Securing Networks with

Cisco FTD

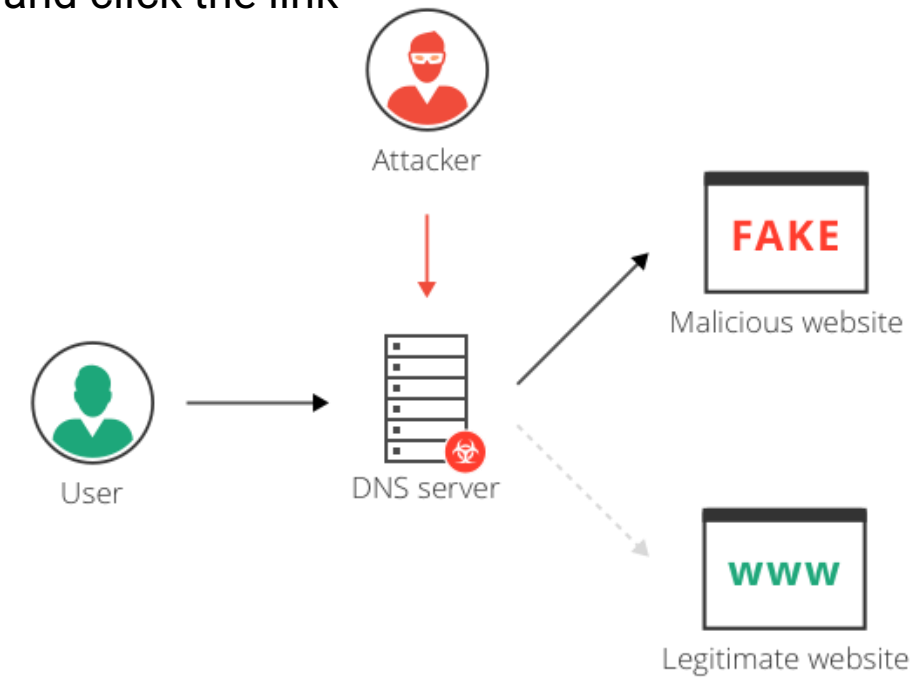
Chapter 11

Domain Name System (DNS) Policy

Mohsen Kheradmand

DNS

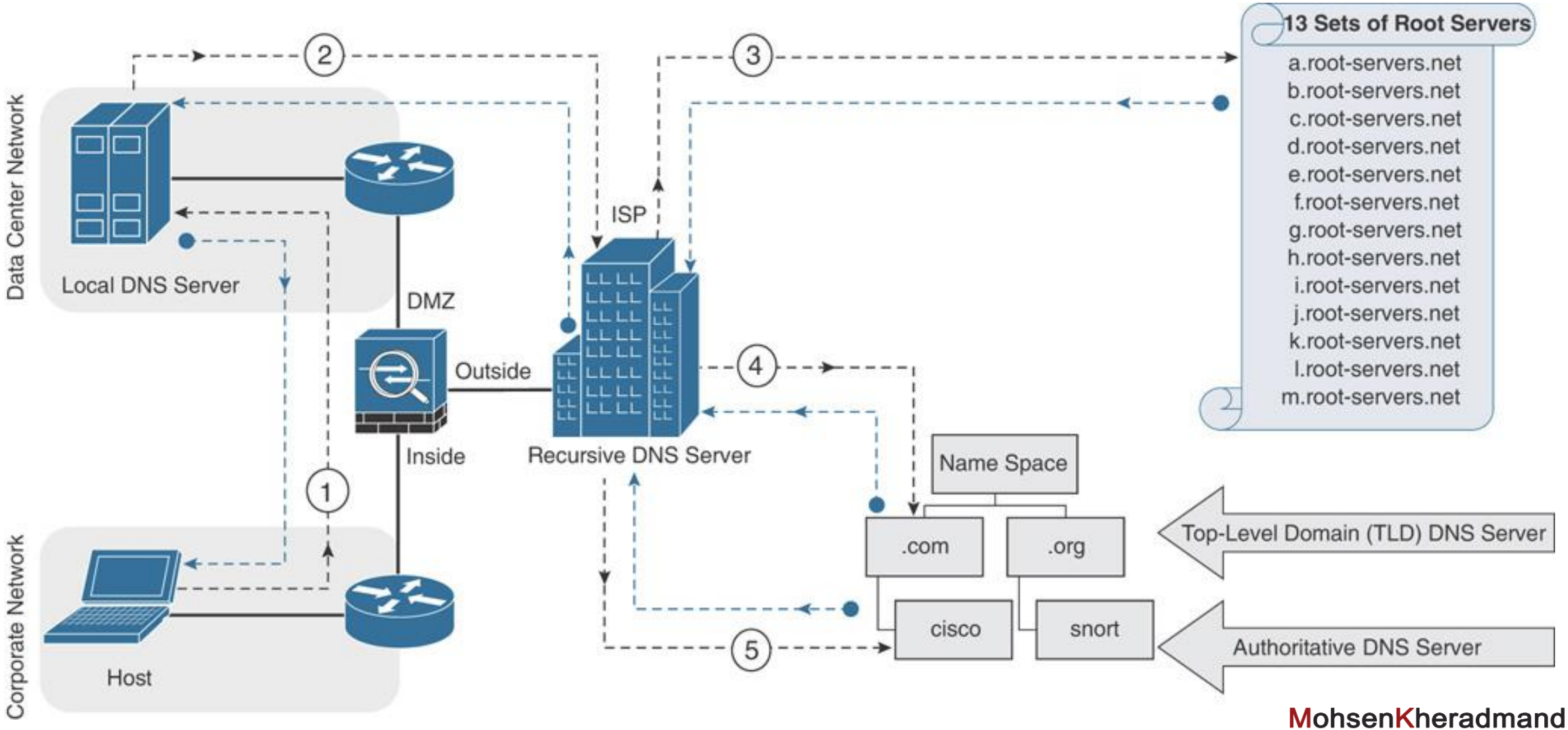
- Attackers often send phishing emails with links to malicious websites.
- A user in your network may be deceived and click the link



- A threat defense can protect DNS queries from phishing
- A DNS policy allows you to block connections based on domain name, using a Block list

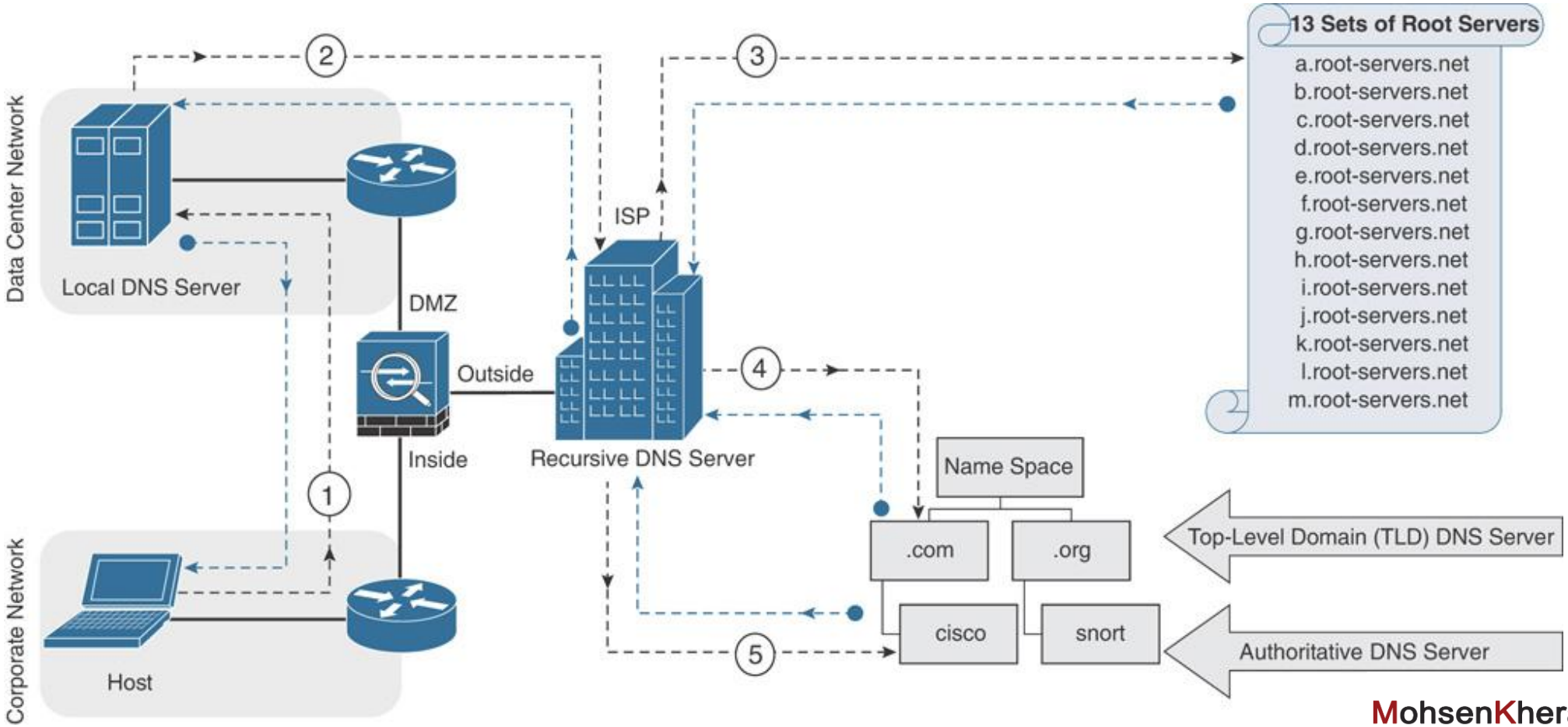
DNS Queries

Let's see how DNS queries resolves



DNS Queries

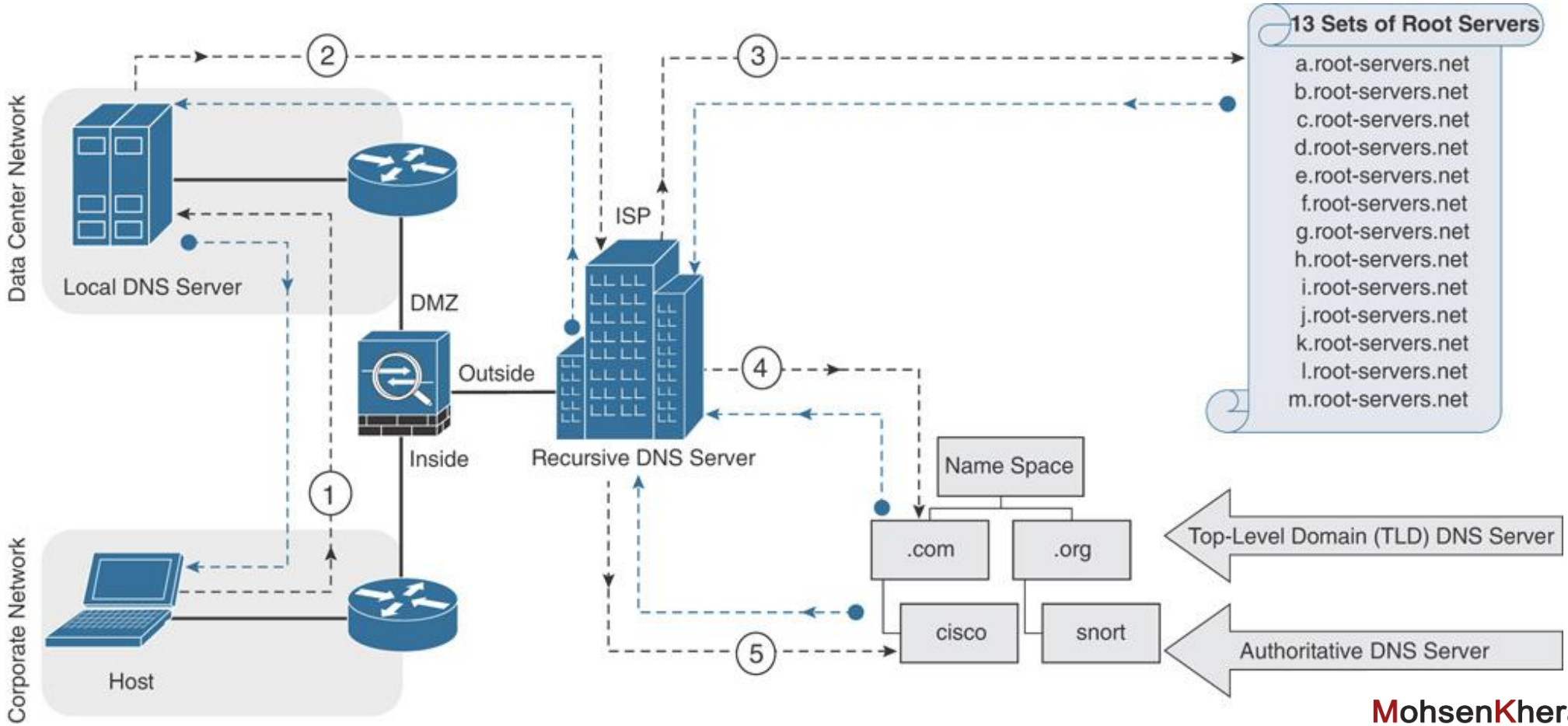
1) The browser sends a query to the local DNS server in your network



DNS Queries

2) If there is no local DNS server or no information is found , the query is sent to recursive DNS server of your ISP

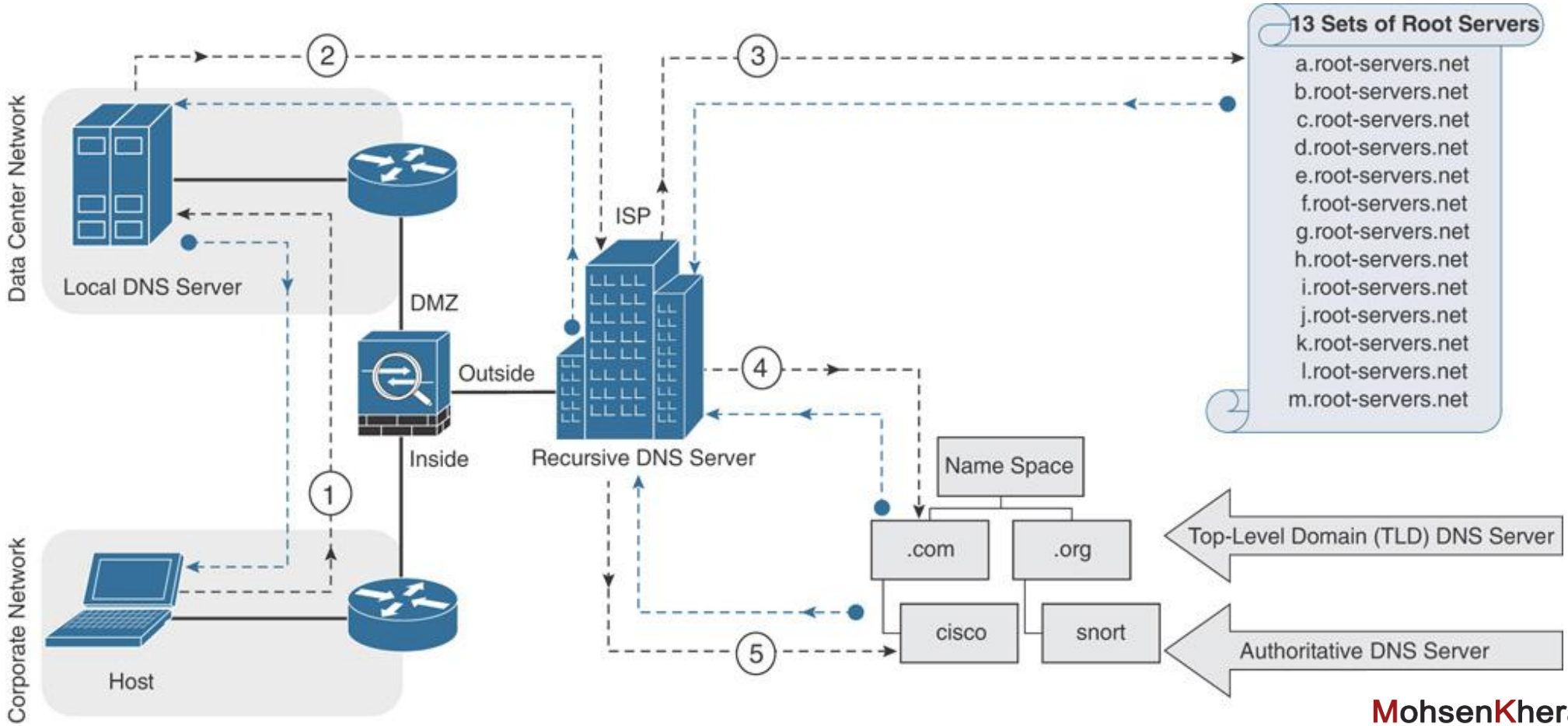
✓ If recursive server has information about that query in its cache , it response and no additional queries are performed



DNS Queries

3) if the recursive server could not help , the query is sent to one of the 13 sets of root name servers

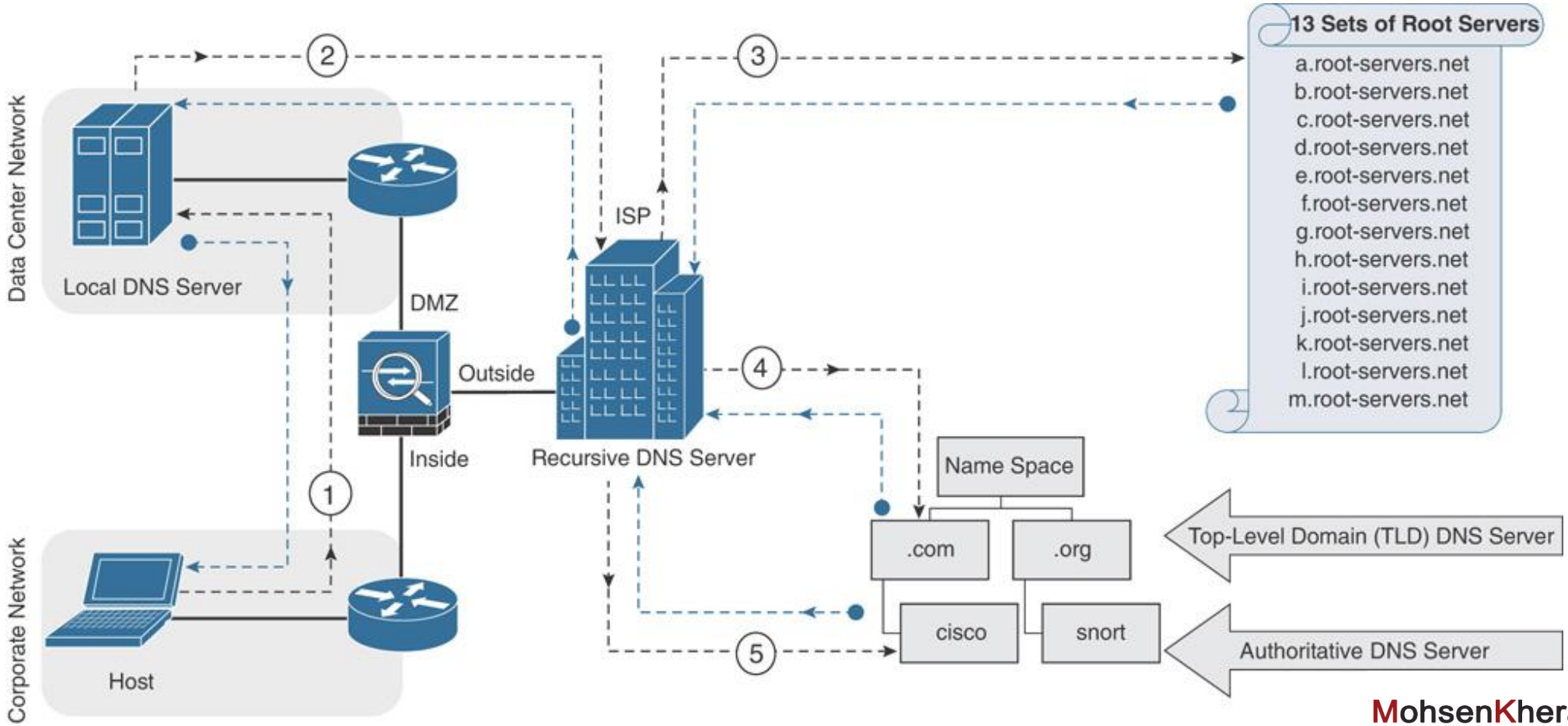
✓ A root server knows the DNS information about a top-level domain (TLD).



DNS Queries

4) The TLD server sends information about the second-level domain and its authoritative name server.

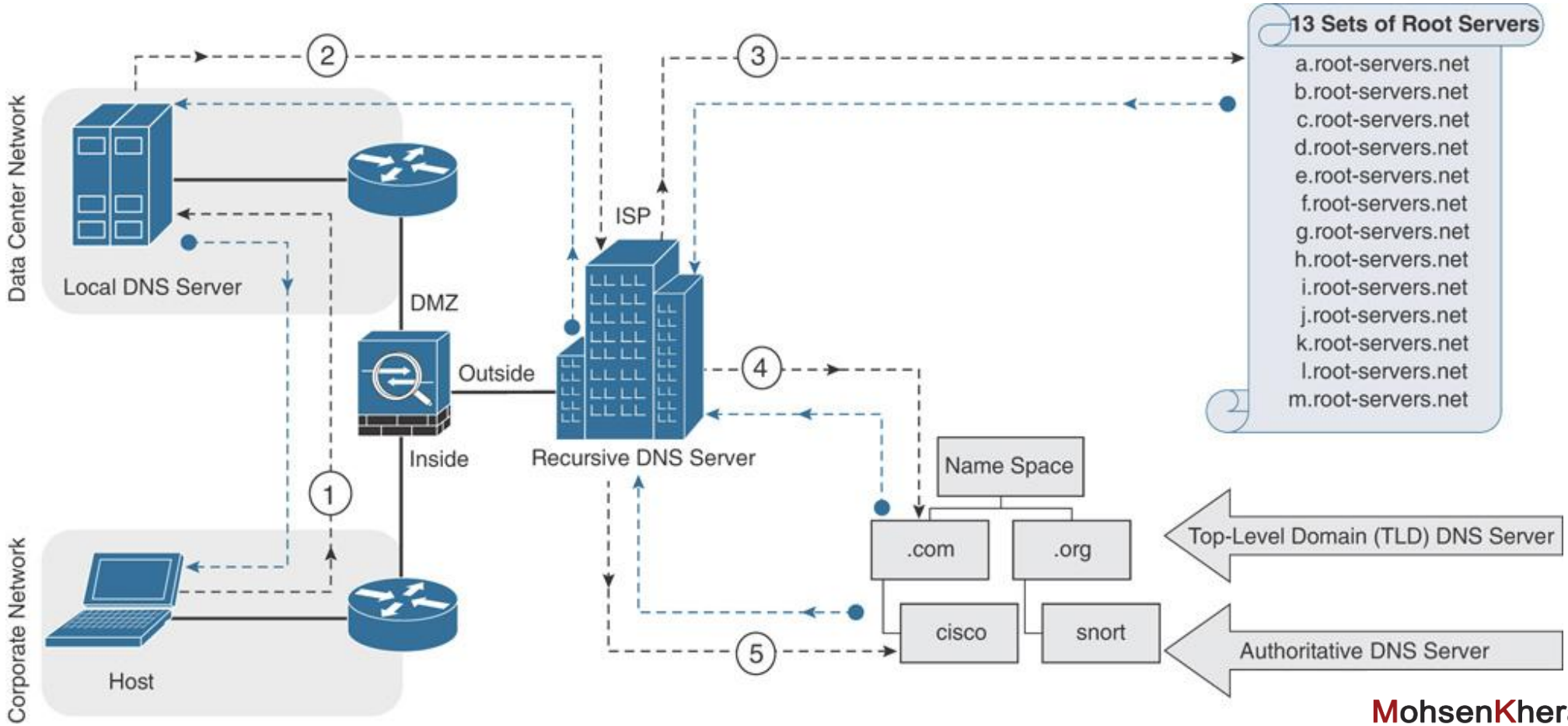
✓ An authoritative name server knows all the addressing information for a particular domain



DNS Queries

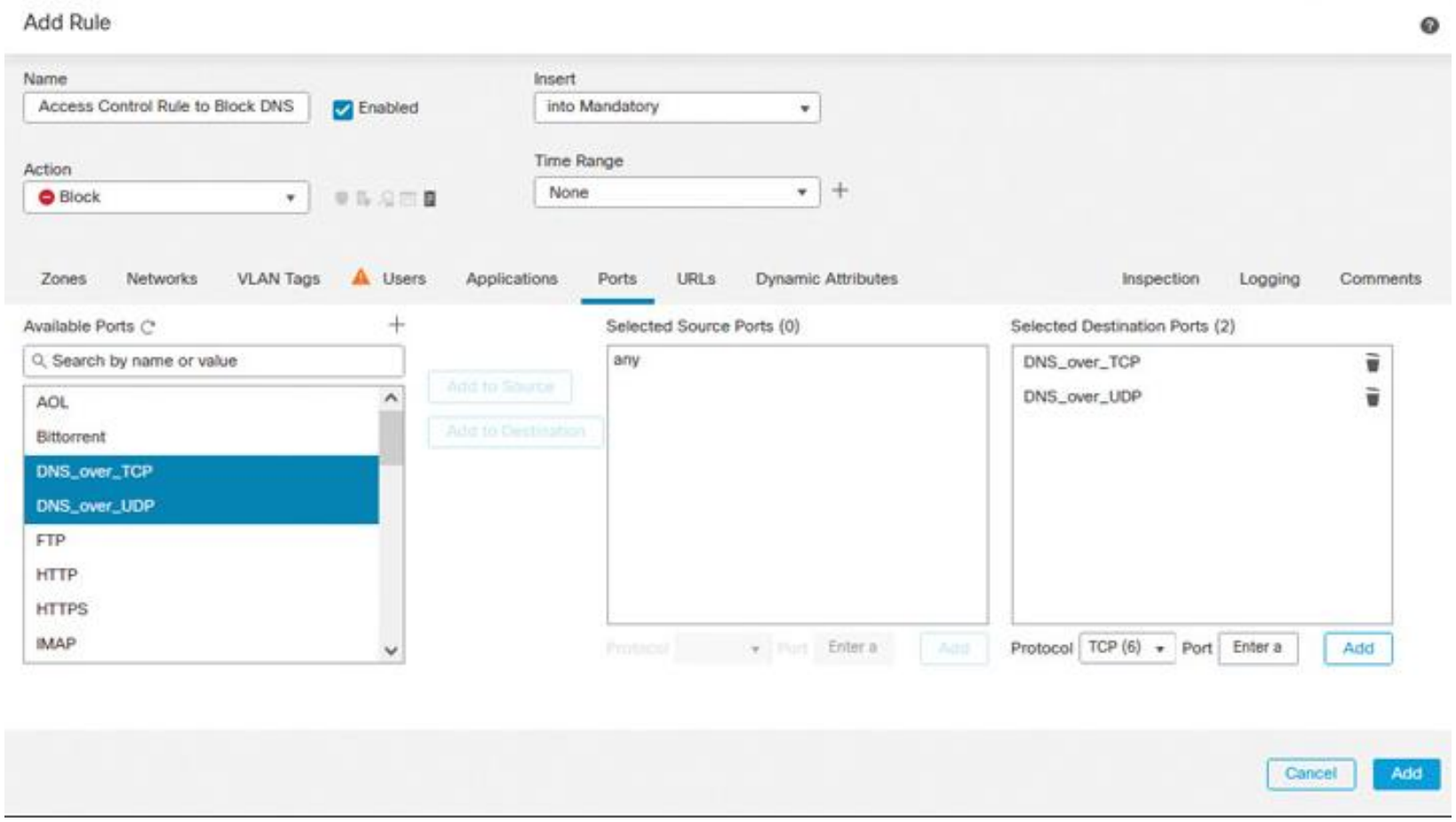
5) The authoritative name server responds to a query to your ISP.

✓ The ISP's recursive server stores the record on its cache and sends the IP address to your browser.



Blocking of a DNS Query Using a Secure Firewall

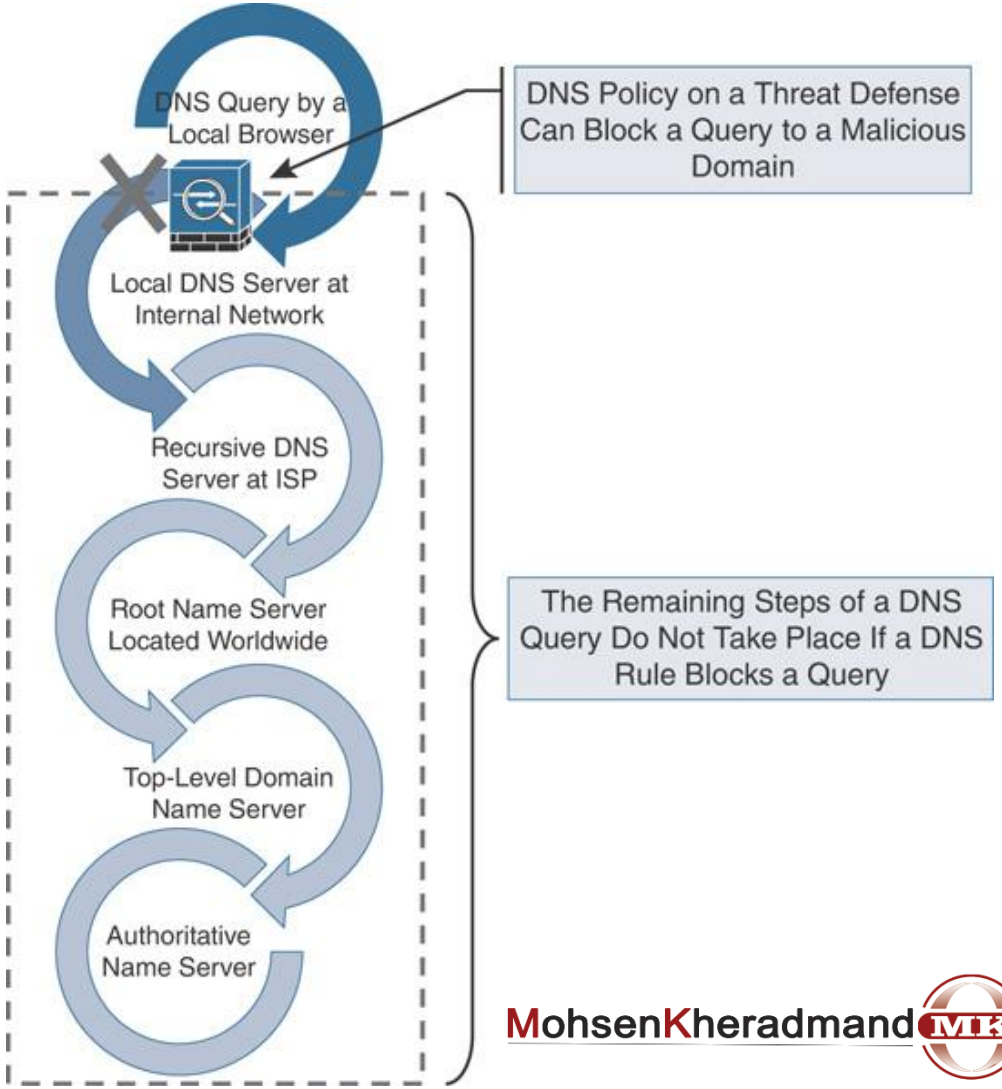
- 1st way is to block DNS traffic using Access Control Policy
  - However , access control rule can not identify any harmful domain based on the web contents



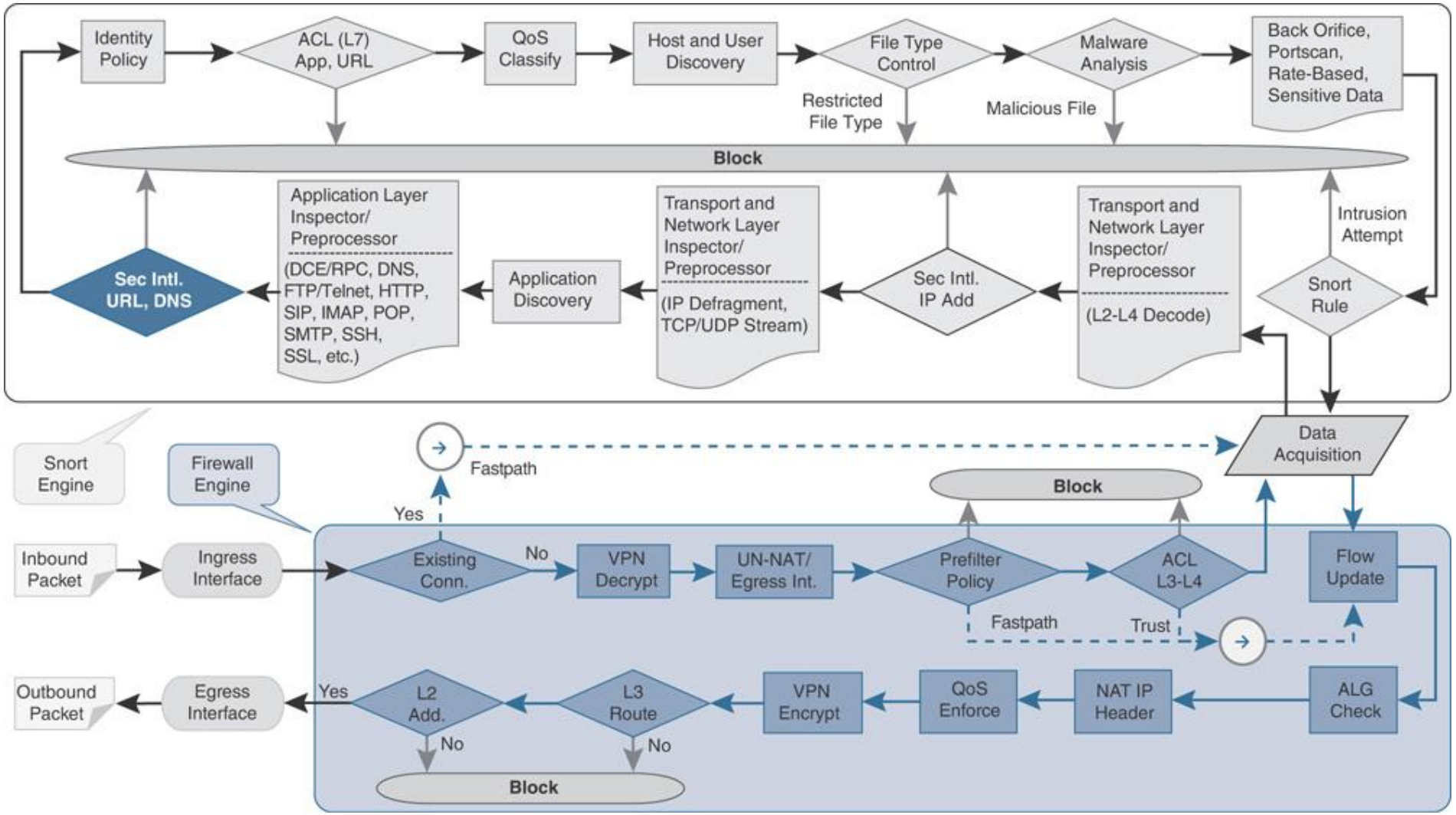
Blocking of a DNS Query Using a Secure Firewall

✓ The **DNS-based Security Intelligence** can identify a susceptible DNS query and block them

- while any queries to legitimate websites are allowed
- The FTD blocks the request for a website before a HTTP connection
- So there is no need to HTTP inspection



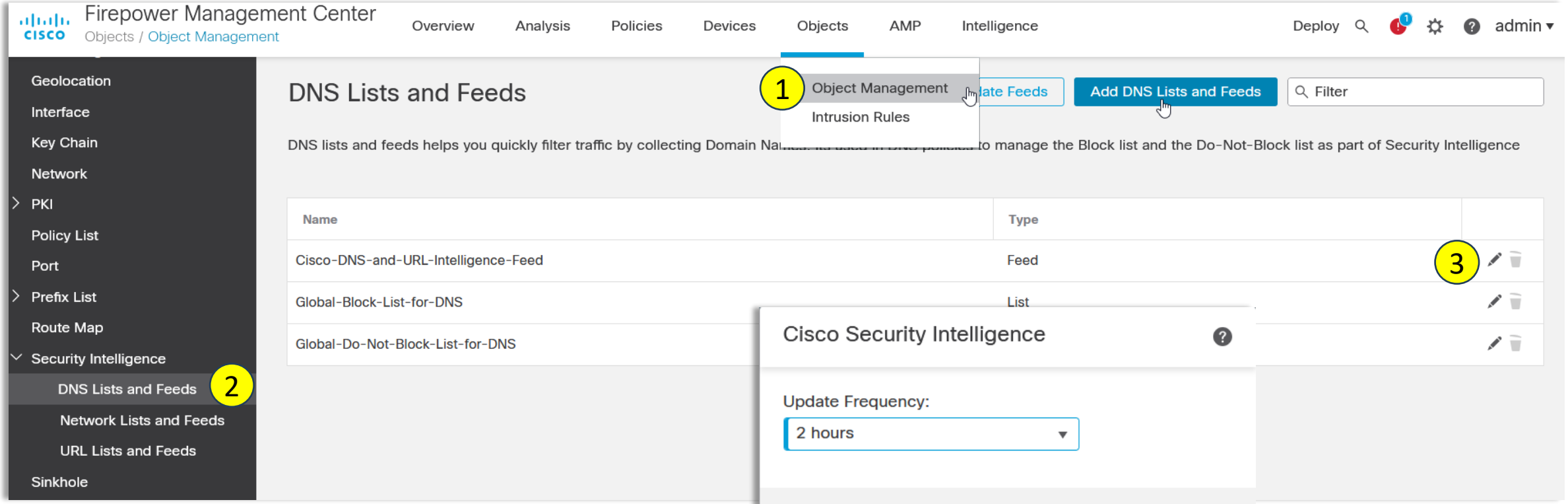
Blocking of a DNS Query Using a Secure Firewall



Sources of Intelligence

1) Feed

- You can update DNS Feeds or Add 3rd party DNS Feed or custom list
- Periodically communicates with the Cisco cloud (or 3rd party cloud) to download the latest feed
- FMC downloads the updates and automatically sends Feed to the FTDs (no need to manual deploy)

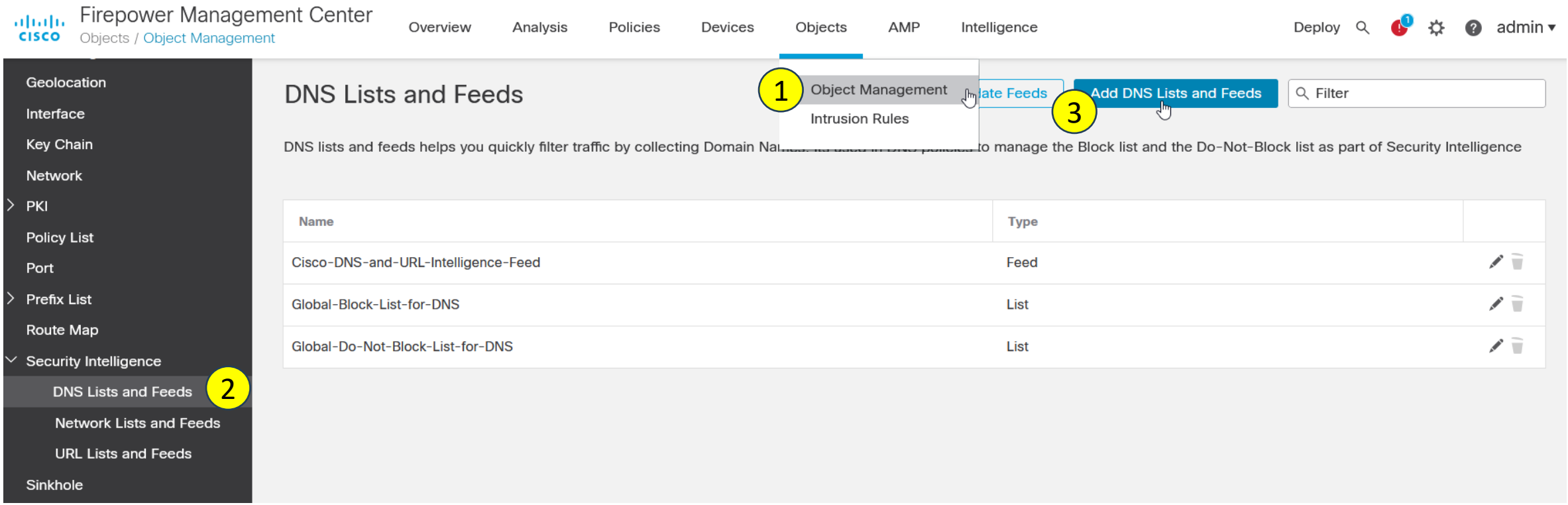


1. Object > Object Management
2. Security Intelligence > DNS List and Feeds
3. Cisco-DNS-and_URL-Intelligence-Fees > click pencil to edit

Sources of Intelligence

2) List / 3rd party Fees

- You can list the domains in a text file (.txt format) and upload the file manually to the management center
- And you can update DNS Feeds by adding 3rd party DNS Feed



1. Object > Object Management
2. Security Intelligence > DNS List and Feeds
3. Add DNS List and Feeds

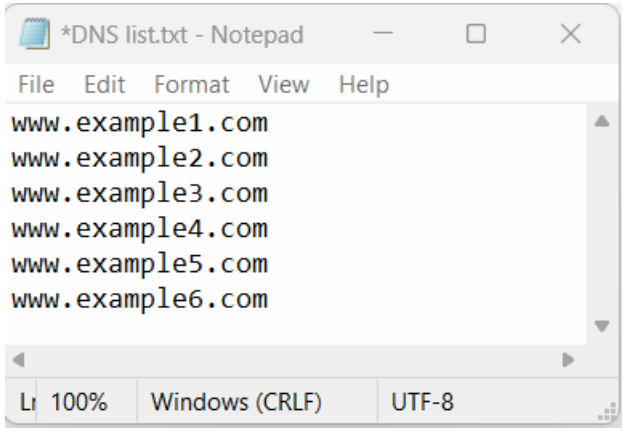
Sources of Intelligence

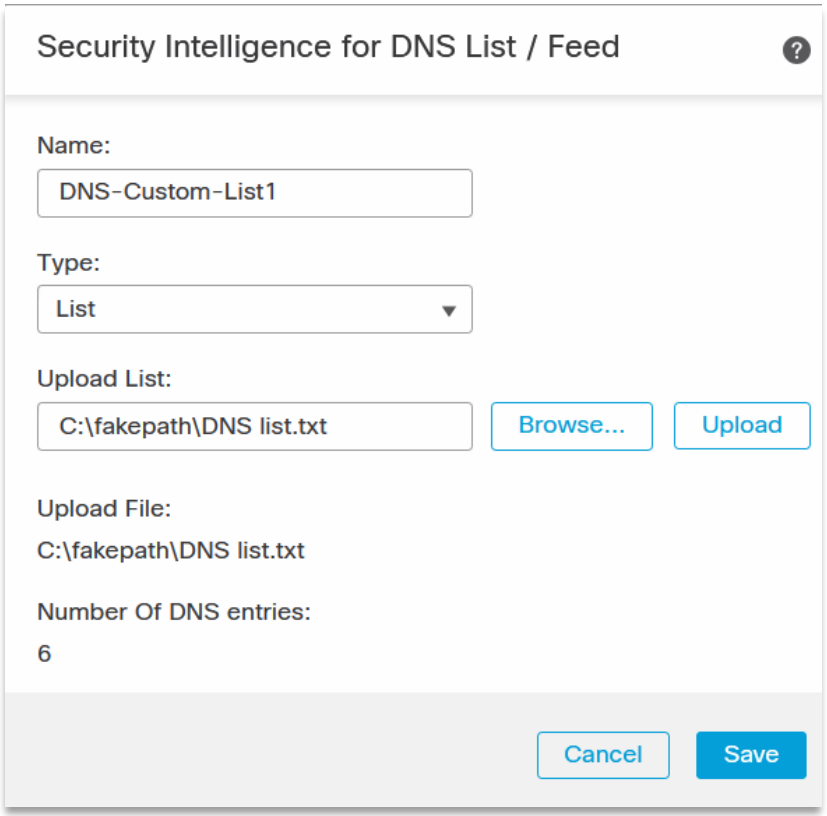
2) List / 3rd party Fees

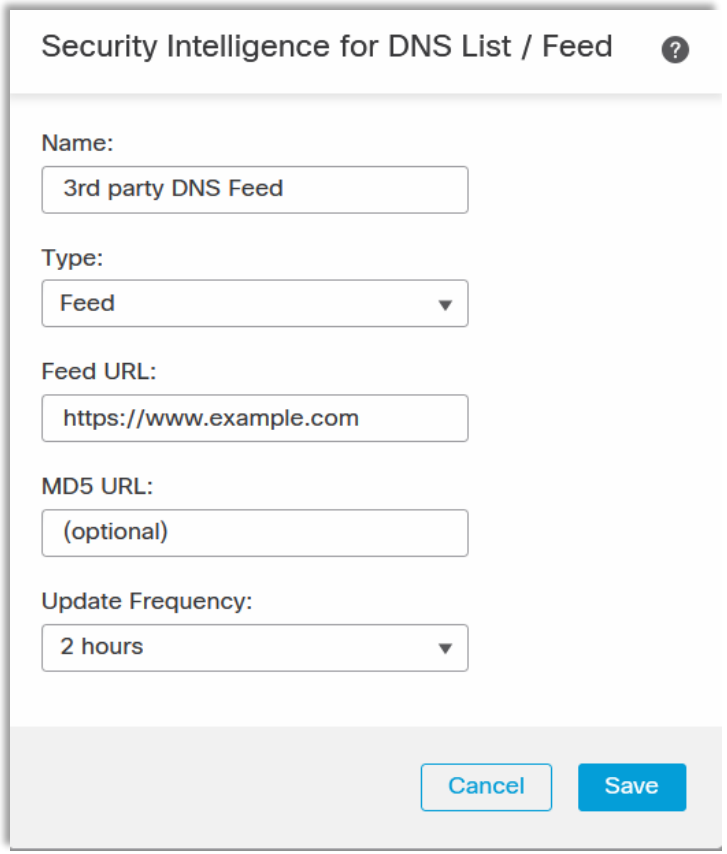
Type of DNS list

>> Feed : to obtain Feed from 3rd party

>> List : to upload a list of DNS Queries



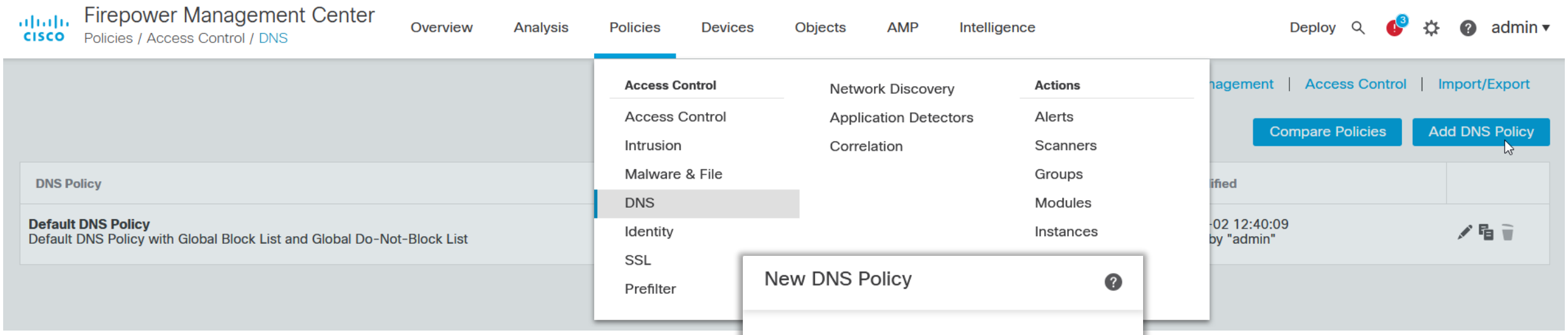


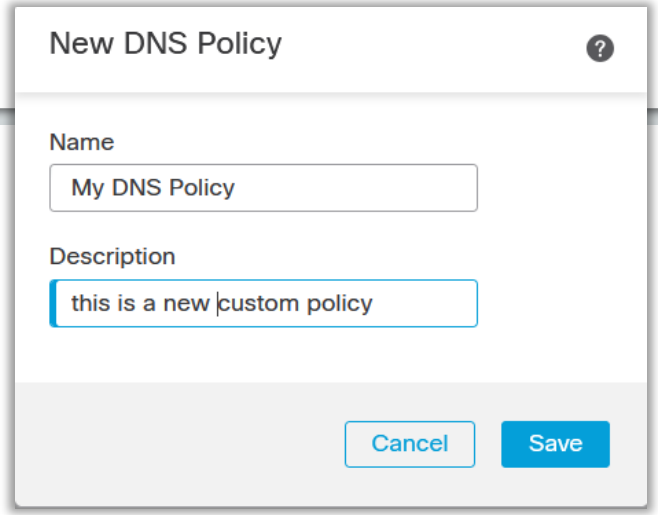


DNS Policy configuration

Step 2 : create a DNS Policy

1) Policies > Access Control > DNS
2) Click Add DNS Policy (or you can edit Default DNS Policy)



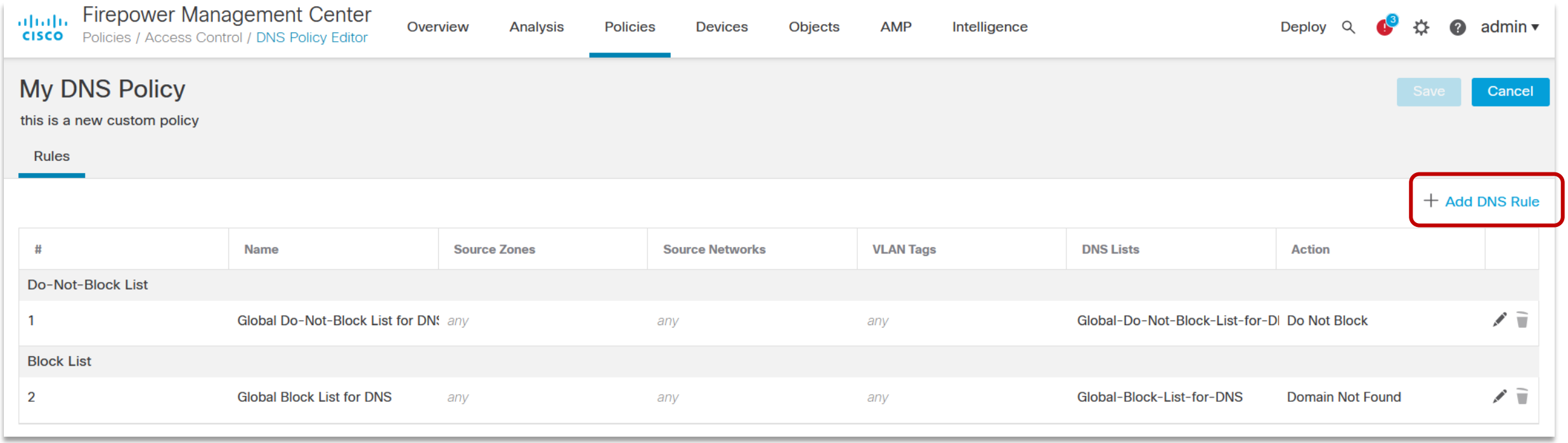


- Enter a name for new Policy
- Optional : enter a description
- Click Save

MohsenKheradmand MK

DNS Policy configuration

3) Click Add DNS Rule



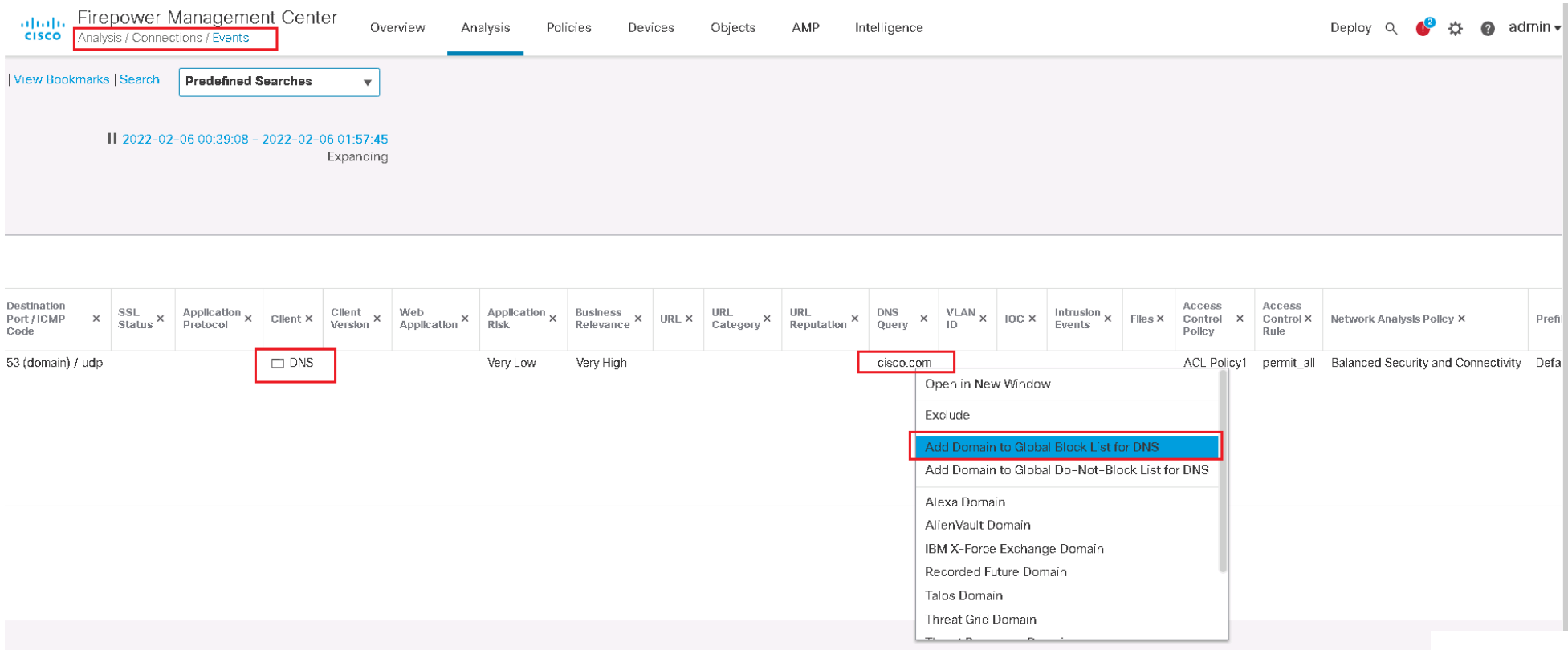
- There is 2 default rule (Global Block and Do-Not-Block list) that can be updated but not edited

DNS Policy configuration

- To add any DNS query to Global lists:

  - Navigate to an **event** that includes an IP address, domain, or URL

  - Right-click the IP address, domain, or URL and select Add to Global Block-list or Do-Not-Block-List

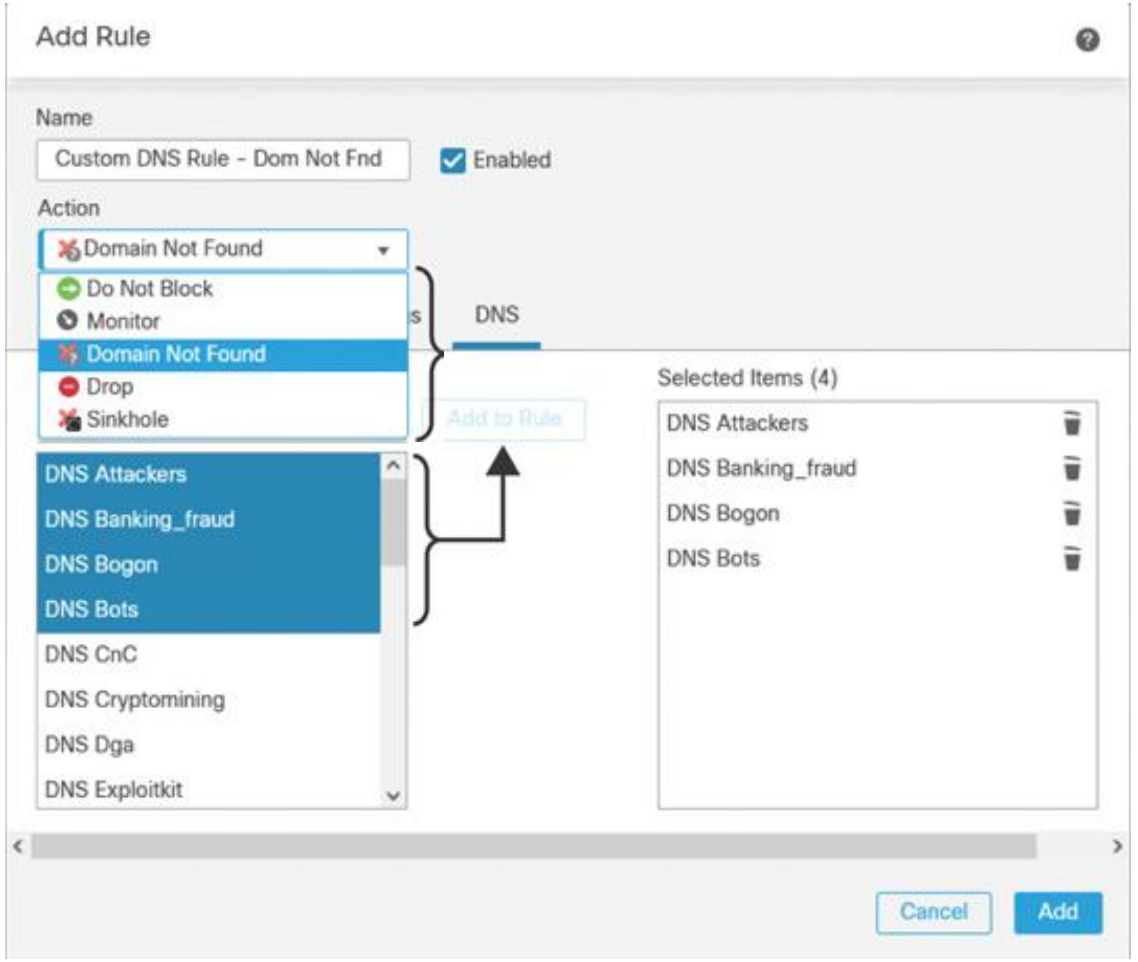


DNS Policy configuration

4) Rule configuration

- **Name** : enter a name for new rule
- **Action** : action against a particular DNS query
  - Do not Block : allows DNS queries for a particular domain to be resolved but there is more inspection
  - Monitor : just monitor the DNS queries for particular domain (generates an alert for that traffic)
  - Domain Not Found: drop the query and user receives an NXDOMAIN , (domain name does not exist)
  - Drop : drops the DNS query for a particular domain , no further inspection (no response message)
  - Sinkhole : the FTD responds to a DNS query with a false IP address (redirect malicious traffic to an alternate location)

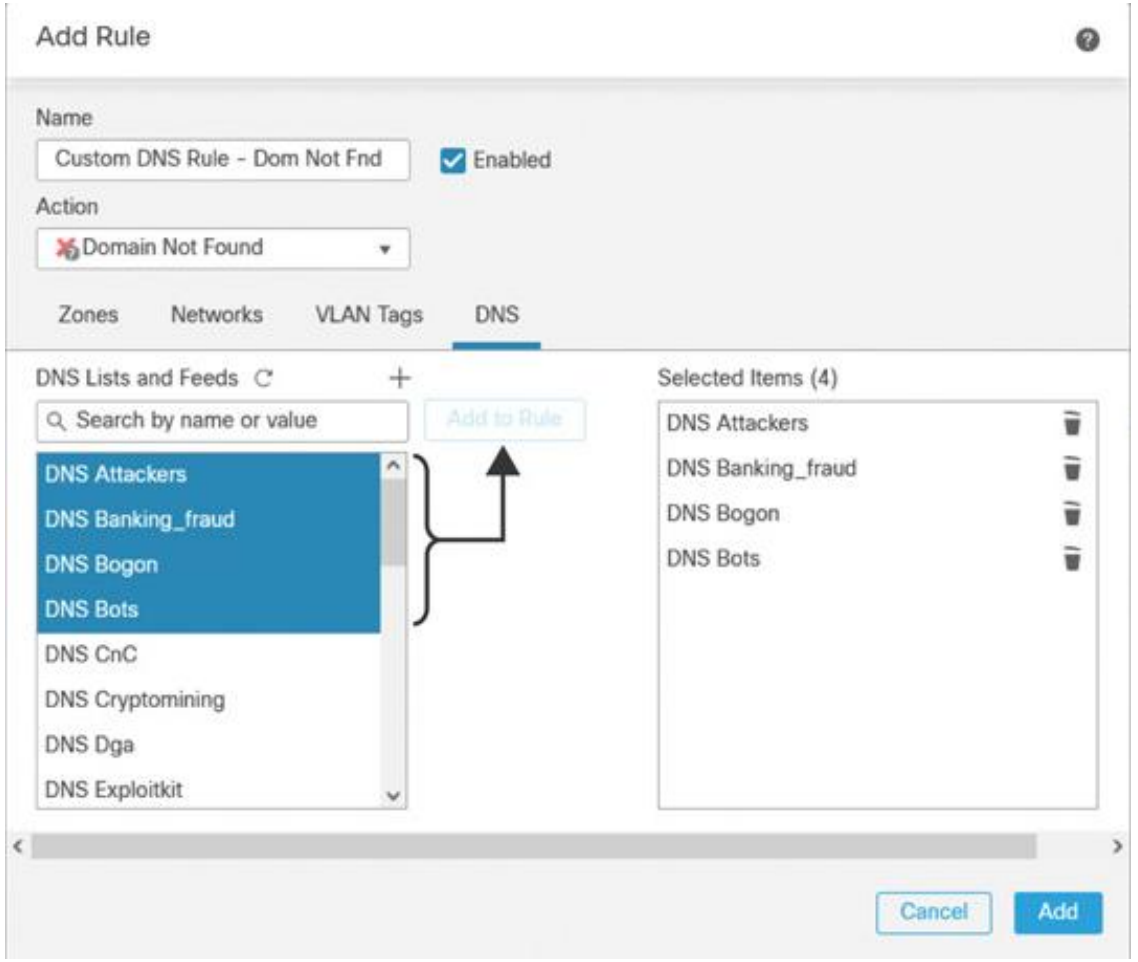
✓ With IP address and URL, the only option is to block the malicious, but by sinkhole you can return a spoofed IP



DNS Policy configuration

4) Rule configuration

- **Name** : enter a name for new rule
- **Action** : action against a particular DNS query
- **DNS :** add desired DNS lists to selected item to take action
- Optionally you can select source Zone , Source network and Source VLAN traffic toward the selected DNS query
- Click the Add button to save the rule and exit the editor



- Do not attempt to Deploy the DNS policy,

  Invoke the DNS Policy into Access Control Rule

Note1 : DNS list and Feeds can be added by objects

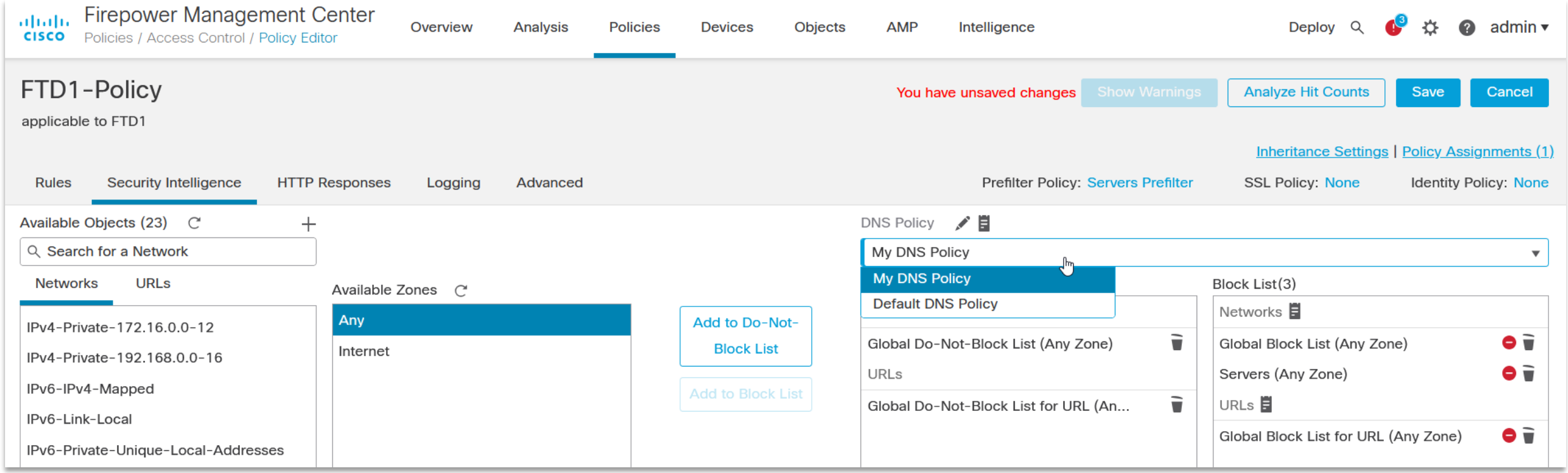
Note2 : For each type of rule action, you need to create a separate DNS rule

DNS Policy configuration

5) Invoke the DNS Policy

Policies > Access Control > Access Control

Edit the desired policy > select Security Intelligence tab > DNS Policy section> select your policy which is created before



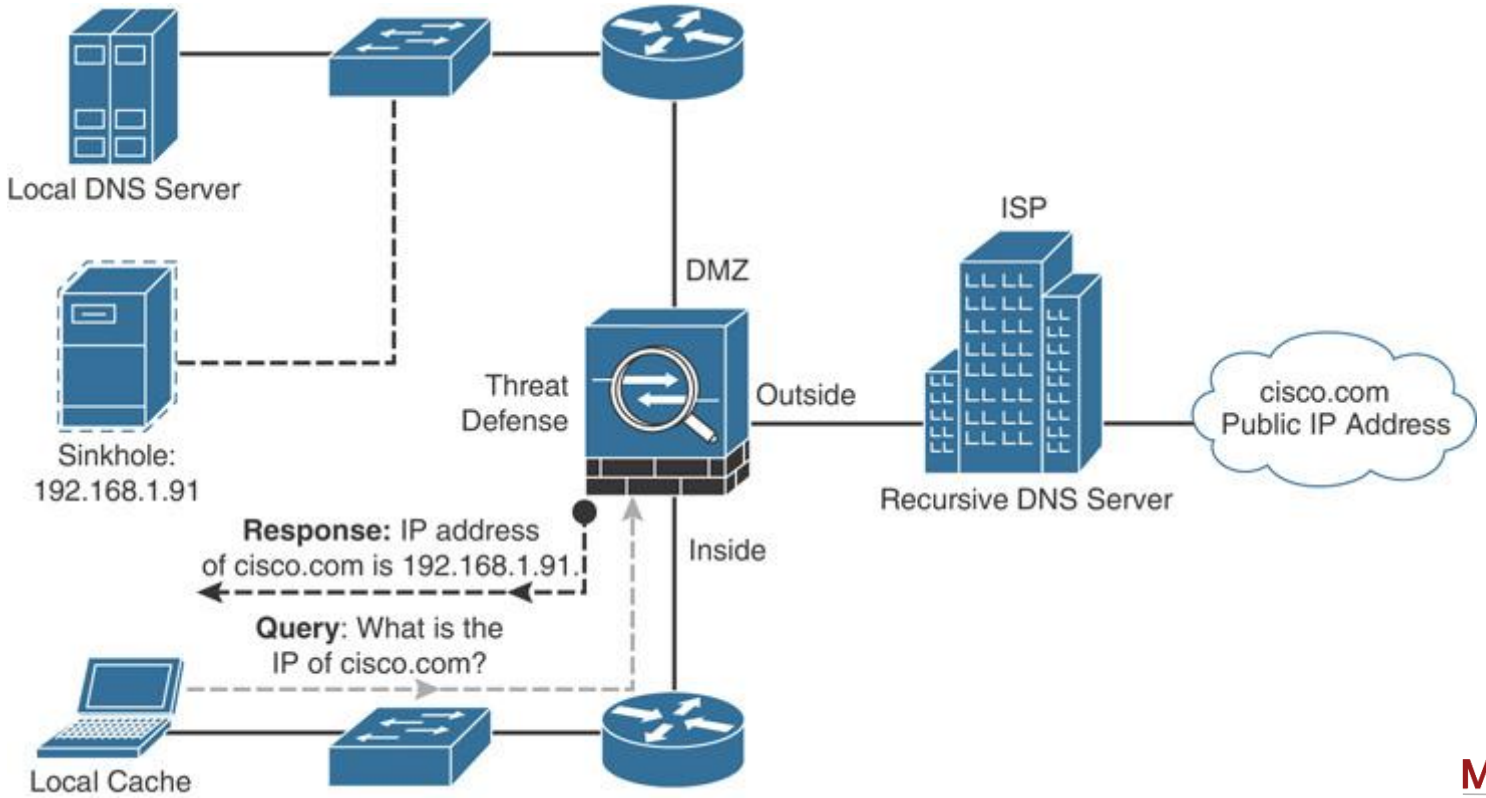
- Click Save
- Deploy the Policy

DNS Policy configuration

Configure the Sinkhole

- Spoofed DNS server :

  The threat defense uses the IP address of this spoofed DNS server as a response to a harmfull DNS query



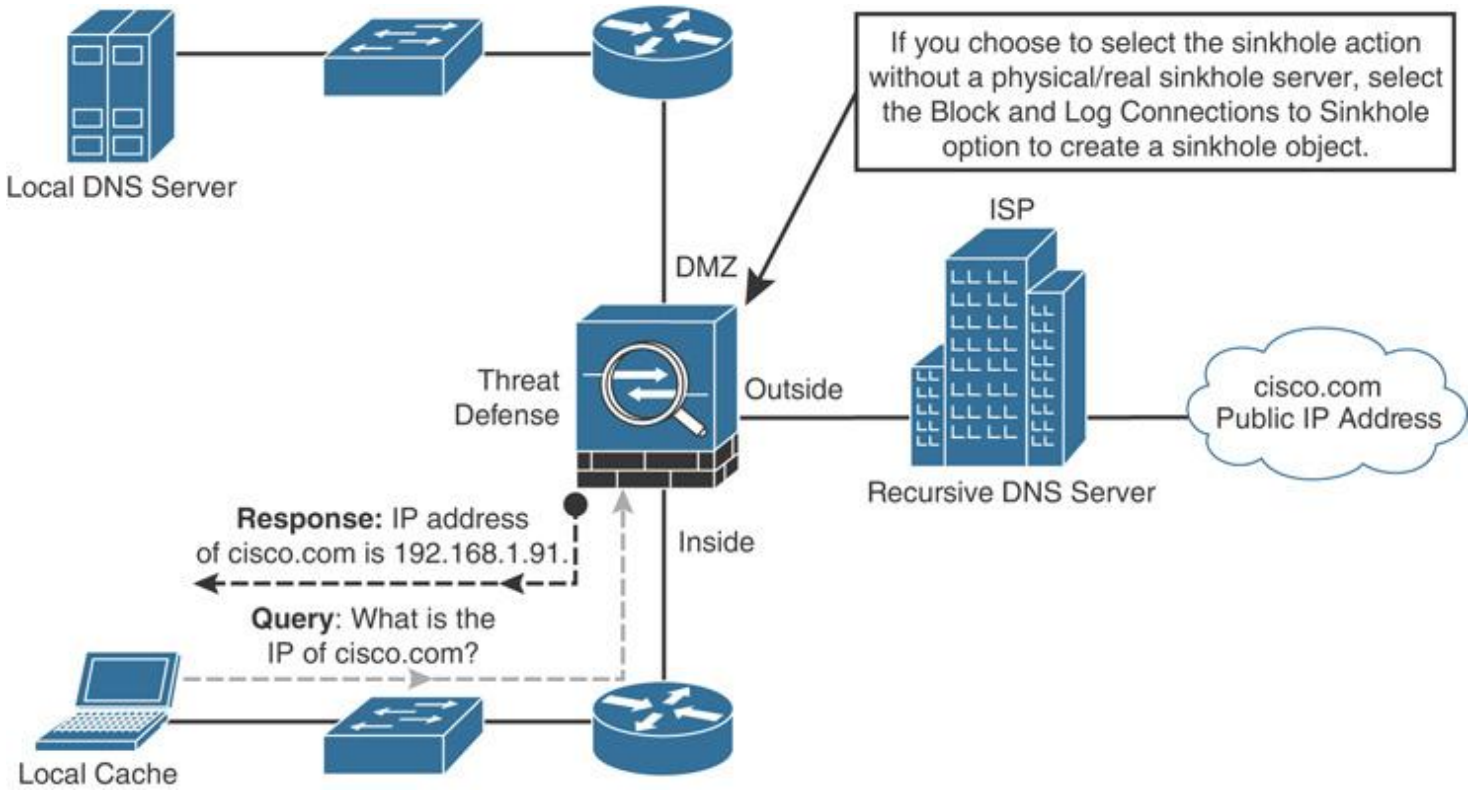
DNS Policy configuration

Configure the Sinkhole

- A sinkhole without a physical spoofed server:

  You can assign any false IP address within a sinkhole object

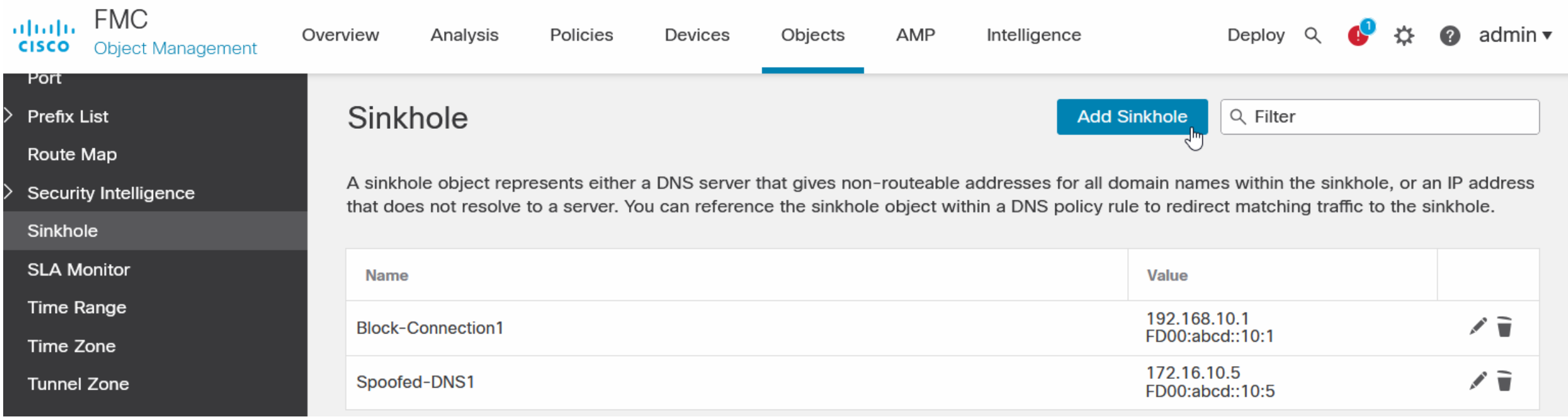
  - If a not-valid sinkhole IP address is returned, then end user attempts to access the sinkhole IP address.



DNS Policy configuration

Configure the Sinkhole

- Spoofed DNS server :
- Click Object > Sinkhole > Add Sinkhole



DNS Policy configuration

Configure the Sinkhole

- **Name :**

  Enter a name for Sinkhole object

- **IP Policy :**

  Enter IPv4 and IPv6 address that will be returned in respond to DNS queries

- **Log Connection to Sinkhole :**

  Log all the connections between the endpoint and sinkhole server

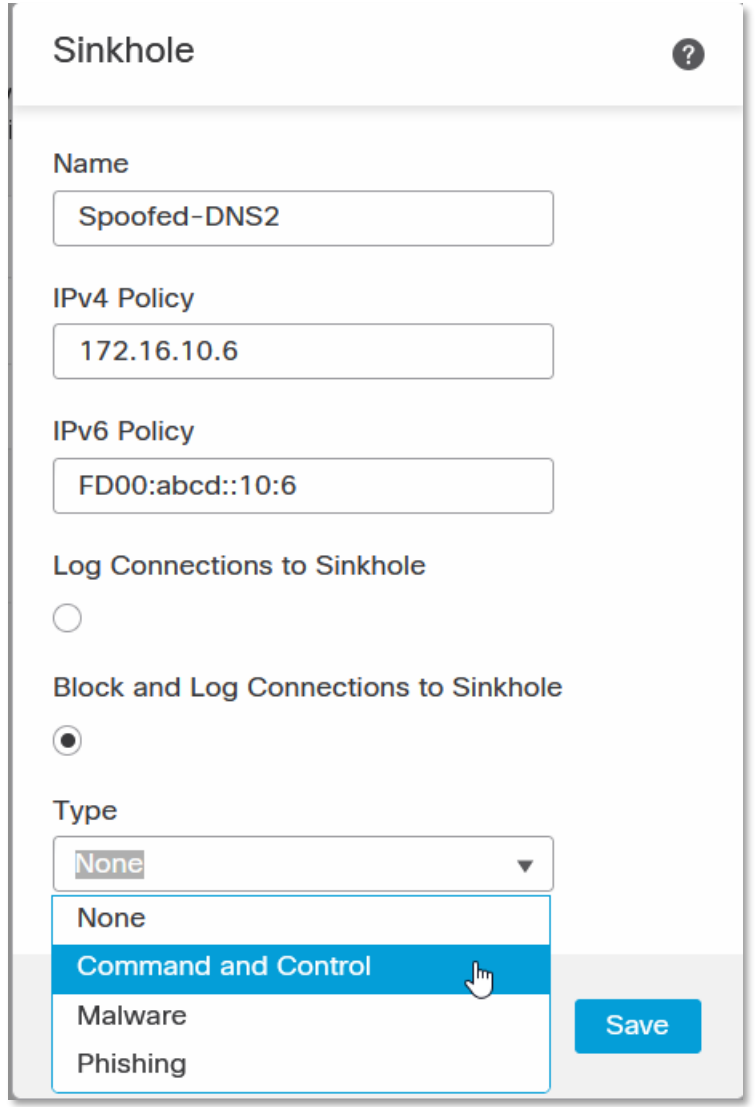
- **Block and Log Connection to Sinkhole :**

  Block the connection and only log at the start of flow connection

  If there is no physical Sinkhole server , return this IP address to clients

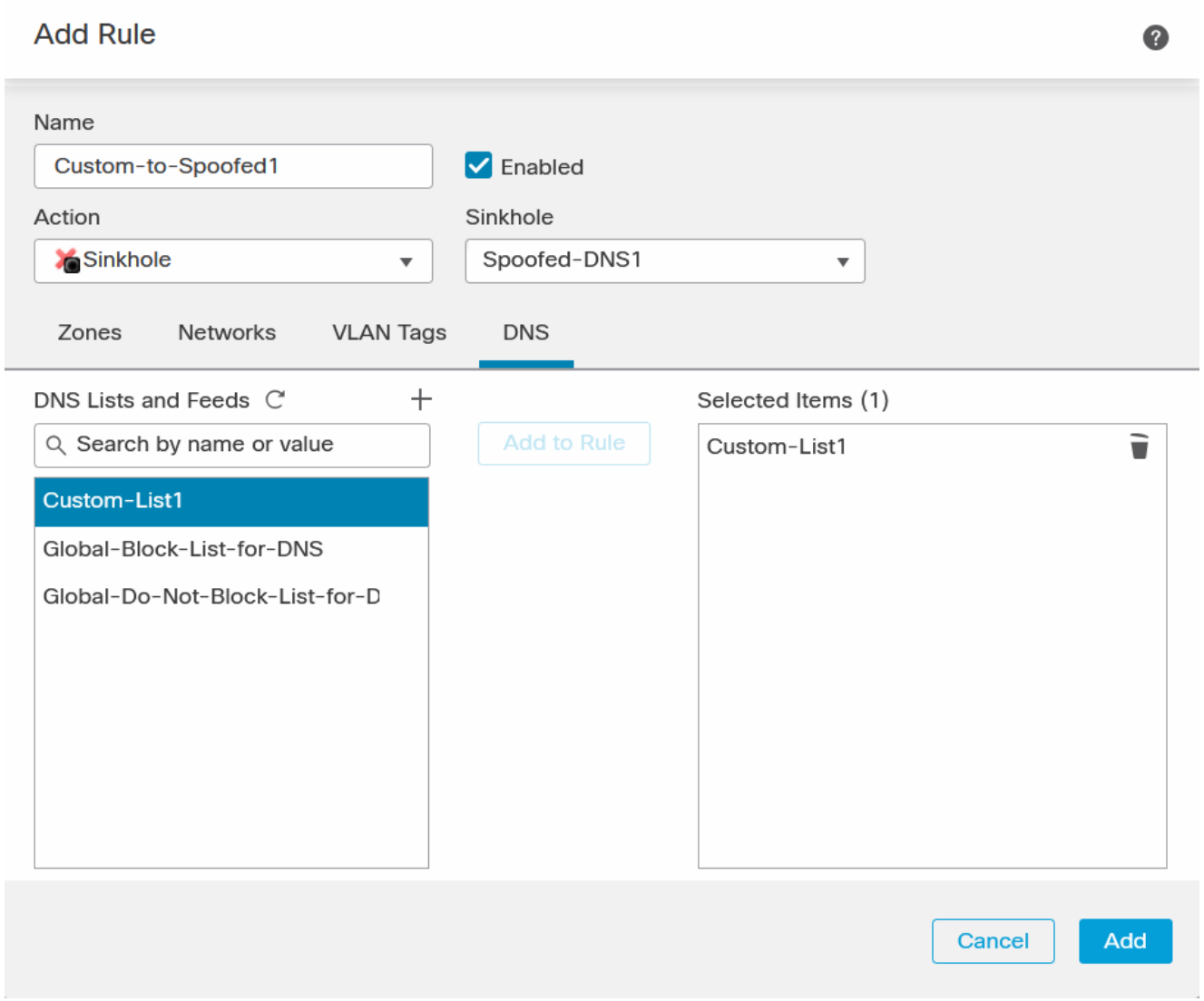
- **Type :**

  The type of IOC (Indication of Compromise) associated with sinkhole event



DNS Policy configuration

- Now you can use configured object to create a rule



Verification

> Analysis

> Connections

> Security Intelligence Events