DNS Titan End-User Security Overview and Configuration

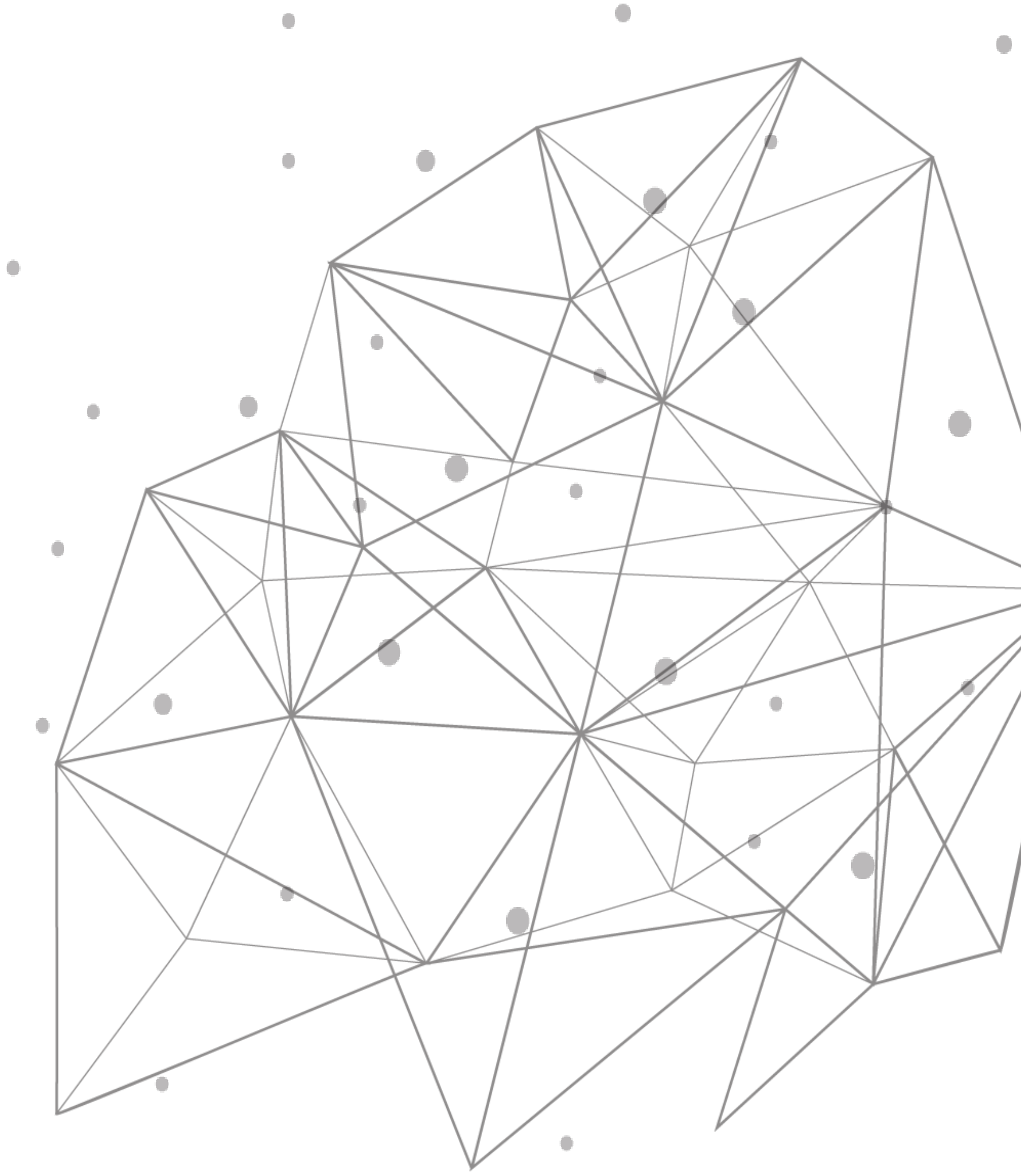


Table of Contents

Introduction

TCPWave's DNS Titan End-User Security prevents users from accessing malicious sites. It explicitly blocks DNS queries for domain names of malicious hosts, queries to malicious DNS servers, and IP addresses of malicious sites in DNS query responses. Also, since this Titan feature provides this protection in DNS servers, it prevents some types of malware from reaching devices. Consequently, there is no need to quickly detect this malware on a device and remove it before it does damage or spreads.

Additionally, although the emphasis here is on protecting end-users, this Titan feature protects all DNS clients, including applications that make DNS queries. Furthermore, it provides this protection without installing and continually updating software on the many DNS clients that exist.

The items to block are based on domain and IP reputation data provided by TCPWave's partner, Spamhaus, a leader in providing high-quality threat intelligence information. This reputation data consists of a feed of continually updated rules in DNS Response Policy Zones (RPZs). By using this information, Titan End-User Security protects users from accessing malicious sites, including malware, ransomware, phishing, adware, and botnet sites.

To enable users to understand and take advantage of DNS Titan End-User Security, information on the following topics is presented in the sections below:

- Spamhaus
- Architecture
- Configuration in TCPWave
- Verification of the configuration
- DNS RPZ reports

Spamhaus

Spamhaus has over twenty years of experience protecting users and networks and is a trusted authority on IP and domain reputation data. Also, they protect over three billion mailboxes globally. Consequently, they are an industry leader for providing threat intelligence data, and leading global technology companies use their datasets. Example customers are provided near the bottom of the page at www.spamhaus.com.

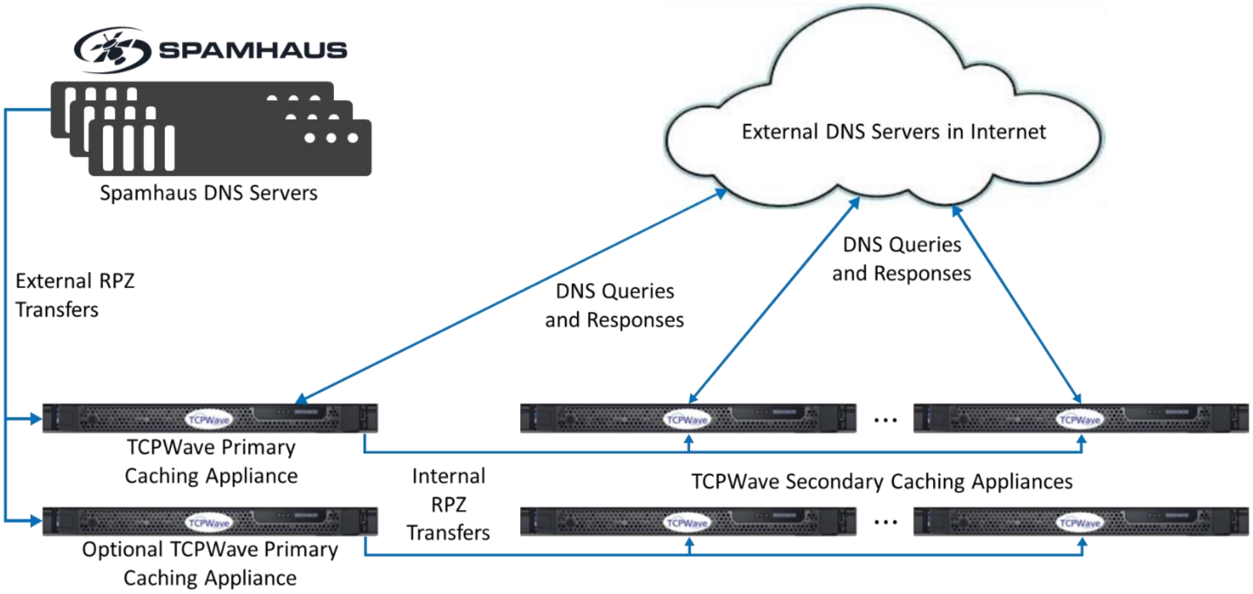
With DNS Titan End-User Security, you benefit from Spamhaus's high-quality threat intelligence in their RPZ data feeds. The following data feeds from Spamhaus are included in DNS Titan End-User Security:

- **Malware Hosts:** Domains identified as hosting malware.
- **Phishing Hosts:** Domains identified as hosting phishing sites.
- **Adware Hosts:** Domains identified as hosting adware.
- **Bad Reputation Hosts:** Uncategorized domains that have a bad reputation. This includes hosts owned by known spammers, payload URLs, malicious tracking domains, and domains associated with low- reputation networks.
- **Botnet Command and Control (C&C) Hosts:** Domains identified as hosting botnet C&C malware.
- **Botnet Hosts:** Domains identified as hosting botnet resources that are not a botnet C&C.
- **Domain Generation Algorithm:** Domains produced by domain generation algorithms. These domains are usually associated with malware.

- **Zero Reputation Domains:** Newly registered domains that have been listed for less than 24 hours. Legitimate organizations rarely use a domain immediately after registering it.
- **Bad Nameserver Hosts:** Domains used for the host records of nameservers that have a bad reputation.
- **Bad Nameserver IPs:** IP addresses of nameservers that host domains and have a bad reputation.
- **Botnet Command and Control (C&C) IPs:** IP addresses identified as hosting botnet C&C malware.
- **Bogons IPs:** IP addresses that have not yet been assigned to an entity should not have any incoming or outgoing traffic.
- **Do Not Route or Peer:** IP addresses that have been identified as being hijacked, belonging to bulletproof hosters, or being leased by professional malicious organizations.
- **Coinblocker:** IP addresses and domains that host cryptojacking scripts, which use the resources of an end user's computer to mine cryptocurrency.
- **Torblocker:** List of known Tor Exit Nodes.

Architecture

An overview of the DNS Titan End-User Security architecture is shown in the figure below. As depicted in it, Response Policy Zones (RPZs) are transferred from Spamhaus DNS servers to a TCPWave primary (or lead secondary) DNS caching appliance. Spamhaus also supports transfers to an optional primary DNS appliance for the site and geographic redundancy. Secondary DNS caching appliances are downstream from the primary DNS appliances and get zone transfers from them.


SPAMHAUS
Spamhaus DNS Servers
External DNS Servers in Internet
External RPZ Transfers
DNS Queries and Responses
DNS Queries and Responses
TCPWave Primary Caching Appliance
Internal RPZ Transfers
TCPWave Secondary Caching Appliances
Optional TCPWave Primary Caching Appliance
...
...

DNS Titan End-User Security Architecture

After zone transfers are complete, the query will be blocked if a DNS query contains a name or IP address defined in an RPZ as malicious. Also, these blocked queries will be logged and used in DNS RPZ reports.

Configuration

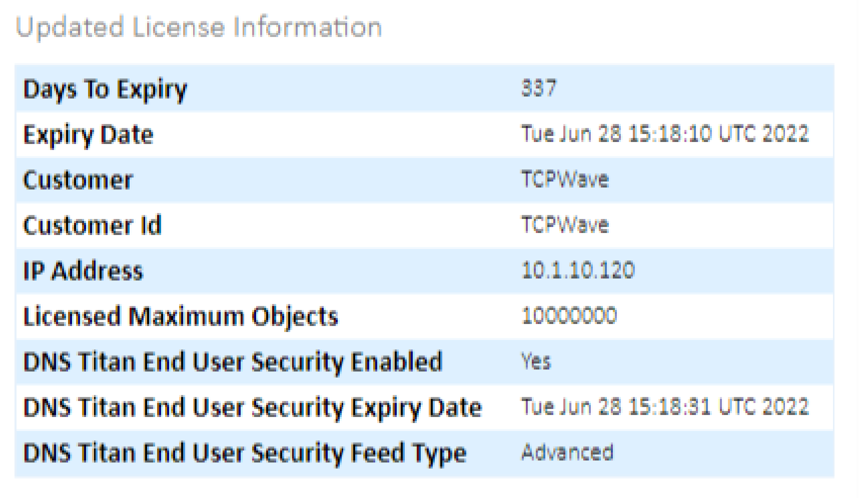
This configuration section explains the steps necessary to use DNS RPZs from Spamhaus in your TCPWave DNS appliances. It explains how to update TCPWave licenses and set up primary (or lead secondary) DNS caching appliances and downstream secondary DNS caching appliances.

Update Licenses

Once purchased, the first step to configuring the new End-User Security feature is updating the IPAM licenses. Do this as follows:

1. Navigate to Administration >> Configuration Management >> License Management.
2. Select the IPAM to update, then click **Update License** and enter the license key provided by TCPWave.
3. Repeat the previous step for other IPAM appliances as needed.

Below is an example of an updated License Information screen. “DNS Titan End User Security Enabled” is “Yes,” and the feed type is “Standard” or “Advanced,” depending on the license purchased.



Updated License Information

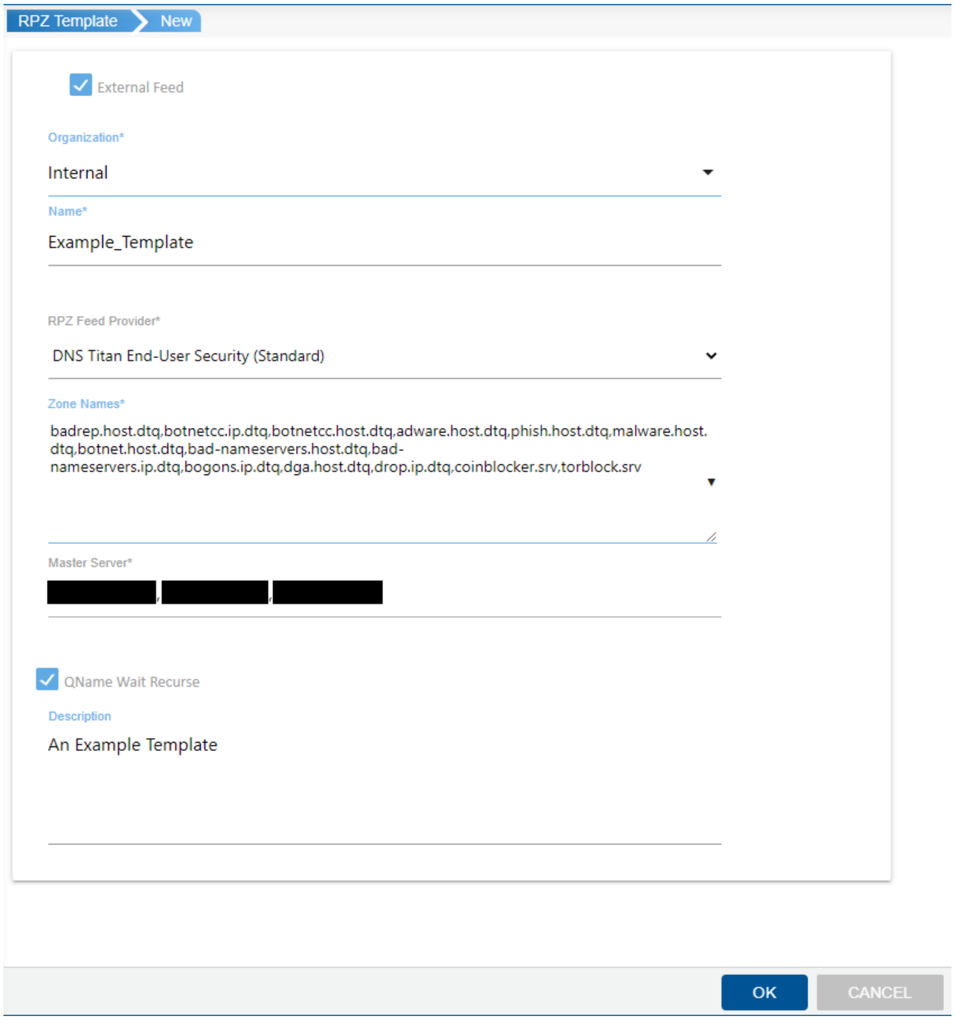
Days To Expiry	337
Expiry Date	Tue Jun 28 15:18:10 UTC 2022
Customer	TCPWave
Customer Id	TCPWave
IP Address	10.1.10.120
Licensed Maximum Objects	10000000
DNS Titan End User Security Enabled	Yes
DNS Titan End User Security Expiry Date	Tue Jun 28 15:18:31 UTC 2022
DNS Titan End User Security Feed Type	Advanced

Create RPZ Templates for Master DNS Appliances

Before applying the End-User Security feature to appliances, you must create the RPZ template for primary (or lead secondary) DNS appliances. (These appliances receive zone transfers from Spamhaus’s DNS servers).

1. At the top of the GUI, navigate to Network Management >> DNS Management >> DNS Security >> DNS Threat Management.
2. Click the RPZ Templates tab.
3. Click **Add** ⊕ to create a new RPZ template**.**
4. Select the **External Feed** box.
5. Select an **Organization**, and enter a **Name** for the template.
6. For **RPZ Feed Provider**, select either “DNS Titan End User Security (Standard)” or “DNS Titan End User Security (Advanced),” depending on which license was purchased.

   Result: The configuration options for the template are updated and automatically populated with Spamhaus’s zones and server IP addresses.
7. Keep **QName Wait Recurse** selected. (It is for a BIND query name policy.) An example screenshot is shown below.



☑ External Feed

Organization*

Internal

Name*

Example_Template

RPZ Feed Provider*

DNS Titan End-User Security (Standard)

Zone Names*

badrep.host.dtq,botnetcc.ip.dtq,botnetcc.host.dtq,adware.host.dtq,phish.host.dtq,malware.host.dtq,botnet.host.dtq,bad-nameservers.host.dtq,bad-nameservers.ip.dtq,bogons.ip.dtq,dga.host.dtq,drop.ip.dtq,coinblocker.srv,torblock.srv

Master Server*

[redacted],[redacted],[redacted]

☑ QName Wait Recurse

Description

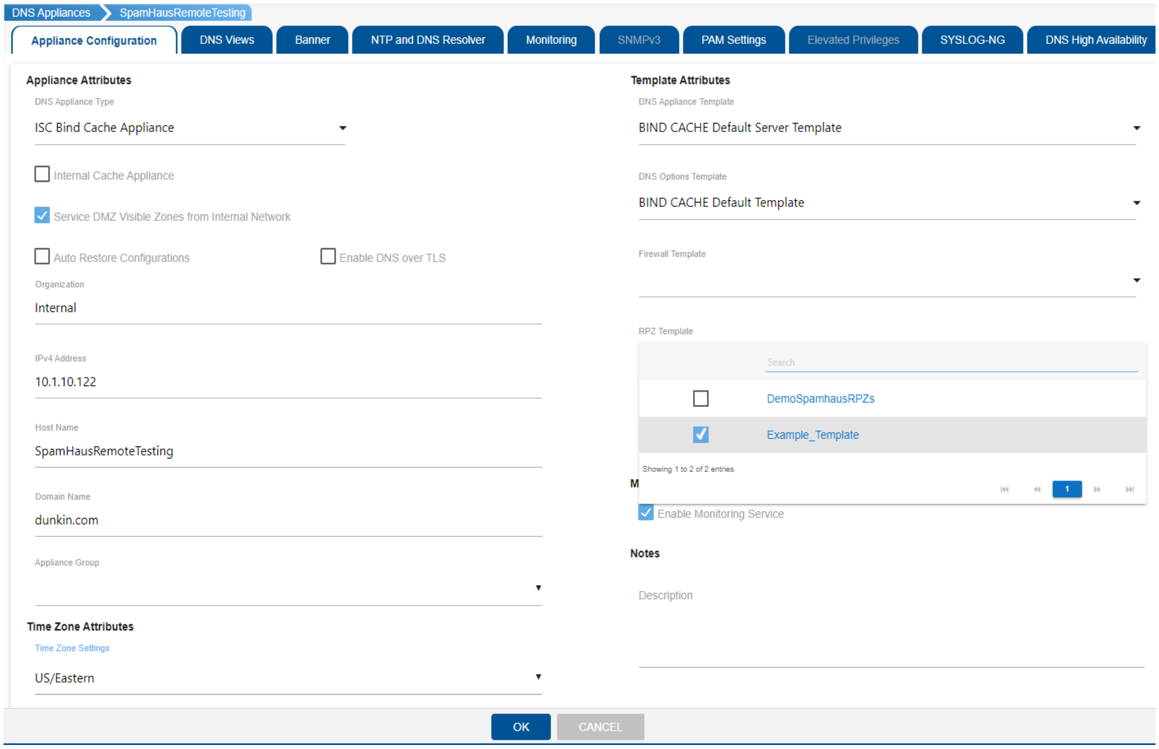
An Example Template

8. Click **OK** to save the template.

Apply RPZ Templates to DNS Appliances

After creating an RPZ template for master appliances, you must apply it to each master DNS appliance. The next section below explains how to create an RPZ template for secondary DNS appliances, which must be applied to them. The steps for applying an RPZ template are the same for the master and secondary appliances, which are as follows:

1. At the top of the GUI, navigate to Network Management >> DNS Management.
2. Click on an appliance to edit it.
3. For **DNS Appliance Type**, select “ISC Bind Cache Appliance.”
4. For **RPZ Template**, select an RPZ template for the master or secondary appliance. An example screenshot is shown below.



DNS Appliances > SpamHausRemoteTesting

Appliance Attributes

DNS Appliance Type: ISC Bind Cache Appliance

☐ Internal Cache Appliance

☑ Service DMZ Visible Zones from Internal Network

☐ Auto Restore Configurations ☐ Enable DNS over TLS

Organization: Internal

IPv4 Address: 10.1.10.122

Host Name: SpamHausRemoteTesting

Domain Name: dunkin.com

Appliance Group:

Time Zone Attributes

Time Zone Settings: US/Eastern

Template Attributes

DNS Appliance Template: BIND CACHE Default Server Template

DNS Options Template: BIND CACHE Default Template

Firewall Template:

RPZ Template

Search

☐ DemoSpamhausRPZs

☑ Example_Template

Showing 1 to 2 of 2 entries

☑ Enable Monitoring Service

Notes

Description

5. Click **OK** to save your configuration.

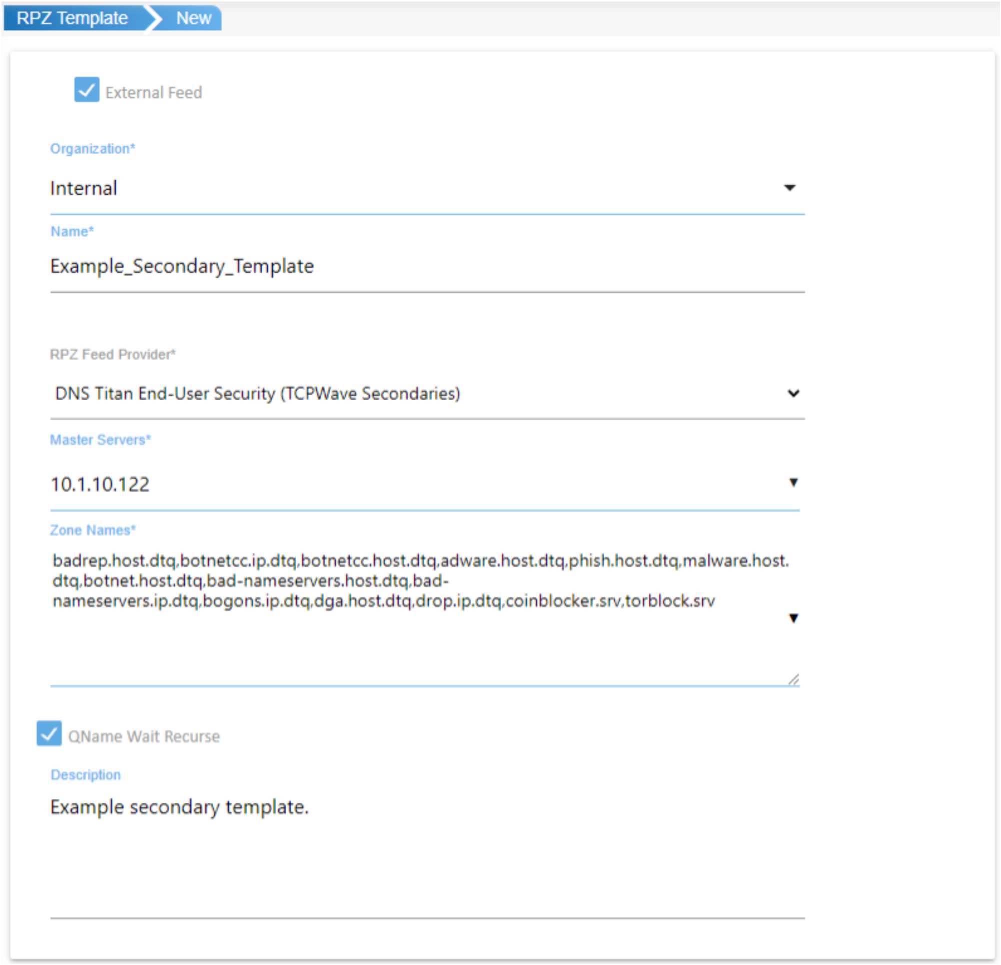
   Result: Your DNS Appliance will be configured for protection using the Spamhaus RPZs after the initial zone transfers are complete.

Create and Apply RPZ Template for Secondary Appliances

Secondary DNS appliances receive zone transfers from a primary (or lead secondary) appliance. To create and apply an RPZ template for a secondary appliance, follow the steps below:

1. At the top of the GUI, navigate to Network Management >> DNS Management >> DNS Security >> DNS Threat Management.
2. Click the RPZ Templates tab.
3. Click **Add** ⊕ to create a new RPZ template**.**
4. Select the **External Feed** box.
5. Select an **Organization**, and enter a **Name** for the template.
6. For **RPZ Feed Provider**, select "DNS Titan End User Security (TCPWave Secondaries)."

   Result: The configuration options for the template will be updated and automatically populated with Spamhaus's zones.
7. For **Master Servers**, select the IP address(es) of the master DNS Appliance(s).
8. Keep **QName Wait Recurse** selected. (It is for a BIND query name policy.) An example screenshot is shown below.



☑ External Feed

Organization*
Internal

Name*
Example_Secondary_Template

RPZ Feed Provider*
DNS Titan End-User Security (TCPWave Secondaries)

Master Servers*
10.1.10.122

Zone Names*
badrep.host.dtq,botnetcc.ip.dtq,botnetcc.host.dtq,adware.host.dtq,phish.host.dtq,malware.host.dtq,botnet.host.dtq,bad-nameservers.host.dtq,bad-nameservers.ip.dtq,bogons.ip.dtq,dga.host.dtq,drop.ip.dtq,coinblocker.srv,torblock.srv

☑ QName Wait Recurse

Description
Example secondary template.

9. Click **OK** to save the template.
10. Applying a template to a secondary DNS appliance is done the same way as for a master DNS appliance. It is described above in the section Apply RPZ Templates to DNS Appliances.

    Note: If you need to apply the RPZ template to many secondary DNS appliances, you may want to use the setdnsserver CLI command.

Verify Configuration

To verify that the Titan End-User Security feature is functioning, you must first wait 15-30 minutes for the initial zone transfers from the Spamhaus DNS servers to the TCPWave primary DNS appliance(s), and then wait additional time for zone transfers to downstream secondary appliances. Shown below is an example of a dig command to that sends a query to a DNS server requesting the IP address of a simulated malicious domain:

```
[root@SpamHausRemoteTesting ~]# dig @10.1.10.122 bad-nameservers-
host-dtq.rpzfeeds.com

; <<>> DiG 9.11.32 <<>> @10.1.10.122 bad-nameservers-host-
dtq.rpzfeeds.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 20323
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0,
ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: d448dd9bc0d95f2884f96150610953b73b81db19f1bb034e (good)
;; QUESTION SECTION:
;bad-nameservers-host-dtq.rpzfeeds.com. IN A

;; ADDITIONAL SECTION:
bad-nameservers.host.dtq. 60     IN      SOA
need.to.know.only. hostmaster.deteque.com. 1628001001 300 60
432000 60

;; Query time: 1 msec
;; SERVER: 10.1.10.122#53(10.1.10.122)
;; WHEN: Tue Aug 03 10:33:27 EDT 2021
;; MSG SIZE  rcvd: 190
```

If the Spamhaus RPZ configuration is correct and the DNS appliances are working, then the dig query will be blocked. In specific, as shown above in the dig output in the HEADER section, the DNS server returns an "NXDOMAIN" (non-existent domain) response to prevent users from accessing the simulated malicious site. (If the Spamhaus RPZ rules were not functioning, then the dig output would contain the IP address for the requested domain.)

The record in the Spamhaus RPZ file that causes the dig query to get blocked is as follows:

```
bad-nameservers-host-dtq.rpzfeeds.com.bad-nameservers.host.dtq.
3600 IN CNAME .
```

This record, which is an RPZ rule, is in the bad-nameservers.host.dtq zone, which is one of the zones that Spamhaus transfers to TCPWave primary DNS appliances.

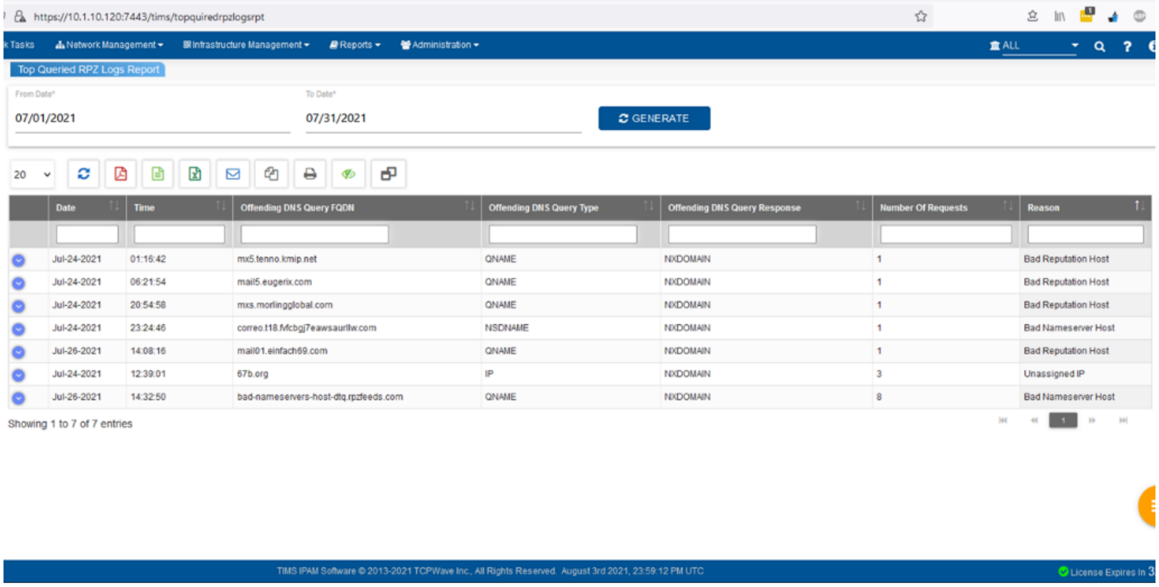
DNS RPZ Reports

TCPWave IPAM provides two reports of blocked DNS queries, which both help security personnel and others understand trends in security threats and better protect users. Also, both of these reports are based on RPZ log files. The Top Queried RPZ Logs Report displays the most frequent DNS queries resolved by RPZ rules. The DNS RPZ Logs Report displays the history of DNS queries that were resolved by RPZ rules. Also, in the second report, you can filter it to see just the queries for a specific appliance or a specific client. To run one of these reports, do the following:

1. Navigate to Reports >> DNS Reports.
2. Search for "RPZ" in the **Search Pages** box.

   Result: Two options appear: "DNS RPZ Logs Report by Appliance" and "Top Queried RPZ Logs Report."
3. Select one of the reports to view.
4. If you selected "Top Queried RPZ Logs Report," enter a range of dates.

5. Click **Generate**. Example screenshots of the reports are shown below.


https://10.1.10.120:7443/tims/topquiredrpzlogsrpt
k Tasks
Network Management
Infrastructure Management
Reports
Administration
ALL
GENERATE
20

Top Queried RPZ Logs Report

From Date* 07/01/2021

To Date* 07/31/2021

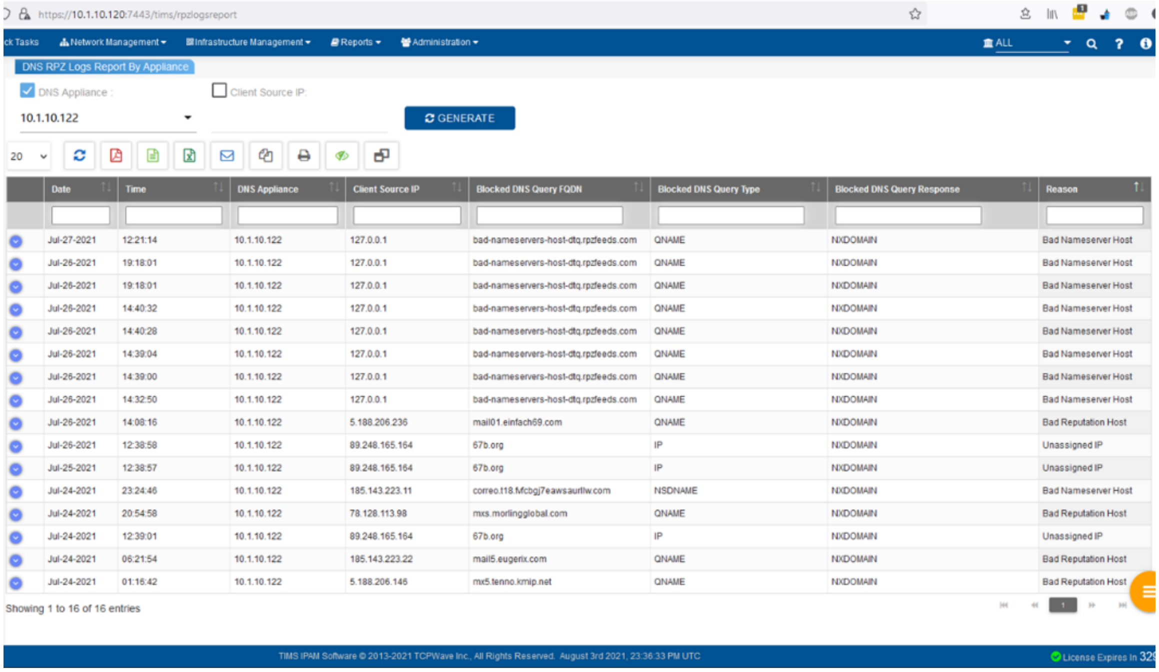
Date	Time	Offending DNS Query FQDN	Offending DNS Query Type	Offending DNS Query Response	Number Of Requests	Reason
Jul-24-2021	01:16:42	mx5.tenno.kmip.net	QNAME	NXDOMAIN	1	Bad Reputation Host
Jul-24-2021	06:21:54	mail5.eugerix.com	QNAME	NXDOMAIN	1	Bad Reputation Host
Jul-24-2021	20:54:58	mxs.morlingglobal.com	QNAME	NXDOMAIN	1	Bad Reputation Host
Jul-24-2021	23:24:46	correo.t18.Mcbgj7eawsaurllw.com	NSDNAME	NXDOMAIN	1	Bad Nameserver Host
Jul-26-2021	14:08:16	mail01.einfach69.com	QNAME	NXDOMAIN	1	Bad Reputation Host
Jul-24-2021	12:39:01	67b.org	IP	NXDOMAIN	3	Unassigned IP
Jul-26-2021	14:32:50	bad-nameservers-host-dtq.rpzfeeds.com	QNAME	NXDOMAIN	8	Bad Nameserver Host

Showing 1 to 7 of 7 entries

TIMS IPAM Software © 2013-2021 TCPWave Inc., All Rights Reserved. August 3rd 2021, 23:59:12 PM UTC

License Expires In 3

Top Queried RPZ Logs Report


https://10.1.10.120:7443/tims/rpzlogsreport
ck Tasks
Network Management
Infrastructure Management
Reports
Administration
ALL
GENERATE
20

DNS RPZ Logs Report By Appliance

☑ DNS Appliance : 10.1.10.122

□ Client Source IP:

Date	Time	DNS Appliance	Client Source IP	Blocked DNS Query FQDN	Blocked DNS Query Type	Blocked DNS Query Response	Reason
Jul-27-2021	12:21:14	10.1.10.122	127.0.0.1	bad-nameservers-host-dtq.rpzfeeds.com	QNAME	NXDOMAIN	Bad Nameserver Host
Jul-26-2021	19:18:01	10.1.10.122	127.0.0.1	bad-nameservers-host-dtq.rpzfeeds.com	QNAME	NXDOMAIN	Bad Nameserver Host
Jul-26-2021	19:18:01	10.1.10.122	127.0.0.1	bad-nameservers-host-dtq.rpzfeeds.com	QNAME	NXDOMAIN	Bad Nameserver Host
Jul-26-2021	14:40:32	10.1.10.122	127.0.0.1	bad-nameservers-host-dtq.rpzfeeds.com	QNAME	NXDOMAIN	Bad Nameserver Host
Jul-26-2021	14:40:28	10.1.10.122	127.0.0.1	bad-nameservers-host-dtq.rpzfeeds.com	QNAME	NXDOMAIN	Bad Nameserver Host
Jul-26-2021	14:39:04	10.1.10.122	127.0.0.1	bad-nameservers-host-dtq.rpzfeeds.com	QNAME	NXDOMAIN	Bad Nameserver Host
Jul-26-2021	14:39:00	10.1.10.122	127.0.0.1	bad-nameservers-host-dtq.rpzfeeds.com	QNAME	NXDOMAIN	Bad Nameserver Host
Jul-26-2021	14:32:50	10.1.10.122	127.0.0.1	bad-nameservers-host-dtq.rpzfeeds.com	QNAME	NXDOMAIN	Bad Nameserver Host
Jul-26-2021	14:08:16	10.1.10.122	5.188.206.236	mail01.einfach69.com	QNAME	NXDOMAIN	Bad Reputation Host
Jul-26-2021	12:38:58	10.1.10.122	89.248.165.164	67b.org	IP	NXDOMAIN	Unassigned IP
Jul-25-2021	12:38:57	10.1.10.122	89.248.165.164	67b.org	IP	NXDOMAIN	Unassigned IP
Jul-24-2021	23:24:46	10.1.10.122	185.143.223.11	correo.t18.Mcbgj7eawsaurllw.com	NSDNAME	NXDOMAIN	Bad Nameserver Host
Jul-24-2021	20:54:58	10.1.10.122	78.128.113.98	mxs.morlingglobal.com	QNAME	NXDOMAIN	Bad Reputation Host
Jul-24-2021	12:39:01	10.1.10.122	89.248.165.164	67b.org	IP	NXDOMAIN	Unassigned IP
Jul-24-2021	06:21:54	10.1.10.122	185.143.223.22	mail5.eugerix.com	QNAME	NXDOMAIN	Bad Reputation Host
Jul-24-2021	01:16:42	10.1.10.122	5.188.206.146	mx5.tenno.kmip.net	QNAME	NXDOMAIN	Bad Reputation Host

Showing 1 to 16 of 16 entries

TIMS IPAM Software © 2013-2021 TCPWave Inc., All Rights Reserved. August 3rd 2021, 23:36:33 PM UTC

License Expires In 32

DNS RPZ Logs Report by Appliance

Advantages

DNS Titan End-User Security provides multiple advantages, including the following:

- It prevents users (and applications) from accessing malicious sites, including malware, ransomware, phishing, adware, and botnet sites.
- It prevents some types of malware from reaching devices, so there is not a need to attempt to quickly detect this malware on a device and remove it before it does damage or spreads.

- It protects without having to install and continually update software on the many DNS clients that exist.
- It protects by using high-quality threat intelligence data from Spamhaus, a trusted authority on IP and domain reputation data and an industry leader for providing threat intelligence data.

TCPWave sets a high security standard by offering scalable, enterprise-grade, and integrated protection of DNS infrastructure. For more information on how TCPWave and its extensive security features can meet your needs, contact the TCPWave Sales Team.