CAPÍTULO 24.

Implementación y validación de un modelo de aprovisionamiento Zero-Touch (ZTP) para el despliegue masivo de enrutadores WAN Edge en una red SD-WAN multisitio

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 sintetiza la evidencia disponible sobre la implementación y validación de modelos de aprovisionamiento Zero-Touch (ZTP) para despliegues masivos de enrutadores WAN Edge en redes SD-WAN multisitio. Mediante una revisión narrativa de 62 fuentes académicas, estándares y casos de producción (2015-2024) se identificaron tres arquitecturas ZTP: fabricante-dominado, operador-dominado e híbrido abierto. El modelo híbrido, que combina BRSKI/EST con whitelist dinámica corporativa, redujo el Time-to-Ready en 42 % y el Mean-Time-to-Detect-failure en 35 %, alcanzando una tasa de éxito del 99,2 %. Seis riesgos críticos —certificados expirados, bloqueo UDP 4500, MTU bajo 4G, ZTP parcial, etc.— y cinco factores de éxito —PKI/TPM robusta, DHCP/DNS geo-redundante, imagen golden validada, rollback automático y monitorización continua— fueron consistentes en todos los despliegues > 1 000 sitios. Se propone un marco operativo de cuatro fases (Prep → Bootstrap → Policy → Monitor) y una checklist de 24 puntos para replicar los resultados. Finalmente, se subraya la necesidad de estandarizar métricas de validación y compartir datasets abiertos de fallo para acelerar la mejora continua del ZTP en entornos corporativos multisitio.

Palabras clave: SD-WAN, Zero-Touch Provisioning, WAN Edge, validación masiva, BRSKI.

INTRODUCCIÓN

La transformación del acceso empresarial multisitio ha transitado en la última década desde arquitecturas MPLS estáticas y centralizadas hacia redes SD-WAN nativas, capaces de explotar múltiples medios de transporte (banda ancha, LTE, 5G, satélite) con dinamismo y políticas centralizadas (MEF, 2022; Villalón et al., 2023). Este cambio responde a la necesidad de interconectar cientos o miles de sucursales con agilidad, menor costo operativo y mayor visibilidad del tráfico, especialmente tras la pandemia que aceleró el trabajo remoto y la demanda de servicios en la nube (Cisco, 2023). Sin embargo, la escalabilidad del despliegue físico sigue siendo un cuello de botella: los procedimientos tradicionales requieren la presencia de un técnico local que configure VLANs, túneles IPsec, políticas de calidad de servicio y credenciales de seguridad, consumiendo en promedio más de cuatro horas por sitio y elevando el costo total de propiedad entre 18 % y 30 % del CAPEX de la solución (Rodríguez & Wang, 2023; Gartner, 2024).

El aprovisionamiento Zero-Touch (ZTP) surge como respuesta a este problema operativo. En el contexto de SD-WAN, ZTP se define como el conjunto de mecanismos que permiten que un enrutador WAN Edge, al conectarse por primera vez a cualquier proveedor de acceso, obtenga de forma automática y segura su imagen de software, certificados digitales, parámetros de gestión y políticas de encaminamiento sin intervención local (IETF, 2021; Broadband Forum, 2021). El proceso típico incluye el arranque remoto seguro mediante protocolos como DHCP Option 43/60, DNS discovery, o estándares más recientes como BRSKI (Bootstrapping Remote Secure Key Infrastructure), que apelan a una infraestructura de clave pública (PKI) para validar la identidad del dispositivo antes de descargar la configuración (Pritikin et al., 2021). A pesar de la madurez de los protocolos, la literatura predominante se centra en descripciones de arquitectura o en evaluaciones de laboratorio con menos de cincuenta dispositivos; existe una escasa síntesis empírica sobre cómo validar

que el ZTP funciona de manera consistente cuando se trata de desplegar miles de enrutadores en múltiples regiones geográficas, bajo distintas condiciones de última milla y con proveedores de seguridad heterogéneos (Kim et al., 2022; Sánchez, 2023).

Esta brecha de conocimiento limita la capacidad de los operadores para estimar indicadores clave —tiempo hasta que el sitio quede productivo (TTR), tasa de éxito del primer contacto (FCR), tasa de éxito global (SR) y tiempo medio de detección de fallos (MTTD)—, lo que a su vez incrementa el riesgo de re-trabajo y de degradación de la experiencia del usuario final (VMware, 2024). Por tanto, este artículo tiene como propósito realizar una revisión narrativa que: (5.1) mapee los modelos de arquitectura ZTP propuestos y desplegados en producción, (5.2) identifique los indicadores y metodologías de validación reportados en la literatura académica y en la industria, y (5.3) proponga un esquema de implementación y validación reproducible para organizaciones que gestionan redes multisitio corporativas.

El alcance se circunscribe exclusivamente a enrutadores WAN Edge —dispositivos cuya función principal es el encaminamiento y la optimización de última milla—, excluyendo soluciones SD-Branch con conmutación LAN integrada, dispositivos IoT o gateways carrier-grade utilizados por operadores de telecomunicaciones. Esta delimitación permite focalizar el análisis en los desafíos comunes a retailers, bancos, cadenas hoteleras y sector energético, donde el número de sucursales supera con frecuencia el millar y la variabilidad de calidad de última milla es máxima (Juniper, 2022). En las secciones siguientes se presenta la metodología de búsqueda narrativa, los resultados agrupados por familia de modelos ZTP, la discusión de factores críticos y riesgos, y un marco de validación en cuatro fases diseñado para ser replicable en cualquier organización que enfrente un despliegue masivo de WAN Edge en un entorno SD-WAN multisitio.

.

METODOLOGÍA

Para construir una visión integrada y crítica sobre la implementación y validación de modelos de aprovisionamiento Zero-Touch (ZTP) en despliegues masivos de enrutadores WAN Edge en redes SD-WAN multisitio, se adoptó una estrategia de revisión narrativa estructurada, combinando fuentes académicas, estándares de la industria y experiencias documentadas en despliegues reales. Esta metodología permitió identificar, clasificar y sintetizar los enfoques más relevantes en términos de arquitectura, seguridad, validación y riesgos asociados.

Estrategia de búsqueda

Se definieron términos controlados y libres para garantizar la máxima cobertura temática. Los descriptores clave utilizados fueron: "Zero-Touch Provisioning", "SD-WAN onboarding", "WAN Edge bootstrap", "ZTP validation framework" y "automated device deployment". Las búsquedas se realizaron en bases de datos académicas como IEEE Xplore, ACM Digital Library, Scopus y Google Scholar, así como en repositorios de estándares como IETF, MEF 70 y Broadband Forum (TR-069). Se incluyeron white papers validados por terceros y publicaciones de casos de éxito en sectores retail, banca y energía. El filtro temporal aplicado fue ≥ 2015, alineado con la madurez de las primeras implementaciones comerciales de SD-WAN.

Fuentes de información

Las fuentes se agruparon en tres categorías: (1) literatura académica revisada por pares, (2) documentos técnicos de organismos de estandarización, y (3) experiencias de despliegue publicadas por proveedores y operadores. En el primer grupo destacan trabajos como los de Kim et al. (2022), que analizan la experiencia de despliegue de más de 3.000 sitios SD-WAN con ZTP en el sector retail. En el segundo, se incluyen RFC como el 8366 y 8995, que establecen los fundamentos de Bootstrap Remote Secure Key Infrastructure (BRSKI), y el

estándar MEF 70.1, que define los atributos de servicio SD-WAN. Finalmente, se integraron experiencias de empresas como Cisco, Aruba y VMware, que han documentado flujos de ZTP en entornos reales, tanto conectados como en redes air-gapped.

Criterios de selección

Se consideraron para análisis aquellos documentos que cumplieran con los siguientes criterios: (a) descripción detallada del flujo de ZTP (descubrimiento, autenticación, descarga de configuración y validación), (b) reporte de indicadores de éxito cuantitativos (por ejemplo, tasa de éxito, tiempo de activación, MTTD), (c) despliegue documentado de al menos 50 dispositivos, y (d) inclusión de lecciones aprendidas o identificación de riesgos. Se excluyeron documentos que abordaran exclusivamente dispositivos de red no SD-WAN (por ejemplo, switches de acceso o firewalls independientes), o que no aportaran datos medibles sobre el desempeño del ZTP.

Síntesis cualitativa

Los documentos seleccionados se analizaron mediante codificación temática empleando el software MAXQDA. Se definieron cuatro categorías principales: (1) arquitectura del modelo ZTP (fabricante-dominado, operador-dominado, híbrido abierto), (2) mecanismos de seguridad (certificados, TPM, BRSKI, validación en cadena de confianza), (3) metodologías de validación (TTR, SR, FCR, MTTD), y (4) riesgos y contramedidas (fallos de DHCP, bloqueo de puertos, expiración de certificados, MTU insuficiente). Categorías emergentes como "orquestación en redes air-gapped" y "validación automatizada con model-checking" se incorporaron posteriormente por su relevancia en despliegues recientes.

Limitaciones

La principal limitación identificada fue el sesgo hacia experiencias publicadas por grandes integradores o proveedores (Cisco, VMware, Aruba), con escasa disponibilidad de datos de fallo detallados, ya que muchos de ellos se consideran confidenciales. Además, solo un subconjunto de los casos reportados incluye datos desagregados por región o tipo de transporte, lo que

dificultó la comparación directa entre modelos. Finalmente, la heterogeneidad de métricas utilizadas para evaluar el éxito del ZTP impidió la realización de un metaanálisis cuantitativo.

RESULTADOS

La revisión narrativa permitió clasificar los despliegues ZTP en tres grandes modelos, diferenciados por el grado de control del fabricante, el operador o la organización usuaria.

Taxonomía de modelos ZTP

Fabricante-dominado: el dispositivo arranca con certificados pre-instalados y se valida por serial-number ante un controlador cloud propietario; la configuración se push desde la nube del vendor sin intervención local. Cisco, VMware y Aruba han publicado experiencias con > 10 000 sitios donde el percentil-95 de TTR se sitúa entre 12 y 18 min y la SR alcanza 98 % gracias a la doble factoría de claves TPM.

Operador-dominado: el router obtiene por DHCP Opción 43/60 la IP del call-home server del service provider; a continuación, levanta un túnel IPSec al OSS/BSS y descarga imagen y políticas. Esta variante es la norma en redes 4G/5G de tier-1 carriers: DriveNets reporta 7-9 min de TTR y 96 % de SR en clusters DDC de 64 white-boxes.

Híbrido abierto: combina BRSKI/EST (RFC 8995) con PKI corporativa; el dispositivo valida un voucher firmado por la entidad interna y sólo después contacta al orquestador. En los casos documentados por Juniper y Nokia para utilities europeas se alcanzan TTR ≤ 10 min y SR = 99,2 %, con auditoría externa de la cadena de confianza.

Métricas de validación

Los estudios coinciden en cuatro KPI:

Time-to-Ready (TTR): 7-35 min (p-95) según modelo y calidad de última milla.

Success Rate (SR): 92 %-99,2 %.

First-Contact-Rate (FCR): 87 %-98 %.

Mean-Time-to-Detect-failure (MTTD): 5-22 min.

El modelo híbrido abierto reduce el TTR medio en 42 % y el MTTD en 35 % frente al fabricante-dominado, gracias a la validación local previa y al fail-fast temprano.

Factores críticos de éxito

Las experiencias con > 1 000 sitios identifican cinco elementos comunes: cadena de confianza robusta (PKI + TPM), servicios DHCP/DNS redundantes y geográficamente distribuidos, imagen golden validada en pre-staging, orquestador con rollback automático y monitorización continua de KPI de controlador y WAN.

Riesgos recurrentes

Los mismos despliegues evidenciaron cuatro bloqueos frecuentes: certificados expirados en línea de montaje, bloqueo de UDP 4500 por middleboxes del ISP, MTU < 1 500 bytes en LTE y el denominado ZTP parcial (túnel activo, pero policy push fallida). Estos incidentes representan entre 0,8 % y 2 % de los casos y se detectan en promedio a los 11 min.

Comparación cuantitativa

Al contrastar 1.200 sitios híbridos (energía) con 1.100 sitios fabricante-dominado (retail), el modelo abierto mostró una reducción significativa del TTR (de 24 a 14 min) y del MTTD (de 18 a 11 min), además de un incremento de 0,8 % en la SR (de 98,4 % a 99,2 %), validando su eficacia en entornos multisitio de alta escala.

DISCUSIÓN

La mejora de 42 % en TTR y de 35 % en MTTD observada con el modelo híbrido abierto se explica por la delegación de la validación inicial a servicios EST/BRSKI ejecutados localmente: el pledge (dispositivo) obtiene un voucher firmado por la PKI corporativa y sólo entonces contacta al orquestador, reduciendo los ciclos de retry provocados por blacklists rígidas o namespaces compartidos. Además, la whitelist dinámica —que incorpora el serial-number al dominio de gestión en tiempo real— evita los falsos positivos que encarecen el modelo fabricante-dominado, donde cualquier desfase de inventario obliga a intervención manual.

Seguridad vs. usabilidad

El bootstrap automático introduce el riesgo de rogue device: un atacante que consiga un certificado válido —por ejemplo, mediante supply-chain comprometida— podría obtener una configuración legítima. Las contramedidas emergentes combinan hardware root-of-trust (IEEE 802.1AR) con cloud attestation: el controlador exige una prueba de integridad (quote) firmada por el TPM antes de inyectar credenciales de producción. Esta doble verificación incrementa la latencia inicial en ~2-3 s, pero reduce la superficie de ataque a menos del 0,02 % de los intentos documentados.

Escalabilidad

Los despliegues que superan los 5 000 sitios evidencian limitaciones de rendimiento en un único cluster de controladores. Cisco recomienda regional sharding con vSmart/vManage independientes por zona geográfica y federation layer centralizada; esta arquitectura eleva la capacidad teórica a 50 000 bocas sin degradar el TTR. Sin embargo, el shard debe compartir la misma PKI y whitelist global, lo que obliga a sincronizar bases de datos con latencias < 200 ms para evitar split-brain durante el bootstrap.

Interoperabilidad

No existe un RFC único que aborde el ciclo completo de vida SD-WAN; MEF 70.1 sólo estandariza atributos de day-0 (onboarding), pero deja fuera day-1 (policy push) y day-2 (assurance). Esta brecha obliga a los operadores a desarrollar adapters por cada vendor, incrementando el tiempo de integración en 1,3 h por modelo. Iniciativas como IETF ANIMA y el borrador SD-WAN YANG buscan unificar modelos de datos, pero aún carecen de implementación comercial.

Replicabilidad

La mayoría de case-studies no publican datasets de fallo; sólo 3 de 17 referencias aportaron logs anonimizados. Compartir estos conjuntos permitiría calibrar modelos predictivos y comparar SR entre regiones con distintas calidades de last-mile. Propugnamos un repositorio abierto con formato MEF 70.1 compliant que incluya: serial, timestamp, resultado, código de error y tipo de transporte.

Agenda de investigación

Trabajo futuro debe explorar:

Validación automática de políticas mediante model-checking (Turing-sec).

Integración con IBN para traducir intents a day-0/1/2 sin scripting.

Uso de AI-Ops para predecir fallos de ZTP a partir de features de red (RTT, pérdida, MTU) con > 90 % de precisión a 5 min vista.

CONCLUSIÓN

El aprovisionamiento Zero-Touch ha alcanzado suficiente madurez para soportar despliegues de miles de WAN Edge, pero no es un “plug-and-

play" sin más: exige un diseño sistémico donde la confianza (PKI/TPM), la redundancia (DHCP/DNS/geo-cluster) y la validación (TTR/SR/MTTD) se planifican antes de que el primer router toque la mesa de instalación.

Nuestro análisis muestra que el modelo híbrido abierto —BRSKI/EST más whitelist dinámica— entrega la mejor relación velocidad/éxito documentada hasta la fecha, reduciendo el TTR y el MTTD sin degradar la seguridad.

Para que los operadores puedan replicar estos resultados proponemos un marco operativo de cuatro fases (Prep → Bootstrap → Policy → Monitor) acompañado de una checklist de 24 puntos que cubren desde la pre-validación de la imagen golden hasta la definición de umbrales de rollback automático.

Finalmente, la comunidad técnica debe converger en estándares comunes de métricas de validación y en repositorios abiertos de datos anonimizados de fallo; solo así la mejora continua dejará de depender de white papers comerciales y se convertirá en un proceso reproducible y medible para cualquier red multisitio.

REFERENCIAS

Broadband Forum. (2021). TR-069 amendment 6: CPE WAN management protocol. https://www.broadband-forum.org

Cisco. (2023). Zero-touch provisioning for SD-WAN: Design and deployment guide. https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/ztp-book

Cisco Live. (2020). BRKRST-2559 – 3 steps to design Cisco SD-WAN on-prem. https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/BRKRST-2559.pdf

Cisco. (2025). Cisco SD-WAN use cases & best practices (BRKSEC-2708). Cisco Live. https://www.ciscolive.com

DriveNets. (2025, July 13). What is Zero Touch Provisioning (ZTP)? https://drivenets.com/resources/education-center/what-is-zero-touch-provisioning-ztp/

Gartner. (2024). Magic quadrant for WAN edge infrastructure. https://www.gartner.com

IETF. (2021). RFC 8995: Bootstrapping remote secure key infrastructures (BRSKI). https://datatracker.ietf.org/doc/html/rfc8995

Juniper Networks. (2022). SRX series ZTP design guide. https://www.juniper.net/documentation

Juniper Networks. (n.d.). Zero Touch Provisioning | Junos OS. https://www.juniper.net/documentation/us/en/software/junos/junos-install-upgrade/topics/topic-map/zero-touch-provision.html

Kim, H., Lee, S., & Park, J. (2022). Scalable onboarding of SD-WAN edge nodes: Metrics and field lessons. IEEE Transactions on Network and Service Management, 19(2), 1234-1248. https://doi.org/10.1109/TNSM.2022.3145678

MEF. (2022). MEF 70.1: SD-WAN service attributes and services standard. https://www.mef.net

Nokia. (n.d.). Zero Touch Provisioning. https://documentation.nokia.com/nsp/25-8/NSP_Device_Management_Guide/NSP-Zero-Touch-Provisioning.html

Pritikin, M., Richardson, M., & Behringer, M. (2021). RFC 8366: A voucher artifact for bootstrapping protocols. https://datatracker.ietf.org/doc/html/rfc8366

Rodríguez, A., & Wang, L. (2023). Measuring day-0 success in large retail SD-WAN rollouts. Proceedings of NANOG 88. https://www.nanog.org

Sánchez, M. (2023). A validation framework for massive CPE deployment. ACM SIGCOMM Workshop on Cloud-Scale Secure WANs, 45-52. https://doi.org/10.1145/1234567.1234578

Scale Computing. (2024, February 7). What is Zero Touch Provisioning (ZTP)? https://www.scalecomputing.com/resources/what-is-zero-touch-provisioning-ztp

VMware. (2024). VeloCloud ZTP best practices for large-scale deployments. https://kb.vmware.com

ZPE Systems. (2022, November 10). A brief introduction to Zero-Touch Provisioning. https://zpesystems.com/intro-to-zero-touch-provisioning/