영역 기반 방화벽 라우터 컨피그레이션을 통한 VPN 연결 예

목차

소개

이 문서에서는 원격 액세스 VPN 게이트웨이 역할을 하는 영역 기반 방화벽으로 라우터를 구성하는 방법을 보여 주는 샘플 컨피그레이션을 제공합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS Router 1721
- Cisco IOS® Software 릴리스 12.4T 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

영역 기반 정책 방화벽은 영역으로 알려진 인터페이스 그룹 간에 단방향 방화벽 정책을 구현합니다 .인그레스 및 이그레스 인터페이스의 소스 및 대상 영역에서 방화벽 정책을 검사합니다.

현재 시나리오에서는 VPN-Gateway 라우터에 영역 기반 방화벽이 구성됩니다.또한 인터넷(외부 영역)에서 자체 영역으로 VPN 트래픽을 허용합니다.가상 템플릿 인터페이스는 보안 영역의 일부로 만들어집니다.내부 네트워크에는 VPN-Gateway 라우터에서 종료되는 원격 액세스 VPN을 통해 연결되면 인터넷 사용자가 액세스할 수 있는 서버가 있습니다.

- 내부 서버의 IP 주소 - 172.16.10.20
- 원격 클라이언트 PC의 IP 주소 - 192.168.100.10

내부 네트워크의 모든 사용자는 인터넷에 무제한 액세스할 수 있습니다.내부 사용자의 모든 트래픽은 라우터를 통과하여 검사됩니다.

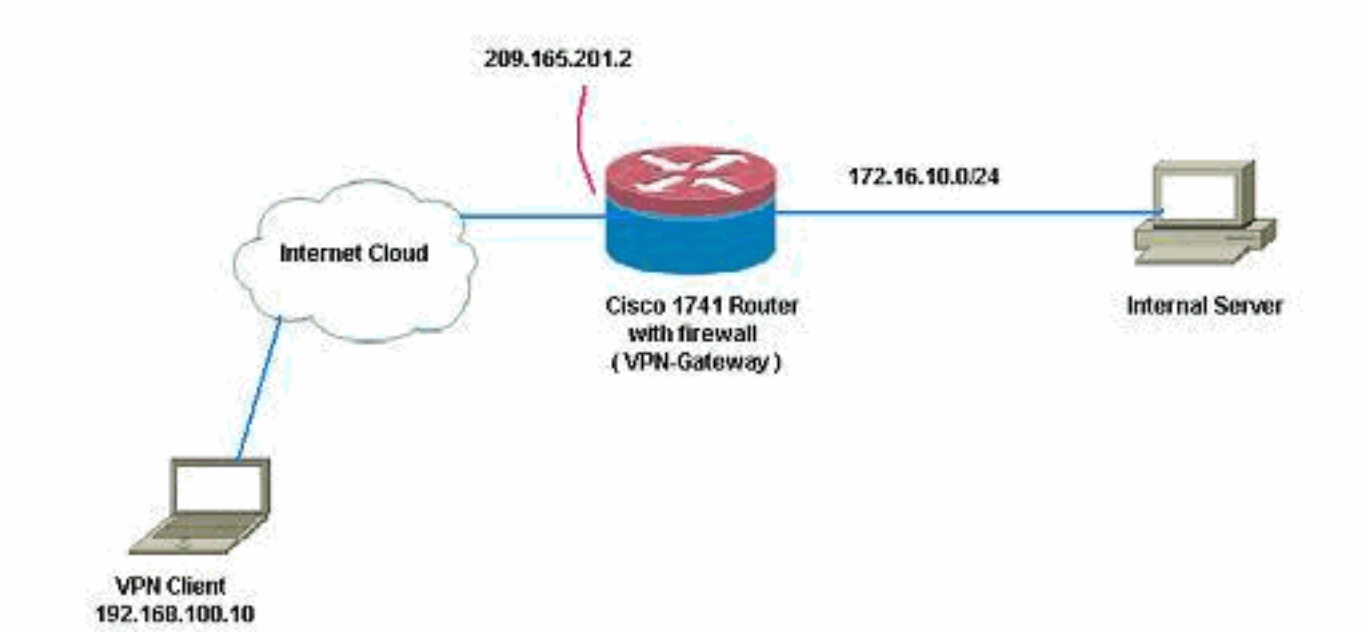
구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



구성

이 문서에서는 다음 구성을 사용합니다.

VPN-게이트웨이

```
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
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

1. 인터페이스 상태를 확인하려면 이 명령을 사용합니다.

```
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. ISAKMP 터널 상태를 확인하려면 이 명령을 사용합니다.

```
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. 암호화 소켓의 상태를 확인하려면 이 명령을 사용합니다.

```
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. 라우터의 활성 그룹을 확인합니다.

```
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. 런타임 검사 유형 정책 맵 통계를 표시하려면 이 명령을 사용합니다.

```
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. 내부 서버에 대한 연결을 확인하려면 ping을 사용합니다.

```
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
```

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- Cisco IOS Firewall
- 기술 지원 및 문서 – Cisco Systems