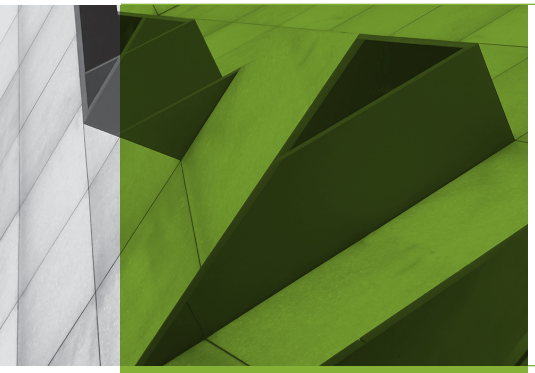


IOT NETWORK SEGMENTATION

Secure network access for IoT devices at distributed enterprises

Challenges

The explosive growth of IoT challenges traditional security practices and expands network access perimeters. IT needs to design flexible, scalable networks that accommodate and unify security policies across a diverse set of devices in both wired and wireless networks.

Solution

Network segmentation leverages an EVPN-VXLAN architecture that supports a highly scalable and agile environment while maintaining the security and performance requirements needed to protect users and IoT devices.

Benefits

- *Enhanced security, visibility, and control of users and IoT devices*
- *Flexible and scalable architecture*
- *Simple, agile network operations*

Solution Brief

Enterprise Internet of Things (IoT) deployments have become business scale. However, most IoT devices connected to enterprise networks are not managed by nor visible to the IT department. As a result, many enterprises fail to meet the basic security, scalability, and agility requirements needed to support these IoT network environments, making them hot targets for security breaches.

Traditional firewalls that sit at the network's edge can't provide sufficient protection; IT teams need to complement these solutions with strategies that secure internal traffic with consistent security policies that protect and minimize the damage caused by cyberattacks.

The Challenge

IoT is one of the biggest contributors to the rising importance of the network edge. As the number of network devices grows, so does network vulnerability—more devices represent a greater threat target. Most IoT devices are narrowly focused with limited power, memory, and bandwidth—they cannot prioritize security features or even allow for software patches. Once breached, an IoT device is one of the easiest ways for hackers to gain network access and move horizontally to launch a system-wide attack in search of sensitive and confidential data. A quick glance at the latest headlines shows why dynamic security is more important than ever.

IT teams are figuring out how to effectively create, enforce, and manage consistent security policies without adding complexity. Network segmentation is an old but reliable way to implement a security strategy that minimizes threats and protects valuable resources and data. And with an Ethernet VPN-Virtual Extensible LAN (EVPN-VXLAN) architecture, policies and workloads can move seamlessly across and within various enterprise sites.

The Network Segmentation Solution

Network segmentation takes a large network and separates it into multiple segments or subnets, whether physically or logically, to improve system performance and security. This is particularly important for IoT devices, as the network needs to allow them to communicate with the management platform or controller but not with each other. The data from IoT devices needs to be segmented for better control of traffic between designated zones.

Admins use firewall VLANs to create group zones divided by geographic location or network layers such as data, application, or network. Once resources are segmented as desired, it becomes easier to understand and control traffic flows and device access. However, it is important to note that firewall VLANs are data link layer (L2) constructs, making it complex and difficult to manage when enterprises expect networks to be agile and resilient. Network segmentation can be further divided via macro and microsegmentation (with inter- and intra-VXLAN policies) across campus and data center devices and applications.

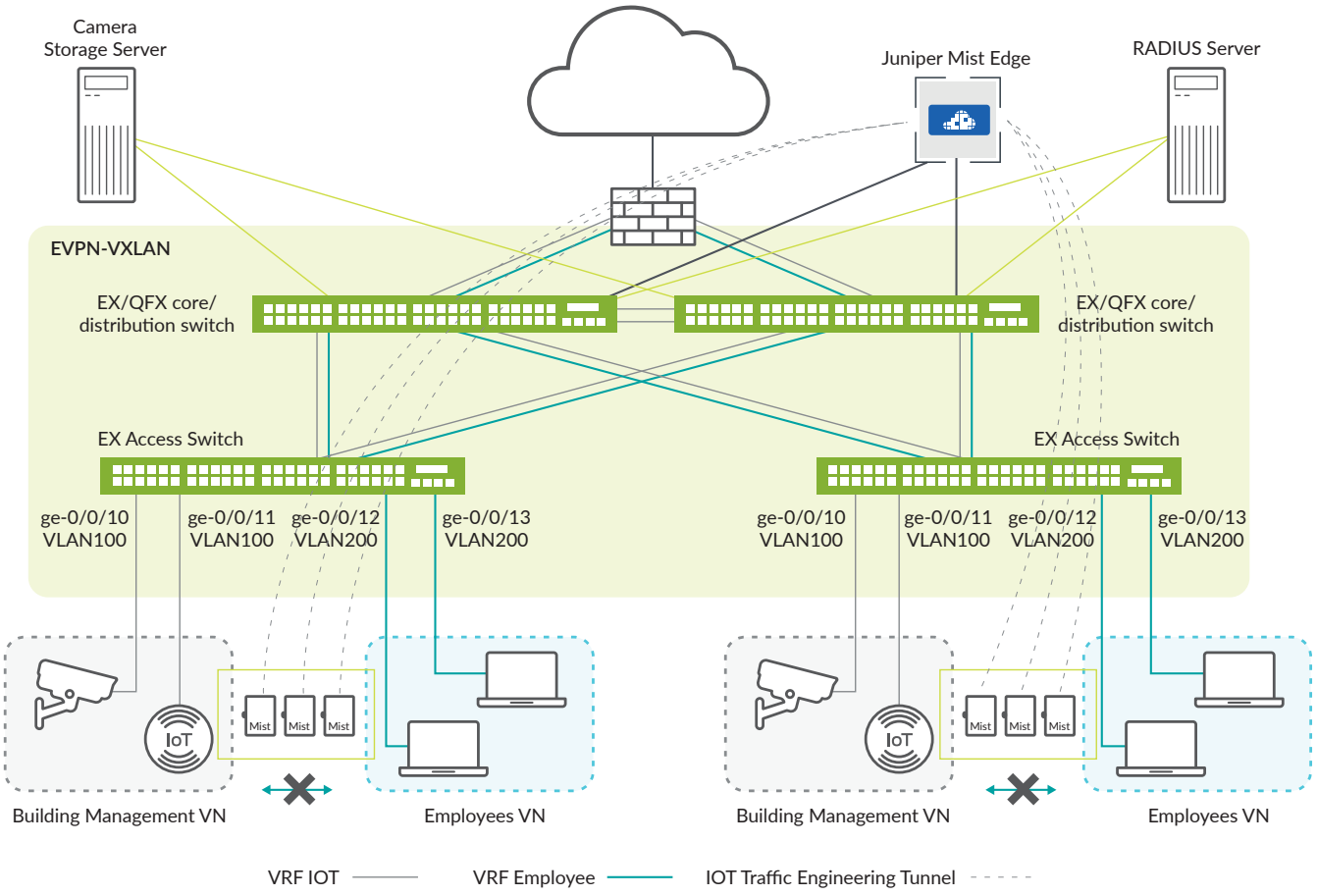
Macrosegmentation

Macrosegmentation is the logical separation of a network of shared devices across shared links. It is achieved in an EVPN-VXLAN network using VLANs at Layer 2 and virtual routing and forwarding (VRF) at Layer 3. VRF implementations impose isolation by keeping IP traffic between two VRFs completely separate.

Figure 1 depicts two VRF implementations, one for IoT devices and one for employees. There is no direct path between the two due to VRF isolation. A VN provides the first level of segmentation, ensuring zero communication between the forwarding domains.

Microsegmentation

Microsegmentation is a more granular segmentation technique that isolates workloads from one another, bringing greater control and reliability while reducing the risk of lateral attacks. This is critical for IoT segmentation, which can flood the local network with traffic if it gets broadcast in its VLAN. Microsegmentation imposes a "zero-trust" model, recognizing unauthorized workload communications using access control lists (ACLs) or firewall filters for intra-virtual network traffic. Micro segmented traffic uses ACLs in addition to VRFs when IoT devices don't need to talk to each other.



VN (Virtual network) first level segmentation ensures zero communication between forwarding domains. Static or dynamic VLAN and Filter assignment prevents lateral east-west communication within the VN

Figure 1: Network segmentation in an end-to-end EVPN-VXLAN architecture

Firewall filters enforce the rules that define whether to permit, deny, or forward packets transiting any Juniper Networks® EX Series Ethernet Switches from a source address to a destination address. Users configure the filters that determine the course of action before a packet exits a port, VLAN, or Layer 3 (routed) interface. These filters are also used to restrict traffic between devices within a particular VLAN—for example, within an IoT VLAN and VRF.

EVPN-VXLAN

To meet the challenges of secure onboarding, provisioning, and access of an exponentially increasing number of smart devices, Juniper offers an EVPN-VXLAN architecture for increased scalability, segmentation, and operational simplification. This architecture is complemented by machine learning and artificial intelligence, vastly improving operations as well as the experiences of IT teams and end users.

EVPN-VXLAN provides Layer 2 connectivity across Layer 3 virtual networks for greater network scalability without the complexity. Users can quickly and safely move workloads between campuses, data centers, and cloud services to increase flexibility, security, and overall IT agility.

Most IoT devices have limited network and security features, requiring Layer 2 adjacency. In the past, the solution was to extend VLANs across campus buildings. This approach, however, is inefficient due to excessive bandwidth consumption and complex VLAN management. EVPN-VXLAN enables network segmentation on a much greater scale than traditional VLANs, which are individually configured while meeting stringent privacy and security requirements.

Features and Benefits

The Juniper segmentation solution delivers the following features and benefits:

- Simple and scalable network operations that adapt to evolving network demands
- End-to-end visibility with deep traffic inspection
- Unified security policies across data center and campus sites

Solution Components

Juniper leverages application-layer protocols like multicast Domain Name System (mDNS), Simple Service Discovery Protocol (SSDP), and HTTP, as well as Layer 2 protocols such as Link Layer Discovery Protocol (LLDP) and 802.1x, to identify various client types such as wireless sensors and IoT devices. The solution includes the following components:

- **Juniper infrastructure:** Juniper Access Points are deployed on premises for Wi-Fi, BLE, and/or IoT access, while EX Series switches and Juniper Networks SRX Series Services Gateways support secure wired campus connectivity and EVPN-VXLAN architectures.
- **Juniper Mist Edge:** Some microservices require that specific functions be handled on premises, whether due to bandwidth, latency, or architecture requirements. Juniper Mist Edge extends select microservices to the customer premises while using Juniper Mist cloud and its distributed software architecture for scalable and resilient operations, management, troubleshooting, and analytics. Customers have the flexibility to deploy a hybrid architecture that extends processing and artificial intelligence to the network edge.
- **Juniper Mist WxLAN:** The Juniper Mist WxLAN solution delivers operational simplicity by automatically detecting and creating policies for role, device type, and user-based access on the network with an inline policy engine. It enables automatic device detection and categorization for security and audit reasons without requiring manual database management.
- **Juniper Connected Security:** Juniper Connected Security delivers automated security policy enforcement via Juniper Mist cloud with Juniper security services such as Juniper Advanced Threat Prevention cloud and the Juniper Advanced Threat Prevention Appliance. When Juniper Advanced Threat Prevention discovers a new threat, it sends an infected host list to Juniper Mist cloud, which generates a security policy and distributes it to the network edge elements, including access-layer devices. Known infected hosts or infected IoT devices are blocked at the port level on the wired switch or wireless access point. If the host or IoT device attempts to connect on a different port or through another switch, the distributed security policy ensures the infected device cannot connect and keeps it quarantined.
- **Interoperability with third-party RADIUS server solutions:** Wireless technology partnership details can be found here, and campus and branch here.

The Segmentation Ecosystem

The Juniper architecture allows for integration with traditional network access control (NAC) vendors to detect and profile IT and IoT devices as they get deployed. Based on the device posture, the Juniper Mist WxLAN fabric coordinates an instant response through policies for Juniper Access Points and EX Series switches. Through partnerships, Juniper offers sophisticated multilayer security policy enforcement and control at the access, aggregation, core, and perimeter, all orchestrated through the Juniper Mist WxLAN microservice in the Juniper Mist cloud architecture.

This provides complete visibility and control to ensure network devices are in compliance with corporate security and risk mitigation policies. Depending on the type of device and how it is used, it may be verified through 802.1X authentication, MAC RADIUS authentication, or captive portal authentication. Users can then apply different policies based on the device type, authorization level, or both to achieve dynamic segmentation.

Network access is further defined with VLANs and firewall filters, which separate and match groups of end devices to the areas of the LAN they require. Using dynamic profiles, in conjunction with the RADIUS authentication protocol, the architecture creates logical VLAN interfaces in the default system and in a specified routing instance. As Dynamic Host Configuration Protocol (DHCP) clients in the same VLAN become active, corresponding interfaces are assigned to any specific routing instances.

Alternatively, Juniper also works with third-party legacy RADIUS solutions to process traditional RADIUS Address Resolution Protocol (ARP) and Change of Authorization (COA) messaging to alter post-connection policies for devices that support Extensible Authentication Protocol (EAP) authentication methods.

Summary—Drive Visibility and Control to Secure Smart Devices with Network Segmentation

The mainstream adoption of IoT and smart devices is reshaping how businesses build secure and scalable networks. Users and devices expect networks to be available anytime and anywhere. When more devices are connected to the network, it expands the attack surface for hackers.

Network segmentation meets all the necessary security, agility, and performance requirements by dividing the network into smaller sections. For more granular policy control, there is macro and microsegmentation. With careful design and implementation, IT teams can build an EVPN-VXLAN architecture that spans multiple sites while maintaining the visibility and control needed to secure IoT devices without compromising network security, agility, or performance.

Next Steps

For more information, please contact your Juniper representative, or go to www.juniper.net.

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable and secure networks to move at the speed of business.

JUNIPER NETWORKS | Driven by Experience™

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

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

3510681-002-EN July 2022