Пример конфигурации "IOS IPSec NAT Transparency с VPN Client"

Содержание

Введение

В этом документе приводится пример конфигурации прозрачного режима NAT (преобразования сетевых адресов) средствами Cisco IOS®. Этот режим позволяет пропускать через NAT или преобразование адресов портов (PAT) трафик IPsec и устраняет множество известных проблем несовместимости между NAT и IPsec.

Предварительные условия

Требования

Для этого документа нет особых требований.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

Маршрутизатор Cisco 2621 с выпуском ПО 12.2.13.7T1 или выше

VPN-клиент Cisco VPN Client 3.6.3 (конфигурация не показана)

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе в действующей сети необходимо понимать последствия выполнения любой команды.

Условные обозначения

Подробные сведения об условных обозначениях см. в документе Условное обозначение технических терминов Cisco.

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание. Получить дополнительные сведения об используемых в данном документе командах можно при помощи Средства поиска команд (только для зарегистрированных пользователей).

Схема сети

В настоящем документе используется следующая схема сети:

Настройка маршрутизатора

Выполните следующие действия:

Команда **show version** отображает версию программного обеспечения, используемую коммутатором.

```
2621#show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IK9O3S3-M), Version 12.2(13.7)T1,
MAINTENANCE INTERIM SOFTWARE
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2002 by cisco Systems, Inc.
Compiled Sat 21-Dec-02 14:10 by ccai
Image text-base: 0x80008098, data-base: 0x818B6330

ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)
ROM: C2600 Software (C2600-IK9O3S3-M), Version 12.2(13.7)T1,
MAINTENANCE INTERIM SOFTWARE

2621 uptime is 33 minutes
System returned to ROM by reload
System image file is "flash:c2600-ik9o3s3-mz.122-13.7.T1"

cisco 2621 (MPC860) processor (revision 0x102) with 60416K/5120K bytes of
memory.
Processor board ID JAB0407020V (2751454139)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
Primary Rate ISDN software, Version 1.1.
2 FastEthernet/IEEE 802.3 interface(s)
2 Channelized T1/PRI port(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102
```

Выполните команду **show run**.

```
2621#show run
Building configuration...

Current configuration : 2899 bytes
!
version 12.2
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
!
hostname 2621
!
boot system flash
logging queue-limit 100
enable secret 5 $1$dGFC$VA28yOWzxlCKyj1dq8SkE/
!
username cisco password 0 cisco123
username client password 0 testclient
aaa new-model
!
!
aaa authentication login userauthen local
aaa authorization network foo local
aaa session-id common
ip subnet-zero
ip cef
!
!
no ip domain lookup
ip domain name cisco.com
!
!
!
!
crypto isakmp policy 20
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp keepalive 40 5
!--- Allows an IPsec node to send NAT keepalive !--- packets every 20 seconds.
crypto isakmp nat keepalive 20
!
crypto isakmp client configuration group cisco
 key test1234
 pool test
 acl 120
!
!
!--- Transform set "test" which uses Triple DES !--- encryptions and MD5 (HMAC
variant) !--- for data packet authentication: crypto ipsec transform-set test
```

```
esp-3des esp-md5-hmac
crypto ipsec transform-set foo esp-3des esp-sha-hmac
!
crypto ipsec profile greprotect
!
!
!--- Dynamic crypto map. crypto dynamic-map dynmap 1
 set transform-set foo
 match address 199
!
!
crypto map test client authentication list userauthen
crypto map test isakmp authorization list foo
crypto map test client configuration address respond
!--- Adds a dynamic crypto map set to a static crypto map set. crypto map test
20 ipsec-isakmp dynamic dynmap
!
!
!
voice call carrier capacity active
!
!
!
!
!
!
!
no voice hpi capture buffer
no voice hpi capture destination
!
!
mta receive maximum-recipients 0
!
!
controller T1 0/0
 framing sf
 linecode ami
!
controller T1 0/1
 framing sf
 linecode ami
!
!
!
interface Loopback0
 ip address 10.100.100.1 255.255.255.0
 ip nat inside
!
interface FastEthernet0/0
 ip address 172.16.142.191 255.255.255.0
 ip nat outside
 no ip route-cache
 no ip mroute-cache
```

```
 duplex auto
 speed auto
 !--- Applies a crypto map set to an interface. crypto map test
!
interface FastEthernet0/1
 ip address 10.130.13.13 255.255.0.0
 duplex auto
 speed auto
!
ip local pool test 192.168.1.1 192.168.1.250
ip nat inside source route-map nonat interface FastEthernet0/0 overload
no ip http server
no ip http secure-server
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.142.1
!
ip pim bidir-enable
!
!
access-list 101 permit ip any any
access-list 101 permit esp any any
access-list 101 permit udp any any eq isakmp
access-list 101 permit ip 192.168.0.0 0.0.255.255 10.100.100.0 0.0.0.255
access-list 111 permit ip 10.100.100.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 112 deny   ip 10.100.100.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 112 deny   ip 10.100.100.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 112 permit ip 10.100.100.0 0.0.0.255 any
access-list 120 permit ip 10.100.100.0 0.0.0.255 192.168.1.0 0.0.0.255
!--- IPsec access list defines which traffic to protect. access-list 199 permit
ip 10.100.100.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 199 permit ip host 172.16.142.191 192.168.1.0 0.0.0.255
!
route-map nonat permit 10
 match ip address 112
!
radius-server authorization permit missing Service-Type
call rsvp-sync
!
!
mgcp profile default
!
dial-peer cor custom
!
!
!
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 password cisco
!
```

```
!
end

2621#
```

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Интерпретатор выходных данных (OIT), доступный только зарегистрированным пользователям, поддерживает некоторые команды **show**. Посредством OIT можно анализировать выходные данные команд **show**.

show crypto isakmp sa – показывает все текущие ассоциации безопасности протокола IKE (Internet Key Exchange, обмен ключами в Интернете) на одноранговом узле.

```
2621#show crypto isakmp sa
  f_vrf/i_vrf    dst             src             state       conn-id slot
       /         172.16.142.191  171.69.89.82     QM_IDLE      4       0
```

show crypto ipsec sa – показывает настройки, используемые текущими ассоциациями безопасности.

```
2621#show crypto ipsec sa

interface: FastEthernet0/0
    Crypto map tag: test, local addr. 172.16.142.191

   protected vrf:
   local  ident (addr/mask/prot/port): (10.100.100.0/255.255.255.0/0/0)
!--- Subnet behind local VPN router. remote ident (addr/mask/prot/port):
(192.168.1.3/255.255.255.255/0/0) !--- Subnet behind remote VPN router.
current_peer: 171.69.89.82:4500 PERMIT, flags={} #pkts encaps: 11, #pkts encrypt:
11, #pkts digest 11 #pkts decaps: 11, #pkts decrypt: 11, #pkts verify 11 #pkts
compressed: 0, #pkts decompressed: 0 #pkts not compressed: 0, #pkts compr.
failed: 0 #pkts not decompressed: 0, #pkts decompress failed: 0 #send errors 0,
#recv errors 0 local crypto endpt.: 172.16.142.191, remote crypto endpt.:
171.69.89.82 !--- IP address of Encapsulating Security Payload (ESP) endpoints.
path mtu 1500, media mtu 1500 current outbound spi: 9A12903F inbound esp sas:
spi: 0xD44C2AFE(3561761534) !--- SPI inbound (ESP tunnel). transform: esp-3des
esp-sha-hmac , in use settings ={Tunnel UDP-Encaps, } slot: 0, conn id: 2002,
flow_id: 3, crypto map: test
        sa timing: remaining key lifetime (k/sec): (4513510/3476)
        IV size: 8 bytes
        replay detection support: Y

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
```

```
      spi: 0x9A12903F(2584907839)
!--- Security parameter index (SPI) outbound (ESP tunnel). transform: esp-3des
esp-sha-hmac , in use settings ={Tunnel UDP-Encaps, } slot: 0, conn id: 2003,
flow_id: 4, crypto map: test
        sa timing: remaining key lifetime (k/sec): (4513511/3476)
        IV size: 8 bytes
        replay detection support: Y

     outbound ah sas:

     outbound pcp sas:

   protected vrf:
   local  ident (addr/mask/prot/port): (172.16.142.191/255.255.255.255/0/0)
!--- Next tunnel. remote ident (addr/mask/prot/port):
(192.168.1.3/255.255.255.255/0/0) current_peer: 171.69.89.82:4500 PERMIT,
flags={} #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0 #pkts decaps: 0, #pkts
decrypt: 0, #pkts verify 0 #pkts compressed: 0, #pkts decompressed: 0 #pkts not
compressed: 0, #pkts compr. failed: 0 #pkts not decompressed: 0, #pkts decompress
failed: 0 #send errors 0, #recv errors 0 local crypto endpt.: 172.16.142.191,
remote crypto endpt.: 171.69.89.82 path mtu 1500, media mtu 1500 current outbound
spi: 1CD14C06 inbound esp sas: spi: 0x1EAC399E(514603422) transform: esp-3des
esp-sha-hmac , in use settings ={Tunnel UDP-Encaps, } slot: 0, conn id: 2000,
flow_id: 1, crypto map: test sa timing: remaining key lifetime (k/sec):
(4434590/3471) IV size: 8 bytes replay detection support: Y inbound ah sas:
inbound pcp sas: outbound esp sas: spi: 0x1CD14C06(483478534) transform: esp-3des
esp-sha-hmac , in use settings ={Tunnel UDP-Encaps, } slot: 0, conn id: 2001,
flow_id: 2, crypto map: test sa timing: remaining key lifetime (k/sec):
(4434590/3469) IV size: 8 bytes replay detection support: Y outbound ah sas:
outbound pcp sas:
```

show crypyo engine connection active – показывает статистику ядра шифрования. Эта команда сообщает число пакетов.

```
2621#show crypyo engine connection active

  ID Interface       IP-Address      State  Algorithm           Encrypt  Decrypt
   4 FastEthernet0/0 172.16.142.191  set    HMAC_MD5+3DES_56_C        0        0
2000 FastEthernet0/0 172.16.142.191  set    HMAC_SHA+3DES_56_C        0        0
2001 FastEthernet0/0 172.16.142.191  set    HMAC_SHA+3DES_56_C        0        0
2002 FastEthernet0/0 172.16.142.191  set    HMAC_SHA+3DES_56_C        0       11
2003 FastEthernet0/0 172.16.142.191  set    HMAC_SHA+3DES_56_C       11        0
```

show crypto engine [brief | configuration] – показывает сводку по конфигурации криптоядер. Эта команда используется в привилегированном режиме EXEC. Эта команда показывает все криптоядра и название продукта AIM-VPN.

```
2621#show crypto engine configuration

        crypto engine name:  unknown
!--- Name of the crypto engine as assigned with the !--- key-name argument in the
 crypto key generate dss command.
```

```
        crypto engine type:  software
!--- If "software" is listed, the crypto engine resides in either !--- the Route
Switch Processor (RSP) (the Cisco IOS crypto engine) or !--- in a second-
generation Versatile Interface Processor (VIP2). serial number: A3FFDBBB crypto
engine state: installed !--- The state "installed" indicates that a crypto engine
is located !--- in the given slot, but is not configured for encryption. crypto
engine in slot: N/A platform: Cisco Software Crypto Engine Encryption Process
Info: input queue size: 500 input queue top: 34 input queue bot: 34 input queue
count: 0 Crypto Adjacency Counts: Lock Count: 0 Unlock Count: 0 crypto lib
version: 14.0.0 ipsec lib version: 2.0.0
```

show crypto isakmp sa detail nat – показывает подробные сведения о NAT с использованием ассоциаций безопасности ISAKMP.

```
2621#show crypto isakmp sa detail nat
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

  f_vrf/i_vrf  Conn id   Local        Remote        Encr Hash Auth DH Lifetime
Capabilities
       /        4     172.16.142.191  171.69.89.82  3des md5       2  23:56:43
CDXN
        NAT keepalive(sec) 20
        In local 172.16.142.191:4500 remote cisco:4500
```

f_vrf/i_vrf – обращенный наружу экземпляр виртуальной маршрутизации и пересылки (F_VRF) и внутренний экземпляр VRF (I_VRF) в ассоциации безопасности IKE. В случае глобального экземпляра FVRF поле `f_vrf` показывается пустым.

Поиск и устранение неполадок

Используйте этот раздел для устранения неполадок своей конфигурации.

Команды для устранения неполадок

Интерпретатор выходных данных (OIT), доступный только зарегистрированным пользователям, поддерживает некоторые команды **show**. Посредством OIT можно анализировать выходные данные команд **show**.

Дополнительные сведения об устранении неполадок см. в разделе Устранение неполадок IP-безопасности – общие сведения и использование команд debug.

Примечание. Перед использованием команд **debug** ознакомьтесь с документом Важные сведения о командах debug.

Эта конфигурация получает сообщения поддержания активности (Keepalive) NAT каждые 20 секунд в соответствии с настройкой.

debug crypto ipsec – показывает данные согласования IPsec на этапе 2.

debug crypto isakmp – показывает процесс согласования по протоколу ISAKMP на этапе 1.

debug crypto engine – показывает зашифрованный трафик.

```
2621#show crypto isakmp sa detail nat
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

  f_vrf/i_vrf  Conn id   Local        Remote        Encr Hash Auth DH Lifetime
Capabilities
       /        4     172.16.142.191  171.69.89.82  3des md5       2  23:56:43
CDXN
        NAT keepalive(sec) 20
        In local 172.16.142.191:4500 remote cisco:4500
```

debug ip packet [detail] – показывает общие отладочные сведения протокола IP и транзакций безопасности с установленными параметрами безопасности IP (IPSO).

debug ip icmp – показывает сведения о транзакциях межсетевого протокола управляющих сообщений (ICMP).

```
2621#show crypto isakmp sa detail nat
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

  f_vrf/i_vrf  Conn id   Local        Remote        Encr Hash Auth DH Lifetime
Capabilities
       /        4     172.16.142.191  171.69.89.82  3des md5       2  23:56:43
CDXN
        NAT keepalive(sec) 20
        In local 172.16.142.191:4500 remote cisco:4500
```

debug crypto ipsec – показывает данные согласования IPsec на этапе 2.

debug crypto isakmp – показывает процесс согласования по протоколу ISAKMP на этапе 1.

debug crypto engine – показывает зашифрованный трафик.

```
2621#show crypto isakmp sa detail nat
```

```
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption

  f_vrf/i_vrf  Conn id   Local         Remote        Encr Hash Auth DH Lifetime
Capabilities
       /        4     172.16.142.191  171.69.89.82  3des md5       2  23:56:43
CDXN
        NAT keepalive(sec) 20
        In local 172.16.142.191:4500 remote cisco:4500
```

Дополнительные сведения

- Страница поддержки клиента Cisco VPN Client
- Протоколы IPsec Negotiation/IKE
- Cisco Systems – техническая поддержка и документация