Hej Grabbar,

Ber om ursäkt att det tagit lite tid för få svar på frågorna!  
Finns på skype johnny.bergklint som jag är inloggad på under arbetstid så skulle ni få lite snabbare svar 😊

Frågor från mail:

* Har du synpunkter/åsiker på tidsåtgången specad i aktivitetslistan?  
    
  *Såg att punkt 2.2 och 2.2.2 är väl ungefär samma sak, punkt 1.4 brukar vi kalla ”rutin för driftsättning” när vi gör uppstartning av alla nya siter. Även vid uppgraderingar och ändringar skall en ”rutin för driftsättning” göras innan ändringar i produktion skapas.*
* Har du synpunkter/åsiker på riskerna & åtgärderna specade i Riskanalysen?

*Riskanalysen saknar beroende från gruppen, vid sjukdom eller bortfall samt beroende av stöd från mig som också kan ses som en risk.*

* Vad är lägsta och högsta internethastighet på de olika siterna?  
    
  *Internethastigheterna varierar beroende på vart i världen som siten finns, den lägsta internethastigheten är T2 line, alltså ungefär 6,3 Mbit/s. VPN uppkopplingarna har minst 2 Mbit/s men flesta har 10 Mbit/s och uppåt.*
* Hur många siter finns det ungefär, hur många nya per år är målet?  
    
  *Det finns idag ca 68 siter, man kan räkna med att minst en avveckling och en tillökning om året i snitt.*
* Vad är lägsta och högsta mängden människor som arbetar på vardera site?  
    
  *Det tre huvudsiterna har fler användare, men vi räknar med ett snitt på 3-4 personer per site som jobbar för er kund. Ungefär 250 - 280 personer ute på siterna som inte är på huvudsiterna. Tokyo och Chicgo har ungefär 20-25 medarbetare medans Stockholm har bort mot 60 stycken. Sen finns det kunder som finns på siterna, det kan variera allt ifrån 1-10 personer på platserna som hyr in sig på infrastrukturen som skall vara segmenterat utanför.*
* Utöver funktionerna listade i den första versionen av WBS’n, har du några ytterligare funktioner och tjänster som vi kanske har missat och bör undersöka?  
    
  *Det jag ser som inte är med eller undersökt är backup och konfigurationshantering när det blir så många siter.*

Frågor från chatt:

* Har fortigate något gre eller ipsec transport mode?   
    
  *Fortigate har fullt IPsec stöd.*
* vad är skillnaden på internetanslutningarna, vpn vs vanlig internet ?  
    
  *VPN nätet är isolerat buret av en leverantör över hela världen dock okrypterat, för att inte alla levererar internet eller finns vissa siter som inte bör skicka företagsdata över internet.*
* Kan vi köra dubbel brandvägg om allt ska genom coresite, så kör enkel brandvägg på varje site och tät brandvägg på core?   
    
  *Det kan vara bra att tänka på redandes vid de tre stora siterna, men ute på resterande siterna räcker det med enkla brandväggarna.*
* Har varje site 1 eller 2 linor till ISP?   
    
  *Siterna är fördelat ungefär lika mellan ISP, ISP och VPN och bara VPN.  Det är enbart Stockholmskontoret som kommer behöver två ISP.*
* Hur brukar ni jobba med forticlient?  
    
  *Forticlient är till för enddevices, med funktioner för webfilter och antivirus samt brandvägg direkt på klienterna. Det används dock inte i denna lösning idag, idag används ett annan produkt för klientskyddet, med kompliteringar från IPS, AV och Webfilter på brandväggar.*
* Hur löser man bristande funktionallitet på linux?   
    
  *Får nog utveckla denna fråga, men vid bristfällande system (vilket OS det än är) så är bra tumregel med att separera och bara tillåta kommunikation med Applicationskontroll.*
* Kör ni fortigates egna anti-virus, eller får var man klara sig själv?   
    
  *Vi kör Fortigates AV som komplement till det klientskydd som finns på datorerna idag.*
* Hur mycket kontroll behövs? Kolla alla paket, även lokalt på datorn, eller bara det som snurrar över nätet.  
    
  *All trafik som kommer till eller lämnar siterna skall vara kontrollerade av AV, APP, IPS och även webfilter.*
* Bättre definierad kund, dom 50 användarna som sitter på vardera site, är det individuella anställda eller uthyrda linor till företag?  
    
  *De kunder som finns ute på siterna är personer som oftast jobbar på svenska företag som behöver ett kontor eller temporärt kontor, så det finns segmenterat nät som avancerat gästnät med kontroll för AV, APP och IPS.*
* Har vi kontroll över dessa 50 användares egna devices, eller är BYOD?  
    
  *Det är BYOD och vi har inget ansvar men bör rapportera om sker något på nätet som är onormal.*
* Om dom hyr ut till små företag alt. individuella kunder, sitter dom lokalt där eller går linan ut till dom på annan ort?  
    
  *De sitter lokalt.*
* Ska wi-fi täcka någonting annat än dom som arbetar på plats?   
    
  *Skall vara teckning där dom sitter och jobbar.*
* Vilken typ av säkerhet behövs på wi-fi, aka, ska ordinarie arbete bara ske på trådad anslutning och wi-fi endast användas till slösurfning?  
   *För internt och för mobiler skall det trådlöst skall det vara uppsatt med EAP-TLS i två olika nät, för kunder skall ett PSK också det avskilt från allt annat, sen skall det finnas ett gästnätverk med CAP.*
* Vad är CAP?  
  *CAP är captiveportal, oftast kopplad till gästnät eller liknande för att kunna fånga upp trafik för autentiserar/registerna gäster på en portal för att ha koll på vem som gör vad.*
* Är FortiGuard värt att använda eller ska vi använda någon annan form av app-kontrol?  
    
  *FortiGuard är riktigt bra, uppdaterar signaturer och du kan även skicka upp egna findings. FortiGuard är ett nätverk som ger alla brandväggar elller övriga säkerhetsprodukter från Fortinet med information om nya hot.*