	YAYASAN PANCA MARGA UNIVERSITAS PANCA MARGA PROBOLINGGO Jalan Yos Sudarso Pabean Dringu Probolinggo 67271			
	STANDART OPERASIONAL PROSEDUR STANDART PTIK **KEAMANAN JARINGAN**			
No. Dokumen: LPMI UPM-13.3-QA/III/2017	Tanggal Pembuatan: 1 Februari 2017	Tanggal Revisi: 1 Maret 2017	Tanggal Implementasi: 6 Maret 2017	Disahkan Oleh : LPMI UPM

1. TUJUAN

Operasional prosedur ini bertujuan untuk memberikan penjelasan mengenai implementasi keamanan jaringan dan firewall untuk menerapkan kebijakan keamanan sistem jaringan pada Universitas Panca Marga. Ini biasanya terjadi setelah penilaian risiko dari sistem secara keseluruhan dilakukan.

2. RUANG LINGKUP

Manual prosedur ini sebagai pedoman penentuan kebijakan keamanan sistem jaringan.

3. DEFINISI

Firewall adalah merupakan sebuah mekanisme pengamanan yang dilakukan dengan cara melakukan kegiatan penyaringan (filtering) paket data yang masuk dan keluar jaringan.Hanya paket yang diijinkan saja yang diperbolehkan melewati firewall untuk menjangkau jaringan tertentu. Firewall dapat berupa perangkat lunak atau perangkat keras yang ditanam perangkat lunak untuk dapat menyaring paket data.

4. PERINGATAN

- Pelaksana tugas bertanggung jawab atas pelaksanaan aktivitas yang telah dibakukan dan ditetapkan.
- Segala bentuk penyimpangan atas mutu baku terkait perlengkapan, waktu maupun output dikategorikan sebagai bentuk kegagalan yang harus dipertanggungjawabkan oleh pelaksana tugas.

5. REFERENSI

Buku pedoman UPM 2016

6. PIHAK YANG TERLIBAT

- Dosen
- Pegawai
- BEM
- UPT/PTIK
- Fakultas
- Program Studi
- Laboratorium
- Tim

PTIK

7. KELEMBAGAAN

Pejabat yang bertanggung jawab memfasilitasi dan mengelola sistem keamanan jaringan.

8. PROSEDUR

Perencanaan dan implementasi firewall dilakukan melalui pendekatan bertahap. Perencanaan firewall dan tahapan pelaksanaannya terdiri dari:

a. Perencanaan, tahap dimana organisasi menentukan firewall yang akan diterapkan dalam menetapkan kebijakan keamanan organisasi.
b. Konfigurasi, tahap instalasi perangkat keras maupun perangkat lunak firewall serta menyiapkan aturan untuk sistem.
c. Pengujian, tahap pengujian yang berfungsi untuk mengevaluasi fungsionalitas, kinerja, skalabilitas dan keamanan dan mengidentifikasi masalah
d. Deployment, tahap penerapan firewall yang telah dikonfigurasi dan melalui tahap pengujian.
e. Pengelolaan, tahapan ini dilakukan selama siklus hidup dari firewall ini, mencakup kegiatan perawatan komponen dan dukungan terhadap masalah operasional.

Perencanaan

Tahap perencanaan untuk memilih dan mengimplementasikan firewall harus dimulai hanya setelah sebuah organisasi telah menetapkan bahwa firewall diperlukan untuk menegakkan kebijakan keamanan organisasi. Ini biasanya terjadi setelah penilaian risiko dari sistem secara keseluruhan dilakukan. Sebuah penilaian risiko meliputi:

a. identifikasi ancaman dan kerentanan dalam sistem informasi,
b. dampak potensial atau besarnya bahaya bahwa hilangnya kerahasiaan, integritas

ketersediaan, atau akan memiliki aset organisasi atau operasi (termasuk misi, fungsi, Citra, atau reputasi) ketika terjadi eksploitasi ancaman kerentanan diidentifikasi

c. identifikasi dan analisis kontrol keamanan untuk system informasi.

Prinsip dasar bahwa organisasi harus mengikuti dalam perencanaan penyebaran firewall meliputi:

Gunakan perangkat sesuai dengan fungsinya. Firewall jangan diimplementasikan pada perangkat yang bukan dimaksudkan untuk firewall. Sebagai contoh perangkat router disediakan untuk menangani fungsi routing, seharusnya router tidak dimanfaatkan untuk melakukan kegiatan filtering yang kompleks. Firewall tidak digunakan untuk menyediakan layanan-layanan lain seperti web server atau mail server.

Terapkan sistem pengamanan berlapis, dengan demikian resiko dapat dikelola dengan lebih baik. Firewall dapat dipasang di beberapa tempat (perimeter, pada bagian yang memiliki data sensitive, dan pada masing-masing computer pengguna). Firewall juga harus menjadi bagian dari program keamanan secara keseluruhan yang juga mencakup produk seperti antimalware dan software intrusion detection.

Perhatikan ancaman internal. Ancaman ini mungkin tidak datang langsung dari orang dalam, tetapi dapat melibatkan host internal terinfeksi oleh malware atau dikompromikan oleh penyerang eksternal. Sistem internal penting harus ditempatkan di belakang firewall internal. Dokumentasikan kemampuan firewall. Setiap jenis firewall memiliki kemampuan dan keterbatasan yang berbeda. Ini kadang-kadang akan mempengaruhi perencanaan kebijakan keamanan organisasi dan strategi penerapan firewall. Setiap fitur yang positif atau negatif mempengaruhi perencanaan ini harus ditulis ke dalam dokumen perencanaan secara keseluruhan.

Beberapa pertimbangan yang perlu dilakukan dalam memilih solusi firewall, antara lain :

Kemampuan

a. Wilayah organisasi mana yang perlu dilindungi ? (perimeter, departemen internal, host dsb)
b. Jenis teknologi firewall mana yang sesuai untuk digunakan untuk melindungi ? (packet filtering, inspeksi stateful, gateway application proxy, dsb)
c. Fitur keamanan tambahan apa yang dimiliki oleh firewall ? (content filtering, VPN, IDS)

Pengelolaan

a. Protokol apa yang digunakan untuk mendukung pengelolaan secara remote terhadap firewall, seperti HTTPS, SSH ? Apakah penggunaan protokol remote terhadap firewall diijinkan dan sesuai dengan kebijakan organisasi?
b. Apakah pengelolaan secara remote dibatasi pada interface firewall dan alamat IP sumber tertentu ?

Kinerja

a. Berapa jumlah maksimum koneksi simultan, throughput yang disupport oleh firewall ?
b. Apakah kebutuhan load balancing dan fail over terhadap firewall diperlukan ?
c. Apakah menggunakan firewall berbasis software atau berbasis hardware ?

Integrasi

a. Apakah ketika firewall terpasang, diperlukan perubahan pada area lain di jaringan ?
b. Apakah sistem logging firewall dapat saling beroperasi dengan sistem log yang sudah tersedia ?
c. Apakah firewall harus kompatibel dengan perangkat lain pada jaringan yang menyediakan sistem keamanan atau layanan lain?

Lingkungan Fisik

a. Di mana firewall secara fisik ditempatkan untuk memastikan keamanan fisik dan perlindungan dari bencana?
b. Apakah ada rak yang memadai atau ruang rak di lokasi fisik di mana firewall akan ditempatkan?
c. Apakah daya tambahan, daya cadangan, AC, dan / atau koneksi jaringan dibutuhkan pada lokasi fisik?

Personil

Apakah sistem administrator membutuhkan pelatihan sebelum firewall ini digunakan?

Kebutuhan Masa Depan

Apakah firewall memenuhi kebutuhan masa depan organisasi?

Konfigurasi Firewall

Tahap konfigurasi melibatkan semua aspek konfigurasi platform firewall. Ini termasuk instalasi perangkat keras dan perangkat lunak, mengkonfigurasi kebijakan, mengkonfigurasi logging dan alert, serta mengintegrasikan firewall ke dalam arsitektur jaringan.

Instalasi Hardware dan Software

a. Setelah firewall dipilih dan tersedia, perangkat keras, sistem operasi dan software firewall harus diinstall.
b. Sebelum software diinstall dan setelah sistem operasi diinstall, sistem operasi perlu diperkuat dengan menginstall patch yang terbaru. Kemudian install software firewall.
c. Berikutnya, sistem firewall perlu dipatch atau diupdate jika vendor menyediakan patch atau pun update dari software firewall tersebut. Hal ini dilakukan baik terhadap firewall jenis hardware maupun firewall berbasis software.
d. Selama proses instalasi dan konfigurasi, hanya administrator yang diijinkan untk mengelola firewall. Semua layanan manajemen untuk firewall, seperti SNMP harus dinonaktifkan secara permanen kecuali diperlukan.
e. Jika firewall memiliki fitur management user, sebaiknya dibuatkan beberapa account untuk personel-personil yang bertanggungjawab mengelola firewall.
f. Firewall jaringan harus ditempatkan di ruangan yang memenuhi persyaratan yang

direkomendasikan. Ruangan yang digunakan secara fisik harus aman untuk mencegah personil yang tidak memiliki hak untuk mengakses firewall

g. Sebaiknya jam internal firewall harus konsisten dengan semua sistem lainnya yang digunakan oleh sebuah organisasi. Hal tersebut dapat dilakukan dengan memanfaatkan sistem NTP server untuk melakukan sinkronisasi dengan sumber waktu otoritatif. Hal ini diperuntukan untuk membandingkan log dari beberapa sistem ketika menganalisis masalah.

Kebijakan Konfigurasi

Setelah perangkat keras dan perangkat lunak yang telah terinstal, administrator dapat membuat kebijakan firewall. Beberapa firewall menerapkan kebijakan melalui aturan eksplisit; beberapa firewall memerlukan mengkonfigurasi pengaturan firewall yang kemudian membuat aturan internal, beberapa firewall membuat kebijakan dan aturan secara otomatis dan ada pula yang menggunakan kombinasi dari ketiga jenis konfigurasi. Hasil akhirnya adalah seperangkat aturan yang disebut ruleset yang menggambarkan bagaimana firewall bertindak. Beberapa vendor memiliki batasan atau saran pada urutan aturan dalam sebuah ruleset. Sementara itu adalah umum untuk memikirkan aturan firewall yang mempengaruhi lalu lintas yang muncul pada antarmuka internal atau eksternal. Untuk membuat ruleset, pertama kali harus ditentukan apa jenis lalu lintas (protokol, alamat sumber dan tujuan, dll) yang dibutuhkan oleh aplikasi disetujui untuk organisasi.

Minimal, aturan yang seharusnya didefinisikan adalah :

a. Port filtering harus diaktifkan di tepi luar jaringan dan di dalam jaringan juga jika diperlukan.
b. Penyaringan konten harus dilakukan sedekat mungkin dengan penerima konten.

Jika menerapkan beberapa firewall perlu memiliki aturan yang sama, aturan-aturan tersebut seharusnya disinkronisasi antar firewall. Hal tersebut biasanya tergantung fitur yang dimiliki oleh firewall.

Konfigurasi sistem pencatatan dan alert

Langkah selanjutnya dalam proses konfigurasi adalah untuk mengatur sistem pencatatan dan alert. Logging adalah langkah penting dalam mencegah dan pemulihan dari kegagalan serta memastikan bahwa konfigurasi keamanan yang tepat diatur pada firewall. Logging yang tepat juga dapat memberikan informasi penting untuk merespon insiden keamanan. Bila mungkin, firewall harus dikonfigurasi baik untuk menyimpan log secara lokal maupun secara terpusat. Keterbatasan sumber daya, kemampuan firewall logging, dan situasi lain dapat mengganggu kemampuan untuk menyimpan log baik lokal maupun terpusat.

Tentukan log apa dan berapa lama log dipelihara, harus dilakukan berdasarkan kasus per kasus. Selain mengkonfigurasi logging, real-time alert juga harus dibentuk untuk memberitahu administrator ketika peristiwa penting terjadi pada firewall. Pemberitahuan dilakukan ketika:

a. Modifikasi atau penghentian aturan firewall

b. Sistem reboot, kekurangan disk, dan peristiwa operasional lainnya

Pengujian

Firewall baru harus diuji dan dievaluasi sebelum di pasang ke jaringan produksi untuk memastikan bahwa mereka bekerja dengan benar. Pengujian harus dilakukan pada jaringan uji tanpa konektivitas ke jaringan produksi. Aspek-aspek yang perlu dievaluasi meliputi:

a. Konektivitas, pengguna dapat membentuk dan memelihara koneksi melalui firewall. Ruleset, Lalu Lintas yang secara khusus diizinkan oleh kebijakan keamanan diperbolehkan. Semua lalu lintas yang tidak diperbolehkan oleh kebijakan keamanan diblokir. Verifikasi ruleset harus mencakup baik meninjau secara manual dan menguji apakah aturan bekerja seperti yang diharapkan. Kompatibilitas Aplikasi, penerapan firewall tidak mengganggu penggunaan aplikasi perangkat lunak yang ada.
b. Manajemen, Administrator dapat mengkonfigurasi dan mengelola solusi efektif dan aman. Logging sesuai dengan kebijakan organisasi dan strategi.
c. Kinerja, memberikan kinerja yang memadai selama pemakaian normal dan puncak. Dalam banyak kasus, cara terbaik untuk menguji kinerja di bawah beban dari implementasi prototipe adalah dengan menggunakan generator lalu lintas simulasi pada jaringan uji coba untuk meniru karakteristik aktual dari lalu lintas yang diharapkan semaksimal mungkin. Simulasi beban yang disebabkan oleh serangan DoS juga dapat membantu dalam menilai kinerja firewall. Pengujian harus menggabungkan berbagai aplikasi yang akan melintasi firewall, terutama yang kemungkinan besar akan terpengaruh oleh masalah jaringan throughput atau latency.
d. Keamanan, implementasi firewall itu sendiri mungkin berisi kerentanan dan kelemahan yang penyerang bisa mengeksploitasi. Organisasi dengan kebutuhan keamanan yang tinggi mungkin ingin melakukan penilaian kerentanan terhadap komponen firewall.

Deployment

Sebelum memasangkan firewall pada jaringan, administrator harus memberitahu pengguna atau pemilik sistem yang berpotensi terkena dampak dari pemasangan firewall yang direncanakan, dan memerintahkan mereka yang untuk memberitahu jika mereka menemui masalah. Setiap perubahan yang diperlukan untuk peralatan lainnya juga harus dikoordinasikan sebagai bagian dari kegiatan pemasangan firewall. Kebijakan keamanan yang diungkapkan oleh konfigurasi firewall harus ditambahkan dengan kebijakan keamanan secara keseluruhan organisasi, dan perubahan yang berkelanjutan untuk konfigurasinya harus diintegrasikan dengan proses manajemen organisasi konfigurasi.

a. Jika terdiri dari beberapa firewall yang diimplementasikan, termasuk firewall pribadi atau di beberapa kantor cabang, pendekatan bertahap harus dipertimbangkan. Prototipe juga akan sangat membantu, terutama untuk mengidentifikasi dan menyelesaikan masalah kebijakan yang saling bertentangan. Ini akan memberikan administrator kesempatan untuk mengevaluasi dampak solusi firewall dan menyelesaikan masalah sebelum dipasang

dibeberapa lokasi.

b. Firewall biasanya bertindak pula sebagai router, firewall harus diintegrasikan ke dalam struktur jaringan routing. Hal ini sering berarti mengganti router yang berada pada tempat yang sama dalam topologi jaringan sebagai mana firewall sedang ditempatkan, tetapi juga dapat berarti mengubah tabel routing untuk router lain dalam jaringan organisasi untuk menangani penambahan ini router baru.

Pengelolaan

Fase terakhir dari perencanaan dan implementasi firewall adalah pengelolaan dan hal ini bersifat jangka panjang. Beberapa tindakan perawatan adalah:

a. instalasi patch untuk perangkat firewall.
b. Melakukan pembaharuan terhadap kebijakan untuk menghadapi jenis ancaman yang baru teridentifikasi.
c. Memantau kinerja firewall dan log untuk memastikan bahwa pengguna mematuhi kebijakan keamanan.
d. Melakukan pengujian periodik untuk memverifikasi bahwa aturan firewall berfungsi seperti yang diharapkan.
e. Menyimpan log.