TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 19 No. 2, Mayo-Agosto, 2020, p.79- 85 ISSN 1729-3804

MODIFICACIONES A LA ARQUITECTURA DE GESTIÓN DE REDES BASADA EN POLÍTICAS

Mónica Peña Casanova[1], Caridad Anías Calderón[2]

[1]Universidad de las Ciencias Informáticas, UCI, Carretera a San Antonio Km 2 1/2, [2]Universidad Tecnológica de La Habana "José Antonio Echeverría", CUJAE, Calle 114 ·11901 entre Ciclo Vía y Rotonda, Mario, La Habana

[1]e-mail: monica@uci.cu

[2]e-mail: cacha@tesla.cujae.edu.cu

RESUMEN

La Gestión de Redes Basada en Política (PBNM del inglés Policy Based Network Management) permite controlar y coordinar, de manera dinámica, los elementos de red y automatizar el proceso de toma de decisiones en la misma. En ambientes distribuidos y heterogéneos es necesario incorporar a esa tecnología elementos que jerarquicen la toma de decisiones y creen la capacidad de comprender distintas definiciones de diferentes modelos de información. Esto a modo de reducir la complejidad y los costos de la gestión de redes asociados con la instalación y actualización del hardware y el software de computadoras, su configuración y mantenimiento. En el presente documento se propone un conjunto de modificaciones a la arquitectura de PBNM propuesta por el IETF, al emplear dos modelos de información: el Modelo Común de Información (CIM del inglés Common Information Model) y Redes Habilitadas para Directorio-nueva generación (DEN-ng del inglés Directory Enabled Network- next generation), los cuales facilitan la integración de modelos de gestión estandarizados y propietarios. Además, como parte de las modificaciones propuestas, se jerarquiza la toma de decisiones en dicha arquitectura otorgándole la capacidad de detectar y resolver conflictos entre las políticas ejecutadas.

PALABRAS CLAVES: Gestión de redes basada en políticas, Modelo común de información, políticas TI, Gestión integrada de redes, Redes Definidas por Software.

POLICY BASED NETWORK MANAGEMENT ARCHITECTURE MODIFICATIONS

ABSTRACT

Policy-based network management (PBNM) allows the dynamic control and coordination of network elements and the automatization of the decision-making process in the network. In distributed and heterogeneous environments, it is necessary to incorporate elements that hierarchize decision making and create the ability to understand different definitions of different information models to reduce the complexity and costs of network management associated with installation and updating. of computer hardware and software, its configuration and maintenance. This document proposes a set of modifications to the PBNM architecture using two information models: Common Information Model (CIM) and Directory Enabled Network- next generation (DEN-ng) which facilitate the integration of standardized and proprietary management models. Besides, the decision takes to process is hierarchized and it gives it the ability to identify and resolve conflicts between the policies implemented.

KEY WORDS: Policy-Based Network Management, Common Information Model, IT Policy, Integrated Network Management, Software Defined Networks

1. INTRODUCCIÓN

El éxito de la introducción de las Tecnologías de la Información (TI) en las organizaciones está determinado por la gestión que se realiza de las mismas, a través de la habilitación de un conjunto de capacidades que forman parte de las prácticas de gestión. El escenario actual, caracterizado por la celeridad de los cambios tecnológicos, la heterogeneidad de tecnologías disponibles, la dispersión que tienen los recursos gestionados; condiciona que los modelos de gestión deban ser independientes de las soluciones tecnológicas, integrados y en la medida de los posible, con comportamientos autonómicos [1]–[3]. Una alternativa a la solución de este problema es la gestión de red basada en políticas la cual permite controlar y coordinar, de manera dinámica los elementos de red, tomando decisiones de forma automática a través de reglas, peticiones de usuarios o de servicios [4]–[6].

Sin embargo, la gestión de redes basadas en políticas no es suficiente para lograr una interoperabilidad entre los sistemas de gestión de red existente. Es necesario seleccionar modelos de información pertenecientes a modelos de gestión estandarizados a partir de sus posibilidades de representación de políticas, así como la capacidad que poseen

de interoperar en este ámbito de la gestión basada en políticas. Por otra parte, la gestión basada en políticas no está exenta de la ocurrencia de conflictos entre las políticas que se ejecutan. Por todo lo anterior, en el presente trabajo se proponen modificaciones a la arquitectura PBNM propuesta por el IETF que facilitan la integración de modelos de gestión estandarizados y propietarios y la solución de conflictos entre políticas. Con ello se permite la automatización de la ejecución de políticas sobre infraestructuras TI heterogéneas y la reduciendo de la complejidad.

2. DESCRIPCIÓN DE LA GESTIÓN BASADA EN POLÍTICAS Y LOS MODELOS DE INFORMACIÓN ASOCIADOS

Westerinen y más adelante Strassner [1], [7], [8], define las políticas como un conjunto de reglas que se utilizan para gestionar y mantener el control de los cambios y/o conservar el estado de uno o varios objetos gestionados. La mayor parte de los sistemas poseen restricciones relacionadas con el tiempo para su operación. Una vía para controlar y coordinar de manera dinámica los elementos de red, tomando decisiones de forma automática a través de reglas y de peticiones de usuarios o de servicios, es la PBNM.

Según el grupo de trabajo del IETF, un modelo de gestión basado en políticas, incluye un contenedor o repositorio de políticas, un punto de decisión de políticas o servidor de políticas (PDP) y uno o varios puntos de ejecución de políticas (PEP). En los PEP se aplican o ejecutan las políticas que gobiernan los dispositivos físicos. El PDP revisa las políticas almacenadas en el contenedor de políticas y efectúa un proceso de toma de decisiones, con independencia de las características de los dispositivos asociados a los PEP. Son los PEP los encargados de traducir las políticas en operaciones o comandos específicos, que puedan ser interpretados por los elementos gestionados por ellos. La Fig. 1 muestra una arquitectura general para un sistema PBNM siguiendo la filosofía cliente-servidor [8].

Para el funcionamiento alineado de PBNM, se requiere diseñar políticas a nivel de negocio y estratificarlas hasta las instancias que se ejecutarán en los PEP. Por otra parte, al segmentar la gestión en dominios, PBNM posee dificultades para el tratamiento de conflictos entre las políticas que se aplican a las diferentes áreas de influencia. Además, cuando se emplea esta arquitectura, es muy importante ser cuidadosos en la selección de los modelos de información que se utilizarán. Ellos determinan la operación sobre múltiples soluciones de gestión integrada, así como soluciones propietarias y contribuyen a la predictibilidad, eficiencia [39].

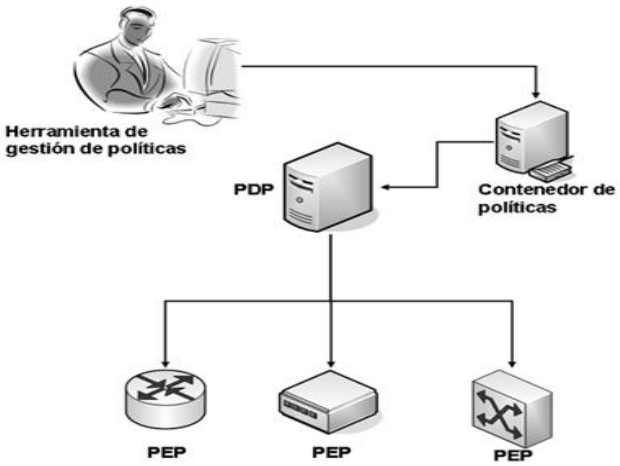

Figura 1: Arquitectura PBNM propuesta por el IETF (basado en [8]).

La definición de políticas en la PBNM se ha trabajado de dos maneras: con la dupla condición-acción, la cual tiene problemas para las capacidades de predicción (no se pueden ejecutar políticas hasta que las condiciones que se evalúan son visibles o perceptibles en la red y los servicios) y de eficiencia (chequear constantemente la ocurrencia de condiciones implica un costo computacional alto); y con la tríada evento-condición-acción, que permite al sistema determinar cuándo serán evaluadas las condiciones a través de eventos [9]. Los eventos de políticas representan los estados del sistema que son relevantes en el contexto de los objetivos de negocio y su realización operacional. Las acciones de políticas son las respuestas deseadas por la organización en caso de que ocurra uno o más eventos de políticas. Las reglas de políticas son los mecanismos que enlazan los eventos de políticas con las acciones de políticas [10].

Para identificar la vigencia del empleo de la PBNM hoy la arquitectura PBNM se aplica a la gestión de diferentes tecnologías [4], [11], [12]: PBNM SDN, PBNM Cloud, PBNM NFV, PBNM Datacenter; de manera creciente. El atributo más importante que ofrece la PBNM es que ofrece cierta abstracción útil para manejar la brecha que existe entre las necesidades del negocio y las políticas de TI a este nivel y el funcionamiento de los elementos de red. Dichas políticas gobiernan el funcionamiento en tiempo real de la infraestructura y proporcionan un poderoso mecanismo para lograr cierto nivel de autonomía en la gestión, alineada así a las necesidades de la organización [13].

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 19 No. 2, Mayo-Agosto, 2020, p.79- 85 ISSN 1729-3804

Para realizar una gestión verdaderamente integrada a través de un modelo de información único, es necesario crear la capacidad de comprender distintas definiciones de diferentes modelos de información. Una vía para tener un control holístico sobre la red y los recursos que forman parte de ella, automatizando las tareas de control, es la gestión basada en políticas. De esta forma es posible aplicar una política de gestión común a los recursos, independiente del modelo de información para el cual fueron definidos.

Con el objetivo de efectuar un análisis crítico de los modelos de información abordados con anterioridad, se definieron un conjunto de criterios, obteniéndose los resultados que se muestran en [14]. Uno de los criterios de evaluación seleccionado para realizar el cotejo es el tipo de modelo, para precisar si son modelos de información genéricos o si se han implementado en tecnologías específicas, como es el caso de los modelos de datos. Los modelos de información cuentan con interfaces bien definidas, sin ambigüedades, abiertos para la implementación, generalmente escalables e independientes de la tecnología, lo que ofrece apertura para los entornos de ejecución de los mismos. Adicionalmente se confrontan los modelos en la integrabilidad, es decir la posibilidad del modelo de información de operar en los modelos de gestión existentes.

La representación de la información de gestión orientada a objetos, es la más adecuada para la representación de políticas ya que facilitan la reutilización, extensibilidad y gestión (creación-borrado-modificación) de las mismas. El soporte a políticas se valora sobre la base de que los lenguajes sean declarativos, permitan el análisis de las políticas creadas, así como la detección de conflictos e inconsistencias entre las mismas. Además, se evalúa que posean facilidad inherente para la estratificación de políticas, es decir la traducción y procesamiento en diferentes niveles de abstracción. Sobre este elemento se profundiza en el criterio tipo de políticas que representan. En ello se valora si los modelos solamente son capaces de representar políticas a bajo nivel (técnico) o si pueden relacionar estas a las necesidades de la organización. Finalmente, se considera la generalización o uso del modelo de información en un ámbito de aplicación amplio, lo cual impacta en la facilidad de adopción y despliegue del mismo.

En [14] se puede apreciar que CIM, SID y DEN-ng son modelos de información, de alta integrabilidad y soporte para la representación de políticas. También se evidencia que la mayor parte de los modelos de información han evolucionado para aprovechar las ventajas de la programación orientada a objetos. Los modelos de información con mayor generalización en su uso son CIM y SMI de SNMP. CIM se destaca por ser el modelo con mayor integrabilidad, lo cual logra gracias a su gestor de objetos, CIMOM que abarca no solamente modelos de gestión estandarizados, sino también algunos propietarios [15], [16].

La capacidad de DEN-ng para representar políticas se considera muy alta, ya que precisa menos recursos para la ejecución de las mismas. La representación ECA empleada por DEN-ng, permite la inclusión, de forma explícita, de eventos que determinan cuándo deben evaluarse las políticas. Además, DEN-ng posibilita la representación del contexto del objeto gestionado [13]. CIM, es un modelo orientado a la extensibilidad, es decir, con capacidad para añadir nuevos tipos de políticas sin tener que redefinirlas completamente. Esto lo garantiza, al permitir la creación de condiciones y acciones propietarias, que solamente tienen que ser interpretadas por el punto de decisión de políticas (PDP) o servidor de políticas que corresponda [15], [16].

3. PROPUESTA DE ARQUITECTURA PBNM MODIFICADA

Para la ejecución de políticas automatizadas en las infraestructuras TI, se propone una modificación a la arquitectura PBNM definida por la IETF. La arquitectura modificada, permite el establecimiento de un enlace entre la configuración de los elementos de la red y las necesidades de la organización, y facilita la detección y corrección de conflictos entre las políticas definidas.

La Fig. 2 muestra la arquitectura PBNM modificada. Dicha modificación consiste en incorporar un Punto de Decisión de Políticas Principal (PDPP). El PDPP tiene una jerarquía superior y puede detectar y resolver conflictos entre políticas. Según lo explicado en el componente diseño de políticas, estos ejecutan una acción para forzar a los PDP a ejecutar políticas para regresar a los PEP a un estado anterior. Lo anterior ocurre, en caso que se manifieste un evento o condición previstos; en la ocurrencia de un evento relacionado con la existencia de conflictos entre las políticas que se ejecutan en las capas jerárquicas inferiores.

Además, se establece el empleo de dos modelos de información, uno a alto nivel y otro a bajo nivel. Como modelo de información para la ejecución de políticas a alto nivel se propone DEN-ng en su versión 7 o superior, entre el PDPP y el PDP. DEN-ng provee capacidad para representar políticas empleando la triada evento-condición-acción. Este elemento habilita la arquitectura para: identificar y resolver conflictos entre las políticas, trabajar con máquina de estado finito y abordar los contextos a partir de su expresividad semántica. La definición de eventos, concede al sistema la posibilidad de determinar cuándo serán evaluadas las condiciones, otorgándole capacidad de respuesta temprana.

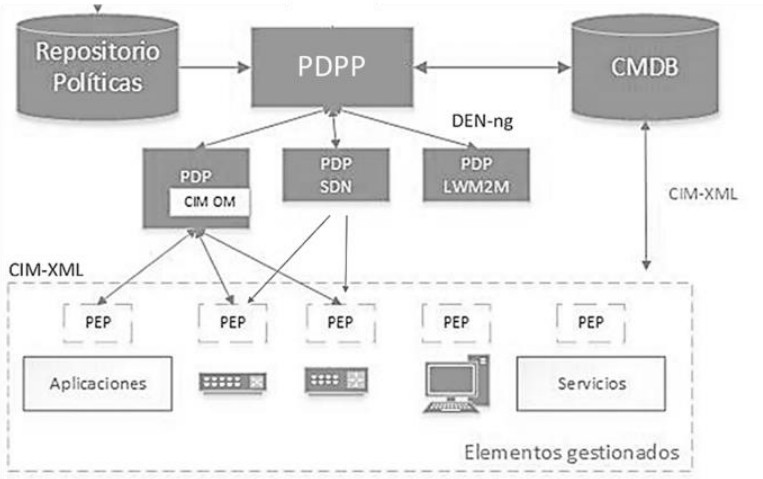

Figura. 2: Propuesta de modificación a la PBNM.

No es necesario que las condiciones sean visibles para que se ejecuten las acciones. Asimismo, al formular las políticas con la triada evento-condición-acción se garantiza mayor eficiencia en el funcionamiento de la arquitectura. Es posible definir eventos a partir de los cuales se evaluarán las condiciones, no teniendo que invertir recursos computacionales y de ancho de banda adicionales, para la evaluación periódica de las mismas.

Para la ejecución de políticas a bajo nivel, se propone el empleo de CIM, del DMTF, como modelo de información entre los PDP y los PEP. CIM, abarca gran cantidad de escenarios de gestión, y tipos de infraestructuras de redes y servicios. Además, permite la operación de la arquitectura tanto en soluciones de gestión integrada como propietaria, ya que es capaz de representar, con mayor integralidad, los diferentes ámbitos de gestión. Su gestor de objetos, CIMOM, se ha extendido hasta comprender los más importantes modelos de gestión estandarizados, así como modelos propietarios. CIMOM, ha desarrollado extensiones para las nuevas tecnologías a gestionar, por ejemplo: las Redes Definidas por Software, la Virtualización de las Funciones de Red y la nube [39]. En general, los elementos que forman parte de la infraestructura subyacente a gestionar soportan implementaciones de CIM.

También se incorpora a la arquitectura propuesta por el IETF, una CMDB. En ella, se registran los atributos de cada instancia de configuración durante su ciclo de vida, las relaciones que la misma posee con otras instancias y los registros vinculados a cada una; por ejemplo, registros de incidentes, problemas o cambios.

ITIL en su versión 3, establece que las CMDB deben almacenar elementos de configuración, asociados al ciclo de vida del servicio, los planes de servicio, los beneficios esperados del mismo y los costos, entre otros. Además, deben contener elementos de configuración del servicio, que abarcan procesos de servicio tales como: las capacidades, los modelos de prestación de servicios y las instancias de servicio. También se recomienda que incorporen, elementos de configuración asociados a las organizaciones entre los que se encuentran: los regulatorios a los que está sujeta dicha organización, las estrategias del negocio, entre otros.

Es importante registrar en la CMDB, elementos de configuración internos y externos. Los elementos de configuración internos comprenden los recursos de los centros de datos, tanto lógicos como físicos. Por su parte, los elementos de configuración externos comprenden la información asociada a proveedores y clientes, acuerdos establecidos y las interfaces a los elementos de configuración que se requieren para que un proveedor entregue un servicio. La CMDB se emplea para la evaluación de condiciones y el registro de las modificaciones que ocurran como resultado de la ejecución de políticas en los PEP.

Para ejecutar las acciones de gestión se utiliza el PDP, especializado en tomar las decisiones de cuáles políticas se deben ejecutar y del procesamiento de las mismas. Esta toma de decisiones, permite alinear las necesidades del negocio con el comportamiento coherente de la infraestructura TI. Para este fin, el PDP transforma las políticas o reglas en representaciones operacionales aptas para ser interpretadas por PEP que se encuentran en los elementos gestionados. Para ello, el PDP debe contar con un motor de inferencia y se basa, para la toma de decisiones, en la información contenida en la CMDB y en el Repositorio de Políticas [14].

Según recomienda el IETF, en el PDP debe existir una aplicación de gestión basada en políticas preferiblemente con interfaz Web, para el monitoreo y control de los elementos que forman parte de la infraestructura que ejecuta las políticas. Dicha aplicación debe permitir modelar las políticas que controlarán el sistema y verificar la no existencia de conflictos entre las políticas existentes, en cada uno de los estratos. Las nuevas políticas de TI que no presentan conflictos con las precedentes, se almacenan en el repositorio de políticas, el cual constituye una base de datos donde se registran todas las políticas a ejecutar.

En el PDPP ocurre el proceso de toma de decisiones de las políticas representadas con la tríada evento-condición-acción. La condición puede contener un conjunto de cláusulas que darán como resultado una condición simple a partir

TELEMÁTICA
REVISTA DIGITAL de las Tecnologías de la Información y las Telecomunicaciones
Revista Telemática. Vol. 19 No. 2, Mayo-Agosto, 2020, p.79- 85 ISSN 1729-3804

de la cual puede evaluarse si esta se satisface consultando la CMDB. En el caso que esté previsto que se ejecuten varias acciones, se establecerá el nivel de prioridad en función de la estrategia de ejecución de las mismas que se define en el PDPP.

4. ANÁLISIS Y DISCUSIÓN DE RESULTADOS

La introducción de las soluciones definidas por software a las redes de telecomunicaciones ha implicado múltiples investigaciones para lograr integrar, su integración a los sistemas de gestión de operaciones en redes. Algunas soluciones han surgido a nivel académico, tales como NetSight [17], OFRewind [18], FlowChecker [19], entre otras. Las cuales se circunscriben a solucionar pequeños problemas y a menudo presentan limitaciones para la automatización y la integración a los flujos de trabajo a nivel de operadores de redes [20]. Algunas organizaciones de estandarización se han dado a la tarea de contribuir en la solución de estas insuficiencias. Por ejemplo el grupo de trabajo del IETF, desarrolla actividades en OAM, IRTF en la RFC 7149 [21] enuncia las preguntas más significativas asociada a la operación de SDN y el Foro de Telegestión investiga en las brechas entre dichas interfaces y la especificación (TR) 228 [22].

Como una alternativa a la solución de este problema y para validar las modificaciones realizadas a la arquitectura PBNM, se desplegó la arquitectura propuesta en para la gestión de una red SDN híbrida en un entorno simulado. La configuración de dicho escenario en la herramienta de simulación GNS3 [23], tal y como se observa en la Fig. 3. El escenario representa una red LAN en la que se implementa un controlador que gestiona la red SDN a través del equipamiento híbrido identificado por el protocolo OpenFlow. Se visualizan, además, un host denominado Admin sobre el que se implementan el repositorio de políticas y la aplicación de monitoreo y control de red Zabbix, y un host Server, el cual presta servicios como DNS, DHCP y FTP a la infraestructura de red tradicional.

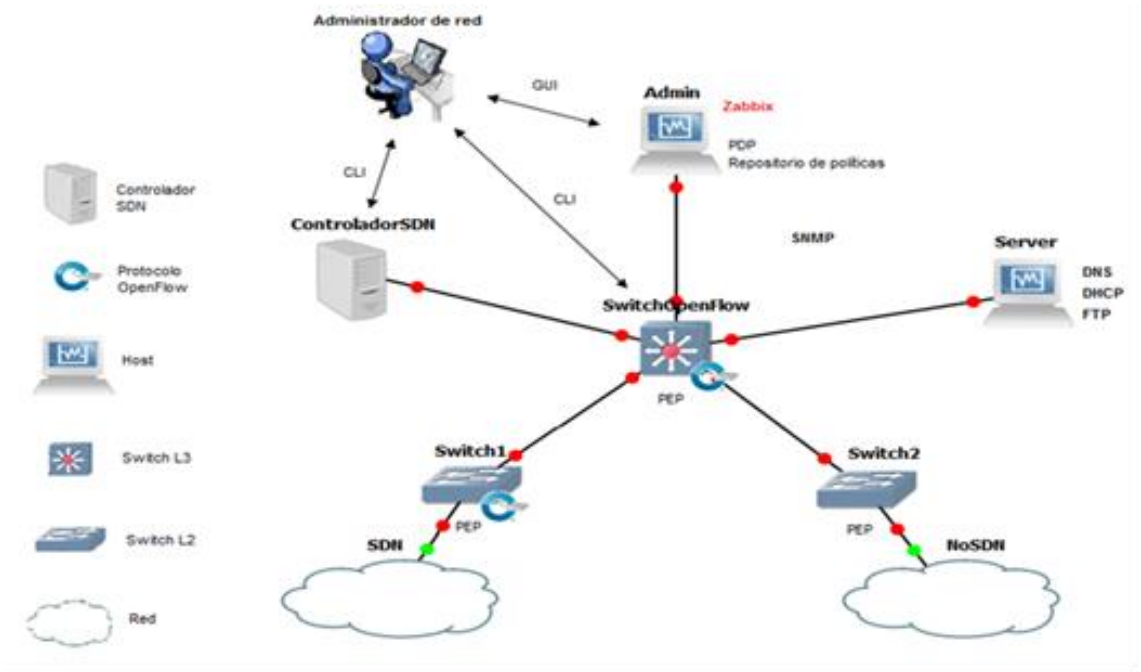

Figura. 3: Escenario de simulación de la arquitectura en red SDN híbrida.

En la Fig. 4 se muestran los componentes arquitectónicos de la arquitectura aplicada a una red SDN híbrida, en ella el PDPP es el encargado enviar políticas a los diferentes tipos de redes. Obtiene estas reglas a través de consultas al contenedor de políticas. En el caso de la red SDN, el controlador SDN funciona como PDP, de manera tal que las políticas implementadas controlan, de manera automatizada, el tráfico de información y la interacción entre el equipamiento de red con soporte OpenFlow, a partir de una extensión del modelo CIM [15].

El PDPP incluye entre sus funciones la validación y la lógica de detección de conflictos de las políticas del PDP SDN y el PDP de la red tradicional. Este puede interactuar con los PDP mediante el protocolo DEN-ng, lo que fortalece la automatización de la contextualización en la ejecución de políticas. El PDPP resuelve el punto único de falla en el controlador SDN, cuando este no está disponible, permitiendo legar el tráfico de la red SDN al PDP, que contiene los

gestores de objeto de CIM para que automáticamente cargue las configuraciones apropiadas en el equipamiento activo minimizando el impacto en el funcionamiento de la red, estas configuraciones podrían enviarse utilizando el protocolo SNMP o mediante la extensión del modelo CIM. Así se logra automatizar la ejecución de políticas de alta disponibilidad. Además, permite un control centralizado sobre los dispositivos que no soportan SDN.

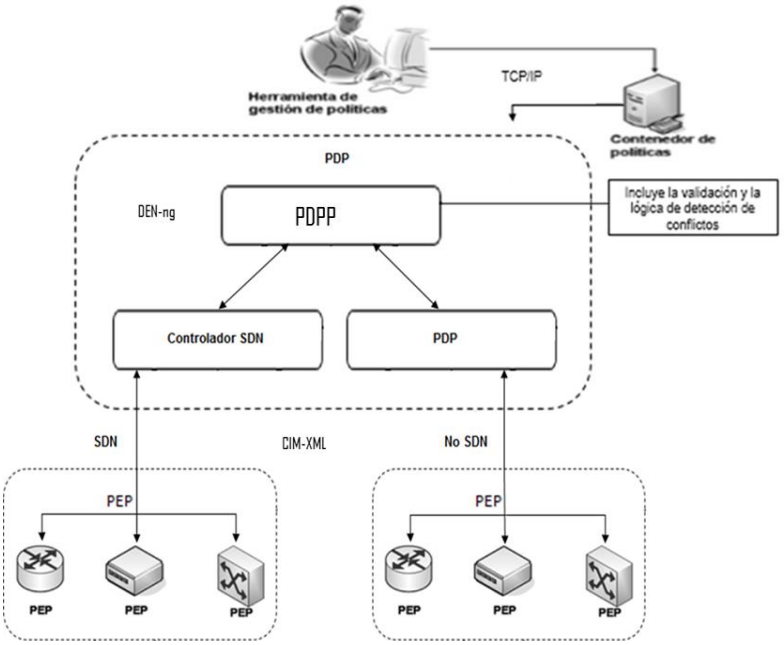

Figura. 4: Aplicación de la arquitectura en una red SDN híbrida.

Si se tratara de una infraestructura SDN/NFV, entonces el PDP CIM OM se ocuparía de la gestión de la red física y lo sistemas de cómputo físicos (utilizando SMASH, DASH) de la red virtual y las máquinas virtuales (utilizando VMAN). En estos recursos correrían las aplicaciones sobre las que se implementan las funciones de red y sobre las que se implementarían los elementos de red de la nube que proveería dinámicamente la infraestructura necesaria (utilizando Cloud, NETMAN). En tanto, el PDP SDN se ocuparía de administrar el control de las funciones de red que correrían sobre los elementos gestionados. Como se puede observar, se lograría tener un control holístico de la red y resolver los conflictos que políticas asociadas a determinadas tecnologías podrían provocar en el resto de los servicios de la red [12].

5. CONCLUSIONES

Las modificaciones propuestas a la arquitectura de gestión basada en políticas facilitan la integración de modelos de gestión estandarizados y propietario y la solución de conflictos entre políticas, permitiendo la automatización de la ejecución de políticas sobre infraestructuras TI heterogéneas y la reducción de la complejidad. La arquitectura para automatizar la ejecución de políticas sobre infraestructuras TI permitió la estratificación de la toma de decisiones.

A partir de la caracterización de diferentes modelos de información para la gestión estandarizada, se seleccionan dos de estos para formar parte de la arquitectura de gestión basada en políticas: el Modelo Común de Información CIM, por su capacidad para representar las diferentes facetas y escenarios de la gestión, su extensibilidad, posibilidad de integración y el amplio soporte ofrecido por los principales fabricantes de tecnologías; y el modelo DEN-ng para la contextualización y aplicación de la PBNM de manera tal que las políticas se ejecuten de manera automatizada. De esta forma, se puedan solucionar los conflictos entre ellas, se logra la integración de la gestión a partir del empleo de modelos de gestión integrada, y se tiene en cuenta el contexto en el que se encuentra cada elemento gestionado.

El empleo de la arquitectura de gestión basada en políticas con los modelos seleccionados en escenarios SDN híbrido y SDN/NFV, mostró su capacidad para automatizar la ejecución de políticas. Los resultados obtenidos unidos a soluciones de inteligencia artificial, machine learning, entre otras, impulsará la gestión autonómica de la red y sus servicios.

REFERENCIAS

[1] J. C. Strassner, *Context-aware dynamic policy selection for load balancing behavior*. Google Patents, 2017.

[2] B. Barafort, A.-L. Mesquida, y A. Mas, «Integrated risk management process assessment model for IT organizations based on ISO 31000 in an ISO multi-standards context», *Comput. Stand. Interfaces*, vol. 60, 2018, doi: https://doi.org/10.1016/j.csi.2018.04.010.

[3] V. Akishin, A. Goldstein, y B. Goldstein, «Cognitive Models for Access Network Management», en *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*, Springer, Cham, 2017, pp. 375-381.

[4] Y. Kryftis, M. Grammatikou, D. Kalogeras, y V. Maglaris, «Policy-Based Management for Federation of Virtualized Infrastructures», *J. Netw. Syst. Manag.*, vol. 25, n.º 2, pp. 229-252, abr. 2017, doi: 10.1007/s10922-016-9390-z.

[5] R. Boutaba y I. Aib, «Policy-based Management: A Historical Perspective», *J. Netw. Syst. Manag.*, vol. 15, n.º 4, pp. 447-480, dic. 2007, doi: 10.1007/s10922-007-9083-8.

[6] K. Odagiri, S. Shimizu, N. Ishii, y M. Takizawa, «Load Experiment of the Cloud Type Virtual Policy Based Network Management Scheme for the Common Use between Plural Organizations», en *2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, 2017, pp. 296-301, doi: 10.1109/WAINA.2017.16.

[7] J. Strassner, S. van der Meer, y J. W.-K. Hong, «The Applicability of Self-Awareness for Network Management Operations», en *Modelling Autonomic Communications Environments*, 2009, pp. 15-28, doi: 10.1007/978-3-642-05006-0_2.

[8] A. Westerinen *et al.*, «RFC 3198 Terminology for Policy-Based Management». nov-2001.

[9] S. B. Calo, D. C. Verma, y E. Bertino, «Distributed Intelligence: Trends in the Management of Complex Systems», en *Proceedings of the 22Nd ACM on Symposium on Access Control Models and Technologies*, New York, NY, USA, 2017, pp. 1–7, doi: 10.1145/3078861.3078881.

[10] J. Strassner, «Chapter 4 - Policy Operation in a PBNM System», en *Policy-Based Network Management*, Burlington: Morgan Kaufmann, 2004, pp. 141-178.

[11] W. Lui *et al.*, «RFC 8338 Policy-Based Management Framework for the Simplified Use of Policy Abstractions (SUPA)». feb-2018.

[12] R. Muñoz *et al.*, «Integrated SDN/NFV Management and Orchestration Architecture for Dynamic Deployment of Virtual SDN Control Instances for Virtual Tenant Networks [Invited]», *J. Opt. Commun. Netw.*, vol. 7, n.º 11, pp. B62-B70, nov. 2015, doi: 10.1364/JOCN.7.000B62.

[13] M. A. Khan, S. Peters, D. Sahinel, F. D. P. Pardo, y X.-T. Dang, «Understanding Autonomic Network Management: A Look into the Past, a Solution for the Future», *Comput. Commun.*, 2018, doi: 10.1016/j.comcom.2018.01.014.

[14] M. P. Casanova y C. A. Calderón, «Selección de modelos de información para gestión integrada de redes y servicios basada en políticas», *Rev. Científica Ing. Electrónica Automática Comun. ISSN 1815-5928*, vol. 39, n.º 3, pp. 77-88, oct. 2018.

[15] B. Pinheiro, R. Chaves, E. Cerqueira, y A. Abelem, «CIM-SDN: A Common Information Model extension for Software-Defined Networking», en *Globecom Workshops (GC Wkshps), 2013 IEEE*, Atlanta, Estados Unidos, 2013, pp. 836-841, doi: 10.1109/GLOCOMW.2013.6825093.

[16] N. Silega, M. Noguera, y D. Macias, «Ontology-based Transformation from CIM to PIM», *IEEE Lat. Am. Trans.*, vol. 14, n.º 9, pp. 4156-4165, sep. 2016, doi: 10.1109/TLA.2016.7785947.

[17] N. Handigol, B. Heller, V. Jeyakumar, D. Mazières, y N. McKeown, «I Know What Your Packet Did Last Hop: Using Packet Histories to Troubleshoot Networks», en *Proceedings of the 11th USENIX Conference on Networked Systems Design and Implementation*, Berkeley, CA, USA, 2014, pp. 71–85.

[18] A. Wundsam, D. Levin, S. Seetharaman, y A. Feldmann, «OFRewind: Enabling Record and Replay Troubleshooting for Networks», en *Proceedings of the 2011 USENIX Conference on USENIX Annual Technical Conference*, Berkeley, CA, USA, 2011, pp. 29–29.

[19] E. Al-Shaer y S. Al-Haj, «FlowChecker: Configuration Analysis and Verification of Federated Openflow Infrastructures», en *Proceedings of the 3rd ACM Workshop on Assurable and Usable Security Configuration*, New York, NY, USA, 2010, pp. 37–44, doi: 10.1145/1866898.1866905.

[20] R. Mijumbi, J. Serrat, J.-L. Gorricho, S. Latre, M. Charalambides, y D. Lopez, «Management and orchestration challenges in network functions virtualization», *IEEE Commun. Mag.*, vol. 54, n.º 1, pp. 98-105, 2016.

[21] M. Boucadair y C. Jacquenet, «RFC 7149 Software-Defined Networking: A Perspective from within a Service Provider Environment». mar-2014.

[22] T. Miyamoto, M. Miyazawa, y M. Hayashi, «Sustainable implementation-level workflow for automating NFV operation», en *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, 2017, pp. 793-796, doi: 10.23919/INM.2017.7987360.

[23] R. Emiliano y M. Antunes, «Automatic network configuration in virtualized environment using GNS3», en *2015 10th International Conference on Computer Science Education (ICCSE)*, 2015, pp. 25-30, doi: 10.1109/ICCSE.2015.7250212.

SOBRE LOS AUTORES

Mónica Peña Casanova, Ingeniera en Telecomunicaciones, Doctora en Ciencias Técnicas, Universidad de las Ciencias Informáticas, La Habana, Cuba monica@uci.cu

Caridad Anías Calderón, Ingeniera en Telecomunicaciones, Doctora en Ciencias Técnicas, Universidad Tecnológica de La Habana CUJAE, La Habana, Cuba cacha@tesla.cujae.edu.cu