คู่มือแนะนำการติดตั้งและใช้งานอุปกรณ์

FortiGate UTM Firewall

FortiOS 5.x (Rev.01)

สารบัญ การใช้งานพื้นฐาน (1)

กล่าวนำเกี่ยวกับ FortiOS 5.x

แนะนำการใช้งาน FortiGate ผ่านทาง WebGUI

ส่วนประกอบ WebGUI หัวข้อ System

ส่วนประกอบ WebGUI หัวข้อ Policy

ส่วนประกอบ WebGUI หัวข้อ Firewall Object

ส่วนประกอบ WebGUI หัวข้อ Security Profile

ส่วนประกอบ WebGUI หัวข้อ VPN

ส่วนประกอบ WebGUI หัวข้อ User&Device

ส่วนประกอบ WebGUI หัวข้อ WiFi Controller

ส่วนประกอบ WebGUI หัวข้อ Log&Report

การสร้างและตั้งค่าเริ่มต้นสำหรับใช้งาน FortiGate UTM Firewall

การตั้งค่า Interface แบบ (Manual ,DHCP ,PPPoE)

การตั้งต่า Routing (Default Route ,Static Route)

การตั้งต่าง DNS ของอุปกรณ์

การตั้งค่า Firewall Interface เป็น DNS Database

สารบัญ การใช้งานพื้นฐาน (2)

การสร้างและตั้งค่าเริ่มต้นสำหรับใช้งาน FortiGate UTM Firewall (ต่อ)

การสร้างและกำหนดสิทธ์ของผู้ดูและระบบ

การตรวจสอบการใช้งาน DHCP ของระบบ

การสร้าง Firewall Object หัวข้อ Address

การสร้าง Firewall Object หัวข้อ Service

การสร้าง Firewall Object หัวข้อ Schedule

การสร้าง Firewall Object หัวข้อ Traffic Shaper

การสร้าง Firewall Object หัวข้อ Visual IP

การสร้าง Security Profie หัวข้อ AntiVirus

การสร้าง Security Profie หัวข้อ WebFilter

การสร้าง Security Profie หัวข้อ Application Control

การสร้าง Security Profie หัวข้อ Intrusion Protection

การสร้าง Security Profie หัวข้อ E-Mail Filter

การสร้าง Security Profie หัวข้อ Data Leak Prevention

การสร้าง Security Profie หัวข้อ Client Reputation

การสร้าง Local User Database

สารบัญ การใช้งานพื้นฐาน (3)

การสร้าง Firewell Policy แบบพื้นฐาน

การสร้าง Policy สำหรับใช้งาน Internet (NAT Enable)

การสร้าง Policy สำหรับการสื่อสารภายใน (NAT Disable)

การสร้าง Policy สำหรับตรวจสอบสิทธิการใช้งาน

การเปิดใช้งาน Function Log

การเปิดใช้งาน SSL Inspection

การเปิดใช้งาน UTM Function

การเปิดใช้งาน Traffic Shaper

การแก้ไข Login Page เบื้องต้น

การใช้งานและอ่านค่า Firewall Log แบบพื้นฐาน

กำหนดค่ารูปแบบการเก็บ Log บน Firewall (สำหรับรุ่นที่รองรับ)

การตั้งค่าให้ Firewall ส่ง Log ไปเก็บที่ Log Device

การอ่านและวิเคราะห์ Firewall Log เบื้องต้น

การตั้งต่า Alert E-Mail

สารบัญ การใช้งานขั้นสูง (1)

การใช้งาน Multi-Link (ECMP Load Balance)

การกำหนด Policy Route

การตั้งค่า Virtual IP และการสร้าง Firewall Policy

การตั้งค่าและใช้งาน Fortinet Single Sign On

การตั้งต่าและใช้งาน Remote Authentication แบบ LDAP

การตั้งต่าและใช้งาน Remote Authentication แบบ RADIUS

การตั้งต่าและใช้งาน Device Control (BYOD)

การตั้งค่าและใช้งาน SSL-VPN (Client to Site)

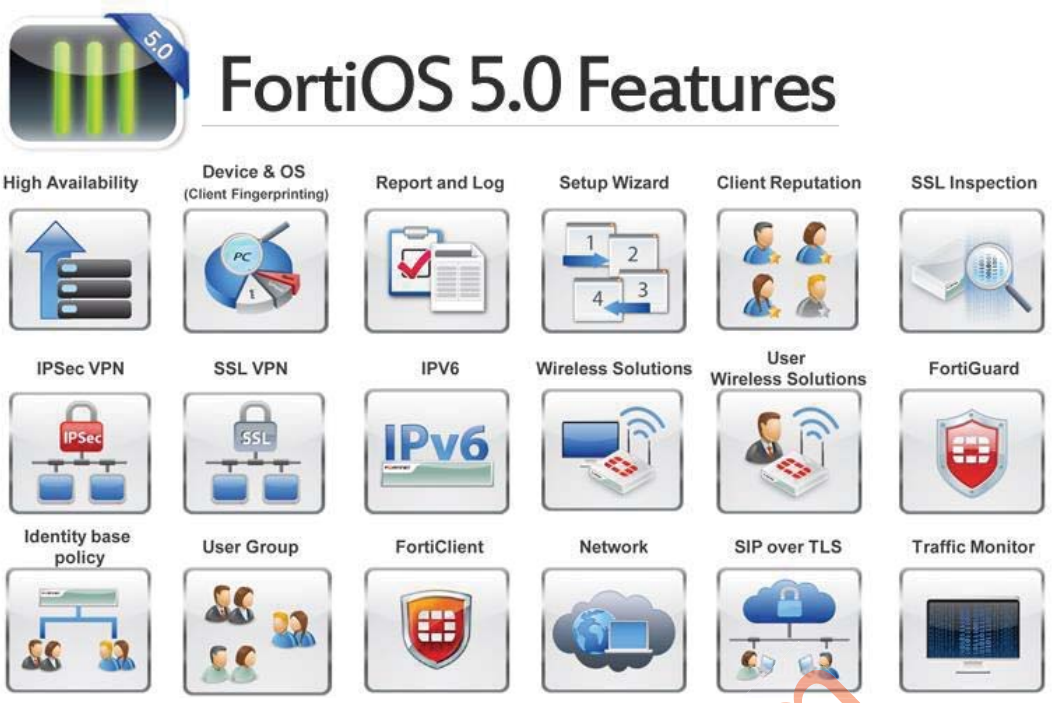
การตั้งค่าและใช้งาน IPSec-VPN (Client to Site)

การตั้งค่าและใช้งาน IPSec-VPN (Site to Site)

การตั้งค่าและใช้งาน WiFi Controller

FortiOS5 Overall Summary Feature

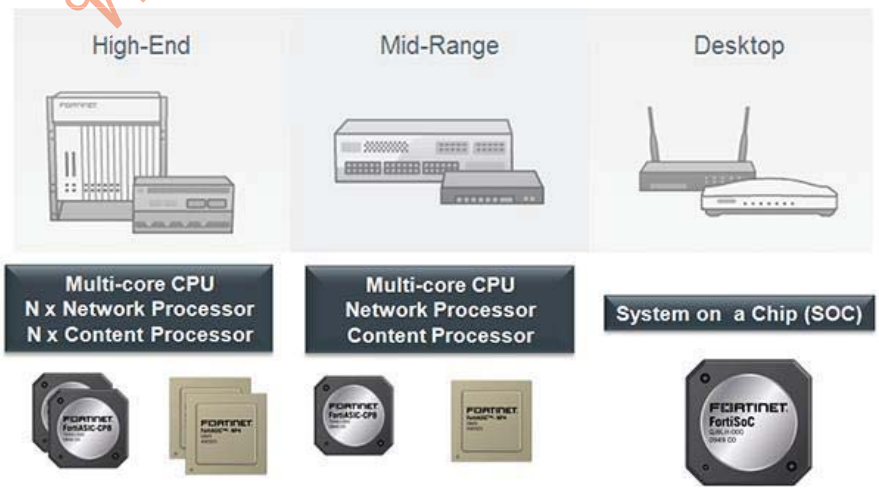
FortiGate UTM Firewall



FortiGate เป็น UTM Firewall ที่รวมการทำงานระหว่าง FortiASIC ,FortiOS ,FortiGuard เข้าด้วยกัน

FortiASIC - Chip ซึ่ง Design ขึ้นเพื่อช่วยการทำงานของ Firewall เฉพาะทาง

- Content Processor ASIC (CP8) ช่วยทางด้าน Content Security
- Network Processor ช่วยทางด้าน Firewall ,VPN ,IPv6 Translation
- Flow Processor ช่วยทางด้าน DDoS (เฉพาะรุ่น)
- Integrated Switching Fabric ASIC ช่วยทางด้าน Connection (เฉพาะรุ่น)
- System-On-A-Chip Processor (Hybrid ASIC) เป็น ASIC ที่รวม CPU

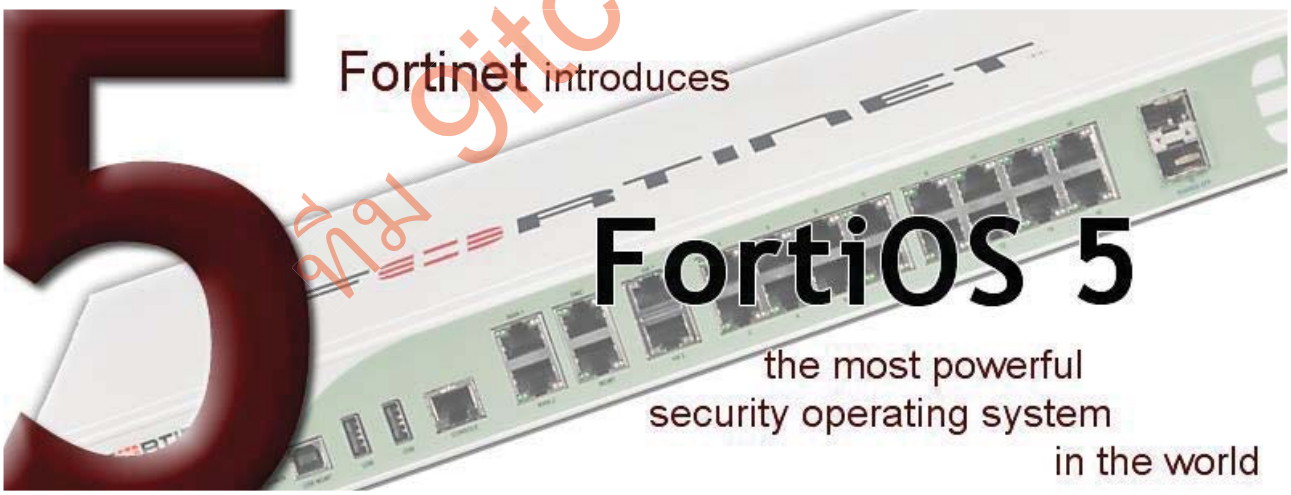


FortiOS - Flexible Network Operating Systems

FortiOS คือ Network Operating Systems ที่มีลักษณะเป็น Security-Hardened OS ซึ่งถูกสร้างและออกแบบมาให้เข้ากันกับการทำงานของ Hardware ของ FortiGate รุ่นนั้นๆ จึงสามารถมั่นใจได้ว่าการทำงานต่างๆ ของระบบจะมีเสถียรภาพ และมีความปลอดภัยสุงสุด

FortiGuard - World Class Threat Intelligence

FortiGuard คือ Signature ของระบบความปลอดภัยต่างๆ ที่ใช้งานใน FortiGate เช่น AntiVirus ,IPS ,Appcation Control ,WebFilter, E-Mail Filter ซึ่งระบบฐานข้อมูลของ FortiGuard นั้นมีการตรวจสอบอย่างดี และ Real-Time Update จึงสามารถมั่นใจได้ว่าระบบ Network ของลูกค้าที่ใช้ FortiGate จะมีความปลอดภัยสุงสุด



FortiOS 5.0 Enhancement Summary

System Administration

- Support configuration from Andriod & iOS devices through USB interface with FortiExplorer App
- Web-based Manager filtering & Columns improvements
- New option to format boot device before firmware update
- New CLI command to set factory default except VDOM/ interface settings
- Ability to disable the console login
- SNMP trap for FortiAP or FortiSwitch events
- SNMP implementation for Intelligent Platform Management Interface (IPMI) sensor
- SNMP Extensions for BGP
- Simplify GUI for FortiGate/FortiWiFi 20C and 40C
- Set DHCP options to get TFTP server IP and config file name to restore the configurations
- New setup wizard, included for all 1U models
- Central management configuration improvement
- Improved support for long hostnames in the CLI prompt

Visibility

- Additional dashboard Widgets
- New & expanded Real-time Sessions Widgets
- Contextual Information: Device, OS, User, destination hostname & geographic visibility
- Unit operation widget on FortiGate 600C, 800C, and 1000C
- Display threat information from FortiGuard Encyclopedia

FortiGuard Services

- FortiGuard Real time GeoIP updates
- FortiGuard SMS messaging service
- FortiGuard NTP & DNS Service
- FortiGuard DDNS Service
- FortiGuard USB Modem DB updates
- FortiGuard Device/OS Visibility signature updates
- Device based licensing for FortiCloud Service

Routing & Network Services

- Support Spanning Tree Protocol (STP) for FortiGate Switch Mode interfaces
- Support Virtual Switch & Hardware Switch feature
- Switch port extensions
- Switch Fabric access control list (ACL)
- WCCP L2 mode
- Support per VLAN MTU setting
- SSH handover support
- Option to restrict the number of IP addresses that can be leased to the same MAC address
- BGP AS-Path rewrite
- Increased Router Policy limit
- Dynamically cost of lag interface
- DNS service profile
- Authentication-based routing

High Availability

- Fortinet redundant UTM protocol (FRUP)
- Support configuration synchronization in standalone mode
- SSL-VPN authentication high availability (HA) failover support

User Based Identity

- Access Based SSO using 802.1x, Captive portal & FortiClient VPN
- Citrix & terminal services SSO Agent
- RADIUS-based SSO (Dynamic Profile)
- Support for secondary/backup remote authentication server
- Direct FSSO Polling Mode from FortiGate
- Support dynamic-profile for SSH proxy
- HTTP-only authentication over HTTPS channel
- Guest access provisioning

OTP Token Server

- Secure OTP seed import
- Soft Token Activation & Management
- JSON API for token support

Device Based Identity

- Device identification
- Device type/group classification & management
- Device based security policy

Endpoint Control

- FortiClient ubiquitous authentication
- FortiClient Registration & Management
- Captive Portal for Endpoint control client checking & install
- FortiClient configuration provisioning for "off-net" security enhancement
- Support device based policy on remote location & routed network
- Endpoint Logging

Client Reputation

- Multi-vector scoring
- Real-time client reputation monitoring

User Notification

- Fortinet Top Bar

Firewall

- Reorganized service items
- Policy list enhancement
- Mac address access list
- Web-based manager support for multicast policy and multicast address
- Dynamic comment field
- GeoIP override
- Improvements to support asymmetric traffic flows
- IP fragment and NAT enhancements
- IP pool fixed port range
- Restriction to virtual IP (VIP) on specific interfaces
- SIP NAT enhancement & support for TLS inspection

FortiOS Configuration Menu Overview

FortiGate UTM Firewall