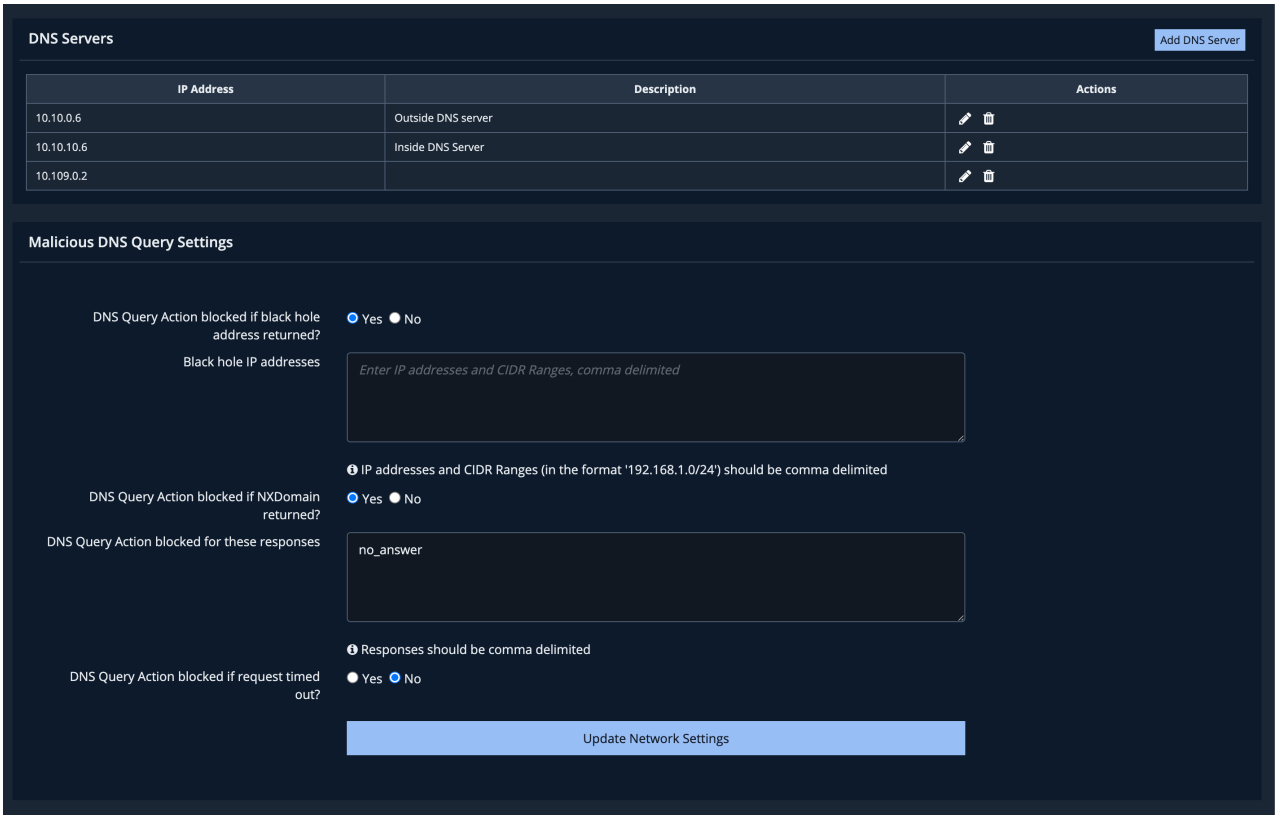
CONFIGURING DNS SETTINGS

The DNS Servers page is where you provide Security Validation with your DNS servers and configure your DNS Rules.

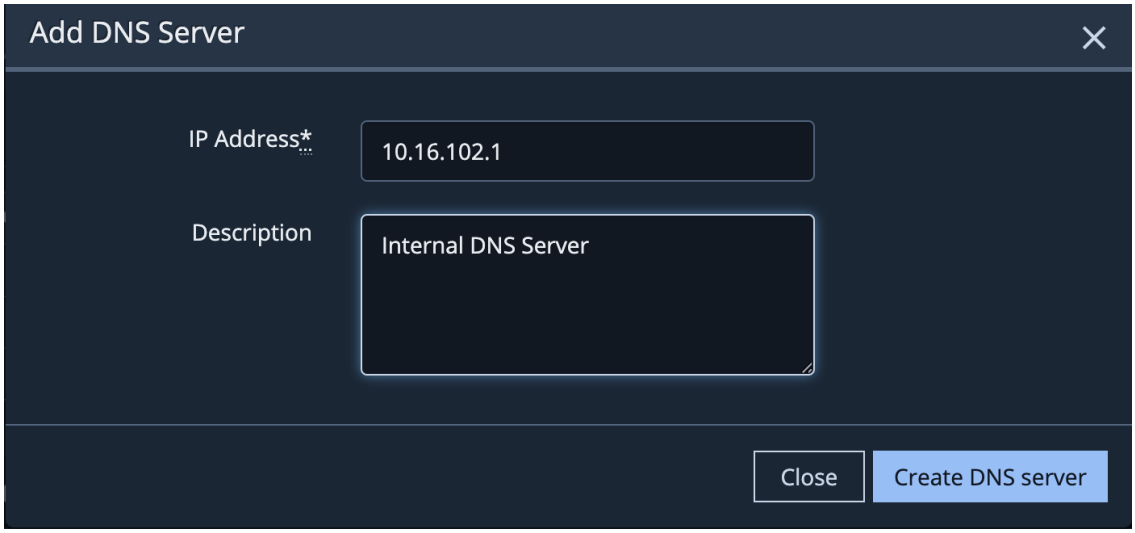


DNS Servers page

To add a new DNS Server

NOTE: The list of servers is automatically updated when Actors are registered, but you can also add DNS Servers.

1. Launch the Director.
2. Go to **Settings > Director Settings**.
3. Select **DNS Servers**.
4. Click **Add DNS Server**.
5. Enter the DNS server's *IP address*.
6. Enter *a description*, if desired.



Add DNS form

7. Click **Create DNS server**; the DNS Server will be added to the table.

To add a Malicious DNS Query Settings

IMPORTANT: This must be set up for Security Validation to know if a Malicious DNS Query Job Action is blocked.

1. Go to **Settings > Director Settings**. The Systems Settings page opens.
2. Select **DNS Servers**.
3. Define if the Action should be blocked if a blackhole address returned where **Yes** means the Director will consider the Action was blocked when the response matches an address in the Blackhole IP addresses field.
4. Enter the **Blackhole IP addresses or CIDR blocks** that you are defining. This is a comma-delimited list of individual IP addresses or CIDR Ranges.
5. Define if the Action should be blocked if the NXDomain returned where **Yes** means the Director will consider the Action was blocked when the response is the NXDOMAIN.
6. Enter **responses** in the DNS query Action blocked for these responses field if your DNS servers return a response other than NXDOMAIN when blocking domain lookups. This will be a comma-delimited list of responses.
7. Define if the DNS Query Action should be blocked if the request timed out by selecting **Yes** or **No**. This allows you to mark DNS timeouts as a blocked event, to align your job results with the response from your network technology providing a timeout value.
8. Click **Update Network Settings**.