



TÀI LIỆU GIỚI THIỆU GIẢI PHÁP

FORTINET UNIVERSAL ZTNA

Truy cập ứng dụng theo danh tính, trạng thái thiết bị và nguyên tắc xác minh liên tục

Thông điệp chính Fortinet Universal ZTNA giúp tổ chức chuyển từ quyền truy cập mạng rộng sang quyền truy cập theo từng ứng dụng, được đánh giá lại theo từng phiên và trạng thái endpoint.

MÃ TÀI LIỆU ARB-TD-ZTNA-001

PHIÊN BẢN 1.0 - DRAFT kỹ thuật

NGÀY BIÊN SOẠN 06/09/2026

ĐƠN VỊ Arbolume

01 • TÓM TẮT ĐIỀU HÀNH

Fortinet Universal ZTNA là gì?

Fortinet Universal ZTNA là mô hình truy cập ứng dụng dựa trên danh tính người dùng, danh tính thiết bị và trạng thái bảo mật của endpoint. Kết nối được thiết lập qua tunnel mã hóa tự động và có thể được đánh giá lại gần thời gian thực trong suốt phiên truy cập.

Giá trị đối với doanh nghiệp

Bài toán	Cách tiếp cận Universal ZTNA	Kết quả kỳ vọng
VPN cấp quyền quá rộng	Phân đoạn truy cập theo từng ứng dụng	Giảm bề mặt tấn công và hạn chế di chuyển ngang
Thiết bị ngoài văn phòng khó kiểm soát	Posture check liên tục từ FortiClient	Chỉ thiết bị đáp ứng điều kiện mới được duy trì truy cập
Chính sách nội bộ và từ xa không đồng nhất	Một chính sách cho người dùng tại chỗ và từ xa	Trải nghiệm và kiểm soát nhất quán
Nhiều agent và console	FortiClient làm unified agent, EMS quản trị tập trung	Giảm phân mảnh công cụ trên endpoint

Phạm vi tài liệu Tập trung vào FortiClient ZTNA Agent, FortiClient EMS và FortiGate ZTNA Application Gateway. Các module EPP/ATP, CASB và SASE chỉ được đề cập ở mức liên quan.

Đối tượng đọc

- Lãnh đạo cần hiểu giá trị, phạm vi đầu tư và lộ trình chuyển đổi.
- Đội IT/ATTT cần nắm kiến trúc, điều kiện kỹ thuật, vận hành và giới hạn.
- Đơn vị tư vấn cần có checklist khảo sát ban đầu trước khi chọn license và mô hình triển khai.

02 • BỐI CẢNH

Vì sao VPN truyền thống chưa đủ?

VPN vẫn hữu ích cho nhiều tình huống, nhưng thường tạo kết nối ở lớp mạng. Nếu quyền truy cập quá rộng hoặc trạng thái thiết bị không được đánh giá liên tục, một tài khoản hay endpoint bị xâm nhập có thể mở rộng phạm vi ảnh hưởng.

Tiêu chí	VPN truyền thống	Fortinet Universal ZTNA
Đối tượng cấp quyền	Mạng hoặc subnet	Ứng dụng cụ thể
Quyết định truy cập	Chủ yếu tại thời điểm kết nối	Theo phiên và có thể đánh giá lại liên tục
Ngữ cảnh	Danh tính người dùng	Người dùng + thiết bị + posture + certificate
Vị trí người dùng	Thường tách nội bộ và từ xa	Chính sách nhất quán, không phụ thuộc vị trí
Bề mặt lộ ra	Có thể thấy vùng mạng sau tunnel	Ứng dụng được ẩn sau ZTNA Application Gateway

Nguyên tắc cốt lõi

- Không mặc định tin cậy vì người dùng đang ở mạng nội bộ.
- Cấp quyền tối thiểu theo từng ứng dụng và vai trò.
- Xác minh danh tính và trạng thái thiết bị trước mỗi phiên.
- Duy trì khả năng đánh giá lại và thu hồi quyền khi posture thay đổi.

Lưu ý kiến trúc ZTNA không đồng nghĩa với loại bỏ VPN ngay lập tức. Fortinet hỗ trợ lộ trình ZTNA over VPN trước khi chuyển sang Full ZTNA.

03 • KIẾN TRÚC

Ba thành phần chính



1. FortiClient - ZTNA Agent

Agent trên endpoint thực hiện steering kết nối, thu thập telemetry, cung cấp danh tính/certificate và gửi trạng thái bảo mật để phục vụ quyết định truy cập. FortiClient cũng có thể cung cấp VPN, web filtering, vulnerability assessment và EPP/ATP tùy license.

2. FortiClient EMS

EMS quản trị tập trung FortiClient, triển khai agent, đồng bộ nhóm, xây dựng Zero Trust tagging rules, cấp phát cấu hình và thực hiện remote action. Có lựa chọn EMS tại chỗ hoặc FortiClient Cloud theo yêu cầu doanh nghiệp.

3. FortiGate ZTNA Application Gateway

FortiGate nhận diện người dùng và posture từ hệ thống FortiClient/EMS, áp dụng policy theo ứng dụng, xác thực theo từng phiên và tạo cổng truy cập tới ứng dụng nội bộ. Theo Ordering Guide, mọi nền tảng FortiGate chạy FortiOS 7.0 trở lên đều hỗ trợ ZTNA Gateway.

	Không cần license ZTNA riêng trên FortiGate Theo Fortinet Ordering Guide, khách hàng mua license FortiClient ZTNA; không cần mua thêm license ZTNA chuyên biệt cho FortiGate làm gateway.
---	---

04 • LƯỒNG TRUY CẬP

Một phiên ZTNA được quyết định như thế nào?



Bước	Hoạt động	Điểm kiểm soát
01	Người dùng mở ứng dụng đã được cấu hình	FortiClient tự động steering lưu lượng
02	FortiClient cung cấp identity, certificate và posture	EMS/FortiGate đối chiếu tag và policy
03	FortiGate xác thực người dùng và thiết bị	Có thể bổ sung SSO, SAML và MFA
04	Tạo tunnel mã hóa đến đúng ứng dụng	Không cấp quyền truy cập toàn bộ mạng
05	Theo dõi posture gần thời gian thực	Thay đổi posture có thể làm thay đổi quyền truy cập
06	Ghi nhận sự kiện và báo cáo	Tích hợp logging/reporting theo kiến trúc đã chọn

Ví dụ posture check

- Thiết bị thuộc đúng nhóm và có certificate hợp lệ.
- Phiên bản hệ điều hành hoặc phần mềm đáp ứng ngưỡng quy định.
- Không phát hiện lỗ hổng nghiêm trọng chưa xử lý.
- Endpoint security đang hoạt động và không bị đánh dấu compromise.

05 • NĂNG LỰC

Các khả năng nổi bật

Nhóm năng lực	Khả năng chính	Ghi chú triển khai
Secure application access	Transparent ZTNA, TCP/UDP forwarding, MFA, SSO/SAML	Policy theo ứng dụng và từng phiên
Endpoint posture	Telemetry, certificate, tagging, continuous monitoring	Dùng làm điều kiện cấp hoặc duy trì quyền
IT hygiene	Vulnerability assessment, remediation, software inventory	Software inventory thuộc EPP/ATP
Endpoint protection	AI-powered NGAV, anti-malware, anti-exploit, ransomware protection	Phụ thuộc EPP/ATP và hệ điều hành
SaaS security	Inline CASB và API-based FortiCASB	Entitlement đi kèm license theo tài liệu Fortinet
Central management	EMS/Cloud, deployment, policy, quarantine, reporting	Central logging yêu cầu FortiAnalyzer

Hỗ trợ nền tảng - điểm cần lưu ý

- Windows, macOS và Linux có phạm vi ZTNA/VPN và posture rộng nhất.
- ZTNA web application trên iOS/Android cần FortiClient/EMS 7.2.2 trở lên và tích hợp MDM.
- Ransomware protection chỉ được tài liệu Fortinet ghi nhận trên Windows.
- FortiClient Linux không hỗ trợ Sandbox integration.
- Tính năng cụ thể phải được đối chiếu với phiên bản FortiClient/EMS và license tại thời điểm báo giá.

06 • LICENSE

Chọn phương án theo nhu cầu

Phương án	Phù hợp khi	Bao gồm nổi bật
ZTNA / VPN Agent	Trọng tâm là secure access, posture và chuyển đổi từ VPN	ZTNA, VPN, MFA, EMS, vulnerability management, web filtering, CASB
EPP / ATP Agent	Muốn hợp nhất secure access và bảo vệ endpoint	Toàn bộ ZTNA/VPN + NGAV, anti-malware, ransomware, media control, sandbox
Managed ZTNA / FortiClient	Đội IT cần giảm tải onboarding và theo dõi	Provisioning, onboarding, Security Fabric integration, vulnerability monitoring

Cloud hay on-premise?

Mô hình EMS	Ưu điểm	Điều cần đánh giá
FortiClient Cloud	Triển khai nhanh, giảm hạ tầng quản trị	Kết nối cloud, lưu trữ và chính sách nội bộ
EMS on-premise	Kiểm soát tại chỗ, phù hợp vùng mạng hạn chế	Máy chủ, backup, nâng cấp và vận hành hệ thống

Quy tắc chọn license Nếu doanh nghiệp cần cả Endpoint Protection và ZTNA, FortiClient EPP/ATP đã bao gồm quyền ZTNA. Không nên mua chồng quyền khi chưa đối chiếu contract và SKU.

07 • LỘ TRÌNH

Chuyển đổi theo bốn giai đoạn

Giai đoạn	Mục tiêu	Đầu ra bắt buộc
1. Khảo sát	Ứng dụng, người dùng, thiết bị, FortiGate/FortiOS, identity và luồng mạng	Danh mục ứng dụng + ma trận user/device/posture
2. ZTNA over VPN	Áp dụng posture tag trên hạ tầng VPN hiện có	Nhóm pilot, policy kiểm thử và phương án rollback
3. Full ZTNA pilot	Đưa một số ứng dụng qua ZTNA Application Gateway	Kết quả UAT, log truy cập, trải nghiệm và ngoại lệ
4. Mở rộng & tối ưu	Mở rộng ứng dụng, tự động hóa và báo cáo	Runbook vận hành, KPI và lịch rà soát policy

Tiêu chí nghiệm thu pilot

- Người dùng đúng vai trò truy cập đúng ứng dụng; người dùng ngoài phạm vi bị từ chối.
- Thiết bị không đạt posture bị chặn hoặc đưa vào luồng remediation.
- MFA/SSO hoạt động đúng với nhóm đã chọn.
- Ứng dụng hoạt động ổn định qua tunnel mã hóa và không mở rộng quyền ngoài thiết kế.
- Log đủ để điều tra sự kiện truy cập và xác định nguyên nhân từ chối.
- Có rollback plan và hướng dẫn hỗ trợ người dùng.

08 • KHẢO SÁT KỸ THUẬT

Checklist trước khi thiết kế

Nhóm thông tin	Câu hỏi cần xác nhận
Endpoint	Số lượng Windows/macOS/Linux/mobile; thiết bị quản lý hay BYOD; MDM hiện có?
Ứng dụng	Web/TCP/UDP; on-premise/cloud; DNS, certificate, port, dependency và mức độ quan trọng?
Danh tính	AD/Entra ID/IdP; SSO, SAML, MFA; nhóm và vai trò truy cập?
FortiGate	Model, FortiOS, HA, interface, SSL inspection và tải hiện tại?
EMS	Cloud hay on-premise; AD/Entra sync; phân nhóm; quyền quản trị và backup?
Posture	Điều kiện tối thiểu; mức độ lỗ hổng; anti-malware; OS version; ngoại lệ?
Vận hành	Ai duyệt policy, xử lý từ chối, quarantine, sự cố và thay đổi ứng dụng?
Tuân thủ	Yêu cầu lưu log, vùng dữ liệu, retention, phân quyền và kiểm toán?

Điểm dừng thiết kế Chưa chốt danh mục ứng dụng, identity source và tiêu chí posture thì chưa nên chốt SKU hoặc cam kết phạm vi triển khai.

Điều kiện áp dụng và tài liệu tham khảo

Giới hạn cần nêu rõ

- ZTNA không tự thay thế toàn bộ NAC, EDR, SIEM hoặc DLP; phạm vi phụ thuộc license và kiến trúc tích hợp.
- Hiệu năng thực tế phụ thuộc model FortiGate, loại ứng dụng, SSL inspection, tải đồng thời và điều kiện mạng.
- Không phải mọi tính năng đều có trên mọi hệ điều hành.
- MFA, SSO, certificate, MDM và identity source có thể cần cấu hình hoặc license riêng.
- Managed FortiClient là dịch vụ tùy chọn của Fortinet; cần xác nhận khả năng cung cấp và điều kiện thương mại tại Việt Nam.
- Tài liệu này là tài liệu giới thiệu kỹ thuật, không thay thế Solution Design, BOM, SOW hoặc xác nhận chính thức của hãng.

Nguồn tham khảo chính

Tài liệu	Phiên bản / thời điểm	Phạm vi sử dụng
FortiClient Data Sheet - The Fortinet Unified Agent	11/2025	Tính năng, bundle, platform support, EMS và dịch vụ
Universal ZTNA Ordering Guide	01/2026; tài liệu cập nhật 02/2026	Kiến trúc, thành phần, license, FortiGate gateway và FAQ
FortiClient ZTNA & Endpoint Protection	Tài liệu tham khảo do người dùng cung cấp	Bối cảnh giải pháp và thuật ngữ tiếng Việt; không dùng số liệu cũ làm căn cứ chính
FortiOS 8.0.0 New Features Guide — Zero Trust Network Access	8.0.0 / 2026	Cấu trúc ZTNA mới, Service Connector và posture tag dual-stack IPv4/IPv6

Bước tiếp theo đề xuất

- Tổ chức workshop 60-90 phút để chốt ứng dụng pilot và nhóm người dùng.
- Kiểm tra model/FortiOS, identity source và yêu cầu EMS.
- Lập ma trận posture và policy theo ứng dụng.
- Đối chiếu license/SKU hiện hành với Fortinet hoặc nhà phân phối trước báo giá.

Arbolume Hỗ trợ xác định phạm vi, đối chiếu license, xây dựng lộ trình pilot và phối hợp nguồn lực triển khai theo phạm vi được thống nhất.

10 • CẬP NHẬT FORTIOS 8.0

Các thay đổi trực tiếp đối với Zero Trust Network Access

FortiOS 8.0 tái cấu trúc các đối tượng ZTNA để linh hoạt hơn khi ghép cổng, máy chủ, portal và policy; đồng thời bổ sung mô hình Service Connector và mở rộng posture tag cho môi trường dual-stack. Các thay đổi dưới đây thuộc mục Zero Trust Network Access của Fortinet, không phải nhóm tính năng LAN Edge.

Nhóm cập nhật	Thay đổi trong FortiOS 8.0	Giá trị triển khai	Điều kiện / Lưu ý
Đơn giản hóa cấu hình	Tách access-proxy thành ZTNA traffic-forwarding proxy, web proxy và web portal; bổ sung ztna.destination; policy tham chiếu trực tiếp destination. GUI có trang Ports mới, cho phép một ZTNA Port dùng chung cho nhiều server và hỗ trợ web portal agentless.	Giảm phụ thuộc giữa các object, tái sử dụng cấu hình tốt hơn và tách rõ web access, traffic forwarding, portal.	Khi nâng cấp cần rà mapping object/policy. Host là trường bắt buộc cho web proxy và traffic-forwarding server trong GUI.
ZTNA Service Connector	FortiGate có thể tạo kết nối điều khiển bền vững tới ZTNA Edge (FortiPAM, FortiProxy hoặc FortiGate), nhận yêu cầu qua control tunnel và proxy tới máy chủ được bảo vệ.	Không cần công khai trực tiếp access proxy/service của FortiGate nội bộ; phù hợp mô hình edge–connector và phân tách vùng mạng.	ZTNA Edge thực hiện kiểm tra và cưỡng chế policy; kết nối connector dùng chứng thư và mTLS.
Posture tag dual-stack	Cho phép áp dụng security posture tag/group IPv6 từ FortiClient EMS trong chính sách ZTNA dual-stack IPv4/IPv6; bổ sung address6 subtype ems-tag và tham số ztna-ems-tag6.	Duy trì quyết định truy cập dựa trên posture khi ứng dụng và endpoint sử dụng IPv6 hoặc môi trường chuyển đổi dual-stack.	Yêu cầu FortiClient và FortiClient EMS 7.4.5 hoặc 8.0.0 trở lên.

Tác động tới thiết kế Arbolume đề xuất

- Dự án mới nên chuẩn hóa object theo cấu trúc FortiOS 8.0; dự án nâng cấp cần lập bảng đối chiếu access-proxy, destination và policy trước khi chuyển đổi.
- Chọn Service Connector khi FortiGate bảo vệ ứng dụng nằm sâu trong mạng và tổ chức không muốn người dùng kết nối trực tiếp tới FortiGate đó từ Internet.
- Nếu có IPv6, bổ sung ca kiểm thử posture tag IPv6 vào UAT; xác nhận đồng thời phiên bản FortiClient và EMS trước khi bật policy dual-stack.
- Các thay đổi này không làm mất yêu cầu nền tảng: danh tính, certificate, posture, MFA/SSO và nguyên tắc cấp quyền tối thiểu theo ứng dụng.

Nguồn: Fortinet, FortiOS 8.0.0 New Features Guide — Zero Trust Network Access (truy cập 06/09/2026).