BAB 3

POLISI DALAM ISU KESELAMATAN

3.0 PRINSIP KEMASKINI POLISI

Prinsip pengemaskinian polisi merujuk kepada pengemaskinian polisi keselamatan yang mengubah polisi dari masa ke semasa mengikut keadaan semasa. Selalunya pengemaskinian polisi merujuk kepada pengemaskinian polisi pada *firewall*. *Firewall* berperanan dalam menghadkan laluan trafik dan ini membolehkan talian menjadi lebih perlahan dengan polisi kawalan yang banyak. Konsep pengemaskinian polisi boleh dilihat sebagai satu kaedah untuk menghadkan polisi statik dan memperbanyakkan polisi secara dinamik. Ini bermakna polisi boleh dikemaskini dan cuma polisi tertentu sahaja wujud pada satu-satu masa. Polisi itu juga tidak terhad dan tidak banyak seperti polisi statik.

Penggunaan polisi statik bermakna polisi telah di tulis pada mula-mula ianya hendak di implementasi dan polisi ini diubah dari masa ke masa mengikut kesesuaian pentadbir rangkaian. Berbeza pula berbanding polisi yang dinamik, ianya berubah mengikut keadaan dan sering berubah, tambahan pula polisi dinamik berubah secara automatik mengikut kesesuaian rangkaian pada masa tertentu.

Memandangkan situasi keselamatan rangkaian berubah mengikut masa dan peredaran zaman, maka polisi yang dinamik menjamin keutuhan sesuatu rangkaian. Pengemaskinian selalu memberi lebih jaminan keselamatan rangkaian. Ini bermakna

penceroboh tidak dapat menjangka polisi sesuatu rangkaian kerana rangkaian sentiasa berubah mengikut keadaan. Ini memberi peluang kepada pentadbir untuk mentadbir sistem secara lebih berkesan.

Namun apa yang ditekankan di sini ialah pengemaskinian yang kerap boleh membuatkan pentadbir berasa beban kerja yang tinggi. Pengemaskinian secara automatik oleh tindakan agen sama ada dalam rangkaian atau luar boleh memudahkan proses kerja. Mod pengoperasian bagi sistem keselamatan rangkaian akan terjamin jika polisi dikonfigurasi secara berkala dan menambah beberapa polisi baru.

Organisasi yang berurusan dengan pengguna yang ramai ada kala tidak dapat memenuhi kehendak pengguna. Pengguna terdiri daripada berbagai tahap kecekapan juga memberi kesan kepada penghasilan rekabentuk polisi rangkaian. Dengan adanya polisi yang dinamik pengguna yang berubah-ubah dapat diselarikan dengan konfigurasi keselamatan rangkaian.

3.1 KONSEP POLISI *FIREWALL*

Konsep polisi *firewall* merangkumi bagaimana *firewall* dikonfigurasi mengikut kesesuaian penggunaan. Konsep polisi *firewall* bergantung bagaimana rangkaian digunakan dan sejauh mana ianya diimplementasi. Secara umum polisi *firewall* di kategori kepada beberapa tahap mengikut kehendak rangkaian. Pembahagian polisi *firewall* dibahagi bergantung kepada risiko sama ada rendah, pertengahan dan juga tinggi. Setiap kategori dibahagi pula kepada tahap penggunaan kepada pengguna biasa, pengurus

rangkaian dan juga juruteknik. Walau bagaimanapun setiap organisasi perlu memberi perhatian kepada implementasi *firewall* biar pun menggunakan polisi berisiko rendah.

3.1.1 Polisi Persekitaran Berisiko Rendah

i. Pengguna

Semua komunikasi dengan dunia Internet mesti melalui laluan yang tertentu yang mana telah ditetapkan oleh pentadbir. Ini bermakna pengguna hanya boleh melayari Internet jika dan jika hanya dibenarkan oleh pentadbir.

Firewall diletakkan di antara rangkaian luar dan juga rangkaian dalaman. Ini bermakna pengguna di luar firewall tidak dapat menghubungi pengguna dalaman dengan mudah dan terus.

Pengguna dalaman tidak boleh keluar daripada rangkaian dalaman tanpa melalui firewall. Kemungkinan juga beberapa protokol tidak dibenarkan dan juga beberapa port ditutup untuk keselamatan. Tetapi jika pengguna memerlukan talian komunikasi port tertentu, pengguna boleh mendapatkan maklumat daripada pengurus rangkaian.

ii. Pengurus Rangkaian

Konfigurasi firewall mesti diletakkan di antara rangkaian yang hendak di kawal. Ini bermakna rangkaian dalaman terasing secara total dari rangkaian luar. Peletakan firewall mesti berpatutan dengan kehendak pentadbir. Ini bertujuan untuk mengelakkan dari serangan rangkaian yang tidak boleh dipercayai.

Pengurus mesti memastikan tiada talian dalaman yang disalahgunakan. Sebagai contoh menghalang dari pengguna dalaman menggunakan modem untuk keluar dari rangkaian dan organisasi.

iii. Juruteknik

Semua firewall mesti dikonfigurasi oleh pentadbir sahaja. Jika berlaku sebarang masalah, pengguna dan pengurus yang tidak berkaitan tidak boleh membaiki kerosakan rangkaian.

Pembaikan untuk semua firewall dalaman mestilah membenarkan pembaikan secara kawalan jauh, namun ianya cuma membenarkan talian kawalan dari alamat dalaman sahaja. Penggunaan alamat dari luar mesti dielakkan. Firewall mestilah berupaya menyediakan audit log bagi semua sesi. Juruteknik mesti memastikan semua komunikasi berada dalam keadaan baik. Menyediakan laporan berkaitan dengan keselamatan dan juga mengemaskini polisi firewall pada masa diperlukan sahaja.

3.1.2 Polisi Persekitaran Berisiko Sederhana

i. Pengguna Biasa

Semua akses ke dalam adalah tidak dibenarkan sama sekali. Jika dibenarkan penggunaan token atau autentikasi mesti diperlukan.

ii. Pengurus

Juga sama seperti pengguna biasa, cuma autentikasi lebih mudah dan memerlukan katalaluan yang sedia ada oleh pengurus. Pengurus boleh mengawal semua peralatan dalaman yang berada dalam firewall.

Semua polisi keselamatan mesti dilihat setiap tiga bulan sekali oleh pentadbir yang bertanggungjawab. Sebarang pertukaran dalam polisi keselamatan mesti melalui polisi firewall. Perubahan dalam firewall mesti selari dengan polisi keselamatan.

iii. Juruteknik

Firewall mesti dikonfigurasi dengan menghalang semua servis dan sentiasa mengawasi perlakuan luar biasa dan juga mengawal untuk mengesan penceroboh. Firewall berupaya untuk memberitahu pentadbir serta merta setiap apa jua perlakuan yang berlaku dalam rangkaian termasuklah pecah masuk dalam rangkaian dan sebagainya.

3.1.3 Polisi Persekitaran Berisiko Tinggi

i. Pengguna Biasa

Semua perkara yang tidak berkaitan dengan polisi tidak dibenarkan sama sekali. Setiap pengguna melayari Internet dilog. Halaman yang tidak berkaitan tidak dibenarkan. Cuma laman web yang berkaitan sahaja dibenarkan. Kegagalan mematuhi arahan akan dikenakan tindakan disiplin oleh pihak atasan.

ii. Pengurus

Sama seperti pengguna biasa, setiap laman dilog dan cuma membenarkan laman web tertentu sahaja dilayari. Kegagalan mematuhi arahan juga akan dikenakan tindakan disiplin.

iii. Juruteknik

Membuat laporan setiap hari berkaitan dengan penggunaan rangkaian. Penyeliaan yang berkala untuk rangkaian. Laporan berkaitan dengan salah guna dilaporkan kepada pihak atasan.

3.2 POLISI BERKESAN RANGKAIAN

Dalam merangka polisi berkesan dalam rangkaian, beberapa perkara perlu dilihat. Sekadar mengetahui apa yang hendak dihalang dan apa yang tidak bukan merupakan polisi yang berkesan. Beberapa aspek perlu dinilai dan dikaji sebelum diletakkan dalam polisi setempat rangkaian. *Firewall* yang mempunyai polisi yang tidak dikaji dan dinilai akan menyebabkan *firewall* tidak berkesan dan mungkin akan memberi impak yang tidak baik kepada rangkaian.

Ini termasuklah menilai setiap servis yang hendak digunakan dan tidak dalam sesuatu rangkaian. Servis seperti FTP, Telnet, pop3 serta SMTP perlu dinilai supaya penggunaan tidak memberi peluang kepada pencerobo untuk mencerobo sistem. Tambahan dengan penggunaan servis HTTP, penggunaan port 80 memberi banyak kesan kepada rangkaian. Ada baiknya jika suatu rangkaian tidak menggunakan port 80 sebaliknya menggunakan

proxy *firewall*, Squid atau proxy port yang lain seperti 3128 atau 8080 selain daripada port 80 untuk melayari Internet.

Penggunaan servis perlu dinilai kerana besar kemungkinan penggunaan servis-servis ini akan memberi peluang kepada pengguna lain menceroboh atau mengguna port sedia ada dalam rangkaian. Berikut adalah ancaman dan beberapa kemungkinan penggunaan servis biasa dalam rangkaian. Servis dan port adalah seperti *SMTP (25), POP3 (110), IMAP (143), TELNET (23), FTP(21), WWW (80).*

3.2.1 Ancaman

Servis dan Port yang dibuka mempunyai ancaman seperti berikut:

i. SMTP (25) : Servis ini sering memberi peluang kepada bukan pengguna sah menggunakan port untuk menghantar email dari *server* tersebut. Sering berlaku email "*spamming*" yang membuat pelambakan email dari satu *server*. Walaupun penggunaan email dipusatkan dengan mudah namun ianya sukar dikonfigurasi untuk keselamatan mutlak.

ii. POP3 (110) : Walaupun pengguna menggunakan katalaluan dan juga kata nama namun ianya boleh memberi peluang kepada pengguna lain untuk melihatnya. Ini disebabkan oleh penggunaan port yang tidak dienkrip. Kebarangkalian penceroboh mendapat maklumat katalaluan adalah tinggi.

iii. IMAP (143) : Ancaman kepada penggunaan servis IMAP tidak begitu ketara berbanding dengan SMTP dan juga POP3 kerana IMAP menggunakan kaedah enkripsi dan autentikasi yang lebih baik. Walaupun begitu ianya masih terancam.

iv. TELNET (23), FTP(21) : Ancaman dalam penggunaan servis ini juga memberi kesan kepada pengguna. Penggunaan Telnet dan FTP adalah tidak selamat kerana penggunaan boleh menjalankan servis dalam pelayan secara kawalan jauh. Masalahnya ialah autentikasi dalam komunikasi Telnet tidak dienkrip dan selamat. Katalaluan yang digunakan juga tidak dienkrip sewaktu penghantaran ke pelayan. Penggunaan SSH dan SFTP dari penggunaan OpenSSH boleh menggantikan Telnet dalam proses kawalan jauh.

v. WWW (80) : Banyak ancaman boleh dilakukan dengan menggunakan port 80 (WWW). Ancaman seperti ancaman WEB-CGI, ancaman WEB-FRONTPAGE, ancaman WEB-PHP dan WEB-IIS. Sebagai contoh serangan ke atas WEB-PHP merujuk kepada serangan yang dilakukan pada laman web berasaskan pelayan yang menggunakan aplikasi web PHP, menggunakan port 80 dan serangan akan mengakibatkan pelayan dikawal oleh penceroboh.

3.2.2 Perkara Dinilai

Banyak perkara yang perlu dipertimbangkan dalam menangani masalah isu keselamatan. Penjelasan setiap polisi yang dibuat adalah berdasarkan kepada penilaian yang dilakukan.

Beberapa aspek perlu dilihat dalam menilai isu keselamatan dan secara umumnya adalah:

i. Keupayaan penceroboh

Merujuk kepada keupayaan penceroboh dan kepandaian penceroboh itu sendiri. Jika dilihat dengan perkembangan serangan dari dahulu hingga sekarang ini jelas berbeza. Dahulu penceroboh lebih pakar dan menggunakan kaedah sendiri untuk menceroboh sesuatu sistem, namun sekarang ini penceroboh boleh terdiri daripada sesiapa sahaja kerana terdapat banyak peralatan yang boleh digunakan oleh mereka. Penggunaan peralatan ini banyak diletakkan di Internet dengan muat turun secara percuma. Komplikasi ini mengakibatkan ramai pengguna Internet cenderung untuk menjadi penceroboh yang kini mudah.

Dengan keupayaan penceroboh yang tidak boleh dijangka, polisi rangkaian perlu lebih ketat dan lebih baik dengan mana boleh menghalang pencerobohan daripada berlaku.

ii. Struktur rangkaian.

Struktur rangkaian juga merupakan perkara yang penting yang mana perlu dinilai. Struktur rangkaian yang kompleks mungkin tidak memerlukan polisi yang ketat. Sebaliknya struktur rangkaian yang mudah mungkin memerlukan polisi yang lebih ketat. Ini disebabkan jika bilangan subnet dalam rangkaian lebih banyak, setiap subnet mempunyai polisi tertentu, maka polisi keselamatan adalah lebih mudah dengan mana setiap *firewall* akan

mempunyai polisi yang tertentu sahaja. Konfigurasi akan bertambah mudah dan senang.

Berbeza dengan penggunaan satu subnet yang besar dan hanya menggunakan satu aplikasi *firewall*, sudah tentu akan memberi satu tamparan hebat kepada pentadbir untuk membuat polisi yang baik untuk mengawal rangkaian. Akibatnya rangkaian akan tidak stabil kerana mempunyai polisi yang ketat.

iii. Aplikasi Pelayan.

Aplikasi pelayan merujuk kepada aplikasi/program yang digunakan dalam pelayan atau host dalam rangkaian. Aplikasi yang mudah tanpa polisi keselamatan sendiri akan memberi peluang kepada penceroboh. Penilaian setiap aplikasi yang digunakan oleh pelayan mesti berupaya untuk menangkis serangan walaupun penceroboh boleh melepasi *firewall*.

Dengan merujuk kepada penggunaan aplikasi bersama dengan aplikasi keselamatan seperti penggunaan Kerberos atau SSH yang berupaya untuk menggantikan aplikasi seperti FTP, TELNET, Rlogin dan RCP. Penggunaan aplikasi keselamatan ini bukan sahaja membantu pelayan dari segi keselamatan data malahan ianya membantu pentadbir untuk melakukan kawalan jauh dengan lebih mudah dan selamat serta terjamin. Penggunaan aplikasi seperti PGP boleh memberi lebih keselamatan kepada penggunaan email sama ada email dalaman atau email luaran.

iv. Risiko polisi.

Seterusnya perkara yang perlu dinilai adalah berkaitan dengan risiko akibat dari polisi dilaksanakan. Ini termasuk laluan keluar masuk yang akan bertambah rumit dan berkemungkinan akan memberikan satu masalah kepada rangkaian dan juga pengguna.

Risiko polisi termasuk wujud masalah dalam pentadbiran rangkaian yang mana akan menjadi sukar kerana beberapa servis perlu dilihat dan diperhati untuk menghasilkan satu polisi yang tidak memberi kesan atau impak yang tinggi kepada pengguna yang berada dalam rangkaian.

3.3 PRINSIP PENGEMASKINIAN POLISI FIREWALL

Proses pengemaskinian polisi keselamatan firewall telah lama diperbincangkan. Walaupun begitu masih tidak banyak mekanisme pengemaskinian digunakan dalam mengemaskini polisi firewall dan selalunya mekanisme yang digunakan adalah sama. Prinsip pengemaskinian polisi firewall tunggal adalah lebih mudah berbanding firewall teragih. Setiap firewall dalam rangkaian mesti mempunyai polisi yang hampir sama dan proses mengemaskini polisi akan memakan masa yang lama jika dilakukan secara satu persatu.

Mekanisme dalam mengemaskini firewall tunggal dibahagi kepada 2 bentuk asas.

i. Manual

   a. Pengemaskinian firewall secara manual merujuk kepada polisi firewall yang direka oleh pentadbir dan dilakukan sendiri menggunakan sentuhan terus kepada sistem.

   b. Prinsip pengemaskinian polisi secara manual selalunya menggunakan peranti web yang mana bertindak sebagai antaramuka kepada pengguna dan pentadbir. Selalunya protokol yang digunakan dalam polisi pengemaskinian secara manual ini menggunakan protokol biasa seperti SSL, https dan TCP melalui port 443.

   c. Transmisi dihantar dari satu agen ke satu agen menggunakan protokol biasa seperti yang dinyatakan di atas jika ianya melibatkan rangkaian yang banyak.

ii. Automatik.

a. Prinsip pengemaskinian automatik merujuk kepada pengemaskinian polisi tanpa memerlukan pentadbir.

b. Pentadbir tidak perlu mencapai firewall untuk proses pengemaskinian.

Samaada secara manual atau automatik, tindakan pengemaskinian dilakukan pada firewall tunggal lebih mudah berbanding firewall teragih. Ini kerana bagi firewall sistem teragih, polisi perlu terlebih dahulu dihantar ke firewall berkenaan dengan cara-cara tertentu. Penggunaan mobile agen oleh Feng Xian (2002) memberi gambaran bahawa proses pengemaskinian polisi dalam rangkaian firewall teragih dapat dilakukan serta dapat memberi tindakan yang baik kepada sistem. Walau bagaimanapun kaedah ini memerlukan penghasilan 2 agen yang bertindak antara satu sama lain. Bermakna jika memerlukan rangkaian yang besar maka lebih banyak agen diperlukan. Selain pengguna mobile agen yang dicadangkan oleh Hai Jin dan rakan-rakan (2002), terdapat 2 lagi kaedah pengemaskinian polisi iaitu penggunaan *COBRA Middleware* dan *RMI Middleware* (Hwang, K. & Gangadharan, M. , 2001).

3.4 PROAKTIF PENGESAN PENCEROBOHAN

Pengesan pencerobohan memainkan peranan yang aktif dalam proses memberi kesan yang amat baik kepada implementasi keselamatan dalam rangkaian. Tindakan proaktif bermakna tindakan yang seiring dan memberi kesan dan impak yang lebih baik dari kesan sedia ada.

Jika dilihat kepada kesan dari sumbangan *firewall* kepada polisi keselamatan komputer, sedia maklum ianya memberi kawalan keselamatan yang baik. Namun jika isu keselamatan dipegang semata-mata oleh *firewall*, ianya tidak memberi kawalan keselamatan secara baik dalam keadaan dinamik. Perolehan dan penggunaan oleh Pengesan Pencerobohan boleh digunakan sebagai alat yang mana bertindak secara aktif dalam memberi peluang kepada kawalan keselamatan supaya lebih baik dan efisien. Penggunaan Sistem Pengesan Pencerobohan (IDS) boleh memberi kesan proaktif kepada penggunaan *firewall* sedia ada.

Penggunaan IDS bukan sahaja digambarkan secara maya oleh penyelidik malahan ianya telah di implementasi supaya penggunaan IDS dapat dimanfaat oleh pentadbir rangkaian sebagai alat yang boleh memberi kesan yang lebih baik dalam kawalan keselamatan rangkaian. Pentafsiran dalam dunia keselamatan dalam rangkaian menjadi lebih kompleks sekarang ini, dan adakala penggunaan seperti IDS dapat membantu polisi kawalan lebih baik.

Kawalan dinamik oleh sistem *firewall* sedia ada dapat memberi kesan yang bukan sahaja memudahkan pihak pentadbir rangkaian malahan ianya memberi masalah yang besar kepada penceroboh untuk menceroboh sistem sedia ada. Ini adalah kerana polisi yang sering berubah dan penceroboh tidak dapat mengenal pasti bentuk polisi yang mana ianya berubah.

Misalan pencerobоh hendak menceroboh dan cuba mengimbas rangkaian secara maya dan mendapati beberapa port/servis dibuka dan dibenarkan pada ketika itu kerana polisi keselamatan rangkaian membenarkannya. Pencerobоh cuba untuk menceroboh selepas mengimbas, tetapi didapati polisi telah berubah dan port/servis berkenaan telah dimansuhkan akibat dari perubahan polisi yang dinamik. Perubahan polisi keselamatan yang dinamik bukan sahaja melambatkan pencerobоh untuk menceroboh, tetapi memberi amaran kepada pentadbir supaya lebih berhati-hati.

Tindakan proaktif IDS dapat memberi maklumat berkenaan dengan sistem yang hendak diceroboh. Hasil tindakan ini membolehkan tindakan dinamik *firewall*. Fungsian *firewall* secara dinamik adalah merupakan lanjutan dari tindakan proaktif IDS. Ini bermakna perubahan sebarang fungsi polisi dalam kawalan keselamatan rangkaian terhadap *firewall* adalah bergantung kepada fungsian IDS. Pemberitahuan perubahan polisi oleh IDS ini membolehkan ianya menjadi satu kawalan yang lebih baik.

Tindakan proaktif ini merupakan tindakan sampingan yang mana menyumbang keadaan lebih baik dalam rangkaian. Pencerobоh yang hendak menceroboh akan mengalami masalah dalam menentukan polisi kawalan semasa kerana wujud satu mekanisme kemaskini oleh *firewall* sendiri atas tindakan atau cetusan dari IDS. Penglibatan IDS dalam kawalan keselamatan bukan merupakan satu bentuk atau cara yang baru dalam dunia keselamatan rangkaian, ianya telah wujud lama dan selama ini penggunaan IDS adalah untuk memantau tindakan pencerobоh dan terpulang kepada pentadbir untuk mengambil tindakan atau tidak. Log yang dihasilkan oleh IDS ada kala tidak diambil

peduli oleh pentadbir sendiri. Walaupun ada pentadbir yang mengambil tindakan kesan pemantauan IDS namun tindakan pentadbir adakala lambat dan pencerobohan telah berlaku.

Penglibatan IDS walaupun memberi kesan yang amat baik, namun jika tindakan proaktif tidak diambil maka IDS akan menjadi bahan sampingan sahaja. Peranan yang dimainkan oleh IDS boleh digunakan dalam menghasilkan satu mekanisme baru dalam proses pengemaskinian polisi dalam *firewall*. Walaupun ianya dianggap satu tambahan kerja bagi pentadbir untuk mengendalikan dua mekanisme yang berbeza yang hendak digabung namun ianya boleh menghasilkan satu kaedah yang bukan sahaja baru malahan membantu pentadbir dalam menghalang penceroboh dari terus bermaharajalela. Penglibatan IDS dalam kawalan keselamatan merupakan satu tambahan kepada penggunaan alatan keselamatan sedia ada dalam rangkaian seperti penggunaan *firewall* dan penggunaan teknik kriptografi.

3.5 KOMUNIKASI MULTICAST & PENGEMASKINIAN POLISI

Konsep komunikasi multicast merupakan konsep yang memberi kelebihan dalam komunikasi dengan memberi peluang penggunaan sumber dengan lebih efisien. Dengan konsep komunikasi multicast, penggunaannya dalam pengemaskinian polisi dapat memberi impak yang lebih baik dan cepat.

Jika komunikasi unicast digunakan maka pengemaskinian polisi akan menjadi tidak efisien dan perlahan. Ini kerana komunikasi multicast mesti menentukan sumber dan

mesti memberi port serta destinasi yang jelas kepada penerima. Tafsiran kepada penerima yang tertentu sahaja bukan melembapkan keadaan malahan memberi kekangan kepada pentadbir dalam melaksanakan mekanisme gabungan IDS dan juga *firewall*.

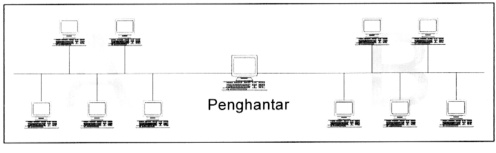
Komunikasi multicast digunakan dalam mekanisme pengemaskinian polisi adalah lebih baik dari komunikasi unicast kerana ianya memberi satu bentuk komunikasi yang mudah dan cepat. Perbezaan jelas dengan menggunakan komunikasi multicast berbanding komunikasi unicast dalam pengemaskinian polisi.

Jadual 3.1 : Perbezaan antara multicast dan Unicast

Perspektif.	**Multicast**	**Unicast**
i. Proses Penghantaran	Tidak Diulang	Perlu Diulang
ii. Proses Penerimaan	Tidak Perlu dinyatakan penerima.	Perlu dinyatakan penerima.
iii. Efisien	Lebih efisien dalam rangkaian setempat	Lebih efisien dalam rangkaian lebih besar.
iv. Keselamatan	Tidak begitu selamat kerana penerima tidak ditetapkan	Lebih selamat kerana penerima diketahui.
v. Kemungkinan diceroboh	Tinggi	Rendah walaupun begitu masih boleh diceroboh.
vi. Penerimaan	Tidak dijangka	Boleh dijangka.

Walaupun penggunaan multicast memberi impak yang kurang baik dalam perbandingan antara unicast tetapi ianya memberi kesan yang baik bila maklumat yang hendak di hantar banyak dan tidak tahu penerimanya. Penjelasan mengenai penerima dalam komunikasi multicast adalah berdasarkan kepada penerima yang menerima paket multicast tidak diketahui. Ini memudahkan pihak pentadbir untuk meletakkan *firewall* tanpa perlu membuat tambahan konfigurasi pada *firewall* utama, iaitu gabungan *firewall* dan IDS.

Penerimaan pengemaskinian polisi adalah lebih baik menggunakan multicast dari unicast kerana multicast tidak perlu mengetahui penerima sebaliknya menghantar polisi baru dalam rangkaian dengan satu nod sahaja. Berbanding dengan unicast, penerima perlu didaftar kepada *firewall* utama yang mana memberi maklumat pengemaskinian polisi. Tambahan pula penggunaan unicast perlu mengulangi proses beberapa kali, sebaliknya multicast cuma menjalankan satu proses dan semua penerima akan menerima serentak.



Rajah 3.1 : Komunikasi multicast

Gambar di atas menunjukkan dua keadaan yang mana multicast lebih baik daripada unicast. Kumpulan A mewakili unicast dan kumpulan B mewakili multicast. Multicast lebih baik apabila.

i. Penghantar menghantar maklumat kepada A dan B dalam masa yang sama.

ii. Salah satu kumpulan dalam A akan menerima maklumat apa yang dihantar kepada mereka cuma memerlukan 5 kali proses penghantaran yang berbeza.

iii. Penghantar menghantar maklumat kepada kumpulan multicast B. Semua menerima data dalam pada masa yang hampir sama tanpa mengulangi proses sebanyak 5 kali.

iv. Jika salah satu penerima dalam kumpulan A menerima data dari penghantar, Penerima lain tidak akan menerima.

v. Jika salah satu penerima dalam kumpulan B multicast menerima, semua penerima dalam kumpulan B akan terima.

Penerimaan data dari penghantar adalah sejajar bagi semua penerima dalam kumpulan B tetapi tidak bagi kumpulan A. Jika setiap proses penghantaran dan penerimaan memerlukan 1 saat. Maka proses penghantaran dan penerimaan dalam kumpulan A adalah 10 saat, berbanding 2 saat bagi proses multicast bergantung kepada komunikasi dalam rangkaian (Anggapan penerima menerima serentak atau masa hampir sama dan sempurna tanpa sebarang gangguan). Proses penghantaran dan penerimaan ini hendaklah dikonfigurasi kepada keadaan bersyarat yang berikut:

i. Setiap penerima kumpulan A mesti mempunyai agen penerima unicast protokol TCP/IP. Contoh : 192.168.0.1 – 192.168.0.5

ii. Setiap penerima kumpulan B mesti mempunyai agen penerima multicast dengan kumpulan multicast yang sama. Contoh : 224.0.0.25

iii. Penghantar mesti menghantar kepada penerima unicast dalam lingkungan IP seperti di atas (192.168.0.1 – 192.168.0.5).

iv. Penghantar mesti menghantar kepada penerima multicast dalam kumpulan multicast 224.0.0.25.

v. Port penghantaran tidak ditetapkan tetapi mesti sama antara penerima dan penghantar.

Proses penghantaran maklumat dalam unicast dan multicast adalah hampir sama antara satu sama lain, cuma multicast memerlukan satu nod yang tidak berulang berbanding dengan unicast yang perlu mengulangi proses sebanyak mana penerima.

Walaupun wujud isu keselamatan dalam rangkaian yang mana multicast tidak begitu selamat dalam proses penghantaran data kerana penerimanya tidak diketahui, namun jika dilihat secara positif ianya boleh memendekkan masa proses penghantaran. Jika isu keselamatan data diungkit, boleh dikatakan semua penghantaran data dalam rangkaian adalah tidak selamat. Oleh sebab itu penggunaan teknik algoritma kriptografi digunakan. Data unicast yang dikata selamat dalam proses penghantaran juga boleh menjadi mangsa kepada penghidu rangkaian dengan menggunakan alatan canggih masa kini. Penggunaan teknik kriptografi boleh memberi lebih keselamatan kepada data yang dihantar kepada penerima mahupun sesiapa sahaja.

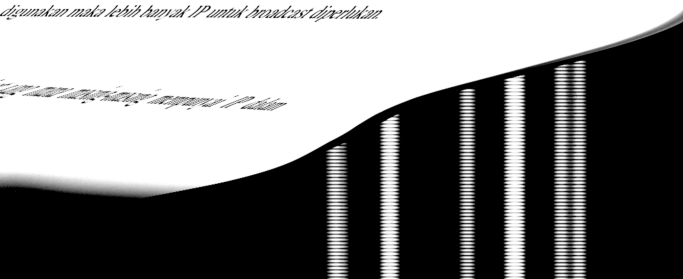
Teknik penggunaan algoritma Kriptografi banyak memberi kesan kepada komunikasi data dalam multicast. Beberapa teknik kriptografi yang digunakan berasaskan kepada teknik asas sama ada penggunaan teknik kripto sistem simetri atau asimetri. Penggunaan teknik simetri adalah dengan menggunakan satu kekunci rahsia untuk proses enkrip atau

dekrip data atau maklumat, berbanding dengan penggunaan asimetri (*public key* kripto sistem) dengan mana menggunakan 2 kekunci berbeza untuk proses enkrip dan dekrip. Satu untuk enkrip dipanggil *public key* dan yang kedua adalah private key untuk tujuan dekrip.

Komunikasi multicast bukan sahaja memberi kelebihan dalam pengemaskian polisi keselamatan *firewall* dalam rangkaian malahan ianya mempercepatkan tindakan (hampir masa nyata). Walaupun mempunyai masalah dalam bentuk tindakan penerima yang tidak diketahui namun penggunaan sistem adalah tertakluk kepada ruang lingkup setempat sahaja. Tambahan kepada beberapa VLAN yang lain memerlukan gabungan unicast dan multicast untuk menghasilkan satu tindakan yang baik.

3.6 MULTICAST DAN BROADCAST

Persoalan timbul bila mana kenapa transmisi broadcast tidak digunakan. Transmisi broadcast merujuk kepada transmisi yang hampir sama dengan transmisi multicast, cuma transmisi broadcast tidak efisien digunakan jika ianya melibatkan lebih daripada 1 subnet. Sebagai contoh penggunaan broadcast merujuk kepada pengguna dalam satu subnet yang sama. Pengguna cuma perlu hantar satu nod sahaja dan semua sistem akan menerimanya. Bermakna ada satu IP untuk broadcast bagi setiap subnet. Jika lebih daripada satu subnet



Jadual 3.2 : IP untuk transmisi Broadcast

Lingkungan alamat IP	IP untuk broadcast	Bilangan hos
192.168.0.1 – 192.168.0.255	192.168.0.255	254
192.168.1.1 – 192.168.1.255	192.168.1.255	254
192.168.2.1 – 192.168.2.255	192.168.2.255	254

Oleh yang demikian penggunaan transmisi secara broadcast kurang efisien berbanding multicast kerana multicast cuma memerlukan satu IP Multicast untuk ketiga-tiga subnet. Maka proses penghantaran akan lebih cepat tanpa perlu merujuk kepada setiap IP broadcast bagi setiap subnet. Tambahan pula bagi IP broadcast banyak perkara dilakukan dengan menggunakan transmisi ini seperti transmisi radio. Penggunaan multicast disebabkan oleh keperluan mesej yang hendak disampaikan hanya kepada nod tertentu sahaja dan bukan kepada semua nod dalam rangkaian.

3.7 KEBARANGKALIAN DALAM MENANGANI ISU KESELAMATAN

Dalam menangani masalah keselamatan dalam rangkaian, beberapa aspek perlu dilihat sama ada tindakan dalam isu keselamatan itu wajar atau tidak. Aspek seperti keperluan semasa perlu dinilai untuk mendapatkan kesan dalam pengambilan polisi keselamatan. Walaupun isu keselamatan merupakan isu yang penting dalam rangkaian dan juga dunia komputer, namun implementasinya perlu dilihat sejauh mana ianya dapat mengelak daripada berlakunya serangan dari penceroboh.

Secara umumnya penglibatan penyelidik dalam menangani isu keselamatan rangkaian telah lama, namun sejauh mana penyelidik dapat menghasilkan satu mekanisme yang benar-benar selamat dan mematuhi semua kehendak dalam rangkaian. Wujud

persefahaman dalam isu keselamatan yang mana setiap rangkaian mesti membuat satu polisi masing-masing yang mana memenuhi kehendak rangkaian sendiri. Persoalannya adakah dengan mewujudkan polisi keselamatan masing-masing akan menyelamatkan keadaan dari pencerobohan?. Ada jawapan yang menyatakan ada dan ada juga yang menyatakan tidak. Kenapa ada dua jawapan yang berbeza-beza sedangkan dunia pengkomputeran memerlukan antara ya atau tidak. 1 atau 0? Mungkinkah wujud kawasan *grey area* yang mana masih belum wujud samaada 1 atau 0.

Kepentingan isu keselamatan adalah nadi kepada pergerakan data dalam rangkaian dan juga dunia perniagaan sekarang ini. Tanpa rangkaian yang selamat, perniagaan yang melibatkan transaksi data dalam rangkaian akan terjejas. Pengguna tidak yakin akan kerahsiaan yang diberikan dalam transaksi yang dibuat.

Setelah lama keselamatan rangkaian diutamakan kini wujud pula isu keselamatan yang memberi tumpuan kepada keselamatan komputer. Dengan anggapan bahawa jika komputer berada dalam keadaan selamat, maka rangkaian juga akan selamat. Anggapan begini mungkin tidak begitu tepat kerana jika pada dasarnya komputer itu dilengkapi dengan semua alatan keselamatan seperti teknologi enkripsi, micro-*firewall*, anti-virus dan juga IDS, mungkin akan berlaku penyalahgunaan alatan teknologi ini dan akhirnya menyebabkan rangkaian dalam keadaan yang tidak selamat.

Tiga asas elemen penting dalam isu keselamatan rangkaian, enkripsi atau teknologi kriptografi, protokol rangkaian dan juga protokol sistem (Walker, S.T, 1989). Ketiga-tiga

elemen ini penting dalam menjamin keselamatan data dalam rangkaian. Elemen ini termasuklah penggunaan algoritma-algoritma yang telah digunakan dalam memberi kesan yang lebih dalam membuat polisi keselamatan.

Pendapat umum mengenai kepentingan dalam isu keselamatan rangkaian sudah menjadi tajuk utama dalam dunia rangkaian. Dari penggunaan teknik dalam kriptografi sehingga kepada alatan yang digunakan seperti *firewall* dan IDS, penterjemahan ilmu keselamatan komputer masih lagi menjadi isu yang tiada penghujung. Kajian mengenai betapa penting keselamatan komputer dan rangkaian sudah termaktub, namun masih tiada lagi kaedah atau mekanisme yang benar-benar selamat dalam rangkaian. Benar-benar selamat bermakna selamat dari semua keadaan dan memenuhi keperluan yang berbeza seperti dalam model OSI. Yang mana boleh menjamin keutuhan rangkaian di setiap aras dalam model OSI.

Ketujuh-tujuh aras yang berbeza mempunyai pendekatan yang berbeza yang mana bermula dengan aras fizikal dengan mengunci tempat simpanan merupakan pendekatan paling ideal. Kemudian pada aras *data link* pula dikawal oleh penggunaan VLAN yang membezakan rangkaian. Aras *transport* dalam rangkaian pula dikawal oleh *firewall* yang mana boleh mendapatkan maklumat mengenai alamat sumber dan destinasi serta port yang digunakan. Pada aras *session* pula penggunaan kata nama dan kata laluan telah lama digunakan dan masih merupakan pendekatan yang paling ideal digunakan. Malang sekali tiada pendekatan yang boleh menangani kesemua masalah keselamatan.

Pendekatan yang boleh dilakukan adalah dengan menggabungkan satu atau lebih teknologi keselamatan agar ianya boleh memberikan kawalan yang lebih baik serta efisien. Bergantung kepada satu kaedah sahaja mungkin akan memberi masalah, tetapi penggunaan lebih dari 1 kaedah juga mungkin akan memberi masalah jika tidak diuruskan dengan betul. Namun penggunaan yang berkala dan dikaji terlebih dahulu sebelum menggabungkan teknologi ini akan memberi kesan yang baik kepada keselamatan rangkaian.

pentadbir. Tindakan daripada amaran yang diberikan tidak dilakukan oleh Snort tetapi akan dilakukan oleh pentadbir.

b. Iptables

Aplikasi yang sedia ada dalam Linux Kernel dan berperanan membentuk micro-*firewall* dalam sistem Linux serta rangkaian.

ii. Aplikasi yang dibangunkan

a. *RedAlert*IDS

Aplikasi asas kepada sistem *RedAlert* yang menjalankan kod untuk memantau, membuat polisi baru dan seterusnya memberi maklumat kepada agen.

b. *RedAlert*Conf

Aplikasi konfigurasi asas kepada *RedAlert*. Ini juga termasuk konfigurasi untuk mengemaskini beberapa bentuk pencerobohan yang hendak dikawal. Polisi untuk *firewall* bagi setiap jenis pencerobohan dicipta di sini.

c. *RedAlert*Uni

Agen unicast yang digunakan untuk proses penghantaran transmisi unicast antara 2 atau lebih subnet.. Agen unicast ini diletakkan pada

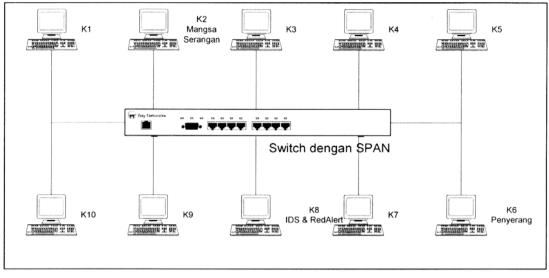
subnet yang berbeza-beza bagi tujuan multicast pada beberapa LAN dan subnet.

d. *RedAlert*Multi

Agen multicast yang menerima polisi baru daripada *RedAlert*IDS. Berperanan dalam menerima, menterjemah dan menghasilkan polisi baru pada micro-*firewall*.

Sistem *RedAlert* ini bertindak menggunakan transmisi multicast bagi proses penghantaran maklumat dan pengemaskinian dilakukan pada setiap hos. Aplikasi *RedAlert*IDS berperanan menghantar polisi baru kepada setiap hos dan diterima oleh *RedAlert*Multi yang merupakan agen multicast. *RedAlert*IDS juga akan menghantar beberapa nod melalui unicast kepada subnet yang lain dan agen *RedAlert*Uni akan menerima maklumat ini, seterusnya akan menghantar semula dalam transmisi multicast kepada setiap hos dalam rangkaian (tertakluk kepada agen *RedAlert*Multi). Penghantaran maklumat adalah dianggap selamat kerana ianya disulitkan dengan kaedah penyulitan simetri dengan menggunakan satu kata kunci yang boleh berubah mengikut pentadbir.

Senario operasi dalam tindakan *RedAlert* adalah seperti digambarkan.



Rajah 4.1 : Konfigurasi ringkas rekabentuk rangkaian sistem RedAlert

Konfigurasi di atas adalah seperti berikut :

1. K1-K10 diletakkan agen *RedAlert*Multi dan juga *firewall* (micro-*firewall*).
2. K2 – Mangsa serangan.
3. K6 – Penyerang atau penceroboh.
4. K8 – Aplikasi Snort IDS dan *RedAlert*.
5. Cisco Catalyst 2900XL/3500 XL Switch dengan Switched Port Analyzer (SPAN).

K6 cuba melakukan serangan ke atas K2. K6 melakukan imbasan port pada K2 kerana ingin melihat port yang boleh diceroboh. K8 memantau setiap paket yang melalui switch tersebut menggunakan SPAN. K8 mendapati K6 cuba untuk menyerang K2 tetapi masih belum menyerang. Bentuk serangan belum pasti cuma imbasan port mungkin permulaan serangan. K2 tidak mengetahui K6 melakukan imbasan. K8 mengesan dan menganggap K6 cuba melakukan serangan. K8 membuat polisi baru yang menghalang K6 dari