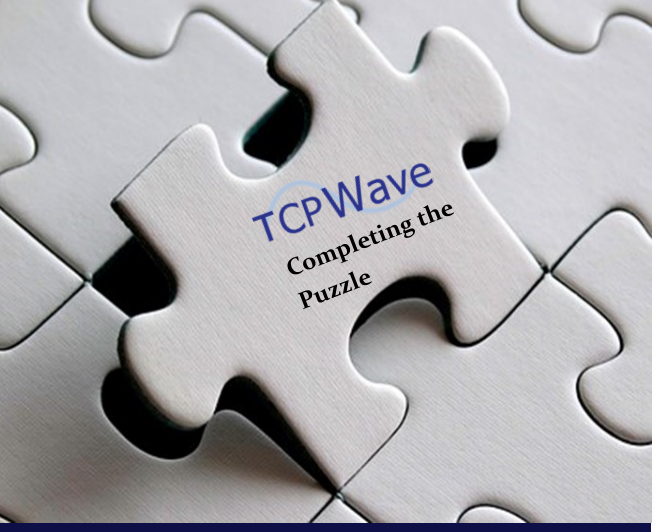
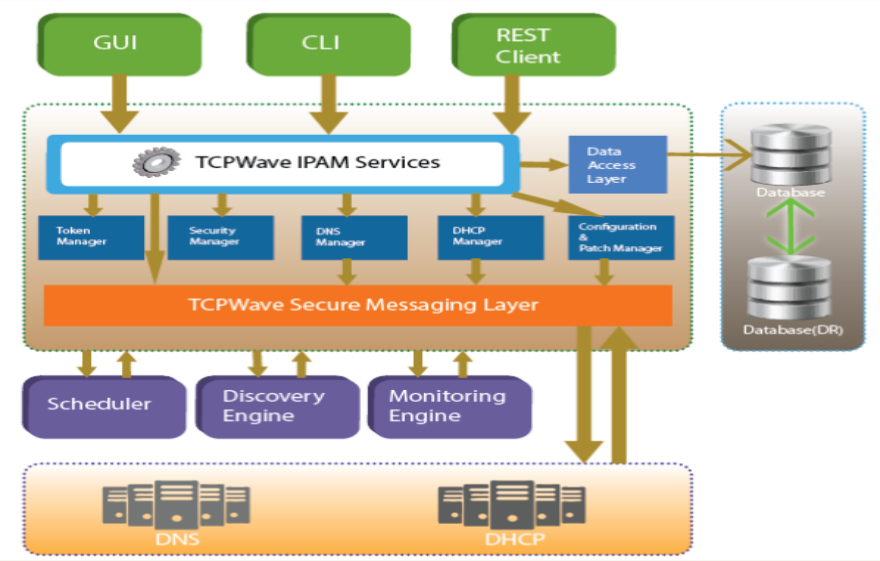
Partnering with our customers to solve their current and future DNS, DHCP and IP Address Management needs



The TCPWave IPAM Solution

Aligning One Single View of your IP Address Space

TCPWave's software for DNS, DHCP and IP Address Management (DDI) includes a full featured and integrate-able solution that helps network administrators eliminate network conflicts and outages, track critical assets, ensure network security and provide reports based on a wide range of parameters, including IP address status (dynamic, static, available, reserved, etc.), networks, subnets, and admin activities. TCPWave IP Address Management (IPAM) allows the Network Personnel to automate the process of allocating and de-allocating IP address resources. This automation is both efficient and intelligent. The IPAM can dynamically manage the available address space by complying with the organization's IP Address and Security policies. TCPWave IPAM provides an intuitive Graphical Web User Interface for managing DDI as well as all related services. TCPWave DDI can manage multiple external DNS hosting services, manage TCPWave DNS in the Cloud as well as multiple DNS vendors to minimize myriad DNS attacks. The architecture and design of the TCPWave DDI solution is built using state of the art technology.



Built With The Latest Technology

TCPWave IPAM is built from scratch using the latest technologies including robust jQuery framework and Java. One of the primary benefits of TCPWave IPAM is the ability to handle cross browser issues seamlessly. TCPWave's IPAM, built using the latest Java technology, is much faster and can seamlessly integrate into the existing automation via RESTful API calls.

Fully published interfaces

TCPWave has a fully published **REST** API. The REST API can be used to communicate with all external REST interfaces. TCPWave provides preconfigured REST communication with all of the most popular public and private Cloud providers allowing customers to stay focused on network obligations. TCPWave's RESTful API comes with extensive documentation and examples.

For legacy communication, TCPWave provides a robust Command Line Interface (**CLI**) .

TCPWave DNS, DHCP and IP Address Management

Transforming customers' Address Space from fragile to agile.

Why TCPWave?

TCPWave was built with native cloud, automation, and virtual computing in scope. Most competing products have been designed and built before any of these robust technologies were born.

Using agile engineering, REST as the core, and Java for the GUI, TCPWave is positioned to quickly adapt to today and tomorrow's rapidly advancing technology.

TCPWave works with customers to ensure integration with any commercial or customer developed application that is needed to acquire or supply information to IPAM.

TCPWave High Availability provides the highest level of availability and security in the industry. With its N>2 IPAM support, three or more IPAM servers can be geolocated around the world. Each server contains **all** of the IPAM data in real-time. Similar to disk RAID, If you loose one IPAM the others will continue without problems. If IPAM servers go down, as long as one is still operating, the remotes will continue to operate with no DNS or DHCP interruption.

TCPWave truly partners with our customers. Necessary enhancements are provided in a timely manner.

Auto Discovery

Auto Discovery is designed for organizations with complex and dynamic network infrastructure. It automatically discovers your network topology and updates itself when new subnets are discovered on the network. The networks and subnets can be configured to be scanned periodically to detect the changes in the network nodes and then update the object data. It can discover all the network devices and their configuration via ICMP, SNMP and NetBIOS protocols and consolidate the newly collected data with the existing data.

Switch Port Discovery

Switch Port Discovery Is designed to discover switches in a given subnet and the devices connected to those switches. As part of the discovery, the VLAN and port details will also be discovered. IP Address, MAC Address, Switch Name, Port Name and Port Duplex settings will be collected for each device. These devices can then be added to TCPWave IPAM subnets.

Cloud Discovery

Cloud Discovery can fully discover subnets, objects and DNS resource records within all major Cloud environments and then update TCPWave DDI.

VMware Discovery

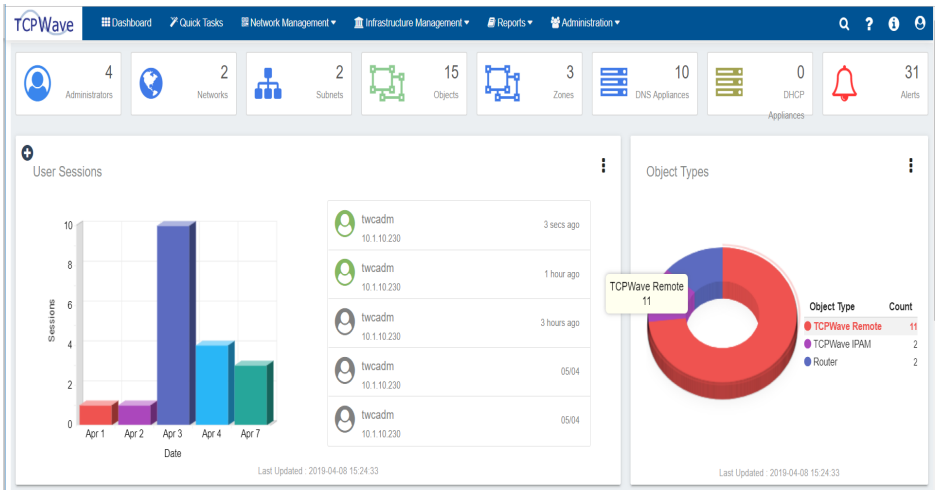
VMware Discovery enables discovery of the virtual instances in the VMware Infrastructure. The discovered objects can then be added to the desired subnets in TCPWave.

AWS Alias Resource Records

TCPWave fully supports AWS Alias RRs.

Simplified Dashboard

TCPWave's IPAM solution provides fault management, performance management, configuration assurance, and patch management in one bundle. There is no need to purchase monitoring software to manage your DNS Infrastructure. TCPWave's IPAM integrates with customer provided EMC SMARTS and automatically sends SNMP alerts when critical events arise in IPAM operation. Scheduled changes can be managed more efficiently and roll backs take place automatically if the change implementation fails. TCPWave also provides a powerful dashboard to monitor all the core components of the DDI infrastructure managed by the TCPWave IPAM with extensive graphing capabilities for performance management metrics. TCPWave's DNS and DHCP appliances are automatically added to the fault and performance monitoring.



Syslog-ng

TCPWave uses syslog-ng instead of syslogd. Syslog-ng provides robust log manipulation and analysis. If customers already use a global syslog-ng manager, TCPWave can forward its logs to the customers' syslog-ng implementation.

IPv4 and IPv6 Support

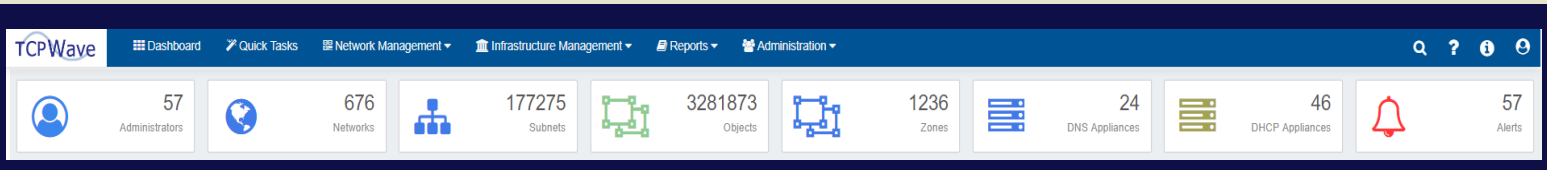
TCPWave's IPAM solution supports both IPv4 and IPv6 out of the box. No additional license is needed for IPv6.

DNS Cookie Support

DNS Cookie is an Extended DNS (EDNS) option which, when both the client and server support it, allows the client to detect and ignore off-path spoofed responses, and the server to determine that a client's address is not spoofed.

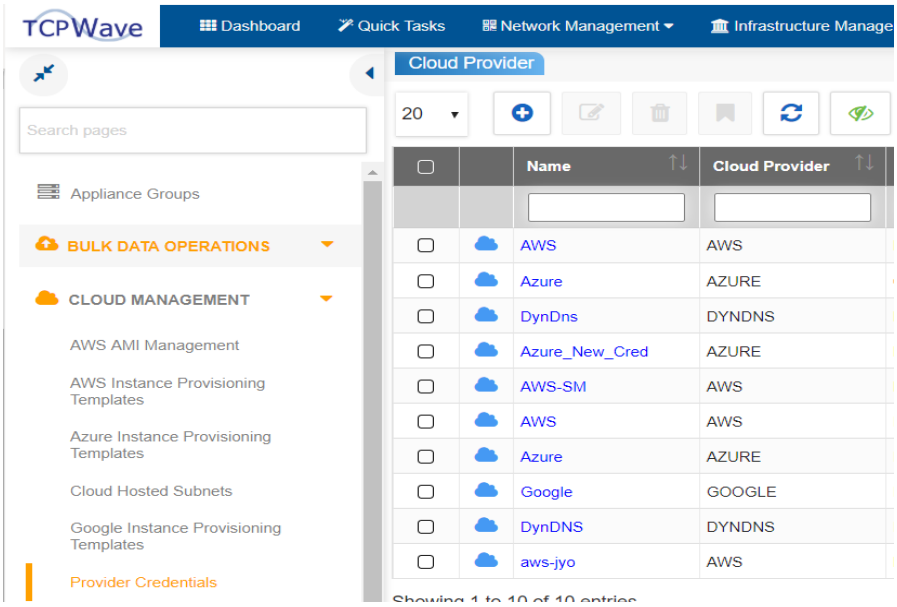
Network and Health Management

TCPWave's IPAM enforces strict database integrity checks. Its smart logic checks the sanity of the DNS and DHCP configuration files before sending them to the remote DNS and DHCP devices. Powerful metrics used by the dashboard assist in identifying bottlenecks in the network. Administrators can use alarm subscriptions to ensure they are informed if any selected alarms are generated.



Unsurpassed Cloud Management

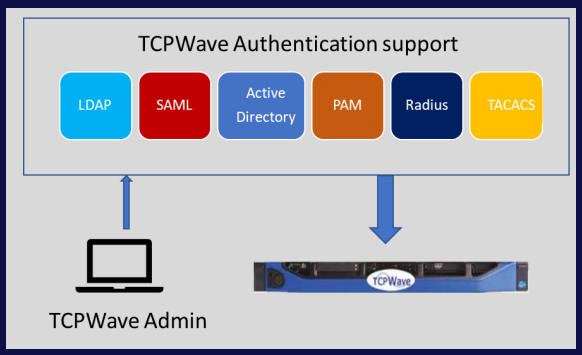
TCPWave has preconfigured its REST interface to communicate with most of the top Cloud providers and is easily configured for any private Cloud. IPAM can host zones in multiple Cloud providers or run the TCPWave DNS server in the cloud. The ability to start up many more DNS servers by cloning the servers in the TCPWave GUI, or manage and update zones in Cloud providers with many points of entry around the world, is necessary to withstand the intensity of today's malicious DDoS attacks.



- Amazon
- Google
- Microsoft Azure
- Dyn/Oracle
- Verisign
- Akamai
- OpenStack

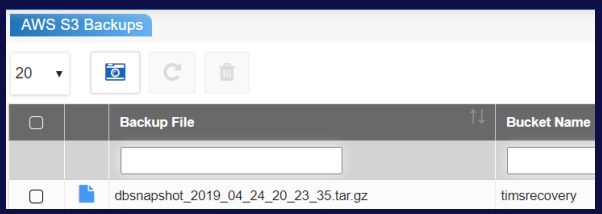
Logon Authentication Support

Customers can use any one of the below popular authentication software services. TCPWave administrators will be authenticated using the customer's corporate security policies. For Active Directory , administrators can inherit the admin roles in AD.



AWS Database Backup Storage

Customers can export database backups directly into AWS.



Terraform Cloud Workflow Integration

TCPWave provides automated DDI workflow from customers internal applications to customers Cloud instances while updating TCPWave.

- Add, Modify and Delete subnets and objects
- Create VPC with custom DHCP Options Set
- Create VPC with next available IP block with given mask
- Create VPC with given IP block
- Create next available Subnet in AWS in given VPC

External DNS Diversification

External DNS diversification is **mandatory** in today's networks. TCPWave will suit your needs whether it is multiple DNS Cloud hosting or dual DNS servers running different code. TCPWave can mange all of this in a single pane of glass.

ServiceNow integration

TCPWave Integrates ServiceNow trouble tickets with TCPWave DDI modifications performed by administrators. All modifications are audited by trouble ticket number. Admins can easily undo all or some modifications by trouble ticket number, or easily search for any modification made using a particular trouble ticket. A global policy can be used to make trouble ticket mandatory for all modifications.

CIO APPLICATIONS TOP 25 CYBER SECURITY COMPANIES - 2017

Secure Message Channel

Traditional DNS is vulnerable to multiple security exploits. Managing DNS with DNSSEC or GSS-TSIG has many operational overheads. Sending DNS updates using UDP port 53 has been proven as an insecure way to operate the mission critical DNS infrastructure. TCPWave has designed a revolutionary **method of securing dynamic changes using a robust security model**. Changes made in the IP Address Management web interface are sent using a secure conduit from the management server to the remote DNS server. Powerful logic developed in Java examines the contents of the update, determines the authenticity of the source IP Address, and verifies if the IPAM server sent the message and then processes the message. After updating the master DNS, the secure conduit service sends an acknowledgement back to the management server. If the acknowledgement is not received, the management server sends a retry. This communication uses a TCP port with a 1024 bit encryption key.

Robust Patching with Workflow

The TCPWave IP Management System's Patch Management component provides a seamless way to patch any system in the IPAM's echo system. The patching is done using IPAM's secure message channel. Every patch is securely encrypted. Robust patching can be applied and rolled back to single appliances or appliance groups. When more than one appliance is selected, the patch can be deployed using workflow: Deploy in sequence and/or in parallel; Rollback on the failed appliance or on all appliances; Deploy immediately or via schedule. So, when a system in the IPAM constellation needs to be patched to fix a problem or for any other reason, the patch management facility of IPAM can be used. Also, it allows the deployment and rollback operations to be scheduled at a later time so that they can be done at off-peak time. The patch contents are first validated before the patch can be uploaded into the patch repository. The validation process includes unzipping the patch and checking for the existence of all the mandatory files. Checks are also done to confirm that the checksum and sizes of the install image specified in the metadata match with the actual values of the install image. If any of these validations fail, the patch upload will not be permitted.

Audit and Traceability

TCPWave's IPAM comes with an extensive audit capability, which provides accurate forensics for IP Audit, subnet audit, network audit, domain audit, etc. You can customize the auditing policies to audit what your Security team is interested in for better audit reviewing. The Login audit enables detection of unauthorized intrusions into the system. A combination of failure and success authentication audits help determine when the breach of security occurred. Isolation and preservation of the security event log helps track users who gained unauthorized admin privileges.

Action	Entity Type	Action Status	Message	Entity	Description
delete	object	Success	Object(s) have been deleted Successfully.	192.168.8.4	Deleted Object(s) Address:192.168.8.4 FQDN: two08-obj-48.afcc.com
modify	zone	Success	Resource record has been added successfully.	azone1.com	Added a Resource Record to Zone: azone1.com,RR: ,Owner: zone1-50.azone1.com.,TTL: 1200,Class: IN,Type: A,Data: 1.2.3.50,Description:

Search Engine

The TCPWave IPAM solution provides a powerful search engine using Elastic search. It can be used to search literally anything in the IPAM subsystem.

Regular expression searches provide detailed search capabilities.

Allowed characters **a-z, A-Z, 0-9, ., @, *, #, -, +, /, (,), ?, &, [,], {, }, |, ~, and space**

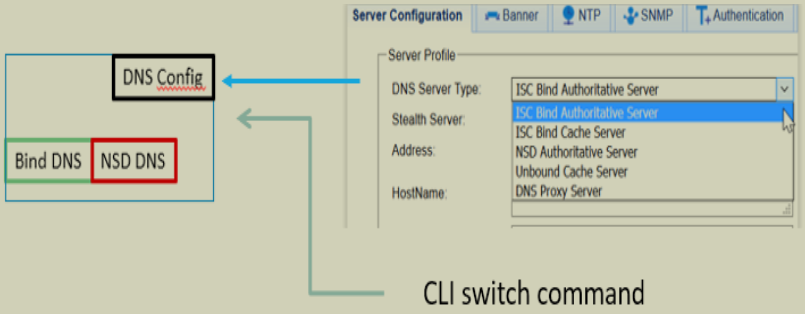
Segregation of Duties

Segregation of Duties are Control Activities that reduce the risk of error and malicious DNS/DHCP activities or human errors, through proper division of tasks between employees. As DNS and DHCP relate to the core functionality of mission critical network services, it is the proper Segregation of Duties in the TCPWave IPAM that prevents the potential for *employee circumvention of controls*. Using the TCPWave IPAM, User Administrators can only create user accounts and cannot alter DNS/DHCP data. Power and Normal accounts can alter DNS/DHCP data but they cannot define user accounts. All the user actions are audited. The various types of administrators and their descriptions are listed below:

- FADM – Functional Admin, All functionality.
- UADM – User Admin, Has access to user administration functionality only.
- SADM – Super Admin, Access to all functionality within the organization, except User administration.
- PADM – Power Admin, Has access to Zone/Domain/Server/Network/Subnet/Scope/Template/Object.
- NADM – Normal Admin, Manage permitted network resources within the organization.
- RADM – Read-only Admin , Read-only access to the resources within the organization.

Dual DNS

When the primary BIND DNS becomes compromised, the monitoring service alerts the administrator who can shut down the BIND DNS and bring up the Unbound DNS for Caching or the NSD DNS for Authoritative.



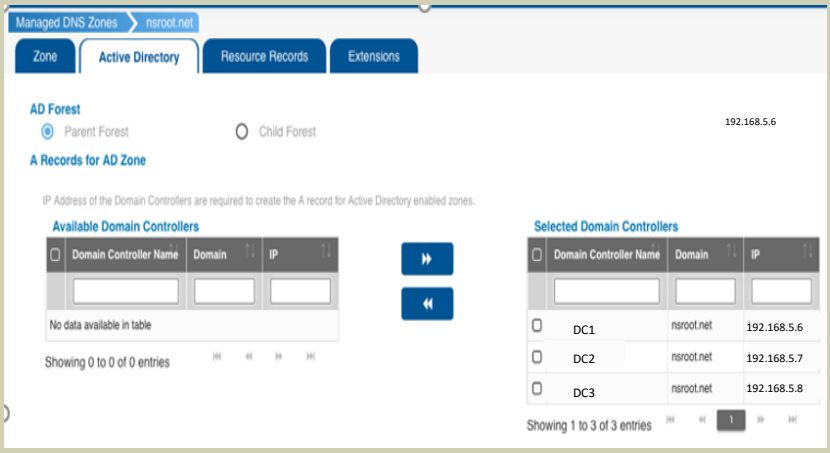
DNSSEC

The DNSSEC features include automatic key generation, zone signing, and scheduled DNSSEC key rollover. The DNSViz tool is provided for analysis and visualization of DNSSEC behavior on DNS Cache Appliances.

Microsoft DNS and DHCP

TCPWave provides full support to manage Microsoft DNS and DHCP servers from the TCPWave GUI without installing an agent on the Microsoft servers using WMI and Power Shell.

TCPWave can also integrate Microsoft DNS managed resource records and DHCP leases into its IPAM for a single view of the customers' network. Direct management is still provided by Microsoft.



Log Forwarding

TCPWave can easily configure logs to be forwarded to **Splunk, syslog-ng, Flume** and **EMC Smarts.** The data can be used for reporting, auditing, capacity planning, and security analysis. If threatening patterns are detected, the customer can use the REST API to dynamically update the DNS firewall rules and block the attack.

Undo Infrastructure

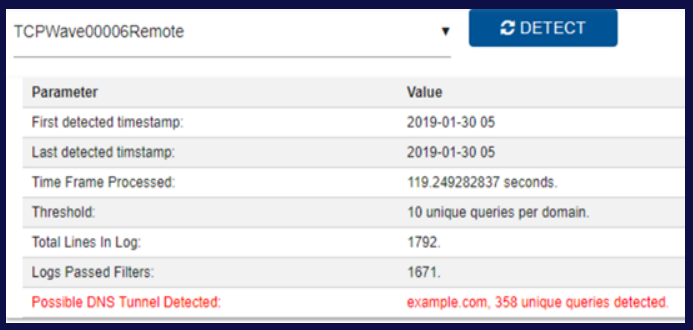
Undo modifications can be performed on **Subnet, Object/RR, Zone**, and **DHCP Scopes. Undo operations can be performed on Add, Modify and Delete operations.**

DNS Tunnel Detection

DNS Tunnel Detection can be enabled on BIND Cache, Unbound and BIND Auth+Cache appliances. Users are given the flexibility to define the thresholds to determine the possibility of the DNS tunnel.

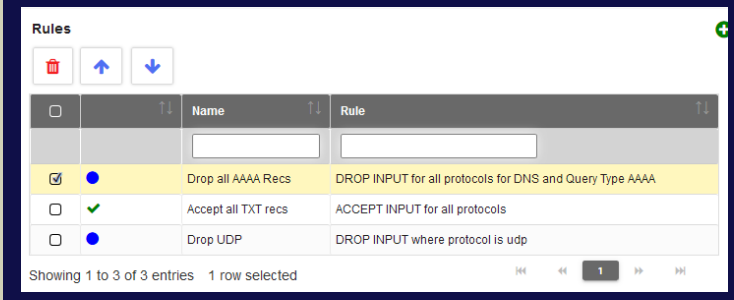
Detection logic drops the SRV and PTR records from the analysis. It considers the queries whose full query/subdomain lengths are greater than the given thresholds and the domains whose number of unique queries exceeds the threshold.

When a domain or domains are detected as possible tunnel domains, the monitoring engine will be triggered to create a critical alert.



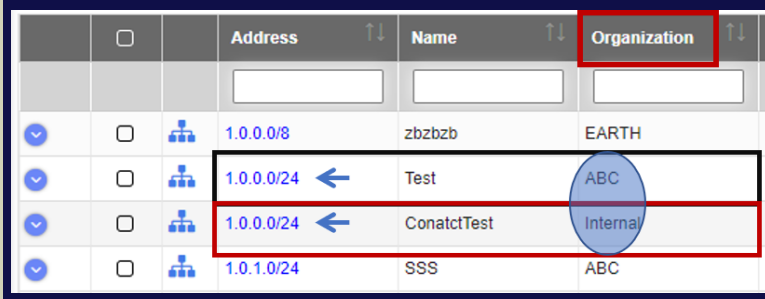
Dynamic DNS Firewall

TCPWave's robust DNS Firewall is managed directly from the GUI at no additional cost to the customer.



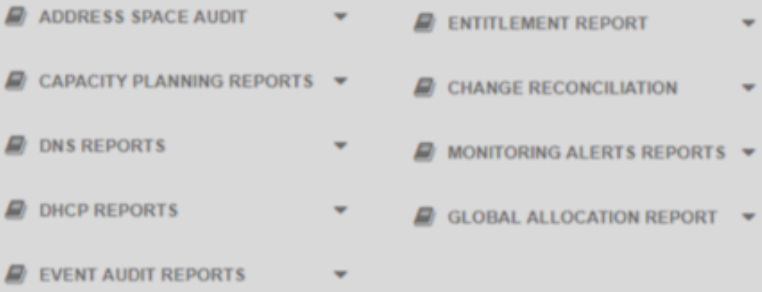
Secure Multitenancy

TCPWave provides multitenancy using Organizations. Overlapping address space is handled with separate Organizations. All address space is visible in a single pane of glass to a super user profiles. Organizations can be imported and exported using the TCPWave bulk data operations.



Robust Reporting

TCPWave DDI provides a full set of comprehensive reports at no extra cost to the customer.

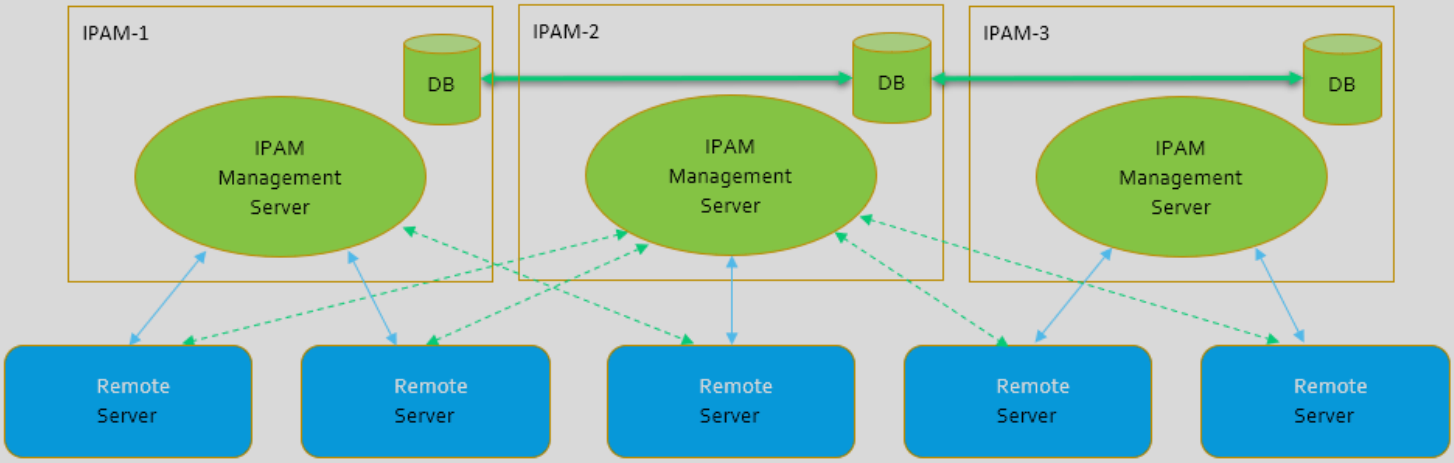


Network Address	%Full
192.168.0.0/24	14.46
192.168.1.0/24	0.91
192.168.2.0/24	24.75
192.168.3.0/24	42.73
192.168.4.0/24	10.68
192.168.5.0/24	35.99
192.168.6.0/24	47.90

High Availability and Scalability

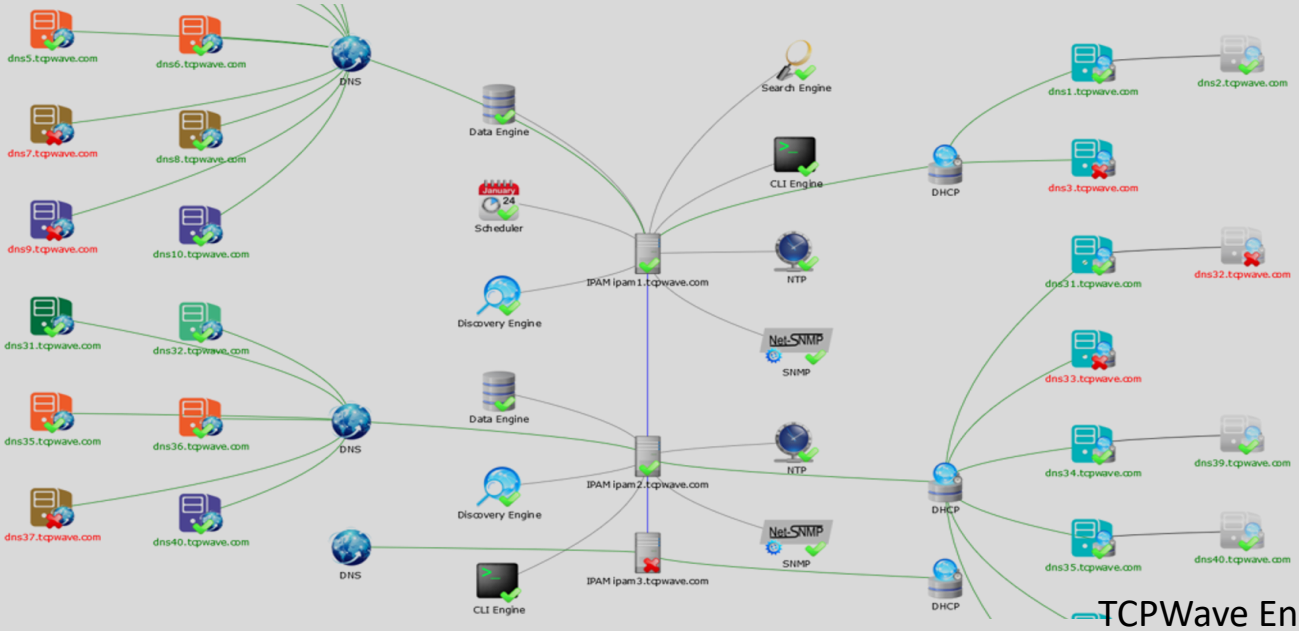
TCPWave IPAM is a highly scalable and reliable IP Address Management solution. It ensures strict database and configuration integrity checks. The solution is built with high availability and disaster recovery management to ensure the continuity of business critical services. The N >2 database configuration allows many IPAM servers to be all active and synchronized in real time.

Example “All Active” IPAM HA configuration with three (3) IPAM Servers

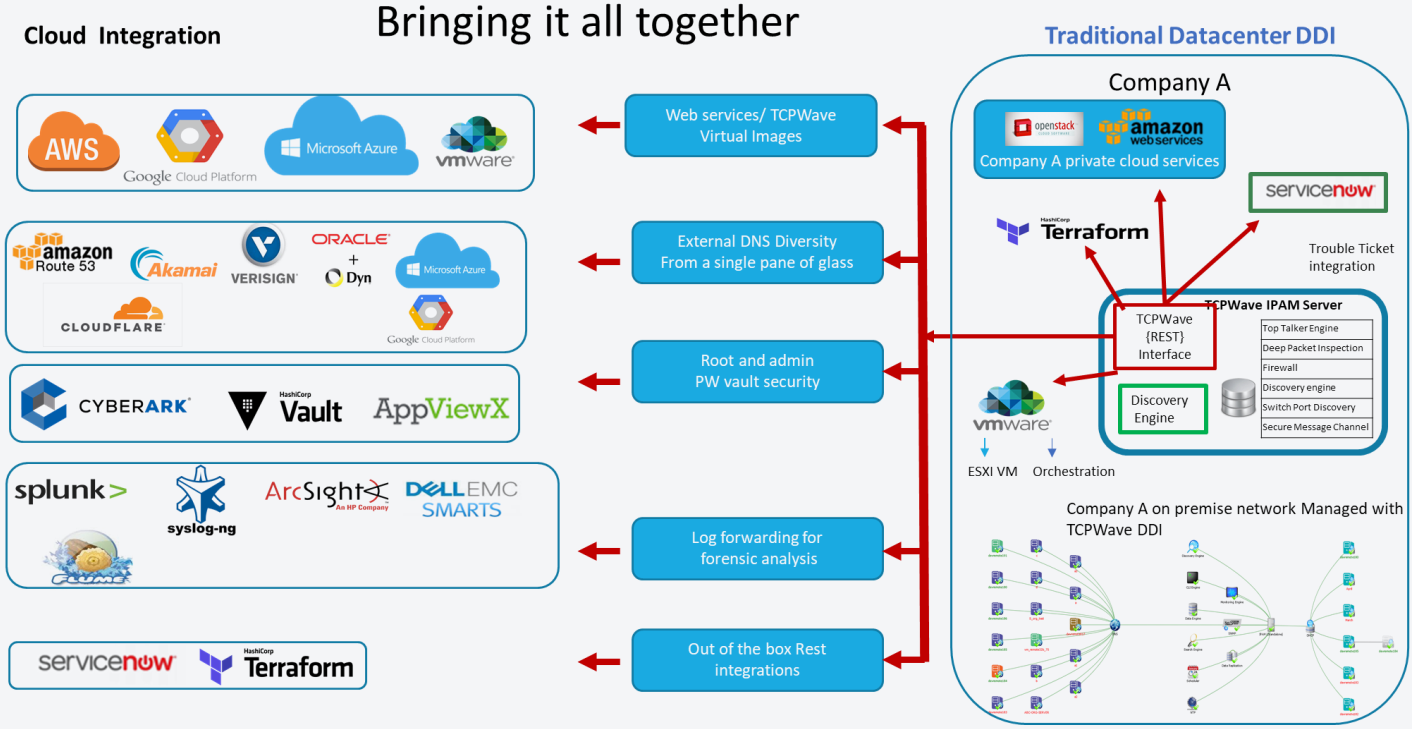


DDI Topology

Topology of all DNS, DHCP, IPAM servers and important services are displayed in the IPAM GUI. If a server or service is down, the name will be red. If the server or service is up, it will be green.



Bringing it all together



As an innovator in Cloud-related services, TCPWave provides state-of-the-art public and private Cloud visibility and operations for DNS, DHCP and IP Address Management (DDI), apart from traditional on-premise DDI services. The company's advanced REST API endpoints for managing its breakthrough services like Dual DNS, IPv4, IPv6, public Cloud extensions, etc., are revolutionizing the way enterprises are automating forward into the future of public Clouds. To learn how TCPWave and its team of Cloud experts are helping enterprises in their Cloud endeavors, visit www.tcpwave.com

Contact Sales at TCPWave.com

TCPWave
World Headquarters
600 Alexander Road
Princeton, NJ 08540 USA