PIX/ASA 7.x en later: Makkelijk VPN met Split Tunneling ASA 5500 als server en Cisco 871 als het Makkelijk VPN-configuratievoorbeeld

Inhoud

Inleiding

Dit document biedt een voorbeeldconfiguratie voor IPsec tussen een Cisco adaptieve security applicatie (ASA) 5520 en een Cisco 871 router die Easy VPN gebruikt. ASA 5520 werkt als de Makkelijk VPN-server en Cisco 871 router werkt als de Easy VPN-externe client. Terwijl deze configuratie een ASA 5520-apparaat gebruikt dat ASA-softwareversie 7.1(1) draait, kunt u deze configuratie ook gebruiken voor PIX-firewallapparaten die PIX-besturingssysteem versie 7.1 en hoger uitvoeren.

Om een Cisco IOS® router als EzVPN in Network Extension Mode (NEM) te configureren die verbonden is met een Cisco VPN 3000 Concentrator, raadpleegt u de Cisco EzVPN-client configureren op Cisco IOS met VPN 3000 Concentrator.

Om IPsec te configureren tussen de Cisco IOS Easy VPN Remote Hardware Client en de PIX Easy VPN Server, raadpleegt u IOS Easy VPN Remote Hardware Client naar een PIX Easy VPN Server Configuratievoorbeeld.

Om Cisco 7200 router als een EzVPN en Cisco 871 router als de Easy VPN-afstandsbediening te configureren raadpleegt u 7200 Easy VPN-server aan 871 Easy VPN-afstandsconfiguratievoorbeeld.

Voorwaarden

Vereisten

Zorg ervoor dat u een basisbegrip van IPsec en de ASA 7.x besturingssystemen hebt.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- De Easy VPN Server is een ASA 5520 die versie 7.1(1) uitvoert.
- De Easy VPN Remote Hardware Client is een Cisco 871-router die Cisco IOS® softwarerelease 12.4(4)T1 draait.

Opmerking: Cisco ASA 5500 Series versie 7.x voert een soortgelijke softwareversie uit die u kunt zien in PIX versie 7.x. De configuraties in dit document zijn van toepassing op beide productlijnen.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

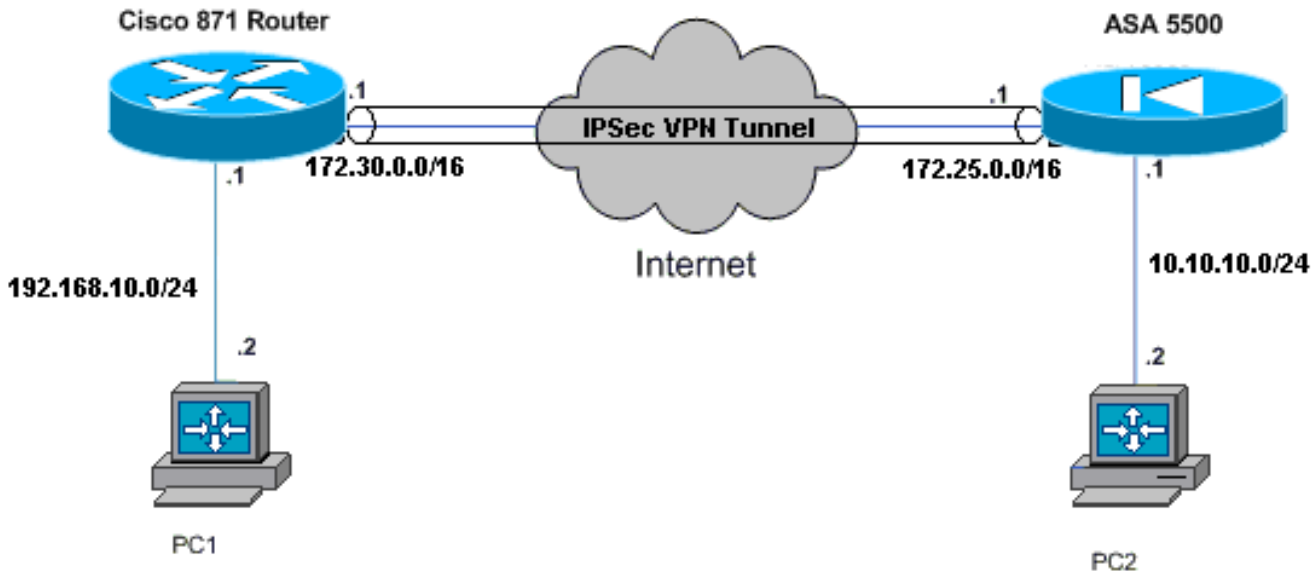
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

N.B.: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te vinden over de opdrachten die in dit document worden gebruikt.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Configuraties

Dit document gebruikt deze configuraties:

- 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#
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Zodra u beide apparaten vormt, probeert de Cisco 871-router de VPN-tunnel in te stellen door automatisch contact op te nemen met ASA 5520 en automatisch het IP-adres van de peer te gebruiken. Nadat de eerste ISAKMP-parameters zijn uitgewisseld, geeft de router dit bericht weer:

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

U moet de opdracht **crypto ipsec client ezvpn xauth** invoeren die u om een gebruikersnaam en wachtwoord vraagt. Dit moet overeenkomen met de gebruikersnaam en het wachtwoord die in de ASA 5520 zijn ingesteld. Zodra de gebruikersnaam en het wachtwoord door beide peers zijn overeengekomen, wordt de rest van de parameters overeengekomen en komt de IPsec VPN-tunnel naar boven.

```
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
```

Gebruik deze opdrachten om te controleren of de tunnel goed werkt op zowel de ASA 5520-router als de Cisco 871-router:

- toon crypto isakmp sa-Toont alle huidige IKE security associaties (SAs) bij een peer. De staat QM_IDLE wijst erop dat de SA authentiek blijft met zijn peer en kan worden gebruikt voor daaropvolgende snelle mode uitwisselingen.

```
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
```

- Laat crypto ipsec sa-displays de instellingen die worden gebruikt door huidige SA's. Controleer voor de peer IP adressen, de netwerken toegankelijk op zowel de lokale als verre eindpunten, en de transformatie die wordt gebruikt. Er zijn twee ESP's (Encapsulation Security Protocol), één in elke richting. Aangezien geen transformatietekens (AH) worden gebruikt, is deze leeg.

```
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:
```

- Laat ipsec sa-displays de instellingen die worden gebruikt door de huidige SA's. Controleer voor de peer IP adressen, de netwerken die bij zowel de lokale als verre eindjes toegankelijk zijn en de transformatiesets die worden gebruikt. Er zijn twee ESP SA's, één in elke richting.

```
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
```

- Laat isakmp sa-displays alle huidige IKE SA's zien bij een peer. De status AM_ACTIVE geeft aan dat de aggregatiemodus is gebruikt voor de uitwisseling van parameters.

```
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
```

Problemen oplossen

Gebruik dit gedeelte om de configuratie van het probleem op te lossen.

- Probleemoplossing van de router
- Probleemoplossing voor de ASA

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten gebruikt.

Probleemoplossing van de router

- **debug crypto isakmp** — Hiermee geeft u de ISAKMP-onderhandelingen van IKE fase 1 weer.
- **debug crypto ipsec**-displays de IPsec-onderhandelingen van IKE fase 2.

Probleemoplossing voor de ASA

- **debug crypto isakmp 127** — Hiermee geeft u de ISAKMP-onderhandelingen van IKE fase 1 weer.
- **debug crypto ipsec 127**-displays de IPsec onderhandelingen van IKE fase 2.

Gerelateerde informatie

- Makkelijk VPN met een ASA 5500 als server en PIX 506E als het configuratievoorbeeld van de client (NEM)
- Cisco ASA 5500 Series productondersteuning voor adaptieve security applicaties
- Cisco 800 Series productondersteuning voor routers
- IPsec-onderhandeling/IKE-protocollen
- Technische ondersteuning en documentatie – Cisco Systems