

Shield Admin Guide

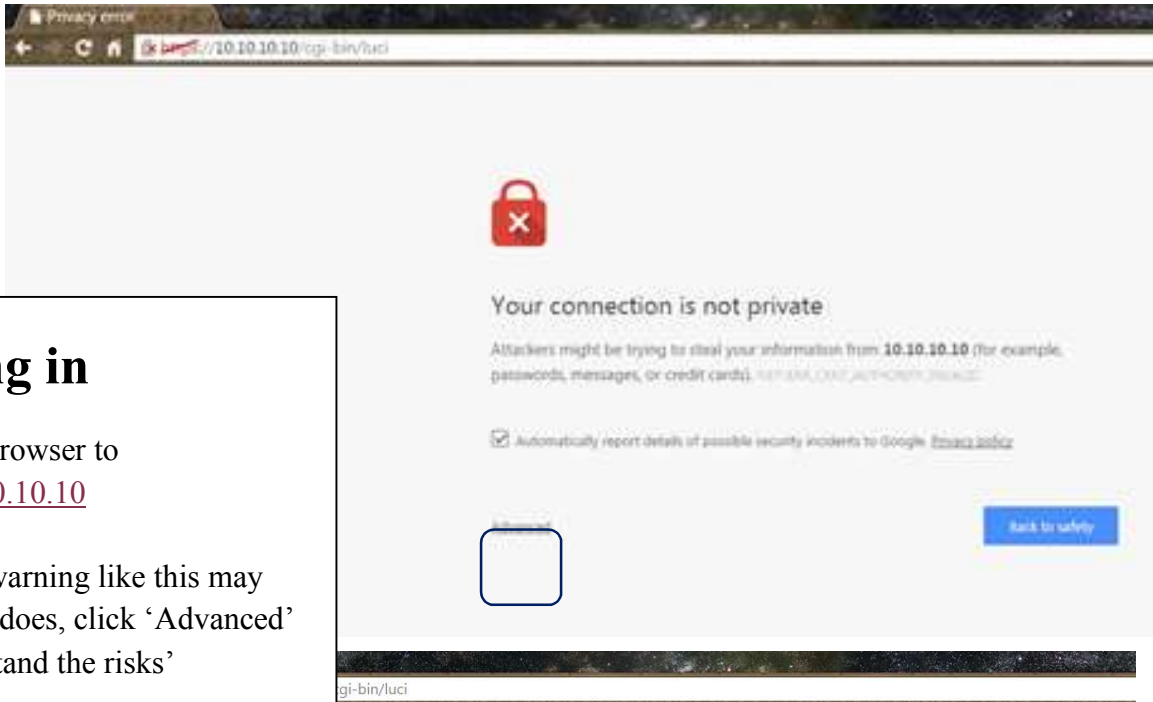


v1.0

Table of Contents

Web User Interface

Logging In.....	2
Status Menu	
Overview.....	3
Firewall.....	4
Routes.....	5
Processes.....	5
Traffic Monitor.....	6
Real-time Graphs.....	7
Advanced Settings.....	8
Update Log.....	8
Removing Banners.....	9
Restarting Shield.....	9
Manual Updating.....	9
Factory Reset.....	10
System Menu	
Time Zone.....	10
System Log.....	11
Language.....	11
Scheduled Tasks.....	12
SSH Access.....	12
System Password.....	12
Backup Config.....	13
Command Line.....	21
Services Menu	
Intrusion Prevention.....	14
Web Filter.....	17
Dynamic DNS.....	18
Network Menu	
Interfaces.....	22
DHCP and DNS.....	26
Hostnames.....	27
Static Routes.....	27
Diagnostics.....	28
Firewall.....	29
Queue Management.....	34

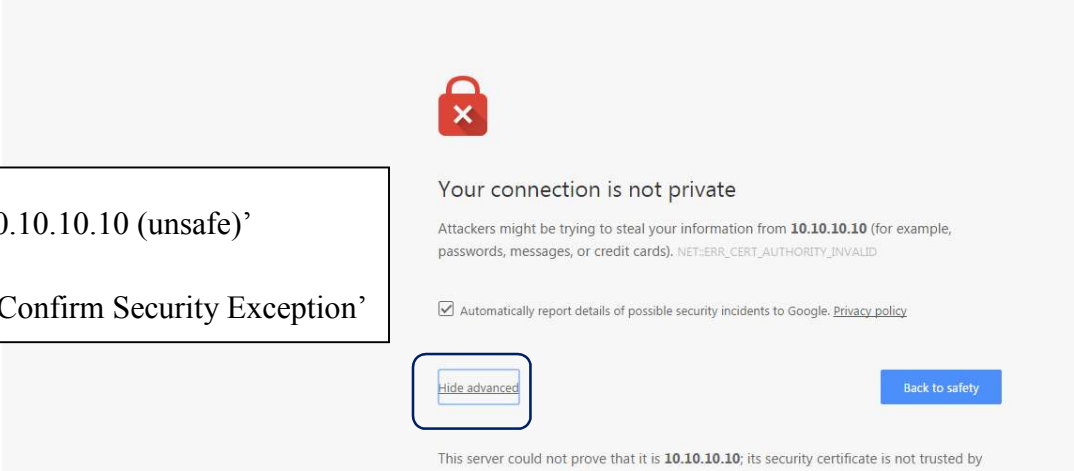


Logging in

Open web browser to <https://10.10.10.10>

A security warning like this may appear, if it does, click 'Advanced' or 'I understand the risks'

Click 'Proceed to 10.10.10.10 (unsafe)' or 'Add Exception → Confirm Security Exception'



Log in to your Shield.

<i>Username</i>	admin
<i>Default Password</i>	itus





Status

System

Hostname	Shield
Model	S001
Serial Number	[REDACTED]
Firmware Version	v1.0 SP1-1124
Operating Mode	UTM Router
Local Time	Tue Nov 24 18:41:30 2015
IPS Last Updated	Nov 17
Web Filter Last Updated	Nov 22
Shield Update Last Run	
Uptime	5h 14m 58s

Overview


The system overview page displays relevant system information in an easy to read dashboard.

Scroll to the bottom of the page to see networks settings and DHCP lease information.

Memory

Total Available	313536 kB / 1011200 kB (31%)
Buffered	22016 kB / 1011200 kB (2%)

Network

Active Connections	165 / 10000 (1%)
IPv4 Status	<div style="border: 1px solid #ccc; padding: 5px;">  Type: dhcp Address: [REDACTED] Netmask: [REDACTED] Gateway: [REDACTED] DNS 1: 75 [REDACTED] DNS 2: 75 [REDACTED] Connected: 5h 13m 58s </div>

DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
android-a2f4a062bafc3b40	10.10.10.228	[REDACTED]	11h 17m 58s
XboxOne	10.10.10.139	[REDACTED]	8h 14m 24s
Amanys-iPhone	10.10.10.170	[REDACTED]	8h 6m 28s
android-f633d78bd0454415	10.10.10.216	[REDACTED]	8h 8m 10s
android-fd9f2a33168cb0ca	10.10.10.176	[REDACTED]	7h 50m 8s
02AA01AC411306XT	10.10.10.208	[REDACTED]	8h 48m 30s
Ayoub	10.10.10.137	[REDACTED]	10h 4m 7s





Firewall Status

IPv4 Firewall

IPv6 Firewall

Actions

- [Reset Counters](#)
- [Restart Firewall](#)

Table: Filter

Chain INPUT (Policy: ACCEPT, Packets: 0, Traffic: 0.00 B)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	50128	5.69 MB	delegate_input	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

Chain FORWARD (Policy: DROP, Packets: 0, Traffic: 0.00 B)

Rule #	Pkts.	Traffic	Target	Prot.	Flags	In	Out	Source	Destination	Options
1	3714803	2.99 GB	NFQUEUE	all	--	*	*	0.0.0.0/0	0.0.0.0/0	NFQUEUE balance 7:8 cpu-fanout
2	0	0.00 B	delegate_forward	all	--	*	*	0.0.0.0/0	0.0.0.0/0	-

Firewall Status

Displays statistical information related to your Shield's firewall. Traffic and packet count information is logged here; this is particularly useful when troubleshooting. From this page you can reset the counters or reset the firewall. From this page you can also access your IPv6 firewall settings. IPv6 is disabled by default.



Active IPv4-Routes

Network	Target	IPv4-Gateway	Metric	Table
wan	0.0.0.0/0	24.130.128.1	0	main
cfg074d8f	10.10.10.0/24		0	main
wan	24.130.128.0/23		0	main
wan	24.130.128.1		0	main

Active IPv6-Routes

Network	Target	Table
cfg074d8f	fd5b:f73b:70c3::/64	main
wan	ff02::1	local
cfg074d8f	ff02::1	local
cfg074d8f	ff00::/8	local
wan	ff00::/8	local

Route Status

Shows Layer 2 and Layer 3 traffic information used by your Shield.

Information found here includes...

- ARP Table
- Routing Table
- IPv6 Neighbors



Processes

This list gives an overview over currently running system processes and their status.

PID	Owner	Command	CPU usage (%)	Memory usage (%)	Hang Up	Terminate	Kill
1	root	/sbin/pro	0%	0%	Hang Up	Terminate	Kill
2	root	[kthread	0%	0%	Hang Up	Terminate	Kill
3	root	[ksoftirq	0%	0%	Hang Up	Terminate	Kill
4	root	[kworker	0%	0%	Hang Up	Terminate	Kill
5	root	[kworker	0%	0%	Hang Up	Terminate	Kill
7	root	[migration	0%	0%	Hang Up	Terminate	Kill
8	root	[rcu_bh]	0%	0%	Hang Up	Terminate	Kill
9	root	[rcu_sched]	0%	0%	Hang Up	Terminate	Kill
10	root	[migration/1]	0%	0%	Hang Up	Terminate	Kill

Processes Status

This provides an overview of everything running on the Shield. If one of the processes begins consuming large amounts of CPU or RAM, it can be seen here. From this page individual services can be terminated or killed.



Graphs

Configuration

Traffic Monitor

Traffic Monitor keeps a log of network traffic for the selected interface(s).

- Monitor selected interfaces
- Bridge: "br-lan" (lan)
 - Ethernet Adapter: "eth0" (wan, wan8)
 - Ethernet Adapter: "eth1"
 - Ethernet Adapter: "eth2"

Traffic Monitor

Under the configuration tab, select the interfaces you'd like to monitor, then hit 'Save & Apply'

The Graphs tab displays statistical information about bandwidth usage for each interface being monitored. To view additional reports, use the drop down menu and 'Update' button.

Reset

ADVANCED



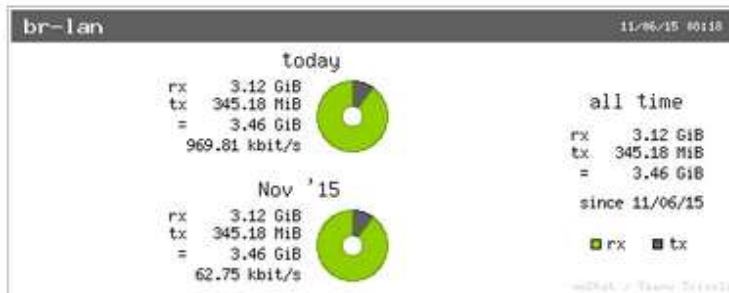
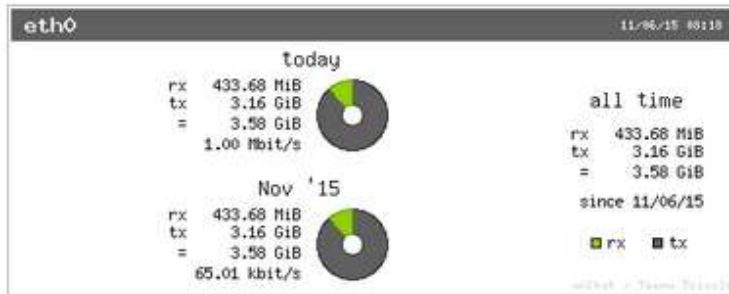
Graphs

Configuration

Traffic Monitor Graphs

Summary display

Update



Load Connections Traffic

Realtime Connections

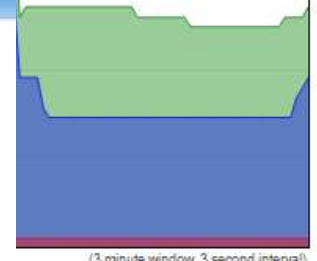
This page gives an overview over currently active network connections.

Active Connections



Load Connections Traffic

CPU Utilization



(3 minute window, 3 second interval)

Peak: 25

Peak: 32

Peak: 1

Real Time Graphs

Traffic – Shows the throughput in and out for each interface.

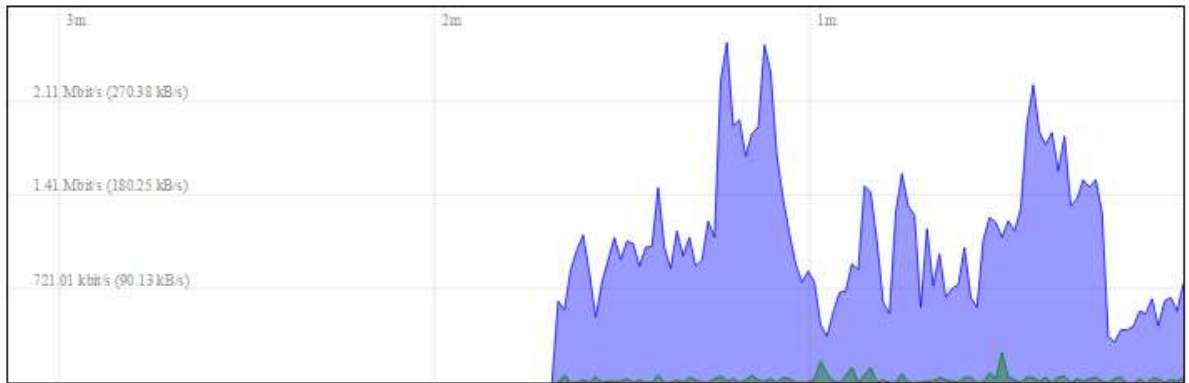
Connections – Shows the volume of UDP & TCP connections.

CPU – Shows the cpu usage relative to each cpu core. (ie, 200%)

15 Minute Load:

br-lan eth0 eth1 eth2

Shield v1.0 SP1-1105



(3 minute window, 3 second interval)

Inbound: 775.98 kbit/s
(97 kB/s)

Average: 884.38 kbit/s
(85.54 kB/s)

Peak: 2.58 Mbit/s
(327.73 kB/s)

Outbound: 50.39 kbit/s
(6.3 kB/s)

Average: 38.4 kbit/s
(4.8 kB/s)

Peak: 246.7 kbit/s
(30.84 kB/s)

Shield v1.0 SP1-1105



ITUS Settings

System Update runs automatically every day. IPS Rules updated 1-2 times per week or as needed. Blacklists are updated periodically. Factory reset takes effect immediately. Do not disconnect power from Shield when performing a factory reset. After the factory reset completes, your Shield will automatically start. Please allow 10 minutes for the process to complete.

Advanced Settings

ITUS Update Log

Remove Banners

Update Shield

Reboot Shield

Factory Reset

Show Advanced Mode:

yes

Save & Apply

Save

Reset

Shield v1.0 SP1-1105

Advanced Settings

This tab can be used to toggle between the 'basic' and 'advanced' graphical user interface. Set the desired mode using the drop down menu, then click save & apply. You may need to refresh your browser to see the newly enabled menu options.



ITUS Settings

System Update runs automatically every day. IPS Rules updated 1-2 times per week or as needed. Blacklists are updated periodically. Factory reset takes effect immediately. Do not disconnect power from Shield when performing a factory reset. After the factory reset completes, your Shield will automatically start. Please allow 10 minutes for the process to complete.

Advanced Settings

ITUS Update Log

Remove Banners

Update Shield

Reboot Shield

Factory Reset

System update utility was last run...

IPS Rules last updated...

Nov 8 02:38

Web Filter last updated...

Nov 5 21:29

Update Log

This tab displays information about the last time the system update utility was run. By default, the system checks for updates once per day between 3am and 4am local time. Service may be interrupted for several minutes during the update.

ITUS Settings

System Update runs automatically every day. IPS Rules updated 1-2 times per week or as needed. Blacklists are updated periodically. Factory reset takes effect immediately. Do not disconnect power from Shield when performing a factory reset. After the factory reset completes, your Shield will automatically start. Please allow 10 minutes for the process to complete.

[Advanced Settings](#)[ITUS Update Log](#)[Remove Banners](#)[Update Shield](#)[Reboot Shield](#)[Factory Reset](#)

System Notification Banners:

Removing Banners

From time to time you may notice system banners appearing in the web user interface. These can be removed by clicking this button.

Shield v1.0 SP1-1105

ITUS Settings

System Update runs automatically every day. IPS Rules updated 1-2 times per week or as needed. Blacklists are updated periodically. Factory reset takes effect immediately. Do not disconnect power from Shield when performing a factory reset. After the factory reset completes, your Shield will automatically start. Please allow 10 minutes for the process to complete.

[Advanced Settings](#)[ITUS Update Log](#)[Remove Banners](#)[Update Shield](#)[Reboot Shield](#)[Factory Reset](#)

Run System Update:

Manual Updating

To manually run the system update utility, click the '**Update Shield**' tab, then click the 'Start' button. No further action is required, the utility will run in the background and may take several minutes to complete. Service may be interrupted during the update.

Shield v1.0 SP1-1105

ITUS Settings

System Update runs automatically every day. IPS Rules updated 1-2 times per week or as needed. Blacklists are updated periodically. Factory reset takes effect immediately. Do not disconnect power from Shield when performing a factory reset. After the factory reset completes, your Shield will automatically start. Please allow 10 minutes for the process to complete.

[Advanced Settings](#)[ITUS Update Log](#)[Remove Banners](#)[Update Shield](#)[Reboot Shield](#)[Factory Reset](#)

Reboot Shield:

Restarting Shield

To restart your shield, click the **Reboot Shield** tab, then use the 'Restart' button. The Shield will immediately restart upon clicking the button, no warning is displayed

ITUS Networks Status System Services Network Logout **ADVANCED**

ITUS Settings

System Update runs automatically every day. IPS Rules updated 1-2 times per week or as needed. Blacklists are updated periodically. Factory reset takes effect immediately. Do not disconnect power from Shield when performing a factory reset. After the factory reset completes, your Shield will automatically start. Please allow 10 minutes for the process to complete.

Advanced Settings ITUS Update Log Remove Banners Update Shield Reboot Shield **Factory Reset**

Factory Reset:

Factory Reset

To **Factory Reset** your Shield, click the 'Factory Reset' tab, then use the 'Start' button. This button can be used to apply system updates which require a factory reset. Do not disconnect power from your Shield during a factory reset. The Shield should come back online in about 10 minutes with default settings restored.

Warning – Clicking 'Start' will immediately trigger the factory reset process. This process is irreversible; nothing is automatically backed up, all settings will return to their original state.

ITUS Networks Status System Services Network Logout **ADVANCED**

System

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

General Settings **Logging** Language and Style

Local Time Fri Nov 6 08:22:54 2015

Hostname

Timezone

Time Zone

To set the local **Time Zone** for your Shield use the 'General Settings' tab. The time zone is used for system and services logs as well as running updates. Services may need to be restarted in order for changes to take effect. After selecting the desired zone, click save & apply.



System

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

General Settings Logging Language and Style

System log buffer size: 1024
kiB

External system log server: 0.0.0.0

External system log server port: 514

Log output level: Error

Cron Log Level: Debug

System Log

The **Logging** tab can be used to configure the system log. This is the general log used by daemon programs running and services. An external syslog server can be specified as well. Warning – Setting the log buffer size too large may have a negative impact on the web interface’s performance.



System

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

General Settings Logging Language and Style

Language: auto

- auto
- Català (Catalan)
- Čeština (Czech)
- Deutsch (German)
- Ελληνικά (Greek)
- English
- Español (Spanish)
- Français (French)
- עברית (Hebrew)
- Magyar (Hungarian)
- Italiano (Italian)
- 日本語 (Japanese)
- Bahasa Melayu (Malay)
- Norsk (Norwegian)
- Polski (Polish)
- Português (Portuguese)
- Português do Brasil (Brazilian Portuguese)
- Română (Romanian)
- Русский (Russian)
- Svenska (Swedish)

Shield v1.0 SP1-1105

Save & Apply Save Reset

Language

To change the language of the graphical user interface, use the **Language and Style** tab. Select the desired language, then click ‘Save & Apply’. Settings will take effect immediately but may require a browser refresh to render.



Router Password

Changes the administrator password for accessing the device

Password

Confirmation

System Password
 To **change** the Shield's **password**, enter the new password twice, then click save & apply.

SSH Access

Dropbear offers SSH network shell access and an integrated SCP server

Dropbear Instance

This section contains no values yet

Add

SSH-Keys

Here you can paste public SSH-Keys (one per line) for SSH public-key authentication.

[Empty text area for SSH keys]

SSH Access
 Enabling SSH Access on the Shield is a 3 step process. Step one, is to click the 'Add' button.
 Step two is selecting interface on which SSH will be accessible then clicking 'Save & Apply'
 Step three is restarting the firewall from the startup tab.



Scheduled Tasks

This is the system crontab in which scheduled tasks can be defined.

```
2 03 * * * sh /sbin/fw_upgrade
*/10 * * * * /usr/sbin/ntpclient -s -p 123 -h 0.us.pool.ntp.org || /etc/init.d/ntpclient restart
```

Scheduled Tasks
 This tab shows the crontab schedule. These are tasks set to run on a specified schedule. By default there are two entries, one for the ntp service, and the other for the update service.

Submit Reset



Initscripts

You can enable or disable installed init scripts here. Changes will applied after a device reboots.
Warning: If you disable essential init scripts like "network", your device might become unusable.

System Startup
Provides the ability to start, stop, restart, and enable/disable various services running on the Shield. Shield's rc.local file can be found at the bottom of this page.

Start priority	Initscript	Enable/Disable			
0	sysfixtime	Enabled			
10	boot	Enabled			
10	system	Enabled			
11	sysctl	Enabled	Start	Restart	Stop
12	log	Enabled	Start	Restart	Stop
12	rpcd	Enabled	Start	Restart	Stop
19	firewall	Enabled	Start	Restart	Stop
20	network	Enabled	Start	Restart	Stop
35	odhcpd	Enabled	Start	Restart	Stop



Configuration Backup

Actions Configuration

Backup / Restore

Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Download backup:

To restore configuration files, you can upload a previously generated backup archive here.

Restore backup: No file chosen

Shield v1.0 SP1-1105

Configuration Backup
The Actions tab provides the ability to download a backup of the Shield's current configuration. Settings can also be uploaded and restored from here.

The configuration tab can be used to define what settings are backed up.

Intrusion Prevention

Changes may take up to 90 seconds to take effect, service may be interrupted during that time. The IPS engine will restart each time you click the Save or Save & Apply button. During the time the IPS engine is restarting, the On/Off button will display 'Off'. It generally takes 1-2 minutes for the IPS to restart. You will need to refresh your browser window or move away from the IPS menu, then back to it in order to see the button refresh to say 'On' once the engine has finished reloading. Do Not Use the On/Off button in conjunction with Save & Apply. Clicking the button when it says 'On' will turn the IPS off. Clicking the button when it says 'Off' will turn the IPS on. Clicking Save & Apply afterwards will cause the system to restart the IPS.

Basic Settings Snort7 Config Snort8 Config Threshold Config Custom Rules Exclude Rules IPS Logs

Status:

Save & Apply Save Reset

Intrusion Prevention

Changes may take up to 90 seconds to take effect, service may be interrupted during that time. The IPS engine will restart each time you click the Save or Save & Apply button. During the time the IPS engine is restarting, the On/Off button will display 'Off'. It generally takes 1-2 minutes for the IPS to restart. You will need to refresh your browser window or move away from the IPS menu, then back to it in order to see the button refresh to say 'On' once the engine has finished reloading. Do Not Use the On/Off button in conjunction with Save & Apply. Clicking the button when it says 'On' will turn the IPS off. Clicking the button when it says 'Off' will turn the IPS on. Clicking Save & Apply afterwards will cause the system to restart the IPS.

Basic Settings Snort7 Config Snort8 Config Threshold Config

```
output alert_fast: alert.fast
# output log_tcpdump: tcpdump.log

include classification.config
include reference.config

include reference.config

var RULE_PATH /etc/snort/rules/
var PREPROC_RULE_PATH /etc/snort/rules/
var BLACK_LIST_PATH /etc/snort/rules/

include $RULE_PATH/local.rules
include $RULE_PATH/snort.rules
#include $PREPROC_RULE_PATH/preprocessor.rules
include $PREPROC_RULE_PATH/decoder.rules
include $PREPROC_RULE_PATH/sensitive-data.rules

include threshold.conf

ipvar HOME_NET any
ipvar EXTERNAL_NET any
ipvar DNS_SERVERS $HOME_NET
ipvar SMTP_SERVERS $HOME_NET
ipvar HTTP_SERVERS $HOME_NET
```

Intrusion Prevention

The On/Off button can be used to toggle the IPS on or off. Clicking the button will immediately toggle the opposite state. So, if the Status is ON, and the button is clicked, the IPS will switch to OFF. Turning ON the IPS may require 90 seconds to take effect and it may be refresh browser to see changed button state.

Save & Apply Save Reset

ITUS Networks Status System Services Network Logout ADVANCED

Intrusion Prevention

Changes may take up to 90 seconds to take effect, service may be interrupted during that time. The IPS engine will restart each time you click the Save or Save & Apply button. During the time the IPS engine is restarting, the On/Off button will display 'Off'. It generally takes 1-2 minutes for the IPS to restart. You will need to refresh your browser window or move away from the IPS menu, then back to it in order to see the button refresh to say 'On' once the engine has finished reloading. Do not use the On/Off button when it says 'On' as this will turn the IPS off. Clicking the button when it says 'Off' will turn the IPS on. Clicking Save & Apply afterwards will cause the system to restart the IPS.

Basic Settings Snort7 Config Snort8 Config

```

output alert_fast: alert.fast
# output log_tcpdump: topdump.log

include classification.config
include reference.config

include reference.config

var RULE_PATH /etc/snort/rules/
var PREPROC_RULE_PATH /etc/snort/rules/
var BLACK_LIST_PATH /etc/snort/rules/

include $RULE_PATH/local.rules
include $RULE_PATH/snort.rules
#include $PREPROC_RULE_PATH/preprocessor.rules
include $PREPROC_RULE_PATH/decoder.rules
include $PREPROC_RULE_PATH/sensitive-data.rules

include threshold.conf

```

Intrusion Prevention

The **Snort7** and **Snort8** Config tabs are used to configure the intrusion prevention system. In router & gateway mode, Shield operates with two instances of Snort running; one on each CPU core. In bridge mode, only one configuration tab is available. In router & gateway modes, Snort is configured to use the netfilter queue data acquisition module. By default, there are two queues utilized. Those are Queue 7 & Queue 8; hence the Snort7, Snort8 naming.

Warning – Incorrect configurations in either of these files may result in the IPS not starting properly. Unless you have a need for something specific, it is recommended you do not change the default settings.

ITUS Networks Status System Services Network Logout ADVANCED

Intrusion Prevention

Changes may take up to 90 seconds to take effect, service may be interrupted during that time. The IPS engine will restart each time you click the Save or Save & Apply button. During the time the IPS engine is restarting, the On/Off button will display 'Off'. It generally takes 1-2 minutes for the IPS to restart. You will need to refresh your browser window or move away from the IPS menu, then back to it in order to see the button refresh to say 'On' once the engine has finished reloading. Do not use the On/Off button when it says 'On' as this will turn the IPS off. Clicking the button when it says 'Off' will turn the IPS on. Clicking Save & Apply afterwards will cause the system to restart the IPS.

Basic Settings Snort7 Config Snort8 Config Threshold Config Custom Rules

```

suppress gen_id 129, sig_id 20
suppress gen_id 129, sig_id 12

```

Intrusion Prevention

Threshold Config

If the IPS logs are repeatedly filled with the same entry over & over, this tab can be used to suppress alerts displayed. In general this should not be necessary. Example entries are included to help show how to format.

ITUS Networks Status System Services Network Logout ADVANCED

Intrusion Prevention

Changes may take up to 90 seconds to take effect, service may be interrupted during that time. The IPS engine will restart each time you click the Save or Save & Apply button. During the time the IPS engine is restarting, the On/Off button will display 'Off'. It generally takes 1-2 minutes for the IPS to restart. You will need to refresh your browser window or move away from the IPS menu, then back to it in order to see the button refresh to say 'On' once the engine has finished reloading. Do not use the On/Off button when it says 'On' as this will turn the IPS off. Clicking the button when it says 'Off' will turn the IPS on. Clicking Save & Apply afterwards will cause the system to restart the IPS.

Config Custom Rules Exclude Rules IPS Logs

Custom Rules

```


```

Intrusion Prevention

Custom Rules

This tab may be used to add custom rules to the IPS. Rules should be formatted for Snort 2.9.7.x. Adding a lot of rules here could result in slow GUI performance. For large rulesets, it is better to include a separate file. Incorrectly formatted rules may cause IPS to fail to load.



Web Filter

Changes may take up to 60 seconds to take effect. Web access may be interrupted

Basic Settings White List Black List Logs

Content filtering:

- Ads
- Blasphemy
- Dating
- Drugs
- Gambling
- Illegal
- Malicious



Web Filter

Changes may take up to 60 seconds to take effect. Web access may be interrupted dur

Basic Settings White List Black List Logs Block Page

```

<HTML>
  <BODY>
    <DIV id="wrapper" style="width:100%; text-align:center">
      <IMG id="wrapper" src="itus_logo.png" width="250" height="250" align="center">
      <P>This domain is blocked by Shield's content filtering system. If you
    </DIV>
  </BODY>
</HTML>

```

</P>

Web Filter

Basic Settings

To enable the web filter simply select the desired category, then click save & apply.

White List

The White List tab may be used to explicitly permit sites normally blocked by Shield. Example entries are included to show how to format.

Black List

The Black List tab may be used to explicitly block sites normally allowed by Shield. Example entries are included to show how to format.

Logs

Displays information about web sites accessed through Shield.

Block Page

This is the HTML page served by the web filter when blocking access. A basic configuration is included; the code may be modified if a custom

To use the web filter with Bridge or Gateway mode, you must set Shield as your DNS server in your router's settings.

Save & Apply

Save

Reset



Dynamic DNS

Dynamic DNS allows that your router can be reached with a fixed hostname.

Overview

Below is a list of configured DDNS configurations and their current state. If you want to send updates for IPv4 and IPv6 you need to define two separate configurations. To change global settings click [here](#)

Configuration	Hostname/Domain Registered IP	Enabled
myddns_ipv4	yourhost.example.com No data	<input type="checkbox"/>
myddns_ipv6	yourhost.example.com No data	<input type="checkbox"/>

Dynamic DNS

Provides access to your network from the WAN using a dynamic IP address. This is generally not necessary however some power users may find the feature useful so we have included it. The following example is included to help configure 'basic' DDNS on Shield. To begin, click the 'edit' button on the IPv4 configuration.

Dynamic DNS

Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.

Details for: myddns_ipv4

Configure here the details for selected Dynamic DNS service.
For detailed information about parameter settings look here.

Basic Settings **Advanced Settings** Timer Settings Log File Viewer

Enabled

If this service section is disabled it could not be started. Neither from LuCI interface nor from console

IP address version IPv4-Address
 IPv6-Address

Defines which IP address 'IPv4/IPv6' is send to the DDNS provider

DDNS Service provider [IPv4]

Hostname/Domain
Replaces [DOMAIN] in Update-URL

Username
Replaces [USERNAME] in Update-URL

Password
Replaces [PASSWORD] in Update-URL

Use HTTP Secure
Enable secure communication with DDNS provider

Path to CA-Certificate
directory or path/file
or IGNORE to run HTTPS without verification of server certificates (insecure)

Dynamic DNS

Basic Settings

Check the box that says 'enabled'.

Keep the default IPv4 Address

Select your DDNS provider from the drop down menu.

Enter your Hostname or Domain, this is often the username dot provider.

Username is the one used with your DDNS provider.

Password is also maintained with DDNS provider.

(Think of it as you are 'logging in' to their server to update IP.)

Enable HTTPS.

If you have difficulty connecting, try entering IGNORE as the CA Cert path.

Click Save & Apply

[Back to Overview](#)

[Save & Apply](#) [Save](#) [Reset](#)

ITUS Networks Status System Services Network Logout ADVANCED

Dynamic DNS

Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.

Overview

Below is a list of configured DDNS configurations and their current state.
 If you want to send updates for IPv4 and IPv6 you need to define two separate Configurations i.e. 'myddns_ipv4' and 'myddns_ipv6'
 To change global settings click [here](#)

Configuration	Hostname/Domain Registered IP	Enabled	Last Update Next Update	Process ID Start / Stop	
myddns_ipv4	ITUS_EXAMPLE.dyndns.org <i>No data</i>	<input checked="" type="checkbox"/>	Never Verify	PID: 5791	Edit Delete
myddns_ipv6	yourhost.example.com <i>No data</i>	<input type="checkbox"/>	Never Disabled	-----	Edit Delete

[Add](#)

Dynamic DNS

From the DDNS page, make sure 'Enabled' is checked, then click 'Start'

[Save & Apply](#) [Save](#) [Reset](#)

Shield v1.0 SP1-1118

ITUS Networks Status System Services Network Logout ADVANCED

Dynamic DNS

Dynamic DNS allows that your router can be reached with a fixed hostname while having a dynamically changing IP address.

Overview

Below is a list of configured DDNS configurations and their current state.
 If you want to send updates for IPv4 and IPv6 you need to define two separate Configurations i.e. 'myddns_ipv4' and 'myddns_ipv6'
 To change global settings click [here](#)

Configuration	Hostname/Domain Registered IP	Enabled	Last Update Next Update	Process ID Start / Stop	
myddns_ipv4	ITUS_EXAMPLE.dyndns.org <i>No data</i>	<input checked="" type="checkbox"/>	Never Stopped	Start	Edit Delete
myddns_ipv6	yourhost.example.com <i>No data</i>	<input type="checkbox"/>	Never Disabled	-----	Edit Delete

[Add](#)

Dynamic DNS

You should see the process ID of the DDNS service. If the system successfully authenticates, you will see the 'update' field here change to a time stamp.

[Save & Apply](#) [Save](#) [Reset](#)

Shield v1.0 SP1-1118



Dashboard Configure

Custom Commands

Command: `ls -alst /etc/config/`

Run Download

Command Line

The configure tab can be used to add commands you'd like executed. Click the 'Add' button then enter a description along with the command.

The Dashboard tab can be used to run the command, display the output and download the output as a text file.

Warning- Be careful. All commands are executed as root.

```
ci
ns
rewall
twork
opbear
stem
us
itrack
stat
tab
tftp
4 -rw-rw-r-- 1 root root 1563 Nov 10 00:25 geoip
4 -rw-rw-r-- 1 root root 715 Nov 7 01:57 dhcp
4 -rw-rw-r-- 1 root root 445 Nov 5 13:40 e2guardian
4 -rw----- 1 root root 158 Nov 2 09:47 squid
4 -rw----- 1 root root 1903 Nov 1 13:19 privoxy
```



Dashboard Configure

Command Line Interface

This page allows you to configure custom shell commands which can be easily invoked from the web interface.




Description	Command	Custom arguments	Public access
A short textual description of the configured command	Command line to execute	Allow the user to provide additional command line arguments	Allow executing the command and downloading its output without prior authentication
<input type="text"/>	<input type="text" value="ls -alst /etc/config/"/>	<input type="checkbox"/>	<input type="checkbox"/> <input type="button" value="Delete"/>
<input type="button" value="Add"/>			
<input type="button" value="Save & Apply"/> <input type="button" value="Save"/> <input type="button" value="Reset"/>			

Shield v1.0 SP1-1118



Interfaces

Interface Overview

Network	Status	Actions
<p>BLOCKDOMAIN</p>  <p>br-lan</p>	<p>Uptime: 3h 45m 7s MAC-Address: 2C:26:5F:80:0B:B5 RX: 1.31 GB (1408667 Pkts.) TX: 315.23 MB (575965 Pkts.) IPv4: 10.10.10.10/24, 10.10.10.11/24 IPv6: FD47:1AB7:5B77::1/60</p>	<p>Connect Stop Edit Delete</p>
<p>LAN</p>  <p>br-lan</p>	<p>Uptime: 3h 45m 7s MAC-Address: 2C:26:5F:80:0B:B5 RX: 1.31 GB (1408667 Pkts.) TX: 315.23 MB (575965 Pkts.) IPv4: 10.10.10.10/24, 10.10.10.11/24 IPv6: FD47:1AB7:5B77::1/60</p>	<p>Connect Stop Edit Delete</p>
<p>WAN</p>  <p>eth0</p>	<p>Uptime: 3h 45m 6s MAC-Address: 00:00:00:00:00:00 RX: 328.79 MB (754237 Pkts.) TX: 1.32 GB (1376401 Pkts.) IPv4: 24.4.200.215/23</p>	<p>Connect Stop Edit Delete</p>

Interfaces

This tab can be used to manage the network configuration of the Shield appliance. In general, the Shield has been preconfigured with an appropriate policy such that this should not be necessary. For power users looking to customize their Shield's networks configuration, this menu provides many powerful options. Configuration will vary with mode of operation. VLANs can be configured here but that is outside the scope of this document.

Warning – Misconfiguring something here could lock you out of your Shield and require a factory reset to recover. It is generally recommended that you not change any of these settings.

BLOCKDOMAIN – This is used by the web filtering system; if this interface is changed or disabled, the web filter may not function correctly.

In Router mode...

The LAN interface is a bridge between eth1 and eth2 with static IP of 10.10.10.10 (default) and DHCP server running for the 10.10.10.0/24 subnet.

The WAN interface is a DHCP client tied to eth0.

In Bridge Mode...

The LAN interface is a bridge running over eth1 with a dynamic DHCP client address. Once Shield has received the address, it is automatically changed to the .111 IP of your local subnet.


The WAN interface consists of two unmanaged interfaces, eth0 and eth2. The bridge is established automatically in software (Snort) rather than using the network configuration menu.



Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

Status  **Uptime:** 6h 22m 7s
 br-lan **MAC-Address:** 2C:28:5F:80:0B:B5
RX: 1.43 GB (1712999 Pkts.)
TX: 701.36 MB (951501 Pkts.)
IPv4: 10.10.10.10/24, 10.10.10.11/24
IPv6: FD47:1AB7:5B77::1/60

Protocol

IPv4 address

IPv4 netmask

IPv4 gateway

IPv4 broadcast

Use custom DNS servers

IPv6 assignment length
Assign a part of given length of every public

IPv6 assignment hint
Assign prefix parts using this hexadecimal su

DHCP Server

Ignore interface Disable DHCP for this interface.

Start
Lowest leased address as offset from the network address.

Limit
Maximum number of leased addresses.

Interfaces -- General Setup

From here you can configure the interface's IP address and the protocol used to obtain it. For example, an interface can be set to have a Static Address, Unmanaged, DHCP Client, or Relay Bridge.

To change between the various options, use the protocol drop down menu then click the 'switch protocol' button.

Based on the configured setting, different options will become available for customizing.

Click Save & Apply to commit changes.

DHCP Server

Depending on the configured mode, a DHCP Server may be enabled by default. To disable, check the 'Ignore Interface' box.



WAN BLOCKDOMAIN LAN

Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

General Setup Advanced Settings Physical Settings Firewall Settings

Bring up on boot

Use builtin IPv6-management

Override MAC address

Override MTU

Use gateway metric

Interfaces - Advanced Settings
From here you can specify if the interface should use IPv6 and/or be brought up at power on.



WAN BLOCKDOMAIN LAN

Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

General Setup Advanced Settings Physical Settings Firewall Settings

Bridge interfaces creates a bridge over specified interface(s)

Enable STP Enables the Spanning Tree Protocol on this bridge

- Ethernet Adapter: "eth0" (wan)
- Ethernet Adapter: "eth1" (lan)
- Ethernet Adapter: "eth2" (lan)
- Ethernet Adapter: "eth3"
- Ethernet Adapter: "gretap0"
- Ethernet Adapter: "ip6gre0"
- Ethernet Adapter: "ip6tln0"
- Ethernet Adapter: "loop0"
- Ethernet Adapter: "loop1"
- Ethernet Adapter: "loop2"
- Ethernet Adapter: "loop3"
- Ethernet Adapter: "npi0"
- Ethernet Adapter: "npi1"
- Ethernet Adapter: "npi2"
- Ethernet Adapter: "npi3"
- Ethernet Adapter: "tunl0"
- Custom Interface:

Interfaces - Physical Settings
Use this tab to apply the logical interface configuration to the physical interface (or software interface). In general, the 3 interfaces that are used here are eth0, eth1, and eth2. A bridge over multiple interfaces may also be configured here (as shown).




Interfaces - LAN

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

Create / Assign firewall-zone

- lan: lan:  
- wan: wan:  
- unspecified -or- create:

 Choose the firewall zone you want to assign to this interface. Select *unspecified* to remove the interface from the associated zone or fill out the *create* field to define a new zone and attach the interface to it.

Interfaces — *Firewall Settings*

From firewall zones can be tied to the interface. The interface will inherit the specified zone's policy.



DHCP and DNS

Dnsmasq is a combined DHCP-Server and DNS-Forwarder for NAT firewalls

Server Settings

- General Settings
- Resolv and Hosts Files
- Advanced Settings

Domain required Don't forward DNS-Requests without DNS-Name

Authoritative This is the only DHCP in the local network

Local server
Local domain specification. Names matching this domain are never

Local domain
Local domain suffix appended to DHCP names and hosts file entries

Log queries Write received DNS requests to syslog

DNS forwardings
List of DNS servers to forward requests to

Rebind protection Discard upstream RFC1918 responses

Allow localhost Allow upstream responses in the 127.0.0.0/8 range, e.g. for RBL

Domain whitelist
List of domains to allow RFC1918 responses for

DHCP and DNS

General Settings

These settings are generally not needed but may be useful to power users. The current DHCP lease table is displayed at the bottom of the page.

Resolv & Host Files

Custom hostfiles can be uploaded to Shield and added from this tab.

Advanced Settings

These settings are generally not needed but may be useful to some power users.

Active DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
android-2d37f459722c581f	10.10.10.251	58:a2:b5:9c:33:00	10h 43m 3s
Amanys-iPhone	10.10.10.125	08:33:4b:26:77:65	11h 5m 55s
android-fd9f2a33168cb0ca	10.10.10.176	34:fc:ef:04:3d:d5	10h 33m 21s
android-a2f4a062bafc3b40	10.10.10.228	1c:b7:2c:07:93:3e	8h 15m 32s
XboxOne	10.10.10.139	50:1a:c5:7a:59:17	7h 1m 4s
02AA01AC411306XT	10.10.10.253	18:b4:30:0b:b4:de	6h 51m 5s
Ayoub	10.10.10.137	8c:70:5a:84:8a:18	11h 9m 33s

Hostnames

Host entries

Hostname	IP address	
<input type="text"/>	<input type="text"/>	<input type="button" value="Delete"/>

Hostnames

Shield will attempt to automatically retrieve the hostname for devices on the networks. This page can be used to add specific entries for each device on the network.

Shield v1.0 SP1-1118

Routes

Routes specify over which interface and gateway a certain host or network can be reached.

Static IPv4 Routes

Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric	MTU	
wan	<input type="text"/>	255.255.255.255	<input type="text"/>	0	1500	<input type="button" value="Delete"/>

Static IPv6 Routes

Interface	Target	Metric	MTU
	<input type="text"/>		

This section contains no values yet

Static Routes

From here you can specify static routes used by Shield. In general these settings are only needed for advanced operation.

Shield v1.0 SP1-1118



Diagnostics

Network Utilities

<input type="text" value="itusnetworks.com"/>	<input type="text" value="itusnetworks.com"/>	<input type="text" value="itusnetworks.com"/>
IPv4 ▾ <input type="button" value="Ping"/>	<input type="button" value="Traceroute"/>	<input type="button" value="Nslookup"/>

Install iptutils-traceroute6 for IPv6 traceroute

```
PING itusnetworks.com (104.28.29.29): 56 data bytes
64 bytes from 104.28.29.29: seq=0 ttl=54 time=9.906 ms
64 bytes from 104.28.29.29: seq=1 ttl=54 time=10.696 ms
64 bytes from 104.28.29.29: seq=2 ttl=54 time=18.438 ms
64 bytes from 104.28.29.29: seq=3 ttl=54 time=11.798 ms
64 bytes from 104.28.29.29: seq=4 ttl=54 time=10.486 ms

--- itusnetworks.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 9.906/12.265/18.438 ms
```

Diagnostics

This page can be used to test connectivity and network operation.



Firewall - Zone Settings

The firewall creates zones over your network interfaces to control network traffic flow.

General Settings

Enable SYN-flood protection

Drop invalid packets

Input: accept

Output: accept

Forward: drop

Zones

Zone → Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan: lan: → wan	accept	accept	accept	<input type="checkbox"/>	<input type="checkbox"/>	Edit Delete
wan: wan: → DROP	drop	accept	drop	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Edit Delete

[Add](#)

[Save & Apply](#) [Save](#) [Reset](#)

Firewall -- General Settings

This page can be used to configure high level policies between the various firewall zones. By default, Shield has been configured with a policy that is acceptable for most small networks.

Firewall - Port Forwards

Port forwarding allows remote computers on the Internet to connect to a specific computer or service within the private LAN.

Port Forwards

Name	Match	Forward to	Enable	Sort
Itusfilter	IPv4-TCP From any host in lan Via IP 10.10.10.11 at port 80	IP 10.10.10.11, port 88 in any zone	<input checked="" type="checkbox"/>	<input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
all-dns-to-itus	IPv4-TCP, UDP From any host in lan Via IP range 10.10.10.0/24 at port 53	IP 10.10.10.10, port 53 in any zone	<input checked="" type="checkbox"/>	<input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>
SlingBox	IPv4-TCP, UDP From any host in wan Via any router IP at port 5001	IP 10.10.10.254, port 5001 in lan	<input checked="" type="checkbox"/>	<input type="button" value="↑"/> <input type="button" value="↓"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

New port forward:

Name	Protocol	External zone	External port	Internal zone	Internal IP address	Internal port
<input type="text" value="New port forward"/>	TCP+UDP	WE	<input type="text"/>	lan	<input type="text"/>	<input type="text"/>

Firewall -- Port Forwards

From here you can configure port forwarding for your Shield. Enter a name for the rule, selecting the protocol, entering the port, external zone, internal zone, internal ip address, and internal port number. Port forwarding is useful for enabling services which may need access from the WAN or to redirect traffic from specific ports.

By default there are entries listed here for the Shield's web filtering system. Do not modify these or it may impact the web filters functionality. Additionally be cautious in using port forwarding as this may result in opening a hole in the firewall from the WAN.

Firewall - Traffic Rules

Traffic rules define policies for packets traveling between different zones, for example to reject traffic between certain hosts or to open WAN ports on the router.

Traffic Rules

Name	Match	Action	Enable	Sort
Allow-DHCP-Renew	IPv4-UDP From <i>any host in wan</i> To <i>any router IP</i> at port 68 on <i>this device</i>	Accept input	<input checked="" type="checkbox"/>	<input type="button" value="Up"/> <input type="button" value="Down"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

Firewall - Traffic Rules

This is one of the most powerful screens in the firewall configuration menus. From here you can enable / disable existing rules, change the order in which rules take effect. Open ports on the firewall, add forwarding rules, and define source NAT rules.

Warning Rules entered manually via the CLI using iptables will not appear in the menu on this page but will be used by Shield.

Open ports on router:

Name	Protocol	External port
<input type="text" value="New input rule"/>	TCP+UDP	<input type="text"/>

New forward rule:

Name	Source zone	Destination zone
<input type="text" value="New forward rule"/>	lan	wan

Source NAT

Source NAT is a specific form of masquerading which allows fine grained control over the source IP used by addresses to internal subnets.

Name	Match
This section contains no values yet	

New source NAT:

Name	Source zone	Destination zone	To source IP	To source port
<input type="text" value="New SNAT rule"/>	lan	wan	- Please ch	Do not rewrite



P2P-Block

P2P-Block is a greylisting mechanism to block various peer-to-peer protocols for non-whitelisted clients.

Settings

Enable P2P-Block

Portrange

Block Time seconds

Whitelisted IPs

Layer7-Protocols

- AIM Chat
- Bittorrent
- eDonkey, eMule, Kademia
- Fasttrack Protocol
- File Transfer Protocol
- Gnutella
- Hypertext Transfer Protocol
- Ident Protocol
- Internet Relay Chat
- Jabber/XMPP
- MSN Messenger
- Network Time Protocol
- POP3 Protocol
- SMTP Protocol
- SSL Protocol
- VNC Protocol

IP-P2P

- eDonkey, eMule, Kademia
- KaZaA, FastTrack
- Gnutella
- Direct Connect
- BitTorrent, extended BT
- AppleJuice
- WinMX
- SoulSeek

Firewall – P2P Block

The P2P Block page adds preliminary support for layer7 filtering. This feature is still considered experimental at this time. To enable the filter, simply click the ‘Enable P2P-Block’ box, select the protocols you’d like blocked, then click Save & Apply. Rules should automatically be added to the firewall to block packets matching the L7 data used by these protocols. More protocols are available via CLI than shown in GUI.

Additional protocols can be found here </etc/l7-protocols/protocols>

This feature can be expanded in the future to also support detecting malware.



Firewall - IPS Redirect

Custom rules allow you to execute arbitrary iptables commands which are not otherwise covered by the firewall framework. The commands are executed after each firewall restart, right after the default ruleset has been loaded.

```
# This file is interpreted as shell script.
# Put your custom Snort iptables rules here

iptables -I FORWARD -j NFQUEUE --queue-balance 7:8 --queue-cpu-fanout # Snort IPv4
ip6tables -I FORWARD -j NFQUEUE --queue-balance 7:8 --queue-cpu-fanout # Snort IPv6

# iptables -t nat -I PREROUTING -p TCP --dport 443 -j REDIRECT --to-port 1337 # SSL Decryption (experimental)

iptables -I FORWARD -m geoip --src-cc CN,RU -j DROP # GeoIP Filter from China & Russia
iptables -I FORWARD -m geoip --dst-cc CN,RU -j DROP # GeoIP Filter to China & Russia
```

Firewall – Custom Rules

Rules entered here should be in iptables format. Whenever the firewall is reset, these rules will automatically be added.

By default there are several rules are included here. Do not remove these as they are needed for redirecting traffic to the IPS.

From here Geographical IP blocking can also be added via custom iptables rules. By default, traffic going to and coming from Russia and China are blocked by Shield.

Adding a ‘#’ to the front of any line will comment out the rule.

Submit

Reset

Shield v1.0 SP1-1118



Smart Queue Management

With SQM you can enable traffic shaping, better mixing (Fair Queuing), active queue length management (AQM) and prioritisation on one network interface.

Queues

Delete

Basic Settings

Queue Discipline

Link Layer Adaption

Enable

Interface name

Download speed (kbit/s) (ingress) set to 0 to selectively disable ingress shaping:

Upload speed (kbit/s) (egress) set to 0 to selectively disable egress shaping:

Add

Save & Apply

Save

Reset

Shield v1.0 SP1-1118

Smart Queue Management

The SQM feature can be used to configure basic quality of service for the Shield. **This feature is still considered experimental.**

To enable SQM, click the 'enable' box, select the interface you'd like it applied to (usually the WAN) then enter the download and upload speed.

This feature may help reduce bufferbloat.



Smart Queue Management

With SQM you can enable traffic shaping, better mixing (Fair Queueing), active queue length management (AQM) and prioritisation on one network interface.

Queues

Delete

Basic Settings

Queue Discipline

Link Layer Adaptation

Queueing discipline: fq_codel (default) ▼

Queue setup script: simple.qos ▼



simple_pppoe.qos:

BW-limited three-tier prioritisation scheme with fq_codel on each queue. Temporary version to implement shaping of pass through PPPoE encapsulated packets.

simplest.qos:

Simplest possible configuration: HTB rate limiter with your qdisc attached.

simple.qos:

BW-limited three-tier prioritisation scheme with fq_codel on each queue. (default)

Show and Use Advanced Configuration

Add

Save & Apply

Save

Reset

Shield v1.0 SP1-1118

Smart Queue Management

Queue Discipline

The queueing discipline is the algorithm used for balancing network traffic. In general it is safe to test different settings here until finding one that works best. The best algorithm will depend on the characteristics of your own network. In general, the default values work well.

Router Mode Tips

Best way to setup router mode

- 1) Connect eth0 to modem
- 2) Connect eth2 to router's wan port
- 3) power on all 3 devices

Use Case 1:

The user boots up or restarts the Shield with only eth2 active.

Topology:

Modem <-> Shield <-> Router/AP/Switch/Computer

Problem:

The device connected to eth2 will not get an ip address.

Solution:

Router/AP/Switch

Eth2 will not serve a DHCP address unless eth0 has first been initialized. This is a known issue which typically only occurs if Shield is powered on with nothing connected to eth0

Windows

- 1) Click the Window Start button
- 2) Go to Control Panel
- 3) Click "View networks status and task"
- 4) Click "Change adapter settings"
- 5) Right click local area connection
- 6) Click disable
- 7) Right click local area connection
- 8) Click enable

Linux & OS X

- 1) Open a Terminal
- 2) `ifconfig <iface> down`
- 3) wait about 60 seconds
- 4) `ifconfig <iface> up`

Gateway Mode Tips

Best way to setup gateway mode

- 1) Connect eth0 to gateway
- 2) power on Shield

Use Case 1:

Gateway mode is considered experimental and is generally not recommended for use in production environments..

Topology:

Gateway Router/AP/Switch <-> Shield

Problem:

Not all traffic is not being inspected by Shield

Solution:

Due to the nature of how Gateway mode operates, it may not be 100% effective in capturing all network traffic as an inline configuration. In general, Bridge or Router mode should be used for production environments requiring 100% inspection.

Bridge Mode Tips

Best way to setup bridge mode

- 1) Connect eth0 to modem
- 2) Connect eth1 to router's lan port
- 3) Wait three minutes
- 4) Connect eth2 to router's wan port

Use Case 1:

The user boots up or restarts the Shield with all three ports connected.

Topology:

Modem <-> Shield <-> Router/AP/Switch/Computer

Problem:

The device connected to eth2 will not get an ip address.

Solution:

Router/AP/Switch

Unplug eth2 for about 1 minute 20 seconds then reconnect cable.

When eth2 is disconnected an alert is triggered in the OS that tells Snort to restart. While Snort is reloading eth2 will be inactive after about 1 minute 30 seconds.

Windows

- 1) Click the Window Start button
- 2) Go to Control Panel
- 3) Click "View networks status and task"
- 4) Click "Change adapter settings"
- 5) Right click local area connection
- 6) Click disable
- 7) Right click local area connection
- 8) Click enable

Linux & OS X

- 1) Open a Terminal
- 2) `ifconfig <iface> down`
- 3) wait about 60 seconds
- 4) `ifconfig <iface> up`

Use Case 2:

The user follows the instructions on the bottom of the Shield and connects eth1 to a modem/gateway, but can't access x.x.x.111.

Topology:

Modem <-> [eth1]Shield

Problem:

eth1 will stay inactive until eth0 is connected.

Solution:

Connect eth0 to modem and eth1 will immediately receive an ip address. Then wait about 3 minutes and connect eth2.