YRKESHÖGSKOLAN
NOVIA

VPN-lösningar för arbetsstationer och mobila enheter

Daniel Westerholm

Examensarbete för Tradenom (YH)-examen

Utbildningen i Informationsbehandling

Raseborg 2019

EXAMENSARBETE

Författare: Daniel Westerholm
Utbildning och ort: Informationsbehandling, Raseborg
Handledare: Klaus Hansen & Per-Erik Finell

Titel: VPN-lösningar för arbetsstationer och mobila enheter

Datum 26.2.2019 Sidantal 37

Abstrakt

Det här examensarbetet är gjort på uppdrag av Oy Snellman Ab som är en koncern inom livsmedelsindustrin. Snellman koncernen är intresserad av att undersöka om Direct Access (arbetsstationer) och IBM MaaS 360 VPN (mobila enheter) kan vara ett komplement till koncernens nuvarande VPN-lösning, eller om man kan förenkla autentiseringen med hjälp av certifikat. De krav som ställs är att VPN-lösningen ur användarnas synvinkel behöver vara enkel och samtidigt säker ur IT-avdelningens synvinkel.

Sammanfattningsvis rekommenderas det att man för arbetsstationer ska ta ibruk en certifikat baserad autentisering istället för att implementera Direct Access. Detta p.g.a. att Direct Access är svår att implementera och att trafiken till- och från servern inte går att övervaka, vilket var ett viktigt krav som ställdes på den kompletterande VPN-lösningen.

För mobila enheter rekommenderas det också att man tar ibruk en certifikat baserad autentisering istället för ibruktagning av IBM MaaS 360 VPN. Jag ser det inte som någon nödvändighet att investera i IBM MaaS 360 VPN, eftersom den funktionsmässiga skillnaden mellan dessa två lösningar är så minimal. Det går enkelt att distribuera Checkpoints egna VPN-applikation och alla inställningar med hjälp av MDM-tjänsten IBM MaaS 360 till alla mobila enheter. I framtiden behöver man ännu utreda hur man på ett smidigt sätt kan distribuera certifikaten till de mobila enheterna och även lagra dessa på en säker plats.

Språk: Svenska Nyckelord: VPN, Direct Access, IBM MaaS 360 VPN, Checkpoint

---

OPINNÄYTETYÖ

Tekijä: Daniel Westerholm
Koulutus ja paikkakunta: Tietojenkäsittely Raasepori
Ohjaaja: Klaus Hansen & Per-Erik Finell

Nimike: VPN-ratkaisut työasemalle ja mobiililaitteelle

Päivämäärä 26.2.2019 Sivumäärä 37

Tiivistelmä

Tämä opinnäytetyö on tehty toimeksiantona elintarvikekonserni Snellman Oy:lle. Snellmanin konserni on kiinnostunut tutkimuksesta Direct Access:in työasemien ja IBM MaaS 360 VPN mobiililaitteiden kyvyistä täydentää konsernin nykyisiä VPN-ratkaisuja. Niillä voidaan myös yksinkertaistaa todennusta varmenteiden avulla. Vaatimukset opinnäytetyön tutkimukselle ovat, että VPN-ratkaisun tulee olla yksinkertainen käyttäjien näkökulmasta ja samaan aikaan turvallinen IT-osaston näkökulmasta.

Yhteenvetona suositellaan että varmennetta käytetään työasemalla todennuksena sen sijaan että Direct Access toteutettaisiin. Tämä johtuu siitä, että Direct Access on vaikea toteuttaa ja että tietoliikenne palvelimelle ja palvelimesta ei toimi ilman valvontaa. Valvonta oli tärkeä vaatimus täydentävälle VPN-ratkaisulle.

Mobiililaitteelle suositellaan myös, että varmennetta käytetään todennuksena. Sen sijaan IBM MaaS 360 VPN:n käyttöönottamista ei suositella. En pidä välttämättömänä, että VPN:ään sijoitetaan IBM MaaS 360, koska toiminnallinen ero näiden kahden ratkaisun välillä on niin minimaalinen. Yksinkertaisin tapa on jakaa Checkpoint omaan VPN-sovellukseen ja kaikki asetukset MDM-palvelun IBM MaaS 360 avulla kaikille mobiililaitteille. Tulevaisuudessa tarvitaan vielä tutkimusta siitä, miten sujuvalla tavalla voidaan jakaa varmenne mobiililaitteelle ja myös varastoida se turvalliseen paikkaan.

Kieli: Ruotsi Avainsanat: VPN, Direct Access, IBM MaaS 360 VPN, Checkpoint

---

BACHELOR'S THESIS

Author: Daniel Westerholm
Degree Programme: Business Information Technology, Raseborg
Supervisor: Klaus Hansen & Per-Erik Finell

Title: VPN-Solutions for Workstations and Mobile Devices

Date 26.2.2019 Number of pages 37

Abstract

This thesis is done on behalf of Oy Snellman Ab which is a concern in the food industry. The Snellman group is interested in investigating if Direct Access (workstations) and IBM MaaS 360 VPN (mobile devices) could potentially be a complement to the concern's current VPN-solution, or if the authentication process could be simplified through the help of certificates. The requirement for the VPN-solution is from an IT-department's perspective that it needs to be simple and safe.

This paper notes that it is recommended that a certificate based authentication method is used for workstations instead of implementing Direct Access. This is because of the difficulty of the implementation of Direct Access as well as the fact that the traffic to and from the server is not monitorable, which was a demand made regarding the additional VPN-solution.

For mobile devices it is also recommended that a certificate based authentication method be used instead of IBM MaaS 360 VPN. I don't see any necessity of investing in IBM MaaS 360 VPN because of the minimal difference in functionality between the two solutions. One could easily distribute Checkpoint's own VPN-application and all necessary settings with the help of the MDM-services IBM MaaS 360 VPN to all mobile devices. In the future there is still a need of investigating how to easily the certificates are distributed to the mobile devices and also how to store them in a secure location.

Language: Swedish Key words: VPN, Direct Access, IBM MaaS 360 VPN, Checkpoint

---

Innehållsförteckning

Förord

Jag vill rikta ett stort tack till Oy Snellman Ab som gett mig chansen att få utföra mitt examensarbete hos dem. Jag vill speciellt rikta ett stort tack till min handledare Per-Erik Finell från Oy Snellman Ab och Sami Laihorinne från Jakobstads Nejdens Telefon för all handledning under examensarbetets gång. Jag vill också tacka min handledare Klaus Hansen från yrkeshögskolan Novia som gett mig många bra tips och råd under skrivandets gång av examensarbetet.

1 Inledning

På våren 2016 gjorde jag min branschpraktik på IT-avdelningen hos Oy Snellman Ab. Jag trivdes väldigt bra och frågade därför av IT-chefen John Aspnäs om det skulle finnas någon möjlighet att få utföra mitt examensarbete där. Han berättade att det fanns en hel del projekt på kommande och därför blev jag lovad att få utföra mitt examensarbete därpå följande år. På vintern 2017 diskuterade jag med John och min handledare Per-Erik Finell om olika projekt som man kunde använda som examensarbete. Jag blev intresserad av ett alternativ som gick ut på att undersöka om man kunde ta ibruk Direct Access (avgiftsfritt) och använda som en kompletterande VPN-lösning på majoriteten av alla arbetsstationer och om det är värt att köpa till IBM MaaS 360 VPN och använda på majoriteten av alla mobila enheter. Det ingick också att undersöka möjligheten att förenkla autentiseringen för den nuvarande VPN-lösningen från Checkpoint (finns redan, en extra funktion i brandväggen) med hjälp av certifikat. I avsnitt 1.3 om målet med examensarbetet så kommer jag berätta ännu noggrannare vad examensarbetet går ut på. Det fanns egentligen två anledningar till varför jag blev intresserad av just det här alternativet och valde att utföra det här som examensarbete. Den första anledningen är att jag alltid har varit intresserad av att förstå hur datorer och nätverk är uppbyggda och kommunicerar med varandra och under utbildningen så växte mitt intresse ännu mera, då vi gick kurser i datakommunikation samt nätverk och operativsystem. Den andra anledningen är att jag väldigt gärna vill fördjupa mina kunskaper så väl teoretiskt som praktiskt inom det här området och eventuellt kunna börja arbeta med det här i framtiden.

1.1 Problembeskrivning

Det problem som användarna upplever med den nuvarande VPN-lösningen är att den anses vara onödigt krånglig och tidskrävande. Detta för att innan en VPN-tunnel kan upprättas in till företaget så behöver användarna utföra en del manuell hantering, med manuell hantering menas t.ex. antalet klickningar och inskrivning av användarnamn och lösenord. Allt det här manuella arbetet som upprättandet av en VPN-tunnel förorsakar gör att användarna tycker det blir för jobbigt och på det sättet inte använder speciellt ofta.

1.2 Syfte

Uppdragsgivarens syfte med det här examensarbetet är att få en enklare VPN-lösning som man kan använda på majoriteten av alla användares arbetsstationer och mobila enheter som skulle förenkla användningen av VPN för att kunna arbeta utanför kontoret.

Mitt eget syfte med det här examensarbetet är att utveckla mina kunskaper om nätverksteknik och IT-säkerhet, eftersom det här är ett stort och intressant område för mig som jag gärna vill börja arbeta med i framtiden.

1.3 Mål

Jag kommer att dela in mitt examensarbete i två delmål och presentera dem närmare här nedanför.

Det första delmålet är att ta reda på om man kan implementera Direct Access i deras nuvarande infrastruktur och använda på majoriteten av alla arbetsstationer som bara behöver kunna upprätta en krypterad VPN-tunnel in till företaget, eller om man skulle kunna förenkla autentiseringen för deras nuvarande VPN-lösning Checkpoint Endpoint Security med hjälp av certifikat.

Det andra delmålet är att ta reda på om man borde införskaffa IBM MaaS 360:s egna VPN-lösning och använda på majoriteten av alla mobila enheter som bara behöver kunna upprätta en krypterad VPN-tunnel in till företaget, eller om man skulle kunna förenkla autentiseringen för deras nuvarande VPN-lösning Checkpoint Capsule Connect & Capsule VPN med hjälp av certifikat.

1.4 Krav

Det ställs förstås också några krav på de kompletterande VPN-lösningarna. Här nedanför presenteras alla krav som ställs och dessa krav kommer senare att användas i en tabell. I tabellen betygsätts sedan VPN-lösningarna beroende på hur bra de uppnår alla krav.

- Enkelhet innebär hur lätt det är för användarna att upprätta en krypterad VPN-tunnel in till företaget. Det handlar t.ex. om att minska antalet klickningar som användarna behöver utföra innan VPN-tunneln är upprättad.

- Distribuering innebär hur lätt det är för IT-avdelningen att distribuera ut VPN-lösningen till användarnas arbetsstationer och mobila enheter.

- Implementering innebär hur lätt det är att implementera VPN-lösningen i deras nuvarande infrastruktur.

- Felsökning innebär hur lätt det är att felsöka om eventuella problem uppstår. Det kan t.ex. vara att en användare inte kan nå en viss specifik server och då behöver det vara lätt att lokalisera var problemet är.

- Spårbarhet innebär hur lätt det är att spåra trafik till- och från Direct Access servern eller VPN-servern för IBM MaaS 360 VPN. Det här kan t.ex. vara att få fram information om vilken användare eller IP-adress som har tagit kontakt med servern och vilken tid det har hänt.

- Skräddarsydda regler innebär hur lätt det är att skapa skräddarsydda regler i brandväggen. Dessa regler kan t.ex. bestå av att blockera vissa IP-adresser från att använda vissa applikationer eller att nå vissa specifika servrar inom företaget.

- Kontroll av trafik innebär att all trafik som kommer in mot brandväggen så behöver granskas av dess virusskydd, intrångsskydd samt applikations- och innehålls filtreringen och om något av dessa inte tillåts passera så blockeras det.

1.5 Avgränsning

Till först hade jag planerat ett examensarbete som skulle ha blivit lite för stort och omfattande att utföra som examensarbete. Jag har därför efter råd från min handledare i skolan valt att avgränsa examensarbetet och endast fokusera på teorin för följande VPN-lösningar nämligen Direct Access, Checkpoint Endpoint Security, Checkpoint Capsule Connect & Capsule VPN och IBM MaaS 360 VPN. Det kommer därför inte att ingå någon uppbyggnad av testversion eller implementation på varken arbetsstationer eller mobila enheter.

1.6 Uppdragsgivare

Jag kommer att utföra det här examensarbetet åt Oy Snellman Ab som är verksamma inom livsmedelsindustrin och deras verksamhet delas in i fem olika verksamhetsområden. Dessa verksamhetsområden är köttförädlingen, färdigmat, foodservice, panini och djurmat. Det

första bolaget som hör till koncernen är Snellmans Köttförädling Ab med fabriken i Jakobstad och är tredje största bolaget inom köttbranschen i Finland. De två andra bolagen tillverkar färdigmat och dessa är Snellmanin Kokkikartano Oy och Carolines Kök Ab med fabriker i både Finland och Sverige. Det tredje bolaget är Snellman Pro Oy med sitt kontor i Jakobstad och är verksamma inom foodservice branschen, vilket innebär att man säljer in Snellmans produkter till restauranger och skolkök. Det fjärde bolaget är Mr. Panini Oy med fabriker i både Finland och Sverige, de tillverkar bröd med valfri fyllning som kan grillas i en smörgås grill. Det femte och sista bolaget är Oy Mush Ltd med fabriken i Jakobstad och de tillverkar djurmat åt både hundar och katter. Inom koncernen så är Leena Laitinen verkställande direktör och personalstyrkan uppnår till totalt 1342 personer och omsättningen uppgick till totalt 296 miljoner euro år 2016. Inom koncernen arbetar alla aktivt för att uppnå deras vision, mission och värderingar och det här har resulterat i nöjda kunder och personal. I figur 1 visas mera information om hela koncernen t.ex. vilka bolag som ingår i koncernen, personalstyrkan för respektive bolag och omsättning. (Snellman 2016)

- Vision: *Mest gillad. Genom kontinuerlig förbättring – vägvisare inom livsmedelsbranschen.*
- Mission: *Vi ger möjlighet till det bättre.*
- Värderingar: *Bemöt andra som du själv vill bli bemött.*

SNELLMAN I KORTHET 2016

VERKSAMHET	BOLAG	BRAND	PERSONAL 31.12.2016	OMSÄTTNING milj. €
KONCERN Snellmankoncernen består av moderbolaget Oy Snellman Ab och fem verksamhetsområden: köttförädling, färdigmat, food service, panini och djurmat.	Oy Snellman Ab	SNELLMAN KONSERNI – KONCERNEN	Totalt 1342	Totalt 296 milj. €
KÖTTFÖRÄDLING Köttförädlingen tillverkar kvalitativa kött- och charkprodukter. Till verksamheten hör primärproduktion, slakteri samt mångsidig tillverkning av färskkötts- och charkprodukter.	Snellmans Köttförädling Ab S-Frost Oy Figen Ab	Snellman figen	967	217 milj. €
FÄRDIGMAT Matfabriken som vill ge människor möjlighet till bättre färdigmat.	Snellmanin Kokkikartano Oy Carolines Kök AB	KOKKIKARTANO Carolines KÖK	222	51 milj. €
FOOD SERVICE Snellman Pro erbjuder högklassiga produkt- och tjänstelösningar för professionella kök.	Snellman Pro Oy	SNELLMAN pro PARASTA MEILTÄ. JA MAAILMALTA.	22	27 milj. €
PANINI Ett produktkoncept med enkel och snabb mat av farskt inhemskt bröd.	Mr. Panini Oy	Mr. Panini	60	12 milj. €
DJURMAT Till 100 procent naturligt, högkvalitativt färskfoder för hundar och katter.	Oy MUSH Ltd	MUSH	37	7 milj. €

Figur 1. Snellman koncernens dotterbolag och dess verksamhetsområden (Snellmans årsberättelse 2016, s. 6).

2 Teori

I teoridelen tas teorin upp som ska ge läsaren en djupare förståelse vad examensarbetet handlar om. Det tas bl.a. upp vad skillnaden är mellan de olika tjänsterna för hantering av mobila enheter som t.ex. EMM, MDM, MAM och går sedan djupare in på vad säker överföring av data innebär. Därefter tas det upp vad VPN innebär och vilka tekniker det finns för att tunnla trafik mellan en användare och server. Tar också upp vad kryptering innebär

och vilka tekniker det finns för att kryptera information. Till sist tas det också upp vad autentisering är och hur det går till.

2.1 EMM

EMM (Enterprise Mobility Management) är en molnbaserad tjänst som kopplar samman användare, mobila enheter, applikationer och dokument. Med EMM kan man som IT-administratör på ett säkert och kontrollerat sätt övervaka och hantera företagets tillgångar samt dokument och även låta användare utnyttja de möjligheter som det mobila arbetslivet erbjuder. I EMM ingår samma funktionaliteter som också ingår MDM och MAM. Jag kommer i de två följande avsnitten att berätta noggrannare om vad MDM och MAM är. Några kända tillverkare av EMM är MobileIron, VMware AirWatch och Samsung Knox. Några nyckelfunktioner som ingår är

- Central styrning av säkerhetsparametrar och policyer
- Enkel integrering med befintlig infrastruktur (Exchange, Active Directory, PKI)
- Rollbaserad konfiguration av slutanvändarprofiler (EVRY u.å.)

2.2 MDM

MDM (Mobile Device Management) är en molnbaserad tjänst som hjälper IT-administratören att kunna hantera mobila enheter på distans, eftersom dessa inte alltid är fysiskt tillgängliga på kontoret. MDM är ett gemensamt namn för en tjänst som tillåter hantering av mobila enheter och inte något speciellt namn för någon tillverkares egna tjänst. Det finns ett flertal olika tillverkare av MDM-tjänster på marknaden och några av dessa är MobileIron, VMware AirWatch och IBM MaaS 360. Det finns många funktioner som ingår i MDM-tjänster och några av dessa är.

- Funktioner som möjliggör att man kan konfigurera egna regler som ökar säkerheten t.ex. regler som bestämmer hur långt och vilka tecken ett lösenord måste innehålla och regler över vilka applikationer som behöver skyddas av ett lösenord.

- Funktioner som möjliggör reglering av vad användarna har möjlighet att utföra med sina mobila enheter. Det kan t.ex. vara vilka applikationer som användarna får installera och inte får installera eller om man tillåts att fabriksåterställa sina mobila enheter.

- Funktioner som avskiljer applikationer som hör till företaget från resten av den mobila enheten antingen i form av en PIN-kod eller uppritande av ett mönster. Det här skyddet är bra om t.ex. barn leker med mobila enheten så kommer barnen inte åt applikationer som hör till företaget som t.ex. innehåller e-post eller annan hemlig information eftersom dessa skyddas av ett lösenord.

- Avancerade funktioner för säkerheten som möjliggör att man kan radera information eller låsa den mobila enheten på distans. Om den skulle bli borttappad eller stulen så går det också att få fram en geografisk positionering på distans.

En MDM-tjänst hjälper t.ex. användare vid ibruktagning av nya mobila enheter eftersom man bara behöver starta upp och lägga in sitt användarnamn, lösenord och domän, därefter installeras allting klart helt automatiskt. Den får all nödvändig information och inställningar från molnbaserade tjänsten t.ex. vilka trådlösa nätverk som behöver finnas, vilka applikationer som ska installeras och inställningar för VPN-profilen. Det händer ibland att mobila enheter blir stulna och då behöver man snabbt få dessa låsta eller tömda och med hjälp av MDM-tjänsten är det väldigt enkelt. (Bergström 2014, 14)

2.3 MAM

MAM (Mobile Application Management) är precis som MDM en tjänst som möjliggör hantering, tillgång, styrning och installation av applikationer som har hämtats från Google Play, Appstore eller applikationer som ägs av företag.

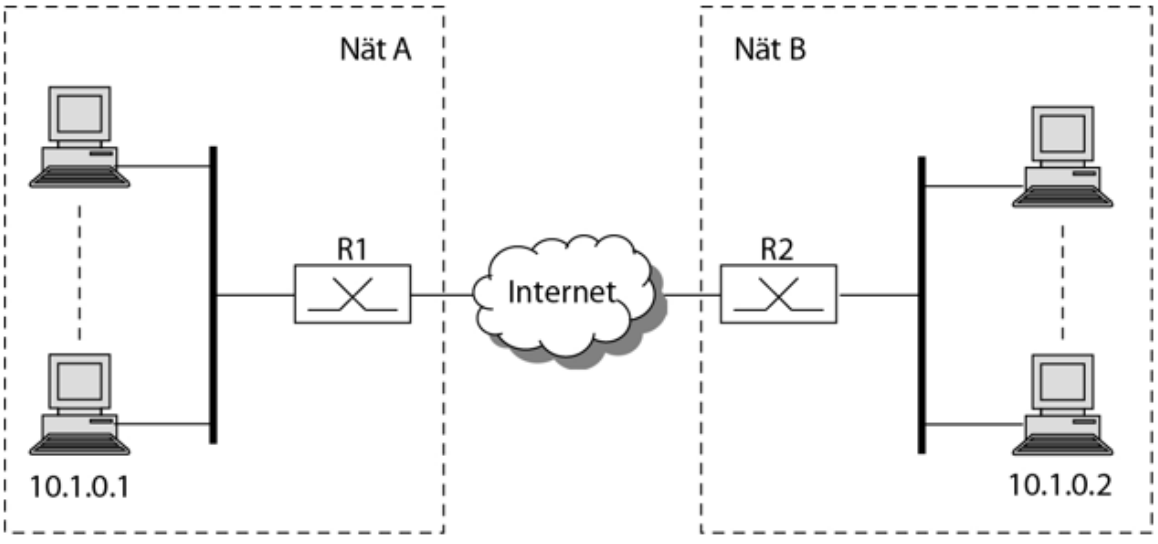
Den stora skillnaden mellan MAM och MDM är att MDM fokuserar på hantering av hela den mobila enheten, medan MAM endast fokuserar på hantering av applikationer. Därmed får man med MAM mindre kontroll över hela mobila enheten, men desto mer kontroll över applikationer.

MAM ger därmed möjlighet att kunna hantera ungefär samma saker som med MDM, men det här görs istället på applikationsnivå. Detta möjliggör att man på ett enkelt sätt kan hantera vilka applikationer som kan ta kontakt med varandra och undvika att viktig information hamnar i fel applikation. Tillverkare av MAM har ofta egna utvecklade applikationer som t.ex. webbläsare, e-post, kalender, kontakter och fildelning. Dessa applikationer är säkra och synkroniseringen mellan applikationerna fungerar bra. (Bergström 2014, 14-15)

2.4 VPN

I ett hem finns det oftast ett flertal uppkopplade apparater med interna IP-adresser som alla är placerade bakom en NAT-enhet. I och med att apparaterna är placerade bakom en NAT-enhet så är alla också skyddade mot avlyssning, eftersom att ingen kommunikation går över internet. Om däremot två användare som befinner sig i samma subnät, men på olika geografiska platser vill kunna kommunicera med varandra på ett säkert sätt, då krävs det en teknik som kallas för VPN. VPN (Virtual Private Network) är en teknik som möjliggör att två användare som befinner sig i samma subnät, men på olika geografiska platser ska kunna kommunicera med varandra på ett säkert sätt över internet med hjälp av en krypterad VPN-tunnel.

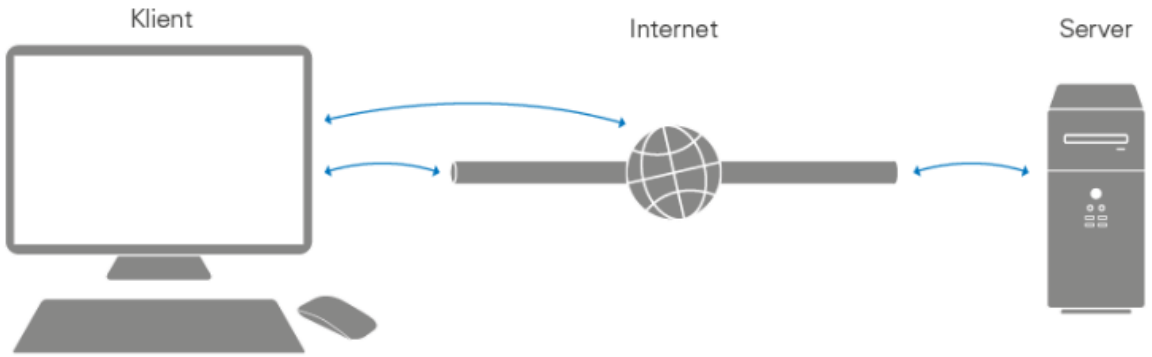
Jag kommer utgående från figur 2 att förklara hur det går till ifall två användare som befinner sig i samma subnät, men på olika geografiska platser ska kunna kommunicera med varandra över internet med hjälp av en krypterad VPN-tunnel. Om t.ex. användaren med IP-adress 10.1.0.1 som befinner sig i Nät A vill kunna skicka information till en annan användare med IP-adress 10.1.0.2 som befinner sig i Nät B. Det hela börjar med att routern R1 tar reda på att användaren med IP-adress 10.1.0.2 befinner sig i Nät B. Den information som användaren med IP-adress 10.1.0.1 vill skicka så packas ner och krypteras med IPSec och skickas sedan iväg till routern R2. Routern R2 packar sedan upp informationen och levererar den vidare till användaren med IP-adress 10.1.0.2. Det är IPSec krypteringen som garanterar att kommunikationen mellan R1 och R2 skyddas mot avlyssning. (Kihl & Andersson 2013, 210-211)



Figur 2. VPN-exempel. (Kihl & Andersson 2013, 211)

2.5 Split tunneling

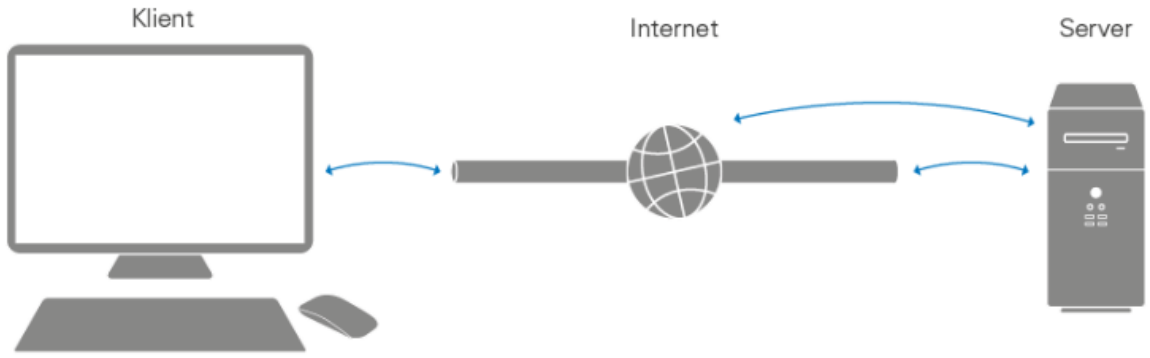
Split tunneling är en teknik som innebär att användare både kan vara anslutna till vanliga internet och samtidigt till företaget. Det här möjliggör för användarna att skicka trafik som innehåller information om företaget igenom en VPN-tunnel, men samtidigt inte skicka vanlig trafik igenom VPN-tunneln. Det här gör att företaget inte behöver investera så mycket pengar i en VPN-tunnel med stor kapacitet. I figur 3 visas hur split tunneling tekniken fungerar. (Kjell 2018)



Figur 3. Split tunneling. (Kjell 2018)

2.6 Full tunneling

Full tunneling är en teknik som innebär att all trafik skickas igenom samma VPN-tunnel. Det spelar ingen roll om trafiken innehåller information om företaget eller om det bara är vanlig internet trafik så kommer allt att skickas igenom samma VPN-tunnel. Fördelen med den här tekniken är att användarna kommer att kunna kringgå geografiska begränsningar, eftersom de använder sig av VPN-tunnelns IP-adress ute på internet. Nackdelen är att det krävs mycket mera kapacitet eftersom all trafik går igenom VPN-tunneln. Det här resulterar i att företaget behöver investera mycket mera pengar i en VPN-tunnel med större kapacitet som klarar av att hantera all trafik. I figur 4 visas hur full tunneling tekniken fungerar. (Kjell 2018)



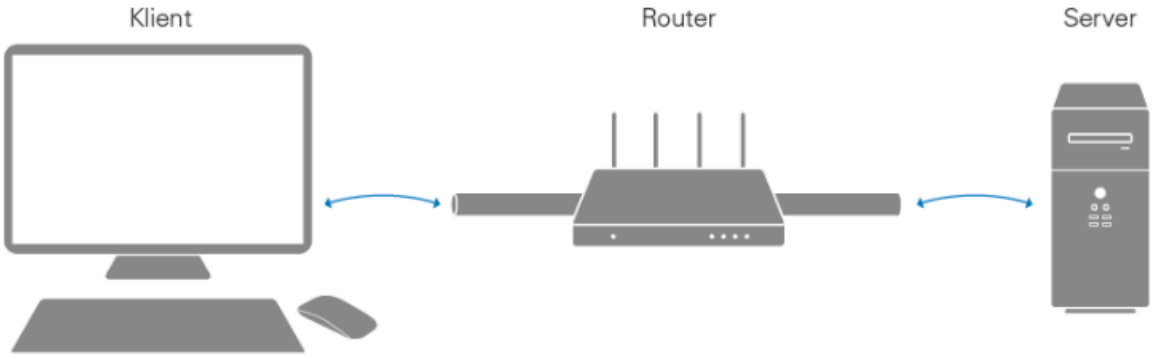
Figur 4. Full tunneling. (Kjell 2018)

2.7 Router

Det är ofta vanligt att användare är placerade bakom en router och för att en VPN-tunnel ska kunna upprättas så behöver routern stödja någon av följande tekniker antingen pass through eller endpoint. Om routern inte stödjer någon av de ovannämnda teknikerna så kommer användarna inte att kunna upprätta någon VPN-tunnel. Jag kommer som nästa att förklara skillnaden mellan dessa två tekniker. (Kjell 2018)

2.7.1 Pass through

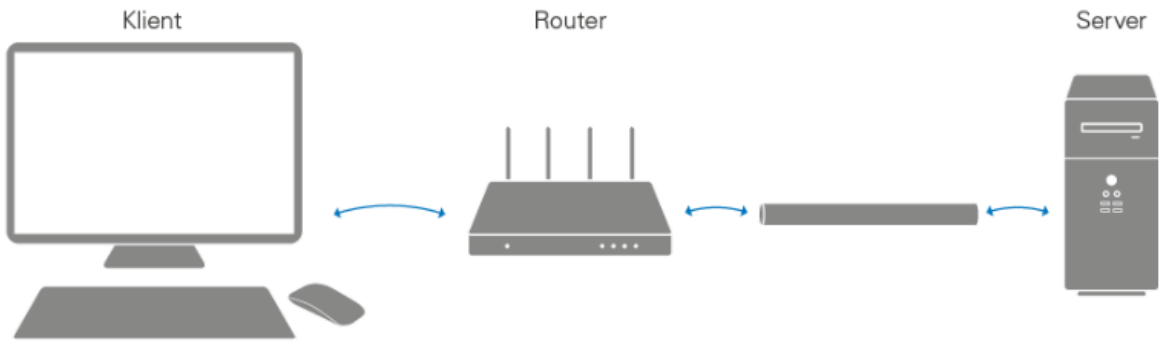
Den första tekniken är pass through och det innebär att routern endast kan släppa igenom en VPN-tunnel till användaren som har upprättat VPN-tunneln. Det här innebär att endast användaren som upprättat VPN-tunneln också är den enda som kan skicka trafik igenom tunneln. Den här tekniken är betydligt vanligare hos routrar för konsumenter än hos endpoint vars routrar är lämpligare för företag. I figur 5 visas hur pass through tekniken fungerar. (Kjell 2018)



Figur 5. Pass through. (Kjell 2018)

2.7.2 Endpoint

Den andra tekniken är endpoint och här innebär det att routern blir slutdestination i VPN-tunneln. Det här innebär att alla användare som är anslutna till routern också kommer att skicka sin trafik igenom VPN-tunneln. Denna teknik är betydligt vanligare hos routrar för företag än t.ex. pass through. Ofta används den här tekniken inom större företag som består av flera mindre företag. Alla användare i de mindre företagen ansluts till deras gemensamma router och deras router ansluts till det större företagets gemensamma router. Det här gör att ingen VPN-tunnel behöver upprättas enskilt för varje användare. I figur 6 visas hur endpoint tekniken fungerar. (Kjell 2018)



Figur 6. Endpoint. (Kjell 2018)

2.8 Kryptering

Kryptering handlar i grund och botten om att göra information som sänds över internet omöjligt att läsa för icke behöriga personer. Det här kan göras på flera olika sätt, men några av dessa sätt är att antingen använda ett kodsystem som är ett överenskommet sätt att byta ut bokstäver mot andra bokstäver, ord eller meningar. Ett annat sätt är chiffer som kastar om bokstäver och siffror och det här resulterar i att informationen blir oläslig innan den okrypteras av mottagaren. Det finns två typer av krypteringsalgoritmer som används för att kryptera och okryptera information. Den första typen är symmetrisk kryptering och andra är asymmetrisk kryptering. Jag kommer att gå igenom dessa två krypteringsalgoritmer här nedanför.

Den första krypteringsalgoritmen är symmetrisk kryptering och här används samma krypteringsnyckel av både sändare och mottagare. Sändaren använder krypteringsnyckeln och en krypteringsalgoritm och mottagaren använder samma krypteringsnyckel och en okrypteringsalgoritm. Innan t.ex. sändaren skickar iväg ett meddelande så krypteras det med hjälp av krypteringsnyckeln och krypteringsalgoritmen. Efter att mottagaren tagit emot

meddelandet så behöver mottagaren använda samma krypteringsnyckel och okrypteringsalgoritmen för att okryptera meddelandet.

Den andra krypteringsalgoritmen är asymmetrisk kryptering och här används två olika krypteringsnycklar. Den första krypteringsnyckeln är publik och används av både sändare och mottagare. Den andra krypteringsnyckeln är privat och används endast av mottagaren. Innan t.ex. sändaren skickar iväg ett meddelande så krypteras meddelandet med hjälp av den publika krypteringsnyckeln. Efter att mottagaren tagit emot meddelandet så används den privata krypteringsnyckeln för att okryptera meddelandet. (Kihl & Andersson 2013, 202-203)

Det finns två olika typer av krypteringar nämligen kryptering av filer och kryptering av trafik. I och med att det här examensarbetet kommer att behandla VPN-lösningar så kommer jag att fokusera på kryptering av trafik. Kryptering av trafik innebär att all information som färdas mellan en sändare och mottagare åker igenom en krypterad VPN-tunnel och det här förhindrar därmed utomstående att kunna se vilken information som färdas eller vilka webbplatser man besöker. Det är dock värt att notera att information som färdas inuti VPN-tunneln inte är krypterad. Jag kommer som nästa att gå igenom de två vanligaste teknikerna för kryptering av trafik nämligen SSL och IPSec. (Edström & Fridh Kleberg 2015)

2.8.1 SSL

SSL (Secure Socket Layer) är en teknik som används för att upprätthålla en säker och autentiserad förbindelse mellan en användare och server. Den här tekniken används främst vid uträttandet av bankärenden över internet eller om man handlar produkter över internet.

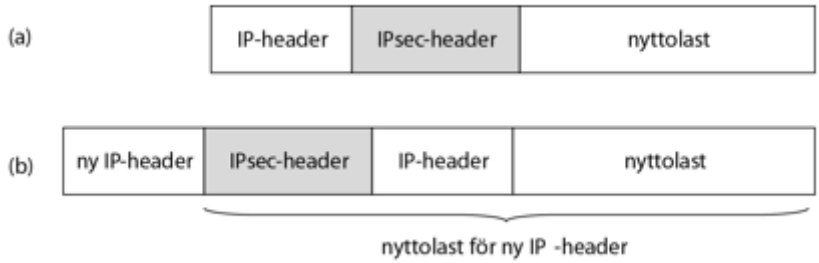
SSL använder sig av transport protokollet TCP (Transmission Control Protocol) och ligger placerat som ett eget skikt mellan applikations- och transportskiktet. Inom SSL tekniken används alltid HTTPS-protokollet vilket innebär att all information krypteras, istället för det vanliga HTTP-protokollet där ingen information krypteras. En SSL session startar alltid med att en användare tar kontakt med servern via en URL-adress (Uniform Resource Locator) som börjar med HTTPS och det första som händer är att servern blir autentiserad för användaren genom att uppvisa ett certifikat. Efter det används certifikatet av användaren för att styrka identiteten hos den certifikatutfärdare som certifikatet representerar och det hela avslutas med att användaren och servern får tillgång till en hemlig krypteringsnyckel. Denna krypteringsnyckel används för att kryptera och okryptera information som färdas mellan användaren och servern. Inom SSL tekniken används symmetrisk kryptering.

Styrkan med SSL tekniken är att information som färdas mellan en användare och server skyddas mot avlyssning från obehöriga eller mot att ändringar görs i informationen. Det här p.g.a. att all information krypteras med antingen en 128 eller 256 bitars krypteringsnyckel. Desto högre antal bitar det är på krypteringsnyckeln så desto svårare blir det för obehöriga avlyssnare att knäcka krypteringsnyckeln. Svagheten med SSL tekniken är att information inte skyddas, ifall servern som användaren kommunicerar med har fått utfärdat ett falskt certifikat av en falsk certifikatutfärdare. Det här gör att användare riskerar att bli utsatta för bedrägerier på internet. (Kihl & Andersson 2013, 220-221)

2.8.2 IPSec

IPSec (Internet Protocol Security). IPSec:s uppgift är att upprätthålla säkerhet för alla IP-paket som färdas mellan två användare över internet. Grundprincipen med IPSec är att två användare kommunicerar med varandra över internet via en säker och logisk förbindelse. Den här säkra och logiska förbindelsen sätts upp och hanteras av ett signaleringsprotokoll som kallas SA (Security Association). Om endast en SA-förbindelse används så kan sändaren bara sända någonting åt mottagaren, vilket kallas för simplex kommunikation. Om mottagaren däremot vill kunna sända någonting tillbaka åt sändaren, då krävs det två SA-förbindelser, vilket kallas för duplex kommunikation.

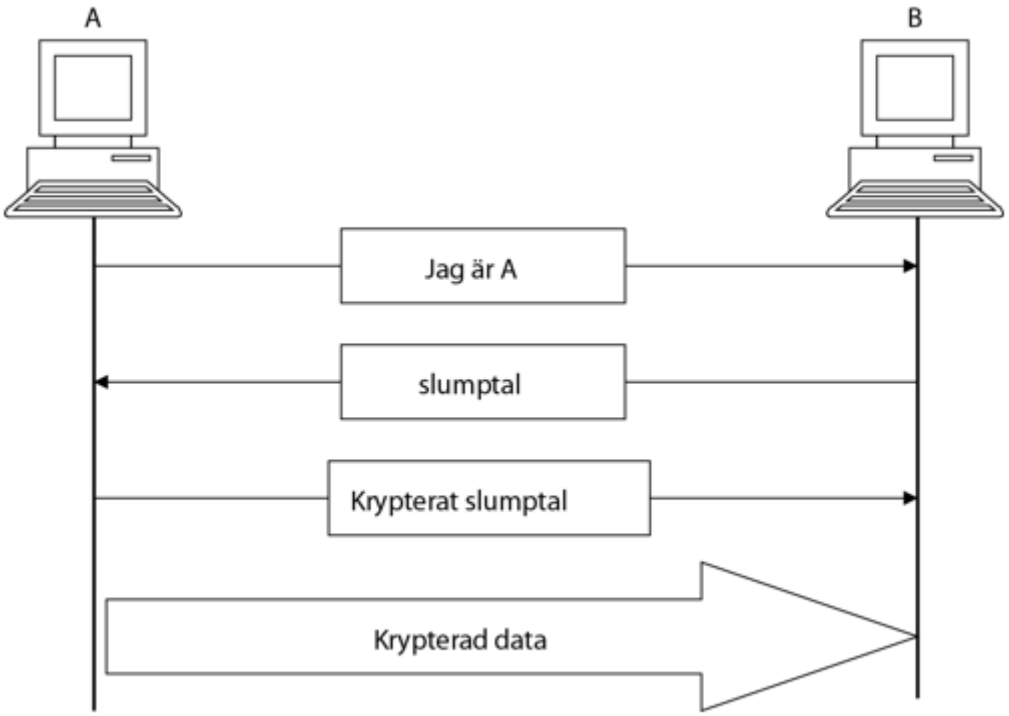
Det går antingen att använda IPSec i transport mode eller tunnel mode. Grundprincipen med både transport- och tunnel mode är att en extra IPSec-header läggs till det nuvarande IP-header paketet. IPSec-headern läggs in på olika ställen beroende på om transport- eller tunnel mode används. I transport mode läggs IPSec-headern in mellan IP-headern och nyttolasten, se figur 7. IPSec: (a) transport mode. Det här innebär att den ursprungliga IP-headern lämnas orörd och okrypterad, men genom IPSec-headern kan man kontrollera att IP-headern och nyttolasten inte har blivit förändrad och samtidigt även kryptera nyttolasten. Det här gör att IP-paketet kan transporteras över internet på ett skyddat sätt, utan att förändringar i IP-headern behöver utföras. I tunnel mode skapas däremot en helt ny IP-header och IPSec-header och dessa placeras sedan framför den ursprungliga IP-headern och nyttolasten, se figur 7. IPSec: (b) tunnel mode. Det här gör att IP-headern och nyttolasten döljs, då det färdas över internet. (Kihl & Andersson 2013, 209)



Figur 7. IPSec: (a) transport mode, (b) tunnel mode. (Kihl & Andersson 2013, 210)

2.9 Autentisering

Autentisering handlar om att veta vem man kommunicerar med och på detta sätt upprätthålla en säker kommunikation. Syftet med autentisering är alltså att ta reda på identiteten på den enhet som man kommunicerar med. En enhet kan t.ex. vara en användare, dator eller server. I och med att det här examensarbetet kommer att handla om VPN-lösningar för arbetsstationer och mobila enheter så kommer jag att fokusera på autentisering av enheter. Utgående från figur 8 kommer jag att gå igenom hur en autentisering fungerar mellan två enheter och i det här exemplet används symmetrisk kryptering. Det hela börjar med att sändare A skickar iväg ett meddelande till mottagare B var man berättar vem man är. Mottagare B svarar genom att skicka iväg ett stort slumptal i klartext, vilket kallas nonce. Mottagare A krypterar sedan slumptalet och skickar iväg det åt mottagare B. Mottagare B okrypterar sedan slumptalet med den gemensamma hemliga nyckeln och om slumptalet är samma som mottagare B sände åt A så är identiteten på A identifierad. På det här sättet får mottagare B identifierat identiteten på mottagare A. Den här typen av autentisering kallas för challenge-respons, vilket på svenska betyder utmaning-svar. Ett exempel på hemlig nyckel är användarens lösenord till någon slags tjänst ute på internet. (Kihl & Andersson 2013, 204-205)



Figur 8. Autentisering av enheter. (Kihl & Andersson 2013, 205)

3 Metod

I metoddelen kommer jag att läsa på och ta fram fakta om fyra olika VPN-lösningar. De två första VPN-lösningarna kommer att vara anpassade för arbetsstationer och dessa är Direct Access och Checkpoint Endpoint Security. De andra två VPN-lösningarna kommer att vara anpassade för mobila enheter och dessa är IBM MaaS 360 VPN och Checkpoint Capsule Connect & Capsule VPN. Den här informationen kommer jag att använda mig av senare i sammanfattningsdelen av examensarbetet, där jag ger min rekommendation på om man ska ta ibruk en kompletterande VPN-lösning eller satsa på en certifikat baserad autentisering.

3.1 Direct Access

Direct Access är en produkt som är utvecklad av Microsoft och som implementerades för första gången i Windows Server 2008 R2. Direct Access är en teknik som innebär att användare kan arbeta någonstans utanför kontoret t.ex. hemifrån och ha tillgång till allt material precis som om användaren satt på kontoret. (Elmsjö a 2010) Microsoft menar ändå att detta inte är någon VPN-lösning eftersom ingen manuell aktivering krävs av användaren för att upprätta en krypterad VPN-tunnel in till företaget. I jämförelse med många andra VPN-lösningar så upprättas en krypterad VPN-tunnel redan då användaren loggar in på sin

arbetsstation eller så fort en internet förbindelse blir tillgänglig. Det är därför Microsoft menar att detta inte är någon VPN-lösning eftersom att användaren inte behöver utföra någon form av manuell aktivering, utan allting sker helt automatiskt. (Strömbergson 2011) Fördelen är att det blir enklare för IT-administratören att komma i kontakt med t.ex. arbetsstationer som sällan är fysiskt närvarande på kontoret för att uppdatera program från en central server eller konfigurera om inställningar via GPO-objekt. (Elmsjö a 2010)

Det finns förstås en del systemkrav för både arbetsstationer och servrar som behöver uppfyllas innan detta kan tas ibruk.

- Operativsystemet på Direct Access servern behöver antingen vara Windows Server 2008 R2 eller nyare
- Operativsystemet på DC:n behöver antingen vara Windows Server 2008 R2 eller nyare
- Operativsystemet på arbetsstationer behöver antingen vara Windows 7 Enterprise eller nyare
- Direct Access kommunicerar endast via IPv6-trafik och därför behöver allt som ska nås inom företagets nätverk kunna kommunicera via IPv6-trafik (Elmsjö b 2010)

3.1.1 DC

En DC (Domain Controller) är en server i en Windows domän som har hand om det övergripande ansvaret för domänens säkerhet. Det här innebär att den bl.a. tar hand om inloggningen av användare i domänen och ger rättigheter till delade resurser. Det kan t.ex. vara en nätverksmapp som ett exempel så kan en användare ha fulla rättigheter till en nätverksmapp, vilket innebär att användaren kan ge andra användare rättigheter till samma nätverksmapp. En annan användare kan t.ex. bara ha läs- och skriv rättigheter till nätverksmappen, vilket innebär att användaren bara kan läsa, öppna och redigera dokument i nätverksmappen. Det här betyder att före en användare får tillgång till några nätverksmappar i domänen så måste användaren autentisera sig mot DC:n och då ges rättigheter till nätverksmappar som användaren har rätt till. Det här betyder att användaren redan vid inloggningen får tilldelat sig sina rättigheter.

På DC:ns operativsystem så installeras sedan ett flertal olika roller som gör att servern kan fungera som en DC. Den första rollen som behöver installeras är AD DS (Active Directory Domain Services) som är en katalogtjänst som hanterar och lagrar all information om

användare i domänen. Det går t.ex. att lagra information om en användares konto som exempelvis namn, lösenord, e-post och telefonnummer. (Bergman 2014, 4) Den andra rollen är AD CS (Active Directory Certificate Services) som möjliggör PKI (Public Key Infrastructure), vilket är ett övergripande namn för all intern hantering av certifikat för hela domänen. Det går bl.a. att skapa, hantera, distribuera, använda, lagra och återkalla certifikat. (Microsoft c 2015) Den tredje rollen är DNS (Domain Name System), vilket är server vars uppgift att sköta om översättningen från en IP-adress som en dator förstår till ett mänskligt namn på en webbplats som en människa lätt kommer ihåg. Det här kan t.ex. att webbplatsen www.osterbottenstidning.fi nås på IP-adressen 176.34.156.182. (Rasmussen 2018)

3.1.2 CA

CA (Certification Authority). Certifikatutfärdarens uppgift är att intyga identiteten hos användare som försöker att ta kontakt med Direct Access servern genom att utfärda ett certifikat åt användarna. Den används också för att förnya certifikat åt användare vars certifikat inte längre är giltigt eller för att upphäva användarnas certifikat av en eller annan orsak. Det finns två olika typer av certifikatutfärdare och kommer som nästa att gå igenom dessa här nedanför.

Den första är en huvudsaklig certifikatutfärdare och behöver vara den mest pålitliga i hela domänen och har normalt sett mycket stränga regler och villkor som behöver uppfyllas för att certifikat ska kunna utfärdas åt andra certifikatutfärdare. Den används endast för att utfärda certifikat åt andra certifikatutfärdare.

Den andra är en underordnad certifikatutfärdare och används endast för att utfärda certifikat åt användare och har normalt sett inte lika stränga regler och villkor som behöver uppfyllas som den huvudsakliga certifikatutfärdaren. Den behöver istället ha fått utfärdat ett certifikat av den huvudsakliga certifikatutfärdaren för att bli en betrodd certifikatutfärdare. (Microsoft 2009)

3.1.3 CRL

CRL (Certificate Revocation List) är en lista över alla användare som fått sina certifikat återkallat av en eller annan orsak, dvs. att alla användare som finns med i listan inte längre har någon tillåtelse att ta kontakt med Direct Access servern. Syftet med listan är alltså att ge information åt Direct Access servern över vilka användare som inte längre har någon

tillåtelse att ta kontakt med den. Den här listan behöver alltså kunna publiceras både internt och externt så att både Direct Access servern och alla användare ute på internet har åtkomst till listan. Direct Access servern begär med en jämn tidsintervall ut en uppdaterad lista över återkallade certifikat från domänens egna certifikatutfärdare. Listan innehåller information om vilket datum som användarens certifikat blev återkallat och vilken certifikatutfärdare som hade utfärdat certifikatet samt orsaken till varför certifikatet blev återkallat. (Elmsjö a 2010)

3.1.4 GPO

I AD (Active Directory) finns GPO (Group Policy Object) implementerat som är ett verktyg som används för att skapa och hantera konfigurationer som sedan kan appliceras på antingen en grupp, användare eller arbetsstationer. Dessa konfigurationer kan t.ex. bestå av regler som styr hur länge en användares arbetsstation kan lämnas olåst innan den låser sig automatiskt eller regler som bestämmer hur långt och vilka tecken (bokstäver, siffror eller special tecken) som ett lösenord behöver innehålla. Dessa konfigurationer skapas och hanteras med hjälp av GPMC (Group Policy Management Console) verktyget på domänens DC.

Ett GPO-objekt består av två olika delar. Den första delen är användardelen, vilket innebär att alla inställningar som görs i användardelen appliceras bara på de användare vars användarkonto knyts till en viss OU eller underliggande OU. Den andra delen är datordelen, vilket innebär att alla inställningar som görs i datordelen appliceras på de arbetsstationer vars datorkonto knyts till en viss OU eller underliggande OU. (Elmsjö 2009, 1-2)

Då man tar ibruk Direct Access så skapas automatiskt två olika GPO-objekt. Det första GPO-objektet som skapas appliceras på en grupp där alla användare finns som ska kunna ta kontakt med Direct Access servern. Där finns bl.a. konfigurerat IP- eller URL-adresser som alla arbetsstationer använder för att kunna ta kontakt med NLS- och Direct Access servern antingen via 6to4, teredo eller IP-HTTPS. Det andra GPO-objektet som skapas appliceras på en grupp dit bara Direct Access servern tillhör och det innehåller bl.a. brandväggsregler för inkommande- och utgående trafik till och från Direct Access servern. (Techworld Sverige 2010)

3.1.5 NLS

NLS (Network Location Server). NLS-serverns uppgift är att avgöra om användare som ska ta kontakt med Direct Access servern befinner sig innanför eller utanför företaget. Om

användare lyckas att ta kontakt med NLS-servern så anses den befinna sig innanför företaget och i så fall behövs ingen krypterad VPN-tunnel upprättas. Om däremot användare inte lyckas att ta kontakt med NLS-servern så anses den befinna sig utanför företaget och i så fall behövs en krypterad VPN-tunnel upprättas. Ifall det är så att användare befinner sig utanför företaget så kommer även NRPT-tabellen att aktiveras och information som berör företaget kommer att skickas igenom en krypterad VPN-tunnel och all annan information skickas okrypterat direkt ut på internet.

Det är oerhört viktigt att NLS-servern endast är tillgänglig för användare som befinner sig innanför företaget, men inte om användare befinner sig utanför företaget. Om t.ex. användare som befinner sig utanför företaget kan ta kontakt med NLS-servern så kommer användare tro att de befinner sig innanför företaget och i så fall kommer ingen krypterad VPN-tunnel upprättas. Det här gör att information som berör företaget kommer att skickas okrypterat direkt ut på internet och kan avlyssnas olovligt av obehöriga. (Microsoft 2013)

3.1.6 NRPT

NRPT (Name Resolution Policy Table) är en tabell som innehåller regler om informationen som färdas ska åka igenom en krypterad VPN-tunnel eller sändas okrypterat direkt ut på internet. I tabellen framgår det t.ex. vilka DNS-förfrågningar som ska anses tillhöra företaget och behöver tas kontakt med via en krypterad VPN-tunnel, resten anses då inte tillhöra företaget och kan tas kontakt med direkt. Om t.ex. en användare som befinner sig utanför kontoret ska ta kontakt med företagets filserver och DNS-förfrågningen görs på fileshare.corp.contoso.com, då är det corp.contoso.com som bestämmer att allt som sänds ska skickas igenom en krypterad VPN-tunnel.

NRPT-tabellen är inte påslagen hela tiden utan är bara påslagen om en arbetsstation befinner sig utanför kontoret och i så fall ska all information som görs på DNS-förfrågningen corp.contoso.com igenom en krypterad VPN-tunnel. Om en användare däremot befinner sig på kontoret så är tabellen avslagen och allt tas kontakt med direkt och inte via någon krypterad VPN-tunnel.

I och med att NLS-servern också innehåller DNS-förfrågningen corp.contoso.com så behöver man skapa en undantagsregel som förhindrar att den kontaktas via en krypterad VPN-tunnel. Det här förhindrar också att en användare som inte befinner sig på kontoret, plötsligt skulle tro att den befinner sig på kontoret. Den här undantagsregeln innebär att om en användare ska ta kontakt med NLS-servern så kommer inte regeln att gälla för DNS-

förfrågningar som görs på corp.contoso.com i tabellen, men den här undantagsregeln gäller endast om en användare tar kontakt med NLS-servern. (Davies 2016)

3.1.7 Tunnling

All kommunikation mellan en användare och Direct Access servern fungerar endast med IPv6-trafik, vilket innebär att IPv6-trafik behöver kunna färdas över ett nätverk som bara stödjer IPv4-trafik. Detta innebär att olika typer av tunnlingstekniker behöver användas. Om t.ex. en användare skulle ha fått en publik IPv6-adress av sin internet leverantör kunde den högst troligtvis ta direkt kontakt med Direct Access servern utan några problem. Nuförtiden är det högst ovanligt att användare skulle få en publik IPv6-adress, då internet till största delen ännu består av gamla IPv4-adresser. Det finns lyckligtvis tre olika tekniker för att undvika problemet. Jag kommer som nästa att gå igenom dessa tre tekniker här nedanför. (Elmsjö b 2010)

3.1.8 6to4

Den första tekniken är 6to4 och den används om en användare har blivit tilldelad en publik IPv4-adress för att ta kontakt med Direct Access servern. På användarens IPv4-adress så skapas en IPv6-adress. Från GPO-objektet har användaren fått information om vilken IP-adress eller URL-adress som ska användas för att ta kontakt med Direct Access servern. Om däremot användaren befinner sig bakom en NAT-enhet så kommer inte den här tekniken att fungera, eftersom en IP-adress inte kan översättas från en intern till en publik IP-adress. I så fall behöver användaren använda sig av en annan teknik som kallas för teredo.

3.1.9 Teredo

Den andra tekniken är teredo och används om en användare befinner sig bakom en NAT-enhet. En teredo adress består av två olika delar som tillsammans bygger upp en komplett IPv6-adress. Den första delen består av Direct Access serverns IP-adress och den andra delen består av användarens IPv4-adress och båda dessa är omvandlade till hexadecimalt format. I brandväggen som användaren befinner sig bakom så behöver UDP (User Datagram Protocol) vara tillåtet, annars kommer inte användaren kunna ta sig ut igenom brandväggen. Om varken 6to4 eller teredo fungerar så befinner sig användaren troligtvis bakom en brandvägg som inte tillåter utgående UDP. I så fall försöker användaren som sista utväg att ta kontakt med Direct Access servern via IP-HTTPS.

3.1.10 Ip-https

Den tredje och sista tekniken är IP-HTTPS och den används om varken 6to4 eller teredo av någon okänd anledning inte fungerar. Som sista utväg försöker då användaren att ta kontakt med Direct Access servern via HTTPS-protokollet och från GPO-objektet som har applicerats på användaren fås information om vilken IP-adress eller URL-adress som ska användas för att ta kontakt med Direct Access servern. Om t.ex. användaren tar kontakt med Direct Access servern via IP-HTTPS så kommer Direct Access servern endast att agera som proxy server, vilket innebär att den tar emot trafiken och sänder trafiken vidare till avsedd destination. Den här tekniken anses ändå vara mest resurskrävande eftersom det är många lager som behöver krypteras och okrypteras. Därför rekommenderas det att användare istället använder sig av antingen 6to4 eller teredo om det bara är möjligt. (Elmsjö a 2010)

3.1.11 Hur fungerar Direct Access

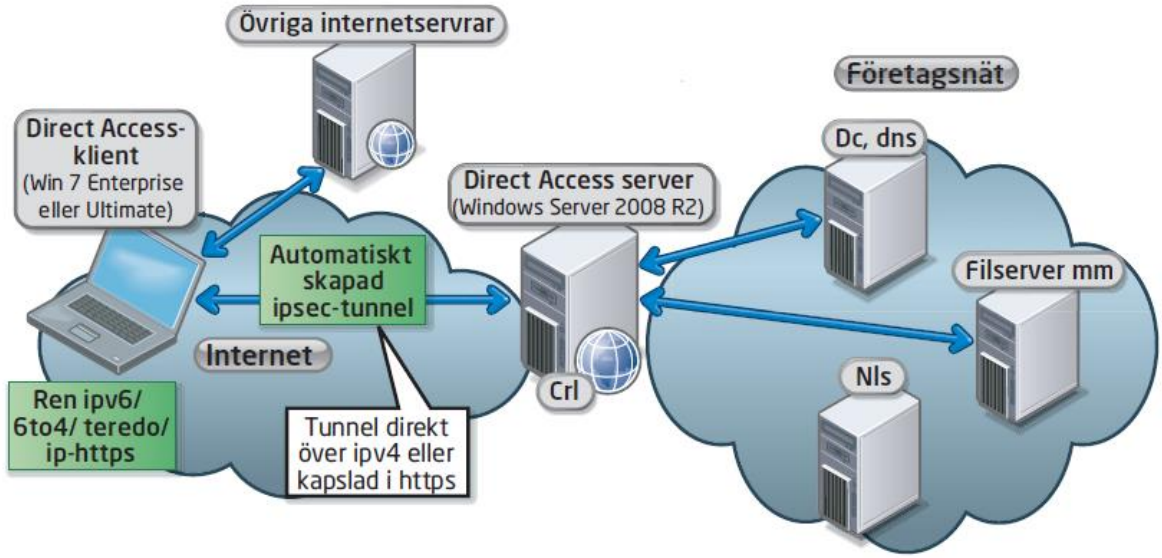
Jag kommer utgående från figur 9 att förklara hur tekniken bakom Direct Access fungerar. Det första som händer vid upprättandet en krypterad VPN-tunnel in till företaget är att arbetsstationen börjar med att ta reda på om den befinner sig innanför eller utanför företaget. Det här gör arbetsstationen genom att försöka ta kontakt med NLS-servern. Om arbetsstationen lyckas att ta kontakt med NLS-servern så anses den befinna sig innanför företaget och i så fall behövs ingen krypterad VPN-tunnel upprättas. Det här innebär att en användare tar direkt kontakt med allt innanför företaget och inte igenom någon krypterad VPN-tunnel. Om arbetsstationen däremot inte lyckas att ta kontakt NLS-servern så anses den befinna sig någonstans utanför företaget och i så fall påbörjas upprättandet av en krypterad VPN-tunnel.

I nästa steg visar arbetsstationen upp sitt certifikat för Direct Access servern och den kontrollerar om certifikatet som uppvisats finns med CRL-listan. Om det uppvisade certifikatet inte finns med i CRL-listan så påbörjas upprättandet av en krypterad IPSec-tunnel mellan arbetsstationen och Direct Access servern. IPSec-tunneln krypteras med en 192-bitarsnyckel, ju högre antal bitar desto svårare blir krypteringen att knäcka för obehöriga.

Arbetsstationen använder sedan antingen en ren IPv6-adress, 6to4, Teredo eller IP-HTTPS för att kunna upprätta en krypterad VPN-tunnel till Direct Access servern. Detta för att övervinna problemet med att kunna sända IPv6-trafik över internet som till största delen bara

stödjer IPv4-trafik mellan arbetsstationen och Direct Access servern. Detta p.g.a. att all kommunikation mellan arbetsstationen och Direct Access servern endast fungerar med IPv6-trafik. Arbetsstationen testar först att använda en ren IPv6-adress sedan 6to4 och som följande Teredo och till allra sist IP-HTTPS.

Nu när en krypterad VPN-tunnel är upprättad så kommer arbetsstationen att få tillgång till NRPT-tabellen från Direct Access servern. NRPT-tabellen talar om för arbetsstationen vilka DNS-förfrågningar som anses vara innanför företaget och behöver kontaktas igenom en krypterad VPN-tunnel och allt annat kan kontaktas direkt utan någon krypterad VPN-tunnel. (Elmsjö b 2010)



Figur 9. Direct Access (Elmsjö 2010, 76)

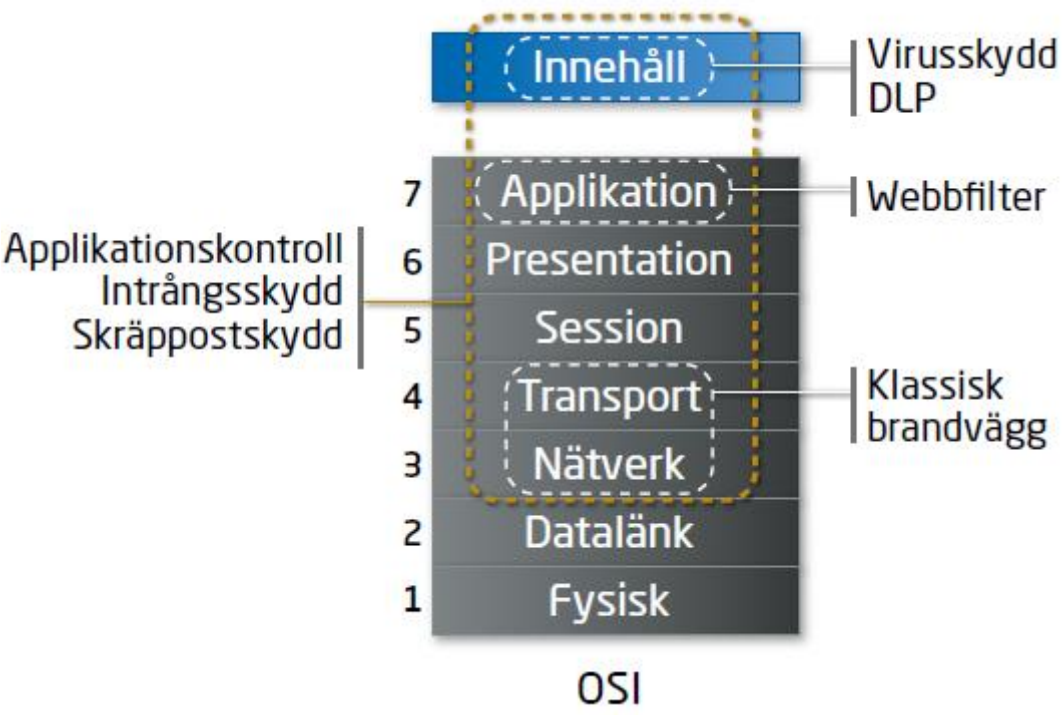
3.2 Checkpoint Endpoint Security

Checkpoint Software Ltd är världsledande och största leverantören av produkter och lösningar inom IT-säkerhet. Företaget grundades år 1993 av Gil Shwed och huvudkvarteret finns för nuvarande i Tel Aviv i Israel. Checkpoint är största tillverkaren av avancerade brandväggar och deras populära brandväggsprodukt kallas Next Generation Firewall, vilket på svenska betyder Nästa Generations Brandväggar. (Checkpoint d u.å.) Jag kommer här nedanför att gå igenom vad skillnaden är mellan nästa generations brandvägg och den gamla vanliga brandväggen som filtrerar på IP-adress och portnummer.

I figur 10 visas OSI-modellen (Open Systems Interconnect) och modellen innehåller 7 olika lager av funktionalitet för nätverkskommunikation. Den gamla brandväggen arbetar endast med lager 3 och 4 från OSI-modellen, vilket innebär att brandväggen bara kan filtrera och

blockera på IP-adress eller portnummer. Om man däremot vill behålla en högre säkerhet så behöver man ännu noggrannare analysera vilken trafik som passerar. Den nya och modernare brandväggen arbetar därför med ett fler antal lager dvs. med lager 3-7 från OSI-modellen och på detta sätt noggrannare kunna analysera vilken trafik som passerar.

- Virusskyddet arbetar på det översta lagret som är innehåll för att hitta elaka exekverbara filer, vilket är filer som går att köra.
- Data loss prevention arbetar också på lager 7 för att hitta information och filer som inte tillåts att passera.
- Webbfilter arbetar på lager 7 för att blockera webbplatser utifrån kategorier.
- Applikationskontrollen arbetar med lager 3-7 för att filtrera bort olika applikationer enligt önskemål.
- Intrångsdetekteringen arbetar också med lager 3-7 för att hitta felaktig användning av protokoll och applikationer.
- Skräppostskyddet arbetar också med lager 3-7 för att filtrera bort oönskade och farliga e-mail. (Techworld Special 2015, 2)



Figur 10. OSI-modellen. (Techworld Special 2015)

Checkpoint vill att man ska lägga många funktioner i samma security gateway dvs. i brandväggen, eftersom det behövs fler funktioner än enbart brandväggen för få en hög säkerhet och kontroll på vad som tillåts- och inte tillåts passera igenom brandväggen. Alla

dessa extra funktioner kallas för software blades, vilket på svenska betyder mjukvarublad. Dessa är alltså förinstallerade funktioner i brandväggen som kan låsas upp med licensnycklar. (Techworld 2015, 9, 12) De extra funktioner som uppdragsgivaren använder i brandväggen är följande.

- Threat Prevention
- IPS
- Application filtering
- URL filtering
- IPSec VPN

Virusskyddet (Threat Prevention) är det skydd i brandväggen som kollar efter kända virus. Virusskyddet innehåller en databas över kända virus signaturer och varje anrop som kommer in mot brandväggen matchas mot databasen och om en matchning eller en fil med virus liknande egenskaper hittas så blockeras anropet. Ifall brandväggen är osäker på om en fil är skadlig eller inte så kan filen provköras i en starkt begränsad miljö. Det här ställer så klart stora prestandakrav på brandväggen.

Intrångsskyddet (IPS) är det skydd i brandväggen som kollar efter inbrottsförsök. Det förhindrar att attackerare ska komma in till företaget via t.ex. kända sårbarheter i operativsystemet, applikationer eller via rena felaktigheter i applikationsprotokollet. Intrångsskyddet fungerar så att alla kommandon eller anrop som kommer in mot brandväggen undersöks och alla kommandon eller anrop som försöker komma in via några av de tidigare nämnda sårbarheterna blockeras.

Applikationsfiltreringen (Application filtering) bedömer om en applikation anses vara tillåten att använda utifrån de regler och policyer som finns hos företaget. I brandväggen finns en databas över hur otillåtna applikationer uppträder och applikationerna identifieras genom IP-adress, innehåll och kommunikationsmönster för att veta vilken applikation det gäller och matcha mot aktuella regler och policyer. Om applikationen inte godkänns utifrån de uppsatta regler och policyer som finns så blockeras den.

Innehållsfiltreringen (URL filtering) bedömer om innehållet på en viss specifik webbplats anses vara tillåtet att besöka utifrån de regler och policyer som finns hos företaget. Genom innehållsfiltreringen i brandväggen kan man blockera att vissa specifika webbplatser inte kan besökas som innehåller porr, rasism, terrorism eller webbplatser som sprider virus eller attackerar användare. (Techworld Special 2015, 3-4)

VPN tillägget (IPSec VPN) är den del i brandväggen som ger användare möjlighet att få full åtkomst till företaget igenom en krypterad VPN-tunnel. Checkpoints brandvägg har sammanlagt tre olika nivåer av IPSec VPN och dessa är Endpoint Security, SecuRemote och SSL-VPN. (Checkpoint e u.å.) Jag kommer att presentera dem närmare här nedanför.

3.2.1 Endpoint Security

Endpoint Security är det som skyddar en användares arbetsstation mot olika typer av IT-hot genom att aktivera strängare brandväggsregler på användarens arbetsstation, ifall den kopplas in i ett okänt nätverk. Den innehåller också en VPN-lösning som tillåter en användare att upprätta en krypterad VPN-tunnel in till företaget. (Checkpoint f u.å.)

3.2.2 SecuRemote

SecuRemote är en lättare version av föregående Endpoint Security med ett begränsat antal funktioner. SecuRemote upprättar endast en krypterad VPN-tunnel in till företaget och ingenting annat. Den största skillnaden från Endpoint Security är att den här inte drar åt brandväggsreglerna i en användares arbetsstation om den befinner sig i ett okänt nätverk. SecuRemote är lämpligare att använda för en utomstående användare som bara behöver kunna upprätta en krypterad VPN-tunnel. Det här kan t.ex. vara om en serviceman behöver komma åt en maskin via nätverket och göra inställningar på den. (Checkpoint c 2018)

3.2.3 SSL-VPN

SSL-VPN är en webbaserad portal som ger användare samma möjligheter att komma in till företaget och få åtkomst till servrar, applikationer och filer som med SecuRemote. Den här tekniken innebär att användare loggar in via en webbaserad portal via det krypterade HTTPS-protokollet, istället för med det vanliga okrypterade HTTP-protokollet. I klar text innebär detta att en användare skriver in adressen i webbläsarens URL-fönster och kan t.ex. se ut så här https://vpn.contoso.com. Inuti portalen finns två lägen och första läget är network mode, vilket innebär t.ex. att en användare kommer åt filer som ligger på filservern. Det andra läget är native application och här krävs det att ett litet program installeras på användarens arbetsstation som ger ut en intern IP-adress som används inom företaget, vilket innebär att en användare kan komma åt applikationer som används inom företaget. (Checkpoint b u.å.)

3.3 Checkpoint Capsule Connect & Capsule VPN

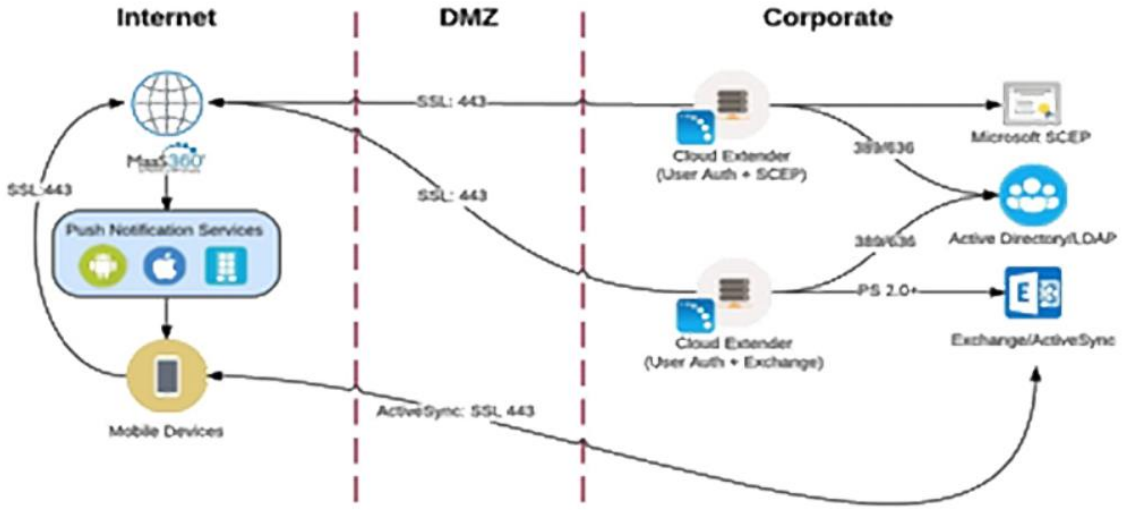
Checkpoint har även utvecklat en VPN-applikation och för mobila enheter med operativsystemet iOS kallas den Checkpoint Capsule Connect och för Android Checkpoint Capsule VPN. Den påminner ganska mycket om Checkpoint Endpoint Security som presenterades i avsnitt 3.2, men den här är istället utvecklad för mobila enheter. Det går att autentisera sig mot brandväggen på två olika sätt, antingen via användarnamn och lösenord eller med hjälp av certifikat. (Checkpoint a 2016, 14-15)

3.4 IBM MaaS 360 VPN

IBM MaaS 360 är en molnbaserad MDM-tjänst som innehåller ett flertal olika produkter som företag kan köpa till för att utveckla sin MDM-tjänst. En av dessa produkter är IBM MaaS 360 VPN som jag kommer att gå igenom i detta avsnitt. Den här produkten gör det möjligt för användare att via sina mobila enheter kunna ta kontakt med VPN-servern och upprätta en krypterad VPN-tunnel in till företaget. Det krävs följande delar för att möjliggöra detta. (IBM a u.å.)

3.4.1 Cloud Extender

Cloud Extendern har som uppgift att koppla samman allt inom företaget så som AD (Active Directory) eller en lokal e-post server (Exchange) till den molnbaserade MDM-tjänsten IBM MaaS 360. Det är en liten Windows applikation som behöver installeras antingen på en lokal- eller en virtuell server som ska vara placerad bakom brandväggen hos företaget och med åtkomst till allt som ska kunna kommunicera med den molnbaserade MDM-tjänsten. Cloud Extendern kommunicerar med den molnbaserade MDM-tjänsten över port 443, vilket innebär att all kommunikation krypteras och protokollet som används är XMPP (Extensible Messaging and Presence Protocol) för att kunna följa med och uppdatera alla åtgärder som utförs i realtid. I figur 11 visas hur kommunikationen fungerar mellan den molnbaserade MDM-tjänsten, Cloud Extendern, AD och Exchange. (IBM b u.å.)



Figur 11. Cloud Extender (IBM b u.å.)

3.4.2 Servern

VPN-servern är dit användare tar kontakt antingen via en IP-adress eller URL-adress för att kunna upprätta en krypterad VPN-tunnel in till företaget. VPN-servern behöver placeras någonstans inom företaget och vara lätt tillgänglig för användare ute på internet. Om många användare behöver kunna ta kontakt med VPN-servern samtidigt, då kan man dela upp VPN-servern och använda den på flera olika servrar, dvs. använda en s.k. DNS Load Balanced URL. (IBM u.å.) Den här tekniken betyder att man använder sig av flera IP-adresser för samma server och delar upp belastningen på varje IP-adress och på detta sätt öka svarstiden och minska belastningen på servern.

3.4.3 Applikation

Applikationen är det program som användare använder på sina mobila enheter för att ta kunna kontakt med VPN-servern och det finns endast tillgängligt för operativsystem så som iOS och Android. För att VPN-applikationen ska få alla nödvändiga inställningar så skapas två olika policyer i den molnbaserade portalen, den ena policyn appliceras på iOS och den andra på Android. Dessa innehåller t.ex. information om vilken IP-adress eller URL-adress som användare använder för att ta kontakt med VPN-servern. VPN-applikationen använder sig sedan av ett certifikat som utfärdats av portalens egna certifikatutfärdare och som används för att kunna autentisera sig mot VPN-servern. På det här sättet behöver användare ange varken användarnamn eller lösenord för att autentisera sig mot VPN-servern och upprätta en krypterad VPN-tunnel in till företaget.

3.4.4 Portalen

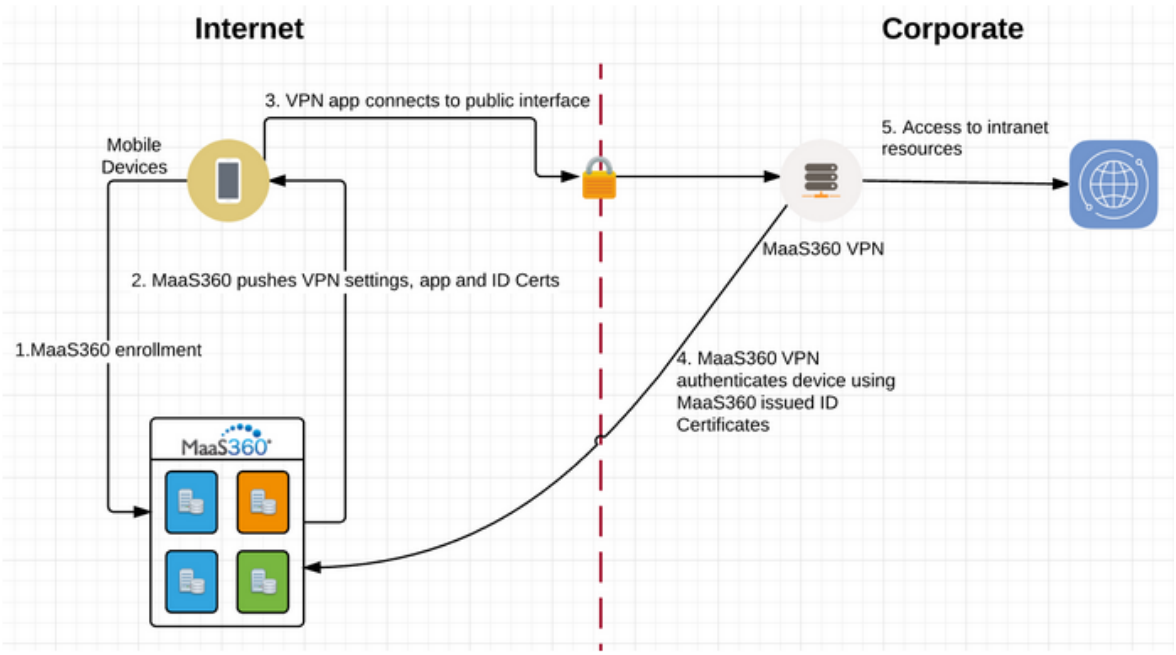
IBM MaaS 360 portalen är en molnbaserad MDM-tjänst någonstans ute på internet varifrån VPN-lösningen kan aktiveras. Det är från portalen som användare hämtar VPN-applikationen, certifikatet och alla nödvändiga inställningar åt sina mobila enheter, då den tas ibruk. I portalen finns också en certifikatutfärdare som skapar certifikat och sedan skickar ut dem till användarnas mobila enheter. Certifikatet används sedan för att användare ska kunna autentisera sig mot VPN-servern och upprätta en krypterad VPN-tunnel in till företaget. (IBM a u.å.)

3.4.5 Hur fungerar IBM MaaS 360 VPN

Jag kommer utgående figur 12 att förklara hur det går till första gången användare med sina mobila enheter ska ta kontakt med VPN-servern och sedan den andra gången, efter att användare har hämtat VPN-applikationen, certifikatet och alla nödvändiga inställningar från portalen.

Den första gången användare ska ta kontakt med VPN-servern så behöver deras mobila enheter registrera sig till portalen och därifrån hämta VPN-applikationen, certifikatet och alla nödvändiga inställningar. Efter att allt detta är hämtat och klart så blir det dags att ta kontakt med VPN-servern. Det hela börjar med att VPN-applikationen tar kontakt med VPN-servern antingen via IP-adress eller URL-adress och visar upp sitt certifikatet för VPN-servern. Följande som händer är att certifikatet som en användare visar upp jämförs med det certifikat som har utfärdats av portalens egna certifikatutfärdare och om dessa två certifikat stämmer överens med varandra så upprättas en krypterad VPN-tunnel in till företaget.

Den andra gången behöver användare bara starta upp VPN-applikationen och klicka på connect knappen för att upprätta en krypterad VPN-tunnel in till företaget. Det går betydligt snabbare den andra gången eftersom allt redan finns lagrat i alla mobila enheter. Den enda skillnaden mellan första och andra gången är att användare bara behöver hämta VPN-applikationen, certifikatet och alla nödvändiga inställningar den första gången som VPN-servern ska kontaktas.



Figur 12. IBM MaaS 360 VPN arkitektur (IBM a u.å.)

4 Sammanfattning

I det här avsnittet kommer jag att gå igenom en sammanfattning av examensarbetet både för arbetsstationer och mobila enheter.

4.1 Arbetsstationer

I det här avsnittet så kommer jag att presentera en sammanfattning av hur bra Direct Access motsvarar de krav som uppdragsgivaren har på den kompletterande VPN-lösningen. Jag kommer också att gå igenom hur ett certifikat skapas i brandväggen, hur det distribueras åt en användare eller till arbetsstationen och hur certifikatet används för att upprätta en krypterad VPN-tunnel. Till sist kommer jag ge min rekommendation på om man behöver ta ibruk Direct Access eller om man istället kan förenkla autentiseringen för deras nuvarande produkt Checkpoint Endpoint Security med hjälp av certifikat.

4.1.1 Direct Access

Jag har använt mig av följande betygsättning, då jag har betygsatt hur bra Direct Access uppfyller de krav som ställs på den kompletterande VPN-lösningen för arbetsstationer.

3 = Lätt, 2 = Medel, 1 = Svårt

Direct Access	Uppfyllelse
Enkel	3
Distribuering	3
Implementering	1
Felsökning	1
Spårbarhet	1
Skräddarsydda regler	2
Kontroll av trafik	2

Figur 13. Kravtabell för Direct Access

Direct Access är väldigt enkel att använda ur en användares synvinkel. Det krävs ingen som helst av manuell hantering från användaren för att upprätta en krypterad VPN-tunnel in till företaget. Det enda som krävs är att användaren har tillgång till en internet förbindelse och en krypterad VPN-tunnel upprättas redan då användaren loggar in på sin arbetsstation. Det är för att den är väldigt enkel att använda som den får betyget 3.

Direct Access är enkel att distribuera ut åt arbetsstationer ur IT-avdelningens synvinkel. Det räcker med att arbetsstationerna är med i domänen och i AD-gruppen dit alla Direct Access arbetsstationer tillhör. Till sist så behöver arbetsstationerna fysiskt ha varit inkopplat i nätverket så att GPO-objektet har kunnat appliceras på dem. Detta krävs för att Direct Access ska kunna användas på alla dessa arbetsstationer. Det är för att den är enkel att distribuera som den får betyget 3.

Direct Access är väldigt svår att implementera i den nuvarande infrastrukturen. Det krävs att allting som finns inom företagets nätverk och ska kunna nås via Direct Access, inte får ha några problem att kunna kommunicera via IPv6-trafik, då servern endast fungerar via IPv6-trafik. Jag fick aldrig demomiljön av Direct Access att fungera så därför är nog svårigheten att implementera väldigt hög. Det är därför som svårigheten att implementera får betyget 1.

Med Direct Access är felsökning och spårbarhet svårt att genomföra. Detta p.g.a. att det inte går att få fram någon information från servern om vilka arbetsstationer och IP-adresser som har tagit kontakt med den samt när en krypterad förbindelse upprättades och kopplades från. Jag har inte kunnat testa om detta är möjligt i praktiken, men utifrån den information jag har

hittat på internet så borde inte detta var möjligt. Det är därför som möjligheten för felsökning och spårbarhet får betyget 1.

Direct Access gör det möjligt att skräddarsy regler med hjälp av brandväggen mellan Direct Access servern och företagets nätverk. Detta innebär att IT-administratören kan skapa skräddarsydda regler i brandväggen och t.ex. reglera vilka användare som ska komma in på vissa VLAN (Virtual Local Area Network). Jag har inte kunnat testa detta i praktiken, men ur ett rent teoretiskt perspektiv så borde detta vara möjligt. Det är därför som möjligheten att skräddarsy regler får betyget 2.

Direct Access gör det också möjligt att kontrollera trafik som kommer in mot brandväggen med hjälp av dess extra funktioner. Då behövs två brandväggar användas och Direct Access servern placeras i ett DMZ område mellan de båda brandväggarna. DMZ (Demilitarized Zone) är ett område som skyddar företagets nätverk ifrån det publika internet. Det här innebär att den första brandväggen ut mot det publika internet, bara släpper igenom trafik som ska till Direct Access servern och den andra brandväggen kontrollerar noggrant all trafik som far in till företagets nätverk. Jag har inte kunnat testa detta i praktiken, men ur ett rent teoretiskt perspektiv så borde detta vara möjligt. Det är därför som möjligheten att kontrollera trafik får betyget 2.

4.1.2 Checkpoint Endpoint Security

I brandväggen från Checkpoint går det att använda certifikat på två olika sätt, vilket också innebär att det är möjligt att ta ibruk en certifikat baserad autentisering och på detta sätt minska antalet klickningar till endast två stycken som en användare manuellt behöver utföra för att upprätta en krypterad VPN-tunnel in till företaget. Jag kommer att berätta mera om dessa två olika sätt här nedanför.

Det första sättet är att använda sig av ett s.k. P12 certifikat, vilket innebär att en IT-administratör skapar certifikatet i brandväggen och ger det ett lösenord. Certifikatet placeras sedan ut under användarens personliga användarmapp på servern och därifrån kan användaren hämta certifikatet och använda det från vilken arbetsstation som helst, förutsatt att den är med i företagets domän. Den här lösningen är absolut inte den enklaste eftersom den kräver att användaren utför många manuella klickningar för att upprätta en krypterad VPN-tunnel, men ur säkerhetssynpunkt det mest säkra eftersom certifikatet skyddas av lösenordet till användarens konto samt lösenordet för certifikatet. Det går förstås att förenkla autentiseringen ytterligare och välja att installera certifikatet under användarens personliga

certifikat på arbetsstationen, vilket innebär att användaren slipper att skriva in lösenordet för certifikatet varje gång en krypterad VPN-tunnel ska upprättas, då skulle det räcka med att klicka på connect knappen. Det finns förstås en liten säkerhetsrisk med detta sätt och det är ifall arbetsstationen blir stulen och någon obehörig slipper att logga in på användarens konto, då kan certifikatet användas helt fritt.

Det andra sättet är att använda sig av en registreringskod som sänds ut till en användare, t.ex. via e-post. Registreringskoden är 12 tecken lång och består av både stora- och små bokstäver, siffror och special tecken. Den är endast giltig i 2 veckor dvs. 14 dagar och kan användas endast en gång. Den fungerar så att certifikatet skapas i brandväggen och med hjälp av registreringskoden så kan användaren hämta ner certifikatet och importera det som P12 eller CAPI. Om man väljer att importera certifikatet som P12 så skyddas certifikatet av ett lösenord och det innebär att lösenordet behöver anges varje gång en krypterad VPN-tunnel ska upprättas. Om man däremot väljer att importera som CAPI så installeras certifikatet direkt under användarens personliga certifikat på arbetsstationen och då behöver man inte ange något lösenord vid upprättandet av en krypterad VPN-tunnel, men certifikatet är inte heller lösenordsskyddat.

4.1.3 Rekommendation

Min egna rekommendation är att det skulle vara enklare och bättre att satsa på en certifikat baserad autentisering, istället för att börja implementera Direct Access i den nuvarande infrastrukturen. Detta p.g.a. att Direct Access är väldigt svår att implementera och en annan stor och bidragande orsak var att det skulle bli omöjligt att övervaka trafiken till- och från Direct Access servern på ett smidigt sätt med hjälp av operativsystemets egna inbyggda övervakningsprogram på servern. Det skulle t.ex. inte gå att spåra användarnas publika IP-adresser om tunnlingstekniken IP-HTTPS används för att ta kontakt med Direct Access servern, eftersom de IP-adresser som då kommer till servern är krypterad och inte kan spåras. Det kommer inte heller gå att spåra trafik från Direct Access servern eftersom all trafik som är avsedd att komma åt någonting inom företagets nätverk så översätts av Direct Access servern. Det här resulterar i en omöjlighet att kunna spåra vilka användare som har tagit kontakt med någonting inom företagets nätverk, eftersom all trafik ser ut att komma från Direct Access servern interna IP-adress.

Ifall man väljer att satsa på en certifikat baserad autentisering så skulle jag rekommendera att man använder sig av det första alternativet som jag berättade om i föregående avsnittet,

se avsnitt 4.1.2. På detta sätt skulle upprättandet av en krypterad VPN-tunnel bli betydligt enklare, eftersom antalet klickningar nu skulle minska till endast 2 st. klickningar. Det här skulle också bli mera säkert ur IT-avdelningens synvinkel eftersom certifikaten placeras under användarnas egna utrymmen på servern, vilket innebär att certifikaten skyddas av lösenordet till varje användares egna användarkonto. Även certifikaten skulle också vara skyddat av ett lösenord som har skapats i samband med certifikatet och detta lösenord behöver man känna till för att kunna använda eller installera certifikatet. Det enda problemet som finns med en certifikat baserad autentisering är att certifikaten bara har en maximal livslängd på 2 år, vilket är lite för kort eftersom arbetsstationerna byts ut vart 3:e år. Det hade varit en ypperlig möjlighet att förnya certifikaten i samband med att arbetsstationerna byts ut, men det här går inte eftersom certifikaten har för kort livslängd. För att undvika det här problemet kan man välja att förnya certifikaten efter halva tiden dvs. 1,5 år efter att arbetsstationerna togs ibruk, efter halva tiden så förnyas certifikaten igen med 1,5 år framåt. Det här innebär att certifikaten är i kraft under hela tiden som arbetsstationerna används.

4.2 Mobila enheter

I det här avsnittet så kommer jag att presentera en sammanfattning av hur bra IBM MaaS 360 VPN motsvarar de krav som uppdragsgivaren har på den kompletterande VPN-lösningen. Jag kommer också att gå igenom om det är möjligt att distribuera Checkpoints egna VPN-applikation, certifikat och alla inställningar åt en användares mobila enhet med hjälp av MDM-tjänsten IBM MaaS 360. Till sist kommer jag ge min rekommendation på om man behöver ta ibruk IBM MaaS 360 VPN eller om man istället kan förenkla autentiseringen för deras nuvarande produkt Checkpoint Capsule Connect & Capsule VPN med hjälp av certifikat.

4.2.1 IBM MaaS 360 VPN

Jag har använt mig av följande betygsättning, då jag har betygsatt hur bra IBM MaaS 360 VPN uppfyller de krav som ställs på den kompletterande VPN-lösningen för mobila enheter.

3 = Lätt, 2 = Medel, 1 = Svårt

IBM MaaS 360 VPN	Uppfyllelse
Enkel	3
Distribuering	3
Implementering	2
Felsökning	2
Spårbarhet	2
Skräddarsydda regler	2
Kontroll av trafik	2

Figur 14. Kravtabell för IBM MaaS 360 VPN

IBM MaaS 360 VPN är väldigt enkel att använda ur användarnas synvinkel, enda som krävs av en användare är att trycka på connect knappen för att upprätta en krypterad VPN-tunnel. Det är därför som den får betyget 3.

Med IBM MaaS 360 är det väldigt enkelt att distribuera ut VPN-produkten åt mobila enheter. Det krävs inte heller någon form av manuell hantering från användarnas sida, utan de mobila enheterna får VPN-applikationen, certifikatet och alla nödvändiga inställningar från den molnbaserade MDM-tjänsten IBM MaaS 360. Det är därför som möjligheten att distribuera får betyget 3.

IBM MaaS 360 VPN borde inte vara speciellt svår att implementera i den nuvarande infrastrukturen. Det enda som krävs är att få brandväggen att kontrollera all trafik som färdas från VPN-servern och in till företagets nätverk. Jag har inte kunnat testa detta i praktiken, men utifrån den information som jag har hittat från internet så borde inte implementeringen vara något större problem. Det är därför som svårigheten att implementera får betyget 2.

Med IBM MaaS 360 VPN är felsökning och spårbarhet svårt att genomföra på ett enkelt sätt. Från den molnbaserade MDM-tjänsten går det inte att få fram någon information om trafik övervakningen till- och från VPN-servern. Det går däremot att få fram logg filer från Cloud Extendern och de hittas under C:\ProgramData\MaaS360\Cloud Extender\logs\VPN, men det är svårt att göra någon vettig filtrering eftersom dessa logg filer bara är vanliga text dokument. Det är därför som felsökning och spårbarhet får betyget 2.

Med IBM MaaS 360 VPN borde det gå att skräddarsy regler. Det skulle t.ex. kunna vara att hantera vilka användare som ska komma åt vissa specifika VLAN:s med hjälp av en brandvägg som är placerad mellan VPN-servern och företagets nätverk. Jag har inte kunnat testa detta i praktiken, men ur ett rent teoretiskt perspektiv så borde detta vara möjligt. Det är därför som möjligheten att skräddarsy regler får betyget 2.

IBM MaaS 360 VPN borde göra det möjligt att kontrollera all trafik som kommer in till företagets nätverk med hjälp av en brandvägg. Brandväggen skulle placeras mellan VPN-servern och företagets nätverk och med brandväggen skulle man kunna kontrollera all trafik som passerar. Jag har inte kunnat testa detta i praktiken, men utifrån den information som jag har hittat från internet så borde detta vara möjligt. Det är därför som möjligheten att kontrollera trafik får betyget 2.

4.2.2 Checkpoint Capsule Connect & Capsule VPN

Det är möjligt att använda sig av den molnbaserade MDM-tjänsten IBM MaaS 360 för att distribuera ut applikationen och alla nödvändiga inställningar åt mobila enheter. IT-administratören behöver bara skapa en VPN-profil och sedan applicera den på en policy som alla mobila enheter får applicerad på sig. Enligt vad jag har hittat från internet så går inte certifikaten att distribuera på samma sätt, vilket är lite synd. Ifall det också hade lyckats att distribuera ut certifikaten på samma sätt så hade detta varit en komplett lösning. Den här konfigurationen gäller endast för mobila enheter med operativsystemet iOS version 7.0 eller högre. Enligt min sökning kring detta på internet så borde det vara exakt samma inställningar för operativsystemet Android också.

Här visas hur inställningarna i moln tjänsten behöver se ut.

- Configure for type: custom SSL
- VPN Connection Name: < site name >
- Identifier: com.checkpoint.CheckPoint-VPN.vpnplugin
- Host Name of the VPN Server: x.x.x.x
- VPN user account: %Username%
- User authtype: certificate
- Apps to use this VPN: com.checkpoint.CheckPoint-VPN.app

4.2.3 Rekommendation

För mobila enheter så skulle jag rekommendera att uppdragsgivaren inte tar och köper till IBM MaaS 360:s egna VPN-lösning, utan istället skulle jag rekommendera att använda sig av en certifikat baserad autentisering med hjälp av Checkpoints egna VPN-applikation (Checkpoint Capsule Connect & Capsule VPN). Detta p.g.a. att den funktionsmässiga skillnaden mellan dessa två lösningar är så minimal. Den första fördelen med att använda Checkpoints egna VPN-applikation är att man på ett väldigt enkelt sätt kan undersöka all typ av trafik som kommer in mot brandväggen med hjälp av följande funktioner virusskyddet, intrångsskyddet, applikations- & innehållsfiltreringen. Den andra fördelen är att man också enkelt kan distribuera ut VPN-applikationen och alla nödvändiga inställningar färdigt gjorda med hjälp av den molnbaserade MDM-tjänsten IBM MaaS 360, vilket innebär att användare inte alls behöver göra någonting för att kunna börja använda VPN-applikationen. Det som man ännu behöver undersöka är hur man på ett smidigt sätt kan distribuera ut certifikaten till alla mobila enheter och även hur man kan lagra certifikaten på en säker plats, vilket ska hindra obehöriga från att komma åt certifikaten. Den enda nackdelen jag ser med Checkpoints egna VPN-lösning för mobila enheter (detsamma gäller också för arbetsstationer) är att för tillfället är inte brandväggen och AD integrerade med varandra, vilket resulterar i att IT-administratören behöver skapa skilda VPN-konton åt alla användare som ska komma in till företaget via en krypterad VPN-tunnel. Därför rekommenderar jag att man skulle ta och integrera brandväggen och AD med varandra och på detta sätt skulle användare kunna använda samma användarnamn som till sina arbetsstationer och sitt certifikat för att autentisera sig mot brandväggen. Det här sparar en hel del arbetstid för IT-administratören eftersom man inte behöver skapa skilda VPN-konton.

5 Kritisk granskning

Om jag skulle göra om det här examensarbetet så skulle jag nog ha fokuserat på att undersöka endast en VPN-lösning antingen för arbetsstationer eller mobila enheter, men inte båda två. Enligt mig blev det lite för mycket att undersöka båda två eftersom tiden var väldigt begränsad, sommarjobbet varade i endast 4 månader och under den tiden borde man ha hunnit ta reda på information om de olika VPN-lösningarna, bygga upp demo miljöer och testa. En annan sak som försvårade den praktiska delen av examensarbetet var att jag saknade rättigheter som domain admin, vilket innebär att man har rättigheter som administratör överallt i hela domänen. Jag skulle behövt ha domän admin rättigheter under sommaren då min handledare Per-Erik Finell var på semester och den virtuella servern där jag byggde upp

demo miljön av Direct Access plötsligt hade låst sig, vilket resulterade i en obrukbarhet. Till sist skulle jag också behövt ha rättigheter till brandväggen för att få testa hur hantering av certifikaten fungerar och hur man tillverkar dom. Samtidigt förstår jag nog också varför jag inte fick rättigheter som domän admin och till brandväggen eftersom ett fel kan få ganska stora konsekvenser för säkerheten.

6 Avslutning

Till sist vill jag bara säga att det har varit enormt lärorikt för mig att få utföra både den teoretiska och praktiska delen av examensarbetet. Jag försökte under sommaren 2017 att bygga upp en demo miljö av Direct Access ute hos uppdragsgivaren, men tyvärr fick jag aldrig demo miljön att fungera, vilket var ganska tråkigt. Jag ser det ändå inte som något misslyckande eftersom jag fick stor kunskap om den teoretiska uppbyggnaden och tekniken bakom Direct Access. Den viktigaste lärdomen jag har fått med mig från examensarbetet är hur svårt det är att hitta en VPN-lösning som är säker ur IT-avdelningens synvinkel och enkel att använda ur användares synvinkel. Om man t.ex. vill ha en VPN-lösning som är säker så kommer den också att bli krångligare att använda eftersom man kanske behöver använda sig av en s.k. tvåfaktorsautentisering. En tvåfaktorsautentisering innebär att man först skriver in sitt användarnamn och lösenord, sedan använder man ännu en kod som har sänts t.ex. till användarens mobiltelefonen för att säkerställa att rätt användare försöker att autentisera sig. Om man däremot vill ha en VPN-lösning som är enkel att använda så behöver man också minska lite på säkerheten dvs. om man använder ett lösenordsskyddat certifikat eller inte. Ett icke lösenordsskyddat certifikat är mycket enklare att använda för autentisering eftersom att inget lösenord efterfrågas, men samtidigt också mycket enklare för brottslingar att stjäla certifikatet. I och med examensarbetet så har mitt intresse för nätverksteknik- och IT-säkerhet vuxit och jag önskar att få börja arbeta med det här i framtiden. I framtiden planerar jag att utveckla mina kunskaper ytterligare inom nätverksteknik- och IT-säkerhet och gå en utbildning som etisk hackare. Inom den här utbildningen lär man sig känna till säkerhetsproblem och risker i olika nätverk samt hur man skyddar sig mot dessa. Man får också teoretiska kunskaper att kunna agera som angripare (hackare) dvs. kunskaper om hur man bryter sig in i ett nätverk. Efter utbildningen kan man börja jobba som IT-säkerhetstekniker, vilket är ett drömyrke för mig.

Källförteckning

Bergman, J., 2014. *Planering av rollbaserade mapprättigheter i Windows-miljö*. Raseborg: Lärdomsprov för tradenom examen. Yrkeshögskolan Novia, Informationsbehandling.

Bergström, B., 2014. *Säker åtkomst till företagsnätverk via mobila enheter*. Helsingfors: Lärdomsprov för ingenjörsexamen. Yrkeshögskolan Arcada, Sektorn för informations- och medieteknik.

Checkpoint a, 2016. *Capsule Connect and Capsule VPN Clients* [Online] http://downloads.checkpoint.com/dc/download.htm?ID=20361 [hämtat: 3.3.2019].

Checkpoint b, (u.å.). *Mobile Access (SSL VPN Portal)* [Online] https://www.checkpoint.com/products/remote-access-vpn/ [hämtat: 3.3.2019].

Checkpoint c, 2018. *SecuRemote* [Online] https://sc1.checkpoint.com/documents/R80.20_GA/WebAdminGuides/EN/CP_R80.20_RemoteAccessVPN_AdminGuide/html_frameset.htm [hämtat: 3.3.2019].

Checkpoint d, (u.å.). *Facts at a Glance* [Online] https://www.checkpoint.com/about-us/facts-a-glance/ [hämtat: 4.3.2019].

Checkpoint e, (u.å.). *IPSec VPN Software Blade* [Online] https://www.checkpoint.com/products/ipsec-vpn-software-blade/ [hämtat: 4.3.2019].

Checkpoint f, (u.å.). *Endpoint Security* [Online] https://www.checkpoint.com/products-solutions/endpoint-security/ [hämtat: 12.3.2019].

Davies, J., 2016. *The Name Resolution Policy Table* [Online] https://docs.microsoft.com/en-us/previous-versions/technet-magazine/ff394369(v=msdn.10) [hämtat: 11.12.2018].

Edström, M. & Fridh Kleberg, C., 2015. *Digitalt självförsvar – en introduktion* [Online] https://www.iis.se/lar-dig-mer/guider/digitalt-sjalvforsvar-en-introduktion/kryptering/ [hämtat: 8.12.2018].

Elmsjö, H., 2009. *Så får du kontroll på Windowsmiljön med GPO* [Online] https://techworld.idg.se/2.2524/1.230192/sa-far-du-kontroll-pa-windowsmiljon-med-gpo [hämtat: 12.12.2018].

Elmsjö a, 2010. *Bakom kulisserna på Direct Access.* [Online] https://www.idg.se/polopoly_fs/1.388881!sa_funkar_direct_access-techworld.pdf [hämtat: 11.12.2018].

Elmsjö b, 2010. *Egen vpn-lösning med Direct Access.* [Online] https://techworld.idg.se/polopoly_fs/1.388913.1316610927!egen_vpn_med_da-techworld.pdf [hämtat: 12.3.2019].

EVRY, (u.å.). *Enterprise Mobility Management, EMM* [Online] https://www.evry.com/sv/branscher-och-tjanster/tjanster/applikationstjanster-och-losningar/mobilitet/mobile-management/emm/ [hämtat: 12.3.2019].

IBM a, (u.å.). *MaaS360 VPN module* [Online] https://www.ibm.com/support/knowledgecenter/en/SS8H2S/com.ibm.mc.doc/ce_source/concepts/ce_vpn_overview.htm [hämtat: 8.12.2018].

IBM b, (u.å.). *Cloud Extender architecture* [Online] https://www.ibm.com/support/knowledgecenter/en/SS8H2S/com.ibm.mc.doc/ce_source/references/ce_architecture.htm [hämtat: 10.3.2019].

Kihl, M. & Andersson, J. A., 2013. *Datakommunikation och nätverk*. 1:3 red. Lund: Studentlitteratur AB.

Kjell & Company, 2018. *VPN-tunnlar* [Online] https://www.kjell.com/se/fraga-kjell/hur-funkar-det/natverk/lokala-natverk/vpn-tunnlar#vpn-principen [hämtat: 8.12.2018].

Microsoft, 2009. *Types of Certification Authorities* [Online] https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732368(v=ws.11) [hämtat: 11.12.2018].

Microsoft, 2013. *Network location server* [Online] https://docs.microsoft.com/en-us/previous-versions/tn-archive/gg315317(v=technet.10) [hämtat: 11.12.2018].

Microsoft, 2015. *Active Directory Certificate Services (AD CS) Introduction* [Online] https://social.technet.microsoft.com/wiki/contents/articles/1137.active-directory-certificate-services-ad-cs-introduction.aspx [hämtat: 11.03.2019].

Rasmussen, H. D., 2018. *Vad är en DNS-server?* [Online] https://pctidningen.se/internet/vad-ar-en-dns-server [hämtat: 11.3.2019].

Snellman, 2016. *Årsberättelse 2016* [Online] https://www.snellmangroup.fi/vuosikertomukset/Snellman_Vuosikertomus_2016.pdf [hämtat: 12.3.2019].

Strömbergson, J., 2011. *Så säkert jobbar du hemma med vpn* [Online] https://techworld.idg.se/2.2524/1.402809/sa-sakert-jobbar-du-hemma-med-vpn/sida/4/3-direct-access [hämtat: 12.3.2019].

Techworld Special, 2015. *Framtidens brandväggar – så fungerar moderna nätverksskydd* [Online] https://whitepaper.idg.se/techworld/techworld-special--framtidens-brandvaggar [hämtat: 8.12.2018]

Techworld Sverige, 2010. *Direct Access i praktiken – Del 4 (Konfiguration av Direct Access)* [Online] https://www.youtube.com/watch?v=KKRhaCIjeU0 [hämtat: 12.12.2018].

Figurförteckning