PIX/ASA 7.x und höher: Easy VPN mit Split Tunneling der ASA 5500 als Server und Cisco 871 als Easy VPN-Remote-Konfigurationsbeispiel

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für IPsec zwischen einer Cisco Adaptive Security Appliance (ASA) 5520 und einem Cisco Router 871 mit Easy VPN. Die ASA 5520 fungiert als Easy VPN-Server, und der Cisco 871-Router fungiert als Easy VPN Remote Client. Bei dieser Konfiguration wird ein ASA 5520-Gerät verwendet, auf dem die ASA-Software Version 7.1(1) ausgeführt wird. Sie können diese Konfiguration jedoch auch für PIX-Firewall-Geräte verwenden, auf denen das PIX-Betriebssystem Version 7.1 und höher ausgeführt wird.

Informationen zur Konfiguration eines Cisco IOS®-Routers als EzVPN im Network Extension Mode (NEM), der mit einem Cisco VPN 3000-Concentrator verbunden wird, finden Sie unter Konfigurieren des Cisco EzVPN-Clients auf Cisco IOS mit dem VPN 3000-Concentrator.

Informationen zum Konfigurieren von IPsec zwischen dem Cisco IOS Easy VPN Remote Hardware Client und dem PIX Easy VPN Server finden Sie unter IOS Easy VPN Remote Hardware Client in einem Konfigurationsbeispiel für einen PIX Easy VPN Server.

Informationen zur Konfiguration eines Cisco 7200-Routers als EzVPN und des Cisco 871-Routers als Easy VPN-Remote finden Sie im Konfigurationsbeispiel für den Easy VPN-Server 7200 zu 871 Easy VPN Remote.

Voraussetzungen

Anforderungen

Vergewissern Sie sich, dass Sie über grundlegende Kenntnisse der Betriebssysteme IPsec und ASA 7.x verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Der Easy VPN-Server ist eine ASA 5520, die Version 7.1(1) ausführt.
- Der Easy VPN Remote Hardware Client ist ein Cisco 871 Router, auf dem die Cisco IOS® Software Version 12.4(4)T1 ausgeführt wird.

Hinweis: Die Cisco Serie ASA 5500, Version 7.x, führt eine ähnliche Softwareversion aus wie die Version 7.x von PIX. Die Konfigurationen in diesem Dokument gelten für beide Produktlinien.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

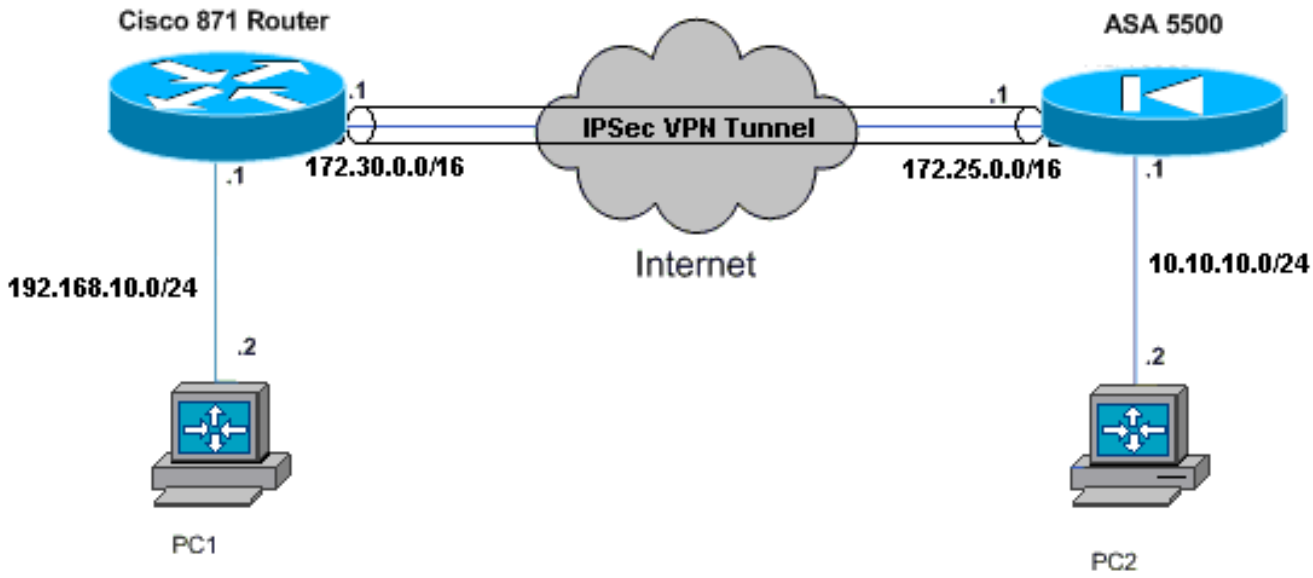
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

- Cisco ASA 5520
- Cisco Router 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#
```

Cisco Router 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#
```

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Sobald Sie beide Geräte konfigurieren, versucht der Cisco 871 Router, den VPN-Tunnel einzurichten, indem er die ASA 5520 automatisch über die Peer-IP-Adresse kontaktiert. Nachdem die ursprünglichen ISAKMP-Parameter ausgetauscht wurden, zeigt der Router die folgende Meldung an:

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

Sie müssen den Befehl **crypto ipsec client ezvpn xauth** eingeben, der Sie zur Eingabe von Benutzername und Kennwort auffordert. Dies muss mit dem auf der ASA 5520 konfigurierten Benutzernamen und Kennwort übereinstimmen. Sobald Benutzername und Kennwort von beiden Peers vereinbart wurden, werden die übrigen Parameter vereinbart und der IPsec-VPN-Tunnel aktiviert.

```
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
```

Verwenden Sie diese Befehle, um zu überprüfen, ob der Tunnel sowohl auf dem ASA 5520- als auch dem Cisco 871-Router ordnungsgemäß funktioniert:

- show crypto isakmp sa: Zeigt alle aktuellen IKE-Sicherheitszuordnungen (SAs) in einem Peer an. Der QM_IDLE-Status gibt an, dass die SA mit ihrem Peer authentifiziert bleibt und für spätere Schnellwechselvorgänge verwendet werden kann.

```
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: Zeigt die von aktuellen SAs verwendeten Einstellungen an. Prüfen Sie, ob die Peer-IP-Adressen, die Netzwerke, auf die sowohl die lokalen als auch die Remote-Endgeräte zugreifen können, und das verwendete Transformationssatz verwendet werden. Es gibt zwei ESP-SAs (Encapsulating Security Protocol), eine in jede Richtung. Da keine Authentifizierungs-Header (AH)-Transformationssätze verwendet werden, sind diese leer.

```
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: Zeigt die von aktuellen SAs verwendeten Einstellungen an. Prüfen Sie, ob die Peer-IP-Adressen, die Netzwerke, auf die sowohl die lokalen als auch die Remote-Endgeräte zugreifen können, und die verwendeten Transformationssätze vorhanden sind. Es gibt zwei ESP-SAs, eine in jede Richtung.

```
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: Zeigt alle aktuellen IKE-SAs in einem Peer an. Der Status AM_ACTIVE gibt an, dass für den Austausch von Parametern der aggressive Modus verwendet wurde.

```
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
```

Fehlerbehebung

In diesem Abschnitt finden Sie eine Fehlerbehebung für Ihre Konfiguration.

- Fehlerbehebung beim Router
- Fehlerbehebung bei der ASA

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

Fehlerbehebung beim Router

- **debug crypto isakmp**: Zeigt die ISAKMP-Verhandlungen für IKE Phase 1 an.
- **debug crypto ipsec**: Zeigt die IPsec-Aushandlungen für IKE Phase 2 an.

Fehlerbehebung bei der ASA

- **debug crypto isakmp 127**: Zeigt die ISAKMP-Verhandlungen für IKE Phase 1 an.
- **debug crypto ipsec 127**: Zeigt die IPsec-Verhandlungen für IKE Phase 2 an.

Zugehörige Informationen

- Easy VPN mit ASA 5500 als Server und PIX 506E als Client (NEM) - Konfigurationsbeispiel
- Produkt-Support für Cisco Adaptive Security Appliances der Serie ASA 5500
- Produktsupport für Cisco Router der Serie 800
- IPSec-Aushandlung/IKE-Protokolle
- Technischer Support und Dokumentation - Cisco Systems