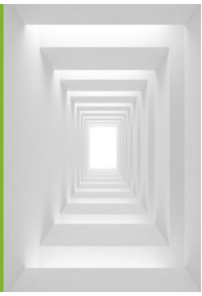
Driven by Experience

Juniper® Validated Design

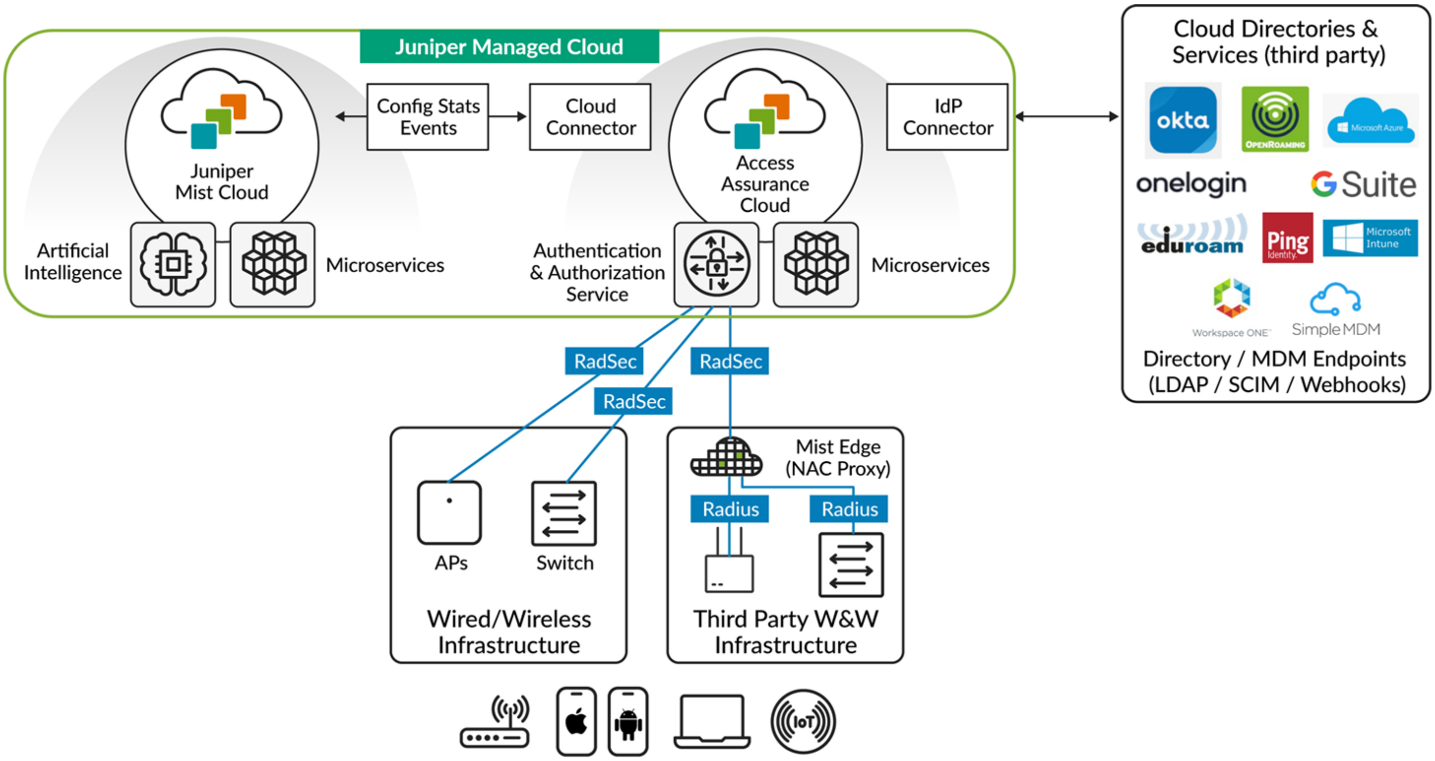
JVD Solution Overview: Juniper Mist™ Access Assurance



sol-overview-JVD-ENTWIRED-MAA-01-01

Executive Summary

Juniper Mist Access Assurance is a cloud-based service that ensures zero-trust, identity-based network access, and full-stack policy and segmentation assignments with end-to-end user experience visibility. The service delivers a suite of access control functionality with a flexible, yet simple, authorization policy framework for onboarding guests, IoT, BYOD, and corporate devices. Client connection is controlled based on user and device identities, regulating access for devices connecting to the network. Access Assurance also provides access control services for devices leveraging 802.1X authentication and MAC Address Bypass for non-802.1X allowlisted and wired IoT devices.



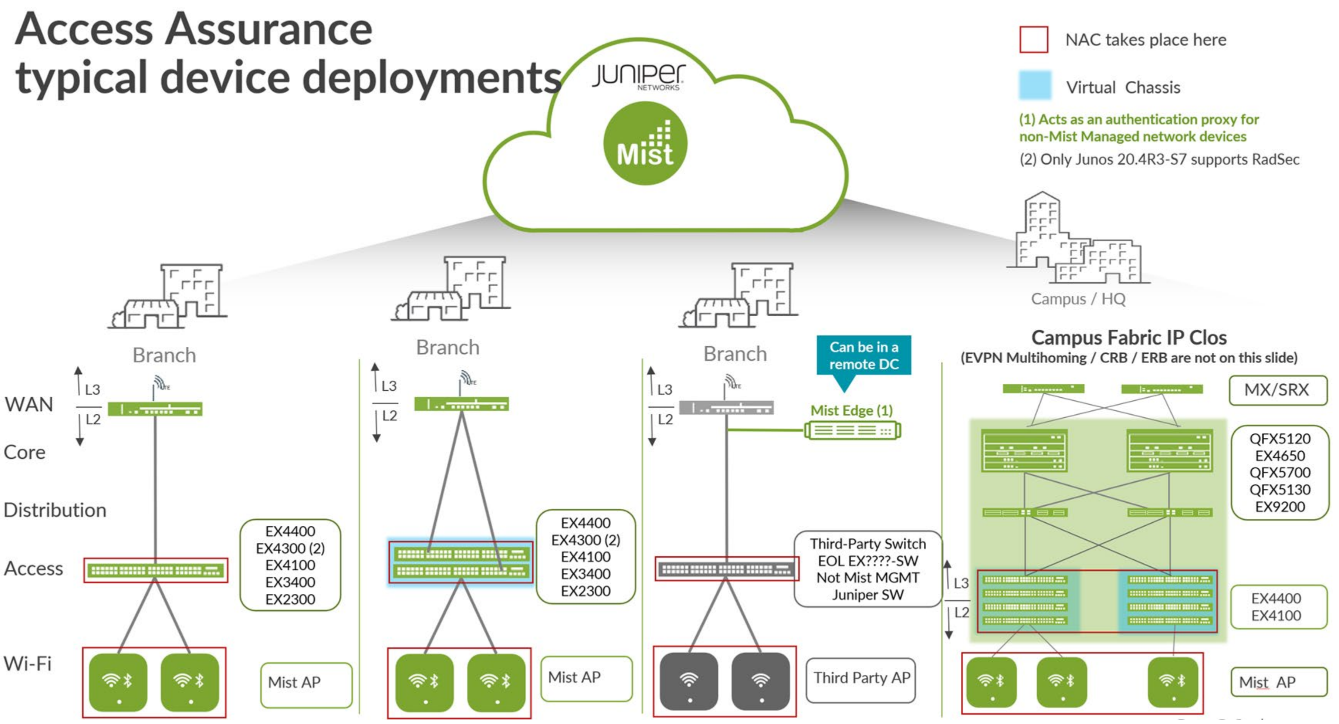
This JVD focuses on all aspects of the Access Assurance offering where the cloud-based Mist Authentication service provides authentication and policy decision making for Wireless or Wired Client independent if they are associated to a Juniper switch, Access Point or to a third-party. The JVD explains the most common deployment scenarios and topologies used. The JVD contains information about the tests operated for these typical deployments as well as best practices.

In the appendix section of this JVD, you will find information about all tasks to be performed when setting up the solution and configuring supplicants, switches and access points, Juniper Mist Edge as proxy and Juniper Mist authentication cloud. After the configuration section, the appendix provides examples of the various authentications performed, how to work with Match Criteria and finally how to use authorization parameters to dynamically apply a policy on the network access device for a certain client used.

Solution Overview

Traditional NAC design mostly encompasses a RADIUS server centrally located in the network. The Juniper Mist Access Assurance solution moves this functionality into the cloud, hence the network administrator is no longer burdened with the installation and maintenance of a RADIUS server. When network access devices, where the RADIUS client function is implemented, communicate to the Juniper Mist authentication cloud, they embed RADIUS messages into a TLS-tunnel called RadSec which is defined in IETF RFC 6614 which provides additional robustness against attacks such as blastradius and is easier to manage in a local enterprise firewall. Older network devices or third-party devices can leverage a Juniper Mist Edge appliance to perform a proxy function where Juniper Mist Edge receives standard RADIUS messages from those devices and then initiates the RadSec tunnel towards Juniper Mist authentication cloud.

By design, NAC solutions are implemented and applied where a client enters the network. For a wired client that needs to be the first switch of the infrastructure and for wireless clients, the Access Point is the place for authentication and later enforcement of any policy of the client traffic applied. This makes a NAC solution independent from the network design being a simple branch or a campus fabric solution with EVPN-VXLAN transport.



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