# CAPÍTULO 23.

# ESTUDIO COMPARATIVO DE LA GESTIÓN DE POLÍTICAS DE TRÁFICO (AAR) EN SOLUCIONES SD-WAN: CISCO VIPTELA VS. FORTINET SECURE SD-WAN

Jaime Jose Saenz Dedios[1]
Emmanuel Jossuet Bereche Quintana[2]
Jaime Leandro Madrid Casariego[3]
Jesús Javier Cobeñas Morales[4]

[1]: Ingeniero de redes y comunicaciones, Docente Universitario.
https://orcid.org/0009-0002-3401-5510

[2]: Ingeniero de Sistemas, Docente Universitario.
https://orcid.org/0009-0003-8776-140X

[3]: Ingeniero de Sistemas, Docente Universitario.
https://orcid.org/0009-0004-9231-5495

[4]: Ingeniero Informático, Docente Universitario.
https://orcid.org/0000-0002-2853-1204

# RESUMEN

Este capítulo de revisión narrativa compara la gestión de políticas de Application-Aware Routing (AAR) en dos plataformas líderes de SD-WAN: Cisco Viptela y Fortinet Secure SD-WAN. Mediante el análisis de documentación oficial, artículos académicos, informes de analistas y casos de estudio publicados entre 2018 y 2024, se examinan cinco dimensiones: arquitectura, funcionalidades de AAR, rendimiento, escalabilidad y seguridad. Cisco Viptela utiliza una arquitectura modular con controladores separados (vSmart, vManage, vBond) que permite alta escalabilidad y granularidad en políticas dinámicas, siendo ideal para grandes corporaciones con redes complejas. Fortinet, en cambio, integra AAR dentro de su stack de seguridad (NGFW, IPS, sandbox) en un único dispositivo FortiGate, ofreciendo menor latencia de inspección y menor TCO para medianas empresas. Los resultados muestran que Viptela domina en entornos multi-tenant y topologías dinámicas, mientras que Fortinet destaca por su simplicidad operativa y protección nativa. La discusión se centra en la aplicabilidad sectorial, la continuidad operativa en entornos cloud-híbridos y las tendencias futuras hacia SASE y automatización cognitiva. La selección entre ambas soluciones debe basarse en el tamaño de la organización, el perfil de seguridad, el presupuesto y la madurez técnica del equipo operativo.

**Palabras clave:** SD-WAN, AAR, Cisco Viptela, Fortinet, seguridad integrada.

# INTRODUCCIÓN

En la economía digital, las aplicaciones ya no son meros soportes de negocio: son el negocio. El 82 % del tráfico empresarial corresponde a aplicaciones en la nube o SaaS que exigen latencias estables, pérdidas mínimas y disponibilidad 24 × 7 (Cisco, 2023). Esta dependencia convierte al tráfico aplicativo en un activo crítico cuya gestión condiciona la productividad, la experiencia de cliente y, en última instancia, los ingresos.

Durante dos décadas, las redes de área amplia (WAN) se basaron en circuitos privados MPLS y políticas estáticas de enrutamiento. La explosión del tráfico híbrido (nube-pública, SaaS, IoT) y la dislocación geográfica de la fuerza laboral revelaron la rigidez de ese modelo: tiempos de provisión de semanas, backhauling ineficiente y costos de ancho de banda crecientes (Gartner, 2023). Como respuesta, el paradigma Software-Defined WAN (SD-WAN) desacopló el plano de control del plano de datos, permitiendo orquestar políticas de manera centralizada y explotar múltiples transportes (MPLS, Internet 5G, LTE) con granularidad de aplicación (Mier, 2021).

Una funcionalidad clave dentro del catálogo de SD-WAN es el Application-Aware Routing (AAR): la capacidad de clasificar flujos en tiempo real —mediante deep packet inspection (DPI), FQDN o comportamiento heurístico— y seleccionar dinámicamente el camino óptimo según criterios de calidad de servicio (QoS), seguridad y costo (Medina & Ríos, 2020). AAR reduce la latencia media de aplicaciones críticas entre un 15 % y un 40 % y disminuye la tasa de abandono de videoconferencias en entornos distribuidos (Fortinet, 2022). Además, al combinarse con Service-Level Agreements (SLA) probados en intervalos de subsegundos, permite la conmutación por error automática antes que el usuario perciba degradación (Herrera et al., 2023).

No obstante, la implementación de AAR varía sensiblemente entre fabricantes. Cisco Viptela, surgida de la adquisición de Viptela en 2017, apuesta por una

arquitectura de control separada (vSmart, vManage, vBond) con políticas de intención declaradas y repositorios centralizados (Cisco, 2023). Fortinet Secure SD-WAN, por su parte, hereda el motor de seguridad FortiASIC y ofrece AAR integrado en el mismo chip que Next-Generation Firewall (NGFW), prometiendo inspección a 3 Gbps sin saltos de servicio (Fortinet, 2022). La elección entre ambos enfoques impacta la latencia de detección de aplicaciones, la escalabilidad de políticas y la complejidad operativa; sin embargo, la literatura técnica carece de estudios comparativos específicos sobre la gestión de políticas AAR que sirvan de guía a arquitectos de red.

Este artículo de revisión narrativa aborda esa laguna. Se examina la forma en que Cisco Viptela y Fortinet Secure SD-WAN conciben, despliegan y monitorizan políticas AAR, diferenciando arquitectura, lenguaje de políticas, escalabilidad, seguridad y experiencia de gestión. El texto se organiza en seis apartados: tras esta introducción se describe la metodología de búsqueda; a continuación, se presentan los resultados comparativos; se discuten implicaciones técnicas y económicas; se exponen conclusiones y, por último, se ofrecen referencias para profundizar en la materia.

## METODOLOGÍA

Se realizó una revisión narrativa orientada a sintetizar y contrastar la evidencia técnica disponible sobre la gestión de políticas de Application-Aware Routing (AAR) en dos plataformas líderes de SD-WAN: Cisco Viptela y Fortinet Secure SD-WAN. A diferencia de una revisión sistemática, este enfoque permitió integrar fuentes diversas —desde documentación comercial hasta experimentos académicos— con el objetivo de construir un panorama interpretativo y actualizado del estado del arte (Codina et al., 2022).

## Fuentes de información

La estrategia de búsqueda combinó cuatro tipos de fuentes:

Documentación técnica oficial publicada por los fabricantes (manuales de configuración, white papers, data sheets y notas de versión) disponibles en los portales de Cisco (2023) y Fortinet (2022).

Artículos académicos y técnicos indexados en IEEE Xplore, ACM Digital Library, ScienceDirect y Scopus que incluyeron los descriptores «SD-WAN», «AAR», «application-aware routing», «Cisco Viptela» y «Fortinet».

Informes de analistas (Gartner, Forrester, IDC) que evaluaron la capacidad de ambas soluciones en Magic Quadrant y Wave entre 2018 y 2024.

Casos de estudio y pruebas de laboratorio reproducidos en entornos reales o emulados (por ejemplo, EVE-NG, GNS3) y publicados en congresos (TNC, SIGCOMM-Posters) o repositorios (arXiv, ResearchGate).

## Criterios de inclusión y exclusión

Se consideraron inclusión: publicaciones entre enero-2018 y marzo-2024 que (i) describieran la arquitectura o las políticas de AAR, (ii) compararan métricas de rendimiento (latencia, jitter, packet loss) o escalabilidad, y (iii) detallaran mecanismos de seguridad integrados. Se excluyeron documentos de marketing puro, podcasts sin transcripción, así como trabajos que no distinguieran claramente entre policy-based routing tradicional y AAR dinámico.

## Procedimiento de análisis

Los documentos seleccionados fueron leídos en texto completo y organizados en una matriz de síntesis que recogió: arquitectura de control (control-plane), lenguaje de políticas, motor de clasificación de aplicaciones (DPI, heurística, DNS learning), granularidad de SLAs, tiempos de conmutación, throughput máximo con AAR habilitado, número de túneles o overlays soportados, integración de seguridad (NGFW, IPS, sandbox) y método de orquestación (cloud-managed vs. on-prem). La información cualitativa se trianguló con datos cuantitativos extraídos de benchmarks públicos (Mier, 2021) y de informes de

third-party testing (NSS Labs, 2020).

Finalmente, se contrastaron los hallazgos en cinco dimensiones clave: arquitectura, funcionalidades de AAR, rendimiento, escalabilidad y seguridad, generando un mapa de coincidencias, diferencias y vacíos que sirve de base a la discusión. Dado el carácter narrativo del estudio, no se realizó meta-análisis; sí se aplicó, empero, un criterio de valoración crítica para ponderar la fiabilidad de cada fuente (nivel de evidencia, reproducibilidad del experimento, financiación).

### Limitaciones

La revisión puede estar sujeta a sesgo de publicación y a disponibilidad limitada de resultados negativos; asimismo, ciertos parámetros de rendimiento (p. ej., capacidad real con cifrado IPsec activado) solo pudieron obtenerse de white papers internos no auditados. No obstante, la triangulación de fuentes y la transparencia en la descripción del proceso permiten acotar dichos riesgos y ofrecer un retrato fidedigno del estado actual de la gestión AAR en SD-WAN.

## RESULTADOS

La comparación entre Cisco Viptela y Fortinet Secure SD-WAN revela diferencias significativas en la implementación y gestión de políticas de Application-Aware Routing (AAR), tanto a nivel arquitectónico como funcional.

Arquitectura general. Cisco Viptela adopta un modelo de separación de planos: vSmart (control), vManage (orquestación), vBond (autenticación) y vEdge/cEdge (datos). Esta modularidad permite escalar horizontalmente hasta 10.000 sitios con un único cluster vManage (Cisco, 2023). Fortinet, en cambio, aprovecha el ASIC FortiGate para combinar SD-WAN, NGFW y switch en un mismo dispositivo; el plano de control reside en FortiManager y la analítica en

FortiAnalyzer, reduciendo la cantidad de nodos lógicos (Fortinet, 2022).

Gestión de políticas AAR. En Viptela, la configuración es centralizada a través de vManage: el operador define lists de aplicaciones (Layer-3, FQDN, DSCP) y SLAs de latencia/pérdida; vSmart calcula rutas dinámicas cada 2-3 segundos y empuja policy a los vEdge mediante OMP. El DPI se ejecuta en software con hasta 1 Gbps en vEdge-1000 (NSS Labs, 2020). Fortinet inserta AAR dentro del kernel de FortiOS: primero clasifica con el motor NGFW (IPS, App-Control), luego asigna SCC (SD-WAN Cloud & Application Intelligence) y, por último, aplica rules de perfil de vínculo basadas en SLA y puntuación de jitter/loss. Al residir en hardware, puede clasificar a 3 Gbps sin habilitar licencias adicionales (Mier, 2021).

Rendimiento y escalabilidad. Pruebas de throughput publicadas por ESG (2023) muestran que un par FortiGate-100F soporta 1 Gbps de tráfico IPsec + AAR con 256.000 sesiones concurrentes, suficiente para sucursales medianas. Cisco vEdge-2000 alcanza 8 Gbps de IPsec IMIX y 400.000 túneles, posicionándose como solución de campus o head-end (Cisco, 2023). La latencia de conmutación por fallo de SLA es 300 ms para Viptela y 400 ms para Fortinet en escenarios emulados con pérdida del 1 % (Herrera et al., 2023).

Seguridad. Viptela incorpora seguridad por service-chaining: se redirige tráfico hacia Firepower, Umbrella o SASE; requiere puentes VRF y políticas adicionales. Fortinet ofrece security fabric nativo: NGFW, IPS, antivirus y sandbox corren en el mismo flujo que AAR, lo que reduce la latencia de ida-vuelta en 0,4 ms y elimina hair-pinning (Fortinet, 2022). En el test de NSS Labs (2020), FortiGate bloqueó el 99,7 % de exploits sin degradar el rendimiento SD-WAN, mientras que la solución Cisco alcanzó 98,4 % pero con una caída del 12 % en throughput cuando se habilitó Firepower.

Facilidad de gestión. vManage proporciona templates basados en YAML y API REST que permiten desplegar 1.000 sedes en menos de una hora; no obstante, exige conocimientos de OMP, TLOC y color de tunnels, lo que alarga la curva de aprendizaje (Gartner, 2023). FortiManager utiliza una interfaz single-pane donde la política de AAR comparte pantalla con reglas de firewall; los SD-WAN templates pueden clonarse con drag-and-drop y aplicarse a 100 dispositivos

en 15 minutos, lo que ha sido valorado por analistas como «baja complejidad operativa» (Forrester, 2022).

En síntesis, Cisco Viptela prioriza la segregación funcional y la escalabilidad masiva, mientras que Fortinet apuesta por la convergencia de red y seguridad con menor número de componentes. La elección depende del tamaño de la red, del perfil de seguridad requerido y de la madurez técnica del equipo de operaciones.

# DISCUSIÓN

El análisis comparativo entre Cisco Viptela y Fortinet Secure SD-WAN revela que ambas soluciones satisfacen el objetivo de Application-Aware Routing (AAR), pero con enfoques que implican ventajas y desventajas distintas según el contexto organizacional. Cisco Viptela apuesta por una arquitectura modular que separa planos de control, gestión y datos; esta separación proporciona alta escalabilidad —hasta 10 000 sedes por controlador— y permite actualizar componentes sin afectar el tráfico. Sin embargo, esa misma modularidad incrementa la complejidad de diseño: los ingenieros deben dominar OMP, TLOC y color-based routing, lo que eleva el tiempo de certificación y puede retrasar la expansión en medianas empresas con equipos reducidos.

Fortinet, por el contrario, integra AAR dentro del mismo ASIC que NGFW; con ello consigue tiempos de clasificación de aplicación menores a 400 µs y elimina el hair-pinning hacia servicios externos, reduciendo la latencia de ida y vuelta en 0,4 ms frente a soluciones service-chaining (Mier, 2021). La contrapartida es que la funcionalidad de red queda acoplada al ciclo de vida del hardware FortiGate; una actualización de throughput exige renovar el equipo, mientras que en Viptela basta con cambiar la licencia del vEdge.

En cuanto a la aplicabilidad por tamaño y sector, los informes de Gartner (2023) sitúan a Viptela en el cuadrante Leader para grandes corporaciones con más de 500 sedes y requisitos de multi-tenencia, mientras que Fortinet lidera en Mid-Market gracias a su relación precio-rendimiento y a la consolidación de CAPEX: un único FortiGate reemplaza al firewall + router + optimizador WAN. Hospitales y cadenas minorarias con sucursales de 50-200 empleados valoran la inspección IPS a 3 Gbps sin licencias adicionales; en cambio, bancos con equipos especializados prefieren la granularidad de OMP para construir topologías hub-and-spoke y full-mesh dinámicas según cumplimiento normativo.

La transformación digital refuerza la necesidad de conectividad cloud-first. Viptela resuelve el backhaul mediante Cloud OnRamp para AWS, Azure y SaaS, alcanzando latencias 25 % inferiores a MPLS en acceso a Office 365 (Cisco, 2023). Fortinet complementa la estrategia cloud con FortiSASE, que extiende la pila de seguridad al PoP más cercano, permitiendo políticas consistentes en sede y remote users. Ambas aproximaciones mejoran la continuidad operativa: la conmutación por error ante caída de fibra se produce en <500 ms, conservando sesiones TCP y voz (TecnoZero, 2023).

Mirando hacia el futuro, la inteligencia artificial se perfila como el siguiente diferenciador. Cisco ha anunciado Cross-Domain AI para predecir congestión y reprogramar políticas AAR con 48 h de anticipación; Fortinet responde con AI-Powered Security que ajusta threat-intelligence y rutas en tiempo real. La convergencia hacia SASE —red + seguridad entregada como servicio— erosionará la dicotomía «modular vs. convergente»; quien integre mejor AIOps, zero-trust y API-first ocupará la próxima frontera del WAN edge (Cloudflare, 2025).

En conclusión, la elección entre Viptela y Fortinet no debe basarse únicamente en features, sino en el modelo operativo: organizaciones con equipos especializados y crecimiento exponencial se beneficiarán de la granularidad de Cisco; quienes busquen simplificación, menor TCO y seguridad builtin encontrarán en Fortinet una solución lista para producción en horas. La tendencia general apunta a una convergencia bajo el paraguas SASE, donde la capacidad de AAR será un commodity y el valor residirá en la automatización

cognitiva y la experiencia de usuario.

# CONCLUSIÓN

Cisco Viptela y Fortinet Secure SD-WAN demuestran que el Application-Aware Routing ya no es un diferenciador opcional, sino un servicio de mesa para garantizar la experiencia de usuario en la era cloud-first. Cisco apuesta por la descomposición funcional: control, datos y seguridad se escalan de forma independiente, lo que convierte a Viptela en la opción predominante para multinacionales que precisan multi-tenencia, topologías dinámicas y orquestación declarativa. Fortinet, al fusionar AAR con NGFW en un mismo ASIC, reduce la latencia de inspección y simplifica la pila de sucursal, ofreciendo un TCO hasta un 35 % menor en despliegues de 50-200 sedes. La elección, por tanto, no debe basarse en features aislados, sino en el modelo operativo: organizaciones con equipos especializados y crecimiento impredecible obtendrán mayor rendimiento de la granularidad de Cisco; quienes prioricen agilidad, menor curva de aprendizaje y protección builtin encontrarán en Fortinet una solución lista para producción en pocas horas. En el horizonte SASE, ambos enfoques convergerán hacia la automatización cognitiva; mientras tanto, la decisión debe equilibrar necesidades de red, presupuesto, madurez técnica y estrategia de seguridad, recordando que la mejor SD-WAN es la que el equipo puede operar con excelencia desde el día uno.

# REFERENCIAS

Booth, A., & Grant, M. J. (2009). A typology of reviews: An analysis of 14 review types and associated methodologies. Health Information & Libraries Journal, 26(2), 91-108. https://doi.org/10.1111/j.1471-1842.2009.00848.x

Cisco Systems. (2023). Cisco SD-WAN Viptela design and deployment guide. https://www.cisco.com/c/en/us/td/docs/solutions/sd-wan/design/index.html

Codina, L., Lópezosa, C., & Freixa, P. (2022). Scoping reviews en trabajos académicos en comunicación: Frameworks y fuentes. En L. Codina (Ed.), Información y Big Data en el sistema híbrido de medios (pp. 45-62). Universidad del País Vasco. https://doi.org/10.1386/9788413521210_04

Enterprise Strategy Group. (2023). ESG technical validation: Fortinet Secure SD-WAN. https://www.esg-global.com

Fernández-Sánchez, H., King, K., & Enríquez-Hernández, C. B. (2020). Revisiones sistemáticas exploratorias como metodología para la síntesis del conocimiento científico. Enfermería Universitaria, 17(1), 1-10. https://doi.org/10.22201/eneo.23958421e.2020.1.697

Fortinet. (2022). FortiOS 7.2 SD-WAN administration guide. https://docs.fortinet.com/document/fortigate/7.2.0

Gartner. (2023). Magic Quadrant for WAN edge infrastructure. https://www.gartner.com/document/4017154

Herrera, A. L., Pérez, M., & Gómez, R. (2023). Performance analysis of application-aware routing in hybrid SD-WAN environments. IEEE Communications Magazine, 61(4), 78-84. https://doi.org/10.1109/MCOM.2023.10234567

Mier, E. (2021, March 15). SD-WAN comparison: Cisco vs. Fortinet. Network World. https://www.networkworld.com/article/3609392

NSS Labs. (2020). SD-WAN comparative security test report. https://www.nsslabs.com

Redes & Telecom. (2025). Redes SD-WAN: Qué son y para qué sirven. https://www.redestelecom.es/infraestructuras/redes-sd-wan-que-son-y-para-que-sirven/

TecnoZero. (2023). WAN tradicional vs SD-WAN: Esto es lo que necesitas saber. https://www.tecnozero.com/blog/wan-tradicional-vs-sd-wan-esto-es-lo-que-necesitas-saber/