Enhancing hybrid workplace environments with DDI Central

Introduction

A hybrid workplace, which enables employees to connect with the organization's network from anywhere, has become a new trend and demand among current employees. A survey conducted by HubSpot in December 2022 states that 63.4% employees' work preference in 2023 was at home, 8.3% in-office, and 28.3% prefer a combination of the both.

Hybrid work provides the flexibility of when, where, and how they work to employees and the ability to change their work environment based on their preferences. According to an article published by Forbes on Gartner's 2020 survey, when an organization with a 40-hour work week moved to a hybrid environment, the percentage of higher performers increased from 36% to 55%.

The demand of a hybrid workplace pushes many IT organizations to spend on the cloud and other SaaS applications to increase productivity and security. They are in need of a platform for securing the network and unified management across the cloud and branches in order to support the hybrid workplace.

Challenges faced by organizations over setting up hybrid workplace

The idea of transforming from edge to cloud architecture can bring in security and privacy concerns for many organizations. Some of the major challenges faced by organizations are:

DNS, DHCP and IPAM challenges:

DNS:

- Provide a fast and reliable DNS response for employees to access an organization's network resources from remote devices.

- Manage DNS configurations and updates for changing network environments and remote access.

- Securing DNS servers from attacks like DNS spoofing and DNS cache poisoning.

DHCP:

- Configure DHCP server for dynamic IP allocation for IP address availability and better connectivity.

- Coordinate DHCP leases to prevent IP address conflicts and devices not get IP assigned.

- Support remote DHCP functionality to allow employees access IP from their remote location.

IPAM:

- Track and manage IP address allocations across hybrid environment for efficient use of IP resources.

- Enable IT admins to make different network planning for supporting in-office and remote devices.

- Unified view and management of network by integrating IPAM solutions with DNS and DHCP servers.

Security challenges:

- Secure the three network systems from unauthorized accesses and threats.

- Monitor, detect, and log reports on network activities for troubleshooting issues

- Implementing DNS Security Extensions (DNSSEC) to protect against DNS related attacks and integrity of DNS responses.

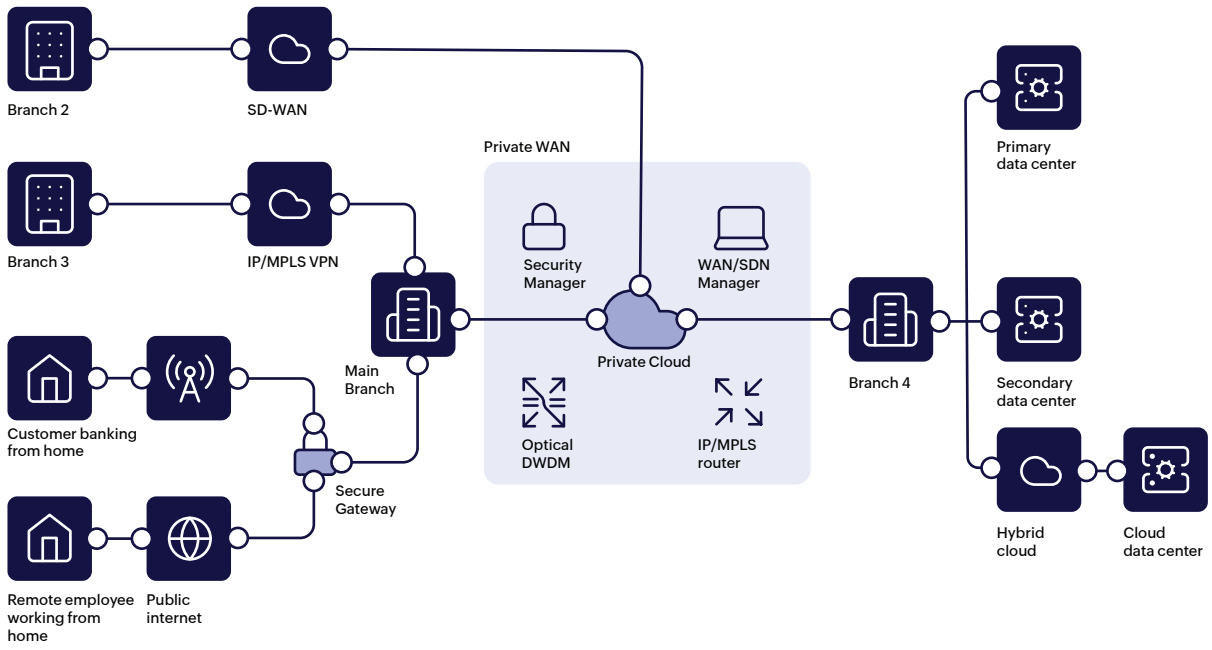
Scalability:

- Handle the increase of devices connecting to the organization's remote hybrid environments.

- Ensure scalability supports network growth and changing environment.

How DDI Central helps in transmitting into the hybrid environment?

DDI Central has several functionalities that can help in securing network resources when moving to an hybrid environment. It also ensures only the employees of the organization can access them. Some of the features in DDI Central are:



Response policy zone: DDI Central allows you to modify your organization's DNS response with the help of response policy zone (RPZ). Administrators can implement custom security policies in DNS Firewall using RPZs, such as blocking unauthorized, malicious domains, redirecting domains to safer page when the query doesn't match the security policies.

These features play a crucial role in securing the organization's network in hybrid workplace environments and protecting both in-office and remote employees from external attacks.

Response rate limiting: Response rate limiting (RRL) protects the DNS server and prevents it from crashing or sending a DNS response to unauthorized queries. When multiple DNS query requests bombards onto the server, RRL steps in and reduces the number of queries entering into the server. This restricts the number of DNS responses for those queries.

RRL prevents DNS server from the potential of abuse and leakage of organization's network data by limiting the response rate, which also helps to load balancing the DNS server. This ensures proper network security and stability alongside server protection for hybrid environments where remote employees need reliable DNS services.

Network segmentation through scopes: Network segmentation is the process of breaking down a larger network into smaller, interconnected subnets and scopes. Both operate individually, which helps in streamlining service, reducing network traffic, and limiting the potential of network breaching.

Network segment helps in hiding critical and sensitive data of the organization into different scopes, protecting them from potential threats. Administrators, or people with role-based access, can access these resources in specific parts of the network, preventing unauthorized ones from getting access. This is important for hybrid environments as external users shouldn't access the organization's network.

DHCP Leases for static and dynamic IP allocations: DHCP leases is the renewal of IP address assigning to the clients after a certain time session, such as 24 hours, to prevent IP exhaustion and network delay. DHCP lease is helpful for hybrid environments as devices of both in-office and remote location needs continuous dynamic IP allocation and renewal for efficient IP resource usage. Also, devices like printers and CCTV cameras need static IPs to be assigned as they need to be consistently connected with the network.

Policy driven automation: Policy driven automation uses predefined policies to automate and manage network services of an organization. They define how DNS responses, IP allocation, renewal, query analytics should be monitored, managed, and executed.

In a hybrid environment, policy driven automation ensures that devices of both inoffice and remote location, follows the security policies. They can automate the administration of role-based access to the network resources for remote employees. Policies can also be set to identify and troubleshoot security threats, such as updating firewall rules, deploying patches, and isolating compromised devices, automatically.

Usecases on how DDI Central can solve real life hybrid workplace challenges

Let's take an IT organization handling the three network services in individual consoles has decided to move to the hybrid workplace environment. Administrating each service separately causes data silos for the admin team.

They are now looking for,

- A centralized platform for managing all three services in one place
- Providing holistic view on the insights of DNS queries, DNS zones, IP allocation and renewal, lease history, and etc.

They decided to choose DDI Central which provides unified management of the core network services, a better analytical view for administrators over the insights of various network tasks, and helps them create better network planning. These factors play a crucial role for them when transferring to a hybrid workplace, where network admins need to assign IPs for both in-office and remote employees using policy driven automation with DHCP fingerprinting, thus preventing external users entering the network.

DDI Central's DHCP scope manager benefits network administrators in managing network efficiently by enabling them make IP address plans and set up security policies for dynamically changing environments, especially for hybrid workplace.

Plus, automating dynamic assigning and renewal of IPs benefits the organization on delivering streamlined network services for their employees in remote location without any outages.

Monitoring DNS and DHCP activities across clusters with the insights given by DDI Central boosts up troubleshooting network breaches, attacks and threats, resulting in a secured network infrastructure with protected network resources that only their employees can access from both in-office and remote locations.

What competitors have? What do we have?

Competitors like Infoblox NIOS DDI, EfficientIP SOLIDserver DDI, Bluecat Integrity [DDI], provide centralized DDI service in the form of hardware appliances with consistent hardware upgrades. They support both on-premise and cloud and help in managing complex network infrastructures like hybrid, multi-cloud, etc.

These companies implement end-of-life policies for their appliances, creating dependencies among the customers for continuous purchase and upgrades, which serves as a disadvantage as large investment is required to be done on first installation and throughout the upgrades.

When it comes to DDI Central, we provide DDI management as a software, working as an overlay on the DNS and DHCP clusters that implements ISC BIND9 and ISC DHCP open source services.

Our software is suitable for businesses of all sizes and budget friendly for smaller enterprises, which is one good advantage amongst the competitors.

Conclusion

DDI Central is a comprehensive full-stack DDI solution designed to simplify network administration and enhance security in hybrid workplace environments. It offers consistent monitoring of DNS and DHCP operations, effectively detecting malicious intrusions from unauthorized external users.

DDI Central ensures seamless management of a large number of devices connecting to the network, providing control over organizational network resources and granting access only to authorized employees.

These features collectively benefit organizations in terms of scalability, reliability, and security. DDI Central marks the start for you digital transformation towards hybrid workplace and ensures your employees work safely from both in-office and remote location in an secured network infrastructure.

DDI Central will be a great choice for you to invest in a centralized platform for network service administration and securing network resources of your organization.