# 00\_Baseline

Opintojakson Turvalliset tietoverkot etätunneilla tehdään PacketTracerillä opintojakson asioita yhteen nivovaan suurempaa tehtävää useassa eri vaiheessa. Tämä on ensimmäinen osa asioista, jota verkossa tehdään.

Tässä vaiheessa tutustutaan pohjaverkkoon viimeistelemällä se toimintakuntoon ja suorittamalla testaukset.

## Pohjatiedosto

Lataa itsellesi alla oleva pohjatiedosto, jota työstät alla annettujen ohjeiden mukaisesti:

<https://www.dropbox.com/s/pxnqr7udjrjwclk/netw_sec_base_v3.pkt?dl=0>

Tallenna tiedosto itsellesi ja käytä tätä samaa tiedostoa aina jatkossa tehtävän edistyessä. MUISTA TALLENTAA SÄÄNNÖLLISESTI.

## Käytetyt IP-verkot

|  |  |
| --- | --- |
| VERKKO | IPv4 |
| ISP CORE | 10.0.0.0/24 |
|  |  |
| CLOUD SERVICES | 1.0.0.0/24 |
| ISP - COMPANY A HQ | 3.0.0.0/24 |
| ISP - COMPANY B | 2.0.0.0/24 |
| ISP - REMOTE/BRANCH/HOME | 4.0.0.0/24 |
|  |  |
| COMPANY A HQ - CORE | 192.168.0.0/24 |
| COMPANY A HQ - INSIDE USERS (vlan1) | 192.168.1.0/24 |
| COMPANY A HQ - INSIDE SERVERS (vlan2) | 192.168.2.0/24 |
| COMPANY A HQ - DMZ | 192.168.3.0/24 |
| COMPANY A BRANCH | 192.168.4.0/24 |
|  |  |
| COMPANY B  - INSIDE | 192.168.1.0/24 |
| COMPANY B - DMZ | 192.168.2.0/24 |
|  |  |
| HOME OFFICE | 192.168… |
| REMOTE OFFICE | 192.168… |

## Laitteiden IP-asetukset

|  |  |  |
| --- | --- | --- |
| LAITE | LIITÄNTÄ | IPv4 OSOITE |
| ISP1 | G0/0/0 | 1.0.0.1/24 |
| ISP1 | G0/0/1 | 10.0.0.1/24 |
| ISP2 | G0/0/0 | 2.0.0.1/24 |
| ISP2 | G0/0/1 | 10.0.0.2/24 |
| ISP2 | G0/0/2 | 3.0.0.1/24 |
| ISP3 | G0/0/0 | 4.0.0.1/24 |
| ISP3 | G0/0/1 | 10.0.0.3/24 |
| HQ\_ROUTER | G0/0/0 (internet) | 3.0.0.2/24 |
| HQ\_ROUTER | G0/0/1 (inside) | 192.168.0.1/24 |
| HQ\_ROUTER | G0/0/2 (dmz) | 192.168.3.1/24 |
| HQ\_S1 | Vlan1 (users) | 192.168.1.1/24 |
| HQ\_S1 | Vlan2 (servers) | 192.168.2.1/24 |
| HQ\_S1 | G1/0/1 | 192.168.0.2/24 |
| A\_BR\_ROUTER | G0/0/0 (inside) | 192.168.4.1/24 |
| A\_BR\_ROUTER | G0/0/1 (internet) | dhcp |
| ASA | myöhemmin |  |
| HOME | 0/0 | dhcp |
| HOME | 0/1 | 192.168.0.1 |
| MX | myöhemmin |  |

# Tehtävä

## Verkon viimeistely

Pohjaverkko on osittain konfiguroitu. Viimeistele tekemällä seuraavat asetukset:

1. Aseta ISP-reitittimet käyttämään keskenään OSPF-reititystä
2. Konfiguroi HQ-reitttimelle liitäntöjen IP-asetukset taulukon mukaisesti sekä staattinen reititys (oletusreitti ja reitit sisäverkkoon)
3. Konfiguroi HQ\_S1 reitittävälle kytkimelle staattinen oletusreitti
4. Konfiguroi BR-reitittimelle liitäntöjen IP-asetukset taulukon mukaisesti
5. Korjaa WWW-palvelimen oletusyhdyskäytävä osoitteeksi 1.0.0.1

Testaa:

|  |  |  |
| --- | --- | --- |
| LÄHDE | KOHDE | TESTI |
| PC4 | WWW | ping |
| PC4 | WWW | www |
| HQ-ROUTER | WWW | ping |
| BR-ROUTER | WWW | ping |
| BR-ROUTER | HQ-ROUTER | ping |

1. *Mikäli jokin testi ei toimi, niin aloita systemaattisempi vianmääritys, etsi ja korjaa vika! Eteenpäin kannattaa siirtyä vasta, kun testit on läpäisty onnistuneesti.*

## Pääkonttorin netti kuntoon

Konfiguroi pääkonttorin (HQ) “netti kuntoon” eli ne puuttuvat asetukset, jotka mahdollistavat yhteydet WWW-palvelimelle kaikilta pääkonttorin päätelaitteilta sekä muualta Internetistä yhteydet DMZ-alueen palvelimelle. Alla tarkempia ohjeita ja speksejä:

1. Mahdollista työasemille ip-asetusten saaminen palvelimelta dhcp-palvelun avulla. Vinkki: Kuinka dhcp-kyselyn voi ohjata toiseen verkkoon?
2. Toteuta NAT reitittimellä HQ-ROUTER seuraavasti:
   1. USERS-verkko käyttää julkisina IP-osoitteinaan puulia, jossa on osoiteet 3.0.0.128-254
   2. SERVERS-verkko käyttää julkisina IP-osoitteenaan puulia, jossa on osoitteet 3.0.0.64-127
   3. A\_DMZ\_SERVER-palvelinta varten tehdään staattinen NAT julkiseksi osoitteeksi 3.0.0.10

Testaa:

|  |  |  |
| --- | --- | --- |
| LÄHDE | KOHDE | TESTI |
| PC1 ja PC2 | A\_INSIDE\_SERVER | dhcp |
| PC1 ja PC2 | WWW | ping |
| A\_INSIDE\_SERVER | WWW | ping |
| A\_DMZ\_SERVER | WWW | ping |
| PC4 | A\_DMZ\_SERVER julkinen | ping |

1. *Mikäli jokin testi ei toimi, niin aloita systemaattisempi vianmääritys, etsi ja korjaa vika! Eteenpäin kannattaa siirtyä vasta, kun testit on läpäisty onnistuneesti.*

## Haarakonttorin netti kuntoon

Konfiguroi haarakonttorin (BR) “netti kuntoon” eli ne puuttuvat asetukset, jotka mahdollistavat yhteydet WWW-palvelimelle kaikilta pääkonttorin päätelaitteilta. Alla tarkempia ohjeita ja speksejä:

1. Luo BR-ROUTERille DHCP-puuli, jolla jaat IP-asetukset automaattisesti työasemille
2. Toteuta NAT BR-ROUTERilla niin, että kaikki laitteet käyttäjät julkisena osoitteenaan BR-ROUTERin julkisen verkon liitännän IP-osoitetta.

Testaa:

|  |  |  |
| --- | --- | --- |
| LÄHDE | KOHDE | TESTI |
| PC5 | BR-ROUTER | dhcp |
| PC5 | WWW | ping |
| PC5 | A\_DMZ\_SERVER | ping |

1. *Mikäli jokin testi ei toimi, niin aloita systemaattisempi vianmääritys, etsi ja korjaa vika! Eteenpäin kannattaa siirtyä vasta, kun testit on läpäisty onnistuneesti.*

## Extrat

Topologia kannattaa viimeistellä huolellisesti. Mitä paremmin sen tekee, sitä vähemmän on tulevaisuudessa peruskonfiguraation suhteen tekemistä.

1. Tallenna kaikkien laitteiden kofiguraatiot
2. Konfiguroi yrityksen COMPANY A access-kytkimet hallittaviksi valitsemalla niille sopivat IP-osoitteet.

## LOPETUS

Tallenna tiedosto itsellesi. Voit jatkaa tulevia etälabroja aina tästä tilanteesta (tai tehdä kaikki labrat “putkeen”).

## Mallikonffeja (minimit)

!OSPF-reititys, pitää konfiguroida kaikille kolmelle ISP-reitittimelle ja kaikki ne verkot, joihin reititin on liitetty, esim.

#ISP\_2:

router ospf 1

 network 3.0.0.0 0.0.0.255 area 0

 network 10.0.0.0 0.0.0.255 area 0

!staattinen reititys, konfiguroidaan HQ-ROuterille kaksi staattista reittiä:

ip route 192.168.1.0 255.255.255.0 192.168.0.2

ip route 192.168.2.0 255.255.255.0 192.168.0.2

!staattiset oletusreitit HQ ja HQ\_S1 laitteille.

!HQ:

ip route 0.0.0.0 0.0.0.0 3.0.0.1

!HQ\_S1:

ip route 0.0.0.0 0.0.0.0 192.168.0.1

!NAT, konfiguroidaan pääkonttorille ja haarakonttorille.

!HQ:

int gi0/0/0

 ip nat outside

int gi0/0/1

 ip nat inside

int gi0/0/2

 ip nat inside

!HQ USERS-verkon nat:

access-list 1 permit 192.168.1.0 0.0.0.255

ip nat pool USERS 3.0.0.128 3.0.0.254 netmask 255.255.255.0 overload

ip nat inside source list 1 pool USERS

!HQ SERVERS-verkon nat:

access-list 2 permit 192.168.2.0 0.0.0.255

ip nat pool SERVERS 3.0.0.64 3.0.0.127 netmask 255.255.255.0 overload

ip nat inside source list 2 pool SERVERS

!HQ staattinen nat

ip nat inside source static 192.168.3.10 3.0.0.10

!BR:

access-list 1 permit any

ip nat inside source list 1 interface gi0/0/1 overload

!DHCP-konffeja sekä HQ\_S1 että BR laitteille vähän eri tarkoitukseen

!HQ\_s1:lle dhcp-pyyntöjen välistys Inside-serverille Users-verkosta:

int vlan 1

 ip helper-address 192.168.2.10

!BR:lle dhcp-puuli:

service dhcp

ip dhcp pool BR

 network 192.168.4.0 255.255.255.0

 default-router 192.168.4.1

ip dhcp excluded-address 192.168.4.0 192.168.4.7

Joitakin konffeja malliksi:

LOPPU