Leveraging the National Cyber Security Centre Protective Domain Name System with iboss cloud

The Protective Domain Name System (PDNS) was created by the National Cyber Security Centre to protect central government departments as well as other public sector organisations across the United Kingdom. The iboss cloud's unique architecture allows the deep content security provided by iboss cloud to be connected to the PDNS service for added protection and to meet government regulations.

Please Note – Use of the Protective Domain Name System is wholly under the control of the NCSC which owns and manages the PDNS service that is intended only for government agencies approved by NCSC. iboss is not affiliated with, or endorsed by, the NCSC. The iboss platform provides the ability to integrate with the PDNS service operated by NCSC only if your organization has been approved by the NCSC to use the PDNS service.

Protective Domain Name System Overview

Protective Domain Name System (PDNS) was built to hamper the use of DNS for malware distribution and operation. It was created by the National Cyber Security Centre (NCSC), and is implemented by Nominet UK. PDNS is a recursive resolver, which means it finds answers to DNS queries. Management of your own domains (authoritative DNS), is done separately to this NCSC service and will not be affected by the adoption of PDNS. It is a free and reliable internet accessible DNS service for the public sector and is one of the NCSC's widely deployed Active Cyber Defence capabilitiesIt has been mandated for use by central government departments by the Cabinet Office. It is also available to other public sector organisations, but subject to approval after submitting an application.

The key benefit is that PDNS prevents access to domains known to be malicious, by simply not resolving them. Preventing access to malware, ransomware, phishing attacks, viruses, malicious sites and spyware at the source makes the network more secure. In addition, PDNS provides organisations that use it with metrics about the health of their networks and gives them NCSC outreach support to resolve any issues. The data from PDNS is also used to inform and support UK government cyber incident response functions in the event of a cyber attack.

Interoperability Challenges with Traditional Cloud based Secure Web Gateways

One of the key requirements for using PDNS is having unique public IP addresses to connect to the service with. The public source IP addresses of an organisation must be registered with the PDNS service before using it. The public source IP addresses are typically the addresses that assigned to the organisation by the Internet Service Provider (ISP) and are used by the organisation to access the Internet. The service uses the source IP address of the clients making DNS requests to allow or deny access to the service which will resolve DNS queries.

Registering an organisation's public IP address with the PDNS service is straight forward when using on-prem Secure Web Gateway proxies. This is because the traffic from the on-prem gateways will exit through the organisation's own network connection which has the source IP addresses registered with the PDNS service. Those IP addresses do not change as all traffic leaving the network from the on-prem gateways will have one of the already registered and allowed addresses for the PDNS service.

When moving to cloud-based security, the Internet traffic source IP address is no longer that of the organisation's, as the traffic leaves the organisation and is forwarded to the cloud security service prior to continuing to the Internet. This is required as the cloud security service provide compliance, malware protection and data loss prevention for traffic as it moves between the organisation and cloud applications. To make things worse, as users move from place to place outside of the organisation's perimeter, their source IP will change depending on whether they are in a coffee shop, an airport or at home. The source IP address will be that of the network which they are accessing the internet from, which would not be registered to the PDNS service and thus not allowed to access its protection.

This poses a challenge for PDNS as the service requires non-changing, registered IP addresses at all times to allow access to the security it provides.

iboss is the only cloud based Secure Web Gateway that provides each customer with a unique and statically defined IP address. This is possible with iboss as the cloud is based upon a containerized architecture vs the shared architecture used by other providers. This also ensures data sovereignty and compliance with regulations such as GDPR.

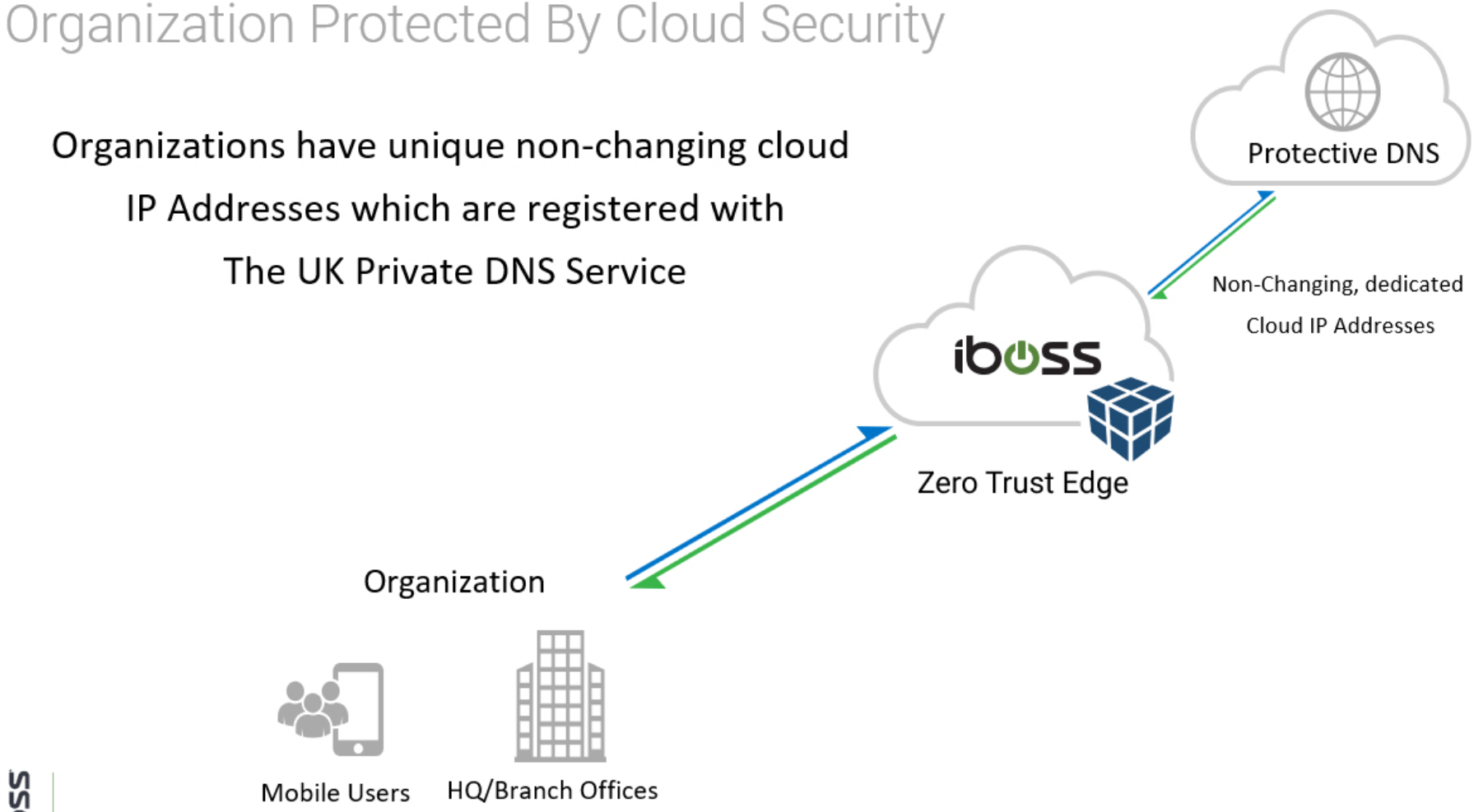
Using PDNS with Cloud Security

With the challenges that changing IP addresses pose to PDNS and the conflict that has with mobility and cloud security, it may appear that using PDNS with cloud security is not an option. Fortunately, the iboss cloud solves this challenge by providing unique and dedicated IP addresses that follow the user, regardless of what location that user is accessing cloud applications from. The reason this is possible is that the iboss cloud is built on the concept of containerization which allows IP addresses to remain unchanged and assigned to an organisation globally. As traffic originates from iboss cloud security, the PDNS service will recognize the IP addresses as belonging to a specific, registered organisation. This allows PDNS to provide an additional layer of protection on top of the deep content, packet and DNS protection provided by iboss cloud.

Architectural Overview

Organization Protected By Cloud Security

Organizations have unique non-changing cloud IP Addresses which are registered with The UK Private DNS Service



Extend Protection by Layering in Protective DNS on Top of the iboss Platform

Integrating with the protective DNS service will apply an additional layer of security on top of the already extensive malware engines and feeds within the iboss cloud platform. Enabling Protective DNS is possible due to the containerized architecture of the iboss cloud platform which allows for dedicated, unique cloud IP addresses which are required by the Protective DNS service.

How It Works

Taking advantage of the Protective DNS service with iboss cloud is easy. To get started:

1. Get an active iboss cloud account.
2. Connect users to the iboss cloud using one of the many cloud connectors. This connects users to iboss cloud regardless of location.
3. Go the Protective DNS information site to register for an account – https://www.ncsc.gov.uk/information/pdns
4. Make a request to iboss to have your account connected to the UK Protective DNS service (Verification of eligibility will be performed. Must be a central government body, emergency service, local authority or devolved administration).
5. Your organisation will be protected by the Protective DNS servers regardless of user location.

Pricing

Protective DNS Integration	
The Protective DNS integration feature is available on all iboss cloud subscriptions at no additional cost. Must be a UK government agency or approved public sector organisation.	Contact Us

About iboss

iboss is a cloud security company that provides organisations and their employees secure access to the Internet on any device, from any location, in the cloud. This eliminates the need for traditional security appliances which are ineffective at protecting a cloud-first and mobile world. Leveraging a purpose-built cloud architecture, iboss is designed to make transitioning from security appliances to cloud security a seamless process. iboss is trusted by more than 4000 organisations worldwide, spans over 100 points of presence globally and is backed by over 110 patents.

To learn more, visit https://www.iboss.com