PIX/ASA 7.x ou posterior: Easy VPN com Split Tunneling ASA 5500 como servidor e Cisco 871 como o exemplo de configuração remota Easy VPN

Contents

Introduction

Este documento fornece uma configuração de exemplo para IPsec entre o Cisco Adaptive Security Appliance (ASA) 5520 e um roteador Cisco 871 que usa Easy VPN. O ASA 5520 atua como o Easy VPN Server e o roteador Cisco 871 atua como o Easy VPN Remote Client. Quando esta configuração usa um dispositivo ASA 5520 que executa a versão de software ASA 7.1(1), também é possível usar esta configuração para os dispositivos PIX Firewall que executam a versão do sistema operacional PIX 7.1 e posteriores.

Para configurar um roteador Cisco IOS® como um EzVPN no Network Extension Mode (NEM) que se conecta a um Cisco VPN 3000 Concentrator, consulte Configuração do Cisco EzVPN Client no Cisco IOS com o VPN 3000 Concentrator.

Para configurar o IPsec entre o Cisco IOS Easy VPN Remote Hardware Client e o PIX Easy VPN Server, consulte Exemplo de Configuração do IOS Easy VPN Remote Hardware Client para um PIX Easy VPN Server.

Para configurar um Cisco 7200 Router como um EzVPN e o Cisco 871 Router como o Easy VPN Remote, consulte Exemplo de Configuração Remota de um 7200 Easy VPN Server para 871 Easy VPN.

Prerequisites

Requirements

Certifique-se de ter uma compreensão básica dos sistemas operacionais IPsec e ASA 7.x.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- O Easy VPN Server é um ASA 5520 que executa a versão 7.1(1).
- O Easy VPN Remote Hardware Client é um roteador Cisco 871 que executa o Cisco IOS® Software Release 12.4(4)T1.

Observação: o Cisco ASA 5500 Series versão 7.x executa uma versão de software semelhante vista no PIX versão 7.x. As configurações neste documento são aplicáveis às duas linhas de produto.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

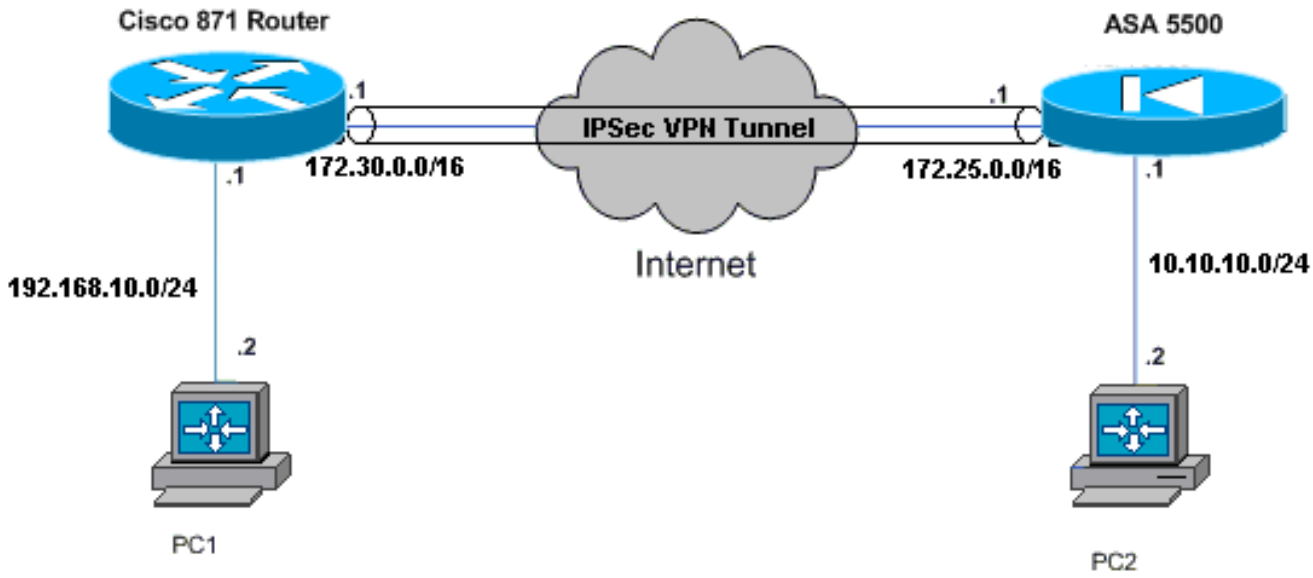
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota:Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações

Este documento utiliza as seguintes configurações:

- Cisco ASA 5520
- Cisco 871 Router

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#
```

Cisco 871 Router

```
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#
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Quando você configura ambos os dispositivos, o roteador Cisco 871 tenta configurar o túnel VPN entrando em contato com o ASA 5520 automaticamente usando o endereço IP do peer. Depois que os parâmetros ISAKMP iniciais são trocados, o roteador exibe esta mensagem:

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

Énecessário inserir o comando **crypto ipsec client ezvpn xauth**, o qual solicitará um nome de usuário e uma senha. Isso deve corresponder ao nome de usuário e à senha configurados no ASA 5520. Depois que o nome de usuário e a senha forem acordados por ambos os peers, o restante dos parâmetros serão acordados e o túnel VPN IPsec será ativado.

```
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
```

Use estes comandos para verificar se o túnel funciona corretamente no ASA 5520 e no roteador Cisco 871:

- **show crypto isakmp sa — Exibe todas as associações de segurança atuais (SAs) de IKE em um peer.** O estado QM_IDLE indica que o SA permanece autenticado com seu par e pode ser usado para trocas de modo rápido subsequentes.

```
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** —Exibe as configurações usadas pelas SAs atuais. Verifique os endereços IP dos pares, as redes acessíveis nas extremidades local e remota e o conjunto de transformações usado. Há duas SAs do protocolo de segurança de encapsulamento (ESP - Encapsulating Security Protocol), uma em cada direção. Como os conjuntos de transformação AH (Authentication Header, cabeçalho de autenticação) não são usados, ele está vazio.

```
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 — Exibe as configurações usadas pelas SAs atuais. Verifique os endereços IP dos pares, as redes acessíveis nas extremidades local e remota e os conjuntos de transformação usados. Há duas SAs ESP, uma em cada direção.

```
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 — Exibe todas as SAs IKE atuais em um peer. O estado AM_ATIVE indica que o modo Aggressive foi usado para a troca de parâmetros.

```
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
```

Troubleshoot

Use esta seção para resolver problemas de configuração.

- Solucionar problemas do roteador
- Solucionar problemas do ASA

A Output Interpreter Tool (somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.

Solucionar problemas do roteador

- **debug crypto isakmp** — Exibe as negociações ISAKMP da fase 1 do IKE.
- **debug crypto ipsec** — Exibe as negociações de IPsec da fase 2 do IKE.

Solucionar problemas do ASA

- **debug crypto isakmp 127** — Exibe as negociações ISAKMP da fase 1 do IKE.
- **debug crypto ipsec 127** —Exibe as negociações de IPsec da fase 2 de IKE.

Informações Relacionadas

- Easy VPN com um ASA 5500 como o Servidor e PIX 506E como o Exemplo de Configuração do Cliente (NEM)
- Suporte de produto dos dispositivos de segurança adaptável Cisco ASA 5500 Series
- Suporte ao produto Cisco 800 Series Routers
- Negociação IPsec/Protocolos IKE
- Suporte Técnico e Documentação - Cisco Systems