Mist
A Juniper Company

Mist WxLAN — Network Access for the Digital Enterprise

From smart factories or hospitality robots to low-energy sensors and cameras in manufacturing and across campuses, hyper-connectivity is running rampant in the enterprise as digital initiatives grow. Enterprise networking teams are not only supporting smart facilities and equipment management, but also implementing the latest roll-out of employee or customer engagement initiatives. With digital transformation, their role of supporting 3-4 company approved devices per employee has dramatically expanded to managing hundreds of different endpoints and applications, where many are running their own proprietary OS. Meanwhile, each class of devices is purpose-built — with specifically defined functions, unique behavior patterns and potential vulnerabilities.

NETWORK ACCESS CHALLENGES IN THE DIGITAL ENTERPRISE

Watching the aforementioned digital transformation initiatives impact their workplace, networking professionals have attempted to regain control with various advanced technologies from next-generation firewalls to numerous policy solutions to securely deploy and manage them. As the benefits of supporting these initiatives are multifold (from introducing operational efficiencies to adding revenue streams), networking teams are seeking digital-ready policy platforms that are designed to not only support use cases for digital business but also leverage all the benefits of modern technologies like cloud and automation.

Unlike existing legacy solutions, which are typically complex bolt-on or overlay solutions, Mist System's WxLAN, a feature of Mist's Wireless or Wired Assurance service from the Mist Cloud, offers enterprises a modern and extensible policy framework for their digital journey. As a Mist Wi-Fi customer, an enterprise gains network visibility and policy enforcement capabilities at the network edge, including IoT devices, without the additional costs of a profiler or policy enforcer (hardware and software) from a legacy solution. This technical brief will highlight some of the features that are essential for digital business along with demonstrating how simple it is to rapidly deploy network segmentation across various user groups and classified endpoints with Mist's WxLAN menu commands. More importantly, Mist's WxLAN aids further business expansion with its 100% API architecture for the following benefits:

- Enable dynamic policy enforcement with leading Network Access Control (NAC) vendors
- Implement additional advanced services like location/zone-based enforcement
- Automation support from Marvis AI

DIGITAL ENTERPRISE AND ROLE-BASED ACCESS POLICES

As digital transformation continues to grow in the enterprise, resourceful networking and security teams have addressed these initiatives with complex and costly role-based access solutions (wireless controllers, next-generation firewalls, NAC and identity management). Initially intended to replace the complex legacy ACL frameworks, NAC solutions became the de facto standard to help manage and secure these devices.

However, as initiatives and device types grew, so did the costs and complexities that were associated with NAC solutions. The recent trend of IoT and headless devices, with little or no proper means of security (No antiviruses and 802.1X supplicants, or even a web browser for guest portal registration), exposed some of its capabilities. Even with the capability of profiling endpoints via MAC Authentication, NAC deployments continued to become complex and costly to manage. Moreover, when it comes to network security, it was common practice to centralize policies on the firewall and, then apply dynamic VLANs for segmentation as the industry best practice. Most access policies required endpoints to support 802.1X/EAP supplicant for secure authentication and dynamic VLAN/policy assignments, while other less-secure devices, such as printers, were left to more default practices like MAC Authentication. Aside from NAC's visibility challenges, many enterprise networks were also being 'flattened', which made the impact of VLAN segmentation, a popular security practice, less impactful. Most of these methods required a complex NAC solution to be installed on-premises, which required integration across the rest of the networking infrastructure. This has always been a challenge for small to medium sized enterprises from day one of any NAC deployments. As digital transformations continued to grow in large enterprises, so did the costs and complexities of supporting NAC today.

DIGITAL-READY ACCESS WITH WXLAN

While endpoints continued to evolve and become pervasive in the enterprise, Mist's AI-driven Enterprise developed an innovative, digital-ready policy fabric, WxLAN, that would support the continuous onboarding of these endpoints for all Mist APs. Offering micro segmentation capabilities of devices even within the same flat Layer 2 network (reference Personal WLAN section), WxLAN leverages contextual menus with user-intent labels, where any client device or network resource can be attached to a label, either in the UI or programmatically using an API. Creating a policy is as simple as matching labels on the left side (users) with labels on the right side (resources) to define access policy actions, such as allowing or denying a resource or invoking a special action like bonjour assistance. Reference the social media blocking in the Policy Assignment use case on Page 2.

With Mist's WxLAN, enterprises can:

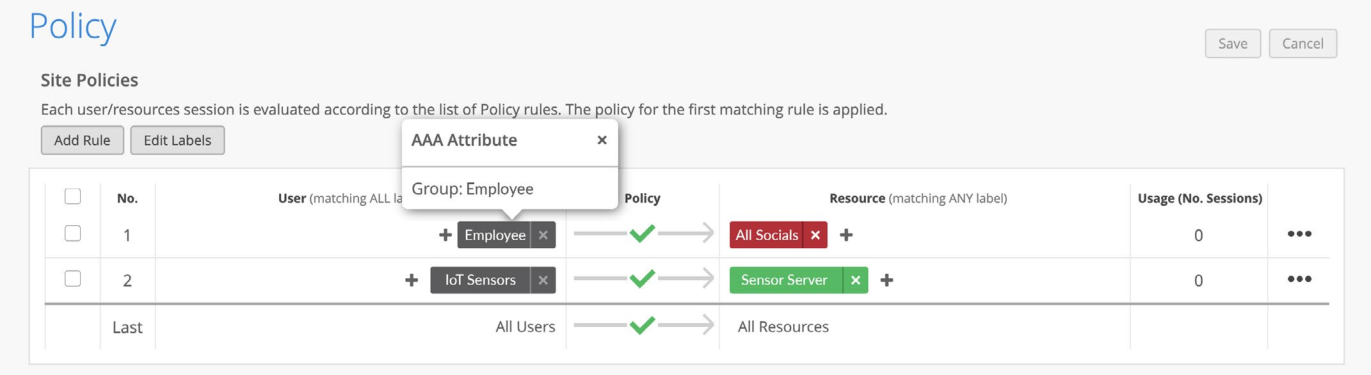
- Quickly rollout secure network segmentation based on user identity (Personal WLAN)
- Allow new types of services to be discoverable by any Wi-Fi clients (Apple TV, AirPlay, Air Print, etc.) and apply category-based policies
- Assign Policy using APIs via integration with 3rd party systems and automate client blacklisting and quarantining rules
- Manage client segmentation, inclusive of IoT

Policy Assignment Blocking Social Media for Your Employees on 802.1X SSID

As many enterprises have wrestled with the digital challenges of Social Media, networking teams have been asked to help define policies and monitor their activities. Many enterprises have Social Media policies and have offered limited access to several groups. See how simple it is to block Social Media via the Policy Assignment feature of Mist's WxLAN below.

For this case, an employee group is identified by a Filter-ID sent by a RADIUS server in Access-Accept. This allows for granular user-based control within the same SSID.

POLICY ASSIGNMENT FEATURE



Policy

Save Cancel

Site Policies

Each user/resources session is evaluated according to the list of Policy rules. The policy for the first matching rule is applied.

Add Rule Edit Labels

AAA Attribute ×

Group: Employee

□	No.	User (matching ALL la	Policy	Resource (matching ANY label)	Usage (No. Sessions)	
□	1	+ Employee ×	✓	All Socials × +	0	•••
□	2	+ IoT Sensors ×	✓	Sensor Server × +	0	•••
	Last	All Users	✓	All Resources		

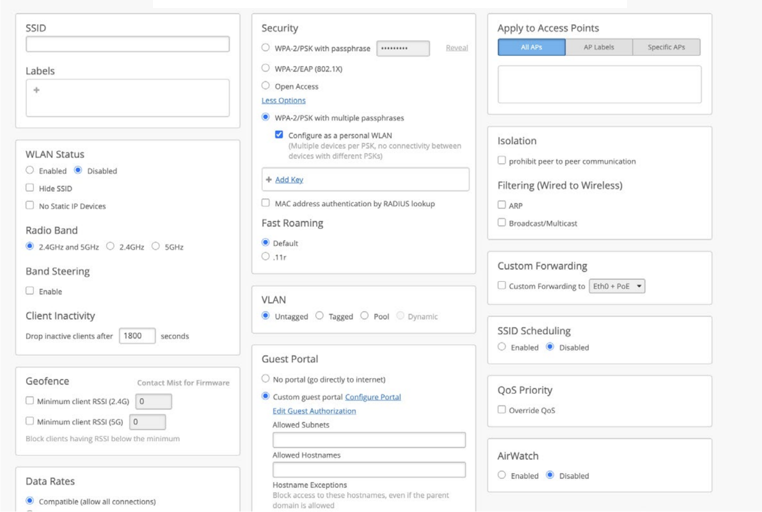
Note that rules are evaluated on a first-match user criterion on the left-hand side. The evaluation goes from top to bottom, first match will be applied, so it is recommended to put your least-specific match criteria to the bottom of the list.

Personal WLAN Rapidly Spin-out Micro-Segments

Whether it's in the main office or in the hotel lobby, enterprises need to deploy micro-segmentation enterprise wide for employees and guests. Micro-segmentation enables secure access polices to be assigned to various devices (i.e. printers dedicated to HR or Guests). Aside from the secure access benefits, Mist's Personal WLAN offers the defined end-user the ease of connection to all the defined devices to their specific group via a single SSID rather than the traditional practices of multiple SSIDs or the complexities of deploying multiple VLANs and ACLs.

In this multi-tenanted network use case, we need to isolate device communication only within the tenant. To implement Personal WLAN, you simply go to the following menu as shown below and 'click' to turn it on.

PERSONAL WLAN IMPLEMENTATION



SSID

Labels
+

WLAN Status
○ Enabled ● Disabled
□ Hide SSID
□ No Static IP Devices

Radio Band
● 2.4GHz and 5GHz ○ 2.4GHz ○ 5GHz

Band Steering
□ Enable

Client Inactivity
Drop inactive clients after 1800 seconds

Geofence Contact Mist for Firmware
□ Minimum client RSSI (2.4G) 0
□ Minimum client RSSI (5G) 0
Block clients having RSSI below the minimum

Data Rates
● Compatible (allow all connections)

Security
○ WPA-2/PSK with passphrase •••••••••• Reveal
○ WPA-2/EAP (802.1X)
○ Open Access
Less Options
● WPA-2/PSK with multiple passphrases
☑ Configure as a personal WLAN
(Multiple devices per PSK, no connectivity between devices with different PSKs)
+ Add Key
□ MAC address authentication by RADIUS lookup

Fast Roaming
● Default
○ .11r

VLAN
● Untagged ○ Tagged ○ Pool ○ Dynamic

Guest Portal
○ No portal (go directly to internet)
● Custom guest portal Configure Portal
Edit Guest Authorization
Allowed Subnets
Allowed Hostnames
Hostname Exceptions
Block access to these hostnames, even if the parent domain is allowed

Apply to Access Points
All APs AP Labels Specific APs

Isolation
□ prohibit peer to peer communication

Filtering (Wired to Wireless)
□ ARP
□ Broadcast/Multicast

Custom Forwarding
□ Custom Forwarding to Eth0 + PoE

SSID Scheduling
○ Enabled ● Disabled

QoS Priority
□ Override QoS

AirWatch
○ Enabled ● Disabled

KEY FEATURES OF MIST'S WXLAN

Key Features	Description	Benefit
Personal WLAN	Offer secure micro-segmented networks across a single WLAN. Create personal WLANs by generating unique keys to access the SSID.	Break away from the complex legacy practices of creating multiple unique SSIDs or setting up rules and groups via VLANS and ACLs. Patent Pending Personal WLAN allows secure onboarding and segmentation of multiple user or device groups on a single common SSID, using personalized pre-shared keys that operate across the entire site. Again, for the end-user in that specific Personal WLAN, s/he will have ease of connection, while providing automatic segmentations from devices using different keys.
Assisted Service Discovery	Allow zero-touch service discovery, like Bonjour* for all users based on their role and location, on enterprise networks.	Get a simple and streamline management tool to help your end users discover the availability of services (Implement Bonjour for Airplay, Airprint, etc.) across the enterprise network.
Policy Assignment	Easily apply policy to endpoints, regardless of their authentication/authorization method. Move away from legacy ACL practices of filtering network traffic with multiple lines of CLI Syntax.	Configure access policies with digital ease via contextual menus that specify intent (i.e.– prohibit access to social media to specific groups) or programmed APIs via automated 3rd party rather than writing multiple lines of correct syntax, which is popular for traditional ACL-based approach.
Embargoed Clients/ Quarantine	Automate unsanctioned or quarantine policies	Mist Open-API platform offers automating embargoed clients and quarantine via integration with 3rd party InfoSEC rather than managing non compliant clients with complex NAC or CLI commands.

Focused to support your enterprise digital transformation, Mist's WxLAN policies help networking teams rapidly define a list of rules, restrictions, and other settings to any device easily so that they are securely managed in the network. Avoid the additional costs and complexities associated with a NAC solution as Mist's WxLAN is included with Mist's Wi-Fi Assurance Subscription.

FOR MORE INFORMATION

To find out more about Juniper Networks and Mist product solutions, please visit www.juniper.net and www.mist.com.

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.

ABOUT MIST

Mist built the first AI-driven, microservices cloud-based Wireless LAN (WLAN), which makes Wi-Fi predictable, reliable, and measurable and enables scalable indoor location services like wayfinding, proximity messaging and asset visibility. In addition, Mist's AI technology plays a key role in bringing automation and insight across the full IT stack, delivering seamless end-to-end user experiences and substantial IT cost savings. In 2019, Mist was acquired by Juniper Networks and operates as a business unit focused on the AI-Driven Enterprise which combines Mist's next-generation wireless platform with Juniper's best-in-class switching, routing, security and SD-WAN solutions to deliver unsurpassed end-to-end user and IT experiences.

* https://developer.apple.com/bonjour/