DNS Protection

Support Course

TRAINING HANDOUT

Version 2 • May 2024

Course Introduction

In this training, you will learn about Sophos DNS Protection.

This new cloud-based service is part of our growing suite of Secure Access Service Edge products and services, expanding upon what we started with Sophos ZTNA and Sophos SD-WAN Orchestration.

Course Agenda

- Module 1: The importance of DNS in cybersecurity
- Module 2: Deploying Sophos DNS Protection
- Module 3: Logs and Reports
- Module 4: Troubleshooting Sophos DNS Protection

Prerequisite

- Sophos Firewall v19.5/v20 Engineer Certified
- Knowledge of Sophos Central and general troubleshooting
- Windows and Linux command line tools and network utilities
- Network Fundamentals – OSI and TCP/IP Model

Certification

To obtain the certification for DNS Protection Support Course you must pass the online assessment.
You will have 1 attempt to pass the assessment with a score of 80% or higher.

Table of Contents

Module 1: The importance of DNS in cybersecurity

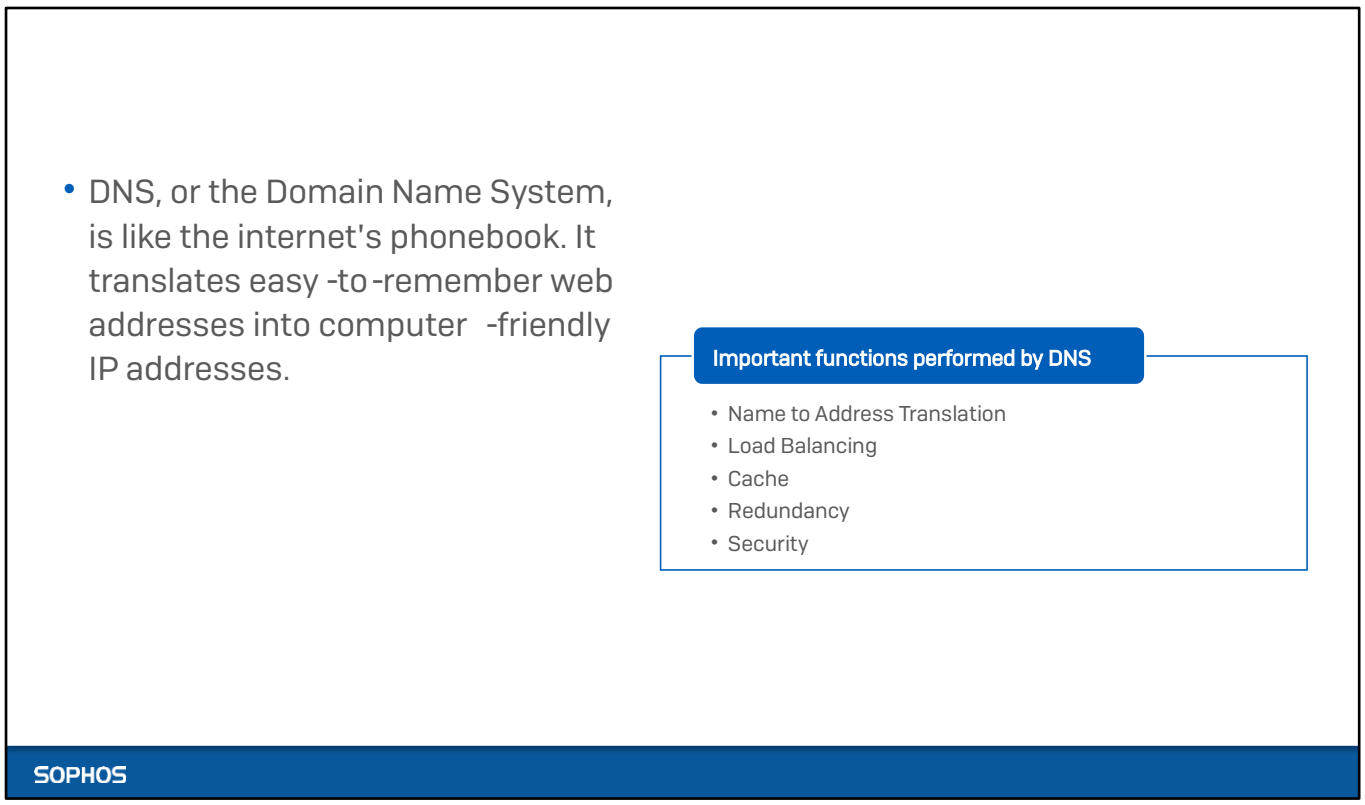
Module Objectives

Once you complete this module you will be able to:

- Understand the role of DNS in networking.
- Understand the importance of DNS in cybersecurity.
- Comparison overview between regular DNS provider and Sophos DNS Protection.
- Understand the role of Sophos DNS Protection
- Key features of Sophos DNS Protection
- License Requirements to use Sophos DNS Protection

SOPHOS

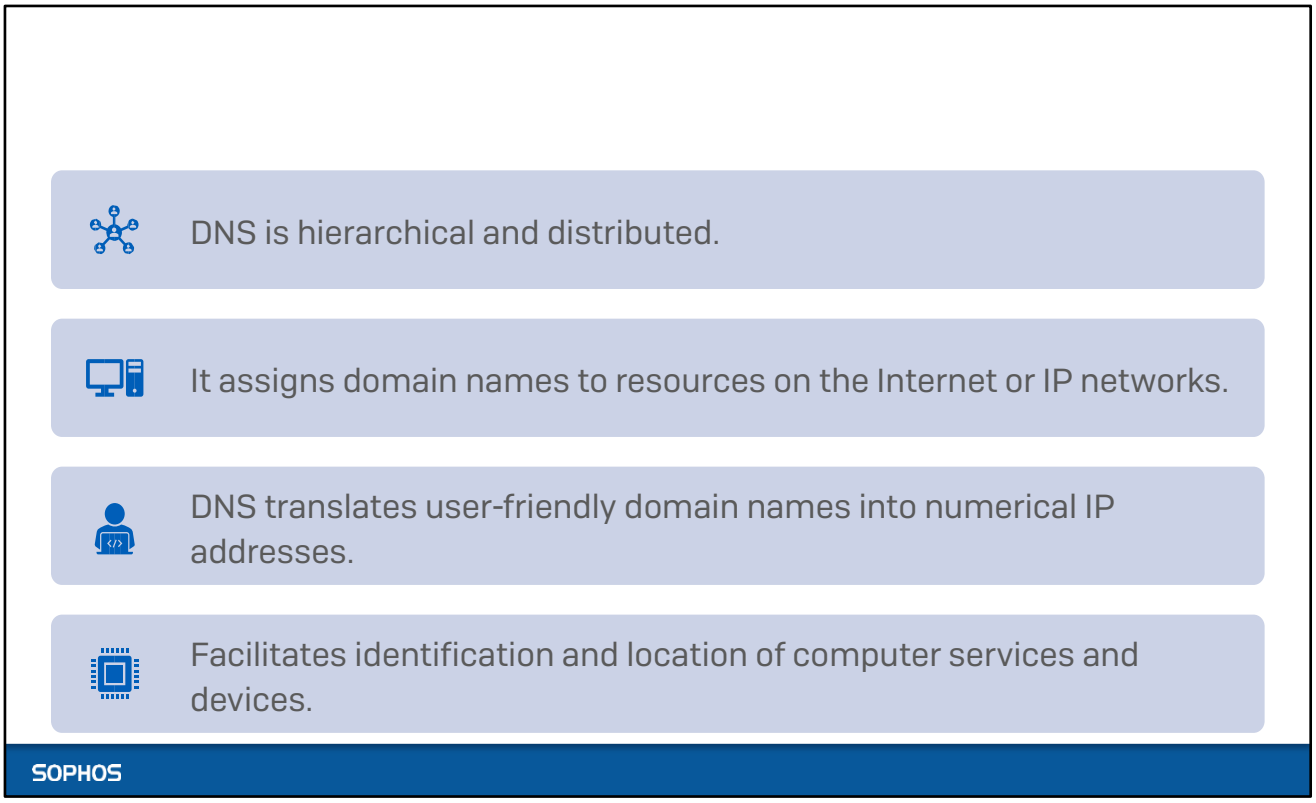
The role of DNS in networking



1.Name to Address Translation: When you type a website address into your browser, DNS finds the corresponding IP address, so your device knows where to connect.
2.Load Balancing: It helps distribute internet traffic evenly across multiple servers to prevent overload and keep websites running smoothly.
3.Cache: DNS servers remember recent translations to speed up future requests, making your browsing experience faster.
4.Redundancy: There are multiple DNS servers worldwide, so if one fails, there are backups to keep things running.
5.Security: DNS also has security measures to protect against hacking and ensure the accuracy of translations.

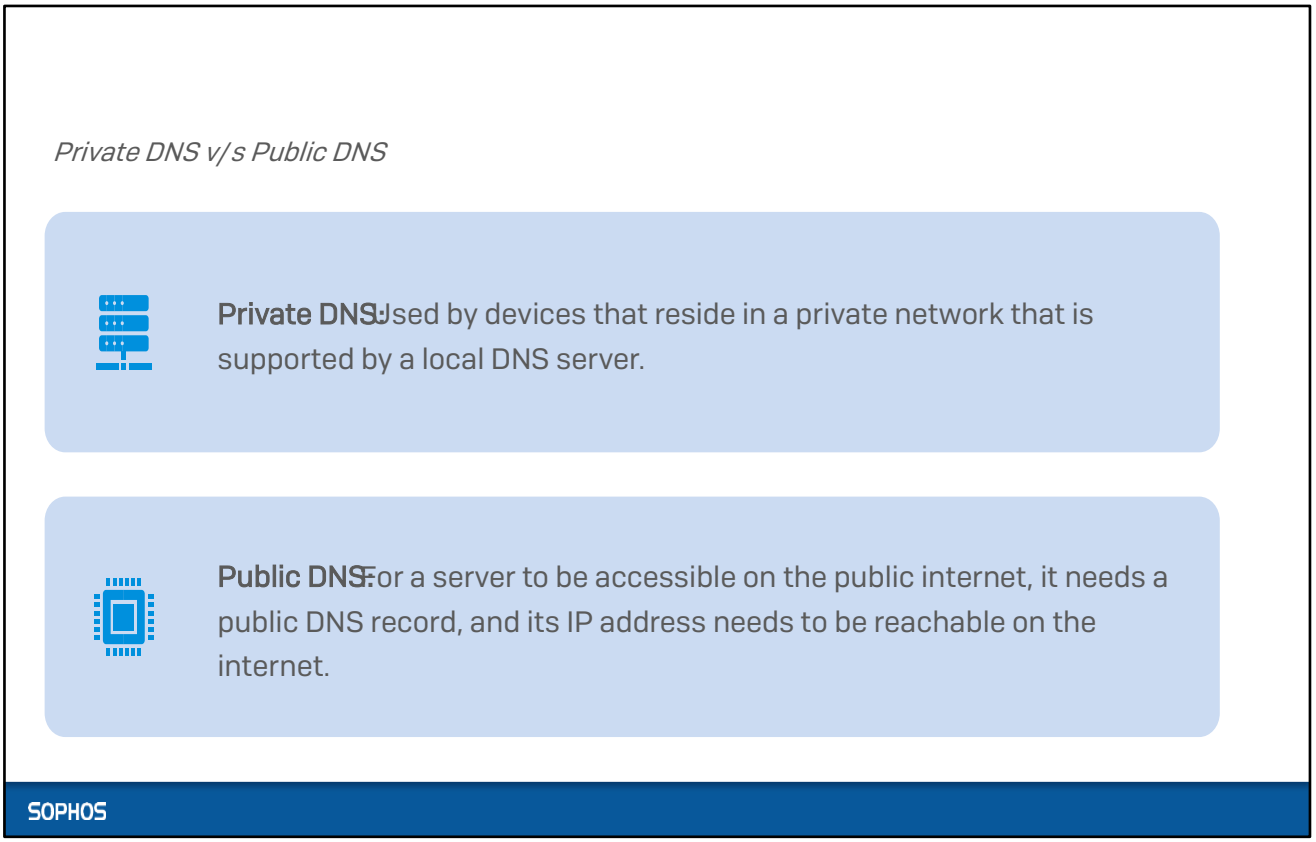
In short, DNS is essential for connecting your devices to websites and services on the internet, making sure everything runs smoothly and securely.

What is DNS?



The Domain Name System (DNS) is a hierarchical and distributed system that assigns domain names to resources on the Internet or other IP networks. It translates user friendly domain names into numerical IP addresses, facilitating the identification and location of computer services and devices.

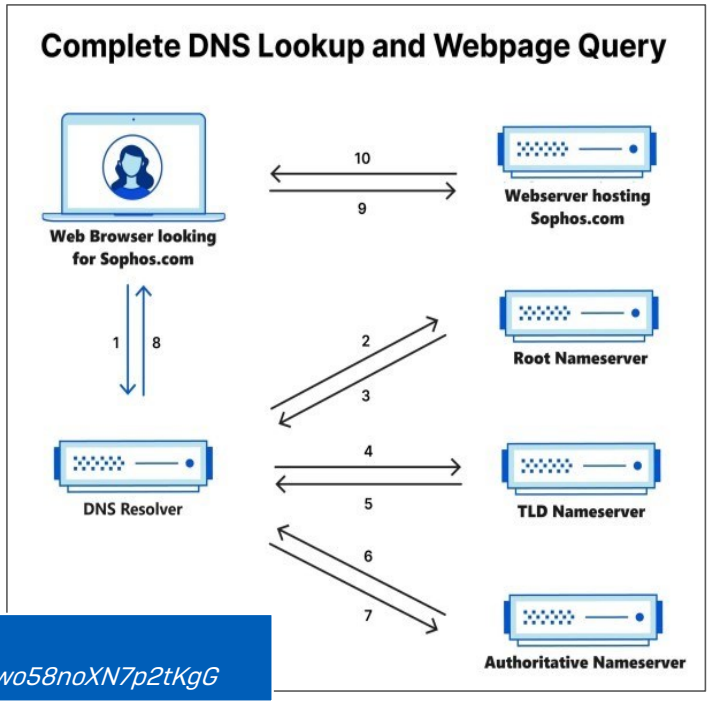
Internal v/s External DNS



Private DNS: Computers that live behind a firewall or on an internal network use a private DNS record so that local computers can identify them by name. Outside users on the internet will not have direct access to those computers.

Public DNS: For a server to be accessible on the public internet, it needs a public DNS record, and its IP address needs to be reachable on the internet.

How DNS works?



Refer to Techvids video at https://techvids.sophos.com/watch/JbNKDsj wo58noXN7p2tKgG

SOPHOS

1. When a user types ‘sophos.com' into a web browser, the query is sent to a DNS recursive resolver on the Internet.
2. The resolver then contacts a DNS root nameserver (.).
3. The root server directs the resolver to a Top-Level Domain (TLD) DNS server, such as .com or .net, which manages domain information.
4. The resolver queries the .com TLD for ‘sophos.com'.
5. The .com TLD responds with the IP address of ‘sophos.com's nameserver.
6. The resolver sends a query to 'sophos.com's nameserver.
7. The IP address for ‘sophos.com' is returned to the resolver.
8. The resolver provides the web browser with the requested domain's IP address.
9. With the IP address obtained, the browser initiates an HTTP request to the server.
10. The server at the IP address returns the web page to be displayed in the browser.

Refer to the Techvids video on DNS at

https://techvids.sophos.com/watch/JbNKDsjwo58noXN7p2tKgG

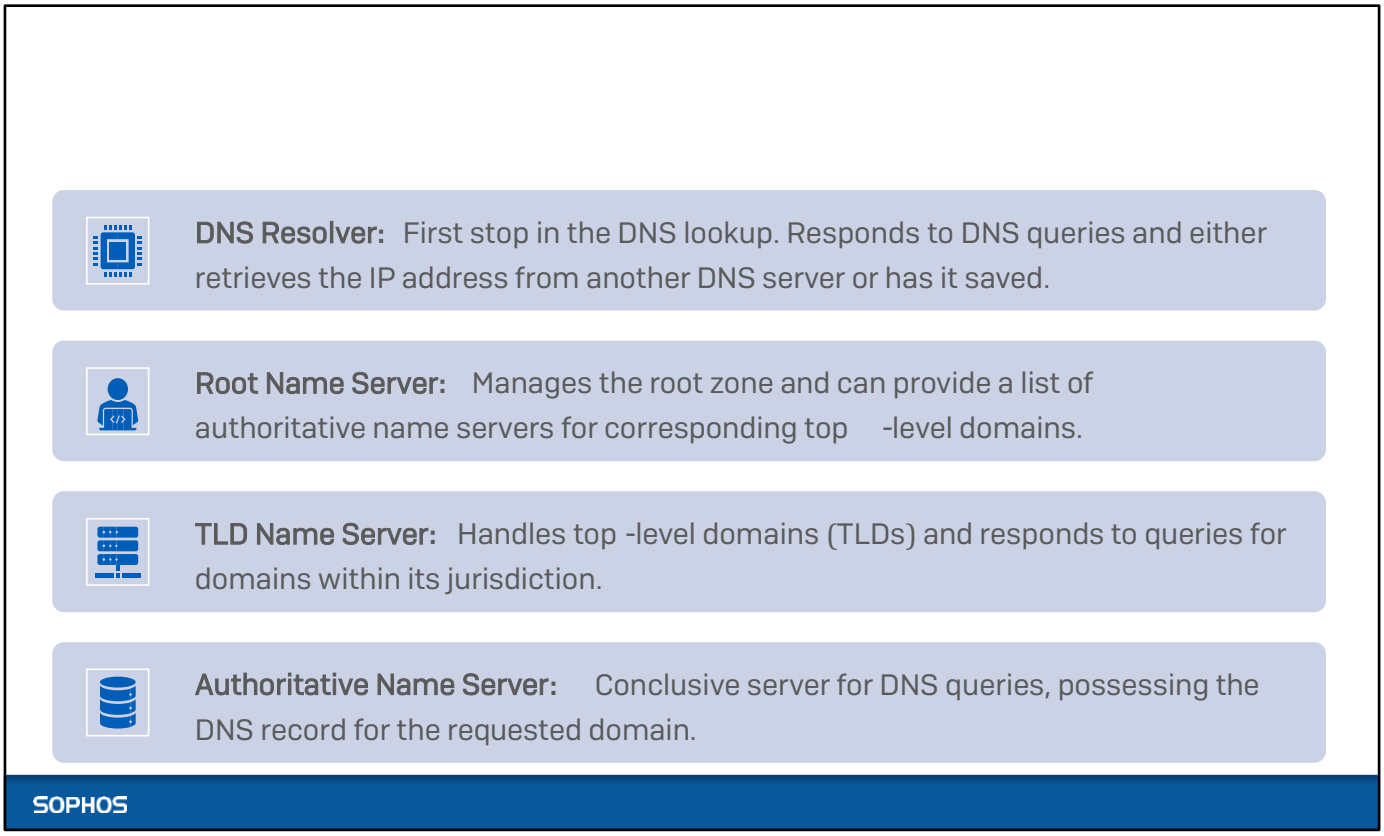
https://nipunsampath.medium.com/dns-for-dummies-cf73e1e261d0

How DNS works?

https://www.youtube.com/watch?v=wHeW0Am9u-Y&ab_channel=SophosSupport

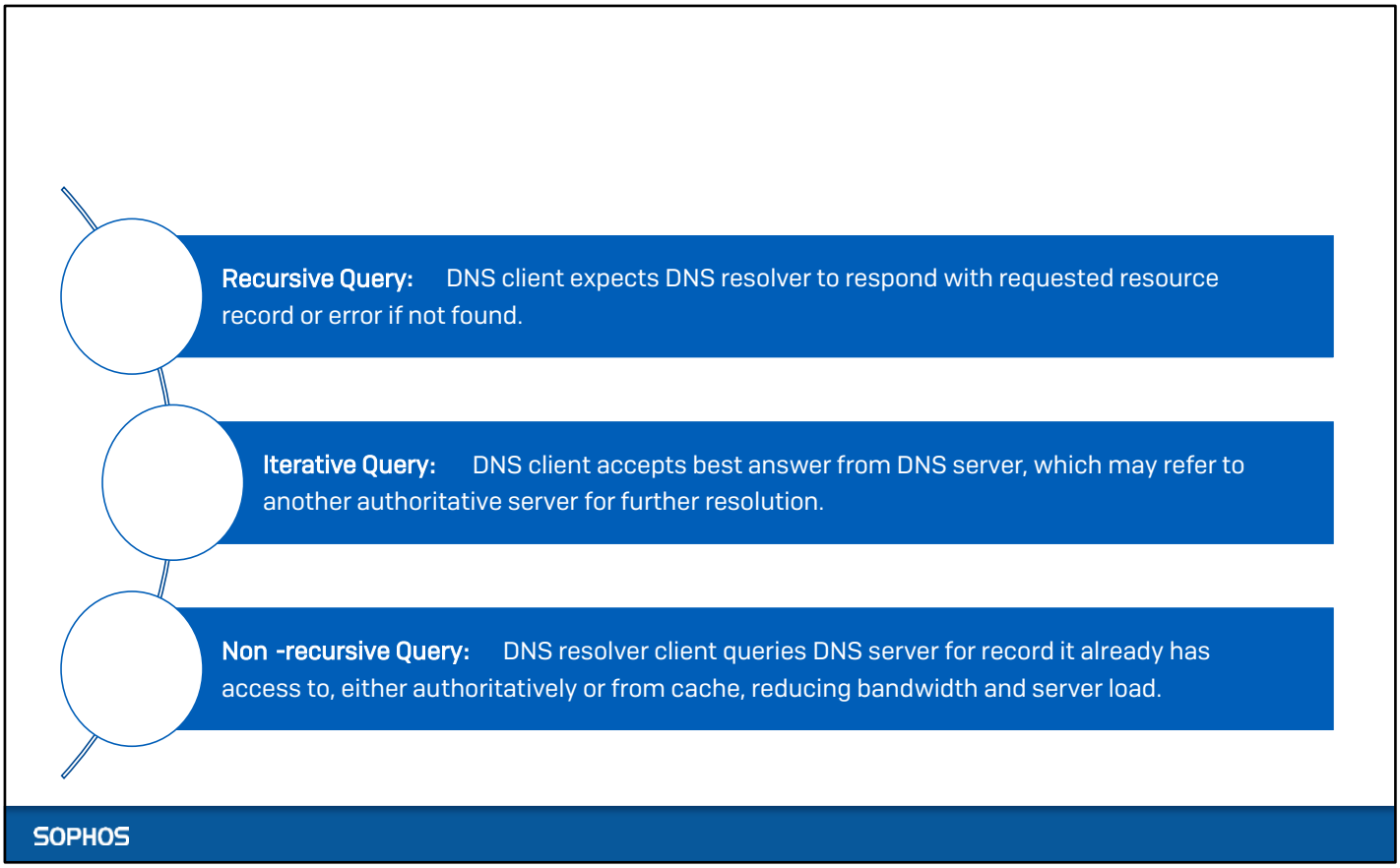
https://techvids.sophos.com/watch/JbNKDsjwo58noXN7p2tKgG

DNS Servers and Roles



- **DNS Resolver:** The DNS Resolver is the First stop in the DNS lookup process and the server that responds to a DNS query and asks another DNS server for the address, or already has the IP address for the site saved.
- **Root Name Server:** A root name server is the name server for the root zone. It responds to direct requests and can return a list of authoritative name servers for the corresponding top-level domain.
- **TLD Name Server:** The top-level domain server (TLD) is one of the high-level DNS servers on the internet. When you search for www.sophos.com, a TLD server for the '.com' will respond first, then DNS will search for 'Sophos.'
- **Authoritative Name Server:** The authoritative name server is the final stop for a DNS query. The authoritative name server has the DNS record for the request.

Types of DNS Queries



- Recursive Query - In a recursive query, a DNS client requires that a DNS server (typically a DNS recursive resolver) will respond to the client with either the requested resource record or an error message if the resolver can't find the record.
- Iterative Query - in this situation, the DNS client will allow a DNS server to return the best answer it can. If the queried DNS server does not have a match for the query name, it will return a referral to a DNS server authoritative for a lower level of the domain namespace. The DNS client will then make a query to the referral address. This process continues with additional DNS servers down the query chain until either an error or timeout occurs.
- Non-recursive Query - typically, this will occur when a DNS resolver client queries a DNS server for a record that it has access to either because it's authoritative for the record or the record exists inside of its cache. Typically, a DNS server will cache DNS records to prevent additional bandwidth consumption and load on upstream servers.

The importance of DNS in cybersecurity

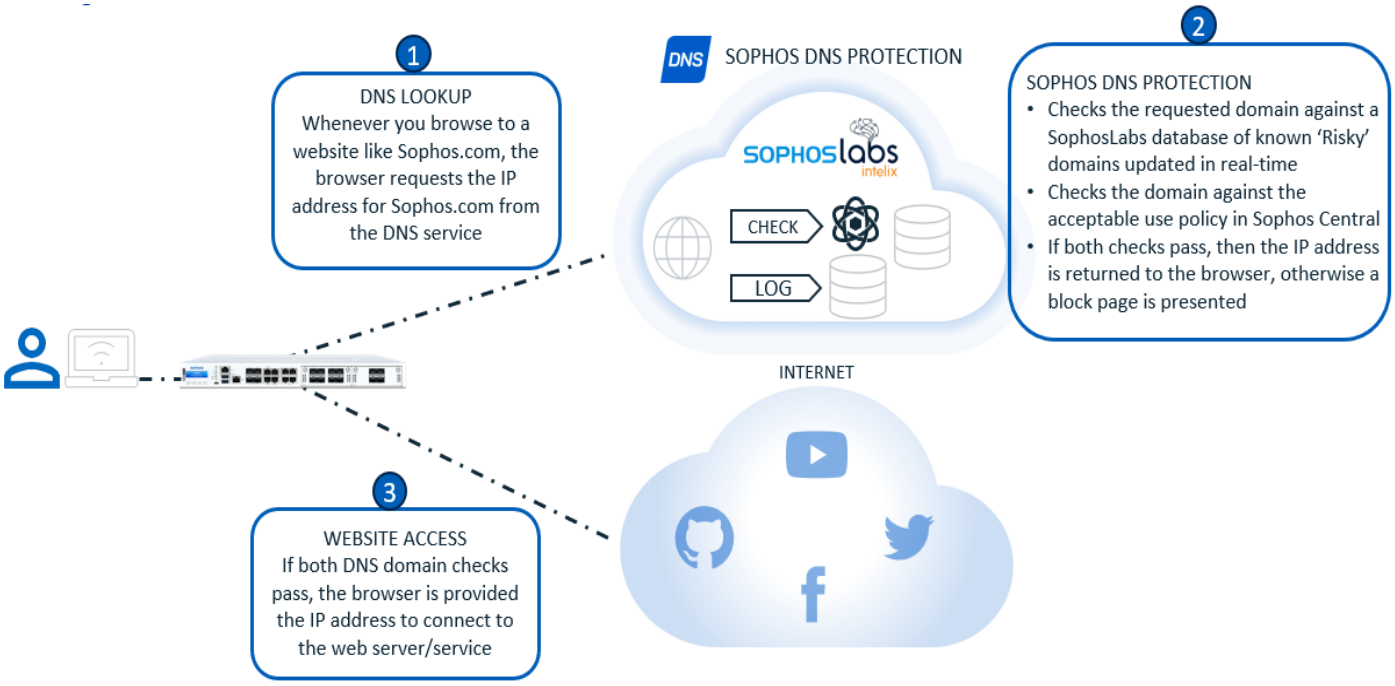
DNS plays a crucial role in cybersecurity due to several key factors:

1. Malware Protection
2. Phishing Prevention
3. Data Loss Prevention
4. Threat Intelligence
5. Incident Response
6. Content Filtering
7. DNS Security Extensions (DNSSEC)

SOPHOS

DNS (Domain Name System) is vital in cybersecurity due to several key factors:

1. Malware Protection: DNS blocks access to known malicious domains, preventing malware infections and communication with command-and-control servers.
2. Phishing Prevention: DNS filtering blocks access to phishing sites, safeguarding users from scams attempting to steal sensitive information.
3. Data Loss Prevention: DNS detects and blocks attempts to exfiltrate data, identifying and halting unauthorized data transfers.
4. Threat Intelligence: DNS traffic analysis helps identify security threats such as botnet activity, malware, or phishing campaigns.
5. Incident Response: DNS logs provide crucial information for incident response investigations, tracing attack origins and affected systems.
6. Content Filtering: DNS filtering enforces content policies, blocking access to inappropriate or non-work-related websites to maintain productivity and security. 7. DNS Security Extensions (DNSSEC): DNSSEC adds cryptographic authentication to DNS responses, preventing DNS spoofing attacks and ensuring data integrity and authenticity.



Sophos DNS Protection blocks access to unwanted web sites or services before the request is even made

Sophos DNS Protection

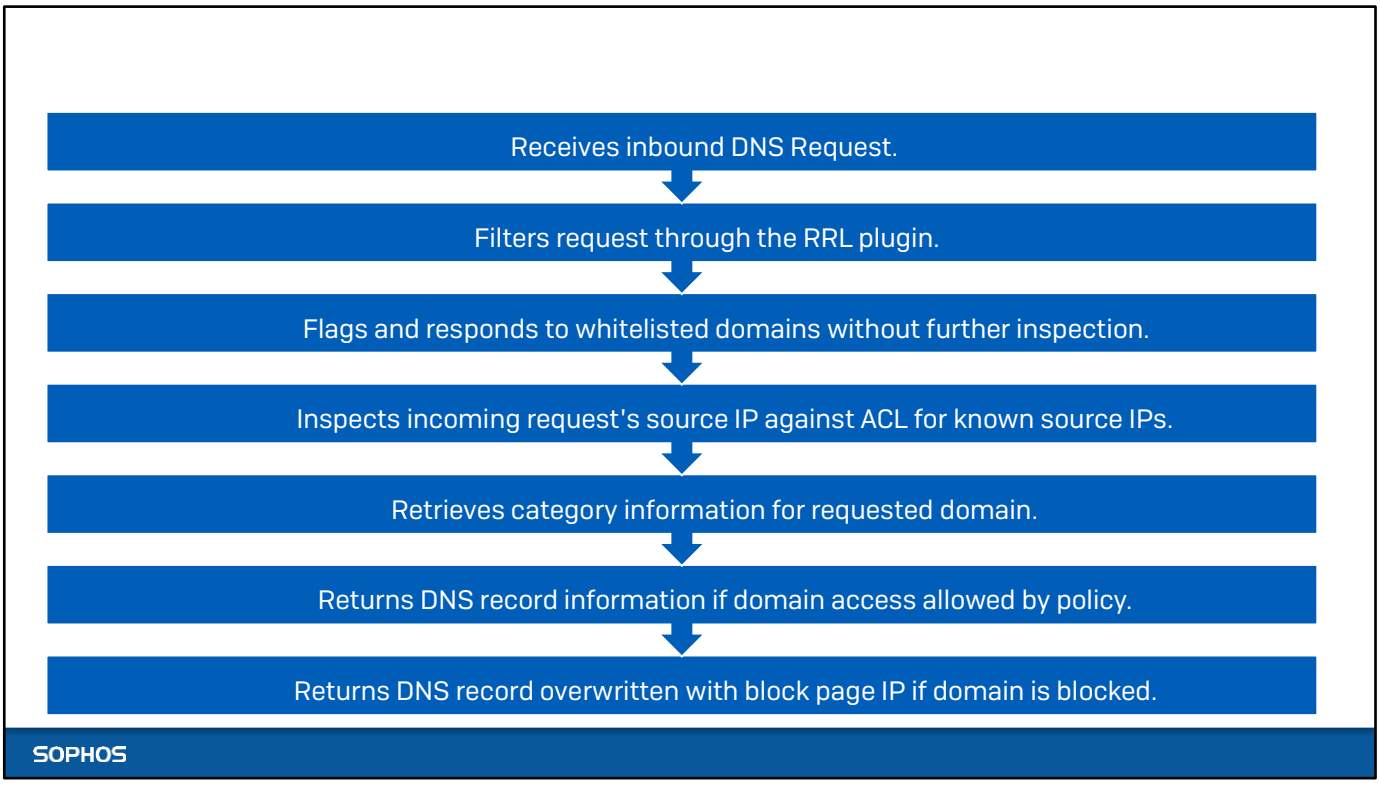
- Sophos DNS Protection is a security solution designed to safeguard networks by filtering DNS queries to block access to malicious or unwanted domains.
- It provides an additional layer of defence against threats by preventing users from accessing harmful websites.
- This service complements existing network security measures (Sophos as well as non-Sophos).
- It can be deployed instantly to enhance overall cybersecurity posture and ensure end users in corporate networks comply with corporate policies when accessing domains and sites on the internet.

Introduction to Sophos DNS

The Role of Sophos DNS Protection

Central Regions	Compatibility	SXL Categorization	A/AAAA Policy Enforcement
• Ireland (Eu-West) • Germany (Eu-Central) • United States (US-East & US-West)	• Works alongside Sophos Firewall and any 3rd parties.	• Same Categorization source as Sophos Firewall.	• Resolves all types of DNS Records. • Policy checks only apply to A, AAAA (Quad A), CNAME and HTTPS records.

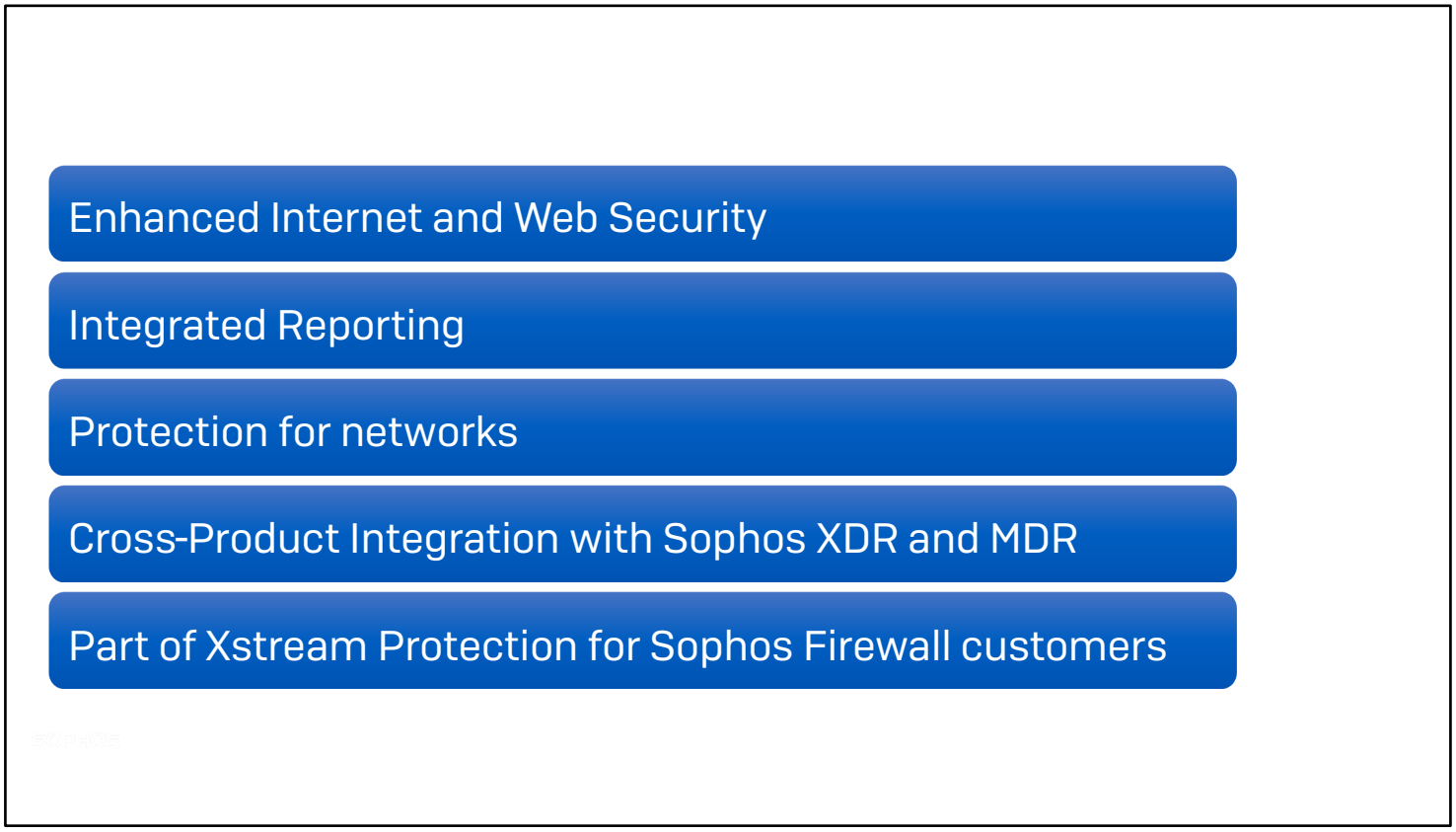
- Sophos DNS Protection is available in these regions: **EU-West (Ireland)**, **EU-Central (Germany)**, **US-East,** and **US-West**. If a customer's region is not supported, we can create a new account in one of the supported regions. However, data migration is currently not available.
- Sophos DNS Protection is backed by Sophos Labs' real-time threat intelligence, protecting the customers networks, sites and devices from malicious domain activity, and allowing them to enact policy for domain categories or domain lists.
- By using Sophos DNS Protection in place of existing public DNS resolver, customers can prevent any devices on their network from accessing domains associated with security threats and other unwanted websites controlled through policy.
- Deploying Sophos DNS Protection on a network protected by Sophos Firewall provides an additional layer of protection that ensures all protocols and ports are protected against accessing risky or inappropriate domains.
- Uses the same services as Sophos Firewall for website categorization, the SXL service.
- DNS Resolution resolvers all types of DNS records but protection policies are only applied on A, AAAA (Quad A), CNAME and HTTPS records.
- Protection policies are enforced based on the requested domain names. Although a DNS query typically seeks one host or domain name, the response may contain multiple 'records' necessary for translating the requested name into an IP address response. This could involve one or more 'CNAME' aliases. The important thing is that we base the policy decision on the originally requested domain, not on any of the CNAMEs that may be used as aliases to resolve, and where CNAMEs are involved, we do NOT apply policy based on the final A or AAAA record that resolves to the IP address. The HTTPS record is a specialized form of the Service Binding (SVCB) DNS record. These provide more detailed information compared to other record types (like A or AAAA) about the services available for a specific domain and play a crucial role in establishing secure network connections like HTTPS by providing essential information including communicating information about supported protocols and ports and can even specify alternate servers to which clients can connect.



DNS Query Resolution in DNS Protection

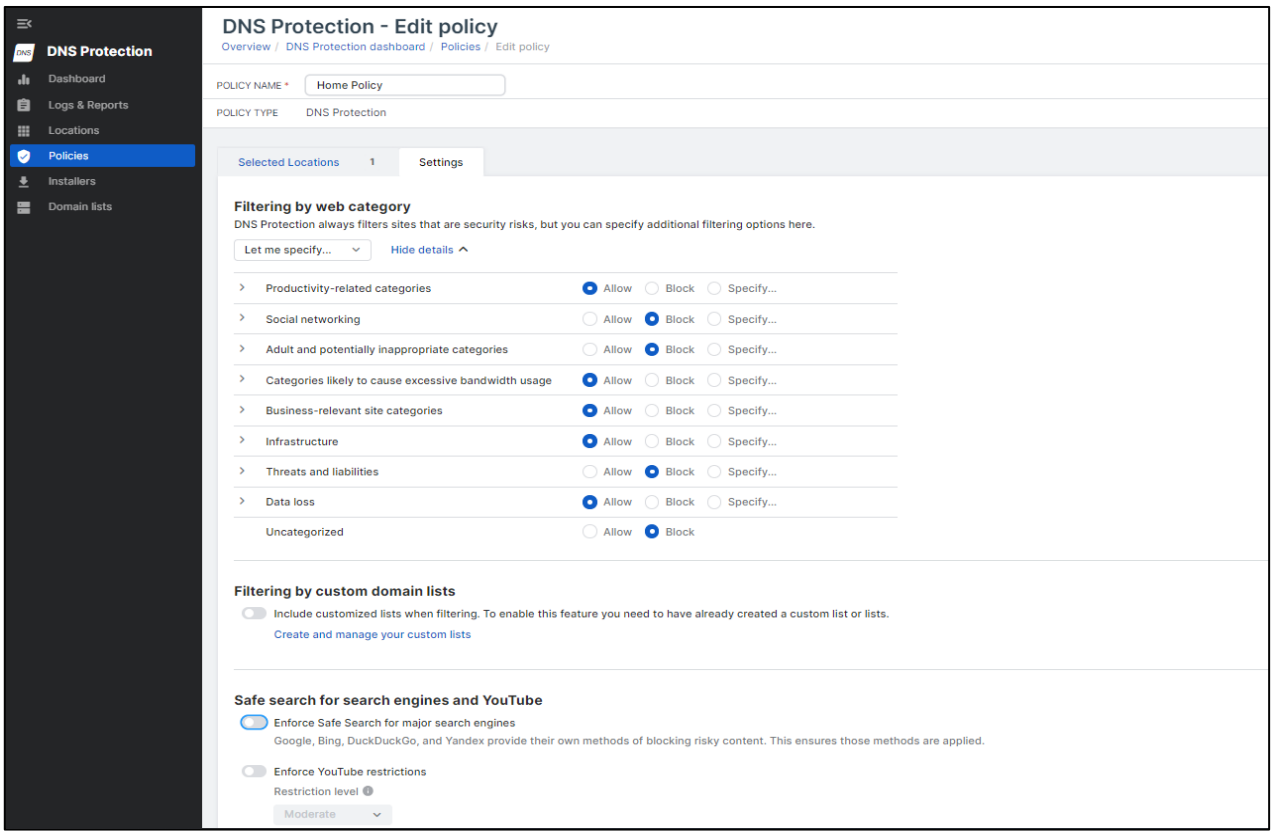
1. Receives inbound DNS Request.
2. Filters request thought Request Rate Limiter (RRL) plugin.
    a. If request count from current IP in last 15 seconds is greater than 200, request will be throttled.
3. If domain is whitelisted, request will be flagged and not be subjected to any further inspection and a response will be sent to the client.
4. Incoming request's source IP is inspected against an ACL to determine if the originating IP is in known source IP list.
    a. If IP is unknown, the request will be dropped. User may or may not be able to connect to the requested website depending on if a fallback DNS server is configured.
    b. If the IP is correctly mapped to a location, but no valid policies are associated with it, then default policy will be used for policy evaluation and only security risk sites/domains will be blocked.
    c. If the IP is mapped correctly to a location and has valid policies associated with it, the set of policies applicable for that particular source IP is retrieved and prepared for evaluation.
5. Next, the category information for the requested domain is retrieved.
    a. First, SXL cache is inspected and used. If not available, then request submitted to SXL backend.
    b. Response received from SXL backend will be cached for subsequent requests for same domain.
6. If the access to the particular domain is allowed by policy, the DNS record information is returned.
7. If the domain is blocked, an DNS record overwritten with the IP information of the block page is returned.

Key Features of Sophos DNS Protection



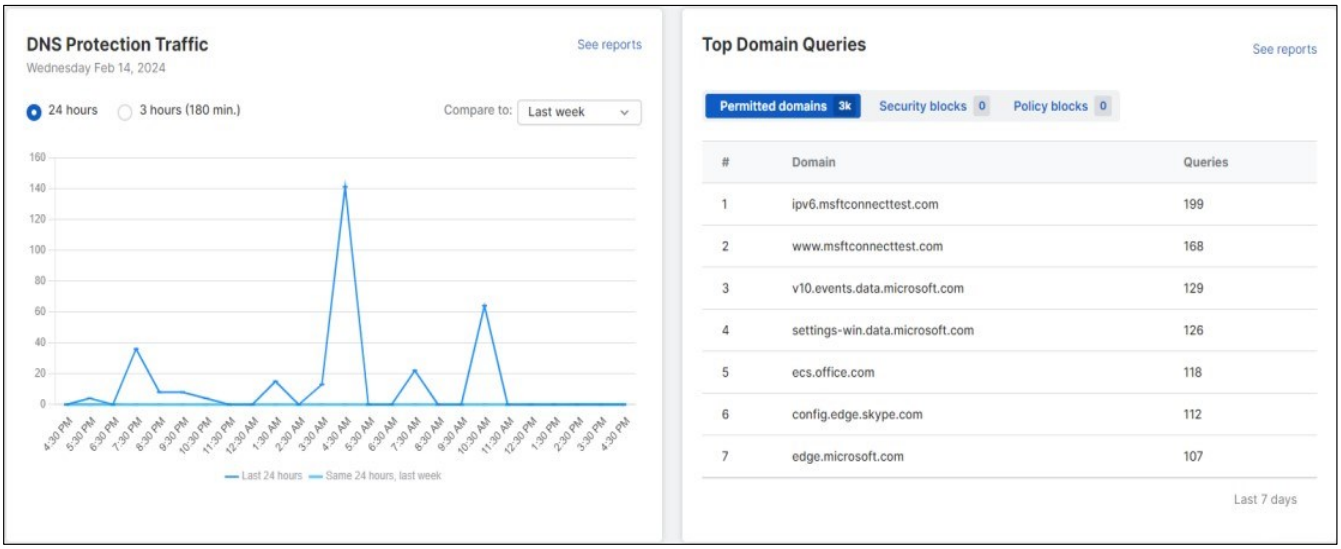
- Enhanced Internet and Web Security
- Integrated Reporting
- Protection for networks
- Cross-Product Integration with Sophos XDR and MDR
- Part of Xstream Protection bundle for Sophos Firewall customers at no extra cost.

Enhanced Internet and Web Security



- **Enhanced Security**: Sophos DNS Protection adds an extra layer of security by blocking access to unsafe and unwanted domains.
- **Complementary Tool**: It works alongside existing network security tools, enhancing their capabilities without disrupting established policies, whether Sophos or non-Sophos.
- **Instant Deployment**: Offers quick deployment, strengthening security without extensive setup, ensuring timely protection.
- **Centralized Management**: Administrators can easily configure and enforce security policies across all devices and endpoints using Sophos Central.
- **Visibility and Control**: Provides real-time visibility into DNS traffic, enabling proactive threat mitigation and granular control over content filtering policies.
- **Scalability**: Adaptable to organizations of all sizes, accommodating changes in network size, user base, and security needs.

Integrated Reporting

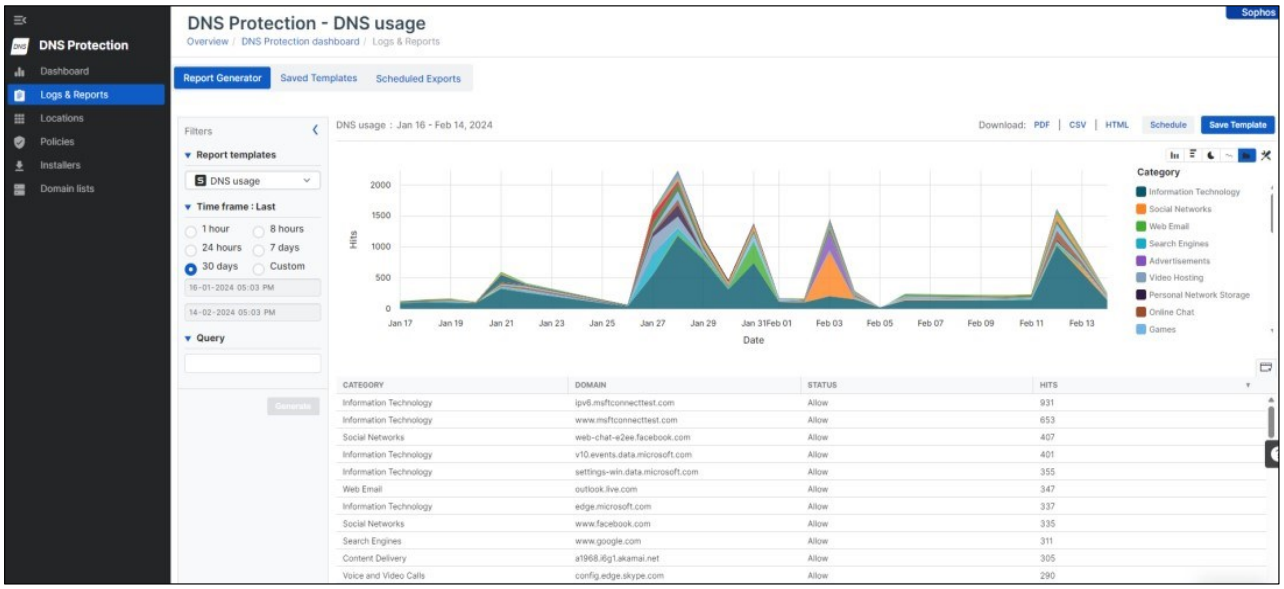


Extensive reporting is included in Sophos Central with log integration into the XDR/MDR data lake

SOPHOS

- Sophos DNS Protection provides in-depth visibility into the domains visited from the customers network with comprehensive dashboarding and reporting.
- DNS Protection reports start out with one simple report template providing detail on the domains queries seen from the customers Locations.
- Data columns can be added or removed as required, and the grouping and totals in the reports will automatically update to suit the selected columns.
- There is also an option to choose from several different chart types to illustrate the data.
- No separate license is required to access the Reporting information.
- Up to three months of logging and reporting information will be stored.
- Reports and logs will be on per location basis and not per user basis.
- Reports stored will contain data for all locations including the recently deleted locations for up to three months.

Integrated Reporting (cont.)



The reports feature enables automatic creation of filters by clicking on relevant data or interactively selecting fields to b uild filter logic.

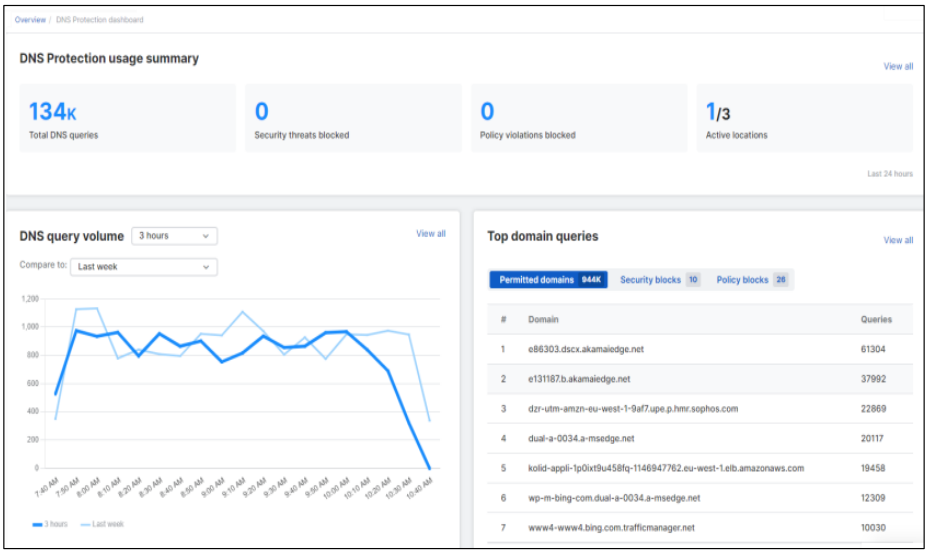
SOPHOS

- The reports also allow to create filters - either automatically by clicking on the data that needs to be focused on, or interactively by selecting fields and building filter logic.
- Reports is still a work in progress so you may find some data is not yet available. In a later update, the ability to save report templates and run scheduled report jobs will be added.

The Dashboard

The Dashboard Displays:

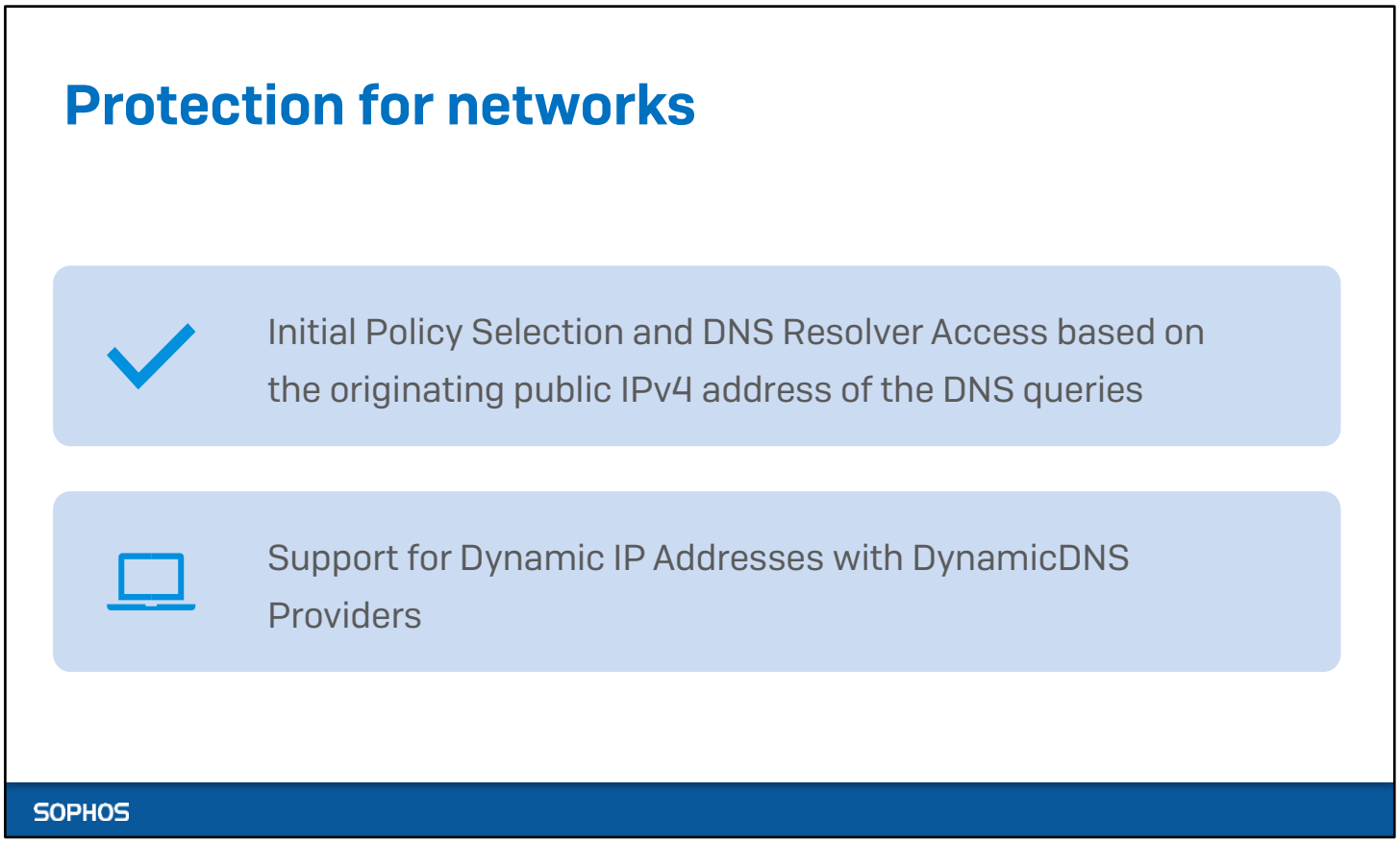
- DNS Traffic Generation
- Timeline Chart
- Table Data



SOPHOS

- A summary of DNS traffic generated under the customer account, security threats blocked, policy violations blocked and active and total added locations.
- Clicking on the 'Active locations' counter will take you to a report highlighting the DNS traffic counts per location.
- Timeline chart displaying query volume over the past 3 or 24 hours or 30 days and option to compare with statistics from last week or last month (last 4 weeks).
- Table presenting query counts and top domains for:
    1. Allowed queries.
    2. Queries blocked for security reasons.
    3. Queries blocked by customer policy.

Protection for networks



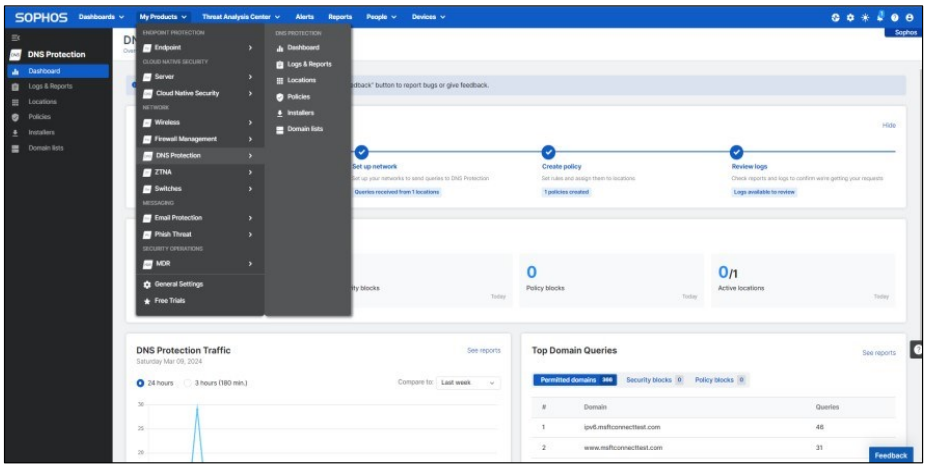
- Initially, policy selection and access to the DNS Resolver will be based on the originating public IPv4 address of the DNS queries. Hence, protecting individual devices that move from network to network (or site to site) will not be possible.
- Dynamic IP addresses are supported when used with a DynamicDNS provider.

Note: In future, we plan to integrate an agent with the endpoint, providing DNS protection and other network-oriented security services for roaming devices, wherever they are.

Cross-Product Integration with Sophos XDR and MDR

Sophos DNS Protection's log data and intelligence is shared with Sophos data lake for Sophos XDR and MDR threat-hunting analysts to help detect active adversaries and threats operating on the network.

Licensing Requirements:



- The initial release of DNS Protection is being added to our Xstream Protection bundle
- DNS Protection to be configured via Sophos Central.

SOPHOS

Included at No Extra Charge for Sophos Firewall customers with Xstream Protection

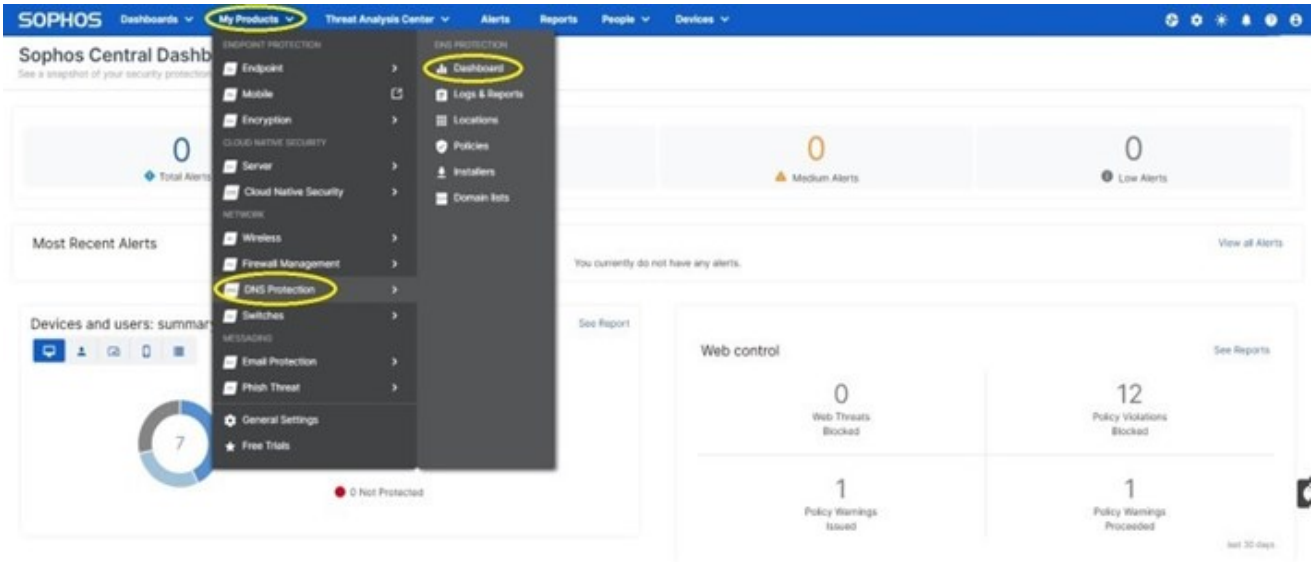
- The initial release of DNS Protection is being added to our Xstream Protection bundle. This price is included and comes at no extra cost.
- Customers are required to have a Sophos Central account to configure DNS Protection.

Module 2: Deploying Sophos DNS Protection

Once you complete this module you will be able to:

- Set up DNS Protection
- Learn about Locations in DNS Protection
- Learn about DNS Resolvers
- Learn about Policies and other options in DNS Protection

Set up DNS Protection



A location can be defined by specifying the IP address from where the network's traffic originates from, the IP address of router's WAN interface.

Since we work in a closed resolver model with the Sophos DNS Protection service, we do not serve to any DNS requests from unknown locations (IP addresses) or locations that have not yet been added by the customer to his Central account, with the exception being that the location/IP address is whitelisted.

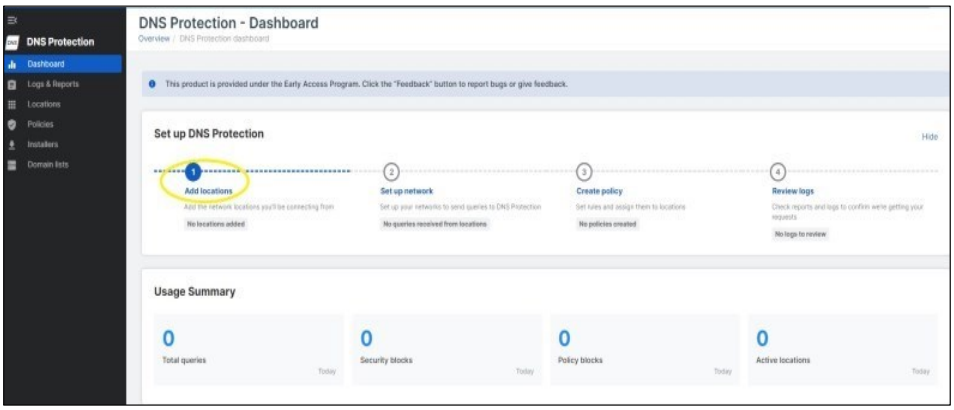
To set up DNS Protection, you must do as follows <DEMO>:

1. Add locations you want to protect.
   https://doc.sophos.com/central/customer/help/enus/ManageYourProducts/DNSProtection/Locations/
   - To add a location, specify the external or public IP address or FQDN used for traffic going to the internet. This may be the address of the internet firewall or router.
2. Set up your network.
   https://doc.sophos.com/central/customer/help/enus/ManageYourProducts/DNSProtection/NetworkSetup/
   - The two DNS Resolver IP addresses used are 193.84.4.4 and 193.84.5.5
   - Will have to be configured based on the customers topology. (See slide - Configuring DNS Resolver Addresses)
   - Download and install the DNS Protection root certificate on all devices.
   - Check your configuration

1. Add policies.
   https://doc.sophos.com/central/customer/help/enus/ManageYourProducts/DNSProtection/Policies/

- Policies can be added to allow or block access to website categories and domains for all locations that have been added under DNS Protection.

Locations



- Locations must be added to Sophos Central.
- Used to identify customer's networks.
- All networks that need to be protected must be added.
- Multiple networks can be added to the same location or have them split into separate locations.
- Takes around 30 seconds to sync new location information with the data plan.
- Maximum 50 locations can be added with maximum 100 items per location.

***Note** : DNS Protection only accepts requests when they originate from configured locations.*

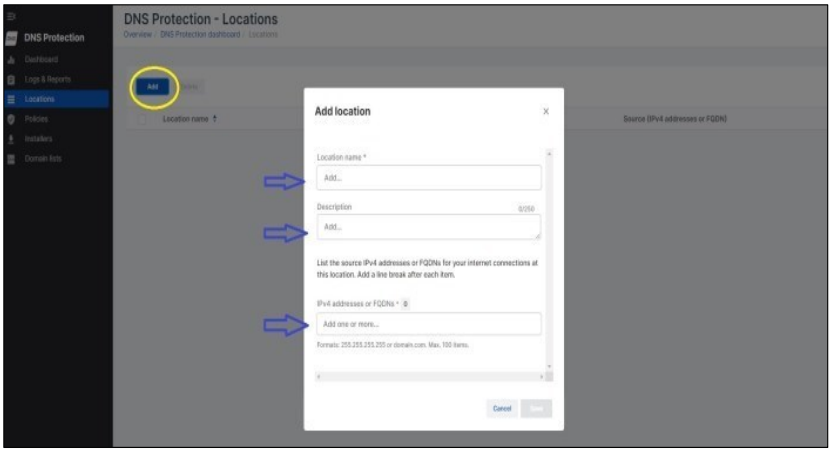
SOPHOS

- To allow networks to access DNS Protection and define policies, locations must be added to Sophos Central.
- DNS Protection uses locations to identify DNS requests from the organization's networks.
- Add all the deployment regions that need to be protected as locations.
- Multiple networks can be added to the same location or have them split into separate locations.
- When a new location is added, it will take around 30 seconds to sync with the Data Plane and allow the customer to access the DNS Resolvers.
- A maximum of 50 locations can be added for a Central account for DNS Protection, with a maximum of 100 items including individual IP addresses and FQDN's that resolve to a single IP address can be added to each individual location.

Note:

DNS Protection service will only process and respond to DNS Requests coming from IP addresses configured as locations in the customers Sophos Central account.
DNS Requests received from non-listed addresses will be ignored by the DNS Protection service.

Locations (Cont.)



- Click Add after selecting Add locations on the previous page.
- Add a name for the location.
- Add description (optional).
- Add individual IPv4 addresses or FQDN's separated by a comma.

Note 1 *: The IP addresses/FQDN to be added must be the public/egress IP addresses and not the local/ LAN addresses.*

Note 2 *: Max 100 items can be added per location.*

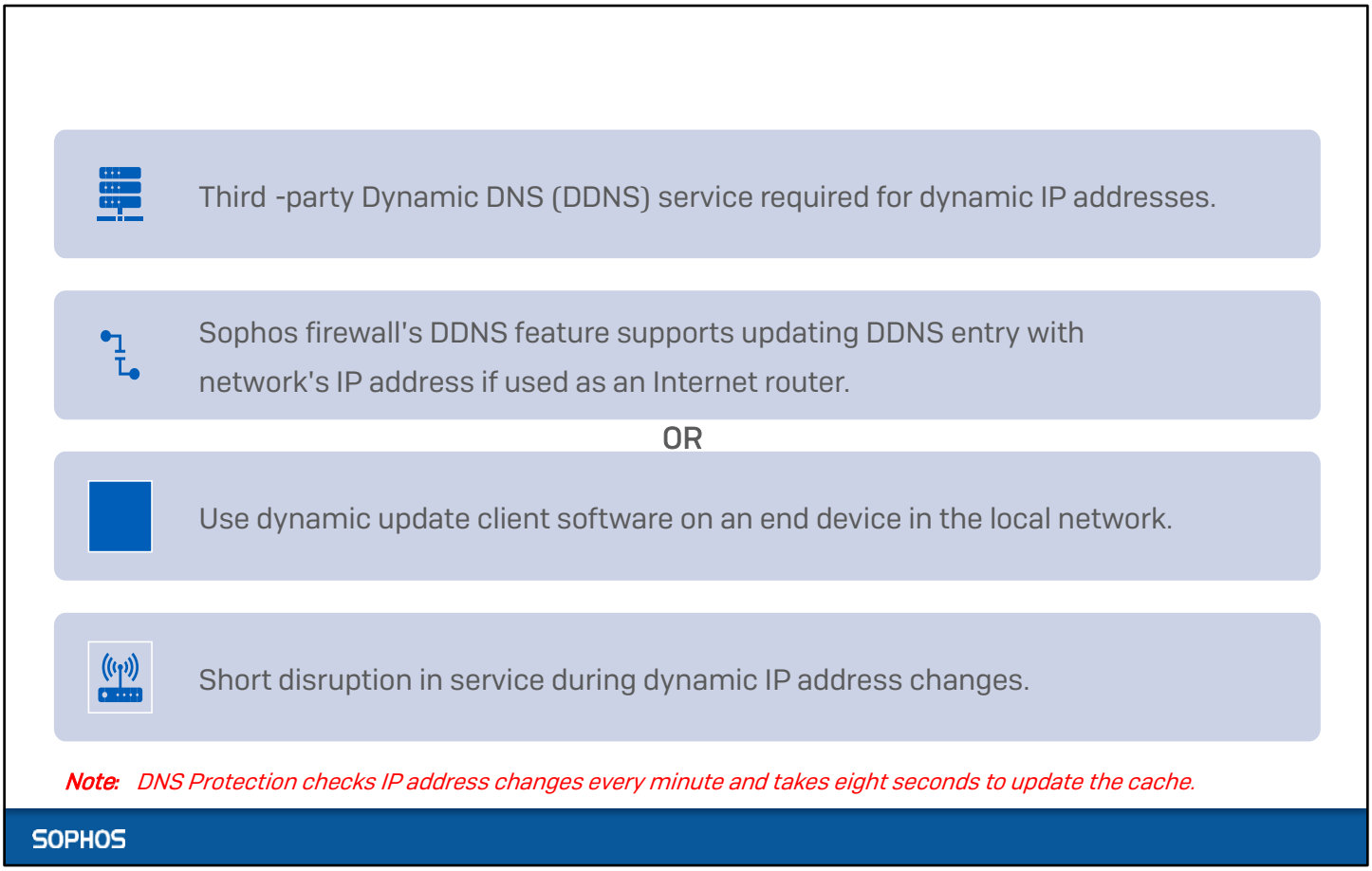
SOPHOS

- Click Add after selecting Add locations on the previous page.
- Add a name for the location.
- Add description (optional).
- Add individual IPv4 addresses or FQDN's separated by a comma.

Note:

1. **The IP addresses/FQDN to be added must be the public/egress IP addresses and not the local/ LAN addresses.**
2. **Max 100 items can be added per location.**

Dynamic Address



If a customer is being allocated his address dynamically by the ISP, then he can still use DNS Protecting using a third-party Dynamic DNS service (DDNS).
If a Sophos Firewall (or any DDNS supporting device, not just firewall) is being used as the edge router, then the DDNS feature of the firewall can be used to keep DDNS entry up to date with the network's IPaddress.
https://docs.sophos.com/nsg/sophos-firewall/20.0/help/enus/webhelp/onlinehelp/AdministratorHelp/Network/DynamicDNS/NetworkDyna micDNSProviderAdd/index.html

If edge device does not support DDNS then any DDNS update client software will have to be installed on a computer in the local network.
This software communicates with the dynamic DNS service provider anytime the IP addresses provided by the ISP is updated, and the dynamic DNS provider in turn updates the DNS with those changes, providing almost instant updates.
When a dynamic IP address changes, users may lose access for some time. This time depends on how long the DDNS service takes to update the IP address and how long DNS Protection takes to check the IP address changes.

Note: DNS Protection checks IP address changes every minute and takes eight seconds to update the cache.

DDNS Services supported by DNS Protection:

- DynDNS
- DynAccess
- EasyDNS
- ZoneEdit
- Google DDNS
- Namecheap
- DNS-O-Matic
- No-IP
- FreeDNS
- Cloudflare

Dynamic DNS (DDNS) services facilitate the mapping of dynamic IP addresses to domain names, enabling remote access to devices or services hosted on networks with changing IP addresses. Here's a brief description of the DDNS providers supported by DNS Protection:

DynDNS: A widely used DDNS service offering reliable dynamic DNS solutions for individuals and businesses.

DynAccess: A DynDNS service providing remote access to network devices, allowing users to manage and control their infrastructure securely.

EasyDNS: A user-friendly DDNS provider offering seamless domain management and DNS services with robust security features.

ZoneEdit: A DDNS service that provides flexible DNS management solutions for businesses and individuals, ensuring reliable access to network resources.
Google DDNS: A dynamic DNS service provided by Google, offering simple and efficient DDNS solutions integrated with Google Cloud Platform services.

Namecheap: A popular domain registrar offering DDNS services, providing users with reliable and cost-effective dynamic DNS solutions.

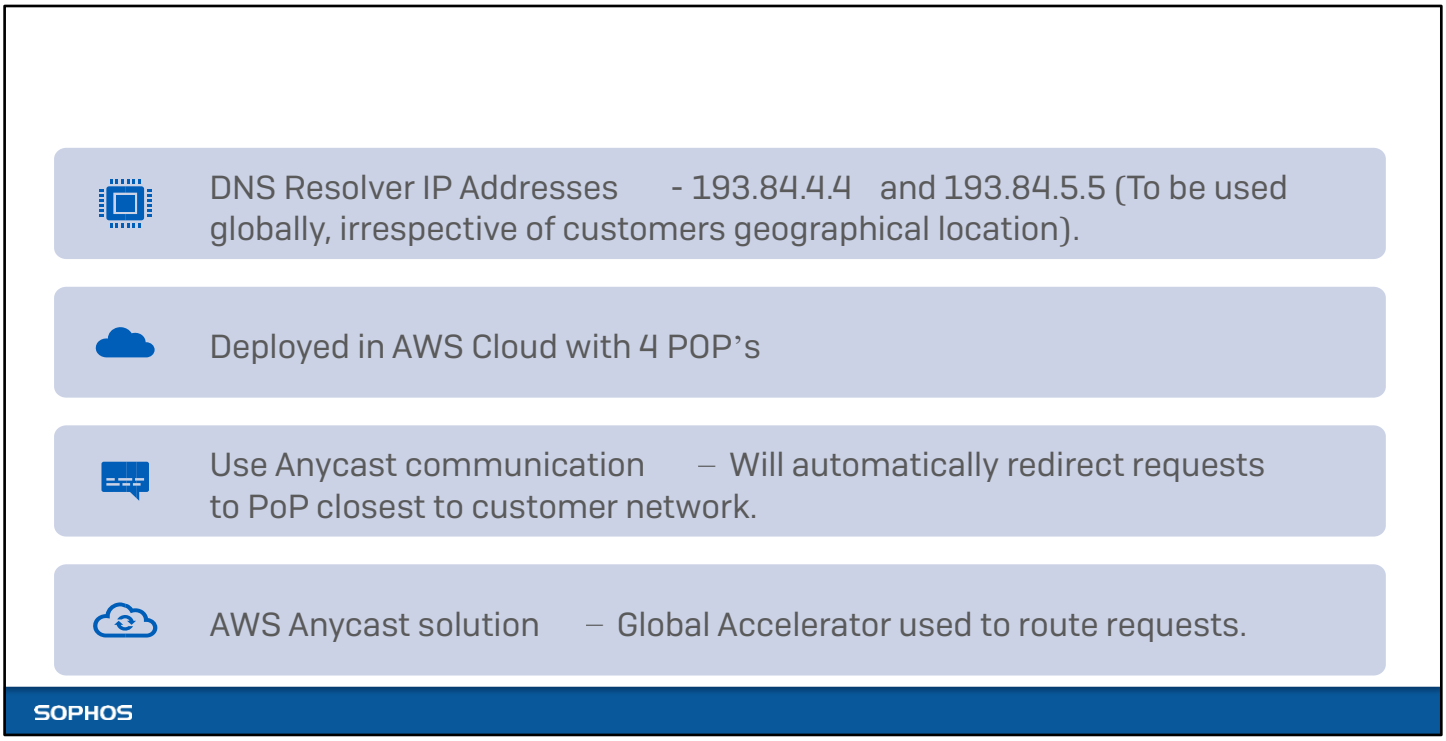
DNS-O-Matic: A dynamic DNS management platform that allows users to update multiple DDNS providers simultaneously, simplifying DNS management tasks.

No-IP: A leading DDNS service provider offering easy-to-use dynamic DNS solutions for remote access and network management.

FreeDNS: A free dynamic DNS service offering basic DDNS functionality for individuals and small businesses, allowing them to map dynamic IP addresses to domain names.

Cloudflare: A globally recognized DDNS provider offering advanced DNS management and security solutions, including DDoS protection and content delivery network (CDN) services.

DNS Resolvers



Currently, two DNS Resolvers addresses of 193.84.4.4 and 193.84.5.5 are required to be configured as the Primary and Secondary DNS resolvers in the customers environment.
Where this is done will depend on the customers topology. (See next slide) •This service is currently being hosted on AWS Cloud with 4 Point-of-Presence (POP's) globally:

- us-west-2 (Oregon)
- us-east-2 (Ohio)
- eu-central-1 (Frankfurt)
- ap-south-1 (Mumbai)

Adding additional POP's will be considered based on the popularity of this service. IPv6 Anycast method of communication is used to route requests from customer networks to the nearest POP automatically.

We use AWS Anycast solution called Global Accelerator to handle routing request coming from customer networks to the closest data plane POP.

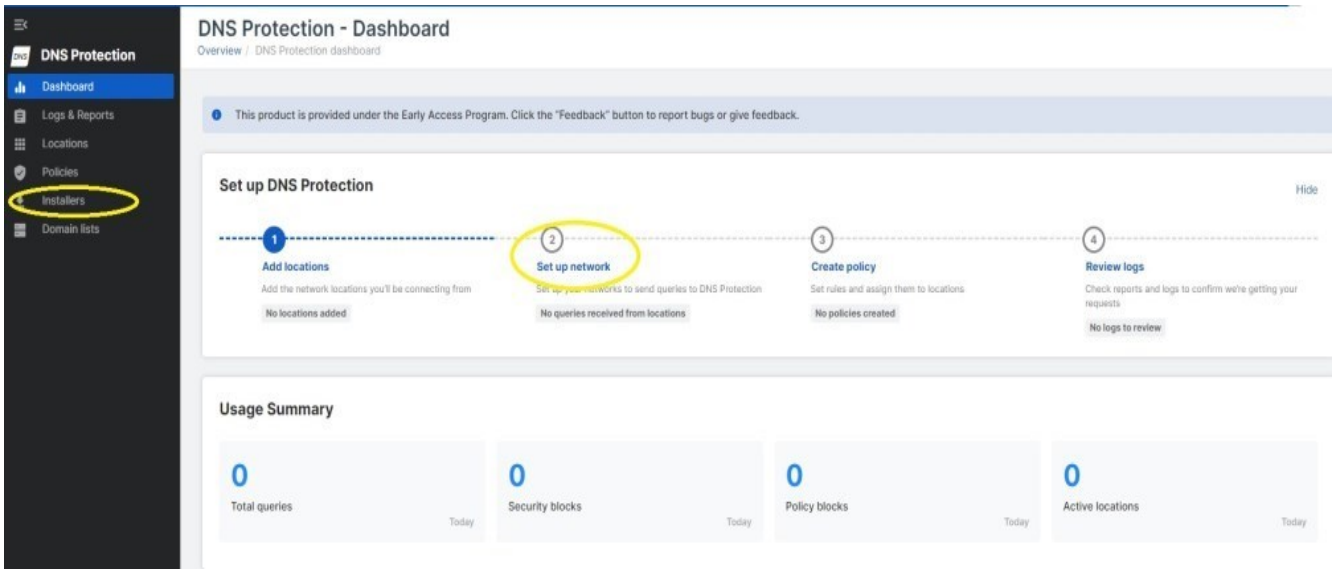
AWS Global Accelerator is used to route requests to Network Load Balancer of their closest region. *https://docs.aws.amazon.com/globalaccelerator/latest/dg/introduction-how-it-works.html*
All customers will be provided with the same two static public IP addresses regardless of where they are located. Global Accelerator will then look after routing requests. If one region goes becomes unhealthy Global Accelerator will detect that the health of that region is not good and direct requests to healthy regions.

Click "Set up network" or "Installers" option to proceed further.

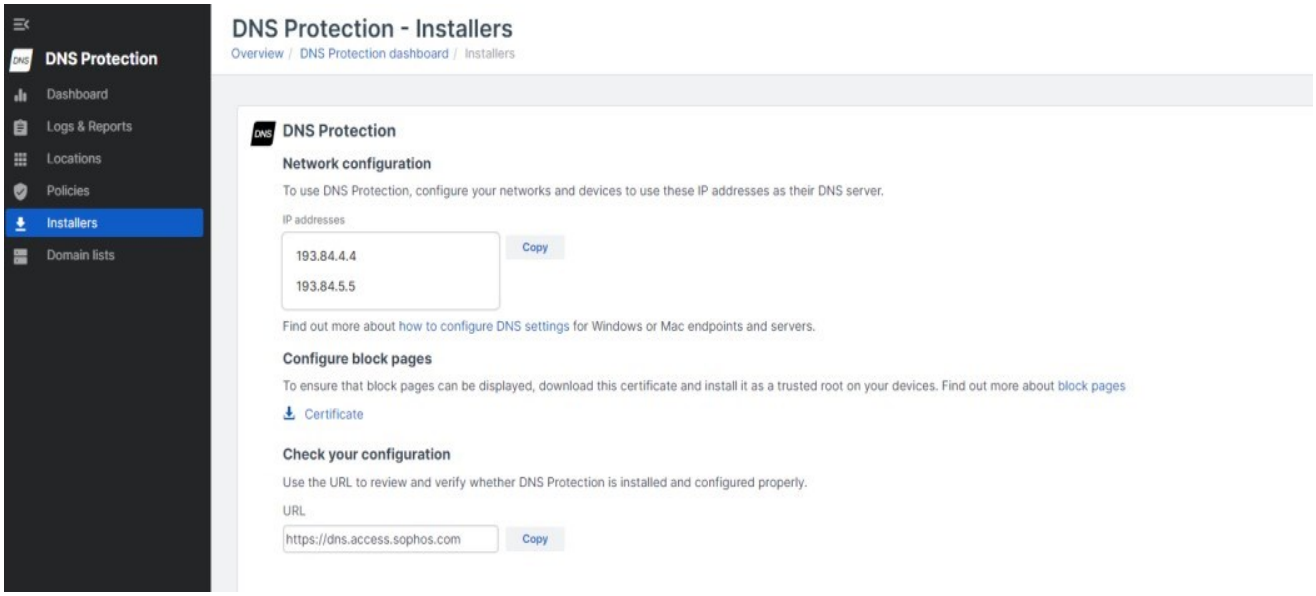
DNS Resolver Addresses

- To set up your network to use DNS Protection, you must update the configuration of your network or devices to ensure that DNS requests are resolved using the DNS Protection IP addresses

- You must set up the network at every location you add to DNS Protection.

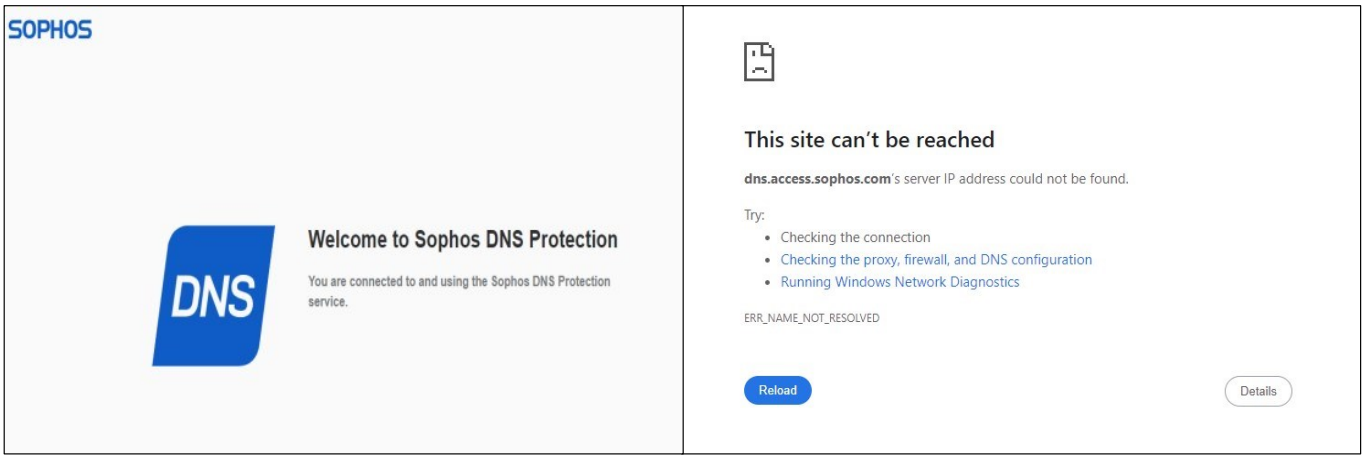


Click “Set up network” or “Installers” option to proceed further.



DNS Protection root certificate

- To ensure the users see block pages, the DNS Protection root certificate must be installed on the users' devices. This is because, when DNS Protection blocks a webpage requested from a customer's location, the Blocked Page presented in the user's browser will be sent by Sophos servers.
- Install the root certificate on Windows devices - https://abnloctrans1.green.sophos/doc/central-customer/bugfix/DOC-6675/enUS/ManageYourProducts/DNSProtection/NetworkSetup/InstallRootCertificateOnWindows/
- Install the root certificate on Mac devices - https://abnloctrans1.green.sophos/doc/central-customer/bugfix/DOC-6675/enUS/ManageYourProducts/DNSProtection/NetworkSetup/InstallRootCertificateOnMacDevices/
- If a Sophos Firewall with SSL/TLS Inspection is in use, then upload the HTTPS scanning CA certificate from the firewall to the user's devices.
- Sophos Firewall: Install the SSL CA certificate - https://support.sophos.com/support/s/article/KB-000035645?language=en_US



***Note** : Also requires the DNS Protection Root Certificate to be installed correctly to have the 'Welcome Page' displayed.*

SOPHOS

Check your configuration

To check your DNS Protection configuration, do as follows:

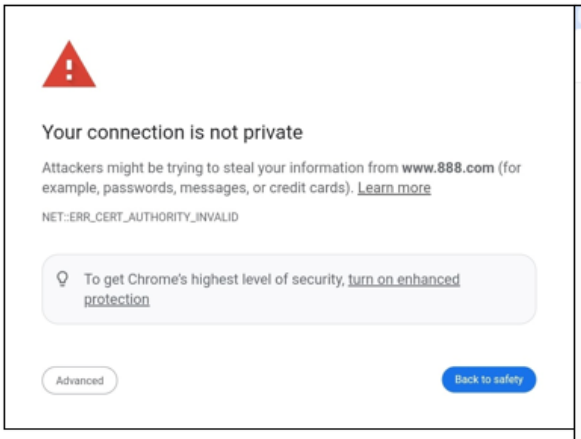
1. Go to **DNS Protection** > **Installers**.
2. Under **Check your configuration**, click **Copy** next to **URL**.

In a web browser, type the URL you copied.

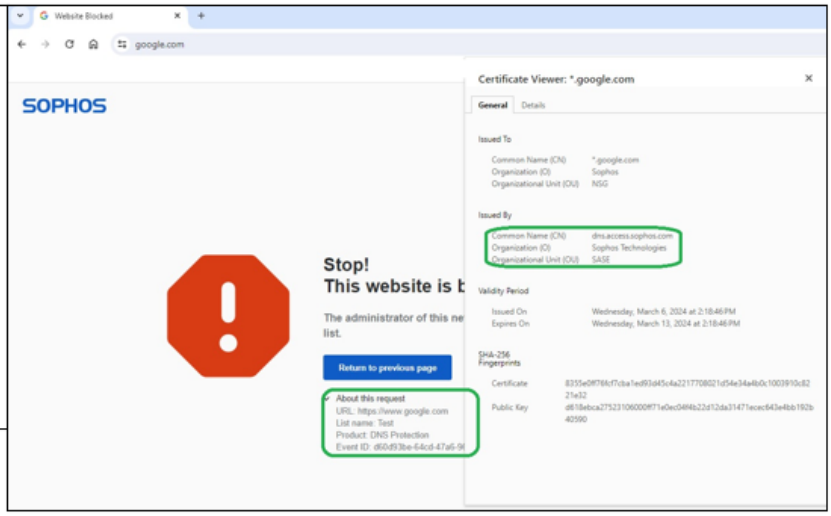
- If you see the welcome message, you've configured DNS Protection correctly.
- The Error message indicates that either incorrect addresses/URL is configured in "Locations" in Central or the local DNS servers/ endpoints are not using the Sophos DNS Resolvers.

Note: For the 'Welcome Page' to be displayed correctly, it is also required that the DNS Protection Root Certificate is installed correctly, or it will result in a browser generated 'Insecure Site' warning because the DNS Protection Root Certificate is not trusted.

DNS Protection root certificate



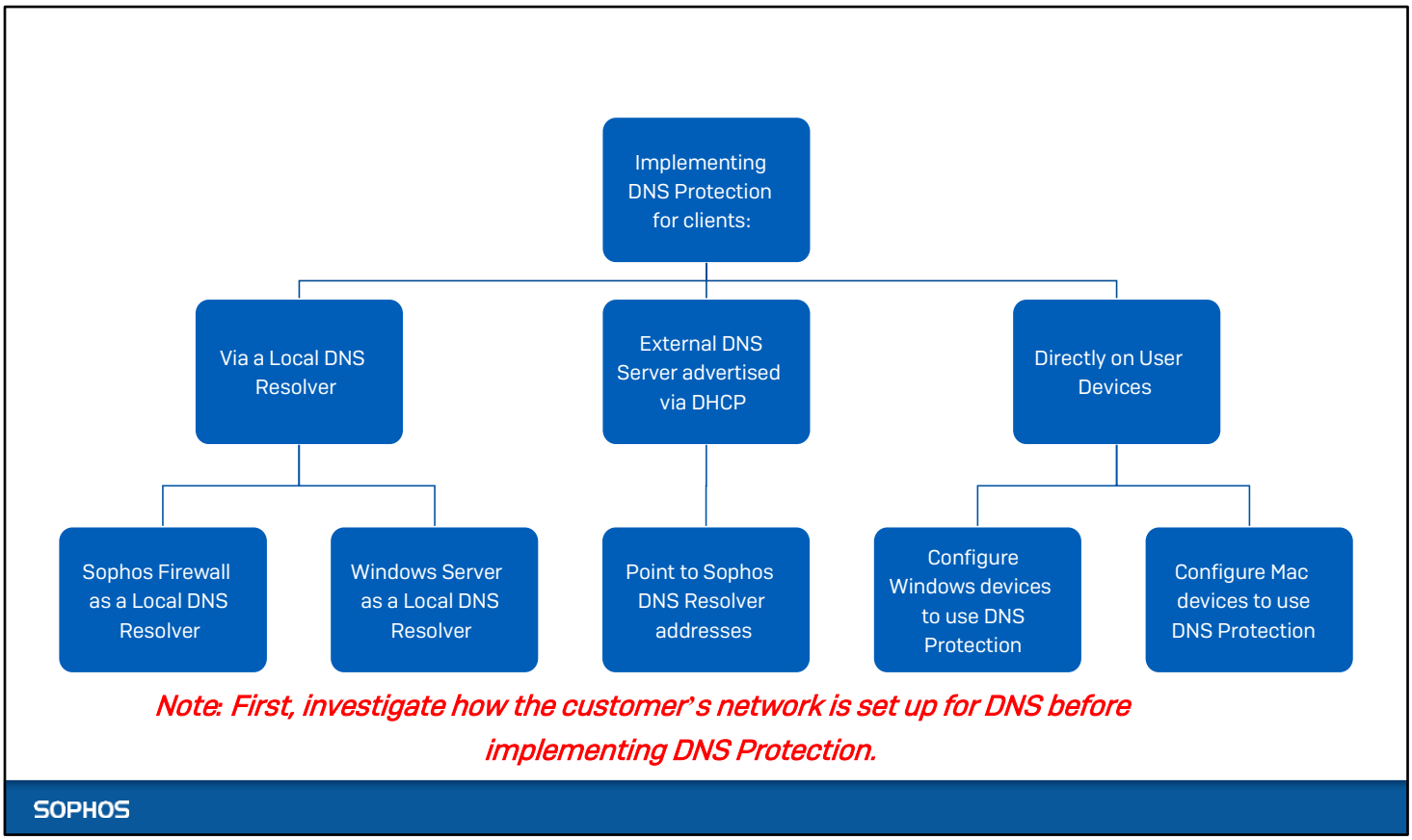
Block Page when the certificate is not installed.



When access is blocked due to a policy block and the certificate information.

When a user attempts to access any malicious or blocked website, they will receive a blocked page that is signed using our own self-signed certificate chain and hence this certificate will need to be trusted by the clients' devices beforehand.

- To ensure the users see block pages, the DNS Protection root certificate must be downloaded from the DNS Protection Set Up page from Sophos Central and installed on the users' devices.
- For Windows Devices - https://doc.sophos.com/central/customer/help/enus/ManageYourProducts/DNSProtection/NetworkSetup/InstallRootCertifica teOnWindows/
- For Mac Devices - https://doc.sophos.com/central/customer/help/enus/ManageYourProducts/DNSProtection/NetworkSetup/InstallRootCertifica teOnMacDevices/
- If a Sophos Firewall with SSL/TLS Inspection is in use, then upload the HTTPS scanning CA certificate used in the firewall to the user's devices.
- https://support.sophos.com/support/s/article/KB000035645?language=en_US



Configuring your network to use DNS Protection

Implementing DNS Protection for clients:

- Via a Local DNS Resolver
- Sophos Firewall as a Local DNS Resolver – *https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/DNSProtection/NetworkSetup/ConfigureSophosFirewallToUseDNSProtection/index.html*

- This can also include a Sophos AP6 access point that is receiving its DNS configuration from a firewall and then publishes this to the end devices that connect to the Wi-Fi networks broadcasted by that AP.

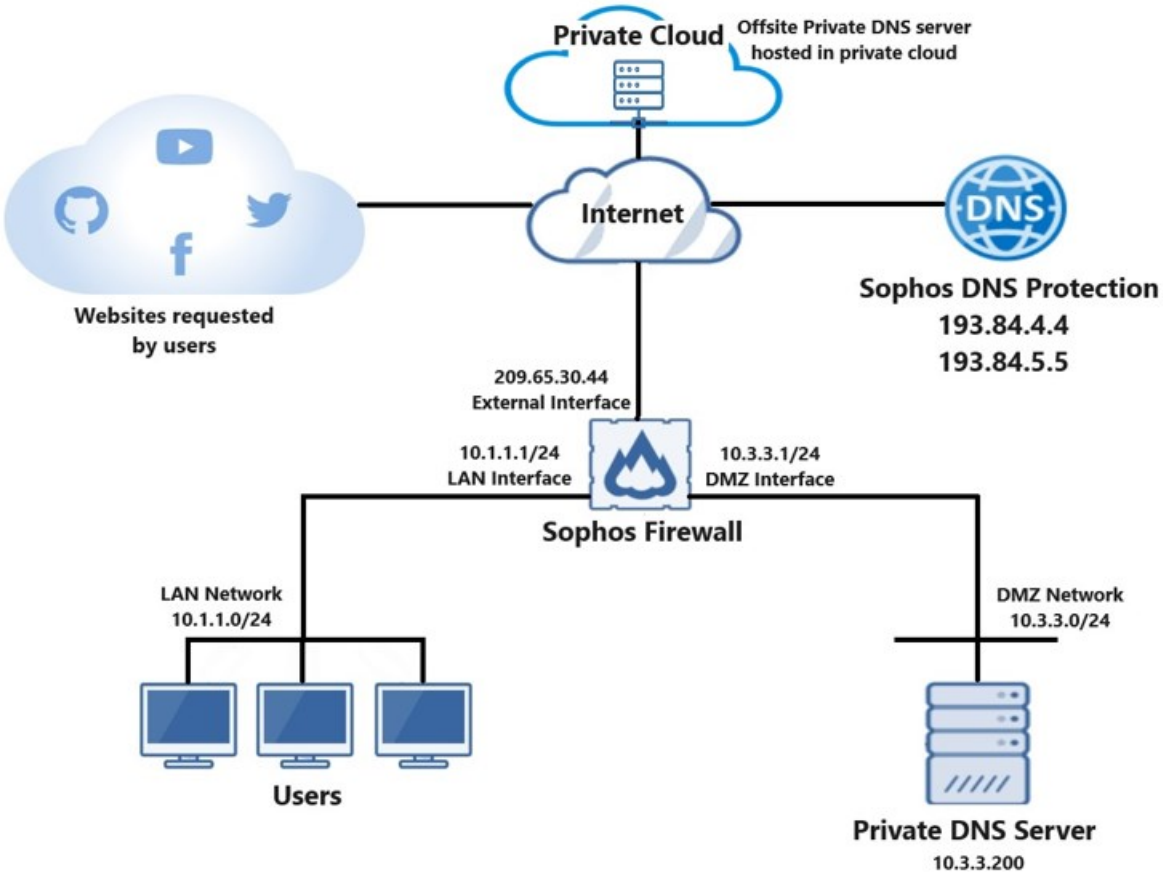
- Based on the DHCP settings, either the firewall will be advertised as the DNS resolver, or the Sophos DNS Protection resolver addresses will be published directly to the wireless clients as DNS server addresses.

- Windows Server as a Local DNS Resolver – *https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/DNSProtection/NetworkSetup/ConfigureWindowsServerToUseDNSPortection/index.html*

- **External DNS Server advertised via DHCP** – Go to the configured DHCP Server and reconfigure the DNS Server addresses to be published to the
  DNS Protection Resolver addresses of 193.84.4.4 and 193.84.5.5
- **Directly on User Devices**
- **Configure Windows devices to use DNS Protection** - *https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/DNSProtection/NetworkSetup/ConfigureWindowsDevicesToUseDNSProtection/index.html*
- **Configure Mac devices to use DNS Protection** - *https://docs.sophos.com/central/customer/help/en-us/ManageYourProducts/DNSProtection/NetworkSetup/ConfigureMacDevicesToUseDNSProtection/index.html*

Note: First, investigate how the customer's network is set up for DNS before implementing DNS Protection.

DNS Deployment Scenarios



Windows DNS Server setup

In this setup, a Windows server deployed in the local network is configured to operate as the primary local DNS resolver (10.3.3.200 in the above topology). The local endpoints are configured to contact this server to resolve their DNS queries.

This local DNS server will primarily serve the local, internal DNS domains and networks and resolutions previously handled and now stored in the cache.

For any external, non-local DNS translations, the DNS Server must be configured with DNS Forwarders; in this example, it will be the Sophos DNS Protection Resolvers (or any other DNS Service provider).

If a DNS Forwarder is not specified, then first the root DNS servers will be queried for zone information, followed by the TLD servers for authoritative DNS server information, who will then be queried for the actual DNS resolution, thereby taking a longer time to complete DNS requests.

The public IP address used for NATing will have to be configured as a location in DNS Protection in Central as the Internal Windows Servers DNS queries will trigger NAT translations.

Sophos Firewall as a DNS server

In this setup, the Sophos Firewall (or any Edge Device) is configured as the

Primary DNS server for the local network. This device will be configured

with appropriate Request Routes to specific local and external networks as per requirement.

Sophos DNS Protection Resolver addresses (or any other DNS Service provider addresses) will be configured as DNS Forwarders to resolve external domains.

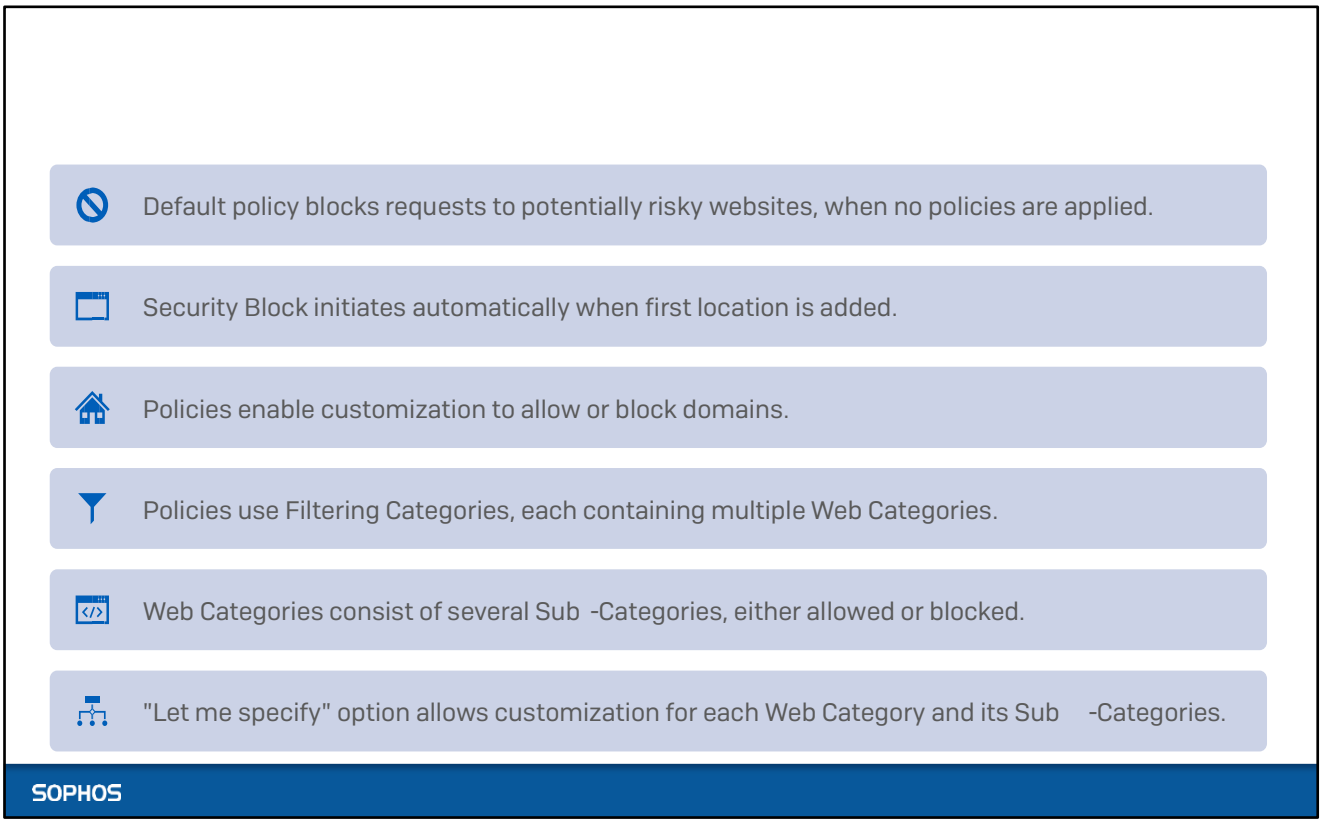
- The Sophos Firewall's Internet facing IP address will have to be configured as a location in DNS Protection in Central.

DHCP Server (or local client config)

- Here, the DHCP Server is configured to directly provide the public DNS provider addresses as DNS Server addresses to the endpoints within the local networks.
- Due to this, the endpoints reach out to the configured DNS servers directly instead of relying on the local DNS resolver to forward their unresolved query to those public DNS servers.
- The public IP address used for NATing will have to be configured as a location in DNS Protection in Central as DNS queries will be received directly from the endpoints.

An offsite DNS server in data center

- Here the DNS Server is deployed off-site in a Data Center/ Cloud environment and all endpoints in all locations of the customer are configured to use this DNS Server as their primary DNS Server.
- This DNS server will be configured with the appropriate Request Routes to point back to the internal networks and domains of the customer and will also be configured to use the appropriate DNS services as DNS Forwarders.
- The offsite DNS server's publicly accessible address will have to be configured as a location in DNS Protection in Central as all DNS queries will be relayed to Sophos from here.



Policies

If no policies have been added for DNS Protection, then all DNS requests from the customer locations will be accepted and responded to except those requesting access to websites that have been categorized as malicious by the SXL service.

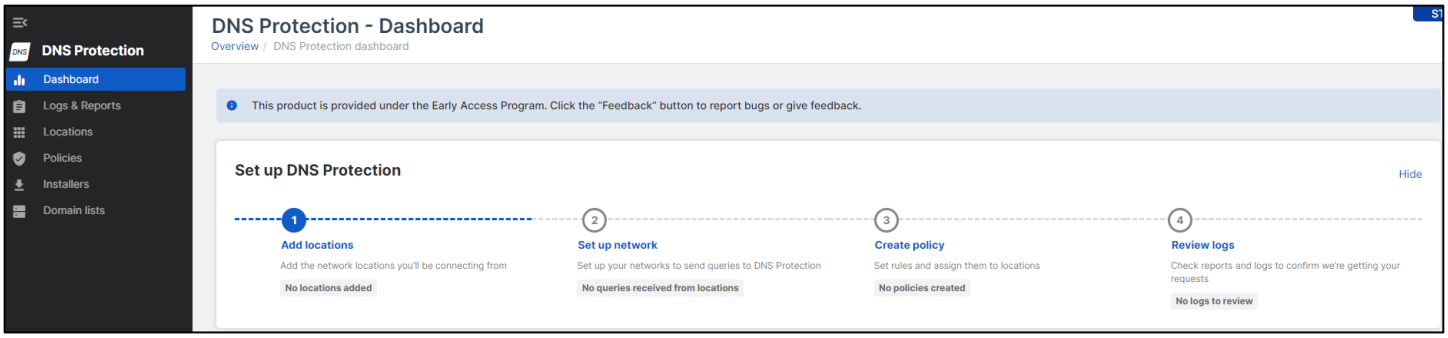
This is done by appending a default policy as soon as the customer adds the first location. This is known as the Security Block.

By adding policies, we can allow or block access to domains by making use of a filtering category that aligns with the corporate security policy.

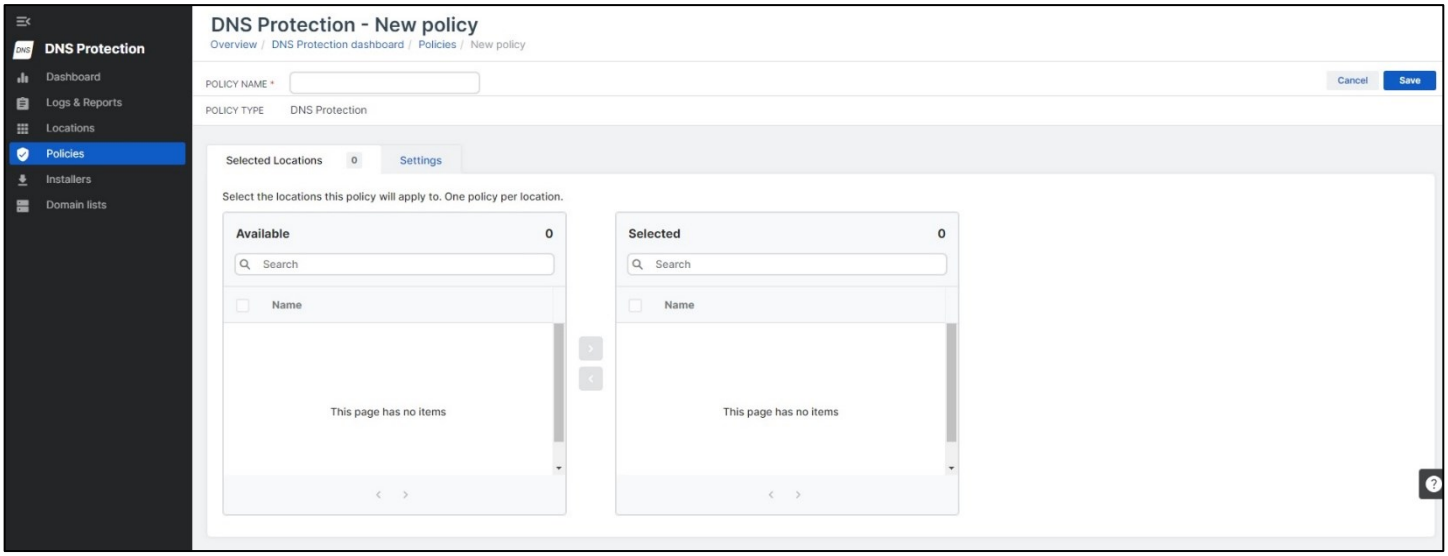
Each Filtering Category has multiple Web Categories.

Each Web Category includes several Sub-Categories that are either allowed or blocked.

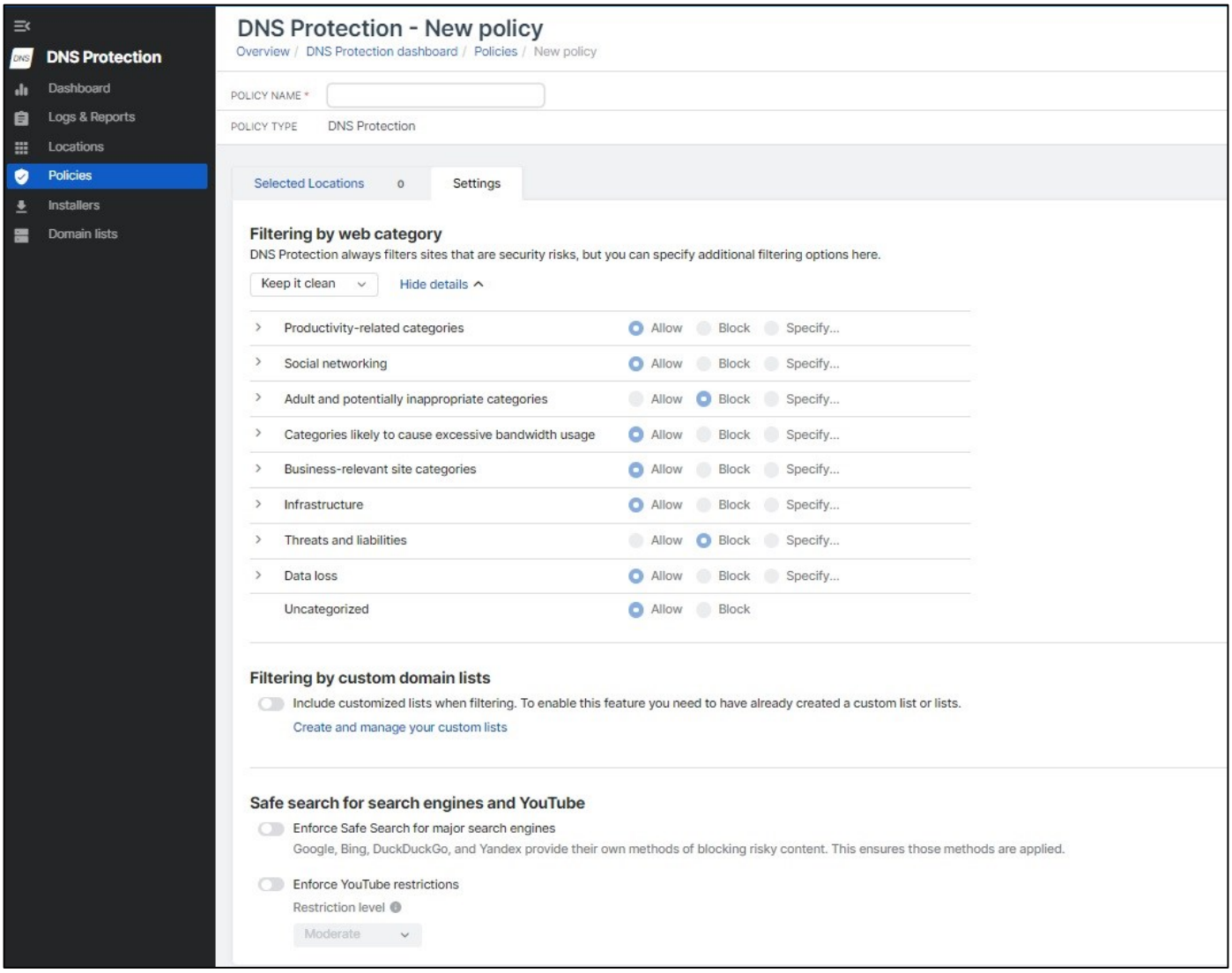
Let me specify option allows customization of allow or block action for each web category and its sub-categories to better align with the corporate policy of the organization.



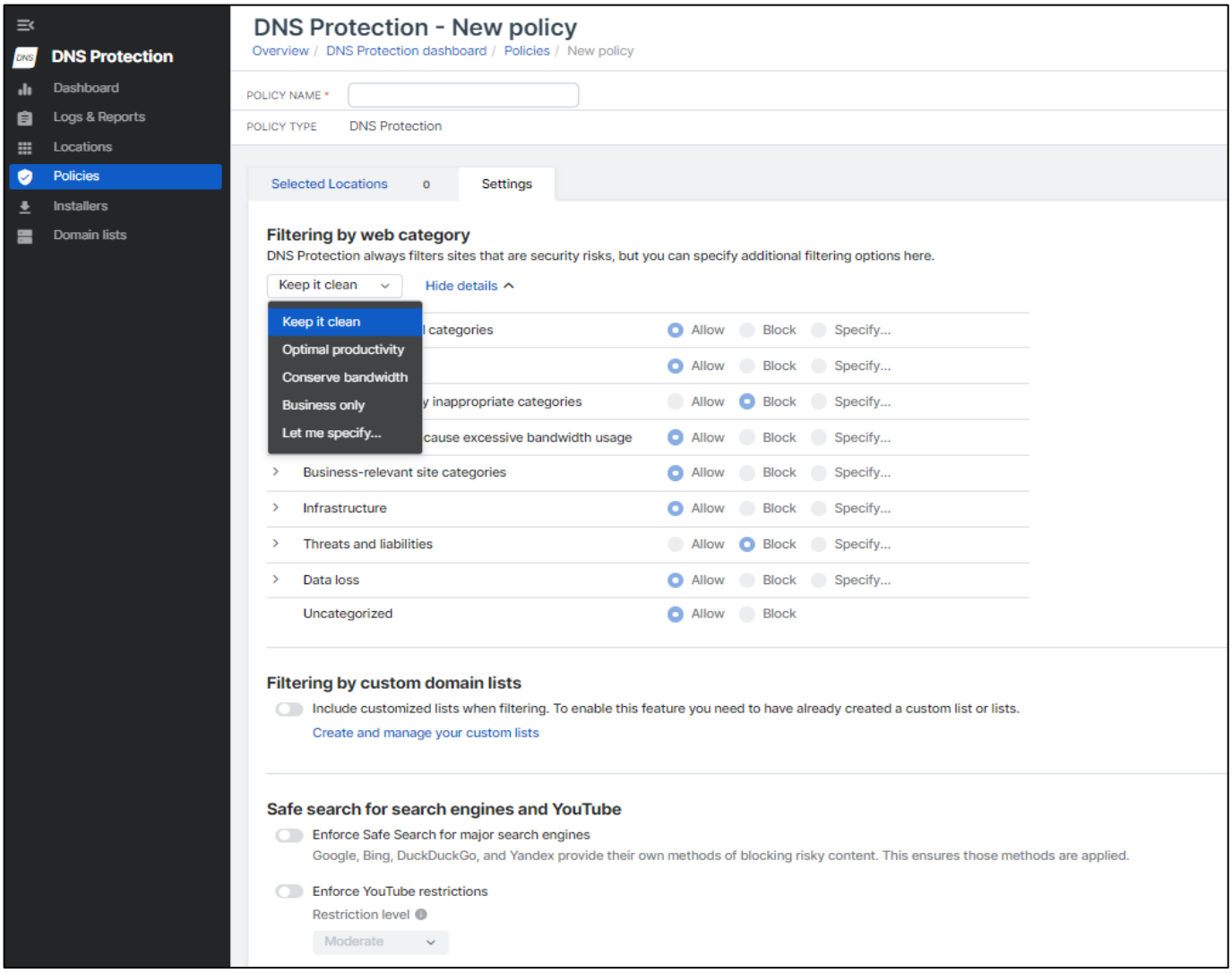
- Click on Create policy from the DNS Protection dashboard or the Policies option from the list.
- Click on Add policy on the next page.



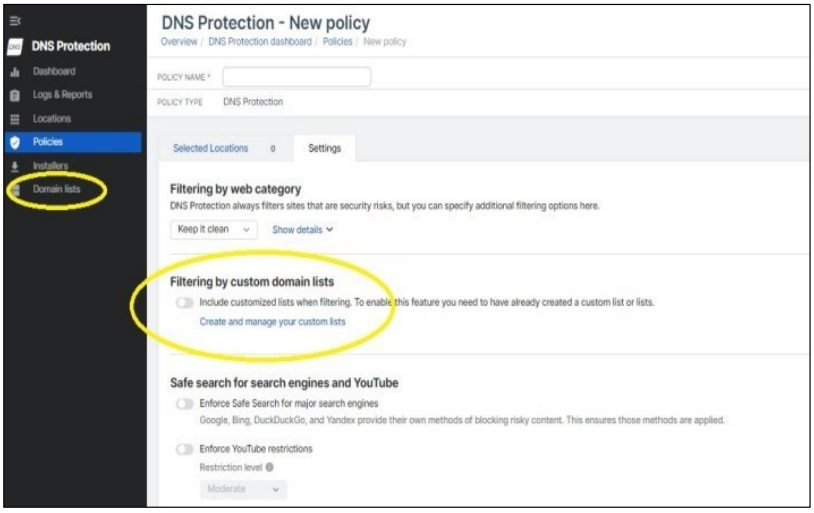
- Assign a name for the policy.
- Move the desired available locations from the left to the selected section on the right.
- Click on the settings tab.



In the settings page, click on the drop-down option under Filtering by web category to reveal additional default settings that are available.



The ‘Let me specify’ option along with the Specify setting allows full customization of the allow and block actions for parent as well as child categories.



- Custom domain list creation available.
- Overrides Web Category filtering, not Security Block.
- Block action prioritized over allow action in conflicts.

Note: *Websites with malicious reputation will always be blocked irrespective of them being allowed in the policy or the custom domain list.*

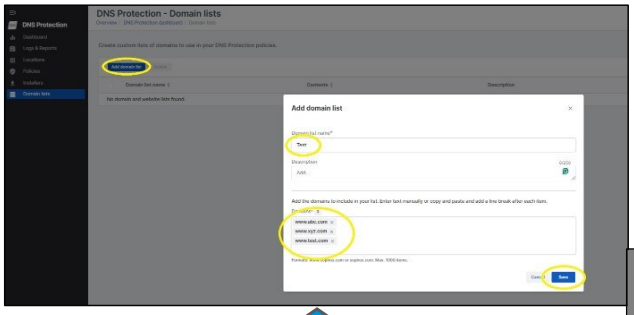
SOPHOS

Custom Domain List

- There is the option to create a custom domain list that contain the list of interested domains, which can then be imported and have allow or block action applied on them.
- The custom domain list actions will overwrite the Web Category filtering but not override the Security Block which is based on the reputation of the web site.
- In case of domain conflicts in the custom domain lists, the block action will take precedence over the allow action.

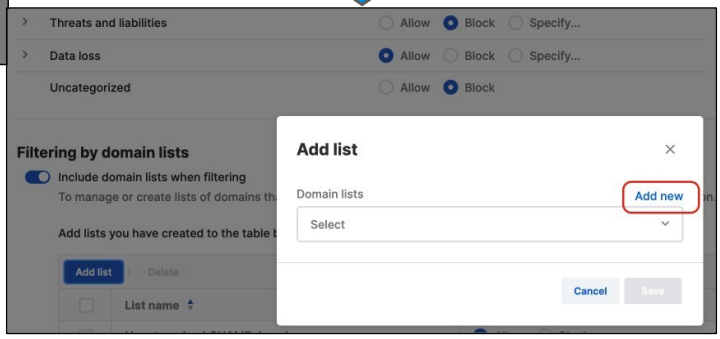
Note: When the 'Allow' action is applied to a Custom Domain List, only the Policy categorizations checks for any website in the domain list are skipped. If the website has a malicious reputation, then it will not be allowed irrespective or the policy or domain list action.

Custom Domain List



Adding a new Custom Domain List using the Domain List page.

Adding new Custom Domain List from the Policy editing page.



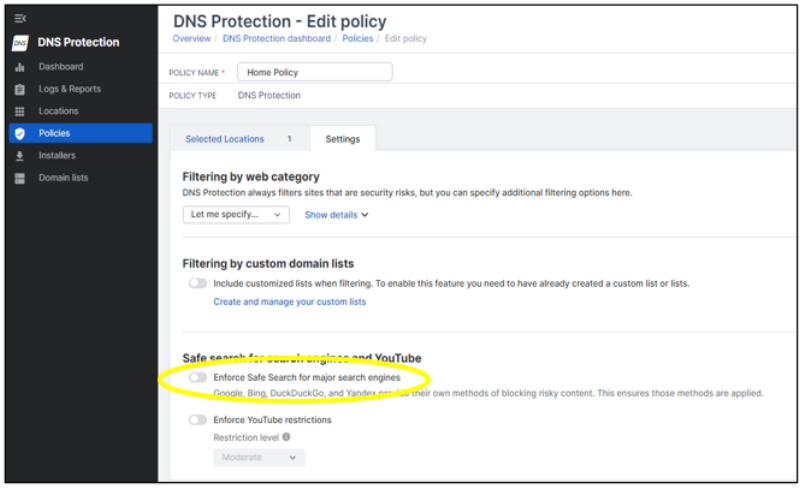
***Note**: Maximum 1000 items can be added to each custom domain list.*

SOPHOS

- Click on Add domain list.
- Assign a name for the domain list, description (optional) and mention the domains that you want to add to this custom domain list.
- Adding a domain example.com in Domain List is equivalent to [*.]example.com. So, if you add this domain list to a policy block, it will block all its sub domain.
  Example abc.example,com, abc.xyz.example.com, abc.pqr.xyz.example.com
- Custom Domain Lists can now also be created from the Policy editing page, when we enable to option to use “Filtering by domain lists” and click on ‘Add list’ and select ‘Add new. The Add domain list pop-up will appear. Once saved, it will automatically be added to the policy in use.

Note: Maximum 1000 items can be added to each custom domain list.

Safe Search for Search Engines



- Safe search support for search engines.
- Achieved using an alternative 'safe' C-NAME published by the search engine. E.g., **forcesafesearch.google.com** for Google.
- Content filtering is fully handled by the search engine operator.

SOPHOS

- There is support for Safe Search for search engines including Google, Bing, DuckDuckGo and Yandex.
- We achieve this by simply forwarding the user request to the "safe C-Name" alternative published by these search engines instead of doing the content filtering ourselves. E.g., **forcesafesearch.google.com** for Google.
- Content filtering is fully handled by the search engine operators as each one has their own methods of blocking risky content.

Safe Search for Search Engines

```
C:\>nslookup -q=CNAME www.google.com 193.84.4.4
Server:  resolver4.dnsprotection.sophos.com
Address:  193.84.4.4

google.com
        primary name server = ns1.google.com
        responsible mail addr = dns-admin.google.com
        serial  = 614386691
        refresh = 900 (15 mins)
        retry   = 900 (15 mins)
        expire  = 1800 (30 mins)
        default TTL = 60 (1 min)
```

With Enforce Safe Search option disabled.

```
C:\>nslookup -q=CNAME www.google.com 193.84.4.4
Server:  resolver4.dnsprotection.sophos.com
Address:  193.84.4.4

www.google.com  canonical name = forcesafesearch.google.com
google.com
        primary name server = ns1.google.com
        responsible mail addr = dns-admin.google.com
        serial  = 614386691
        refresh = 900 (15 mins)
        retry   = 900 (15 mins)
        expire  = 1800 (30 mins)
        default TTL = 60 (1 min)
```

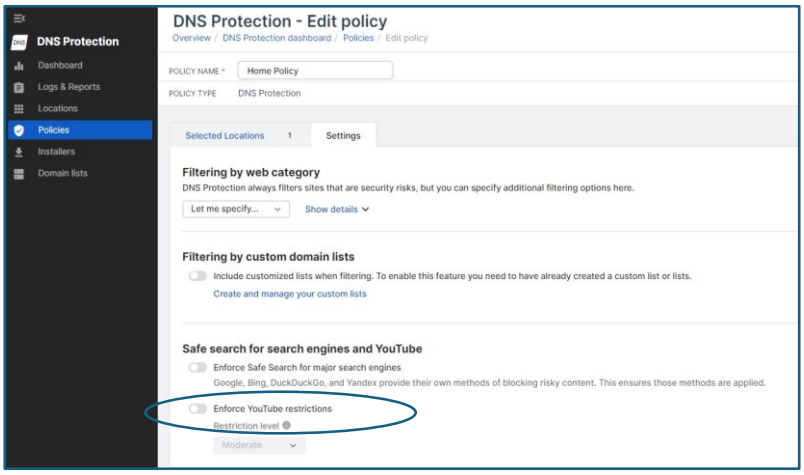
With Enforce Safe Search option enabled.

SOPHOS

Output of the nslookup –q=CNAME www.google.com 193.84.4.4 command with Enforce Safe Search option disabled and enabled under DNS Protection in Sophos Central.

YouTube Restrictions

There is also the option to enable YouTube Restriction based on moderate and strict levels for YouTube content.
This feature prevents users from being presented with potentially inappropriate content when the search in YouTube.
Restriction severity can be set to be either Moderate or Strict.
Uses 'safe' CNAME restrict.youtube.com.
https://support.google.com/a/answer/6212415?hl=en

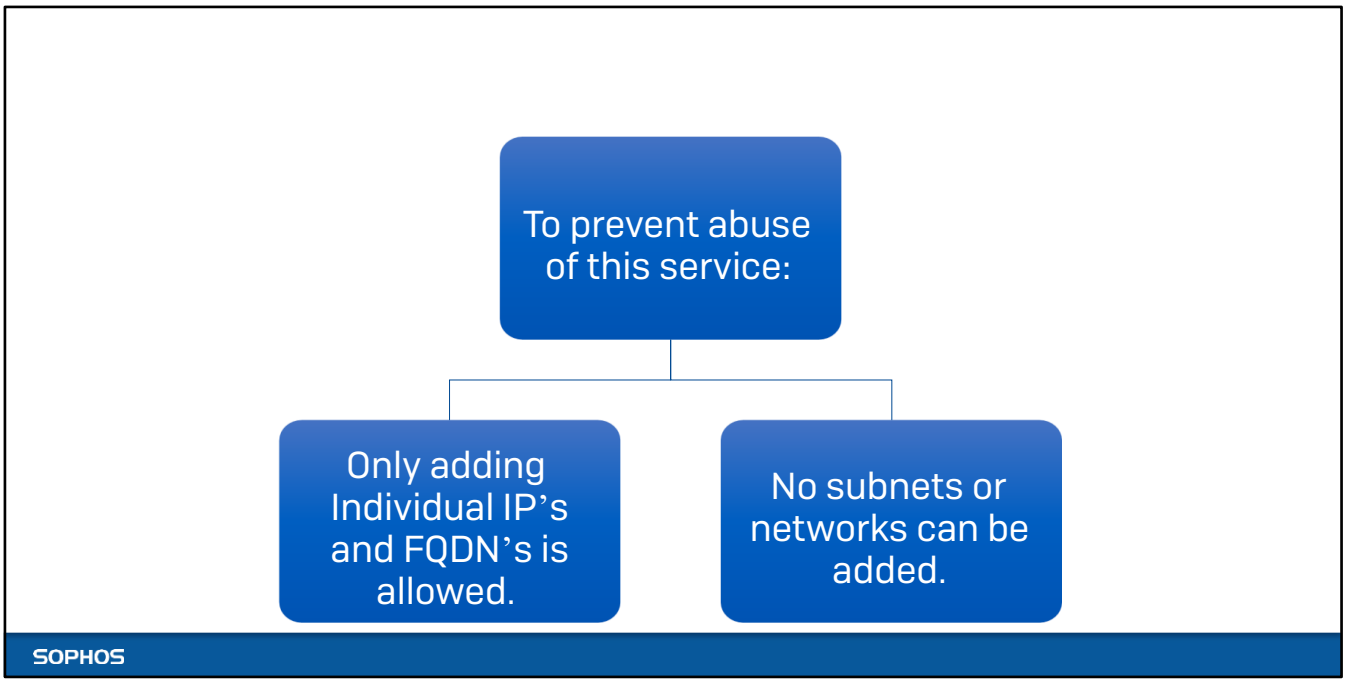



```
C:\>nslookup -q=CNAME www.youtube.com 193.84.4.4
Server:  resolver4.dnsprotection.sophos.com
Address:  193.84.4.4

Non-authoritative answer:
www.youtube.com canonical name = youtube-ui.l.google.com
```

```
C:\>nslookup -q=CNAME www.youtube.com 193.84.4.4
Server:  resolver4.dnsprotection.sophos.com
Address:  193.84.4.4

www.youtube.com canonical name = restrict.youtube.com
youtube.com
        primary name server = ns1.google.com
        responsible mail addr = dns-admin.google.com
        serial  = 614386691
        refresh = 900 (15 mins)
        retry   = 900 (15 mins)
        expire  = 1800 (30 mins)
        default TTL = 60 (1 min)
```

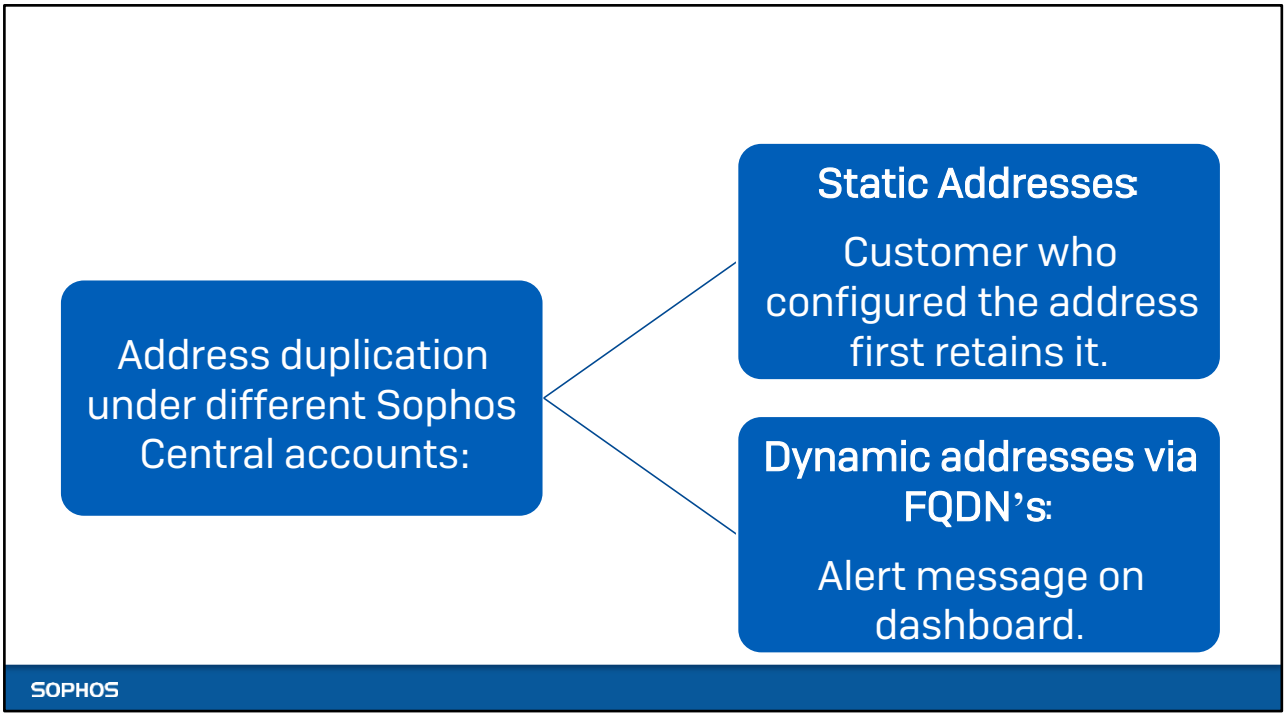
Output of the **nslookup –q=CNAME www.youtube.com 193.84.4.4** command with the **Enforce YouTube Restrictions OFF** and **ON** under DNS Protection in Sophos Central.

Additional Information



To prevent this service from being abused by malicious users who might add IP addresses not associated with themselves as their locations, we don't support adding subnets and whole networks when adding a location and instead have limited to only adding individual IP addresses and FQDNs that resolve to a single address.

Additional Information 2

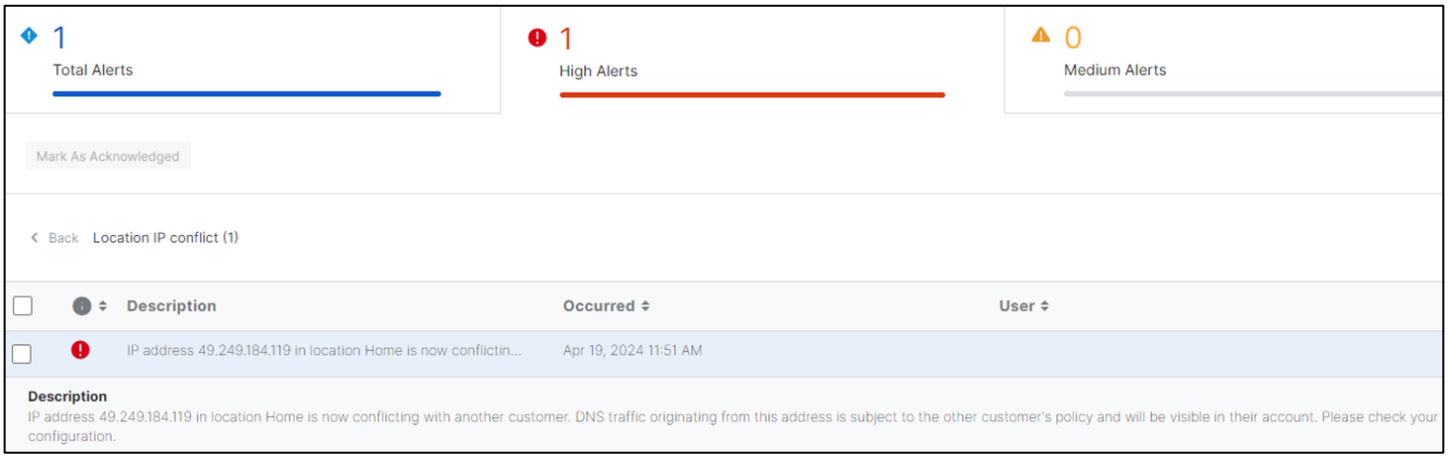


In case there's address duplication under different Sophos Central accounts when adding a location:

For Static Addresses: If two customers end up adding the same IP address as a location statically, then the customer who added the address first retains it and the customer who tried to add it later will get a "Duplicate IP addresses, Domain names in configuration" error message.

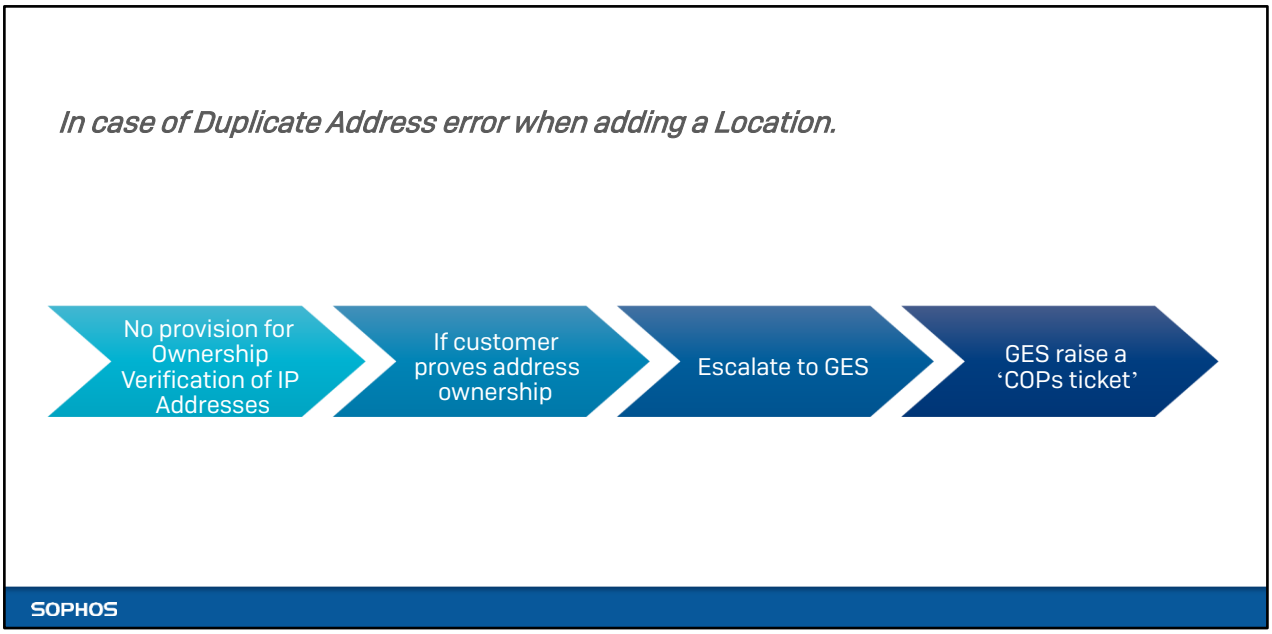
For FQDN's: A high severity alert will be raised if the IP address for your FQDN changes, and the new IP address is already registered as a location in another customer account. The customer who has the address already registered will retain it.

Alert message on customer dashboard



Alert message displayed on customer dashboard in Sophos Central informing the customer about the conflict with the IP address that was added as location with another customer's policy.

Additional Information 3

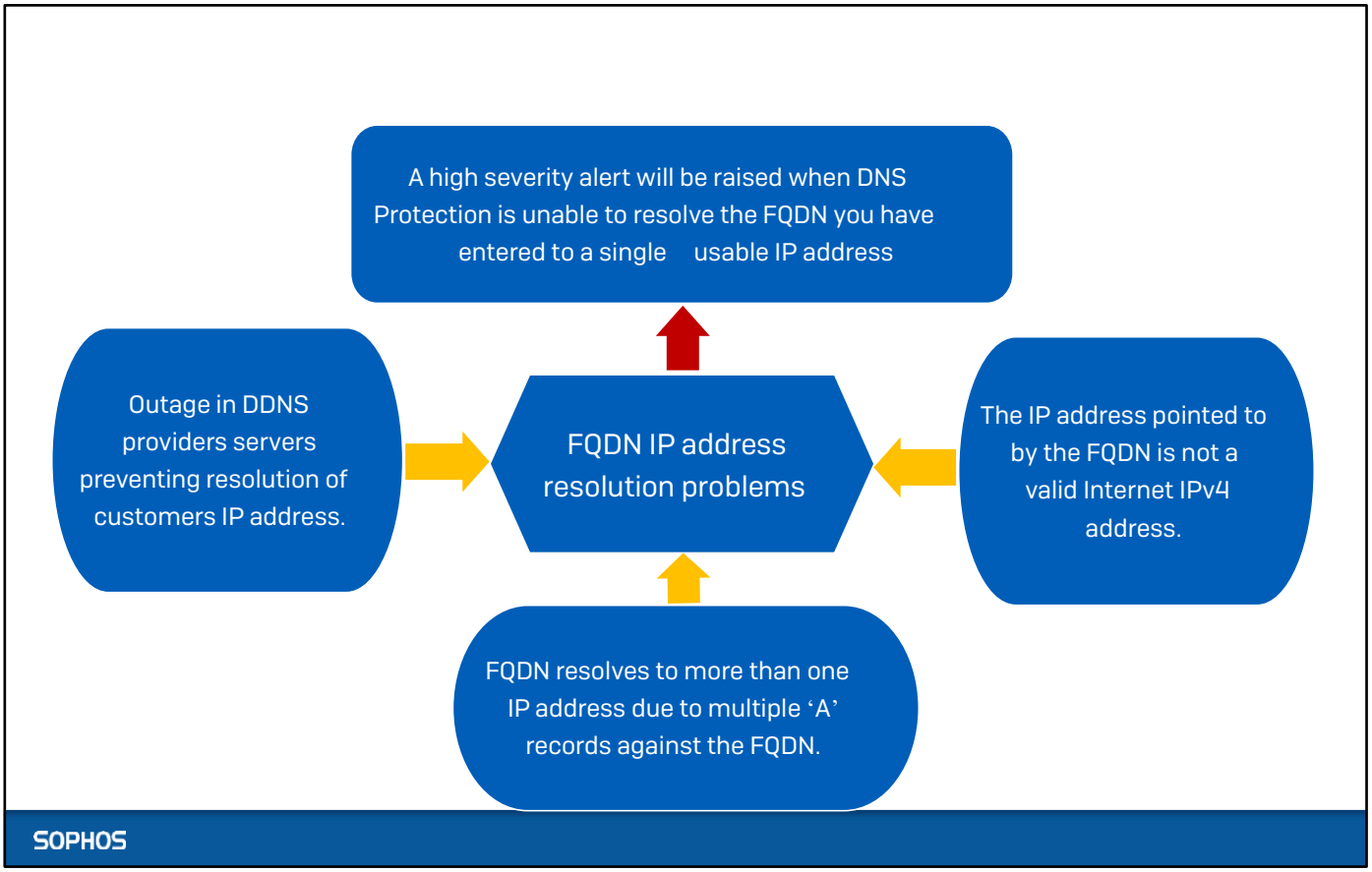


- There is no provision to verify the customer's ownership of IP addresses.
- But if a customer proves that they're the current owner of the IP address and is unable to add it as a location in DNS Protection, then the case can be escalated to the GES, who can then raise a 'COPs ticket' to investigate which other customer has the same IP address added to their location database and take necessary action.

Additional Information 4

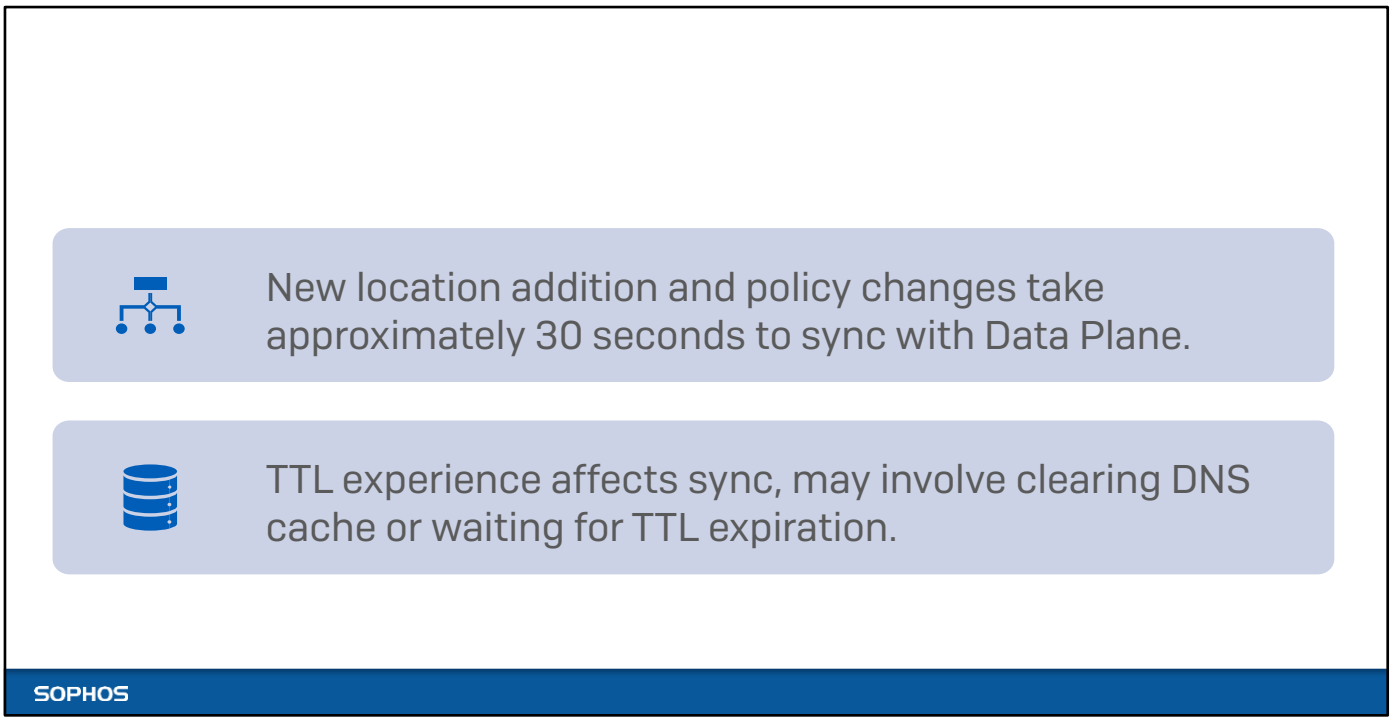
FQDN IP address resolution problems: A high severity alert will be raised when DNS Protection is unable to resolve the FQDN you have entered to a single usable IP address.

- Possible causes include:
  - An outage at DDNS providers servers preventing resolution of customers dynamic address and FQDN.



  - FQDN resolves to more than one IP address due to multiple 'A' records against the FQDN.
  - The IP address pointed to by the FQDN is not a valid Internet IPv4 address.

Additional Information 5



When a new location is added, it will take around 30 seconds to sync with the Data Plane and allow the customer to access the DNS Resolvers.

This is also applicable to any policy changes that are done.

The TTL experienced also plays a role to play as it might involve having to clear the DNS cache or wait till the TTL expires for the sync to happen.

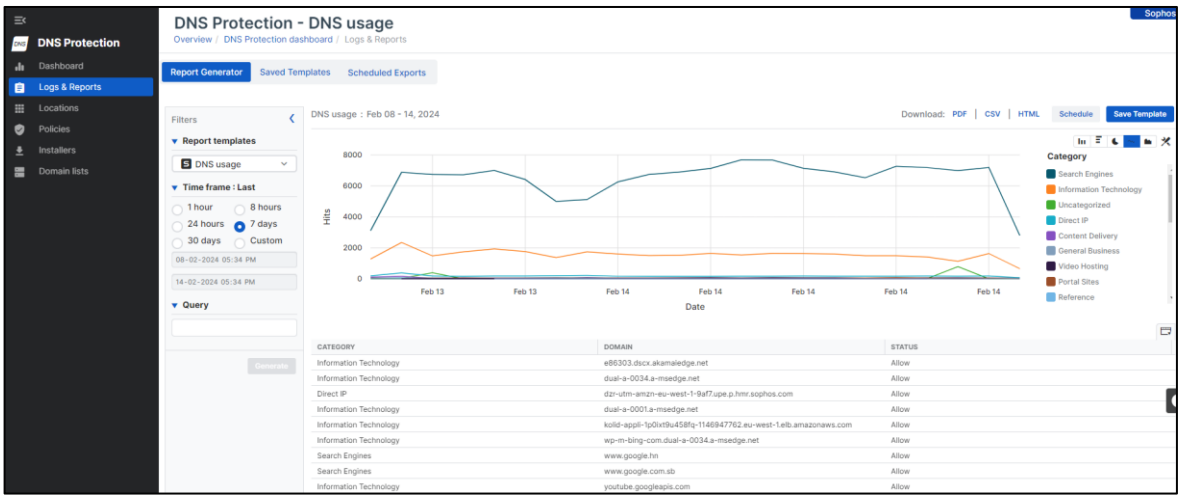
Module 3: Troubleshooting Sophos DNS Protection

Objectives:

Once you complete this module you will be able to:

- Logs & Reports
- Filters
- List of Operators
- Charts
- Tables
- Schedule Reports
- Generate an Export Manually
- Save a Report Template

Logs & Reports



The **Logs & Reports** page provides detailed reports on DNS Protection features. You can select a report template, specify filters, and generate a report. You can save templates for your frequently-generated reports and set up export schedules for reports.

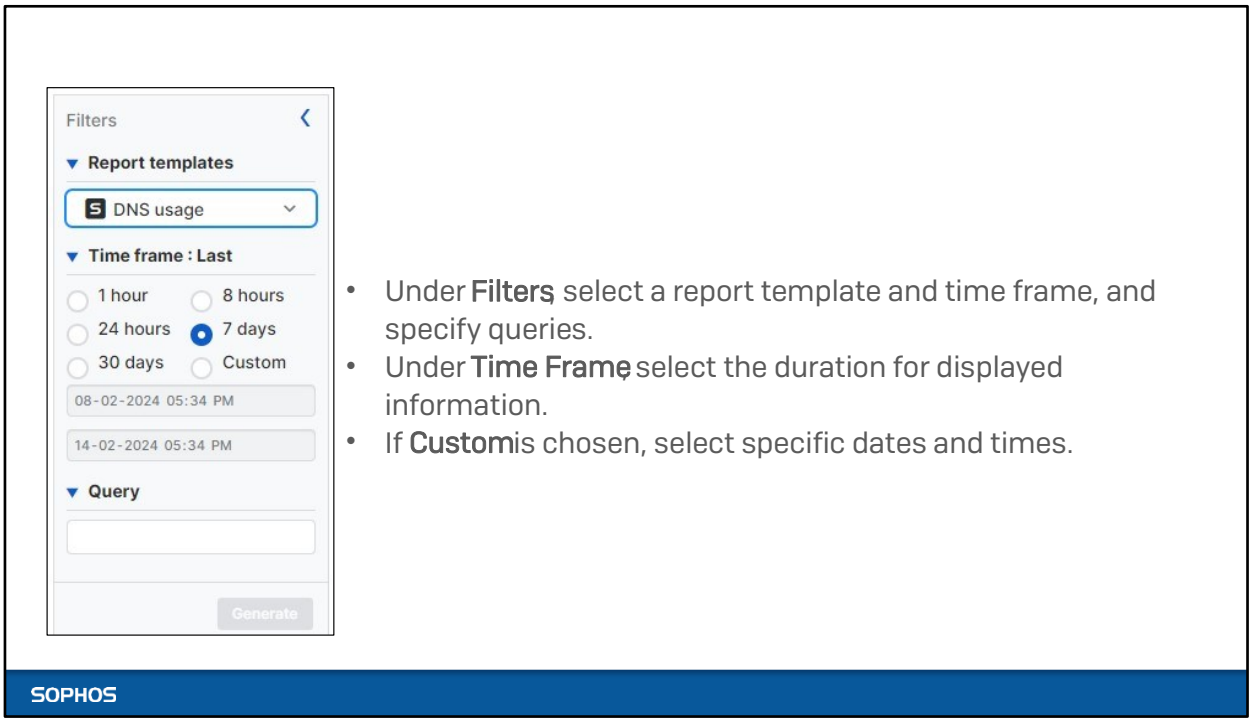
The **Report Generator** tab includes the following areas:

- Filters
- Chart
- Table
- Schedule reports
- Save templates

Note:

1. The data in the reports is always at least 15 minutes behind real-time.
2. If you update the location or policy name, the new name may take between 30 minutes and 4 hours to reflect in Logs & Reports.

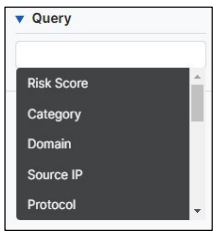
Filters



- Under **Filters**, select a report template and time frame, and specify queries.
- Under **Time Frame**, select the duration for displayed information.
- If **Custom** is chosen, select specific dates and times.

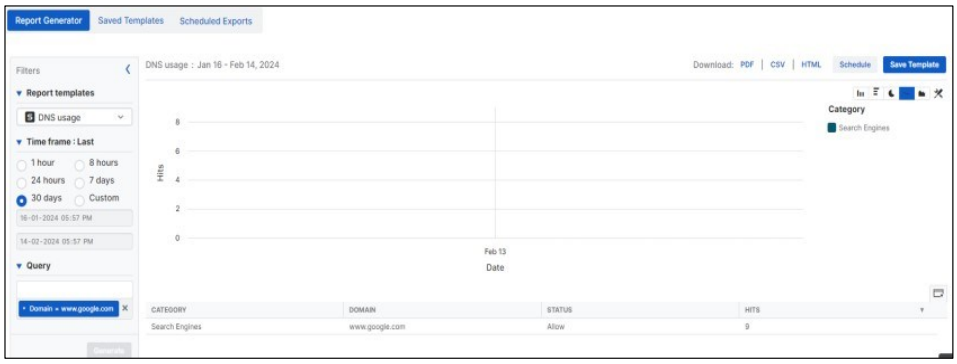
- Under **Filters**, you can select a report template and time frame. You can also specify queries.
- Under **Time frame**, you can specify the time frame for which information is shown by selecting one option. If you select **Custom**, you can select the dates and times between which information is shown.

Add Filters



1. Under **Query** , select or enter the name of the column on which you want to filter.
2. Enter the values by which you want to filter the report.

3. To change the operator used for comparison, click the equals sign next to the column name, and select an option from the drop -down list.



View after the report is generated.

SOPHOS

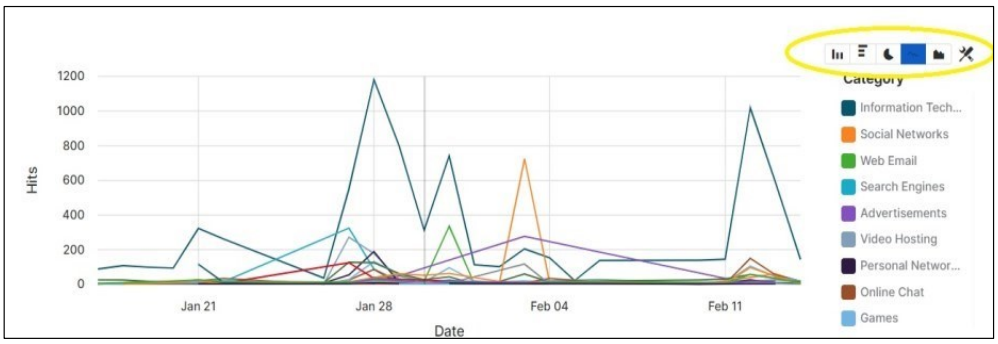
To add filters, do as follows:

- Under Query, select or enter the name of the column on which you want to filter.
- Enter the values by which you want to filter the report.
- To change the operator used for comparison, click the equals sign next to the column name, and select an option from the drop-down list.

List of Operators:

Operator	Rows shown
=	Rows in which the column value matches the value you want to filter. The value is case-sensitive. e.g. **DOMAIN = www.bing.com**
!=	Rows in which the column value does not match the value you want to filter. The value is case-sensitive.
<	Rows in which the column value is less than the value you want to filter (applies only to numeric values)
<=	Rows in which the column value is less than or equal to the value you want to filter (applies only to numeric values)
>	Rows in which the column value is greater than the value you want to filter (applies only to numeric values)
IN	Rows in which the column value matches any value in a comma-separated list of values you want to filter The values are case-sensitive. e.g. **Destination IP IN 13.107.21.200,204.79.197.200**
~	Rows in which the column value matches a wildcard expression you want to filter. The wildcard is an asterisk: * The expression isn't case-sensitive. e.g. URL ~ *amazon*

Chart



You can select the chart type in the top right of the area.

- Bar
- Horizontal bar
- Pie
- Line
- Stack-area

SOPHOS

To select which information is shown on each axis, do as follows:

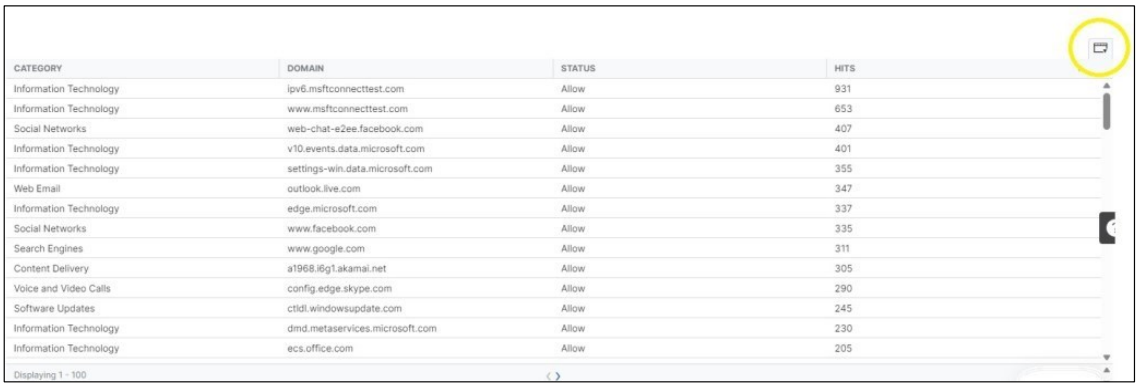
1. Click the wrench button in the top right of the area
2. In the top box, select which information is shown on the x-axis.
3. In the next box, click the arrow and select which information is shown on the yaxis.
4. If a line or stack-area chart is shown, in the bottom box, click the arrow and select which information is shown on the z-axis.

When you select a different chart type, it shows default information on each axis, even if you previously changed it.

If you hover over the chart, the data values are shown.

Note: The bar and pie charts show records for only the top 10 categories.

Tables



CATEGORY	DOMAIN	STATUS	HITS
Information Technology	ipv6.msftconnecttest.com	Allow	931
Information Technology	www.msftconnecttest.com	Allow	653
Social Networks	web-chat-e2ee.facebook.com	Allow	407
Information Technology	v10.events.data.microsoft.com	Allow	401
Information Technology	settings-win.data.microsoft.com	Allow	355
Web Email	outlook.live.com	Allow	347
Information Technology	edge.microsoft.com	Allow	337
Social Networks	www.facebook.com	Allow	335
Search Engines	www.google.com	Allow	311
Content Delivery	a1968.i6g1.akamai.net	Allow	305
Voice and Video Calls	config.edge.skype.com	Allow	290
Software Updates	ctldl.windowsupdate.com	Allow	245
Information Technology	dmd.metaservices.microsoft.com	Allow	230
Information Technology	ecs.office.com	Allow	205

Displaying 1 - 100

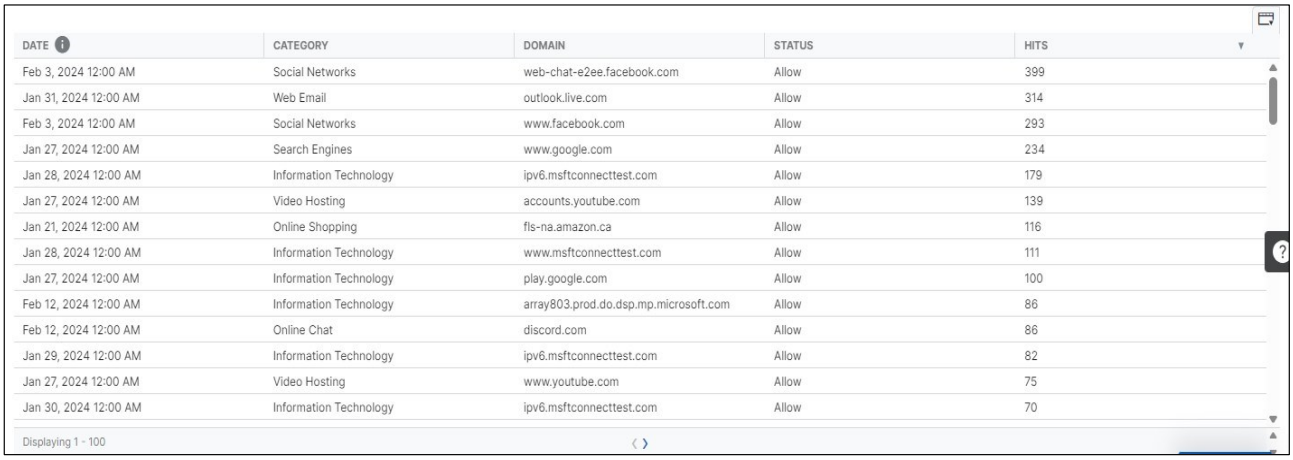
When the table is first shown, it uses a default set of columns. You can select which columns to show by clicking the column selection button in the top right of the table area.

SOPHOS

To add a filter from the table, click a value under the column on which you want to filter. The column and its value appear under **Query**. You can select multiple columnvalue pairs. Click **Generate** to generate the report.

You can click the column headers to sort the values in ascending or descending order.

Tables with the Date column



DATE	CATEGORY	DOMAIN	STATUS	HITS
Feb 3, 2024 12:00 AM	Social Networks	web-chat-e2ee.facebook.com	Allow	399
Jan 31, 2024 12:00 AM	Web Email	outlook.live.com	Allow	314
Feb 3, 2024 12:00 AM	Social Networks	www.facebook.com	Allow	293
Jan 27, 2024 12:00 AM	Search Engines	www.google.com	Allow	234
Jan 28, 2024 12:00 AM	Information Technology	ipv6.msftconnecttest.com	Allow	179
Jan 27, 2024 12:00 AM	Video Hosting	accounts.youtube.com	Allow	139
Jan 21, 2024 12:00 AM	Online Shopping	fls-na.amazon.ca	Allow	116
Jan 28, 2024 12:00 AM	Information Technology	www.msftconnecttest.com	Allow	111
Jan 27, 2024 12:00 AM	Information Technology	play.google.com	Allow	100
Feb 12, 2024 12:00 AM	Information Technology	array803.prod.do.dsp.mp.microsoft.com	Allow	86
Feb 12, 2024 12:00 AM	Online Chat	discord.com	Allow	86
Jan 29, 2024 12:00 AM	Information Technology	ipv6.msftconnecttest.com	Allow	82
Jan 27, 2024 12:00 AM	Video Hosting	www.youtube.com	Allow	75
Jan 30, 2024 12:00 AM	Information Technology	ipv6.msftconnecttest.com	Allow	70

Displaying 1 - 100

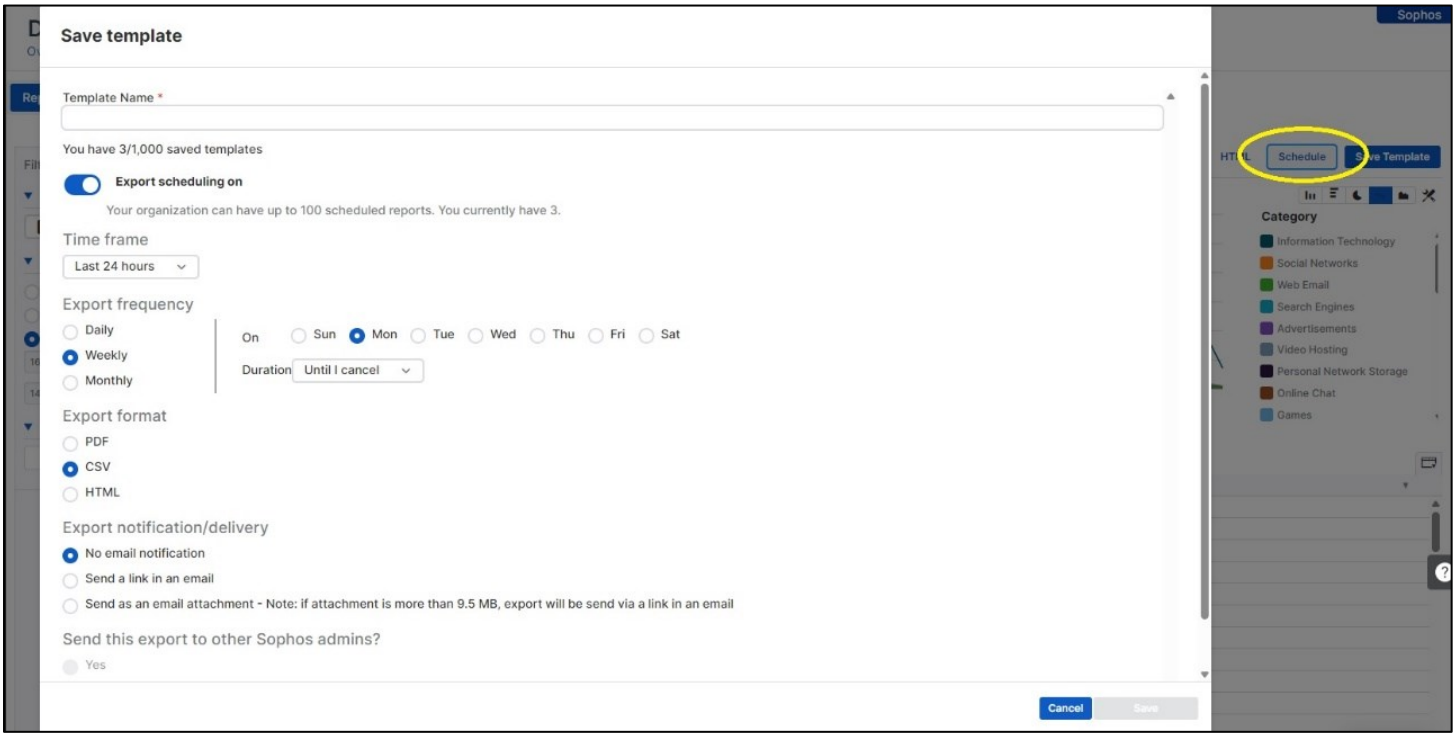
Time frame	Row grouping
1 hour, 8 hours	Rows in which the date, hours, and minutes are the same.
24 hours, 7 days, and custom selection of <= 7 days	Rows in which the starting hour is the same.
For 30 days and custom selection of > 7 days	Rows in which the days have a default timestamp of 12:00 AM.

SOPHOS

If the date column is shown, duplicate rows are grouped on the date and time as follows:

Time frame	Row grouping
1 hour, 8 hours hours, and minutes are the same.	Rows in which the date,
24 hours, 7 days, and custom selection of <= 7 days hour is the same.	Rows in which the starting
For 30 days and custom selection of > 7 days have a default timestamp of 12:00 AM.	Rows in which the days

Schedule reports



You can set up export schedules for reports. You can create a maximum of 100 schedules.

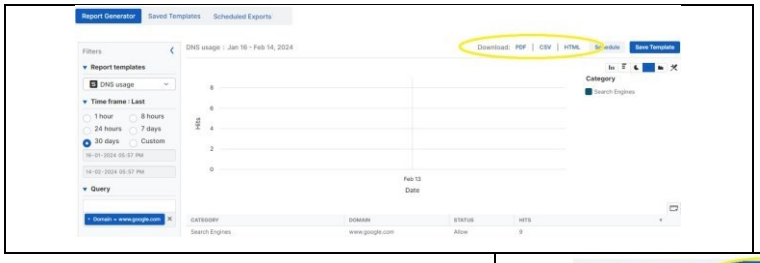
To set up an export schedule for reports, do as follows:

1. Click Schedule.
2. Enter a Template Name.
3. Select the Time frame for the data you want to include.
4. Configure the Export frequency settings as follows:
    a) Select one of the following options:
        - Daily: If you select this option, all days of the week are selected.
        - Weekly: If you select this option, select a day of the week on which you want to export the report.
        - Monthly: If you select this option, select a day of the month on which you want to export the report.
    b) In Duration, select one of the following options:
        - Until I cancel: Reports are exported according to the configured frequency until you cancel the schedule.

        To cancel a schedule, in the Scheduled Exports tab, select a schedule and click Delete.

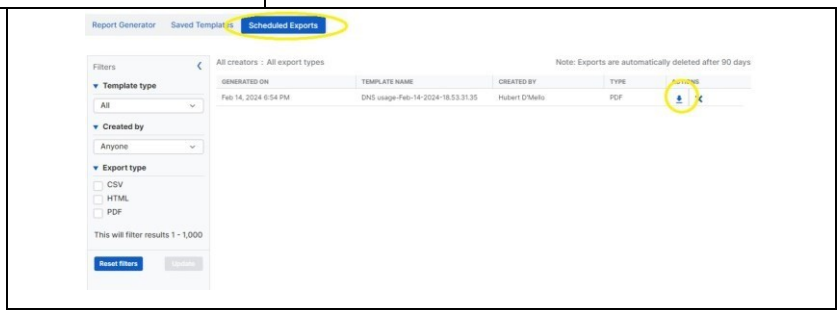
        - Ends on: Select a date when you want to end the schedule.
5. Select the Export format. (Formats available PDF, CSV, or HTML).
6. Select the **Export notification/delivery** method.
    - It is recommended to send the link in an email if the report includes personally identifiable information.
    - The report is sent to the Sophos Central email address, as specified in **Account Details**.
    - You must enter your Sophos Central sign-in credentials to view reports from a link.
    - Reports can be sent to other Sophos Central administrators too.

Click **Save.**



To generate an export manually without creating a schedule, click on PDF, CSV or HTML option that is highlighted.

Download the exported reports from **Scheduled Exports**. The exported reports are deleted after 90 days.

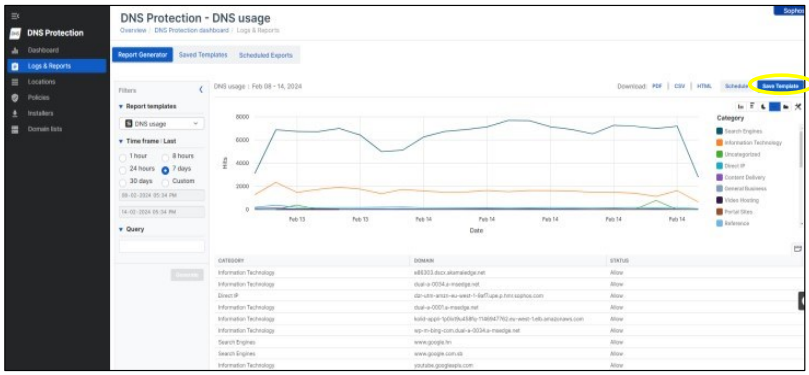


Generate an Export Manually

To generate an export manually without creating a schedule, click on PDF, CSV or HTML option that is highlighted.

Download the exported reports from **Scheduled Exports**. The exported reports are deleted after 90 days.

Save a Report Template



Click **Save Template** to save the selected report template with any of the filters or display settings that you've applied

You also can turn export scheduling on and off for this report template.

SOPHOS

Click **Save Template** to save the selected report template with any of the filters or display settings that you've applied, including the following:

- Query filters
- Chart type
- Chart axes
- Table sorting
- Table columns

Saving your templates prevents you from having to make all the selections again. The report template is saved to the **Saved Templates** tab. The data and timeframe aren't saved with the template.

Note:

1. **You can create a maximum of 1000 templates across DNS Protection, ZTNA, and Sophos Firewall reports.**
2. **Reports can be generated only on per-location basis and not on per-user basis.**

You also can turn export scheduling on and off for this report template. To update a template, in the **Saved Templates** tab, select a template and click **Update.**
To delete a template, in the **Saved Templates** tab, select a template and click **Delete**.

You can delete only 25 templates at a time.

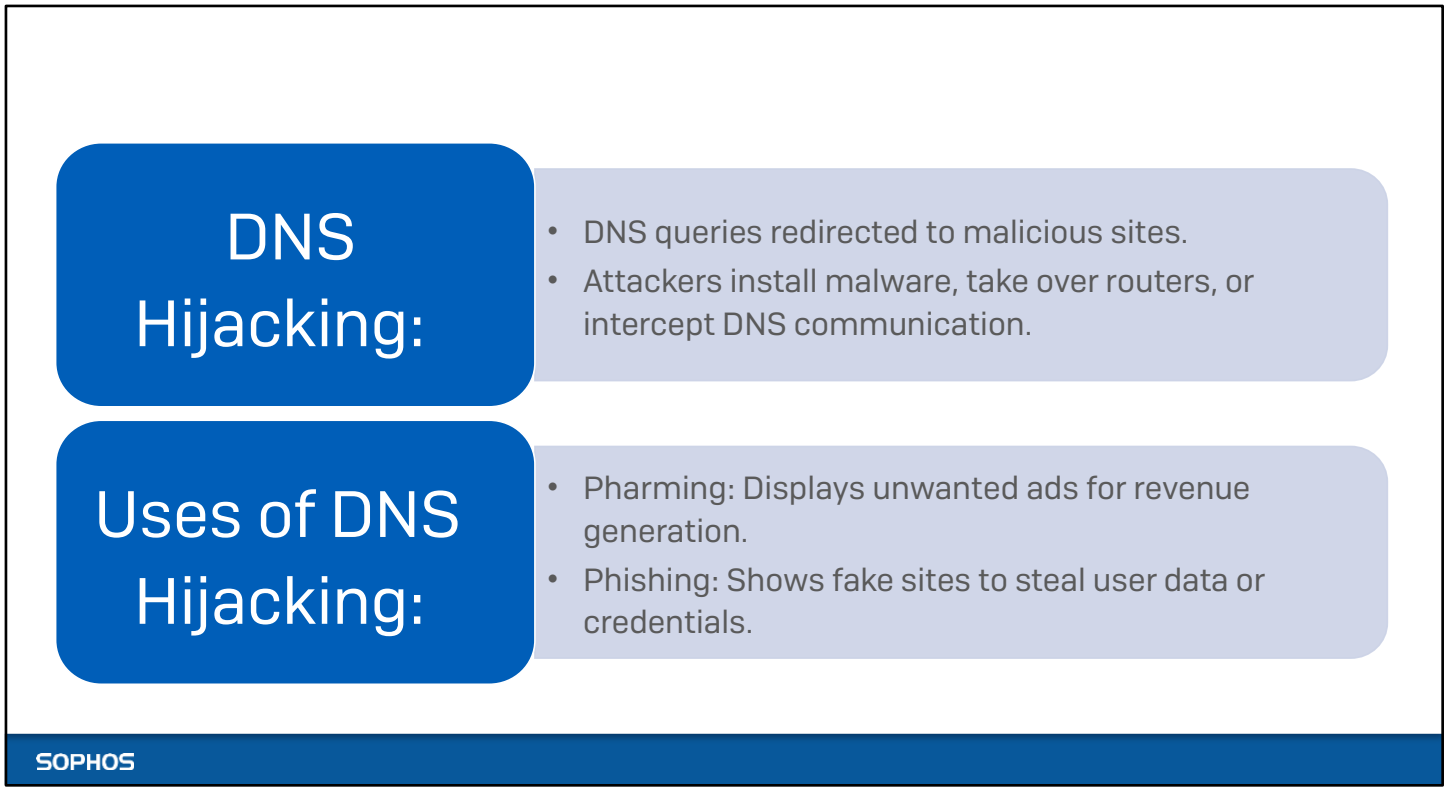
Module 4: Troubleshooting Sophos DNS Protection

Module Objectives:

Once you complete this module you will be able to:

- DNS Hijacking/DNS Redirection
- Verifying if DNS Protection is being used.
- DNS Protection policies not getting applied.
- DNS Protection not supported in Sophos Central Region.
- Customer website categorized wrongly.
- Updated policy not enforced immediately.
- Allowed domain is blocked.
- Duplicate IP address error message.
- Adding an Unresolving FQDN as a Location
- Troubleshooting Partial loading of web pages
- Issues with Internet access on Apple devices
- When multiple DNS Forwarders are configured
- Getting customer up and running in critical situations.

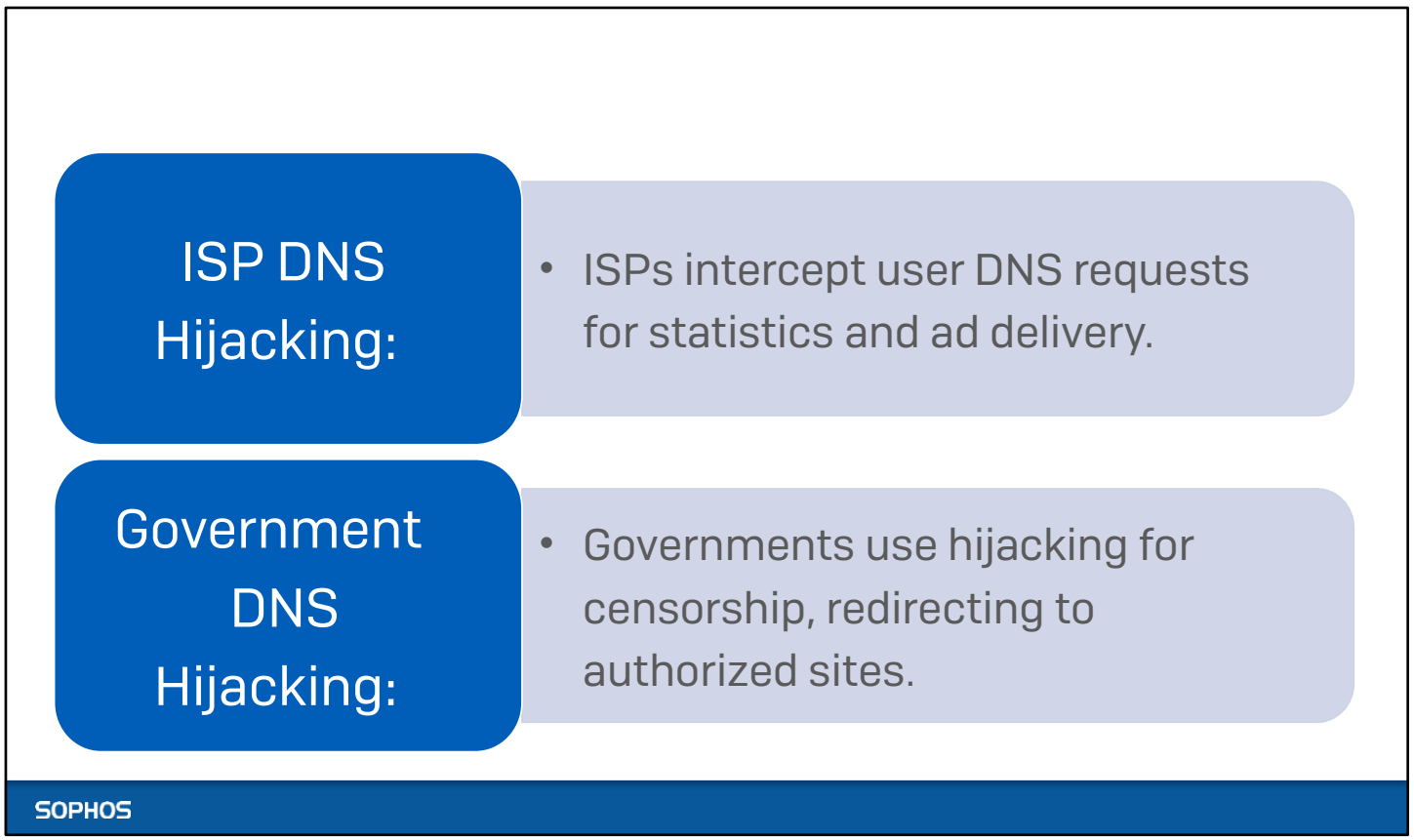
DNS Hijacking/ DNS Redirection



DNS hijacking or DNS redirection is a type of DNS attack in which DNS queries are incorrectly resolved to unexpectedly redirect users to malicious sites. To perform the attack, perpetrators either install malware on user computers, take over routers, or intercept or hack DNS communication.

DNS hijacking can be used for pharming (to display unwanted ads to generate revenue) or for phishing (displaying fake versions of sites users' access and stealing data or credentials).

DNS Hijacking/ DNS Redirection

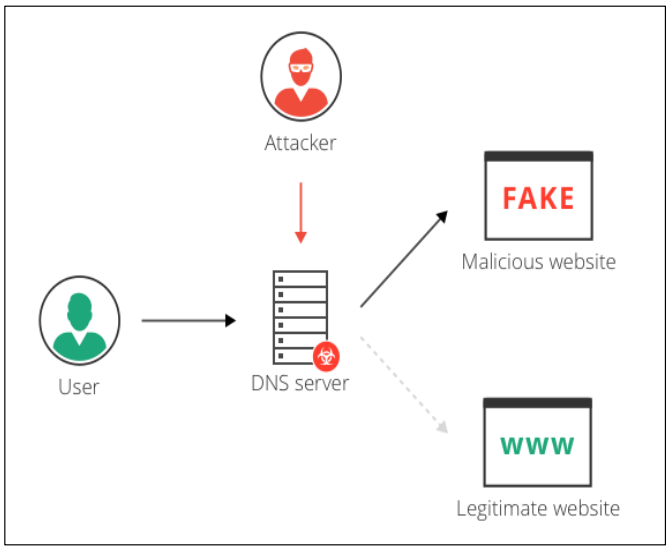


Many ISP's also use a type of DNS hijacking, to take over a user's DNS requests, collect statistics and return ads when users access an unknown domain.

Some governments also use DNS hijacking for censorship, redirecting users to government-authorized sites.

DNS hijacking attack types

- **Local DNS Hijack** : Trojan malware alters user's computer DNS.
- **Router DNS Hijack** : Attackers alter router DNS for all users.
- **Man -in -the -Middle DNS Attacks** : Intercept DNS communication to redirect.
- **Rogue DNS Server** : Hackers alter DNS records for malicious redirection.



SOPHOS

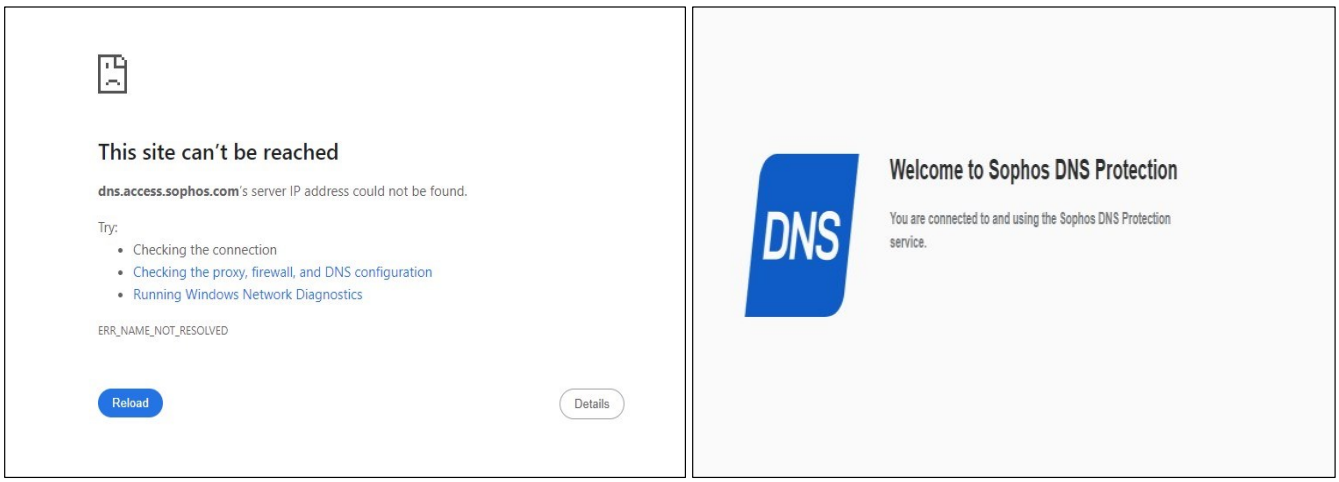
- **Local DNS Hijack**: In this scenario, attackers install Trojan malware on a user's computer. This malware alters the local DNS settings, diverting the user's DNS queries to malicious sites. Essentially, the user's computer becomes compromised, leading to unintended redirections to harmful destinations.
- **Router DNS Hijack**: Attackers target routers, gaining unauthorized access to them. Once compromised, they overwrite the router's DNS settings, affecting all devices connected to that router. This widespread impact allows attackers to redirect DNS queries from multiple users to malicious sites, posing a significant threat to network security.
- **Man-in-the-Middle (MitM) DNS Attacks**: In a MitM DNS attack, attackers intercept communication between a user and a legitimate DNS server. They then manipulate the DNS responses, providing different destination IP addresses that lead to malicious sites instead of the intended destinations. This type of attack can occur in various scenarios, including public Wi-Fi networks or compromised network infrastructure.
- **Rogue DNS Server**: Attackers target DNS servers directly by hacking into them. Once compromised, they modify the DNS records stored on the server. By altering these records, they redirect DNS queries sent to the compromised server to malicious sites of their choosing. This type of attack can have widespread consequences, affecting all users and devices relying on the compromised DNS server for name resolution.

Verify if DNS is being handled by Sophos

Test connection to internally hosted domain

The quickest way to verify if DNS is being handled by Sophos is to check if this URL is accessible.

https://dns.access.sophos.com



SOPHOS

Test connection to internally hosted domain.

dns.access.sophos.com is an internally hosted domain which will only get resolved if the client is connected to the Sophos DNS Server properly else it will return ERR_NAME_NOT_RESOLVED error.

Check if DNS Protection can resolve for your Location.

Manual Queries – Using nslookup (without specifying a particular DNS server address)

```
C:\>nslookup dns.access.sophos.com
Server:  dns.google
Address:  8.8.8.8

Name:    dns.access.sophos.com
```

When 'other' public DNS server is being used. Will not resolve dns.access.sophos.com

```
C:\>nslookup dns.access.sophos.com
Server:  UnKnown
Address:  172.16.16.16

Non-authoritative answer:
Name:    dns.access.sophos.com
Address:  65.2.44.210
```

When DNS Protection is set up correctly, but end device is configured to query an internal DNS server.

```
C:\>nslookup dns.access.sophos.com
Server:  resolver4.dnsprotection.sophos.com
Address:  193.84.4.4

Name:    dns.access.sophos.com
Address:  43.205.193.65
```

When DNS Protection is set up correctly and end device is configured to query the DNS Protection servers.

Manual Queries – Using nslookup (without specifying a particular DNS server address)

1. When 'other' public DNS server is being used, it will not resolve dns.access.sophos.com. This indicates the DNS Protection is not set up correctly and the end devices are not configured to query the Sophos DNS Protection Resolver addresses.
2. When DNS Protection is set up correctly, but end device is configured to query an internal DNS server which is being used as a Forwarder.
3. When DNS Protection is set up correctly and end device is configured to query the DNS Protection servers.

Manual Queries – Using nslookup and dig

Manual Queries– Using nslookup and DNS Protection Resolver IP Addresses.

```
> nslookup dns.access.sophos.com 193.84.4.4
Server:  resolver4.dnsprotection.sophos.com
Address:  193.84.4.4

Name:    dns.access.sophos.com
Address:  13.235.3.251

> nslookup dns.access.sophos.com 193.84.5.5
Server:  resolver5.dnsprotection.sophos.com
Address:  193.84.5.5

Name:    dns.access.sophos.com
Address:  13.235.3.251
```

Note: This is to only check if DNS Protection servers can resolve DNS requests from your locations.

Nslookup on a Windows Device

You can use nslookup - just remember that it doesn't necessarily use the same DNS server in the same order as the underlying operating system does.

A successful response indicates that DNS Protection is set up correctly for your location but does not necessarily indicate that DNS Protection is being used to resolve actual DNS requests.

Note:

This is to only check if DNS Protection servers can resolve DNS requests from your locations.

nslookup may not work for querying DNS Protection if the devices are configured to use a local DNS Server or DNS Cache to forward requests to DNS Protection.

Check if DNS Protection can resolve for your Location

Manual Queries – Using dig on a Linux device

```
sophos@Linux-Client:~$ dig dns.access.sophos.com

; <<>> DiG 9.18.1-1ubuntu1.1-Ubuntu <<>> dns.access.sophos.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 390
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;dns.access.sophos.com.         IN      A

;; AUTHORITY SECTION:
dns.access.sophos.com.  59      IN      SOA     ns-494.awsdns-61.com. awsdns-hostmaster.amazon
.com. 1 7200 900 1209600 86400

;; Query time: 7 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Thu Mar 14 13:42:45 EDT 2024
;; MSG SIZE  rcvd: 128
```

SOPHOS

Manual Queries – Using dig on a Linux device

DNS protection can resolve for the location as all settings are configured correctly.

Check if end-device is using DNS Protection

PowerShell's Resolve-DnsName cmdlet

```
PS C:\> Resolve-DnsName dns.access.sophos.com

Name                           Type TTL   Section    PrimaryServer          NameAdministrator           SerialNumber
----                           ---- ---   -------    -------------          -----------------           ------------
dns.access.sophos.com          SOA  60    Authority  ns-494.awsdns-61.com   awsdns-hostmaster.amazon.co 1
                                                                            m


PS C:\> Resolve-DnsName -name dns.access.sophos.com -server 8.8.8.8 -type NS

Name                           Type   TTL   Section    NameHost
----                           ----   ---   -------    --------
dns.access.sophos.com          NS     21600 Answer     ns-1450.awsdns-53.org
dns.access.sophos.com          NS     21600 Answer     ns-2016.awsdns-60.co.uk
dns.access.sophos.com          NS     21600 Answer     ns-494.awsdns-61.com
dns.access.sophos.com          NS     21600 Answer     ns-625.awsdns-14.net
```

When DNS Protection is not in use.

```
PS C:\> Resolve-DnsName dns.access.sophos.com

Name                                           Type   TTL   Section    IPAddress
----                                           ----   ---   -------    ---------
dns.access.sophos.com                          A      5     Answer     43.205.193.65
```

When DNS Protection is configured correctly and in use.

Manual Queries – PowerShell's Resolve-DnsName cmdlet

Note: nslookup is the classic tool for testing DNS resolution, but it does not make use of the system's DNS client. You will not necessarily get the same response running nslookup as a regular system application or browser would get.

The best option when trying to emulate what system applications are seeing is to use the Resolve-DnsName cmdlet. This requires the use of PowerShell.

You can also use Resolve-DnsName to check a specific server, do different types of queries etc

https://learn.microsoft.com/en-us/powershell/module/dnsclient/resolve-dnsname?view=windowsserver2022-ps

- Windows OS has a DNS resolver subsystem used by most apps
  - Nslookup does not use this, may choose a different DNS server
- Every real or virtual network interface can have different DNS server config

```
PS C:\> Get-DnsClientServerAddress

InterfaceAlias               Interface Address ServerAddresses
                             Index     Family
--------------               --------- ------- ---------------
Local Area Connection* 10           12 IPv4    {100.64.0.3}
Local Area Connection* 10           12 IPv6    {}
Ethernet                            13 IPv4    {10.46.149.1, 10.46.10.1}
Ethernet                            13 IPv6    {}
Loopback Pseudo-Interface 1          1 IPv4    {}
Loopback Pseudo-Interface 1          1 IPv6    {fec0:0:0:ffff::1, fec0:0:0:ffff::2, fec0:0:0:ffff::3}
```

- Each interface has a 'Metric' (not the same as a routing metric or Index) that dictates which DNS server is queried first

```
PS C:\> Get-NetIPInterface | Select-Object -Property InterfaceAlias, InterfaceMetric, InterfaceIndex | Sort-Object -Property InterfaceMetric

InterfaceAlias               InterfaceMetric InterfaceIndex
--------------               --------------- --------------
Local Area Connection* 10                  1             12
Ethernet                                  25             13
Local Area Connection* 10                 25             12
Loopback Pseudo-Interface 1               75              1
Loopback Pseudo-Interface 1               75              1
```

- If the first doesn't respond, it will send queries to the others

SOPHOS

Windows: If nslookup works, but browser or Resolve-DnsName don't

In the examples, we can see that two interface on this device are configured with DNS Server addresses - 'Ethernet' and 'Local Area Connection 10'

Running the second set of commands shows the InterfaceMetric which reveals that the system will first use the DNS Server for Local Area Connection 10, before sending the query to the servers configured for 'Ethernet'.

Windows DNS server configurations are tied to specific network interfaces. Windows has a DNS client service that performs DNS lookups on behalf of most apps on the system.

The DNS Client service queries the DNS servers in the following order:

1. The DNS Client service sends the name query to the first DNS server on the preferred adapter's list of DNS servers and waits one second for a response.
2. If the DNS Client service does not receive a response from the first DNS server within one second, it sends the name query to the first DNS servers on all adapters that are still under consideration and waits two seconds for a response.
3. If the DNS Client service does not receive a response from any DNS server within two seconds, the DNS Client service sends the query to all DNS servers on all adapters that are still under consideration and waits another two seconds for a response.
4. If the DNS Client service still does not receive a response from any DNS server, it sends the name query to all DNS servers on all adapters that are still under consideration and waits four seconds for a response

5. If it the DNS Client service does not receive a response from any DNS server, the DNS client sends the query to all DNS servers on all adapters that are still under consideration and waits eight seconds for a response.

This aspect of DNS configuration on Windows is used by ZTNA – by setting up a fake DNS server address (100.64.0.3) on a virtual interface and setting it with the lowest metric, ZTNA can respond to queries for services that it manages and redirect connections to the ZTNA gateway. But this can also be used by other products and may disrupt configurations provided by DHCP settings or direct configuration of a Wireless interface.

Another issue we've seen that could be exposed by these commands, is that a customer has a dual IPv4/IPv6 network. If their IPv6 setup provides IPv6 addresses for DNS servers, those servers could be used instead of the correct DNS Protection service. Either

(a) change DHCP6 configuration to not provide DHCP server addresses, or provide fake addresses

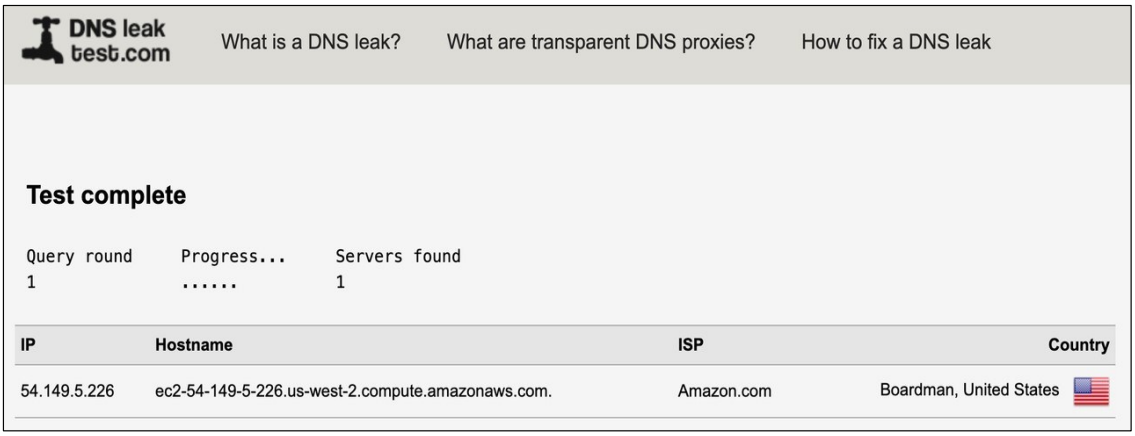
(b) if using a local DNS server on IPv6, make sure that it the local server can forward all queries to DNS Protection over IPv4

DNS Leak Test

Verify if DNS is being handled by Sophos

DNS Leak Test

To get more insight into where your DNS lookups are being resolved, a useful tool is the site www.dnsleaktest.com



Result from a device that is using Sophos DNS Protection, whose requests are handled by the US -West -2 location in Oregon, USA

SOPHOS

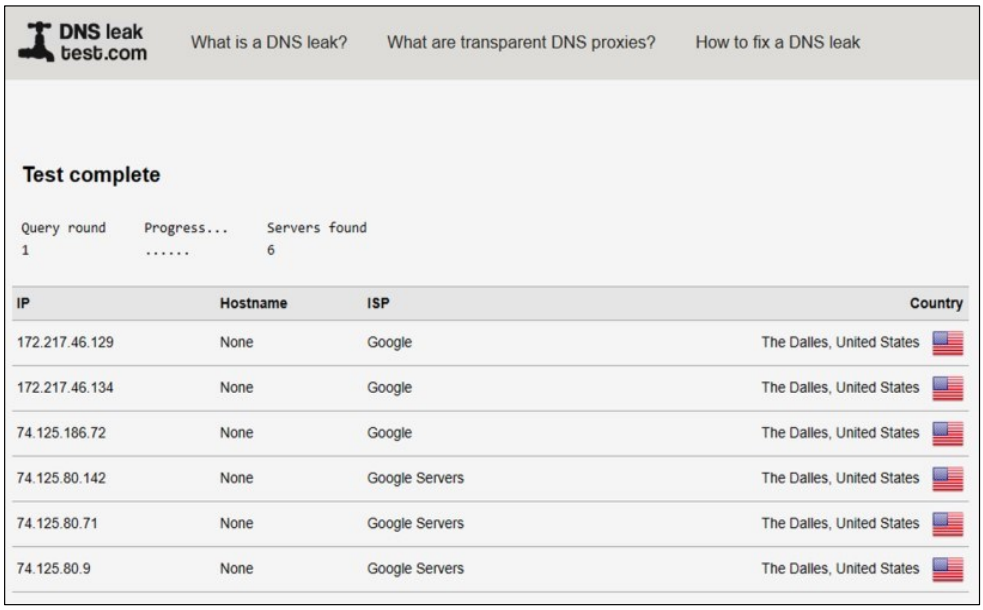
To get more insight into where your DNS lookups are being resolved, a useful tool is the site www.dnsleaktest.com

This site causes your browser to trigger DNS requests to customized domain names. The DNS servers for the site can then observe incoming requests to your customized domain names and tell you where those requests came from.

It can give you a clue about which DNS service is actually handling your requests. And if DNS Protection is being used, it will actually give you information about which of our POPs is handling your requests.

Result from a device that is using Sophos DNS Protection, whose requests are handled by the US-West-2 location in Oregon, USA

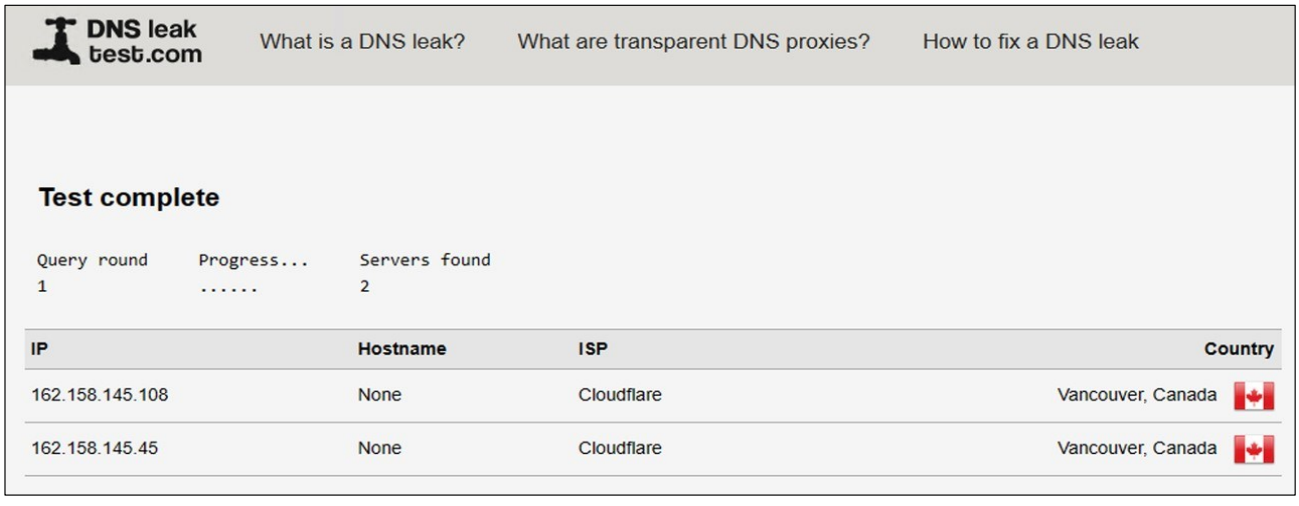
Note: This is particularly useful if you think the device is configured to use DNS Protection, but when you test it by looking up dns.access.sophos.com, it fails to resolve correctly.



Result for a device using Google's 8.8.8.8 service

SOPHOS

Result for a device using Google's 8.8.8.8 service

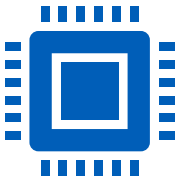


Result for a device using Cloudflare 1.1.1.1

SOPHOS

Result for a device using Cloudflare 1.1.1.1.

Why DNS traffic is not being resolved by DNS Protection?



ISP-level diversion

Some ISPs divert all outbound DNS queries to be handled by their own DNS Resolvers.

In-browser diversion

Most modern browsers support direct querying of 'Secure DNS' services via DNS over HTTPS (DoH), including Firefox, Chrome, and Edge.

ISP-level diversion

Some ISPs (notably Comcast) divert all outbound DNS queries to be handled by their own DNS Resolvers. This is not widely publicized but is exposed to customers as a security feature. It can be turned off in the Comcast customer portal, although reports suggest that it does not always stay 'off'. Some customers have reported that they need to work with Comcast support in order to get it turned off permanently.

Note:

- If it is found that the customer's ISP is hijacking their DNS queries, ask the customer to reach out to their ISPs technical support team to assist them in disabling any DNS redirection on the customer's router/modem.
- Comcast offers a feature called 'SecurityEdge', which is a DNS filtering service that overrides anything set at the client device level. If an organization is behind a Comcast modem with SecurityEdge enabled, all DNS queries will be redirected to NetActuate or Comcast DNS servers. A customer may be able to disable the feature by logging into their Comcast portal and turning off "SecurityEdge" under "Internet" tab. If the customer is not sure whether their Comcast service is enabled with SecurityEdge or how to disable it, ask them to contact the Comcast support team.

In-browser diversion

Most browsers now provide a feature allowing them to directly query 'Secure DNS' services, usually using DNS over HTTPS. Firefox, Chrome and Edge all offer this feature. They all give customers the choice between a handful of built-in providers that they know about.

Check browser settings for DNS over HTTPS

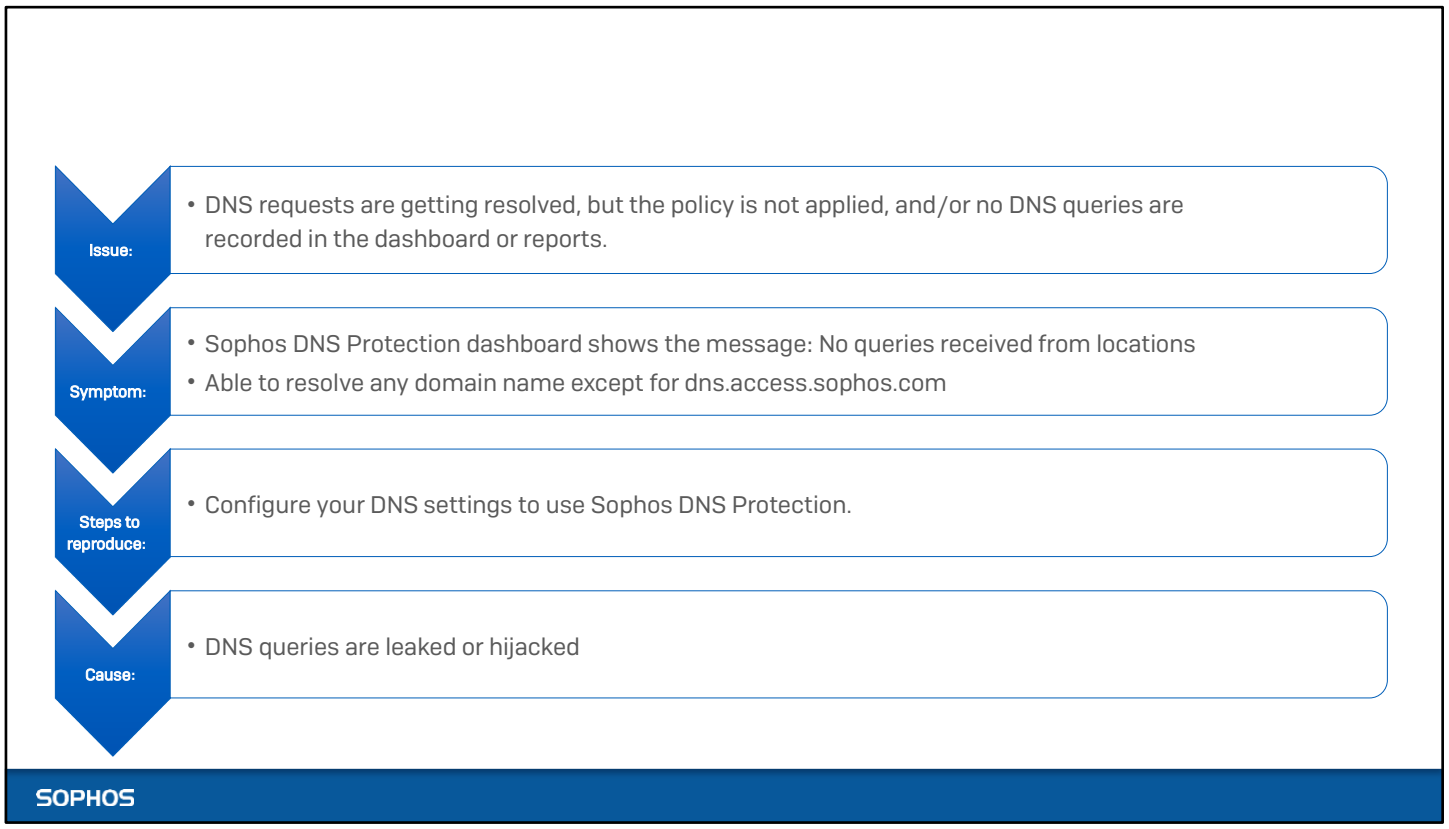
Chrome: Settings > Privacy and security > Security > Advanced > Always use secure connections

Edge: Settings > Privacy, Search and Services > Security > Use secure DNS to specify how to lookup the network address for websites

Firefox: Settings > Privacy & Security > DNS over HTTPS

Safari: Safari doesn't have its own settings - to use DNS over HTTPS with Safari, but this can be enabled in Mac system preferences.

DNS Protection policies not getting applied



Issue:

- DNS requests are getting resolved, but the policy is not applied, and/or no DNS queries are recorded in the dashboard or reports.

Symptom:

- Sophos DNS Protection dashboard shows the message: No queries received from locations
- Able to resolve any domain name except for dns.access.sophos.com **Steps to reproduce:**
- Configure your DNS settings to use Sophos DNS Protection.

Cause:

- DNS queries are leaked or hijacked

DNS Protection policies not getting applied (cont.)

Resolution:

- Review your DNS configuration using some of the below -mentioned tools
  - ipconfig for Windows or dig for Linux and macOS
  - nslookup
  - ping
  - Traceroute
- Check if you have leaked or hijacked DNS queries
  - Go to https://www.dnsleaktest.com/
  - Do a standard or extended test.
  - Review the result.

***Note** : Your DNS queries are not compromised if no third -party ISPs show.*

SOPHOS

Resolution:

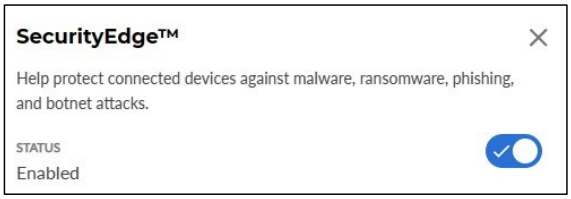
- Review your DNS configuration using some of the below-mentioned tools
- ipconfig for Windows or dig for Linux and macOS
- nslookup
- ping
- Traceroute
- Check if you have leaked or hijacked DNS queries 1. Go to https://www.dnsleaktest.com/
  2. Do a standard or extended test.
  3. Review the result.

Note: Your DNS queries are not compromised if no third-party ISPs show.

DNS Protection policies not getting applied (cont.)

If customer's ISP is Comcast:	Comcast uses a feature called **Comcast Business SecurityEdge** that redirects DNS traffic to their DNS servers. This is turned on by default.
	Ask the customer to turn off this feature.

1. Sign in to your Comcast Business account.
2. Scroll down and go to Subscribed Services > Business Internet.
3. Click MANAGE INTERNET.
4. Click the > symbol next to SECURITYEDGE to open the status page.
5. Toggle the switch to off.



SOPHOS

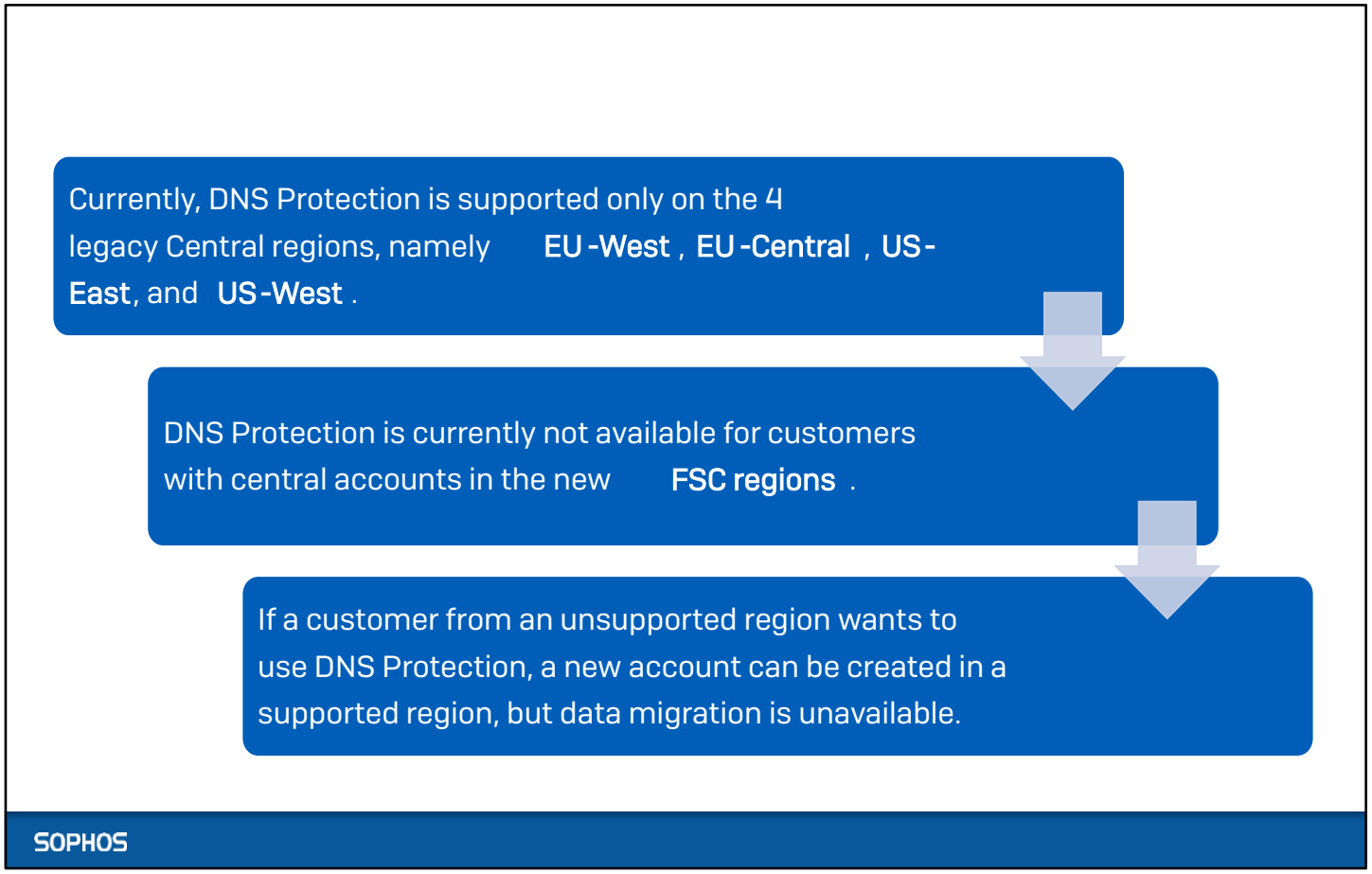
Steps to turn off SecurityEdge in Comcast

1. Sign in to your Comcast Business account.
2. Scroll down and go to Subscribed Services > Business Internet.
3. Click MANAGE INTERNET.
4. Click the > symbol next to SECURITYEDGE to open the status page.
5. Toggle the switch to off.

https://support.sophos.com/support/s/article/KB-000045817?language=en_US&c__displayLanguage=en_US

Note:
This feature sometimes automatically turns on by itself. To turn it off permanently, ask the customers to get assistance from their Comcast support team.

DNS Protection not supported in Sophos Central Region



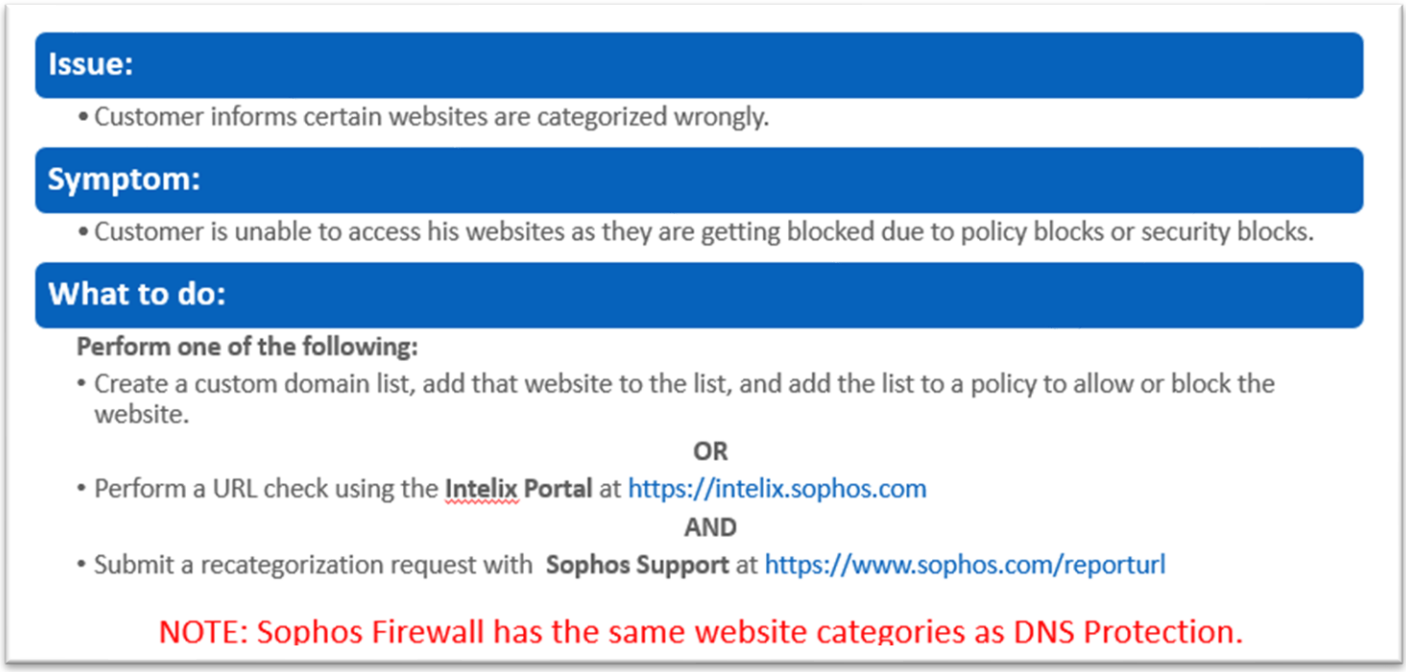
Currently, DNS Protection is supported only on the 4 legacy Central regions, namely EU-West, EU-Central, US-East, and US-West.

DNS Protection is currently not available for customers with central accounts in the new FSC regions.

If a customer from an unsupported region still wants to use DNS Protection, then we can create a new account in one of the supported regions. However, data migration is currently not available.

Misscategorized Customer's Websites

Customer websites categorized wrongly



Issue:

Customer informs certain websites are categorized wrongly.

Symptom:

Customer is unable to access his websites as they are getting blocked due to policy blocks or security blocks.

What to do:

Create a custom domain list, add that website to the list, and add the list to a policy to allow or block the website.

OR

Confirm the website category using the Intelix Portal at https://intelix.sophos.com to perform a URL check.

https://support.sophos.com/support/s/article/KB-000033301?language=en_US

Submit a recategorization request with Sophos Support at

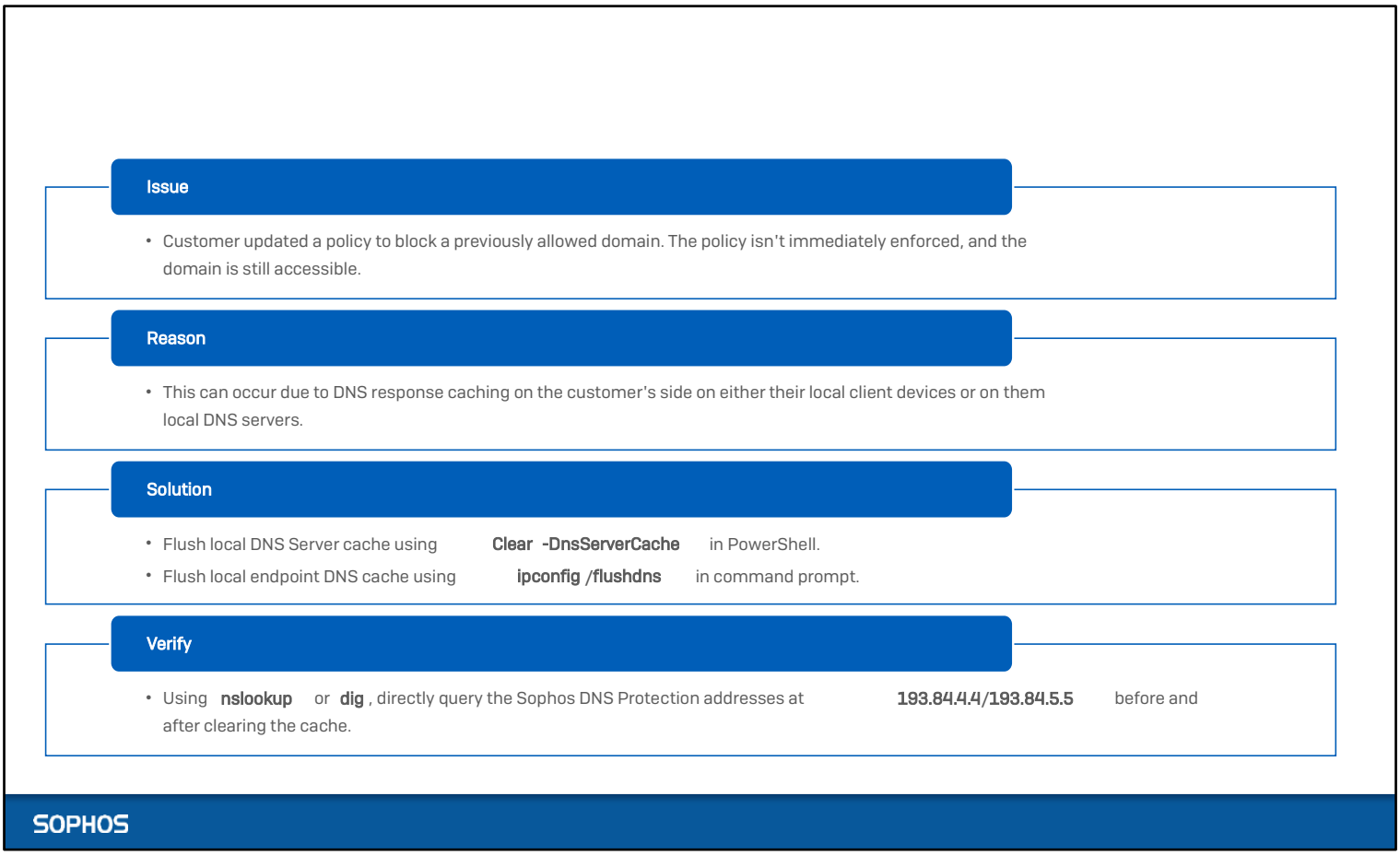
https://www.sophos.com/reporturl

To do this, do as follows:

- Under Submit a Sample, click Web Address (URL).
- In Web Address (URL), enter the website you want us to recategorize.
- In Product/Services, select Sophos XG Firewall (Uses same website categories as DNS Protection)
- In Comments, mention that this recategorization request is for DNS Protection, not Sophos Firewall. You can also add other details about your request.
- Add your personal details.
- Click Submit URL.

Note: Sophos Firewall has the same website categories as DNS Protection.

Updated policy isn't immediately enforced



Issue

- Customer updated a policy to block a previously allowed domain. The policy isn't immediately enforced, and the domain is still accessible.

Reason

- This can occur due to DNS response caching on the customer's side on either their local client devices or on their local DNS servers. In this case, the domain is accessible until its DNS TTL expires.

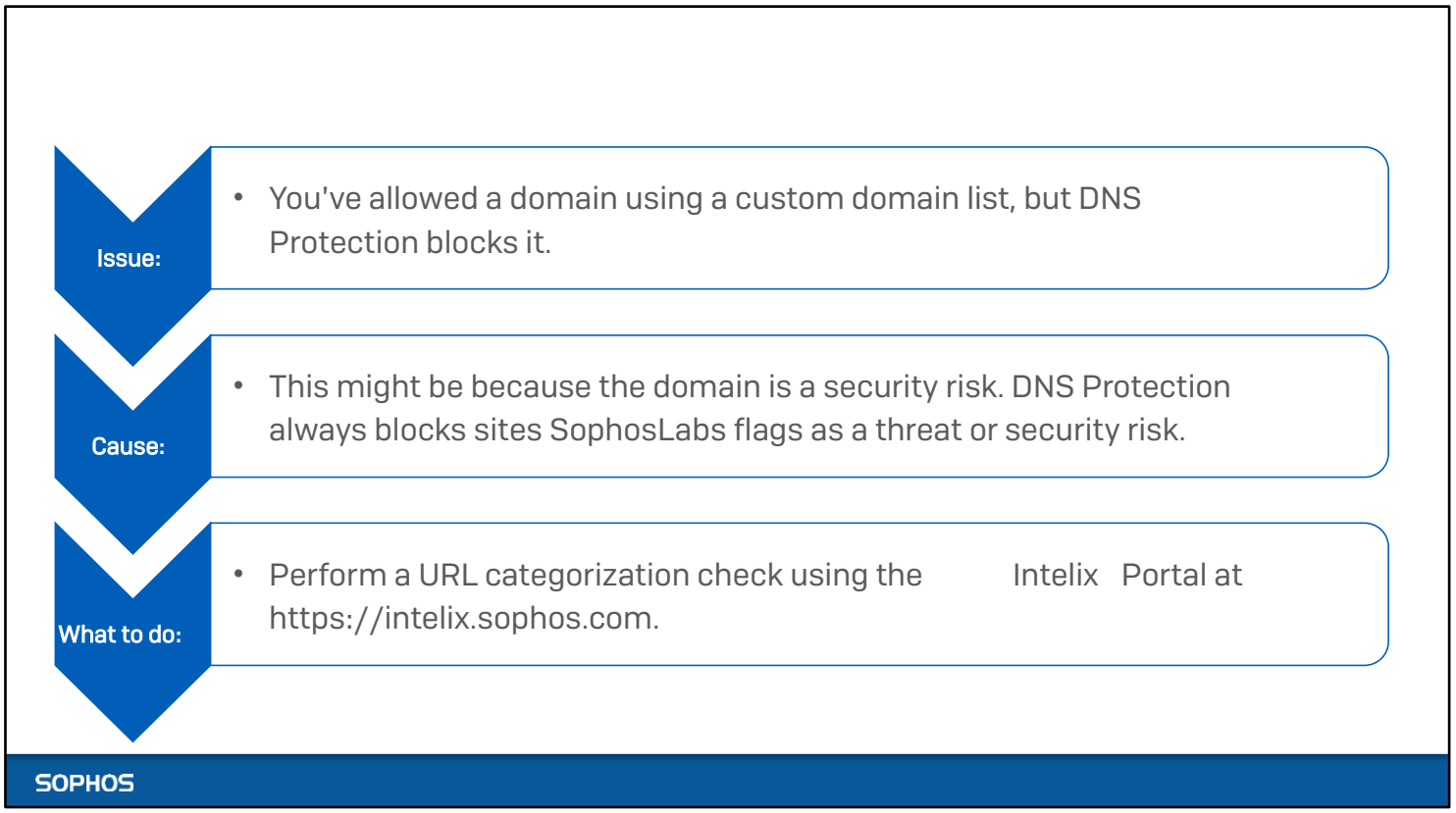
Solution

- Flush local DNS Server cache using **Clear-DnsServerCache** in PowerShell or **ipconfig/flushdns** or **dnscmd /clearcache** in command prompt or go to **DNS Manager** – select **DNS Server - Action - Clear Cache**.
- Flush local endpoint DNS cache using **ipconfig /flushdns** in command prompt or **Clear-DnsClientCache** in PowerShell.

Verify

- Using nslookup or dig, directly query the Sophos DNS Protection addresses at 193.84.4.4/193.84.5.5 before and after clearing the cache.

Allowed domain is blocked



Issue:

- You've allowed a domain using a custom domain list, but DNS Protection blocks it.

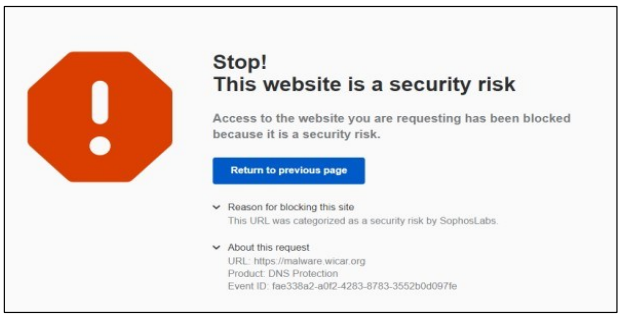
Cause:

- This might be because the domain is a security risk. DNS Protection always blocks sites SophosLabs flags as a threat or security risk.

What to do:

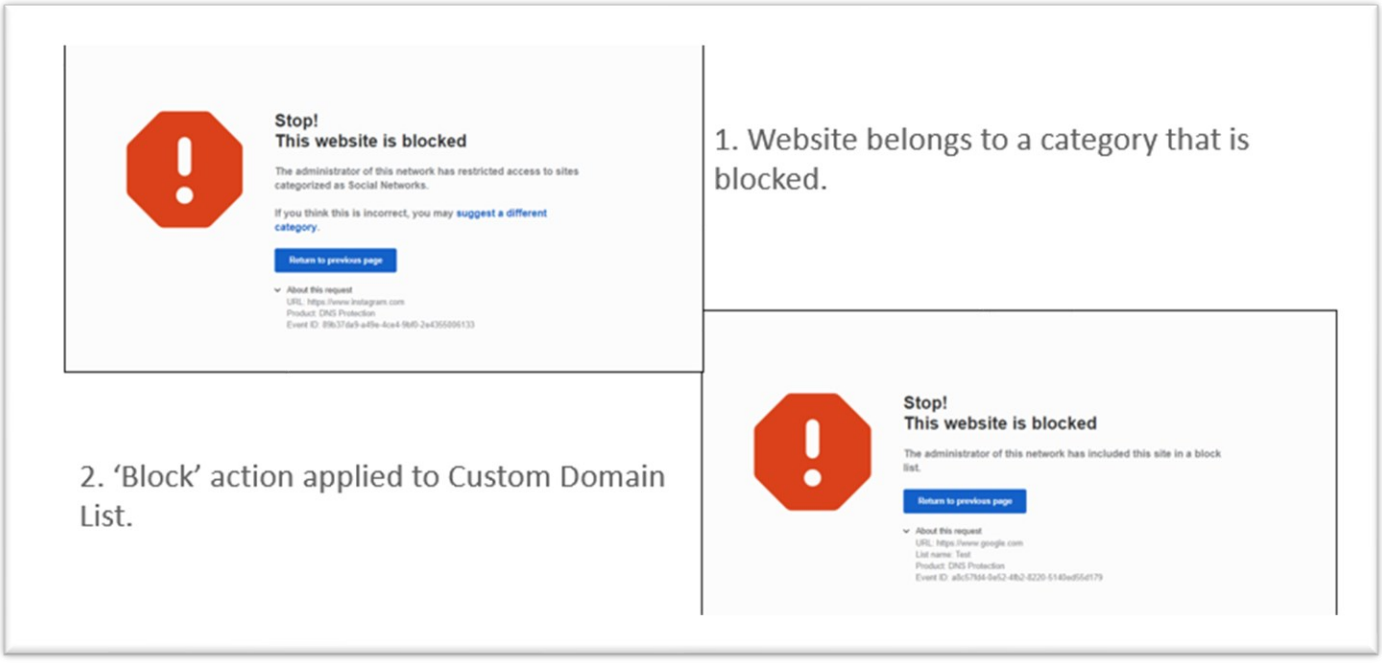
- Perform a URL categorization check using the **Intelix Portal** at *https://intelix.sophos.com*.

Block Pages



Website is blocked as its reputation has been rated as malicious by SophosLabs

Block page displayed when users attempt to access a website whose reputation has been rated as malicious by SophosLabs and hence blocked due to Security Block by DNS Protection.



1. Block page displayed when a user tries to access a website that belongs to a web category that has the 'Block' action specified in the DNS Protection Policy.

2. Block page displayed when a user tries to access a website that is listed in a custom domain list with a block action in the policy setting.

Duplicate IP address error

- Error message displayed if customer tries to register IP address or domain already in use across Central accounts.
- Response messages include tracing with traceID and correlationID values for reference.

SOPHOS

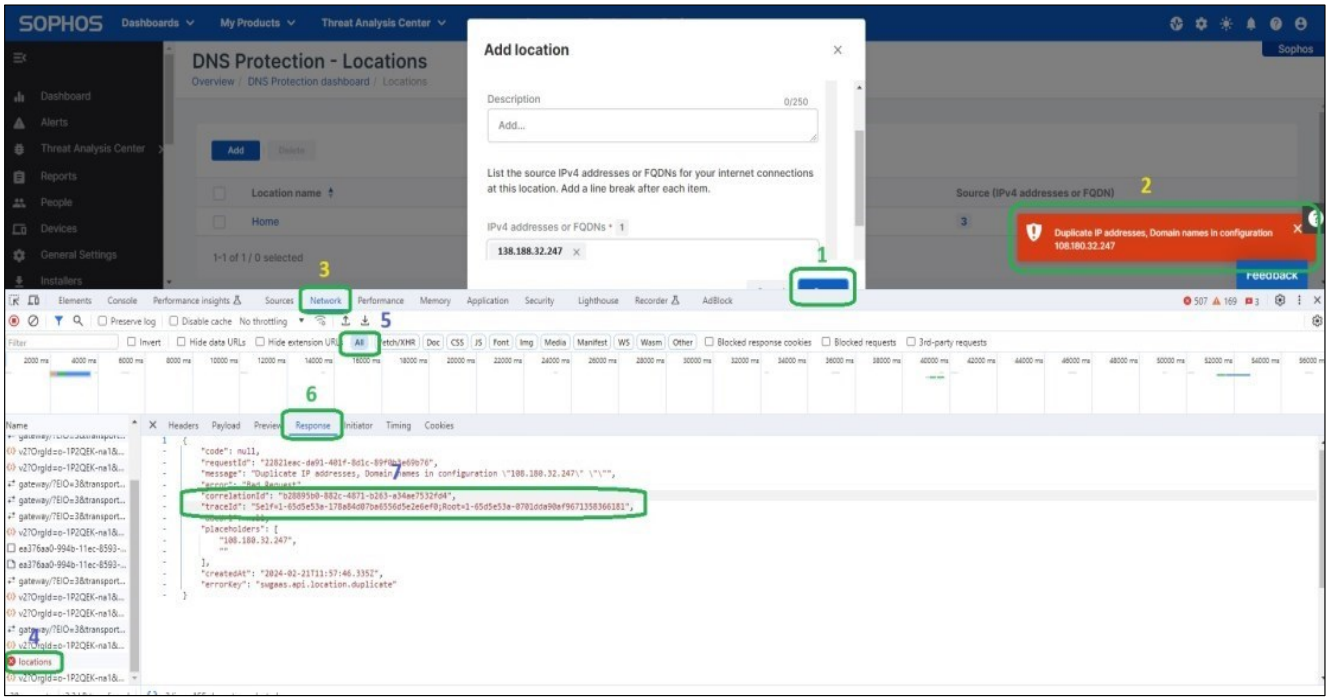
When customers attempt to register an IP address or Domain name as a location in DNS Protection, they will see this error message if that IP or domain names has already been registered under the customer's or any other Central account.

This message may not always be very descriptive about what exactly is the error encountered by the customer. Hence it might be necessary to investigate it further by making use of Logz.io.

Traceable values are included in the response messages as part of the payload the customer's browser will receive when he encounters this error.

Look out for two values: traceID and correlationID

Finding traceID and correlationID in the browser.

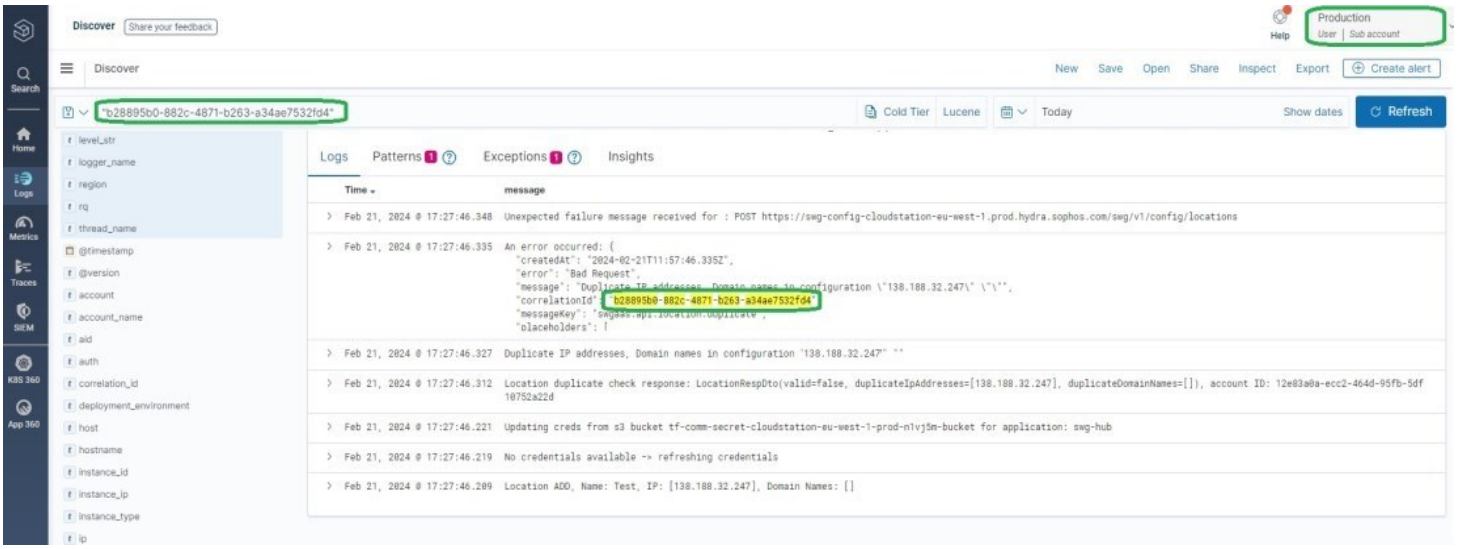


1. Login to the Central account and attempt to add the same IP address or Domain name that resulted in the error message previously.
2. Right click in the web browser -> **Inspect** -> **Network** Tab -> **All** -> Click on **Locations** under **Name** -> **Response**

Note: 'Locations' will appear once you click on the 'Save' option in the web page in Central.

The traceID and/or the correlationID values can then be searched for in Logz.io

Searching in Logz.io



1. Select **Production** sub-account.
2. Enter the traceID or correlationID values in the search bar.
3. Set the time settings.

Note: This will mostly be useful when the customer encounters error that is not very descriptive.

Adding an Unresolving FQDN as a Location

Adding an Unresolving FQDN as a Location

- Error message displayed when an adding an unresolving FQDN as a location.
- Same traceable values of traceID and correlationID can be used to further inspect.

SOPHOS

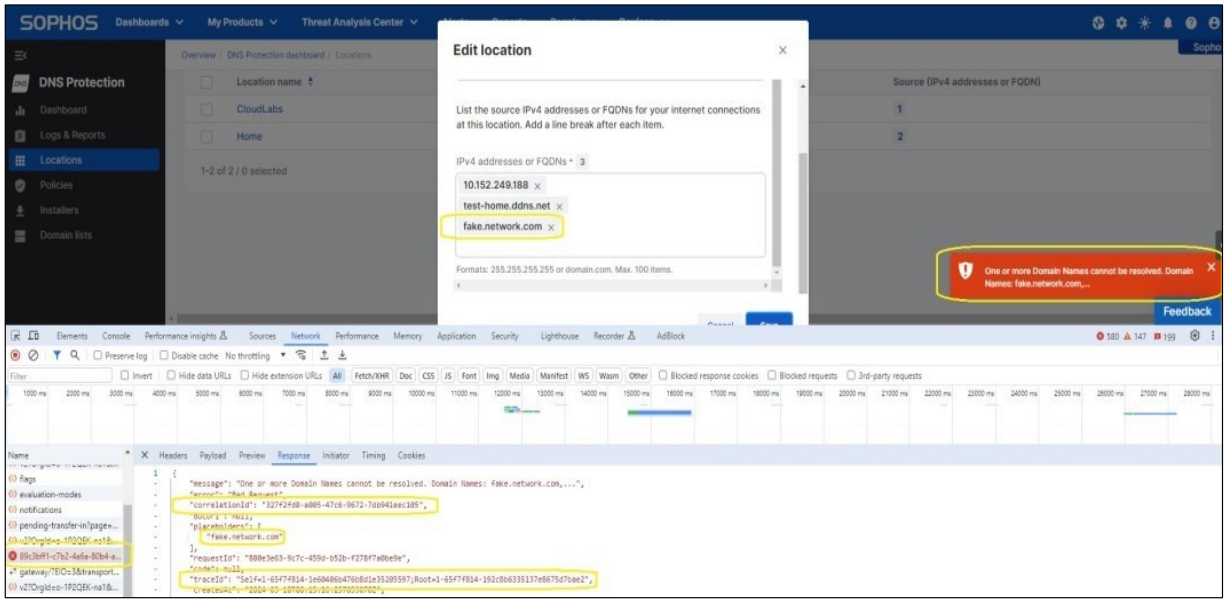
This error message will get displayed when an attempt to add an FQDN that does not resolve to an IP address is made as a new Location.

The same traceable values discussed earlier; traceID and correlationID can be used to further investigate the error in Logz.io.

Finding traceID and correlationID in the browser.

Adding an Unresolving FQDN as Location

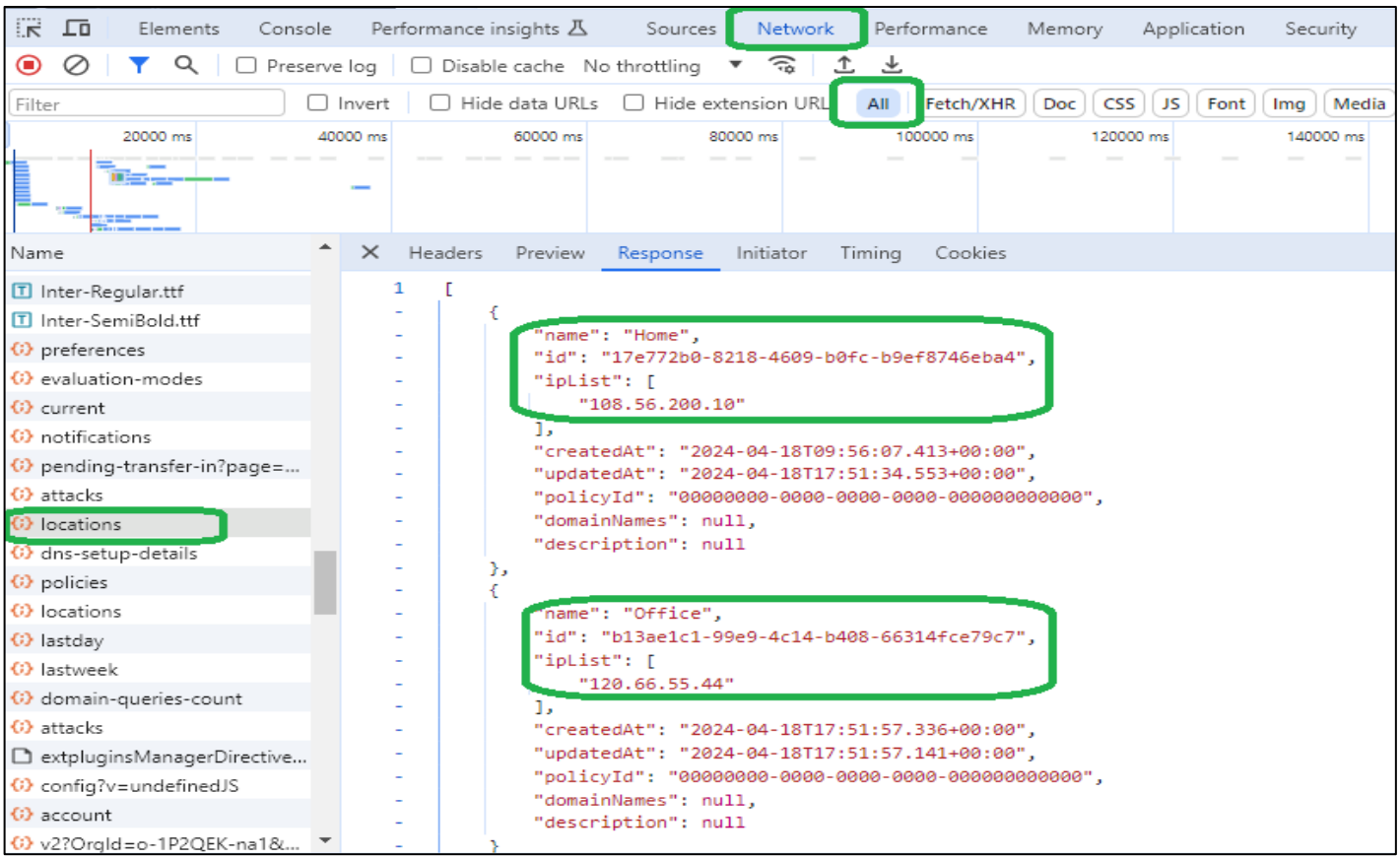
Upon investigating using web browser developer tools



SOPHOS

The traceID and/or the correlationID values can then be searched for in Logz.io

Finding additional useful information – Location ID



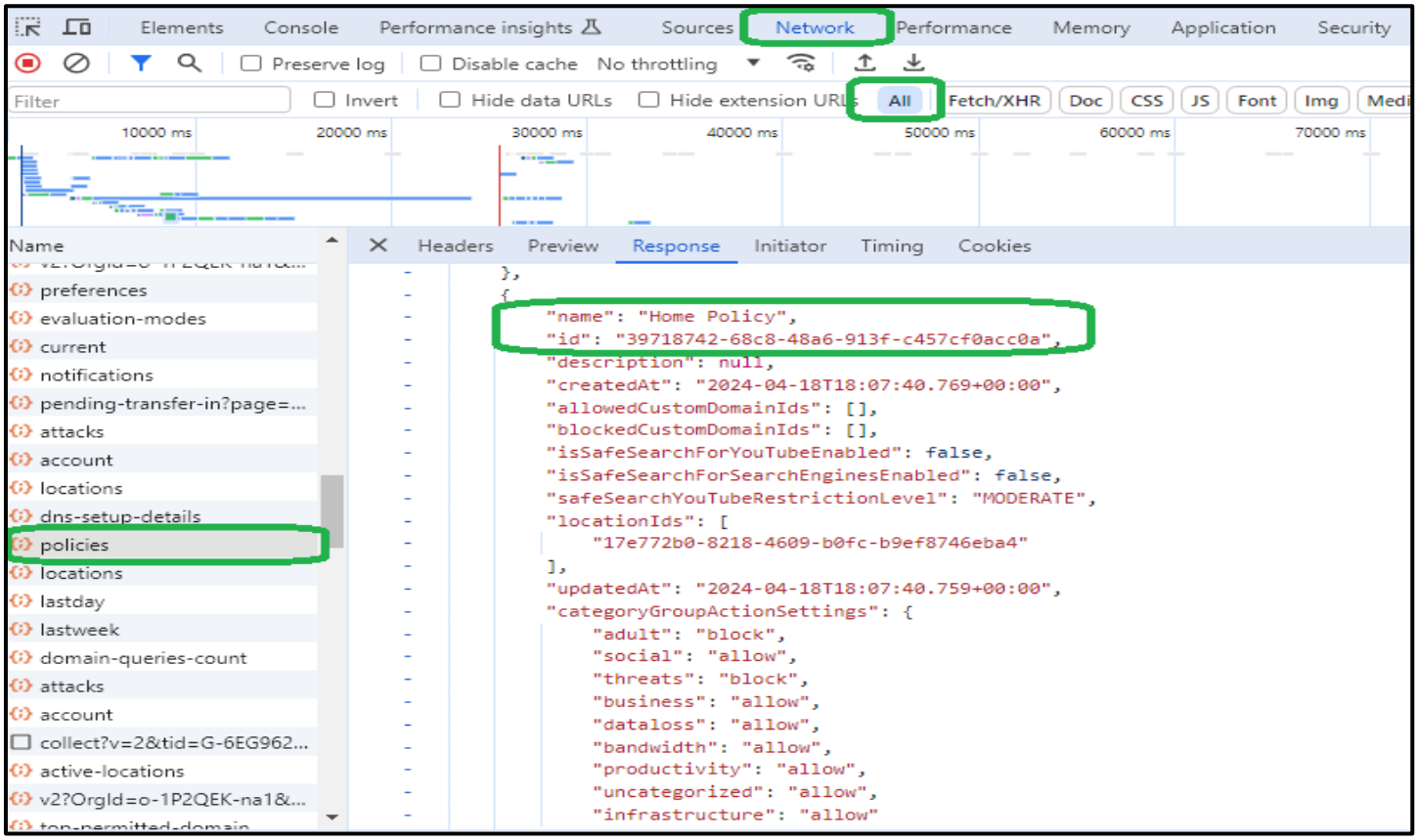
Using web browser developer tools – Find Location ID value:

1. Open **developer tools** in web browser -> **Dashboard** under DNS Protection in Sophos Central.
2. In **developer tools** -> **Network** -> **All** -> **locations** under **Name** -> **Response** -> Find "**name**" and "**id**" values.
3. Search using ID value in Logz.io and adjust the time parameter to find all messages sent by Central regarding that location.

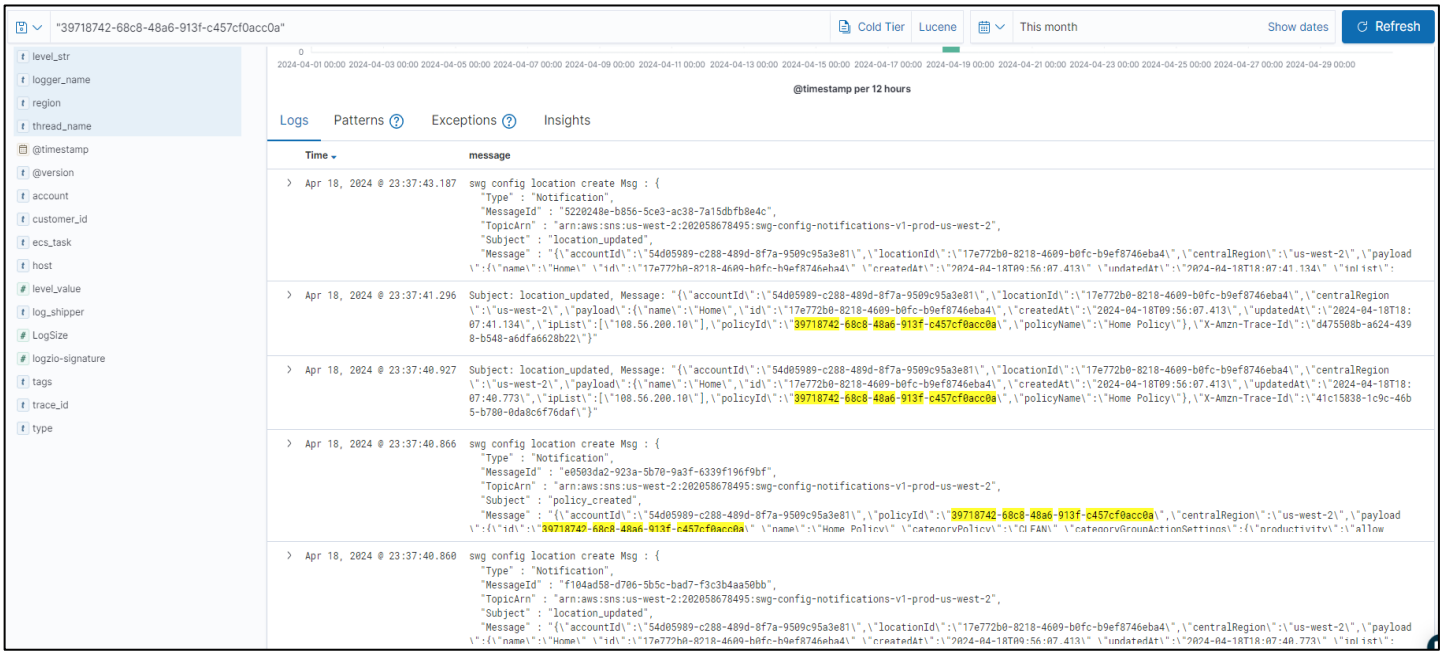
Using Location ID value to search in Logz.io

Finding additional useful information – Policy ID

Using web browser developer tools – Find Policy ID value:

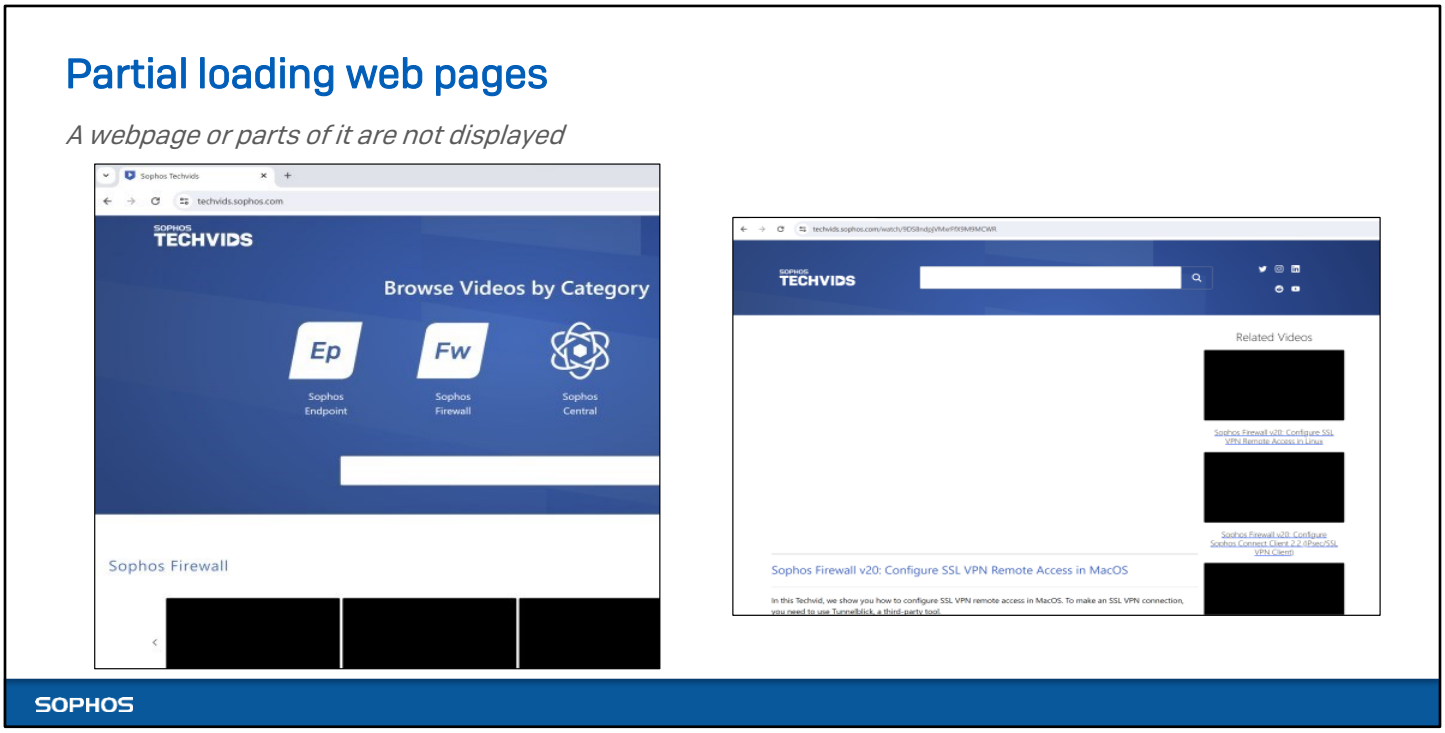


1. Open **developer tools** in web browser -> **Dashboard** under DNS Protection in Sophos Central.
2. In **developer tools** -> **Network** -> **All** -> **policies** under **Name** -> **Response** -> Find "**name**" and "**id**" values.
3. Search using ID value in Logz.io and adjust the time parameter to find all messages sent by Central regarding that location.



Using Policy ID value to search in Logz.io

Partial loading web pages

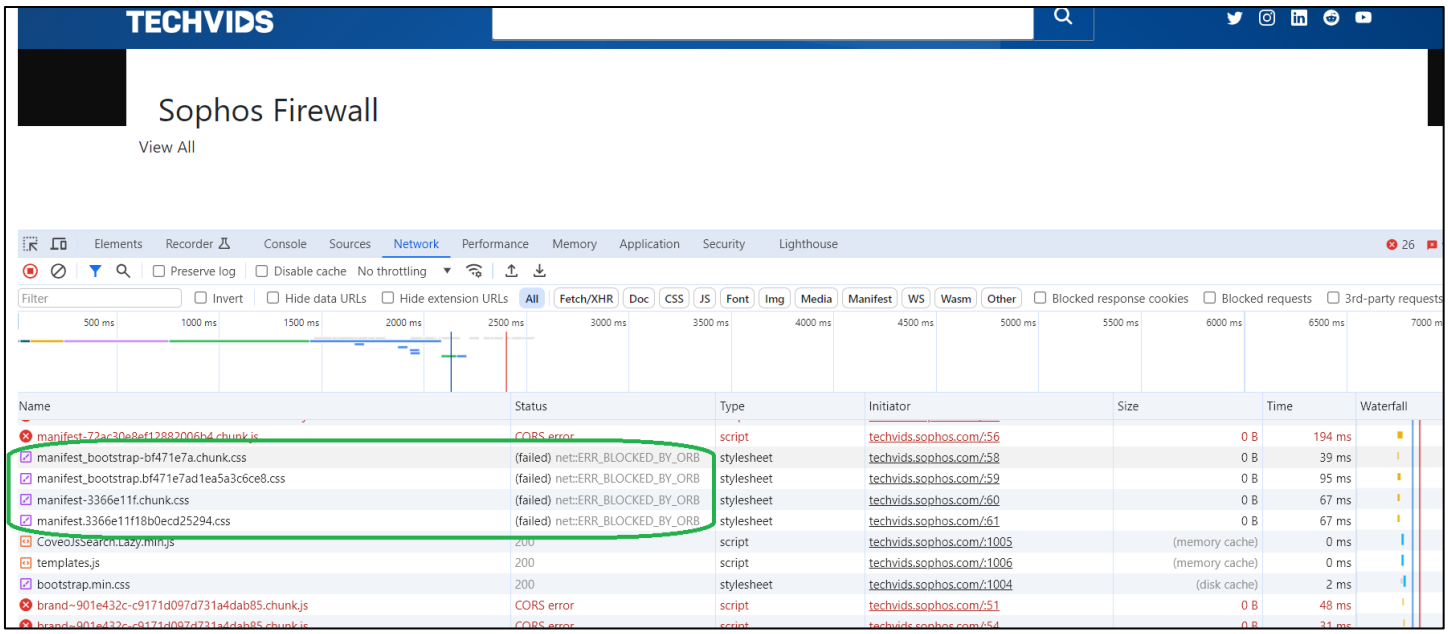


A webpage or parts of it are not displayed

This issue may arise when portions of a web page are concealed, left blank, or display an error message. This situation can occur if the accessed web page contains content from another site, such as an advertisement, which is being blocked. The block could be due to security measures flagging the content as malicious, or it could be a result of a policy block implemented in DNS Protection by the customer or a custom domain list configured to block the domain in question.

Troubleshooting partially loading web pages - 1

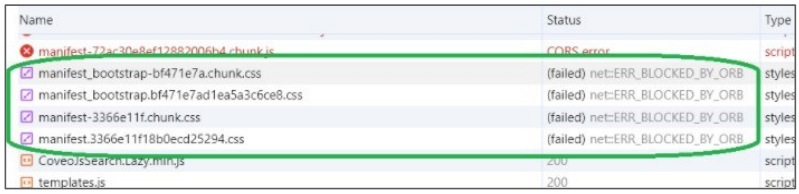
Inspecting web browser data for partially loaded web pages



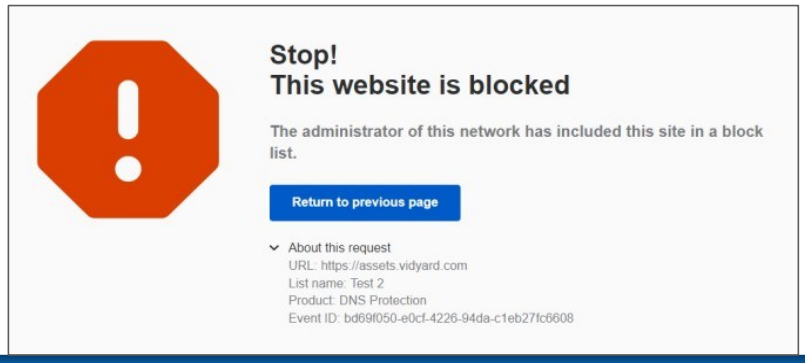
Upon inspecting the web browser data, you may notice some error messages regarding parts of the parent web page that got blocked along with the reason of the failure to load the content.

Troubleshooting partially loading web pages - 2

Inspecting web browser data for partially loaded web pages



Double clicking on the error messages will result to access the URL



In this instance, it is revealed that the site is blocked due to a custom block list in DNS Protection policy.

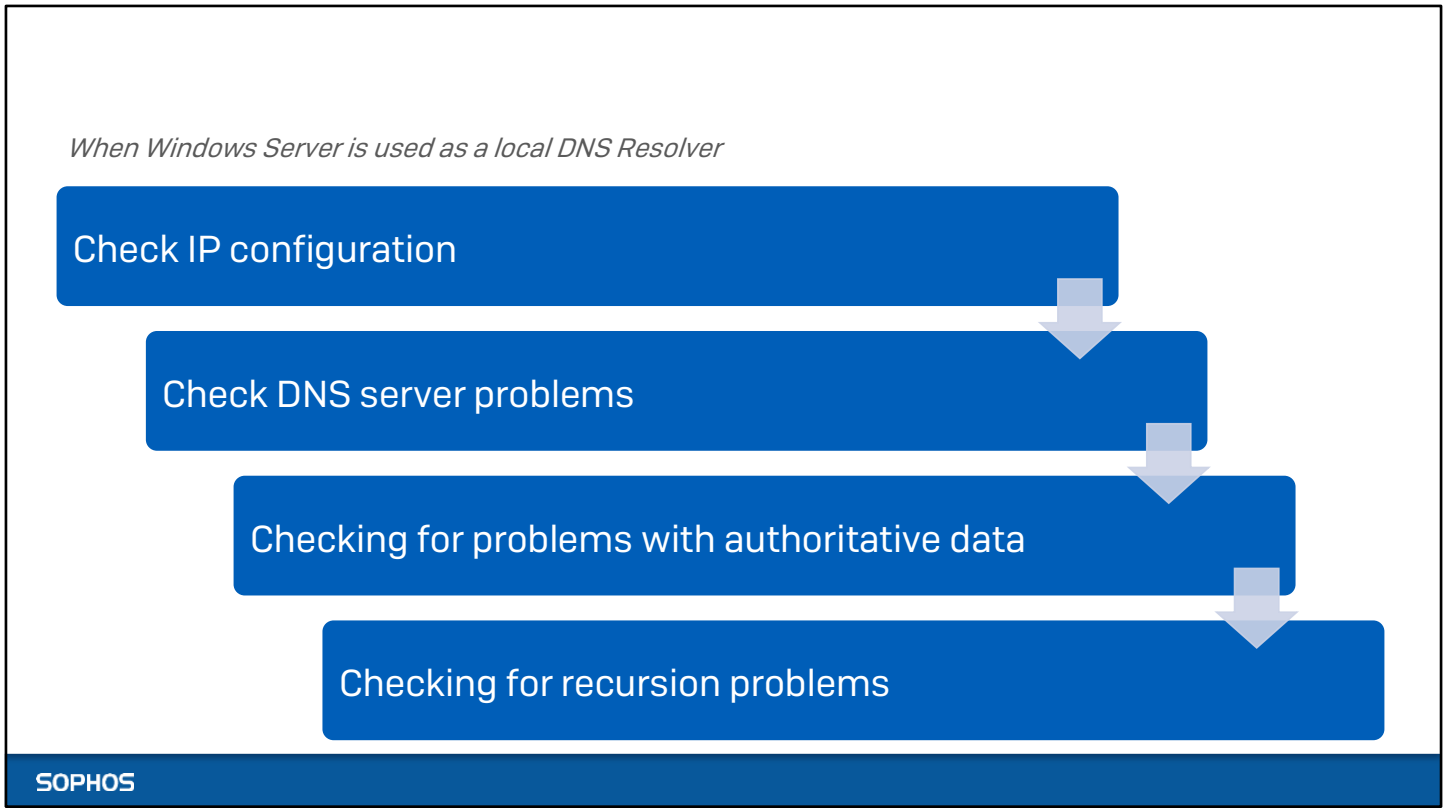
SOPHOS

Double clicking on the error messages will result in an attempt being made to access the URL, resulting in a block page being presented in return.

In this instance, the block page reveals that the site is blocked due to a custom block list in the DNS Protection policy with a block action.

https://learn.microsoft.com/en-us/windows-server/networking/dns/troubleshoot/troubleshoot-dns-server

Validating a Customer's DNS Servers



Check IP configuration

1. Run ipconfig /all at a command prompt, and verify the IP address, subnet mask, and default gateway.

2. Check whether the DNS server is authoritative for the name that is being looked up.

3. Run the command: **nslookup <name> <IP address of the DNS server>**

4. If you get a failure or time-out response, Checking for recursion problems.

5. Flush the resolver cache using the following command: **dnscmd /clearcache** in command prompt or **Clear-DnsServerCache** in PowerShell.

6. Repeat step 3.

Check DNS server problems

Check the following logs to see whether there are any recorded errors:

- Application
- System
- DNS Server

Run the following command and check whether the DNS server is reachable from client computers:
nslookup <client name> <server IP address>

1. If the resolver returns the IP address of the client, the server does not have any problems.

2. If the resolver returns a "Server failure" or "Query refused" response, the zone is probably paused, or the server is possibly overloaded.
   Check the General tab of the zone properties in the DNS console.

3. If the resolver returns a "Request to server timed out" or "No response from server" response, the DNS service probably is not running.
   Try to restart the DNS Server service by entering the following at a command prompt on the server: **net start DNS**

4. If the issue occurs when the service is running, the server might not be listening on the IP address that you used in your nslookup query.
   On the **Interfaces** tab of the server properties page in the DNS console, check if the DNS server is configured to limit service to specific list of IP addresses.

5. If the server is located on another network that is reachable only through an intermediate host (such as a packet filtering router or proxy server).
   The DNS server might be configured to use a non-standard port to listen for and receive client requests instead of the default UDP port 53.
   Check on the intermediate device if it is configured to use default or alternate ports for DNS.
   If not, check if the packet filters or port rules on the firewall to allow traffic on UDP/TCP port 53 and allow if not.

Checking for problems with authoritative data

Check whether the server that returns the incorrect response is a primary server for the zone or a server that's hosting a secondary copy of the zone.

If the server is a primary server

- The issue might be caused due to user error when users enter data into the zone.
- Or due to issues with Active Directory replication or dynamin update.

If the server is hosting a secondary copy of the zone

1. Examine the zone on the primary server by examining the properties of the secondary zone in the DNS console.
    a. If the name is not correct on the primary server, go to step 4.
2. If the name is correct on the primary server, check whether the serial number on the primary server is less than or equal to the serial number on the secondary server.
    a. If it is, modify either the primary server or the secondary server so that the serial number on the primary server is greater than the serial number on the secondary server.
3. On the secondary server, force a zone transfer from within the DNS console or by running the following command: **dnscmd /zonerefresh <zone name>**
4. Examine the secondary server again to see whether the zone was transferred correctly. If not, there is probably a zone transfer problem.

Checking for recursion problems

For recursion to work successfully, all DNS servers that are used in the path of a recursive query must be able to respond and forward correct data. If they can't, a recursive query can fail for any of the following reasons:

- The query times out before it can be completed.
- A server that's used during the query fails to respond.
- A server that's used during the query provides incorrect data.

Begin troubleshooting at the server used in the original query.

- Check if the server forwards queries by examining the Forwarders tab in the DNS console.
- If the "Enable forwarders" checkbox is selected and one or more servers are listed, the server forwards queries.

If the server forwards queries, check for issues affecting the server it forwards queries to.

- If the server is healthy and can forward queries, repeat this step, and examine the server to which this server forwards queries.
- If this server does not forward queries to another server, test whether this server can query a root server by using the following command:

  nslookup

  server <IP address of server being examined>

  set q=NS

If the resolver returns the IP address of a root server:

- There may be a broken delegation between the root server and the name or IP address being resolved.
- **Test a broken delegation.**

  Nslookup

  server <server IP address>

  set norecursion

  set querytype= <resource record type> <FQDN>

If the resolver returns a "Request to server timed out" response:

- Verify if the root hints point to functioning root servers.
- **To view the current root hints**
  1. Start the **DNS console**.
  2. Add or connect to the DNS server that failed a recursive query.
  3. Right-click the server and select **Properties**.
  4. Click **Root Hints**.

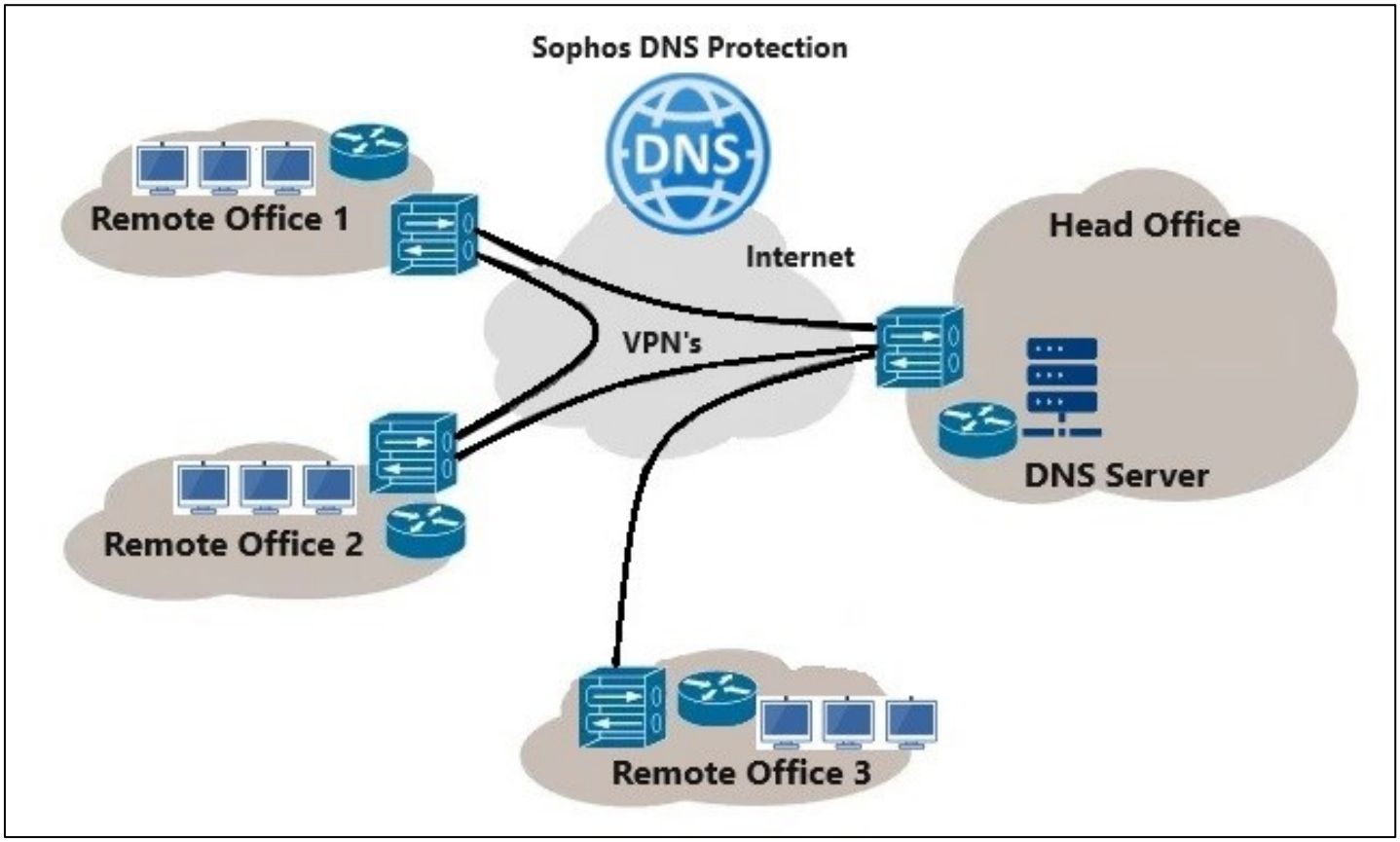
If the root hints are correct:

- Investigate potential network issues or firewall configurations hindering resolver queries to the server.

Consider adjusting the recursive timeout default if necessary.

Scenario: Centrally located DNS Server as Resolver

DNS Server located in the Head Office and the DNS clients are distributed in several Branch Offices

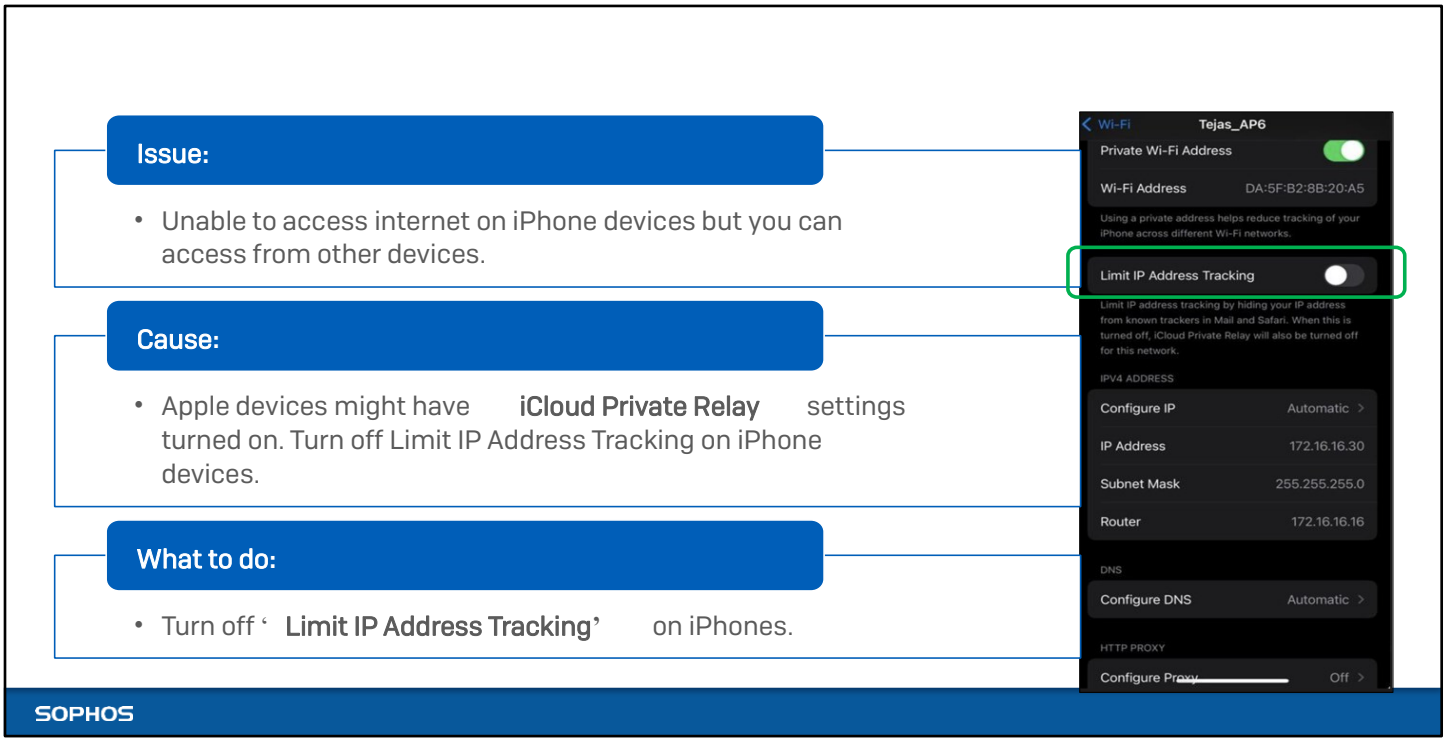


In this scenario, the endpoints located in all the remote offices are configured to reach out to the DNS Server located in the Head Office as their Primary Resolver. As such, all DNS queries from all endpoints is directed to the DNS Server in the head office. This DNS Server in turn is configured with the appropriate Request Routes to all the internal corporate networks and domains and to use Sophos DNS Protection as a Forwarder to resolve all external domains.

In such situation, it is needed to have only the DNS Server's publicly reachable address or publicly resolvable FQDN listed as a Location under DNS Protection in Sophos Central, as all DNS queries from all endpoints will be re-routed to DNS Protection Resolvers by the DNS Server in the Head Office.

Note: If unsure what the public IP address associated with a device is, then run checks on https://www.ipchicken.com/ or https://whatismyipaddress.com/ from the same device (DNS Server in HO in above scenario) that will be forwarding DNS Requests to the Sophos DNS Protection service.

Issues with Internet access on Apple devices



Issue:

Unable to access internet on iPhone devices but you can access from other devices.

Cause:

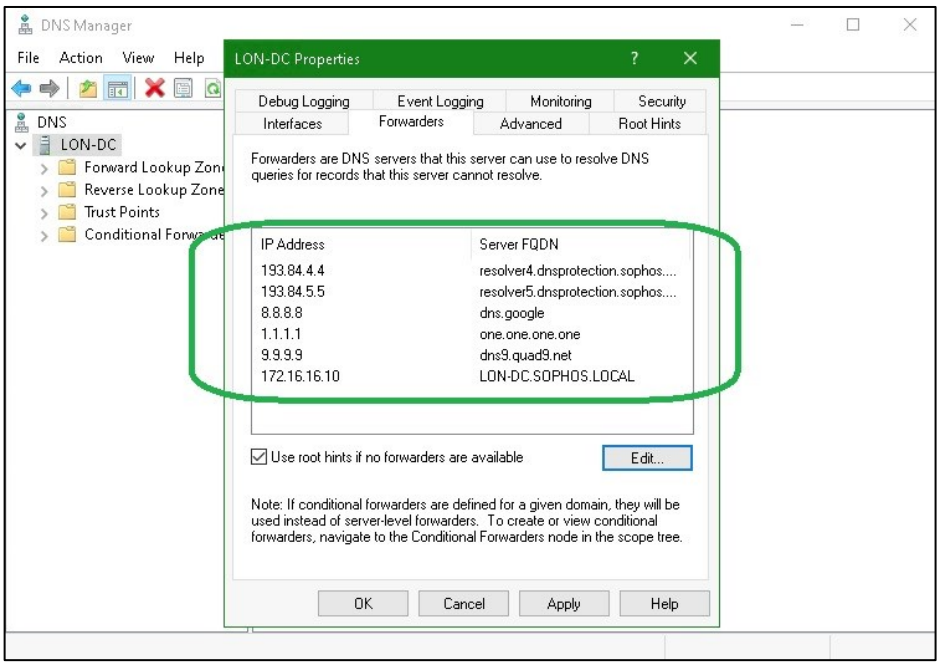
Apple devices might have **iCloud Private Relay** settings turned on. Turn off Limit IP Address Tracking on iPhone devices.

What to do:

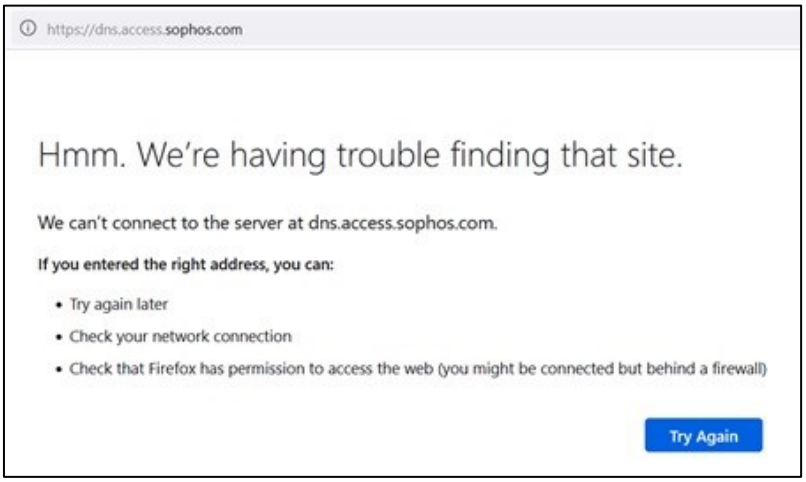
Turn off '**Limit IP Address Tracking**' on iPhones.

https://developer.apple.com/support/prepare-your-network-for-icloud-private-relay

Multiple DNS Forwarder Configured



Configuring multiple DNS forwarders pointing to multiple other DNS servers may cause unpredictable and inconsistent behaviour and results.



Although it adds fault tolerance to the DNS infrastructure, when multiple forwarders are configured, it will result in DNS names to continue to be resolved in the event of failures of the configured Server.

When two or more Forwarders are configured, the DNS Server when it receives a query for a record in a zone it is not authoritative for, will need to use the forwarders. It will forward the query to the first address in the list and wait for a timeout period **(Forwarding Timeout)** (Default 3 seconds, configurable) for a response.

If no response is received within the timeout period, it will query the second address in the Forwarders list and so on.

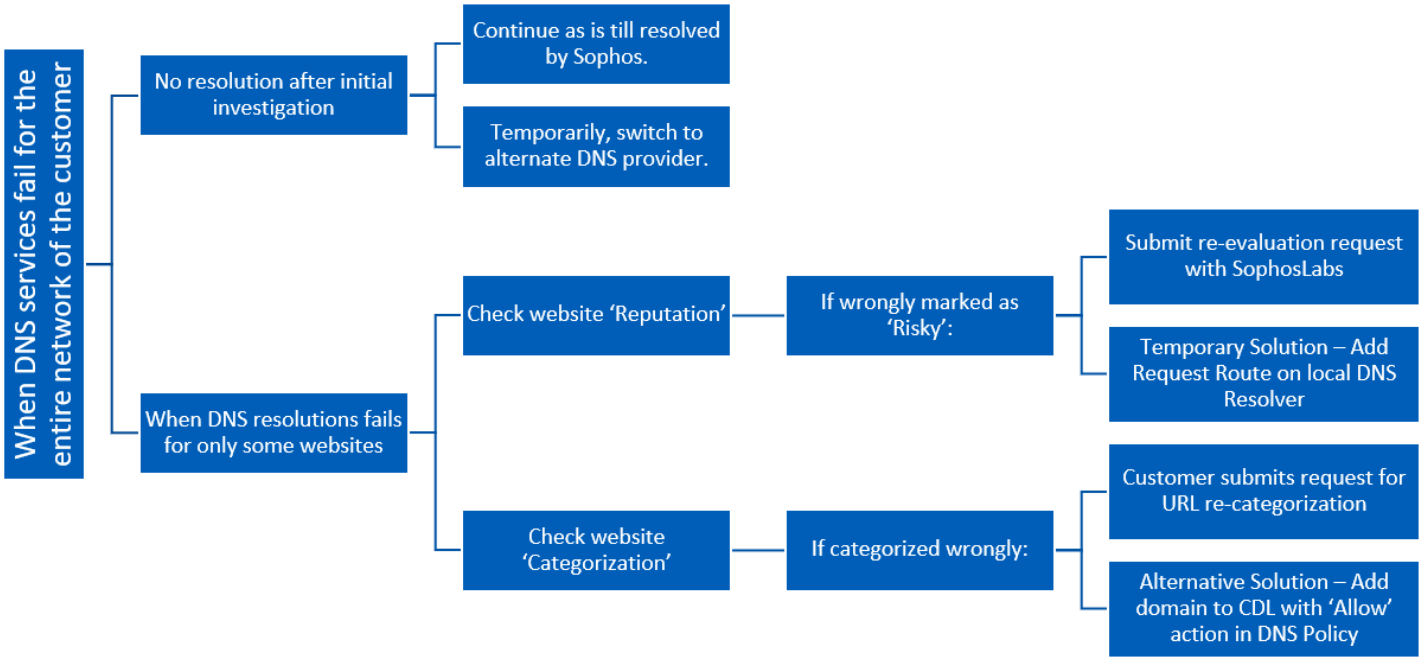
There is a second timeout period called **Recursion Timeout** (Default 8 seconds) that refers to how long the DNS Server will wait for the remote servers to respond to the recursive query before terminating the search. If the **Recursion Timeout** expires, the DNS server will reply back to the client with a Server Failure.

If the DNS Server managed to contact all Forwarders before the **Recursion Timeout** expired without getting a response, it will try to use root hints for name resolution (default setting).

What are the root hints?
The root hints are a list of the servers that are authoritative for the root domain ".", along with their IPv4 and IPv6 addresses. In other words, this is a collection of NS, A, and AAAA records for the root nameservers.

Note: All DNS settings should be configured to send all DNS queries only to Sophos DNS Protection Resolver address to obtain consistent and secure resolution.

Getting customer up and running in critical situations



When DNS services fail for the entire network of the customer.

If there is no immediate resolution after initial investigation, reach out to the customer and explain the severity of the situation and ask customer if they would either:

- Like to continue with the current setup and wait **(without DNS resolution)** till Sophos inspects and resolves the issue.
- In case of a P1 situation, as a temporary measure, suggest switching to an alternative public DNS service provider to get access to DNS resolution, without the security of DNS Protection services.

When DNS resolutions fail for only some websites.

Check if those websites have a 'Risky' reputation.

If wrongly marked 'reputation' as Risky:

Support submits a request for re-evaluation with SophosLabs - **https://portal.labs.sophos/tools/uri/editor/**

Temporary Solution – Add a Request Route on the local DNS Resolver to forward DNS requests for the said domain to an alternate DNS provider. (Best solution if demands access to the URL and cannot wait for the re-evaluation result).

https://docs.sophos.com/nsg/sophos-firewall/20.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Network/DNS/NetworkDNSRequestRouteAdd/index.html

Alternative Solution 1 –

- Add DNS Host entry pointing to that specific website and its IP address. (Only one address can be mapped per entry for a domain).

https://docs.sophos.com/nsg/sophos-firewall/20.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Network/DNS/NetworkDNSHostEntryAdd/index.html

Alternative Solution 2 –

- If end devices are configured to use DNS Protection directly, Add an entry in the 'Hosts' file on the affected device for the inaccessible website with its domain name and IP address. (Will require to map every IP address associated with the domain).

  For Windows - c:\Windows\System32\Drivers\etc\hosts

  For Mac - /private/etc/hosts

  For Linux - /etc/hosts

Check the website category –

https://intelix.sophos.com/url

If 'categorized' wrongly:

- Ask the customer to submit the URL for re-categorization at *https://support.sophos.com/support/s/filesubmission?language=en_US*

- Alternate Solution – Add the affected domain to a Custom Domain List (CDL) and apply the allow action to it in the DNS Protection policy.

Training Feedback

TRAINING FEEDBACK

Feedback is always welcome

The course page has feedback section and feel free to participate.

SOPHOS

Next Steps

Now that you have completed this course, you should:

- Complete the assessment in the SupportLMS
- You will have one attempt to pass the assessment