STANDAR OPERASIONAL PROSEDUR

MANAJEMEN FIREWALL & KEAMANAN AKSES

DOKUMEN SOP	
Nomor SOP	*009/PPTIK/SOP/2024*
Tanggal Pembuatan	*15 Desember 2021*
Tanggal Revisi	*01 Desember 2024*
Tanggal Efektif	*01 Januari 2025*
Edisi/Revisi	*01*
Halaman	*1 dari 10*

UNIVERSITAS MUHAMMADIYAH MATARAM

PUSAT PENGEMBANGAN TEKNOLOGI INFORMASI DAN KOMUNIKASI (PPTIK)

Terakreditasi B

Alamat: *Jl. KH. Ahmad Dahlan No. 1, Pagesangan, Mataram, NTB 83127*
Telepon: *(0370) 633723* | **Fax:** *(0370) 633723*
Email: *pptik@ummat.ac.id* | **Website:** *https://pptik.ummat.ac.id*

LEMBAR PENGESAHAN

Jabatan	*Nama*	*Tanda Tangan*	*Tanggal*
Dibuat oleh:*Security Analyst*	.....	.....	...../...../2024
Diperiksa oleh:*Koordinator Keamanan*	.....	.....	...../...../2024
Disetujui oleh:*Kepala Bidang Keamanan*	.....	.....	...../...../2024
Disahkan oleh:*Kepala PPTIK*	.....	.....	...../...../2024

1. TUJUAN

Prosedur ini bertujuan untuk: 1. Menyediakan framework pengelolaan firewall yang komprehensif 2. Mengamankan jaringan dari ancaman siber internal dan eksternal 3. Mengimplementasikan defense-in-depth strategy 4. Memastikan compliance dengan regulasi keamanan 5. Memfasilitasi audit trail dan forensik

2. RUANG LINGKUP

SOP ini mencakup: - Konfigurasi dan manajemen firewall perimeter dan internal - Pengelolaan security zones dan policy - Intrusion Detection/Prevention System (IDS/IPS) - Web Application Firewall (WAF) - VPN management - Security monitoring dan log analysis - Incident response terkait firewall

3. DEFINISI

Istilah	*Definisi*
Firewall	*Sistem keamanan yang mengontrol lalu lintas berdasarkan security rules*
NGFW	*Next-Generation Firewall dengan fitur advanced (DPI, IPS, App Control)*
ACL	*Access Control List, daftar aturan akses*
DMZ	*Demilitarized Zone, zona buffer antara internal dan external*
IDS/IPS	*Intrusion Detection/Prevention System*
WAF	*Web Application Firewall untuk proteksi aplikasi web*
VPN	*Virtual Private Network untuk akses remote yang aman*
DPI	*Deep Packet Inspection, analisis konten paket data*

4. REFERENSI

1. *UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016 tentang ITE*
2. *UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi*
3. *PP No. 71 Tahun 2019 tentang PSTE*
4. *ISO/IEC 27001:2022 tentang ISMS*
5. *NIST Cybersecurity Framework*
6. *CIS Controls v8*
7. *Kebijakan Keamanan Informasi PPTIK*

5. PENANGGUNG JAWAB

No	*Jabatan*	*Tanggung Jawab*
1	*Kepala PPTIK*	*Approval kebijakan strategis*

No	Jabatan	Tanggung Jawab
2	Kepala Bidang Keamanan	Oversight keamanan
3	Koordinator Keamanan	Perencanaan dan review
4	Security Analyst	Implementasi dan monitoring
5	Network Administrator	Support konfigurasi
6	SOC Operator	Monitoring 24/7

6. ARSITEKTUR KEAMANAN

6.1 Security Zones

Zone	Deskripsi	Trust Level
UNTRUST	Internet/External	0 (Lowest)
DMZ	Server publik (Web, Mail)	25
INTERNAL	Jaringan internal kampus	75
TRUSTED	Server internal, Database	100 (Highest)

6.2 Firewall Layers

Layer	Type	Function
Perimeter	NGFW	Internet gateway, first line defense
DMZ	Firewall	Protect public-facing servers
Internal	Firewall/ACL	Segmentasi antar VLAN
Application	WAF	Protect web applications
Endpoint	Host Firewall	Per-device protection

7. PROSEDUR

7.1 Permintaan Rule Firewall Baru

No	Aktivitas	Pelaksana	Waktu	Output	Dokumen
1	Submit request dengan justifikasi bisnis	Pemohon	-	Request Form	FM_NET_030
2	Review security implications	Security Analyst	1 hari	Security Review	FM_NET_030
3	Risk assessment	Security Analyst	1 hari	Risk Score	FM_NET_031
4	Approval berdasarkan risk level	Approval Matrix	1-3 hari	Approval	FM_NET_030
5	Design rule configuration	Security Analyst	1 hari	Rule Design	FM_NET_032
6	Peer review	Coordinator	1 hari	Peer Review	FM_NET_032

No	Aktivitas	Pelaksana	Waktu	Output	Dokumen
	konfigurasi				
7	Implement di test environment	Security Analyst	1 hari	Test Config	-
8	Testing dan validation	Security Analyst	1 hari	Test Result	FM_NET_033
9	Implement di production	Security Analyst	Scheduled	Rule Active	FM_NET_034
10	Post-implementation verification	Security Analyst	1 hari	Verification	FM_NET_034
11	Documentation dan closure	Security Analyst	1 hari	Closed	FM_NET_034

7.2 Matriks Approval Rule Firewall

Risk Level	Kategori	Approval	Timeline
Low	Standard port, internal only	Security Analyst	1 hari
Medium	External access, non-critical	Koordinator	3 hari
High	DMZ, database access	Kepala Bidang	5 hari
Critical	Any-any, sensitive data	Kepala PPTIK	7 hari

7.3 Pengelolaan Blocking/Unblocking

No	Aktivitas	Pelaksana	Waktu	Output	Dokumen
1	Request dengan alasan jelas	Pemohon	-	Request	FM_NET_035
2	Verifikasi legitimasi request	Security Analyst	30 menit	Verified	FM_NET_035
3	Check security implications	Security Analyst	30 menit	Assessment	FM_NET_035
4	Approval (sesuai kategori)	Approver	Varies	Approved	FM_NET_035
5	Implement perubahan	Security Analyst	15 menit	Changed	FM_NET_035
6	Verify dan confirm	Security Analyst	15 menit	Confirmed	FM_NET_035
7	Set expiry (temporary rules)	Security Analyst	5 menit	Timer Set	FM_NET_035

7.4 IDS/IPS Management

No	Aktivitas	Pelaksana	Frekuensi	Output	Dokumen
1	Signature update	Security Analyst	Daily/Auto	Updated	-
2	Review detected	SOC Operator	Real-time	Alert	FM_NET_036

No	Aktivitas	Pelaksana	Frekuensi	Output	Dokumen
	threats			Review	
3	Tune false positives	Security Analyst	Weekly	Tuned Rules	FM_NET_037
4	Threat intelligence integration	Security Analyst	Weekly	TI Updated	-
5	IPS policy review	Koordinator	Monthly	Policy Updated	FM_NET_038
6	Performance impact assessment	Security Analyst	Monthly	Assessment	FM_NET_038

7.5 Security Monitoring

No	Aktivitas	Pelaksana	Frekuensi	Output	Dokumen
1	Real-time monitoring dashboard	SOC Operator	24/7	Live Status	-
2	Alert triage dan response	SOC Operator	Real-time	Response	FM_NET_036
3	Log analysis dan correlation	Security Analyst	Daily	Analysis	FM_NET_039
4	Threat hunting	Security Analyst	Weekly	Hunt Report	FM_NET_040
5	Security metrics reporting	Koordinator	Monthly	Metrics	FM_NET_041
6	Compliance audit trail review	Koordinator	Quarterly	Audit Report	FM_NET_042

7.6 Firewall Rule Review

No	Aktivitas	Pelaksana	Frekuensi	Output	Dokumen
1	Identify unused/expired rules	Security Analyst	Monthly	Rule List	FM_NET_043
2	Review rule effectiveness	Security Analyst	Quarterly	Effectiveness	FM_NET_043
3	Optimize rule ordering	Security Analyst	Quarterly	Optimized	FM_NET_043
4	Cleanup deprecated rules	Security Analyst	Quarterly	Cleaned	FM_NET_043

No	Aktivitas	Pelaksana	Frekuensi	Output	Dokumen
5	Comprehensive policy review	Koordinator	Annual	Policy Review	FM_NET_044
6	External security audit	External Auditor	Annual	Audit Report	-

7.7 VPN Management

No	Aktivitas	Pelaksana	Waktu	Output	Dokumen
1	VPN access request	Pemohon	-	Request	FM_NET_045
2	Verify identity dan need	Security Analyst	1 hari	Verified	FM_NET_045
3	Approval (sesuai level)	Approver	1-3 hari	Approved	FM_NET_045
4	Create VPN account	Security Analyst	1 hari	Account	FM_NET_045
5	Configure access restrictions	Security Analyst	1 hari	Restricted	FM_NET_045
6	Issue credentials securely	Security Analyst	1 hari	Credential	FM_NET_045
7	User acknowledgement	User	1 hari	Signed	FM_NET_046
8	Periodic access review	Security Analyst	Quarterly	Review	FM_NET_047

8. KEBIJAKAN FIREWALL

8.1 Default Policies

Zone Transition	Default Action	Exception
UNTRUST → Any	DENY	Explicit allow only
DMZ → INTERNAL	DENY	Specific service only
INTERNAL → DMZ	ALLOW	Logged
INTERNAL → UNTRUST	ALLOW	Content filtered
Any → TRUSTED	DENY	Strict approval only

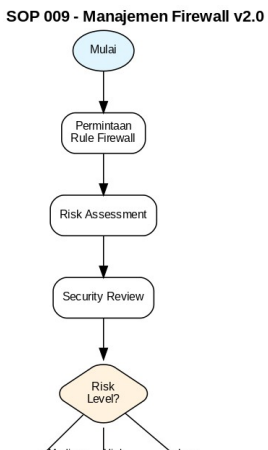
8.2 Prohibited Actions

1. **Any-Any Rules**: *Dilarang tanpa approval Kepala PPTIK*
2. **Default Allow**: *Semua zona harus default deny*
3. **Permanent Exceptions**: *Max 1 tahun, harus direview*
4. **Unencrypted Access**: *Dilarang untuk data sensitif*

9. KEY PERFORMANCE INDICATORS

KPI	*Target*	*Pengukuran*
Rule Review Compliance	*100%*	*Quarterly*
False Positive Rate	*< 5%*	*Monthly*
Rule Processing Time	*< 5 hari*	*Per request*
Security Incident from Firewall Gap	*0*	*Annual*
Audit Compliance	*100%*	*Annual*

10. FLOWCHART



11. DOKUMEN TERKAIT

Kode	*Nama Form*	*Fungsi*
FM_NET_030	*Form Permintaan Rule Firewall*	*Request rule baru*
FM_NET_031	*Form Risk Assessment Firewall*	*Penilaian risiko*
FM_NET_032	*Form Rule Design & Peer Review*	*Desain konfigurasi*
FM_NET_033	*Form Testing Result*	*Hasil testing*

Kode	Nama Form	Fungsi
FM_NET_034	Form Implementation Log	Log implementasi
FM_NET_035	Form Blocking/Unblocking Request	Request blokir
FM_NET_036	Form Alert Triage	Triase alert
FM_NET_037	Form False Positive Tuning	Tuning FP
FM_NET_038	Form IPS Policy Review	Review IPS
FM_NET_039	Form Log Analysis Report	Analisis log
FM_NET_040	Form Threat Hunting Report	Laporan threat hunting
FM_NET_041	Form Security Metrics	Metrik keamanan
FM_NET_042	Form Compliance Audit Trail	Audit trail
FM_NET_043	Form Rule Review Worksheet	Review rule
FM_NET_044	Form Annual Policy Review	Review tahunan
FM_NET_045	Form VPN Access Request	Request VPN
FM_NET_046	Form VPN User Agreement	Agreement user
FM_NET_047	Form VPN Access Review	Review akses VPN

12. CATATAN REVISI

Revisi	Tanggal	Uraian Perubahan	Oleh
00	15/12/2021	Dokumen awal	Tim PPTIK
01	01/12/2024	Penambahan: NGFW, IDS/IPS, WAF, VPN management, security zones, risk assessment, threat hunting, compliance audit, KPI	Tim PPTIK