# Índice



## Introdução

Este documento fornece uma configuração de exemplo que demonstra como configurar um roteador com o Firewall baseado zona que igualmente serve como o gateway de VPN remoto-acess.

## Pré-requisitos

### Requisitos

Não existem requisitos específicos para este documento.

### Componentes Utilizados

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

- Roteador 1721 do Cisco IOS
- Liberação 12.4T do Cisco IOS ® Software e mais tarde

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

### Convenções

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

## Informações de Apoio

os Firewall Zona-baseados da política executam a política de firewall unidirecional entre grupos

de relações conhecidas como zonas. Estes examinam a fonte e as zonas de destino do ingresso e das interfaces de saída para uma política de firewall.

Na encenação atual, o Firewall Zona-baseado é configurado no roteador do gateway de VPN. Permite o tráfego VPN do Internet (zona da parte externa) à zona do auto. A interface de molde virtual é feita como parte da zona de Segurança. A rede interna tem um server que os usuários no Internet possam os alcançar uma vez sejam conectados com o acesso remoto VPN que termina no roteador do gateway de VPN.

- Endereço IP de Um ou Mais Servidores Cisco ICM NT do server?172.16.10.20 interno
- Endereço IP de Um ou Mais Servidores Cisco ICM NT do cliente remoto PC?192.168.100.10

O acesso irrestrito é permitido a todos os usuários na rede interna ao Internet. Todo o tráfego dos usuários internos é inspecionado na passagem através do roteador.

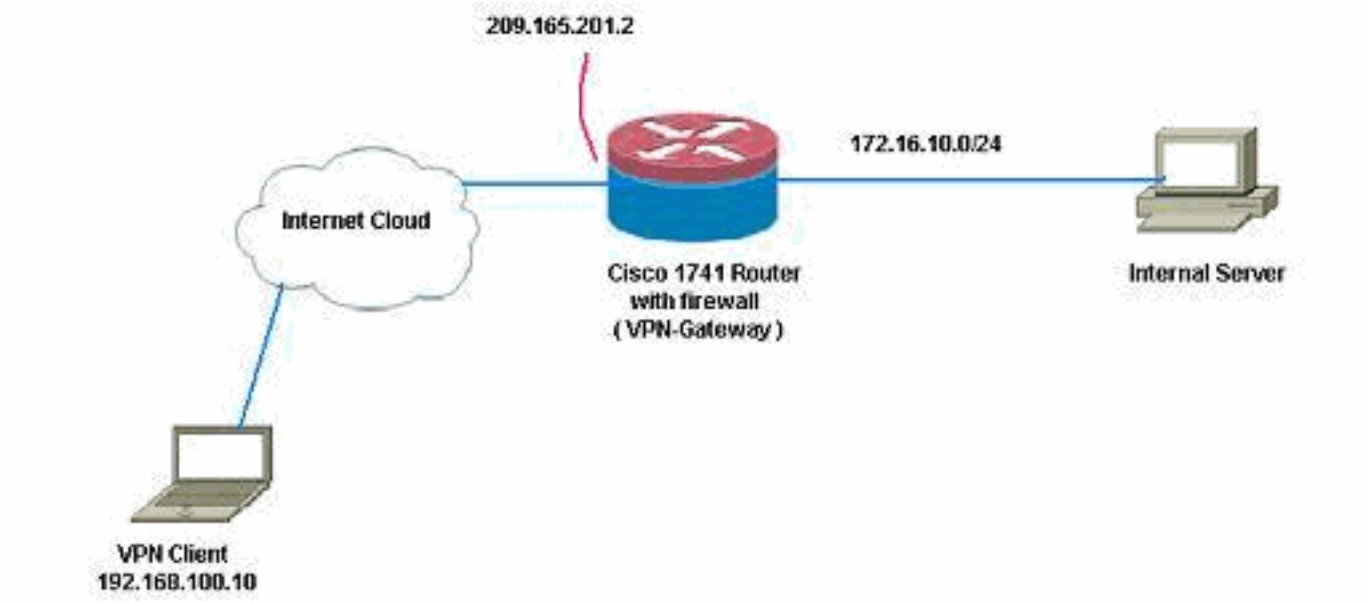
# Configurar

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 nesta seção.

## Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:




## Configurações

Este documento utiliza as seguintes configurações:

| Gateway de VPN |
| --- |
| VPN-Gateway#**show run**Building configuration...Current |

```
configuration : 3493 bytes!version 12.4service
timestamps debug datetime msecservice timestamps log
datetime msecno service password-encryption!hostname
VPN-Gateway!boot-start-markerboot-end-marker!!aaa new-
model!!!--- Define local authentication aaa
authentication login default localaaa authorization
network default local !!!--- Output suppressed! !!---
Define the isakmp policy parameterscrypto isakmp policy
1 encr 3des authentication pre-share group 2!crypto
isakmp key cisco123 address 0.0.0.0 0.0.0.0crypto isakmp
keepalive 10!!!--- Define the group policy
informationcrypto 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
profilecrypto isakmp profile vi   match identity group
cisco   isakmp authorization list default   client
configuration address respond   virtual-template 1!!!---
Define the transform-set parameterscrypto ipsec
transform-set set esp-3des esp-sha-hmac !!!--- Define
the IPSec profilecrypto ipsec profile vi set transform-
set set  set isakmp-profile vi!!!!!!!--- Define the
local username and passwordusername cisco privilege 15
password 0 ciscoarchive log config  hidekeys!!!!---
Define the Zone based firewall Class mapsclass-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 smtpclass-map type inspect
match-all ICMP-cmap match access-group name ICMPclass-
map type inspect match-all IPSEC-cmap match access-group
name ISAKMP_IPSECclass-map type inspect match-all
SSHaccess-cmap match access-group name SSHaccess!!!---
Define the Zone based firewall Policy mapspolicy-map
type inspect inside-outside-pmap class type inspect
Internet-cmap  inspect class type inspect ICMP-cmap
inspect class class-default  droppolicy-map type inspect
outside-inside-pmap class type inspect ICMP-cmap
inspect class class-default  droppolicy-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 zoneszone security insidezone security
outside!!!--- Define zone-pairszone-pair security
inside-to-outside source inside destination outside
service-policy type inspect inside-outside-pmapzone-pair
security outside-to-router source outside destination
self service-policy type inspect Outside-Router-
pmapzone-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 rangeip
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 0line aux 0line vty 0
4!end
```

# Verificar

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

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

1. Use este comando a fim verificar o status da interface.`VPN-Gateway#`**`show ip interface brief`**`Interface IP-Address OK? Method Status ProtocolEthernet0 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. Use este comando a fim verificar o status de túnel ISAKMP.`VPN-Gateway#`**`show crypto isakmp sa`**`IPv4 Crypto ISAKMP SAdst src state conn-id slot status209.165.201.2 192.168.100.10` **`QM_IDLE`** `1001 0` **`ACTIVE`**`IPv6 Crypto ISAKMP SA`
3. Use este comando a fim verificar o estado de soquetes criptos.`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 os grupos ativos no roteador.`VPN-Gateway#`**`show crypto session summary detail`**`Crypto session current statusCode: C - IKE Configuration mode, D - Dead Peer Detection K - Keepalives, N - NAT-traversal, X - IKE Extended Authentication` **`Interface: Virtual-Access2Profile: viGroup: cisco`**`Assigned address: 5.0.0.1` **`Uptime: 00:13:52Session 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. Use este comando a fim indicar o tempo de execução inspecionam o tipo estatísticas do mapa de política.`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. Use o sibilo a fim verificar a Conectividade ao servidor interno.
```
E:\Documents and
Settings\Administrator>ping 172.16.10.20Pinging 172.16.10.20 with 32 bytes of data:Reply
from 172.16.10.20: bytes=32 time=206ms TTL=254Reply from 172.16.10.20: bytes=32 time=63ms
TTL=254Reply from 172.16.10.20: bytes=32 time=20ms TTL=254Reply from 172.16.10.20: bytes=32
time=47ms TTL=254Ping 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

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

# Informações Relacionadas

- Cisco IOS Firewall
- Suporte Técnico e Documentação - Cisco Systems