Upprätthållande av nätverkssäkerhet inom småföretag

En studie om hur lokala nätverk byggs upp och hur man i småföretag upprätthåller säkerhet och identifierar hot

Innehållsförteckning

Referat

1. Introduktion

I en tid där cyberhot mot företag blivit vardag är upprätthållandet av nätverkssäkerhet viktigare än någonsin. Speciellt småföretag, som inte besitter samma resurser som sina storskaliga konkurrenter, ligger i riskzonen och behöver satsa på att bygga upp stabila nätverk så framtida angrepp inte blir ohanterliga och lämnar irreversibla skador efter sig. För det är inte frågan om *om* ett företag kommer bli utsatt, utan *när*.

Begreppet småföretag är brett, men som utgångspunkt i den här avhandlingen ligger mindre företag som använder sig av lokala nätverk (LAN) för att upprätthålla sin verksamhet. Nätverk binder ihop alla tekniska enheter runt om oss. Mellan dessa enheter sker kommunikation och datautbyte. Det finns många typer av nätverk. De vanligaste är personliga nätverk (PAN), redan nämnda LAN, stadsnätverk (MAN) och globala nätverk (WAN). PAN består av enskilda personers sammankopplade teknik. LAN ansluter datorer och enheter i ett begränsat område, oftast samma byggnad. MAN kopplar samman nätverk över större områden såsom städer. WAN används för att sluta samman nätverk över hela världen.

LAN har många användningsområden. J.Fortier et al. diskuterar ett flertal exempel på hur företag kan dra nytta av LAN [1]. Ett LAN kopplar samman närliggande enheter och möjliggör snabb och smidig delning av resurser och data på både lokal och global nivå. Nätverkstrafiken i ett LAN kan övervakas och säkerhetssystem implementeras. LAN är flexibla och kan struktureras enligt de behov företaget har, och kan sedan modifieras och expanderas i takt med introduktionen av ny teknologi. Genom att bygga upp stabila LAN och utrusta dem med pålitliga säkerhetskomponenter minimeras risken för lyckade cyberattacker.

2. Uppbyggnad av lokala nätverk

De säkerhetssystem småföretag väljer att implementera i sina nätverk anpassas efter nätverkets uppbyggnad. LAN kan struktureras på många sett med datorkommunikation och dataöverföring i åtanke.

2.1 Modellering och standarder

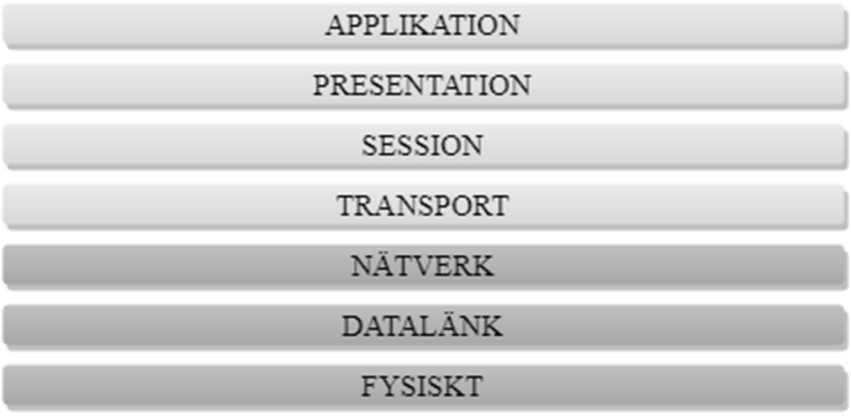
En nätverksmodell är en abstraktion av ett nätverkssystem och dess komponenter [1]. Nätverksmodeller strävar efter att använda universella standarder för att möjliggöra kommunikation med enheter utanför nätverket. Standarderna som följs tas ofta fram av neutrala organisationer, såsom internationella standardiseringsorganisationen (ISO) och institutet för elektriska och elektroniska ingenjörer (IEEE). Kommunikation mellan enheter i LAN upprätthålls genom att följa IEEE 802-standarden. IEEE har utvecklat strukturer och nätverksstandarder för bland annat lokala nätverk och stadsnätverk, uppbyggda av protokoll och procedurer som möjliggör både trådbunden och trådlös kommunikation på global nivå. Nätverksarkitektur använder sig i regel av de öppna systemens sammankopplingsmodell, OSI-modellen (ISO/IEC 7498), som tagits fram av ISO.

2.2 Nätverksprotokoll

Enheter i ett nätverk kallas för noder [1]. Noder kopplas upp till nätverk och kommunicerar med andra noder genom nätverksgränssnitt, som byggs upp av lager av protokoll. Protokoll fungerar som instruktioner för dataöverföring, så noderna vet hur data ska grupperas, adresseras och kvitteras. Data som skickas över nätverk kallas allmänt för meddelanden [2], och struktureras enligt de protokoll som används. Ett typiskt meddelande består av två komponenter: adressinformation och data. Adressinformation är bitar som innehåller information om mottagarna och avsändarna av data. Data är informationen som ska överföras.

2.3 OSI och TCP/IP

I OSI-modellen delas nätverkskommunikation upp i sju lager, där varje lager består av protokoll som tilldelats egna uppgifter. De sju lagren är applikations-, presentations-, sessions-, transport-, nätverks- och datalänksskiktet samt det fysiska skiktet. De tre förstnämnda lagren grupperas i ett övre lager som hanterar data på applikationsnivå, och de resterande fyra i ett nedre lager som koncentrerar sig på datatransport.



Figur 2.1: OSI-modellen.

Mängden protokoll i varje lager varierar beroende på de funktioner nätverket har. Pramberger [3] har samlat ett stort utbud av protokoll på en hemsida och listar i vilka lager de funktionerar. I det övre lagret i LAN kan det hittas flera exempel på välkända protokoll. I applikationsskiktet finns *HyperText Transfer Protocol* (HTTP) och *File Transfer Protocol* (FTP). HTTP används för att hämta material från webbsidor och FTP för att flytta filer mellan datorer. I presentationsskiktet sköter protokollet transportlagersäkert (TLS) om datakryptering. I sessionsskiktet finns *Layer 2 Forwarding Protocol* (L2F) och *Layer 2 Tunneling Protocol* (L2TP), som båda används för att etablera virtuella privata nätverk (VPN).

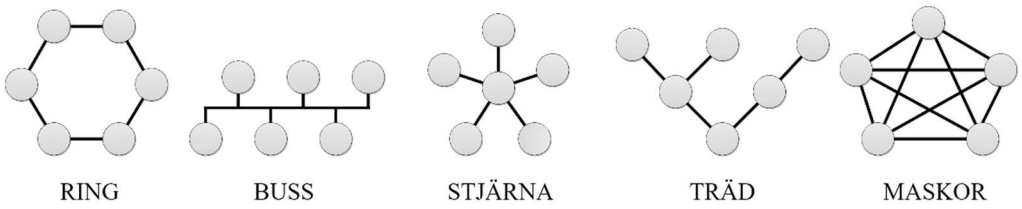
Likaså finns det välkända exempel på protokoll i det nedre lagret. I transportskiktet finns *Transmission Control Protocol* (TCP) och *User Datagram Protocol* (UDP), som båda används vid transport av data. TCP är förbindelseorienterat och kräver en anslutning mellan två noder för att överföra data mellan dem, medan UDP är förbindelselöst och kan överföra data utan en direkt anslutning [4]. I nätverksskiktet hittas IP-protokoll, som hanterar transport av data utifrån IP-adresser i adressinformationen. Datalänksskiktet kan delas upp i två underskikt enligt IEEE 802-standarden, *Logical Link Control* (LLC) och *Media Access Control* (MAC). LLC ansvarar för multiplexering av nätverksprotokoll och i MAC sköter protokollen om datainkapsling. Slutligen, i det fysiska skiktet, konverteras data till bitar som kan överföras i form av signaler eller vågor.

En annan nätverksmodell är TCP/IP-modellen, som också bygger på protokollagren i OSI-modellen [2]. Det övre lagret i OSI-modellen fungerar som ett enda applikationsskikt i TCP/IP. I stället för sju lager består arkitekturen av fyra eller

fem lager, beroende på om datalänkslagret är hopslaget med det fysiska lagret. Ett välbekant WAN, internet, använder sig av TCP/IP och är uppbyggt av ett länk-, internet-, transport-, och applikationsskikt. Som synes används benämningen internetskikt i stället för nätverksskikt, vilket är standard för alla TCP/IP-modeller.

2.5 Datorkommunikation

Noderna i LAN kan kopplas ihop enligt olika mönster, vilket kallas nätverkstopologi. Nätverkstopologi existerar på både fysisk och logisk nivå. Sammankopplandet av enheter kan alltså vara konkret, såsom hur kablarna dras mellan nätverkets datorer, eller abstrakt, där nätverkets struktur och dataflöde teoretiseras. Noderna kan kopplas som ringar, bussar, stjärnor, träd eller maskor [1], se figur 2.2. I en ringtopologi är varje nod kopplad till enbart två grannoder, vilket skapar en cirkelstruktur. Data kan endast flöda åt ett håll, om noderna inte har dubbla förbindelser till sina grannoder, vilket möjliggör dataflöde också åt motsatt håll. I busstopologin kopplas alla noder till en och samma sträcka. I stjärntopologin kopplas alla noder till en nätverksväxel (kapitel 2.8), och formar en stjärnstruktur. I en trädtopologi är varje nod kopplad till högst två andra noder, och skapar en trädstruktur med över- och underordnade noder. I masktopologi kopplas alla noder till varandra. Det är också möjligt att kombinera de olika topologierna, vilket kallas hybridtopologi.



Figur 2.2: Nätverkstopologier.

Relationen mellan enheter i ett nätverk kan antingen vara icke-hierarkisk (eng. *peer-to-peer*) eller klient-server (eng. *client-server*) [2]. I klient-servermodellen fungerar en eller flera datorer som servrar. Servrarnas uppgift är att ta emot förfrågningar från de resterande datorerna, klienterna, och förse dem med de tjänster som efterfrågas. Klienterna är ofta mindre utrustade datorer, eftersom de inte har samma behov av minnesallokering och -kapacitet. I den icke-hierarkistiska modellen är alla datorer i nätverket likadant utrustade och fungerar både som

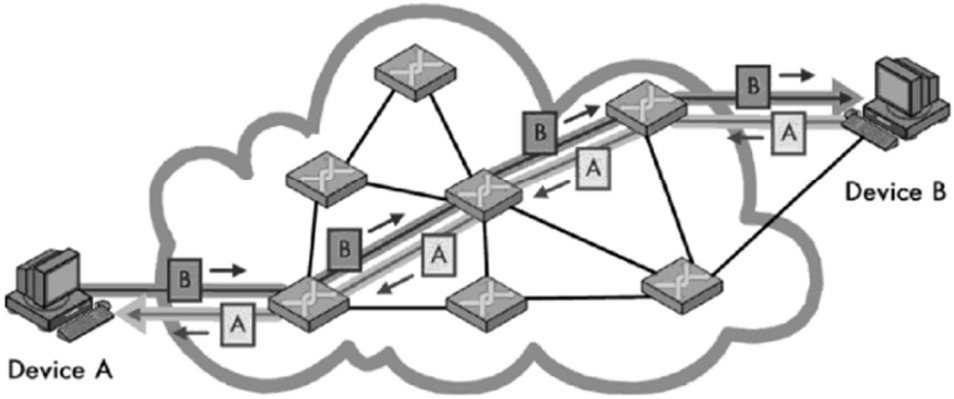
servrar och klienter. Datorerna hanterar varandras förfrågningar och upprätthåller dataöverföring i nätverket. Alla datorer sparar också sina egna data, jämfört med i klient-servernätverk där data sparas i servrarna.

Kommunikation mellan noder kan dirigeras på fyra olika sätt [2]. Den vanligaste metoden är enkelsändning (eng. *unicasting*), där data överförs från en enhet till en specifik mottagare. Det finns också flersändning (eng. *multicasting*), som är en dirigeringsmetod där en enhet överför data till en mottagargrupp bestående av flera andra enheter. Nästsändning (eng. *anycasting*) har på liknande sätt en specifik grupp mottagare, men avläser IP-adresser för att hitta den närmast liggande enheten i gruppen och förmedlar data enbart till den. Slutligen finns också bredsändning (eng. *broadcasting*), där data överförs från en enhet till alla andra enheter i nätverket.

2.6 Dataöverföring

Processen att överföra data mellan noder kallas dataöverföring. Dataöverföring i ett nätverk kan mätas i hastighet, bandbredd, genomströmning och latens [2] – överföringshastighet, den potentiella mängden data som kan transporteras i ett tidsintervall, den faktiska mängden data som transporteras i tidsintervallet och tidssambandet mellan förfrågan och överföring. Beroende på vilka funktioner som prioriteras i ett nätverk struktureras dataöverföringen efter det.

Hur enheter kopplas till varandra baserar sig på om de är anslutningsorienterade (eng. *connection-oriented*) eller anslutningsfria (*eng. connectionless*) [2]. Anslutningsorienterade enheter måste skapa en logisk anslutning mellan varandra innan dataöverföring kan påbörja, jämfört med anslutningsfria enheter som inte kräver en logisk anslutning. Således sker dataöverföring mellan enheter genom kretskoppling eller paketförmedling [2]. När kretskopplade enheter etablerar en anslutning är de bundna till varandra under hela kommunikationen, så data kan strömma direkt mellan enheterna. Vid paketförmedling delas data som ska överföras upp i små paket som kan ta olika vägar för att nå den andra enheten, och kräver därför ingen direkt anslutning.



Figur 2.3: Anslutningsorienterat nätverk [2] (tillfällig bild).

Sammankopplade enheter kan kommunicera över en förbindelse på tre sätt [5]. De tre överföringslägena är simplex, halvduplex och helduplex. Simplex innebär att data bara strömmar åt ett håll. Den ena parten kan enbart skicka data och den andra enbart ta emot. Duplex betyder att data kan strömma åt två håll. Vid användning av halvduplex kan båda parterna skicka och ta emot data, men enbart en i taget. När en enhet skickar data, måste den andra enheten ta emot all data och vänta på att överföringen slutförts innan en ny överföring kan påbörjas. Helduplex innebär att båda parterna kan skicka och ta emot data ömsesidigt. Enheterna behöver alltså inte vänta på att den andra enheten ska bli färdig, utan data kan strömma åt båda hållen samtidigt. Vid användning av simplex och halvduplex kan dataströmmen nyttja hela kommunikationskanalen, medan de två olikriktade strömmarna i fullduplex måste dela på utrymmet.

2.7 Trådlösa och trådbundna nätverk

Anslutningen mellan tekniska enheter kan vara trådbunden eller trådlös, varav nätverk av den sistnämnda typen har blivit allt vanligare i takt med utvidgningen av smarta enheter och effektiva mobilnät.

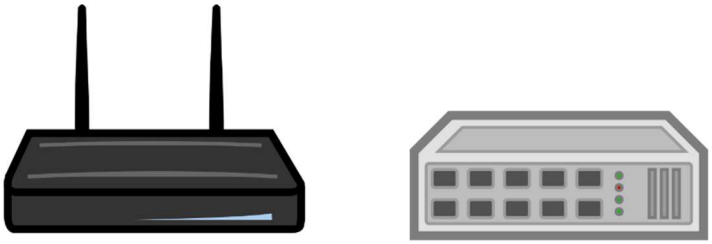
När enheterna i LAN kommunicerar trådlöst kallas nätverket för ett trådlöst lokalt nätverk (WLAN). Trots namnet använder sig WLAN ändå av trådbundna komponenter. Data i trådlösa nätverk överförs genom elektromagnetiska eller infraröda vågor som transporteras genom luften [6]. Det vanligaste trådlösa nätverket är Wi-Fi, som följer IEEE 802.11-standarden och hittas i många LAN både i privat och offentligt bruk. Allmänt känt är också Bluetooth, som följer IEEE

802.15-standarden och använder radiovågor för att överföra data trådlöst, ofta inom privata nätverk. Trådlösa nätverk är ofta smidiga att använda tack vare lättillgängligheten, men över lag är trådbundna nätverk effektivare när det kommer till dataöverföring.

Liksom namnet antyder, ansluts enheter i ett trådbundet nätverk med hjälp av fysiska trådar och kablar som transporterar data. De vanligaste komponenterna är koppartråd, parttvinnande kablar och fiberoptiska kablar gjorda i antingen plast eller glas [6]. Den mest allmänkända formen av trådbundet nätverk är Ethernet, som följer IEEE 802.3-standarden. Ethernet används inte bara LAN, utan också i större utsträckning så som MAN.

2.8 Nätverkskomponenter

Utöver de för ögat osynliga standarder som tillämpas på mjukvarunivå, så tillämpas också standarder på de fysiska nätverkskomponenterna vid uppbyggnad av nätverk. Ihopkopplandet av enheter kan göras med hjälp av nätverksväxlar (eng. *switches*). Tekniska enheter kopplas till portarna som finns på nätverksväxeln och får således direkt kontakt till alla andra uppkopplade enheter. Alla enheter har unika MAC-adresser, så genom att avläsa inkommande datapakets avsändar- och mottagaradresser kan nätverksväxeln hantera dataöverföring och skicka vidare data till rätt uppkopplade enheter. Nätverksväxlar kan vara hanterade (eng. *managed*) eller ohanterade (eng. *unmanaged*) [7], varav de förstnämnda kräver konfigurering vid installering men därför också erbjuder högre säkerhet än ohanterade nätverksväxlar.



Figur 2.4: Router och nätverksväxel (tillfällig bild).

Hopkoppling av nätverk sker genom routrar, antingen trådlöst eller trådbundet. En router kopplar ihop enheter och nätverksväxlar med andra nätverk, och används för

att bilda större sammanhängande nätverk [8]. Routrar tar emot datapaket och avläser adressinformationen, för att sedan föra vidare paketen till rätt mottagare i rätt nätverk. Inom LAN används routrar ofta för att koppla ihop nätverket med det globala nätverket internet. Internetuppkopplingen fås via ett modem, som är en nätverkskomponent med den specifika uppgiften att ge nätverk tillgång till internet. Uppkopplingen fås från en internetleverantör (ISP). Routrar och modem samverkar ofta genom att routern upprätthåller det lokala nätverket och modemet förser det med internet.

3. Hårdvara och mjukvara för nätverkssäkerhet

3.1 Kryptering

3.2 Brandväggar

3.3 Virusskydd

3.4 IPS och IDS

3.5 VPN

4. Förverkligande av nätverkssäkerhet inom småföretag

Nätverkssäkerhet inom företag innebär att skydda nätverket från hot utifrån och upprätthålla funktionalitet som håller data säkert i företaget. Att förstå var det lönar sig att satsa mer på säkerheten är en väsentlig del av upprätthållandet av nätverket. Säkerheten i ett nätverk kan kontrolleras och delas upp i tre olika nivåer [12]. Den första nivån är att förhindra hot, den andra att upptäcka hot och den tredje att motverka hot och åtgärda skador. Säkerheten i de olika nivåerna baserar sig på hur nätverket är uppbyggt och de säkerhetsmetoder som finns att tillgå. Skriftlig säkerhetspolitik (eng. *security policy*) [14] kan användas som en garanti på att allt i nätverket konfigureras på rätt sätt. Viktigt att komma ihåg är att säkerhet är en process som aldrig tar slut, utan som ständigt måste underhållas.

4.1 Dataformer

Alla företag besitter data som behöver säkras. Säkerhetsåtgärder i ett nätverk bör anpassas efter värdet på den data som ska skyddas, med tanke på att småföretag ofta har ofta en begränsad mängd resurser. Företagsdata kan antingen vara i ett vilande stadie, i en slutpunkt eller i ett rörande stadie [13], och alla stadier kräver egna säkerhetsåtgärder. Vilande data är data som ligger orört i exempelvis filsystem och databaser. Här spelar åtkomstreglering en stor roll för att se till att enbart rätt personer kommer åt platsen där data ligger lagrad. Data i en slutpunkt data är data som befinner sig i slutpunkter i nätverket. Till exempel datorer och externa hårdskivor. Också här är åtkomstreglering viktigt, men på en fysisk nivå där enbart rätt personer har tillgång till rätt avdelningar och maskiner. Rörlig data är data som rör sig inom och utanför nätverket, exempelvis genom filöverföring och mejl. På den här nivån kommer nätverksövervakning in i bilden.

4.2 Risker och hot

Hot inom företag kan vara störningar eller uppstå till följd av obehörig åtkomst [12]. Störningar sker i samband med mänskliga och tekniska fel, och grundar sig i nätverkets uppbyggnad. Exempelvis när en del av nätverket fallerar ska inte hela nätverket slockna. Obehörig åtkomst syftar på situationer där personer kommer åt data de egentligen inte ska ha tillgång till, så data riskerar att bli stulen eller obehörigt modifierad.

Risker kan i alla fall inte tas bort helt, men kan minskas [14]. Man kan antingen undvika risken genom att strukturera om nätverk eller databasen. En risk kan lindras. Man kan också lägga ansvaret på en tredjepart som får ta hand om risken, även om det inte garanterar säkerhet heller. Till slut kan man också bara acceptera att risken finns, för inget system är hundraprocentigt säkert för alltid. Då gäller det att övervaka systemet noggrannt och kanske lägga extra resurser på det här området.

För att minska på hot finns det vid säkerhetsställning av nätverk tre områden [14] som bör tas i beaktande: människor, procedur och teknologi. Människor, eller mer specifikt arbetare, måste förstå sig på allvaret med nätverkssäkerhet och vara beredda på att upprätthålla det. Säkerhetsprocedurer och -rutiner måste finnas och följas för att hålla nätverket säkert. Teknologin, alltså hårdvaran och mjukvaran i nätverket som används för att hålla nätverket säkert, måste passa nätverksstrukturen och vara av tillräckligt god kvalitet.

4.3 Förhindrade av hot

För att förhindra hot från att uppstå kan företag använda sig av analyser [14]. I en risksanalys strukturerar man upp hotfulla scenarion och vilka åtgärder som ska tas om de skulle uppstå. I en konsekvensanalys ligger fokus på vad kostnaderna för dessa scenarion skulle bli. Detta ger en bättre bild på var företager ska satsa sina resurser. Exempel på hotfulla scenarion är då nätverket fallerar eller saktas ner till följd av teknikfel eller utomstående attacker. Genom att analysera nätverkets topologi (kapitel 2.5) och dataöverföring (kapitel 2.6), kan man hitta svaga punkter dit fler säkerhetsresurser måste fokuseras.

Utöver den tekniska biten är en viktig faktor vid förhindrande av hot i företag att utbilda personalen. Simpla åtgärder kan räcka en lång väg, såsom att lära personal vara uppmärksamma för misstänkt aktivitet i nätverket och att påminna dem om att inte lämna olåsta arbetsenheter oövervakade. Beroende på de arbetsroller som finns i företaget, är användarna i olika riskgrupper. Ju större tillgång i företagets nätverk anställda har, desto större är risken att deras åtkomst missbrukas, vilket kan ske till följd av både misstag och medvetet handlande. Det gäller alltså att se till att en anställd enbart har tillgång till den data denne behöver och förhindra åtkomsten för alla obehöriga, vilket kallas identitets- och åtkomsthantering. Identitets- och åtkomsthantering bygger på sekretess, integritet och tillgång [12], vilket betyder att

enbart auktoriserade användare har tillgång till nätverket, att användare enbart har tillgång till och kan modifiera data de behöver, och att användare alltid har tillgång till data då de behöver den.

4.4 Nätverksövervakning

4.5 Åtgärdande av skador

5. Avslutning

Källförteckning

[1] Paul J. Fortier, George R. Desrochers (1990) “Modeling and Analysis of Local Area Networks”

[2] Charles M. Kozierok (2005) “The TCP/IP Guide: A Comprehensive, Illustrated Internet Protocols Reference”

[3] Roman Pramberger “Open Systems Interconnection model” https://osi-model.com/ (hämtad 18.02.2022)

[4] IBM “TCP/IP TCP, UDP, and IP protocols” https://www.ibm.com/docs/en/zos/2.2.0?topic=internets-tcpip-tcp-udp-ip-protocols (hämtad 26.02.2022)

[5] Behrouz A. Forouzan (2007) “Data Communications and Networking”

[6] GeeksforGeeks “Wired and Wireless Networking” https://www.geeksforgeeks.org/wired-and-wireless-networking/ (18.02.2022)

[7] Gary McCauley “Network Switch: Managed vs Unmanaged” https://www.fieldengineer.com/blogs/network-switch-managed-vs-unmanaged (28.02.2022)

[8] Java T Point “Switch Vs. Router” https://www.javatpoint.com/switch-vs-router (hämtad 26.02.2022)

[12] Pramod Pandya (2014) “Network and System Security: Chapter 9. Local Area Network Security”

[13] Lyong S.L. Liu, D. Richard Kuhn (2010) Data Loss Prevention, p.10-13

[14] Syngress, et. al (2006) “Firewall Policies and VPN Configurations”