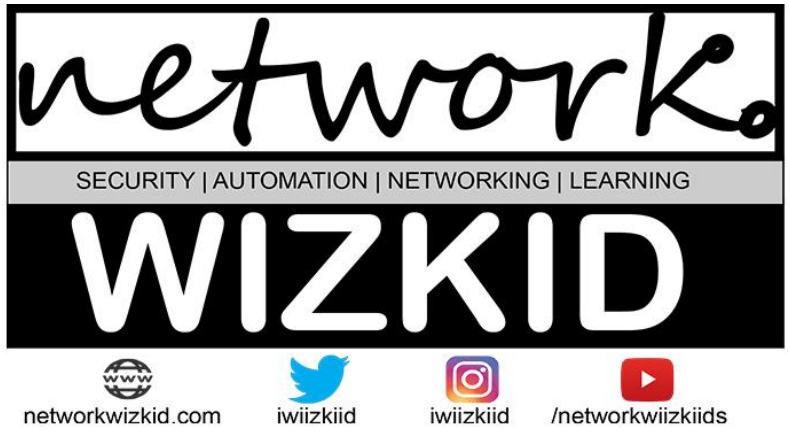
Duo Network Gateway (DNG) – Protecting RDP Servers & a Brief DNS Review

Duo Lab Sessions with Kelvin

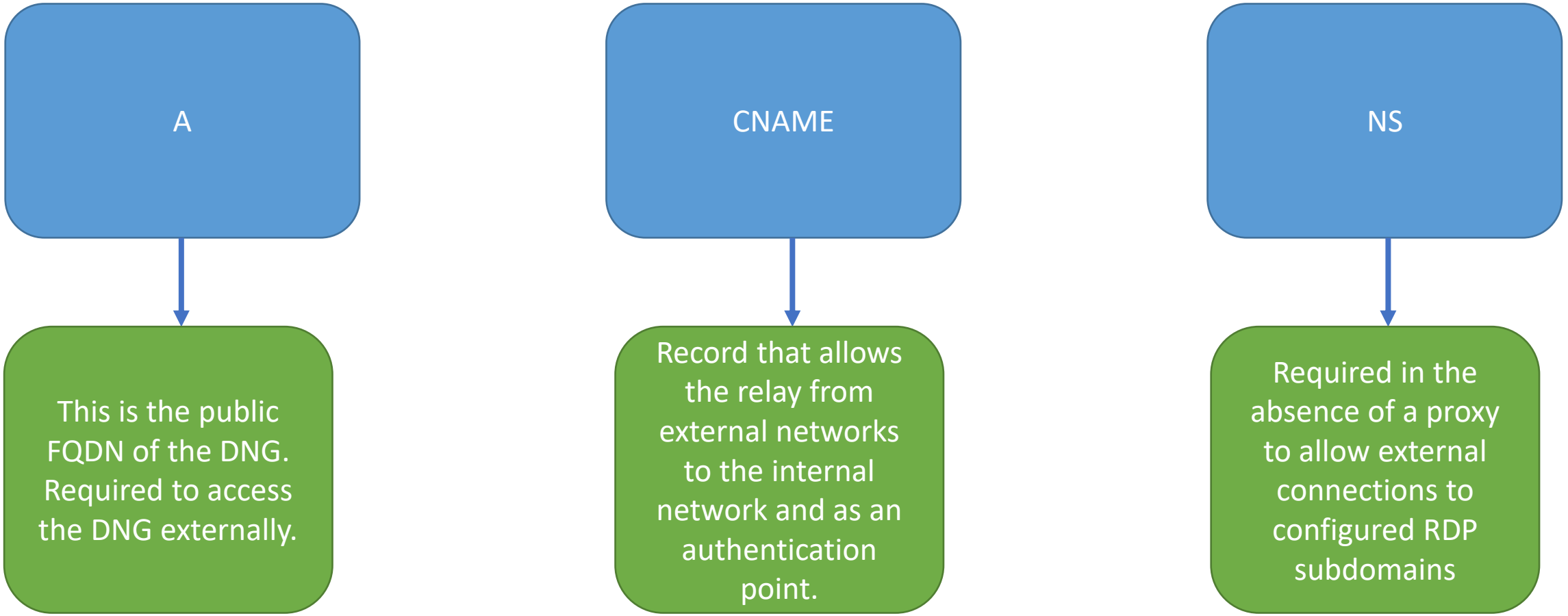
#NetworkWizkids



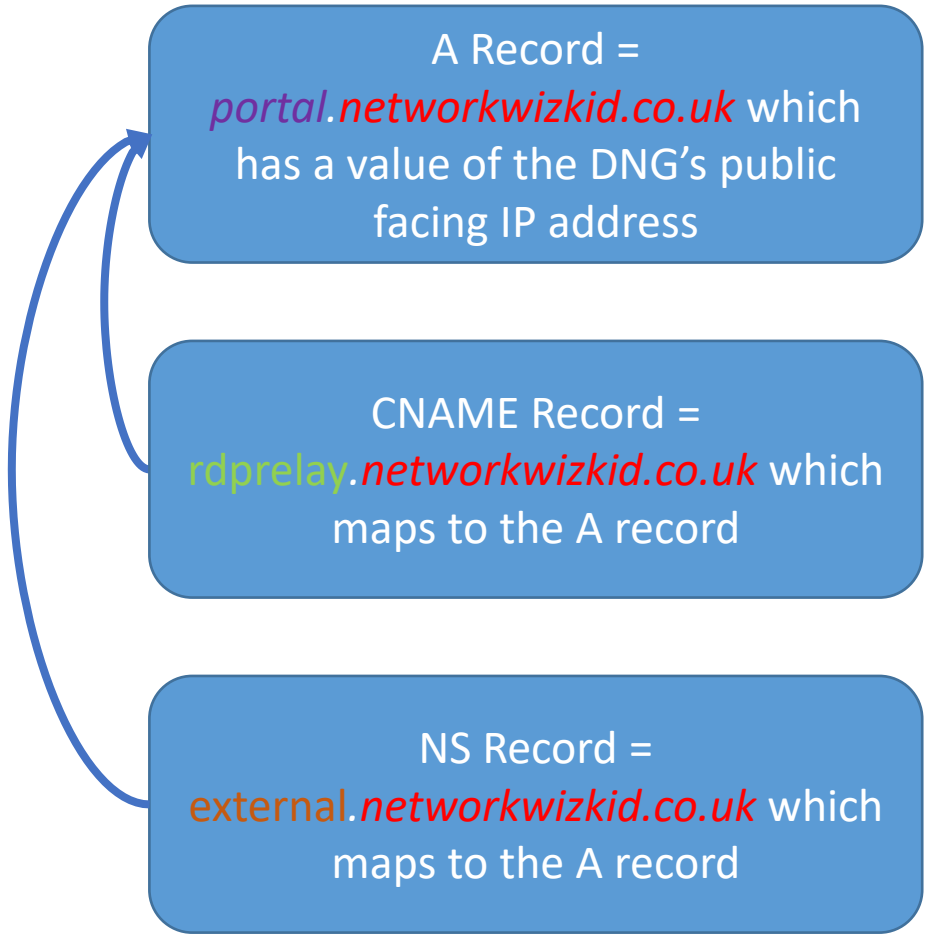
Brief Overview of DNS - A,NS & CNAME Records

Record Type	Description
A	(Address) Maps FQDN to an IPv4 address. In the case of the DNG, the name of the A record will contain the IPv4 address value of the DNG.
NS	(Name Server) Specifies which name server/s are authoritative for the domain and/or subdomain. When a name server is “Authoritative”, it is the name server that hosts the DNS records. Delegation is fundamentally the most important use for a NS record which allows us to delegate part of the domain to other DNS servers. In the case of the DNG, the NS record is used for subdomain delegation. The record created will point to the DNG where there is a correspondence between your external and internal domain.
CNAME	(Canonical Name) Acts as an alias and points to another domain or subdomain. In the case of the DNG, this is used as a relay between the external and internal network and as an authentication point against the application being protected.

DNG DNS Record Types for RDP



DNG DNS Record Types for RDP Example



Key

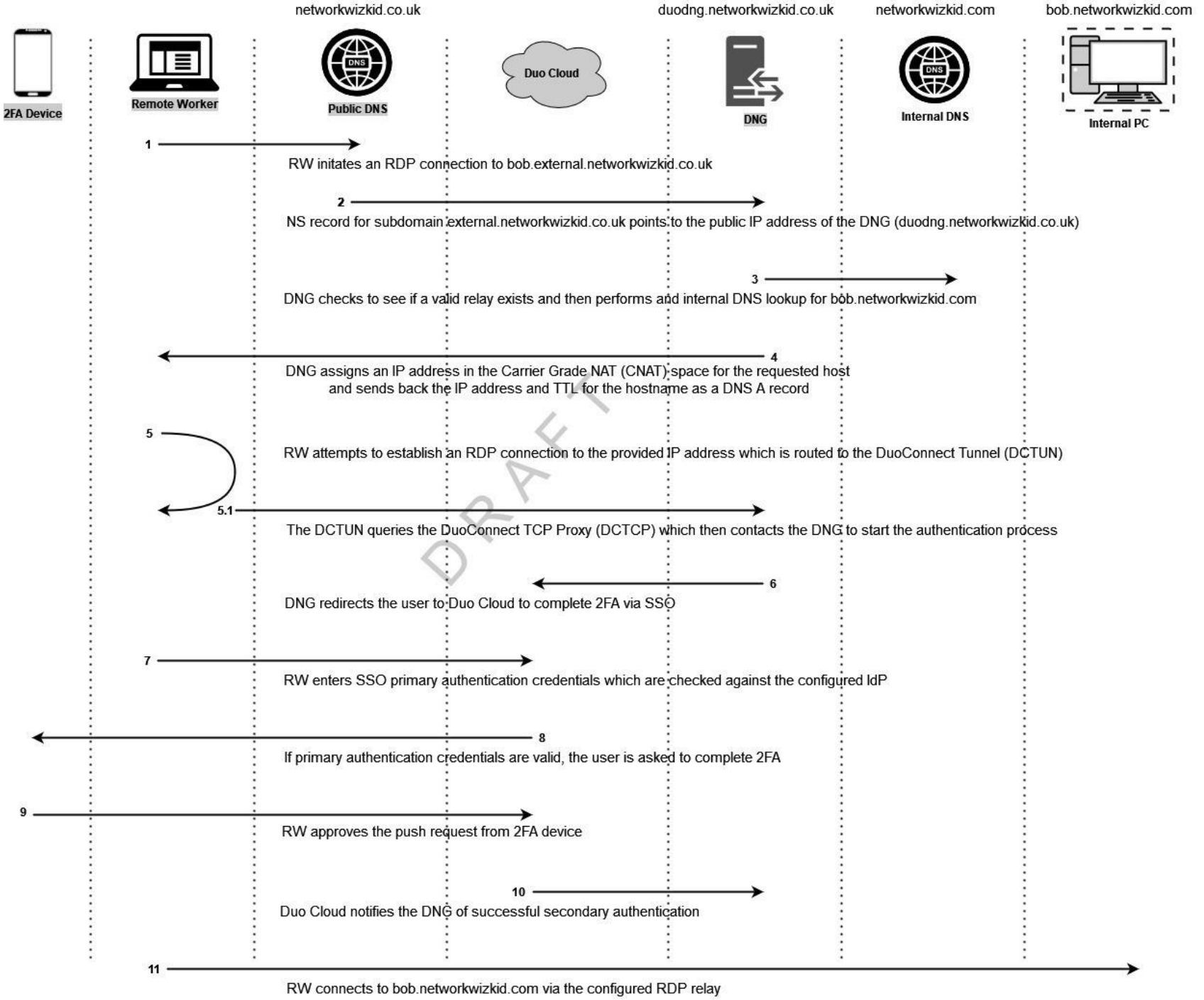
Red: Domain
Purple: DNG name
Green: RDP Auth Relay
Orange: Subdomain

Building on the Duo DNG Documentation

Domains	
Internal Domain	internal.com
Public Domain	external.com

DNS Type	Name	Value	TTL (sec)	Example
A	portal	111.211.222.42	300	portal.external.com will point to the public IP address of your DNG
CNAME	rdp-relay	portal.external.com	300	rdp-relay.external.com is an alias for portal.external.com A CNAME is used to access protected web applications and SSH servers but the user will use the NS record for RDP access.
NS	rdp	portal.external.com	300	Users that want to access an RDP host on internal.com with a hostname of rdphost would have a FQDN of: rdphost.internal.com This is protected by CNAME: rdp-relay.external.com and therefore users would connect using the hostname of the machine followed by the NS record. Example: rdphost.rdp.external.com

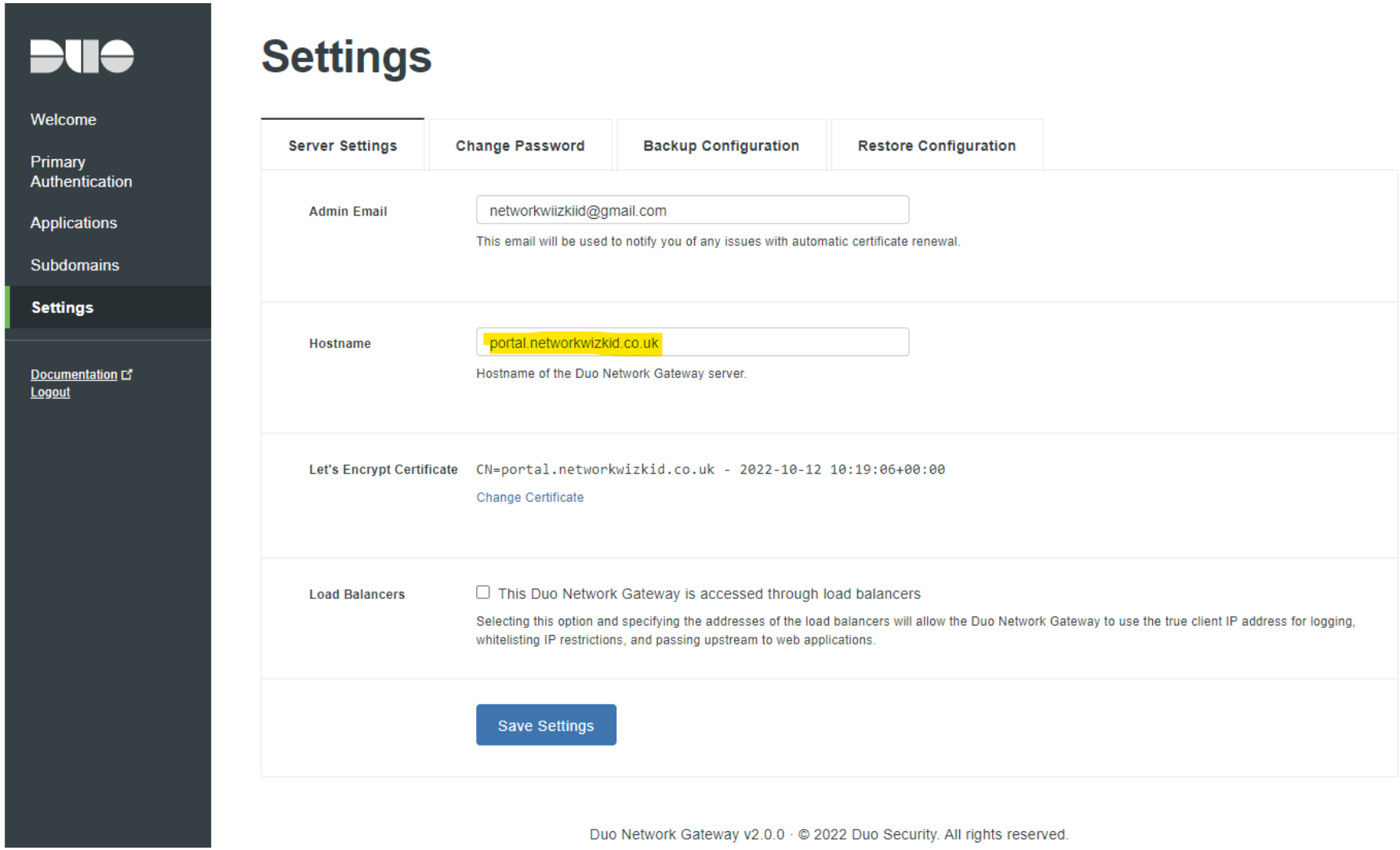
RDP Flow Example



DNG DNS Record Types Locations (A Record)

A

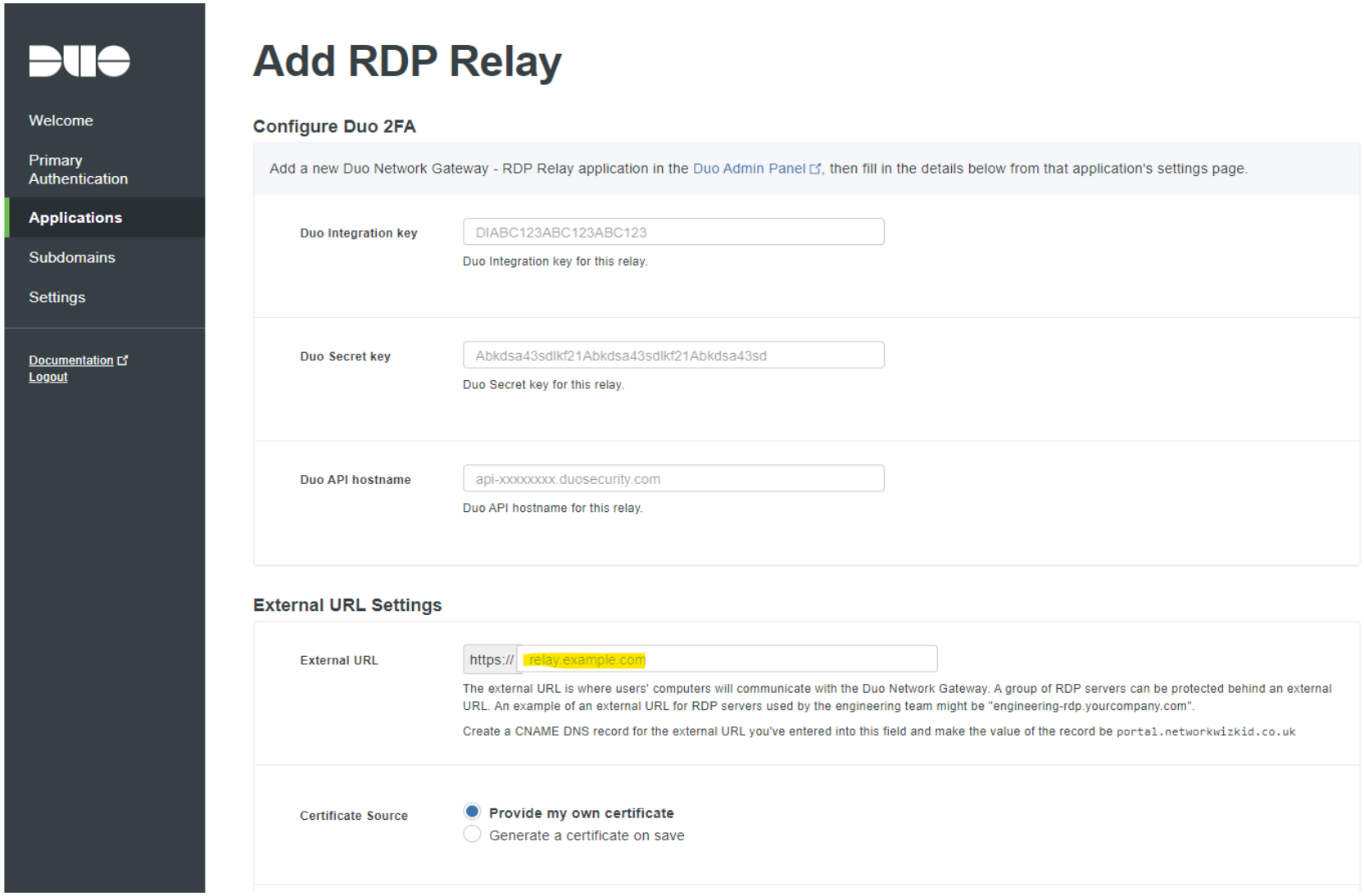
This is the public FQDN of the DNG. Required to access the DNG externally.



DNG DNS Record Types Locations (CNAME Record)

CNAME

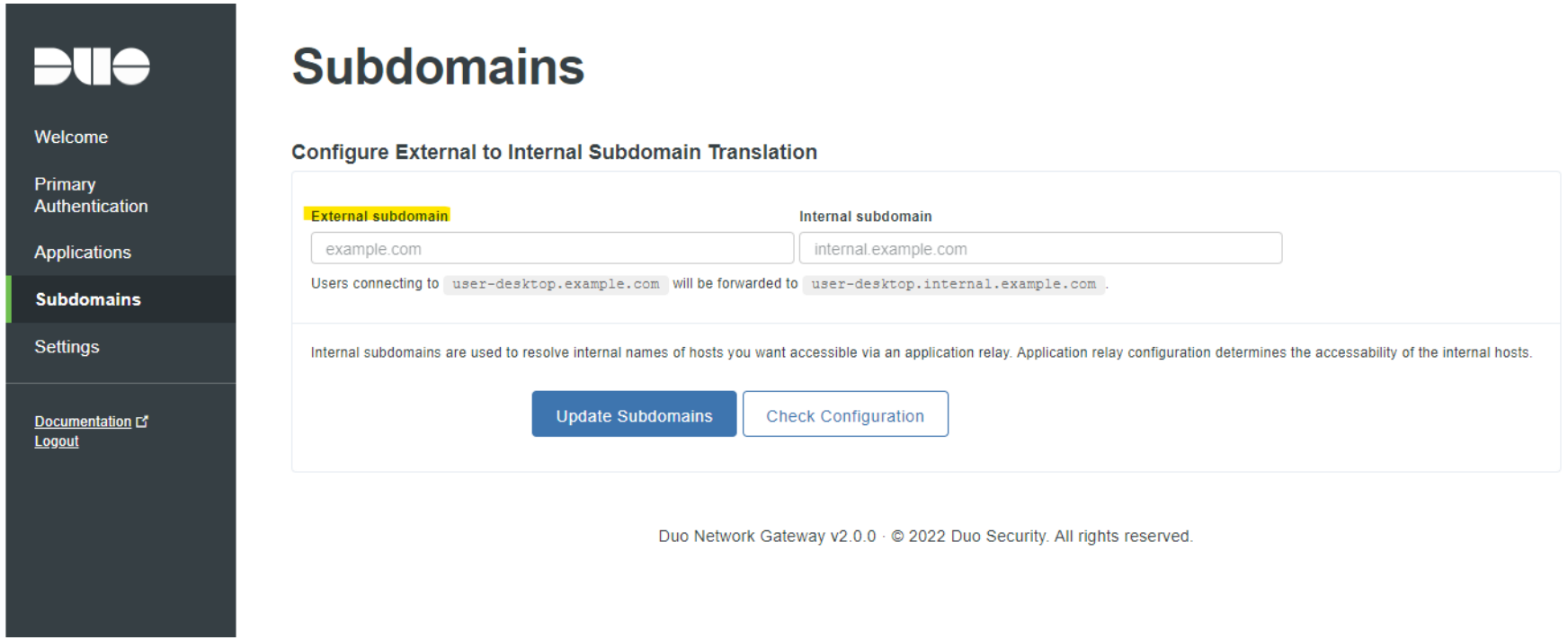
Record that allows the relay from external networks to the internal network and as an authentication point.



DNG DNS Record Types Locations (NS Record)

NS

Required in the absence of a proxy to allow external connections to configured RDP subdomains



Don’t Forget About Firewall Rules

Protocol	Port	Direction	Reason
HTTP (TCP)	80	Bidirectional (DMZ <-> External)	HTTP communication to and from DNG
HTTPS (TCP)	443	Bidirectional (DMZ <-> External)	HTTPS communication to and from DNG
DNS (TCP & UDP) ***(Only for RDP)***	53	Bidirectional (DMZ <->External)	DNS communication to and from DNG
HTTPS (TCP)	8443	Unidirectional (Internal -> DMZ)	Access the DNG for management tasks
RDP (TCP) ***(Only for RDP)***	3389	Unidirectional (DMZ -> Internal)	DNG communication with RDP servers
SSH (TCP) ***(Only for SSH)***	22	Unidirectional (DMZ -> Internal)	DNG communication with SSH servers
HTTP/S	80/443	Unidirectional (DMZ -> Internal)	DNG communication with web applications
Others rules may be required so please assess your environment.			

Prerequisites

- DNG (2.0.0+) installed with initial configuration done
- DNS records in place
- Firewall rules in place
- Certificate requirements

Summary of the Configuration Steps

1. Protect an RDP server via the Duo Admin Panel
2. Configure the DNG for RDP
3. Configure sub-domain on the DNG
4. Download and configure Duo Connect and Duo Device Health
5. Test connectivity to RDP server

Useful Links

- www.youtube.com/networkwiizkiids
- www.networkwizkid.com
- www.twitter.com/iwiizkiid
- https://duo.com/docs/dng
- https://duo.com/docs/sso
- https://duo.com/docs/dng#relays-and-subdomains
- https://www.cloudflare.com/en-gb/learning/dns/dns-records/
- https://duo.com/docs/dng#protect-rdp-servers-with-duo-network-gateway