Advanced Configuration

https://campus.barracuda.com/doc/6160405/

Virus Protection

By default, virus scanning is automatically enabled on the Barracuda Web Security Gateway, and the virus definitions are updated on a regular basis (hourly by default) using Energize Updates.

When virus scanning is enabled, all traffic processed by the Barracuda Web Security Gateway is scanned for viruses and any traffic that contains a virus is blocked. If you already have anti-virus software protecting your web traffic, you can turn off virus scanning on the Barracuda Web Security Gateway using the **BASIC > Virus Checking** page. Otherwise, it is recommended to leave this feature turned on. This feature includes the option to block encrypted archives such as zip, tar, and rar files that are password protected, as viruses. The maximum encrypted file/archive size that can be scanned and blocked is 10Mbytes.

With version 11.0 and higher, when a virus is detected by ATP or the enhanced virus checking engine, the user will be presented with a block page per the example below. Note that, unlike other block pages, this block page is *not* configurable in the Barracuda Web Security Gateway web interface.

Viruses detected by the basic virus scanning feature on the Barracuda Web Security Gateway (i.e. when **Enable Virus Protection** is set to **Yes** on the **BASIC > Virus Checking** page) will result in the block page customizable on the **BLOCK/ACCEPT > Block Messages** page.

Advanced Threat Protection

With version 11.0 and higher, the Barracuda Web Security Gateway provides subscription-based access to the Advanced Threat Protection (ATP) service to analyze web traffic for viruses in a separate, secured cloud environment. Beyond the basic Barracuda Web Security Gateway virus scanning, the ATP service detects new threats and determines whether to block scanned files that are

found to be infected. Configure on the **BASIC > Virus Checking** page. See Advanced Threat Protection Configuration for details.

Proxy Settings

Use the **ADVANCED > Proxy** page to configure proxy settings for peer proxies, headers, HTTP and HTTPS ports as well as exceptions to proxy authentication by source IP address, domain name, header pattern or destination IP address. Note that peer proxy only works with inline deployments - for details, see Deploying the Barracuda Web Security Gateway with a Peer Proxy.

Web Caching

Web caching on the Barracuda Web Security Gateway can accelerate web page downloads and also reduce traffic on the external network connections. For these reasons, it is recommended to keep web caching enabled. Use the **ADVANCED > Caching** page to enable or disable web caching, to clear the cache or to create exceptions for domains you don't want the Barracuda Web Security Gateway to cache.

Figures

1. virus_block_page.jpg