How to Configure DNS Sinkholing in the Firewall

https://campus.barracuda.com/doc/79462920/

DNS sinkholing is a special method for deliberately giving out false IP addresses for domain names. This method can be used for securing clients on a LAN against access to malicious sites.

When DNS sinkholing is activated on the CloudGen Firewall, a DNS access to a malicious site is intercepted, and the querying client is informed accordingly. Unlike for real DNS interception, DNS sinkholing does not resolve any domain names into IP addresses. Instead, based on a configured blacklist, it replaces the A and AAAA DNS response by a fake IP address that is said to be the DNS sinkhole IP address. For this reason, DNS sinkholing does not rely on any caching mechanism.

If you must protect your network against access to malicious domains for other record types, use the DNS interception feature, instead. For more information, see How to Configure DNS Interception.

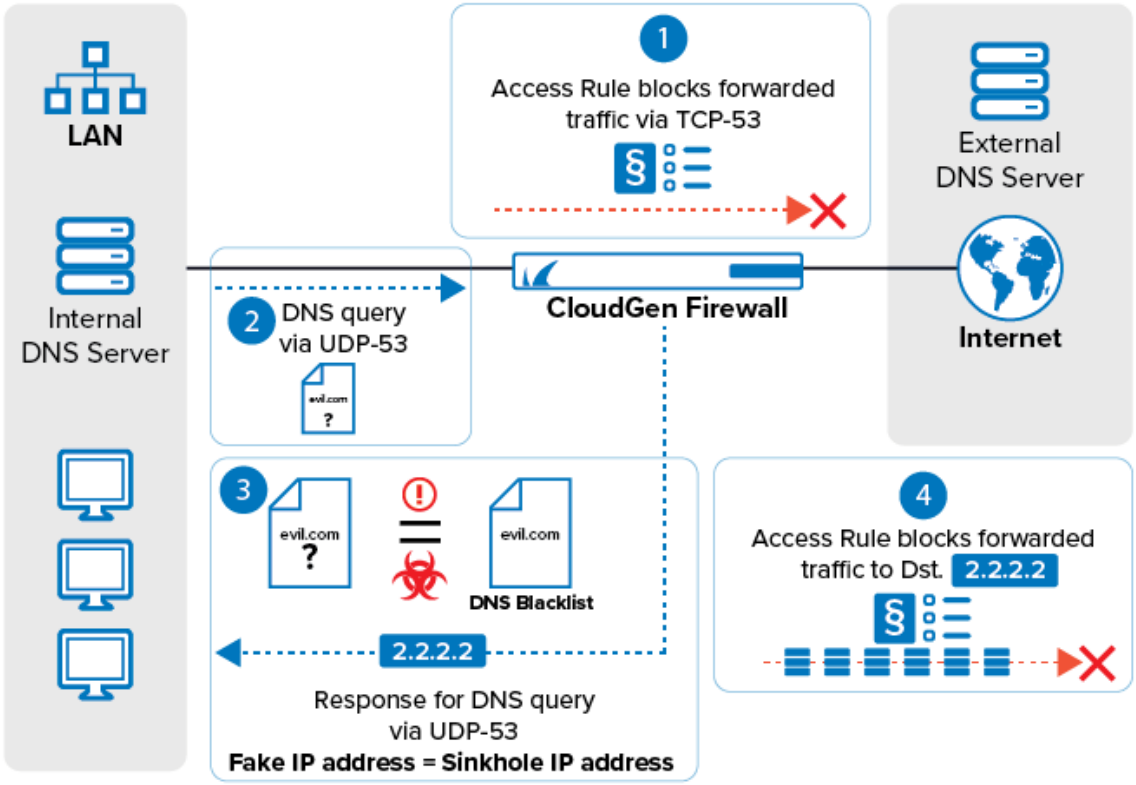
How the Protection Works

DNS relies on the usage of both the UDP-53 and the TCP-53 protocol. UDP is preferred for DNS queries and short answers, e.g., between client PCs and DNS.

Whereas UDP is considered the primary choice for all DNS queries with short answering times, TCP is designed for larger data transmissions to avoid truncated UDP answering packets, e.g., zone transfers between domain name servers (DNSs). TCP-53 is also used as a fallback strategy in case of communication problems via UDP.

DNS sinkholing relies on the principle of intercepting DNS queries via single UDP packets because the transmitted requests can easily be verified against configured entries in a blacklist before the request hits a DNS. This blacklist can either be configured locally on the CloudGen Firewall or can be part of an ATP cloud blacklist that requires a valid ATP license. In case the CloudGen Firewall detects such a packet, it sends a fake IP, which is the sinkhole IP address to the querying source. When the client later tries to access this fake IP address, another access rule blocks the traffic to this fake IP address and sends an appropriate response to the client.

In order to prevent circumvention by an interposed DNS on a LAN, which could eventually transform the client PC UDP-53 query into a query via a zone transfer, TCP-53 must be blocked prior to enabling DNS sinkholing. Also, the caches on the internal DNS must be flushed.



The attempt to access the sinkhole IP address is logged in the Threat Scan and Firewall Monitor.

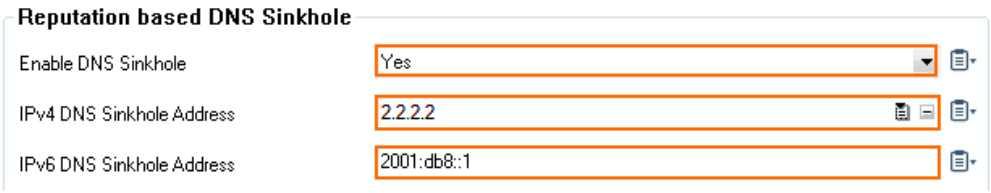
Before You Begin

The following example for DNS sinkholing assumes that a client PC tries to access a malicious site with a preceding DNS request to an internal DNS on the LAN. Because this DNS eventually could consult an external DNS on the WAN, the following preconditions must be met:

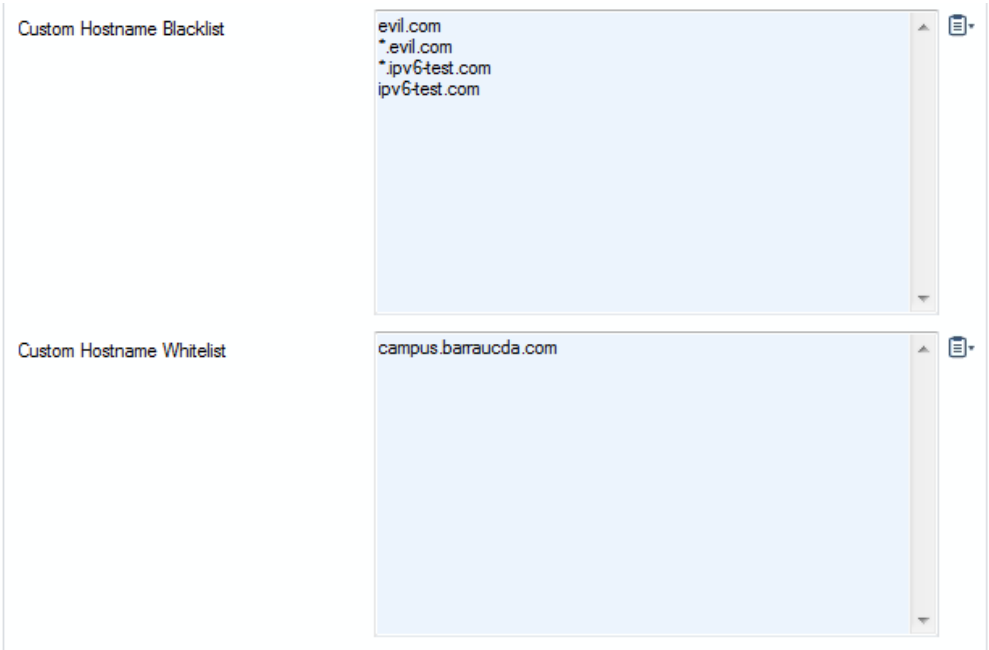
- Verify that all client PCs refer to the internal DNS.
- Verify that the caches on the querying source(s), e.g., querying client(s) / internal DNS, are flushed prior to activating DNS sinkholing on the CloudGen Firewall.
- Although every DNS query must use UDP-53 as the first choice, DNSs can initiate queries via TCP-53 as well, e.g., for zone transfers. Also, a manually initiated query via TCP-53 can be sent from a client PC. This could circumvent the UDP-53 protocol, which must be applied for DNS sinkholing. Because DNS sinkholing relies on UDP-53, you must block forwarded traffic for TCP-53 on the CloudGen Firewall. However, be aware that an internal DNS will not be able to do zone transfers to an external one.
- Identify an IPv4 and IPv6 DNS sinkhole / fake IP address. This IP address must not be in the same network as the client or the internal DNS, e.g., 2.2.2.2.
- In order to sync with the Barracuda Botnet and Spyware database, an Advanced Threat Protection subscription is required.

Step 1. Enable DNS Sinkhole

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Settings**.
2. Click **Lock**.
3. In the left menu, click **DNS Sinkhole**.
4. From the **Enable DNS Sinkhole** list, select **Yes**.
5. Enter the **IPv4 DNS Sinkhole Address**. Enter an IPv4 address that is not on your network. E.g., 2.2.2.2
6. Enter the **IPv6 DNS Sinkhole Address**. Enter an IPv6 address that is not on your network. E.g., 2001:db8::1



7. Enter blacklisted domains in the **Custom Hostname Blacklist**. Use one line per domain. * and ? wildcard characters are allowed. E.g., add entries for `google.com` and `*.google.com` to block **google.com**, including all subdomains
8. Enter whitelisted domains in the **Custom Hostname Whitelist**. Use one line per domain. * and ? wildcard characters are allowed.

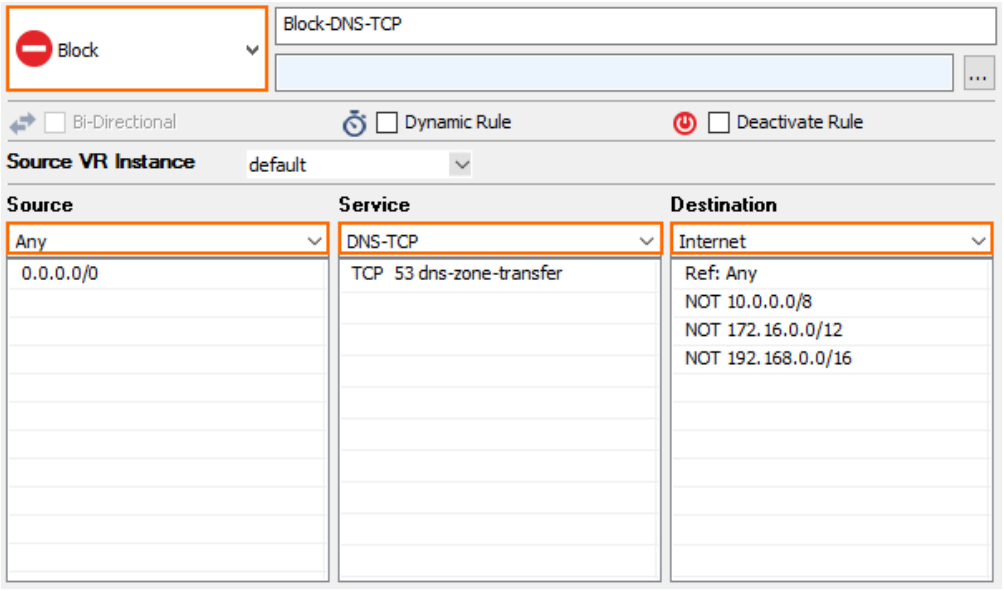


9. Click **Send Changes** and **Activate**.

Step 2. Block TCP DNS Queries

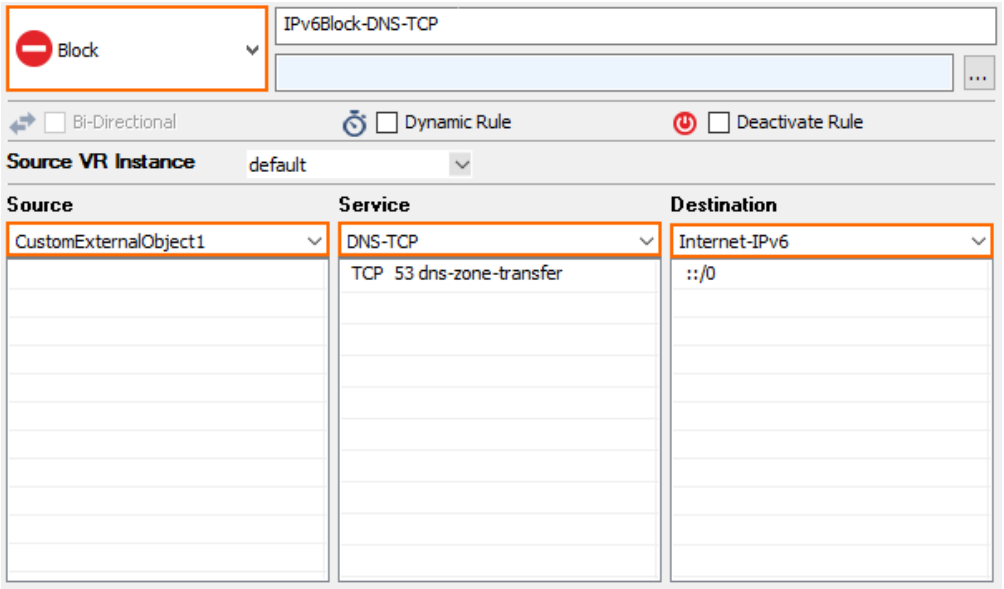
To avoid clients from circumventing the DNS sinkhole, block DNS queries via TCP for IPv4 and IPv6.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Either click the plus icon (**+**) in the top right of the ruleset, or right-click the ruleset and select **New > Rule**.

4. Configure the access rule:
   - **Action** – Select **Block**.
   - **Source** – Select **Any**.
   - **Service** – Select **TCP DNS**
   - **Destination** – Select **Internet**.


5. Click **OK**.
6. Either click the plus v6 icon (**+V6**) in the top right of the ruleset, or right-click the ruleset and select **New > IPv6 Rule**.

7. Specify the following settings to block traffic to the IPv6 sinkhole address:
   - **Action** – Select **Block** or **Deny**.
   - **Source** – Select **Any** or enter `::/0`.
   - **Service** – Select **Any**.
   - **Destination** – Select **Internet**.

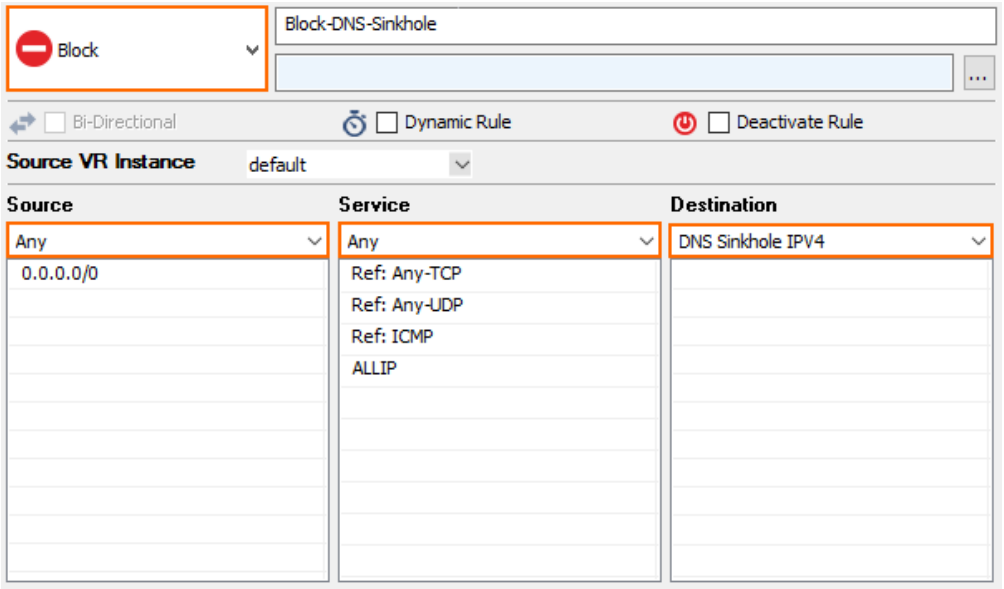


8. Click **OK**.
9. Drag and drop both access rules so that no rule above it matches the same traffic.
10. Click **Send Changes** and **Activate**.

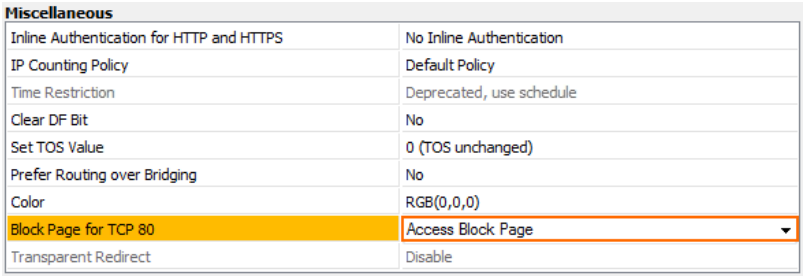
Step 3. Create Access Rules to Block Fake IP Addresses

Most blacklisted domains are accessed by bots and spyware on the client's computer. You can create a block rule with block page for HTTP traffic for those cases where the client enters the forbidden domain in the browser.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Specify the following settings to block the IPv4 sinkhole address:
   - **Action** – Select **Block** or **Deny**.
   - **Source** – Select **Any**.
   - **Service** – Select **Any**.
   - **Destination** – Select **DNS Sinkhole IPv4**.

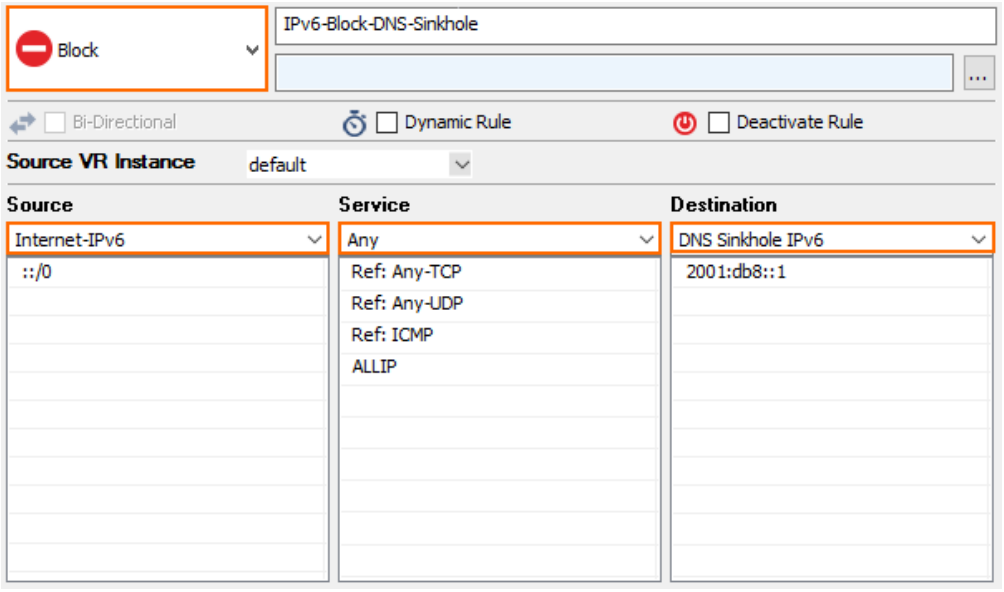


4. In the left menu, click **Advanced.**
5. In the **Miscellaneous** section, from the **Block Page for TCP 80** list, select **Access Block Page**.



6. Click **OK**.
7. Either click the plus v6 icon (**+V6**) in the top right of the ruleset, or right-click the ruleset and select **New > IPv6 Rule**.

8. Specify the following settings to block traffic to the IPv6 sinkhole address:
   - **Action** – Select **Block** or **Deny**.
   - **Source** – Select **Any** or enter `::/0`.
   - **Service** – Select **Any**.
   - **Destination** – Select **DNS Sinkhole IPv6**.

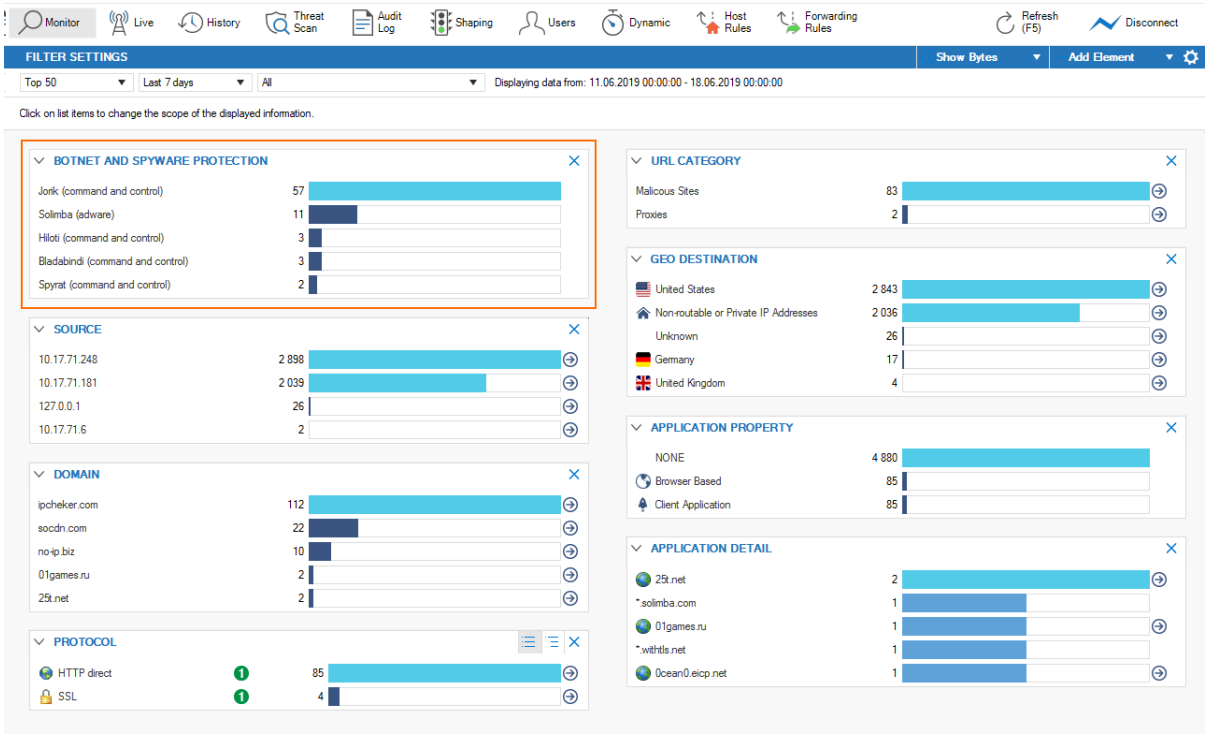


9. Click **OK**.
10. Drag and drop the access rule so that no rule above it matches the same traffic.
11. Click **Send Changes** and **Activate**.

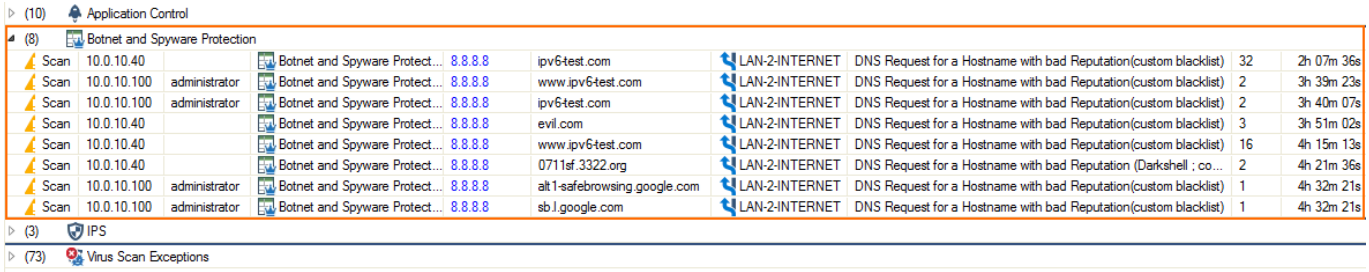
Clients attempting to access malicious domains via HTTP are redirected to a block page. For all other services, the connection is reset.

Monitoring

Go to **FIREWALL > Monitor**. In the **BOTNET AND SPYWARE PROTECTION** element, connections blocked by DNS Sinkhole are listed.



Go to **FIREWALL > Threat Scan**. Expand the **Botnet and Spyware Protection** section to view the intercepted DNS requests.



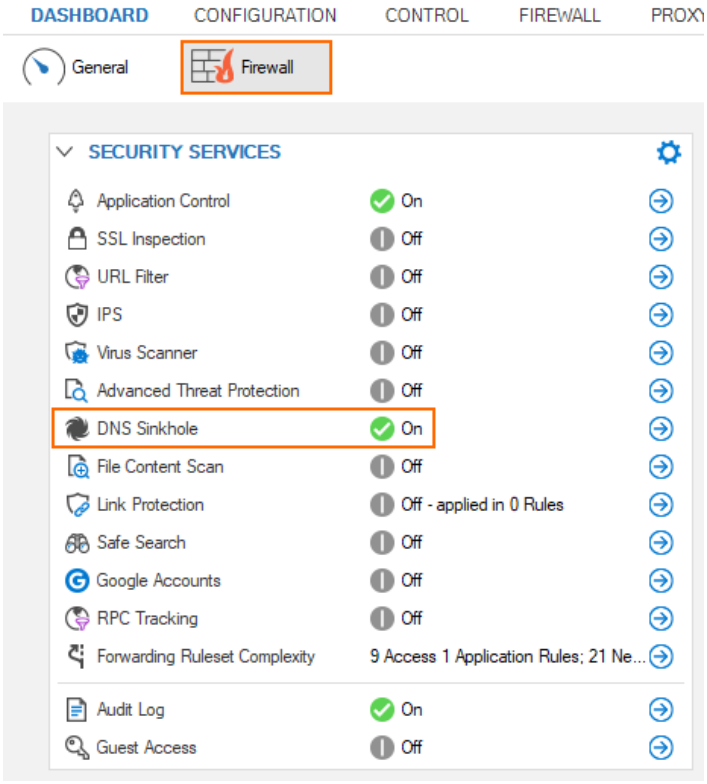
Events

When a client accesses the DNS Sinkhole address, the **5004 – DNS Sinkhole address accessed** event is triggered. For more information, see Security Events.

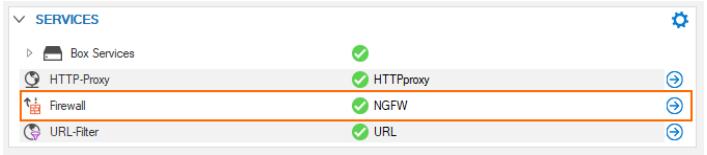
Troubleshooting DNS Sinkholing

In case DNS sinkholing does not produce the expected results, you can check the following options:

1. Go to **DASHBOARD > Firewall**. In the element **SECURITY SERVICES**, verify that the option **DNS Sinkhole** is set to **On**.



2. Log into your firewall via SSH. Use the shell command `dmseg` to check whether DNS Blacklist is enabled/disabled and monitoring access to the configured blacklisted domains.
   If necessary, enable DNS Blacklisting manually with the command `dnsblacklistctrl enable`.
3. In case DNS sinkholing is not active, although it has been activated before, go to **CONTROL > Services**. In the section **SERVICES**, click the blue arrow icon to the right of **Firewall** and click **Restart Service**.



Figures