WSC 2007 Japani karsintatehtävä

Tehtävänäsi on suunnitella, konfiguroida ja testata suurehkolle IT-alan yritykselle IT-infra. Täydellinen suunnitelma IP avaruuksineen, konfigurointineen ja testauksineen päivineen toteutetaan mahdollisimman täydellisenä laboratorioympäristössä. Tämä suunnitelma myös arvioidaan puolueettomien tahojen toimesta.

Parhaan (toimivimman) suunnitelman tehnyt ja toteuttanut palkitaan tiivistunnelmaisella Japanin matkalla loppuvuodesta 2007 ;-)

Nettiyhteydet ovat käytettävissä, kunhan saat ne ensin toimimaan.
Onnea matkaan ja muistakaa että toiminnallisuus ratkaisee!

Yrityksen perustiedot ja henkilömäärät.

Kyseessä on IT alan yritys. Yrityksen henkilöstömäärä on kaiken kaikkiaan vähän alle 1000 kappaletta ja se kasvaa koko ajan.
Yrityksen suomen toimipisteissä voidaan lähteä liikkeelle oletuksesta, että jokaisella työntekijällä on käytössään tietokone ja verkkoyhteys. Ulkomaiden toimipisteissä tilanne on erilainen.

Yrityksen alkuperäinen ja vanha pääkonttori sijaitsee Turussa ja sinne on sijoitettuna noin 500 henkilöä. Pääkonttorissa toimivat yrityksen suunnittelu, markkinointi, hallinto ja tuotekehitys.

Henkilömäärä jakautuu vanhassa pääkonttorissa osastoittain seuraavat:

Suunnittelu	320 hlöä
Markkinointi	40 hlöä
Tuotekehitys	150 hlöä
Hallinto	20 hlöä

Yrityksen laajentuessa pääkonttori jäi pieneksi ja siksi firma on joutunut ostamaan lisää toimitiloja. Uudessa pääkonttorissa toimivat suunnittelu ja tuotekehitysosastot. **Näiden osastojen tulee olla loogisesti samaa verkkoa vanhan pääkonttorin osastojen kanssa.**
Uuden pääkonttorin henkilömäärät ovat:

Suunnittelu	150 hlöä
Tuotekehitys	150 hlöä

Suunnitteluun kaavaillaan kuitenkin jo palkattavaksi lisää henkilöstöä tulevaisuudessa. Visio on maksimissaan noin sadasta hengestä. Markkinointi tarvitsee myös lisää työvoimaa. Tarve on korkeintaan 30 hengelle.

Yrityksen tuotanto on ulkoistettu Intiaan ja siellä olevilla työntekijöillä ei tietokoneita ole käytössään. Kuitenkin tehtaan työnjohto tarvitsee yhteydet kotimaahan. Työnjohdossa on noin 80 henkilöä ja lisää ei olla palkkaamassa. Heidän verkon käyttönsä on erittäin vähäistä, mutta tarve ottaa yhteyksiä suomeen on silti olemassa.

Kysynnän kasvaessa näitä toimipisteitä saattaa tulla maailmalle lisääkin. **Vähintään viiteen toimipisteeseen lisää on varauduttava**. Henkilömäärä näissä tuotantolaitoksissa on vakio.

****

Tehtävä Päivälle 1

Tehtävässä on kuvattu yrityksen tarpeet ja laitteet, jolla testiympäristössä toimitaan. **Toteutustapa- ja järjestys on käytännössä vapaa**, mutta tarpeiden ja vaatimusten mukaisesti luonnollisesti eletään. Tehtävän eri kohtien täydellisestä suorituksesta saatavat pisteet on merkitty paperin oikeaan laitaan.
Huomaa, että jokainen verkkolaite käynnistetään uudelleen ennen arviointia.
****

Osa 1. Yrityksen fyysisen IT:n tarpeet ja kuvaus

Koko testiverkko rakennetaan kahdella Cisco 2621-reitittimellä, sekä Cisco Catalyst 2950 kytkimillä. Tuotantoverkossa on tietenkin käytössä järeämmät laitteet, mutta toiminnaltaan lähes identtiset. Palvelimina toimivat DELL Poweredge 1800 sarjan serverit Perc4/sc RAID-ohjaimella.

Asenna Windows palvelimeen kaksi SCSI-levyä.

1p)

Luo niiden välille RAID-1

2p)

ja asenna Windows 2003 server per seat -tilaan yhdelle osiolle. Osio koko levypakan kokoiseksi.

2p)

Laitehallinnan tulee olla siisti (ei mitään herjoja)

-1p/virhe

Intiaan menevä reititin on edellisen ylläpitäjän jäljiltä jollain tavalla konfiguroituna, mutta ylläpitäjä poistui keskuudestamme. Ota se käyttöön toiseksi reitittimeksi, sekä talleta kaikki mahdollinen olemassa oleva konfiguraatio siitä palvelimelle tekstitiedostoksi kansioon "intia". Tiedoston nimeksi "konffis.txt".

5p)

konfiguraatio tuhottu -3p)

Toinen reititin olikin sitten valmiiksi alustettu, sillä joku on onnistunut tyhjentämään siitä koko Flashin! Palauta IOS reitittimeen. Löydät IOSin työasemaltasi.

6p)

Runkoreititin ja kytkin ovat vanhan pääkonttorin toimitiloissa. Runkoyhteyden tulee olla gigainen. *Reitittimessä tosin ei ole tällä hetkellä kuin sadan megan portit, mutta ei anneta sen häiritä labran pystyttämistä kytkimen puolella.*

1p)

Pääkonttorin AD palvelimelle annetaan myös gigainen yhteys. Voit käyttää kumpaa palvelinta hyvänsä.

1p)

Pääkonttorien välinen verkkoyhteys tehdään kahdennetulla sadan megan ethernet yhteydellä siten, että yhteys toimii normaalisti 200Mbps nopeudella mutta jos toinen katkeaa, niin nopeus vain tippuu 100Mbps:ksi ja yhteys ei mene poikki. Katso tarkemmin kytkennät ja konfiguraatiot seuraavasta osasta.

Kytkennät 1p)

Tee kaksi kaapelia em. kytkinten välille, pituudeltaan liittimien päistä mitattuna tasan metri. Mittaa niiden toiminta. Aikaa näiden kaapeleiden tekemiseen ja mittaukseen on yhteensä kymmenen minuuttia. Kun aloitat, niin ilmoita siitä tuomar(e)ille.

Mitta oikein 2p
Mittaus läpi 2p
Värikoodit oikein 2p
Mitta väärin -1p/sentti
aika ylittyi -4p

Käytettävissäsi on ~2 metrin suoria kaapeleita rajattomat määrät, kaksi parimetristä konsolikaapelia ja yksi sarjakaapeli. Kaikki muut tehtävässä tarvittavat kaapelit joudut tekemään itse. Räkkejä ja laitteita ei tule liikutella. Näiden piuhojen tekemisessä ei ole mitta- eikä aikarajaa, eikä niistä tule plus- tai miinuspisteitä.

Internet-yhteydet Intian päässä ovat niin epäluotettavia, että niihin ei uskallettu luottaa, joten tälle välille on liisattu T1 yhteys suoraan Turusta Intiaan. Yhteys luodaan PPP-protokollan avulla ja käyttäen CHAP autentikointia. Nyt välistä jätetään modeemit pois ja testauksessa käytetään DCE-DTE –kaapelia, jolloin pääkonttorin reititin saa ottaa roolin kellopulssien jakamisessa.

6p)

Firmalla on myös patalaiskoja johtajia, jotka eivät viitsi työpaikalle asti raahautua aina töitä tekemään. Heille tulee luoda "kotiin" langaton verkkoyhteys, josta he voivat sohvalla istuen napata yhteyden työpaikalleen. Käytettävissä on Buffalo airstation, sekä Cisco Aironet tukiasemia. Asenna testipomolle jompikumpi käyttöön. SSID: japani1 Salaukseksi WPA-TKIP ja avaimeksi "woldskills". Tuomarit osoittavat pomon "kotikoneen" ja verkkoliitynnän sijainnin.

4p)

Osa2. Firman loogisen verkon kuvaus

Koko sisäverkon toimintaan on varattu IP avaruus 172.16.32.0/20. **Jokainen erillinen osasto tulee olla hallittavissa pääsylistoin ja reitittimen suodatussäännöin**. DMZ toimii julkisessa IP avaruudessa: 203.197.130.0/28. **Tee verkkosuunnitelma Excel –taulukkoon ja esittele se tuomareille.** Suunnitelmasta tulee käydä ilmi jokaisen osaston verkon verkko-osoitteet, käytettävät IP osoitteet, ja aliverkon peite ja ja yhdyskäytävä (joka verkon ensimmäinen osoite). Varaudu perustelemaan suunnitelmasi.
Myös tulevaisuuden tarpeet ennakoidaan suunnitelmassa.

Mahdolliset tulevien toimipisteiden verkot jätetään verkkoavaruudessa viimeisiksi, josta niitä voidaan "napsia" käyttöön tarvittaessa.

20p

Kaikki IP osoitteet lukuun ottamatta pääkonttorin reitittimen ulospäin lähtevää porttia, tulee olla kiinteitä. DHCP palvelin tuodaan vasta huomenna paikalle ;-)

Reititys

Firman sisäverkkojen reititys hoidetaan sisäisesti kokonaan OSPF-protokollan avulla (Area 0). Ulkoverkkoon, eli operaattorille päin sallitaan pelkän DMZ:n mainostus. Huomaa, että myös mahdollisten uusien tulevien tehtaiden asetusten tulee olla valmiiksi konfiguroituna runkoreitittimeen.

12p)

Kaikki sisäinen liikenne ajetaan ulos internetiin NAT/PAT:in läpi yhtä ja ainutta IP osoitetta pitkin. Tämä osoite tulee operaattorilta automaattisesti. Tuomarit näyttävät liityntärajapinnan sijainnin.

8p)

Vanhan pääkonttorin kytkin konfiguroidaan seuraavasti:

Portit 1-5	Suunnittelu
Portit 6-10	Markkinointi
Portit 11-15	Tuotekehitys
Portit 16-20	Hallinto
Portit 21-22	DMZ
Portit 23&24	Linkki uuteen pääkonttoriin

Uuden pääkonttorin kytkinkonfiguraatio

Portit 1-10	Suunnittelu
Portit 11-20	Tuotekehitys
Portit 23&24	Linkki vanhaan pääkonttoriin.

Eri osastojen nimet ja niitä vastaavat portit tulee pystyä selvittämään kytkimestä käsin.

9p)

Kaikki ulkoapäin tuleva pptp-vpn ohjataan Windows 2003 –palvelimeen, jolla yhteys muodostetaan.

3p)

Verkkokäytännöt ja pääsylistat

Active Directoryä tulee hallitsemaan Windows 2003 Server –palvelinrauta ja se sijoitetaan samaan loogiseen verkkoon Hallinnon kanssa. Anna palvelimen osoitteeksi Hallinnon verkon viimeinen käytettävä IP osoite.

1p)

Tähän kyseiseen palvelimeen tulee päästä siis mistä verkosta hyvänsä, mutta muuten hallinnon verkkoon miltään muulta osastolta ei tule päästä.

3p)

Tuotanto-osastoilta (siis yhdeltäkään) ei tule päästä firman verkon kautta julkiseen internetiin tietoturvaongelmien vuoksi.

5p)

Kaikille muille osastoille nettiyhteydet kuitenkin sallitaan.

1p)

Osastojen välinen keskenäinen liikennöinti on kielletty lukuun ottamatta Hallintoa, joka saa liikennöidä vapaasti mihin haluaa.

10p)

Kaikki osastot saavat kuitenkin ottaa yhteyden yrityksen AD palvelimeen, ja DMZ:taan.

5p)

Ulkoa päin (internetistä) kaikki yhteydet on oletuksena kielletty sisäverkkoon, lukuun ottamatta DMZ:taa. Kuitenkin johdolle on sallittu käyttää pptp-VPN yhteyttä ulkoa sisäverkkoon.

3p)

Runkokytkimelle määritellään VTP domain nimeltä WSC ja otetaan käyttöön v2-tila. Kytkimen tulee toimia VTP Serverinä. Muut suomen kytkimet konfiguroidaan VTP clienteiksi.

5p)

Kaikista reitittimistä ja kytkimistä tulee ottaa varmuuskopio Windows-palvelimen TFTP-palveluun. Niiden ottaminen tulee olla mahdollista myös tulevaisuudessa.

2p)

Asenna Windows palvelimeen syslog-palvelu ja ohjaa kaikki Intian reitittimen kriittiset ilmoitukset tälle palvelimelle.

3p)

Päivä2

Osa 3 Active Directoryn ja Windows palvelimen toiminta.

Palvelimessa on edellisen päivän jälkeen esiasennettuna Windows 2003 server –käyttöjärjestelmä kahden levyn RAID1-osiolla. Ota käyttöön toiset kaksi levyä ja tee myös niistä RAID1.

2p)

Viides levy asennetaan hot-spareksi siltä varalta, että jokin kiintolevy rikkoutuu.

2p)

RAID-ohjaimen hallinta tulisi pystyä hoitamaan myös Windowsista käsin ilman, että konetta tarvitsee boottailla jos tulee vaikkapa levyrikko.

2p)

Jos koneessa ei ole vielä winkkarin Sp1:stä, niin asenna se. Sen voit imuroida joko netistä, tai osoitteesta \\10.5.81.205\jako. Käyttäjä wsc, salasana Qwerty1

2p)

Palvelimeen asennetaan Active Directory ja annetaan sen DNS nimeksi "AD.WSC.fi".

2p)

Jokaisella eri osastolla tulee olla omat organisaatioyksiköt sekä koneille, että työntekijöille.

5p)

Luo palvelimeen seuraavat käyttäjät.

Käyttäjä	Salasana	Ryhmä	Osasto
Antti	Qwerty1	Administrators	Suunnittelu
Olli	Asdfgh2	Administrators	Tuotekehitys
Seppo	Zxcvbn3	Users	Tuotanto
Tomi	Qazwsx4	Backup operators	Markkinointi

4p)

Luo jokaiselle osastolle myös valmis template-käyttäjä, joista uusia työntekijöitä voidaan näppärästi kopioida.

5p)

Yhteiset käytännöt toimialueella:

- Salasana vähintään 6 merkkinen ja viiden salasanan historia tulee muistaa.

2p)

Eri osastoille määrätään seuraavat käytännöt, rajoitukset ja oikeudet.

Hallinto

- oikeus käyttää etäyhteyksiä ja etähallintaa (vpn ja rdp)
- **eivät** saa sammuttaa palvelinta

3p)

Suunnittelu

- jokaiselle oma liikkuva profiili ja kotikansio k: -asemaksi . Kaikille yhteinen työkansio t: -asemaksi.
- ”omat tiedostot” edelleenohjataan kotikansioon

3p)

Tuotekehitys

- työaika kaikilla rajoitettu 9-17. Tämän jälkeen heitetään automaattisesti toimialueelta ulos.

2p)

Markkinointi

- Markkinoinnin jäsenten kirjautuessa toimialueelle, tulee Internet Explorerin välityspalvelimen osoitteeksi pakottaa www-cache.turkuai.fi:8080.
- Heille myös pakotetaan palomuuri käyttöön ilman poikkeuksia.
- Kotikansio verkon yli Z: -asemaksi. Aseman tulee sijaita palvelimen toisella RAID1 osiolla.
- Levytilanrajoitus markkinointiporukalle 50 megaa ja hälytysrajaksi 40 megaa.

4p)

Ajoittain hallinnolla käy vieraita saunatiloissa, jotka haluavat lukea sähköpostinsa. Heitä varten luodaan vierailutunnus, joilla päästään hallinnon verkosta nettiin. Tällä tunnuksella ei kuitenkaan saa olla mitään oikeutta mihinkään palvelimella oleviin työtiedostoihin.

1p)

Liitä käytössä oleva työasemasi (pöytäkone) toimialueelle Intiaan.

2p)

Määrittele, että tuotannon jäsenien kirjautuessa koneelle, pakotetaan asentumaan ryhmäkäytännöllä Adobe Acrobat reader.

4p)

Imuroi netistä WSUS (windows server update services) SP1:n kanssa ja asenna se koneeseesi (palvelimeen).

4p)

Määrittele, että XP:n ja w2k3:n päivitykset ladataan palvelimelle iltaisin kello 23:00.

2p)

Liitä pomon läppäri AD:hen.

1p)

Ajasta päivitykset asentumaan kello 11:30 pakotetusti sekä Intian työasemiin, että pomon läppäriin.

4p)

Vierailija tunnuksen ollessa potentiaalinen tietoturvariski, palvelimelle luodaan systeemi, jolla vieraan työasemalleen päästänyt johtaja, voi luoda satunnaisen kertakäyttösalasanan vieraalle klikkaamalla taustapöydällään olevaa kuvaketta (password).
Käyttäjätunnuksen ja salasanan tulee tulostua ruudulle.

4p)

Kun vieras on poistunut, klikkaa hän toista kuvaketta (reset password) joka muuttaa salasanan satunnaisesti joksikin toiseksi. Tämä ei saa tulostua ruudulle.

3p)

RAS yhteydet

Asenna pptp-vpn -palvelin palvelimelle, jotta pomon etäyhteydet saadaan toimimaan turvallisesti kotoa käsin.

2p)

Pomo seilaa kannettavallaan kodin ja työpaikan väliä ja toisinaan hänen tarvitsee päästä myös kotoansa käsin yrityksen toimialueelle sisään. Pomon kannettavaan rakennetaan VPN tunneli kotoa työpaikalle ja varmistetaan että yhteys toimii myös kotona langattomasti.

2p)

Kannettavan VPN yhteydessä tulee olla mahdollisuus kytkeä se päälle ennen koneelle sisäänkirjautumista, jolloin voidaan kirjautua toimialueelle turvallista yhteyttä pitkin.

2p)

Osa4. LINUX-palvelin

Linux palvelin pystytetään firman DMZ verkkoon ja sen käyttöön tulee julkinen ip osoite. Palvelimen tehtävänä on hoitaa firman julkisia internet palveluita, sekä osia sisäisistä palveluista.
Nimi: linux.wsc.fi
palvelut:

- dns
- www
- dhcp (sisäisille osoitteille)
- sähköposti

DNS PALVELIN

Firma omistaa dns toimialueen wsc.fi. Pystytä DNS-palvelin, joka hoitaa wsc.fi toimialueen pääpalvelimen virkaa. Lisäksi dns palvelimen tulee ylläpitää varmuuskopiota/peiliä firman ActiveDirectoryn dns-palvelimesta.

DNS palvelimen speksit:

- Domain: **wsc.fi**
  Juuripalvelin: linux.wsc.fi
  Domainista tulee löytyä myös seuraavat nimet:
  www.wsc.fi viittaa linux.wsc.fi
  intra.wsc.fi viittaa linux.wsc.fi
  mail.wsc.fi viittaa linux.wsc.fi
  2p)
- Domain: **ad.wsc.fi**
  Juuripalvelin: Windows 2003 palvelin
  2p)
- Käänteinen nimipalvelin julkisille IP osoitteille.
  dns palvelimen tulee jakaa dns nimi kaikille julkisille ip osoitteille, joita wsc.fi domainiin on asetettu. Nimien tulee vastata wsc.fi domainia.
  2p)
- Käänteinen nimipalvelin sisäisille IP osoitteille.
  palvelimen tulee jakaa dns nimet sisäisille ip osoitteille.
  2p)

Vaatimuksena kuitenkin on ettei AD:n tiedot saa näkyä ulkoverkkoon, vain privaatti verkkoon.
2p)

WWW-PALVELIN

Firmalla on tarvetta kahdelle www-palvelulle, julkinen ja sisäinen. Toteuta nämä palvelut linux-palvelimella. Käytössäsi on kuitenkin vain yksi ip osoite, joka on varattu linux palvelimelle. **(2p)**
Julkinen www-palvelu: www.wsc.fi
Sisäinen ww-palvelu: intra.wsc.fi
Muilla dns nimillä tulee näkyä virhesivu, jossa lukee "Palvelua ei ole olemassa" **(2p)**

Asenna myös SSL-salattu http palvelin, jolla pääsee intra.wsc.fi sisältöön. **(2p)**
Molempiin palveluihin tulee päästä sisäverkosta normaalilla salaamattomalla HTTP:llä. **(2p)**
Ulkoverkosta ei kuitenkaan saa päästä intra.wsc.fi palveluun ilman salausta. **(2p)**

Tuomarit toimittavat palveluiden sisällön.

SÄHKÖPOSTI

Asenna linux palvelimeen SMTP postipalvelin, joka vastaanottaa posteja toimialueelle wsc.fi. **(1p)**
Linux palvelin hallitsee sähköpostitunnuksia.
Palvelimen tulee myös välittää eteenpäin virtuaaliverkoista lähetetty posti. **(2p)**
Ulkoverkosta tullutta postia ei saa välittää eteenpäin. **(1p)**
Palvelimen tulee myös vastaantottaa toimialueelle ad.wsc.fi lähetetty posti. **(2p)**

Postiosoitteiden tulee toimia ulkoverkosta muodossa tunnus@wsc.fi
2p)

Käyttäjien tulee pystyä lähettämään ja vastaanottamaan postia mail.wsc.fi palvelinta käyttäen. Protokollina käytetään SMTP ja IMAP protokollia.
2p)

Luo kaksi kokeilutunnusta palvelimelle. pomo@wsc.net ja testi@wsc.net.
2p)

DHCP palvelin

Linux palvelin hoitaa myös kaikki työasemien DHCP kyselyt. Asenna dhcp palvelin siten, että se kykenee jakamaan kaikille osastoille ip-osoitteet. Kaikista osastoista tulevat dhcp kyselyt tulee ohjautua linux palvelimelle.
5p)

Aseta dhcp jakamaan seuraavat yhteysasetukset:
- verkkoasetukset: ip, verkkomaski, yhdyskäytävä
- dns-palvelin: linux-palvelin
- dns-toimialue: ad.wsc.fi

2p)

TIETOTURVA
Linux palvelimella tulee näkyä ulospäin ainoastaan edellämainitut palvelut, sekä SSH etähallintaa varten. Mitään muita verkkopalveluita ei tule sallia.
2p)

Root-käyttäjä ei saa päästä sisälle SSH yhteydellä.
1p)

Liite1 kaaviokuva verkon loogisesta toiminnasta.