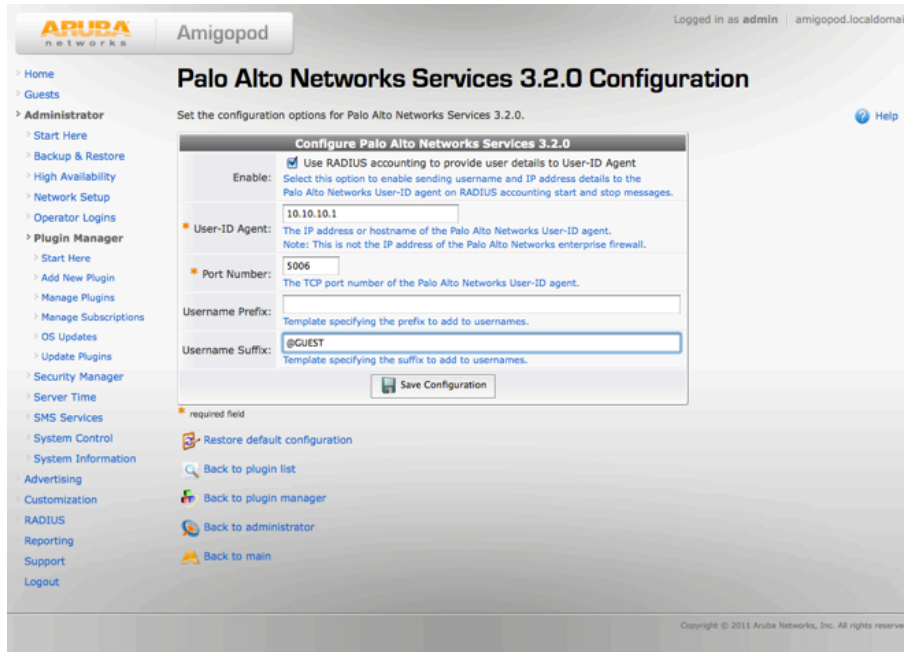




Traditional firewall policies are based solely on IP address, but the dynamic allocation of IP addresses to corporate and guest users means that the user and group associations are not reflected in those policies. Palo Alto Networks' User-ID technology seamlessly integrates with a wide range of enterprise directories to identify users of the corporate network. Aruba Networks has developed a plug-in for the Amigopod that utilizes the Palo Alto Networks XML API to extend the User-ID technology to guest users and employee owned mobile devices.



Configuration of the Palo Alto Networks Plug-in on the Amigopod

Once users are uniquely identified, security policies on the Palo Alto Networks next-generation firewall can be granularly defined based on the user name and/or group membership, not merely the source IP. This cohesive user identification system removes the unknowns from a firewall policy and provides network operators complete visibility and control over the applications and resources available to all network users. The combined solution provides safe enablement of resources to the entire network population.

Use-cases for this solution include:

- Securing users and devices as they access web content on guest Wi-Fi networks
- Enabling safe use of employee owned mobile devices while on the corporate network
- Protecting corporate data by allowing access to important network applications while protecting from potentially dangerous or non-compliant applications
- Identify traffic by user and application for full visibility and control of network resources
- Right-size the security infrastructure with integrated wired and wireless policies compliance and enforcement

## PALO ALTO NETWORKS

Palo Alto Networks™ next-generation firewalls enable unprecedented visibility and granular policy control of applications and content – by user, not just IP address – at 20 Gbps network throughput levels. Based on patent-pending App-ID™ technology, Palo Alto Networks firewalls accurately identify and control applications – regardless of port, protocol, evasive tactic or SSL encryption – and scan content to stop threats and prevent data leakage. Enterprises can, for the first time, embrace Web 2.0 and maintain complete visibility and control, while significantly reducing total cost of ownership through device consolidation.



## ARUBA NETWORKS

Aruba is a 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.



## LEARN MORE

For more information on the Palo Alto Networks/Aruba solution, contact:



Palo Alto Networks  
3300 Olcott Street  
Santa Clara, CA 95054  
Main: (408) 753-4000  
[www.paloaltonetworks.com](http://www.paloaltonetworks.com)



Aruba Networks  
1344 Crossman Ave.  
Sunnyvale, CA 94089-1113  
Main: +1-408-227-4500  
[www.arubanetworks.com](http://www.arubanetworks.com)