

Exemple de configuration de connexion VPN via un routeur de pare-feu basé sur une zone

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Informations générales](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

[Introduction](#)

Ce document fournit une configuration d'échantillon qui explique comment configurer un routeur avec le Pare-feu basé par zone qui servent également de passerelle VPN de distant-access.

[Conditions préalables](#)

[Conditions requises](#)

Aucune spécification déterminée n'est requise pour ce document.

[Composants utilisés](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Routeur Cisco IOS 1721
- Version de logiciel 12.4T et ultérieures de Cisco IOS®

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Informations générales

les Pare-feu basés sur zone de stratégie implémentent la stratégie unidirectionnelle de Pare-feu entre les groupes d'interfaces connues sous le nom de zones. Ceux-ci examinent la source et les zones de destination du d'entrée et des interfaces de sortie pour une stratégie de Pare-feu.

Dans le scénario en cours, le Pare-feu basé sur zone est configuré sur le routeur de passerelle VPN. Il permet le trafic VPN de l'Internet (zone d'extérieur) à la zone d'individu. L'interface de modèle virtuel est faite en tant qu'élément de la zone de Sécurité. Le réseau interne a un serveur que les utilisateurs sur l'Internet peuvent les accéder à une fois sont connectés par l'Accès à distance VPN qui se termine sur le routeur de passerelle VPN.

- Adresse IP du serveur interne — 172.16.10.20
- Adresse IP du PC de client distant — 192.168.100.10

Tous les utilisateurs sur le réseau interne on un accès à Internet sans restriction. Tout le trafic des utilisateurs internes est examiné sur traverser le routeur.

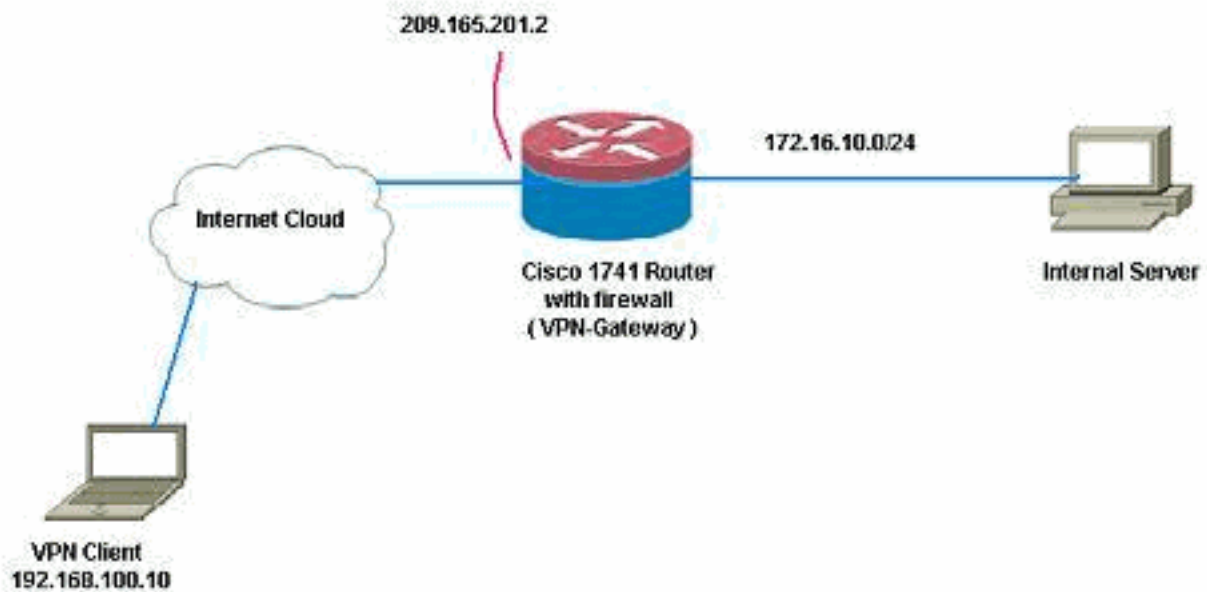
Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Utilisez l'outil [Command Lookup Tool](#) (clients [enregistrés](#) seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

Ce document utilise les configurations suivantes :

Passerelle 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

```

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'[Outil Interpréteur de sortie](#) (clients [enregistrés](#) uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show**.

1. Employez cette commande afin de vérifier l'état d'interface.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-Templat1	209.165.201.2	YES	TFTP	down	down

2. Employez cette commande afin de vérifier l'état de tunnel d'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. Employez cette commande afin de vérifier l'état de cryptos sockets.
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-Templat1-head-0"

4. Vérifiez les groupes actifs sur le routeur.
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. Employez cette commande afin d'afficher le délai d'exécution examen des statistiques de carte de stratégie de type.
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. Employez le ping afin de vérifier la Connectivité au serveur interne.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
```

[Dépannez](#)

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- [Cisco IOS Firewall](#)
- [Support et documentation techniques - Cisco Systems](#)