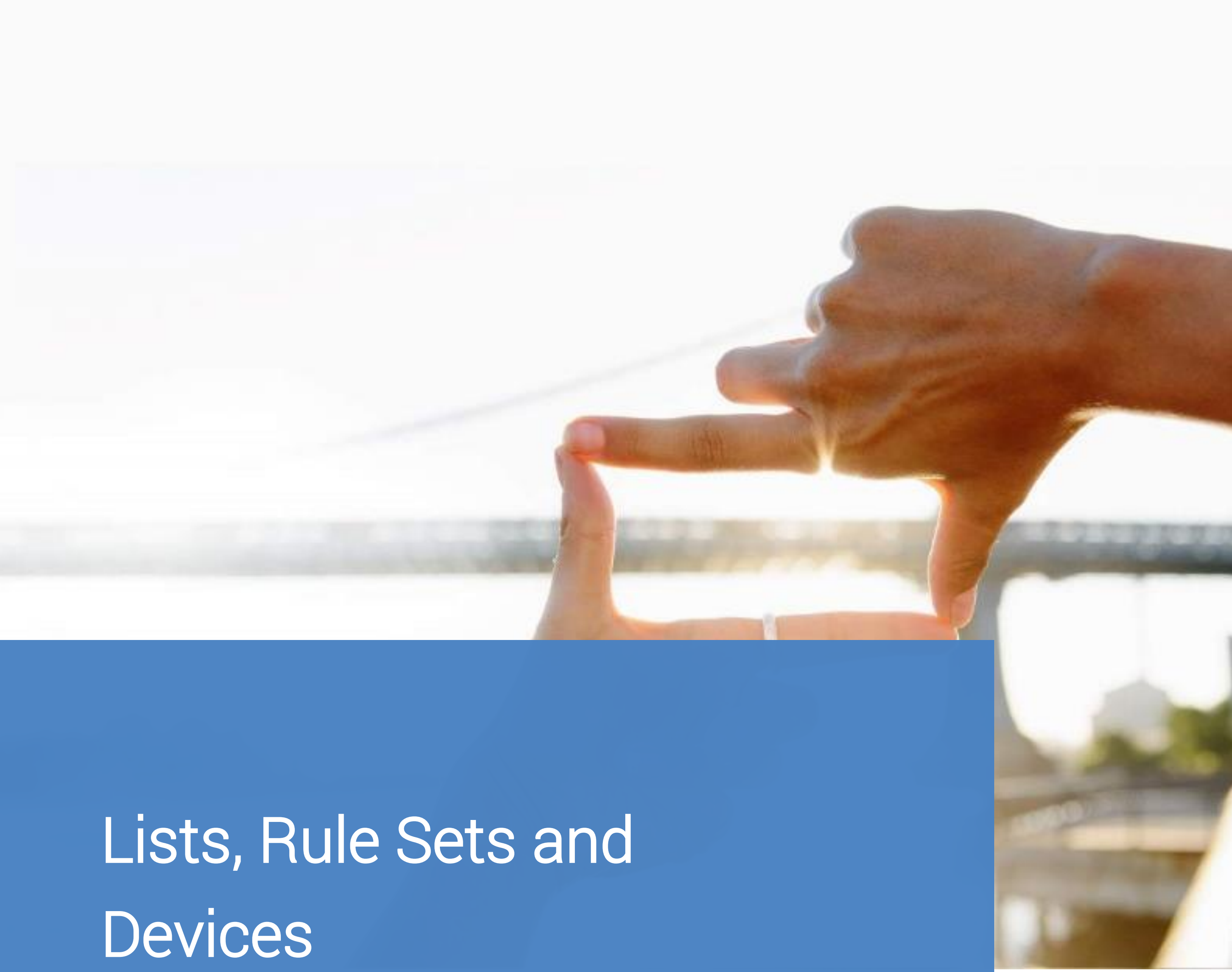
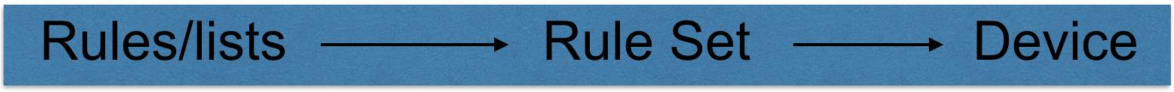


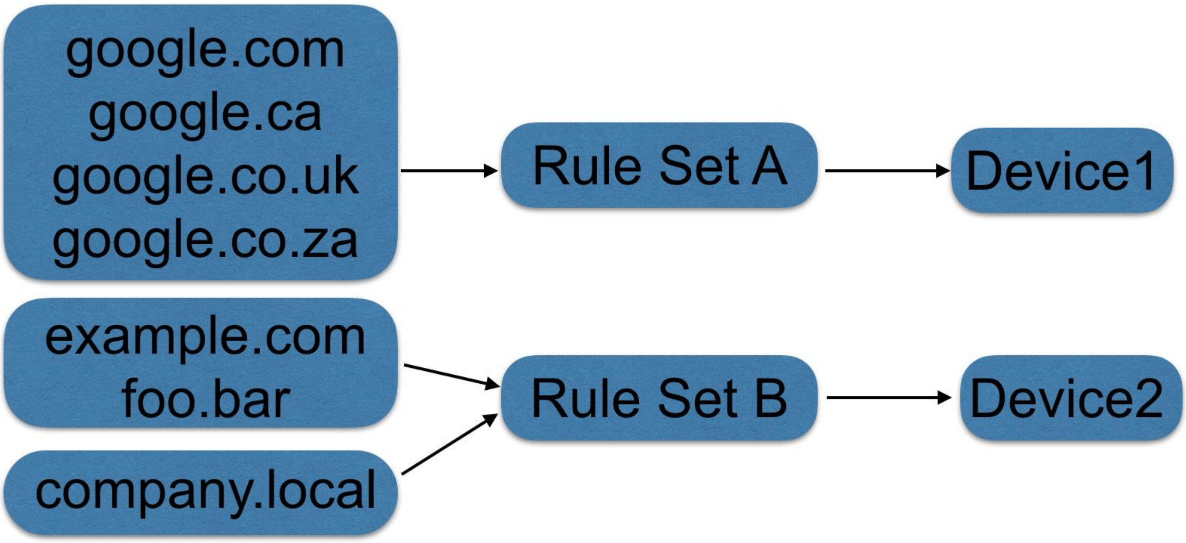
Lists, Rule Sets and Devices

GATEWAY.MANAGEMENT

Introduction

This illustration is designed to show the relationship between Rules (lists), Rule Sets and Devices:





Creating and Managing Rules (or lists)

1. Lists are the basic building block of this software stack. Each line in a list consists of a partially qualified domain name (PQDN) or fully qualified domain name (FQDN). The distinction is in context of how else a given domain name may be used. Furthermore, each list in its entirety is either treated:

   a. To exclude subdomains, or
   b. To include subdomains

As an example of each, consider the following **white list** and the resulting behaviour:

White list entry (**excluding** subdomains):	Consider subdomain	How it would be treated
google.com	www.google.com	**Disallowed** since www is a subdomain of google.com and subdomains are **excluded**
	docs.google.com	**Disallowed** since docs is a subdomain of google.com and subdomains are **excluded**

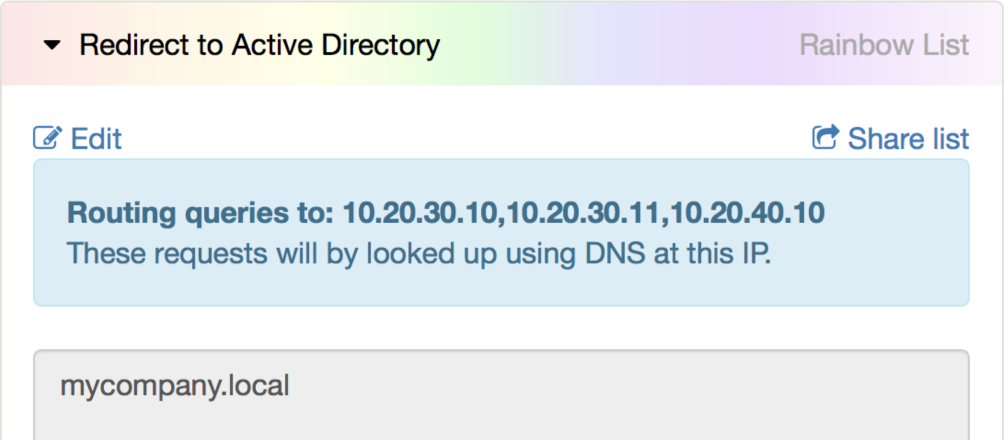
White list entry (**including** subdomains):	Consider subdomain	How it would be treated
google.com	www.google.com	**Allowed** since www is a subdomain of google.com and subdomains are **included**
	docs.google.com	**Allowed** since docs is a subdomain of google.com and subdomains are **included**

2. **White lists**: these apply in a block-all-allow-some methodology. When a Rule Set is based on white lists, that's the only time white lists apply.
   These are **domains** that are **allowed**. (subdomain inclusion/exclusion switch applies)

3. Blacklists: these apply in **all** Rule Sets and override all other lists.
   These are **domains** that are **blocked**.

4. Rainbow lists: these apply in all Rule Sets
   These are **domains** which are to be **re-directed** to other DNS server(s). There are several scenarios when this applies, including:

   a. Internal Active Directory domains where this may apply, for example:
   mycompany.local is authoritative on Active Directory, so it is forwarded like this:

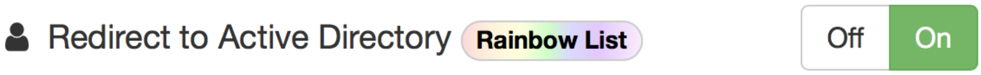


▾ Redirect to Active Directory

Routing queries to: 10.20.30.10,10.20.30.11,10.20.40.10
These requests will by looked up using DNS at this IP.

mycompany.local

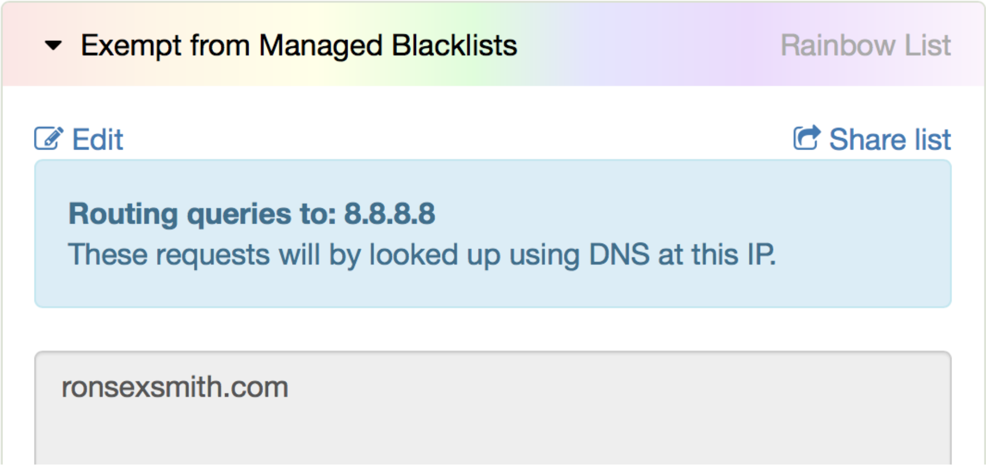
   And then it must be enabled in all applicable Rule Sets as shown here:



Redirect to Active Directory **Rainbow List** Off [✓ On]

   b. When an exception needs to be made within another list, managed or otherwise, without disabling the entire list within a Rule Set. For example, ronsexsmith.com is often mistaken as a domain containing adult content, known as a false positive. In order for ronsexsmith.com to work properly without disabling the entire blacklist it may be a part of, it can be made part of a rainbow list in order to provide an exception like this:

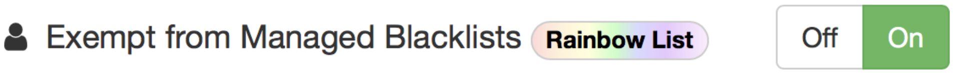
ronsexsmith.com re-directed to 8.8.8.8 for name resolution.
In the User Interface it appears like this first to create the list:



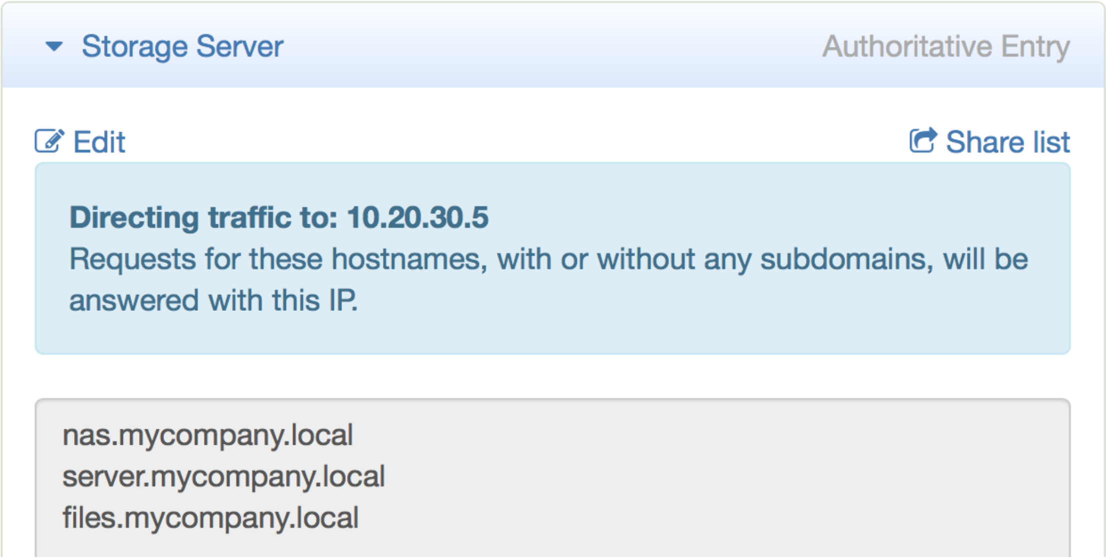
Routing queries to: 8.8.8.8
These requests will by looked up using DNS at this IP.

ronsexsmith.com

And then it must be enabled in all applicable Rule Sets as shown here:



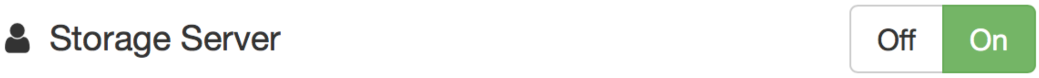
5. Authoritative Lists: for simple IPv4 A records this is list serves to authoritatively resolve hostnames to A record. For example if a NAS device is to be known by FQDNs of nas.mycompany.local as well as server.mycompany.local and files.mycompany.local:



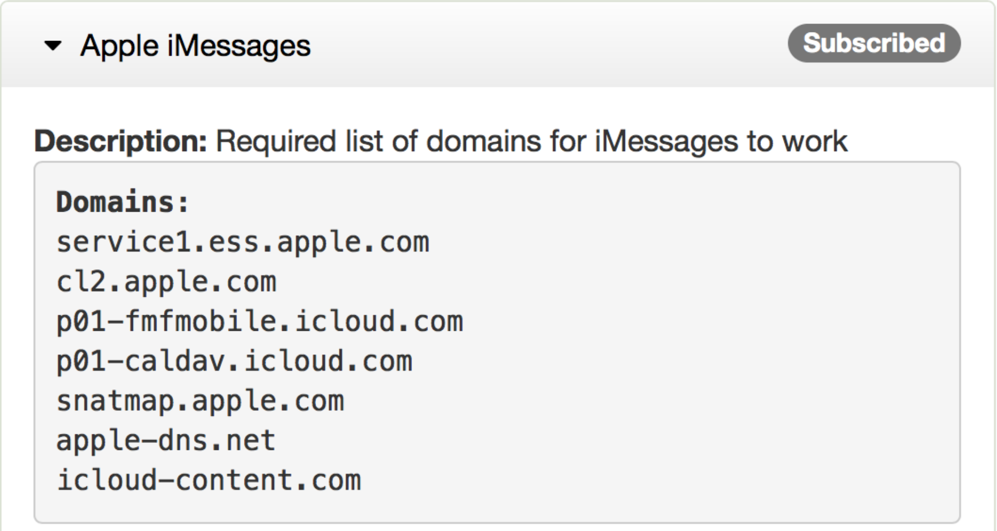
Directing traffic to: 10.20.30.5
Requests for these hostnames, with or without any subdomains, will be answered with this IP.

nas.mycompany.local
server.mycompany.local
files.mycompany.local

And then it must be enabled in all applicable Rule Sets as shown here:



6. Verified White lists (subscriptions): these are collections of domains which are all required for one specific server. For example in order for Apple iMessages to work, the following domains are required and available for automatic enablement:

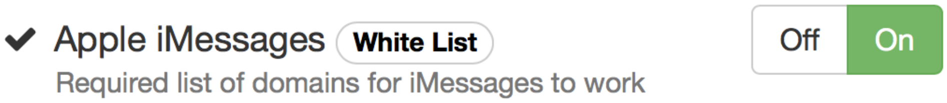


Apple iMessages

Description: Required list of domains for iMessages to work

```
Domains:
service1.ess.apple.com
cl2.apple.com
p01-fmfmobile.icloud.com
p01-caldav.icloud.com
snatmap.apple.com
apple-dns.net
icloud-content.com
```

And then it must be enabled in all applicable Rule Sets as shown here:



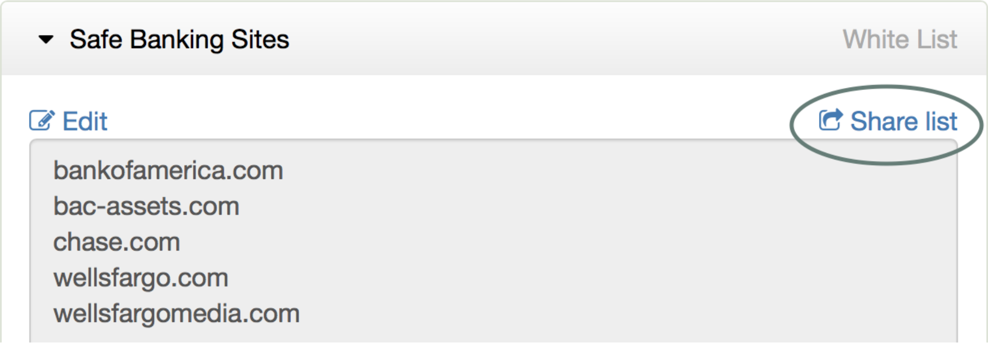
✓ Apple iMessages White List

Required list of domains for iMessages to work

(see later section on Auto-whitelisting for the more common websites/service where the cloud crawler dynamically retrieves dependencies)

7. Sharing White lists: determining required white lists for specific environments may represent careful curation efforts. In order for such lists to be made immediately available to any other site, whether at another account or other locations within the same account, this feature allows for shared lists to immediately propagate to all other shared subscriptions with these simple steps:

   a. Create a rule or list such as this one called “Safe Banking Sites”:

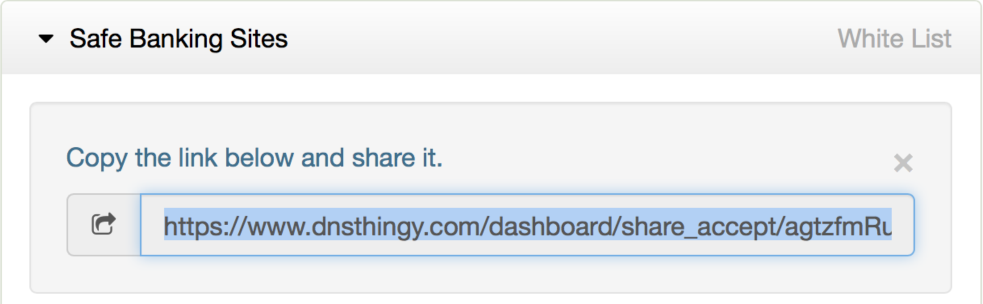


Safe Banking Sites

White List

bankofamerica.com
bac-assets.com
chase.com
wellsfargo.com
wellsfargomedia.com

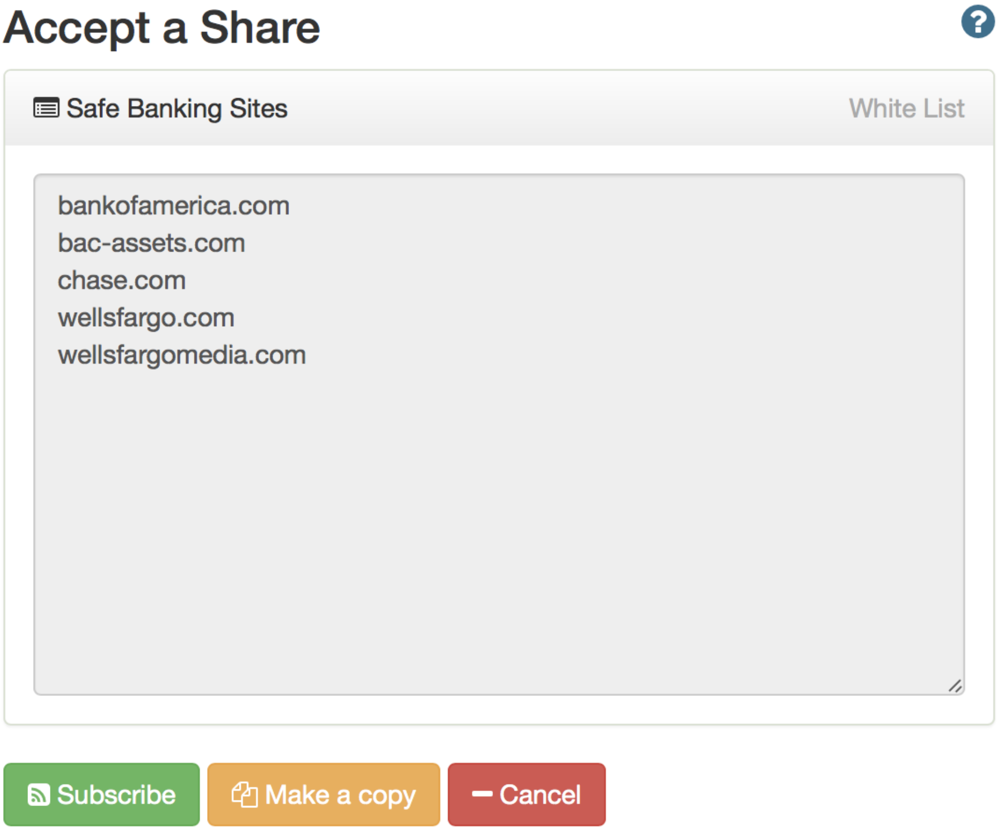
b. Once created, click on “Share list” for the URL to display:



Copy the link below and share it.

https://www.dnsthingy.com/dashboard/share_accept/agtzfmRu

c. The recipient needs only log into their own dashboard and use the shared URL to subscribe, which results in this option:

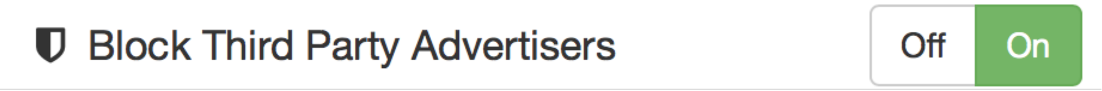


bankofamerica.com
bac-assets.com
chase.com
wellsfargo.com
wellsfargomedia.com

d. **Subscribe** ensures all original list changes are immediately propagated.

e. **Make a copy** makes a one-time copy of the existing list and ignores any original list owner future changes.

8. Managed Lists: some of these are included with every instance of this software stack including the most commonly-used third party ad networks that appears as follow on any Rule Set based on Black lists:



Block Third Party Advertisers

9. Order of Operation: Upon software startup, lists are retrieved from the cloud controller and stored in RAM (memory) on your local gateway/standalone device stack. As soon as a match is found, no further list inspection occurs. The order of list types which are consulted is as follows:

   a. Authoritative
   b. Rainbow
   c. Black
   d. White

Special cases are handled as appropriate as is required for forced SafeSearch (Google and Bing) as well as forced SafetyMode (YouTube).

Not all rules/lists apply to all Rule Sets. Consider this summary of which rule type are applicable to which type of Rule Sets:

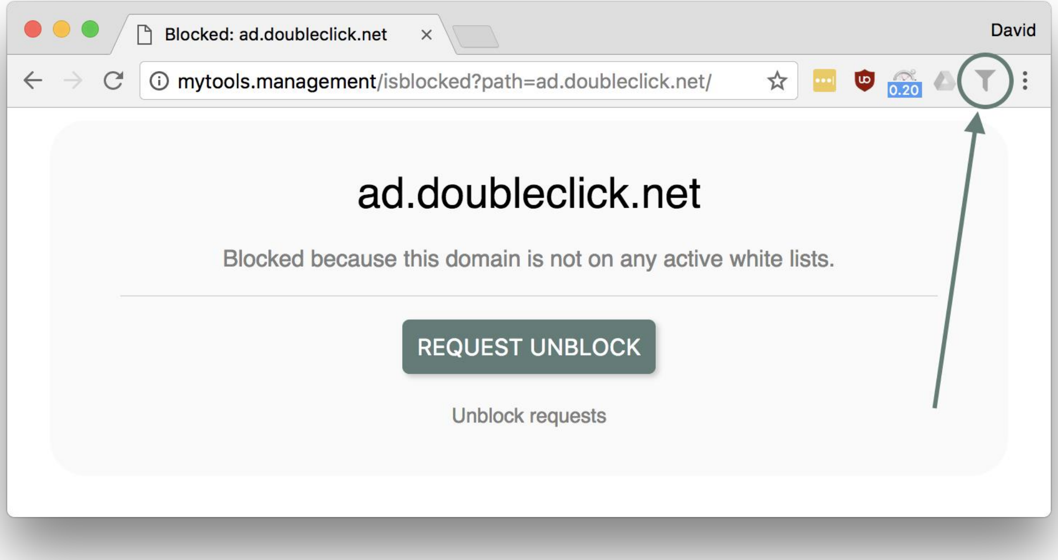
Rule Set based on:	White list Rule Set	Black list Rule Set	Unfiltered Rule Set
White Lists	Yes	Does not apply	Does not apply
White List [Verified] Subscriptions	Yes	Does not apply	Does not apply
Black Lists	Yes	Yes	Does not apply
Rainbow Lists	Yes	Yes	Yes
Authoritative Lists	Yes	Yes	Yes
“Unblock request” feature on block page	*Yes*	*No*	*No*

Public Suffix

In order to avoid leakage to the public Internet of domain queries which are not a valid public suffix, such queries never egress the software stack. The public suffix is updated daily as available from publicsuffix.org.

Blocked domains

Domains which are blocked are **not responded** with NXDOMAIN.
Instead, they are answered with the local, internal private IPv4 address selected during the software stack installation. This is essential in order for the endpoint to be able to presented with a block page when requesting an http resource. https sites are never intercepted with man-in-the-middle techniques, but rather are handled with an extension called "**Block Page Assistant**" which, when used in conjunction with this software stack, gracefully redirects blocked https resources to http://mytools.management/isblocked?blockedsite.com. See here for a real-life example, note the arrow to the extension that achieves this redirection gracefully when accessing https://ad.doubleclick.net for example:



Blocked: ad.doubleclick.net
David
mytools.management/isblocked?path=ad.doubleclick.net/
0.20
REQUEST UNBLOCK
Unblock requests

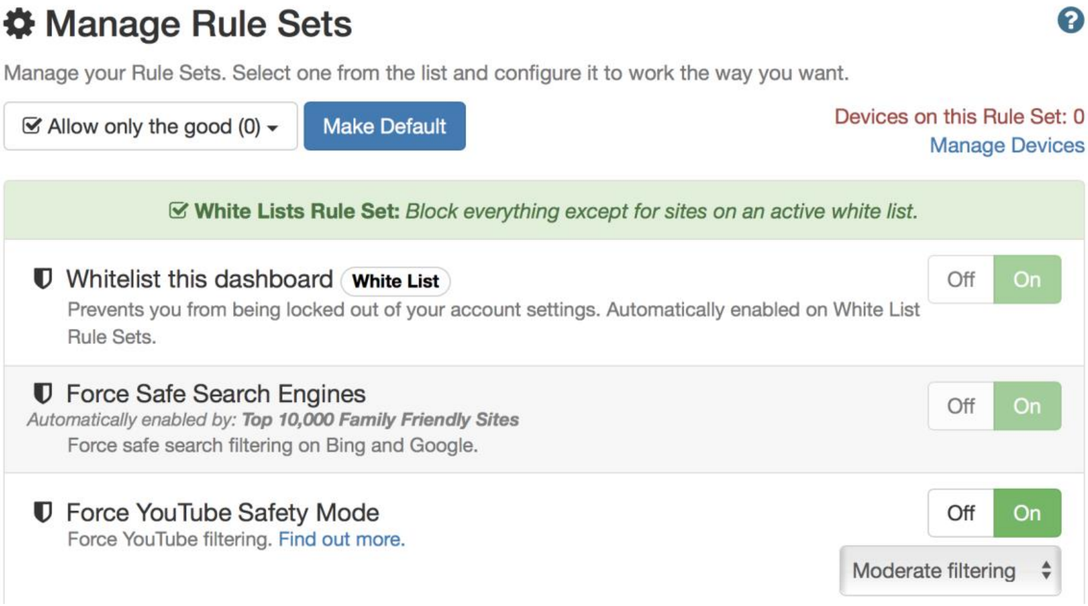
ad.doubleclick.net

Blocked because this domain is not on any active white lists.

Note that "**Request Unblock**" feature only appears on Rule Sets based on Whitelists.

Creating and Managing Rule Sets

1. Introduction to Rule Sets: Rule Sets can also be thought of as a policy. Each Rule Set is made up of a number of lists, each of which is either OFF or ON. Here is a typical Rule Set based on White lists:



Manage Rule Sets

Manage your Rule Sets. Select one from the list and configure it to work the way you want.

☑ Allow only the good (0) ▾ | Make Default

Devices on this Rule Set: 0
Manage Devices

☑ **White Lists Rule Set:** *Block everything except for sites on an active white list.*

Whitelist this dashboard **White List** — Off [✓ On]
Prevents you from being locked out of your account settings. Automatically enabled on White List Rule Sets.

Force Safe Search Engines — Off [✓ On]
Automatically enabled by: ***Top 10,000 Family Friendly Sites***
Force safe search filtering on Bing and Google.

Force YouTube Safety Mode — Off [✓ On]
Force YouTube filtering. Find out more.
Moderate filtering

Below those three features/lists are all other white, black, rainbow, authoritative lists, etc.

2. Rule set types:

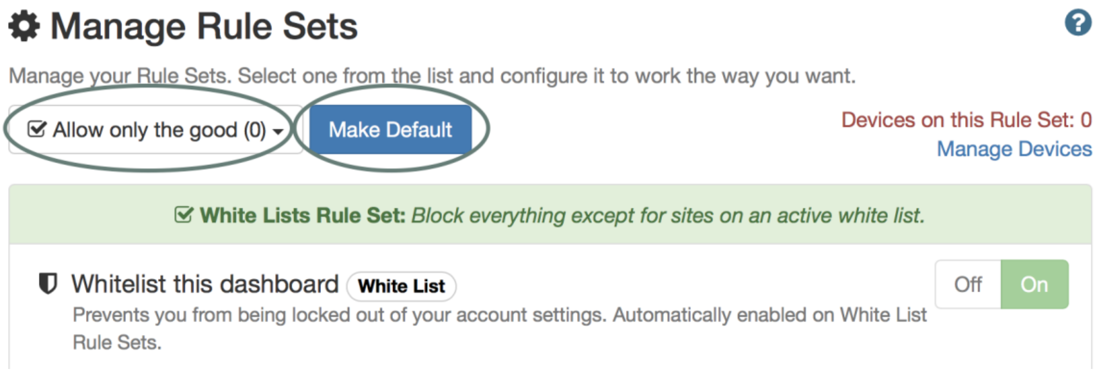
   a. **White lists**: in this type of Rule Set, all list types may be used, but the important consideration is that it adopts the method of block-all-allow-some. Unless a domain is on a white list, and such a white list is set to ON (enabled), the domain will not resolve to its authoritative public IP address.

   b. **Black lists**: refer to chart of Rules and Rule Sets above, and note that not all list types apply. Mainly **white lists do not apply**. This ruleset adopts a method of allow-all-block-some.

   c. **Unfiltered**: refer to chart of Rules and Rule Sets above, and consider that this ruleset type is rarely used except when a device should proceed on an unfiltered basis. In such events, rainbow and authoritative lists still apply.

   d. **Schedules**: ideal when devices are ideally suited for different Rule Sets at different times of day. For example, desktop devices that remain powered on 24/7 for purposes of updating and off-hour maintenance require no other access other than vendor software updates and managed service provider remote access. A security-conscious environment would benefit from a strict whitelist during off-hours.

3. Rule set assignments: Each device is represented by a unique MAC address (when enrollment is automatic), or by IP address (when enrollment is manual). Each software stack has a default ruleset, which can be changed at any time as shown here:



Manage Rule Sets

Manage your Rule Sets. Select one from the list and configure it to work the way you want.

☑ Allow only the good (0) ▾ | Make Default

Devices on this Rule Set: 0
Manage Devices

☑ **White Lists Rule Set:** *Block everything except for sites on an active white list.*

Whitelist this dashboard **White List** — Off / On

Prevents you from being locked out of your account settings. Automatically enabled on White List Rule Sets.

From Manage Rule Sets -> Select the drop-down list -> Make Default. All newly-discovered or newly-added devices going forward are then assigned the new default Rule Set.

How devices are enrolled and named

Device enrollment is fully automated. Normally, no action is required as devices are listed automatically by its broadcast name, such as "**Johnny's iPhone**".

Only when broadcast names are unable to be determined by the filtering service, does it fall back to the manufacturer of the MAC address. Here are some examples:

- MAC addresses starting with **00:00:00** are **Xerox**
- MAC addresses starting with **A8:66:7F** are **Apple**
- MAC addresses starting with **80:C1:6E** are **HP**

Having the MAC address visible provides you with the best ability to control your rule sets, which will follow the MAC address. In other words, if a device changes its IP address, the rule set will still apply. If the MAC address listed on the dashboard does not match, that happens when OSI layer 2 visibility is not available. This means that the filtering service received a different MAC address then your actual device. This can happen in the following circumstances:

- A router (layer 3) is between your filtering service and the device
- A bridge is between your filtering service and the device

Furthermore, the following are conditions where the broadcast name (NetBIOS) name may be unavailable to the filtering service:

- Device has a firewall turned on
- Device has NetBIOS bindings disabled
- Filtering is run on a stand-alone device (such as ClearOS in standalone mode)

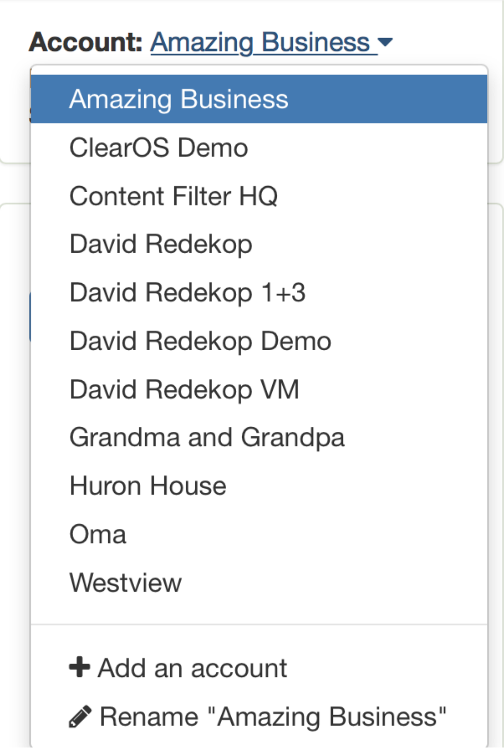
Enrollment happens automatically upon the first received DNS query. Devices remain in the list until they are deleted.

Accounts, Locations and Administrative Users

Accounts are associated with these properties:

- Separate Billing relationship from other “accounts”
- Separate devices running on-premise software stack
- No automatic presence of Rules (lists) created in other accounts

However, from one user account, all access accounts are accessible as shown here:

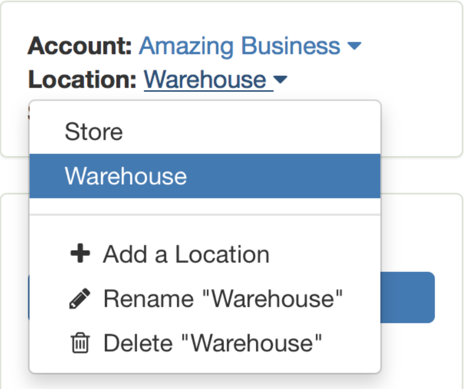


Account: Amazing Business

Locations, on the other hand, refer to separate geographical locations but also carry these properties:

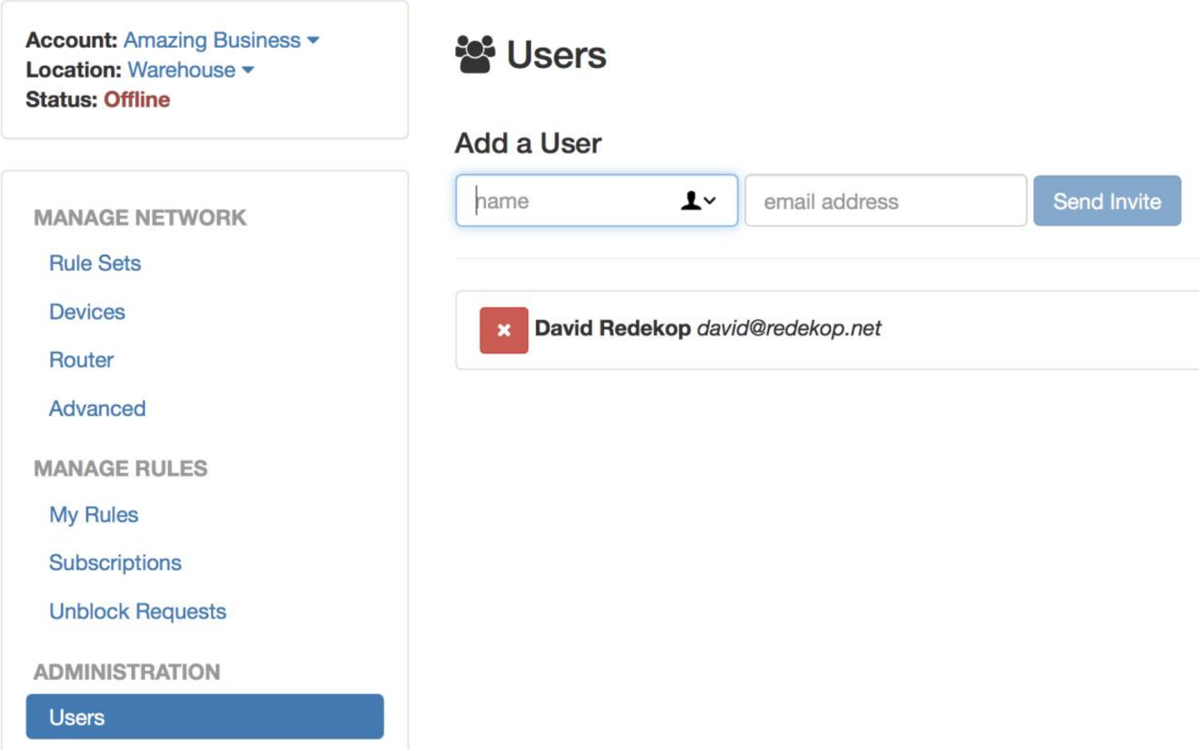
- All location within the same account **share the same administrative access**
- All locations within the same account **share Rules/lists**
- Each location (even within the same account) carries **distinct Rule Sets**

An example of the user experience when navigating to other locations within an account:



Account: Amazing Business
Location: Warehouse

Administrative users are added by initiation of an email invitation under Administration -> Users -> name/email and then choosing **Send Invite**:



Account: Amazing Business
Location: Warehouse
Status: Offline

David Redekop *david@redekop.net*

Other Documentation

This information is provided in conjunction with other documents and videos as outlined here:

0	Product Overview and Availability
1	Procurement, Introduction and pre-installation
2	Installation and deployment
3	Lists, Rule Sets and Devices (this document)
4	Don’t Talk To Strangers (DTTS)
5	Customization and Tailoring

Support

Email for support:	support@gateway.management
Technical Training available at:	http://support.gateway.management