

Conexión VPN con el ejemplo de configuración Zona-basado del router de escudo de protección

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

[Introducción](#)

Este documento proporciona una configuración de muestra donde se explica cómo configurar un router con un firewall basado zona que se utiliza también como gateway de VPN de acceso remoto.

[prerrequisitos](#)

[Requisitos](#)

No hay requisitos específicos para este documento.

[Componentes Utilizados](#)

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Router 1721 del Cisco IOS
- Versión 12.4T del Cisco IOS ® Software y posterior

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

[Convenciones](#)

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

[Antecedentes](#)

los Firewall Zona-basados de la directiva implementan las políticas del firewall unidireccionales entre los grupos de interfaces conocidas como zonas. Éstos examinan la fuente y las Zonas de destino del ingreso y de las interfaces de egreso para las políticas del firewall.

En el escenario actual, el Firewall Zona-basado se configura en el router del gateway de VPN. Permite el tráfico VPN de Internet (zona del exterior) a la zona del uno mismo. La interfaz de plantilla virtual se hace como parte de la zona de Seguridad. La red interna tiene un servidor que los usuarios en Internet puedan accederlos una vez estén conectados con el VPN de acceso remoto que termina en el router del gateway de VPN.

- Dirección IP del servidor interno — 172.16.10.20
- Dirección IP del cliente remoto PC — 192.168.100.10

No prohíben todos los usuarios en la red interna el acceso sin restricciones a Internet. Todo el tráfico de los usuarios internos se examina en el paso a través del router.

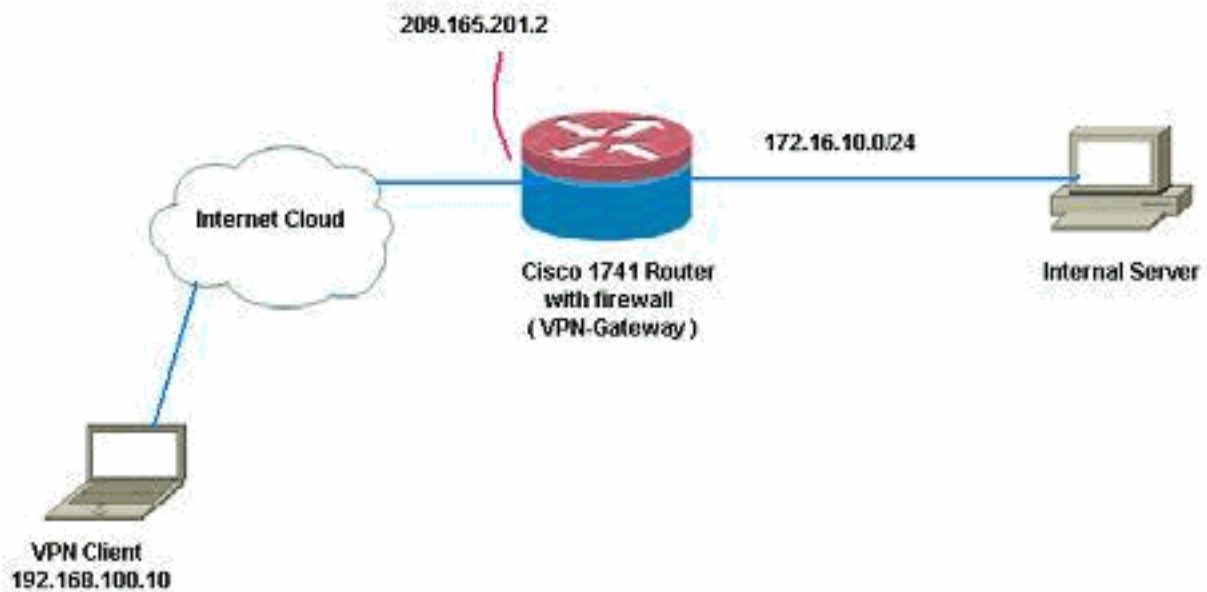
[Configurar](#)

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta [Command Lookup Tool](#) ([clientes registrados solamente](#)) para obtener más información sobre los comandos utilizados en esta sección.

[Diagrama de la red](#)

En este documento, se utiliza esta configuración de red:



Configuraciones

En este documento, se utilizan estas configuraciones:

Gateway de VPN

```

VPN-Gateway#show run
Building configuration...

Current configuration : 3493 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname VPN-Gateway
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
!--- Define local authentication aaa authentication
login default local
aaa authorization network default local
!
!--- Output suppressed !! --- Define the isakmp
policy parameters crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
!
crypto isakmp key cisco123 address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 10
!
!--- Define the group policy information crypto isakmp
client configuration group cisco
  key cisco

```

```
dns 6.0.0.2
wins 7.0.0.1
domain cisco.com
pool dpool
acl 101
!!-- Define the ISAKMP profile crypto isakmp profile vi
  match identity group cisco
  isakmp authorization list default
  client configuration address respond
  virtual-template 1
!
!!-- Define the transform-set parameters crypto ipsec
transform-set set esp-3des esp-sha-hmac
!
!!-- Define the IPSec profile crypto ipsec profile vi
set transform-set set
set isakmp-profile vi
!
!
!
!
!!-- Define the local username and password username
cisco privilege 15 password 0 cisco
archive
  log config
  hidekeys
!
!
!!-- Define the Zone based firewall Class maps class-
map type inspect match-any Internet-cmap
  match protocol icmp
  match protocol tcp
  match protocol udp
  match protocol http
  match protocol https
  match protocol pop3
  match protocol pop3s
  match protocol smtp
class-map type inspect match-all ICMP-cmap
  match access-group name ICMP
class-map type inspect match-all IPSEC-cmap
  match access-group name ISAKMP_IPSEC
class-map type inspect match-all SSHaccess-cmap
  match access-group name SSHaccess
!
!!-- Define the Zone based firewall Policy maps policy-
map type inspect inside-outside-pmap
  class type inspect Internet-cmap
  inspect
  class type inspect ICMP-cmap
  inspect
  class class-default
  drop
policy-map type inspect outside-inside-pmap
  class type inspect ICMP-cmap
  inspect
  class class-default
  drop
policy-map type inspect Outside-Router-pmap
  class type inspect SSHaccess-cmap
  inspect
  class type inspect ICMP-cmap
  inspect
```

```

class type inspect IPSEC-cmap
  pass
class class-default
  drop
!
!!--- Define zones zone security inside
zone security outside
!
!!--- Define zone-pairs zone-pair security inside-to-
outside source inside destination outside
  service-policy type inspect inside-outside-pmap
zone-pair security outside-to-router source outside
destination self
  service-policy type inspect Outside-Router-pmap
zone-pair security outside-to-inside source outside
destination inside
  service-policy type inspect outside-inside-pmap
!
!
!
interface Ethernet0
  ip address 172.16.10.20 255.255.255.0
!!--- Define interface as part of inside zone zone-
member security inside
  half-duplex
!
interface FastEthernet0
  ip address 209.165.201.2 255.255.255.224
!!--- Define interface as part of outside zone zone-
member security outside
  speed auto
!
interface Virtual-Templatel type tunnel
  ip unnumbered FastEthernet0
!!--- Define interface as part of outside zone zone-
member security outside
  tunnel source FastEthernet0
  tunnel mode ipsec ipv4
  tunnel protection ipsec profile vi
!
!!--- Define the local pool range ip local pool dpool
5.0.0.1 5.0.0.3 !! --- Output suppressed ! ip access-
list extended ICMP permit icmp any any echo permit icmp
any any echo-reply permit icmp any any traceroute ! ip
access-list extended ISAKMP_IPSEC permit udp any any eq
isakmp permit ahp any any permit esp any any permit udp
any any eq non500-isakmp ! ip access-list extended
SSHaccess permit tcp any any eq 22 ! access-list 101
permit ip 172.16.10.0 0.0.0.255 any ! ! ! control-plane
! ! line con 0 line aux 0 line vty 0 4 ! end

```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

[La herramienta Output Interpreter Tool \(clientes registrados solamente\)](#) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

1. Utilice este comando para verificar el estatus de la interfaz.VPN-Gateway#`show ip interface brief`

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0	172.16.10.20	YES	NVRAM	up	up
FastEthernet0	209.165.201.2	YES	NVRAM	up	up
Virtual-Access1	unassigned	YES	unset	down	down
Virtual-Access2	209.165.201.2	YES	TFTP	up	up
Virtual-Template1	209.165.201.2	YES	TFTP	down	down

2. Utilice este comando para verificar el estado del túnel ISAKMP.VPN-Gateway#**show crypto isakmp sa**

```
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status
209.165.201.2 192.168.100.10 QM_IDLE          1001    0 ACTIVE
```

IPv6 Crypto ISAKMP SA

3. Utilice este comando para verificar el estado de los socketes crypto.VPN-Gateway#**show crypto socket**

Number of Crypto Socket connections 1

```
Vi2 Peers (local/remote): 209.165.201.2/192.168.100.10
Local Ident (addr/mask/port/prot): (0.0.0.0/0.0.0.0/0/0)
Remote Ident (addr/mask/port/prot): (5.0.0.1/255.255.255.255/0/0)
IPSec Profile: "vi"
Socket State: Open
Client: "TUNNEL SEC" (Client State: Active)
```

Crypto Sockets in Listen state:

Client: "TUNNEL SEC" Profile: "vi" Map-name: "Virtual-Template1-head-0"

4. Verifique a los grupos activos en el router.VPN-Gateway#**show crypto session summary detail**

Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, X - IKE Extended Authentication

Interface: Virtual-Access2

Profile: vi

Group: cisco

Assigned address: 5.0.0.1

Uptime: 00:13:52

Session status: UP-ACTIVE

Peer: 192.168.100.10 port 1069 fvrf: (none) ivrf: (none)

Phase1_id: cisco

Desc: (none)

IKE SA: local 209.165.201.2/500 remote 192.168.100.10/1069 Active

Capabilities:CD connid:1001 lifetime:23:46:05

IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 5.0.0.1

Active SAs: 2, origin: crypto map

Inbound: #pkts dec'ed 10 drop 0 life (KB/Sec) 4520608/2767

Outbound: #pkts enc'ed 10 drop 0 life (KB/Sec) 4520608/2767

5. Utilice este comando para visualizar el tiempo de ejecución examinan las estadísticas de la correspondencia de políticas del tipo.VPN-Gateway#**show policy-map type inspect zone-pair**

Zone-pair: inside-to-outside

Service-policy inspect : inside-outside-pmap

Class-map: Internet-cmap (match-any)

Match: protocol icmp

0 packets, 0 bytes

30 second rate 0 bps

Match: protocol tcp

0 packets, 0 bytes

30 second rate 0 bps

Match: protocol udp

```
    0 packets, 0 bytes
    30 second rate 0 bps
Match: protocol http
    0 packets, 0 bytes
    30 second rate 0 bps
Match: protocol https
    0 packets, 0 bytes
    30 second rate 0 bps
Match: protocol pop3
    0 packets, 0 bytes
    30 second rate 0 bps
Match: protocol pop3s
    0 packets, 0 bytes
    30 second rate 0 bps
Match: protocol smtp
    0 packets, 0 bytes
    30 second rate 0 bps
Inspect
  Session creations since subsystem startup or last reset 0
  Current session counts (estab/half-open/terminating) [0:0:0]
  Maxever session counts (estab/half-open/terminating) [0:0:0]
  Last session created never
  Last statistic reset never
  Last session creation rate 0
  Maxever session creation rate 0
  Last half-open session total 0

Class-map: ICMP-cmap (match-all)
  Match: access-group name ICMP
  Inspect
    Session creations since subsystem startup or last reset 0
    Current session counts (estab/half-open/terminating) [0:0:0]
    Maxever session counts (estab/half-open/terminating) [0:0:0]
    Last session created never
    Last statistic reset never
    Last session creation rate 0
    Maxever session creation rate 0
    Last half-open session total 0

Class-map: class-default (match-any)
  Match: any
  Drop
    0 packets, 0 bytes
Zone-pair: outside-to-router

Service-policy inspect : Outside-Router-pmap

Class-map: SSHaccess-cmap (match-all)
  Match: access-group name SSHaccess
  Inspect
    Session creations since subsystem startup or last reset 0
    Current session counts (estab/half-open/terminating) [0:0:0]
    Maxever session counts (estab/half-open/terminating) [0:0:0]
    Last session created never
    Last statistic reset never
    Last session creation rate 0
    Maxever session creation rate 0
    Last half-open session total 0

Class-map: ICMP-cmap (match-all)
  Match: access-group name ICMP
  Inspect
    Packet inspection statistics [process switch:fast switch]
    icmp packets: [93:0]
```

```
Session creations since subsystem startup or last reset 6
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [0:2:0]
Last session created 00:07:02
Last statistic reset never
Last session creation rate 0
Maxever session creation rate 2
Last half-open session total 0
```

Class-map: IPSEC-cmap (match-all)

```
Match: access-group name ISAKMP_IPSEC
Pass
57 packets, 7145 bytes
```

Class-map: class-default (match-any)

```
Match: any
Drop
2 packets, 44 bytes
```

Zone-pair: outside-to-inside

Service-policy inspect : outside-inside-pmap

Class-map: ICMP-cmap (match-all)

```
Match: access-group name ICMP
Inspect
Packet inspection statistics [process switch:fast switch]
icmp packets: [1:14]
```

```
Session creations since subsystem startup or last reset 2
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [1:1:0]
Last session created 00:09:15
Last statistic reset never
Last session creation rate 0
Maxever session creation rate 1
Last half-open session total 0
```

Class-map: class-default (match-any)

```
Match: any
Drop
0 packets, 0 bytes
```

6. Utilice el ping para verificar la Conectividad al servidor interno.E:\Documents and Settings\Administrator>**ping 172.16.10.20**

Pinging 172.16.10.20 with 32 bytes of data:

```
Reply from 172.16.10.20: bytes=32 time=206ms TTL=254
Reply from 172.16.10.20: bytes=32 time=63ms TTL=254
Reply from 172.16.10.20: bytes=32 time=20ms TTL=254
Reply from 172.16.10.20: bytes=32 time=47ms TTL=254
```

Ping statistics for 172.16.10.20:

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 20ms, Maximum = 206ms, Average = 84ms
```

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- [Cisco IOS Firewall](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)