KRYEMINISTRIA

AGJENCIA KOMBËTARE PËR SIGURINË KOMPJUTERIKE (ALCIRT)

RREGULLORE PËR MENAXHIMIN E FIREWALL-VE

Miratuar me Urdhrin nr.10 datë 25.04. 2016 të Drejtorit të Agjencisë Kombëtare për Sigurinë Kompjuterike (ALCIRT).

Prill, 2016

Përmbajtje

Përkufizime

- *Wireless* – Komunikim me valë (pa tel).

- *Log* – Konsiderohet çdo shënim dixhital mbi një ngjarje ose aktivitet të caktuar.
- *Malware* – Një software i rrezikshëm, i cili ka qëllim ndërprerjen e operimit të një sistemi kompjuterik, mbledhjen e informacionit në mënyrë të paautorizuar ose marrjen në kontroll të një sistemi kompjuterik.
- *Antivirus / Antispyware/ Antimalware*- programe të cilat bëjnë të mundur kontrollin, identifikimin, eleminimin e programeve kompjuterike të dëmshme të instaluara në kompjutera (virus, trojan etj)
- *Firewall* – Pajisje apo një program kompjuterik që është i konfigururar për të kontrolluar trafikun që kalon nëpër rrjet, duke e lejuar apo bllokuar atë në bazë të një grupi rregullash.
- *Intrusion Detection technology* - Teknologji inspektimi që analizon protokollet në shtresën e aplikimit për të krahasuar profilet e aktivitetit të protokollit të prodhuesit me eventet e observuara për të identifikuar devijimet.
- *Incident Kompjuterik* – ngjarje e ndodhur në një kompjuter dhe që dëmton konfidencialitetin, integritetin apo disponueshmërinë e një kompjuteri apo sistemi; apo të dhënat që mban ai.
- *Storage* – Memorje kompjuterike të cilat përdoren për ruajtjen masive të të dhënave
- *Software* – Programe kompjuterike
- *VPN* – Rrjete private virtuale të cilat ofrojnë siguri të lartë
- *Application-Proxy Gateway* – cilësi e firewall-eve të avancuar që kombinojnë kontrollin e aksesit në shtresën më të ulët me funksionalitetet e shtresës më të lartë.
- *Proxies* – Aplikacione të cilat lehtësojnë aksesin në Internet
- *Routera* – Pajisje rrjeti të cilat bëjnë menaxhimin dhe dërgimin e paketave të rrjetit
- *Switche* – Pajisje rrjeti të cilat bëjnë dërgimin e paketave të rrjetit
- *Username* – emër përdoruesi, varg karakteresh që identifikon në mënyrë unike një përdorues në një sistem apo rrjet kompjuterik.

- *Password* – fjalëkalim, kod sekret i një përdoruesi që nuk duhet të njihet nga përdoruesit e tjerë, dhe që i përdorur bashkë me UserID, lejon aksesimin e një sistemi.
- *IDPS* – Sisteme për parandalimin e sulmeve kibernetike të cilat monitorojnë rrjetat ose sistemet kompjuterike.
- *Network* – Rrjet kompjuterik.
- *TLS* – Protokoll kriptografik i cili ofron siguri për transportin e të dhënave në Internet.
- *IP* – Adresë elektronike e përbërë nga një numër prej 32 bitesh.
- *UDP* – Protokoll rrjeti i cili përdoret në rastet kur nuk nevojitet një transferim i besueshëm.
- *FTP* – Teknologji e cila lejon transferimin e skedarëve në Internet.
- *Worm* – Malware i cili replikon veten në sa më shumë sisteme kompjuterike.
- *SMNP* – Protokoll standart i Internetit për menaxhimin e pajisjeve të rrjetave IP.
- *Enkapsulim* – Procesi i paketimit të të dhënave të nivelit paraardhës dhe shtimi i të dhënave të nivelit aktual gjatë procesit të paketës.
- *Host* – Kompjuter kryesor ose kontrollues i cili jep shërbime kompjuterike ose të dhënakompjuterave ose terminaleve të lidhur nëpërmjet rrjetit.
- *HTTP* – Protokoll aplikacioni për sisteme të shpërndara.
- *ICMP* – Protokoll bazë Interneti i përdorur kryesisht për shkëmbimin e mesazheve të gabimit.
- *Port span* – Procesi i kopjimit të trafikut të rrjetit në një portë tjetër për arsye monitorimi.
- *DHCP* – Protokoll rrjeti i cili menaxhon pajisjet e lidhura në rrjet.
- *Tunning* – Proces konfigurimi për rritje performance.
- *Spoofed* – Imitim i adresës në mënyrë që të duket sikur është dikush tjetër.
- *DNS* – Shërbim në Internet që përkthen emrat e domaineve në adresa IP.
- *Active X* – Bashkësi teknologjish e përdorur për shpërndarjen e informacionit.
- *Handshake* – Procesi i fillimit të komunikimit mes dy pajisjeve.
- *Payload* – Përmbajtja e paketës së rrjetit.
- *Debugging* – Procesi i gjetjes së gabimeve.
- *Cashing* – Kalimi në pjesën e memorjes e cila ka shpejtësi mjaft të lartë komunikimi.
- *Scalability* – Aftësia për t'u përshtatur me rritjet sasiore në te ardhmen.
- *Stateful firewall* – çdo firewall që realizon inspektim *stateful* të paketave është një firewall që ruan gjurmët e gjendjes së lidhjeve në rrjet. Firewall-i është i programuar që të

dallojë paketat legjitime që vijnë nga tipe të ndryshme të lidhjeve. Vetëm paketat që përputhen me një gjendje lidhjeje që njihet do të lejohen nga firewall-i. Të tjerat do të refuzohen.

- *Stateless firewall* – firewall i cili trajton secilën paketë individualisht. Ky firewall nuk ka dijeni nëse paketa është pjesë e një komunikimi ekzistues, po krijohet komunikim i ri, apo është thjesht paketë e rreme.

Përmbledhje

Firewall-et janë pajisje ose programe që kontrollojnë mënyrën e kalimit të trafikut të rrjetit midis këtij të fundit dhe host-it i cili mund të ketë gjendje të ndryshme sigurie. Dikur, firewall-et shpërndaheshin në të gjithë perimetrin e rrjetit. Kjo bënte të mundur pajisjen me masa mbrojtëse të hoste-ve të brendshëm, por gjithsesi nuk bëhej njohja e të gjitha instancave dhe formave të sulmeve dhe të sulmeve që dërgohen nga një host i brendshëm tek një tjetër, të cilët shpesh nuk kalojnë në firewall-et e rrjetit. Për këtë arsye dhe për faktorë të tjerë, projektuesit e rrjeteve shpesh përfshijnë firewall-e funksionale në vende të tjera jashtë perimetrit të rrjetit për të siguruar një nivel më të lartë sigurie si dhe të mbrojnë pajisjet e lëvizshme të cilat janë vendosur në rrjetin e jashtëm.

Kërcënimet gradualisht kanë kaluar nga të qënurit më të përhapur në shtresën e ulët të trafikut të rrjetit tek shtresa e aplikimit, gjë që ka reduktuar efektivitetin e përgjithshëm të firewall-ve në ndalimin e kërcënimeve që kalojnë në rrjetin e komunikimit. Megjithatë, firewall-et ende duhet të bllokojnë kërcënimet që vazhdojnë të jenë në shtresën e trafikut të rrjetit. Firewall-et gjithashtu mund të ofrojnë mbrojtje në shtresën e aplikimit, duke plotësuar aftësitë e teknologjive të sigurisë së rrjetit.

Ekzistojnë disa tipe firewall-esh, të cilët variojnë nga mënyra e analizimit të trafikut në rrjet dhe lejimi ose bllokimi i instancave specifike duke krahasuar karakteristikat e trafikut me politikat ekzistuese. Të kuptuarit e kapaciteteve të secilit tip firewall-i, dhe dizenjimit të politikave për firewall-et dhe përvetësimin e një teknologjie firewall-i për të adresuar në mënyrë sa më efektive nevojat e institucioneve, janë kritike për të realizuar mbrojtjen e trafikut të rrjetit. Kjo rregullore jep një pamje të përgjithshme të teknologjive të firewall-eve, diskuton kapacitetet e tyre të sigurisë, avantazhet dhe disavantazhet në detaje. Gjithashtu në këtë dokument jepen shembuj se ku mund të vendosen firewall-et në rrjet dhe implikime të vendosjes së firewall-eve në vendndodhje të veçanta. Në këtë dokument jepen rekomandime për krijimin e politikave për firewall-in dhe për zgjedhjen, konfigurimin, testimin, shpërndarjen dhe menaxhimin e zgjidhjeve per firewall-in.
Rregullorja nuk mbulon teknologjitë që quhen "Firewall" por kryesisht ekzaminon vetëm aktivitetet në shtresën e aplikimit, jo në shtresën e ulët të trafikut të rrjetit. Teknologjitë që janë të fokusuara në aktivitete të llojeve të veçanta të aplikimeve, siç janë firewall-et që bllokojnë e-mailet me përmbajtje të dyshimtë, nuk mbulohen në detaje në këtë dokument.
Për të përmirësuar efektivitetin dhe sigurinë e firewall-eve, institucionet duhet të implementojnë rekomandimet e mëposhtme:

Krijimin e një politike për firewall-in që specifikon se si duhet të trajtohet trafiku hyrës dhe dalës i rrjetit.
Politika e firewall-it përcakton se si firewall-i i institucionit duhet të trajtojë trafikun hyrës dhe atë dalës në rrjet për një adresë IP specifike, dhe për rang adresash, protokollesh, aplikimesh dhe tipet e përmbajtjeve të bazuara në informacionet e politikave të sigurisë së institucionit.

Institucionet duhet të realizojnë një analizë risku për të krijuar një listë me tipin e trafikut që ka nevojë institucioni dhe se si duhet të sigurohet ky i fundit – duke përfshirë tipet e trafikut që mund të përshkojnë firewall-in në rrethana të veçanta. Shembuj të kërkesave të politikave janë lejimi vetëm i protokolleve IP (Internet Protocol) të kalojnë, përdorimin e IP burim dhe destinacion, protokolli TCP (Transmission Control Protocol) të caktuar, dhe aksesimin e portave UDP (User Datagram Protocol), tipet e protokollit ICMP (Internet Control Message Protocol) dhe kodet që do të përdoren. Trafiku hyrës dhe dalës që nuk është i lejuar sipas politikës së firewall-it duhet të bllokohet, sepse ky trafik nuk i nevojitet institucionit. Kjo praktikë redukton rrezikun e sulmeve dhe gjithashtu mund të reduktojë trafikun në rrjetin e institucionit.

Identifikimi i të gjitha kërkesave që duhet të konsiderohen kur përcaktohen firewalle-t që do implementohen.

Institucionet duhet të konsiderojnë disa elementë në proceset e zgjedhjes dhe planifikimit të firewalle-ve. Ata duhet të përcaktojnë cilat hapësira të rrjetit duhet të mbrohen, dhe cilat tipe të teknologjisë së firewalle-ve do të jenë më efektive për tipet e trafikut që kërkojnë mbrojtje. Gjithashtu duhet konsideruar rëndësia e performancës, për integrimin e firewall-eve në rrjetin ekzistues dhe për infrastukturat e sigurisë. Dizenjimi i zgjidhjeve të firewall-eve përfshin kërkesa që lidhen me mjedisin fizik dhe personelin si dhe konsiderata për kërkesa në të ardhmen, si për shembull adoptimi i teknologjive të reja IPv6 ose rrjetat private virtuale (VPN).

Krijimi i një bashkësie rregullash të cilat zbatohen nga politikat e firewall-it gjatë mbajtjes së perfomancës së tij.

Grupi i rregullave të firewall-it duhet të jetë sa më specifik në lidhje me trafikun e rrjetit që ato kontrollojnë. Krijimi i një grupi rregullash përfshin përcaktimin e tipeve të trafikut që kërkohen, duke përfshirë protokollet që firewallet mund të kenë nevojë për qëllime menaxhimi. Detajet e krijimit të bashkësisë së rregullave ndryshojnë nga tipi i firewall-it dhe nga produktet specifike, por shumë firewall-e mund të mund ta përmirësojnë performancën e tyre duke optimizuar bashkësinë e rregullave të tyre.

Menaxhimi i arkitekturës së firewall-eve, politikave, programeve dhe komponentëve të tjerë përgjatë gjithë jetës së firewall-it.

Ka shumë aspekte të menaxhimit të firewall-it. Për shembull, zgjedhja e llojit ose llojeve të firewall-eve për të implementuar dhe pozicioni i tyre brenda rrjetit mund të ndikojë dukshëm në politikat e sigurisë që firewalli mund të zbatojë. Komponentët e perfomancës së firewall-it duhet të monitorohen për të identifikuar dhe adresuar çështjet e burimeve potenciale. Loget dhe alertet duhet të monitorohen në mënyrë të vazhdueshme për të identifikuar kërcënimet – ato të suksesshme dhe të pasuksseshme. Rregullat e firewall-eve dhe potitikat duhet të menaxhohen nga procese të kontrolluara për shkak të impaktit në sigurinë dhe operacionet e biznesit. Firewall-et duhet të përditësohen në mënyrë periodike për të shmangur vulnerabilitetet.

1. Hyrje

Agjencia Kombëtare për Sigurinë Kompjuterike (ALCIRT) bazuar në Vendimin Nr. 766 datë 14.09.2011, e ndryshuar, në zbatim të pikës 3 gërma d)

"Nxjerr rregullat e sigurisë së rrjeteve dhe të sistemeve kompjuterike shtetërore".

1.1 Qëllimi

Kjo rregullore ka për qëllim të ndihmojë institucionet të kuptojnë nevojën për një menaxhim efikas të teknologjive firewall dhe politikave të firewall-eve. Ai jep udhëzime praktike për zhvillimin e politikave dhe zgjedhjen, konfigurimin, testimin, implementimin dhe menaxhimin e firewall-it.

1.2 Fusha e zbatimit

Kjo rregullore është krijuar së pari për stafin teknik të teknologjisë së informacionit, si për personelin e rrjetit, të sigurisë dhe për menaxherët dhe administratorët e sistemeve, të cilët janë përgjegjës për dizenjimin e firewall-eve, zgjedhjen, implementimin dhe menaxhimin e tyre. Përmbajtja e rregullores supozon zotërimin e njohurive bazë për rrjetin dhe sigurinë e rrjetit.

1.3 Struktura e dokumentit

Rregullorja është e organizuar në katër kapituj:

- Kapitulli i dytë paraqet disa teknologji firewall-esh ku përfshihen filtrimi i paketave, inspektimi i paketave, aplikimin proxy gateway dhe gjithashtu jep informacion mbi firewall-et host-based personalë.
- Kapitulli i tretë paraqet vendosjen e firewall-eve në arkitekturën e rrjetit.
- Kapitulli i katërt paraqet politikat e firewall-eve dhe jep rekomandime mbi tipet e trafikut të cilësuar si të ndaluar.
- Kapitulli i pestë paraqet një pamje të përgjithshme të planifikimit dhe implementimit të firewall-eve. Ky seksion liston faktorët që duhen konsideruar për zgjedhjen e firewall-eve, dhe ofron rekomandime për konfigurimet e firewall-eve, testimin, implementimin dhe menaxhimin.

2. Pasqyrë e teknologjive të Firewall-it

Firewall-et janë pajisje ose programe që kontrollojnë mënyrën e kalimit të trafikut në rrjet midis këtij të fundit dhe host-it, i cili mund të ketë gjendje të ndryshme sigurie. Ndërsa firewall-et diskutohen shpesh në kontekstet e lidhjes së Internetit, ata mund të kenë zbatueshmëri edhe në mjedise të tjerë rrjetesh. Për shembull, shumë rrjete institucionesh implementojnë firewall-e për të kufizuar lidhjet drejt rrjetit të brendshëm dhe nga rrjeti i brendshëm drejt rrjetit të jashtëm. Duke implementuar firewall-e për të kontrolluar rrjetin, institucionet mund të parandalojnë aksesin e paautorizuar në burimet dhe sistemet e tij. Përfshirja e një firewall-i ofron një shtresë shtesë për sigurinë.

Ekzistojnë disa tipe të teknologjive firewall. Një mënyrë për të krahasuar kompatibilitetin është të shohësh në shtresën TCP/IP të secilit. Komunikimet TCP/IP përbëhen nga katër shtresa që

punojnë së bashku për të transferuar të dhënat midis hosteve. Kur një përdorues dëshiron të transferojë të dhëna në rrjet, të dhënat kalojnë nga shtresa më e lartë nëpërmjet shtresës së mesme në shtresën më të ulët, duke shtuar informacion në secilën prej tyre. Shtresa më e ulët dërgon të dhënat e mbledhura në rrjetin fizik, duke i dërguar më pas ato në shtresat më të larta drejt destinacionit. E thënë ndryshe, të dhënat që prodhohen nga njëra shtresë enkapsulohen në një njësi më të madhe në shtresën poshtë saj.

Shtresa e aplikimit Kjo shtresë dërgon dhe merr të dhëna për aplikime të caktuara, si Domain Name System (DNS), Hypertext Transfer Protocol (HTTP), dhe Simple Mail Transfer Protocol (SMTP). Shtresa e aplikimit ka shtresa protokolli brenda saj. Për shembull, SMTP enkapsulon Kërkesën për Komente (RFC – Request for Comments), e cila enkapsulon Multipurpose Internet Mail Extensions (MIME), e cila enkapsulon të tjerë formate si Hypertext Markup Language (HTML).
Shtresa e transportit Kjo shtresë ofron lidhje për transportin e shërbimeve në shtresën e aplikimit midis rrjeteve, dhe mund të sigurojë besueshmërinë e komunikimit. TCP (Transmission Control Protocol) dhe UDP (User Datagram Protocol) janë protokollet që përdoren më shpesh në shtresën e transportit.
Shtresa IP (e njohur edhe si shtresa e rrjetit) Kjo shtresë ruton paketat në rrjet. Protokolli i Internetit i versionit 4 (IPv4) është protokolli kryesor i shtresës së rrjetit. Protokollë të tjerë të përdorur në këtë shtresë janë IPv6, ICMP dhe IGMP.
Shtresa e Hardware (e njohur gjithashtu si Shtresa Data Link) Kjo shtresë trajton komunikimet në komunikimet e shtresës fizike. Protokolli më i njohur i kësaj shtrese është Ethernet.

Adresat në shtresën e të dhënave (Data Link), të cilat janë përcaktuar tek ndërfaqja e rrjetit janë të referuara si adresa *media akses kontroll* (MAC)-një shembulli kësaj është një adresë Etherneti që i përket një karte Etherneti. Politikat e firewall-it rrallëherë kanë lidhje me shtresën e të dhënave. Adresave në shtresën e rrjetit u referohemi si adresa IP. Shtresa e transportit identifikon aplikimet specifike në rrjet dhe sesionet e komunikimit; një host mund të ketë një numër të pacaktuar sesionesh të shtresave të transportit me hoste të tjerë në të njëjtin rrjet. Shtresa e transportit mund të përfshijë gjithashtu dhe nocionin e portës - numri i portës së destinacionit përgjithësisht identifikon një shërbim pritës në host-in e detinacionit, dhe porta e burimit përgjithësisht identifikon numrin e portës në host-in e burimit ku host-i i destinacionit duhet t'i përgjigjet.

Protokollet e transportit si TCP dhe UDP kanë porta, ndërkohë që protokollet e tjera të transportit nuk kanë. Kombinimi i portës burim me adresën IP-të burimit dhe i adresës IP të destinacionit me portën destinacion ndihmojnë në përcaktimin e sesionit. Shtresa më e lartë përfaqëson aplikimet e përdoruesve përfundimtarë - firewall-et mund të inspektojnë trafikun e aplikimit dhe mund t'i përdorin ato si baza për vendimet e politikave.

Firewall-et bazë mund të operojnë në një ose disa shtresa - zakonisht në shtresat e ulëta - kur shumica e firewall-eve të avancuar operojnë në të gjitha shtresat. Këto të fundit mund të perfomojnë një ekzaminim më të detajuar dhe më të rregullt.

2.1.0 Teknologjitë e firewall-eve

Ky seksion i rregullores ofron një pamje të përgjithshme të teknologjive të firewall-it dhe informacionet bazë mbi kapacitetet e tipeve që përdoren më shpesh. Procesi i implementimit të firewall-it është i kombinuar dhe me teknologji të tjera sidomos me rout-imin dhe me teknologji të tjera që shpesh shoqërohen me firewall-in por janë pjesë e këtyre teknologjive të tjera. Për shembull: NAT (Network Address Translation) konsiderohet se është teknologji firewall-i por në fakt është teknologji rout-imi. Shumë firewall-e përfshijnë elementë të karakterit filtrues për të zbatuar politikat e institucionit që nuk janë të lidhura në mënyrë të drejtpërdrejtë me sigurinë. Disa firewall-e kanë të përfshirë dhe teknologjitë IPS (Intrusion Prevention System), të cilat mund të reagojnë ndaj sulmeve që zbulojnë për të parandaluar dëme në sisteme që janë të mbrojtura me firewall.

Firewall-et shpesh janë të vendosur në perimetrin e rrjetit. Firewall-et e tillë mund të kenë një ndërfaqe të jashtme dhe të brendshme, ku ndërfaqja e jashtme është e vetmja që ndodhet në rrjetin e jashtëm. Këto dy ndërfaqe shpeshherë referohen përkatësisht si të mbrojtura dhe të pambrojtura respektivisht. Megjithatë të thuash për diçka nëse është apo nuk është e mbrojtur shpeshherë është e papërshtatshme sepse politikat e firewall-it punojnë në të dyja drejtimet; për shembull, mund të ekzistojë një politikë që ndalon ekzekutimin e një kodi të ekzekutueshëm për t'u dërguar nga brenda perimetrit jashtë tij.

2.1.1 Filtrimi i paketave

Veçoria kryesore e një firewall-i është filtrimi i paketave. Firewall-at e vjetër që ishin vetëm filtrues paketash ishin në thelb pajisje rout-imi të cilat ofronin funksionalitete për kontrollin e aksesit për adresat e host-eve dhe sesionet e komunikimit. Këto pajisje që njihen edhe si firewall-e inspektimi *stateless*, (shih përkufizimin: *stateless inspection firewalls*) nuk lënë gjurmë të gjendjes së rrjedhës së trafikut që kalon përmes firewall-it, që do të thotë për shembull: se ato nuk mund të shoqërojnë kërkesat e shumta brenda një sesioni të vetëm tek të tjerët. Filtrimi i paketave është në thelb të firewall-ve modern, por ka disa firewall-e që shiten sot të cilët bëjnë vetëm *statelesspacket filtering (shih te përkufizimet)*. Ndryshe nga filtrat më të avancuar, filtrat e paketave (*packet filters)* nuk fokusohen tek përmbajtja e paketave. Funksionalitetet e kontrollit të aksesit të tyre menaxhohen nga një grup direktivash që u referohemi si grup rregullash. Aftësitë e filtrimit të paketave janë ndërtuar në shumicën e sitemeve të operimit dhe pajisjet që janë të afta të bëjnë rout-im. Shembulli më i zakonshëm i një pajisje të pastër filtrimi paketash është një rout-er rrjeti që implementon listën e kontrollit të aksesit.

Firewall-et në formën e tyre më të zakonshme operojnë në shtresën e rrjetit. Kjo ofron kontrollin e aksesit të rrjetit bazuar në disa pjesë të veçanta të informacionit që ndodhet në paketa, ku përfshihen:

- Adresa IP e paketës së burimit ---adresa e host-it nga i cili paketa ka origjinën (si: 192.168.1.1)
- Adresa IP e paketës së destinacionit --- adresa e host-it ku paketat po mundohen të arrijnë (si: 192.168.2.1)

- Rrjeti ose protokolli i transportit që është përdorur për komunikimin ndërmjet host-it të burimit dhe atij të destinacionit si: TCP, UDP ose ICMP.
- Disa karakteristika të sesioneve të komunikimit të shtresës së transportit, siç është sesioni i portës së burimit dhe të destinacionit.
- Ndërfaqe që përshkohen nga paketa dhe drejtimet e tyre (hyrëse dhe dalëse).

Filtrimi i trafikut që është i drejtuar përbrenda njihet edhe si filtrim hyrës (*ingress filtering*). Edhe trafiku që del jashtë mund të filtrohet, dhe procesi njihet si filtrim dalës (*egress filtering)*. Institucionet mund të zbatojnë kufizime mbi trafikun e tyre hyrës, të tilla si bllokimi i përdorimit të protokollit FTP (*File Transfer Protocol)* ose parandalimin e sulmeve DoS (*Denial of Service)* që iniciohen nga brenda institucionit kundrejt subjekteve të jashtëm. Institucionet duhet të lejojnë vetëm atë trafik dalës që përdor adresat IP të burimit në përdorim nga institucionet – proces që ndihmon në bllokimin e trafikut me adresa të rreme (*spoofed addresses)* që rrjedhin në rrjete të tjerë. Adresat e rreme mund të shkaktohen nga evente keqdashëse të tilla si infektime nga malware (*malware infections)* ose host-e të kompromentuar që përdoren për të sulmuar, ose nga keqkonfigurim i paqëllimtë.

Filtrat e paketave *stateless* në përgjithësi janë më vulnerabël ndaj sulmeve që shfrytëzojnë problemet brenda specifikimeve të protokollit TCP/IP. Për shembull: shumë filtra paketash e kanë të pamundur të detektojnë se kur informacioni i adresës në shtresën e rrjetit të një pakete ka qenë i rremë ose i ndryshuar. Sulmet *spoofing*, si përdorimi i adresave të rreme në kokat e paketave, zakonisht përdoren për të shmangur kontrollet e sigurisë në platformat e firewall-eve. Firewall-et të cilët operojnë në shtresat e larta mund të pengojnë sulmet *spoofing* duke verifikuar që sesioni i komunikimit është krijuar, ose duke autentikuar përdoruesit para se të lejojë shkëmbimin e informacionit. Për këtë arsye shumë firewall-e që përdorin filter paketash ruajnë gjendjen e informacionit të paketave që kalojnë në firewall.

Disa filtra paketash mund të filtrojnë specifikisht paketa që janë të fragmentuara. Fragmentimi i paketave lejohet nga specifikimet e TCP/IP. Megjithatë fragmentimi i paketave është përdorur për t'i bërë sulmet të vështira për t'u zbuluar (duke i vendosur në brendësi të paketave të fragmentuara), dhe vetë fragmentimi është përdorur si një formë sulmi. Për shembull: disa sulme të bazuara në rrjet kanë përdorur paketa të cilat nuk duhet të ekzistonin në komunikime normale, si dërgimi i fragmenteve të paketave, por jo i fragmentit të parë, ose dërgimit të fragmenteve të paketave që mbivendosin njëra-tjetrën. Për të parandaluar përdorimin e paketave të fragmentuara në sulme, disa firewall-e janë konfiguruar që t'i bllokojnë paketat e fragmentuara.

Sot, paketat e fragmentuara në Internet shpesh krijohen jo për shkak të sulmeve, por për shkak të teknologjive të rrjeteve virtuale private (VPN) që enkapsulojnë paketa brenda paketave të tjera. Nëse enkapsulimi i paketave mund tëshkaktojë tejkalimin e përmasave maksimale të mediumit të transmetimit, njëra nga paketat duhet të fragmentohet. Bllokimi i paketave të fragmentuara nga firewall-et është fenomen i zakonshëm i ndërveprimit të rrjetit virtual privat (VPN).

Disa firewall-e mund të riasemblojnë fragmentet përpara se t'i kalojnë ato në rrjetin e brendshëm, megjithatë kjo kërkon burime shtesë të firewall-it, veçanërisht memorie. Firewall-et që kanë cilësinë e riasemblimit duhet të implementohen me kujdes, përndryshe mund të sulmohen me DDoS. Zgjedhja e implementimit të bllokimit, riasemblimit, ose kalimi i paketave të fragmentuara vendoset nga ndërveprimi midis rrjetit dhe sistemit në tërësi. Në këtë mënyrë, bllokimi automatik i të gjithë paketave të fragmentuara nuk është i rekomandueshëm për shkak të nevojës së përdorimit të fragmentimit në Internet.

2.1.2 Inspektimi Stateful

Inspektimi *stateful* përmirëson funksionimin e filtrimit të paketave duke ndjekur gjendjen e lidhjes *(state of connections)* dhe bllokimin e paketave të cilat devijojnë nga gjendja e përcaktuar. Ashtu si në filtrimin e paketave, inspektimi *stateful* monitoron paketat në shtresën e rrjetit dhe i inspekton ato për të parë nëse ato përputhen me rregullat ekzistuese të firewall-it, ose ndryshe nga filtrimi i paketave inspektimi *stateful* mban gjurmët për secilën lidhje në një tabelë gjëndjeje (*state table)*. Ndërsa detajet e tabelës së gjendjes variojnë nga lloji i firewall-it, ata përgjithësisht përfshijnë adresën IP të burimit, adresën IP të destinacionit, numrat e portave dhe informacion mbi gjendjen e lidhjes.

Ekzistojnë tri gjendje kryesore për trafikun TCP – krijimi i lidhjes, përdorimi dhe përfundimi (i cili i referohet përfundimit të një kërkese në fund të komunikimit dhe gjendjen e një lidhjeje që qëndron joaktive për një kohë të gjatë). Inspektimi *stateful* në firewall ekzaminon vlerat e caktuara në kokat e TCP për monitorimin e secilës gjendje. Çdo paketë e re krahasohet nga firewall-i me tabelën e gjendjeve të firewall-it për të përcaktuar nëse gjendja e paketës përputhet me gjendjen e saj të pritshme. Për shembull, një sulm mund të gjenerojë një paketë me një kokë që tregon se është pjesë e një komunikimi ekzistues, me shpresën se do të kalojë nëpër firewall. Nëse firewall-i përdor inspektimin *stateful,* së pari verifikon që paketa është pjesë e një komunikimi ekzistues në tabelën e gjendjeve.

Në rastin më të thjeshtë, një firewall do të lejojë kalimin e paketave që duken sikur janë pjesë e komunikimeve ekzistuese (ose e një komunikimi që nuk është krijuar plotësisht). Megjithatë, shumë firewall-e e njohin gjendjen e makinave për protokollet si TCP dhe UDP, dhe ata mund të bllokojnë paketa që nuk përputhen saktësisht me gjendjen e përshtatshme të makinës. Për shembull, zakonisht firewall-et kontrollojnë atributet si sekuenca e numrave të TCP dhe i refuzojnë paketat që janë jashtë kësaj sekuence. Kur firewall-i ofron edhe shërbimin NAT (*Network Address Translator)*, shpesh përfshin dhe informacione për NAT në tabelën e tij të gjendjes.

Tabela 2-1 jep një shembull të një tabele gjendjeje. Nëse një pajisje në rrjetin e brendshëm (për shembull 192.168.1.100) tenton të lidhet me një pajisje jashtë firewall-it (192.0.2.71) tentativa e lidhjes në fillim kontrollohet për të parë nëse lejohet nga bashkësia e rregullave të firewall-it. Nëse po, në tabelën e gjendjes shtohet një rresht i ri që tregon krijimin e një sesioni të ri, siç është treguar në tabelën 2-1 në rreshtin e parë tek "Gjendja e lidhjes". Nëse 192.0.2.71 dhe

192.168.1.100 përfundojnë TCP *handshake,* gjendja e lidhjes do të ndryshojë nga "E inicuar" në "E krijuar" dhe trafiku që përkon me këtë rresht lidhjeje do të lejohet të kalojë nga firewall-i.

Tabela 2-1 Shembull i një tabele gjendjeje

Adresa burim	Porta burim	Adresa destinacion	Porta destinacion	Gjendja e lidhjes
192.168.1.100	1030	192.0.2.71	80	E iniciuar
192.168.1.102	1031	10.12.18.74	80	E krijuar
192.168.1.101	1033	10.66.32.122	25	E krijuar
192.168.1.105	1035	10.231.32.12	79	E krijuar

Për shkak se disa protokolle, si për shembull UDP, janë *connectionless* dhe nuk kanë një proces formal për inicializimin, krijimin dhe përfundimin e një lidhjeje komunikimi, gjendja e tyre nuk mund të përcaktohet në shtresën e transportit si në rastin e TCP. Për këto protokolle, shumica e firewall-eve me inspektimin *stateful* mund të gjurmojë vetëm adresat IP burim dhe destinacion dhe portat. Paketat UDP duhet të përputhen me një rresht nga tabela e gjendjeve bazuar në elementët e mësipërm - një përgjigje DNS nga burimet e jashtme do të lejohet të kalojë vetëm nëse firewall-i ka detektuar më përpara një *query DNS* nga një burim i brendshëm. Meqë firewall-i e ka të pamundur të përcaktojë kur një sesion komunikimi ka përfunduar, rreshti hiqet nga tabela e gjendjeve pasi është arritur një vlerë e parakonfiguruar përfundimi. Firewall-et në nivelin e komunikimit mund të njohin DNS mbi UDP që do përfundojë sesionin pasi është marrë përgjigja nga DNS. Në të njëjtën mënyrë mund të funksionojë edhe me protokollin Network Time Protocol (NTP).

2.1.3 Firewall-et e aplikimeve

Një element i ri në inspektimin *stateful* është dhe shtimi i aftësive në analizën *stateful* të protokollit*,* të cilës disa prodhues i referohen si *deep packet inspection.* Analiza *stateful* e protokollit përmirëson standartet e inspektimit *stateful* duke shtuar teknologjinë bazë *intrusion detection.* Kjo bën që një firewall të lejojë ose të mos lejojë aksesin duke u bazuar në mënyrën se si një aplikim ekzekutohet në rrjet. Për shembull, një firewall aplikimi mund të përcaktojë nëse e-maili përmban bashkëlidhur tipe që institucioni nuk i lejon, si një skedar të ekzekutueshëm .exe. Një veçori tjetër është që firewall-i mund t'i bllokojë lidhjet mbi të cilat janë duke u kryer veprime specifike. Kjo veçori gjithashtu mund të përdoret për të lejuar ose mohuar faqet Web të cilat përmbajnë lloje të veçanta të përmbajtjeve siç janë Java ose ActiveX ose ato që kanë certifikata Secure Sockets Layer (SSL) të nëshkruara nga një autoritet çertifikues i veçantë (CA).

Firewall-et e aplikimeve mund të bëjnë të mundur dhe identifikimin e sekuencave të papritura të komandave të tilla si përdorimi i së njëjtës komandë në mënyrë të përsëritur ose përdorimi i një komande që nuk është e paraprirë nga një tjetër komandë nga e cila është varur. Këto komanda të dyshimta shpesh e kanë origjinën nga sulmet "buffer overflow", sulme DoS, programe

keqdashëse, dhe nga forma të tjera sulmesh që kryhen brenda aplikimeve të protokolleve si: Hypertext Transfer Protocol (HTTP).
Një tjetër cilësi është edhe vlefshmëria e komandave individuale hyrëse, gjatësia minimale dhe maksimale e argumentave. Për shembull, argumenti i një *username* me gjatësi 1000 karaktere është dyshues. Firewall-et e aplikimeve implementohen për protokollet HTTP, protokollet e e-mailit (SMTP, Post Office Protocol) dhe Internet Message Access Protocol (IMAP), Voice over IP (VoIP) dhe Extensible Markup Language (XML).

Firewall-et që kanë cilësitë e inspektimit *stateful* dhe aftësitë e analizimit të protokollit *stateful* së bashku, nuk mund të bëjnë më shumë zbulime dhe parandalime të sulmeve krahasuar me sistemet IDPS.

2.1.4 Application-Proxy Gateway

Këto firewall-e përmbajnë një agjent proxy që vepron si një ndërmjetës midis dy host-eve që dëshirojnë të komunikojnë me njëri-tjetrin, dhe nuk lejon kurrë lidhje direkte ndërmjet tyre. Çdo përpjekje e suksesshme lidhjeje aktualisht rezulton në krijimin e dy lidhjeve të ndara – një midis klientit dhe serverit proxy, dhe tjetrës midis serverit proxy dhe destinacionit të vërtetë. Për shkak se host-et e jashtme komunikojnë vetëm me agjent proxy, adresat IP të brendshme nuk janë të dukshme për rrjetin e jashtëm. Agjenti proxy ndërvepron drejtpërdrejt me bashkësinë e rregullavetë firewall-it për të përcaktuar nëse një instancë konkrete e trafikut të rrjetit të lejohet të kalojë përmes firewall-it.

Përveç bashkësisë së rregullave të firewall-it disa agjent proxy kanë kompetenca të kërkojnë autentifikim për çdo përdorues individual rrjeti. Ky autentifikim mund të marrë disa forma, përfshirë ID-në e përdoruesit dhe fjalëkalimin, elementë biometrikë etj.

Njëlloj si aplikimet e firewall-eve, dhe proxy gateway operojnë në shtresën e aplikimit dhe mund të inspektojnë përmbajtjen aktuale të trafikut. Këto gateway gjithashtu mund të kryejnë dhe TCP *handshake* me sistemin burim dhe janë të afta të mbrojnë kundër shfrytëzimit në çdo sekuencë të komunikimit. Për më tepër portat mund të marrin vendime për të lejuar ose mos lejuar trafikun bazuar në header-in e protokollit të aplikimit ose payload-in. Në momentin që *gateway* përcakton se të dhënat duhen lejuar, ato dërgohen drejt hostit destinacion.

Application-proxy gateways ndryshojnë firewall-et e aplikimeve. Së pari, një *application-proxy gateway* mund të ofrojë një nivel më të lartë sigurie për disa aplikime sepse pengon lidhjet direkte ndërmjet dy host-eve dhe inspekton përmbajtjen e trafikut për të identifikuar shkeljet e politikave. Avantazh tjetër i rëndësishëm është që disa *application-proxy gateway* kanë aftësi të dekriptojnë paketa, t' i ekzaminojnë ato dhe t'i rienkriptojnë përpara se t'i dërgojnë ato në hosti-n e destinacionit. Kur zgjidhet lloji i firewall-it që do implementohet, është e rëndësishme të vendoset nëse firewall-i në të vertetë duhet të veprojë si një proxy aplikimi në mënyrë që të përputhet me politikat e veçanta të nevojshme nga institucioni.

Firewall-et me *application-proxy gateway* mund të kenë gjithashtu disavantazhe kur krahasohen me filtrimin e paketave dhe inspektimin *stateful*. Së pari, për shkak të inspektimit të detajuar të paketave, firewall-i harxhon më shumë kohë për të lexuar dhe për të interpretuar çdo paketë. Për shkak të kësaj këto *gateway* nuk janë të përshtatshëm për aplikacionet me bandwidth të lartë ose aplikacionet në kohë reale, por ekzistojnë edhe *application-proxy gateway* të vlerësuara me bandwidth të lartë. Për të reduktuar ngarkesën në firewall, për të siguruar shërbimet që nuk janë sensitive në kohë si e-mail dhe trafiku në web, mund të përdoret proxy server i dedikuar. Një

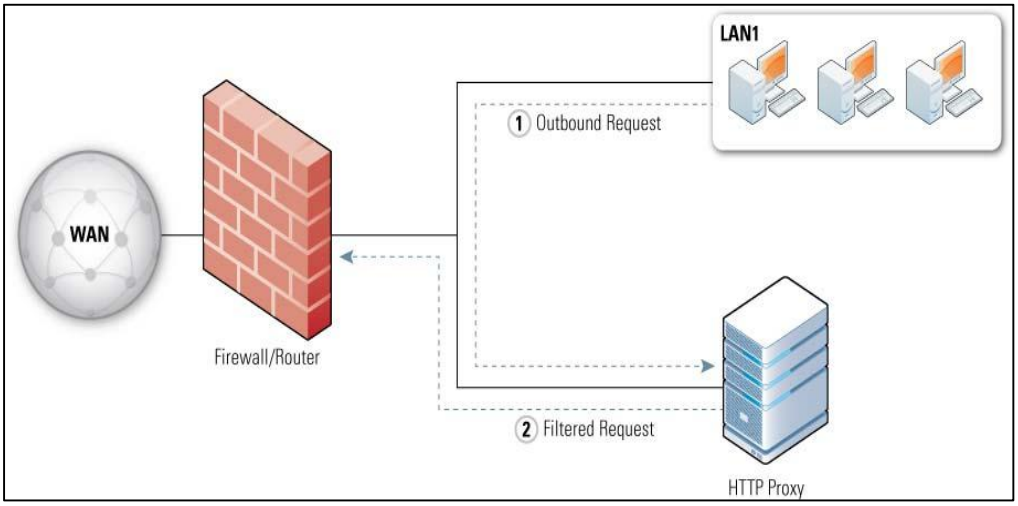
disavantazh tjetër është që *application-proxy gateway* tenton të jetë i limituar në termat e suportit për protokollet dhe aplikacionet e reja të rrjetit. Shumë prodhues të *application-proxy gateways* ofrojnë agjentë të përgjithshëm proxy për të suportuar protokolle ose aplikacione të papërcaktuar të rrjetave. Këta agjentë të përgjithshëm tentojnë të mohojnë shumë nga pikat e forta të arkitekturës së *application-proxy gateway* sepse ata thjesht lejojnë trafikun të kalojë përmes firewall-it.

2.1.5 Serverat Proxy të dedikuar

Serverat proxy të dedikuar dallojnë nga *application-proxy gateways* për arsye se zakonisht kanë aftësi më të limituara për *firewalling*. Shumë servera të dedikuar proxy janë specifikë për aplikacionet, dhe disa performojnë analizë dhe validim të protokolleve si HTTP.Për shkak se këto servera kanë aftësi të limituara *firewalling*, si bllokimi i trafikut bazuar në burimin ose destinacionin e tij, ata implementohen zakonisht në platformat tradicionale të firewall-eve. Zakonisht, një firewall kryesor mund të pranojë trafikun hyrës, të përcaktojë se cili aplikacion është targetuar dhe të drejtojë trafikun tek serveri proxy i duhur (për shembull *email proxy)*. Ky server duhet të kryejë filtrim ose logim në trafik, dhe më pas i përcjell ato në sistemin e brendshëm. Një server proxy mund të pranojë trafikun dalës direkt nga sistemi i brendshëm, ta filtrojë ose ta përshkojë dhe ta kalojë atë në firewall për ta dërguar jashtë. Një shembull tipik është HTTP proxy, i implementuar pas firewall-it – përdoruesit që duan të lidhen me këtë proxy duhet të lidhen nëpërmjet shërbimeve të jashtme web. Serverat proxy të dedikuar janë përdorur në përgjithësi për të ulur ngarkesën e firewall-t dhe të kryejnë filtrimin e specializuar që mund të jetë i vështirë për t'u kryer nga vetë firewall-i.

Në vitet e fundit, përdorimi i serverave proxy për trafikun hyrës është ulur në mënyrë drastike. Kjo ndodh sepse një server proxy për trafikun hyrës duhet të imitojë kapacitetet e serverit real që po mbron, gjë që e bën gati të pamundur kur bëhet fjalë për të ruajtur një server me shumë karakteristika. Përveç kësaj, karakteristikat kryesore që duhet të kenë serverat proxy për trafikun hyrës (log-imi, kontrolli i aksesit) zakonisht janë të ndërtuar në serverat realë. Shumë servera proxy në përdorim janë server proxy për trafikun dalës, dhe zakonisht janë HTTP proxy.

Në figurën më poshtë tregohet një diagramë e thjeshtë e rrjetit që implementon një proxy server të dedikuar HTTP, i cili është vendosur pas një tjetër sistemi firewall-i. Proxy HTTP do të trajtojë lidhjet dalëse tek web serverat e jashtëm dhe filtrimin e përmbajtjeve aktive. Kërkesat nga përdoruesit në fillim shkojnë tek proxy, dhe proxy pastaj i dërgon kërkesat në web server-in e jashtëm. Përgjigja nga ai web server pastaj kthehet tek proxy, i cili e përcjell tek përdoruesi.



2.1.6 Rrjeti privat virtual (VPN)

Pajisjeve firewall ndonjëherë u kërkohet të bëjnë më tepër se thjesht bllokimin e trafikut të padëshiruar. Një kerkesë e zakonshme për këta firewall-e është të enkriptojnë dhe të dekriptojnë trafikun specifik të rrjetit që rrjedh midis rrjetit të mbrojtur dhe atij të jashtëm. Kjo përfshin pothuajse gjithmonë rrjetin privat virtual (VPN), të cilët përdorin protokolle shtesë për të enkriptuar trafikun dhe ofrojnë autentikim të përdoruesit dhe kontroll të integritetit. VPN-të shpesh përdoren për të ofruar një komunikim rrjeti të sigurt nëpër rrjetet e pasigurta. Për shembull, teknologjia VPN është gjerësisht e përdorshme për të zgjeruar rrjetin e mbrojtur në një institucion të madh përmes Internetit, dhe shpesh për të ofruar kontroll *remote* në rrjetin e brendshëm të institucionit nëpërmjet Internetit. Dy zgjedhjet e zakonshme për të siguruar VPN-të janë IPsec dhe SSL/TLS (*Secure Sockets Layer/Transport Layer Security*).

Dy arkitekturat më të zakonshme të rrjetit privat virtual (VPN) janë *gateway-to-gateway* dhe *host-to-gateway*. Arkitekturat *gateway-to-gateway* lidhin faqet *(site*) nëpërmjet përdorimit të portave të rrjetit privat virtual (VPN), rast i ngjashëm me lidhjen e filialeve të një institucioni me zyrën qendrore. Një rrjeti privat virtual (VPN) gateway zakonisht është pjesë e një pajisje tjetër rrjeti siç mund të jetë firewall ose router. Arkitektura e tipit të dytë, *host to gateway,* ofron një lidhje të sigurtë të përdoruesve në rrjet, që zakonisht quhen përdorues në distancë, dhe vendosen jashtë institucionit. Në këtë rast, përdoruesi krijon një lidhje të sigurt me gateway-n e institucionit. Për VPN-të gateway-to-gateway dhe host-to-gateway, funksionalitetet e VPN-së janë shpesh pjesë e vetë firewall-it. Vendosja e saj pas firewall-it kërkon që trafiku i VPN-së të kalojë përmes firewall-it ndërkohë që ndodh enkriptimi, duke parandaluar inspektimin e trafikut nga firewall-i.

I gjithë aksesi në distancë (host-to-gateway) me VPN lejon administratorin e firewall-it që të vendosë se cili nga përdoruesit do ketë akses në burime të caktuara të rrjetit. Ky kontroll aksesi është zakonisht i mundur për t'u realizuar me grupe përdoruesish ose me përdorues individualë. Kjo do të thotë që politikat e VPN-së përcaktojnë se cilët përdorues apo grupe janë të autorizuar për të aksesuar burimet. VPN-të zakonisht punojnë me protokolle autentifikimi si për shembull Remote Authentication Dial In User Service (RADIUS). RADIUS përdor disa tipe kredencialesh

për autentifikim, si për shembull username dhe fjalëkalim, nënshkrim dixhital dhe pajisje hardware (*hardware tokens*). Një tjetër protokoll i përdorur shpesh nga VPN është LDAP (Lightweight Directory Access Protocol), i cili është i përdorshëm veçanërisht për të përcaktuar aksesin për përdorues individualë dhe grupe.

Për të aktivizuar funksionalitetin VPN në një firewall kërkohen burime shtesë që varen nga sasia e trafikut që rrjedh nëpër VPN dhe llojin e enkriptimit që është duke u përdorur. Për disa mjedise, trafiku shtesë lidhur me VPN mund të kërkojë planifikime shtesë të kapaciteteve dhe burimeve. Planifikimi është gjithashtu i nevojshëm për të përcaktuar llojin e VPN (gateway-to-gateway dhe /ose host-to-gateway) që duhet të përfshihet në firewall.

2.1.7 Kontrolli i aksesit në rrjet (Network Access Control)

Një tjetër kërkesë e firewall-eve në kufirin e rrjetit është të realizojë kontrolle përdoruesish për lidhjet hyrëse nga përdorues në distancë (remote users) dhe lejojë ose mos lejojë aksesin bazuar në këto kontrolle. Ky kontroll, i cili zakonisht quhet network access control (NAC) ose network access protection (NAP), lejon aksesin bazuar në kredencialet e përdoruesve dhe rezultatet e kryera nga kontrolli i realizuar në kompjuterat e përdorur. Ky kontroll zakonisht konsiston në pajtueshmërinë e elementeve të mëposhtëm me politikat e institucionit:

- Përditësimet më të fundit kundër malware-ve dhe software-t e firewall-it
- Rregullat e konfigurimit për antimalware-t dhe software-t e firewall-it
- Koha që ka kaluar nga skanimi i fundit për malware
- Niveli i patch-ve për sistemin e operimit dhe aplikacionet e zgjedhura
- Konfigurimi i sigurisë për sistemin e operimit dhe aplikacionet e zgjedhura

Nëse kredencialet e përdoruesve janë të pranueshme, por vetë pajisja nuk e kalon me sukses kontrollin, përdoruesi dhe pajisja mund të marrin akses të limituar në rrjetin e brendshëm.

2.1.8 Menaxhimi i unifikuar i kërcënimeve (UTM – Unified Threat Management)

Shumë firewall-e kombinojnë karakteristika të shumta në një sistem të vetëm, ideja është se kjo është më e lehtë për të ngritur dhe për të mirëmbajtur politikën në një sistem të vetëm sesa në shumë sisteme që janë të vendosur në të njëjtin vend në rrjet. Një sistem UTM zakonisht ka një firewall, funksionalitet pë detektim malware-sh dhe fshirjen e tyre, për detektimin dhe bllokimin e programeve të rrezikshme etj. Ka disa avantazhe dhe disavantazhe për shkrirjen e funksioneve në një sistem të vetëm. Për shembull, implementimi i një UTM redukton kompleksitetin duke e bërë një sistem të vetëm përgjegjës për shumë objektiva, por gjithashtu kërkon që UTM të ketë të gjitha cilësitë e duhura për të arritur secilin prej objektivave. Një tjetër aspekt lidhet me performancën: një sistem i vetëm që menaxhon disa punë duhet të ketë burime të mjaftueshme si shpejtësinë e CPU-së dhe memorjen për çdo punë që realizon.

2.1.9 Firewall-et e aplikimeve web

Protokollet HTTP të përdorur në web server janë shfrytëzuar nga sulmuesit në shumë mënyra, si vendosja e një programi me qëllim të keq në kompjuterin e dikujt duke naviguar në web ose mashtrimin e një personi në zbulimin e informacionit privat të cilin ata nuk mund ta kenë ndryshuar. Shumë nga këto shfrytëzime mund të detektohen nga aplikacione firewall-i të specializuara të quajtura firewalle aplikimi web që qëndrojnë përpara web serverit.

Firewall-et e aplikimeve web janë relativisht teknologji të reja, krahasuar me teknologji të tjera firewall-esh dhe llojet e kërcënimeve që ata mund të zvogëlojnë janë ende duke ndryshuar në mënyrë të shpeshtë. Për shkak se ata janë të vendosur në hyrje të web serverit për të parandaluar sulme në të, janë konsideruar të ndryshëm nga firewall-et tradicionalë.

2.1.10 Firewall -et për Infrastrukturat Virtuale

Shumë zgjidhje virtualizimi lejojnë më shumë se një sistem operimi të ekzekutohet njëkohësisht në një kompjuter të vetëm, ku secili sillet sikur të ishte një kompjuter i vërtetë. Kjo gjë ka filluar të përdoret shpesh kohët e fundit sepse mundëson përdorim eficent të burimeve hardware. Shumë nga këta tipe virtualizimesh përfshijnë virtualizim rrjeti, i cili lejon sistemet e shumta të operimit të komunikojnë sikur janë në një rrjet Ethernet të zakonshëm, edhe pse nuk ka asnjë pajisje rrjeti.

Aktiviteti i rrjetit që kalon direkt në sistemin operativ të virtualizuar brenda host-it nuk mund të monitorohet nga një firewall i jashtëm. Megjithatë, shumë sisteme virtualizimi shpesh e kanë të para konfiguruar firewall-in ose lejojnë palë të treta software-sh që të shtohen në formë plug in-esh. Përdorimi i firewall-eve për monitorimin e rrjeteve virtuale është relativisht një fushë e re e teknologjive firewall, dhe kjo ka gjasa të ndryshojë në mënyrë të konsiderueshme duke parë përdorimin në rritje të virtualizimit.

2.2 Kufizimet e Inspektimit të Firewall-it

Firewall-et mund të punojnë me efikasitet vetëm në atë trafik të cilin mund ta monitorojnë. Pavarësisht teknologjisë së zgjedhur të firewall-it, një firewall që nuk e kupton trafikun që rrjedh përmes tij nuk do ta trajtojë si duhet trafikun. Për shembull, të lejojë trafikun që duhet të ishte bllokuar. Shumë protokolle rrjeti përdorin kriptografinë për të fshehur të dhënat e trafikut. Firewall-et gjithashtu nuk mund të lexojnë të dhënat e aplikimit që janë të enkriptuara, si e-mailet që enkriptohen duke përdorur S/MIME ose protokolle OpenPGP ose skedarë që janë enkriptuar manualisht. Psh. IPv6 mund të “tunneled” në IPv4 në shumë mënyra të ndryshme. Përmbajtja mund të jetë ende e pa enkriptuar por nëse firewall-i nuk kupton pjesën e mekanizmit të përdorur për “tunneling”, trafiku nuk mund të interpretohet.

Në të gjitha këto raste, rregullat e firewall-it do përcaktojnë se çfarë duhet bërë me trafikun e enkriptuar ose me trafikun që nuk është i enkriptuar. Të gjithë institucionet duhet të kenë politika rreth trajtimit të trafikut në të tilla raste, si lejimin ose bllokimin e trafikut të enkriptuar që nuk është autorizuar per të qënë i tillë.

2.3 Përmbledhje e Rregullave

Pikat e mëposhtme përmbledhin rekomandimet kryesore nga ky kapitull të detyrueshme për zbatim:

- Përdorimi i NAT duhet të konsiderohet një formë rout-imi, jo një tip firewall-i.

- Institucionet duhet të lejojnë vetëm atë trafik hyrës që përdor adresat IP burim që janë në përdorim nga institucioni.

- Kontrolli i pajtueshmërisë është i dobishëm në një firewall vetëm atëherë kur ai mund të bllokojë komunikimet të cilat mund të jenë të dëmshme në mbrojtjet e sistemeve.

- Kur zgjedhim tipin e firewall-it që do përdoret, është e rëndësishme të vendoset nëse ai duhet të sillet si një proxy për aplikacionet.

3. Firewall-et dhe Arkitekturat e Rrjetave

Firewall-et janë përdorur për të ndarë rrjetat me kërkesa të ndryshme sigurie, të tillë si Interneti dhe rrjeti i brendshëm që mban server me të dhëna të ndjeshme. Institucionet duhet të përdorin firewall aty ku rrjeti dhe sistemi i brendshëm ndeshen me rrjetin dhe sistemet e jashtme, dhe atje ku kërkesat e sigurisë ndryshojnë nga rrjeti i brendshëm. Ky seksion ka për qëllim që të ndihmojë institucionet të përcaktojnë se ku duhet vendosur një firewall. Dhe se ku duhen vendosur sistemet e tjera dhe rrjetet në lidhje me firewall-in.

Meqënëse një nga funksionet kryesore të një firewall-i është të parandalojë hyrjen e trafikut të padëshiruar në firewall-in e rrjetit, firewall-i duhet të jetë vendosur në kufijtë e rrjetit logjik. Kjo normalisht do të thotë se firewall-et janë pozicionuar ose si një nyje ku rrjeti ndahet nëpër path-e të shumta, ose në linjë të vetme path-i. Në rrjetat e routuara firewall-i përgjithësisht qëndron pikërisht në vendin pak përpara se trafiku të hyjë në router dhe ndonjëherë bashkëshoqërohet me router-in. Është shumë e rrallë vendosja e firewall-it sipas mënyrës multi-path pas router-it sepse pajisja firewall do ketë nevojë të shohë çdo path që ekziston në situatë tipike. Shumica e pajisjeve firewall hardware kanë aftësi routimi, dhe në switch-e rrjeti një firewall është shpesh pjesë e vet switch-it për t'i mundësuar atij mbrojtjen sa më shumë të jetë e mundur.

Prodhuesit e firewall-eve shpesh variojnë në terminologjinë e tyre në rrjedhë logjike të trafikut të firewall-it. Një firewall merr trafikun që nuk ka qënë i kontrolluar, e kontrollon atë sipas politikave të firewall-it dhe pastaj trafiku kalon në përputhje me rrethanat (për shembull, lejon trafikun të kalojë, e bllokon atë, e kalon pasi ka bërë disa modifikime). Për shkak se i gjithë trafiku në rrjet ka një drejtim, politikat janë bazuar në drejtimin që lëviz trafiku.Për qëllimet e kësaj rregulloreje, trafiku që nuk është kontrolluar ende vjen nga "ana e pambrojtur" e firewall-it dhe po lëviz drejt "anës së mbrojtur." Disa firewall-e kontrollojnë trafikun në të dy drejtimet.

Kapitulli 2 liston shumë tipe të ndryshme teknologjish firewall –i. Firewall-et e rrjetit janë pothuajse gjithmonë pajisje hardware me ndërfaqe rrjeti të shumfishtë, host-based.

3.1 Modele Rrjeti me Firewall-e

Figura 3.1 jep një model tipik rrjeti me pajisje hardware firewall që vepron si router. Ana e pambrojtur e firewall-it lidhet me një path të vetëm të quajtur 'WAN' dhe ana e mbrojtur lidhet me tre path-e të quajturr 'LAN1' (local area network), 'LAN2' dhe 'LAN3'. Firewall-i vepron si router për trafikun midis path-it wide area network (WAN) dhe path-eve LAN. Në figurë një nga path-et LAN ka gjithashtu një router, disa institucione preferojnë të përdorin shtresa të shumëfishta të router-it për shkak të politikave të rout-imit të trashëguara brenda rrjetit.

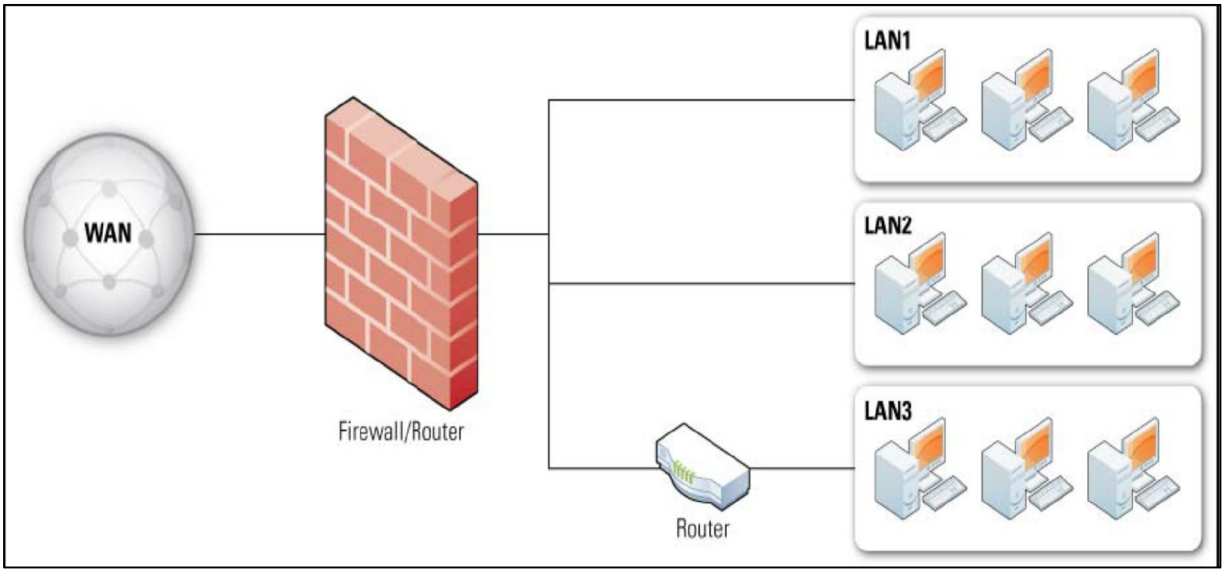


Figura 3.1 Rrjet i thjeshtë i routuar me pajisje firewall-i

Shumë pajisje firewall-i kanë një tipar të quajtur DMZ, akronim që lidhet me zonat e demilitarizuara. Ndërkohë që nuk ekziston asnjë përkufizim i vetëm teknik për DMZ-të e firewall-it, ata përgjithësisht janë ndërfaqe routimi, që janë të ngjashme me ndërfaqet e gjetura në anën e mbrojtur të firewall-it. Ndryshimi kryesor është që trafiku që lëviz midis DMZ-së dhe ndërfaqeve të tjera në anën e mbrojtur të firewall-it vazhdon kalon përmes firewall-it dhe mund të ketë të aplikuar politikat e mbrojtjes së firewall-it. DMZ-të janë ndonjëherë të nevojshme për ato institucione, trafiku i të cilave duhet të anashkalojë disa nga politikat e firewall-eve (për shembull, për shkak se DMZ janë mjaft të ngurtësuara), por trafiku që vjen nga ana e sistemeve të tjera duhet të kalojë patjetër përmes firewall-it.Vendosja e serverave, të tillë si web dhe mail server, në DMZ është e zakonshme. Një shembull i tillë është treguar në figurën 3.2, një model i thjeshtë rrjeti me firewall me DMZ. Trafiku nga Interneti shkon nëpër firewall dhe është i routuar tek sistemi i anës së mbrojtur të firewall-it ose tek sistemi i DMZ-së. Trafiku midis sistemit të DMZ-së dhe sistemit në rrjetin e mbrojtur shkon përmes firewall-it dhe mund të ketë të aplikuar politikat e firewall-it.

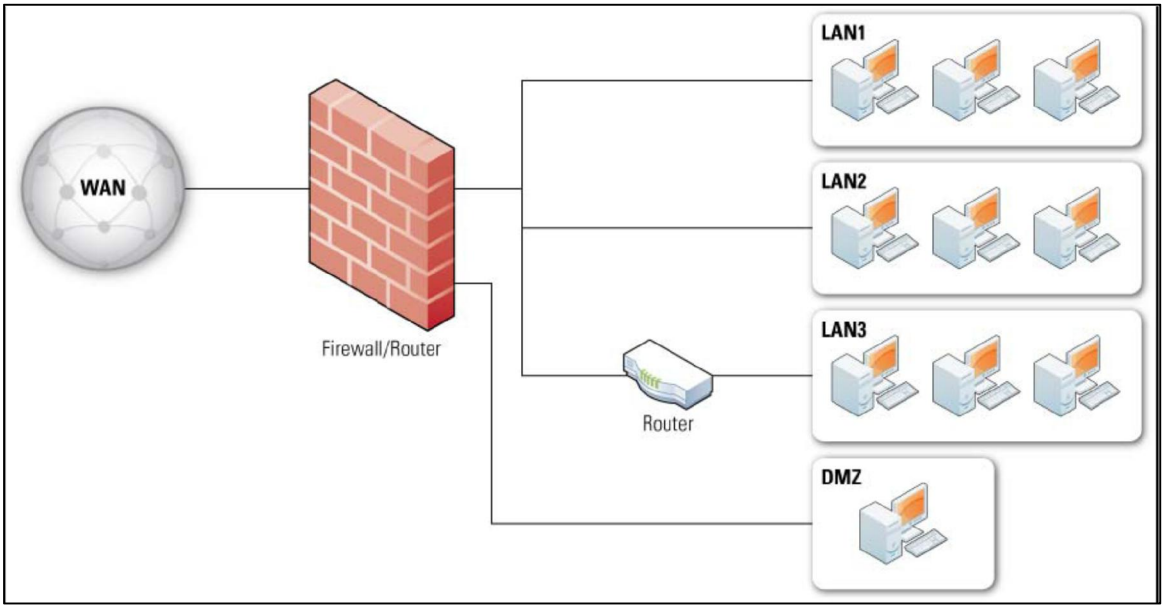


Figura 3.2 Firewall-i me DMZ

Shumë arkitektura rrjetash janë hiearkike, që do të thotë që një path i vetëm nga një rrjeti i jashtëm ndahet në shumë path-e në rrjetin e brendshëm dhe përgjithësisht është më efiçente vendosja e një firewall-i në vendin ku ndahet path-i. Megjithatë mund të ketë arsye për të pasur një firewall shtesë në brendësi të rrjetit, të tillë që të mbrojë një bashkësi kompjuterash nga një tjetër. Nëse arkitektura e rrjetit është jo hiearkike, të njëjtat politika firewall-i mund të jenë përdorur në të gjitha hyrjet e rrjetit. Në shumë institucione është menduar të jetë vetëm një hyrje në rrjet, por hyrjet e tjera janë ngritur në një ad-hoc bazik shpesh në mënyra të cilat nuk janë lejuar nga politikat e përgjithshme. Në këtë situatë nëse një firewall i konfiguruar siç duhet nuk është vendosur në çdo pikë hyrje, trafikut me qëllim të keq (*malicious traffic)* që normalisht do të jetë i bllokuar nga hyrje kryesore mund të hyjë në rrjet me mënyra të tjera.

Diagramat në figurat 3.1 dhe 3.2 tregojnë secila një firewall të thjeshtë; megjithatë, shumë implementime përdorin firewall-e të shumtë. Disa prodhues shesin firewall-e me disponueshmëri të lartë (*high-availability HA*), të cilët lejojnë një firewall të marrë përsipër një tjetër edhe nëse firewall-i i parë dështon ose mbahet offline për qëllime mirëmbajtjeje. Firewall-et me disponueshmëri të lartë janë vendosur në çifte në të njëjtin vend në topologjin e rrjetit në mënyrë që ata të dy të kenë të njëjtat lidhje të jashtme dhe të brendshme. Ndërsa firewall-et me disponueshmëri të lartë mund të rrisin besueshmërinë, ata gjithashtu mund të sjellin disa probleme, të tilla si nevoja për të kombinuar log-et mes firewall-eve çift dhe konfuzione të mundshme të administratorëve kur konfigurojnë firewall-et. Funksionalitetet e firewall-eve me disponueshmëri të lartë mund të ofrohen nga teknika të ndryshme të prodhuesve specifikë.

3.2 Firewall-et që veprojnë si Përkthyes Adresash Rrjeti

Shumë firewall-e mund të kryejnë përkthim të adresave të rrjetit (NAT- *Network Address Translator*). NAT nuk është pjesë e funksionalitetit të sigurisë së një firewall-i. Përfitimi i sigurisë së NAT-it është që parandalimi i kontaktit të host-it jashtë firewall-it me një host prapa

NAT-it mund të arrihet po aq lehtë nga një firewall pa ndihmën e protokolleve që nuk punojnë mirë mbrapa NAT. Megjithatë aktivizimi i NAT në një firewall është përgjithësisht më i thjeshtë se konfigurimi i duhur i politikave të firewall-it për të pasur të njëjtën mbrojtje, kështu që shumica mendojnë se NAT është tipari kryesor i sigurisë.

Përgjithësisht, një NAT vepron si një router që ka një rrjet me adresa private në brendësi dhe një adresë të vetme publike në pjesën e jashtme. Mënyra se si një NAT kryen këtë përkthim adresash shumë-në-një *(many-to-one)* varion nga implementimi, por pothuajse gjithmonë përfshin elementët e mëposhtëm:

- Host-et në brendësi të rrjetit inicojnë lidhje me rrjetin e jashtëm duke bërë që NAT të përcaktojë porta burimi për lidhjen në porta burimi të ndryshme nga ato që kontrollohen nga NAT. NAT përdor numrin e portës së burimit për të përcaktuar lidhjet nga jashtë në host-et në brendësi.
- Host-et jashtë rrjetit nuk mund të inicializojnë kontakte me host-et brenda rrjetit. Në disa firewall-e, NAT mund të jetë konfiguruar për të përcaktuar një portë destinacioni të veçantë në NAT tek një host i veçantë në brendësi të NAT, për shembull të gjitha kërkesat HTTP të cilat shkojnë tek NAT mund të jenë drejtuar tek një host i vetëm në anën e mbrojtur të firewall-it. Kjo cilësi shpesh quhet *pinholing.*

Edhe pse NAT-et nuk janë në vetvete karakteristika të sigurisë të një firewall-i, ata ndërveprojnë me politikat e sigurisë së firewall-it. Për shembull, ekzistojnë politika që kërkojnë që të gjithë serverat HTTP të aksesueshëm nga jashtë të jenë në DMZ, dhe duhet të parandalojë NAT nga pinholing i TCP në portën 80. Një tjetër shembull që NAT ndërvepron me politikën e sigurisë është aftësia për të identifikuar burimin e trafikut në log-et e një firewall-i. Nëse një NAT është në përdorim, duhet të raportojë adresat private në log-e në vend të adresave të përkthyera publike, përndryshe log-et gabimisht do të identifikojnë shumë host-e nga një adresë e vetme publike.

3.3 Arkitektura me shumë shtresa e firewall-it

Nuk ka asnjë kufizim për vendin se ku do vendoset firewall-i në një rrjet. Ndërsa firewall-et duhet të jenë në kufijtë e një rrjeti logjik, krijimin e një "kufiri të brendshëm" dhe "të jashtëm" në të dyja anët e firewall -t, një administrator rrjeti mund të dëshirojë që të ketë kufij shtesë brenda rrjetit dhe të vendosë firewall-e shtesë në kufij të tillë. Përdorimi i shtresave të shumta të firewall-ve është mjaft i zakonshëm për të siguruar më shumë mbrojtje.

Një situatë tipike që kërkon shtresa të shumta të rrjetit të firewall-eve është prezenca e përdoruesve të brendshëm me nivele të ndryshme të besimit. Për shembull, një institucion mund të dojë të mbrojë databazën e kontabilitetit nga të qenurit e aksesueshme nga përdorues të cilët nuk janë pjesë e Departamentit të Kontabilitetit. Kjo mund të realizohet duke vendosur një firewall në kufirine rrjetit (për të parandaluar aksesin e përgjithshëm në rrjet nga Interneti) dhe një tjetër në kufirin e rrjetit të brendshëm që përcakton kufirin e Departamentit të Kontabilitetit. Firewall-i i brendshëm mund të bllokojë aksesin në serverin e bazës së të dhënave nga jashtë

rrjetit, ndërsa lejon akses të kufizuar të burimeve të tjera në rrjet. Një përdorim tipik për firewall-et brenda rrjetit me firewall-et anësorë përfshin vizitorët të cilët kanë nevojë për akses në Internet.

Vendosja e një firewall-i brenda një rrjeti që ka një tjetër firewall në kufirin e tij, kërkon planifikim të mirë dhe koordinim të politikave për të parandaluar gabimet e paqëllimshe në siguri. Një trajtim më i mirë është dublikimi i politikave të firewall-it të jashtëm, që janë gjithashtu të rëndësishme për firewall-et e brendshëm. Kjo mund të jetë e vështirë nëse firewall-et nuk janë në gjendje të koordinojnë politikat e tyre automatikisht e cila është veçanërisht e mundshme kur firewall-et u përkasin prodhuesve të ndryshëm.

Një problem tjetër i përbashkët me përdorimin e shumë shtresave të rrjetit të firewalle-ve është vështirësia në rritje që paraqitet në gjetjen e problemeve të firewall-it. Nëse një firewall qëndron midis një përdoruesi dhe një serveri, dhe përdoruesi nuk mund të lidhet dot me serverin, është e lehtë të kontrollosh log-et e firewall-it për të parë nëse lidhja është e lejuar. Por nëse janë përfshirë shumë firewall-e, problemi fillon bëhet më i vështirë sepse një administrator duhet të lokalizojë gjithë zinxhirin e firewall-eve dhe të kontrollojë log-et e tyre për të gjetur origjinën e problemit. Prania e shtresave të shumta të *application-proxy gateway* është veçanërisht shqetësuese, sepse çdo portë mund të ndryshojë një mesazh, që e bën edhe më të vështirë gjurmimin.

3.4 Përmbledhje e Rregullave

Pikat e mëposhtme përmbledhin rekomandimet kryesore nga ky kapitull:

- Firewall-i duhet të përshtatet me modelin e një rrjeti aktual. Megjithatë, një institucion mund të ndryshojë arkitekturën e tij të rrjetit në të njëjtën kohë që ai vendos një firewall si pjesë e përmirësimit të përgjithshëm të sigurisë.

- Arkitektura të caktuara të përbashkëta të rrjetit çojnë në zgjedhje të ndryshme të vendosjes së një firewall-i, kështu që një institucion duhet të vlerësojë se cila arkitekturë punon më mirë për qëllimet e tij të sigurisë.

- Nëse një firewall anësor ka një DMZ, duhet përcaktuar se cilat nga shërbimet duhet të realizohen nga DMZ dhe cilat duhet të qëndrojnë brenda rrjetit.

- Mos u mbështesni në NAT për të siguruar përfitimet e firewall-it.

- Në disa mjedise, vendosja e firewall-ve njëri pas tjetrit mund të rritë sigurinë e dëshiruar, por në përgjithësi shtresa të shumta të tilla firewall-esh mund të rritin kompleksitetin.

4. Politikat e firewall-eve

Një politikë firewall-i tregon se si firewall-et duhet ta trajtojnë trafikun e rrjetit për adresa IP specifike dhe rangun e adresave, protokollet, aplikimet dhe tipet e përmbajtjes bazuar në politikat e informacionit të institucionit. Përpara se politika e firewall-it të krijohet, duhet të kryhet analiza e riskut për të krijuarn jë listë të trafikut të nevojshëm për institucionin dhe kategorizimin se si ata të jenë të sigurtë – duke përfshirë ato tipe trafiku që kalojnë nëpër firewall-e dhe në çfarë rrethanash kalojnë. Kjo analizë risku duhet bazuar në vlerësimin e kërcënimeve dhe dobësive: kundërmasat në mënyrë që të reduktohen dobësitë; dhe impakti nëse sistemi ose të dhënat janë të kompromentuara. Politikat e firewall-it mund të jenë të dokumentuara në planin e sigurisë së sistemit, të mirëmbajtura dhe të përditësuara ndërkohë që rriten sulmet dhe dobësitë. Politika duhet të përfshijë udhëzime specifike për mënyrën e adresimit të ndryshimeve në bashkësinë e rregullave.

Përgjithësisht, firewall-et mund të bllokojnë gjithë trafikun hyrës dhe atë dalës që nuk lejohet nga politika e firewall-it – trafik që nuk është i nevojshëm për institucionin. Kjo praktikë njihet si bllokim i zgjedhur/paracaktuar (*default*), redukton rrezikun e sulmeve, gjithashtu redukton trafikun në rrjetet e institucionit. Për shkak të natyrës dinamike të host-eve, rrjeteve, protokolleve dhe aplikacioneve, bllokim I zgjedhur/paracaktuar (*default*) është trajtim më i sigurtë se lejimi i gjithë trafikut që nuk është ndaluar në mënyrë eksplicite.

Ky kapitull ofron detaje se çfarë tipesh trafiku duhen bllokuar.

4.1 Politikat e bazuara në Adresa IP dhe Protokolle

Politikat e firewall-eve duhet të lejojnë vetëm protokollet e IP –ve të nevojshme. Shembuj të zakonshme të protokolleve IP të përdorura janë: ICMP, TCP dhe UDP. Protokolle IP të tjera, si komponente IPsec, *ESP (Encapsulating Security Payload)* dhe *AH (Authentication Header)* dhe protokollet e routimit duhet të kalojnë përmes firewall-it. Këto protokolle të nevojshme duhet të jenë kufizuar kur është e mundur në host-et specifike dhe rrjetet brenda institucionit me nevojën e përdorimit të tyre. Duke lejuar vetëm protokollet e nevojshme, të gjithë protokollet IP të panevojshëm bllokohen automatikisht.

4.1.1 Adresat IP dhe Karakteristika të tjera të IP-ve

Politikat e firewall-it duhet të lejojnë vetëm përdorimin e burimeve dhe adresave IP destinacion të përshtatshme. Rekomandimet specifike për adresat IP përfshijnë:

- Trafiku me burime ose adresa destinacioni të pavlefshme duhet bllokuar gjithmonë, pavarësisht nga vendodhja e firewall-it.
- Trafiku me një adresë burim të pavlefshme për trafikun hyrës ose adresë destinacion të pavlefshme për trafikun dalës duhet të bllokohet në perimetrin e rrjetit. Ky trafik shpesh shkaktohet nga një software dashakeq, imitim i adresave (*spoofing*), sulmet DoS, ose nga pajisje të pakonfiguruara mirë.
- Trafiku me adresë destinacioni private për trafikun hyrës ose adresë burimi për trafikun dalës duhet të bllokohet në perimetrin e rrjetit. Pajisjet e perimetrit të rrjetit mund të kryejnë shërbime të përkthimit të adresave për të lejuar host-et e brendshme me adresat private për të komunikuar nëpërmjet perimetrit, por adresat private nuk duhet të kalojnë nëpërmjet perimetrit të rrjetit.
- Trafiku dalës me adresa burimi të pavlefshme duhet të bllokohet. Ky shpesh quhet dhe filtrim dalës. Sistemet që janë kompromentuar nga sulmuesit mund të përdoren për të sulmuar

sistemet e tjera në Internet; duke përdorur adresa burim të pavlefshme ndalimi i këtyre sulmeve bëhet shumë I vështirë për t'u ndaluar. Bllokimi i këtij lloj trafiku në një firewall institucioni ndihmon në reduktimin e efikasitetit të këtyre sulmeve.

- Trafiku hyrës me adresë destinacioni në firewall, në vetvete duhet bllokuar, vetëm nëse firewall-i ofron shërbime për trafikun hyrës që kërkon lidhje të drejpërdrejtë – për shembull nëse firewall-i është duke vepruar si një proxy aplikimi.
- Trafiku që përmban informacione rout-imi për IP e burimeve, i cili lejon sistemin të specifikojë router-at që paketat do përdorin ndërsa shkojnë nga burimi në destinacion. Kjo mund të lejojë në mënyre potenciale një sulmues për të ndërtuar një paketë që anashkalon kontrollet e sigurisë së rrjetit. Rout-imi i IP-së së burimit është përdorur shumë rrallë në rrjetet moderne.
- Trafiku nga jashtë rrjetit përmban adresa transmetimi që janë të drejtuara për brenda rrjetit. Çdo sistem që i përgjigjet transmetimit të drejtuar, do t'i dërgojë përgjigjen e tij sistemit të specifikuar nga burimi, në vend të sistemit burim. Këto paketa mund të jenë përdorur për të shkaktuar 'stuhi' të mëdha të trafikut të rrjetit nëpërmjet sulmeve DoS. Transmetimi normal i adresave, si dhe adresat e përdorura për *IP multicast*, mund ose nuk mund të jenë të përshtatshme për bllokimin në firewall-in e institucionit.

Firewall-et në perimetrin e rrjetit duhet të bllokojnë gjithë trafikun hyrës në rrjete dhe host-e që duhet të jenë të pa aksesueshëm nga rrjeti i jashtëm. Këto firewall-e gjithashtu duhet të bllokojnë gjithë trafikun dalës nga rrjeti i institucionit dhe host-et që nuk duhet të jenë të lejuara të aksesojnë rrjetin e jashtëm. Vendimi se cila nga adresat duhet të bllokohet është shpesh një nga aspektet që kërkon më shumë kohë për zhvillimin e politikave të IP-ve të firewall-it. Ky aspekt është gjithashtu një nga më të gabueshmit, sepse adresa IP e lidhur me një entitet të padëshiruar shpesh ndryshon me kalimin e kohës.

4.1.2 IPv6

IPv6 është versioni i ri që po implementohet çdo ditë e më tepër. Edhe pse formati i brendshëm i gjatësisë së adresës IPv6 ndryshon nga IPv4, shumë cilësi të tjera mbeten të ngjashme. Për cilësitë e ngjashme mes tyre, firewallet duhet të punojnë njësoj. Për shembull, bllokimi i gjithë trafikut hyrës ose dalës që nuk lejohet nga politika e firewall-it, do të realizohet pavarësisht versionit të adresave IPv4 apo IPv6.

Kështu, disa firewalle nuk e trajtojnë fare trafikun IPv6; të tjerë e trajtojnë por kanë limitime për filtrimin e trafikut; e ndërsa të tjerë mund ta filtrojnë në mënyrë të ngjashme si trafikun e IPv4. Të gjithë institucionet që vendosin të lejojnë ose jo trafikun IPv6 në rrjetin e brendshëm duhet të implementojnë një firewall që është në gjendje ta filtrojë trafikun. Këta firewall-e duhet të kenë cilësitë e mëposhtme:

- Firewall-i duhet të jetë i aftë të përdorë adresat IPv6 në të gjithë rregullat e filtrimit që përdorin adresat IPv4.
- Ndërfaqja e administrimit duhet të lejojë administratorin të klonojë rregullat e IPv4 për IPv6.

4.1.3 TCP (Transmission Control Protocol) dhe UDP (User Datagram Protocol)

Protokollet e aplikimit mund të përdorin TCP (Transmission Control Protocol), UDP (User Datagram Protocol) ose të dyja, varet nga konstrukti i protokollit. Një server aplikimi zakonisht dëgjon një ose disa porta të fiksuara TCP ose UDP. Disa aplikacione përdorin një portë të vetme, por shumica e aplikacioneve përdorin shumë porta. Për shembull, megjithëse SMTP përdor portën TCP 25 për të dërguar e-mail, ai përdor portën TCP 587 për marrjen e e-mailit. FTP (File Transfer Protocol) përdor të paktën dy porta, një nga të cilat mund të jetë e paparashikueshme, dhe ndërsa shumica e web serverave përdorim vetëm portën TCP 80, është e zakonshme që të ketë edhe faqe web që përdorin porta të tjera të tilla si portën TCP 8080. Disa aplikacione përdorin TCP dhe UDP së bashku; për shembull *DNS lookup* mund të ndodhë në portën UDP 53 ose në portën TCP 53.

Si me aspektet e tjera të rregullave të firewall-it, politikat e bllokimit të zgjedhur/paracaktuar (deny by default) duhet të jenë përdorur për trafikun hyrës TCP dhe UDP. Politikat më pak të rrepta janë përdorur përgjithësisht për trafikun dalës TCP dhe UDP, sepse shumica e institucioneve lejojnë përdoruesit e tyre të aksesojnë një diapazion të gjerë të aplikacioneve të jashtme të lokalizura në miliona host-e të jashtme.

Përveç lejimit dhe bllokimit të trafikut UDP dhe TCP, shumë firewall-e janë gjithashtu të aftë të raportojnë ose të bllokojnë trafikun UDP dhe TCP të keqformuar dhe drejtuar për në firewall ose tek host-et që janë të mbrojtura nga firewall-i. Ky trafik është përdorur shpesh për të skanuar host-et, dhe ka mundësi të jetë përdorur nga disa tipe të caktuar sulmesh. Firewall-i mund të ndihmojë për bllokimin e aktiviteteve të tilla – ose tek e fundit të raportojë kur ndodhin aktivitetet.

4.1.4 ICMP (Internet Control Message Protocol) Protokoll bazë Interneti i përdorur kryesisht për shkëmbimin e mesazheve të gabimit

Sulmuesit mund të përdorin lloje të ndryshme ICMP (Internet Control Message Protocol) dhe kode për të kryer zbulime ose për të manipuluar rrjedhën e trafikut. Gjithsesi ICMP nevojitet për shumë gjëra të dobishme, për të marrë një performancë të arsyeshme në Internet. Disa politika firewall-i bllokojnë të gjithë trafikun ICMP, por kjo shpesh shfaq probleme me diagnostikimin dhe perfomancën. Politika të tjera të zakonshme lejojnë gjithë trafikun dalës ICMP, por limitojnë atë hyrës për këto tipe.

Për të parandaluar aktivitetet me qëllim të keq, firewall-et në perimetrin e rrjetit duhet të mohojnë gjithë trafikun ICMP hyrës dhe dalës përveç atyre tipeve dhe kodeve që specifikisht janë lejuar nga institucioni. Për ICMP në IPv4, 3 mesazhet e tipit ICMP duhet të mos jenë të filtruara sepse përdoren për diagnostikime të rëndësishme rrjeti. Komanda *ping* (ICMP kodi 8) është një diagnostikim rrjeti i rëndësishëm, por ping-et hyrëse janë shpesh të bllokuara nga politikat e institucionit për të parandaluar sulmuesit të mësojnë më shumë për topologjinë e rrjetit të institucionit. Për ICMP në IPv6 duhet të jenë të lejuara shumë tipe mesazhesh në rrethana specifike për të mundësuar tipare të ndryshme IPv6.

ICMP është përdorur shpesh nga protokollet e nivelit të ulët të rrjetit për të rritur shpejtësinë dhe besueshmërinë e rrjetave. Prandaj, ICMP në rrjetin e një institucioni përgjithësisht nuk duhet të

jetë i bllokuar nga firewall-et që nuk janë në perimetrin e rrjetit, përveç kur nevojat e sigurisë peshojnë më shumë se nevojat operacionale të rrjetit. Në mënyrë të ngjashme, nëse një organizatë ka më shumë se një rrjet, ICMP që vjen apo shkon në rrjetet e tjera brenda institucionit nuk duhet të jetë e bllokuar.

4.1.5 Protokollet IPsec

Një institucion ka nevojë të ketë një politikë për të lejuar ose jo VPN të IPsec që nisin ose mbarojnë brenda perimetrit të rrjetit. Protokollet ESP dhe AH përdoren për VPN e IPsec, dhe firewall-et që bllokojnë këto protokolle nuk do të lejojnë VPN e IPsec të kalojë. Ndërkohë që bllokohet ESP, mund të pengojë përdorimin e enkriptimit për të mbrojtur të dhënat e ndjeshme, dhe gjithashtu mund të detyrojë përdoruesit të cilët normalisht do të enkriptojnë të dhënat e tyre me ESP për të lejuar atë të inspektohet.

Institucionet që lejojnë VPN e IPsec duhet të bllokojnë ESP dhe AH përveç atyre drejt dhe nga adresat e rrjetit të brendshëm – këto adresa i përkasin portave të IPsec që janë lejuar për të qenë pikat fundore të VPN. Duke zbatuar këto politika do t'i kërkohet punonjësve që brenda një institucioni të njihen me politikën e duhur për të hapur ESP dhe /ose për të aksesuar AH tek routerat e IPsec. Kjo gjithashtu do të zvogëlojë sasinë e trafikut të koduar nga brenda rrjetit dhe që nuk mund të shqyrtohet nga kontrollet e sigurisë e rrjetit.

4.2 Politikat e bazuara në aplikacione

Në fillim firewall –et përdoreshin thjesht për të bllokuar trafikun e padëshiruar ose të dyshimtë në kufirin e rrjetit. Në ditët e sotme kanë një përdorim tjetër, ata e lejojnë trafikun e destinuar për një server të veçantë brenda rrjetit, por e kapin këtë trafik në një server që e proceson atë njësoj si një firewall i bazuar në porta. Teoria është që firewall-et e aplikimeve ose proxy-it mund të mbrojnë serverin më mire sesa serveri mbron veten – dhe gjithashtu mund të fshijë trafikun e dëmshëm përpara se ai të arrijë serverin, duke ndihmuar në reduktimin e ngarkesës në server. Në disa raste, një firewall aplikimi ose proxy mund të fshijnë atë trafik që një server nuk mund ta fshijë vetë sepse ai ka kapacitet shumë të mirë filtrimi. Një firewall aplikimi ose proxy mund të parandalojnë serverin nga aksesimi direkt në rrjetin e jashtëm.

Nëse është e mundur, aplikacionet hyrëse të firewall-eve dhe proxy duhet të jenë përdorur për çdo server që nuk ka siguri të mjaftueshme për t'u mbrojtur nga aplikacionet tipike sulmuese. Kushtet kryesore se kur duhet të vendoset ose jo një aplikacion firewall-i ose proxy janë:

- A është në dispozicion një firewall i përshtatshëm aplikim-i? Ose nëse është e përshtashme, është në dispozicion një proxy i përshtashëm aplikimi?

- A është tashmë serveri i mbrojtur mjaftueshëm nga firewall-et ekzistuese?

- A është e lehtë të përditësohen rregullat e filtrimit në serverin kryesor dhe në aplikimin firewall ose proxy për të trajtuar kërcënimet e zhvilluara së fundmi?

Proxy-t e aplikimeve mund të sjellin probleme nëse nuk janë të përshtatshëm. Vetëm nëse është i përditësuar dhe më efiçent se serveri mund të vazhdojë të përdoret. Firewalle-t e aplikimeve mund të sjellin gjithashtu probleme nëse nuk janë mjaftueshëm të shpejtë për të trajtuar trafikun e destinuar për në server. Megjithatë, është e rëndësishme të konsiderohen burimet e serverit-nëse serveri ka mjaftueshëm burime për të përballuar sulmet potenciale, nuk është e nevojshme përdorimi i firewall-it të aplikimeve apo proxy.

Kur një firewall aplikimi ose proxy hyrës është prapa perimetrit të firewall-it ose në firewall-in DMZ (demilitarized zone), perimetri i firewall-it duhet të realizojë bllokimin bazuar në adresat IP, të përshkruara më herët në këtë seksion për të reduktuar ngarkesën në firewall-in e aplikimit ose proxy.

Aplikacionet proxy për trafikun dalës janë të dobishëm për detektimin e atyre sistemeve që bëjnë lidhje të papërshtatshme ose të rrezikshme nga brendësia e rrjetit të mbrojtur. Deri tani lloji më i zakonshëm i proxy për trafikun dalës është HTTP. Ato lejojnë një institucion të filtrojë përmbajtjet e rrezikshme përpara se ato të arrijnë PC-në e kërkuar. Gjithashtu ndihmojnë një institucion të kuptojë sa më mirë trafikun në web nga përdoruesit e tij, dhe të detektojë aktivitetet që kanë filluar të kalojnë përgjatë HTTP. Kur një HTTP proxy filtron përmbajtjen ai mund të lajmërojë përdoruesit që faqja që është vizituar ka dërguar përmbajtje të filtruar.

4.3 Politikat e Bazuar në Identitetin e Përdoruesve

Filtrimi tradicional i paketave nuk mund të shikojë identitetin e përdoruesve të cilët janë duke komunikuar në trafik duke kaluar firewall-in, kështu që teknologjitë e firewall-eve nuk mund të kenë politika që lejojnë ose refuzojnë aksesin bazuar në këto identitete. Megjithatë, shumë teknologji të tjera firewall-esh mund ta shohin identitetin e përdoruesit, prandaj miratojnë politika të bazuara në autentikimin e tyre. Një nga mënyrat më të zakonshme për të zbatuar politikën e identifikimit të përdoruesve është nëpërmjet përdorimit të VPN. Si VPN i IPsec ashtu edhe VPN i SSL kanë mënyra të ndryshme të autentifikimit të përdoruesve, si për shembull me autentifikimin me shumë faktorë ose përdorimi i çertifikatave dixhitale që kontrollohen nga secili përdorues. NAC është gjithashtu një metodë e zakonshme për firewall-et që lejon ose mohon aksesin e përdoruesve në burime të caktuara të rrjetit.

Firewall-et që i zbatojnë politikat bazuar në identitetin e përdoruesve duhet t'i reflektojnë ato në log-et e tyre. Kjo do të thotë që, nuk mjafton thjesht që të ketë logim nga adresa IP nga e cila një përdorues i caktuar është lejuar të ketë akses nga politikat, por gjithashtu është e rëndësishme që të dihet identiteti i përdoruesit.

4.4 Politikat bazuar në aktivitetin e rrjetit

Disa firewall-e lejojnë administratorin të bllokojë lidhjet e vendosura pas një periudhe të caktuar pasiviteti. Për shembull, në qoftë se një përdorues jashtë firewall-it është loguar në serverin e skedarëve, por nuk ka bërë asnjë kërkesë përgjatë 15 minutave, politikat e vendosuara mund të bllokojnë çdo komunikim të mëtejshëm të asaj lidhjeje. Politikat e bazuara në kohë, janë të dobishme në pengimin e sulmeve të shkaktuara nga logimi i përdoruesve që janë larg kompjuterit për një kohë të caktuar dhe një përdorues tjetër që është ulur dhe është duke përdorur lidhjen e vendosur. Megjithatë, këto politika mund gjithashtu të mos jenë të duhurat për përdoruesit të cilët vendosin lidhje, por nuk i përdorin ato shpesh. Për shembull, një përdorues mund të lidhet me një server skedarësh për të lexuar një skedar dhe më pas shpenzon shumë kohë për të edituar skedarin. Nëse përdoruesi nuk e ruan skedarin në server përpara se firewall-it t'i përfundojë koha e qëndrimit aktiv, ndryshimet e bëra nuk do të ruhen.

4.5 Përmbledhje e Rregullave

Pikat e mëposhtme përmbledhin rregullat kryesore nga ky kapitull, të detyrueshme për zbatim:

- Politika e firewall-it të një institucioni duhet të jetë e bazuar në një analizë gjithpërfshirëse rreziku.

- Politikat e firewall-it duhet të jenë të bazuara në bllokimin e gjithë trafikut hyrës ose dalës, duke bërë përjashtim për trafikun e dëshiruar.

- Politikat, përveç përmbajtjes duhet të marrin në konsideratë burimin dhe destinacionin e trafikut.

- Shumë lloje të trafikut IPv4, të tilla si me adresat e pavlefshme ose private, duhet të jenë të bllokuara që në konfigurimet bazë.

- Institucionet duhet të kenë politika për trajtimin e trafikut IPv6 hyrës dhe atij dalës.

- Një institucion duhet të përcaktojë se cili aplikacion mund të dërgojë trafik brenda ose jashtë rrjetit të tij dhe të bëjë politika firewall-i për bllokimin e aplikacioneve të tjera.

5 Planifikimi dhe Implementimi i Firewall-eve

Ky kapitull fokusohet në planifikimin dhe implementimin e firewall-eve. Me aplikimin e një teknologjie të re, planifikimi dhe implementimi i firewall-eve duhet të trajtohen në faza. Nëse ndiqet hap pas hapi një planifikim i qartë, mund të arrihet implementim i suksesshëm. Implementimi me faza mund të minimizojë çështjet e paparashikuara dhe të identifikojë më herët kërcenime të mundshme. Ky kapitull shqyrton në thellësi çdo planifikim të firewall-eve dhe fazat e zbatimit, duke përfshirë:

1. **Plani.** Faza e parë e procesit ka të bëjë me identifikimin e të gjitha kërkesave që një institucion duhet të marrë parasysh kur të përcaktojë se cili nga firewall-et duhet implementuar për të zbatuar politikat e sigurisë së një institucioni.

2. **Konfigurimi.** Faza e dytë ka të bëjë me të gjitha aspektet e konfigurimit të platformës së firewall-eve. Kjo përfshin instalimin hardware dhe software si dhe ngritjen e rregullave të sistemit.

3. **Testimi**. Faza tjetër ka të bëjë me implementimin dhe testimin e zgjidhjes së projektuar. Qëllimet kryesore të testimit janë për të vlerësuar funksionalitetet, përfomancën, shkallëzueshmërinë dhe sigurinë e zgjidhjes dhe për të identifikuar ndonjë çështje të tillë si ndërveprimi me komponentët.

4. **Vendosja.** Pasi testimi është i përfunduar dhe të gjitha çështjet janë zgjidhur, faza e ardhshme fokusohet në vendosjen e firewall -ve.

5. **Menaxhimi.** Pasi është vendosur firewall-i, ai është i menaxhuar përgjatë gjithë ciklit të jetës përfshirë mirëmbajtjen e komponentëve dhe suportin për çështjet operacionale. Kyproces i ciklit të jetës përsëritet kur përmirësime ose ndryshime të rëndësishme duhet të përfshihen në zgjidhje.

5.1 Plani

Faza e planifikimit për përzgjedhjen dhe implementimin e firewall-it duhet të fillojë vetëm atëherë pasi një institucion ka përcaktuar atë që është e nevojshme për një firewall për të zbatuar politikat e sigurisë. Kjo zakonisht ndodh gjatë një vlerësimi risku për të gjithë sistemin. Një vlerësim risku përfshin:

1. Identifikimin e kërcënimeve dhe dobësive në sistemin e informacionit;
2. Ndikime të mundshme apo përmasat e dëmitimit nga humbja e konfidencialitetit, integritetit dhe disponueshmërisë së aseteve të institucionit ose operacioneve të tij;
3. Identifikimin dhe analizën e kontrolleve të sigurisë për sistemin e informacionit;

Parimet themelore që institucionet duhet të ndjekin në planifikimin e vendosjes të firewall-eve përfshijnë:

- **Përdorimi i pajisjeve ashtu siç ato janë të destinuara të përdoren**. Firewall-et duhet të përdoren vetëm si firewall. Përveç kësaj nga firewall-et nuk duhet të pritet që të ofrojë shërbime-jo sigurie të tilla si: të veprojë si web server ose e-mail server.

- **Krijimi i mbrojtjes në thellësi.** Mbrojtja në thellësi përfshin krijimin e shumë shtresave të sigurisë. Kjo e lejon riskun të jetë më i menaxhueshëm, sepse nëse një shtresë e mbrojtjes kompromentohet, një tjetër shtresë është aty që të ndalojë sulmin. Në rastet e firewall-eve, mbrojtja në thellësi mund të realizohet duke përdorur firewall-e të shumtë përgjatë institucionit, përfshirë perimetrin, përpara departamenteve të ndjeshëm në brendësi, dhe në çdo kompjuter individual. Që një mbrojtje në thellësi të jetë sa më efektive, firewall-et duhet të jenë pjesë e një programi sigurie të përgjithshme që përfshin produkte të tilla si, programe të cilat bëjnë të mundur kontrollimin, identifikimin, eleminimin e programeve kompjuterike të dëmshme të instaluara në kompjutera (virus, trojan etj) dhe programe zbulimi ndërhyrjesh.

    - **Kushtoji vëmendje kërcënimeve të brendshme.** Duke përqëndruar vëmendjen vetëm në kërcënimet e jashtme mund të lihet një rrjetë e gjerë e hapur për sulmet nga brenda. Këto kërcënime nuk mund të vijnë nga brenda, por mund të përfshijnë hoste të brendshme të infektuar nga programe kompjuterike të rrezikshme (malware) ose të kompromentuar nga sulmet e jashtme. Sistemet e brendshme të rëndësishme duhet të vendosen prapa firewalle-ve të brendshëm.

- **Dokumento aftësitë e firewall-eve.** Çdo model i firewall-eve ka aftësi dhe kufizime të ndryshme. Këto ndikojnë në planifikimin e politikave të sigurisë së institucionit dhe në strategjinë e shpërndarjes së firewall-eve. Çdo karakteristikë që ndikon pozitivisht ose negativisht në planifikim duhet të jetë e shkruar në dokumentin e përgjithshëm të planifikimit.

Mbani mend se shprehja "Gjithë rregullat janë bërë për t'u thyer" aplikohet kur implementohen firewall-et. Ndërsa implementuesit e firewall-eve duhet të kenë parasysh rregullat e mësipërme gjatë planifikimit, çdo rrjet dhe institucion ka kërkesa të veçanta dhe që mund të kërkojnë zgjidhje të veçanta.

Institucionet kur duan të bëjnë blerjen dhe implementimin e zgjidhjeve firewall duhet të marrin në konsideratë pikat si me poshtë.

- Kapacitetet e Sigurisë
- Cila zonë e institucionit duhet të jetë e mbrojtur (perimetri, departamentet e brendshme, shërbimet specifike etj)?
- Cilat tipe teknologjish firewall-i do të adresojnë më mirë llojet e trafikut që duhet të mbrohen (filtrim paketash, inspektim, aplikacione firewall-i, aplikacionet proxy-gateway etj)?

- Çfarë karakteristikash sigurie shtesë – të tilla si kapacitete zbulimi ndërhyrjesh, rrjet privat virtual (VPN), dhe filtrim përmbajtjesh – i duhet firewall-it të suportojë?

- Menaxhimi

- Cilat protokolle suporton firewall-i për menaxhim në distancë, siç janë HTTP mbi SSL, SSH, ose akses mbi kabëll serial?
- A janë protokollet e menaxhimit në distancë të pranueshme për përdorim bazuar në politikat e institucionit?
- A mundet që aksesi në distancë të kufizohet vetëm tek disa ndërfaqe të firewall-it dhe adresa IP burim siç janë ato në rrjetin e brendshëm?
- A lejohet menaxhim qendror i disa pajisjeve firewall nga i njëjti prodhues?
- Nëse ky menaxhim është i mundur a duhet ndonjë aplikacion i veçantë nga prodhuesi apo mund të përdoren aplikacione të tjera?

- Performanca

- Çfarë sasie transmetimi, numër lidhjesh në mënyrë simultane, lidhje për sekond dhe vonesash lejohen në mënyrë që firewall-i të mos kthehet në një bllokues për aksesin në rrjet, për trafikun e tanishëm dhe atë që pritet në të ardhmen?
- A kërkohet numri i dështimeve dhe ngarkesa si faktor për të siguruar disponueshmëri të lartë?
    - A duhet marrë në konsideratë nëse firewall është hardware-based apo software-based?

- Integrimi

    - A do t'i duhet firewall-it hardware i veçantë në mënyrë që të integrohet në rrjetin e një institucioni?
    - A duhet firewall-i të jetë kompatibël me pajisjet e tjera në rrjet që ofrojnë siguri ose shërbime të tjera?

- A komunikon log-imi i firewall-t me sisteme të tjera të menaxhimit të logeve?
- A do të duhet ndryshimi i hapësirave të rrjetit për të instaluar firewall-in?

- Ambienti fizik

  - Ku do të vendoset firewall-i fizikisht për të pasur siguri fizike dhe mbrojtje nga dukuritë natyrore e jo vetëm?
  - A ka hapësirë të mjaftueshme atje ku do të vendoset?
  - A do të duhet shtesa në fuqi elektrike, backup elektrik, kondicionimin dhe lidhjet fizike në ambientin fizik ku do të instalohet firewall-i?

- Personeli

  - Kush do të jetë përgjegjës për menaxhimin e firewall-it?
  - A kanë nevojë administratorët e sistemit për trajnime para se firewall-i të instalohet?

- Kërkesat në të ardhmen

A i përmbush firewall-i kërkesat e institucionit në të ardhmen, si implementimi i IPv6 apo rritja e bandwidth? Kërkesat si më poshtë duhen patur parasysh kur blihen dhe instalohen firewall-e host-based ose personalë :

- A i plotësojnë kërkesat minimale të firewall-it serverat dhe kompjuterat ku do të instalohet?

- A do të jetë kompatibël me software të tjerë sigurie në server ose workstation?

- A mundet firewall-i të raportojë thyerjet e politikave në një server qëndror?

- A mund të kyçet në mënyrë që vetëm administratorët të mund t'a modifikojnë?

- A do të konfliktojë firewall-i me firewall-e të tjerë të instaluar tek sistemet e operimit të hosteve?

5.2 Konfigurimi

Faza e konfigurimit përfshin gjithë hapat e konfigurimit të platformës së firewall-it. Kjo përfshin instalimin e hardware dhe software, konfigurimin e politikave, konfigurimin e log-eve dhe alarmeve dhe integrimin e firewall-it në arkitekturën e rrjetit.

5.2.1 Instalimi i hardware dhe software

Mbasi është zgjedhur dhe blerë firewall-i, hardwar-i, sistemi i operimit duhet të instalohet në një firewall software-based. Më pas duhen instaluar patch dhe duhen bërë përditësime. Gjatë kësaj kohe firewall-i duhet të forcohet që të ulen rreziqet ndaj tij dhe sistemit të operimit. Duhen instaluar gjithashtu konsolat për akses në distancë .

Gjatë instalimit dhe konfigurimit vetëm administratorët duhet të aksesojnë firewall-in. Të gjitha pjesët e menaxhimit, si SNMP, duhen ç'aktivizuar nëse nuk duhen. Nëse firewall-i lejon llogari të veçanta administratori, atëhere duhet konfiguruar nga një për secilin.

Firewall-et e rrjetit duhen vendosur në dhoma që plotësojnë rekomandimet e shitësit në lidhje me temperaturën, lagështinë, hapësirën, energjinë etj. Dhoma gjithashtu duhet të ketë sigurinë e nevojshme fizike për të ndaluar personelin e paautorizuar të aksesojë firewall-in.

Krahasimi i log-eve nga burime të ndryshme është shumë i rëndësishëm kur kryhen analizat, prandaj ora e brendshme e çdo firewall-i duhet të jetë konsistente me sistemet e tjerë të institucionit. Kjo arrihet nëpërmjet një autoriteti qëndror i cili bën sinkronizimin.

5.2.2 Konfigurimi i politikave

Mbas instalimit dhe sigurimit të hardware dhe software administratorët duhet të krijojnë politikat. Disa firewall-e implementojnë politikat me rregulla specifike, disa kërkojnë konfigurim të firewall-ve dhe krijojnë rregullat vetë, disa i krijojnë automatikisht, disa të tjerë kombinojnë të tre teknikat. Përfundimi është një bashkësi rregullash (rule set) që përshkruajnë si do të sillet firewall-i.

Këto "rule set" duhet të përshkruajnë rregullat dhe politikat e institucionit të specifikuara në planin e sigurisë. Për të krijuar këtë bashkësi rregullash duhen përcaktuar tipet e trafikut për aplikacionet e aprovuara nga institucioni. Kjo duhet të përfshijë protokollet që i duhen firewall-ve për punën e përditshme.

Detajet e krijimit të rregullave varen nga tipi dhe produkti specifik. Për shembull shumë firewall-e kontrollojnë trafikun nëpërmjet rregullave në mënyrë sekuenciale. Për këto firewall-e rregullat me probabilitetin më të lartë duhen vendosur sa më lart në listë.

Ato gjithashtu i duhen punonjësve që auditojnë rregullat. Pavarësisht se komentet duken si pa rëndësi ato kanë mjaft vlerë me kalimin e kohës. Gjithashtu ndryshimet e rregullave dhe komentet duhen mbajtur në log-e të caktuara.

Minimalisht rregullat e mëposhtme duhen shënuar:

- Filtrimi i portave duhet aktivizuar për pjesën e jashtme të rrjetit dhe në disa pjesë brenda tij.
- Filtrimi i përmbajtjes duhet të bëhët sa më i shpeshtë të jetë e mundur.

Ka shumë mënyra për caktimin e rregullave dhe çdo institucion duhet të ketë kërkesat dhe personat e përfshirë në këtë proces.

Nëse disa rregulla janë të njëjta për disa firewall -e atëherë ato duhen sinkronizuar. Kjo bëhet sipas asaj që ka lejuar shitësi. Duhet pasur parasysh se disa firewall -e kanë politika të ndryshme në varësi të vendodhjes në rrjetin e institucionit.

5.2.3 Konfigurimi i log-eve dhe alerteve

Hapi tjetër është konfigurimi i log-eve dhe alerteve. Log-imi është hap kritik për rregullimin në rast dështimesh dhe duhet për t'u siguruar që konfigurimi i sigurisë është i saktë. Nëse bëhet siç duhet, log-imi ndihmon shumë për hetimin dhe zgjidhjen e incidenteve. Kur është e mundur firewall-i duhet t'i ruajë ato lokalisht dhe t'i dërgojë në një infrastrukturë qëndrore.

Nëse firewall-i lejon llogari me të drejta të ndryshme duhet krijuar një e cila ka vetëm të drejta leximi, për analiza logesh. Kjo llogari mund të përdoret dhe për auditime dhe raste kur duhen vetëm të drejta leximi.

Përveç log-eve edhe alarmet duhen konfiguruar. Tek to mund të përfshihen:

- Çdo modifikim ose ç'aktivizim i rregullave të firewall-it
- Restart, mungesë memorje ose probleme të tjera operacionale
- Ndyshime të tjera të statusit, nëse lejohet.

5.3 Testimi

Firewall-i i ri duhet testuar dhe vlerësuar përpara instalimit në mënyrë që të sigurohet që punon në mënyrë korrekte. Testimi duhet bërë në ambient testimi pa lidhje me ambientin e prodhimit. Ky testim duhet të tentojë të replikojë ambientin e prodhimit sa më afër të jetë e mundur. Aspekte të zgjidhjes e cila do të vlerësohet janë si më poshtë:

- **Lidhja** Përdoruesit mund të vendosin dhe mbajnë lidhje përmes firewall-it.

- **Bashkësia e rregullave** Lejohet vetëm trafiku i cili është në përputhje me politikën e sigurisë. Ai i cili nuk lejohet ndalohet nga firewall-i. Verifikimi i rregullave përfshin verifikimin manual dhe testimin nëse punojnë siç duhet.

    - **Kompatibiliteti me aplikacionet.**Firewall-et personalë ose host-based nuk ndërhyjnë në aplikacionet ekzistuese. Kjo përfshin edhe komunikimin e rrjetit mes komponentëve të aplikacionit.

- **Menaxhimi.** Administratorët mund ta menaxhojnë dhe konfigurojnë zgjidhjen në mënyrë të sigurtë.

- **Log-imi.** Funksionet e log-imit dhe menaxhimit janë në përputhje me politikat dhe strategjitë e institucionit.

- **Performanca.** Zgjidhja ofron performancë të pranueshme në kushte normale dhe trafiku të rënduar. Në raste të tilla është mirë të përdoren gjenerues trafiku për përmasat e rasteve normale ose trafikut të rënduar. Simulimi i sulmeve Distributed Denial-of-Service (DDoS) gjithashtu mund të ndihmojë në vlerësimin e performancës. Testimi duhet të përfshijë tipe të ndryshme aplikacionesh që kalojnë përmes firewall-it, sidomos ato që krijojnë vonesa.

- **Siguria e implementimit.** Vetë firewall-i mund të ketë dobësi të cilat mund të përdoren nga sulmuesit. Institucionet me kërkesa të larta sigurie duhet të testojnë vetë firewall-in dhe pjesët e tij.

- **Lidhja e komponentëve.** Pjesët e ndryshme të zgjidhjes firewall duhet të komunikojnë pa probleme, kjo është shumë e rëndësishme kur pjesët janë nga prodhues të ndryshëm.

- **Sinkronizimi i politikave.** Nëse ka disa firewall-e që kanë politika të sinkronizuara duhen testuar këto politika në skenarë të ndryshëm.

- **Funksionalitete shtesë.** Funksione shtesë, si rrjeti virtual privat (VPN) ose programe të cilat bëjnë të mundur kontrollimin, identifikimin, eleminin e programeve kompjuterike të dëmshme të instaluara në kompjutera (virus, Trojan etj), gjithashtu duhen testuar.

5.4 Instalimi

Pasi ka përfunduar testimi dhe janë zgjidhur të gjitha çështjet, faza pasardhëse e planifikimit dhe implementimit të firewall-it është vendosja, që duhet të bëhet në përputhje me politikat e kompanisë. Para vendosjes së firewall-it, administratorët duhet të lajmërojnë përdoruesit apo zotëruesit e sistemeve që kanë mundësi për t'u prekur nga ndryshimet, mbi vendosjen e planifikuar, dhe t'i udhëzojnë kush duhet të lajmërohet nëse paraqesin ndonjë problem. Edhe ndryshimet e tjera të nevojshme për pajisje të tjera duhet të koordinohen si pjesë e vendosjes së firewall-it. Politikat e sigurisë që shprehen përmes konfigurimit të firewall-it duhet t'u shtohen politikave të tjera të sigurisë së kompanisë, dhe ndryshimet e vazhdueshme të konfigurimeve duhet të integrohen me proceset e menaxhimit të konfigurimit të organizatës. Nëse vendosen firewall-e të shumëfishta, duke përfshirë firewall-e personale apo në degë të ndryshme të zyrave, duhet marrë në konsideratë një përqasje graduale apo e ndarë në faza; gjithashtu, një program pilot mund të ishte i dobishëm, veçanërisht për të identifikuar dhe zgjidhur çështje të politikave që ndeshen me njëra-tjetrën. Kjo do t'u sigurojë administratorëve një mundësi për të vlerësuar impaktin e zgjidhjes së firewall-it dhe do të zgjidhë çështje të mundshme para vendosjes në gjithë kompaninë.

Të lidhësh një firewall me rrjetin e institucionit kërkon më shumë se sa vetëm të vendosësh firewall-in në rrjedhën e trafikut nga jashtë, brenda rrjetit përfshihet gjithashtu integrimi i firewall-it me elementë të tjerë të rrjetit që do të ndërveprojnë me firewall-in. Duke qënë se firewall-et zakonisht sillen si router-a, firewall-i duhet të integrohet në strukturën e route-imit të rrjetit. Kjo zakonisht do të thotë zëvendësimin e ndonjë router-i që është në të njëjtin

pozicion në topologjinë e rrjetit siç është vendosja e firewall-it, por mund të duhet edhe ndryshimi i tabelave të route-imit në mënyrë që edhe router-at e tjerë të rrjetit të institucionit të përballojnë shtimin e këtij router-i të ri. Nëse elementët në rrjet përdorin route-im dinamik, këtyre elementëve mund të duhet t'u ndryshohet konfigurimi në mënyrë që të jenë në dijeni të route-imit të firewall-it. Gjithashtu, switch-i i rrjetit nga ana e jashtme e rrjetit që mbrohet mund të duhet të rikonfigurohet për të përballuar adresimin e firewall-it. Nëse firewall-i është një bashkësi sistemesh me parashikim dështimesh mes sistemeve, switch-i i rrjetit mund të duhet të konfigurohet për të përballuar dështimet e mundshme.

5.5 Administrimi

Faza e fundit është edhe faza më e gjatë dhe është ajo e menaxhimit të zgjidhjes pas implementimit. Ajo përfshin mirëmbajtjen e arkitektures, rregullave, politikave, softwar-it dhe gjithë pjesëve të tjera të zgjidhjes. Një rast është kur duhen zgjedhur dhe implementuar patche të ndryshme. Një rast tjetër është përditësimi i rregullave të ndryshme. Performanca e firewall-it duhet monitoruar në mënyrë të vazhdueshme po ashtu si loget dhe alarmet. Gjithashtu rregullat dhe konfigurimi duhen bërë backup në mënyrë të vazhdueshme. Është mirë që politikat e firewallit të shikohen në mënyre të rregullt. Çdo rishikim duhet të ketë një liste me gjithë ndryshimet e vërejtura që nga auditimi i fundit. Mundësisht ekspertë të jashtëm duhet të bëjnë auditime në raste të rralla. Disa mjete lejojnë auditime automatike për rregulla të panevojshme ose për rregulla të rekomanduar por që mungojnë. Në qoftë se janë në dispozicion mjete të tilla ato duhen përdorur rregullisht. Institucionet duhet të marrin në konsideratë kryerjen e testeve të ndryshme për penetrimin në mënyrë që të vlerësojnë sigurinë e përgjithshme të rrjetit të tyre. Këto teste lejojnë të kuptohet nëse rregullat (rule set) e firewallit po vepron siç duhet. Ato duhen përdorur si shtesë ndaj auditimeve të zakonshme dhe jo t'i zëvendësojnë ato.