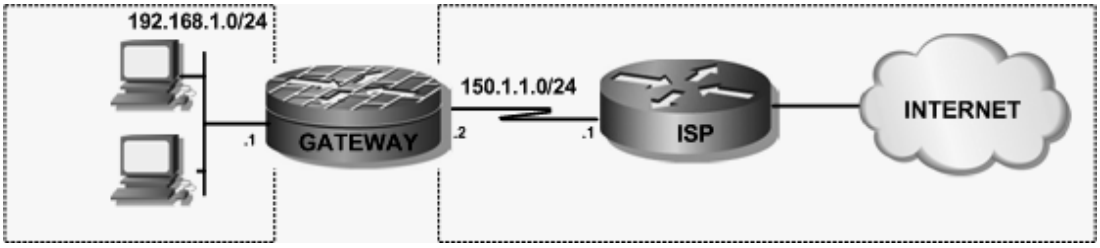
LAB – Cấu hình IOS Firewall cơ bản



Mô tả

Thực hiện **Inspect** cho những dịch vụ hoạt động trên TCP và UDP đảm bảo truy cập dịch vụ ngoài Internet thành công cho những loại ứng dụng này.

Đảm bảo từ bên ngoài không được phép truy cập vào bên trong mạng 192.168.1.0/24.

Cấu hình đầy đủ

GATEWAY

```
Building configuration...
Current configuration : 1495 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname GATEWAY
!
ip inspect name INSPECTION tcp
ip inspect name INSPECTION udp
!
voice-card 0
 no dspfarm
!
interface FastEthernet0/0
 ip address 192.168.1.1 255.255.255.0
 ip inspect INSPECTION in
 duplex auto
```

```
 speed auto
!
interface FastEthernet0/1
 no ip address
 duplex auto
 speed auto
!
interface Serial0/0/0
 ip address 150.1.1.2 255.255.255.0
 ip access-group 100 in
 clock rate 2000000
!
ip route 0.0.0.0 0.0.0.0 150.1.1.1
!
no ip http server
no ip http secure-server
!
access-list 100 deny ip any any
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
scheduler allocate 20000 1000
```

ISP

```
Building configuration...
Current configuration : 1347 bytes
!
hostname ISP
!
interface FastEthernet0/0
```

```
 ip address 151.1.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address dhcp
 ip nat outside
 ip virtual-reassembly
 duplex auto
 speed auto
!
interface Serial0/2/0
ip address 150.1.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
!
ip classless
ip route 192.168.1.0 255.255.255.0 150.1.1.2
!
!
no ip http server
no ip http secure-server
ip nat inside source list 1 interface FastEthernet0/1 overload
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 150.1.1.0 0.0.0.255
!
```

Kiểm tra

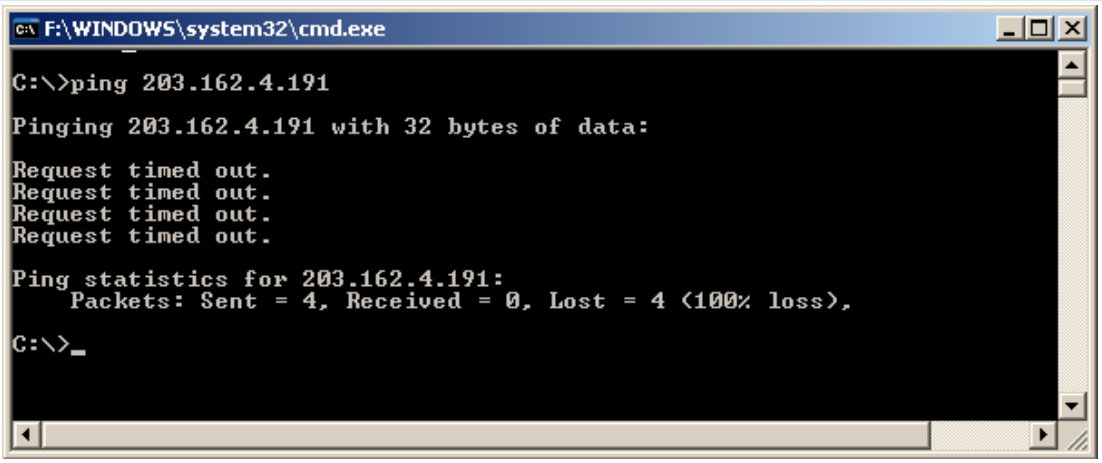
Thực hiện truy cập dịch vụ Web.

Thông tin bảng trạng thái.

```
GATEWAY#sh ip inspect sessions
```

```
Established Sessions
 Session 479FEC78 (192.168.1.2:1901)=>(63.245.209.93:80) tcp SIS_OPEN
 Session 479FEF38 (192.168.1.2:1153)=>(203.162.4.191:53) udp SIS_OPEN
 Session 479FE438 (192.168.1.2:1904)=>(198.133.219.25:80) tcp SIS_OPEN
 Session 479FE9B8 (192.168.1.2:1902)=>(63.245.209.93:80) tcp SIS_OPEN
 Session 479FE178 (192.168.1.2:1905)=>(198.133.219.25:80) tcp SIS_OPEN
 Session 479FE6F8 (192.168.1.2:1903)=>(212.58.226.33:80) tcp SIS_OPEN
 Session 479FDEB8 (192.168.1.2:1906)=>(198.133.219.25:80) tcp SIS_OPEN
GATEWAY#sh ip inspect statistics
Packet inspection statistics [process switch:fast switch]
  tcp packets: [0:246]
  udp packets: [1:7]
Interfaces configured for inspection 1
Session creations since subsystem startup or last reset 7
Current session counts (estab/half-open/terminating) [5:0:0]
Maxever session counts (estab/half-open/terminating) [7:1:1]
Last session created 00:00:25
Last statistic reset never
Last session creation rate 7
Maxever session creation rate 7
Last half-open session total 0
TCP reassembly statistics
  received 0 packets out-of-order; dropped 0
  peak memory usage 0 KB; current usage: 0 KB
  peak queue length 0
```

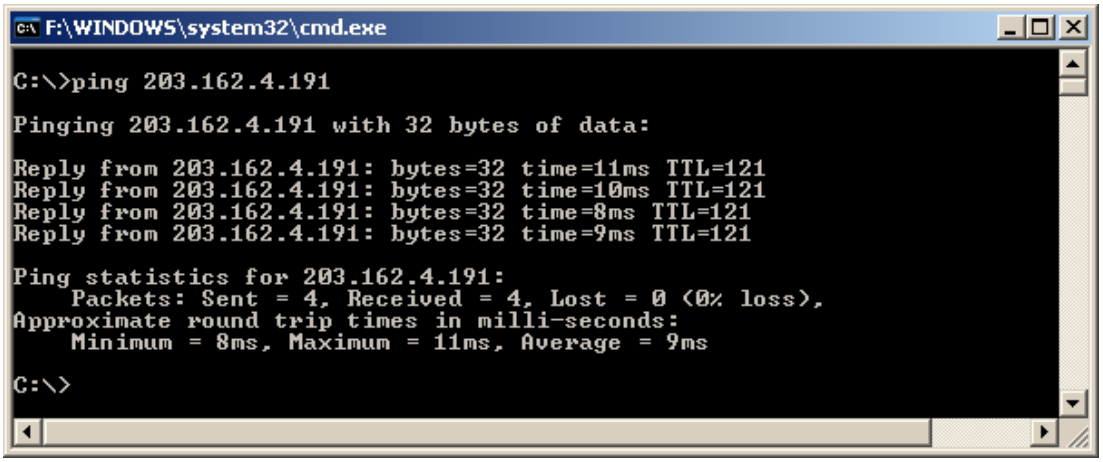
Do chỉ thực hiện inspect tcp và udp nên khi thực hiện với icmp sẽ không thành công.



Hình 2.93.

Có thể thực hiện inspect cho icmp để cho phép echo-reply được trả về.

```
GATEWAY(config)#ip inspect name INSPECTION icmp
```



Hình 2.94.

```
GATEWAY#sh ip inspect sessions

Established Sessions

 Session 479FDEB8 (192.168.1.2:8)=>(203.162.4.191:0) icmp SIS_OPEN
```

Dùng câu lệnh này để cho phép kiểm tra những kết nối được **inspect**.

```
GATEWAY(config)#ip inspect audit-trail

GATEWAY(config)#

*Feb 13 03:08:22.223: %FW-6-SESS_AUDIT_TRAIL_START: Start tcp session:
initiator (192.168.1.2:2118) -- responder (198.133.219.25:80)

*Feb 13 03:08:22.795: %FW-6-SESS_AUDIT_TRAIL_START: Start tcp session:
initiator (192.168.1.2:2119) -- responder (198.133.219.25:80)
```

```
*Feb 13 03:08:22.795: %FW-6-SESS_AUDIT_TRAIL_START: Start tcp session:
initiator (192.168.1.2:2120) -- responder (198.133.219.25:80)

*Feb 13 03:08:23.699: %FW-6-SESS_AUDIT_TRAIL_START: Start tcp session:
initiator (192.168.1.2:2121) -- responder (198.133.219.25:80)
```