

µFirewall


Quick Start User Guide

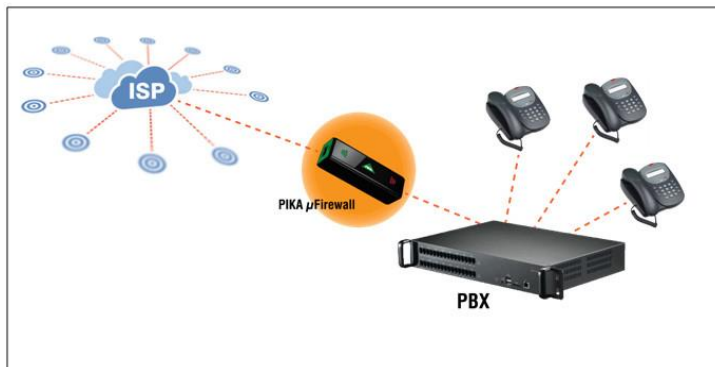


The µFirewall (“µWARP”) is an innovative tool designed to protect against VoIP based network attacks. The µWARP has no IP address allowing it to appear “invisible” and making it virtually impossible to detect or interact with. The device utilizes a low latency processor to process packets at close to 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

The µWARP device 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 µWARP and plug another RJ-45 into the other side terminating on the local PBX WAN input.

 It is important that µWARP 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.

Establish a call from the PBX to a phone on the WAN side of the µWARP. This will allow the µWARP to detect which Ethernet port is connected to the PBX and which is connected to the WAN.



The µWARP must have Internet access in order to operate. This allows the device to periodically verify its authenticity with the PIKA host server and confirm it has not been tampered with.

LED Indications

The µWARP has several LED’s used to indicate both physical network connection status and Firewall application status. Aside from the LED’s (green and orange) left and right of the network interface connections used to indicate network active traffic, there are also red and green LED’s on the main board. Table 1 LED Indicator Meanings describes the various LED indications.








Led	State	Description
	Solid red	An IP address has been blocked and SIP requests from the entity are being dropped for the allotted timeframe.
	Blinking red, fast (¼ second)	A SIP entity has sent unauthenticated request to 5 or more user accounts
	Blinking red, slow (½ second)	Authentication has failed for a specific user account 3 or more times in a row.
	Solid	Firewall application is active.
	Blinking green (1 second on / 1 off)	USB memory key is inserted and has been detected.
	Blinking green (¼ second on / ¼ off)	USB memory key files are being processed.
	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

µFirewall

Quick Start User Guide



Logging and Statistical Analysis

µWARP logs are gathered by inserting a (FAT32 formatted) USB memory stick into either of the µWARP USB ports. Upon insertion, the four onboard LED's will flash green indicating the µWARP is accessing the memory stick. A **logfiles** folder will be created under the root folder of the memory stick and is intended to store runtime logs currently on the µWARP. The runtime logs are:

- **messages** - contains syslog information gathered by the operating system kernel,
- **pkvsf_<ddmmyyyy>_<X>.log** - contains all warnings and errors logged by the firewall application, and
- **pkvqueue_<ddmmyyyy>_<X>.log** - contains information pertaining to an internal queuing mechanism and only relevant to PIKA engineering staff.

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

With the USB key inserted, all runtime logs are written to the root folder of the USB memory stick. Included are the **pkvsf** and **pkvqueue** log files. Additional statistical information will be included within the **pkvsf** log.

Statistical Analysis

The **pkvsf** runtime log will contain configuration and statistical information at the beginning of the first log file generated on insertion of a USB key. Gathering updated configuration and statistical information will require the removal and reinsertion of the USB key. Figure 1 Sample pkvsf Log File depicts an actual pkvsf log file.

The first nine lines represent current configuration parameter settings (see Application Customization) followed by two lines indicating the MAC addresses assigned to both eth0 and eth1 on the device. The remaining statistical information provides an overview for both system attack and active user status. Statistics are separated into three groupings **Audit Tools**, **user** and **saddr**.

The **Audit Tools** group contains counters for various common SIP based auditing tools. 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 LED's being lit.

```
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: |                               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 00:00:25.224: |                               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 |          b1 |          b1 |          b1 |
Jan 1 00:00:25.224: | 95.230.40.30 |          0 |          b1 |          b1 |          b1 |
Jan 1 00:00:25.224: | 97.132.23.21 |          0 |          b1 |          b1 |          b1 |
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 **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 µWARP'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 generated in the 'pkvsf' log file. For example:

Jan 1 00:05:35.051: [callid:NmlxMDQ3YTFjMzY2OTY1MmFkM2IzNzhIMzg5MTA4NDI.] User 1000 not allowed, drop packet

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 'b' 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 LED's 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 from 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.

Logging Configuration Parameters

The logging verbosity, file size and length are all configurable with the use of a configuration file called pkvsf.conf. Add any logging parameters to this file and place it in the root directory of any FAT32 formatted USB stick. Then inserting this stick into either USB port on the µWARP will read any of the following parameters and automatically apply any changes (if a parameter is not present the default is used):

log_level

This parameter determines the logging verbosity level while logging to the USB key. When increasing this level it is important to consider the current call traffic level as significant logging may affect overall performance. There are currently eight levels of verbosity available. 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.
(Parameter default value = 4)

log_max_filesize

This value determines the maximum log file size in bytes.
(Parameter default value = 1000000)

log_max_numfiles

This value determines the maximum number of log files that will be collected on the USB key. When the maximum size is reached on the maximum number of files the oldest file will be overwritten.
(Parameter default value = 2)

pcap_tracing

By setting this parameter to 'true' the µWARP will begin capturing a Wireshark type trace dump on the USB key. All TCP/IP packets that pass through the µWARP will be captured to a file on the USB key 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.
(Parameter default value = false)

Application Configuration Parameters

Although not required the µWARP is customizable behaviorally. This may be accomplished with use of the configuration file called pkvsf.conf.

user_max_failure

When µWARP detects a number of failed authentication attempts equal to the value assigned to this parameter all further attempts from this entity are blocked. All further requests from this entity will remain blocked for the number of seconds assigned to the 'user_block_duration' parameter.
(Parameter default value = 9)

user_block_duration

This parameter specifies the length in seconds that SIP requests will be dropped when 'user_max_failure' detection has occurred on a specific SIP entity.
(Parameter default value = 300)

μFirewall

Quick Start User Guide



user_block_not_registered

When this parameter is set 'true' μWARP will drop all SIP Invite requests from any SIP entity that has not registered successfully.
(Parameter default value = false)

saddr_max_failure

This parameter indicates the number of times the firewall will allow a SIP entity to send account probing SIP Requests without successful registration attempt.
(Parameter default value = 10)

saddr_block_duration

This parameter specifies the length in seconds that SIP requests will be drop when 'saddr_max_failure' detection has been triggered against a specific SIP entity.
(Parameter default value = 1800)

Configuration File Example

It is important to ensure that proper syntactical 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;
```

Blacklisted Addresses

The μWARP also provides the ability to blacklist specific IP addresses. When an address is blacklisted all received SIP requests from this source address will be intercepted and dropped. A blacklist may be added by adding a complete list of IP addresses to a file called **vabl.txt** as follows:

```
85.17.30.17
86.57.69.110
95.76.64.12
```

```
97.78.67.68
207.107.229.2
```

Now place this file in the root directory of a FAT32 formatted USB key and then insert it into either USB port. The μWARP will indicate that it is updating the internal blacklist by flashing the green LED's on/off at a ¼ second interval. You will know the update has completed when the green LED's flash rate regresses to a 1 second interval that indicates the USB stick is being accessed. This blacklist will remain persistent after a reboot and may only be changed by adding a new vabl.txt via USB key.

Future Release Considerations

Future release enhancements include IP address whitelist support and cloud based device management. An administrator would log in to PIKA host server within the cloud and manage all μWARP devices remotely. From the PIKA host server, attack statistics could be viewed, white- and blacklists could be modified, remote firmware updates could be scheduled and various reports could be generated (e.g. call volume).

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 loses power?

A: If the unit loses power, no network traffic will be passed through the μWARP 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 μWARP.

Q: How do I know if the μWARP is functioning?

A: The μWARP 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 μWARP network interface connects to the WAN?

A: No. The μWARP 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 μWARP?

A: The μWARP 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 μWARP 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