



TÀI LIỆU GIỚI THIỆU GIẢI PHÁP

FORTIOS 8.0

SECURE NETWORKING HỢP NHẤT

FortiGate + FortiSwitch + FortiAP + Secure SD-WAN

THÔNG ĐIỆP CHÍNH

FortiOS 8.0 không tạo ra kiến trúc hợp nhất từ đầu. Phiên bản này mở rộng khả năng quản trị, quy mô, kiểm soát truy cập và tối ưu đường truyền trên nền tảng Secure Networking đã có.

MÃ TÀI LIỆU ARB-TD-FOS80-001

PHIÊN BẢN 1.0 - DRAFT kỹ thuật

NGÀY BIÊN SOẠN 07/09/2026

ĐƠN VỊ Arbolume

01 • TÓM TẮT ĐIỀU HÀNH

Convergence trong FortiOS 8.0 nên hiểu thế nào?

Fortinet không có một chương riêng mang tên “Convergence” trong New Features Guide. Khái niệm này được hình thành khi đặt cạnh nhau bốn nhóm cải tiến: giao diện quản trị FortiSwitch, LAN Edge cho switch và wireless, Secure SD-WAN, cùng vai trò FortiGate làm điểm thực thi chính sách.

CÁCH NÓI ĐÚNG

FortiOS 8.0 tiếp tục làm sâu hơn nền tảng Secure Networking hợp nhất: một hệ điều hành và một điểm quản trị cho bảo mật, LAN, WLAN và WAN trong các mô hình phù hợp.

Giá trị dành cho doanh nghiệp

Nhu cầu	FortiOS 8.0 hỗ trợ	Kết quả kỳ vọng
Giảm phân mảnh vận hành	Quản trị FortiGate, FortiSwitch và FortiAP từ FortiOS	Giảm số giao diện và thao tác phân tán
Kiểm soát access layer	PoE, NAC, 802.1X, trusted host và switching nâng cao	Gắn chính sách truy cập với cổng và thiết bị
Tối ưu WAN	Steering theo băng thông, SLA và các cơ chế overlay	Sử dụng đa đường truyền chủ động hơn
Mở rộng hạ tầng	Tăng số switch được quản lý trên một số model	Phù hợp deployment có quy mô lớn hơn

Đối tượng đọc

- Lãnh đạo cần đánh giá giá trị hợp nhất và phạm vi đầu tư.
- Đội IT/ATTT cần nắm điểm mới, điều kiện kỹ thuật và giới hạn.
- Đơn vị tư vấn cần có cơ sở chọn model, thiết kế pilot và đối chiếu license.

02 • KIẾN TRÚC HỢP NHẤT

Bốn lớp chức năng

FortiGate	FortiSwitch	FortiAP	Secure SD-WAN
Security gateway	Access LAN	Wireless LAN	WAN/overlay
Policy, routing, visibility	FortiLink, VLAN, PoE, NAC	SSID, radio, CAPWAP, MLO	SLA, steering, duplication, FEC
Điểm điều phối	Thiết bị được quản lý	Thiết bị được quản lý	Năng lực tích hợp trong FortiOS

Luồng traffic thực tế

Người dùng kết nối qua FortiAP hoặc FortiSwitch. FortiGate nhận ngữ cảnh từ lớp access, thực thi security/routing và chọn đường WAN theo policy cùng trạng thái SLA. FortiSwitch và FortiAP không thay FortiGate thực thi toàn bộ chức năng bảo mật; chúng đưa khả năng quan sát và điều khiển tới sát thiết bị đầu cuối.

PHẠM VI

Đây là tài liệu giới thiệu kỹ thuật. Thiết kế cuối cùng vẫn phải xác nhận model, FortiOS/FortiAP/FortiSwitch firmware, license, topology, số lượng thiết bị và yêu cầu hiệu năng.

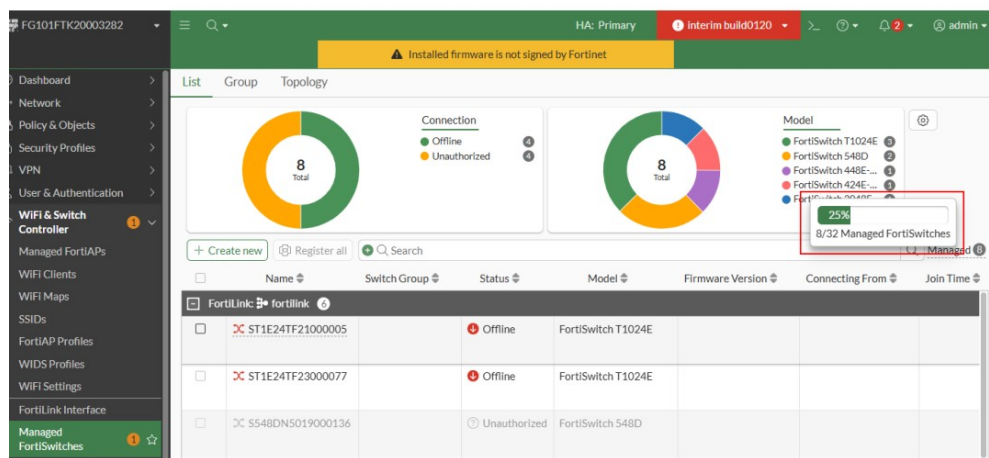
Những gì không nên quảng bá là mới

- FortiGate quản lý FortiSwitch và FortiAP đã có trước FortiOS 8.0.
- Secure SD-WAN và Performance SLA không phải lần đầu xuất hiện ở 8.0.
- MLO đã có hỗ trợ CLI từ FortiOS 7.6.5; điểm mới được guide nhấn mạnh ở 8.0 là GUI support.

03 • FORTIGATE QUẢN TRỊ FORTISWITCH

Giao diện quản trị LAN Edge rõ ràng hơn

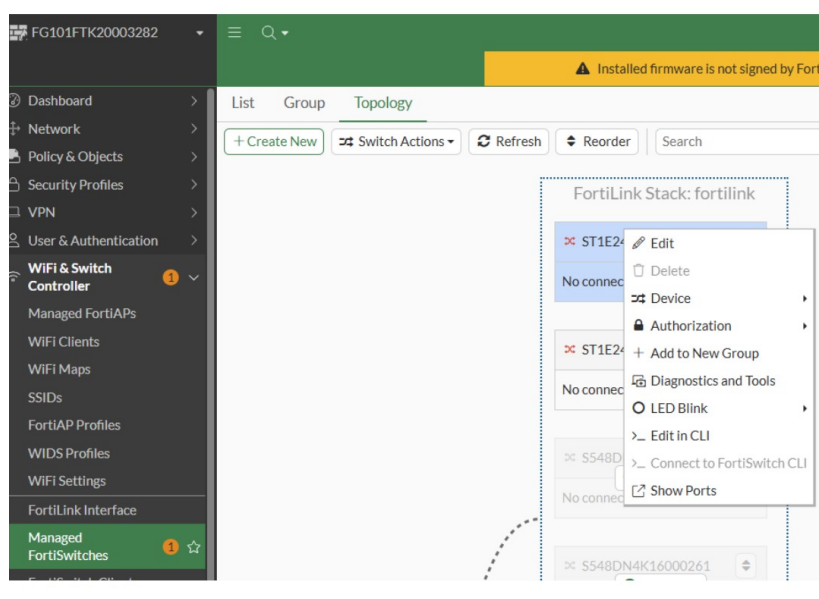
FortiOS 8.0 cải thiện WiFi & Switch Controller > Managed FortiSwitches. Tooltip hiển thị số switch đang quản lý so với giới hạn của FortiGate; quản trị viên có thể đổi switch group bằng menu chuột phải.



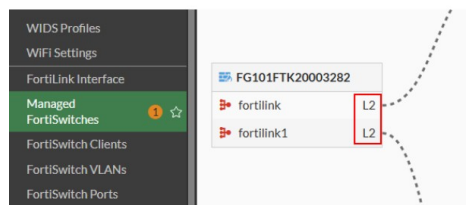
You can now change the group that the managed switch belongs by right-clicking on the switch in the *WiFi & Switch Controller page > Managed FortiSwitches page*.

Hình 1. Managed FortiSwitches: trạng thái, nhóm thiết bị và số lượng switch được quản lý.

Topology view được làm đồng nhất hơn với List view: các lệnh quản trị chính xuất hiện ngay trên sơ đồ và loại kết nối FortiLink được hiển thị. Giá trị thực tế là giảm chuyển đổi giao diện khi kiểm tra topology hoặc thao tác với switch.



You can now see the type of FortiLink connection in the *Topology view*.



Hình 2. Topology view hiển thị loại FortiLink và các thao tác quản trị switch.

04 • QUY MÔ VÀ ĐIỀU KHIỂN ACCESS LAYER

Tăng số FortiSwitch được quản lý

FortiOS 8.0 tăng giới hạn managed FortiSwitch trên một số model. Đây là thay đổi định lượng rõ nhất khi đánh giá khả năng mở rộng của kiến trúc hợp nhất.

Nhóm thiết bị FortiGate/FortiFirewall	Trước 8.0	FortiOS 8.0
Các model FG/FWF 50G được guide liệt kê	8	16
FG-200G / FG-201G	64	96
FG-2600F / FG-2601F	196	300

Release number of supported switches

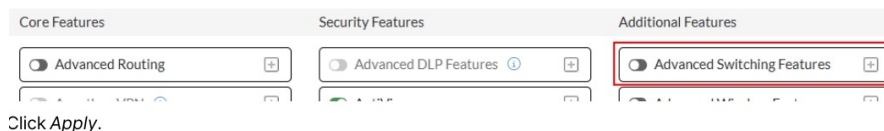
The number of supported FortiSwitch devices has increased for some FortiGate, FortiWiFi, and FortiFirewall models. This change enhances scalability for larger deployments.

FortiGate, FortiWiFi, or FortiFirewall model	Number of supported FortiSwitch units
FG-50G, FG-50GP, FG-51G, FG-51GP, FG-50G-5G, FG-51G-5G, FG-50G-DSL, FG-50G-SFP, FWF-50G, FWF-51G, FWF-50G-SFP, FWF-50G-5G, FWF-51G-5G, FWF-50G-DSL	16 (from 8)
FG-200G, FG-201G	96 (from 64)
FG-2600F, FFW-2600F, FG-2601F	300 (from 196)

Hình 3. Bảng giới hạn switch trong FortiOS 8.0 New Features Guide.

Điều khiển sâu hơn theo cổng

- PoE: đặt mức công suất tối đa 30 W, 60 W hoặc class-based; class-based là mặc định.
- EEE qua LLDP: quảng bá và điều khiển Energy Efficient Ethernet trên managed FortiSwitch.
- Trusted host: giới hạn địa chỉ IPv4/IPv6 được phép truy cập tài khoản quản trị switch.
- Advanced Switching Features: mở thêm LLDP, QoS, VLAN policy, PTP và các công cụ nâng cao trong GUI.



FortiOS 8.0 New Features Guide

Hình 4. Bật Advanced Switching Features trong System > Feature Visibility.

05 • NAC VÀ 802.1X

Kết hợp kiểm soát truy cập trên cùng một switch port

FortiOS 8.0 đưa luồng cấu hình FortiSwitch NAC kết hợp 802.1X lên GUI. Trước đó guide ghi nhận use case này được thực hiện qua CLI. Khi endpoint xác thực, RADIUS trả về nhóm người dùng; FortiGate đối chiếu nhóm và NAC policy để áp dụng quyền phù hợp.

ĐIỀU KIỆN BẮT BUỘC

Use case NAC kết hợp 802.1X yêu cầu 802.1X MAC-based authentication. Port-based authentication không được hỗ trợ. RADIUS phải trả về Fortinet-Group-Name và FortiGate phải có user group tương ứng.

To use NAC with 802.1 authentication, you must specify 802.1X MAC-based authentication. 802.1X port-based authentication is not supported.

The following are the prerequisites for this feature:

- The RADIUS server must return the Fortinet-Group-Name RADIUS attribute with the user group information.
- The FortiGate device must have a user group matching the Fortinet-Group-Name RADIUS attribute, and the RADIUS server can be added as a member to the user group.

Hình 5. Điều kiện NAC + 802.1X trong tài liệu Fortinet; nội dung chính đã được diễn giải bằng tiếng Việt ở trên.

Ý nghĩa vận hành

- Cổng switch trở thành điểm thực thi chính sách truy cập thay vì chỉ vận chuyển Layer 2.
- Quyền truy cập có thể thay đổi theo danh tính/nhóm thay vì gắn cứng với vị trí vật lý.
- Cần kiểm thử kỹ MAB, RADIUS attribute, guest/BYOD và tình huống RADIUS gián đoạn.

06 • FORTIGATE + FORTIAP

Quản lý FortiAP qua IPv6

FortiOS 8.0 cho phép FortiGate trực tiếp quản lý FortiAP qua IPv6 cho discovery, CAPWAP data channel, nâng cấp firmware, tunnel-mode SSID và bridge-mode SSID. Trên nền tảng NP7/NP7lite, CAPWAP IPv4/IPv6 có thể được offload; guide nêu rõ NP6/NP6xlite không hỗ trợ CAPWAP offloading cho trường hợp này.

Tối đa 16 VAP trên FortiAP G/K-series

Các model FortiAP G-series và K-series được hỗ trợ có thể đạt tối đa 16 Virtual AP. Đây là thay đổi hữu ích khi cần tách nhiều SSID/role, nhưng số SSID thực tế vẫn nên tối ưu để tránh tăng beacon overhead và làm giảm hiệu quả phổ tần.

Các cải tiến wireless đáng chú ý khác

Nhóm	Thay đổi	Giá trị
CAPWAP	Cải thiện độ ổn định session, đặc biệt trong môi trường NAT/cloud	Giảm gián đoạn quản lý AP
IPsec offload	Hỗ trợ offload lưu lượng IPsec từ FortiAP trên nền tảng phù hợp	Giảm tải xử lý
VLAN	Kết hợp DVLAN từ RADIUS với VLAN pooling	Phân đoạn người dùng linh hoạt
802.1X SSID	RADIUS authentication survivability	Duy trì xác thực cục bộ trong thời gian RADIUS lỗi

07 • WI-FI 7 MLO

GUI support cho FortiAP K-series

Multi-Link Operation (MLO) thuộc IEEE 802.11be, cho phép thiết bị sử dụng đồng thời nhiều băng tần như 2,4 GHz, 5 GHz và 6 GHz nhằm tăng thông lượng, giảm độ trễ và tăng độ tin cậy. FortiOS 8.0 bổ sung hỗ trợ cấu hình MLO trong GUI; CLI support đã xuất hiện từ 7.6.5.

Table showing radio support for FortiAP K-series models and radio support:

FortiAP Model	2.4 GHz radio	5 GHz radio	6 GHz radio
FAP-231K	✓	✓	✓
FAP-23JK	✓	✓	✓
FAP-241K	✓	✓	✓
FAP-243K	✓	✓	✓
FAP-441K*	N/A	✓	✓
FAP-443K*	N/A	✓	✓

Hình 6. Các radio hỗ trợ MLO trên những model FortiAP K-series được guide liệt kê.

Điều kiện thiết kế

- Đối chiếu đúng model FortiAP, firmware và capability của client.
- Security mode phải tương thích: WPA3-SAE, WPA3-Enterprise, WPA3-only-Enterprise hoặc OWE theo guide.
- Không coi Wi-Fi 7/MLO là mặc định cần thiết cho mọi dự án; ưu tiên bài toán mật độ, latency và vòng đời thiết bị.

KHUYẾN NGHỊ ARBOLUME

Với doanh nghiệp vừa và nhỏ, chỉ đưa MLO vào BOM khi client roadmap và nhu cầu hiệu năng chứng minh được giá trị. Không tăng chi phí chỉ để có nhãn Wi-Fi 7.

08 • FORTIAIOPS VÀ DARRP

AI hỗ trợ tối ưu radio - không thay controller

Khi FortiGate được quản lý bởi FortiAIops và bật darrp cùng ai-darrp-support, FortiAIops có thể thu thập dữ liệu radio/channel qua REST API, chạy thuật toán DARRP và kích hoạt thay đổi channel từ xa. FortiGate vẫn là wireless controller và giữ ngữ cảnh quản trị FortiAP.

Thành phần	Vai trò
FortiAP	Cung cấp dữ liệu radio, channel và thực thi cấu hình RF
FortiGate	Controller, policy và điểm trao đổi dữ liệu quản trị
FortiAIops	Phân tích, chạy DARRP và đưa ra/áp dụng đề xuất channel

LƯU Ý

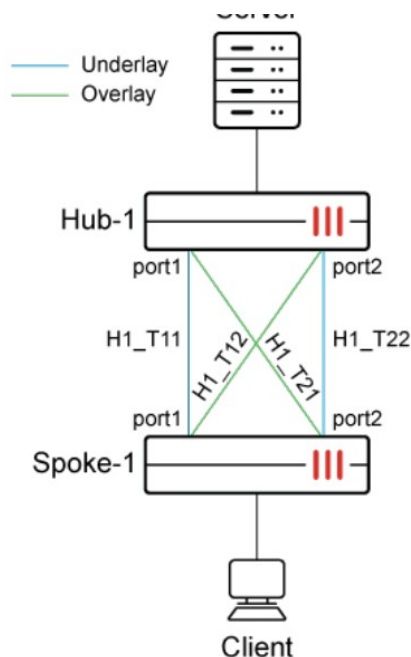
FortiAIops là thành phần bổ sung. Cần xác nhận subscription, quyền truy cập cloud, dữ liệu được gửi đi và quy trình phê duyệt thay đổi RF trước khi đưa vào thiết kế.

09 • SECURE SD-WAN TRONG FORTIOS 8.0

Steering theo băng thông khả dụng của underlay

FortiOS 8.0 bổ sung các hash mode inbandwidth, outbandwidth và bibandwidth để phân phối phiên dựa trên băng thông khả dụng. Với bandwidth-type đặt là underlay, quyết định steering có thể phản ánh tình trạng đường truyền vật lý bên dưới overlay thay vì chỉ nhìn từng tunnel độc lập.

Hash mode	Cách lựa chọn
inbandwidth	Ưu tiên interface còn nhiều băng thông khả dụng cho chiều vào
outbandwidth	Ưu tiên interface còn nhiều băng thông khả dụng cho chiều ra
bibandwidth	Đánh giá đồng thời băng thông khả dụng hai chiều
source-ip / source-dest-ip	Giữ tính ổn định của phiên dựa trên trường IP



Hình 7. Nhiều overlay cùng sử dụng hai underlay vật lý trong ví dụ của Fortinet.

10 • CÁC CẢI TIẾN SD-WAN KHÁC

Tính năng	Cơ chế	Ý nghĩa vận hành
ToS-based duplication	Dùng ToS để chọn traffic cần nhân bản	Áp dụng duplication có chọn lọc
Bandwidth threshold	Dừng duplication khi vượt ngưỡng overlay/underlay	Tránh làm nghẽn đường truyền
SLA theo volume	Đánh giá link dựa trên lượng traffic quan sát	Bổ sung góc nhìn ngoài latency/jitter/loss
Packet duplication	Nhân bản gói trên nhiều đường phù hợp	Tăng khả năng chịu lỗi cho traffic quan trọng
FEC	Bổ sung gói sửa lỗi cho luồng nhạy cảm	Giảm tác động của packet loss
Overlay/underlay visibility	Làm rõ quan hệ tunnel và đường vật lý	Chẩn đoán sự cố nhanh hơn
SLA/health-check	Theo dõi chất lượng đường truyền liên tục	Steering dựa trên trạng thái thực tế

Cách Arbolume đánh giá

Không nên bật đồng loạt mọi cơ chế. Duplication và FEC có thể tăng overhead; steering theo bandwidth cần số liệu bằng thông chính xác; SLA cần ngưỡng phù hợp từng ứng dụng. Thiết kế nên xuất phát từ nhóm traffic, mức độ quan trọng và chi phí đường truyền.

NGUYÊN TẮC

Mỗi SD-WAN rule phải trả lời được ba câu hỏi: bảo vệ ứng dụng nào, dựa trên SLA nào và hành vi khi cả hai đường đều suy giảm là gì?

11 • MA TRẬN ĐIỂM MỚI VÀ GIÁ TRỊ

Lớp	Điểm mới/được mở rộng trong 8.0	Tác động
Quản trị	Managed FortiSwitch GUI và topology rõ hơn	Giảm thao tác, tăng visibility
Quy mô	Tăng giới hạn switch trên một số FortiGate	Mở rộng deployment
Access LAN	PoE, EEE, trusted host, switching GUI	Điều khiển sâu hơn theo cổng
Identity/NAC	NAC + 802.1X trong GUI	Gắn quyền truy cập với danh tính
Wireless	IPv6 management, 16 VAP, CAPWAP, VLAN/RADIUS	WLAN linh hoạt và bền vững hơn
Wi-Fi 7	GUI support cho MLO	Khai thác FortiAP K-series dễ hơn
AIOps	FortiAIops điều phối DARRP từ xa	Tối ưu RF dựa trên dữ liệu
WAN	Bandwidth-aware steering và overlay/underlay enhancements	Tối ưu đa đường truyền

Thông điệp sử dụng trong tư vấn

ĐỀ XUẤT

FortiOS 8.0 mở rộng mô hình Secure Networking hợp nhất từ việc quản trị tập trung sang khả năng kiểm soát và tối ưu sâu hơn trên LAN, WLAN và WAN. Giá trị cuối cùng phụ thuộc vào thiết kế policy, model và điều kiện vận hành thực tế.

12 • LỘ TRÌNH ĐÁNH GIÁ VÀ PILOT

Giai đoạn	Việc cần làm	Đầu ra
1. Khảo sát	Model/firmware, topology, switch/AP, WAN, identity và ứng dụng	Sơ đồ hiện trạng + gap list
2. Đối chiếu	Kiểm tra compatibility matrix, release notes và license	Danh sách tính năng khả dụng
3. Thiết kế pilot	Chọn site, SSID/VLAN, nhóm người dùng và hai đường WAN	Test plan + rollback plan
4. Kiểm thử	NAC/802.1X, failover, SLA, RF, visibility và log	Biên bản kết quả
5. Mở rộng	Chuẩn hóa template, backup và giám sát	Kế hoạch rollout

Checklist trước khi chốt thiết kế

- FortiGate model và giới hạn managed switch/AP đã được xác nhận?
- FortiSwitch/FortiAP model và firmware có nằm trong ma trận hỗ trợ?
- RADIUS/identity source đã trả đúng attribute cho NAC/802.1X?
- Mục tiêu của từng SSID/VLAN và số VAP có hợp lý?
- SLA WAN phản ánh yêu cầu thực của ứng dụng?
- Đã có backup, rollback, lịch bảo trì và tiêu chí nghiệm thu?

13 • GIỚI HẠN VÀ NGUỒN THAM KHẢO

Giới hạn cần nêu rõ

- Không phải mọi tính năng có trên mọi model hoặc mọi tổ hợp firmware.
- Giới hạn switch/AP, hiệu năng security và throughput phải đối chiếu datasheet/model matrix.
- Một số năng lực cần FortiAI Ops, RADIUS, subscription hoặc hệ thống nhận dạng bổ sung.
- Ảnh giao diện trong tài liệu là trích đoạn minh họa từ Fortinet; menu có thể thay đổi theo build.
- Tài liệu này không thay thế Solution Design, BOM, SOW hoặc xác nhận chính thức của hãng.

Nguồn tham khảo chính

Tài liệu	Phạm vi sử dụng
FortiOS 8.0.0 New Features Guide	GUI, SD-WAN, LAN Edge Wireless và Switch Controller
Trang 18-20	Improve switch management
Trang 151-224	SD-WAN overlay/underlay và Performance SLA
Trang 453-508	LAN Edge - Wireless
Trang 509-530	LAN Edge - Switch Controller

Bước tiếp theo đề xuất

- Tổ chức workshop kỹ thuật 60-90 phút để chốt topology và use case ưu tiên.
- Lập bảng model/firmware/license cho thiết bị hiện có và thiết bị dự kiến.
- Thực hiện pilot nhỏ trước khi chuẩn hóa cấu hình cho toàn hệ thống.

ARBOLUME

Hỗ trợ rà soát hiện trạng, xác định phạm vi pilot, đối chiếu tính năng và xây dựng lộ trình triển khai phù hợp với nguồn lực đội IT.