PIX/ASA 7.x и более поздние: Пример конфигурации Easy VPN с ASA 5500 разделенного туннелирования в качестве сервера и Cisco 871 в качестве удаленного клиента Easy VPN

Содержание

Введение

В этом документе приводится пример настройки протокола IPsec между устройством адаптивной защиты Cisco (Adaptive Security Appliance) ASA 5520 и маршрутизатором Cisco 871 с помощью Easy VPN. Устройство ASA 5520 действует как сервер Easy VPN, а маршрутизатор Cisco 871 — как удаленный клиент Easy VPN. Хотя в этой конфигурации используется устройство ASA 5520 с программным обеспечением ASA версии 7.1(1), эту конфигурацию также можно применять для межсетевых экранов PIX с операционной системой PIX версии 7.1 и более поздними.

Чтобы настроить маршрутизатор Cisco IOS® как EzVPN в режиме расширения сети (NEM), которая подключена к концентратору Cisco VPN 3000, см. раздел Настройка клиента EzVPN Cisco на IOS Cisco с концентратором VPN 3000.

Чтобы настроить IPsec между аппаратным удаленным клиентом Cisco IOS® Easy VPN и сервером PIX Easy VPN, см. раздел Пример настройки аппаратного удаленного клиента IOS Easy VPN для сервера PIX Easy VPN.

Чтобы настроить маршрутизатор Cisco 7200 как EzVPN и маршрутизатор Cisco 871 как Easy

VPN Remote, см. раздел Пример настройки сервера 7200 Easy VPN для 871 Easy VPN Remote.

Предварительные условия

Требования

Необходимо иметь основные представления о протоколе IPsec и операционных системах ASA 7.x.

Используемые компоненты

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

- Сервер EasyVPN — это ASA 5520 с версией 7.1(1).
- Удаленный аппаратный клиент Easy VPN — это маршрутизатор Cisco 871 под управлением ПО Cisco IOS® версии 12.4(4)T1.

Примечание: Версия 7.x серии 5500 Cisco ASA выполняет подобную версию программного обеспечения, замеченную в Версии PIX 7. x. Настройки, приведенные в этом документе, применимы к обеим линиям продуктов.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Настройка

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

Примечание: Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

Схема сети

В настоящем документе используется следующая схема сети:

Конфигурации

Эти конфигурации используются в данном документе:

- Cisco ASA 5520

- Маршрутизатор Cisco 871

Cisco ASA 5520

```
ciscoasa#show run
: Saved
:
ASA Version 7.1(1)
!
hostname ciscoasa
!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.25.171.1 255.255.0.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!--- Output is suppressed. access-list no-nat extended
permit ip 10.10.10.0 255.255.255.0 192.168.10.0
255.255.255.0 access-list ezvpn extended permit ip
10.10.10.0 255.255.255.0 192.168.10.0 255.255.255.0

access-list Split_Tunnel_List remark The corporate
network behind the ASA
access-list Split_Tunnel_List standard permit 10.10.10.0
255.255.255.0
nat (inside) 0 access-list no-nat
access-group OUT in interface outside
route outside 0.0.0.0 0.0.0.0 172.25.171.2 1
!--- Use the group-policy attributes command in !---
global configuration mode to enter the group-policy
attributes mode.

group-policy DfltGrpPolicy attributes
 banner none
 wins-server none
 dns-server none
 dhcp-network-scope none
 vpn-access-hours none
 vpn-simultaneous-logins 3
 vpn-idle-timeout 30
 vpn-session-timeout none
 vpn-filter none
 vpn-tunnel-protocol IPSec
 password-storage enable
 ip-comp disable
 re-xauth disable
 group-lock none
 pfs disable
 ipsec-udp enable
 ipsec-udp-port 10000

 split-tunnel-policy tunnelspecified
```

```
 split-tunnel-network-list value Split_Tunnel_List
 default-domain none
 split-dns none
 secure-unit-authentication disable
 user-authentication disable
 user-authentication-idle-timeout 30
 ip-phone-bypass disable
 leap-bypass disable
!--- Network Extension mode allows hardware clients to
present a single, !--- routable network to the remote
private network over the VPN tunnel. nem enable
 backup-servers keep-client-config
 client-firewall none
 client-access-rule none
username cisco password 3USUcOPFUiMCO4Jk encrypted
http server enable
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
!--- These are IPsec Phase I and Phase II parameters. !-
-- The parameters have to match in order for !--- the
IPsec tunnel to come up. crypto ipsec transform-set
mySET esp-des esp-md5-hmac
crypto dynamic-map myDYN-MAP 5 set transform-set mySET
crypto map myMAP 60 ipsec-isakmp dynamic myDYN-MAP
crypto map myMAP interface outside
isakmp identity address
isakmp enable outside
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400

tunnel-group DefaultRAGroup general-attributes
 default-group-policy DfltGrpPolicy

tunnel-group DefaultRAGroup ipsec-attributes
 pre-shared-key *

telnet timeout 5
ssh timeout 5
console timeout 0
!
: end
ciscoasa#
```

Маршрутизатор Cisco 871

```
C871#show running-config
Current configuration : 1639 bytes
!
version 12.4
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname C871
!
boot-start-marker
boot-end-marker
!
!
```

```
ip cef
!
!--- Creates a Cisco Easy VPN Remote configuration and
enters the !--- Cisco Easy VPN Remote configuration
mode. crypto ipsec client ezvpn ASA
!--- The IPsec VPN tunnel is automatically connected
when the Cisco !--- Easy VPN Remote feature is
configured on an interface. connect auto
!--- The group name should match the remote group name.
group DefaultRAGroup key cisco
!--- Specifies that the router should become a remote
extension of the !--- enterprise network at the other
end of the VPN connection. mode network-extension
!--- Sets the peer IP address or hostname for the VPN
connection. peer 172.25.171.1
!--- Specifies how the Easy VPN Client handles extended
authentication (Xauth) requests. xauth userid mode
interactive
!--- Output is suppressed. ! interface FastEthernet0 !
interface FastEthernet1 ! interface FastEthernet2 !
interface FastEthernet3 ! !--- Assigns a Cisco Easy VPN
Remote configuration to an outside interface. interface
FastEthernet4 ip address 172.30.171.1 255.255.0.0 ip
access-group 101 in no ip redirects no ip unreachables
no ip proxy-arp ip nat outside ip virtual-reassembly ip
route-cache flow duplex auto speed auto crypto ipsec
client ezvpn ASA
!
!--- Assigns a Cisco Easy VPN Rremote configuration to
an outside interface. interface Vlan1 ip address
192.168.10.1 255.255.255.0 ip access-group 100 out no ip
redirects no ip unreachables no ip proxy-arp ip nat
inside ip virtual-reassembly ip route-cache flow ip tcp
adjust-mss 1452 crypto ipsec client ezvpn ASA inside
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.30.171.2
!
!--- Enables NAT on the inside source address. ip nat
inside source route-map EzVPN1 interface FastEthernet4
overload
!
access-list 100 permit ip any any
access-list 101 permit ip any any
access-list 103 permit ip 192.168.10.0 0.0.0.255 any
!
route-map EzVPN1 permit 1
 match ip address 103
!
end
C871#
```

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. Посредством OIT можно анализировать выходные данные команд show.

После настройки обоих устройств маршрутизатор Cisco 871 попытается настроить туннель VPN, автоматически подключившись к ASA 5520 с помощью IP-адреса однорангового узла. После обмена начальными параметрами ISAKMP, маршрутизатор отображает данное сообщение:

```
Pending XAuth Request, Please enter the
 following command: crypto ipsec client ezvpn xauth
```

Необходимо ввести команду crypto ipsec client ezvpn xauth, которая запрашивает имя пользователя и пароль. Эти данные должны соответствовать имени пользователя и паролю, настроенным на ASA 5520. После подтверждения имени пользоваетля и пароля обоими узлами происходит подтверждение остальных параметров и VPN-туннель IPsec устанавливается.

```
EZVPN(ASA): Pending XAuth Request, Please enter the following command:

EZVPN: crypto ipsec client ezvpn xauth

!--- Enter the crypto ipsec client ezvpn xauth command.


crypto ipsec client ezvpn xauth

Enter Username and Password.: cisco
Password: : test
```

Используйте эти команды, чтобы проверить, правильно ли работает туннель на устройстве ASA 5520 и на маршрутизаторе Cisco 871:

- show crypto isakmp sa – отображает все текущие сопоставления безопасности IKE (SA) на одноранговом узле. Состояние QM_IDLE означает, что SA остается аутентифицированным со своим узлом и может использоваться для последующих обменов в быстром режиме.

  ```
  show crypto isakmp sa
  IPv4 Crypto ISAKMP SA
  dst             src             state          conn-id slot status
  172.25.171.1    172.30.171.1    QM_IDLE           1011    0 ACTIVE

  IPv6 Crypto ISAKMP SA
  ```

- show crypto ipsec sa — отображает настройки, используемые текущими SA. Проверьте наличие IP-адресов для однорангового узла, доступность сетей как местную, так и удаленную, а также используемый набор преобразования. Есть две SA протокола ESP, по одной в каждом направлении. Так как наборы преобразования заголовка аутентификации (AH) не используются, они пусты.

  ```
  show crypto ipsec sa

  interface: FastEthernet4
      Crypto map tag: FastEthernet4-head-0, local addr 172.30.171.1

     protected vrf: (none)
     local  ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
     remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
     current_peer 172.25.171.1 port 500
       PERMIT, flags={origin_is_acl,}
      #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.: 172.30.171.1, remote crypto endpt.: 172.25.171.1
     path mtu 1500, ip mtu 1500
     current outbound spi: 0x2A9F7252(715092562)

     inbound esp sas:
      spi: 0x42A887CB(1118341067)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 39, flow_id: C87X_MBRD:39, crypto map: FastEthernet4-head-0
        sa timing: remaining key lifetime (k/sec): (4389903/28511)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x2A9F7252(715092562)
        transform: esp-des esp-md5-hmac ,
        in use settings ={Tunnel, }
        conn id: 40, flow_id: C87X_MBRD:40, crypto map: FastEthernet4-head-0
        sa timing: remaining key lifetime (k/sec): (4389903/28503)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

- show ipsec sa – отображает настройки используемые текущими SA. Проверьте наличие IP-адресов для однорангового узла, доступность сетей как местную, так и удаленную, а также используемые наборы преобразования. Есть две SA ESP, по одной в каждом направлении.

```
ciscoasa#show ipsec sa
interface: outside
    Crypto map tag: myDYN-MAP, seq num: 5, local addr: 172.25.171.1

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0)
      current_peer: 172.30.171.1, username: cisco
      dynamic allocated peer ip: 0.0.0.0

      #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 comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.25.171.1, remote crypto endpt.: 172.30.171.1

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 42A887CB

    inbound esp sas:
      spi: 0x2A9F7252 (715092562)
         transform: esp-des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 8, crypto-map: myDYN-MAP
         sa timing: remaining key lifetime (sec): 28648
```

```
        IV size: 8 bytes
        replay detection support: Y
    outbound esp sas:
      spi: 0x42A887CB (1118341067)
        transform: esp-des esp-md5-hmac
        in use settings ={RA, Tunnel, }
        slot: 0, conn_id: 8, crypto-map: myDYN-MAP
        sa timing: remaining key lifetime (sec): 28644
        IV size: 8 bytes
        replay detection support: Y
```

- show isakmp sa-отображает все текущие SA протокола IKE на одноранговом узле. Состояние AM_ACTIVE означает, что для обмена параметрами использовался агрессивный режим.`ciscoasa#`**`show 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: 172.30.171.1
    Type    : user            Role    : responder
    Rekey   : no              State   : AM_ACTIVE
```

Устранение неполадок

Используйте этот раздел для устранения неполадок своей конфигурации.

- Диагностика маршрутизатора
- Диагностика ASA

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

Примечание: Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

Диагностика маршрутизатора

- **debug crypto isakmp-отображает согласования ISAKMP первого этапа IKE.**
- **debug crypto ipsec-отображает согласования IPsec второго этапа IKE.**

Диагностика ASA

- **debug crypto isakmp 127-отображает согласования ISAKMP первого этапа IKE.**
- **debug crypto ipsec 127-отображает согласования IPsec второго этапа IKE.**

Дополнительные сведения

- Пример конфигурации Easy VPN с ASA 5500 в качестве сервера и PIX 506E в качестве клиента (NEM)
- Поддержка устройств адаптивной безопасности Cisco ASA серии 5500
- Поддержка маршрутизаторов серии Cisco 800

- Согласование IPsec/Протоколы IKE
- Cisco Systems – техническая поддержка и документация