

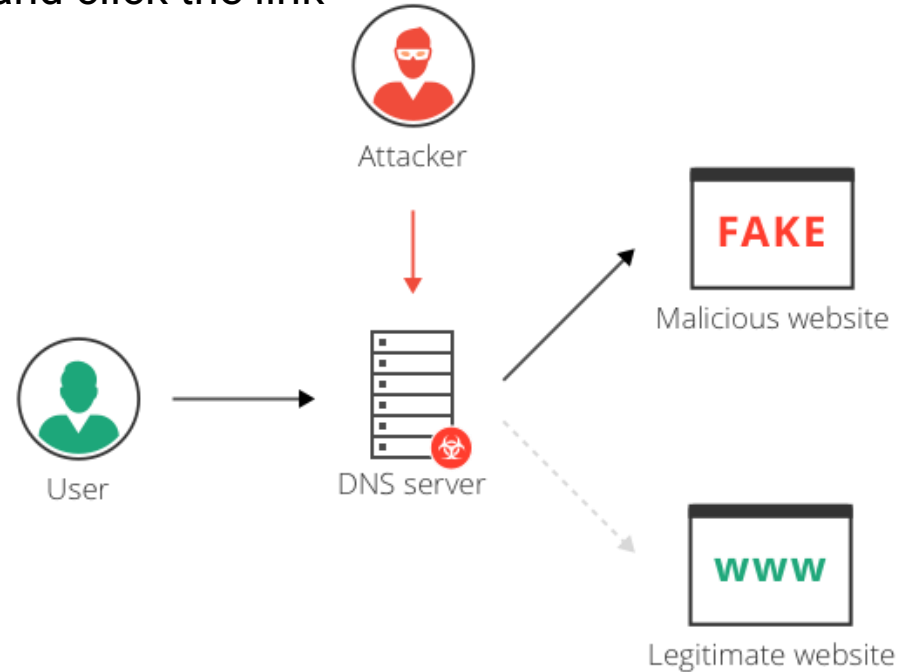
Securing Networks with
Cisco FTD

Chapter 11

Domain Name System (DNS) Policy

Mohsen Kheradmand

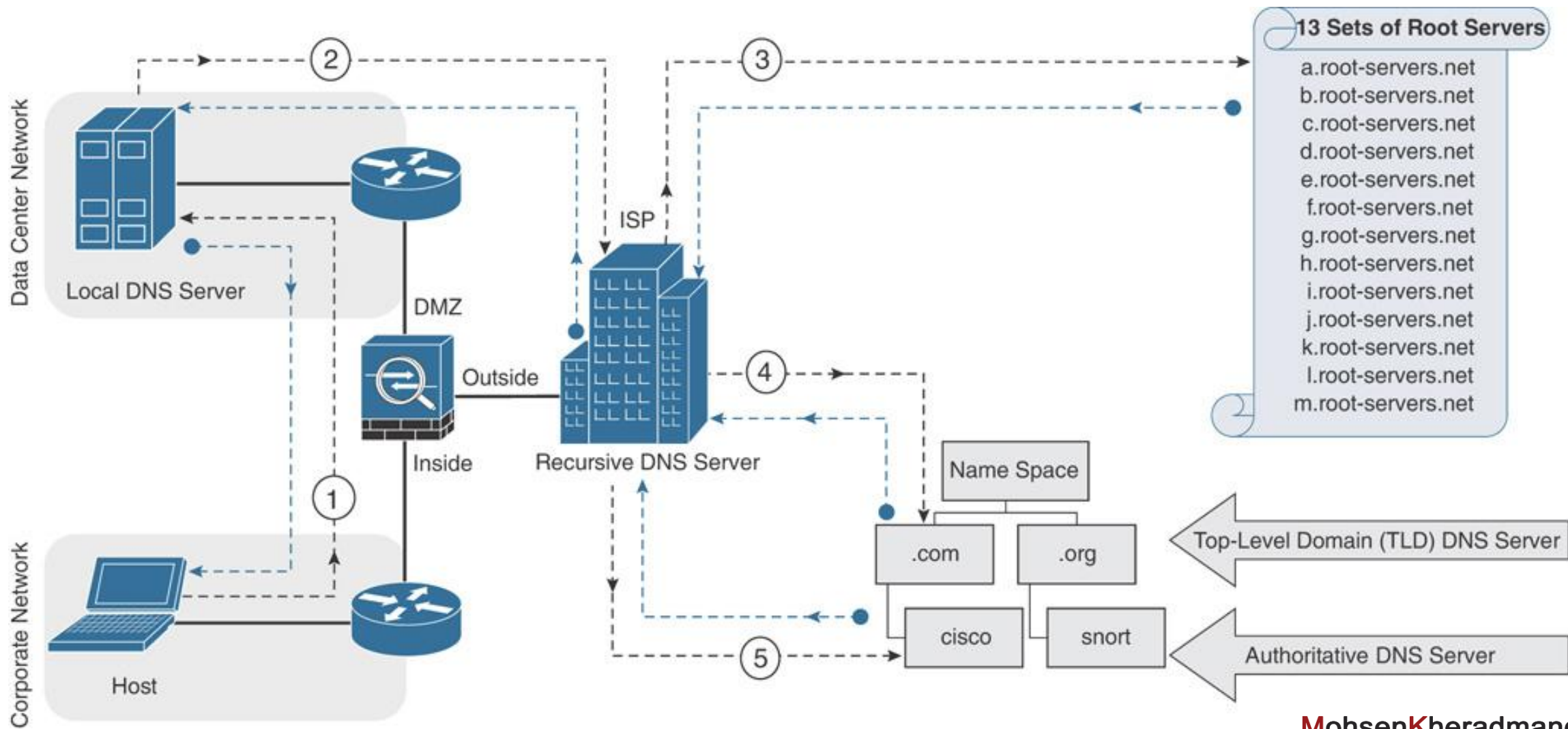
- Attackers often send phishing emails with links to malicious websites.
- A user in your network may be deceived and click the link



- 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

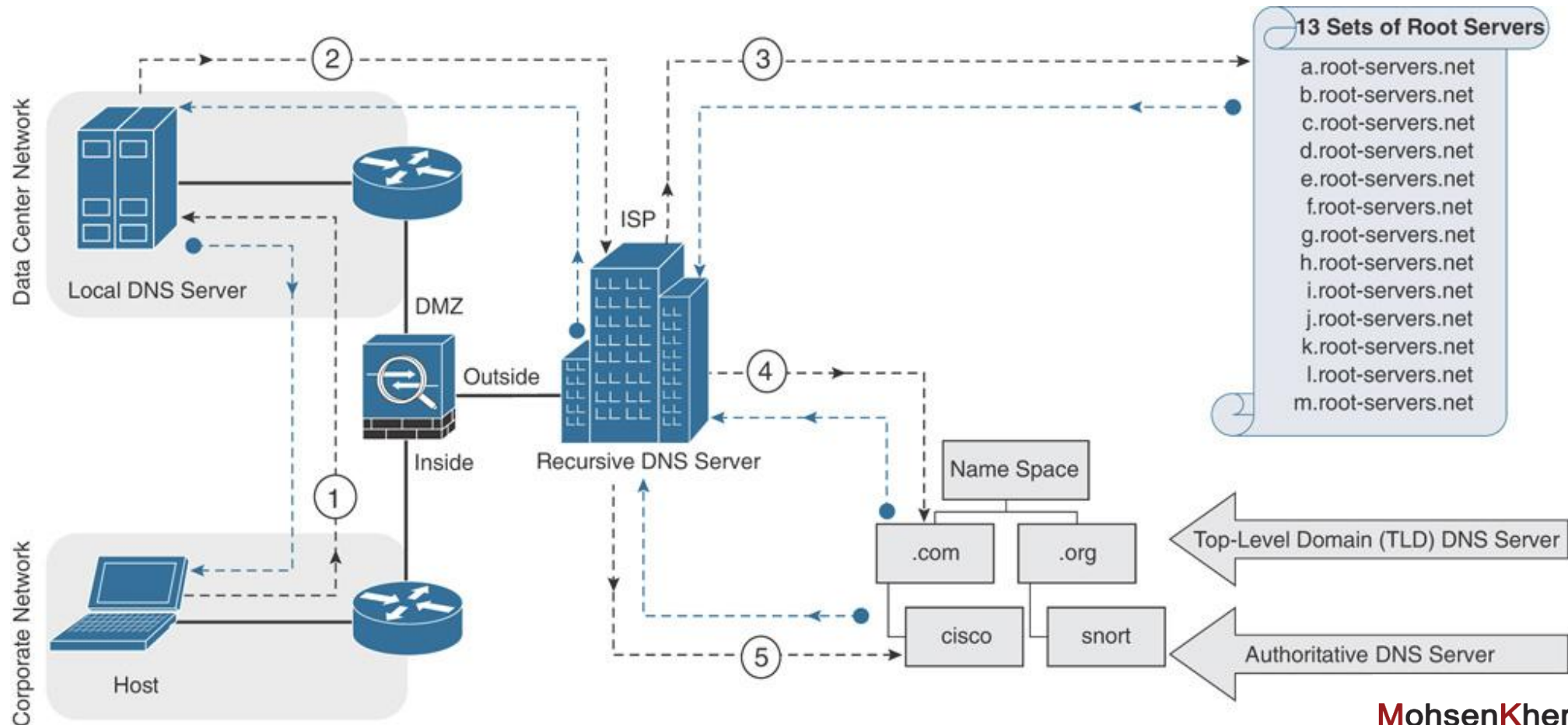
DNS Queries

Let's see how DNS queries resolves



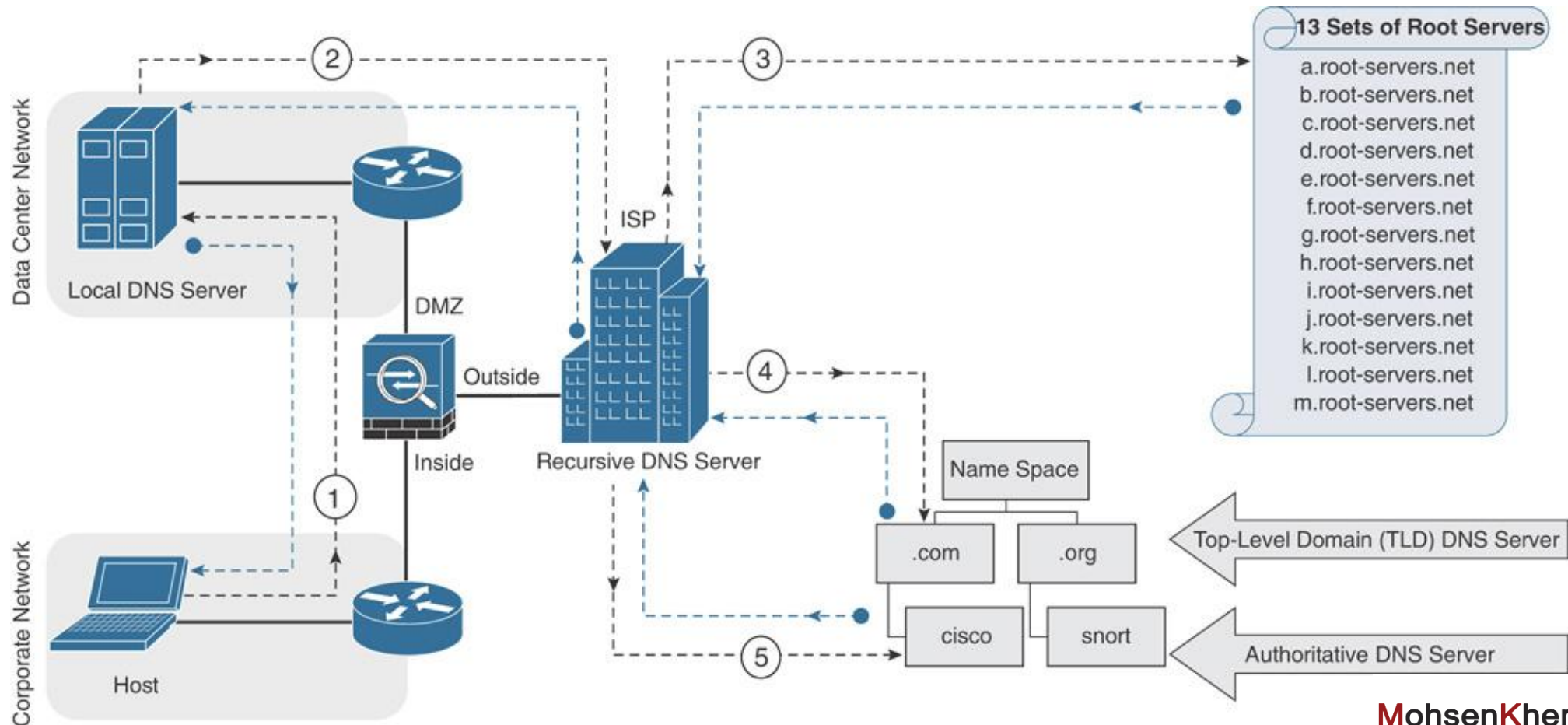
DNS Queries

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



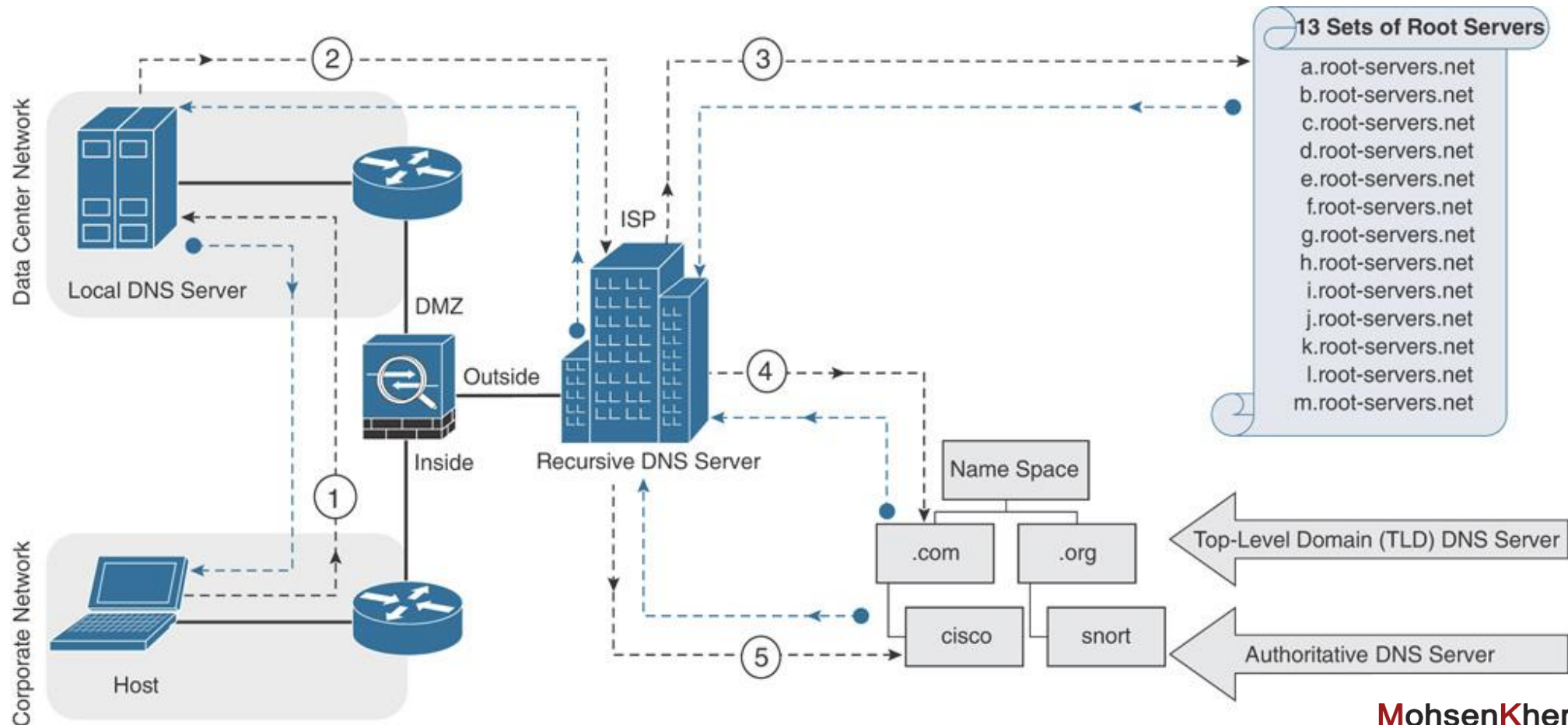
DNS Queries

- 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



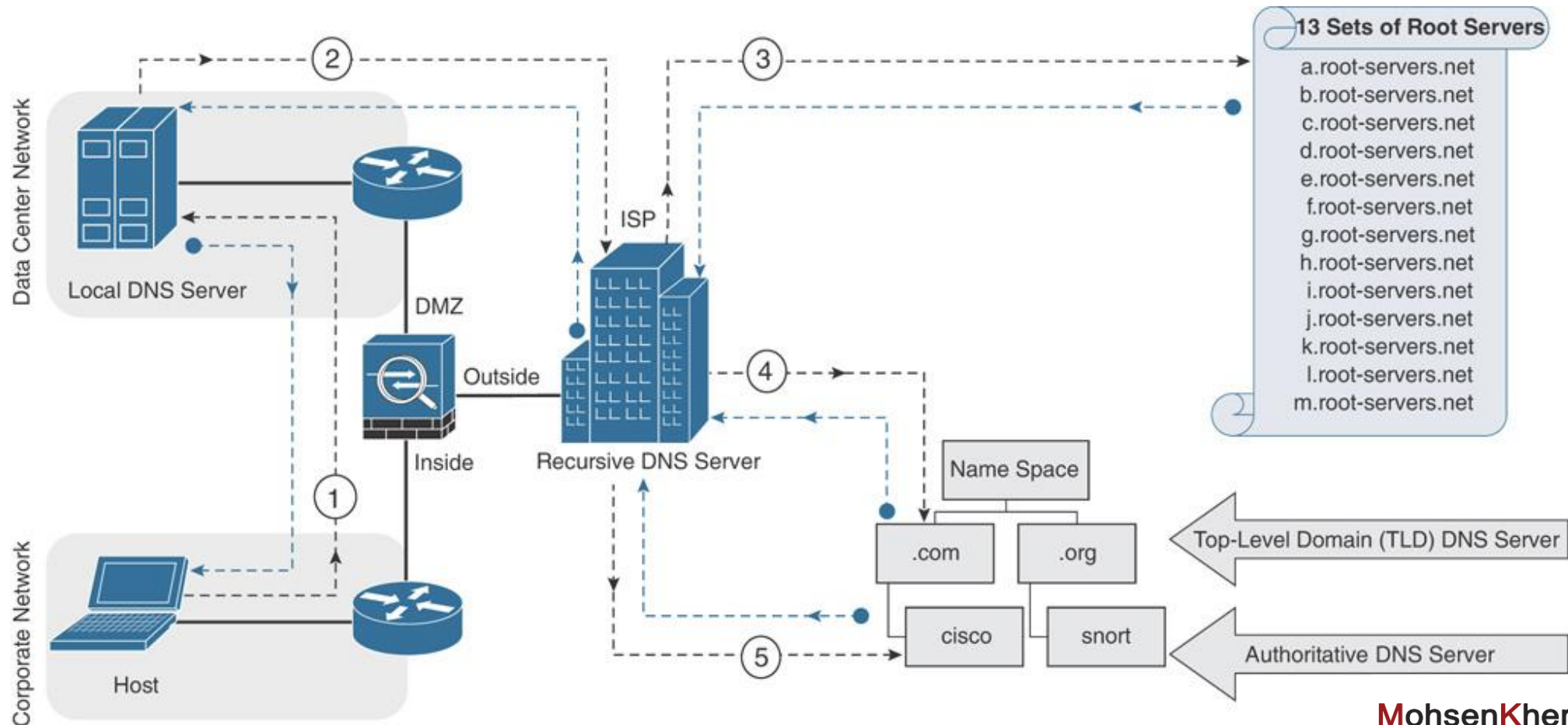
DNS Queries

- 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).



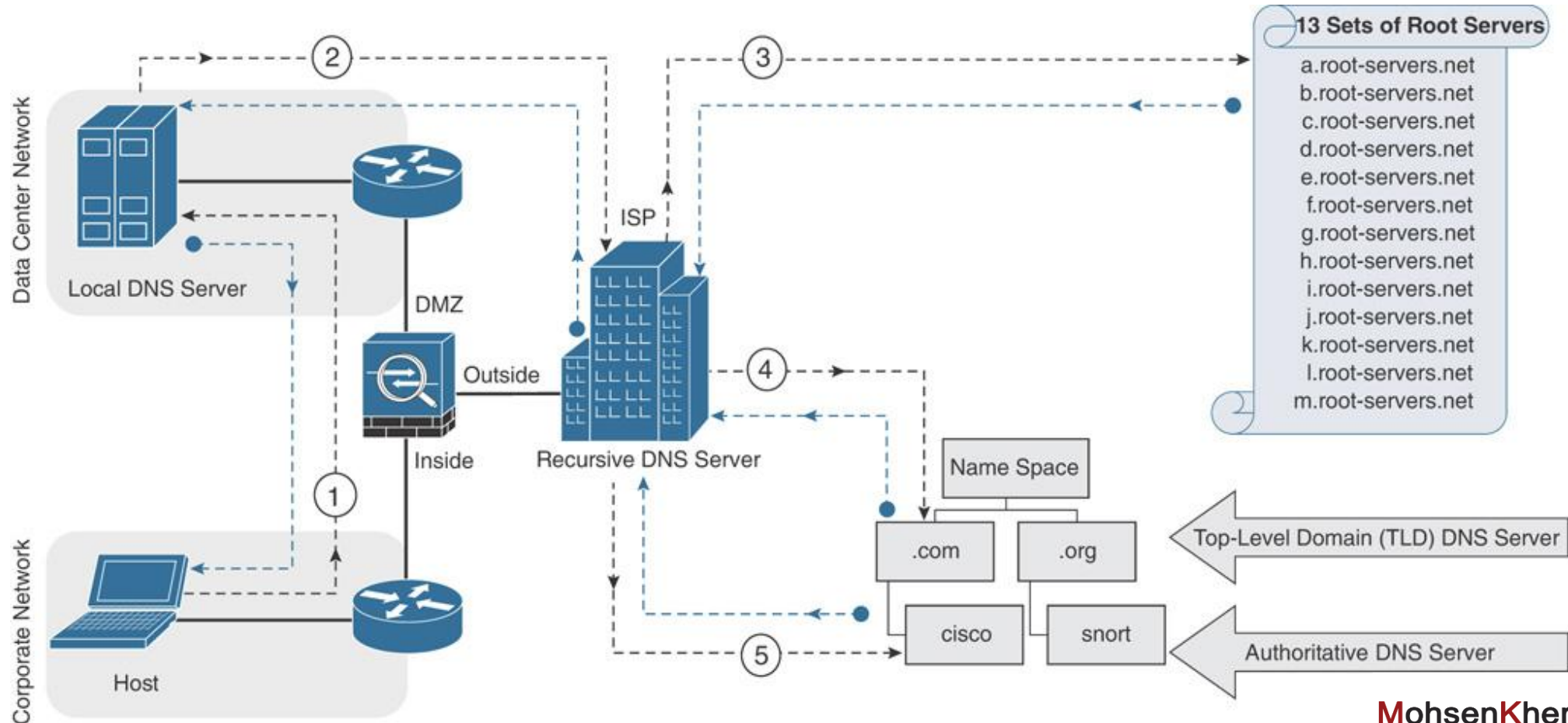
DNS Queries

- 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

Add Rule

Name: Access Control Rule to Block DNS ☒ Enabled

Insert: into Mandatory

Action: Block

Time Range: None

Zones Networks VLAN Tags **Users** Applications **Ports** URLs Dynamic Attributes Inspection Logging Comments

Available Ports

Search by name or value

- AOL
- Bittorrent
- DNS_over_TCP**
- DNS_over_UDP**
- FTP
- HTTP
- HTTPS
- IMAP

Add to Source

Add to Destination

Selected Source Ports (0)

any

Selected Destination Ports (2)

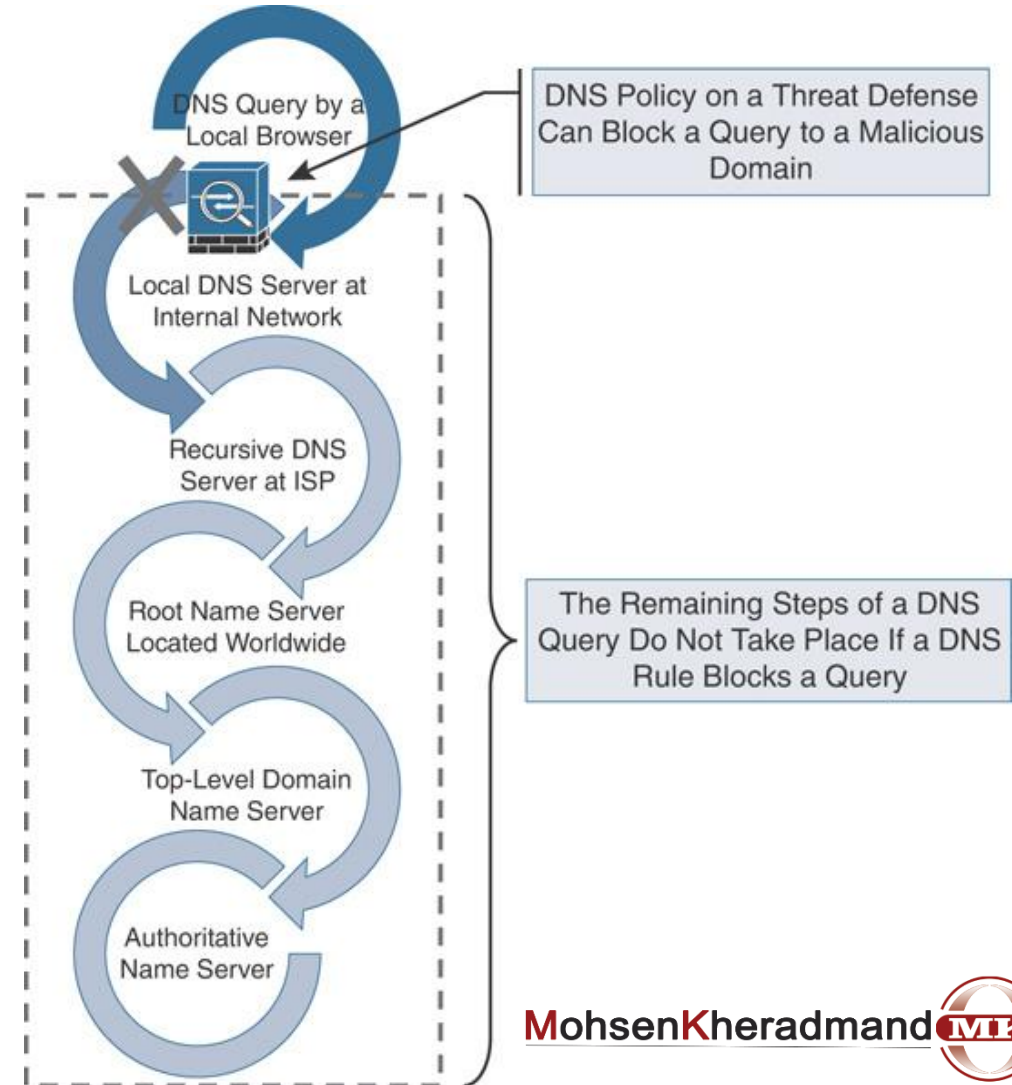
- DNS_over_TCP
- DNS_over_UDP

Protocol TCP (6) Port Enter a Add

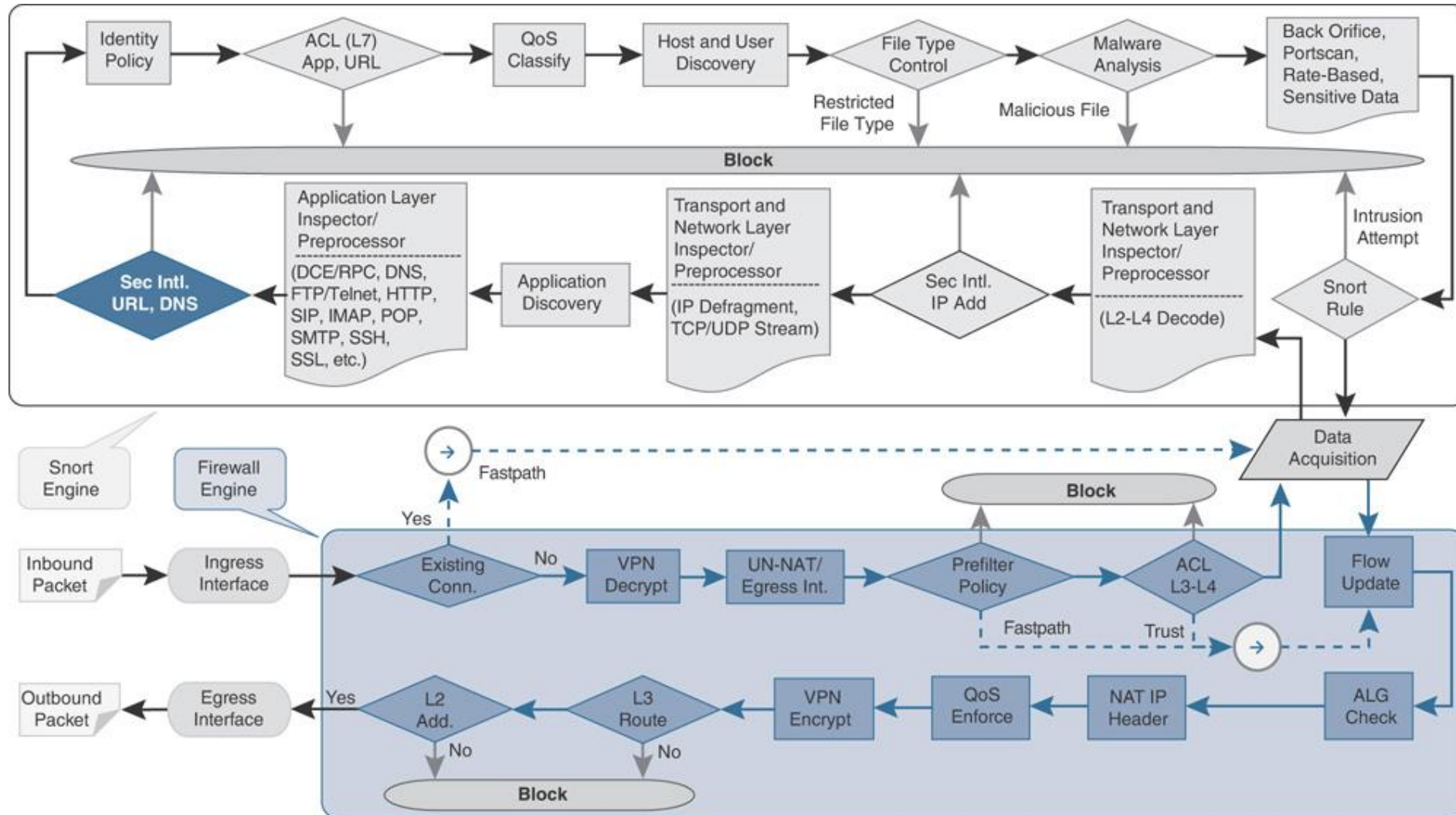
Cancel Add

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)

The screenshot shows the Firepower Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Objects' tab is selected, and the 'Object Management' dropdown menu is open, showing 'Intrusion Rules' and 'Update Feeds'. The 'Update Feeds' button is highlighted with a yellow circle labeled '1'. The 'Add DNS Lists and Feeds' button is also visible. The main content area is titled 'DNS Lists and Feeds' and contains a table with the following data:

Name	Type	
Cisco-DNS-and-URL-Intelligence-Feed	Feed	 
Global-Block-List-for-DNS	List	 
Global-Do-Not-Block-List-for-DNS		 

A modal dialog titled 'Cisco Security Intelligence' is open, showing the 'Update Frequency' dropdown menu set to '2 hours'. The 'Save' button is highlighted with a yellow circle labeled '3'. The sidebar on the left shows the 'Security Intelligence' section expanded, with 'DNS Lists and Feeds' highlighted by a yellow circle labeled '2'.

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

The screenshot shows the Cisco Firepower Management Center interface. The top navigation bar includes links for Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. The left sidebar shows a tree view with categories like Geolocation, Interface, Key Chain, Network, PKI, Policy List, Port, Prefix List, Route Map, and Security Intelligence. The 'Security Intelligence' category is expanded, showing 'DNS Lists and Feeds' (highlighted with a yellow circle and the number 2). The main content area is titled 'DNS Lists and Feeds' and contains a table with the following data:

Name	Type	
Cisco-DNS-and-URL-Intelligence-Feed	Feed	 
Global-Block-List-for-DNS	List	 
Global-Do-Not-Block-List-for-DNS	List	 

Three yellow circles with numbers 1, 2, and 3 highlight specific steps: 1. Object Management, 2. DNS Lists and Feeds, and 3. Add DNS Lists and Feeds.

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

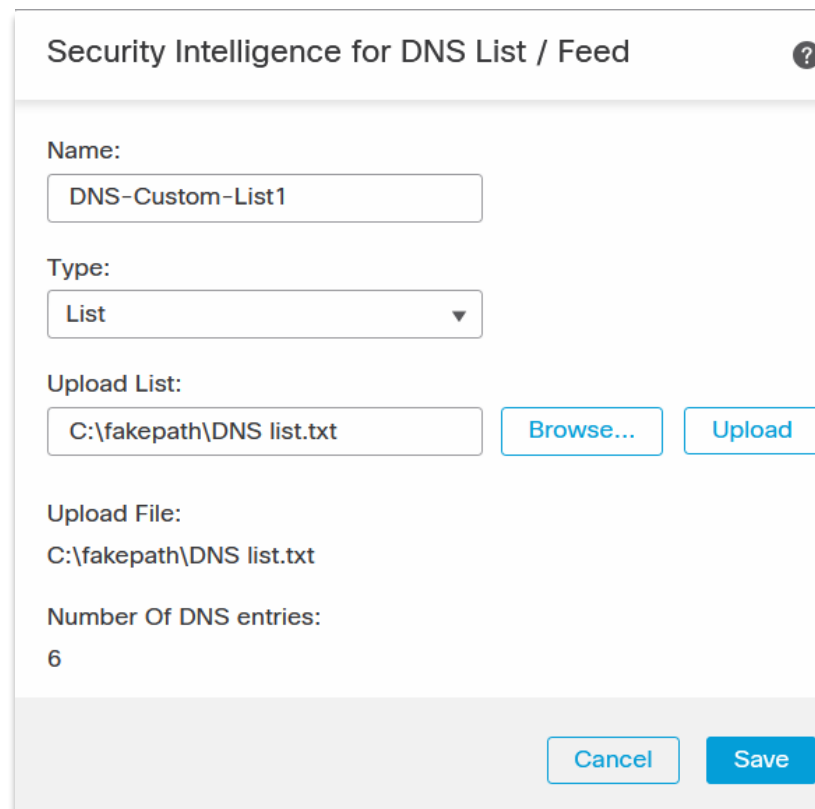
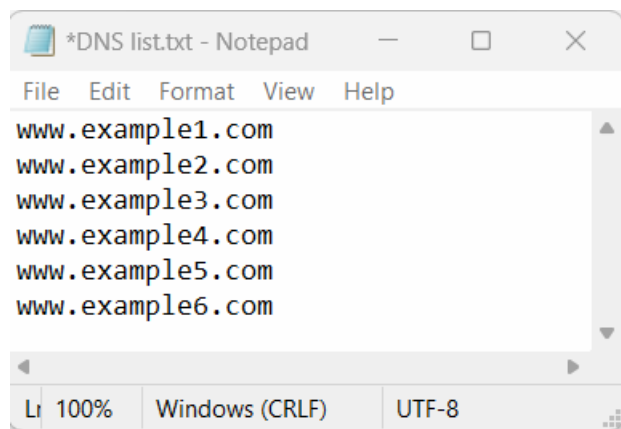
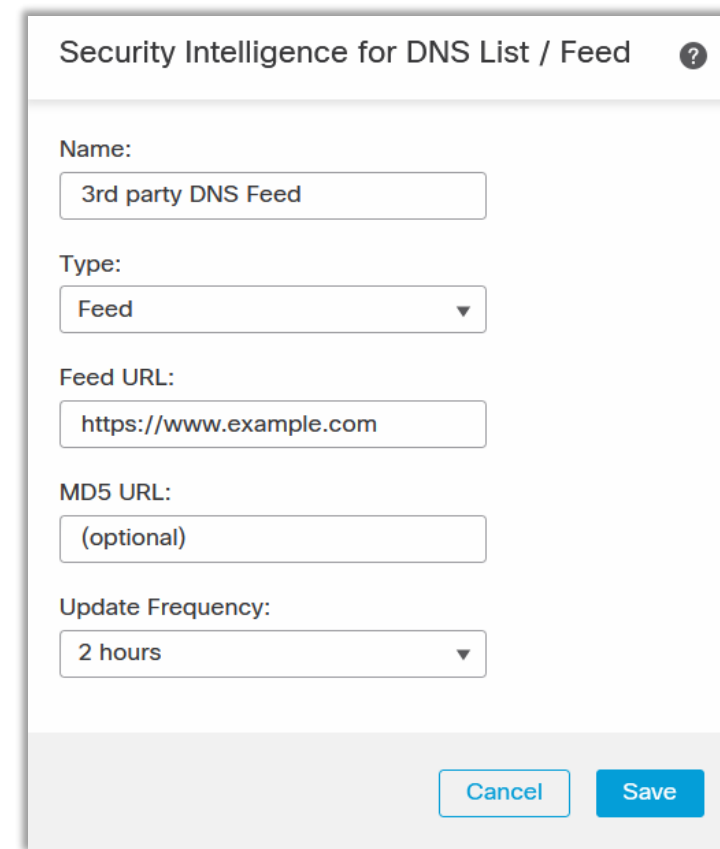
Sources of Intelligence

2) List / 3rd party Fees

Type of DNS list

>> **Feed** : to obtain Feed from 3rd party

>> **List** : to upload a list of DNS Queries

A screenshot of the 'Security Intelligence for DNS List / Feed' dialog box. The 'Name' field is 'DNS-Custom-List1'. The 'Type' dropdown is set to 'List'. The 'Upload List' field shows 'C:\fakepath\DNS list.txt' with 'Browse...' and 'Upload' buttons. The 'Upload File' field also shows 'C:\fakepath\DNS list.txt'. The 'Number Of DNS entries' is set to '6'. 'Cancel' and 'Save' buttons are at the bottom right.A screenshot of the 'Security Intelligence for DNS List / Feed' dialog box. The 'Name' field is '3rd party DNS Feed'. The 'Type' dropdown is set to 'Feed'. The 'Feed URL' field is 'https://www.example.com'. The 'MD5 URL' field is '(optional)'. The 'Update Frequency' dropdown is set to '2 hours'. 'Cancel' and 'Save' buttons are at the bottom right.

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)

The screenshot shows the Cisco Firepower Management Center interface. The top navigation bar includes the Cisco logo, the title 'Firepower Management Center', and a breadcrumb trail: 'Policies / Access Control / DNS'. The main navigation tabs are 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Policies' tab is active, and a sub-menu is open showing 'Access Control', 'Network Discovery', and 'Actions'. Under 'Access Control', 'DNS' is selected. The 'Actions' menu is also open, showing 'Alerts', 'Scanners', 'Groups', 'Modules', and 'Instances'. On the right side, there are buttons for 'Compare Policies' and 'Add DNS Policy'. Below these, a table lists existing policies, including the 'Default DNS Policy' with the description 'Default DNS Policy with Global Block List and Global Do-Not-Block List'. A 'New DNS Policy' dialog box is open in the foreground, with the 'Name' field containing 'My DNS Policy' and the 'Description' field containing 'this is a new custom policy'. The dialog box has 'Cancel' and 'Save' buttons at the bottom.

Firepower Management Center
Policies / Access Control / DNS

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy 🔍 3 ⚙️ ? admin ▼

Management | Access Control | Import/Export

Compare Policies Add DNS Policy

DNS Policy

Default DNS Policy
Default DNS Policy with Global Block List and Global Do-Not-Block List

New DNS Policy

Name
My DNS Policy

Description
this is a new custom policy

Cancel Save

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

DNS Policy configuration

3) Click Add DNS Rule

 Firepower Management Center

Policies / Access Control / DNS Policy Editor

Overview

Analysis

Policies

Devices

Objects

AMP

Intelligence

Deploy 🔍 3 ⚙️ ? admin ▾

My DNS Policy

this is a new custom policy

Save Cancel

Rules

+ Add DNS Rule

#	Name	Source Zones	Source Networks	VLAN Tags	DNS Lists	Action	
Do-Not-Block List							
1	Global Do-Not-Block List for DNS	any	any	any	Global-Do-Not-Block-List-for-DNS	Do Not Block	 
Block List							
2	Global Block List for DNS	any	any	any	Global-Block-List-for-DNS	Domain Not Found	 

- 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

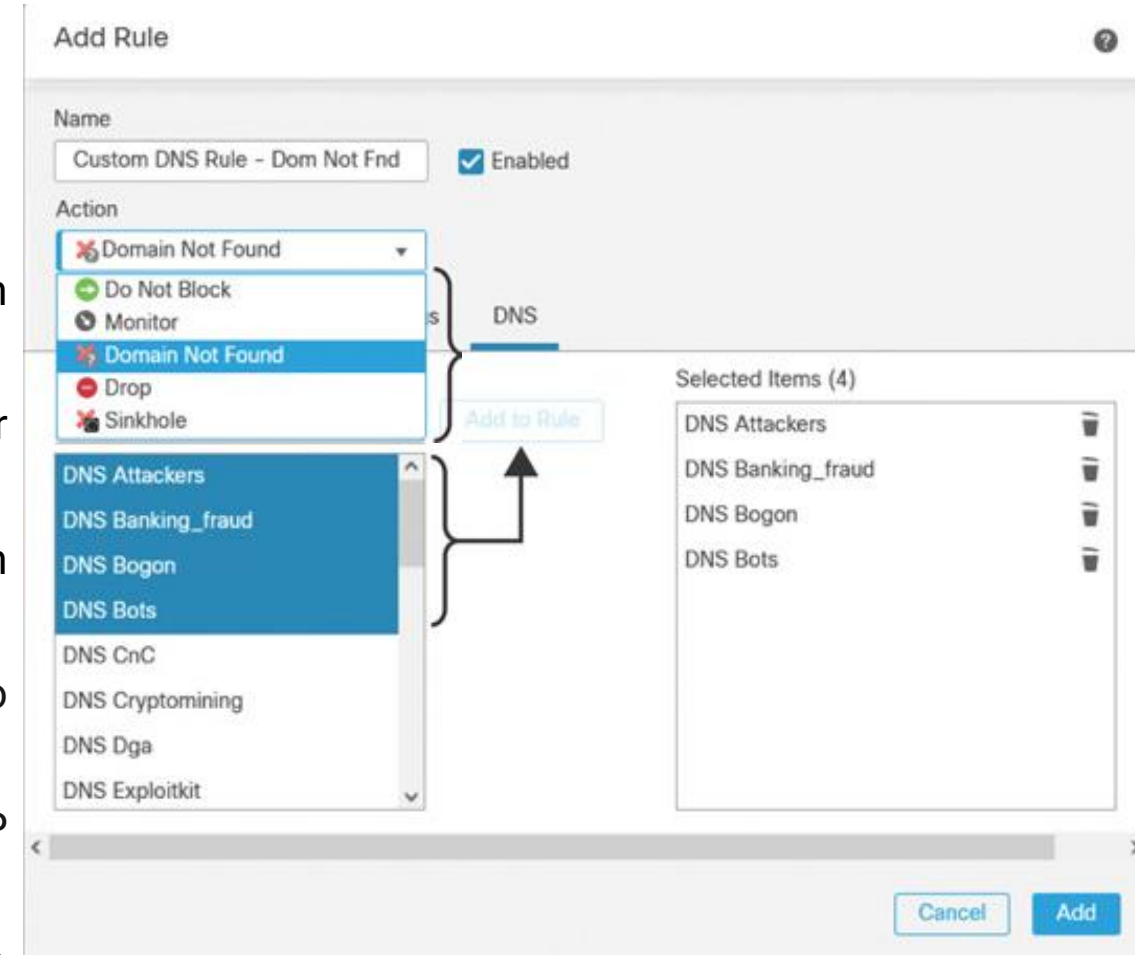
The screenshot shows the Cisco Firepower Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Analysis' tab is selected, and the 'Connections / Events' sub-tab is active. A search bar and 'Predefined Searches' dropdown are visible. Below the search bar, a time range '2022-02-06 00:39:08 - 2022-02-06 01:57:45' is shown with an 'Expanding' status. A table of events is displayed with columns for various attributes. A right-click context menu is open over the 'cisco.com' domain in the 'DNS Query' column. The menu options include 'Open in New Window', 'Exclude', 'Add Domain to Global Block List for DNS' (highlighted), 'Add Domain to Global Do-Not-Block List for DNS', and several other domain-specific options.

Destination Port / ICMP Code	SSL Status	Application Protocol	Client	Client Version	Web Application	Application Risk	Business Relevance	URL	URL Category	URL Reputation	DNS Query	VLAN ID	IOC	Intrusion Events	Files	Access Control Policy	Access Control Rule	Network Analysis Policy	Profile
53 (domain) / udp			☐ DNS			Very Low	Very High				cisco.com					ACL Policy1	permit_all	Balanced Security and Connectivity	Defa

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

The screenshot shows the 'Add Rule' configuration window. The 'Name' field is 'Custom DNS Rule - Dom Not Fnd' and is checked as 'Enabled'. The 'Action' is 'Domain Not Found'. The 'DNS' tab is selected. The 'DNS Lists and Feeds' section shows a list of items: 'DNS Attackers', 'DNS Banking_fraud', 'DNS Bogon', 'DNS Bots', 'DNS CnC', 'DNS Cryptomining', 'DNS Dga', and 'DNS Exploitkit'. The first four items are selected. A bracket groups these four items, with an arrow pointing to the 'Add to Rule' button. The 'Selected Items (4)' section shows the same four items: 'DNS Attackers', 'DNS Banking_fraud', 'DNS Bogon', and 'DNS Bots'. At the bottom right, there are 'Cancel' and 'Add' buttons.

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

The screenshot displays the Cisco Firepower Management Center (FMC) interface for configuring a DNS Policy. The top navigation bar includes the Cisco logo, 'Firepower Management Center', and various tabs: Overview, Analysis, Policies (selected), Devices, Objects, AMP, and Intelligence. The breadcrumb trail is 'Policies / Access Control / Policy Editor'. The main header shows 'FTD1-Policy' applicable to FTD1, with a warning 'You have unsaved changes' and buttons for 'Show Warnings', 'Analyze Hit Counts', 'Save', and 'Cancel'. Below the header, the 'Security Intelligence' tab is active, showing 'Prefilter Policy: Servers Prefilter', 'SSL Policy: None', and 'Identity Policy: None'. The 'Available Objects (23)' section on the left lists Networks and URLs. The 'Available Zones' section lists 'Any' and 'Internet'. The 'DNS Policy' section on the right shows a dropdown menu with 'My DNS Policy' selected, and a list of policies including 'Global Do-Not-Block List (Any Zone)', 'URLs', and 'Global Do-Not-Block List for URL (Any Zone)'. The 'Block List(3)' section on the right lists 'Global Block List (Any Zone)', 'Servers (Any Zone)', and 'Global Block List for URL (Any Zone)'.

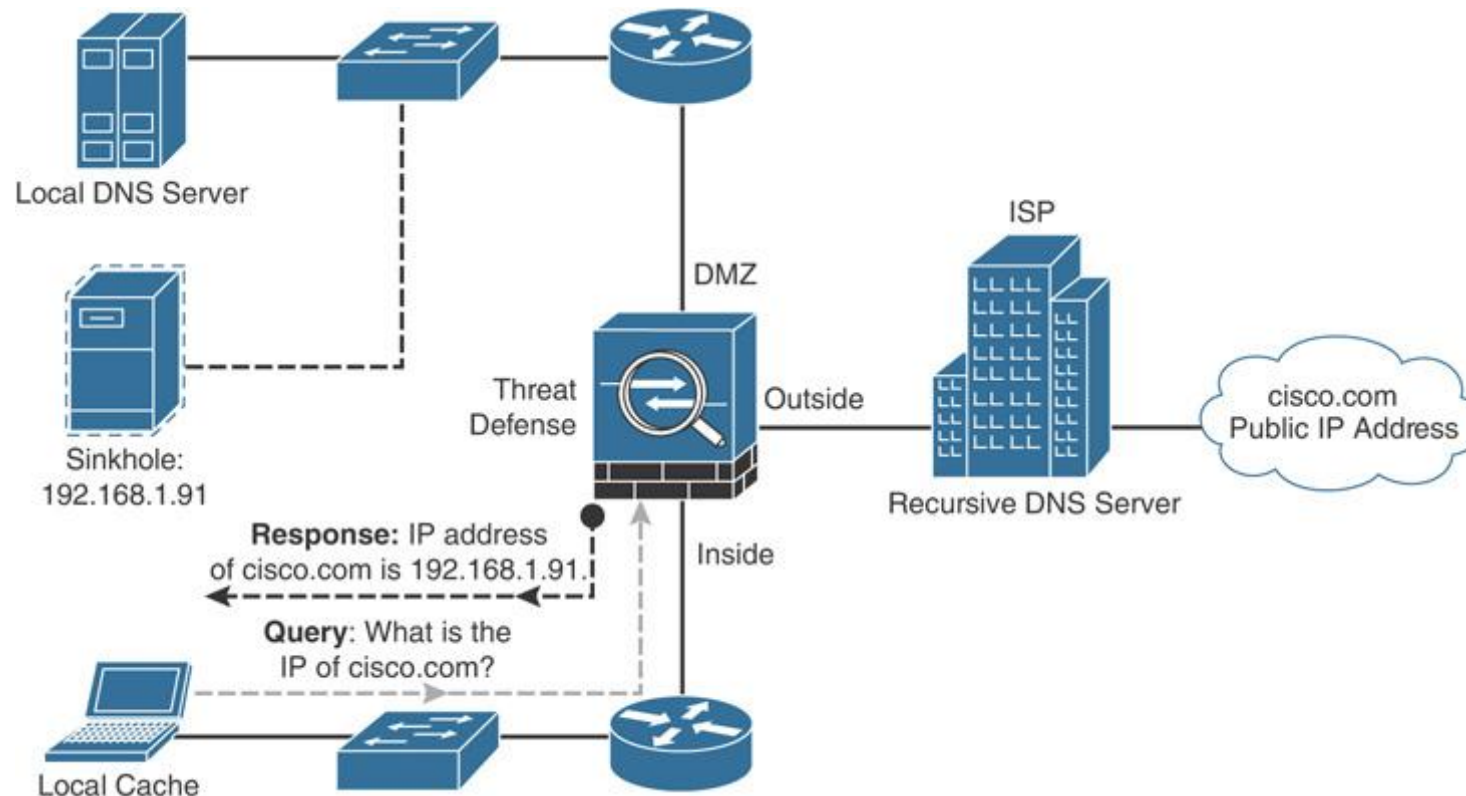
- Click Save
- Deploy the Policy

DNS Policy configuration

Configure the Sinkhole

- Spoofed DNS server :

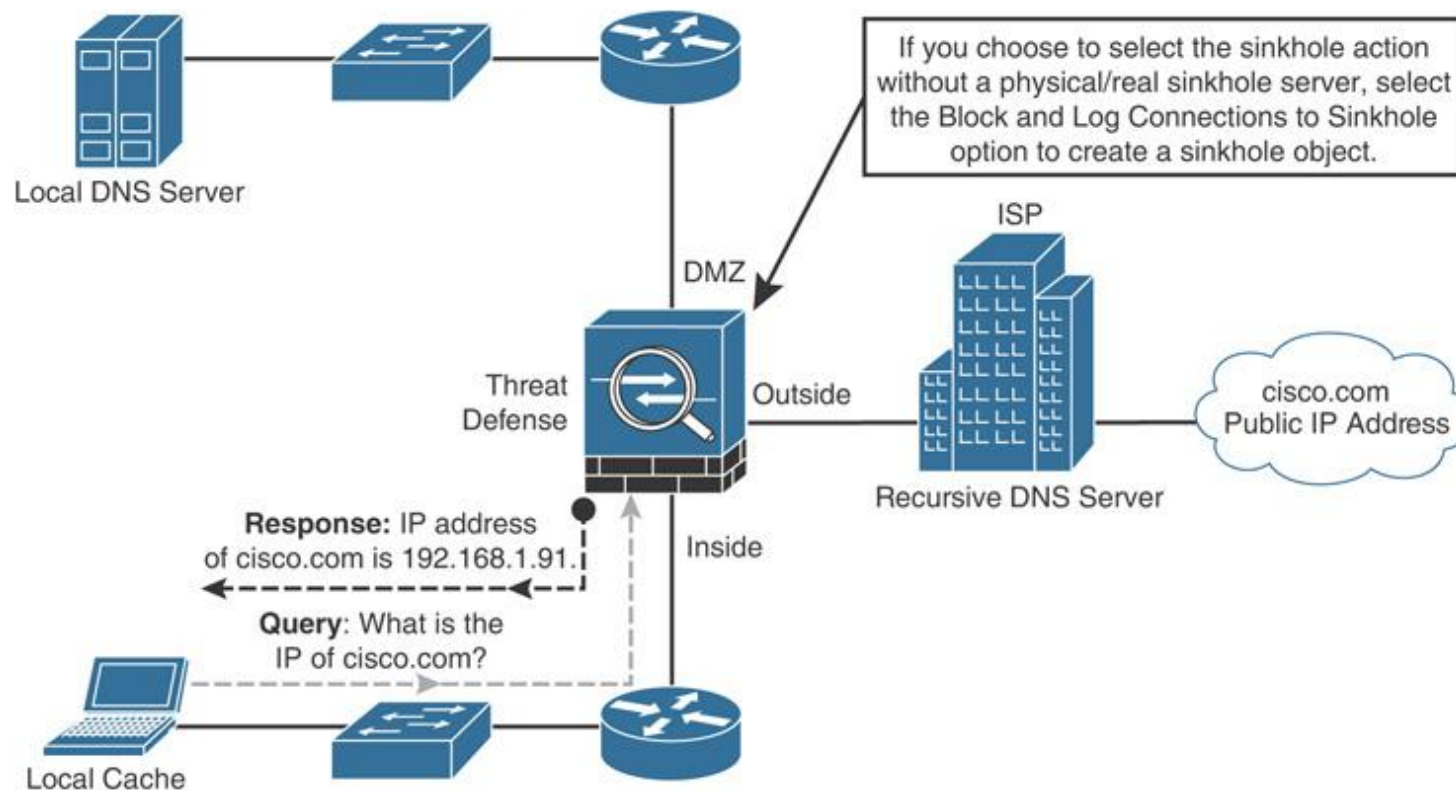
The threat defense uses the IP address of this spoofed DNS server as a response to a harmful DNS query



DNS Policy configuration

Configure the Sinkhole

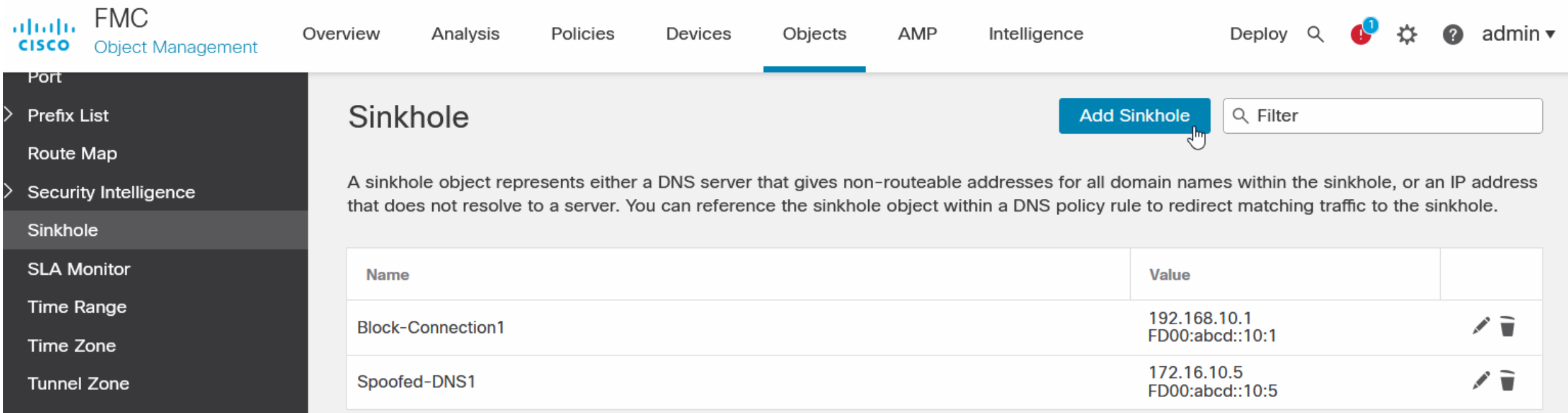
- A sinkhole without a physical spoofed server:
You can assign any false IP address within a sinkhole object
- If a not-valid sinkhole IP address is returned, then end user attempts to access the sinkhole IP address.



DNS Policy configuration

Configure the Sinkhole

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



The screenshot shows the Cisco FMC Object Management interface. The top navigation bar includes tabs for Overview, Analysis, Policies, Devices, Objects (selected), AMP, and Intelligence. On the right, there are icons for Deploy, search, notifications, settings, help, and a user profile labeled 'admin'. A left sidebar contains a tree view with categories like Port, Security Intelligence, and Sinkhole. The main content area is titled 'Sinkhole' and features an 'Add Sinkhole' button and a search filter. Below this is a descriptive paragraph about sinkhole objects. At the bottom, a table lists existing sinkhole objects with their names and values.

Sinkhole [Add Sinkhole](#)

A sinkhole object represents either a DNS server that gives non-routeable addresses for all domain names within the sinkhole, or an IP address that does not resolve to a server. You can reference the sinkhole object within a DNS policy rule to redirect matching traffic to the sinkhole.

Name	Value	
Block-Connection1	192.168.10.1 FD00:abcd::10:1	 
Spoofed-DNS1	172.16.10.5 FD00:abcd::10:5	 

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

Sinkhole

Name
Spoofed-DNS2

IPv4 Policy
172.16.10.6

IPv6 Policy
FD00:abcd::10:6

Log Connections to Sinkhole
☐

Block and Log Connections to Sinkhole
☒

Type
None

- None
- Command and Control
- Malware
- Phishing

Save

DNS Policy configuration

- Now you can use configured object to create a rule

Add Rule

Name

Custom-to-Spoofed1

☒ Enabled

Action

 Sinkhole

Sinkhole

Spoofed-DNS1

Zones

Networks

VLAN Tags

DNS

DNS Lists and Feeds

Search by name or value

Custom-List1

Global-Block-List-for-DNS

Global-Do-Not-Block-List-for-D

Add to Rule

Selected Items (1)

Custom-List1

Cancel

Add

Verification

- > Analysis
- > Connections
- > Security Intelligence Events

This Packet Is Blocked by the IP-Based Security Intelligence, Not by the DNS Policy

Security Intelligence Events

No Search Constraints ([Edit Search](#))

Security Intelligence with Application Details

Jump to...

	☐ + First Packet x	Action x	Reason x	Security Intelligence x Category	Destination Port / ICMP Code x	DNS Query x	DNS Response x
▼	☐ 2020-12-01 17:27:21	Block	IP Block	Malware	58603 / tcp		
▼	☐ 2020-12-01 17:25:09	Allow	DNS Monitor	DNS Spyware	53 (domain) / udp	news06.biz	No Error
▼	☐ 2020-12-01 17:23:12	Sinkhole	DNS Block	DNS Malware	53 (domain) / udp	wowize.xyz	Sinkhole response from firewall
▼	☐ 2020-12-01 17:23:12	Sinkhole	DNS Block	DNS Malware	53 (domain) / udp	wowize.xyz	Sinkhole response from firewall
▼	☐ 2020-12-01 17:10:45	Block	DNS Block	DNS CnC	53 (domain) / udp	dcapib.com	No Error
▼	☐ 2020-12-01 17:03:58	Domain Not Found	DNS Block	DNS Attackers	53 (domain) / udp	ero.bckd.ir	NXDOMAIN response from firewall

< < Page 1 of 1 > > Displaying rows 1-6 of 6 rows

[View](#) [Delete](#)

[View All](#) [Delete All](#)

Actions That You Enabled Within Each DNS Rule

Categories That You Added to a Rule

Client and Server Communications

MohsenKheradmand

