How to Add Domains and DNS Records

https://campus.barracuda.com/doc/41109753/

Configure the Barracuda NextGen X-Series Firewall to be the authoritative DNS server for your domains or subdomains to take advantage of Split DNS or dead link detection.

Step 1. Make the X-Series Firewall the authoritative DNS server at your domain registrar

To become the authoritative DNS server for a domain contact the registrar for your domain to use the static or dynamic WAN IP addresses of your X-Series Firewall.

Hosting a subdomain

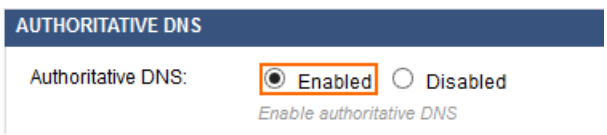
If you want to delegate a subdomain to the X-Series Firewall, add ns1 and ns2 records to the zone file of the domain where it is stored at the registrar. If the domain is **yourdomain.com**, and you want to host **subdomain.yourdomain.com** add the following DNS records:

- `subdomain IN NS ns1`
- `subdomain IN NS ns2`
- `ns1 IN A <WAN IP 1 OF YOUR BARRACUDA FIREWALL>`
- `ns2 IN A <WAN IP 2 OF YOUR BARRACUDA FIREWALL>`

Step 2. Enable authoritative DNS on the X-Series Firewall

In the **DNS Servers** table, you can view a list of the static IP addresses for which the DNS Server service is enabled (**NETWORK > IP Configuration**). Dynamic IP addresses are not listed. An access rule is created in step 3 to redirect incoming DNS requests on dynamic interfaces to the DNS service on the firewall. The access rule **LOCALDNSCACHE** must be active after enabling authoritative DNS for local clients to access the DNS server.

1. Go to the **NETWORK > Authoritative DNS** page.
2. Enable **Authoritative DNS**.

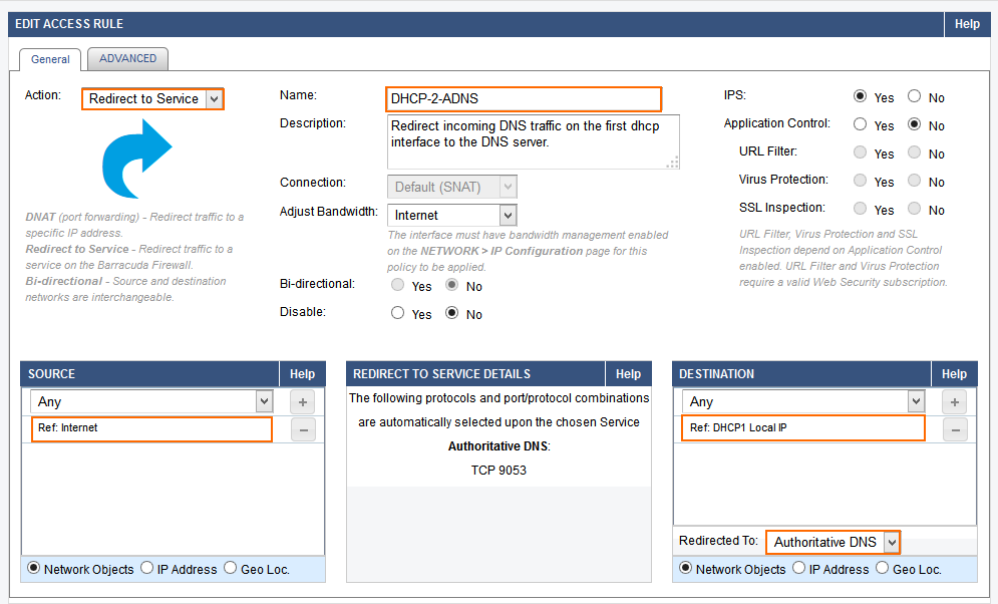


3. Click **Save**.

Step 3. (Dynamic WAN connections only) Create a redirect access rule

To redirect DNS traffic for dynamic WAN interfaces you must redirect the incoming traffic to the authoritative DNS service.

1. Go to the **FIREWALL > Firewall Rules** page.
2. Click on **Add Access Rule**.
3. Create a **Redirect to Service** rule:
   - **Name** – Enter a name for the access rule, e.g. DHCP-2-ADNS
   - **Source** – Select **Internet** and click **+**.
   - **Destination** – Select the network object for the dynamic interface and click **+**. Repeat for each dynamic WAN connection. E.g., **DHCP1 Local IP**
   - **Redirect To** – Select **Authoritative DNS**.
4. Click **Save**.

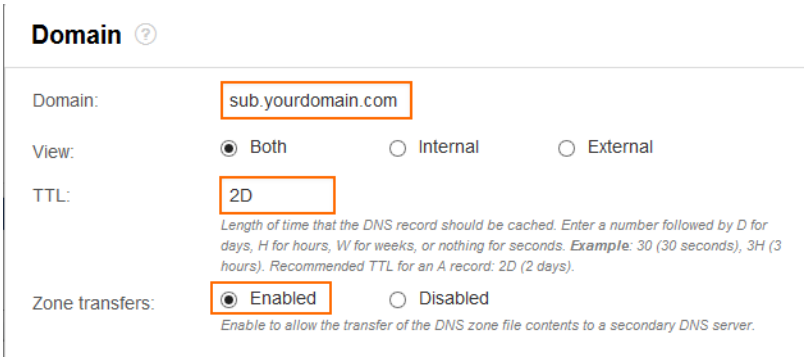


5. Place the access rule toward the top of the ruleset so that no access rule before it matches incoming DNS traffic on dynamic interface(s).

Step 4. Add a domain

Add a new domain to the ADNS configuration.

1. Go to the **NETWORK > Authoritative DNS** page.
2. In the **DNS RECORDS** section click on **Add New Domain**. The **DOMAIN** windows opens.



3. Enter the settings for the domain or subdomain:
   - **Domain** – Enter the domain or subdomain. E.g., `yourdomain.com` or `subdomain.yourdomain.com`
   - **Access to Domain/Zone**
     - **Internal and External** – The DNS Server answers queries from all networks.
     - **Internal** – The DNS Server answers queries from trusted networks.
     - **External** – The DNS Server answers queries from untrusted networks.
   - **TTL (Time to Live)** – This value determines how long DNS records are cached by recursive DNS servers. Use **D** for days, **H** for hours, **W** for weeks or nothing for seconds. Recommended TTL for a **A** records: 2D.
   - **Zone Transfers** – Enable to allow recursive DNS server to cache DNS records. Disable to force clients to query the DNS server on the firewall directly for each DNS request. Default: enabled.
4. Click **Save**.

The domain or subdomain is now listed in the **DNS RECORDS** section. **NS** and **SOA** records are automatically created for the new domain. The **NS** records are set to the static IP addresses with the DNS server listener enabled.

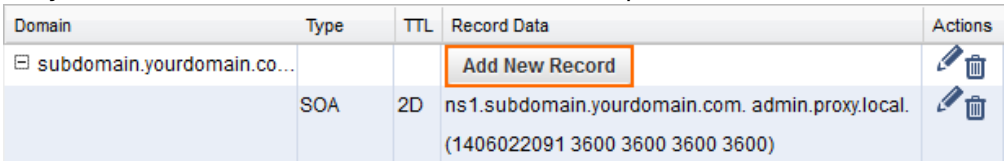
Domain	Name	Type	TTL	Links	IP	Health	Record Data	Actions
⊟ subdomain.yourdomain.co...							Add New Record	
		SOA	2D				ns1.subdomain.yourdomain.com. admin.proxy.local. (1406022091 3600 3600 3600 3600)	
	ns3	A	2D	p1	10.0.10.6	⚠	10.0.10.5	
	ns1	A	2D	p3	62.99.0.68	⚠	10.0.10.5	
	ns2	A	2D	p3:0	62.99.0.67	⚠	10.0.10.5	
		NS	2D				ns3	
		NS	2D				ns2	
		NS	2D				ns1	

Step 5. Add DNS records for the domain

You can now create DNS records for your domain or subdomain.

1. Go to the **NETWORK > Authoritative DNS** page.

2. In the **DNS Records** section click on the **Add New Record** button in the **Record Data** column for your domain. The **DNS RECORD** window opens.



3. Select the **Type** of **DNS Record**. E.g., `testrecord`
4. Enter the parameters required for the chosen DNS record type.

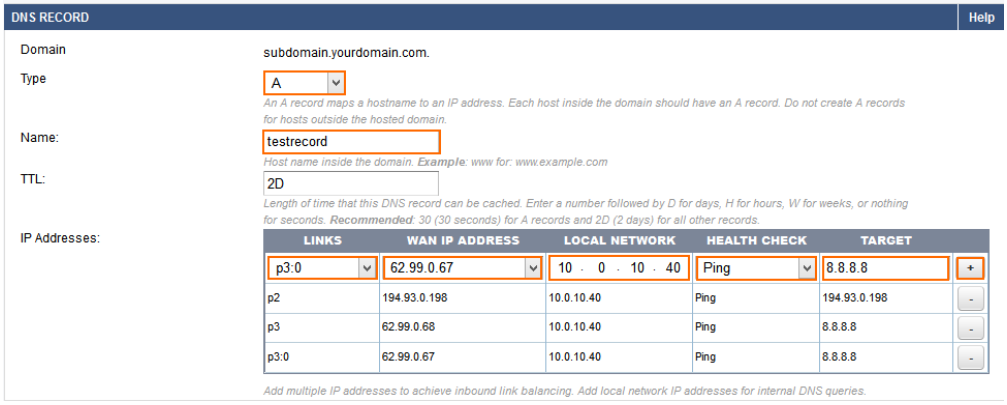
Record	Description
Start of Authority (SOA)	The SOA record defines the global settings for the hosted domain or zone. Only one SOA record is allowed per hosted domain or zone.
Name Server (NS)	NS records specify the authoritative name servers for this domain. One NS record for each name server in the **DNS Servers** table is generated.
Address (A)	A records map a hostname to an IP address. Each host inside the domain should be represented by an A record. One A record is created for each name server in the **DNS Servers** table. An A record is also created for each matching domain name found in 1:1 NAT and Port Forwarding rules.
Mail Exchanger (MX)	MX records point to the email servers that are responsible for handling email for a given domain. There should be an MX record for each email server, including any backup email servers. If an email server lies within the domain, it requires an A record for each name server. If the email server is outside the domain, specify the FQDN of the server, ending with a dot. Example: `mail.my-isp.net`
Text (TXT)	Text records allow text to be associated with a name. This can be used to specify Sender Policy Framework (SPF) or DomainKeys records for the domain.
Canonical Name (CNAME)	A CNAME record provides a mapping between this alias and the true, or canonical, hostname of the computer. It is commonly used to hide changes to the internal DNS structure. External users can use an unchanging alias while the internal names are updated. If the real server is outside the domain, specify the FQDN of the server, ending with a dot. Example: `server1.my-isp.net` If a domain name has a CNAME record associated with it, then it cannot have any other record types. Do not use CNAME defined hostnames in MX records.
Service (SRV)	Service records are used to store the location of newer protocols, such as SIP, LDAP, IMAP, and HTTP.
Pointer (PTR)	PTR records point to a canonical name. The most common use is to provide a way to associate a domain name with an IP address.
Other (OTHER)	Use an OTHER record to add a type of DNS record that is not supported, such as NAPTR.

5. Configure **IP Addresses** for the record (do this for all interfaces you want to use:
   - **LINKS** – Select the interface for which this response is valid. **ANY** is valid for all interfaces, **INTERNAL ONLY** only for requests coming from **Trusted Networks**.

- **WAN IP ADDRESS** – Enter the IP address which will be returned for DNS requests from the Internet.
- **LOCAL NETWORK** – Enter the IP address which will be returned for DNS requests from **Trusted Networks**.

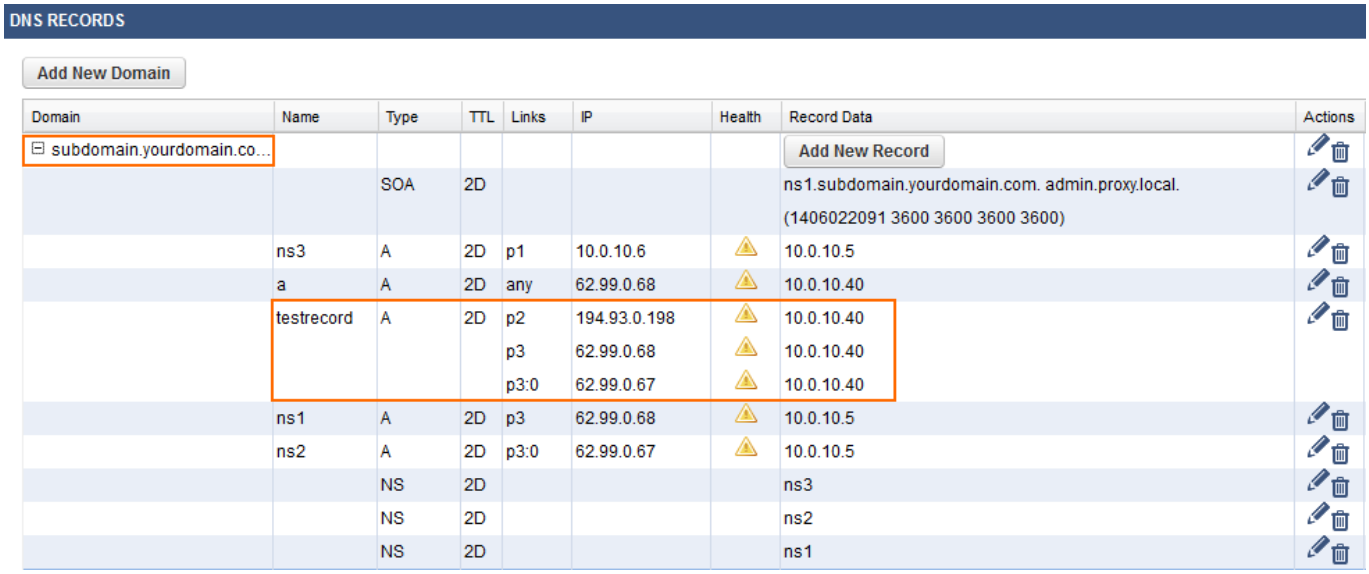
  If a **Internal Only** and a WAN interface IP address exist for the same record, the WAN IP ADDRESS and the Internal Only IP address will be returned when queried from the internal network. Always define a **Local Network** for WAN interfaces to avoid this behavior.
- **HEALTH CHECK** – Select the health check type: **Ping, DNS, Host:Port**. The **TARGET** will be checked by this method periodically to verify that the link is still up. When the health check fails this IP address is removed from the DNS response. Default Interval: 60 seconds.
- **TARGET** – The **IP address**, **DNS name**, or **Host:Port** target which will be checked periodically. Use a health check target that is behind the interface chosen as the **LINK**. Default interval: 120 seconds

6. Click **+**



7. Repeat 5. and 6. for the other interfaces if necessary.
8. Click **Save**.

The DNS records are now listed in the **DNS RECORDS** section. Refresh the page until the health check checks for all records turn green.



Step 6. Test your DNS records

From a host on the Internet, run.

```
nslookup - [YOUR WAN IP WITH DNS SERVER ENABLED]
```

Enter the domain names and verify that the WAN IP address for the interface or ANY IP Address is returned.

Repeat with a host in your local network

```
nslookup - [LOCAL IP OF YOUR BARRACUDA FIREWALL WITH DNS SERVER ENABLED]
```

Enter the domain names and verify that the LOCAL NETWORKS IP for the interface or ANY IP Address is returned.

When not using the X-Series Firewall DNS directly, it might take some time for your changes to be distributed throughout the Internet. A new domain name might take up to a day until it is accessible via other DNS servers. If the DNS record is modified, any server on the Internet that has the old DNS records will not request an update until the TTL of the original record has expired.

Expert Settings

To change expert settings for the ADNS service append the following string to the URL: `&expert=1`

- **Health Check interval** – Time interval in seconds between health checks.
- **Update Dynamic Interface IP every** – Interval in seconds for checks of IP changes to dynamic interfaces

Figures

1. ADNS01.png
2. ADNS_FWRule_01.png
3. ADNS02_1.png
4. ADNS06.png
5. ADNS05.png
6. ADNS03.png
7. ADNS04.png
8. enable_expert_mode_00.png