Mälardalen University
School of Innovation, Design and Engineering
Västerås, Sweden

---

DVA227 - Projekt i Nätverksteknik

# Projekt Bolaget

## Projektrapport
## Ver 1 Rev 2

**Grupp 4**

Mikael Andersson
man16057@student.mdh.se
Vilhelm Beijer
vbr16001@student.mdh.se
Isak Söderström
ism16002@student.mdh.se

Kursansvarig, Lärare & Examinator: Joakim Rydén
joakim.ryden@mdh.se
Mälardalen University, Västerås, Sweden

Lärare: Sara Lundahl
sara.lundahl@mdh.se
Mälardalen University, Västerås, Sweden

Skapad: 12 april 2018
Uppdaterad: 21 maj 2018 11:15

# Innehåll



# Figurer



# Tabeller

# 1 Inledning

I början av februari tilldelades vi ett projekt av Johnny Bergklint på Netsecure. Projektet gick ut på att standardisera nya branch-siter åt ett företag, fortsättningsvis benämnt som "Bolaget", som har dessa typer av siter runt om i världen. I denna rapport presenteras resultatet av arbetet kring detta projekt, vilket i stor del går ut på att ta fram designförslag och idéer för att driftsätta nya siter. På grund av sekretessen kring projektägaren kunde inte en fullständigt detaljerad plan levereras, men detta arbetet kan ses som ett embryo till en färdig lösning.

# 2 Hårdvarulayout

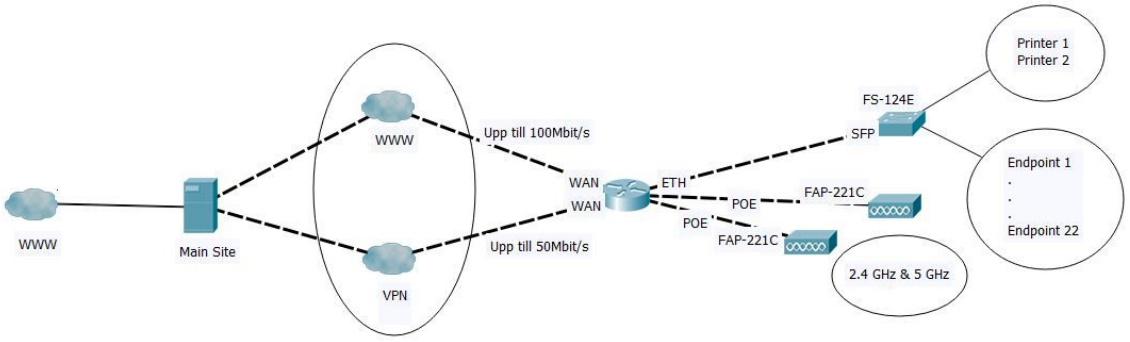
Vi har valt att använda produkter från Fortinet då det finns ett partnersamarbete mellan dem och Netsecure. Vad vi kan se är Fortinets utbud väl tillräckligt för den utrustning vi har valt och priset har legat jämnt eller lägre gentemot andra märken för den prestanda som behövts.

## 2.1 Minimikrav

- Högst 24 personer på varje site.
- Högst 6 kontorsenheter t.ex. printers, ip-telefoner.
- Högst 2 AP:s på varje site, dessa ska stödja dual-radio (dvs 2.4 Ghz & 5Ghz)
- Varje site har upp till två anslutningar till core siterna.
  - En krypterad anslutning över internet med hastighet upp till 100 Mbit/s.
  - En VPN-anslutning över ett privat nätverk som är isolerat från internet med hastighet upp till 50 Mbit/s.

Efter dessa minimikrav designades följande topologi för siterna, vilket kan ses i Figur 2.1:

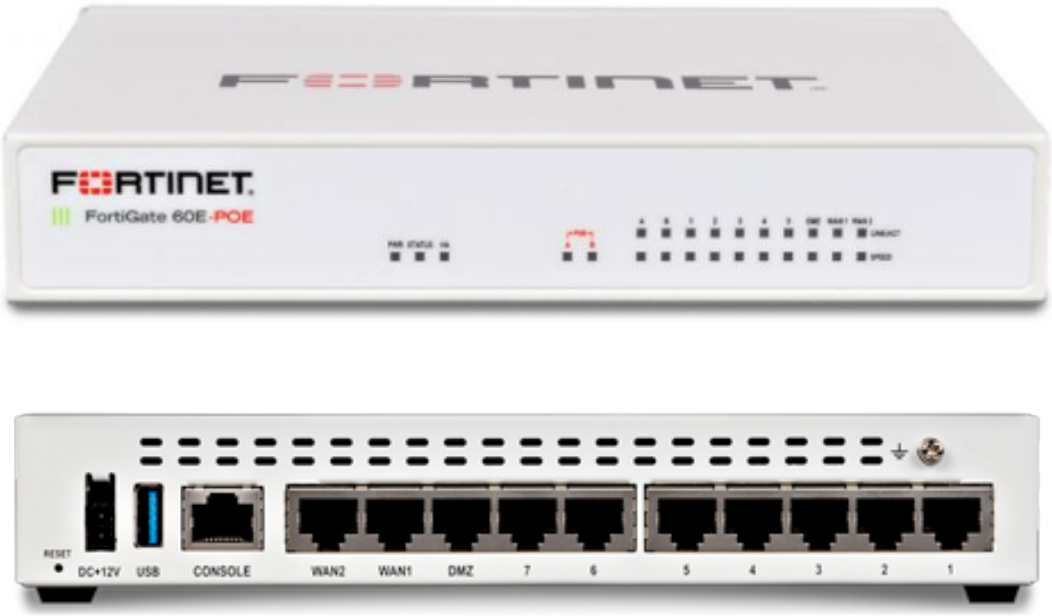
- En FortiGate 60E-PoE router kopplad till ISP och/eller VPN beroende på det lokala förutsättningarna.
- En FortiSwitch 124E kopplad till routern för användare.
- Två FortiAP 221C access-punkter kopplade direkt till routern med PoE.




Figur 2.1: Topologi för hårdvarulayout.

## 2.2 Routing & Brandvägg

Routern och brandväggen som valts till projektets lösning är FortiGate 60E-PoE, se Figur 2.2. Denna routern valdes för att det är den billigaste router som uppfyller minimikraven på överföringshastigheten även när alla brandväggsfunktioner används. Den har tillräckligt många portar för att täcka de behov som behövs samt PoE som behövs till accesspunkter.




Figur 2.2: FortiGate 60E-PoE.

## 2.3 Switching

FortiSwitch 124E är switchen som valdes och precis som med routern var det priset kontra prestanda som avgjorde valet. FortiSwitch 124E är Fortinets billigaste 24-portars switch och en sådan täcker de maximala antalet användare som kan komma att finnas på vardera site. Switchen kan ses i Figur 2.3.


Figur 2.3: FortiSwitch 124E

### 2.4 Wireless

FortiAccessPoint 221C är en av Fortinets enklare trådlösa accesspunkter men innehar tillräckligt med funktionalitet för att täcka de krav som kunden har ställt, exempelvis 2x2 MIMO och dual-radio för att kunna köra både på 2.4Ghz och 5Ghz bandet [1]. Access-punkten kan ses i Figur 2.4.


Figur 2.4: FortiAccessPoint 221C

### 2.5 Fysisk Säkerhet

Vi ger följande rekommendationer för att säkra siternas hårdvara:

- Låsta rackskåp/dörrar där hårdvara är placerad.
- Ge endast fysisk access till personal som anses vara behöriga.
- Utbilda personalen på plats.
- RJ45-lås på anslutna kablar.

## 3 Mjukvarulayout

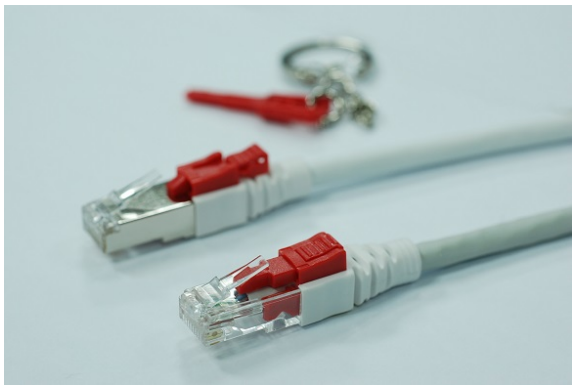
Efter diskussion med projektägare för att ta reda på kundens behov har en lista på funktioner och tjänster tagits fram. Varje funktion eller tjänst förklaras här nedan tillsammans med en motivation till varför vi anser att det bör vara en del av detta nätverk.

### 3.1 IPSEC

Till att börja med måste det förklaras att det som tidigare nämnts som VPN-anslutning egentligen är ett privat nätverk som går mellan vissa siterna or core-siterna. Detta innebär att vissa siterna har koppling till varandra men inte ut på internet förutom via koppling till någon av core-siterna på detta privata nätverk.
Lösningen kommer oavsett vara att sätta upp en GRE-tunnel mellan siten och närmaste core-site, säkra denna med IPsec för att se till att alla paket är krypterade och kräva att all trafik går via core-siterna på väg ut mot internet. Detta ger att alla paket kan bli ordentligt undersökta eftersom den tuffare brandväggen kommer sitta centralt. Hastigheten på VPN-anslutningarna är rapporterat lägre vilket innebär att det på siter där det finns både internet och VPN-anslutning kommer internetanslutningen användas då den har högre hastighet och VPN-anslutningen kommer användas som backup.

### 3.2 Port-säkerhet

Portar måste säkras både fysiskt och i mjukvara, och till det fysiska skyddet är tanken att använda sig av pluggade portar där man sätter in plastpluggar i portarna som gör att kablar inte går att sätta in där. Det finns även plastpluggar som man sätter på befintliga anslutna kablar, se Figur 3.1, som gör att kabeln inte går att dra ut utan att förstöra kabeln. Allt detta används för att förhindra datastöld och olaga intrång i switchar och routrar. När det kommer till mjukvarusäkerheten kommer de portar som inte används vara inaktiverade och på de portar som är i drift används 802.1x där varje användare som ska ansluta sig till det trådade nätverket behöver ett certifikat som godkänns delas ut av PKI-servern och autentiseras med RADIUS mot AD-servern.



Figur 3.1: Ett exempel på säkerhetslås för RJ45-kontakter.

### 3.3 Admin-access & Deployment

Admin-access kommer att lösas genom autentisering mot RADIUS där en användargrupp är konfigurerade som administratörer och med deras inloggningsuppgifter kan de logga in i alla enheter på alla siter. På enheterna kommer det även finnas ett lokalt konto för administratörer som backup ifall enheten inte kan nå RADIUS-servern. All kommunikation mellan administratörer och enheter sker över SSH version 2 och alla konfigurationstillfällen loggas centralt för att hålla reda på vem som gjort vad och när.

Siterna finns i flera olika länder och utrustningen måste skeppas ner dit. När utrustningen transporteras ska det ej finnas någon konfiguration på dem eftersom paketet kan bli stulet. Skulle paketet bli stulet och det exempelvis är brandväggskonfiguration på enheten kan den som stjäl enheten se hur brandväggen är konfigurerad och då hitta eventuella säkerhetshål in i nätverket. Planen är istället att skicka enheterna till siterna helt tomma, och väl på plats koppla upp dem, ge dem en publik IP-adress för att de ska bli nåbara från en av core-siterna och därifrån skicka färdiga konfigurationer till enheten som läser in detta och sedan är klar för att kopplas ihop med det resterande nätverket.

### 3.4 DNS

Alla core-siter kommer att ha en DNS-tjänst rullande på samma server som AD, vilket betyder att det kommer vara åtminstone en per core-site och dessa är redundanta mot varandra precis som AD är mellan core-siterna. Skulle mot förmodan alla DNS-servrar gå ner samtidigt kommer användarmaskinerna kopplas mot Fortiguards DNS (En säkerhetsfunktion som ingår i brandväggen) för att kunna ta sig ut på internet.

### 3.5 Storm Control

Storm control har valts att läggas till som funktion i vår lösning för att det är en enkel och bra lösning som skyddar LAN från DOS-attacker eller dålig nätverkskonfiguration. Trafik som stormar, vare sig det är på grund av en angripare eller felaktig konfiguration, skapar onödig trafik på nätverket och degraderar nätverks prestanda. Konfiguration av Storm control på Fortinet-switchar är globalt på hela switchen och görs genom att specificera en maximal tröskel i paket per sekund (pps) [2, s. 48]. Om denna gräns överstigs blockar switchen några paket från att gå igenom tills pps har blivit mindre än den tillåtna tröskeln.

### 3.6 NTP

Tidssynkronisering i nätverk är en väldigt viktig del när man ska administrera, säkra och lösa eventuella problem som kan uppstå i ett nätverk. Detta för att de flesta problem kan bara fastställas och lösas när man vet vad som hände och när det hände och utan den exakta tiden är det ofta omöjligt att bestämma var problemet ligger. NTP har valts som protokoll för tidssynkronisering för att det anses vara ett State of the Art tidssynkroniserings-protokoll och tidsförskjutningen är bara någon millisekund över internet och ännu lägre på ett lokalt LAN. NTP-servern är tänkt att bli placerad på core-siterna som sedan de mindre siterna synkroniserar sig emot. På grund av att NTP använder ett hierarkiskt system för synkronisering kan siter som tappar anslutning mot core fortfarande ha rätt tid då den närmsta enheten mot NTP-servern kommer bli ansvarig för synkronisering. Detta är viktigt eftersom tiden fortfarande då är rätt och synkad med andra enheterna i nätverket även när siten inte kan nå core.

### 3.7 Loggning

Att sätta upp ett bra system för att övervaka och spara loggar i ett nätverk är kritiskt för både administration och säkerhet. I vår lösning har vi tänkt att spara loggar lokalt i 24 timmar för trafik som går igenom routrarna och sedan skicka de loggarna till en central loggserver på core. Om siterna inte kan nå core och ladda upp sin logg för de senaste 24 timmarna ska de sparas lokalt tills de kan kommunicera med core igen. Fortinet-enheter kör FortiOS och det erbjuder en robust loggningsmiljö där man kan övervaka, spara samt rapportera trafik och event som har med brandväggen att göra [3]. Man kan både välja att spara lokalt på enheten och skicka till en eller flera loggservrar.

### 3.8 DHCP

En DHCP-server är tänkt att placeras ut lokalt på varje site för att dela ut IP-adresser för det spann som den siten är tilldelad. Genom att placera en DHCP-servern på varje site istället för på core kommer det leda till att de lokala enheterna på siterna fortfarande kan få en IP-adress tilldelad även om den siten inte kan nå core. FortiGate 60E på varje site kommer att användas som den lokala DHCP servern för att den är enkel att konfigurera och behöver man inte ha någon extra server bara för DHCP.

### 3.9 Firewall

FortiGate har en inbyggd brandvägg med IPS och threat protection [4]. Med hjälp av FortiGuard kan varje FortiGate snabbt uppdatera dess signaturlistor för kända virus, trojaner och maskar att blockera. FortiGuard har också ett inbyggt App Control-system för eventuella begränsningar av förbjudna program eller tjänster. FortiGate 60E-PoE-modellen kan med alla tjänster aktiverade skyffla 200 Mbps av data, väl tillräckligt för det satta minimikravet.

### 3.10 FortiClient

FortiClient är Fortinets egna program för end-point-skydd, dvs ett antivirusprogram för klienter [5]. FortiClient använder FortiGuard för att enkelt kunna uppdatera dess signaturlista. Dock är det upp till användarna att säkra sin utrustning för att vi inte har någon kontroll över deras enheter så vi kan endast rekommendera ett antivirus skydd.

### 3.11 RADIUS

FortiGates kan enkelt konfigureras så att klienter ska autentisera med vald metod (MS-CHAP, CHAP, PAP) till en RADIUS server. Helst bör ett autentiserat certifikat användas för att säkerställa att RADIUS servern är genuin.

### 3.12 NAT

NAT används inom hela nätverket då kanske endast ett eller ett fåtal publika IP-adresser finns tillgängliga och alla enheter samt klienter använder privata adresser. Dock behöver siternas routrar inte behandla NAT då enligt vår föreslagna design konverteras all NAT-trafik hos core-siterna innan data skickas ut på publikt internet.

## 4 IP-Design

Tanken med IP-designen är att använda privata adresser över hela nätverket. Detta på grund av att all trafik från siterna kommer gå över en VPN-länk till Core och därefter ut på nätverket. Detta innebär att hela företagets nät blir ett virtualiserat privat nätverk. För att adressering ska vara så enkel som möjligt blir varje site tilldelad ett löpnummer som representerar den andra oktetten i IP-adressen (ex. 10.**55**.0.0) vilket då är IP-adressen till site nummer 55. Den tredje oktetten i IP-adressen representerar de olika VLAN som finns på siten (ex. 10.55.**20**.0) som är IP-adressen för site nummer 55 och VLAN 20. På det här sättet finns det även utrymme för expansion av fler siter då de enkelt kan läggas till utan att IP-planen behöver göras om. Det är också enkelt att avveckla siter och då frigöra det IP-spannet för användning till en annan site.

### 4.1 VLAN

Det ska finnas minst 5 VLAN på varje site, en för varje typ av användare/enhet som finns på siten. Dessa VLAN är MGMT, User, Office Equipment, Wi-Fi och Guest. Om det finns fler typer kan flera VLAN läggas till. De olika VLAN:en ska inte kunna kommunicera direkt med varandra av säkerhetsskäl med undantag från till exempel User och Office Equipment då det kan vara en användare på User VLAN:et som vill kunna printa ut något. Vi ser ingen anledning till att en Guest användare ska kunna kommunicera med User- eller Office Equipment-VLAN:en. Exempel på IP-adresserna för VLAN:en kan ses i Tabell 4.1.

Tabell 4.1: Exempel på delegering av VLAN

| | |
|---|---|
| MGMT | 10.0.10.0/24 |
| User | 10.0.20.0/24 |
| Office Equipment | 10.0.30.0/24 |
| Guest | 10.0.40.0/24 |
| Wi-Fi | 10.0.50.0/24 |

### 4.2 Subnetting

Eftersom varje VLAN får ett eget spann på 253 användaradresser behöver ytterligare subnetting inte genomföras. Alla siter och enheter har tillräckligt med adresser för att hålla subnettingen enkel och lätt att förstå.

## 5 Test

Testdelen av denna rapport är mer utav av checklista för uppsättning av nya siter, med punkter för vad som ska göras innan miljön sätts upp och vad man bör undersöka för att se till att enheterna fungerar som de ska.

### 5.1 Hårdvara

Här nedan presenteras sådant som är viktigt att tänka på inför driftsättningen av hårdvaran på en ny site.

#### Routing & Switching

- Är enheterna inkopplade på ett korrekt sätt?
- Starta igång enheten och sätt i USB-minnet med start konfigurationen så att enheten kan ta emot resterande konfiguration från core.
- Ta emot konfigurationen från core och driftsätt nätverket.
- Kan enheterna nå core?
- Kan enheterna nå varandra i det lokala nätverket?
- Aktivera alla tjänster.
- Deaktivera alla oanvända portar.
- Plugga alla oanvända portar.
- Låsa använda portar med RJ45-lås.
- Alla enheter ska vara inmonterade i rackskåp som ska låsas.

#### Wireless

- Montera Accesspunkterna.
- Koppla till routern och lås kontakten.
- Gör enheten redo för att ta emot konfiguration från core.

### 5.2 Funktioner/tjänster

Här presenteras en checklista för de tjänster som ska startas vid driftsättning av ny site, och vad som är viktigt att funktionstesta under själva driftsättningen.

#### IPsec

- Sätt upp både VPN och GRE-tunnel om möjligheten ges.
- Kontrollera att man kan pinga från site till core på båda anslutningarna om båda finns.
- Använd Wireshark eller liknande för att undersöka att paket krypteras korrekt.

**DNS**

- Pinga DNS-servern på core för att se att den är online.
- Se till att enheterna kan ta sig till alla backup-DNS:er inklusive den utanför core.

**DHCP**

- Kolla att DHCP-utdelning fungerar.
- Är IP-adresserna som delas ut korrekta?

**Firewall**

- Starta brandväggen.
- Uppdatera databasen med signaturer och se till att den är aktuell.
- Testa att nå ut på internet med program som inte ska nå ut och se till att de blir blockerade korrekt. (ex. Facebook-chatt fungerar, men inte video eller upload/download.)

**Loggning**

- Fungerar loggningen och skickar den till core.
- Om anslutningen till core går ner sparas loggningen lokalt tills den kan skickas igen till core.
- Loggas det som ska loggas?

**RADIUS**

- Se till att allt som använder RADIUS som autentiseringsmetod fungerar ex. 802.1x, SSH.

**NTP**

- Se till att NTP-servern på core är synkar mot en genuin tidskälla.
- Kontrollera att alla enheter har samma tid och är synkroniserade med NTP-servern på core.

**VLAN**

- Är VLAN-en korrekt uppsatta?
- Se till att de VLAN som ska kunna kommunicera kan det och de VLAN som inte ska kunna kommunicera inte kan göra det.
- Kolla så att enheter är på rätt VLAN.

# 6 Avslut

Detta är det lösningsförslag som vi tagit fram och vi hoppas att det ska vara till nytta i framtiden. Vi vill uttrycka ett tack till NetSecure och Johnny för att vi fick ta oss an detta projekt, det har varit både intressant och lärorikt.

## Referenser

[1] Fortinet Inc. (mars 2018). FortiAP Series, Fortinet Inc, URL: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiAP_11ac_Series.pdf (hämtad 2018-05-07).

[2] ——, (12 oktober 2015). FortiSwitch Admin Guide, Fortinet Inc, URL: https://docs.fortinet.com/uploaded/files/2466/fortiswitchos-admin-guide-33x.pdf (hämtad 2018-05-07).

[3] ——, (16 december 2014). FortiOS Handbook - Logging and Reporting for FortiOS 5.0, Fortinet Inc, URL: https://docs.fortinet.com/uploaded/files/1084/fortigate-loggingreporting-509.pdf (hämtad 2018-05-07).

[4] ——, (april 2018). ForiGate/FortiWiFi 60E Series, Fortinet Inc, URL: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_FortiWiFi_60E_Series.pdf (hämtad 2018-05-07).

[5] ——, (2018). FortiClient, Fortinet Inc, URL: https://www.forticlient.com/ (hämtad 2018-05-07).