Authoritative and Caching DNS

https://campus.barracuda.com/doc/8650782/

The Barracuda NextGen Firewall X-Series can use a caching DNS to speed up frequently queried DNS requests in the network, or can be configured to act as an authoritative DNS server for your domains. The caching DNS and the authoritative DNS are two separate, mutually exclusive services on the NGX.

Enable Authoritative DNS to allow intelligent responses to DNS requests by evaluating link state and source IP address before answering the DNS request. You can use either static or dynamic WAN IP addresses.To use the ADNS server for internal clients the **LOCALDNSCACHE** access rule must be active.

Caching DNS intercepts DNS requests from your network to external DNS servers and if the answer to the request is present in the local cache, replies to the query speeding up DNS queries in your network and saving bandwidth in the process. DNS caching is always active when ADNS is enabled, all DNS requests are redirected to the local ADNS server.

Caching DNS

Enable Caching DNS for all connections by setting **Caching DNS** on the **NETWORK > IP Configuration** page to **Yes**. This setting is overridden when the authoritative DNS server is enabled.

Authoritative DNS

You must change the settings at your domains registrar to allow the X-Series Firewall to act as the nameserver for your domain. After adding the domain you can configure the following record types:

- **A** — Use this DNS record to match an IPv4 IP address to a hostname. Each host in a domain should have an A record.
- **NS** — NS records specify the authoritative name servers for the (sub)domain. If the domain name server is inside the domain, enter the FQDN ending with a dot. E.g., ns.example.com.
- **MX** — Use this type of DNS record to define the mail servers for the network. If multiple mail servers are used enter a preference between 0 and 65535. The MX record with the lowest preference is used first by the sending agent. If not available the server with the next higher preference is tried until a successful connection can be established.
- **TXT** — This record associates a text string with the hostname. Use this for services which do not have a DNS record type of their own such as SPF.
- **CNAME** — This creates an alias for an already existing cannonical name. The link target does

not have to be a part of the domain. E.g., Create a CNAME record which points **www.cuda-inc.com** to **www.barracuda.com**
- **SRV** — Define services available in the domain such as LDAP or SIP.
- **PTR** — PTR records point to a canonical name. Unlike CNAME the host name is returned and not resolved. Use for reverse DNS lookups.
- **OTHER** — Use this to define a DNS record which is not listed above.

DNS zone transfer blocking

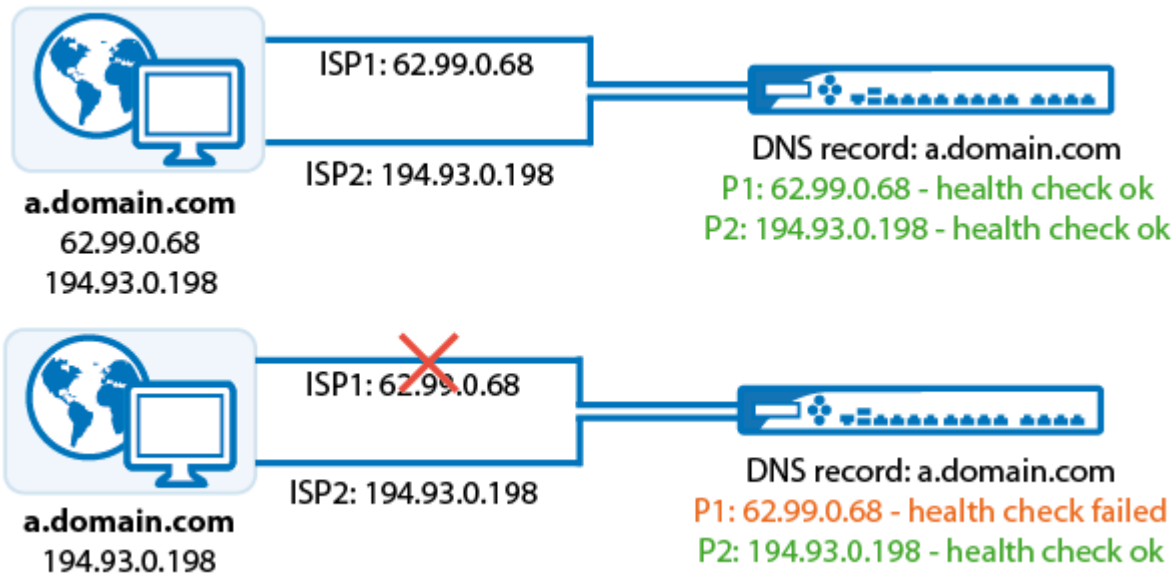
The X-Series Firewall can be configured to block zone transfers on some or all of the domains that it hosts. An AXFR/IXFR query that is sent from another DNS server to the firewall (to request a copy of the DNS records) is rejected if zone transfers are disabled for that domain. By default, zone transfers are enabled for all domains created. This feature is necessary if you want to force all DNS requests to be handled directly by the firewall and the results not to be cached by recursive DNS servers. DNS zones, which are only reachable internally are not transferred to other DNS servers.

Split DNS

The X-Series Firewall can return different IP addresses depending on the source IP address of the DNS request. When configured a client in the internal network receives the local IP address of the server while a client from the Internet is responded to with the external WAN IP address.

For more information, see How to Add Domains and DNS Records.

Link failover and monitoring



If multiple ISP connections are used, create a DNS records for each interface to return DNS answers based on which connection is used for the incoming DNS request. During normal operation with all ISP connections up the DNS server returns the complete list of all IP addresses (for all interfaces). The client will then choose the IP address out of the list that most closely resembles its own IP address (RFC-3484). This behavior can not be influenced by the DNS server. The firewall continuously checks the health check targets defined in each DNS record. In case one of the health check fails, the corresponding DNS record is removed from the list of returned IP addressed. This ensures that the clients will not try to connect to an unavailable IP address. Depending on the time to live (TTL) configured, it will take some time for the change of the DNS response to be propagated to all recursive DNS servers. Using shorter TTL will speed up this process, but increase the number of DNS queries on the firewall.

Figures