

Self-Service firewall guide for HfL schools

This is a user guide which has been tailored for Herts for Learning schools, providing guidance on how to use the Self-Service firewall feature, found within RM SafetyNet. By default, all schools on the network are protected by the central firewall which is managed by RM. However, some schools may wish to manage their own security profile. HfL is keen to be as flexible as possible and therefore we are happy to devolve responsibilities to schools. For read/write access to be set up, the Head Teacher will need to email Kevin Crawley (kevin.crawley@hfleducation.org) to authorise this.

Once access has been set up, the user can log into RM SafetyNet using their existing credentials. If the credentials have been misplaced, these can be resent. Once logged in, the access defaults to the management of the web filtering. To change this to the Self-Service firewall (and Self-Service DNS) you will need to change the setting, found in the top left-hand corner and toggle from RM SafetyNet to RM Connectivity Services.

You should then see this screen:



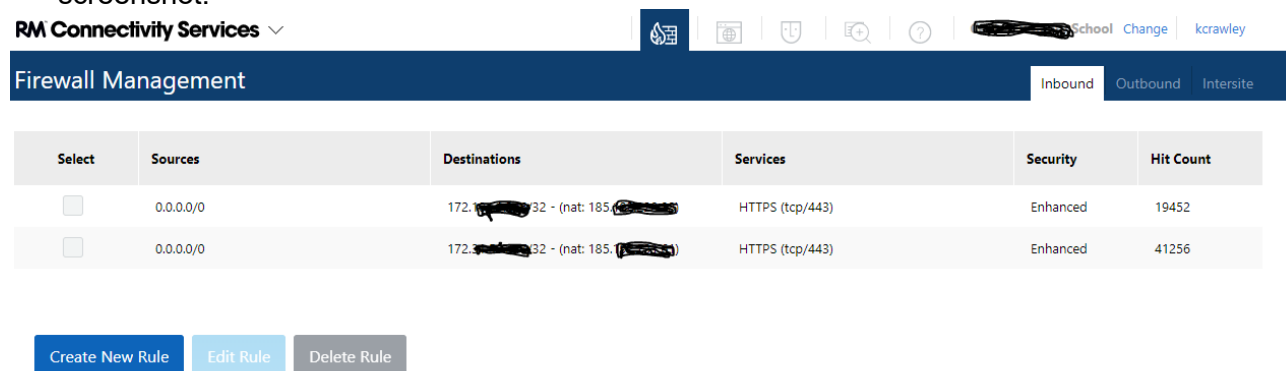
On the upper tab, click on the first option to access the Self-Service firewall.

The lower tab is then split up into three sections;

- 1) Inbound – where you can view/create inbound firewall rules. There's further advice on this below.
- 2) Outbound – where you can view/create outbound firewall rules. There's further advice on this below.
- 3) Intersite – where you can view the site-to-site access you have with other schools. This is only available through 'read only' access. The reason for this, is that implementing rules between various sites will need both schools to authorise access. That said, it does also show access between a school's curriculum network (172* range) and their transparent proxy network (10* range). Should you wish to permit access between your school and another site, or if you wanted to permit access between your curriculum and transparent networks, you will need to log a call with the HfL Support Desk by emailing support@hfleducation.org

Inbound rules

To view inbound rules, you will need to click on the inbound tab, as per the below screenshot:



For each firewall rule, the following information is then displayed:

Select	Sources	Destinations	Services	Security	Hit Count
--------	---------	--------------	----------	----------	-----------

Sources – this is the IP address/address range that will have access to connect into the school on this rule. Note; 0.0.0.0/0 is the entire internet (i.e ANY).

Destinations – this is the internal IP address that the inbound rule will route sessions to. You will also see the NAT'd IP address in brackets.

Services – these are the ports that access has been permitted on. The screenshot above show that on the listed example, access is permitted through HTTPS only.

Security – the vast majority of the time this will be set to Enhanced. This means that all of the traffic coming into the school on the rule will have all the extra security features that the HfL offering provides. It is recommended that you leave this set to Enhanced, rather than Standard. The final security setting is VOIP. This means SIP ALG is enabled and this option will be required for certain VOIP/SIP firewall deployments (SIP Application-level Gateway inspects SIP/VOIP traffic).

Hit Count – this is the amount of recent hits for the specific firewall rule.

To create an inbound rule, you will need to click on the Create New Rule button;

Create New Rule

If you can't see this, it is likely that your account only has read only access permitted. You should contact Herts for Learning support to query this further. However, as explained above, we will require authorisation from the Head Teacher before anyone can have read/write access permitted.

Assuming, you can create the rule, you will then have four fields to enter text;

Create Inbound Rule

Instructions:

- Enter the external source IPs that require access to a LAN IP in your establishment. For policies where you would like any external IP access, use 0.0.0.0/0 or leave the field blank.
- Select the service you would like to allow access over if the service you require is not in the drop-down you can create your own for example, tcp/8001.
- Enter the destination LAN IP you would like to allow access to. Where you would like access to multiple LAN IP's, you will need to create multiple policies.
- When the rule is created, a NAT entry will automatically be created.

External Source IP ranges ⓘ

0.0.0.0/0 +

Selected IP ranges:

Services allowed ⓘ

Select or Type +

Selected Services:

Destination LAN IP ⓘ

+ Selected IP:

Inspection: ⓘ

Standard

Cancel Create

External Source IP ranges – this is the public IP address range that the rule will allow access from. You will need to enter individual IP addresses one-by-one. Alternatively, you can enter subnets in CIDR format. If you are struggling to enter a range of addresses, please speak to the HfL Support and they can arrange the firewall rule being set up.

If you want access permitted from the entire internet (i.e. ANY), you can enter 0.0.0.0/0 or just leave it blank. The only time you would do this, would be if you can't lock access down to particular source IP addresses. Allowing access from the entire internet significantly increases how risky a firewall rule is - and where possible, this should be avoided. The HfL support team is always happy to offer advice. Once the source IP addresses are added, click on the plus icon and move to the next field.

Services allowed – these are the ports that access will be permitted on. Enter the services/ports by clicking on the plus icon.

Destination LAN IP – this will be the internal IP address inside the school that you are allowing sessions to connect into. Enter the IP address by clicking on the plus icon.

Inspection – It is very likely that you will want this left to Enhanced. This means that the extra security features that schools have available will be running over the traffic. This defaults to Standard so be sure to change it to Enhanced.

You can then save the firewall rule by clicking on Create.

After a few moments, the inbound rule will then be listed with all the other inbound firewall rules. The NAT'd IP address will be also be present. You could also create a corresponding DNS record with the IP address within the DNS Self-Service area of SafetyNet if you want (you will need to enter the external IP address within the external DNS zone, and internal IP address within the internal DNS zone) - further DNS support can be found here: <https://hfl-broadband.co.uk/wp-content/uploads/2019/07/Self-Service-DNS-in-Herts.doc.pdf>

To edit or to delete an inbound firewall rule, you will need to select the firewall rule in question by ticking the box next it.

Firewall Management

Select	Sources	Desti
<input type="checkbox"/>	0.0.0.0/0	172.1
<input checked="" type="checkbox"/>	0.0.0.0/0	172.1

Create New Rule

Edit Rule

Delete Rule

You can then either edit or delete the rule by clicking on the relevant option towards the bottom of the page. If you can't see this, it may be that you only have read only access permitted. You should contact Herts for Learning support to query this further.

Outbound rules

To create an outbound rule, you will once again need to click on the Create New Rule button. You have two options when permitting outbound access. You will either create a firewall rule to an Internet Service Database (ISDB) ruleset, or you can create access through a custom rule. To choose which type of outbound firewall you wish to create, you will need to move the slider to either basic (for an ISDB rule) or Custom for all other rules:

Create Outbound Rule

For ease of use, it is recommended to create outbound policies using built-in ISDB Destinations. These are a common set of centrally managed cloud services which are automatically updated. If the application you need to permit is not available, switch to custom mode to create your own.

Instructions:

- Enter the LAN range you would like to have access to the service.
- When the rule is created, a NAT entry will automatically be created.

Basic ☒ Custom

LAN IP ranges ⓘ

 +

Selected IP ranges:

ISDB Destination ⓘ

 +

Selected ISDB entries:

Inspection: ⓘ

Cancel

Create

ISDB firewall rules

RM's firewall provider is Fortinet and they have firewall rulesets you can use that permits access to specific third parties. This is really helpful as it avoids you having to obtain a

firewall instruction from the third parties - as Fortinet have already done this for you. It also means if the third parties update their firewall requirements – such as changes to their public IP address range, Fortinet should update the ISDB ruleset and access should continue to work.

Using WhatsApp as example, if you wish to create a rule to permit access to WhatsApp, simply enter the internal IP addresses in the LAN IP ranges that require access to this rule. You will need to either enter IP addresses singularly, or by adding a subnet in CIDR format.

In the search field within in the ISDB Destination, if you type WhatsApp, you will see the ISDB rule appear:

ISDB Destination ⓘ



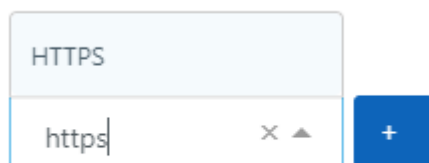
Click on the plus icon to add it.

Finally change the inspection of the traffic to Enhanced and click on create. This will save the firewall rule and access will immediately be in place.

Custom rules

Similar to the ISDB rules, you will need to enter the internal IP addresses in the LAN IP ranges that require access to this rule. You will need to either enter IP addresses singularly, or by adding a subnet in CIDR format.

In the Services Allowed field, search on the ports and add them by using the blue icon.



Selected Services:

Within the External IPs, you will need to add the entire destination of where you will be communicating with. You can only enter public IP addresses – either singularly or in CIDR format. If you need to add a range of addresses that doesn't work neatly within the CIDR format, or you wish to enter FQDNs, this will need to be logged to RM firewall engineers to action through the HfL Support Desk.

If you want access permitted to the entire internet (i.e. ANY), you can enter 0.0.0.0/0 or just leave it blank. However, it's good practice to lock the firewall rule down to a specific destination. If you create an outbound rule to the entire internet on HTTP and HTTPS for example, you are potentially creating an unfiltered and unmonitored internet connection. If you have any queries, please get in touch with the HfL Support Desk who can offer advice.

You will then need to change the inspection to Enhanced, because it defaults to Standard. This will force on the extra security features that HfL schools have included.

The final stage will be to click on Create and the firewall rule will then be made live.

Note: if you are trying to edit and make changes to a firewall rule that has access permitted to an FQDN, you will see that there isn't a box to select that particular row. That is because all firewall rules involving FQDNs needs to be updated by the RM firewall engineers and you will need to log a support call with the HfL Support Desk by emailing support@hfleducation.org