# 通过基于区域的防火墙路由器进行 VPN 连接的配置示例

## 目录



## 简介

本文档提供了一个配置示例，说明如何使用基于区域的防火墙（同时还可充当远程访问 VPN 网关）来配置路由器。

## 先决条件

### 要求

本文档没有任何特定的要求。

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS 路由器 1721
- Cisco IOS软件版本12.4T和以后

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

### 规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

# 背景信息

基于区域的策略防火墙在称为区域的接口组之间实施单向防火墙策略。这些防火墙用于检查输入和输出接口的源区域和目的地区域是否实施了防火墙策略。

在当前情景中，基于区域的防火墙已配置到 VPN 网关路由器上。它允许从 Internet（外部区域）到自身区域的 VPN 流量通过。虚拟模板接口可作为安全区域的一部分。内部网络中有一个服务器，Internet 上的用户在通过远程访问 VPN（终止于 VPN 网关路由器）建立连接后可以访问该服务器。

- 内部服务器的 IP 地址 - 172.16.10.20
- 远程客户端 PC 的 IP 地址 - 192.168.100.10

允许内部网络的所有用户对 Internet 进行无限制的访问。来自内部用户的所有数据流在通过路由器时都要经过检查。

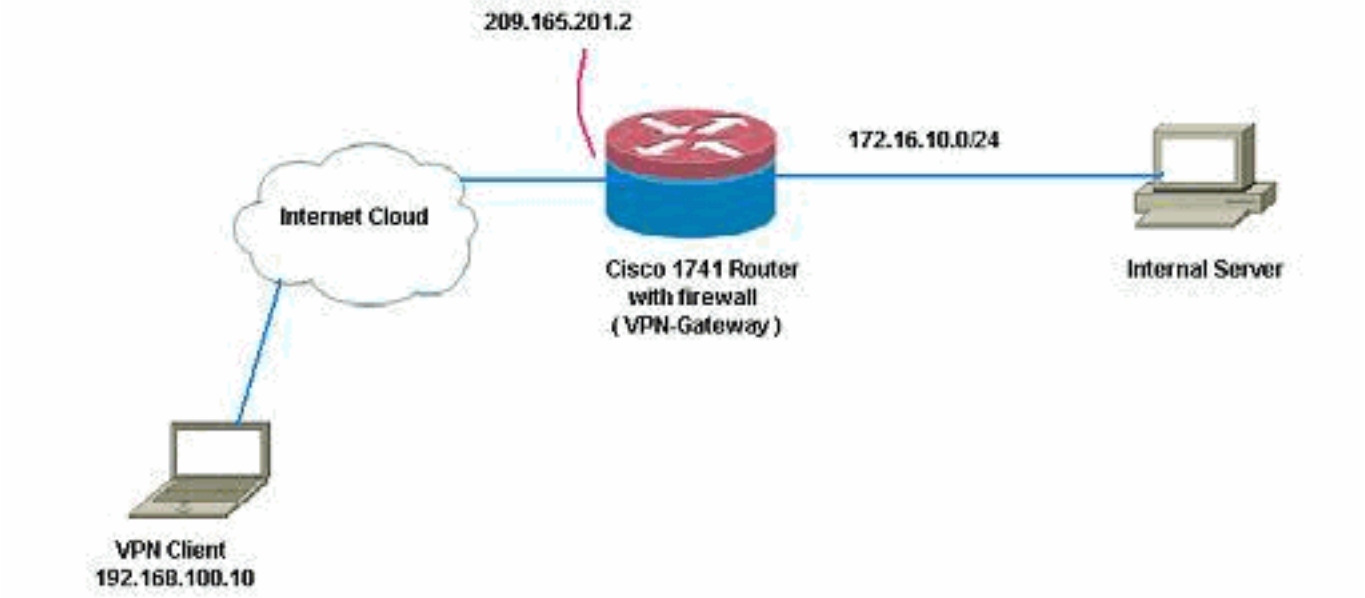
# 配置

本部分提供有关如何配置本文档所述功能的信息。

**注意：** 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

## 网络图

本文档使用以下网络设置：




## 配置

本文档使用以下配置：

| VPN 网关 |
| --- |
| 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-Template1 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
```

# 验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

1. 请使用此命令来验证接口状态。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. 请使用此命令来验证 ISAKMP 隧道状态。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. 请使用此命令来验证加密套接字的状态。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. 验证路由器上的活动组。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. 请使用此命令来显示运行时检查类型策略映射统计数据。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. 请使用 ping 来验证与内部服务器的连接。`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
```

## 故障排除

目前没有针对此配置的故障排除信息。

## 相关信息

- Cisco IOS 防火墙
- 技术支持和文档 - Cisco Systems