

WarpVM - AWS User Guide

# *WarpVM - AWS*

---

## USER GUIDE



Software Version: we-9.9-17331:0046

## WarpVM - AWS Disclosures

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR BADU REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. BADU AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL BADU OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF BADU OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

*WarpEngine*, *WarpGateway*, *WarpVM*, and *WarpTCP* are registered trademarks of Badu Networks and/or its affiliates in the United States and certain other countries.

Badu and the Badu Logo are trademarks of Badu Networks, Inc. and/or its affiliates in the U.S. and other countries. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Badu and any other company. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Screenshots and images in this document may be slightly different than your screens. Depending on the version of *WarpVM* you have installed, and the browsers (and shells) you use, your screen may not perfectly match what is presented in this document. However, every effort has been made to present accurate information in this document.

# User Guide Contents

**WarpVM - AWS Disclosures**

**User Guide Contents**

**Introduction to WarpVM**

**WarpVM System Requirements**

**WarpTCP Theory of Operation**

**Browser Interface & Login**

**WarpVM Operating Modes**

**WarpAdmin: Status Page**

**WarpAdmin: Interfaces Page**

**WarpAdmin: System Page**

**WarpAdmin: Diagnostics**

**Examples of Selective Bypass Rules**

**WarpVM Known Issues**

**Contact Badu Networks**

**WarpVM Warranty Information**

## Introduction to WarpVM

*WarpVM* takes TCP streams arriving at the device, terminates them, and issues a transparent (if SNAT is disabled) stream to the destination. By applying stream termination, the WarpTCP proxy can take over the TCP congestion control on the outbound portion of the terminated stream as well as acting as a better client for the server. The modifications are designed to drive more data and to provide increased throughput without changing the TCP protocol.

The proxy service is designed to be highly available and recovers from unexpected errors or faults rapidly. If the system is configured in bypass mode, the system will allow traffic to flow without termination. Termination is on a per TCP session basis.

The following guide will help you through setup and configuration of the *WarpVM* software.

# WarpVM System Requirements

This document assumes that you have launched an image from the *WarpVM* AMI.

## Requirements:

- Instance type must be **c4.2xlarge**
- The instance must be **HVM**
- **Enhanced Networking** must be enabled on your instance
  - This can only be done from the AWS CLI with the instance stopped.
  - Make sure to update the instance id and region for the examples below.
  - To check if your instance has enhanced networking enabled, look at the value of `SriovNetSupport`. No value means not enabled.

```
$ aws ec2 describe-instance-attribute --instance-id i-1234567abc
--attribute sriovNetSupport --region us-west-1
{
  "InstanceId": "i-1234567abc",
  "SriovNetSupport": {}
}
```

- To enable enhanced networking, set `SriovNetSupport` to "simple":

```
$ aws ec2 modify-instance-attribute --instance-id i-1234567abc
--sriov-net-support simple --region us-west-1
```

- You can run the describe command again to verify that the change was successful.

```
$ aws ec2 describe-instance-attribute --instance-id i-1234567abc
--attribute sriovNetSupport --region us-west-1
{
  "InstanceId": "i-1234567abc",
  "SriovNetSupport": {
    "Value": "simple"
  }
}
```

- There must be four interfaces attached to your instance, each in a different subnet (eth1 is currently unused, but it needs to be present)
  - eth0: Management port
  - eth1: Reserved
  - eth2: Client side (downstream) interface
  - eth3: Server side (upstream) interface
- In order to access the WarpAdmin web-based GUI, your security group must allow TCP ports 80 and 443

By default, the WarpAdmin GUI will be available on the primary eth0 IP address. You may want to attach an elastic IP to this interface in order to access the GUI for configuration purposes.

The sections that follow will walk you through accessing this web-based GUI and configuring the system.

## WarpTCP Theory of Operation

*WarpTCP* can improve the TCP throughput in networks where the throughput is limited by TCP and not by any physical or quality of service BW constraint.

- *WarpTCP* proxies are configured between two physical or logical interfaces as pairs
- TCP sessions are terminated and proxied unless bypassed by specific bypass rules defined for each proxy logical pair
  - The downstream TCP connection utilizes Badu Networks' *WarpTCP* congestion control which handles congested networks much better than standard TCP.
- All other traffic passing through the proxy is bypassed and not terminated, for example:
  - Multicast
  - UDP
  - Other protocols
- VLANs are not supported by AWS

Some example network conditions that lead to significant TCP throughput improvements are:

- TCP traffic traveling through VPN tunnels
- Congested Wifi networks
- Long distance connections

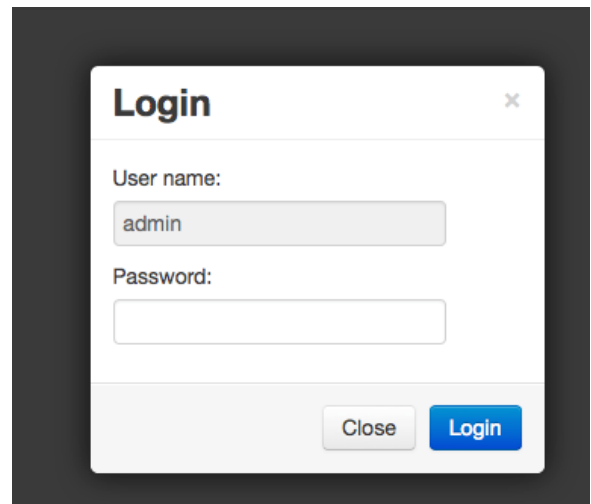
## Browser Interface & Login

After connecting to the proxy on eth0 (using the elastic IP you attached to the primary private IP address on the eth0 interface), navigate to the *WarpAdmin* GUI in your web browser. You should address your elastic IP, for example: <https://1.2.3.4>. This GUI will be used for configuring and managing the *WarpVM* software that controls the proxy. The first thing that will be displayed is the login dialog, which grants access to the management GUI.

### Default Credentials

**Username:** admin

**Password:** <interface-id>

A screenshot of a web browser window showing a 'Login' dialog box. The dialog has a title bar with 'Login' and a close button. It contains two input fields: 'User name:' with the text 'admin' entered, and 'Password:' which is empty. At the bottom right, there are two buttons: 'Close' and 'Login'.

**Login Prompt**

Once logged in, management access can be configured by adding an additional interface (IP address) on eth0 (provided one has been attached in AWS), as well as providing management access through one of the proxied interfaces on a specific port (eth2 or eth3).

# WarpVM Operating Modes

## Operating Modes

In AWS, the WarpVM operating modes are restricted such that only Gateway mode is available. This section describes this mode and provides detailed information for its configuration.

In Gateway mode, the proxy terminates the TCP session and then establishes another session downstream from the proxy. The data within the TCP packet is buffered waiting to be sent down stream, but it is not modified in any way. As a result the proxy can support encrypted traffic such as HTTPS. This method of breaking the TCP session allows the use of WarpTCP to manage the congestion control in transmitting to the downstream device. If there is jitter in the downstream network that causes standard TCP to back off, WarpTCP has the opportunity to do well. From the perspective of the client and server, there is no way to tell that the WarpTCP proxy is present other than comparing the TCP packet sequence numbers at the client and server.

Item	Gateway
DHCP support	Yes (Untested in AWS)
Routing changes on Gateways	Yes
Route traffic only on the proxy subnet	No
Management access over proxied interface	Yes
Source NAT	Yes
Selective Bypass Rules	Yes
SMB + IP Broadcast support (Windows® Share)	No
Forward Broadcast and Multi-cast traffic	No

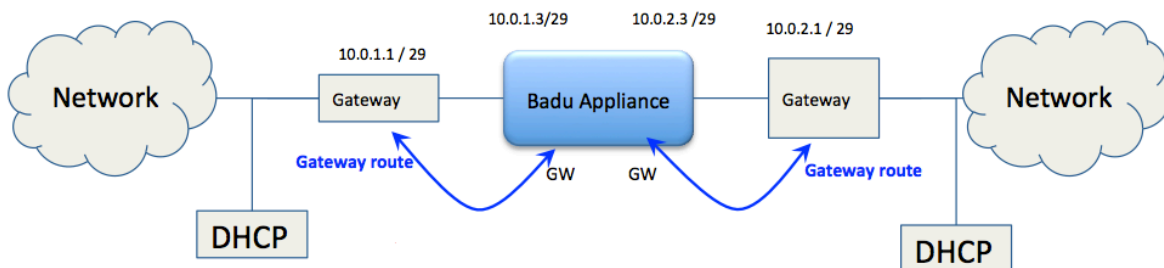
## Gateway Mode

Gateway mode allows the most control over the networking environment. However, it also requires the most changes to the network surrounding the proxy. The requirements are as follows:

- IP addresses for each proxied interface (eth2, eth3)
- Routing changes on each of the Downstream and Upstream Gateways

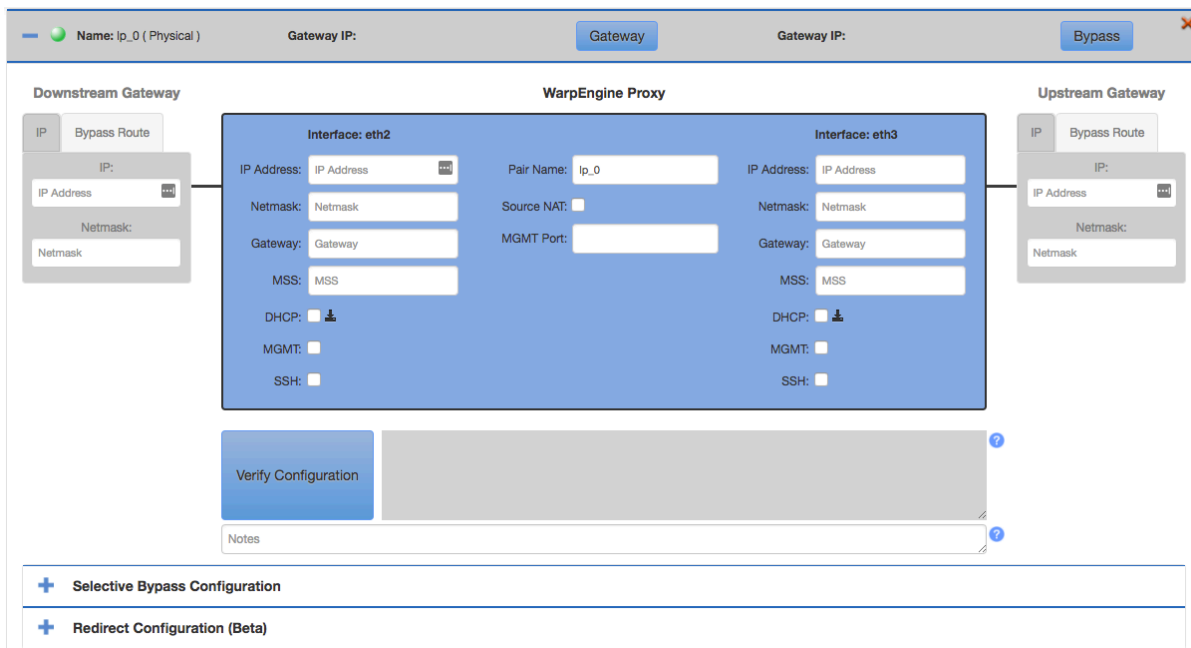
In the example network below WarpVM is placed between two gateways in a network. The Gateway and IP addresses for WarpVM are shown above and below the Proxy. The routes that need to be added to the two gateways for proxy operation are shown in blue, while the rules that need to be added for HW bypass operation are indicated in red.

### Example deployment in Gateway mode



Within WarpAdmin, the configuration for the proxy is selected for each logical pair. The fields in Gateway mode are essentially a superset of all of the fields used by the different modes.





### Required Fields:

- **Eth3 IP Address:** + Netmask: The IP address for the proxy
- **Eth3 Gateway:** The IP address that data is routed to if the IP address is not in the bridge's local subnet.
- **Eth3 Netmask:** + Netmask: The IP address for the proxy
- **Eth2 IP Address:** + Netmask: The IP address for the proxy
- **Eth2 Gateway:** The IP address that data is routed to if the IP address is not in the bridge's local subnet.
- **Eth2 Netmask:** + Netmask: The IP address for the proxy

### Optional fields :

- **Bypass:** When active all TCP traffic on this logical interface will be forwarded, and not be proxied.
- **MSS:** The maximum TCP data payload size
- **Name:** A user defined name for the proxy logical pair
- **Source NAT:** Enable source NAT on the proxy
- **MGMT:** Enable management through this logical pair
- **MGMT port:** If Management is enabled on the logical pair, it is accessible on this port number. To access MGMT on this port you need to set the browser to `https://<logical pair IP address>:<MGMT port>`
- **DHCP:** Enables the proxy IP address to be provided by a DHCP server. (Untested in AWS)

### Upstream Gateway and Downstream Client fields:

In order to help the user configure the proxy in the network environment, network data fields have been provided that indicate some key properties of the surrounding network. Then when the [Verify Configuration](#) button is pressed the configuration of the proxy is compared against these values in order to validate the configuration. The question mark to the right of [Verify Configuration](#) message field shows a list of the necessary conditions for a valid configuration.

### Selective Bypass

The WarpAdmin allows the user to selectively proxy different TCP traffic based on its source and destination. The table below provides a filter that allows the user implement these rules. It will not function as a firewall.

Any traffic which matches the designed filter will result in the traffic being bypassed around the proxy, so that the TCP session is not broken. This filter applies to the direction the TCP packets are traveling, and then internally the bypass is implemented to take care of the replies, or reverse traffic on the same TCP session.

Each TCP packet has the selective bypass rules tested against it. The fields in a single row are logically AND for the bypass to be true. Additional bypass rules or rows are logically OR.

As a result a single bypass rule can be made very specific and then multiple rules can be used to cover a number of very specific source or

destinations.

**Required fields:** None

**Optional fields:**

- **Initiated from:** The side of the proxy that the TCP packet is coming from.
- **Source IP:** The IP address of the source. A " \* " indicates any
- **Netmask:** The Netmask combined with the IP address provides the ability to bypass traffic coming from an entire subnet. If a single IP address is desired, 255.255.255.255 can be used and 255.255.255.0 would cover the 255 IP addresses in the subnet.
- **Source Port:** The source port that the traffic is coming from.
- **Destination IP:** The destination of the TCP session being established
- **Destination Netmask:** When combined with the IP address, an entire destination subnet can be bypassed.
- **Destination port:** The port that the traffic is going to.
- **Add BGP Bypass Rule:** Automatically add the bypass rules for BGP which is a destination port of 179.

Implementing selective bypass can be particularly useful in testing the benefit of WarpTCP in comparison to standard TCP (Cubic). The setup for a test would include a client and a server, with two IP addresses, connected through a congested network. The proxy can then be configured to bypass the traffic only going to one of the servers IP addresses. Then downloads or uploads can be made to these servers in an alternating fashion with a program. This method removes several key effects that can adversely effect the validity of the test:

- Network can change congestion levels very rapidly and a large number of tests can be required to get a statistically meaningful result.
  - How many samples are required depends on the desired confidence interval typical numbers are between 10 and 100.
- The network that the TCP sessions experience is identical for both proxied and unproxied traffic.
- Statistical tools can be used to determine both the benefit and the confidence interval of the result.

**Selective Bypass Configuration**

Initiated From	Source IP	Source Netmask	Port	Destination IP	Destination Netmask	Port	
Downstream ▾	*	255.255.255.0	*	*	255.255.255.0	*	↻ ↕ ↴

**Redirect:**

*Experimental*

The redirect option allows you to specify a server (or servers) to redirect traffic to. If multiple servers are specified, traffic will be redirected to each in a round-robin fashion.

If the "Enable Interface as Destination" box is checked, it will enable that interface to accept traffic and will then redirect that traffic to the specified server(s). This can be useful when Source NAT is enabled.

# WarpAdmin: Status Page

To reach the Status page, you will need to successfully login. The Status page is segmented into three functioning sections: Alarms, Control, and Performance Graphs.

BADU
Status
Interfaces
System
Diagnostics
Help
▶ proximus
Proxy State: ● **Licensed** [Logout](#)

System Alarms Actions
Clear Filters
Page Size: 100

Alarm #	Alarm Code	Severity	Type	Start	End	Message	ACK by	Notes
337	140 : bnwTcpUp	Cleared	Equipment	14:43:18 02/17/2017	14:43:18 02/17/2017	WarpEngine Proxy is up		
336	268 : bnwTcpWeSwitchPartition	Information	Communication	14:43:13 02/17/2017	14:43:13 02/17/2017	User [admin] has switched to Partition Number: 3		
335	116 : bnwTcpLogin	Minor	UserAction	14:42:59 02/17/2017	14:42:59 02/17/2017	User [admin] logged in		

### CPU

### Proxied TCP Sessions

### Memory

### Throughput (LAN3 <-> LAN4)

### Throughput (MGMT)

© Copyright BADU Networks Inc; 2014-2017; All rights reserved

## Status Page

## Alarms

- Badu's WarpEngine provides real-time notification alarms, which help aid users in monitoring and configuring the appliance.
  - Alarms can be viewed by using the scroll bar located on the right side of the section.
  - Alarms can be filtered by clicking on the filter icon at the top of each column.

- Filters**

- Each column can be used to filter the alarms by clicking the desired filter icon.

<input type="checkbox"/>	Alarm # ▼	Alarm Code ▼	Severity ▼	Type ▼	Start ▼	End ▼	Message ▼ ?	ACK by ▼	Notes ▼
--------------------------	-----------	--------------	------------	--------	---------	-------	-------------	----------	---------

- Action Dropdown**

- By selecting alarms using the checkbox in the left column, you can apply the same action to multiple alarms. For example, you can acknowledge all selected alarms at once, instead of individually acknowledging them.
- You can also change the severity of selected alarms.

- Severity**

- There are 6 different severity levels:
  - Critical (red)
  - Major (orange)
  - Minor (yellow)
  - Warning (blue)
  - Information (white)
  - Cleared (green)

- Date Range**

- A date range can be entered by selecting the Start or End filters.

**Start Filter** ✖

---

Range Start:

Range End:

Date Range Window

## Setting New Hostname:

You can set a new host name by clicking on the text "localhost.localdomain". The color of the following text will vary.

Setting a new host name will allow you to uniquely identify each machine on your network.

Note: This can be done from any page of the admin interface.

▶ localhost.localdomain

### Set New Hostname ✕

New Hostname:

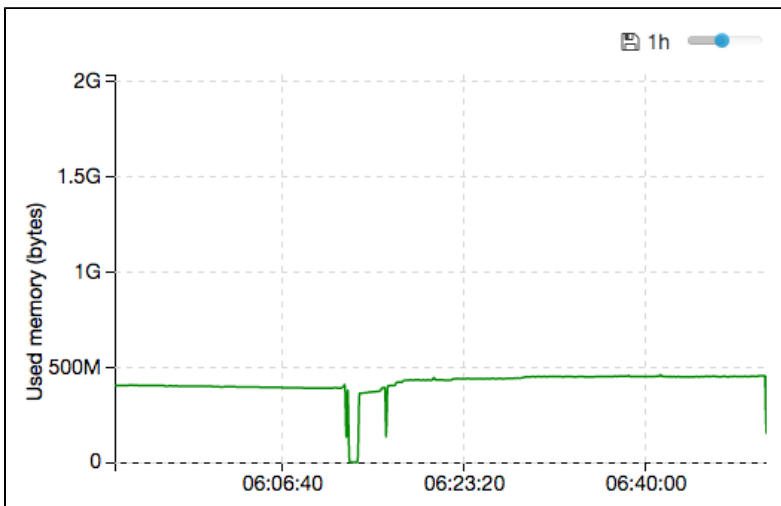
Changing hostname requires a proxy reboot.

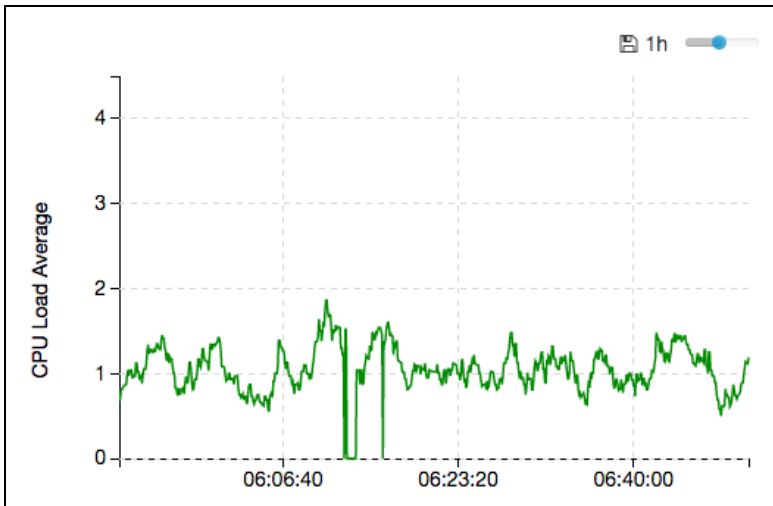
Cancel
Set

1. Enter your new desired hostname (this is limited by standard DNS characters)
2. Press the set button. Set

### System Graphs

- These graphs include the CPU load average, as well as the memory utilization.
- The data from the graphs is logged in a database for future review.
- Note that when the Box is rebooted, there will be no data recorded.





### Traffic Plots

Traffic that passes through the proxy can be logged and monitored real time. This feature is enabled in the Interfaces page and the resulting graphs are shown in the Status page.

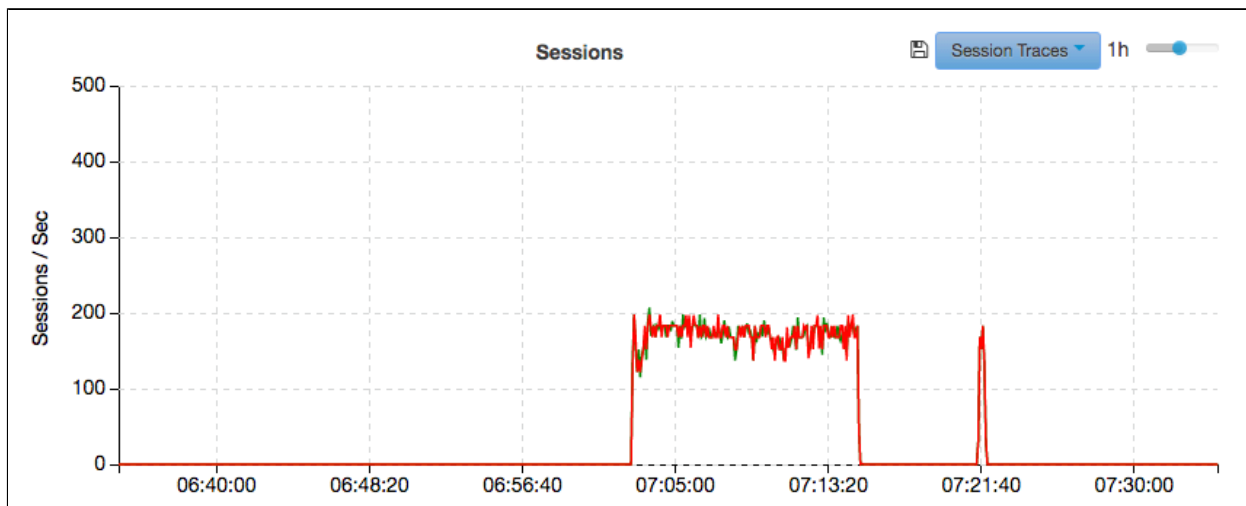
Real time graphs can include:

- Total data through each physical interface
- Proxied traffic through each logical interface
- Number of sessions open per logical interface
- Number of sessions opened per second per logical interface
- Number of sessions closed per second per interface

Within each graph there are common functions:

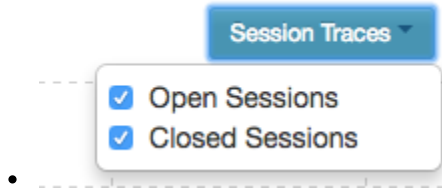
- X axis scale (slider)
- filter based on source and destination of the traffic
- Select traces to graph

### Sessions Graph



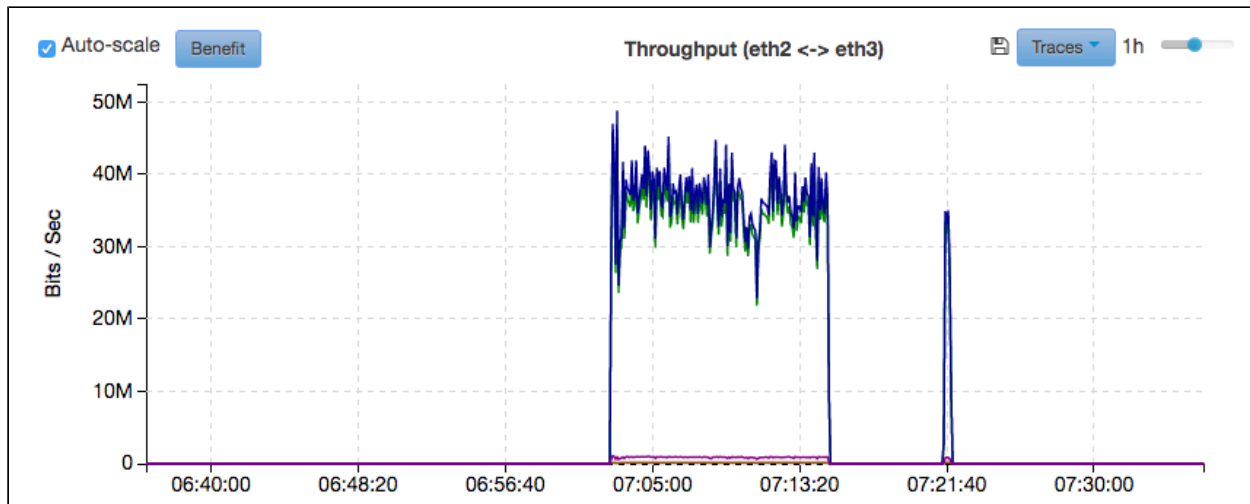
### Session Traces

- The Session Traces dropdown allows you to filter what results are displayed on the graph. You have the ability to filter between open sessions and closed session.
- To enable a filter, select the checkbox next to that filter. Once the checkmark is displayed, the associated information will now be displayed on the graph.

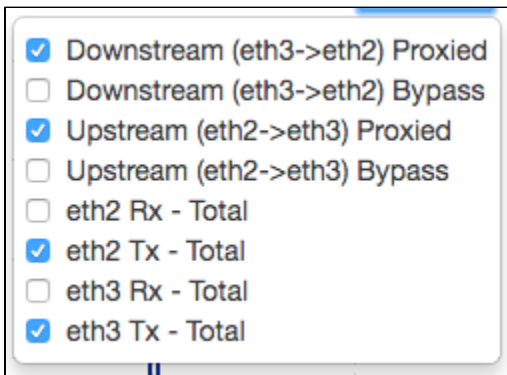


The throughput graph shows both the total throughput through the Ethernet interfaces, as well as the portion which is proxied data. Note that any traffic that is not TCP such as UDP or other protocols would make up a significant portion of the difference. In addition the proxied data does not include the TCP headers per packet, while the ethernet interface data rate includes all bytes sent.

### Throughput graph



- **Traces**
  - The Traces dropdown allows you to filter what results are displayed on the graph. You have the ability to filter specific ports and the upstream/downstream traffic.
  - To enable a filter, select the checkbox next to that filter. Once the checkmark is displayed, the associated information will now be displayed on the graph.



- **Auto-scale**
  - The Auto-scale tool will scale your graph's Y-axis according to the maximum height in the data. This tool is helpful when trying to

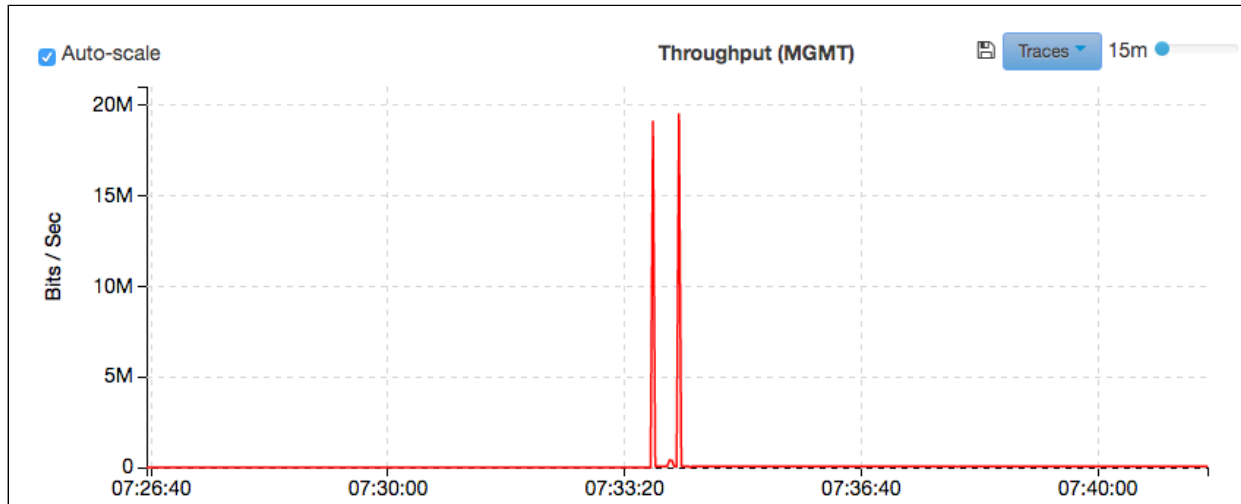
analyze graph data, that might not reach or come close to the maximum of the Y-axis (1G).

- To enable Auto-scale, select the checkbox. Once the checkmark is displayed, the graph will be scaled.

- Auto-scale

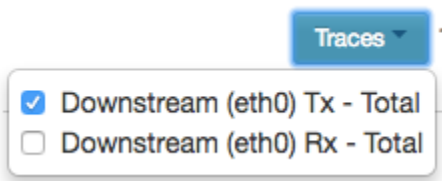
A throughput graph is also provided for the MGMT (management) Eth0 interface.

### MGMT



### Traces

- The Traces dropdown allows you to filter what results are displayed on the graph.
- To enable a filter, select the checkbox next to that filter. Once the checkmark is displayed, the associated information will now be displayed on the graph..



### Auto-scale

- The Auto-scale tool will scale your graph's Y-axis according to the maximum height in the data. This tool is helpful when trying to analyze graph data, that might not reach or come close to the maximum of the Y-axis (1G).
- To enable Auto-scale, select the checkbox. Once the checkmark is displayed, the graph will be scaled.

- Auto-scale

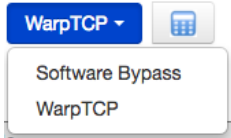


# WarpAdmin: Interfaces Page

The Interfaces Page is used for setting up WarpVM to operate within your network configuration.

The Tabs at the top of the page include the Management tab, as well as each of the physical interface pairs.

At the far right a pull-down allows the user to select the global modes of operation for the proxy, including:



- [WarpTCP](#) WarpTCP
- [SW bypass](#): All traffic is routed through the device, but TCP sessions are not terminated and no acceleration happens. Software Bypass
- [HW bypass](#): Not supported in AWS
- The subnet calculator allows you to calculate IP address ranges for different subnets.
  - Enter the desired ip address and CIDR notation.

## MGMT Tab

Under the from the top down there is a grey box indicating the physical properties of the interface, followed by the the proxy configuration, and associated management server information box.

MGMT eth2 <-> eth3
WarpTCP

### Warp Management Interface

Physical Interface	
Name	eth0
Link Status	<span style="color: green;">●</span>
MAC Address	08:00:27:e4:59:20
Speed (Mbps)	1000
MTU	1500 <input type="text"/>

#### WarpEngine Proxy MGMT

WarpEngine Fixed MGMT
Log interface

DHCP	IP address	Netmask	Gateway	VLAN ID	VLAN Name	Physical port	Delete
	10.10.10.10	255.255.255.0				eth0:M	
<input type="checkbox"/>	<input type="text" value="10.200.10.213"/>	<input type="text" value="255.255.255.0"/>	<input type="text" value="10.200.10.1"/>	<input type="text"/>	<input type="text"/>	eth0	<input type="button" value="✕"/>

#### WarpEngine MGMT On Proxy Interfaces

IP address	Netmask	Gateway	Port	VLAN ID	VLAN Name	Physical port
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

#### Management Server

IP:

Netmask:

VLAN ID:

Verify Configuration

?

?

The information in the WarpEngine Management interface box represents the hardware information for this Ethernet port .

- **MTU**: Sets the maximum Ethernet payload data size on the physical interface. This can be left blank and will be handled by default or can be modified within the valid range for the Ethernet port.

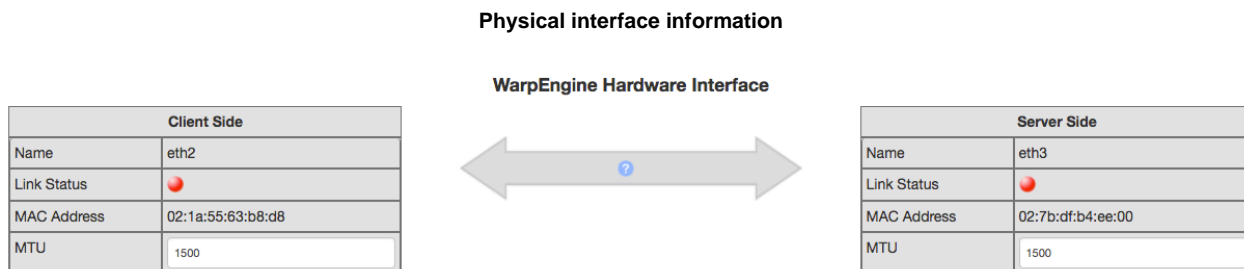
- **Traffic Analysis:** Can be enabled by pressing the "Traffic Analysis" button located underneath the WarpEngine Management interface box.
  - When Traffic analysis is enabled, a packet capture is taken on the MGMT physical interface and a popup window displays information on the traffic. The details of this popup are included under Traffic analysis.
- **Fixed MGMT:** The management interface always has 10.10.10.10/24 available on Eth0. In addition the user can add an additional management interface to work with the users management network.
- **MGMT on Proxy interface:** It is possible to connect to the WarpAdmin through one of the proxied logical pairs on a specific port. The IP address and port are selected on the interface itself and then displayed here.
- **Verify configuration:** In order to help with the configuration of the management interface this utility checks for common mistakes and connectivity, to verify that the configuration is set up correctly.
- **Verify configuration messages:** The window next to the verify configuration section displays warnings and errors from the verification check. In addition the help button next to it, this field displays all of the items that are necessary for the operation of the proxy as well as their verification status.
- **Management server:** This section is used by the verify configuration utility to ensure that the management interface is configured correctly.
- **Notes:** User notes can be saved here
- **Save:** The changes that are made to the MGMT interface are not saved until this is selected.

**NOTE:** MGMT can also be enabled for proxy interfaces on the eth2<->eth3 tab in certain modes. The management port (eth0) should **never** be on the same network as the proxy interfaces (eth2/eth3). If this happens, the network routing won't work, and you may see weird network behavior.

If you want to enable access to the WarpAdmin GUI from the proxy network, you will need to check the MGMT box on the proxy interface. Then you can access the GUI at the proxy interface IP with the specified port number (from the main network).

### Eth2<->Eth3 Tab

For each physical pair of interfaces there is a tab for defining its operation. The tab is separated into two different sections, the first relating to the physical interface and the second relates to the configuration of logical pairs. Each logical pair implements an independent proxy. The physical interfaces are referred to as upstream and downstream sides of the proxy. The upstream side is usually associated with the server, and is the external port when Source NAT is used.

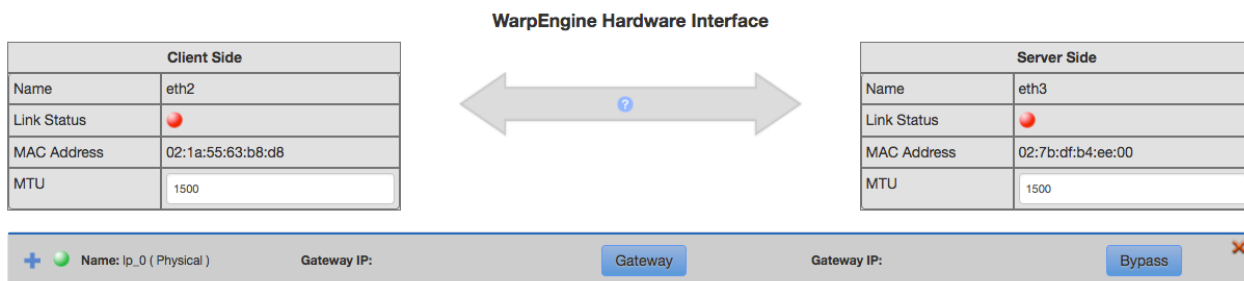


### Physical port fields:

- **Name:** The name of the physical interface
- **Link Status:** Red for not connected, Green for link detected.
- **MAC address:** MAC address for the physical interface
- **Speed:** The link speed that the interface has negotiated.
- **MTU:** The desired MTU or Ethernet payload size. If left blank, the system will use the default configuration.

### Logical / proxy configuration:

In this part of the configuration, individual proxies are configured and added or deleted. The details of each of the proxy mode are covered in the Operating Modes section of the user guide.



**Key functions:**

- **Save:** Save the current configuration
- **Cancel:** Cancel any changes made to the current configuration

# WarpAdmin: System Page

The System Page is used for viewing Proxy configuration, utilities, and proxy software.

## Proxy Information:

The proxy information tab contains information about the proxy and the software that is installed on it.

Proxy Information

[Utilities](#)
[Database](#)
[Administration](#)
[SNMP](#)
[Manager](#)
[Alarm Modifications](#)
[Accounts](#)

**Proxy Information:**

Model: <input type="text" value="WarpVM-AWSM-1G [ instance type : c4.2xlarge]"/>	Licensed Features: <input type="text"/>
Serial Number: <input type="text" value="i-0c1ae45021afc0518"/>	Sessions Left: <input type="text" value="0"/>
Software: <input type="text" value="9.9-dev_ami_ben 17331:0046"/>	Proxy Uptime: <input type="text" value="0 days 00:16:54"/>
Admin: <input type="text" value="170117.1632"/>	Proxy Time: <input type="text" value="03/31/2017 15:24:13 (GMT+0)"/>
Kernel: <input type="text" value="4.4.0-baduwarptcp-170318.1625-fuzzybottom"/>	Admin Time: <input type="text" value="03/31/2017 15:24:13 (GMT+0)"/>
BIOS Version: <input type="text" value="4.2.amazon"/>	NTP Server: <input type="text"/>

## Input:

- [Set time](#): Set the time on the WarpEngine Appliance. This is the time that will be used in the logged data.

### Set System Date and Time ×

Please set your settings below:

NTP Server:   Enable

Date and Time:

Timezone:

Note: Changing time on the proxy will require restart

## Set System Date and Time:

- [NTP server](#): Entry for the NTP server is used.
- [Date and time](#): Manually set the time on the Proxy.
- [Set](#): Saves the configuration.



## Utilities

Under the systems page, the utilities tab supports different functions for the proxy.

### Utilities Tab

[Proxy Information](#)
[Utilities](#)
[Database](#)
[Administration](#)
[SNMP](#)
[Manager](#)
[Alarm Modifications](#)
[Accounts](#)

#### Firmware Partitions

Partition	Date	Active
Active: 9.9-master	17215:0111	
Inactive: 9.9-master	17215:0111	
Manufacturing: 9.9-master	17215:0111	

Select Partition ▾

#### Proxy Configuration

[Import](#)
[Export](#)

#### System Control

[Shutdown](#)
[Reboot](#)
[Factory Defaults](#)

### System Page - Utilities

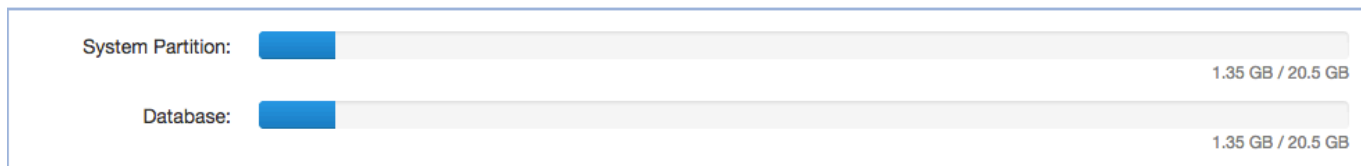
#### Utility tab inputs:

- **Firmware Partitions:** These are updated with a software update
  - **Partition:**
    - This is a list of all of the partitions on the box. There is an original read-only partition that will always be present. When the box is updated, 2 more partitions can be added. As a result, there will be a current partition, a previous partition, and the factory-installed partition. When an additional update is applied, the previous partition is replaced with the new partition, and the older partition is deleted. The factory installed partition is never removed.
    - In the event that the factory partition is selected, it behaves as if the box was updated to this partition. The factory partition is never actually active.
  - **Date:** The date each partition was installed.
  - **Active:** Green indicates the active partition. All others are grey.
  - **Select Partition button:** This selects which partition is currently active.
- **Proxy configuration:** The configuration of the proxy can be exported or saved to a file for future use.
  - **Import:** Upload a configuration file to the proxy. This file would have come from a previous export from the proxy.
  - **Export:** Download the current proxy configuration. In the future it can be imported to recover the same state.
- **Reset functions:**
  - **Shutdown:** Turn off the proxy. This should be done prior to unplugging the box in order to prevent issues with the file system.
  - **Reboot:** Reboot the proxy
  - **Reset to factory defaults:** Clear the config files and return to initial factory state. This does not clear the database.

#### Database

This section allows management of database storage limits and historical data.

### File System Usage



### Age Limit Storage

Limits:	
Alarm Age Limit	<input type="text" value="30"/>
Data Age Limit	<input type="text" value="30"/>

### Historical Data Storage

CPU		
Memory		
Sessions		
Throughput		

**Save** Cancel

- **File System Usage:**
  - **System Partition:** This is a bar indicating the amount of data used in the system partition that is available for the user.
  - **Database:** This is a bar indicating the amount of data used in the historical database vs the total available space in that partition. It only indicates storage that can be affected by the user. When the bar reaches 80% it turns yellow.
- **Age Limit Storage:**
  - **Limits:** User can specify the length of time (in days) that each item will be stored.
- **Historical Data Storage:**
  - **Trashcan:** This deletes the historical data of this type. A popup warns the user with OK / Cancel.
  - **Download:** This downloads the particular data type to a CSV file with headers for each column.
    - A popup allows the user to select a time or date range.
    - The popup also allows user to select data resolution; 15 minutes, 1 hour, or 24 hours.

## Administration

This tab is used for administering the Proxy.

- This tab includes changing passwords
- Allow SSH access to the proxy
- Licensing
- Firmware updates
- Remote support
- SOS file generation

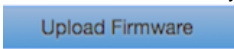
One of the first things that should be done when deploying the proxy is to change the administrator's password. Currently WarpEngine only supports a single user account.

### WarpAdmin Admin Password

Out of the box, the password is "password"

### Firmware Update Procedure:

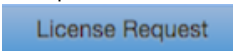
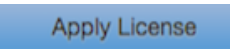
In order to update the latest firmware to the following:

1. Visit the BADU Networks licensing and update website: <http://license.badunetworks.com/>
2. Log in with your user name and password.
3. Download the latest software for your product
4. Choose 
5. Upload firmware

### Licensing Procedure:


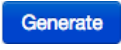

In order to operate with high performance the WarpAdmin must be licensed with a valid license.

Licensing steps:

1. **Before proceeding**, make sure you are not in hardware bypass mode. Licensing will fail if hardware bypass is active!
2. Update the firmware using the steps above
3. Download License request 
4. Log onto the BADU Networks Licensing and update website: <https://license.badunetworks.com/>
5. Choose request license tab -> Upload request
6. Upon success, download the license
7. Upload the license to the admin using 
8. Upon successful licensing a popup will indicate success. A short time later the license indicator will indicate that it was successful.

### Generate New SSH Key:

Creating a ssh key will allow the user to ssh into the machine and run a limited set of commands, which can assist in debugging network issues. The ssh key can be set to expire after a programmed period of time. SSH access is only provided through using a key and not a password. The ports that support ssh access are defined in the GUI.

1. Decide whether or not you would like the ssh key to expire at some time. If not then skip step 2 and select "Key never expires" checkbox. If so, proceed step 2.
2. Select the date that you would like the ssh key to expire. Use the calendar icon to select the desired expiration date. 
3. Select the key size that you would like to associate with the ssh key.
  - a. The larger the key size is, the longer it takes to generate, but the more secure it will be.
4. Press the Generate button 
5. The Download SSH Key pop up will be displayed. Press the Download button to download the key. 
  - a. The key will begin to download to your computer.

### Current Key Expiration:

This field can be used to reference the expiration date of your current ssh key.

Also you can download this ssh key at any time by pressing the key icon.



Current Key Expiration:

04:05:39 PM 05/21/16 (GMT-7)

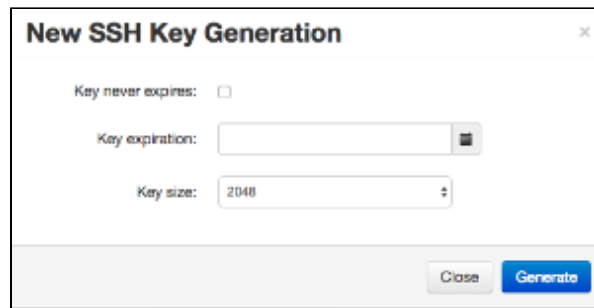


**Generate SOS File**

Generate SOS File

In the event that something bad happens to the proxy software, a debug file can be created that gives information on the status of the box.

Select "Generate SOS File" to generate the SOS file and then e-mail it to [support@badunetworks.com](mailto:support@badunetworks.com)

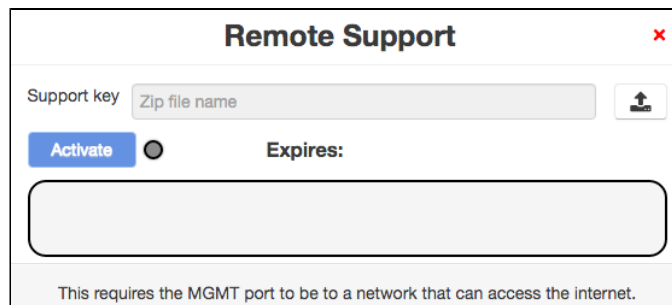


### Remote support

The remote support function allows Badu Networks technicians to help solve issues with WarpEngine by logging onto the Proxy remotely. In order to enable this support do the following:

- Configure the proxy with a default gateway so that it could reach the internet.
- Obtain a remote support key from Badu Networks, and upload the support key in the support key dialog as shown below.
  - The key will only be active for a limited time.
- Press the Activate button to activate the connection.
  - When the remote connection has been established the button next to the activate button will turn green.

Log messages will be displayed in the remote support dialog shown below.



In order to be able to access the WarpEngine Admin and also have a connection to the internet, the WarpEngine Eth0 can be connected to a switch which is also connected to the internet gateway. The only requirement is that the WarpEngine Admin is on the same subnet as the PC which is trying access it.

### SNMP

This configuration allows the user to configure the WarpEngine with multiple SNMP managers.



### SNMP Configuration

Configuration Name	<input type="text"/>
SNMP Version	3
Destination IP Address	<input type="text"/>
Destination Port	162
Security Level	authPriv
Security Name	1 - 32 characters
Authentication Engine Id	10 - 64 digits
Auth Password	8 - 16 characters
Privacy Password	8 - 16 characters
Authentication protocol	SHA
Privacy Protocol	AES

Add

#### Testing:

Alarm Code	<input type="text"/>
Notes	<input type="text"/>

Test

- **Add:** Add a configuration for another outgoing connection
  - **Configuration Name:** The name of this particular configuration
  - **SNMP Version:** Version of the SNMP software (defaults to v3).
  - **Destination IP Address:** The IP address of the Manager
  - **Destination Port:** The port that the manager uses for SNMP (defaults to 162)
  - **Security Level:** authPriv, noAuthPriv, noAuthNoPriv
  - **Security Name:** The login user name for the manager
  - **Authentication Engine ID:** A 2 – 32 char hex string which acts similar to an SNMP user name
  - **Auth Password:** The manager auth password
  - **Privacy Password:** The manager privacy password
  - **Authentication Protocol:** SHA or MD5
  - **Privacy Protocol:** DES, AES, AES128, AES256
- **Testing:** This is used to artificially generate SNMP notifications.
  - When a Proxy creates an alarm, it is sent as a notification to the manager. This alarm can then be re-issued to the NMS.

### Alarm Modifications

- Alarm modifications modify the alarm generation on the proxy. The modifications can be initiated on the proxy or on the Manager.
  - The values are stored on the Proxy and Cached on the Manager display
  - In the event that they are created on the proxy, the Alarm modification is sent to the manager over the secure communications

rest interface.

- When the WarpEngine first connects to the manager, it sends all of its Alarm modifications to the Manager.
- When a WarpEngine is disconnected from the manager, the manager flushes all modifications associated with the proxy.
- When rules are being sent to or from the WarpEngine, a queue is kept that survives rebooting the proxy. The action is removed from the queue when it is acknowledged as complete.

Proxy Information Utilities Database Administration SNMP Manager Alarm Modifications Accounts

Alarm Modification Add Clear

Type	Severity	Alarm ID	Active time	Delay (ms)	Execute Action
Select Type ▾	Select Severity ▾	Select Alarm ID ▾	From: Not defined Till: Not defined	Multiple events buffering delay: Not defined	☑ Select Action ▾

Apply modification rules - Not started. 0 / 0

Active Alarm Modifications Clear Filters Page Size: 100 ▾

Type ▾	Alarm Code ▾	Action ▾	User ▾	Source ▾	Date ▾
== Empty ==					

- **Alarm Modification:**
  - **Add:** Add a new set of rules defined by what the user entered. Does nothing if the user didn't enter anything.
  - **Filter bar:** this bar creates a filter + action that is flattened and then written as individual rules to the active alarms table. The filters are logically ANDed to select which alarms to create the rule for.
  - **Type:** This allows the user to select one or more Alarm types with a pull-down
  - **Severity:** Select the severity of the alarms to select
  - **Alarm ID:** A pull-down of the IDs that meet the other filter conditions.
  - **Active Time:** Define an active period for the modification rule
  - **Delay (ms):** Specify a delay for the modification rule
  - **Execute Action:** This is the modification that will be made to all of the alarms that match the filter.
- **Active Alarm Modifications:**
  - The table lists all of the alarms which are currently active.
    - Each row corresponds to a single rule / modification
    - Each Column can be filtered and sorted. Sort applies to one column, but the filters are all logically ANDed.
  - **Type:** the type of alarm
    - Filter: pull down multiple selection, sort (ascending / descending)
  - **Alarm Code:** Code for the active alarm
    - Filter: List selection of alarm codes
  - **Action:** the action that will be carried out on the Alarm
    - Filter: pull down for the different actions, sort Ascending / descending.
  - **User:** the user associated with the alarm
  - **Source:** the source of the alarm
  - **Date:** the date of the alarm

## Accounts

Create and manage user accounts and their permissions.

Proxy Information Utilities Database Administration SNMP Manager Alarm Modifications Accounts

**Current User**

User Name	admin
Name	admin
Phone	n/a

Change Password

User Permissions Clear Filters Page Size: 100 ▾

Select	User Name	Name	Phone	Role	User Permissions	
					Admin	Read Only
<input type="checkbox"/>	admin	admin	n/a	Admin	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

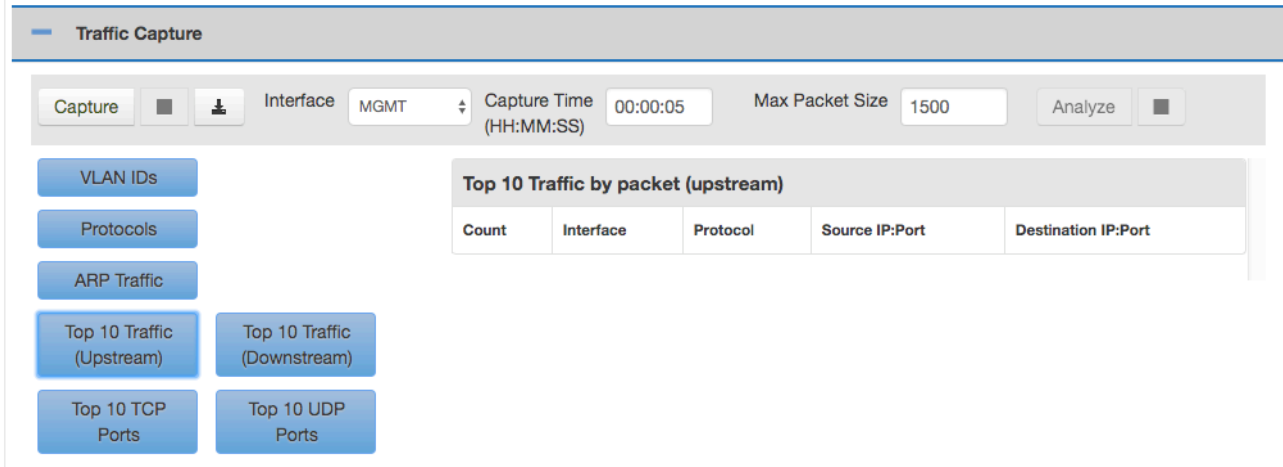
- **Current User:** Displays information about the current user
  - **Change Password:** Allows user to change their password
- **User Permissions:** This table displays all users and their information
  - **Select:** Checkboxes allow editing multiple users at once
  - **User Permissions:** Define permissions for each user (currently only two options, Admin and Read-Only)
  - **New User:** Create a new user

# WarpAdmin: Diagnostics

Diagnostic and troubleshooting data can be collected through capturing data passing through the Proxy.

## Traffic Capture:

The traffic analysis function allows the user to take a packet capture on both of the physical ports and do a basic analysis of the results. This can be particularly useful for debugging configuration issues. Note that the Analysis of large capture files can be quite CPU intensive, and may disrupt the collection and display of graph data.



## Inputs:

- **Capture:** Start the packet capture. The user can browse away or even log off the proxy during the capture
- **Stop:** Stop the packet capture (active when the capture is in progress). The capture will be analyzed and displayed after the capture is complete.
- **Download:** Download the raw capture files in Zip format. The captured files persist on the proxy until another packet capture is run, or the box is rebooted.
- **Interface:** The interface that the capture will be taken on
- **Capture time (HH:MM:SS):** The amount of time that the packet capture will run.
- **Max packet size:** The maximum number of bytes to capture per packet
- **Analyze:** Once the capture has been taken it can either be analyzed, or downloaded.
- **Stop Analysis:** This allows the user to stop the analysis while it is processing. For large captures the analysis may take a good deal of time.
- **Cancel [ X ]:** This button stops the current capture

## Display:

Pressing each of the display buttons shows the corresponding analysis to the right of the buttons.

- **VLAN IDs:** These are the VLAN IDs seen in the capture files (VLANs not supported in AWS)
- **Protocols:** The different protocols seen on those interfaces
- **ARP:** The ARP messages seen on each of the interfaces.
- **Top 10 traffic (by packet):** Statistics for the traffic seen on the interfaces, sorted by the number of packets.
- **Top 10 TCP ports:** Display statistics on the ports being used by the TCP traffic
- **Top 10 UDP ports:** display the statistics for the top UDP ports used in the capture

# Examples of Selective Bypass Rules

## WarpEngine Selective Bypass Rules

The selective bypass rules can be used to choose which TCP flows should be accelerated and which ones should bypass the proxy. These rules apply to each individual logical pair on each interface.

Initiated From	Source IP	Netmask	Port	Destination IP	Destination Netmask	Port	
Downstream	*	255.255.255.255	*	*	255.255.255.255	179	⊙ ⊙ ⊙
Upstream	*	255.255.255.255	*	*	255.255.255.255	179	⊙ ⊙ ⊙

Within the selective bypass section UI, it is possible to select the source subnet / destination subnet as well as the source and destination port.

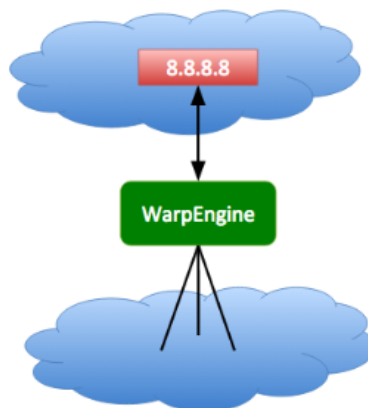
For all TCP packets the bypass filter is applied to determine if the packet should be proxied. If any of the bypass rules is TRUE, then the packet is bypassed and not proxied. Within each rule, the conditions are logically ANDed so that the TCP packet must match all of the conditions. **Since TCP has a returning path for each session, the returning path bypass rule is automatically added, but not shown.**

Please use the "Initiated From" field to determine whether the TCP session is coming from upstream or downstream. The host that sends the initial SYN packet is the initiator. That host may be on the client side the proxy (i.e., "downstream") or the server side of the proxy (i.e., "upstream"). Please select accordingly.

### Example configurations:

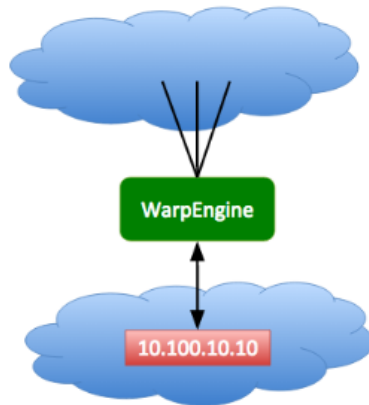
#### Bypass Source IP

- **Select: Bypass Source IP**
  - Select only Source IP
    - IP: 8.8.8.8
    - Netmask: 255.255.255.255
- **Result:** All packets in sessions initiated by 8.8.8.8 will pass through WarpEngine untouched.



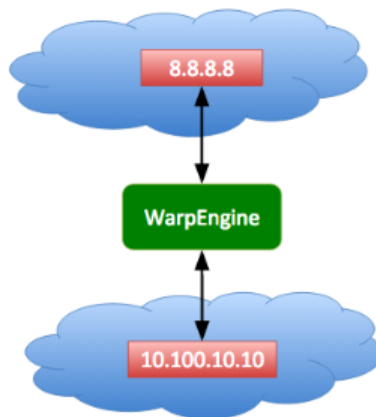
#### Bypass Destination IP

- **Select: Bypass Destination IP**
  - Select only Destination IP
    - IP: 10.100.10.10
    - Netmask: 255.255.255.255
- **Result:** All packets in sessions destined for 10.100.10.10 will pass through WarpEngine untouched.



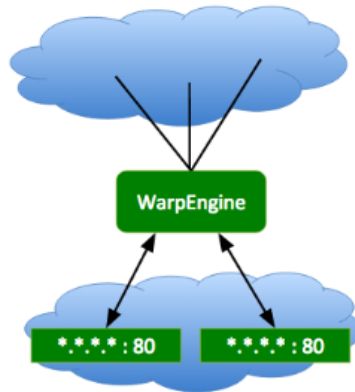
### Bypass Source & Destination IP

- **Select: Bypass Source and Destination IP**
  - Select Source IP
    - IP: 8.8.8.8
    - Netmask: 255.255.255.255
  - Select Destination IP
    - IP: 10.100.10.10
    - Netmask: 255.255.255.255
- **Result:** All packets in sessions initiated by 8.8.8.8 going to and from 10.100.10.10 will pass through WarpEngine untouched.



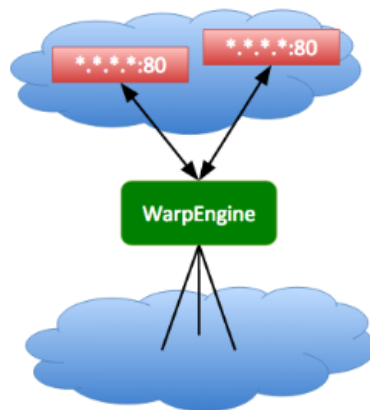
### Bypass Source Port

- **Select: Bypass Source Port**
  - Select only Source port
    - Port: 80
- **Result:** All packets in sessions originating from port 80 will pass through WarpGateway untouched



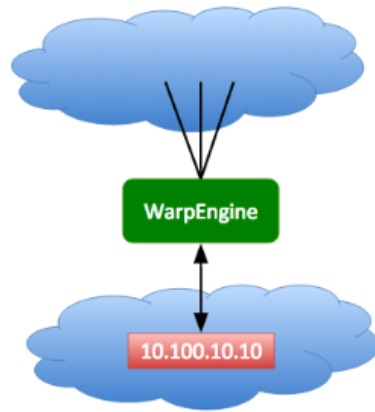
**Bypass Destination Port**

- **Select: Bypass Destination Port**
  - Select only Destination port
    - Port: 80
- **Result:** All packets in sessions going to port 80 will bypass the proxy and not be accelerated



**Bypass Both Destination & Source Ports**

- **Select: Bypass both Destination and Source Ports**
  - Select
    - Destination Port: 80
    - Source Port: 81
- **Result:** All packets in sessions originating from port 81 and going to port 80 will bypass the proxy, and not be accelerated.





## WarpVM Known Issues

- If your browser is having issues communicating with the WarpAdmin GUI, please make sure the WarpAdmin IP address is a trusted site in your browser settings.

Release notes for this release can be obtained on the Badu Networks Licensing web site at [license.badunetworks.com](https://license.badunetworks.com).

## Contact Badu Networks

Email: [support@badunetworks.com](mailto:support@badunetworks.com)

Phone: (949) 310-5390

Fax: (888) 958-7697

Address: 2640 Main Street, Irvine, CA 92614

# WarpVM Warranty Information

## Limited Software Warranty

Badu warrants that the encoding of the software program on the media on which the Product is furnished will be free from defects in material and workmanship, and that the Product shall substantially conform to its user manual, as it exists at the date of delivery, for a period of ninety (90) days. Badu's entire liability and Your exclusive remedy under this warranty shall be, at Badu's option, either: (i) return of the price paid to Badu for the Product, resulting in the termination of this Agreement, or (ii) repair or replacement of the Product or media that does not meet this limited warranty. EXCEPT FOR THE LIMITED WARRANTIES SET FORTH IN THIS SECTION, THE PRODUCT AND ANY SERVICES ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED. BADU DOES NOT WARRANT THAT THE PRODUCT WILL MEET YOUR REQUIREMENTS OR THAT ITS OPERATION WILL BE UNINTERRUPTED OR ERROR FREE. BADU DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. Some jurisdictions do not allow the exclusion of implied warranties or limitations on how long an implied warranty may last, so the above limitations may not apply to You. This warranty gives You specific legal rights. You may have other rights that vary from state to state.

THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY FROM STATE TO STATE (OR JURISDICTION TO JURISDICTION). BADU'S RESPONSIBILITY FOR MALFUNCTIONS AND DEFECTS IN HARDWARE IS LIMITED TO REPAIR AND REPLACEMENT AS SET FORTH IN THIS LIMITED WARRANTY STATEMENT. ALL EXPRESS AND IMPLIED WARRANTIES FOR THE PRODUCT, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF AND CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, ARE LIMITED IN DURATION TO THE LIMITED WARRANTY PERIOD SET FORTH ABOVE AND NO WARRANTIES, WHETHER EXPRESS OR IMPLIED, WILL APPLY AFTER SUCH PERIOD. SOME STATES (OR JURISDICTIONS) DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

BADU DOES NOT ACCEPT LIABILITY BEYOND THE REMEDIES SET FORTH IN THIS LIMITED WARRANTY STATEMENT OR LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION ANY LIABILITY FOR PRODUCTS NOT BEING AVAILABLE FOR USE OR FOR LOST DATA OR SOFTWARE. SOME STATES (OR JURISDICTIONS) DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE EXCLUSION OR LIMITATION MAY NOT APPLY TO YOU.

These provisions apply to Badu's one-year limited warranty only. For provisions of any on-site service contract covering your system, refer to the separate on-site service contract.