



Network Access Control Integration with Aruba Wireless Local Area Networks Increases Safety and Security

Executive Summary

NAC provides many benefits including compliance control, threat mitigation, and visibility into endpoints. However, it has limitations on uses with guests and dynamic policy assignments. By using NAC integrated with the native Aruba API, CyberGatekeeper offers NAC without these compromises while leveraging the full capabilities offered by Aruba controllers.

Overview

The unprecedented adoption of 802.11n has given employees faster and more ubiquitous wireless access to the organization's network than ever before. Education and healthcare organizations that rely on mobility have been particularly quick to deploy Wireless Local Area Network (WLAN) technology. However, the concurrent explosion of personal Wi-Fi devices like smart phones and iPads means the enterprise network has become exposed to more unmanaged devices than ever before.

The risk of unauthorized devices intruding on the network means administrators must find a way to limit access to authorized devices. With improved visibility into users, configurations, and patches, the network can dynamically prevent or restrict access for devices failing to meet corporate security policy.

Current NAC solutions using RADIUS EAP provide important benefits including:

- Out-of-band implementation does not create a bottleneck in wireless throughput and provides scalability
- Solution provides for audit of connected endpoints post-admission, depending on agent type
- Solution supports full use of the Aruba role-based access control (RBAC) and Quality of Service (QoS)
- Solution can provide a full audit and remediation of endpoints running the desktop agent
- Solution is deployable on a per-SSID basis

With CyberGatekeeper, branch offices can be centrally managed, leveraging infrastructure and personnel at the main site, while larger sites may have locally (or centrally) managed NAC components as requirements dictate. Access and compliance policies may be consistent across all locations or vary with local or regional requirements. Reporting can be centralized to accumulate enterprise-wide compliance information for audit purposes.

Applicable policy elements include the standard antivirus, patch and firewall tests, but also a rich extended capability to audit compliance for unique configurations including in-house developed or third-party applications.

The Challenge

Although traditional NAC solutions using RADIUS EAP offer many benefits, they also have limitations for guests, users without admin privileges, and changing policies on the fly. These operations require administrative privileges on the endpoint or the real time notifications lacking in the standard RADIUS protocol.

This means that guests do not have access, changing access policies post-admission is slow, and large infrastructure changes are needed. NAC using EAP also requires deployment of many new servers and updating existing ones.

The Solution

In the latest version of InfoExpress CyberGatekeeper, NAC features have been implemented with Aruba's API. By combining Aruba's native interface with RADIUS EAP, CyberGatekeeper offers faster wireless deployments and more capabilities than just using RADIUS EAP alone. Key benefits available exclusively to customers using the integrated approach:

- Solution works with captive portal authentication
- Solution does not require a special supplicant
- Guests can use dissolvable web agents
- Guests do not need to have administrator access
- Access policies are independent of the client software and are easily updated (including mid-session)
- Solution reduces load on backend servers as need for re-authentication is virtually eliminated
- Solution supports both managed and unmanaged endpoints
- Solution works with all supported OSs (Windows, Mac, and Linux)

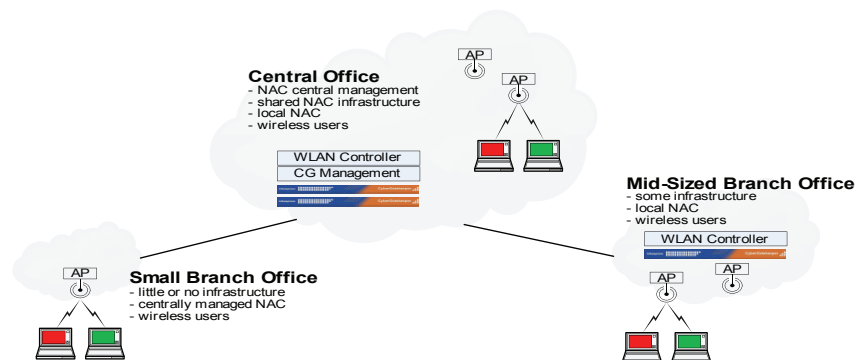


Figure 1 provides an overview of the components. Using CyberGatekeeper appliances, deployed centrally or locally to larger sites, enforcement on an Aruba wireless network can be centrally managed, yet effective in protecting the entire wireless network. CyberGatekeeper appliances interface directly with Aruba WLAN controllers to initiate enforcement actions when needed. CyberGatekeeper can automatically apply and enforce policies for all wireless users at any corporate location with minimal network disruption.

The integrated solution requires only the minimum Aruba software version 3.4.0 with Policy Enforcement Firewall and operates in both the 802.1x and Captive Portal authentication modes.

Summary

Due to extensive cost savings, ease of use, productivity gains and increased access to the Internet, WLAN technology will continue to be deployed by organizations of all sizes. With easier access to the network by Wi-Fi enabled devices, network administrators must increase their security posture to include Network Access Control (NAC).

Administrators must continue to guard against worms, unauthorized devices, and malware on their wireless networks. CyberGatekeeper NAC from InfoExpress limits the exposure to these threats by ensuring each connecting endpoint is properly configured. The result is that fewer endpoints are allowed to operate with outdated configurations, and infections are stopped at the perimeter. This reduces the cost of operations and lowers the risks associated with today's mobile work force.

Links for more information:

For more information on InfoExpress' industry-leading CyberGatekeeper Family of NAC products, go to www.infoexpress.com

InfoExpress was first to implement the tools now known as Network Access Control (NAC). It's proven, innovative CyberGatekeeper Family of NAC products offer:

- Authentication of all users and devices
- Definition of flexible audit policies
- Assessment & reporting on device configuration
- Isolation of non-compliant / unknown devices & users
- Remediation (or cleaning) of non-compliant devices
- Support for RADIUS EAP, in-line bridge, and other NAC enforcement methods