

ARUBA NETWORKS AND OPENDNS ENTERPRISE

Strengthen your wireless networks' defenses against the latest security threats while enforcing corporate Internet usage policy

As enterprises adapt their networks to enable more employee mobility across the organization and distributed locations, they must provide protection against evolving Web threats and apply policy to manage how employees and guests navigate the Internet. Enterprises need a flexible solution that provides protection and control without tying up significant IT resources to deploy and manage it.

Aruba Networks and OpenDNS have developed an integrated solution to provide joint customers with Internet security protection and Web filtering in a simple to deploy and manage cloud-based solution. OpenDNS Enterprise offers businesses of all sizes a proactive layer of protection against malicious Web threats and control over how their users navigate the Internet. OpenDNS in combination with Aruba's solutions enables enterprises to benefit from additional user productivity through mobility and Web filtering policy enforcement as well as enhanced Web security while lowering capital and ongoing operational costs.

PROTECT WIRELESS NETWORKS AND USERS AGAINST THE LATEST WEB SECURITY THREATS

With the proliferation of Web 2.0 sites, malware, botnet and phishing attacks have increased significantly, leaving businesses vulnerable to drive by downloads, key loggers, Trojans and other malicious threats. OpenDNS's innovative security approach delivers phishing, botnet and malware site protection at the DNS level. Malicious, compromised and infected sites are identified and blocked from resolving during DNS resolution, stopping users from unknowingly going to known sites that can infect users machines. By operating at the DNS level, OpenDNS Enterprise prevents malware and malicious content from reaching the network and reduces the chance for the network and user to become infected.

In addition to protecting networks from external attacks, OpenDNS also provides protection and mitigation against botnet infections that can threaten your network from roaming or external devices that connect to the network. OpenDNS detects botnet activity on your network and instantly cuts off their ability to access and communicate with their command and control center. This prevents botnets from spreading to more machines on the network and stops them from sending out confidential data and personal information to hackers outside the firewall. After the botnet is blocked, OpenDNS also provides the ability to detect which machine on the network is infected, allowing IT administrators to quarantine and clean the infected end point.

WHY ARUBA AND OPENDNS

- Verified interoperability, ensuring hassle-free deployments
- Provides protection for all connected devices
- Managed from Web-based console; no on-site presence required, simplifying management of remote and branch office deployments
- Easily scales from 1 to 1000 locations

MANAGE HOW EMPLOYEES AND GUESTS NAVIGATE THE INTERNET

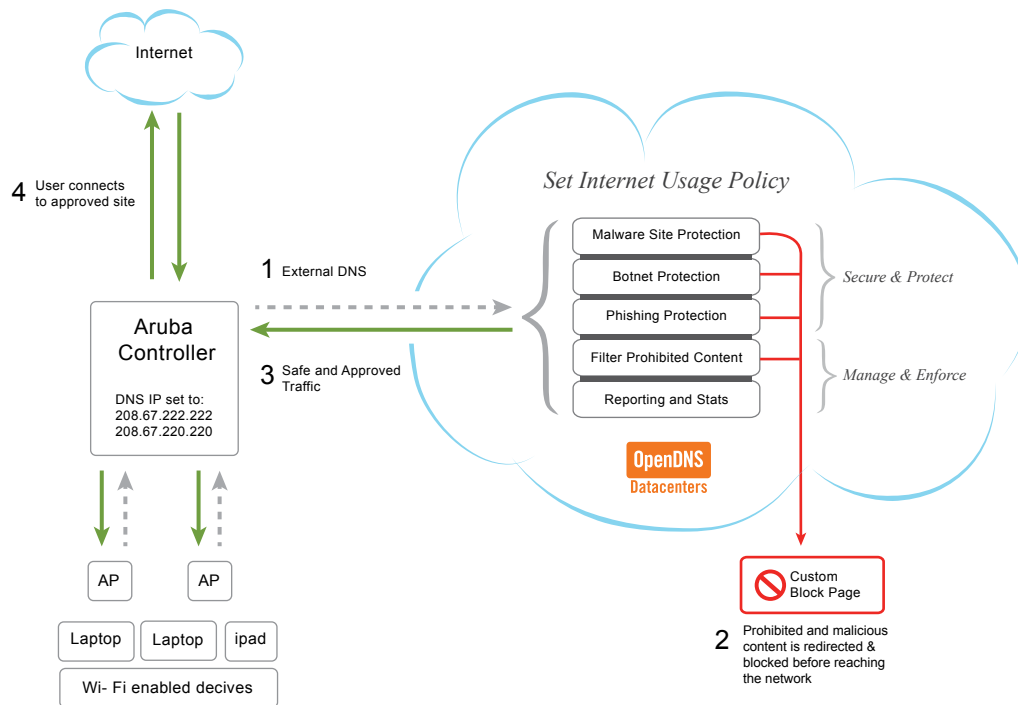
OpenDNS's rich database of more than 57 categories and millions of domains allows businesses to limit their exposure to liability, increase productivity and control bandwidth usage by managing access to non-business related or inappropriate sites on their network. Paramount to extending the network beyond the corporate headquarters is enforcing Internet access policies no matter whether the device is a PC, laptop or CEO's iPad connected to the corporate network.

The Web based administration console allows quick set up and management of Web filtering policies on a per-site or per network basis. IT Administrators also have the option to grant trusted users the ability to bypass some or all of the Web filtering settings. This flexibility gives businesses control without limiting the productivity of groups that may require access to certain sites.

SIMPLE TO DEPLOY, EASY TO MANAGE AND SCALABLE

Since OpenDNS is a cloud based service it can be quickly and easily deployed across 1 to 1000's of locations without the need to install additional hardware or software on site. Set up and deployment takes 30 minutes or less. All configuration, management and reporting is done through the Web-based dashboard that is accessible from anywhere and at any time enabling businesses to simplify their networks and reduce on going costs.

ABOUT OPENDNS



OpenDNS is the world's leading provider of Internet security and DNS services that enables the world to connect to the Internet with confidence on any devices, any where, any time. OpenDNS provides millions of businesses, schools and households with a safer, faster and more intelligent Internet experience by protecting them from malicious Web threats, providing them control over how users navigate the Internet while dramatically increasing the network's overall performance and reliability.

ABOUT ARUBA

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. To learn more, visit Aruba at www.arubanetworks.com. For real-time news updates follow Aruba on [Twitter](#) and [Facebook](#).



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