Solution Brief

Aerohive NETWORKS

Barracuda

Aerohive and Barracuda

Technical Solution Brief

Table of Contents

Introduction	3
The Aerohive Networks and Barracuda Solution	3
How It Works	4
Step-by-Step	4
Configuring the Barracuda NG Firewall	6
Summary	7
About Aerohive and Barracuda	8

Introduction

Connecting people wirelessly is the norm today with the use of multiple devices for business-critical and personal activities. Access to the Internet is vital for doing business. Having a solution that protects you from Internet content that detracts from your organization's goals and secures against dangers is essential. Setting limits on what Web content users are able to access can be essential for businesses involved in education, health care, high finance, or government work bound by regulatory requirements. Even small and family-run retailers must meet strict standards concerning credit card data.

The Children's Internet Protection Act (CIPA) is a federal law enacted by Congress in December 2000 to address concerns about access to offensive content over the Internet on school and library computers. Schools and libraries are required to certify that they have their safety policies and technology in place before receiving E-Rate funding.

Aerohive's application visibility and policy enforcement functionality provides an administrator with extremely detailed and granular information and controls to optimize users' application experience at the edge of the network. Aerohive can customize how applications are prioritized, de-prioritized, or blocked based on all available context, including identity of the user, device type, location on the network, and the time of day. This is extremely useful for ensuring that traffic is appropriately categorized and potentially blocked before it ever even gets onto the network infrastructure, saving valuable resources and providing an extra layer of security. However, many networks require aggregated controls as well as edge-based enforcement, and when you combine the Aerohive mobility-optimized access layer with Barracuda Web Filter and NG Firewall, administrators get a comprehensive solution that provides increased productivity, protects from dangers and importantly, in school and library environments, protects children from cyber bullying and predators.

The Aerohive Networks and Barracuda Networks Solution

Aerohive has the advantage of knowing all the available user context because devices are connecting and users are authenticating to the access points and switches directly in order to gain access to the network. Barracuda NG Firewalls and Web Filters, alternatively are generally installed at the gateway to the network everything coming or going in aggregate, but the user context is often obscured due to all the network infrastructure between the gateway and the connected client. Together, Aerohive and Barracuda Networks solve the problems of the mobile first enterprise by combining information about user context with application visibility and controls. Content filtering policies can be customized to restrict specific websites or look for patterns in web addresses. Administrators can also create policies that control web file downloads based on their file types.

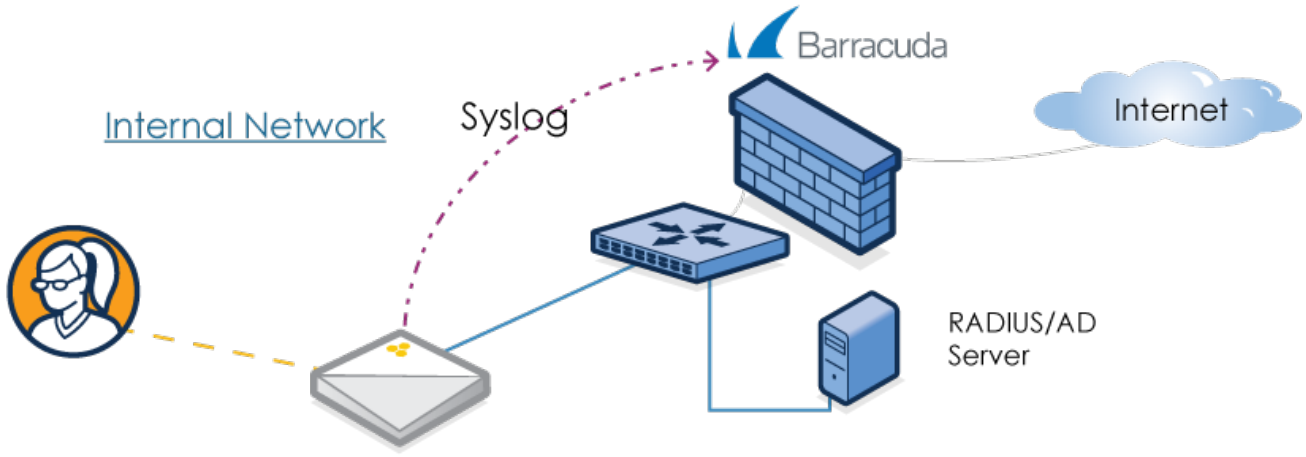
Aerohive's Cooperative Control networking infrastructure equipment along with Barracuda Web Filter and NG Firewall provide a comprehensive and robust solution for optimizing the user experience on a mobile-first network. Together, this solution provides many benefits, including:

- **Enhanced user-identity awareness and Enforcement** – Aerohive devices can provide user identity, device type, and IP address information to the Barracuda Web Filters and NG Firewalls to enhance the UserID functionality that allows Barracuda to create security policies to make policy decisions based on context
- **Client-less Operation –** Barracuda's and Aerohive's interactive communication provides seamless, enhanced security to connected clients and the Aerohive devices. All inbound and outbound traffic is forwarded to the Barracuda device without the need to install client profiles or agents.
- **Zero-Cost Data Performance –** Barracuda gathers information from Aerohive devices as part of normal authentication. There is no in-line performance hit for using this integration to enhance application control on the network.

- **Comprehensive Application Visibility and Control –** Together, Aerohive and Barracuda Networks allow administrators to enforce application controls at both the edge of the network and at the gateway, ensuring applications are identified and prioritized/de-prioritized/blocked based on context at the ideal enforcement point.

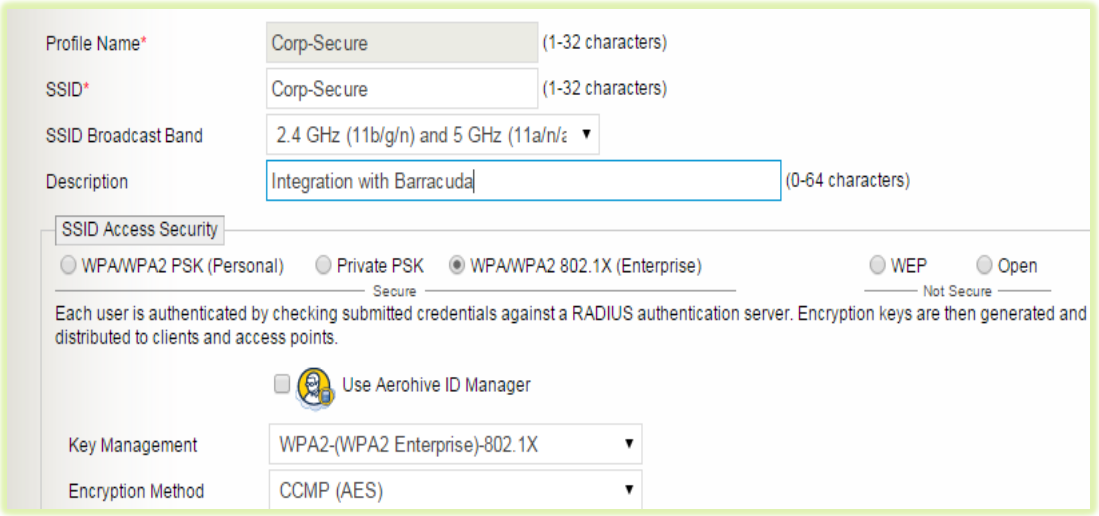
How It Works

The Aerohive and Barracuda solution leverages Barracuda NG Firewalls or Barracuda Web Filters to work with Aerohive access points, switches and routers. The Aerohive administrator simply selects Aerohive as the access point vendor in Barracuda's configuration settings and then configure the syslog object to direct to the Barracuda Web Filter or Barracuda NG Firewall.

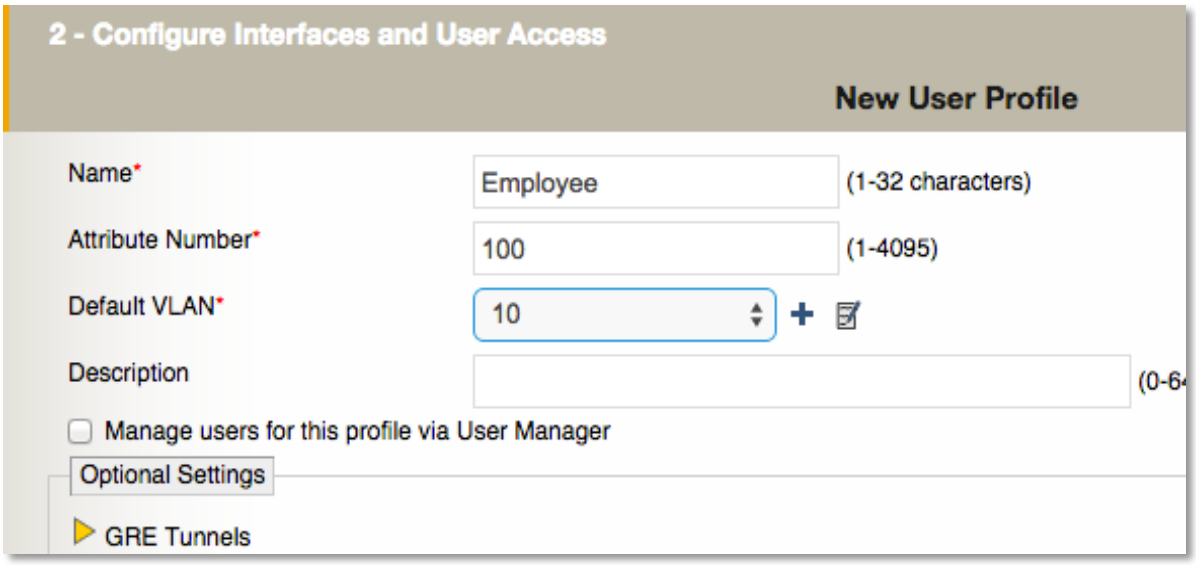


Step-by-Step

1) Configure SSID – WPA2 Enterprise (802.1x)



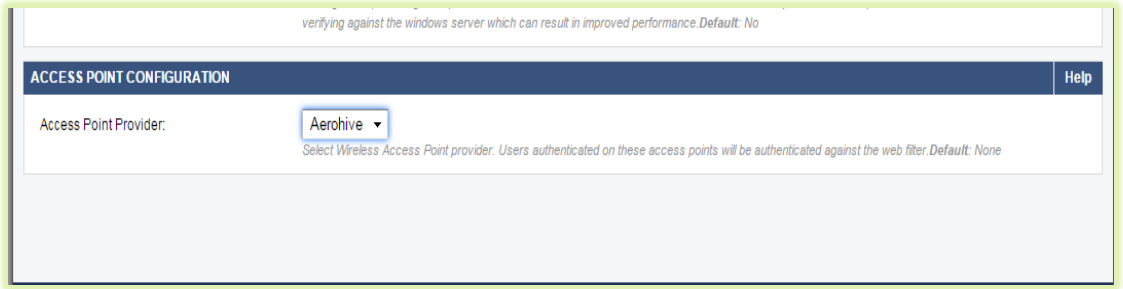
2) Configure User Profile(s)



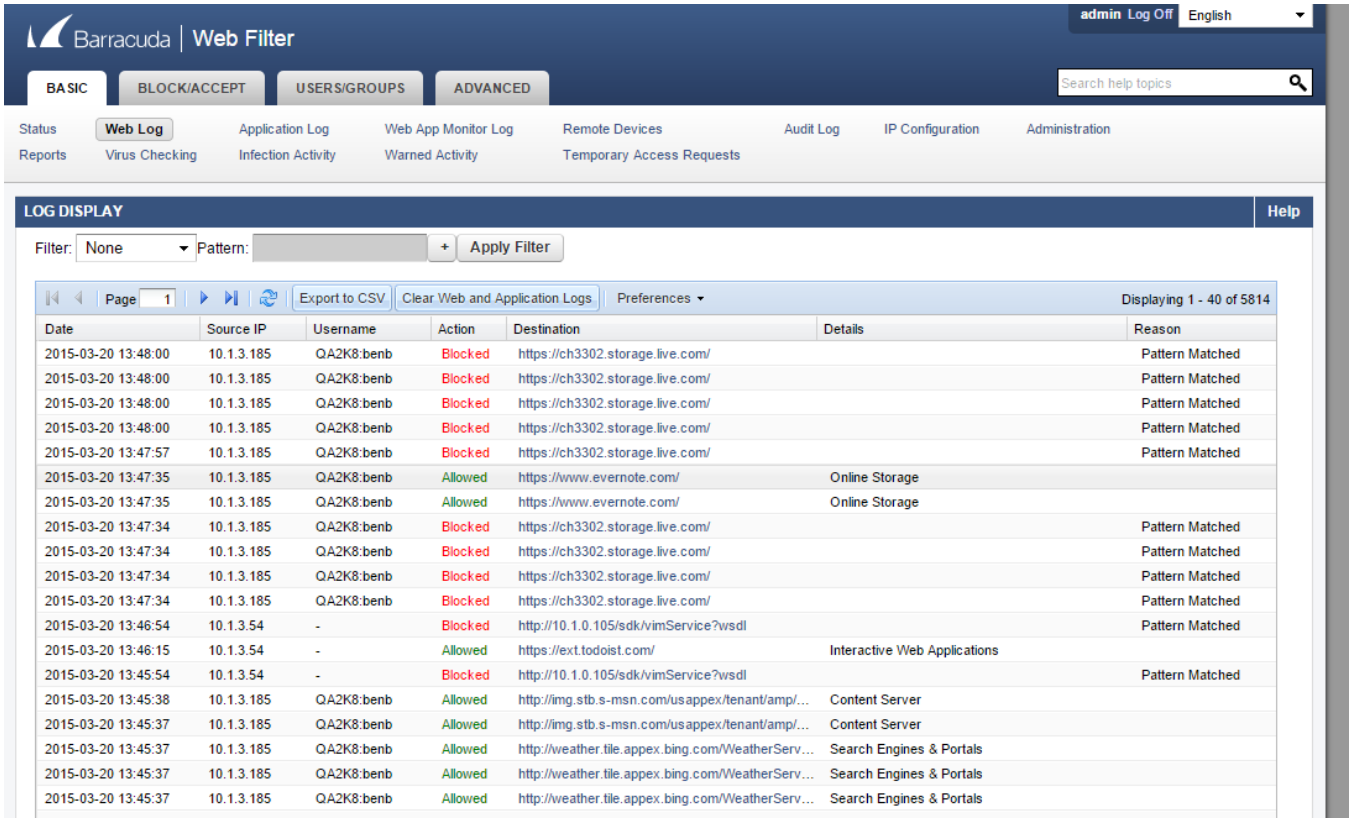
3) Configure Syslog

4) Upload configuration

5) Configure Barracuda Web Filter to recognize Aerohive as an access point vendor

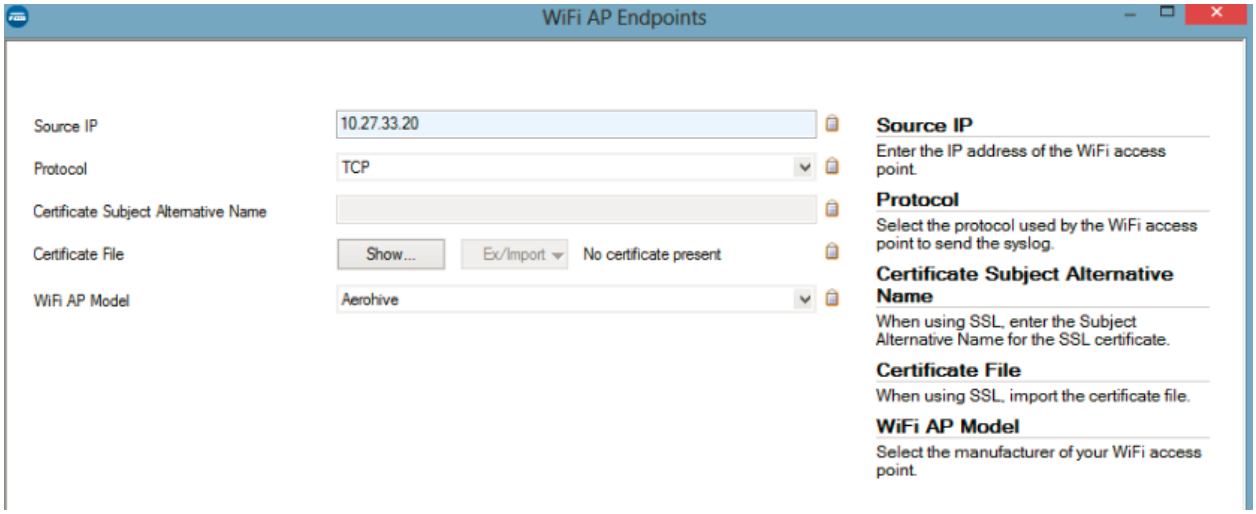


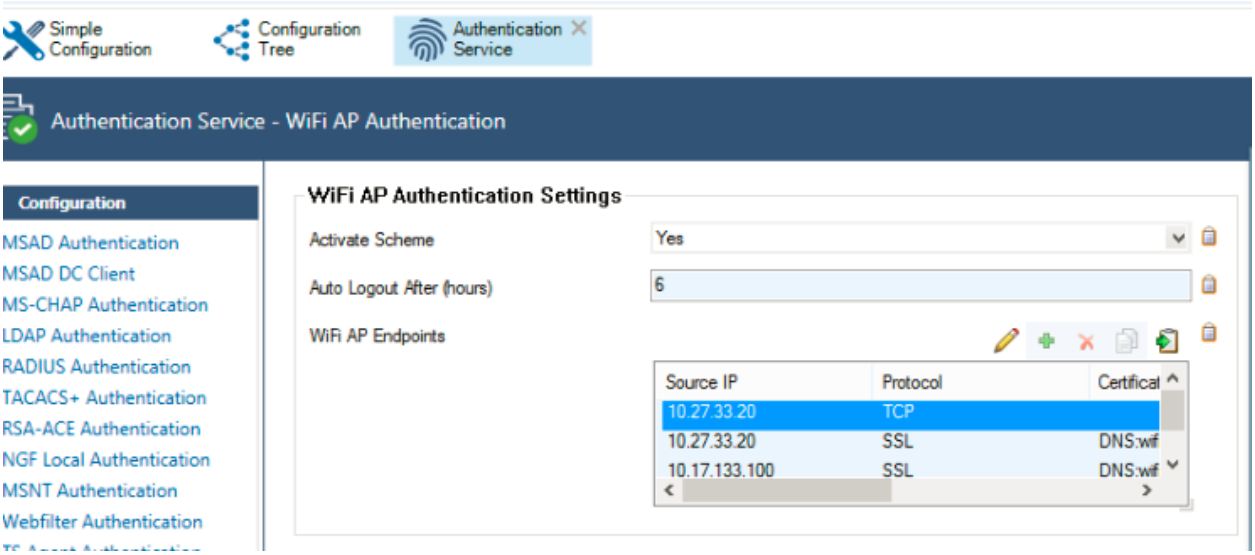
6. Connect to Barracuda appliance and observe the reports and forensics



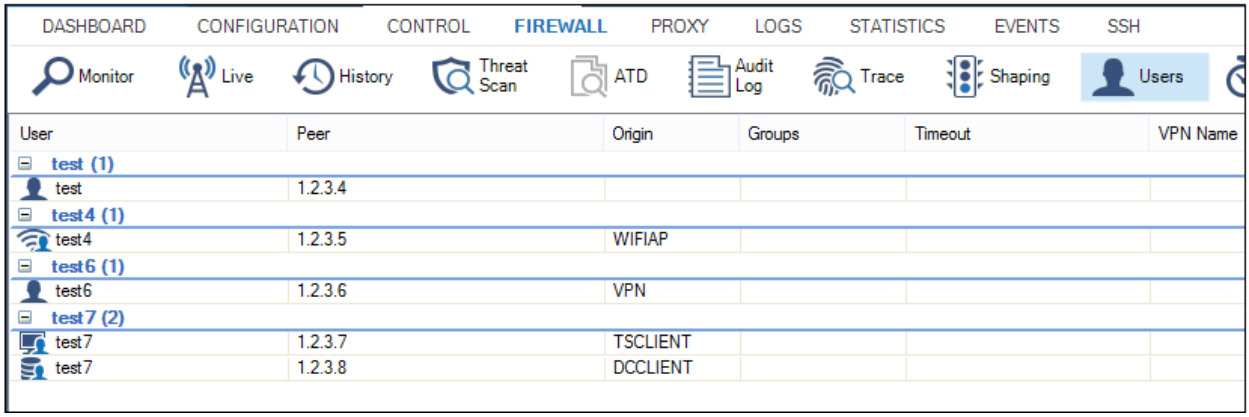
Configuring the Barracuda NG Firewall

1) Under Authentication Service enter the IP address of the Aerohive Access Point and select AP model > Aerohive





2) Connect with your username and observe the results in Dashboard



Summary

Aerohive and Barracuda's synergistic integration provides enterprises with enhanced application and enhancement, as well as regulatory compliance combined with the cloud managed zero-client security solution. Aerohive access points, switches, and routers provide quick remote office connections with integrated DHCP, DNS, routing, wireless, and wired security. Barracuda Web Filter and NG Firewalls integrated with the context available from Aerohive's mobility platform enables businesses to use the same firewall and context-based filtering policies on wired and wireless networks.

About Aerohive Networks, Inc.

Aerohive (NYSE: HIVE) enables our customers to simply and confidently connect to the information, applications, and insights they need to thrive. Our simple, scalable, and secure platform delivers mobility without limitations. For our over 20,000 customers worldwide, every access point is a starting point. Aerohive was founded in 2006 and is headquartered in Sunnyvale, CA. For more information, please visit http://www.aerohive.com, call us at 408-510-6100, follow us on Twitter @Aerohive, subscribe to our blog, join our community or become a fan on our Facebook page.

About Barracuda Networks, Inc.

Barracuda (NYSE: CUDA) provides cloud-connected security and storage solutions that simplify IT. These powerful, easy-to-use and affordable solutions are trusted by more than 150,000 organizations worldwide and are delivered in appliance, virtual appliance, cloud and hybrid deployments. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data security. For additional information, please visit barracuda.com.

Aerohive Networks, Inc.
330 Gibraltar Drive
Sunnyvale, California 94089 USA

phone: 408.510.6100
toll-free: 866.918.9918
fax: 408.510.6199

www.aerohive.com
info@aerohive.com

Barracuda Networks, Inc.
3175 S. Winchester Blvd.
Campbell, CA 95008

408.342.5400 (US)
888.268.4772 (Canada)