



828 West Taft Avenue
Orange, CA 92865
714-282-6111
714-282-6116 Fax
www.8e6.com

8e6 3000 | Enterprise Filter



R3000 Enterprise Filter vs. Integrated Solutions

Scope

The scope of this white paper is to discuss network installation options for the R3000 Enterprise Filter and how it differs from integrated or embedded solutions.

Product Definition

The 8e6 R3000 Enterprise Filter is a hardware-based appliance solution that allows users to monitor, filter and log an organization's Internet traffic. Through user-defined parameters based on 8e6's 75+ categories of Web content, an R3000 filter will help improve employee productivity, reduce liability and preserve network resources.

Overview

The R3000 is a stand-alone filtering appliance engineered to fulfill the filtering requirements of organizations without the need to integrate with specific hardware or be embedded into networking devices that already specialize in other core functions.

For example, caching devices were designed to optimize network performance by caching web pages or other files so that the cache could satisfy successive requests for the information rather than requiring the user to repeatedly access the Internet. The bandwidth savings enjoyed by organizations that invest in caching technologies would remain intact with the installation of an R3000 because the caching device will not suffer from decreased response times or be required to use up precious internal resources participating in URL redirection. Shared caching and filtering functionality, on the other hand, would end up enduring the drawbacks of an integrated solution.

Firewall or Proxy servers with options for integrated or embedded solutions can also realize the same benefits. The R3000 was designed from the ground up as a specialized appliance to take care of Internet filtering leaving your Firewall, Cache Engines or Proxy Servers to perform the core tasks they were designed to accomplish.

The R3000 has flexible installation options which, based on network and/or specific requirements, can be configured in one of three modes: Invisible, Router or Firewall.

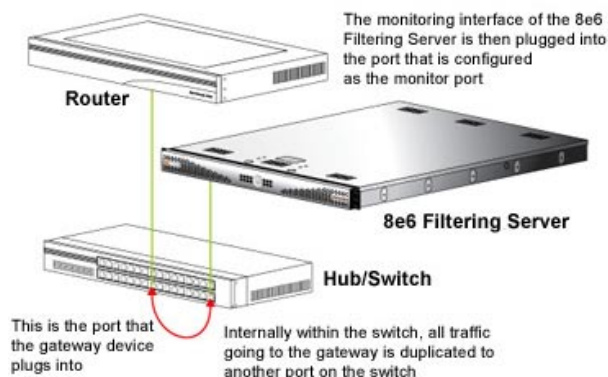
Installation Modes

Invisible Mode

Invisible mode allows for the R3000 to filter without requiring an administrator to route traffic to the R3000. The R3000 works in conjunction with the port mirroring capability that is an inherent function with most switches available today including, but not limited to, those manufactured by Cisco and 3COM (Network TAPS may also be used where port mirroring is not an option). Traffic destined for one or more “source” ports will be internally copied across the backplane of the switch to a “monitor” port on the switch. The R3000’s filtering interface will be connected to this monitor port so it can analyze the packets. It then compares the requests against its library of URLs or packet signatures and replies with a mitigating response only if the request violates the policy established by the administrator. If the request does not violate policy, the original packet or web request is allowed to continue without interference since the switch provided the R3000 with a copy of the request. The need to redirect the request just to be able to check it is essentially eliminated. This is in sharp contrast to solutions where the request, good or bad, must be stopped and redirected to a filtering server so a decision can be made to allow or deny the request.

The R3000’s Invisible mode option provides organizations with the fastest response time when it comes to accessing the web. Organizations that require Internet filtering, but do not want the added latency presented by stop-and-check solutions will find the R3000’s Invisible mode a welcome feature.

This diagram illustrates how the R3000 is connected to the managed switching hub. The R3000 port is configured with the “port monitoring” function enabled. This allows the port to mirror the port that is connected to the router.



Installation Modes (continued)

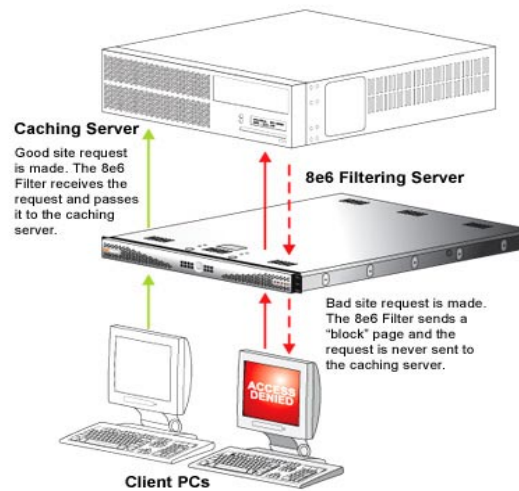
Router/Firewall Modes

In Router or Firewall Mode, the R3000 can be configured so that it is installed in-line or in the flow of traffic. In these modes, the R3000 essentially becomes a pass-through solution and traffic must be routed to the R3000 appliance.

In Firewall mode, the packet will be inspected for inappropriate requests before the packet is allowed to proceed. If the packet contains an inappropriate request, the packet is not allowed to exit the R3000 and a terminated session and/or block page will be the result. If the request is appropriate, the R3000 will release the packet unchanged.

In Firewall mode, the R3000 can be installed in a manner whereby it will actually prolong the useful life of caching devices, as it will filter URL requests prior to sending the request to a caching device

In this set-up, a local caching proxy will not affect the R3000, even if it is unfiltered and contains cached "bad" pages, since no request can pass until after it is filtered.



Summary

The R3000 was designed to be a stand-alone, best-of-breed Internet filtering product not required to support proprietary protocols or be installed on networking equipment originally intended to provide other primary functions in addition to URL filtering.

This allows the end-user to avoid the problem of increased degradation of performance, which usually results in the expense of purchasing additional cache engines/firewalls/proxies or hardware upgrades much sooner than expected.

The R3000 leverages the networking hardware already in place at many organizations and ultimately improves their performance when added functionality such as URL filtering and/or IM/P2P traffic mitigation is required.