8) + NONE (0) : 64

[IKEv1]: IP = 10.0.0.2, : DPD
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, P1 : 64800 .

MM6.
, .

[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, ID
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR ID 10.0.0.2
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2,
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, ISAKMP
[IKEv1]: IP = 10.0.0.2, tunnel_group 10.0.0.2
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, Oakley

[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, IKE QM: = 7b80c2b0

1.
ISAKMP .
:
10.0.0.2 ipsec-l2l
10.0.0.2 IPSec
Cisco

[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, 1
[IKEv1]: IP = 10.0.0.2,   : DPD
DPD   , 1 .
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, P1   : 82080 .

IPSec: SA, 0x53FC3C00,
SCB: 0x53F90A00,
:
SPI: 0xFD2D851F
: 0x00006000
VPIF: 0x00000003
: l2l
:
: 240

2 ( ) .

[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, IKE SPI   : SPI = 0xfd2d851f
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, oakley constucting
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2,
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2,   IPSEC
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2,   IPSec
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, Proxy Id
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, Proxy Id:
: 192.168.1.0 255.255.255.0 1 0
: 192.168.2.0 255.255.255.0 1 0
(192.168.1.0/24) expcted (192.168.2.0/24)
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, IKE,
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, qm
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, IKE, 1- QM PKT: = 7b80c2b0
[IKEv1]: IP = 10.0.0.2, (msgid=7b80c2b0) IKE_DECODE : HDR + (8) +
SA (1) + (10) + ID (5) + ID (5) + (11) + NONE (0) : 200

QM1.
Proxy Id IPsec.
:
crypto ipsec
transform-set esp-sha-
hmac aes ESP
TRANSFORM
VPN access-list icmp
192.168.1.0
255.255.255.0
192.168.2.0
255.255.255.0

QM1.

========== QM1
==========>

[IKEv1]: IP = 10.0.0.2, IKE QM: = 52481cf5
[IKEv1]: IP = 10.0.0.2, IKE_DECODE (msgid=52481cf5) : HDR + (8)
+ SA (1) + (10) + ID (5) + ID (5) + NONE (0) : 172

[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2,
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, SA
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2,
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, ID

[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID -
192.168.2.0 - 255.255.255.0[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, IP ID :
192.168.2.0, 255.255.255.0, 1, 0
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, ID
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID -
192.168.1.0 - 255.255.255.0
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, IP ID : 192.168.1.0, 255.255.255.0,
1, 0

[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, QM IsRekeyed sa,
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, , = MAP, seq = 10...
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, , MAP , seq = 10
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, IKE : MAP
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, IPSEC
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, # 1 IPSEC, # 1 # 10
IPSEC

[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, IKE: SPI!

QM1 .
2 (QM).

QM1.
IPsec.
: crypto ipsec
transform-set esp-sha-
hmac aes ESP
TRANSFORM
VPN access-list icmp
192.168.1.0
255.255.255.0
192.168.2.0
255.255.255.0
MAP 10 VPN

(192.168.2.0/24
192.168.1.0/24) .

- .

QM2.

IPSec: SA, 0x53FC3698,
SCB: 0x53FC2998,
:
SPI: 0x1698CAC7
: 0x00004000
VPIF: 0x00000003
: l2l
:
: 240
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, IKE SPI : SPI = 0x1698cac7
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, oakley
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2,
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, IPSEC
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, IPSec
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, Proxy Id
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, Proxy Id:
: 192.168.2.0 255.255.255.0 1 0
: 192.168.1.0 255.255.255.0 1 0
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, qm
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, IKE, 2- QM PKT: = 52481cf5
[IKEv1]: IP = 10.0.0.2, (msgid=52481cf5) IKE_DECODE : HDR + (8)
+ SA (1) + (10) + ID (5) + ID (5) + NONE (0) : 172

, , Crypto ACLS.

QM2.

<========================== QM2
==========================

QM2 .

[IKEv1]: IP = 10.0.0.2, IKE_DECODE (msgid=7b80c2b0) : HDR + (8) +
SA (1) + (10) + ID (5) + ID (5) + (11) + NONE (0) : 200
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2,
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, SA
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2,
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, ID
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID -
192.168.1.0 - 255.255.255.0

QM2.

[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, ID
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, ID_IPV4_ADDR_SUBNET ID -
192.168.2.0 - 255.255.255.0

2.

[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2,
[IKEv1]: (outb SPI[4]lattributes):
[IKEv1]: 0000: DDE50931 80010001 00020004 00000E10... 1.....
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, , IPSec 28800 3600
ASA IPSec.
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, IPSEC
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, !

"MAP" 10
access-list "VPN".

[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, NP MAP 10 VPN ACL:
cs_id=53f11198; rule=53f11a90
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, !
IPSec: SA, 0x53FC3698,
SCB: 0x53F910F0,
:
SPI: 0xDDE50931
: 0x00006000
VPIF: 0x00000003
: l2l
:

SPI 0xfd2d851f
0xdde50931for .

: 240
IPSec: OBSA, SPI 0xDDE50931
IPSec: VPN, SPI 0xDDE50931
: 0x00000005
SA: 0x53FC3698
SPI: 0xDDE50931
MTU: 1500
VCID: 0x00000000
: 0x00000000
SCB: 0x01CF218F
: 0x4C69CB80

IPSec: VPN, SPI 0xDDE50931
 VPN: 0x000161A4
IPSec: , SPI 0xDDE50931
 src: 192.168.1.0
 src: 255.255.255.0
 dst: 192.168.2.0
 dst: 255.255.255.0
 src
: 0
: 0
Op:
 dst
: 0
: 0
Op:
: 1
 : tRUE
SPI: 0x00000000
SPI : fALSE
IPSec: , SPI 0xDDE50931
ID : 0x53FC3AD8
IPSec: , SPI 0xDDE50931
 src: 10.0.0.1
 src: 255.255.255.255
 dst: 10.0.0.2
 dst: 255.255.255.255
 src
: 0
: 0
Op:
 dst
: 0
: 0
Op:
: 50
 : tRUE
SPI: 0xDDE50931
SPI : tRUE
IPSec: , SPI 0xDDE50931
ID : 0x53F91538
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, NP MAP 10 VPN ACL:
cs_id=53f11198; rule=53f11a90
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, LAN-LAN (10.0.0.2) , SPI =
0xfd2d851f, SPI = 0xdde50931
IPSec: IBSA, SPI 0xFD2D851F
IPSec: VPN, SPI 0xFD2D851F
: 0x00000006
SA: 0x53FC3C00
SPI: 0xFD2D851F
MTU: 0
VCID: 0x00000000
 : 0x000161A4
SCB: 0x01CEA8EF
QM3.
: 0x4C69CB80
SPI, .
IPSec: VPN, SPI 0xFD2D851F
 VPN: 0x00018BBC
IPSec: VPN 0x000161A4, SPI 0xDDE50931
: 0x00000005
SA: 0x53FC3698
SPI: 0xDDE50931
MTU: 1500
VCID: 0x00000000
 : 0x00018BBC
SCB: 0x01CF218F

: 0x4C69CB80
IPSec: VPN, SPI 0xDDE50931
 VPN: 0x000161A4
IPSec: , SPI 0xDDE50931
ID : 0x53FC3AD8
IPSec: SPD, SPI 0xDDE50931
ID : 0x53F91538
IPSec: , SPI 0xFD2D851F
 src: 192.168.2.0
 src: 255.255.255.0
 dst: 192.168.1.0
 dst: 255.255.255.0
 src
: 0
: 0
Op:
 dst
: 0
: 0
Op:
: 1
 : tRUE
SPI: 0x00000000
SPI : fALSE
IPSec: , SPI 0xFD2D851F
ID : 0x53F91970
IPSec: , SPI 0xFD2D851F
 src: 10.0.0.2
 src: 255.255.255.255
 dst: 10.0.0.1
 dst: 255.255.255.255
 src
: 0
: 0
Op:
 dst
: 0
: 0
Op:
: 50
 : tRUE
SPI: 0xFD2D851F
SPI : tRUE
IPSec: , SPI 0xFD2D851F
ID : 0x53F91A08
IPSec: , SPI 0xFD2D851F
 src: 10.0.0.2
 src: 255.255.255.255
 dst: 10.0.0.1
 dst: 255.255.255.255
 src
: 0
: 0
Op:
 dst
: 0
: 0
Op:
: 50
 : tRUE
SPI: 0xFD2D851F
SPI : tRUE
IPSec: , SPI 0xFD2D851F
ID : 0x53F91AA0

QM3.

[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, IKE, 3- QM PKT: = 7b80c2b0

========== QM3

==========>

[IKEv1]: IP = 10.0.0.2, (msgid=7b80c2b0)

IKE_DECODE : HDR + (8) + NONE (0) :76

[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, IKE KEY_ADD SA: SPI = 0xdde50931

[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, : KEY_UPDATE, spi 0xfd2d851f

[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, P2 : 3060

.

[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, 2 (msgid=7b80c2b0)

2. SPI.

[IKEv1]: IP = 10.0.0.2, IKE_DECODE (msgid=52481cf5) : HDR + (8) + NONE (0) : 52

QM3 receivd fom.

[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2,

[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, IPSEC

[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, !

[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, NP MAP 10 VPN ACL: cs_id=53f11198; rule=53f11a90

[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, !

IPSec: SA, 0x53F18B00, SCB: 0x53F8A1C0,

:

SPI: 0xDB680406

: 0x00004000

VPIF: 0x00000003

: l2l

:

: 240

IPSec: OBSA, SPI 0xDB680406

IPSec: VPN, SPI 0xDB680406

: 0x00000005

SA: 0x53F18B00

SPI: 0xDB680406

MTU: 1500

VCID: 0x00000000

: 0x00000000

SCB: 0x005E4849

: 0x4C69CB80

IPSec: VPN, SPI 0xDB680406

VPN: 0x0000E9B4

IPSec: , SPI 0xDB680406

src: 192.168.1.0

src: 255.255.255.0

dst: 192.168.2.0

dst: 255.255.255.0

src

: 0

: 0

Op:

dst

: 0

: 0

Op:

: 1

: tRUE

SPI: 0x00000000

SPI : fALSE

IPSec: , SPI 0xDB680406

ID : 0x53F89160

IPSec: , SPI 0xDB680406

src: 10.0.0.1

src: 255.255.255.255

dst: 10.0.0.2

dst: 255.255.255.255

QM3. SA . , SPI .

src
: 0
: 0
Op:
dst
: 0
: 0
Op:
: 50
: tRUE
SPI: 0xDB680406
SPI : tRUE
IPSec: , SPI 0xDB680406
ID : 0x53E47E88
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, NP MAP 10 VPN ACL:
cs_id=53f11198; rule=53f11a90
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, LAN-LAN (10.0.0.2) , SPI =
0x1698cac7, SPI = 0xdb680406
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, IKE KEY_ADD SA: SPI =
0xdb680406
IPSec: IBSA, SPI 0x1698CAC7
IPSec: VPN, SPI 0x1698CAC7
: 0x00000006
SA: 0x53FC3698
SPI: 0x1698CAC7
MTU: 0
VCID: 0x00000000
: 0x0000E9B4
SCB: 0x005DAE51
: 0x4C69CB80
IPSec: VPN, SPI 0x1698CAC7
VPN: 0x00011A8C
IPSec: VPN 0x0000E9B4, SPI 0xDB680406
: 0x00000005
SA: 0x53F18B00
SPI: 0xDB680406
MTU: 1500
VCID: 0x00000000
: 0x00011A8C
SCB: 0x005E4849
: 0x4C69CB80 SPI SA .
IPSec: VPN, SPI 0xDB680406
VPN: 0x0000E9B4
IPSec: , SPI 0xDB680406
ID : 0x53F89160
IPSec: SPD, SPI 0xDB680406
ID : 0x53E47E88
IPSec: , SPI 0x1698CAC7
src: 192.168.2.0
src: 255.255.255.0
dst: 192.168.1.0
dst: 255.255.255.0
src
: 0
: 0
Op:
dst
: 0
: 0
Op:
: 1
: tRUE
SPI: 0x00000000
SPI : fALSE

IPSec: , SPI 0x1698CAC7
ID : 0x53FC3E80
IPSec: , SPI 0x1698CAC7
src: 10.0.0.2
src: 255.255.255.255
dst: 10.0.0.1
dst: 255.255.255.255
src
: 0
: 0
Op:
dst
: 0
: 0
Op:
: 50
: tRUE
SPI: 0x1698CAC7
SPI : tRUE
IPSec: , SPI 0x1698CAC7
ID : 0x53FC3F18
IPSec: , SPI 0x1698CAC7
src: 10.0.0.2
src: 255.255.255.255
dst: 10.0.0.1
dst: 255.255.255.255
src
: 0
: 0
Op:
dst
: 0
: 0
Op:
: 50
: tRUE
SPI: 0x1698CAC7
SPI : tRUE
IPSec: , SPI 0x1698CAC7
ID : 0x53F8AEA8
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, : KEY_UPDATE, spi 0x1698cac7
[IKEv1 DEBUG]: = 10.0.0.2, IP = 10.0.0.2, P2 : 3060 . IPsec .
[IKEv1]: = 10.0.0.2, IP = 10.0.0.2, 2 (msgid=52481cf5) 2. / .

Туннельная проверка

Примечание: Так как ICMP используется для инициирования туннеля, только один КОНТЕКСТ БЕЗОПАСНОСТИ IPSEC подключен. Протокол 1 = ICMP.

```
show crypto ipsec sa
interface: outside
  Crypto map tag: MAP, seq num: 10, local addr: 10.0.0.1
   access-list VPN extended permit icmp 192.168.1.0 255.255.255.0 192.168.2.0 255.255.255.0
   local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/ 1/0)
   remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/ 1/0)
   current_peer: 10.0.0.2
   #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
   #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 4, #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.: 10.0.0.1/0, remote crypto endpt.: 10.0.0.2/0
   path mtu 1500, ipsec overhead 74, media mtu 1500
   current outbound spi: DB680406
   current inbound spi : 1698CAC7
  inbound esp sas:
   spi: 0x 1698CAC7 (379112135)
      transform: esp-aes esp-sha-hmac no compression
      in use settings ={L2L, Tunnel, }
      slot: 0, conn_id: 16384, crypto-map: MAP
      sa timing: remaining key lifetime (kB/sec): (3914999/3326)
      IV size: 16 bytes
      replay detection support: Y
      Anti replay bitmap:
       0x00000000 0x0000001F
  outbound esp sas:
   spi: 0xDB680406 (3681027078)
      transform: esp-aes esp-sha-hmac no compression
      in use settings ={L2L, Tunnel, }
      slot: 0, conn_id: 16384, crypto-map: MAP
      sa timing: remaining key lifetime (kB/sec): (3914999/3326)
      IV size: 16 bytes
      replay detection support: Y
      Anti replay bitmap:
      0x00000000 0x00000001 show crypto isakmp sa

  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: 10.0.0.2
   Type    : L2L             Role    : responder
   Rekey   : no              State   : MM_ACTIVE
```

Дополнительные сведения

- Отличное место для начала является статьей Википедии относительно IPSec. Стандарт и ссылки содержат много полезных сведений
- Устранение неполадок IPsec - общие сведения и использование команд debug
- Cisco Systems – техническая поддержка и документация