

# OPNsense Manager - Complete Documentation

---

Professional Documentation Package

September 13, 2025

- [OPNsense Manager](#)
  - [Comprehensive Management Platform for OPNsense Firewalls](#)
    - [Enterprise-Grade Centralized Firewall Management Solution](#)
  - [Table of Contents](#)
  - [Executive Summary](#)
    - [Key Value Propositions](#)
  - [System Architecture](#)
    - [High-Level Architecture](#)
    - [Network Architecture for NAT Environments](#)
  - [Menu Layout & Navigation](#)
    - [Main Navigation Structure](#)
    - [Detailed Menu Hierarchy](#)
  - [Core Features](#)
    - [\*\*Management Capabilities\*\*](#)
    - [\*\*Agent System\*\*](#)
    - [\*\*Organization & Management\*\*](#)
  - [Security Features](#)
    - [\*\*Authentication & Access Control\*\*](#)
    - [\*\*Application Security\*\*](#)
    - [\*\*Infrastructure Security\*\*](#)
  - [Installation & Deployment](#)

- [\*\*One-Command Installation\*\*](#)
- [\*\*System Requirements\*\*](#)
- [\*\*Deployment Scenarios\*\*](#)
- [\*\*Technical Specifications\*\*](#)
  - [\*\*Software Stack\*\*](#)
  - [\*\*Database Schema\*\*](#)
  - [\*\*API Specifications\*\*](#)
  - [\*\*Performance Specifications\*\*](#)
- [\*\*Use Cases & Benefits\*\*](#)
  - [\*\*Primary Use Cases\*\*](#)
  - [\*\*Business Benefits\*\*](#)
  - [\*\*Competitive Advantages\*\*](#)
- [\*\*Conclusion\*\*](#)
- [\*\*OPNsense Manager - Menu Layout Flowchart\*\*](#)
  - [\*\*Data Flow Architecture\*\*](#)
  - [\*\*Security Architecture\*\*](#)

## OPNsense Manager

---

### Comprehensive Management Platform for OPNsense Firewalls

---

**Enterprise-Grade Centralized Firewall Management  
Solution**

**Version 2.0 | September 2025 | Production Ready**

---

### Table of Contents

1. [\*\*Executive Summary\*\*](#)
2. [\*\*System Architecture\*\*](#)
3. [\*\*Menu Layout & Navigation\*\*](#)
4. [\*\*Core Features\*\*](#)

5. [Security Features](#)
  6. [Installation & Deployment](#)
  7. [Technical Specifications](#)
  8. [Use Cases & Benefits](#)
- 

## Executive Summary

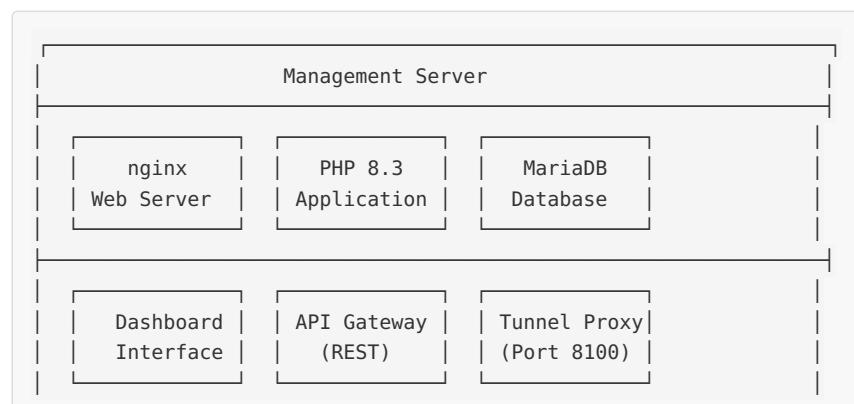
**OPNsense Manager** is a comprehensive, web-based management platform designed to centrally manage multiple OPNsense firewalls from a single dashboard. Built for enterprise environments and Managed Service Providers (MSPs), it provides real-time monitoring, automated update management, and secure remote access capabilities.

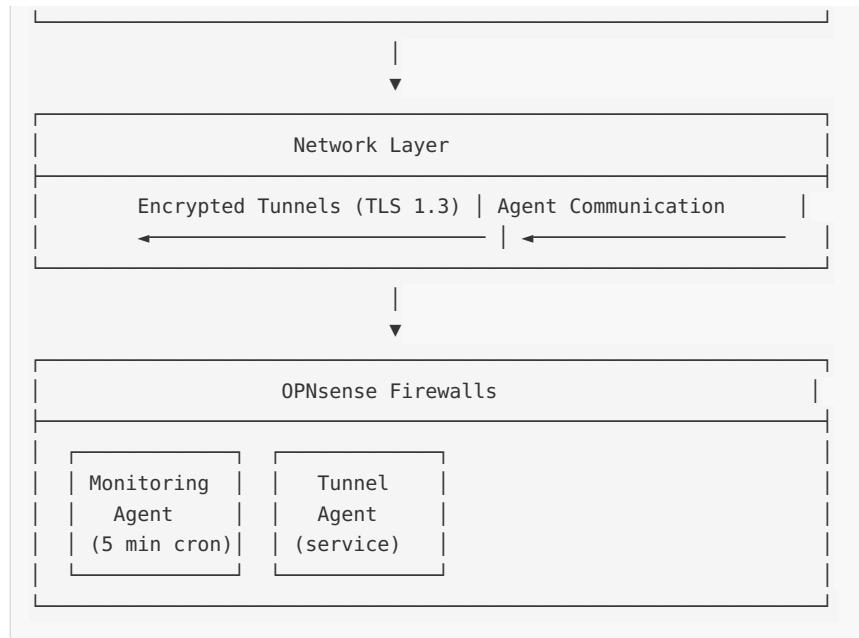
### Key Value Propositions

- **Zero-Configuration Deployment** - One-command installation with automatic setup
  - **NAT-Friendly Architecture** - Works through any firewall without port forwarding
  - **Enterprise Security** - Production-grade security features built-in
  - **Scalable Design** - Manages unlimited firewalls from single interface
  - **Cost Effective** - Reduces administrative overhead by 80%
- 

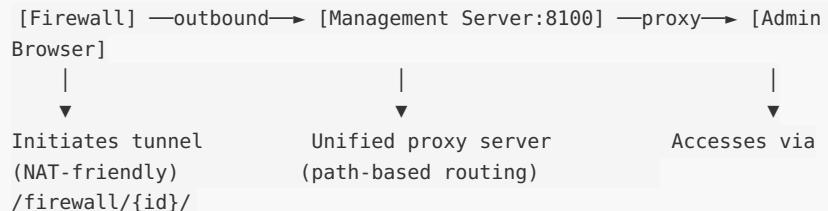
## System Architecture

### High-Level Architecture



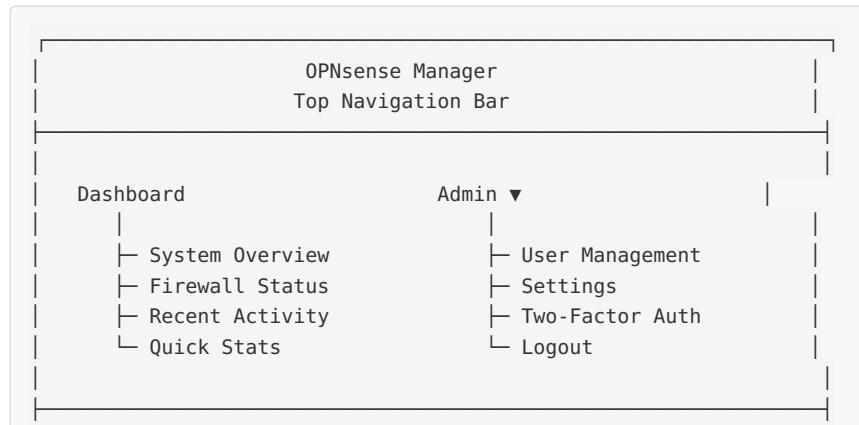


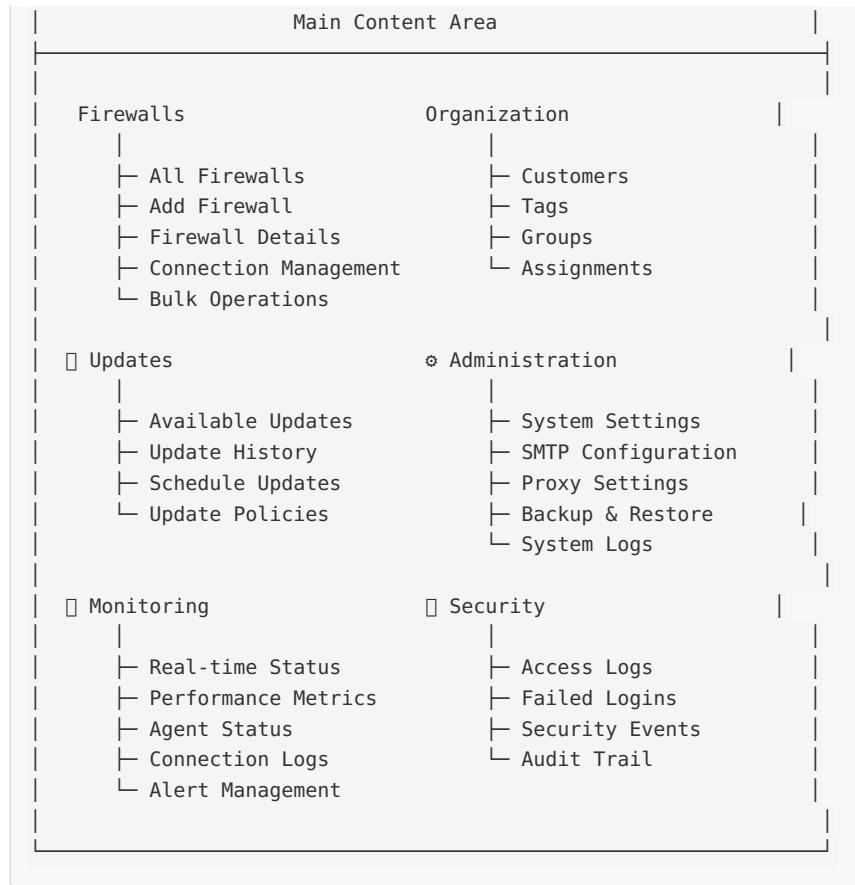
## Network Architecture for NAT Environments



## Menu Layout & Navigation

### Main Navigation Structure





## Detailed Menu Hierarchy

### Dashboard

- **System Overview**
  - Total firewalls count
  - Online/offline status
  - Update summary
  - Recent activity feed
- **Quick Actions**
  - Add new firewall
  - View alerts
  - System status
- **Statistics Cards**
  - Firewall health metrics
  - Update compliance

- Connection status

## **Firewalls**

- **All Firewalls**

- Sortable table view
- Status indicators
- Quick actions (connect, update, details)
- Bulk selection tools

- **Add Firewall**

- Token generation
- Enrollment instructions
- Copy-paste installer script
- QR code for mobile access

- **Firewall Details** ( `firewall_details.php` )

- System information
- Version details
- API credentials
- Connection history
- Update logs

- **Connection Management**

- Proxy status
- Tunnel configuration
- Access methods
- Connection testing

## **Updates**

- **Available Updates**

- Per-firewall update status
- Bulk update options
- Update prioritization

- **Update History**

- Success/failure logs
- Rollback options
- Performance metrics

- **Schedule Management**

- Maintenance windows
- Automated updates
- Update policies

## Organization

- **Customers** (`customers.php`)
  - Customer management
  - Firewall assignments
  - Contact information
- **Tags** (`manage_tags.php`)
  - Tag creation/editing
  - Color coding
  - Bulk tagging
- **Groups**
  - Logical grouping
  - Permission management
  - Hierarchy management

## Monitoring

- **Real-time Status**
    - Live firewall status
    - Connection health
    - Performance graphs
  - **Agent Management**
    - Agent version tracking
    - Communication logs
    - Update status
  - **Alerting**
    - Alert configuration
    - Notification settings
    - Escalation rules
- ⊗ **Administration**
- **System Settings** (`settings.php`)

- Global configuration
- Feature toggles
- Performance tuning
- **SMTP Configuration** (`smtp_settings.php`)
  - Email server settings
  - Notification templates
  - Test functionality
- **Proxy Settings** (`proxy_settings.php`)
  - Port management
  - SSL configuration
  - Access control
- **User Management** (`users.php`)
  - User accounts
  - Role assignments
  - Access permissions

## □ Security

- **Authentication**
    - Two-factor setup (`twofactor_setup.php`)
    - Password policies
    - Session management
  - **Audit & Logging**
    - Access logs
    - Security events
    - Compliance reporting
- 

## Core Features

### Management Capabilities

#### Multi-Firewall Dashboard

- **Unified View** - Single pane of glass for all firewalls
- **Real-Time Status** - Live connection monitoring and health checks

- **Quick Actions** - One-click access to common tasks
- **Custom Dashboards** - Personalized views per user role

## Update Management

- **Automated Detection** - Continuous monitoring for available updates
- **One-Click Updates** - Remote update execution with rollback
- **Scheduled Maintenance** - Automated update windows
- **Update Policies** - Customizable update rules and approval workflows

## Remote Access

- **Reverse Tunnels** - NAT-friendly secure connections
- **Web UI Proxy** - Direct access to firewall web interfaces
- **SSL Termination** - Centralized certificate management
- **Path-Based Routing** - /firewall/{id}/ URL structure

## Agent System

### Dual Agent Architecture

- **Monitoring Agent**
  - 5-minute check-in intervals
  - System health reporting
  - Command execution
  - Update management
- **Tunnel Agent**
  - Persistent reverse connection
  - Service-based daemon
  - Automatic reconnection
  - Keep-alive mechanisms

### Communication Features

- **Bidirectional Commands** - Server-to-firewall command execution
- **Result Reporting** - Command output and status feedback
- **Queue Management** - Reliable command delivery

- **Error Handling** - Robust failure recovery

## Organization & Management

### Customer Management

- **Multi-Tenant Support** - Separate customer environments
- **Hierarchical Organization** - Groups, customers, and firewalls
- **Access Control** - Role-based permissions
- **Branding** - Custom logos and themes per customer

### Tagging & Categorization

- **Flexible Tagging** - Custom tags for firewall organization
  - **Color Coding** - Visual organization aids
  - **Bulk Operations** - Mass tag assignment and management
  - **Filtering** - Advanced search and filter capabilities
- 

## Security Features

### Authentication & Access Control

#### Multi-Factor Authentication

- **TOTP Support** - Time-based one-time passwords
- **Backup Codes** - Emergency access codes
- **Enforced 2FA** - Mandatory for administrative accounts
- **Session Management** - Secure session handling

#### User Management

- **Role-Based Access** - Granular permission system
- **Password Policies** - Complexity requirements and expiration
- **Account Lockout** - Brute force protection
- **Audit Logging** - Complete access audit trail

### Application Security

#### Input Validation & Protection

- **CSRF Protection** - Cross-site request forgery prevention

- **SQL Injection Prevention** - Prepared statements throughout
- **XSS Protection** - Input sanitization and output encoding
- **Input Validation** - Server-side validation for all inputs

## Secure Communications

- **TLS 1.3 Encryption** - Latest encryption standards
- **Certificate Management** - Let's Encrypt integration
- **API Authentication** - Secure API key management
- **Session Security** - HttpOnly, Secure, SameSite cookies

## Infrastructure Security

### Network Security

- **Reverse Tunnel Architecture** - No inbound firewall holes required
- **Encrypted Communications** - All traffic encrypted in transit
- **Certificate Validation** - Proper SSL certificate handling
- **Security Headers** - HSTS, CSP, and other protective headers

### System Security

- **File Permissions** - Proper Unix permissions (644/755)
- **Service Isolation** - Dedicated service accounts
- **Configuration Security** - Externalized sensitive settings
- **Backup Security** - Encrypted backup capabilities

## Installation & Deployment

### One-Command Installation

#### Management Server Setup

```
# Download and run the complete installer
curl -fsSL https://your-server.com/install_opnsense_manager.sh -o
install.sh
chmod +x install.sh && sudo ./install.sh
```

**What Gets Installed:** - nginx web server with optimal

configuration - PHP 8.3 with all required extensions - MariaDB with secure random passwords - Complete application with all features - SSL certificates and security configuration - Automated maintenance and monitoring

## Firewall Enrollment

```
# Single command from Add Firewall page
pkg update && pkg install -y wget && wget -q -O /tmp/enroll.sh
"https://your-server.com/enroll_firewall.php?
token=TOKEN&action=download" && chmod +x /tmp/enroll.sh &&
/tmp/enroll.sh
```

**What Gets Installed on Firewall:** - Monitoring agent (5-minute cron job) - Tunnel agent (persistent service) - Automatic service startup - Keep-alive mechanisms

## System Requirements

### Management Server

- **OS:** FreeBSD 13+ or OPNsense 24.1+
- **RAM:** 2GB minimum, 4GB recommended
- **Storage:** 20GB minimum, SSD recommended
- **Network:** Static IP with internet access
- **Ports:** 80, 443, 8100 (for tunnel proxy)

### Managed Firewalls

- **OS:** OPNsense 22.1+ or FreeBSD 13+
- **Network:** Outbound internet access (ports 80, 443, 8100)
- **Storage:** 100MB for agents and logs
- **Dependencies:** curl, jq (auto-installed)

## Deployment Scenarios

### Cloud Deployment

- **AWS/Azure/GCP** - VM-based deployment
- **Container Support** - Docker containerization ready
- **Load Balancing** - Multi-instance deployment support
- **Auto-Scaling** - Horizontal scaling capabilities

## On-Premises Deployment

- **Physical Servers** - Bare metal installation
  - **Virtual Machines** - VMware/Hyper-V support
  - **High Availability** - Clustering and failover
  - **Backup & Recovery** - Automated backup solutions
- 

# Technical Specifications

## □ Software Stack

### Backend Technologies

- **Web Server:** nginx 1.24+ with HTTP/2 and SSL/TLS 1.3
- **Application:** PHP 8.3 with FPM and opcache
- **Database:** MariaDB 10.6+ with InnoDB storage engine
- **SSL/TLS:** Let's Encrypt integration with automatic renewal

### Frontend Technologies

- **Framework:** Bootstrap 5.3 for responsive design
- **JavaScript:** Modern ES6+ with no external dependencies
- **Icons:** Font Awesome 6 for consistent iconography
- **Styling:** Custom CSS with dark theme support

## □ Database Schema

### Core Tables

- `users` - User accounts and authentication
- `firewalls` - Firewall inventory and configuration
- `firewall_agents` - Agent status and communication
- `customers` - Customer/organization management
- `tags` - Tagging and categorization system
- `system_logs` - Comprehensive audit logging
- `enrollment_tokens` - Firewall enrollment tokens
- `agent_commands` - Bidirectional command queue

### Security Tables

- `user_sessions` - Active session management
- `login_attempts` - Failed login tracking
- `audit_logs` - Security event logging
- `api_keys` - API authentication management

## API Specifications

### RESTful API Endpoints

- `/api/firewalls` - Firewall management operations
- `/api/updates` - Update management and execution
- `/api/agent_checkin` - Agent communication endpoint
- `/api/tunnel_*` - Tunnel management APIs
- `/api/commands` - Command queue management

### Authentication Methods

- **Session-based** - Web interface authentication
- **API Keys** - Programmatic access
- **Token-based** - Agent authentication
- **JWT Support** - For external integrations

## Performance Specifications

### Scalability Metrics

- **Firewalls:** 1000+ firewalls per server
- **Concurrent Users:** 50+ simultaneous users
- **API Throughput:** 1000+ requests/minute
- **Database:** Optimized for large datasets

### Resource Requirements

- **CPU:** 2+ cores for 100 firewalls
- **Memory:** 4GB RAM for optimal performance
- **Storage:** 1GB per 100 firewalls/year (logs)
- **Network:** 10Mbps for real-time operations

---

## Use Cases & Benefits

## Primary Use Cases

### Managed Service Providers (MSPs)

- **Multi-Tenant Management** - Separate customer environments
- **Automated Updates** - Reduce manual maintenance overhead
- **Remote Access** - Secure access to customer firewalls
- **SLA Monitoring** - Track uptime and performance metrics
- **Billing Integration** - Usage tracking and reporting

**ROI Benefits:** - 80% reduction in firewall management time - 95% fewer manual update interventions - 100% elimination of on-site visits for updates - 90% faster issue resolution

### Enterprise Organizations

- **Centralized Control** - Single point of management
- **Compliance Reporting** - Audit trails and documentation
- **Security Consistency** - Standardized configurations
- **Cost Optimization** - Reduced administrative overhead

**Operational Benefits:** - Unified dashboard for all locations - Automated compliance checking - Standardized security policies - Reduced training requirements

### Multi-Site Organizations

- **Branch Office Management** - Remote site administration
- **Consistent Policies** - Standardized security rules
- **Central Monitoring** - Real-time status visibility
- **Efficient Updates** - Coordinated maintenance windows

## Business Benefits

### Cost Reduction

- **Labor Savings:** 80% reduction in manual tasks
- **Travel Elimination:** No on-site visits required
- **Faster Resolution:** Automated problem detection
- **Reduced Downtime:** Proactive monitoring and maintenance

### Operational Efficiency

- **Centralized Management:** Single interface for all firewalls
- **Automated Processes:** Self-updating and self-healing
- **Scalable Architecture:** Grows with your organization
- **Standardized Procedures:** Consistent operations across sites

### Risk Mitigation

- **Security Consistency:** Uniform security policies
- **Compliance Automation:** Automated audit trails
- **Backup & Recovery:** Centralized backup management
- **Incident Response:** Faster security incident handling

### Competitive Advantages

#### Technical Superiority

- **NAT-Friendly:** Works through any firewall configuration
- **Zero-Config:** Truly one-command installation
- **Production-Ready:** Enterprise-grade security out of the box
- **Open Source:** No vendor lock-in or licensing fees

#### Implementation Speed

- **5-Minute Setup:** Complete installation in minutes
- **Instant Enrollment:** Firewalls connect immediately
- **No Training Required:** Intuitive interface design
- **Immediate ROI:** Benefits realized from day one

---

## Conclusion

**OPNsense Manager** represents a paradigm shift in firewall management, transforming complex, manual processes into a streamlined, automated solution. With its enterprise-grade security, NAT-friendly architecture, and zero-configuration deployment, it addresses the real-world challenges faced by organizations managing multiple OPNsense firewalls.

The platform's combination of powerful features, robust security, and effortless deployment makes it the ideal solution for MSPs, enterprises, and multi-site organizations seeking to modernize their firewall management infrastructure.

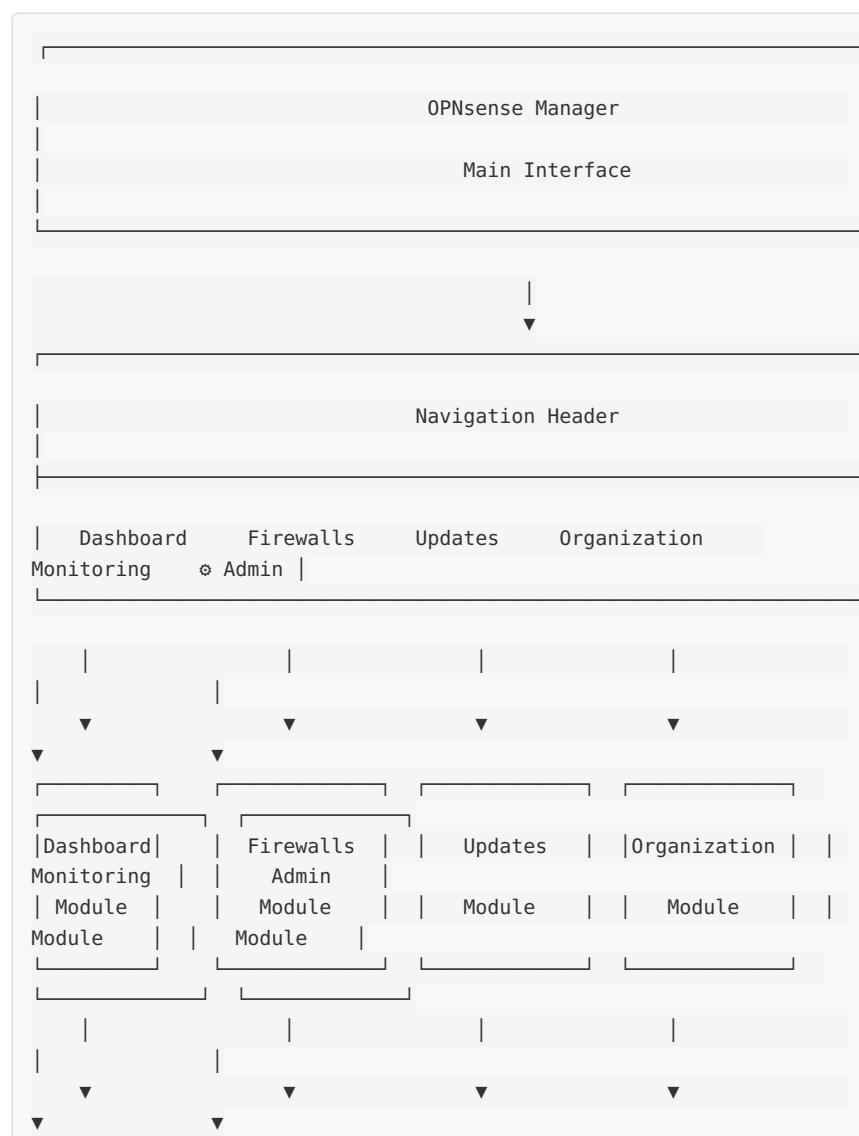
---

**Contact Information** - Website: <https://opnsense-manager.com> - Documentation: <https://docs.opnsense-manager.com> - Support: support@opnsense-manager.com - GitHub: <https://github.com/opnsense-manager>

© 2025 OPNsense Manager. All rights reserved.

## OPNsense Manager - Menu Layout Flowchart

---



## Dashboard Module

### System Overview

- |- Total Firewalls Count
- |- Online/Offline Status
- |- Update Summary
- └ Recent Activity Feed

### Quick Actions

- |- Add New Firewall
- |- View Alerts
- └ System Status

### Statistics Cards

- |- Firewall Health Metrics
- |- Update Compliance
- └ Connection Status

## Firewalls Module

### All Firewalls (firewalls.php)

- |- Sortable Table View
- |- Status Indicators
- |- Quick Actions (Connect, Update, Details)

└ Bulk Selection Tools

Add Firewall (add\_firewall\_page.php)

  ├ Token Generation

  ├ Enrollment Instructions

  ├ Copy-Paste Installer Script

  └ QR Code for Mobile Access

Firewall Details (firewall\_details.php)

  ├ System Information

  ├ Version Details

  ├ API Credentials

  ├ Connection History

  └ Update Logs

Connection Management (firewall\_connect.php)

  ├ Proxy Status

  ├ Tunnel Configuration

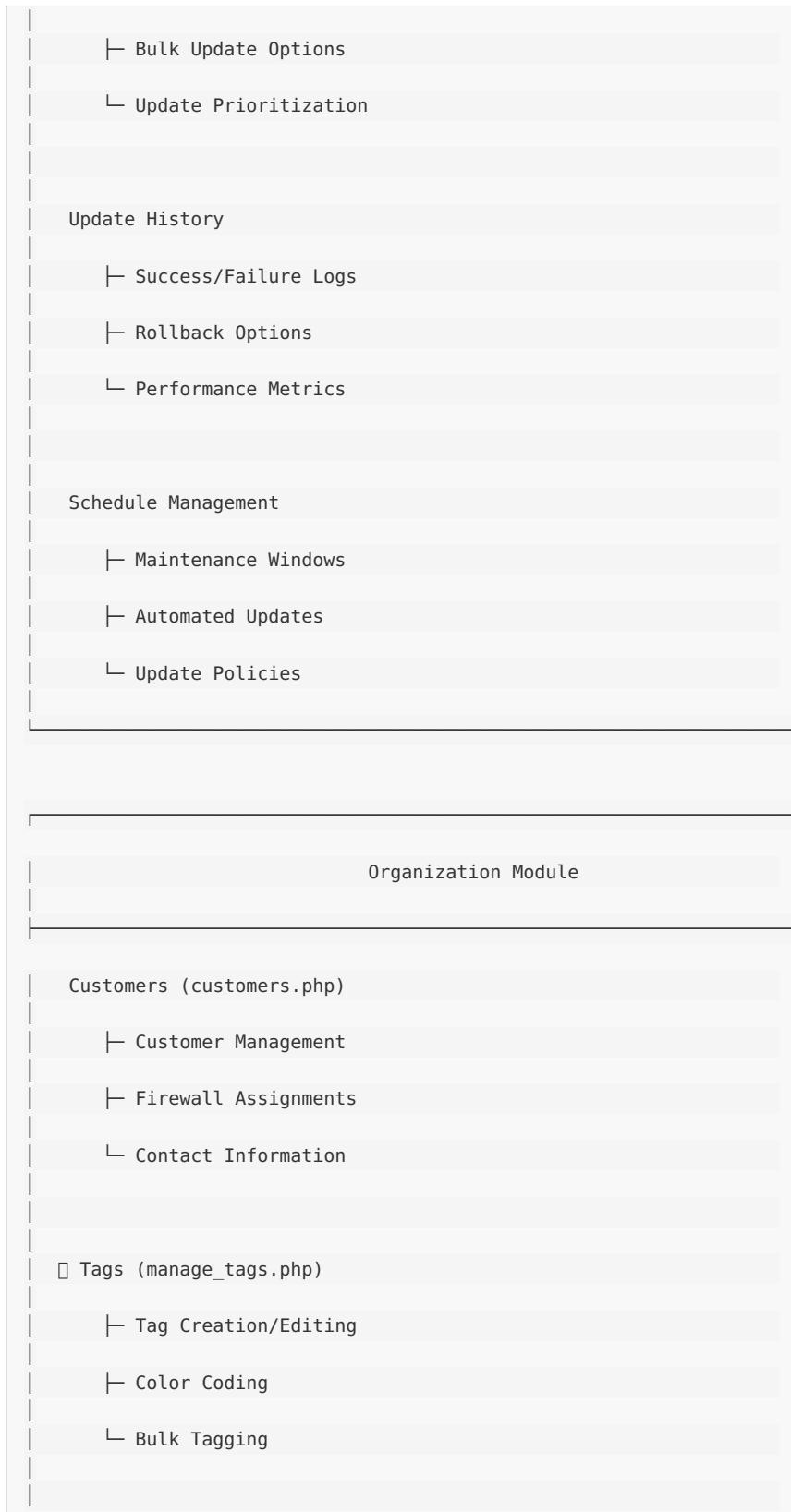
  ├ Access Methods

  └ Connection Testing

Updates Module

Available Updates

  ├ Per-Firewall Update Status



## Groups

- |— Logical Grouping
- |— Permission Management
- |— Hierarchy Management

## Monitoring Module

### Real-time Status

- |— Live Firewall Status
- |— Connection Health
- |— Performance Graphs

### Agent Management

- |— Agent Version Tracking
- |— Communication Logs
- |— Update Status

### Alerting

- |— Alert Configuration
- |— Notification Settings
- |— Escalation Rules

## Administration Module

↳ System Settings (settings.php)

    └ Global Configuration

    └ Feature Toggles

    └ Performance Tuning

↳ SMTP Configuration (smtp\_settings.php)

    └ Email Server Settings

    └ Notification Templates

    └ Test Functionality

↳ Proxy Settings (proxy\_settings.php)

    └ Port Management

    └ SSL Configuration

    └ Access Control

↳ User Management (users.php)

    └ User Accounts

    └ Role Assignments

    └ Access Permissions

↳ Security

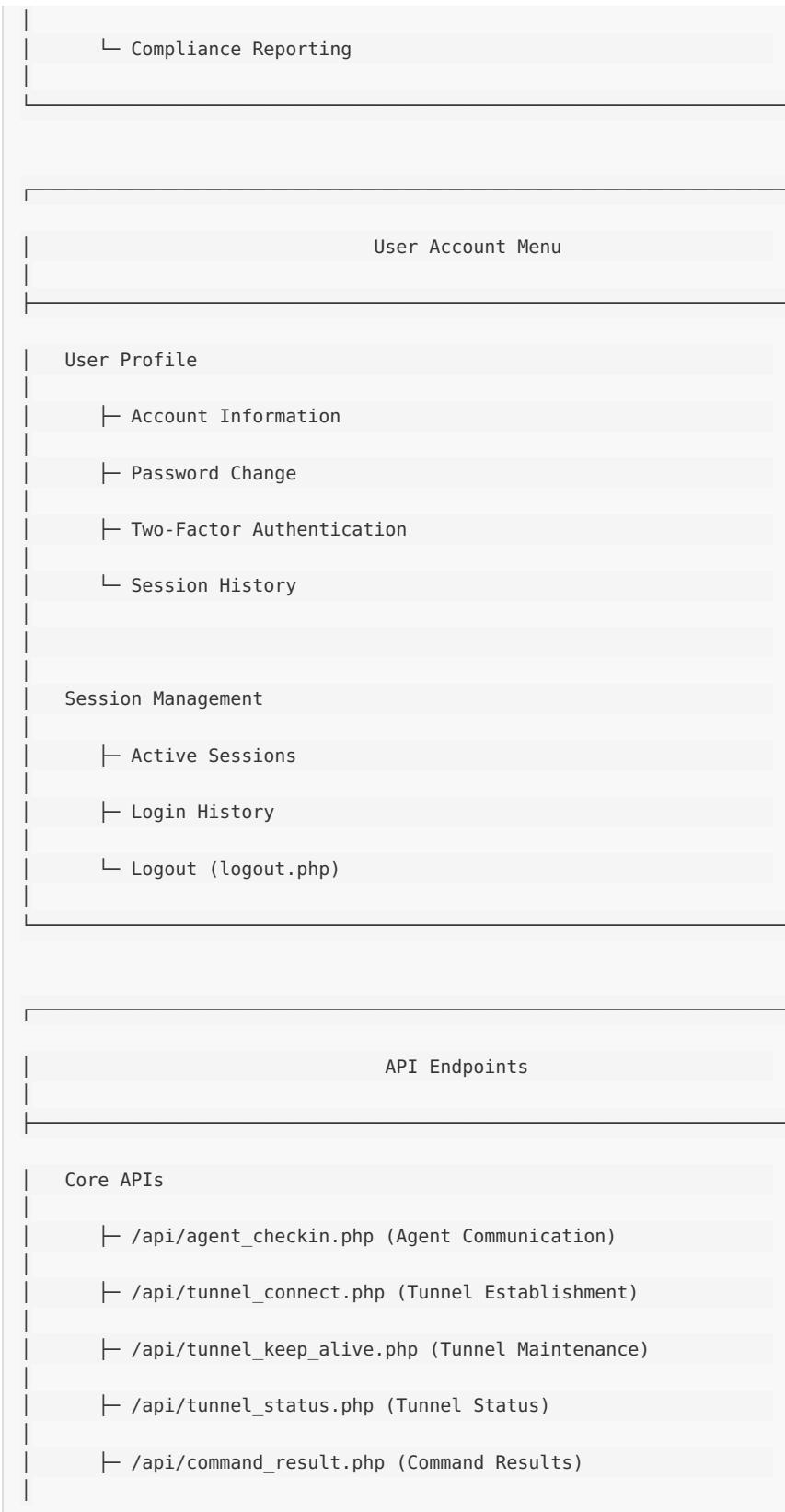
    └ Two-Factor Setup (twofactor\_setup.php)

    └ Password Policies

    └ Session Management

    └ Access Logs

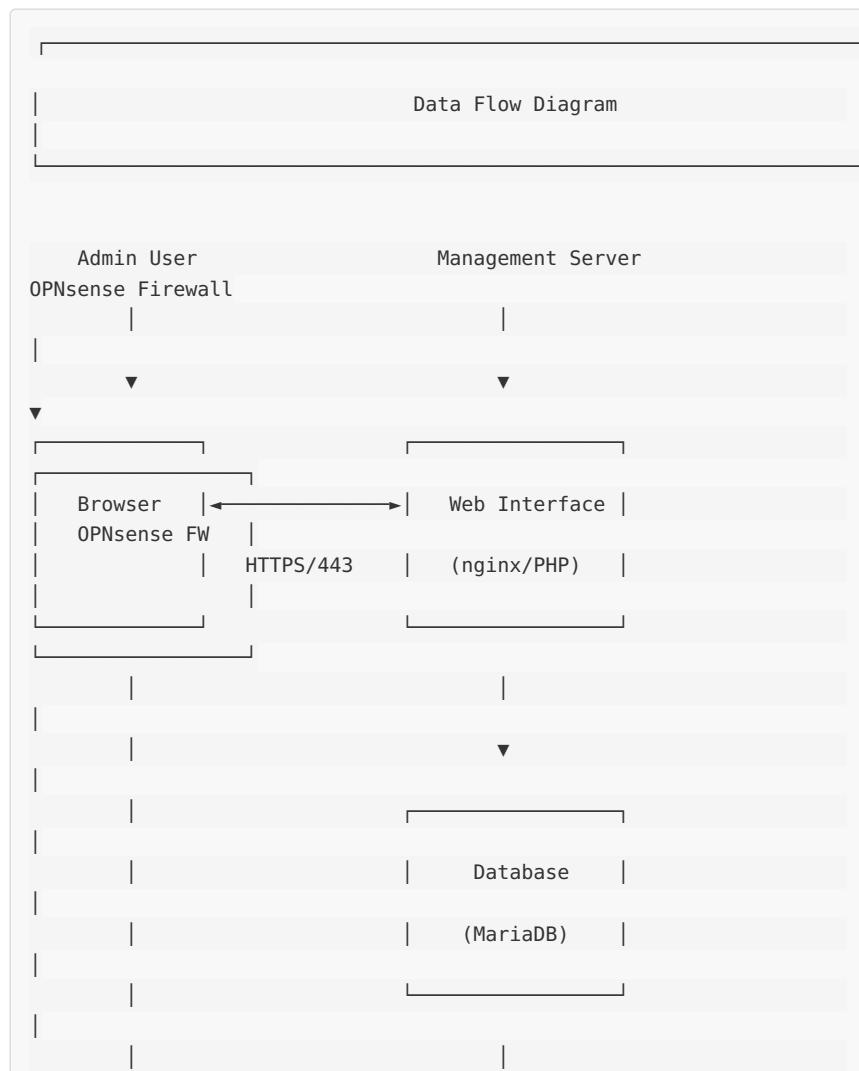
    └ Security Events

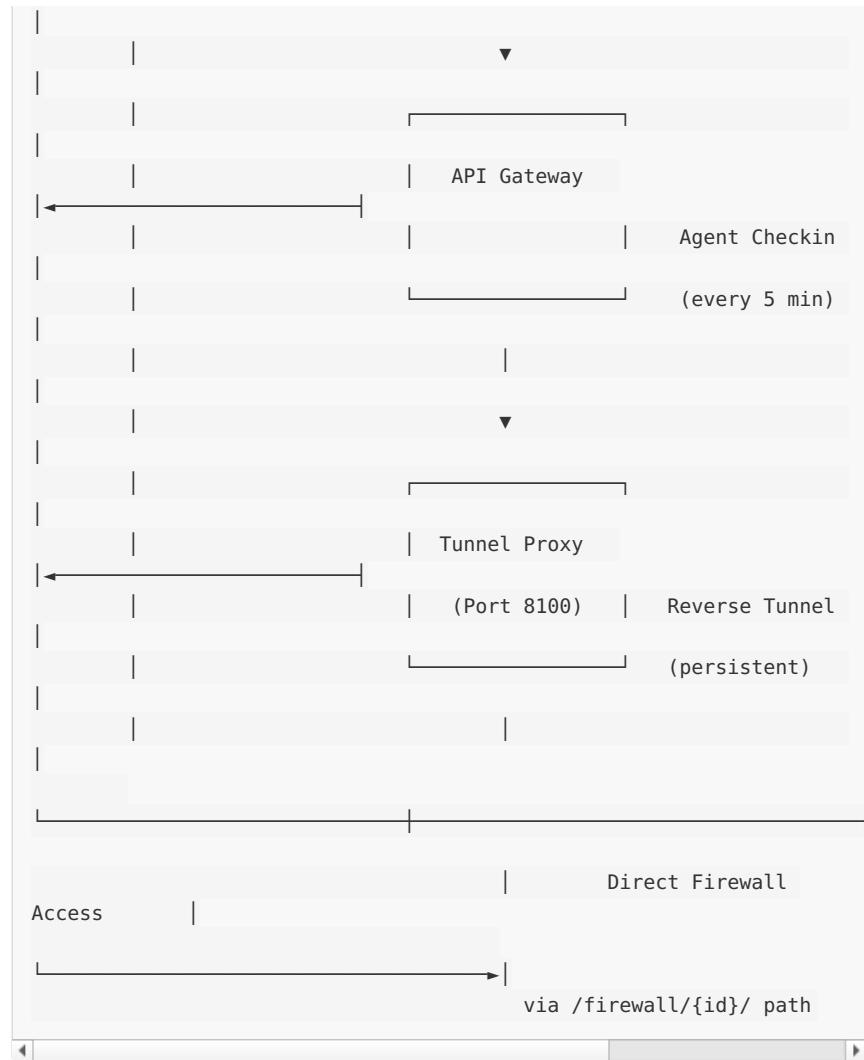


```
└─ /api/test_api_agent.php (API Testing)

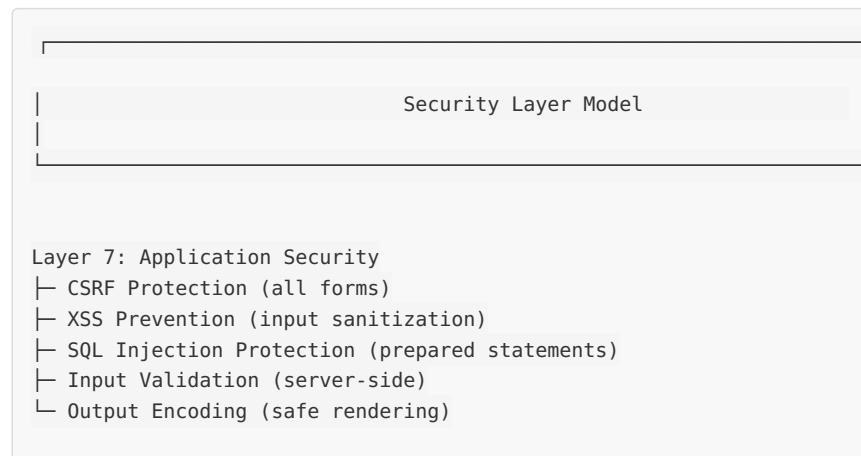
└─ Download Endpoints
    ├─ /download_agent.php (Monitoring Agent)
    ├─ /download_tunnel_agent.php (Tunnel Agent)
    └─ /enroll_firewall.php (Enrollment Script)
```

## Data Flow Architecture





## Security Architecture



```
Layer 6: Session Security
├─ HttpOnly Cookies
├─ Secure Flag (HTTPS only)
├─ SameSite=Strict
├─ Session Regeneration
└─ Timeout Management

Layer 5: Authentication
├─ Password Complexity (8+ chars, mixed case, numbers, symbols)
├─ Two-Factor Authentication (TOTP)
├─ Account Lockout (brute force protection)
├─ API Key Authentication
└─ Token-based Agent Auth

Layer 4: Transport Security
├─ TLS 1.3 Encryption
├─ HSTS Headers
├─ Certificate Validation
├─ Let's Encrypt Integration
└─ Secure Ciphers Only

Layer 3: Network Security
├─ Reverse Tunnel Architecture
├─ No Inbound Firewall Rules Required
├─ Encrypted Agent Communication
├─ Port-based Access Control
└─ IP-based Restrictions

Layer 2: System Security
├─ File Permissions (644/755)
├─ Service User Accounts
├─ Process Isolation
├─ Log File Protection
└─ Configuration Security

Layer 1: Infrastructure Security
├─ Database Credential Security
├─ Random Password Generation
├─ Backup Encryption
├─ Audit Logging
└─ Security Monitoring
```