WSC 2009 Kanada 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 Kanadan matkalla loppuvuodesta 2009 ;-)

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

Yrityksen perustiedot ja henkilömäärät.

Kyseessä on mobiiliteknologiaan erikoistunut yritys. Yrityksen henkilöstömäärä on kaiken kaikkiaan vähän alle 15000 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 1000 henkilöä. Pääkonttorissa toimivat yrityksen suunnittelu, markkinointi, hallinto ja tuotekehitys.

Henkilömäärä jakautuu vanhassa pääkonttorissa osastoittain seuraavat:

Suunnittelu	445 hlöä
Markkinointi	267 hlöä
Tuotekehitys	213 hlöä
Hallinto	75 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	450 hlöä
Tuotekehitys	250 hlöä

Suunnitteluun kaavaillaan kuitenkin jo palkattavaksi lisää henkilöstöä tulevaisuudessa. Visio on maksimissaan noin kahdesta sadasta hengestä. Markkinointi tarvitsee myös lisää työvoimaa. Tarve on korkeintaan 60 hengelle.

Johtuen suomalaisten liittymisestä EU:n päästökauppaan, tuotanto on ulkoistettu Kiinaan koska paikalliset kivihiilivoimalat eivät tuota saasteita lainkaan. Siellä työskentelevillä henkilöillä ei ole omia tietokoneita käytössään, mutta heidän täytyy pystyä käyttämään yrityksen yhteisiä koneita omilla tunnuksillaan, joten sinun tulee luoda myös heille omat käyttäjätunnukset. Tuotannossa työskentelee noin 10000 henkilöä. Tietokoneita ja muita IP –osoitteita puhuvia laitteita tuotannossa on noin 700 kappaletta.

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

****

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.

Huomaa, että jokainen verkkolaite käynnistetään uudelleen ennen arviointia.

Osa 1. Yrityksen fyysisen IT:n tarpeet ja kuvaus

Verkko tulee olemaan luonnollisesti aika järeä, mutta sen toimintaa simuloidaan ensin laboratorioympäristössä. Tehtävässä käytetään myös tuotantoon otettavia Ciscon verkkotuotteita, joten lopullinen konfiguraatio ja topologia voidaan siirtää tarvittaessa moneen eri laitteeseen.

Tavoitteena on saada aikaan ns. plug and play –verkko, jossa laitteet voidaan lähettää yksinkertaisen ohjeistuksen kanssa toiselle puolelle maailmaa ja laittaa johto kiinni. Konfiguroi laitteen siihen malliin, että tämä onnistuu ja että voit jatkaa konfigurointia suomesta käsin.
Lentolippuja firmalla ei ole varaa ostaa ja liftaamalla perillepääsy ei ole välttämättä itsestäänselvyys. Soutuvene saattaa löytyä toimitusjohtajan kesämökiltä…

Palvelimiksi on hankittu DELL Poweredge 1800 sarjan serverit Perc4/sc RAID-ohjaimella ja kuudella scsi- levyllä.

Serverit tulee asentaa toimintaiskuun niin, että järjestelmä on sekä nopea, että luotettava. Sen pitää kestää myös RAID-ohjaimen hajoaminen ilman, että dataa menetetään. Kuitenkin datan pitää liikkua rivakasti ja yhden kiintolevyn hajoaminen korvataan automaattisesti uudella kiintolevyllä.

Yhteys suomen ja Kiinan välillä toteutetaan käyttämällä E1 –yhteyttä. Rajapintana on V.35 –liityntä. Sinun ei tarvitse välittää muista kuin toimipisteiden laitteista. Suomen, venäjän ja kiinan operaattorit hoitavat datan pisteiden välillä. Labrassa testit suoritetaan käyttämällä välillä olevien modeemien sijasta DCE/DTE –kaapelia.

Suomi-Kiina sarjakaapeliyhteys tulee olla autentikoitu. Muuten veli venäläinen varastaa datan kesken matkan.

Kiinasta on omat nettiyhteydet ulos, joka hoituu paikallisen puhelinoperaattorin ADSL –linjalla. Labrassa ei adsl linjaa kuitenkaan käytetä, vaan tehdään testaukset normaalilla ethernet –verkolla.

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.*

Pääkonttorin AD palvelimelle annetaan myös gigainen yhteys.

Toinen ostamistasi kytkimistä on firmasta pois potkitun työntekijän TJ-pilan jälkeen vailla IOSia. Päivitä siihen uusi käyttöjärjestelmä tuomareiden antamasta tiedostosta.

Toiselle reitittimelle on mahdollisesti käynyt samoin. Tähän ei sitten olekaan IOSia valmiiksi tarjolla.

Pääkonttorin rakennusten 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.

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.

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.

Osa 2. Firman loogisen verkon kuvaus

Liitteessä 1 on suurpiirteinen kuvaus verkon toiminnasta.

Sisäverkossa käytetään 10- sarjan osoitteita. Laske edellisessä osassa saamiesi tietojen perusteella sopivat verkot osastoille ja huomioi tässä myös tulevaisuuden tarpeet. Tee osoitteista **selkeä** dokumentaatio.

Tuotanto-osastoja on tällä hetkellä vain yksi, mutta koska niitä näytetään tarvitsevan lisää, laske valmiiksi viidelle osastolle sopivat verkkoavaruudet.

Kaikkia osastoja tulee olla mahdollista hallita loogisesti omina kokonaisuuksinaan, esimerkiksi reitittimien pääsylistoin. Kaikkien osastojen tulee myös olla yhtä ja samaa loogista verkkoa. Osaston sisäisiä reitityksiä ei haluta, koska se rajoittaisi turhaan liikennöintinopeutta.

Verkossa ei harrasteta reititysprotokollien käyttämistä, joten määrittele kaikki reitit staattisiksi.

Kiina kytketään liisatun linjan kanssa suoraan Suomeen kiinni, mutta tätä yhteyttä käytetään vain AD palvelimien väliseen liikennöintiin ja palvelimen ylläpitoon etäyhteydellä. Muu liikenne kiinasta ajetaan NAT/PAT:in läpi vain yhden IP osoitteen kanssa maailmalle. Kiinalaisilla ei saa olla suoraa pääsyä suomen verkkoon palvelimien välistä liikennettä lukuun ottamatta!

Kiinaan toimitetaan reititin ja kytkin valmiiksi konfiguroituna. Konffaa laitteet toimimaan ja anna ne tuomareille "postitettaviksi". Toimitus kiinaan kestää noin tunnin.

Tuotekehitysosasto pidetään ulkomaailmalta suojassa siten, että sen yhteydet julkiseen nettiin sallitaan vain osoitteen 10.5.145.8 läpi käyttäen TCP-porttia 8080. Muille osastoille ei määritellä rajoituksia, mutta DNS –kyselyt sallitaan **vain** AD-palvelimelle ja siitä ulos. Suoraan julkisen DNS palvelimen (193.94.126.1) kanssa keskustelee vain AD palvelin.

Suomessa niin ikään liikenne ohjataan NATin läpi julkiseen internetiin. Suomessa on kuitenkin trafiikkia sen verran enemmän, että julkiseen verkkoon annetaan viisi IP osoitetta, jota voidaan dynaamisesti käyttää NAT/PATin yhteydessä.

Suojattuja etäyhteyksiä varten sinun tulee ohjata suomen reitittimestä pptp-vpn –liikenne verkon AD palvelimelle. Ts. Pääkonttorin serveriä pitää pystyä hallitsemaan myös muualta tarvittaessa.

Verkossa tulee olemaan myös DMZ –alue, johon voidaan työntää kaikki ulospäin näkyvät palvelimet. DMZ –alueen IP avaruus 10.5.81.112/29

Osa 3. Active Directoryn ja Windows palvelimien toiminta.

Uusiin palvelimiin tulee kaikkiin Windows 2008 käyttöjärjestelmäksi. Firman pääpalvelin sijoitetaan pääkonttorin tiloihin ja samalla otetaan yrityksessä AD –järjestelmä käyttöön.

Kiinaan asennetaan myös Windows 2008 Server, mutta sillä erolla että sen tulee toimia domainin toisena AD-palvelimena, joskin ReadOnly tilassa (RODC). Tämä kyseinen rauta on jo paikoillaan kiinassa esiasennettuna. Sinun tulee hoitaa kaikki konfiguraatiot tähän palvelimeen verkon ylitse. Myös Kiinan DHCP palvelu tulee asentaa tähän samaiseen rautaan.

Firmalla on toimiva palvelin Windows 2003 –alustalla ja sen päällä pyörii putiikin tuotannonohjausjärjestelmä. Rauta alkaa olla kuitenkin jo eläkeiässä ja nopeus ei enää riitä kasvaneen yrityksen tarpeisiin.

Vanha palvelin tulee siirtää uuteen pääkonttorin rautaan virtuaalipalvelimeksi lennossa niin, että se jatkaa toimintaansa aivan kuten ennenkin. Yrityksen käyttöön on myöhemmin tulossa VMWare ESXi virtuaalisointialusta, mutta kustannus syistä nyt yrityksen pääkonttorin palvelimeen asennetaan VMWare Server ja virtuaalikoneet siirretään uuteen virtuaalisointialustaan myöhemmin.

Hoida homma niin, että tähän vanhaan tuotannonohjauspalvelimeen, tai sitä pyörittävään uuteen palvelimeen ei tule yli viiden minuutin käyttökatkosta ;-) Ota yhteyttä tuomareihin, kun aiot laittaa vanhan lihoiksi ja uuden tulille.

Kiinaan tuleville käyttäjille luodaan kaikille tunnus, kotikansiot ja työkansiot valmiiksi. Kansiot sijaitsevat fyysisesti Kiinan palvelimessa.
Luo käyttäjät niin, että käyttäjätunnus on ”ChinaUserX”, missä X on juokseva numerointi. Kaikilla käyttäjillä tulee olla oletussalasanana Qwerty1, joka pakotetaan vaihtamaan ensimmäisen kirjautumisen yhteydessä.

Kotikansio tulee näkyä käyttäjälle X- asemana ja työkansio Z-asemana. Työkansioon on pääsy kaikilla työntekijöillä, mutta kotikansioiden tulee olla privaatteja, pois lukien adminit ja systeemi.

Tietoturvasyistä asiakkaan tietohallinto haluaa, että Domain Admins tasoisia tunnuksia ei heidän verkossaan käytetä.

Tästä syystä sinun tule luoda ADn seuraavat ryhmät:

Ryhmän nimi	**Oikeudet palvelimiin**	**Oikeudet työasemiin**
Server Admins	Administrator	Ei mitään
Workstation Admins	Ei mitään	Administrator

Sekä seuraavat käyttäjät:

Käyttäjä:	**Ryhmä:**	**Salasana:**
srvadmin	Server Admins	Qwerty1
wksadmin	Workstation Admins	Qwerty1

Domainin "Administrator" tunnus tulee nimetä "batman" nimiseksi ja disabloida. Tämä tunnus enabloidaan vain silloin kun sitä tarvitaan ja muuten se pidetään disabloituna.

Kaikkien verkkolaitteiden sisäänkirjautumiset tulee autentikoida Windows 2008:n Radius –palvelimelle. Luo tätä varten serverille käyttäjä "netuser" salasanalla "Qwerty1". Luo em. käyttäjälle ryhmä "netadmins" ja anna ryhmälle oikeus logata verkkolaitteisiin sisään.

Luo myös käyttäjä "vpnuser" ja laita hänet ryhmään "vpnusers". Salli em. ryhmälle vpn:n käyttö W2k8 palvelimen kautta. Huomioi, että vpn käyttäjä EI saa ottaa verkkolaitteisiin yhteyttä ja verkkoadmini EI saa päästä vpn:llä sisään.

VPN:n toiminta tullaan testaamaan ulkoa käsin, joten kirjoita tähän IP osoite, jota pitkin VPN:llä pääsee sisään verkkoon. Tuomarit ovat sen verran laiskoja, että eivät jaksa konffeista asiaa tutkia: _____

Jaa kaikille markkinointiosaston koneille Adobe Acrobat Reader 9 automaattisesti AD:n kautta.

Kiinan serverillä on systeemi valmiiksi asennettuna. Tilatussa serverissä on kuitenkin vielä kolme käyttämättä jäänyttä levyä, joille pitäisi rakentaa RAID 5 järjestelmä. Levyt ovat jo palvelimessa kiinni.

Kiinalaisille käyttäjille, joita tuppaa olemaan aika monta, pitää rajoittaa kotikansioiden koko maksimissaan 10 megatavuun.

Suomessa tulee joka osastolle luoda templatekäyttäjä, jota voidaan hyödyntää uusien

käyttäjien luomiseen.

Osa4. LINUX-palvelin

Linux palvelin pystytetään yrityksen DMZ verkkoon ja sen käyttöön tulee julkinen ip osoite. Rautakustannuksissa säästämiseksi palvelin sijoitetaan Windows 2008 palvelimen päällä pyörivään VMWareen. Palvelimen tehtävänä on hoitaa firman julkisia internet palveluita, sekä osia sisäisistä palveluista.

Firma omistaa dns toimialueen **turhayritys.fi**. Pystytä DNS-palvelin, joka hoitaa **turhayritys.fi** toimialueen pääpalvelimen virkaa. Lisäksi dns palvelimen tulee ylläpitää varmuuskopiota/peiliä firman ActiveDirectoryn dns-palvelimesta. DNS nimien selvitys tulee toimia myös käänteisesti molemmissa domaineissa.

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

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.
Julkinen www-palvelu: www.turhayritys.fi
Sisäinen intranet palvelu: intra.<määrittämäsi domain>
Muilla dns nimillä tulee näkyä virhesivu, jossa lukee ”Palvelua ei ole olemassa”.

Tietoturvasyistä intra sivusto tulee olla SSL-salattu. Tämän lisäksi intra saa olla käytettävissä vain domainin käyttäjillä, kuitenkaan käyttäjät eivät halua kirjoittaa tunnuksia joka kerta kun he menevät intraan, joten authentikointi tulee tapahtua automaattisesti. Intra sivun tulee olla myös kaikkien koneiden internet selaimen aloitussivu.

Linux palvelimen tulee hoitaa myös kaikki Suomen työasemien DHCP kyselyt. Asenna dhcp palvelin siten, että se kykenee jakamaan kaikille osastoille ip-osoitteet.

Kaikista verkkolaitteiden deny –pääsylistoista ohjataan lokit syslog palvelimelle, joka sijaitsee linux –koneessa. Kaikista edellä mainituista hälytyksistä tulee lähteä myös sähköpostia osoitteeseen alert876@gmail.com smtp palvelin on mail.turkuai.fi.

Linux palvelimesta tulee näkyä ulospäin ainoastaan edellä mainitut palvelut, sekä SSH etähallintaa varten. Mitään muita verkkopalveluita ei tule sallia. Tässä tulee kuitenkin ottaa huomioon normaalit SSHn tietoturvamääritykset.

Toteuta Linuxin varmuuskopiointi niin, että Linuxin konfiguraatiotiedostot (/etc –kansion sisältö) varmuuskopiodaan joka yö klo 22 Windows palvelimelle.
Tämän lisäksi nämä varmuuskopiot halutaan ajettavan varmistusnauhalle joka lauantai

klo 01:00.

Yrityksen verkkotulostin HP LaserJet 5 (IP: 10.5.81.13) tulee jakaa verkkoon Linux-palvelimelta. Tulostimen tulee olla myös automaattisesti käyttäjien käytettävissä kirjautuivatpa he mille tahansa yrityksen työasemalle.

Verkkoliikenteen vähentämiseksi tulee yritykselle konfiguroida proxy palvelu käyttöön. Kaikkien koneiden verkkoliikenteen tulee automaattisesti kulkea tämän proxyn läpi.

Liite1

Looginen topologiakuva verkosta