

===== ASA CONFIG (Zone: Debian = INSIDE, R1 = OUTSIDE) =====

hostname ciscoasa

```
interface GigabitEthernet0/0
  nameif INSIDE
  security-level 100
  ip address 192.168.10.1 255.255.255.0
```

```
interface GigabitEthernet0/1
  nameif OUTSIDE
  security-level 0
  ip address 192.168.20.1 255.255.255.0
```

```
route OUTSIDE 0.0.0.0 0.0.0.0 192.168.20.2
```

```
access-list INSIDE_TO_R1 extended permit tcp host 192.168.10.10 host 192.168.20.2 eq ssh
access-list INSIDE_TO_R1 extended permit icmp any any
access-list INSIDE_TO_R1 extended permit tcp host 192.168.10.10 host 192.168.20.2 eq telnet
access-group INSIDE_TO_R1 in interface INSIDE
```

```
access-list OUT_TO_TACACS extended permit tcp host 192.168.20.2 host 192.168.30.10 eq tacacs
access-group OUT_TO_TACACS in interface OUTSIDE
```

```
access-list OUT_TO_INSIDE_ICMP extended permit icmp any any
access-group OUT_TO_INSIDE_ICMP in interface OUTSIDE
```

===== R1 CONFIG =====

hostname R1

```
interface Ethernet1/0
  ip address 192.168.20.2 255.255.255.0
  no shutdown
```

```
interface Ethernet1/1
  ip address 192.168.30.1 255.255.255.0
  no shutdown
```

```
ip route 0.0.0.0 0.0.0.0 192.168.20.1
```

```
tacacs-server host 192.168.30.10 key tacacs123
```

```
aaa new-model
aaa authentication login default group tacacs+ local
aaa authorization exec default group tacacs+ local
```

```
username admin privilege 15 secret localadminpass
```

```
line vty 0 4
  login authentication default
  transport input ssh telnet
```

```
ip ssh version 2
crypto key generate rsa modulus 1024
```

```
===== UBUNTU SERVER (TACACS+) CONFIG =====
```

```
# /etc/tacacs+/tac_plus.conf
key = "tacacs123"
```

```
user = admin {
    default service = permit
    login = cleartext "adminpass"
    service = exec {
        priv-lvl = 15
    }
}
```

```
user = admin1 {
    default service = permit
    login = cleartext "admin1pass"
    service = exec {
        priv-lvl = 1
    }
}
```

```
sudo systemctl restart tacacs_plus
```

```
===== DEBIAN CONFIG =====
```

```
# /etc/network/interfaces
auto lo
iface lo inet loopback
```

```
allow-hotplug ens4
iface ens4 inet static
    address 192.168.10.10
    netmask 255.255.255.0
    gateway 192.168.10.1
```

```
# DHCP t?m (k?t n?i cloud)
sudo dhclient ens5
```

```
# Test SSH ho?c Telnet t? Debian ??n R1
ssh -oKexAlgorithms=+diffie-hellman-group14-sha1 \
    -oHostKeyAlgorithms=+ssh-rsa \
    -oCiphers=+aes128-cbc admin@192.168.20.2
```

```
# ho?c telnet
telnet 192.168.20.2
```

```
===== S? ?? m?ng =====
```

```
Debian (192.168.10.10)  -> INSIDE
ASA Gi0/0                -> INSIDE (192.168.10.1)
ASA Gi0/1                -> OUTSIDE (192.168.20.1)
```

R1 (192.168.20.2) -> OUTSIDE  
Ubuntu (192.168.30.10) -> sau R1 (ngoài ASA)