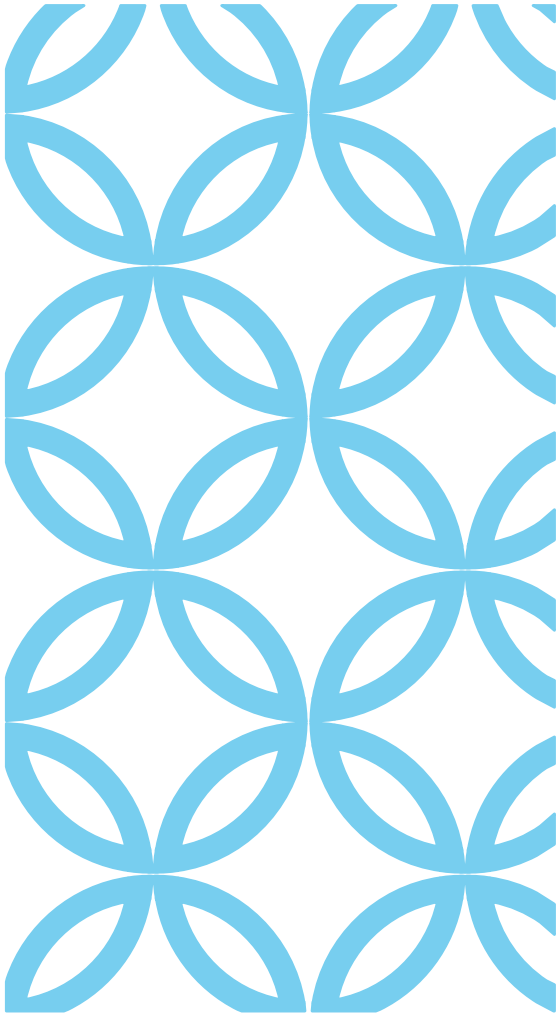
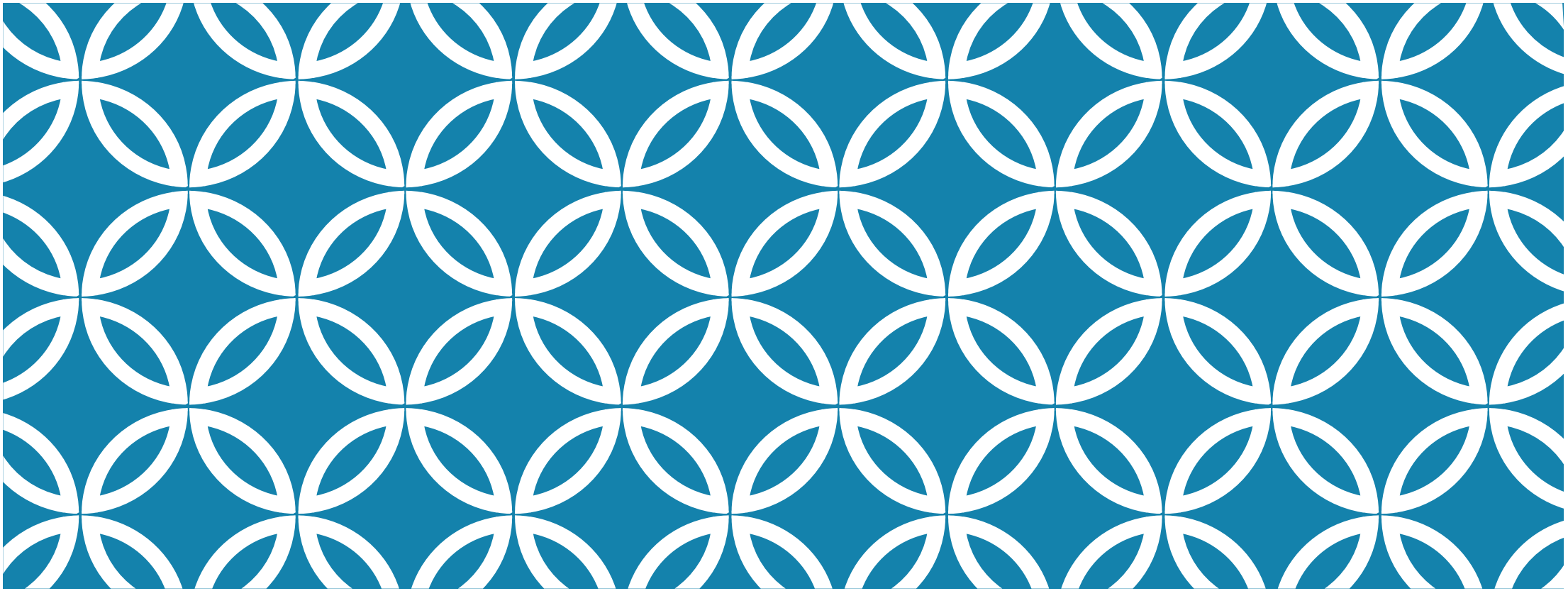


40 yhp

Campus Mölndal

GRUNDLÄGGANDE MOLNAPPLIKATIONER

VECKA 3



NÄTVERK

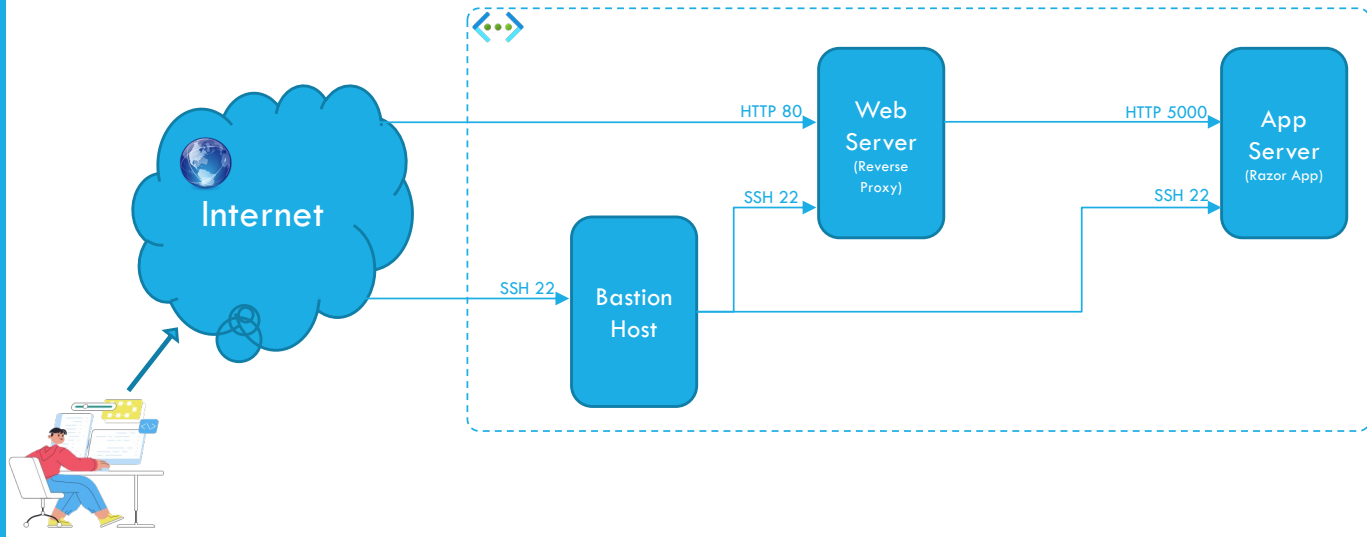
Vecka 3

VECKANS MÅL

NÄTVERK OCH SÄKERHET

Provisionera en produktionsmiljö (PROD Environment) till webb-appen

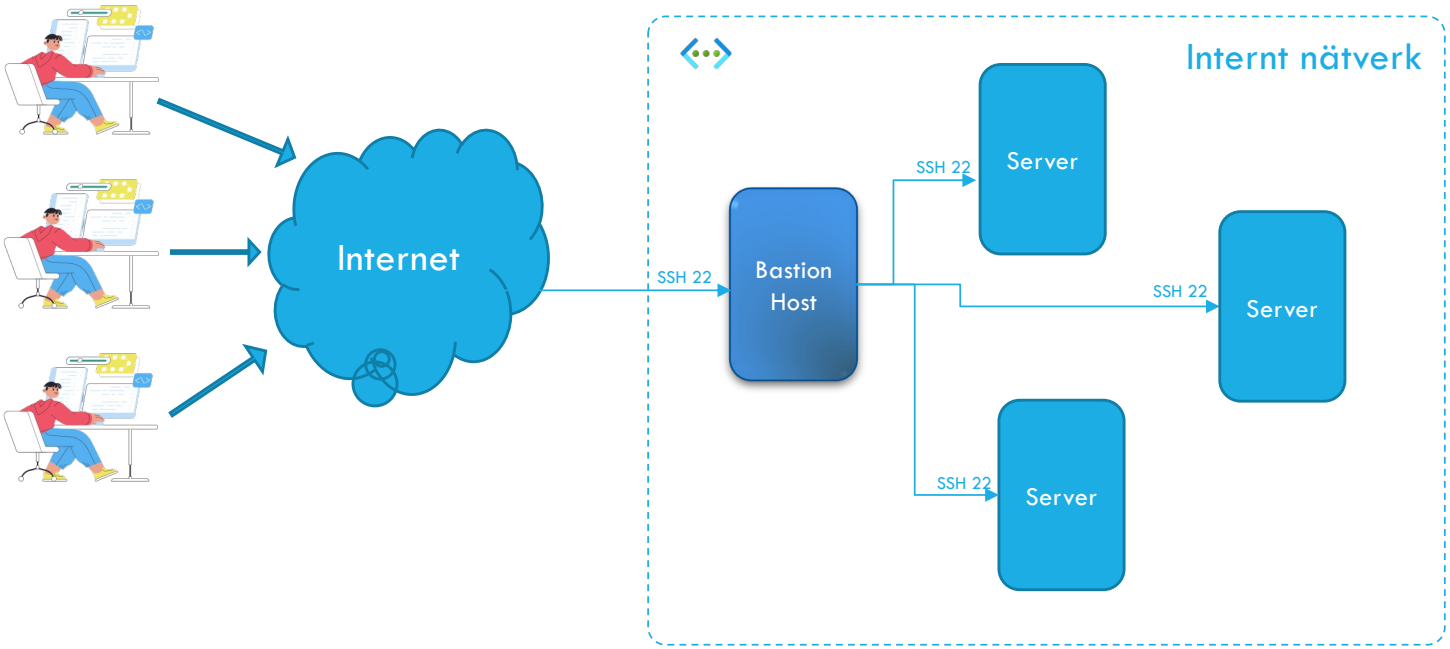
- med Bastion Host för SSH
- med Reverse Proxy för HTTP
- med NSG, ASG och ServiceTags



VNET – VIRTUAL NETWORK

- VNet är ett virtuellt nätverk helt definierat i mjukvara
- VNet spänner över en Region men definieras i en Resource Group
- VNet kan kopplas till andra nätverk genom
  - VNet peering
  - VPN
  - ExpressRoute
- Ett virtuellt nät delas in i ett eller flera subnät
- NSG filtrerar nätverkstrafiken
- Resurser i ett virtuellt nät har default tillgång till internet

VAD ÄR EN BASTION HOST?



VAD ÄR EN BASTION HOST?

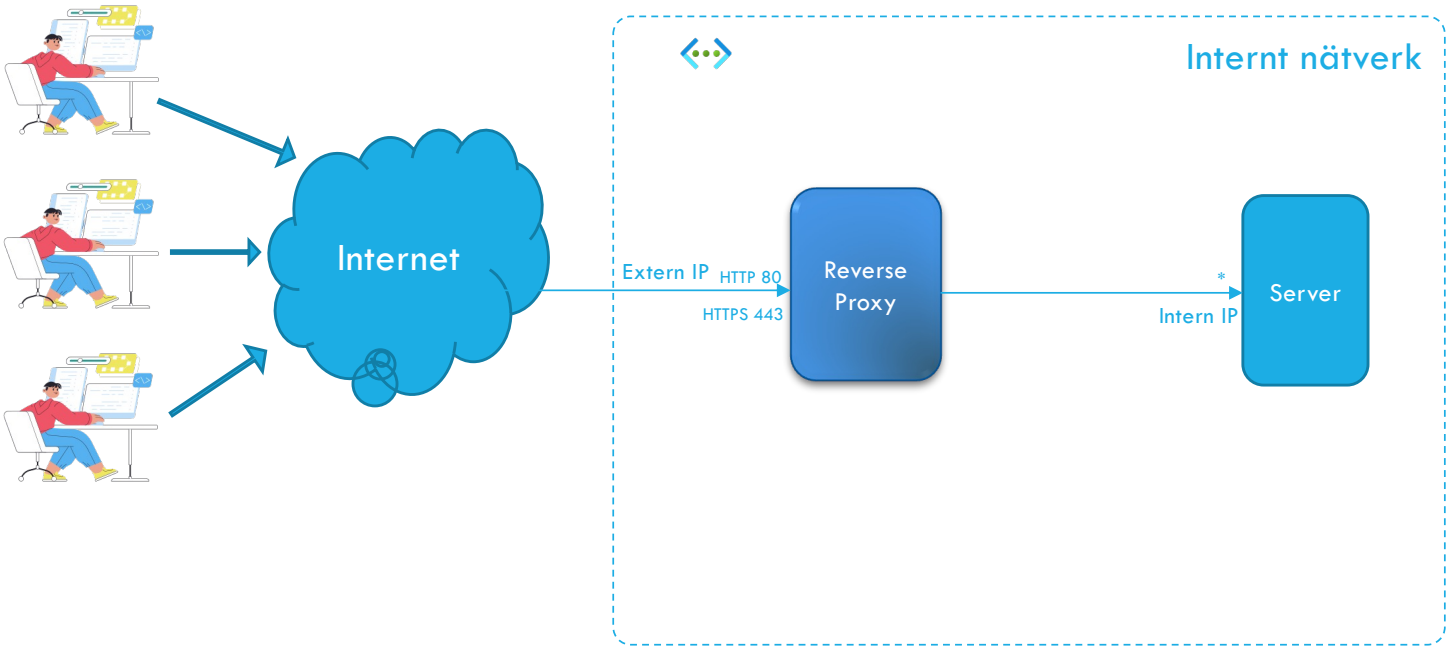
En bastion host används för att skydda enheter eller system inom ett nätverk genom att:

- hantera externa anslutningar till det interna nätverket.
- övervaka och spåra aktiviteter
- skydda från obehörig åtkomst

Best practices:

- installera säkerhetsmjukvara
- avinstallera allt som inte behövs
- använd SSH Agent

VAD ÄR EN REVERSE PROXY?



VAD ÄR EN REVERSE PROXY?

En Reverse Proxy ligger mellan en klient och en server (ofta en applikationsserver)

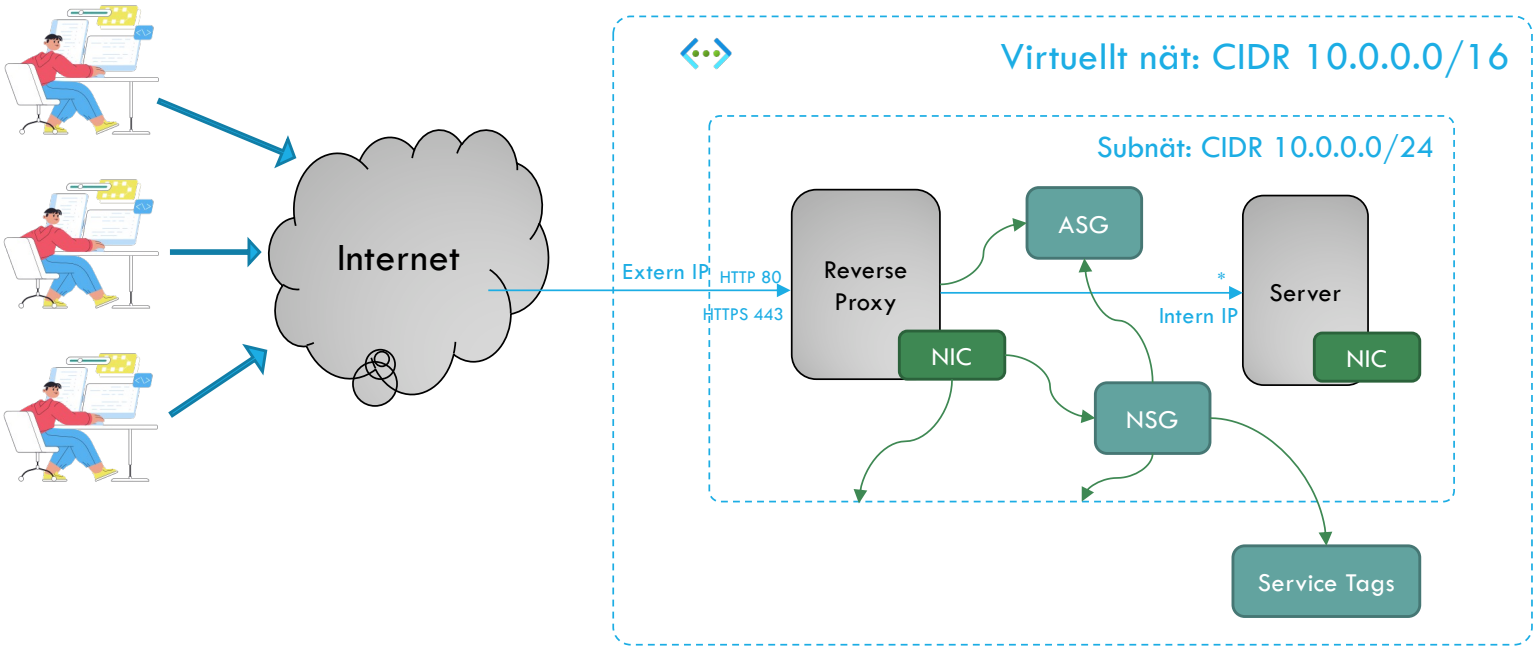
Vanliga funktioner är:

- SSL Offloading – hanterar certifikat och avkrypterar trafiken innan den går vidare till applikationsservern
- Trafikstyrning – dirigerar trafik till en backend server baserat på URL: protokoll, domain eller path (`https://www.example.com/blog/`)
- Cachning – Avlastar applikationsservern med ofta efterfrågat innehåll

Men även:

- Lastbalansering
- Filtrera och blockera skadlig trafik
- Föra statistik

VAD ÄR NSG, ASG OCH SERVICE TAGS?



VAD ÄR NSG, ASG OCH SERVICE TAGS?

NSG - Network Security Group

- Definierar nätverksregler på subnät-nivå
- Fungerar som en NACL – Network Access Control List
- Kan associeras antingen med en NIC eller med ett Subnet

ASG - Application Security Group

- Definierar nätverksregler på applikationsnivå
- Kan associeras till exempelvis en VM
- NSG-regler kan tillämpas på alla VM som tillhör en viss ASG

Service Tags

- Används för att definiera nätverksregler till tjänster på Azure

NSG - NETWORK SECURITY GROUP

Nätverksregel (5 Tuples)

1. Source IP: IP-adressen för den enhet som initierar anslutningen.
2. Source port: Porten som används av källenheten för att initiera anslutningen.
3. Destination IP: IP-adressen för den enhet som anslutningen ska skickas till.
4. Destination port: Porten som ska användas av destinationenheten för att ta emot anslutningen.
5. Protocol: Protokollet som används för att skicka data, till exempel TCP eller UDP.

Ordningen spelar roll

- Prioritet bestämmer ordningen som säkerhetsregler utvärderas i (högst prio först)
- NSG-regler prioriteras med heltal mellan 100 och 4096, där lägre tal har högre prioritet

CIDR

Classles Inter-Domain Routing (CIDR)

IP-adresser är uppdelade i två delar: **nätverksadressen** (identifierar ett helt nät eller ett subnät) och **värdadressen** (identifierar en specifik maskinanslutning till nätverket). Denna uppdelning används för att kontrollera hur trafik **routas** bland IP-nätverk.
(https://sv.wikipedia.org/wiki/Classless_Inter-Domain_Routing)

- 192.168.0.0/**24** representerar de **256** IPv4-adresserna mellan 192.168.0.0 och 192.168.0.255. Class C
- /**16** 255.255.0.0 $2^{16} = 65{,}536$ adresser Class B
- 0.0.0.0/0 betyder **alla** adresser

NON-ROUTABLE ADDRESS SPACE

Det finns inte tillräckligt med IPv4-adresser

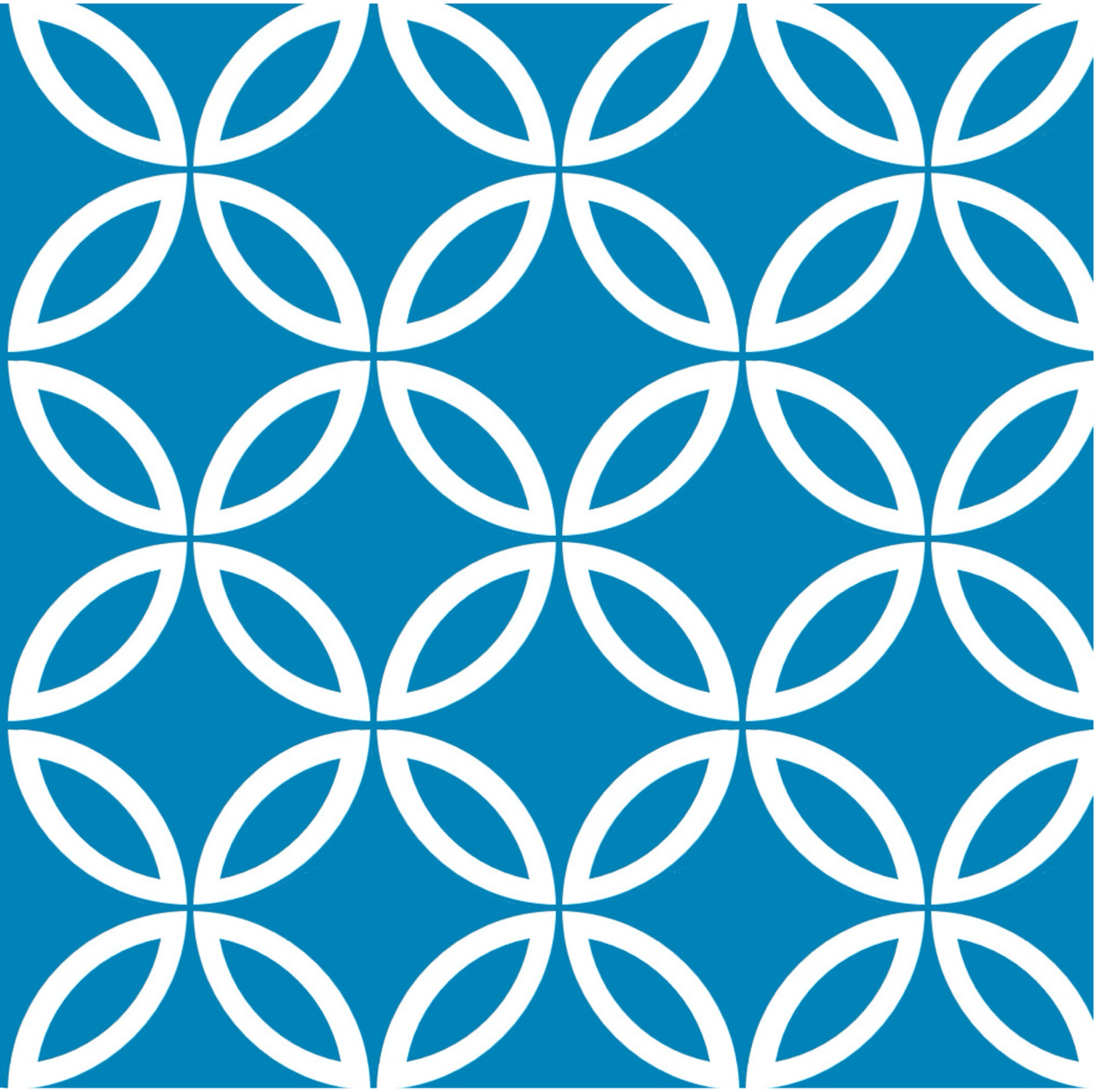
1996 definierades tre nätverk som kan användas till interna nätverk

- 10.0.0.0/8 (Range: 10.0.0.0 – 10.255.255.255)
- 172.16.0.0/12 (Range: 172.16.0.0 – 172.31.255.255)
- 192.168.0.0/16 (Range: 192.168.0.0 – 192.168.255.255)

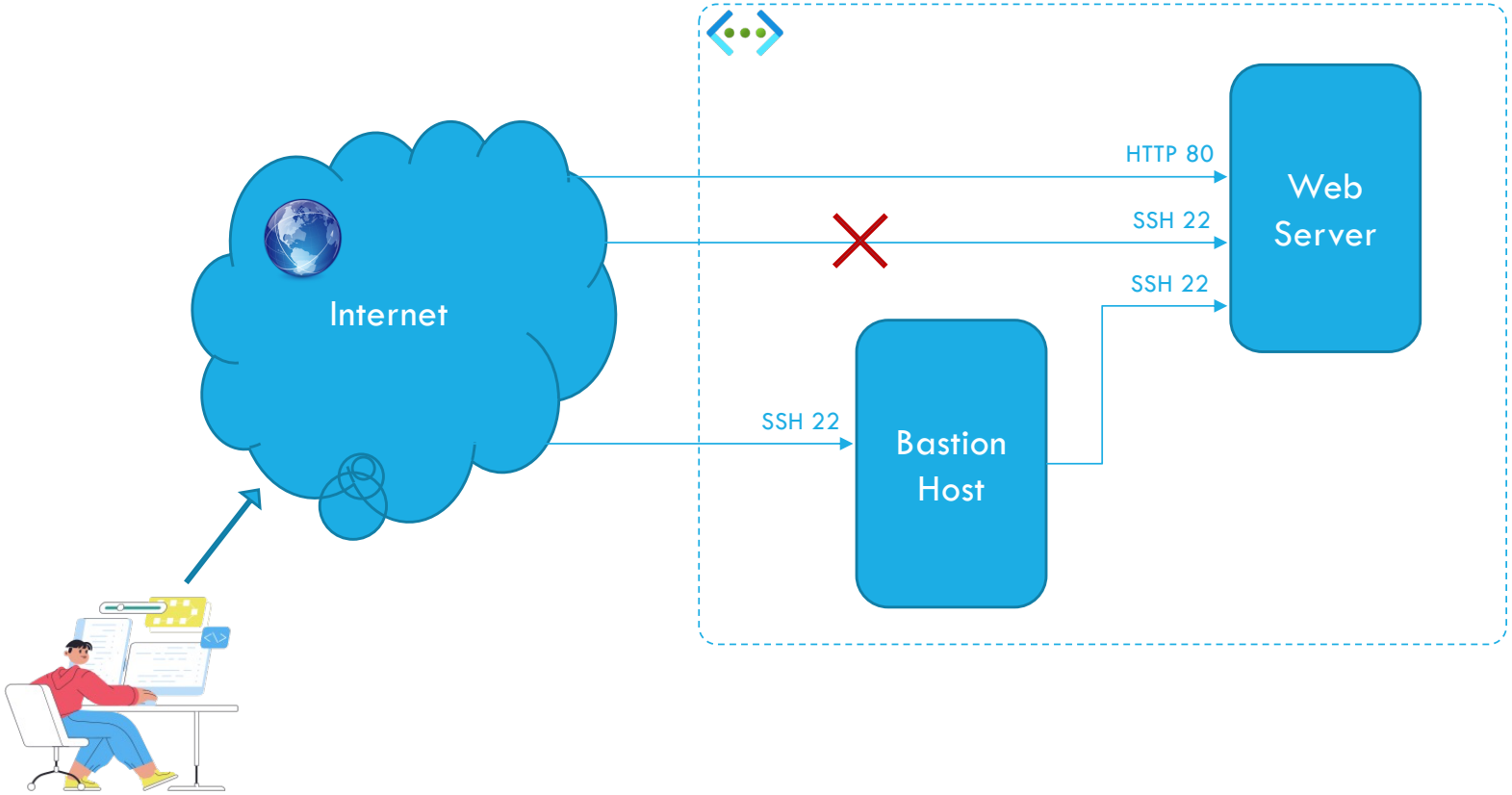
För att kommunicera ut på Internet används NAT (Network Address Translation)

DEMO

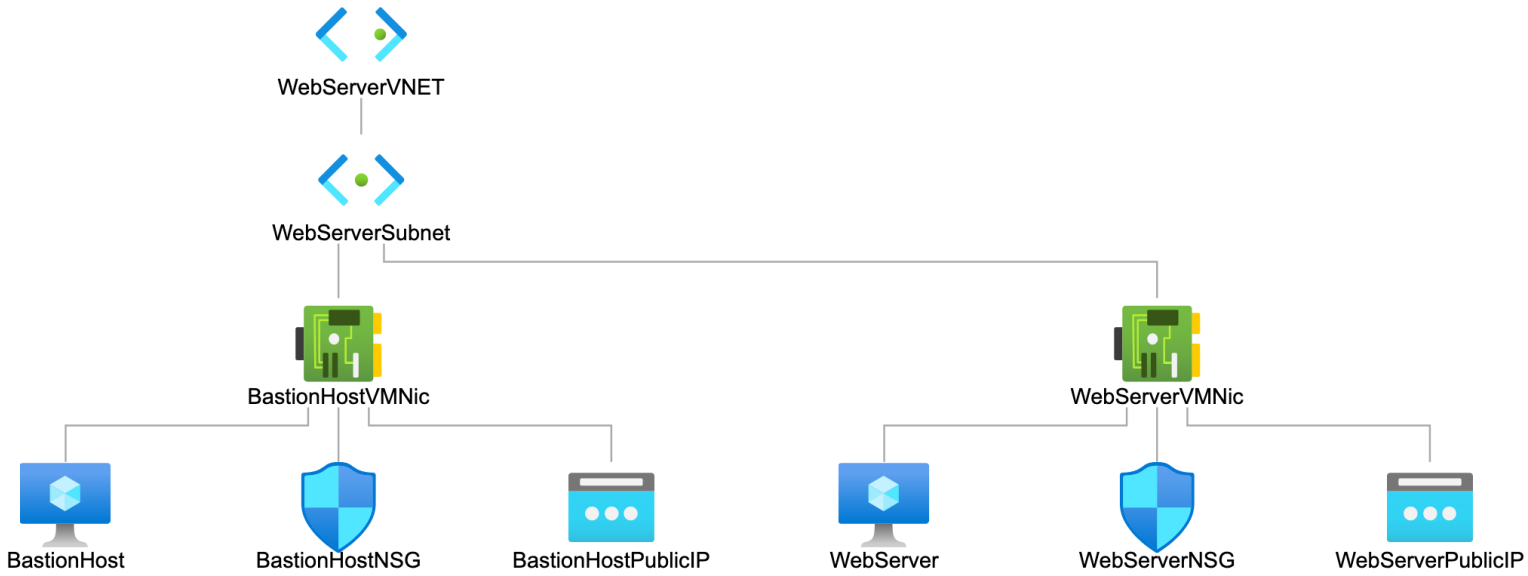
Bastion Host



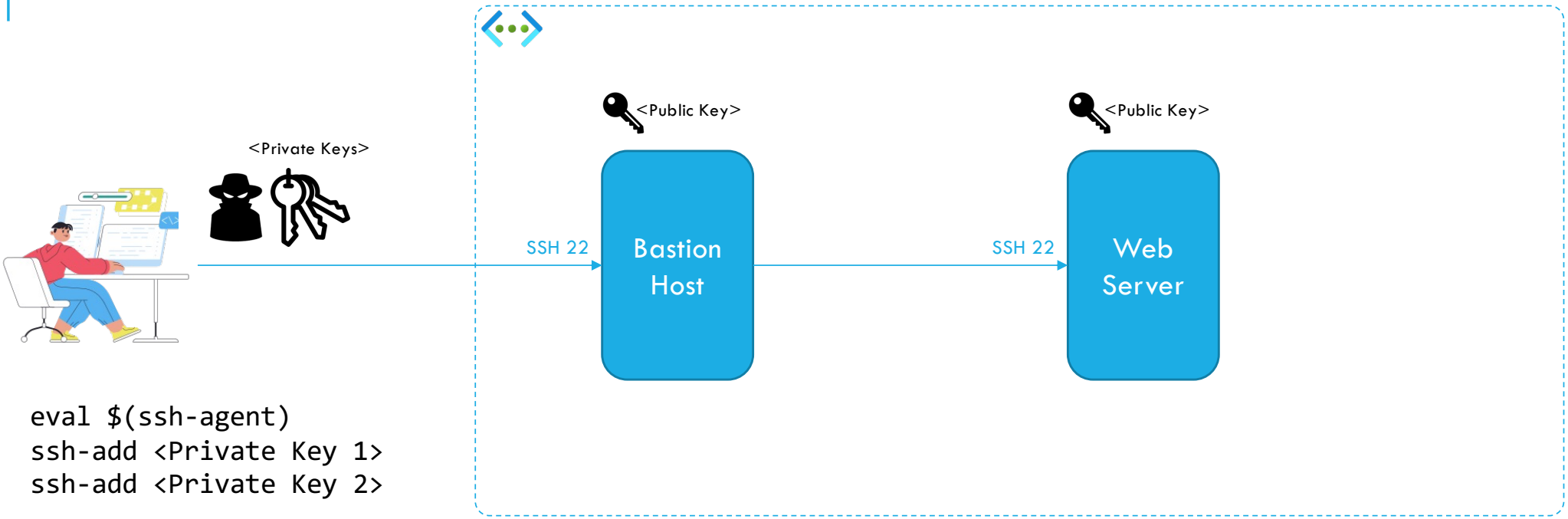
DEMO: BASTION HOST



TOPOLOGI


WebServerVNET
WebServerSubnet
BastionHostVMNic
WebServerVMNic
BastionHost
BastionHostNSG
BastionHostPublicIP
WebServer
WebServerNSG
WebServerPublicIP

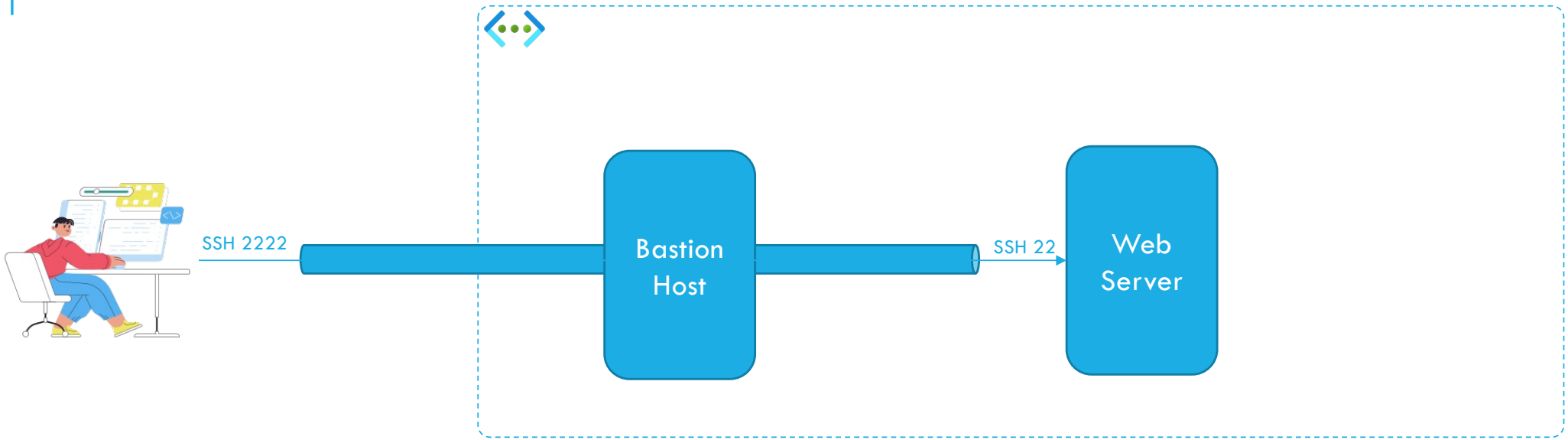
SSH AGENT




```
eval $(ssh-agent)
ssh-add <Private Key 1>
ssh-add <Private Key 2>
…
ssh-add -l

ssh -A user@IP
```

SSH TUNNEL




```
ssh -A -N -L 2222:<WebServerIP>:22 azureuser@<BastionHostIP>
scp -A -P 2222 myfile.txt azureuser@localhost:~/myfile.txt
```

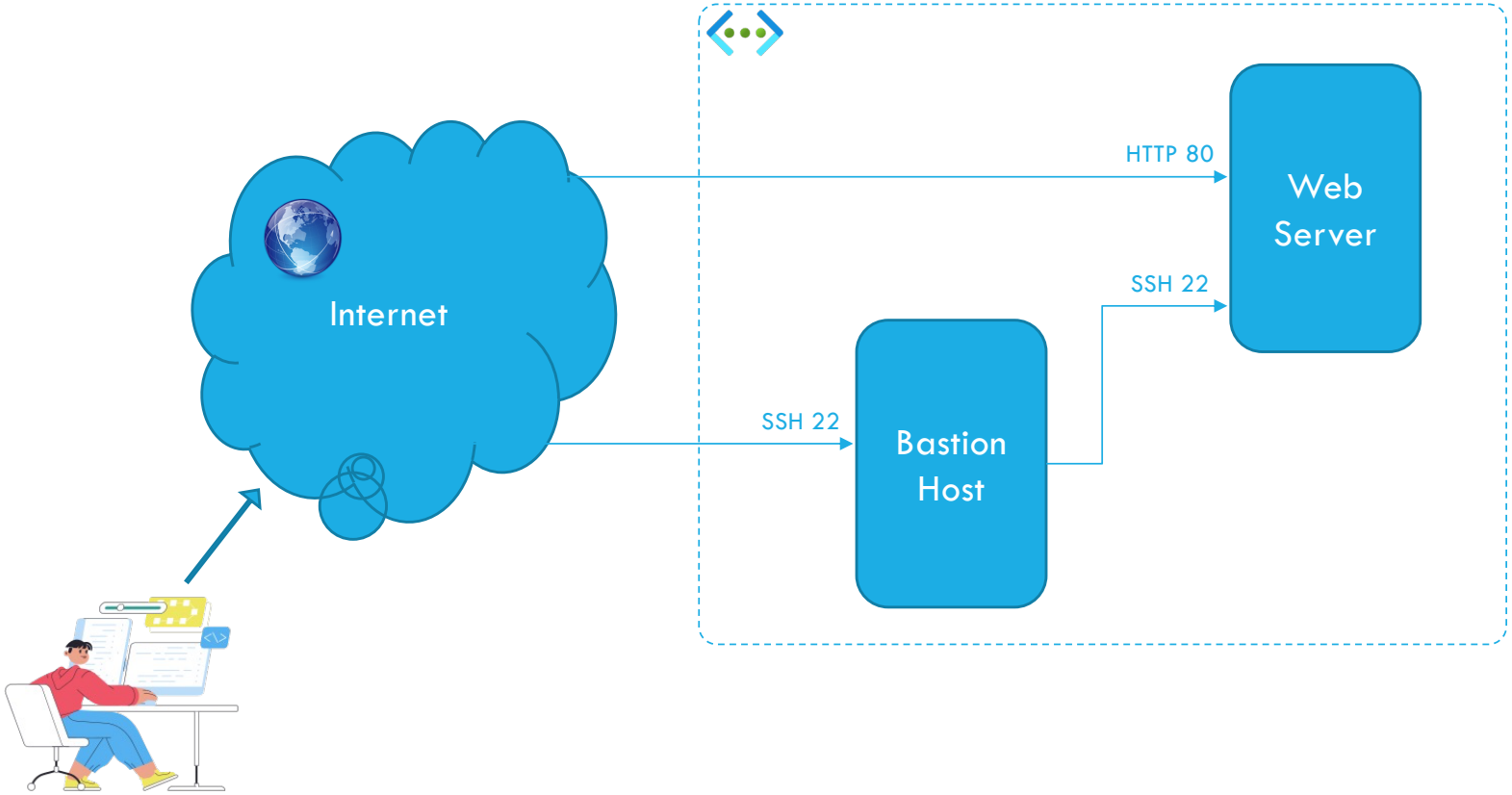
ÖVNING: BASTION HOST OCH NSG

Skapa två servrar

- Bastion Host
  - öppen på port 22 (SSH)
- Web Server
  - med Nginx installerad
  - öppen på port 80 (HTTP)
  - öppen på port 22 (SSH)

1. Logga in på båda och se att det fungerar
2. Ändra NSG på Web Server genom att helt ta bort SSH-regeln
3. Verifiera att du inte längre kan logga in på Web Server
4. Ladda en SSH Agent med nödvändiga privata nycklar och logga in med SSH Agent till Bastion Host och därifrån vidare till Web Server
5. Reflektera kring vilka nätverksregler som verkar gälla inom ett VNet

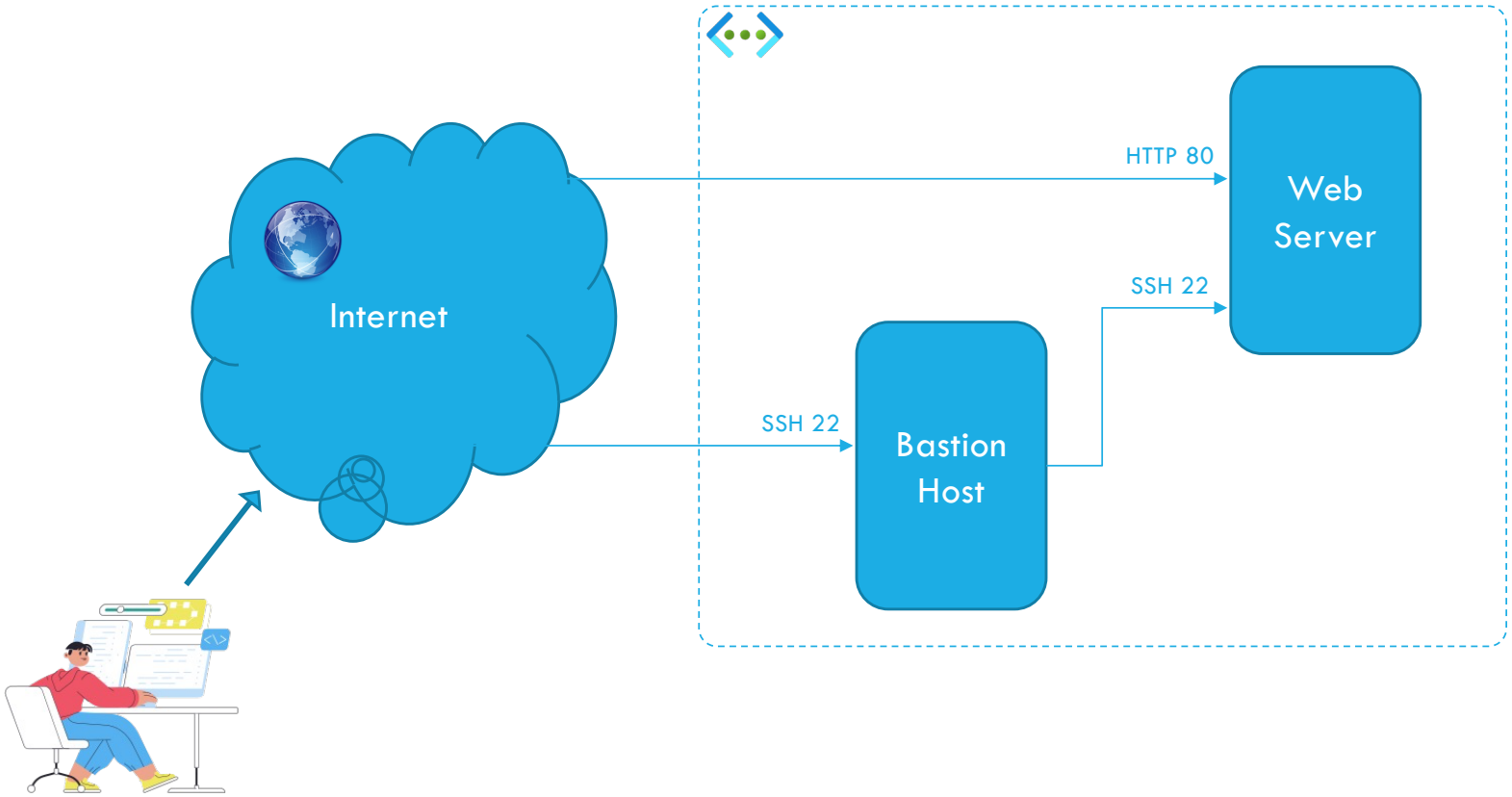
DEMO: ASG OCH SERVICE TAGS



Skapa en ASG

- BastionASG
  - associera till Bastion Host
- Web Server NSG
  - deny all SSH
  - öppna port 22 (SSH) från Bastion Host med ASG
  - öppna port 80 (HTTP) från internet med Service Tag

ÖVNING: ASG OCH SERVICE TAGS



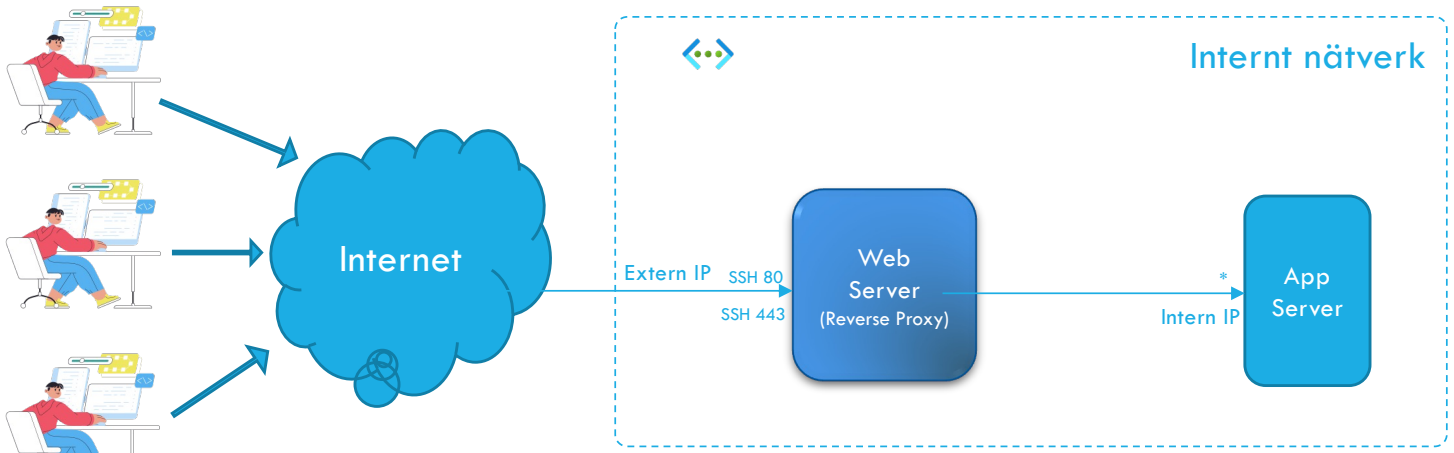
Skapa ASG

- BastionASG
  - associera till Bastion Host
- Bastion Host NSG
  - öppna port 22 (SSH) från internet med Service Tag
- Web Server NSG
  - öppna port 80 (HTTP) från Internet med Service Tag
  - öppna port 22 (SSH) från Bastion Host med ASG

Extra – Subnet NSG

- Skapa en ny NSG
  - koppla NSG:n till subnätet istället
  - Byt ut de två servrarnas NSG:er till den nya och radera de två gamla
  - Skriv alla regler för en säker nätverksmiljö i den nya NSG:n
  - Använd ASG:er och Service Tags

DEMO: REVERSE PROXY



/etc/nginx/sites-available/default

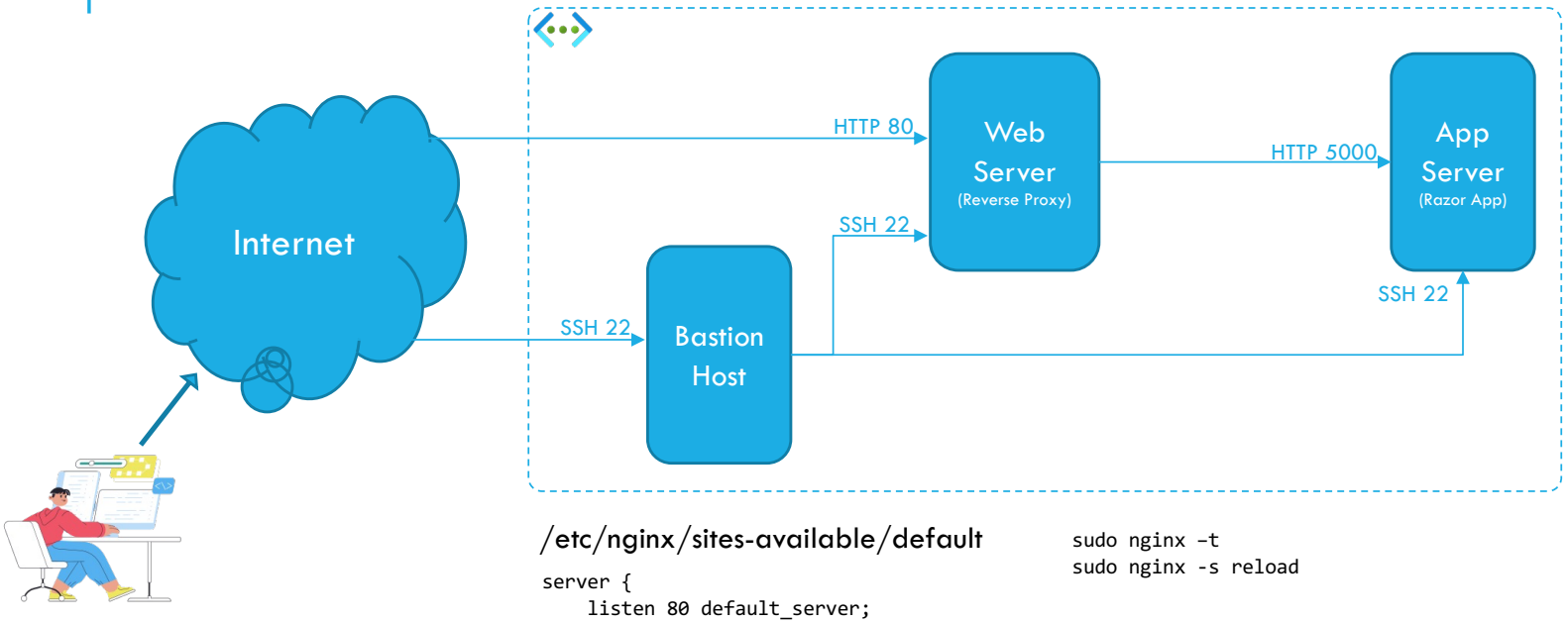
```
server {
    listen 80 default_server;
    location / {
        proxy_pass         http://<AppServerIntIP>:5000;
        proxy_http_version 1.1;
        proxy_set_header   Upgrade $http_upgrade;
        proxy_set_header   Connection keep-alive;
        proxy_set_header   Host $host;
        proxy_cache_bypass $http_upgrade;
        proxy_set_header   X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header   X-Forwarded-Proto $scheme;
    }
}
```

Skapa två VM

- App Server
  - installera dotnet och Razor App
  - lyssnar på port 5000
- Web Server
  - installera Nginx som reverse proxy
  - uppdatera server block

```
sudo nginx -t
sudo nginx -s reload
```

ÖVNING: REVERSE PROXY



/etc/nginx/sites-available/default

```
server {
    listen 80 default_server;
    location / {
        proxy_pass         http://<AppServerIntIP>:5000;
        proxy_http_version 1.1;
        proxy_set_header   Upgrade $http_upgrade;
        proxy_set_header   Connection keep-alive;
        proxy_set_header   Host $host;
        proxy_cache_bypass $http_upgrade;
        proxy_set_header   X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header   X-Forwarded-Proto $scheme;
    }
}
```

```
sudo nginx -t
sudo nginx -s reload
```

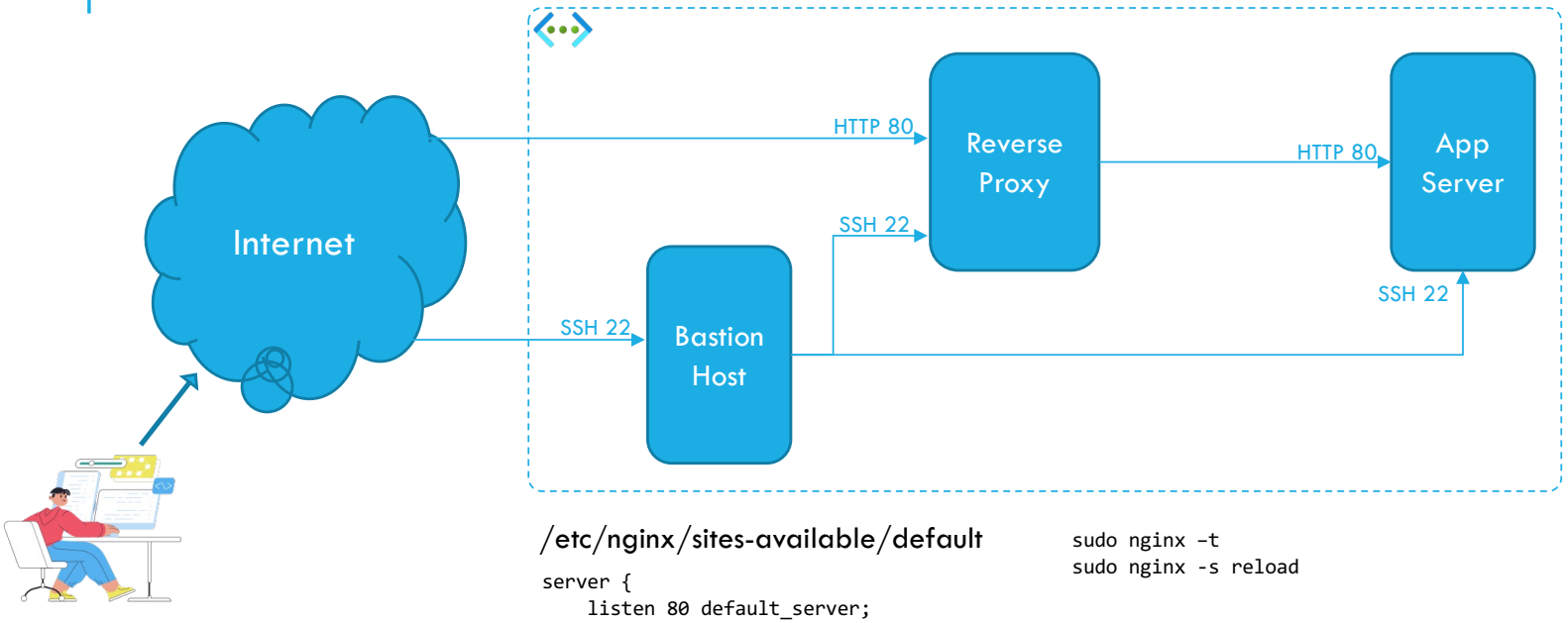
Skapa tre VM

- App Server
  - installera dotnet och Razor App
  - lyssnar på port 5000
- Web Server
  - installera Nginx som reverse proxy
  - uppdatera server block
- Bastion Host
  - installera fail2ban

Säkerhet

- Designa nätverket så att
  - Det endast går att ansluta via SSH till servrarna via Bastion Host
  - Det endast går att nå applikationen genom Reverse Proxy
- Hur påverkar designen möjligheten att deploya applikationen?

ÖVNING: REVERSE PROXY



/etc/nginx/sites-available/default

```
server {
    listen 80 default_server;
    location / {
        proxy_pass         http://<AppServerIntIP>:5000;
        proxy_http_version 1.1;
        proxy_set_header   Upgrade $http_upgrade;
        proxy_set_header   Connection keep-alive;
        proxy_set_header   Host $host;
        proxy_cache_bypass $http_upgrade;
        proxy_set_header   X-Forwarded-For $proxy_add_x_forwarded_for;
        proxy_set_header   X-Forwarded-Proto $scheme;
    }
}
```

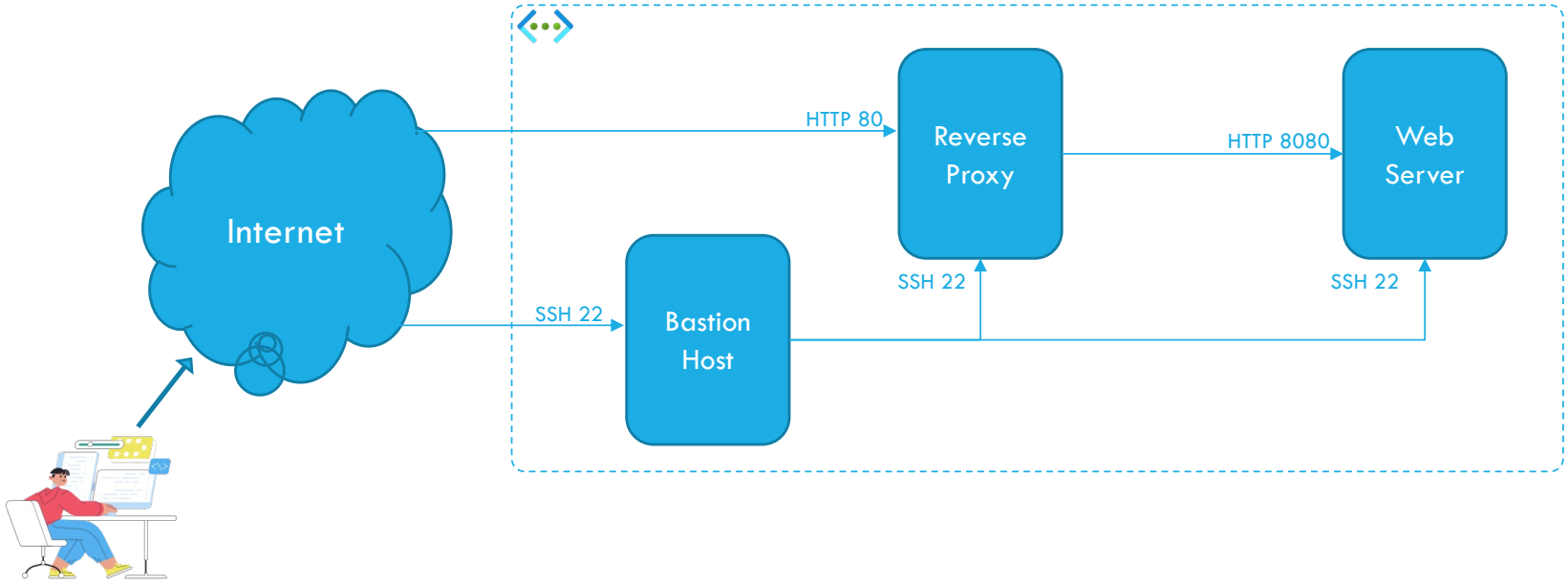
```
sudo nginx -t
sudo nginx -s reload
```

Skapa tre VM

- App Server
  - installera Nginx
- Reverse Proxy
  - installera Nginx som reverse proxy
  - uppdatera server block
- Bastion Host
  - installera fail2ban

Säkerhet

- Designa nätverket så att
  - Det endast går att ansluta via SSH till servrarna via Bastion Host
  - Det endast går att nå applikationen genom Reverse Proxy
- Hur påverkar designen möjligheten att deploya applikationen?


Internet
HTTP 80
Reverse Proxy
HTTP 8080
Web Server
SSH 22
Bastion Host
SSH 22
SSH 22