



Aruba's Network Access Control Solution

Access control is more important than ever for companies today as they are exposed to the security implications of mobile devices and as network security compliance becomes more critical. While Network Access Control (NAC) initially focused on a snapshot of the endpoint and user credentials for a static port, it now must accommodate the dynamic nature of mobile users and devices. Aruba NAC addresses this need with a user-centric access control architecture that adjusts network delivery in real-time based on a user's business needs and the security risk that they pose at any given time.

Mobile NAC

Aruba's NAC solution is standards-based, providing strong security and mobile context to any policy infrastructure. The Aruba solution determines information about the user by asking a series of questions such as:

- **User Identity:** Who is the user? What role does the user have in the organization? What is the user allowed to do?
- **Compliance:** What version of antivirus software is the endpoint running? Where is the user accessing the network? What applications is the user attempting to access? Does the user's traffic contain any viruses, worms, malware, etc?
- **Enforcement:** How do we enforce that policy? How do we help users

remediate if non-compliant? How do we handle users who cannot be assessed?

By mapping detailed administrative policies to usage policy enforcement rules, enterprises can use Aruba to achieve improved security, risk reduction and network optimization.

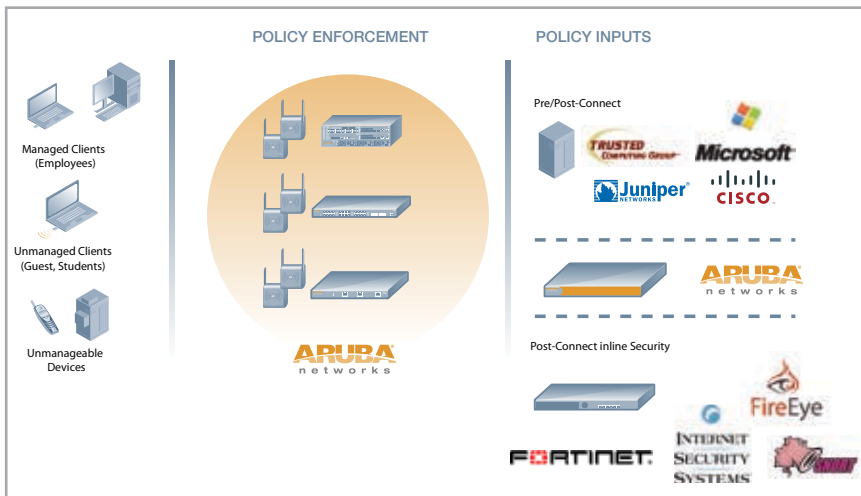
Aruba provides all the components of a comprehensive NAC offering and provides standard interfaces for interoperating with third-party NAC solutions such as Microsoft Network Access Protection (NAP), Juniper Unified Access Control (UAC) and Cisco NAC (CNAC). Using the Aruba Extended Services Interface (ESI), the Aruba solution can also correlate the results of traffic inspection by inline security devices.

How Aruba Enables NAC

- **Policy Enforcement:** The Mobility Controller is the primary component of the Aruba NAC solution, correlating policy input from multiple sources and acting as a secure policy enforcement engine. Policy is enforced using the controller's integrated role-based stateful firewall. This provides stateful policy enforcement and a very secure method of quarantine and remediation of non-compliant users and devices.
- **Policy Inputs (Pre/Post-Connect):** The Aruba Endpoint Compliance System (ECS) can be used as a policy decision point in place of, or in parallel with, a standards-based policy server such as Microsoft Network Policy Server (NPS) or Juniper Steel-Belted Radius (SBR). ECS is especially well-suited for networks with large populations of transient users (e.g., schools, hospitals etc). Although these appliances focus

Benefits:

- User-centric architecture brings context of mobility to NAC
- One configuration for wired, wireless, and remote access
- Integrates with existing security and policy infrastructure
- Pervasive security with role-based policy enforcement



on establishing policy at the time of authentication, most can do some level of continuous evaluation.

- **Security Services (Post-Connect Inline Security):** For complete post-connect NAC, inline security devices can be used to evaluate traffic in real-time. The Aruba Controller can forward traffic by protocol to these devices and act immediately on anomaly detection, virus discovery and the like.

Aruba's user-centric architecture is able to add the consideration of mobility to access control. This is a vital dimension to consider since using a static security policy to handle a mobile user can have only limited effect at best. Aruba's solution combines access control with a deep understanding of mobile users and devices to create a dynamic solution that moves with the user. Aruba NAC provides mobile context to the three major areas of NAC: identity, compliance and enforcement

USER IDENTITY

The first requirement for network access control is determining who the user is and what that user should be allowed to do. To determine the authentication state of a user and the role of the user in the organization, Aruba interfaces with backend databases such as RADIUS, LDAP, and Active Directory through a broad range of authentication options. In an educational setting, for example, identity-based access control permits faculty to have different access rights than students, and lets organizations give Internet access to visitors without compromising internal security

COMPLIANCE

Once identity is established through authentication, the Aruba Mobility Controller can consider compliance with other factors such as endpoint posture, user behavior, and environmental factors. The Controller can correlate all this information to provide the right level of network access. Non-compliant systems can be blocked from network access entirely or placed into a quarantine role so that automatic remediation may be performed. Compliance should be considered both at the time of authentication (pre-connect) and on an ongoing basis (post-connect).

A pre-connect check is primarily based on comparing client security settings against baseline enterprise security policies such as anti-virus software version, firewall settings or operating system patches. Aruba provides this compliance assessment with the Aruba ECS product.

In addition to its own ECS, Aruba integrates with third-party compliance assessment systems including Microsoft NAP, Cisco NAC, Juniper UAC, InfoExpress, Symantec and any vendor compliant with the Trusted Computing Group's Trusted Network Connect (TNC) initiative. As a member of the Trusted Computing Group, Aruba serves as a Policy Enforcement Point (PEP) in the TNC architecture and is active in the TNC working group in developing tighter integration and better standardization between compliance assessment system vendors.

For post-connect compliance, it's necessary to do both periodic checks on client settings as well as real-time traffic inspection. The Aruba ECS will implement periodic scans of endpoints that are associated with the network and the Aruba Mobility Controller uses network protocol to integrate with inline security devices to identify threats in real time.

Aruba allows any network service device such as an anti-virus gateway, IDS/IPS, infection detector, or proxy to be connected to a Mobility Controller through the Aruba ESI software module. The ESI module inspects traffic by protocol and redirects specific protocols to a load-balancing function that distributes traffic to a cluster of network service devices.

Devices that discover infections or non-compliant behavior can signal quarantine or blacklist actions to the Aruba Mobility Controller through a simple XML API or through industry-standard syslog. This method of post-admission compliance is also useful for application-specific devices such as networked printers and Wi-Fi phones that cannot run an endpoint compliance agent on their OS.

NETWORK-BASED USAGE POLICY ENFORCEMENT

Once identity and compliance state have been determined, the Aruba system applies role-based access control through flexible stateful firewall rules.

Benefits of the Aruba NAC Solution

Aruba is focused on enabling secure user-centric networks for enterprises. Aruba NAC takes a multipoint assessment of the user and device and provides policy enforcement over wired, wireless and remote access. Enforcement is pervasive — following the user anywhere they connect, and dynamic — changing as their security

Aruba provides a unique advantage over traditional LAN switches through the use of firewall-based enforcement. The Aruba Policy Enforcement Firewall (PEF) monitors per user traffic and enforces usage policies on a continuous basis. This is especially compelling for implementing per-user quarantine roles.

In a traditional LAN switch, non-compliant users are placed into a separate quarantine VLAN where non-compliant clients are still able to communicate amongst each other, even if access to the larger network is blocked. When network access is provided through an Aruba Mobility Controller, however, non-compliant clients are immediately placed into isolation from other users through firewall rules. These firewall rules can be written to permit communication with remediation servers, and can even apply web-based captive portal rules to display custom web pages to users.

Using a stateful firewall allows policies to be dynamic as well. As any characteristic of the user or device changes, so does their access control policy. For instance, a student walking from a public area into a classroom should have their policy changed automatically to one that is more restrictive. As different characteristics of a user or device change in a mobile environment, it could make sense to have dynamic policies adjust privileges automatically for bandwidth availability, application usage, quality of service, etc.

state or behavior changes. With mobile computing devices outselling desktop systems two-to-one, networks must be designed for users who move from one location to another. By integrating mobility with NAC, Aruba provides a comprehensive solution that secures all users and all types of devices, for all access methods.



WWW.ARUBANETWORKS.COM

1322 Crossman Avenue. Sunnyvale, CA 94089 | Tel. +1 408.227.4500 | Fax. +1 408.227.4550