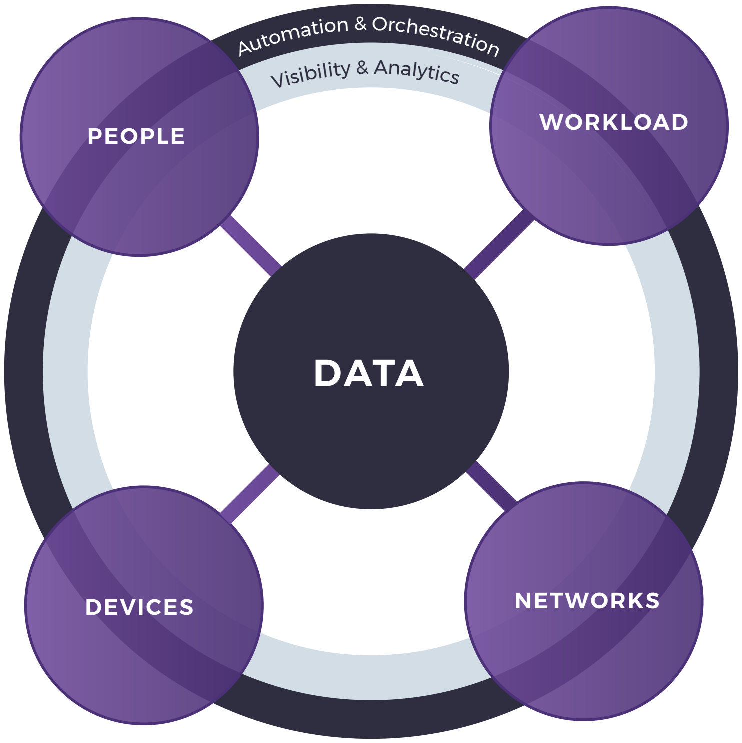
WHITE PAPER

Enabling Zero Trust Security with NS1

NS1.

NS1.COM
05-20

John Kindervag, during his tenure as a vice president and principal analyst for Forrester Research, proposed the zero trust framework as a more rigorous approach to implementing security than the prevalent "trust but verify" methodologies. Zero Trust is based on the assumption that threats can arise anywhere, inside or outside the network, and that every component of the network where data, assets, applications and services reside must be validated and secured. The framework also prescribes that organizations adopt automation, orchestration and visibility to ensure that configurations and policies are applied consistently and in a timely manner across the environment while minimizing the scope for human error.



Since its publication over a decade ago, the zero trust framework has found broad adoption especially in the light of an evolving threat landscape and increasing complexity of enterprise networks. Organizations adopting zero trust principles must extend the framework to all parts of their infrastructure for it to be truly effective.

DNS, DHCP and IPAM (DDI) are critical components of any network. As a result they also form a part of the attack surface and should be considered as part of the overall security posture. NS1's modern Enterprise DDI and DNS solutions play a key role in enabling zero trust architectures for application and access networking infrastructures:

> Zero Trust is based on the assumption that threats can arise anywhere, inside or outside the network, and that every component of the network where data, assets, applications and services reside must be validated and secured.

Automation and orchestration

NS1's software defined deployment and API-first management enables network and DevOps teams to automatically orchestrate and manage their DNS and DDI deployments as part of their overall application and network infrastructure. NS1 solutions integrate with Infrastructure-as-code tools like Terraform and Ansible, workflow automation tools like ServiceNow and our API's support automation of routine tasks such as:

- Creation of networks by configuring IP ranges and managing IP allocations.
- Creation and management of DNS zones and records
- Automatically assign IPs to new devices by managing DHCP scopes, scope groups, leases, and IP reservations for new devices (e.g. printers, VoIP phones, etc.)

This provides a number of security and operational benefits including:

Elimination of manual errors

Using infrastructure as code standardizes procedures resulting in a repeatable, consistent configuration. Standardization puts an end to 'it worked in my environment' or 'it worked on my machine'. Configuration drifts across different environments can be minimized, thus preventing human error.

Version control

Configuration of network services can be version controlled which serves as a form of documentation. It's easy to track the network or infrastructure changes to DNS. It's also easy to rollback to a known 'golden' state in case there are any issues.

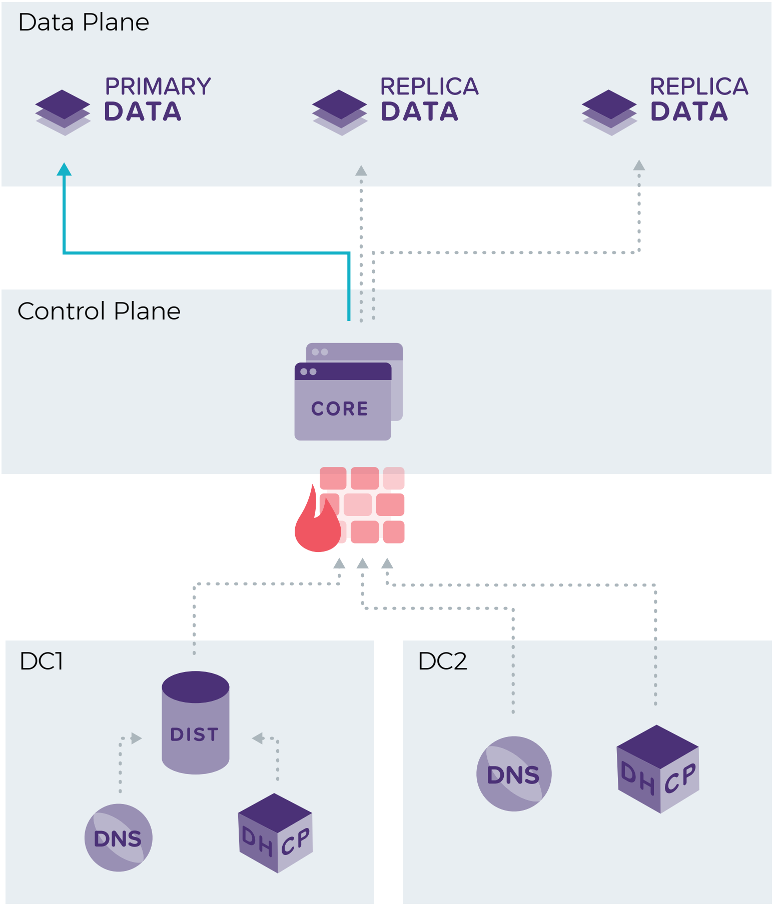
Efficiency and speed

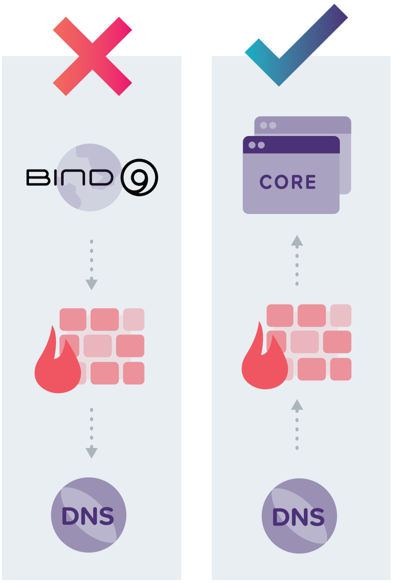
Automation enables network administration across large-scale, distributed systems.NS1's APIs are 10x faster than legacy solutions. High-performance APIs minimize downtime and poor performance of applications as changes to infrastructure that inform traffic steering and DNS responses can be propagated instantly, reflecting real-time infrastructure conditions. Metadata updates such as availability/latency of web servers or load balancers can be executed in real-time improving application performance and reliability.

Data Security and Access Control

NS1 DDI provides a variety of controls for granular, roles-based delegation for managing who has access to which zones (RBAC), records, or record types as well as strong sign-on procedures and activity logging.

NS1's DDI data architecture also adheres to zero trust principles. Rather than the core control plane initiating an outbound connection with each of the DNS & DHCP servers like traditional DDI technologies, the DNS & DHCP servers adhere to a subscriber model wherein they establish a connection to the core container and listen for updates. This improves the scalability of the platform and avoids unnecessary pin-holes on internal firewalls.



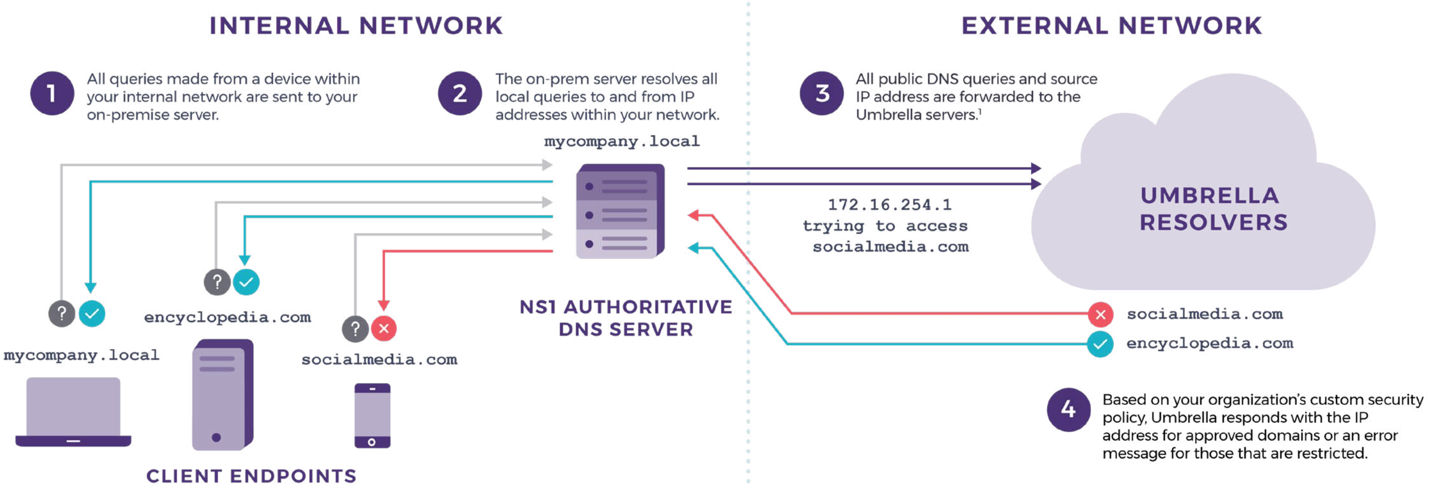


Visibility, Validation and Response

NS1's Enterprise DDI seamlessly integrates with Cisco Umbrella to provide an end to end solution to inspect and validate outbound requests. When NS1 Enterprise DDI and Cisco Umbrella are deployed together, NS1 Enterprise DDI serves as the authoritative DNS server for all traffic internal to the network behind the firewall. It forwards all outbound DNS requests along with client identity information to Umbrella, which in turn acts as the recursive DNS responder for all external domains. This allows Umbrella to apply security policies to protect the user from known malicious threats. The integration allows users to get the best of intelligent DNS traffic steering behind the firewall while protecting outbound queries with Umbrella resulting in performant, secure, and resilient DNS internally and externally. Increased visibility into client identity also enables response automation and reduces mean time to remediate (MTTR).

Webpage
NS1 + Cisco

Blog
NS1 Enterprise DDI and Cisco Umbrella



1 All queries made from a device within your internal network are sent to your on-premise server.

2 The on-prem server resolves all local queries to and from IP addresses within your network.

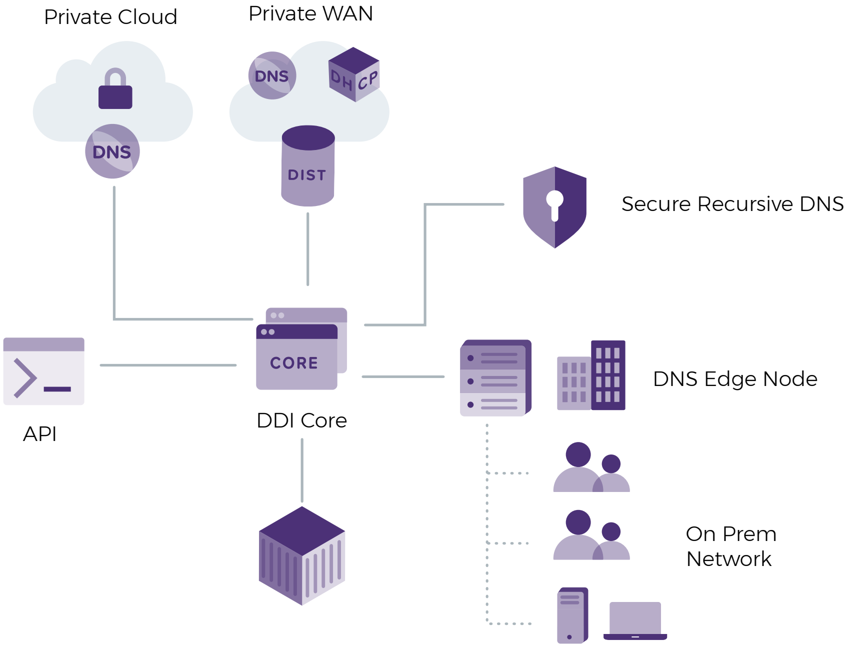
3 All public DNS queries and source IP address are forwarded to the Umbrella servers.[1]

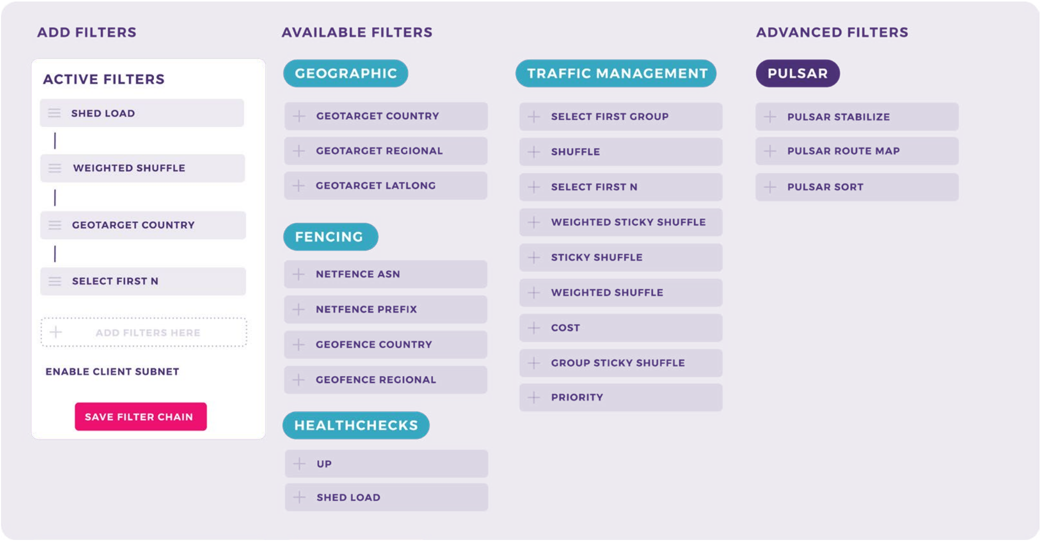
4 Based on your organization's custom security policy, Umbrella responds with the IP address for approved domains or an error message for those that are restricted.

Additionally, NS1 solutions integrate with a variety of authentication tools (such as Okta), monitoring solutions (such as AWS Cloudwatch, Datadog and Catchpoint), and workflow automation tools (such as Slack, ServiceNow, Pager Duty) to provide security and IR teams better control and insights into network activity.

Segmentation

For distributed networks and edge devices, NS1's software defined deployment enables infrastructure teams to deploy DNS and DHCP capabilities closest to the users and devices that need it. NS1's modern DHCP and IPAM capabilities make it easy to create policies for internal segmentation. NS1 Enterprise DDI also provides advanced traffic steering capabilities built on patented Filter Chain technology. This enables traffic to be intelligently routed across network and application partitions.





ADD FILTERS

ACTIVE FILTERS

- SHED LOAD
- WEIGHTED SHUFFLE
- GEOTARGET COUNTRY
- SELECT FIRST N

+ ADD FILTERS HERE

ENABLE CLIENT SUBNET

SAVE FILTER CHAIN

AVAILABLE FILTERS

GEOGRAPHIC

- GEOTARGET COUNTRY
- GEOTARGET REGIONAL
- GEOTARGET LATLONG

FENCING

- NETFENCE ASN
- NETFENCE PREFIX
- GEOFENCE COUNTRY
- GEOFENCE REGIONAL

HEALTHCHECKS

- UP
- SHED LOAD

TRAFFIC MANAGEMENT

- SELECT FIRST GROUP
- SHUFFLE
- SELECT FIRST N
- WEIGHTED STICKY SHUFFLE
- STICKY SHUFFLE
- WEIGHTED SHUFFLE
- COST
- GROUP STICKY SHUFFLE
- PRIORITY

ADVANCED FILTERS

PULSAR

- PULSAR STABILIZE
- PULSAR ROUTE MAP
- PULSAR SORT

Domain Security

In addition to internal DNS, external DNS services are a major part of the attack surface. Given the mission critical nature of DNS, attackers frequently launch volumetric attacks like distributed denial of service (DDoS) and subversion attacks like DNS hijacking to cause business disruption and compromise users. NS1 provides a comprehensive solution for external DNS and traffic management that fully supports modern security postures.

NS1s Managed DNS is a global, over-built, DDoS resilient Anycast network with a strong reliability history backed by a 100% uptime SLA. It can also be deployed as a fully dedicated, single tenant, globally anycasted DNS network dedicated to your zones. This is physically and logically separate from the NS1 Managed DNS network and provides all the benefits including single pane of glass management and support for full traffic management while delivering DNS redundancy without the complexity and risk of multiple providers. In addition, it also enables easy implementation of DNSSEC through a point and click interface or API implementation along wth full traffic management for your signed zones. Just like the DDI solution, NS1's managed DNS gives your teams visibility into DNS usage that can provide insight into potential misuse by external actors. This includes record-level reporting, integrations with monitoring and reporting systems, visibility into anomalous traffic, and unused records reports, net fencing for the control to prevent your sites from receiving traffic from countries or regions you wish to exclude. Lastly, NS1's internal and external DNS solutions are built on a common platform with a consistent usage model. This simplifies policy management and minimizes administrative overhead.

Datasheet
Managed DNS

Webpage
DNS Security

White Paper
Getting Serious About DNS Security

About NS1

NS1 is the leader in next generation DNS solutions that orchestrate the delivery of the world's most critical internet and enterprise applications. Only NS1's purpose-built platform, which is built on a modern API-first architecture, transforms DNS into an intelligent, efficient and automated system, driving dramatic gains in reliability, resiliency, security and performance of application delivery infrastructure. Many of the highest-trafficked sites and largest global enterprises trust NS1, including Salesforce, LinkedIn, Dropbox, Nielsen, Squarespace, Pandora and The Guardian.