PIKA µFirewall User Guide

Version 1.1 July 2014

Introduction

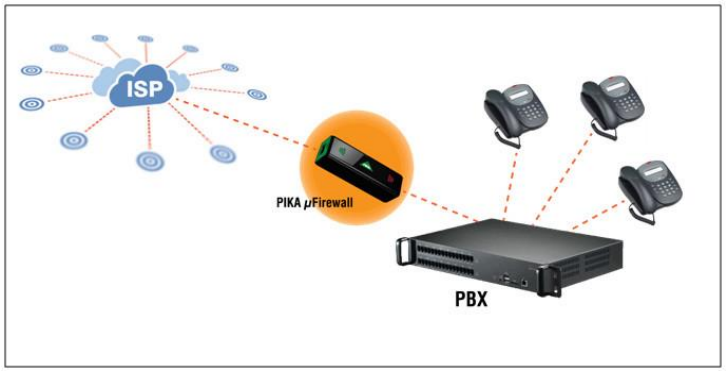
The PIKA µFirewall is an innovative tool designed to protect against VoIP-based network attacks. µFirewall has no IP address allowing it to appear "invisible" and making it virtually impossible to detect or interact with. The device utilizes a low latency processor to process packets at close to wire speed while protecting against many common VoIP attacks (*). Such attacks include SIP Denial of Service (DoS), theft of service and user account probes from malicious attack scripts like SIPVicious, VoIPER or SiVus.

Installation

PIKA µFirewall is easily installed at your location, requires no special skills and absolutely no configuration. The device comes with a standard USB power cable that plugs into either of the USB ports located on either end of the device. The device is inserted directly in front of your existing telephone system with no specific direction in which the device must be inserted. Plug the RJ-45 cable coming from the WAN/ISP into either side of the µFirewall and plug another RJ-45 into the other side terminating on the local PBX WAN input.

For a video of the µFirewall installation process, see our Youtube channel: Installation Video

⚠ It is important that PIKA µFirewall is the first device to terminate ahead of the PBX WAN connection.



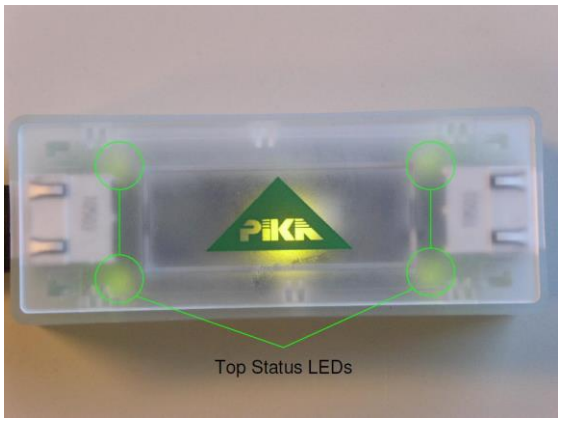
Once booted, the green and orange LED's associated with the physical network ports will become active and the four internal green LEDs will light up solid to indicate that the firewall is active.

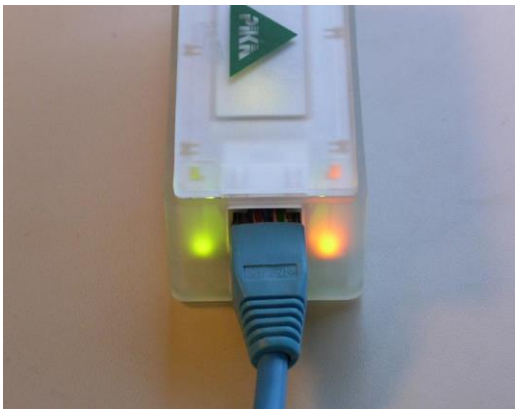
LED Indicators

PIKA µFirewall has several LEDs used to indicate both physical network connection status and Firewall application status.

A. **Status:** (red/green) four on top and four on bottom of case.

B. **Network Activity:** (green and orange) left and right of the network interface connectors.
Table 1 LED Indicator Meanings describes the various LED indications.





LED	Colour	State	Description
Status		Solid red	An IP address has been blocked and SIP requests from the entity are being dropped for the allotted timeframe.
Status		Blinking red, fast (¼ second)	A SIP entity has sent unauthenticated request to 5 or more user accounts
Status		Blinking red, slow (½ second)	Authentication has failed for a specific user account 3 or more times in a row.
Status		Solid	Firewall application is active (if no USB stick installed)
Status		Blinking green (1 second on / 1 off)	USB memory key is inserted and has been detected.
Status		Blinking green (¼ second on / ¼ off)	USB memory key files are being processed.
Network		Solid green and blinking orange, based on network traffic	On each side of both network interface connectors is a green LED to indicate physical connection status and an orange LED to indicate network activity.

Table 1 LED Indicator Meanings

Advanced Device Operations

Using a USB Stick

The PIKA µFirewall supports an external FAT32 formatted USB stick which can be used to read and update firmware versions, customize behaviour, program black lists and to extract firmware version and logging and statistical information from the unit.

When using the USB stick to update **configuration** and **black list** information, read **logs** and **firmware version**, the µFirewall will indicate that it is updating and processing the internal files by flashing the green LED's on/off at a ¼ second interval.
You will know the update has completed when the green LEDs flash rate slows to a 1 second interval indicating the USB stick is being accessed. See **Table 1 LED Indicator Meanings**
The time required for this process varies depending on the size of the log files, typically 30-60 seconds.

When using the USB stick to **update firmware**, refer to section "Updating Firmware" for specific details.

Operating notes on using the USB Stick

a) If the USB stick is inserted before the VoIP Firewall has booted it will prevent the pkvsf logs from being created.

b) If a *.bin firmware file is present on the USB stick no logs will be generated.

c) Each time the USB stick is inserted it will update the "PIKA VoIP Firewall Statistics" section of the **pkvsf** log file as highlighted in the "***Statistical Analysis – Reading Log files"*** section of this manual.

d) The USB logging mechanism will contain one active logging session only.
If you want to preserve logs, copy them to a computer before re-insertion of the USB stick.

e) The unit itself has enough internal storage for about 2 days of logging before overwriting logs, however, the "PIKA VoIP Firewall Statistics" section of the **pkvsf** log file is always preserved.

All this considered, normally the USB stick would be inserted into a unit which has been running for while.
The resulting pkvsf log file will contain Protection Summary chart (ie. 'PIKA VoIP Firewall Statistics').
In most cases, this is all that is required by users.

Reading Firmware version

The µFirewall firmware version is obtained from the USB stick by reading the file named **\uWARP\uwarp-version.txt** .

Updating Firmware

Upgrade of the µFirewall firmware is manually updated with a copy of the firmware on a FAT32 formatted USB stick. The firmware can be downloaded from the following link - uFirewall Firmware Update. Copy this firmware file to the root folder of the USB stick. Power on the µFirewall and wait until all the green LEDs light up. Insert the USB stick into the free USB port on the device. The upgrade can take some time so please be patient. The lights will blink when the USB is inserted. After approximately 2 minutes, the lights will go dark as the unit reboots and then the lights will light back up again. You should leave the USB stick in the µFirewall at this point. After approximately 30 seconds you should see the RED/GREEN LEDs blink back and forth to confirm the upgrade is completed. Once the LEDs go solid GREEN, you can remove the USB stick.

A demonstration of this upgrade procedure can be seen on the PIKA Technologies YouTube channel.

Customizing Device Behaviour

Although not necessary, the µFirewall behaviour can be customized through a USB stick containing a configuration file called **pkvsf.conf** .
Default operation of the device can be customized by adding logging and application configuration parameters to this file and place it in the root directory of any FAT32 formatted USB stick. Inserting this stick into either USB port on the µFirewall will read any of the parameters described here and automatically apply any changes. Once set, parameters are persistent until changed again.

Note:
If a logging parameter is not present the default is used.
If a configuration parameter is not present, the current setting will be preserved, and will not revert to the default.

It is important to ensure that proper syntax rules are followed when creating the pkvsf.conf configuration file. The '#' character signifies that the remaining text is merely a comment of the creator. Parameter definitions must follow the format '<parameter>=<value>;'.
For example:

```
# Pika VoIP Stealth Firewall Configuration File

# user settings
user_max_failure=9;
user_block_duration=300;
user_block_not_registered=false;

# saddr settings
saddr_max_failure=10;
saddr_block_duration=1800;
```

Configuring Firewall Parameters

The behaviour of the firewall is customized using the following parameters in **pkvsf.conf :**

Parameter	Description	Default	Maximum
user_max_failure	Maximum number of failed authentication attempts allowed. All further requests from this entity will remained blocked for the number of seconds assigned to the 'user_block_duration' parameter.	9	
user_block_duration	Length in seconds that SIP requests will be blocked when 'user_max_failure' detection has occurred on a specific SIP entity.	300	214,000,000
user_block_not_registered	When 'true' µFirewall will drop all SIP Invite requests from any SIP entity that has not registered successfully. Using False is strongly recommended!	False	
saddr_max_failure	The number of times the µFirewall will allow a SIP entity to send account probing SIP Requests without successful registration attempt	10	
saddr_block_duration	Length in seconds that SIP requests will be blocked when 'saddr_max_failure' detection has been triggered against a specific SIP entity.	1800	214,000,000

Refer to the section "**Using a USB Stick"** for details about how to update the µFirewall through USB.

Creating Blacklisted Address Lists

A list of black listed IP addresses can be added to µFirewall. When an address is blacklisted all received SIP requests from this source address will be intercepted and dropped. A blacklist may be added by creating a complete list of IP addresses to a file called **vabl.txt** , placed in the root directory of a FAT32 formatted USB stick.
Syntax is shown in the following example:

```
85.17.30.17
86.57.69.110
95.76.64.12
97.78.67.68
207.107.229.2
```

Refer to the section "**Using a USB Stick"** for details about how to update the µFirewall through USB.

This blacklist will remain persistent after a reboot and may only be changed by adding a new vabl.txt via USB stick.

Configuring Logging Parameters

The logging verbosity, file size and length are all configurable using the following parameters in a file on the USB sick named **pkvsf.conf** :

parameter	description	Value	default
log_level*	Determines the logging verbosity level while logging to the USB stick. As the level increases it also includes all logs from the previous log level in addition to the current level value.	0 – Emergency – the system is unusable. 1 – Alert logs – action must be taken immediately 2 – Critical – critical condition encountered 3 – Error – Error condition encountered 4 – Warning – Warning condition encountered 5 – Notice – Normal but significant event encountered 6 – Informational – Informational messaging. 7 – Debug – Designer level debug messaging.	4
log_max_filesize	Determines the maximum log file size in bytes.		1000000
log_max_numfiles	Determines the maximum number of log files that will be collected on the USB stick. When the maximum size is reached on the maximum number of files the oldest file will be overwritten.		2
pcap_tracing	Setting this parameter to 'true' the µFirewall will begin capturing a Wireshark type trace dump on the USB stick. All TCP/IP packets that pass through the µFirewall will be captured to a file on the USB stick called **pkvsf_<ddmmyyyy_X>.pcap** . The rules outlined by '**log_max_filesize'** and '**log_max_numfiles'** also apply to this parameter and the file(s) it generates.		false

** When increasing log_level it is important to consider the current call traffic level as significant logging may affect overall performance*

Refer to the section "**Using a USB Stick"** for details about how to update the µFirewall through USB.

Gathering Logs and Statistical Analysis

µFirewall logs are gathered by inserting a (FAT32 formatted) USB memory stick into either of the µFirewall USB ports. Upon insertion, the four onboard LEDs will flash green indicating the µFirewall is accessing the memory stick. The **\uWARP\logfiles** folder will be created under the root folder of the memory stick and is intended to store runtime logs currently on the µFirewall. The runtime log and version log files are:

\uWARP\pkvsf_<ddmmyyyy>_<X>.log - contains all warnings and errors logged by the firewall application
\uWARP\logfiles\uwarp-version.txt – contains the firmware version of the unit.

Other log files are created on the USB stick for use by PIKA Technical Support department.

NOTE: In the file names, <ddmmyyyy> refers to day, month and year and <X> is a three digit file index number.

Please note there is a known issue which sometimes results in Jan 1, 1970 set as the time in the logs. PIKA intends to address this in future revisions

Gathering updated configuration and statistical information from the µFirewall requires removal and re-insertion of the USB stick

Refer to the section "**Using a USB Stick"** for details about how to update the µFirewall through USB.

Reading Log files

The **pkvsf** runtime log will contain configuration and statistical information at the beginning of the first log file generated on insertion of a USB stick.

Note for best results in displaying log files use a plain text editor.
MS NOTEPAD will not display logs correctly.

The following depicts an actual pkvsf log file:

```
pkvsf v1.1.1.4 (Apr 25 2013 16:54:44)
Log File (created on: Thu Jan  1 00:00:25 1970)

Jan  1 00:00:25.162: -- Current config after USB triggered update --
Jan  1 00:00:25.215:    [log_level] = [-1]
Jan  1 00:00:25.215:    [log_max_filesize] = [-1]
Jan  1 00:00:25.215:    [log_max_numfiles] = [-1]
Jan  1 00:00:25.215:    [pcap_tracing] = [false]
Jan  1 00:00:25.216:    [user_max_failure] = [9]
Jan  1 00:00:25.216:    [user_block_duration] = [300]
Jan  1 00:00:25.216:    [user_block_not_registered] = [false]
Jan  1 00:00:25.216:    [saddr_max_failure] = [250]
Jan  1 00:00:25.216:    [saddr_block_duration] = [1800]
Jan  1 00:00:25.217: interface [eth0] has MAC address [00:1e:84:00:11:22]
Jan  1 00:00:25.218: interface [eth1] has MAC address [00:1e:84:00:22:11]
Jan  1 00:00:25.220: |-------------------------------------------------------------------------|
Jan  1 00:00:25.220: |                 PIKA VoIP Firewall Statistics                           |
Jan  1 00:00:25.220: |-------------------------------------------------------------------------|
Jan  1 00:00:25.220: |       useragent | dropped                                               |
Jan  1 00:00:25.220: |-------------------------------------------------------------------------|
Jan  1 00:00:25.221: |friendly-scanner |       0                                               |
Jan  1 00:00:25.221: |          VoIPER |       0                                               |
Jan  1 00:00:25.222: |   SIVuS scanner |       0                                               |
Jan  1 00:00:25.222: |-------------------------------------------------------------------------|
Jan  1 00:00:25.222: | Total user agent items     3                                            |
Jan  1 00:00:25.222: |-------------------------------------------------------------------------|
Jan  1 00:00:25.222: |-------------------------------------------------------------------------|
Jan  1 00:00:25.222: |            user | dropped | failure | total failure | total success |
Jan  1 00:00:25.223: |-------------------------------------------------------------------------|
Jan  1 00:00:25.222: |            1000 |       0 |       0 |             0 |             2 |
Jan  1 00:00:25.222: |            1001 |      17 |       6 |             6 |             0 |
Jan  1 00:00:25.222: |            1006 |       0 |       0 |             3 |            10 |
Jan  1 00:00:25.223: |-------------------------------------------------------------------------|
Jan  1 00:00:25.223: | Total user items     3                                                  |
Jan  1 00:00:25.223: |-------------------------------------------------------------------------|
Jan  1 00:00:25.223: |-------------------------------------------------------------------------|
Jan  1 00:00:25.224: |           saddr | dropped | failure | total failure | total success |
Jan  1 00:00:25.224: |-------------------------------------------------------------------------|
Jan  1 00:00:25.224: |   192.168.68.44 |       0 |       0 |             0 |             0 |
Jan  1 00:00:25.224: |    192.168.68.6 |      36 |      10 |             0 |             0 |
Jan  1 00:00:25.224: |     85.17.30.17 |     123 |      bl |            bl |            bl |
Jan  1 00:00:25.224: |    95.230.40.30 |       0 |      bl |            bl |            bl |
Jan  1 00:00:25.224: |    97.132.23.21 |       0 |      bl |            bl |            bl |
Jan  1 00:00:25.224: |-------------------------------------------------------------------------|
Jan  1 00:00:25.224: | Total saddr items     5                                                 |
Jan  1 00:00:25.224: |-------------------------------------------------------------------------|
```

Figure 1 Sample pkvsf Log File

The **"Current config after USB triggered update"** section represents current configuration parameter settings (see *Firewall Behaviour Customization*).

The next two lines indicating the **MAC addresses** assigned to both eth0 and eth1 on the device.

The **"PIKA VoIP Firewall Statistics"** section provides an overview for both system attack and active user status in three groupings **user agent**, **user** and **saddr**.

User agent group

The "**user agent"** group contains counters for detections of various common malicious attack scripts ("SIP auditing tools") such as friendly-scanner, VoIPER and SIVus scanner. Incoming packets are checked for attributes associated with these tools and, if found, will be dropped. Dropped packets will result in the appropriate tool counter being incremented and the red LEDs being lit (see Table 1 - LED Indicator Meanings for details).

User group

The "**user"** group identifies all SIP user accounts that are actively registered as well as any attempts on an account that failed authentication. Multiple failed authentication attempts for a specific account will result in the authenticating device being blocked for a period of time. The µFirewall's red LED's will be lit to indicate that packets are being dropped. Each time an authentication request is dropped, a log will be appended in the **'pkvsf'** log file. For example:

Jan 1 00:05:35.051: [callid:NmIxMDQ3YTFjMzY2OTY1MmFkM2IzNzhlMzg5MTA4NDI.] User 1000 not allowed, drop packet

Saddr group

The "**saddr"** group identifies all blacklisted IP addresses and any IP address identified as the source of a SIP signalling request. A blacklisted IP address entry may be identified by having the **'bl'** designation in the 'failure', 'total failure' and 'total success' columns.

All SIP requests received from a source address identified as a black listed address will be dropped and the red LEDs are lit to reflect this. The columns associated with each group contain the following information:

dropped - This column reflects the number of dropped SIP packets dropped form a specific source after having been blocked.

failure - This column indicates the number of concurrent failures that have taken place against the user account or address. If the entity is successful prior to being blocked this count will be reset to zero.

total failure – This is a running count of all failures against a particular user account or IP address.

total success – This column applies only to the group '**user**' and indicates the number times the account was successfully authenticated.

Disclaimer

This device is not a replacement (nor compensates) for PBX Security Best Practices. Your PBX should be protected by a data firewall and secure passwords should be used.

Frequently Asked Questions

Q: What will happen if the unit losses power?
A: If the unit loses power, no network traffic will be passed through the µFirewall and the PBX behind the device is then no longer able to make or receive calls. It is recommended that the µFirewall is powered from the same UPS (Uninterruptable Power Supply) as the PBX to ensure continuous power.

Q: Where does the power cord connect?
A: The power cord connects to either USB port located at the end of the µFirewall.

Q: How do I know if the µFirewall is functioning?
A: The µFirewall green network interface LED's will be solid and both orange LED's will blink to indicate network traffic. The four internal green LED's will be solid indicating the firewall application is operational.

Q: Does it matter which µFirewall network interface connects to the WAN?
A: No. µFirewall is bi-directional. The WAN and PBX/Call Server may be connected to either of the two network interface ports.

Q: Where should I physically connect the µFirewall?
A: µFirewall should be connected in series with the PBX/Call Server's uplink to the WAN/ISP.

Q: What will happen if my phone fails authentication more than 9 times?
A: After 9 failed attempts the µFirewall will block all subsequent SIP requests from the phone for 5 minutes. Verify that your username and password is correct and reattempt the registration after the allotted time.

TECHNICAL SUPPORT

PIKA Technical Support can be reached by telephone or email:
Phone: +1-613-591-1555
Email: support@pikatech.com