portnox™

Segmenting Your Network with Dynamic VLAN Assignment

Blog article Sep 16,2020

What is Dynamic VLAN?

VLANs (Virtual Local Area Networks) enable segmentation of the main organizational network. In practice, VLANs allow network administrators to keep devices and network resources separated despite being connected to the same physical network.

Dynamic VLAN assignment separates and isolates devices into different network segments based on the device or user authorization and their characteristics. The flow of traffic between those VLANs is governed by a firewall or another routing device which can then enforce specific network access rules.

Why Use Dynamic VLANs?

Segmenting the network is a security best practice, and in some cases is even a regulatory requirement – such as with PCI. Network segmentation is a measure that improves the effectiveness of all the current investments in other security tools, and can by itself help to prevent significant damage to critical organizational data across the network after a company has been breached.

Automating VLAN assignments and eliminating the need for manual intervention has historically been a challenge for network security teams. Today, automatic VLAN assignment is best implemented by the use of a RADIUS service, which functions as follows:

1. A device connects to one of several the network access layers: wired ethernet switch or WiFi SSID
2. The network access layer sends a request to the RADIUS server with the user's credentials or certificates (using 802.1X)
3. The RADIUS server sends a reply which contains attributes that provide the switch or access point with information on the device VLAN, result in properly VLAN assignment

Portnox in partnership with Full Control Networks
T: 01677 428700
E: info@fullcontrolnetworks.co.uk

portnox™

Common Dynamic VLAN Assignment Use Cases

Network and security administrator most commonly encounter these use cases for dynamic VLAN assignment:

1. The Sales & Marketing department does not need access to R&D resources, while R&D should not have access to the Finance Department resources. Using dynamic VLANs, each department will be placed in the correct VLAN with the required access.
2. Devices that fail to authenticate due to wrong credentials or incorrect/expired certificate will be placed in a quarantine VLAN with internet access only.
3. IP Phones using a dedicated voice VLAN and should be placed on that VLAN upon successful authentication.
4. MAC bypass for devices that do not support 802.1X should be placed in their own dedicated VLAN.
5. Devices that fail posture assessment (such as those without updated AntiVirus) should be placed in a quarantine VLAN with limited access.
6. Employees connecting to one single WiFi SSID and get different access (VLANs) based on their authentication repository LDAP groups.

Dynamic VLAN Assignment with Portnox CLEAR

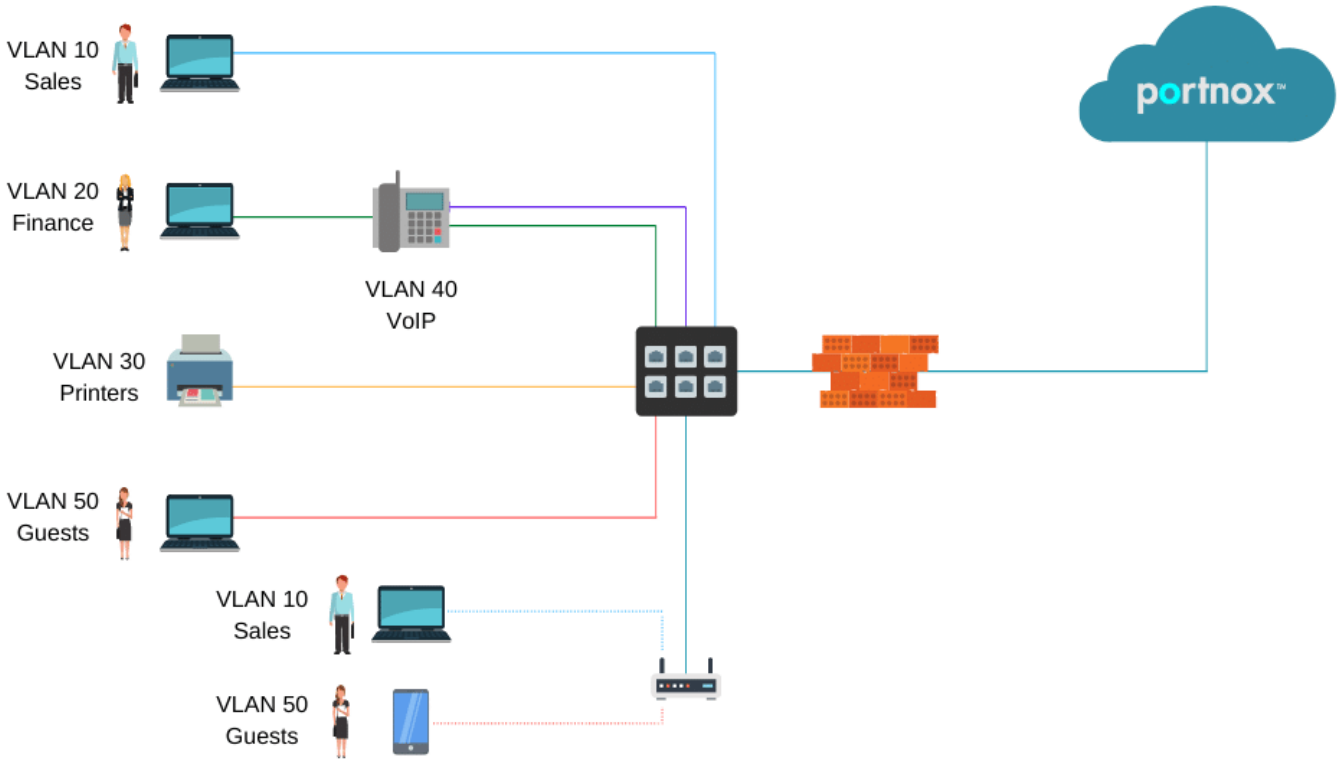
As mentioned earlier, the implementation of dynamic VLAN assignment has often been challenging for organizations since additional servers were needed on-site at the datacenter. This forced network teams to manage redundancies, complex configurations, and on-going maintenance.

To paint a clearer picture of this headache, consider this:

Take the case of connecting a new department, branch, or merely onboarding a lot of new employees at once…this can cause a surge in demand, which will in turn cause the whole network to “shutdown,” thus not accepting anyone who tries to connect.

Portnox CLEAR is a network access control solution, deployed as a cloud service, that provides all the mentioned use cases and more. CLEAR simplifies the implementation process of dynamic VLAN assignment. CLEAR allows you to easily set-up a cloud RADIUS server in a single click, and integrate with various authentication repositories like on-premise Active Directory, Azure AD, GSuite, OKTA. Plus, you can enforce your own unique access control policy to dynamically assign users to their respective VLANs.

In addition to VLAN assignment based on credentials authorization, CLEAR also allows you to implement dynamic VLAN assignment based on risk violation. This means that even devices that have authenticated successfully to the wired or wireless network can be dynamically moved to a dedicated VLAN if they fall out of compliance.



In the diagram above:

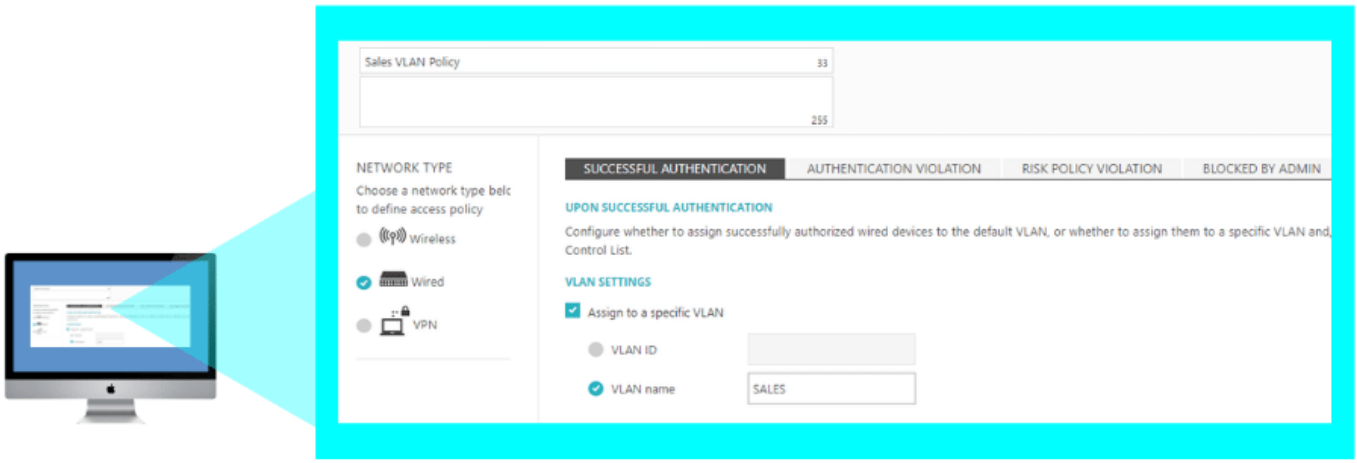
1. PCs are dynamically assigned to the VLAN based on their credentials/certificate.
2. IP Phones are assigned to the VOIP VLAN.
3. Printers are assigned to the printers VLAN.
4. Guests devices assigned to the internet-only access/quarantine VLAN.

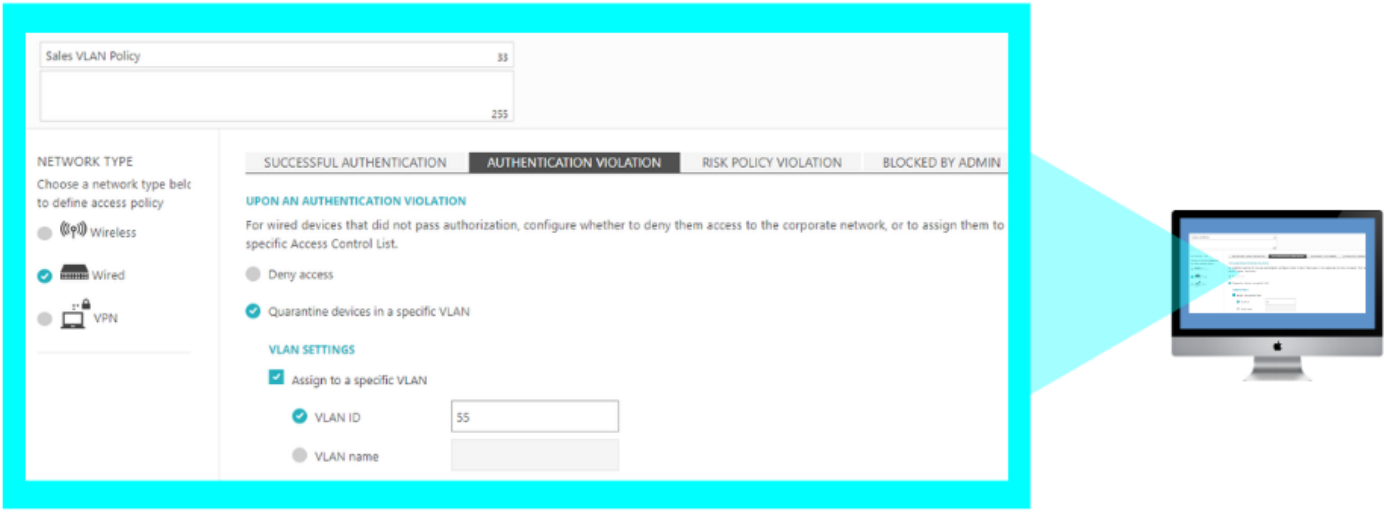
How it Works – Setting up Dynamic VLAN Assignment in Portnox CLEAR:

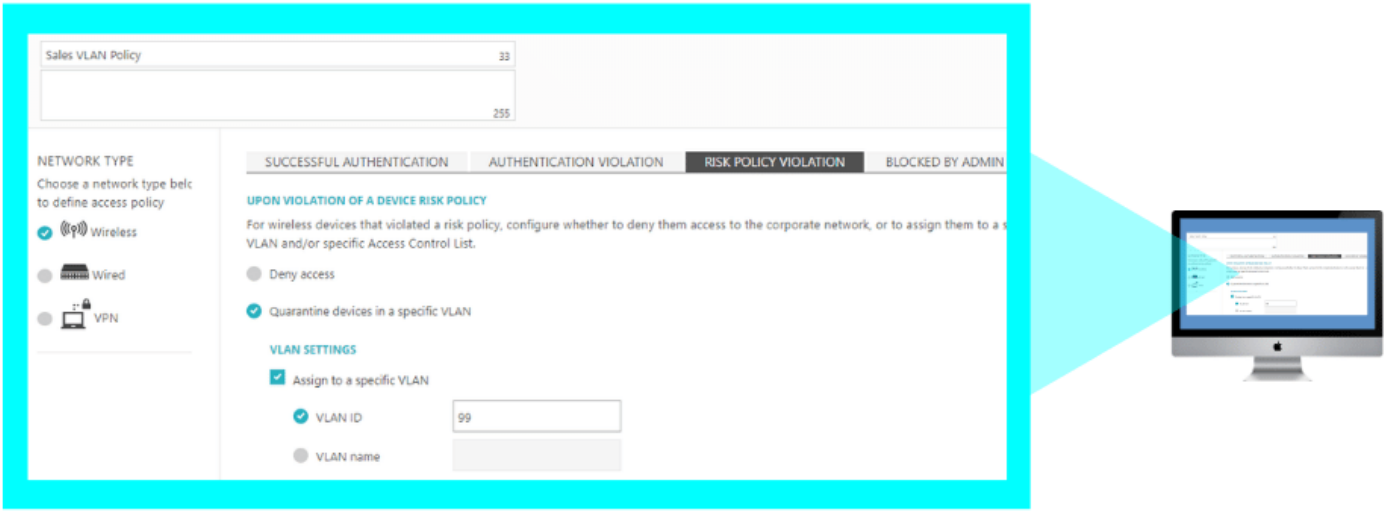
1. Enable Cloud RADIUS

In the CLEAR portal, create your one-click cloud RADIUS server: Go to **Settings > Services > CLEAR RADIUS Service**, and add your RADIUS service instance:

portnox™







Portnox in partnership with Full Control Networks
T: 01677 428700
E: info@fullcontrolnetworks.co.uk