



PARTNER SOLUTION BRIEF

Impulse Point

Aruba Networks and Impulse Point

Using Aruba's User Centric Network Architecture to Enforce Safe•Connect Network Access Control

Access control is more important than ever for companies as they are exposed to the security implications of mobile devices and as network security compliance becomes more critical. To address this need, Impulse Point's Safe•Connect™ Network Access Control (NAC) Solution has been validated to work with Aruba Networks User Centric Network architecture to provide Single Sign-On (SSO) authentication and real-time endpoint security posture assessment and enforcement. The combined solution provides comprehensive Network Access Control (NAC) and leverages Aruba's powerful Policy Enforcement Firewall.

Safe•Connect NAC Overview

Safe•Connect's NAC Policy Enforcer detects and registers unknown devices on the network and administers a lightweight persistent or temporary/dissolvable agent to determine the security posture of the device. The agent will continue to conduct real-time security assessment (pre- and post-connect) to ensure ongoing network protection. Safe•Connect will inform the Aruba controller of policy decisions based on the real-time assessment of the client's security posture, and assign the device to a restricted access "remediation/quarantine role" based on the organization's acceptable use network policy.

Aruba Policy-Based NAC Enforcement

For network access control, Aruba provides a unique advantage over typical LAN infrastructure through the use of firewall-based policy enforcement. Fully integrated within the Aruba controller architecture, the Policy Enforcement Firewall (PEF) monitors per-user traffic and enforces usage policies in real time.

Safe•Connect's continuous posture assessment capability leverages Aruba's PEF technology to assign per-user quarantine roles for clients that are not compliant with security requirements. In a traditional LAN switch, non-compliant users are placed into a separate quarantine VLAN, and a number of different techniques are used to force the client to obtain a new IP address in that VLAN. Non-compliant clients are still able to communicate amongst each other, even if access to the larger network is blocked. However, when network access control is provided

through an Aruba Controller, non-compliant clients maintain the same IP address but are immediately placed into isolation from other users through firewall rules. These firewall rules can be written to permit communication with remediation servers, or restrict a device to Internet-only guest access; and can even apply web-based captive portal rules to display custom web pages to users.

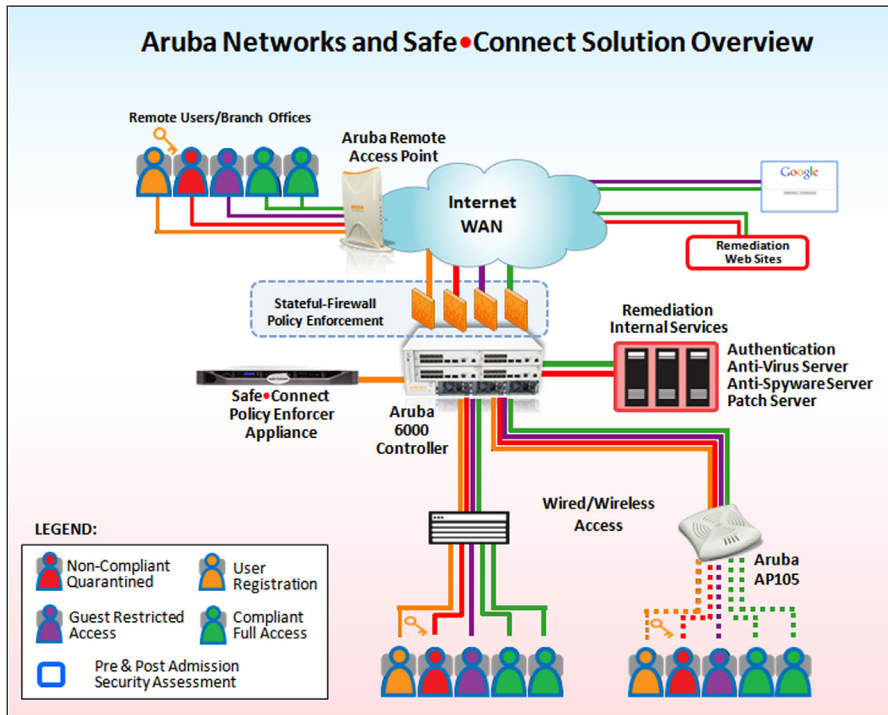
Aruba can provide this level of policy enforcement over wireless and wired networks that extend from central to remote branch locations or home users. In the case where users connect using Aruba's Remote Access Points or VIA software client, firewall-based policy enforcement is applied by the Aruba architecture in the same manner as when a user connects locally at a campus location. Safe•Connect can also be leveraged in this scenario, extending posture assessment and enforcement to these remote users.

Benefits:

- Delivered as a managed service for ease of deployment and low TCO
- Highly scalable, distributed design
- Pre- & Post-Admission checks across wired, wireless, and VPN
- Integrates with Aruba's firewall-based policy enforcement
- Single Sign-On (SSO) Support

The Aruba-based Safe•Connect NAC solution is easy-to-deploy and maintain. Impulse Point supports its Safe•Connect product as an operationally managed service, providing proactive system monitoring; problem determination and resolution ownership; application of software maintenance, security and device updates, and functional version upgrades; and remote daily backup and hardware replacement.

Aruba Networks and Safe•Connect Solution Overview



PARTNER SOLUTION BRIEF

Impulse Point



About Impulse Point:

Designed for highly scalable and vendor diverse environments, Impulse Point's Safe•Connect™ Network Access Control solution enables organizations to automate and enforce end user authentication, anti-virus, anti-spyware, Microsoft security patches, P2P file sharing, power management, and custom endpoint security policies. For more information, please visit www.impulse.com.

About Aruba:

Aruba is the global leader in distributed enterprise networks. Its award-winning portfolio of campus, branch/teleworker, and mobile solutions simplify operations and secure access to all corporate applications and services - regardless of the user's device, location, or network. This dramatically improves productivity and lowers capital and operational costs. Listed on the NASDAQ and Russell 2000® Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, and Asia Pacific regions. To learn more, visit Aruba at <http://www.arubanetworks.com>. For real-time news updates follow Aruba on Twitter, Facebook, or the Green Island News Blog.



WWW.ARUBANETWORKS.COM | 1344 Crossman Avenue. Sunnyvale, CA 94089

1-866-55-ARUBA | Tel. +1 408.227.4500 | Fax. +1 408.227.4550 | info@arubanetworks.com