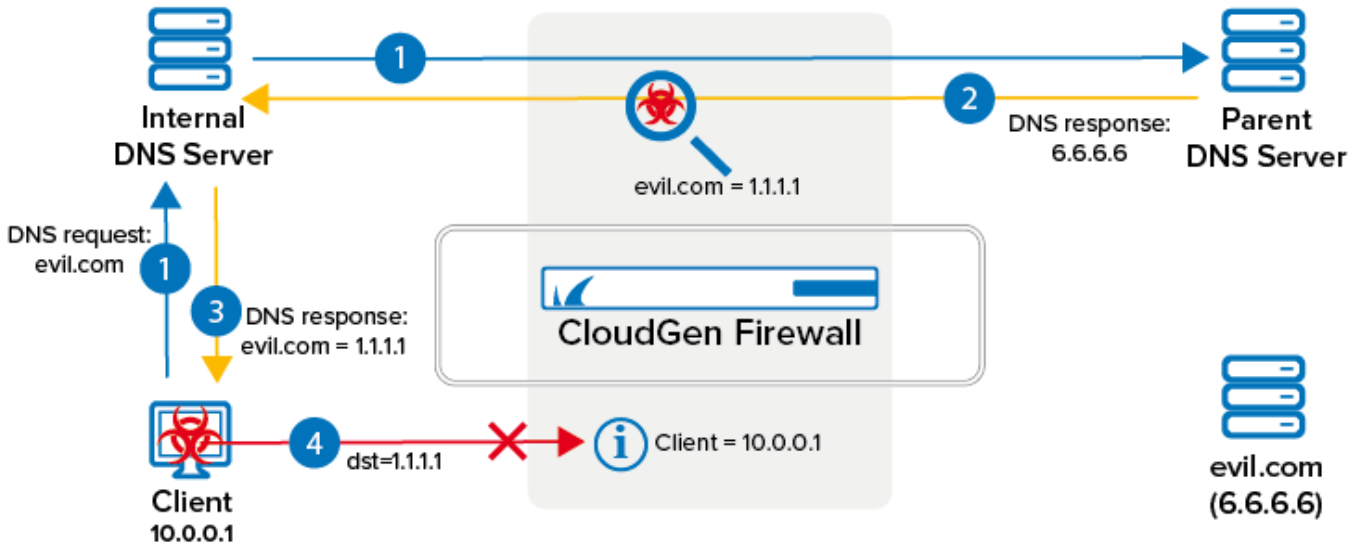
Botnet and Spyware Protection in the Firewall

https://campus.barracuda.com/doc/98210195/

To protect your network against botnets and spyware, the CloudGen Firewall monitors what domains are accessed by the clients in the network. If malicious sites or domains are accessed by any protocol whatsoever, not just HTTP or HTTPS, the firewall redirects the traffic to a fake IP address and monitors access to that IP address to identify infected clients.

DNS Sinkhole



DNS sinkholing blocks clients from accessing malicious domains by monitoring UDP DNS requests passing through the firewall. TCP DNS requests are not monitored. These DNS requests can originate directly with the client if an external DNS server is used, but may also come from an internal DNS server querying the parent DNS server. Since both the host and the forwarding firewall are monitored, DNS sinkholing also works for DNS caching and DNS servers running as a service on the firewall. The firewall monitors the DNS response and modifies the A and AAAA DNS responses to return fake IP addresses if the domain is considered to be malicious. The client then attempts to access the fake IP address, allowing the firewall to determine the IP address of the client, even if an internal DNS server is used. This information is made available to the admin through the Firewall Monitor and the Threat Scan page in Barracuda Firewall Admin. Compared with the URL Filter service, which also blocks access to malicious sites, DNS sinkholing is not limited to the HTTP and HTTPS protocols, thereby offering better protection against malware.

The local botnet database on the CloudGen Firewall is synced with the online botnet database and has the option to override it with manual allow lists and block lists. An Advanced Threat Protection subscription is required.

For more information, see How to Configure DNS Sinkholing in the Firewall.

Configuring Botnet and Spyware Protection for Web Traffic

If you are not using a DNS sinkhole, you can configure the URL filtering in the firewall to achieve similar results for HTTP and HTTPS traffic. This allows you to restrict access to malicious websites that may compromise the security of your client. The **Malicious Sites** URL category contains the same domain reputation database as used by the DNS sinkhole. Create a URL Filter policy object and set the **Malicious Sites** category to **Block** and use it in the application rule matching your web traffic. When access to a malicious site is detected, the user is redirected to a custom block page. A valid Energize Updates subscription is required to enforce Botnet and Spyware protection for web traffic.

For more information, see How to Configure Botnet and Spyware Protection for Web Traffic.

Figures