How to Configure DNS Blacklisting

https://campus.barracuda.com/doc/46209378/

To redirect blacklisted domains on the firewall level, use DNS blacklisting. The Barracuda NextGen Firewall F-Series scans replies from the DNS servers and manipulate the replies if blacklisted hostnames are found. DNS blacklisting only works for UDP DNS queries. If the DNS queries use TCP, the blacklist is not applied.

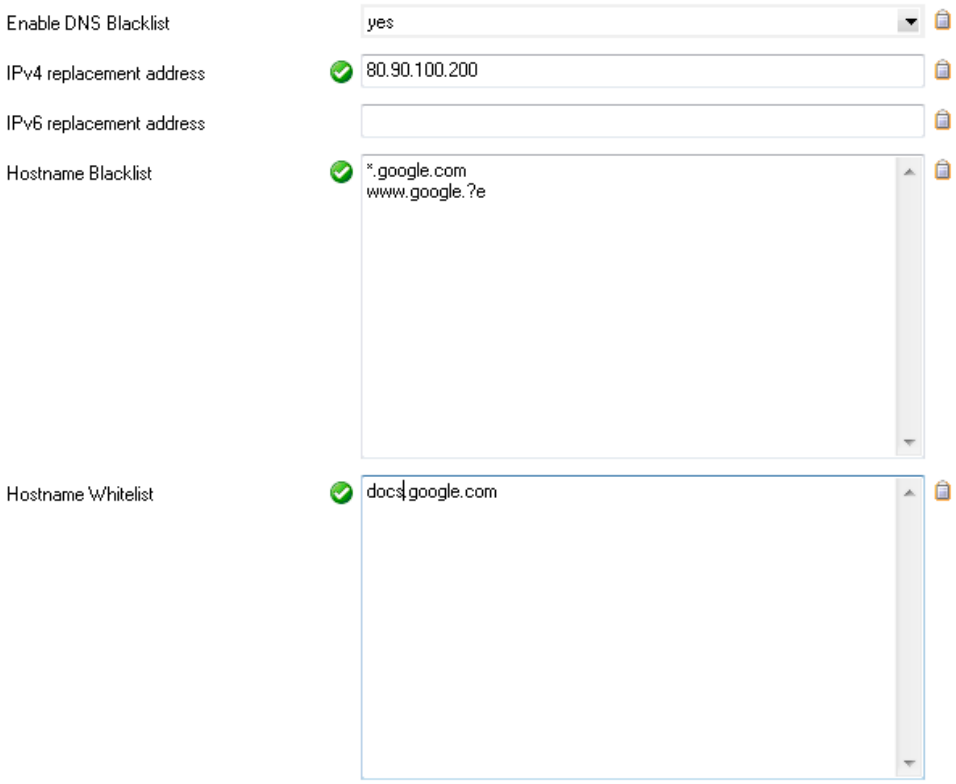
- The DNS query is intercepted and the A record is replaced with a replacement IP address.
- The DNS query is intercepted and answered with *NXDOMAIN*, signaling the hostname does not exist.

Webbrowsers or the operating systems local DNS cache, may use the DNS replies stored in their local caches, circumventing DNS blacklisting.

Configure DNS Blacklisting

Configure domains that should be blocked or redirected.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > *your virtual server* > Assigned Services > Firewall > Forwarding Settings**.
2. In the left navigation, click **DNS Blacklist**.
3. Click **Lock**.
4. Enable **DNS Blacklisting**.
5. Configure an IPv4 and or IPv6 address which will be returned for blacklisted domains.
6. Enter a list of hostnames in the **Hostname Blacklist** area. These domains will be blacklisted. You can use the following wildcards: * and ? to block multiple domains.
   Example: *.google.com will filter all subdomains of google.com, while www.google.?e will filter domains, such as www.google.de and www.google.se.
7. Enter exempted domains in the **Hostname Whitelist** area. These domains will not be blocked, even if they are included in the **Hostname Blacklist**.



8. Click **Send Changes** and **Activate**.

If queries are blocked/replaced due to blacklisting, an entry is added in the **IPS** section of the Threat Scan Page.

AID	Act...	Source	Service	Destination	Scan Result	IPS Seve...	IPS Category	Rule	C..	Last
(10) IPS										
S-16	Scan	62.99.0.40	google.com	216.239.32.10	DNS Blacklist	Medium	Access Control	BOX-DNSREC-OUT	10	32s
S-17	Scan	62.99.0.40	google.com	216.239.34.10	DNS Blacklist	Medium	Access Control	BOX-DNSREC-OUT	17	32s
S-18	Scan	62.99.0.40	google.com	216.239.36.10	DNS Blacklist	Medium	Access Control	BOX-DNSREC-OUT	8	1m 37s
S-19	Scan	62.99.0.40	google.com	216.239.38.10	DNS Blacklist	Medium	Access Control	BOX-DNSREC-OUT	1	1m 37s
S-20	Scan	62.99.0.40	www.google.com	216.239.36.10	DNS Blacklist	Medium	Access Control	BOX-DNSREC-OUT	6	57s
S-21	Scan	62.99.0.40	www.google.at	216.239.38.10	DNS Blacklist	Medium	Access Control	BOX-DNSREC-OUT	1	55s
S-22	Scan	62.99.0.40	google.at	216.239.36.10	DNS Blacklist	Medium	Access Control	BOX-DNSREC-OUT	9	29s
S-23	Scan	62.99.0.40	www.google.at	216.239.34.10	DNS Blacklist	Medium	Access Control	BOX-DNSREC-OUT	1	25s

Figures

1. DNS_Backlisting.png
2. FW_DNS_Blacklist.png