

Juniper® Validated Design

JVD Solution Overview: Microsegmentation with VXLAN Group-Based Policies in IP Clos Fabric

Sol-overview-IPCLOS-GBP-01-01



Executive Summary

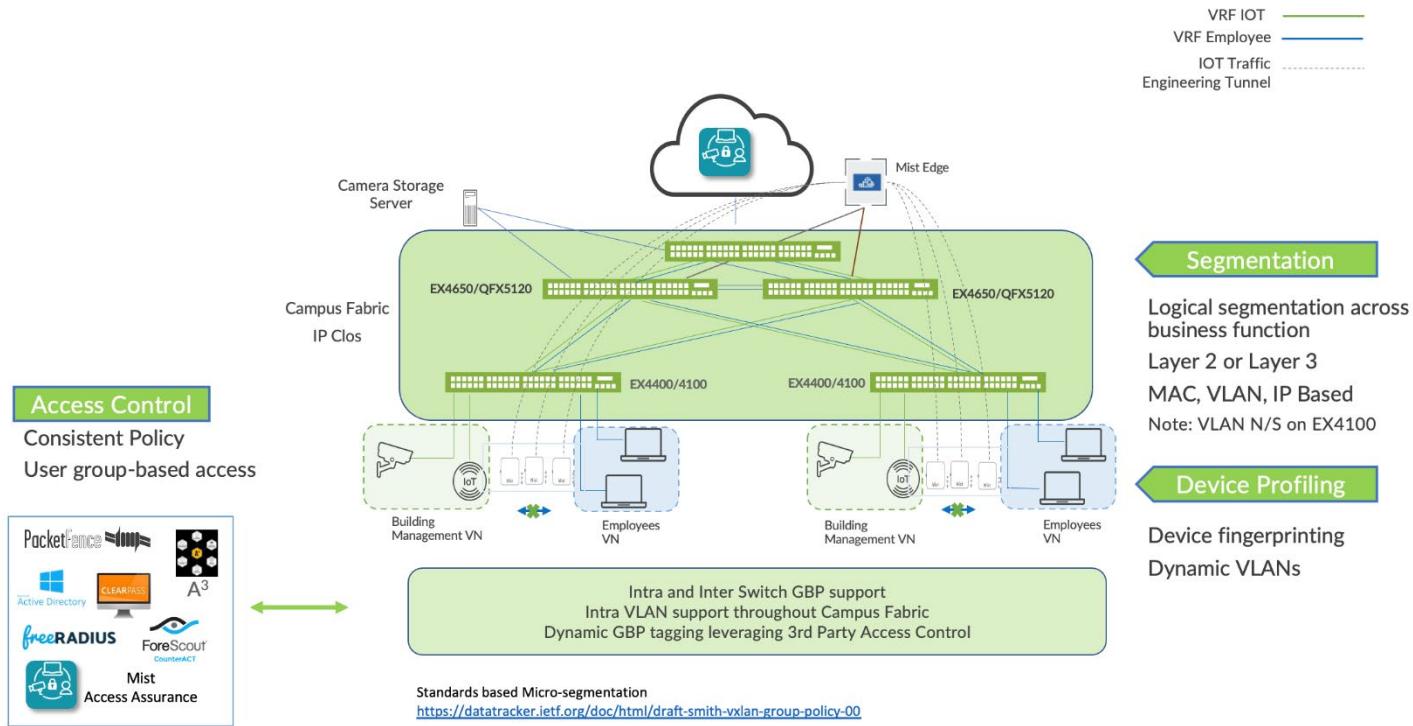
Enterprise networks are undergoing massive transitions to accommodate the growing demand for cloud-ready, scalable, and efficient networks. There's also demand for the plethora of Internet of Things (IoT) and mobile devices. As the number of devices grows, so does network complexity including an ever-greater need for microsegmentation and security. To meet these challenges, you need a network with automation and Artificial Intelligence (AI) for operational simplification. A Juniper Networks Campus Fabric IP Clos, supporting microsegmentation through the use of group-based policies (GBP), is a highly scalable, standards-based (<https://www.rfc-editor.org/rfc/rfc8365>) architecture that delivers consistent and optimized enterprise security, managed through the Juniper Mist portal.

Solution Overview

With GBP, you can enable microsegmentation at the access layer within a Campus Fabric IP Clos while leveraging EVPN-VXLAN to provide traffic isolation within and between broadcast domains. This solution also allows you to simplify security policies across a campus fabric.

There are several benefits of GBP microsegmentation:

1. Standards based—<https://datatracker.ietf.org/doc/html/draft-smith-vxlan-group-policy-00>
2. Simplified Workflow—GBP is administered through the Juniper Mist cloud, providing a simple and well understood workflow for network-wide policy control and enforcement. GBP also simplifies network configuration by reducing the number of firewall filters needed to ensure lateral threat protection.
3. Consistency—GBP provides consistent security policies across the enterprise targeting customers managed through the Juniper Mist portal.
4. Location-agnostic connectivity—GBP leverages underlying VXLAN technology to provide location agnostic endpoint access control.
5. More granular control—As GBP is enforced as a Layer 2 method, you gain tighter control than with traditional ACL-based methods. With VXLAN GBP, you can block traffic inside the same VLAN.
6. Network Access Control—GBP uses either static or dynamic tagging of wired clients.
 - Static GBP tagging allows you to assign GBP tags by IP prefixes, MAC addresses, VLAN IDs, and ports (based on the switch model) throughout all access ports of the fabric.
 - Dynamic tagging works with industry standards-based RADIUS Network Access Control (NAC) platforms including our cloud-based Juniper Mist Access Assurance.



Juniper's Campus Fabric IP Clos architecture, based on a VXLAN overlay with an EVPN control plane, provides microsegmentation using GBP. GBP blocks lateral threats, a requirement in most IoT use cases, while simplifying and optimizing enterprise security workflows through the Juniper Mist portal. Juniper is uniquely positioned to bring GBP to its full potential by providing an efficient and standards-based microsegmentation solution that includes a robust EVPN-VXLAN implementation at the access layer in a Campus Fabric IP Clos architecture using Juniper Networks® EX4400 and EX4100 Switches.



Corporate and Sales Headquarters

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.207.125.700
Fax: +31.207.125.701

Copyright 2024 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Juniper, Junos, and other trademarks are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. Other names may be trademarks of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.