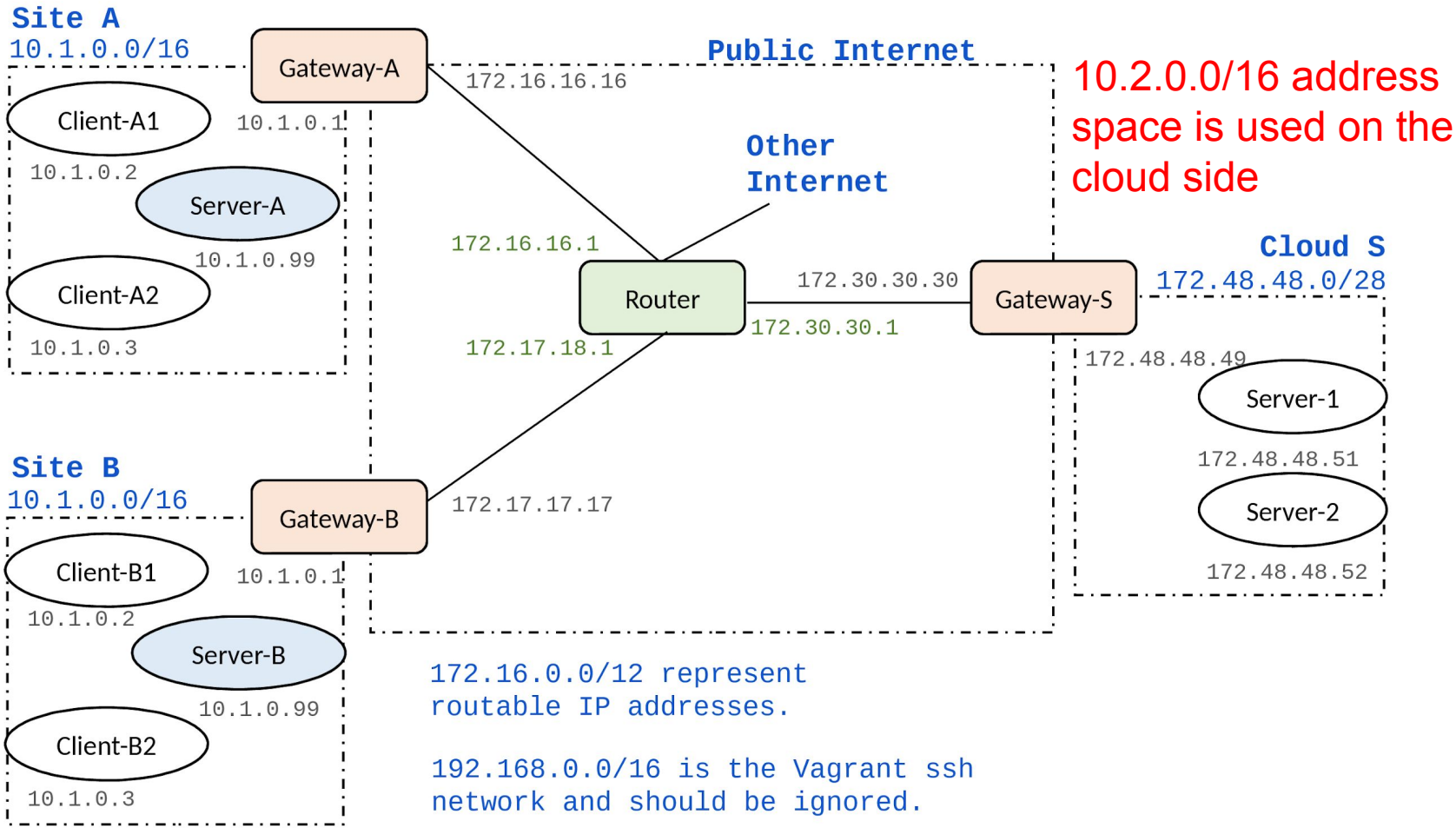
VPN tunneling

Oksana Baranova & Arthur Carels

Professors: Tuomas Aura, Aleksi Peltonen

January 2021


Site A
10.1.0.0/16
Gateway-A
Public Internet
172.16.16.16
10.2.0.0/16 address space is used on the cloud side
Client-A1
10.1.0.1
10.1.0.2
Server-A
10.1.0.99
Client-A2
10.1.0.3
Other Internet
172.16.16.1
Router
172.30.30.30
Gateway-S
172.30.30.1
Cloud S
172.48.48.0/28
172.48.48.49
Server-1
172.48.48.51
Server-2
172.48.48.52
172.17.18.1
Site B
10.1.0.0/16
Gateway-B
172.17.17.17
Client-B1
10.1.0.1
10.1.0.2
Server-B
10.1.0.99
Client-B2
10.1.0.3
172.16.0.0/12 represent routable IP addresses.
192.168.0.0/16 is the Vagrant ssh network and should be ignored.

GOALS

1. VPN tunnel between clients and cloud servers
2. Traffic in tunnel encrypted (ESP)
3. Set up proper routing rules

General security

SOLUTION

- Authentication by secret
- Creation of private subnetwork for servers (10.2.0.0/16)
- iptables: → NAT port forwarding

Gateway configuration

etc/ipsec.conf

```
conn S_TO_A
        type = tunnel
        authby=secret
        left=172.30.30.30
        leftsubnet=172.30.30.30/32
        right=172.16.16.16
        rightsubnet=172.16.16.16/32
        ike=aes256-sha2_256-modp2048!
        esp=aes256-sha2_256!
        keyingtries=0
        ikelifetime=1h
        lifetime=8h
        dpddelay=30
        dpdtimeout=120
        dpdaction=restart
        auto=start
```

/etc/ipsec.secrets

```
 # This file holds shared secrets for authentication.

 172.30.30.30 172.16.16.16 : PSK
"dKVLhZa/cXQg2x3CCRxUYqfQPFMp0HO2"
 172.30.30.30 172.17.17.17 : PSK
"syMhWOzOvfwoQ9lg/C6q/+DSJEEOkIWO "
```

Keys generated via

head -c 24 /dev/urandom | base64

→ Randomness

Working tunnel

(router): *sudo tcpdump -i enp0s8*

Note: All traffic is encrypted

Note: Only public addresses of gateway are exposed

```
vagrant@router:~$ sudo tcpdump -i enp0s8
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s8, link-type EN10MB (Ethernet), capture size 262144 bytes
20:58:06.391653 IP 172.17.17.17 > 172.30.30.30: ESP(spi=0xc5e19356,seq=0x1e3), length 104
20:58:06.392249 IP 172.30.30.30 > 172.17.17.17: ESP(spi=0xc5247a30,seq=0x1d6), length 104
20:58:06.445278 IP 172.17.17.17 > 172.30.30.30: ESP(spi=0xc5e19356,seq=0x1e4), length 104
20:58:06.448143 IP 172.17.17.17 > 172.30.30.30: ESP(spi=0xc5e19356,seq=0x1e5), length 264
20:58:06.449041 IP 172.30.30.30 > 172.17.17.17: ESP(spi=0xc5247a30,seq=0x1d7), length 104
20:58:06.454664 IP 172.30.30.30 > 172.17.17.17: ESP(spi=0xc5247a30,seq=0x1d8), length 392
20:58:06.454712 IP 172.30.30.30 > 172.17.17.17: ESP(spi=0xc5247a30,seq=0x1d9), length 104
20:58:07.408132 IP 172.17.17.17 > 172.30.30.30: ESP(spi=0xc5e19356,seq=0x1e8), length 104
20:58:07.412661 IP 172.30.30.30 > 172.17.17.17: ESP(spi=0xc5247a30,seq=0x1db), length 104
20:58:07.416318 IP 172.17.17.17 > 172.30.30.30: ESP(spi=0xc5e19356,seq=0x1e9), length 104
20:58:07.416514 IP 172.17.17.17 > 172.30.30.30: ESP(spi=0xc5e19356,seq=0x1ea), length 264
20:58:07.419225 IP 172.30.30.30 > 172.17.17.17: ESP(spi=0xc5247a30,seq=0x1dc), length 104
20:58:07.424747 IP 172.30.30.30 > 172.17.17.17: ESP(spi=0xc5247a30,seq=0x1dd), length 392
20:58:07.425066 IP 172.30.30.30 > 172.17.17.17: ESP(spi=0xc5247a30,seq=0x1de), length 104
20:58:07.425776 IP 172.17.17.17 > 172.30.30.30: ESP(spi=0xc5e19356,seq=0x1eb), length 104
20:58:07.427786 IP 172.17.17.17 > 172.30.30.30: ESP(spi=0xc5e19356,seq=0x1ec), length 104
20:58:07.428472 IP 172.30.30.30 > 172.17.17.17: ESP(spi=0xc5247a30,seq=0x1df), length 104
20:58:08.416027 IP 172.17.17.17 > 172.30.30.30: ESP(spi=0xc5e19356,seq=0x1ed), length 104
20:58:08.421185 IP 172.30.30.30 > 172.17.17.17: ESP(spi=0xc5247a30,seq=0x1e0), length 104
20:58:08.423919 IP 172.17.17.17 > 172.30.30.30: ESP(spi=0xc5e19356,seq=0x1ee), length 104
20:58:08.424409 IP 172.17.17.17 > 172.30.30.30: ESP(spi=0xc5e19356,seq=0x1ef), length 264
20:58:08.429358 IP 172.30.30.30 > 172.17.17.17: ESP(spi=0xc5247a30,seq=0x1e1), length 104
20:58:08.438783 IP 172.30.30.30 > 172.17.17.17: ESP(spi=0xc5247a30,seq=0x1e2), length 392
20:58:08.438995 IP 172.30.30.30 > 172.17.17.17: ESP(spi=0xc5247a30,seq=0x1e3), length 104
20:58:08.439985 IP 172.17.17.17 > 172.30.30.30: ESP(spi=0xc5e19356,seq=0x1f0), length 104
20:58:08.442746 IP 172.17.17.17 > 172.30.30.30: ESP(spi=0xc5e19356,seq=0x1f1), length 104
20:58:08.444005 IP 172.30.30.30 > 172.17.17.17: ESP(spi=0xc5247a30,seq=0x1e4), length 104
20:58:09.429605 IP 172.17.17.17 > 172.30.30.30: ESP(spi=0xc5e19356,seq=0x1f2), length 104
20:58:09.433188 IP 172.30.30.30 > 172.17.17.17: ESP(spi=0xc5247a30,seq=0x1e5), length 104
20:58:09.437272 IP 172.17.17.17 > 172.30.30.30: ESP(spi=0xc5e19356,seq=0x1f3), length 104
20:58:09.437411 IP 172.17.17.17 > 172.30.30.30: ESP(spi=0xc5e19356,seq=0x1f4), length 264
20:58:09.442779 IP 172.30.30.30 > 172.17.17.17: ESP(spi=0xc5247a30,seq=0x1e6), length 104
20:58:09.450100 IP 172.30.30.30 > 172.17.17.17: ESP(spi=0xc5247a30,seq=0x1e7), length 392
20:58:09.450186 IP 172.30.30.30 > 172.17.17.17: ESP(spi=0xc5247a30,seq=0x1e8), length 104
20:58:09.451722 IP 172.17.17.17 > 172.30.30.30: ESP(spi=0xc5e19356,seq=0x1f5), length 104
20:58:09.454037 IP 172.17.17.17 > 172.30.30.30: ESP(spi=0xc5e19356,seq=0x1f6), length 104
20:58:09.455484 IP 172.30.30.30 > 172.17.17.17: ESP(spi=0xc5247a30,seq=0x1e9), length 104
20:58:10.435001 IP 172.17.17.17 > 172.30.30.30: ESP(spi=0xc5e19356,seq=0x1f7), length 104
```

Questions + demo