SOP Pengelolaan Firewall dan Keamanan Jaringan

1. Tujuan
Menetapkan prosedur pengelolaan, pengawasan, dan pemeliharaan sistem keamanan jaringan kampus, termasuk konfigurasi firewall, WAF, dan mekanisme perlindungan server terhadap ancaman siber.

2. Ruang Lingkup
SOP ini berlaku untuk seluruh server dan layanan jaringan kampus yang dikelola oleh unit STK, meliputi:

- Web server kampus (termasuk VPS Centminmod)
- Database server eksternal
- Infrastruktur jaringan (LAN/WAN/Wi-Fi)
- Akses antar sistem internal dan public
-

3. Definisi

- WAF (Web Application Firewall): Firewall di level provider yang melindungi aplikasi web dari serangan seperti SQL injection, XSS, dan DDoS.
- CSF (ConfigServer Security & Firewall): Sistem firewall berbasis iptables yang diintegrasikan dalam Centminmod untuk pengaturan keamanan server.
- Port filtering: Pembatasan akses port berdasarkan kebijakan keamanan.
- Whitelist / Blacklist: Daftar IP yang diizinkan atau ditolak untuk mengakses sistem.

4. Prosedur
A. Lapisan 1 – WAF Provider

1. Konfigurasi Awal
    - Pastikan domain dan subdomain yang dilindungi sudah terhubung ke WAF provider.
    - Terapkan kebijakan keamanan standar:
        - Proteksi DDoS aktif
        - Rate limiting untuk permintaan HTTP
        - Block otomatis untuk serangan SQLi dan XSS
    - Gunakan mode “Full SSL (Strict)” untuk komunikasi HTTPS aman.
2. Monitoring
    - Pantau dashboard WAF secara berkala.
    - Jika ada insiden (misalnya IP diblokir karena serangan), catat ke log keamanan mingguan.
3. Penanganan Insiden
    - Bila WAF mendeteksi serangan berulang, lakukan:
        - Validasi sumber trafik
        - Jika serangan berasal dari IP spesifik, tambahkan ke daftar block permanen (via WAF dashboard)
    - Laporkan ke admin jaringan utama jika diperlukan.

B. Lapisan 2 – CSF (Server Level)

1. Konfigurasi Dasar
    - Aktifkan CSF bawaan Centminmod:
    - csf -e
    - Tutup semua port yang tidak diperlukan.
    - Buka hanya port penting:
        - 22 (SSH) — gunakan key pair dan ubah port default jika memungkinkan
        - 80 (HTTP)
        - 443 (HTTPS)
        - 25/465/587 (jika diperlukan untuk SMTP)
2. Whitelist IP Admin
    - Tambahkan IP admin ke whitelist di /etc/csf/csf.allow
    - echo "123.123.123.123 # Admin Office IP" >> /etc/csf/csf.allow
    - csf -r
3. Blacklist IP Penyerang
    - Jika ada IP mencurigakan, tambahkan ke blacklist:
    - csf -d 45.67.89.101 "Attempted Brute Force"
4. Rate Limit dan Flood Protection
    - Aktifkan modul LF_DAEMON untuk mendeteksi serangan login SSH, FTP, SMTP.
    - Pastikan parameter CONNLIMIT diset untuk mencegah flood connection.
5. Audit dan Update Berkala
    - Audit konfigurasi CSF minimal setiap bulan.
    - Pastikan Centminmod dan CSF dalam versi terbaru.

C. Integrasi dan Monitoring

1. Integrasi Keamanan Terpadu
    - Semua insiden firewall dan WAF dicatat dalam log keamanan harian.
    - Log dikumpulkan ke dashboard pemantauan insiden STK.
2. Monitoring Publik
    - Status jaringan publik dan server dapat dipantau melalui
      👉 https://usscampus.instatus.com/
3. Backup Konfigurasi Keamanan
    - Backup file konfigurasi CSF dan log keamanan menggunakan Restic bersama backup sistem VPS rutin.

5. Tanggung Jawab

Pihak	Tugas
Admin Jaringan	Mengelola konfigurasi WAF dan CSF, memantau trafik, serta melakukan pembaruan.
SysAdmin Server	Menjalankan audit sistem, memperbarui Centminmod, serta menjaga keamanan SSH.
Kepala STK	Mengesahkan kebijakan firewall dan keamanan jaringan serta meninjau laporan bulanan.

6. Dokumentasi dan Review
   - Semua perubahan konfigurasi dicatat dalam Log Perubahan Keamanan (Security Change Log).
   - Review SOP dilakukan setiap 6 bulan atau setelah ada insiden besar.