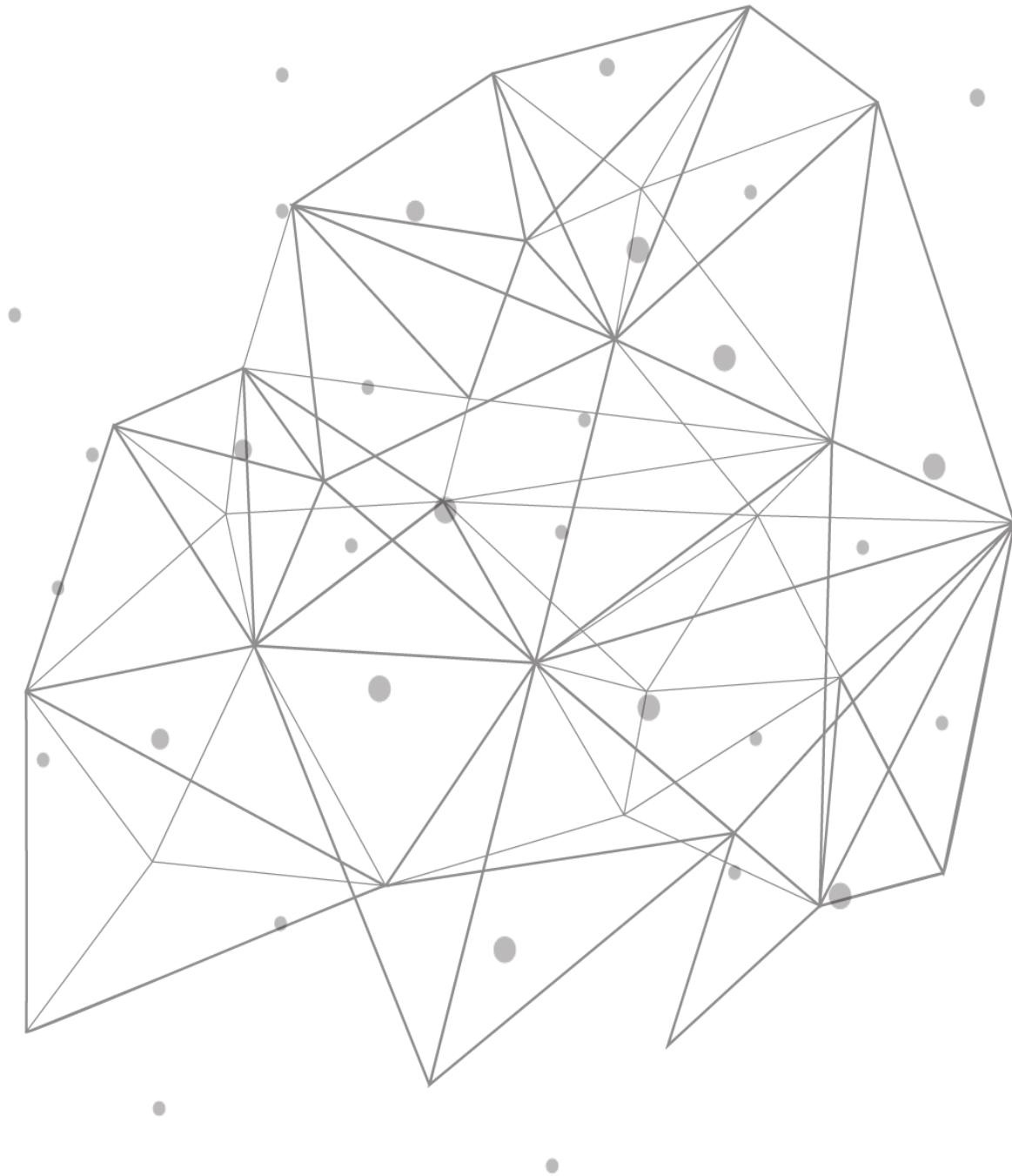

TCPWave DDI

DNS IPv4 Reports



Introduction

A DDI solution (DNS, DHCP, and IP address management) is an essential tool for any organization. As the organizations grow, they continue to add new IP addresses at an ever-increasing pace. TCPWave's DDI solutions provide organizations with the tools needed to monitor and administer their IP addresses, DNS, and DHCP services on a real-time basis. Its integrated, centralized approach to deliver enterprise-grade DDI - supports existing and evolving IT needs while providing the highest standards for security and uptime. It ensures operational efficiency and reduced cost. As the organization's network data lies within the application, the TCPWave reporting framework monitors your core services to keep the applications up and running. It ensures robust visibility to reduce the risk of DNS-based vulnerabilities. This whitepaper provides insights on the DNS IPv4 Reports.



DNS Reports

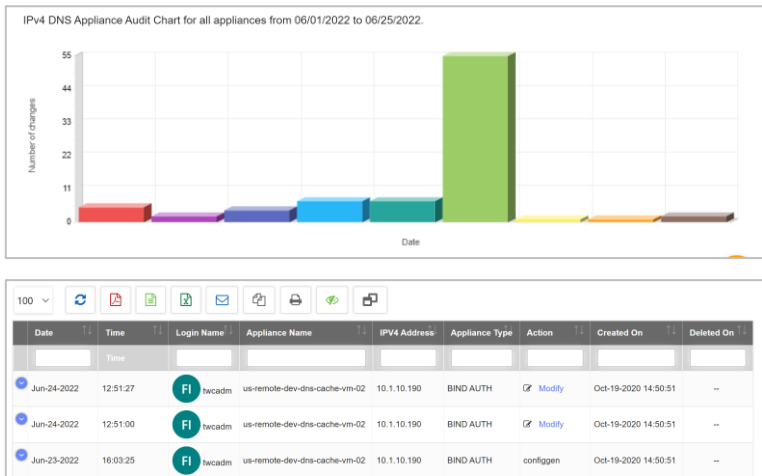
The DNS reports are grouped as follows:

- IPv4 DNS Reports
 - IPv4 DNS Appliance Audit
 - DNS ACL Audit
 - DNS TSIG Key Audit
 - DNS Internal Hints Audit

- DNS Dotted Hostnames Report
- DNS Instant Traffic Report
- DNS Contingency Switch Report
- IPv6 DNS Reports
 - IPv6 DNS Appliance Audit
 - IPv6 Reverse Zones Audit
- DNS Template Reports
- DNS Zone Reports
- DNS RPZ Reports
- DNS Views Reports
- DNS Query Reports
- DNS Security Reports
- Microsoft DNS Reports

IPv4 DNS Reports

Report Name	IPv4 DNS Appliance Audit
Description	It provides complete audit information regarding operations performed on a specific DNS Appliance or All Appliances by an administrator. The IPAM retrieves and displays the information for a specified time provided by the users
Grid Data	<ul style="list-style-type: none"> ● Date ● Time ● Login Name ● Appliance Name ● IPv4 Address ● Appliance Type ● Action ● Status ● Created On ● Deleted On ● Message ● Description

Report Name	IPv4 DNS Appliance Audit																																				
<p>Bar Chart Data</p>	<p>Displays the following information of all the appliances for the specified date range.</p> <ul style="list-style-type: none"> On X-axis: Displays the date on which the operations were performed. On Y-axis: Displays the number of modifications made on the appliances. 																																				
<p>Sample Report</p>	 <p>IPv4 DNS Appliance Audit Chart for all appliances from 06/01/2022 to 06/25/2022.</p> <table border="1"> <thead> <tr> <th>Date</th> <th>Time</th> <th>Login Name</th> <th>Appliance Name</th> <th>IPv4 Address</th> <th>Appliance Type</th> <th>Action</th> <th>Created On</th> <th>Deleted On</th> </tr> </thead> <tbody> <tr> <td>Jun-24-2022</td> <td>12:51:27</td> <td>fi@cadm</td> <td>us-remote-dev-dns-cache-vm-02</td> <td>10.1.10.190</td> <td>BIND AUTH</td> <td>Modify</td> <td>Oct-19-2020 14:50:51</td> <td>--</td> </tr> <tr> <td>Jun-24-2022</td> <td>12:51:00</td> <td>fi@cadm</td> <td>us-remote-dev-dns-cache-vm-02</td> <td>10.1.10.190</td> <td>BIND AUTH</td> <td>Modify</td> <td>Oct-19-2020 14:50:51</td> <td>--</td> </tr> <tr> <td>Jun-23-2022</td> <td>16:03:25</td> <td>fi@cadm</td> <td>us-remote-dev-dns-cache-vm-02</td> <td>10.1.10.190</td> <td>BIND AUTH</td> <td>configgen</td> <td>Oct-19-2020 14:50:51</td> <td>--</td> </tr> </tbody> </table>	Date	Time	Login Name	Appliance Name	IPv4 Address	Appliance Type	Action	Created On	Deleted On	Jun-24-2022	12:51:27	fi@cadm	us-remote-dev-dns-cache-vm-02	10.1.10.190	BIND AUTH	Modify	Oct-19-2020 14:50:51	--	Jun-24-2022	12:51:00	fi@cadm	us-remote-dev-dns-cache-vm-02	10.1.10.190	BIND AUTH	Modify	Oct-19-2020 14:50:51	--	Jun-23-2022	16:03:25	fi@cadm	us-remote-dev-dns-cache-vm-02	10.1.10.190	BIND AUTH	configgen	Oct-19-2020 14:50:51	--
Date	Time	Login Name	Appliance Name	IPv4 Address	Appliance Type	Action	Created On	Deleted On																													
Jun-24-2022	12:51:27	fi@cadm	us-remote-dev-dns-cache-vm-02	10.1.10.190	BIND AUTH	Modify	Oct-19-2020 14:50:51	--																													
Jun-24-2022	12:51:00	fi@cadm	us-remote-dev-dns-cache-vm-02	10.1.10.190	BIND AUTH	Modify	Oct-19-2020 14:50:51	--																													
Jun-23-2022	16:03:25	fi@cadm	us-remote-dev-dns-cache-vm-02	10.1.10.190	BIND AUTH	configgen	Oct-19-2020 14:50:51	--																													

Report Name	DNS ACL Audit
<p>Description</p>	<p>It provides the complete audit information regarding DNS ACL operations performed by an administrator based on the selected date range.</p>
<p>Grid Data</p>	<ul style="list-style-type: none"> Date Time Login Name Administrator ACL Name Action Status Message

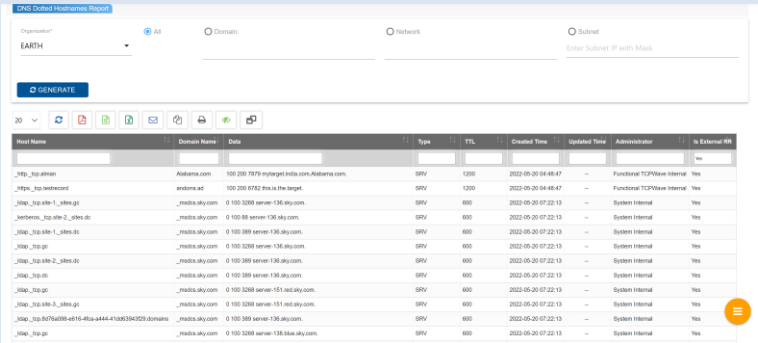
Report Name DNS ACL Audit	
	<ul style="list-style-type: none"> Description
Bar Chart Data	<p>Displays the following information for the specified date range.</p> <ul style="list-style-type: none"> On X-axis: Displays the date on which the changes were made on a particular ACL. On Y-axis: Displays the number of changes made on a particular ACL for a specified date range.
Sample Report	

Report Name DNS TSIG Key Audit	
Description	It displays the information about the actions performed on the DNS TSIG keys in the TCPWave IPAM application.
Grid Data	<ul style="list-style-type: none"> Date Time Login Name Administrator TSIG Key Name Algorithm Action Status

Report Name	DNS TSIG Key Audit
	<ul style="list-style-type: none"> Secret Key
Bar Chart Data	<p>Displays the following information for the specified date range:</p> <ul style="list-style-type: none"> On X-axis: Displays the date on which the changes were made on a particular TSIG key. On Y-axis: Displays the number of changes made on a particular TSIG key for a specified date range.

Report Name	DNS Internal Hints Audit
Description	This report provides information about the change history of DNS internet root hints based on the specified date range.
Grid Data	<ul style="list-style-type: none"> Time Action Login Name Administrator TTL NS record IPv4 IP Address IPv6 IP Address
Sample Report	<p>The screenshot shows a report titled "DNS Internal Hints Audit" with a date range from 06/01/2022 to 07/01/2022. Below the date range is a table with the following columns: Time, Action, Login Name, Administrator, TTL, NET, IPv4 IP Address, IPv6 IP Address, and Description. The table contains 13 rows of data, each representing a change to a different root hint (A through M). The descriptions include "FORMERLY NS.INTERNIC.NET", "FORMERLY NS.NI.ISB.EDU", "FORMERLY C.PS.NET", "FORMERLY TERP.UMD.EDU", "FORMERLY NS.NASA.SOV", "FORMERLY NS.NIC.EDU.MIL", "FORMERLY AOE.ARL.ARMY.MIL", "FORMERLY NS.NIC.NORDU.NET", "OPERATED BY VERISIGN, INC.", "OPERATED BY RIPE NCC", "OPERATED BY ICANN", and "OPERATED BY WIDE".</p>

Report Name	DNS Dotted Hostnames Report
Description	It displays the audit information about the Dotted Hostnames for Object, Resource

Report Name	DNS Dotted Hostnames Report																																																																																																			
	Record, and Zone Resource Record. You can filter the report to return the entire organization's list or for a specific domain, network, or subnet.																																																																																																			
Grid Data	<ul style="list-style-type: none"> • Host Name • Domain Name • Data • Type • TTL • Created Time • Updated Time • Administrator • Is External RR 																																																																																																			
Sample Report	 <table border="1"> <thead> <tr> <th>Host Name</th> <th>Domain Name</th> <th>Data</th> <th>Type</th> <th>TTL</th> <th>Created Time</th> <th>Updated Time</th> <th>Administrator</th> <th>Is External RR</th> </tr> </thead> <tbody> <tr> <td>_ftp._tcp.alpha</td> <td>Alabama.com</td> <td>100 200 7979 mytarget.india.com:Alabama.com.</td> <td>SRV</td> <td>1200</td> <td>2022-05-20 04:48:47</td> <td>-</td> <td>Functional TCPWave Internal</td> <td>Yes</td> </tr> <tr> <td>_ftp._tcp.beta</td> <td>androme.ad</td> <td>100 200 6762 this is the target.</td> <td>SRV</td> <td>1200</td> <td>2022-05-20 04:48:47</td> <td>-</td> <td>Functional TCPWave Internal</td> <td>Yes</td> </tr> <tr> <td>_ftp._tcp.alpha_1_alpha.gi</td> <td>_medica.sky.com</td> <td>@ 100 3208 server-136.sky.com.</td> <td>SRV</td> <td>600</td> <td>2022-05-20 07:22:15</td> <td>-</td> <td>System Internal</td> <td>Yes</td> </tr> <tr> <td>_medica._tcp.alpha_2_alpha.do</td> <td>_medica.sky.com</td> <td>@ 100 88 server-136.sky.com.</td> <td>SRV</td> <td>600</td> <td>2022-05-20 07:22:15</td> <td>-</td> <td>System Internal</td> <td>Yes</td> </tr> <tr> <td>_ftp._tcp.alpha_1_alpha.do</td> <td>_medica.sky.com</td> <td>@ 100 389 server-136.sky.com.</td> <td>SRV</td> <td>600</td> <td>2022-05-20 07:22:15</td> <td>-</td> <td>System Internal</td> <td>Yes</td> </tr> <tr> <td>_ftp._tcp.alpha_2_alpha.do</td> <td>_medica.sky.com</td> <td>@ 100 3208 server-136.sky.com.</td> <td>SRV</td> <td>600</td> <td>2022-05-20 07:22:15</td> <td>-</td> <td>System Internal</td> <td>Yes</td> </tr> <tr> <td>_ftp._tcp.alpha</td> <td>_medica.sky.com</td> <td>@ 100 389 server-136.sky.com.</td> <td>SRV</td> <td>600</td> <td>2022-05-20 07:22:15</td> <td>-</td> <td>System Internal</td> <td>Yes</td> </tr> <tr> <td>_ftp._tcp.alpha_3_alpha.gi</td> <td>_medica.sky.com</td> <td>@ 100 3208 server-151.net.sky.com.</td> <td>SRV</td> <td>600</td> <td>2022-05-20 07:22:15</td> <td>-</td> <td>System Internal</td> <td>Yes</td> </tr> <tr> <td>_ftp._tcp.alpha_2_alpha.gi</td> <td>_medica.sky.com</td> <td>@ 100 389 server-136.sky.com.</td> <td>SRV</td> <td>600</td> <td>2022-05-20 07:22:15</td> <td>-</td> <td>System Internal</td> <td>Yes</td> </tr> <tr> <td>_ftp._tcp.alpha</td> <td>_medica.sky.com</td> <td>@ 100 389 server-136.sky.com.</td> <td>SRV</td> <td>600</td> <td>2022-05-20 07:22:15</td> <td>-</td> <td>System Internal</td> <td>Yes</td> </tr> </tbody> </table>	Host Name	Domain Name	Data	Type	TTL	Created Time	Updated Time	Administrator	Is External RR	_ftp._tcp.alpha	Alabama.com	100 200 7979 mytarget.india.com:Alabama.com.	SRV	1200	2022-05-20 04:48:47	-	Functional TCPWave Internal	Yes	_ftp._tcp.beta	androme.ad	100 200 6762 this is the target.	SRV	1200	2022-05-20 04:48:47	-	Functional TCPWave Internal	Yes	_ftp._tcp.alpha_1_alpha.gi	_medica.sky.com	@ 100 3208 server-136.sky.com.	SRV	600	2022-05-20 07:22:15	-	System Internal	Yes	_medica._tcp.alpha_2_alpha.do	_medica.sky.com	@ 100 88 server-136.sky.com.	SRV	600	2022-05-20 07:22:15	-	System Internal	Yes	_ftp._tcp.alpha_1_alpha.do	_medica.sky.com	@ 100 389 server-136.sky.com.	SRV	600	2022-05-20 07:22:15	-	System Internal	Yes	_ftp._tcp.alpha_2_alpha.do	_medica.sky.com	@ 100 3208 server-136.sky.com.	SRV	600	2022-05-20 07:22:15	-	System Internal	Yes	_ftp._tcp.alpha	_medica.sky.com	@ 100 389 server-136.sky.com.	SRV	600	2022-05-20 07:22:15	-	System Internal	Yes	_ftp._tcp.alpha_3_alpha.gi	_medica.sky.com	@ 100 3208 server-151.net.sky.com.	SRV	600	2022-05-20 07:22:15	-	System Internal	Yes	_ftp._tcp.alpha_2_alpha.gi	_medica.sky.com	@ 100 389 server-136.sky.com.	SRV	600	2022-05-20 07:22:15	-	System Internal	Yes	_ftp._tcp.alpha	_medica.sky.com	@ 100 389 server-136.sky.com.	SRV	600	2022-05-20 07:22:15	-	System Internal	Yes
Host Name	Domain Name	Data	Type	TTL	Created Time	Updated Time	Administrator	Is External RR																																																																																												
_ftp._tcp.alpha	Alabama.com	100 200 7979 mytarget.india.com:Alabama.com.	SRV	1200	2022-05-20 04:48:47	-	Functional TCPWave Internal	Yes																																																																																												
_ftp._tcp.beta	androme.ad	100 200 6762 this is the target.	SRV	1200	2022-05-20 04:48:47	-	Functional TCPWave Internal	Yes																																																																																												
_ftp._tcp.alpha_1_alpha.gi	_medica.sky.com	@ 100 3208 server-136.sky.com.	SRV	600	2022-05-20 07:22:15	-	System Internal	Yes																																																																																												
_medica._tcp.alpha_2_alpha.do	_medica.sky.com	@ 100 88 server-136.sky.com.	SRV	600	2022-05-20 07:22:15	-	System Internal	Yes																																																																																												
_ftp._tcp.alpha_1_alpha.do	_medica.sky.com	@ 100 389 server-136.sky.com.	SRV	600	2022-05-20 07:22:15	-	System Internal	Yes																																																																																												
_ftp._tcp.alpha_2_alpha.do	_medica.sky.com	@ 100 3208 server-136.sky.com.	SRV	600	2022-05-20 07:22:15	-	System Internal	Yes																																																																																												
_ftp._tcp.alpha	_medica.sky.com	@ 100 389 server-136.sky.com.	SRV	600	2022-05-20 07:22:15	-	System Internal	Yes																																																																																												
_ftp._tcp.alpha_3_alpha.gi	_medica.sky.com	@ 100 3208 server-151.net.sky.com.	SRV	600	2022-05-20 07:22:15	-	System Internal	Yes																																																																																												
_ftp._tcp.alpha_2_alpha.gi	_medica.sky.com	@ 100 389 server-136.sky.com.	SRV	600	2022-05-20 07:22:15	-	System Internal	Yes																																																																																												
_ftp._tcp.alpha	_medica.sky.com	@ 100 389 server-136.sky.com.	SRV	600	2022-05-20 07:22:15	-	System Internal	Yes																																																																																												

Report Name	DNS Instant Traffic Report
Description	It displays the statistical information about DNS Queries Record Types, Top 100 Domain Names Requested, and Top 100 DNS Clients.
Tab Data	<ul style="list-style-type: none"> • Requested DNS Resource Record Types <ul style="list-style-type: none"> ○ DNS Queries Record Types ○ Total DNS Queries Processed • Top 100 Domain Names Requested <ul style="list-style-type: none"> ○ Fully Qualified Domain Name ○ Total Number of Requests • Top 100 DNS Clients

Report Name **DNS Instant Traffic Report**

- DNS Client Name
- Total Number of Requests

Sample Report

The sample report consists of three screenshots from the TCPWave DNS Instant Traffic Report interface. Each screenshot shows the report configuration for 'EARTH' organization and 'CERT-INTERNAL-CACHE' appliance, with a 'GENERATE' button.

Screenshot 1: DNS Queries Record Types

DNS Queries Record Types	Total DNS Queries Processed
NS	33900
SOA	54600
A	14162
PTR	1628
CNAME	30
AFSDB	5
MX	2
AAAA	2

Screenshot 2: Fully Qualified Domain Name

Fully Qualified Domain Name	Total Number of Requests
.	959
CERT-AUTH-MASTER.DNS1.welcome.tcpwave.com	862
www.com	3504
138.138.in-addr.arpa	3504
138.138.in-addr.arpa	3503
aaaa000.com	3503
com	3502
gov	3501
140.140.in-addr.arpa	3501
abc.com	3500

Screenshot 3: DNS Client Name

DNS Client Name	Total Number of Requests
10.1.10.242	330750
localhost	75291
10.1.10.142	124

Report Name **DNS Contingency Switch Report**

Description It provides the complete audit information about the switch operations performed on a service based on the specified date range.

- Grid Data**
- Time
 - Service Name

Report Name	DNS Contingency Switch Report
	<ul style="list-style-type: none"> • Service Mode • CNAME • Target RR • Administrator • Schedule Job • Execution Status
<p>Sample Report</p>	

Conclusion

With such a robust and powerful monitoring engine embedded as an integral part of the TCPWave IPAM, organizations can dramatically improve their service level agreements and keep their mission-critical services up and running. The network administrators have the power to manage the entire DDI suite with the most reliable, secure services and the best real-time views – all from a single pane of glass that serves as a single source of truth. For a quick demo on enforcing monitoring and enhancing the organization’s DNS service availability, contact the [TCPWave Sales Team](#).