exinda SD-WAN

HELP MANUAL

Find out how to set up and configure Exinda SD-WAN in different environments and how to customize advanced features.

Document Version: 1.07.4.9

Last updated (month/day/year): 11/25/2021

Contents

Copyrights, Trademarks, Warranty, Disclaimers

0.0.1 Copyrights and Trademarks

This Broadband Bonding Network Appliance (TM) includes certain embedded software and firmware (collectively, "Software"). The Software is a trade secret of GFI, Inc. and is protected by various copyright and other intellectual property laws and treaties. No license is granted to you to reproduce, modify or create derivative works of, distribute, display or perform such Software. You may not reverse engineer, disassemble, decompile, or otherwise attempt to discover the source code for the Software. You may use the Software solely as embedded in this Exinda SD-WAN.

0.0.2 Hardware warranty and Disclaimers

GFI warrants that this Exinda SD-WAN is free from physical defects in material and workmanship for 12 months from the date of purchase, when used within the limits set forth in the User Manual.

If you purchased the Exinda SD-WAN from a third party, contact that third party to receive warranty support. If you purchased the Exinda SD-WAN directly from GFI, to receive warranty support contact GFI Technical Support in order to obtain a Return Material Authorization (RMA) number and a description of the RMA process.

In the event this Exinda SD-WAN proves defective during the warranty period, GFI, in its sole discretion, either repairs the Exinda SD-WAN, replaces the Exinda SD-WAN with a new or refurbished Exinda SD-WAN or refunds the price paid for the Exinda SD-WAN. The new or refurbished Exinda SD-WAN is warranted for the balance of the original warranty period. The foregoing shall be the sole and exclusive remedy for a breach of the foregoing warranty.

In order to receive warranty support you must have your proof of purchase and the product serial id number. Return requests cannot be processed without proof of purchase. When returning the Exinda SD-WAN, you must mark the RMA number clearly on the outside of the package and include a copy of your original proof of purchase.

All customers located outside of the United States of America and Canada must pay for shipping and handling charges to return a defective Exinda SD-WAN.

The foregoing warranty shall be void and of no force or effect if:

» the Exinda SD-WAN is modified by any person other than GFI or is installed, operated or maintained in any manner that is inconsistent with the terms in this User Manual.

» the external Exinda SD-WAN housing is opened or tampered with.

» the Exinda SD-WAN is subject to any abuse, negligence or misuse, including without limitation physical or electrical abuse or stress, or exposure to water or fire.

Except for the limited express warranty set forth above, GFI networks makes no other warranties or representations regarding this Exinda SD-WAN or this user manual, express or implied. GFI networks disclaims all other warranties and representations, express, implied, statutory and otherwise, including, without limitation, any warranty of uninterrupted, error-free or bug-free operation, the implied warranties of non-infringement, merchantability and fitness for a particular use or purpose and any warranty as to quality or performance. No person, representative or firm is authorized to extend, enlarge or otherwise modify the limited warranty set forth above. If the exclusion of implied warranties contained herein is prohibited by applicable law, then the applicable implied warranties are limited to the duration of the express warranty described above.

0.0.3 Limits on Liability

In no event shall GFI networks' aggregate liability exceed the price paid for the Exinda SD-WAN. To the maximum extent permitted by applicable law, in no event shall GFI networks be liable for any indirect, special, punitive, incidental, or consequential damages, even if GFI networks was advised or aware of the possibility of such damages, and regardless of the form of action, whether in contract, tort, negligence, strict product liability or otherwise. This limitation is separate and independent of any other remedy limitations and shall not fail if such other limitation on remedy fails of its essential purpose. This limitation shall not apply to personal injury caused by the Exinda SD-WAN.

0.0.4 End User License Agreement

> **Important**
> Please read this end user license agreement carefully.

Downloading, installing or using GFI or GFI-supplied software constitutes acceptance of this agreement. GFI is willing to license the software to you only upon the condition that you accept all of the terms contained in this license agreement plus any additional limitations on the license set forth in a supplemental license agreement. To the extent of any conflict between the terms of this license agreement and any supplemental license agreement, the supplemental license agreement shall apply. by downloading, installing or using the registration number, product authorization key, license key, license file, or software, using the equipment that contains this software, or clicking an "accept" button (or a logical equivalent) during the installation or downloading process, you are binding yourself and the business entity that you represent (collectively, "customer") to this agreement and any supplemental license agreement. If you do not agree to all of the terms of this agreement and any supplemental license agreement, then GFI is unwilling to license the software to you and:

» do not download, install or use the software

» you may return the software (including any unopened cd package or usb-keys) and any written materials for a full refund, or, if the software and written materials are supplied as part of another product, you may return the entire product for a full refund. Your right to return and refund expires 30 days after purchase from GFI or an authorized GFI reseller, and applies only if you are the original end user purchaser.

The following terms of this end user license agreement and any supplemental license agreement (collectively the "EULA") govern customer's access and use of each GFI or GFI-supplied software ("software"), except to the extent:

» There is a separate signed agreement between customer and GFI governing customer's use of the software, or

» The software includes a separate "click-accept" license agreement or third party license agreement as part of the installation and/or download process governing customer's use of the software. To the extent of a conflict between the provisions of the foregoing documents, the order of precedence shall be:

a. The signed agreement

b. The click-accept agreement or third party license agreement

c. This EULA.

License

Conditioned upon compliance with the terms and conditions of this EULA, GFI grants to customer a nonexclusive and nontransferable license to use for customer's internal business purposes the software and the documentation for which customer has paid the required license fees. In order to use the software, customer may be required to input a registration number or product authorization key and register customer's copy of the software on line at GFI's web site to obtain the necessary license key or license file.

Customer's license to use the software shall be limited to, and customer shall not use the software in excess of, a single hardware chassis or card or such number and types of agent(s), concurrent users, sessions, IP addresses, port(s), seat(s), server(s), site(s), or features and feature sets as are set forth in the applicable end user license agreement supplement and in the applicable purchase order accepted by GFI and for which customer has paid the required license fee.

Unless otherwise expressly provided in the documentation or any applicable supplemental license agreement, customer shall use the software solely as embedded in, for execution on, or (where the applicable documentation permits installation on non- GFI equipment) for communication with GFI equipment owned or leased by customer and used for customer's internal business purposes. No other licenses are granted by implication, estoppel or otherwise.

> **Note**
> For evaluation or beta copies for which GFI does not charge a license fee, the above requirement to pay license fees does not apply.

General Limitations

This is a license, not a transfer of title, to the software and documentation, and GFI retains ownership of all copies of the software and documentation. Customer acknowledges that the software and documentation contain trade secrets of GFI, its suppliers or licensors, including but not limited to the specific internal design and structure of individual programs and associated interface information. Except as otherwise expressly provided under this EULA, customer shall have no right, and customer specifically agrees not to:

i. transfer, assign or sublicense its license rights to any other person or entity, or use the Software on unauthorized or second-hand GFI equipment, and Customer acknowledges that any attempted transfer, assignment, sublicense or use shall be void;

ii. make error corrections to or otherwise modify or adapt the Software or create derivative works based upon the Software, or permit third parties to do the same;

iii. reverse engineer or decompile, decrypt, disassemble or otherwise reduce the Software to human-readable form, except to the extent otherwise expressly permitted under applicable law notwithstanding this restriction;

iv. use or permit the Software to be used to perform services for third parties, whether on a service bureau or time sharing basis or otherwise, without the express written authorization of GFI; or

v. disclose, provide, or otherwise make available trade secrets contained within the Software and Documentation in any form to any third party without the prior written consent of GFI. Customer shall implement reasonable security measures to protect such trade secrets.

To the extent required by law, and at Customer's written request, GFI shall provide the Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of GFI's applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which GFI makes such information available.

Upgrades and Additional Copies

Notwithstanding any other provision of this EULA:

1. Customer has no license or right to use any additional copies or upgrades unless customer, at the time of acquiring such copy or upgrade, already holds a valid license to the original software and has paid the applicable fee for the upgrade or additional copies;

2. Use of upgrades is limited to GFI equipment for which customer is the original end user purchaser or lessee or who otherwise holds a valid license to use the software which is being upgraded; and

3. The making and use of additional copies is limited to necessary backup purposes only.

Proprietary Notices

Customer agrees to maintain and reproduce all copyright and other proprietary notices on all copies, in any form, of the Software in the same form and manner that such copyright and other proprietary notices are included on the Software. Except as expressly authorized in this EULA, Customer shall not make any copies or duplicates of any Software without the prior written permission of GFI.

Term and Termination

This EULA and the license granted herein shall remain effective until terminated. Customer may terminate this EULA and the license at any time by destroying all copies of the Software and any Documentation. Customer's rights under this EULA terminates immediately without notice from GFI if Customer fails to comply with any provision of this EULA. Upon termination, Customer shall destroy all copies of the Software and Documentation in its possession or control. In addition, the provisions of the sections titled "U.S. Government End User Purchasers" shall survive termination of this EULA.

1. use or permit the Software to be used to perform services for third parties, whether on a service bureau or time sharing basis or otherwise, without the express written authorization of GFI; or

2. disclose, provide, or otherwise make available trade secrets contained within the Software and Documentation in any form to any third party without the prior written consent of GFI. Customer shall implement reasonable security measures to protect such trade secrets.

To the extent required by law, and at Customer's written request, GFI shall provide the Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of GFI's applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which GFI makes such information available.

Export, Re-export, Transfer and Use controls

The software, documentation and technology or direct products thereof (hereafter referred to as software and technology), supplied by GFI under this EULA are subject to export controls under the laws and regulations of the United States (U.S.). Customer shall comply with such laws and regulations governing export, re-export, transfer and use of GFI software and technology and obtains all required U.S. and local authorizations, permits, or licenses. GFI and customer each agree to provide the other information, support documents, and assistance as may reasonably be required by the other in connection with securing authorizations or licenses.

Upgrades and Additional Copies

Notwithstanding any other provision of this EULA:

1. Customer has no license or right to use any additional copies or upgrades unless customer, at the time of acquiring such copy or upgrade, already holds a valid license to the original software and has paid the applicable fee for the upgrade or additional copies;

2. Use of upgrades is limited to GFI equipment for which customer is the original end user purchaser or lessee or who otherwise holds a valid license to use the software which is being upgraded; and

3. The making and use of additional copies is limited to necessary backup purposes only.

Proprietary Notices

Customer agrees to maintain and reproduce all copyright and other proprietary notices on all copies, in any form, of the Software in the same form and manner that such copyright and other proprietary notices are included on the Software. Except as expressly authorized in this EULA, Customer shall not make any copies or duplicates of any Software without the prior written permission of GFI.

Term and Termination

This EULA and the license granted herein shall remain effective until terminated. Customer may terminate this EULA and the license at any time by destroying all copies of the Software and any Documentation. Customer's rights under this EULA terminates immediately without notice from GFI if Customer fails to comply with any provision of this EULA. Upon termination, Customer shall destroy all copies of the Software and Documentation in its possession or control. In addition, the provisions of the sections titled "U.S. Government End User Purchasers" shall survive termination of this EULA.

Government End User Purchasers

The software and documentation qualify as "commercial items," as that term is defined at federal acquisition regulation ("far") (48 c.f.r.) 2.101, consisting of "commercial computer software" and "commercial computer software documentation" as such terms are used in far 12.212. consistent with far 12.212 and DOD far supp. 227.7202-1 through 227.7202-4, and notwithstanding any other far or other contractual clause to the contrary in any agreement into which this EULA may be incorporated, customer may provide to government end user or, if this EULA is direct, government end user acquire, the software and documentation with only those rights set forth in this EULA. Use of either the software or documentation or both constitutes agreement by the government that the software and documentation are "commercial computer software" and "commercial computer software documentation," and constitutes acceptance of the rights and restrictions herein.

Support information

If you purchased your Exinda SD-WAN directly from GFI, please visit the support portal at Support.

You can access the knowledge base when you create your account.

Introduction

Software-defined Wide Area Network (SD-WAN) refers to the concept of combining different WAN interfaces to create a unified WAN.

SD-WAN gives more flexibility and reliability due to automatic failover in case there is an issue with the primary internet link. It also increases the application performance as it maximizes all WAN links simultaneously.

Exinda SD-WAN are highly versatile devices that can provide true bandwidth aggregation in a variety of settings. These include standalone operation, point-to-point communication between two sites, as well as supporting robust data communication across a large global enterprise. In all cases, the Exinda SD-WAN devices enable high performance, high reliability data communications by making concurrent use of all available communication resources. By using the most cost effective communication resources available at a site location, the WAN performance and reliability can be significantly improved in a cost effective manner.

0.1 Features

- Ethernet WAN ports are compatible with any broadband modem technology, such as ADSL, ADSL2, ADSL2+, VDSL, VDSL2, T1, Cable Modem, Satellite, 2G, 3G, 4G LTE etc. via 10/100 baseT, 1GigE and 10GigE Ethernet, and USB interfaces.
- Web-based Exinda SD-WAN Management Interface allowing easy configuration and monitoring.
- Bonded Internet service is provided through one or more Ethernet LAN ports.
- Stateful Firewall.
- Traffic Monitoring.
- Traffic filtering and interface binding.
- Dynamic Traffic shaping, prioritization, QoS shaping, and QoS reservations.
- Seamless support of legacy networks without re-configuration of existing network.
- Configurable DHCP server for auto-addressing (optionally enabled).
- Support for DMZ and port forwarding and firewall functions (optionally enabled).
- UPnP support (optionally enabled).
- VRRP support (optionally enabled).
- Parallel DNS queries on all active WAN interfaces for reduced DNS latency and increased reliability.
- Domain name blocking and DNS redirection.
- Session Continuity for automatic allocation of available WAN resources without interruption.
- Syslog server and SMTP MIBv2 support.

0.2 Hardware series

The Exinda SD-WAN dedicated hardware series include the EXSD-300, EXSD-1000, and EXSD-10G.

The **EXSD-300** model is a rack mountable device with 4 WAN connections and 2 LAN connections that are available through Ethernet connector (RJ-45, 10/100/1000 Mbps) on the front panel. Two USB ports are available for wireless WAN connections. There is also a serial port connector on the front panel reserved for future use.

Additional models include **EXSD-1000** with 4 additional WAN ports model and Performance Pack, **EXSD-1000** with 8 additional WAN copper ports model, **EXSD-1000** with 8 additional WAN fiber optic ports model.

The **EXSD-10G** model is the device with two 10 Gbps fiber optic LAN and two 10 Gbps fiber optic WAN ports and ten 1 Gbps copper WAN ports.

The USB ports on any Exinda SD-WAN device can also be used for resetting the unit to factory default settings.

Each Ethernet connector has two LED indicators associated with it. One LED is lit for a logical connection to a device on the opposite end of the cable. The other LED is lit indicating data transfer. An LED on the front panel indicates the unit is powered up.

0.2.1 Exinda SD-WAN hardware and software specifications

Below are Exinda SD-WAN hardware (standalone) and software specifications.

Exinda SD-WAN EXSD-300

Exinda SD-WAN EXSD-300 Hardware Specifications

Specification	Details
Mechanical dimensions	438(W) x 292.1(D) x 44(H) mm, 17.25″(W) x 11.5″(D) x 1.73″(H)
Weight	10.4 lbs
Input power requirement	200 W full-range ATX
USB ports	2 (for cellular data)
LAN ports (10/100/1000 baseT, auto-sensed)	4 RJ45 Ethernet WAN ports. 4 more or 8 more RJ45 Ethernet WAN ports add-on option
Certifications	FCC, CE, RoHS-5, ICES-03, UL, cUL
Operating temperature	32 – 104°F, 0 – 40°C
Operating humidity range	20 - 90% RH
Storage temperature range	-4 – +158°F, -20 – +70°C

Exinda SD-WAN EXSD-300 Software Specifications

Specification	Details
Max throughput	Base: 1 Gbps (load balancing), 300 Mbps (standalone) , 100 Mbps (peered). Higher performance available in EXSD-1000 models
Max number of concurrent IP sessions	150,000 (1,000,000 with EXSD-1000 and EXSD-10G models)
Device management	SNMP, Remote Syslog, Email alerts
DHCP and DNS servers	DNS relay, Parallel DNS optimization, DHCP server
DDNS	Support for dynamic DNS for multiple interfaces
WAN Configuration	Static IP, PPPoE, DHCP or Pass Through. Failover-only or aggregate modes for cellular and other WAN ports. Interface binding
Routing	NAT and IP forwarding, QoS and inbound/outbound VOIP quality management

Exinda SD-WAN EXSD-1000

Exinda SD-WAN EXSD-1000 Hardware Specifications

Specification	Details
Mechanical dimensions	438(W) x 292.1(D) x 44(H) mm, 17.25″(W) x 11.5″(D) x 1.73″(H)
Weight	10.4 lbs
Input power requirement	80 plus 250 W full-range ATX
USB ports	2 (for cellular data)
LAN ports (GbE, auto-sensed)	2 GbE copper RJ45 Ethernet connector. One WAN port to LAN port fail-to-wire in case of a power outage
WAN ports (GbE, auto-sensed)	8 GbE copper WAN ports (model E)
Certifications	FCC, CE, RoHS-2, UL
Operating temperature	32 – 104°F, 0 – 40°C
Operating humidity range	20 - 90% RH
Storage temperature range	-4 – +158°F, -20 – +70°C

Exinda SD-WAN EXSD-1000 Software Specifications

Specification	Details
Max throughput	1 Gbps (load balancing), 940 Mbps (standalone) , 800 Mbps (peered)
Max number of concurrent IP sessions	1,000,000
Device management	SNMP, Remote Syslog, Email alerts
DHCP and DNS servers	DNS relay, Parallel DNS optimization, DHCP server
DDNS	Support for dynamic DNS for multiple interfaces
WAN Configuration	Static IP, PPPoE, DHCP or Pass Through. Failover-only or aggregate modes for cellular and other WAN ports. Interface binding
Routing	NAT and IP forwarding, QoS and inbound/outbound VOIP quality management

Exinda SD-WAN EXSD-10G

Exinda SD-WAN EXSD-10G Hardware Specifications

Specification	Details
Mechanical dimensions	438(W) x 292.1(D) x 44(H) mm, 17.25″(W) x 11.5″(D) x 1.73″(H)
Weight	10.4 lbs
Input power requirement	80 plus 250 W full-range ATX
USB ports	2 (for cellular data)
LAN ports (GbE, auto-sensed)	2x 10 GbE fiber Ethernet connectors

Specification	Details
WAN ports (GbE, auto-sensed)	10x 1 GbE copper WAN ports, 2x 10 GbE fiber Ethernet ports
Certifications	FCC, CE, RoHS-2, UL
Operating temperature	32 – 104°F, 0 – 40°C
Operating humidity range	20 - 90% RH
Storage temperature range	-4 – +158°F, -20 – +70°C
Storage humidity range	5 – 95%, non-condensing

Exinda SD-WAN EXSD-10G Software Specifications

Specification	Details
Max throughput	10 Gbps (standalone) , 800 Mbps (peered)
Max number of concurrent IP sessions	1,000,000
Device management	SNMP, Remote Syslog, Email alerts
DHCP and DNS servers	DNS relay, Parallel DNS optimization, DHCP server
DDNS	Support for dynamic DNS for multiple interfaces
WAN Configuration	Static IP, PPPoE, DHCP or Pass Through. Failover-only or aggregate modes for cellular and other WAN ports. Interface binding
Routing	NAT and IP forwarding, QoS and inbound/outbound VOIP quality management

0.3 Exinda SD-WAN licensing

Exinda SD-WAN requires a specific license to be activated.

0.3.1 Entering license key

Once you log in to the Exinda SD-WAN Management Interface, enter the Activation license on the Admin tab.

For more information, refer to Accessing the Exinda SD-WAN Management Interface (page 14).

> One license can only be used on a single appliance.

Exinda SD-WAN Management Interface

0.4 Accessing the Exinda SD-WAN Management Interface

The Exinda SD-WAN takes approximately 60 seconds to initialize after powering up. After that, you can access the Exinda SD-WAN Management Interface. Connect an Ethernet cable from a PC to any of the Exinda SD-WAN's LAN ports and go to `http://192.168.254.99/` in a browser.

The Exinda SD-WAN Management Interface is accessible on any computer with a web browser on the local network. With the local network configured, it is not necessary to plug the computer directly into the Exinda SD-WAN in order to access the Exinda SD-WAN Management Interface.

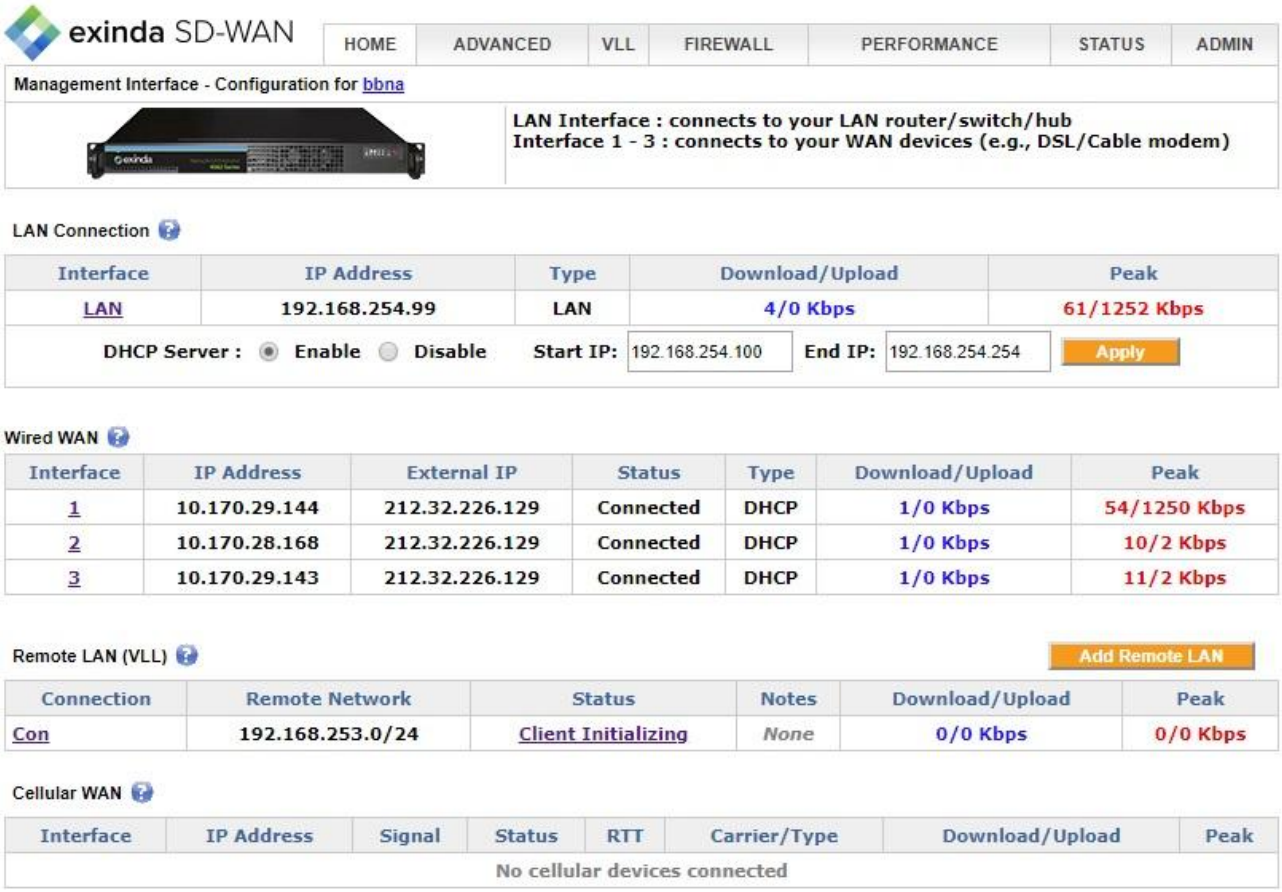
If the Exinda SD-WAN Management Interface cannot be accessed, make sure the management computer is configured to accept a "dynamic IP" address from a DHCP server which is in this case, the DHCP server of the Exinda SD-WAN. By default, the DHCP server of the Exinda SD-WAN is enabled, but it can be disabled through the Exinda SD-WAN Management Interface. In order to access the Exinda SD-WAN Management Interface when the DHCP server is disabled and no other active DHCP is accessible, a static IP address should be assigned to the management computer. It is recommended to use the static IP address `192.168.254.10` for the management computer in this case.

The Exinda SD-WAN Management Interface presents up the following tabs to access its functionality: Home, Advanced, VLL, Firewall, Status, and Admin.

0.5 Connect Exinda SD-WAN to broadband modems

Exinda SD-WAN requires connection of one or more modems, such as DSL, cable, or cellular broadband. Configure the modems for operation according to the ISP's instructions and then configure the WAN ports of the Exinda SD-WAN. In many cases the modems are set for DHCP by default, and no additional configuration is required. Some cable modems may require a power-cycle (turn off and on) to associate with a new MAC address after connecting to the Exinda SD-WAN.

Note that some older modem models may require a reset to associate with a new MAC address when connecting to the Exinda SD-WAN. This may further require the modems to be reconfigured with the parameters from the ISP.



Screenshot 1: Exinda SD-WAN Management Interface

In order to connect each wireline modem, use an Ethernet cable to connect the "LAN" or "Ethernet" port of the modem and connect the other end of the cable to any wired WAN port of the Exinda SD-WAN. One of the LEDs on the connector on the Exinda SD-WAN lights up after both the modem and the Exinda SD-WAN are powered on and the modem is properly connected to the Exinda SD-WAN.

If the modems do not use DHCP, the WAN connection details need to be configured for each non-DHCP modem in the Exinda SD-WAN Management Interface, as detailed below.

0.5.1 Configuration of wired WAN ports

For each wired WAN port there is a corresponding status row on the Home tab. Each port is labeled with an index from 1 (WAN1) to 4 (WAN4) (or 2, 8 or 12 depending on the model) which is visible on the front panel of the Exinda SD-WAN, as well as in the left column of the tab of the Exinda SD-WAN Management Interface.

Each active wired WAN port on the Exinda SD-WAN which is connected to a modem needs to be configured with an IP address.

To configure a wired WAN port, click on the corresponding port index in the first column of the tab. If the wired WAN port is not in use, select **Disable** and click **OK**. Otherwise, select **Enable**, then specify the configuration mode for the WAN port, either DHCP, Static, PPPoE, or Pass Through, as appropriate.

After configuring each wired WAN port, click **OK** to save the corresponding WAN port settings.

Since there is probably more than one service account being used with the Exinda SD-WAN, make sure the information entered corresponds to the correct modem and port index as determined by how the modems are connected to the Exinda SD-WAN with the Ethernet cables.

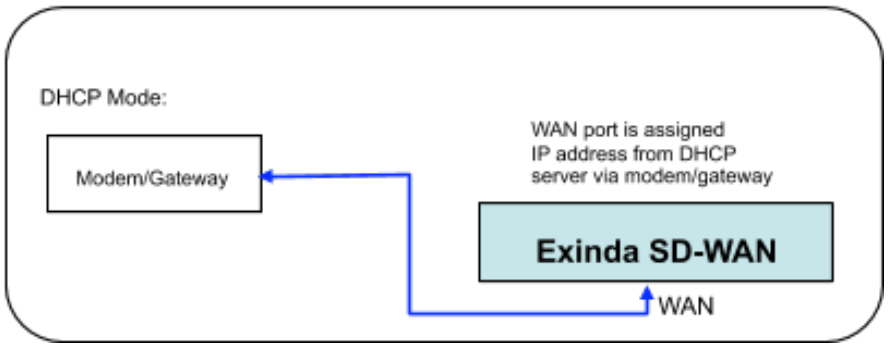
Once a WAN port is configured, the **IP Address** column for the corresponding row is filled in automatically. The "External IP Address" is the IP address that can be used to reach the corresponding WAN port from the Internet. This

address usually differs from the IP address of the WAN port when a dynamic IP address is assigned via DHCP. The **Status** column corresponding to the WAN port is updated, as appropriate.

For each active WAN port, the tablemenu shows the rate information on each interface for monitoring the status of each Internet connection in real time.

DHCP mode

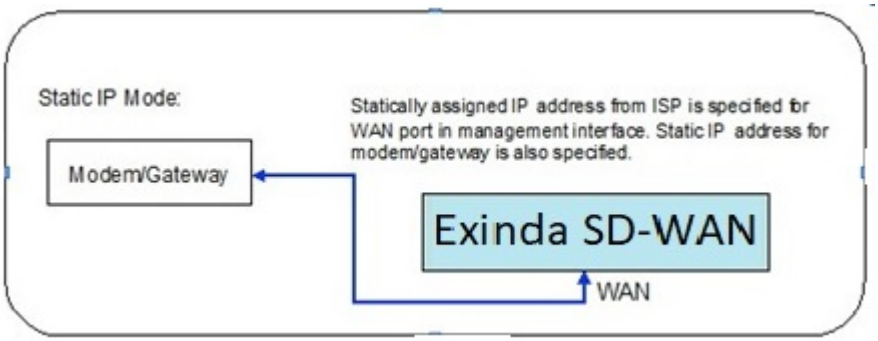
This is the default configuration mode for each wired WAN port on the Exinda SD-WAN. Typically a DSL or cable modem has a DHCP server which is capable of assigning an IP address, called a "dynamic IP address". In this case, the DSL or cable modem automatically configures the attached wired WAN port on the Exinda SD-WAN and no manual configuration is necessary. Optionally, alternate DNS servers may be specified that override those that are provided by the modem.



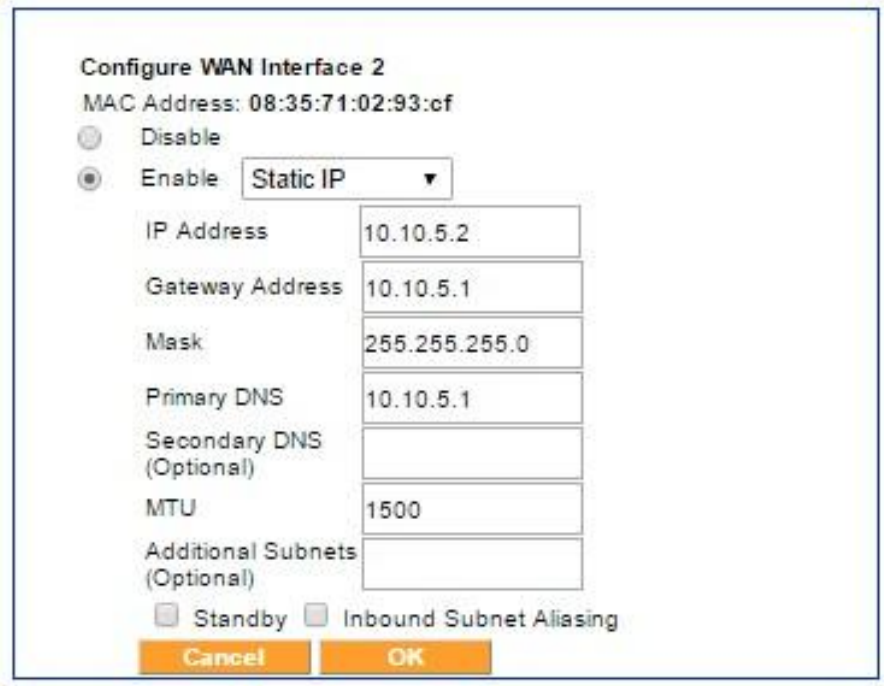
Screenshot 2: The DHCP Mode

Static IP mode

If a static IP address is assigned to a service account from the ISP, then the Static IP mode should be selected for the corresponding Exinda SD-WAN wired WAN port. The assigned static IP address needs to be entered in the User Configuration tab for the corresponding Exinda SD-WAN wired WAN port. If the ISP has assigned several static IP addresses for the same service account, one of these static IP addresses needs to be assigned to the corresponding wired WAN port on the Exinda SD-WAN.



Screenshot 3: The Static IP mode



Screenshot 4: An example of Static IP configuration for WAN interface

The **Gateway IP** address, the **Mask** of the network, and **Primary DNS** for the service account also need to be filled in; these parameters should be provided by the ISP. You can check the **Inbound Subnet Aliasing** check box if required. A field for optionally entering an IP address for a secondary DNS server is also provided.

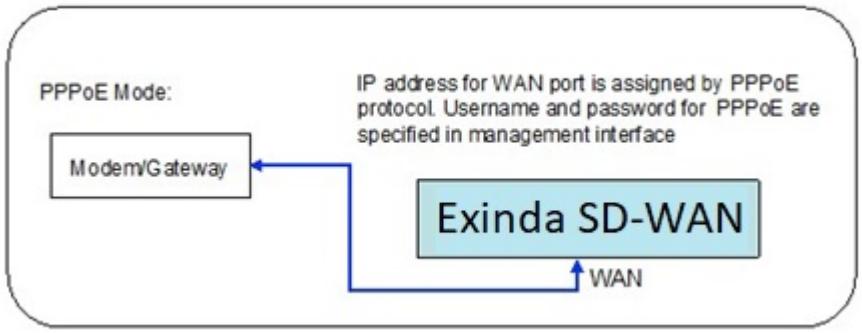
Finally, one or more IP subnets may be specified in **Additional Subnets**. The additional subnets should be specified in CIDR notation (for example, `172.16.1.0/24`) with comma deliminators. Normally, this field should be left blank, but if one or more additional subnets are specified, the designated WAN interface which is in Static IP mode is prepared to send and receive traffic to and from the specified subnet.

Inbound subnet aliasing

For each WAN port configured in the Static IP mode, there is an option to activate the Inbound Subnet Aliasing. If this option is enabled, the Exinda SD-WAN device acts as a proxy in the ARP protocol for all IP addresses in the IP address range that are specified by the given IP address and subnet mask. This may be necessary in order for inbound traffic from the Internet to reach all of the devices in the specified subnet.

PPPoE

Some of the older DSL modems use the PPPoE protocol to configure IP addresses. If that is the case, the PPPoE mode should be selected for the corresponding Exinda SD-WAN wired WAN port. The username and password given by the ISP for the corresponding service account should be entered for the corresponding Exinda SD-WAN wired WAN port.



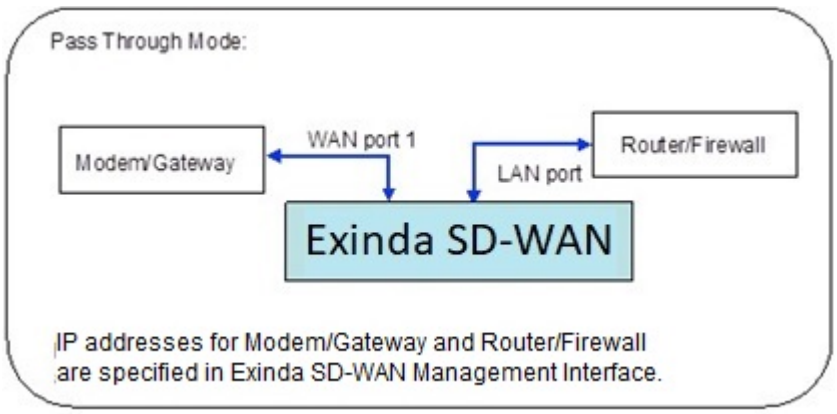
Screenshot 5: The PPPoE mode

Screenshot 6: The PPPoE mode menu

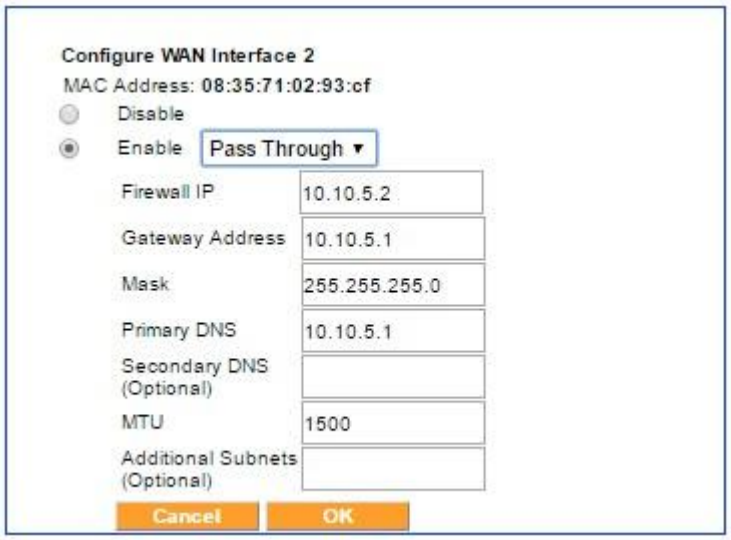
If there is uncertainty as to what type of IP address configuration schemes are used by the modems, contact your ISP.

Pass Through mode

When installing the Exinda SD-WAN in an existing network with a single wired WAN backhaul connection, reconfiguration of the legacy network is not required for an Exinda SD-WAN that is configured in the Pass Through mode. This mode is available on the WAN ports. This can be useful if the legacy network is relatively complex, and the network administrator does not desire to make any configuration changes to the existing network. For example, the network administrator may wish to retain all of the existing configuration parameters of the firewall device in the legacy network.



Screenshot 7: The Pass Through mode



Screenshot 8: The Pass Through mode menu

In legacy networks, a gateway or modem device that provids the WAN backhaul connection is connected directly to a router/firewall device. After installation of the Exinda SD-WAN in the Pass Through mode, the Exinda SD-WAN is inserted in-line between the gateway router/modem and the router/firewall device with the gateway/modem connected to one of the WAN ports and the router/firewall connected to one of the Exinda SD-WAN LAN ports, as indicated in the illustration above. In order to configure the Pass Through mode, the Exinda SD-WAN Management Interface prompts the user to enter the IP address of the gateway/modem to be connected to that WAN port, the IP address of the firewall, the netmask of the network behind the firewall device, and the IP address of the primary DNS server. An entry for the IP address of a secondary DNS server is optional.

Note that in the Pass Through mode, WAN port 1 is not assigned an IP address. Also, it is important to note that by configuring WAN port 1 in the Pass Through mode, the Exinda SD-WAN disables its DHCP server*. The values entered on the Pass Through mode settings are exactly identical to the values for the firewall.

* As a result, when the Exinda SD-WAN is configured in Pass Through mode, it may be necessary to manually assign a static IP address to the PC which is used to access the Exinda SD-WAN Management Interface, if there is no active DHCP server to assign it a dynamic IP address.

Standby mode

Each enabled WAN port can be put in the Standby mode if desired. In this mode, a WAN port is not normally used unless no other WAN connectivity is available. This mode should be used if it is desired to use the WAN resource only as a backup in case of failure of the primary WAN connections. In order to put a WAN port in the Standby mode, select the displayed check box.

0.5.2 Using a Cellular Mobile Data Card

The Exinda SD-WAN has two USB ports which may be used as WAN interfaces for connecting to a cellular data modem. Please contact Support for the list of supported air cards.

In order to use your data card, first configure it with your personal computer using the instructions from your mobile wireless service provider. Once the card is configured, you can use it with your Exinda SD-WAN. To do this, plug your wireless data card into the Exinda SD-WAN after it has booted up. After a few seconds, the Exinda SD-WAN Management Interface includes the status for Cellular WAN interface or interfaces in the table displayed at the bottom of the Home tab.

In order to configure the cellular WAN interface, on the home page of the Exinda SD-WAN Management Interface, click the mouse on the interface index on the left side of the Cellular WAN connection table. A menu is displayed for

configuring the corresponding interface as CDMA or HSPA/GSM and for optionally setting the interface into standby mode. The **Carrier** and, depending on the mode, **APN** may need to be entered. The **Username** and **Password** may also be required for configuring the interface.

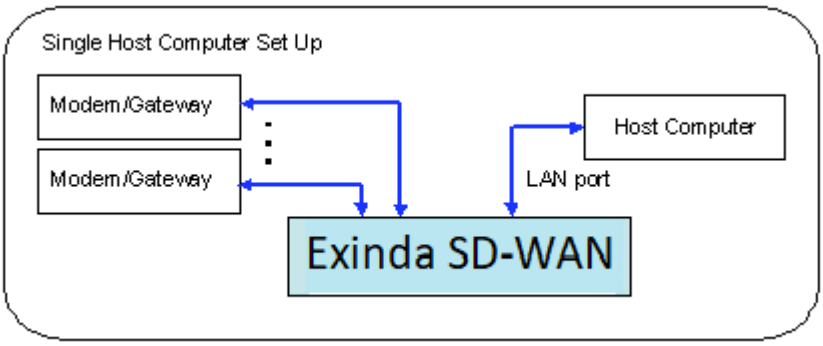
When the cellular WAN interface is in the Standby mode, it is only used when all other WAN interfaces are in the inactive state. This is useful if the cellular WAN interface is used for a service provider that charges a fee that depends on data usage. When at least one of the other interfaces enters the active state, the cellular WAN interface is not used while it is in the Standby mode. When the cellular WAN interface is not in the Standby mode, the Exinda SD-WAN uses the cellular WAN interface as much as possible in order to improve performance.

0.6 Connect PC and local network to Exinda SD-WAN

After setting up the modems that are connected to the Exinda SD-WAN, any of the LAN ports on the Exinda SD-WAN accesses bonded Internet links. There are several ways the Exinda SD-WAN LAN ports can be used.

0.6.1 As a regular Ethernet connection

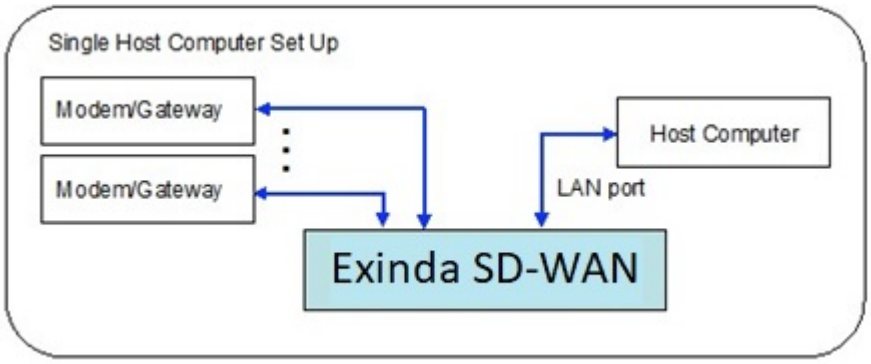
Connect an Ethernet cable to any of the LAN ports of the Exinda SD-WAN and attach the other end of the Ethernet cable to a PC or laptopc which is provided bonded Internet access. Other PC or laptops can plug into the other LAN ports of the Exinda SD-WAN.



Screenshot 9: Exinda SD-WAN LAN ports used as a regular Ethernet connection

0.6.2 By using an Ethernet Switch

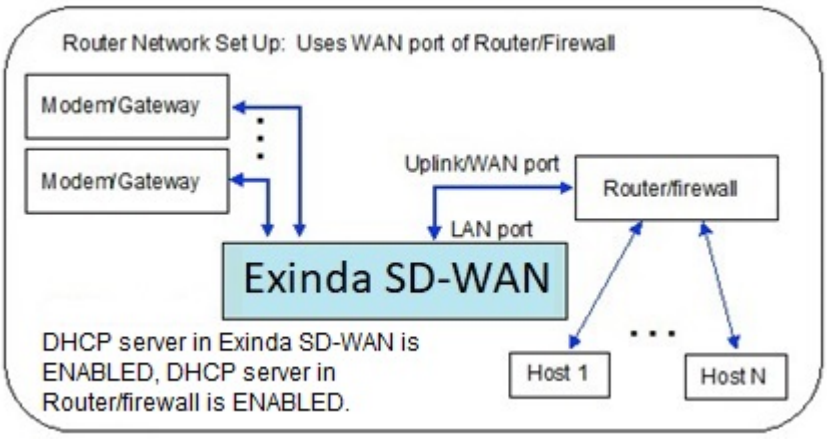
If the number of computer devices (such as PCs and laptops) to be supported is greater than the number of LAN ports on the Exinda SD-WAN (two), an Ethernet switch can be connected to one of the LAN ports of the Exinda SD-WAN. Any port of the Ethernet switch may also be used to provide bonded Internet access to a local device.



Screenshot 10: Exinda SD-WAN LAN ports used with an Ethernet switch

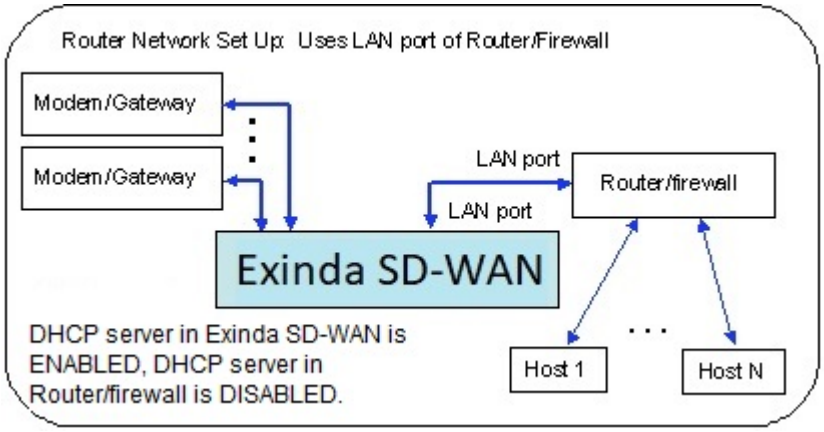
0.6.3 With a Router

Connect the WAN/Internet port of the router to one of the Exinda SD-WAN LAN ports. The DHCP server in the Exinda SD-WAN should be enabled to assign the router/firewall an IP address. The DHCP server in the router/firewall should also be enabled for the host computer devices which are attached to the router/firewall through the LAN port of the router/firewall. It may be necessary to configure the DHCP server of the router/firewall to set the DNS server address for its clients to the IP address of the Exinda SD-WAN (by default this is set to `192.168.254.99`) rather than the IP address of an external DNS server.



Screenshot 11: Exinda SD-WAN LAN ports used with a router WAN port

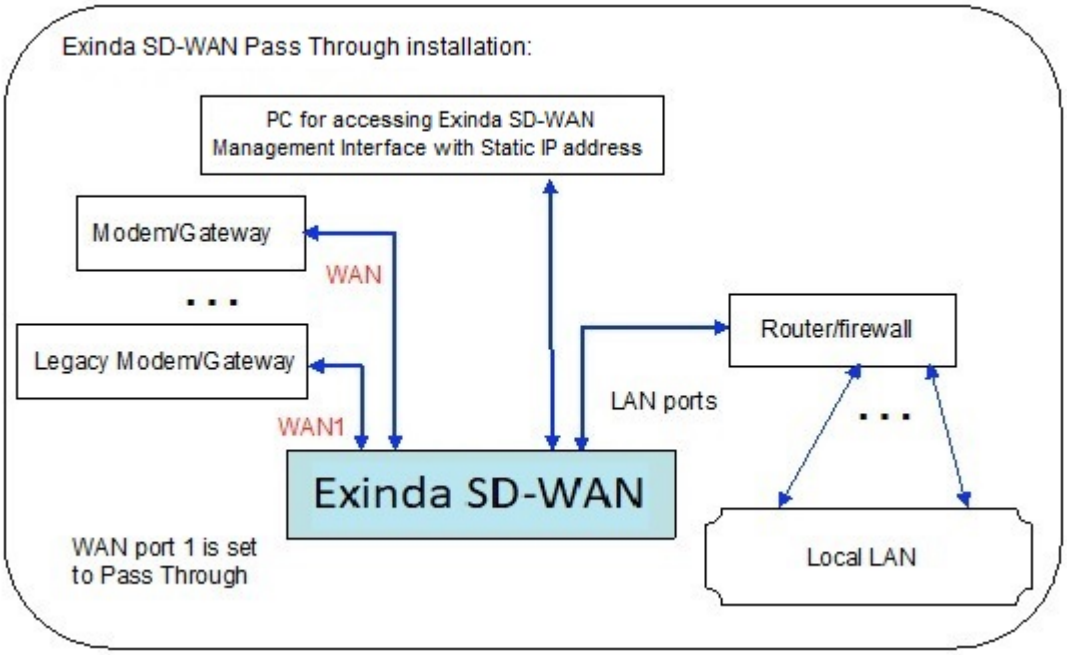
Alternatively, one of the Exinda SD-WAN LAN ports can be connected to a LAN port on the router. In this case, the DHCP server needs to be disabled on the router, so that it does not conflict with that of the Exinda SD-WAN. With this configuration, UPnP support is available.



Screenshot 12: Exinda SD-WAN LAN ports used with a router LAN port

0.6.4 Configuring the Pass Through mode

The Exinda SD-WAN device is inserted in-line between the legacy modem/gateway and the router/firewall. The legacy modem/gateway is connected to WAN port 1 of the Exinda SD-WAN and the router/firewall is connected to the LAN port of the Exinda SD-WAN. Additional modem/gateways for the network are connected to other WAN ports of the Exinda SD-WAN. The following illustration shows the network above after installation of the Exinda SD-WAN.



Screenshot 13: Exinda SD-WAN Pass Through configuration

The Exinda SD-WAN can first be configured by plugging a PC into one of the LAN ports of the Exinda SD-WAN, as shown above, and accessing the Exinda SD-WAN Management Interface. After the Exinda SD-WAN is appropriately configured, the Exinda SD-WAN Management Interface can be accessed by any PC on the Local LAN.

Note that when the Exinda SD-WAN is configured in the Pass Through mode, the DHCP server within the Exinda SD-WAN is disabled. Therefore, it is generally necessary to manually assign a static IP address to the PC through which the Exinda SD-WAN Management Interface is accessed.

0.7 Advanced features

Here you can find the advanced features of the Exinda SD-WAN.

IP address for Exinda SD-WAN LAN

By default, the LAN interface of the Exinda SD-WAN is assigned the IP address `192.168.254.99`. This is the IP address through which the Exinda SD-WAN Management Interface is accessed.

It is possible to change the IP address of the Exinda SD-WAN LAN interface. This should be done with extreme care, as changing this affects the manner in which the Exinda SD-WAN Management Interface is accessed. In particular, it is important to remember the IP address that is assigned to the Exinda SD-WAN LAN. It is not possible to access the Exinda SD-WAN Management Interface without this information.

To set the Exinda SD-WAN LAN IP address, click the Home tab of the Exinda SD-WAN Management Interface. In the LAN configuration table, in the Interface column, click **LAN**. A prompt appears requesting for an IP address. If the value is changed for this IP address, it is imperative that the new value be remembered. The network mask for the Exinda SD-WAN LAN can also be set under **Mask**. By default, the network mask is set to `255.255.255.0`.

DHCP server

The DHCP server on the Exinda SD-WAN can be enabled or disabled via the radio buttons on the Home tab in the LAN configuration table. The “starting IP address” for the DHCP server can also be configured here. When the DHCP server inside the Exinda SD-WAN is enabled, it starts assigning dynamic IP addresses starting from the configured address. This may be useful in some cases to avoid conflicts with manually assigned static IP addresses. The default starting IP address

is 192.168.254.100. An ending IP address can also be specified. The default ending IP address is 192.168.254.254.

The DHCP server is enabled by default. It is automatically disabled when the Pass Through mode is enabled on any of the WAN ports.

The specified IP address range for DHCP is also the range of local IP addresses that can be reached by VPN clients that are terminated on the Exinda SD-WAN.

The DHCP lease time and maximum number of leases can be set from the "DHCP Server Additional Settings" section in the Advanced tab. The gateway IP and WINS Server IP may also be set there. The name of the server IP for internal domains may be specified as well.

Support for PPTP

The Exinda SD-WAN is able to terminate VPN connections by using the PPTP protocol. By default, this feature is disabled.

To configure this feature, select the Advanced tab within the Exinda SD-WAN Management Interface and click on the entry for PPTP in the table (the default entry is **Disabled**). A pop-up window appears, which allows this feature to be configured. To enable the feature, select **Enable** and enter a name and password pair, and click **Apply**.

After the feature has been enabled, PPTP clients may access the LAN by using the same address range as DHCP with the specified name and password.

Support for UPnP

By default, the Exinda SD-WAN is configured to support UPnP which enables auto-configuration of IP addressing features for certain applications.

Normally, support for UPnP should be disabled when running the Exinda SD-WAN in the Pass Through mode since this functionality would already be provided by a device in the legacy network.

Inbound port forwarding

Inbound port forwarding allows external computers on the internet to access devices in the local network through the same IP address. Normally this feature is used with static IP address assignment, but it can be used with any of the IP address configuration modes for the Exinda SD-WAN WAN ports. Inbound port forwarding is not recommended for the Pass Through mode of operation on WAN interface 1, since this function, if required, would already be handled by the legacy network that was kept intact without any changes during the installation.

By default, all inbound Internet traffic is blocked, except for ICMP traffic. Selected inbound internet traffic can be allowed or blocked by configuration of one or more forwarding rules. To configure a rule for forwarding inbound Internet traffic, select the Firewall tab, and click **Add Firewall Rule**. Select **Inbound** as a **Direction**.

In order to configure a rule for forwarding inbound Internet traffic, an **Interface** must also be specified on the pop-up menu. You can specify **ALL WAN** which means that traffic from all WAN interfaces, wired or cellular is the target of the rule. Alternatively, a forwarding rule for a single WAN interface can be specified in the drop-down menu. In order for cellular WAN interfaces to become available, the corresponding cellular WAN interface should be configured first. In addition, if any remote LAN connections have been configured (with the optional VLL feature), they also appear in the menu as possible targets of the forwarding rule.

Traffic from a specific protocol or from all protocols can be specified as the target of the forwarding rule by selecting under **Protocol/Action**. **TCP**, **UDP**, **ICMP**, **IPSec**, and **PPTP** are available, as is **Any** which is interpreted as all protocols. A specific protocol other than the above can also be specified by selecting **Other** and entering the corresponding protocol number.

Adding an inbound forwarding rule causes the targeted traffic to be forwarded to the **Local IP** address designated in the pop-up menu, unless the **Discard** option is selected in which case the targeted traffic is discarded.

Specifying a WAN port number causes all traffic destined to the specified port to be forwarded to the specified Local IP address. More generally, a range of WAN ports can also be specified by designating a second WAN port, which is the

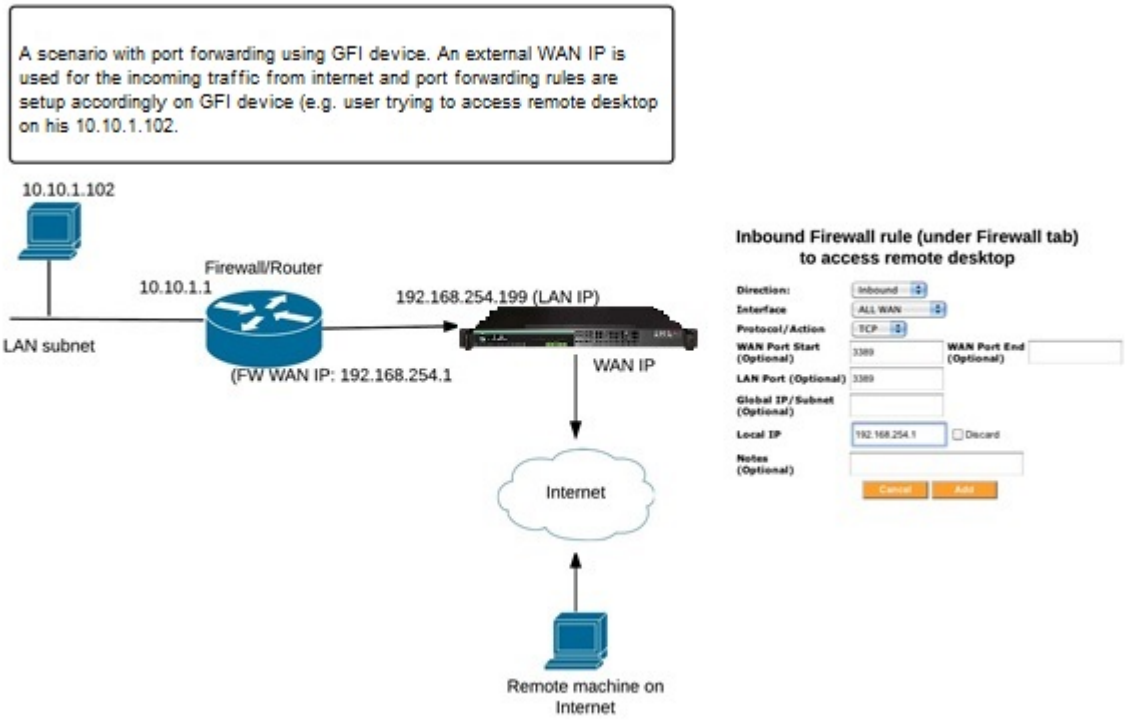
end of the port range. It is delivered to the same destination port unless a LAN port is specified, in which case it is delivered to the specified LAN port.

A **Global IP** address may also be optionally specified, which signifies that only that traffic which is destined to the specified Global IP address should be forwarded to the specified Local IP address.

A text string can also be entered in **Notes**, to provide a mechanism for the operator to remember the reason or context of the forwarding rule.

After specifying all desired conditions in a forwarding rule for inbound traffic, click **Add** to load the forwarding rule into the Exinda SD-WAN. Multiple forwarding rules can be added to provide more flexible forwarding of traffic. If a forwarding rule that was added previously needs to be deleted, click **Delete** next to the listed forwarding rule. If a forwarding rule needs to be edited, the rule can first be deleted and the modified rule can then be entered as before. The Exinda SD-WAN processes arriving traffic by sequential application of the specified forwarding rules. This means if there are conflicts in the forwarding rules, the forwarding rule nearest the top of the list takes precedence. By default, the list of forwarding rules is such that rules entered earlier is lower in the list, so the most recently added rule always take precedence.

Here is an example scenario for a user accessing his desktop remotely:



Screenshot 14: Example scenario for a user accessing his desktop remotely

Outbound port blocking and NAT

Outbound port blocking allows a network operator to block all outgoing traffic from a specified source port, protocol, and optionally a specified source IP address or subnet.

By default, all outbound internet traffic is allowed. To configure a rule for blocking outbound Internet traffic, click the **Firewall** tab to display the menu and click **Add Firewall Rule**. Select **Outbound** as a **Direction**. Use the menu under **Protocol/Action** to select which protocol should be denied outbound access.

Alternatively, you can specify an arbitrary protocol by selecting **Other** and entering the corresponding protocol number. You can also select **Deny Any** to deny all outbound traffic based on protocol. Finally, you can select the **No NAT** option if you wish to disable the Network Address Translation (NAT) function on the specified outbound traffic. By default, NAT is applied to all outgoing traffic, meaning that the source IP address of egress packets that originate on the Exinda SD-WAN LAN is replaced with the IP address of the corresponding WAN interface, and selecting the No NAT option disables the NAT function for the targeted traffic.

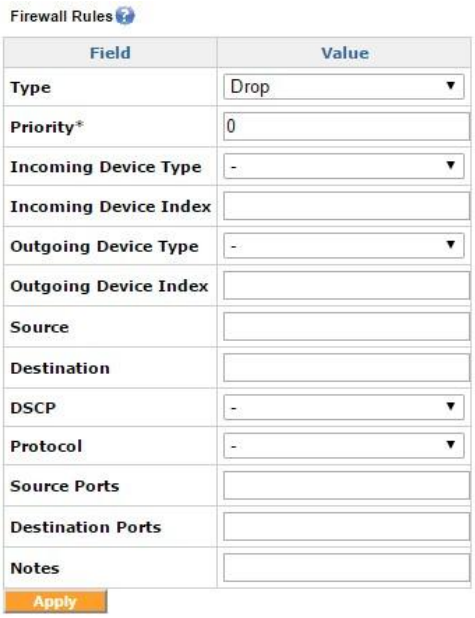
Optionally, a Source Port index for the targeted traffic can be specified. Thus, only packets with a Source Port value matching the entered value is targeted. Also optionally, a source IP address can be specified so that only traffic with a source IP address matching the designated address is targeted. Generally, an IP subnet can also be specified in CIDR notation, for example, `192.168.1.0/24`. In this case, traffic originating from the specified subnet is targeted. The targeted traffic by definition satisfies all the matching conditions, so that effectively the conditions are logically concatenated to specify the targeted traffic.

A text string can also be entered in **Notes**, to provide a mechanism for the operator to remember the reason or context of the outbound rule.

Multiple outbound blocking rules can be added to provide more flexible blocking of traffic. If a traffic blocking rule that was added previously needs to be deleted, click **Delete** next to the listed blocking rule. If a blocking rule needs to be edited, the rule can first be deleted and the modified rule can then be entered as before. The Exinda SD-WAN processes outgoing traffic by sequential application of the outbound rules specified. This means if there are conflicts in the outbound rules, the outbound rule nearest the top of the list takes precedence. By default, the list of outbound rules is such that rules entered earlier is lower in the list, so the most recently added rule always takes precedence.

Normally outbound blocking rules should not be specified when the Exinda SD-WAN is configured in Pass Through mode since such blocking would already be done by the legacy network.

Advanced firewall rules for filtering



Screenshot 15: The Firewall Rules configuration screen

The advanced firewall rules allow characterizing traffic based on the Incoming Device Type and the Outgoing Device Type, or both. The "Type" field is the action that the rule takes on the traffic that is matched. The type can be either ACCEPT, DROP or REJECT. ACCEPT takes the matched traffic, DROP drops the traffic and REJECT would send an ICMP unreachable packet to the sender and then DROP the packet.

The traffic can be filtered based on the Source IP, destination IP, source ports or destination ports. An IP subnet also can be specified with a CIDR notation, e.g. 192.168.1.0/24.

Multiple firewall rules can be added to achieve a combination by means of priority. The priority is in ascending order, so the rule with a lower priority is processed first. So to accept a particular IP address and drop all other traffic, we have the ACCEPT rule with a lower priority and the DROP rule with a higher priority.

DMZ support

Support for a DMZ (demilitarized zone) can be enabled through the Firewall tab within the Exinda SD-WAN Management Interface.

The DMZ feature of the Exinda SD-WAN allows the user to specify the IP address of a local computer that has been designated as the DMZ. The specified IP address is called the "DMZ IP address". When the Exinda SD-WAN receives a packet from the internet over any of the WAN ports then the Exinda SD-WAN forwards the packet to the specified DMZ address if none of the port forwarding rules apply to the given packet.

If no port forwarding rules are specified and a DMZ IP address is specified, then all packets received on a WAN port is forwarded to the local computer with the specified DMZ IP address. It should be noted that if one or more port forwarding rules are specified that they take precedence over the forwarding of traffic to a DMZ, if the DMZ feature is enabled. Moreover, it should be noted that any port forwarding that occurs as a result of the UPnP feature being enabled takes precedence over any port forwarding rules.

Setting up a DMZ is useful if there are several computers in the local network, but only one of them (that has been designated as the DMZ) is desired to be directly accessible via the Internet. Normally, support for DMZ should be disabled when running the Exinda SD-WAN in the Pass Through mode since a DMZ would already be implemented in the legacy network.

The DMZ feature can be configured by clicking on the status **Enabled** or **Disabled** for DMZ in the configuration table and selecting the appropriate radio button. If **Enable** is selected, then the IP address for the DMZ must be specified. When you click **Apply**, the DMZ feature is configured accordingly.

Dynamic DNS

The Exinda SD-WAN supports inbound load balancing and inbound link fail-over via Dynamic DNS (DDNS). This feature allows management of inbound traffic (traffic which is originally initiated from the Internet). This feature is configured via the Advanced tab. It is disabled by default and three modes are supported currently through the Dynamic DNS service at afraid.org, dyndns.org, and changeip.com. To properly configure this feature, a service account should first be set up with afraid.org, dyndns.org, or changeip.com. Details of the service are available from these service providers. Once the service account has been set up the corresponding mode can be selected by clicking on the status entry (“Disabled” or “Enabled”) for “Dynamic DNS” in the configuration table. The various options is displayed, and the Exinda SD-WAN Management Interface then prompts for a Username, Password, and Hostname, which should be provided by the Dynamic DNS provider. By clicking Apply, the Dynamic DNS feature is configured accordingly.

For afraid.org's round-robin DDNS to work correctly, it requires unlinking of entries for the same domain (one entry for each Exinda SD-WAN WAN connection is required). For more information, see the `afraid.org` FAQ at `http://freedns.afraid.org/`.

> DDNS is a service that is hosted by companies with no connection to GFI. GFI makes no warranty as to the reliability of these services. For mission critical applications, it is strongly advised that the reliability of the service be used considered before deployment.

Support for dynamic DNS on multiple interfaces is also available.

Screenshot 16: Multiple DYNDNS Setup screen

Load balancing weights

Weights may be set per interface for load balancing. These weights adjust the proportion of traffic that is handled by each WAN interface.

To configure these, click the Advanced tab and then click **Add** next to **Load Balancing Weights**.

For setting the weights per interface, it is recommended that you use the rounded value of the kbit/s rate of the respective WAN interfaces.

Connectivity check settings

The settings for connectivity check may be adjusted on the Advanced tab of the Exinda SD-WAN Management Interface. These settings determine how the Exinda SD-WAN discovers and monitors the connectivity of the individual WAN interfaces.

The Exinda SD-WAN attempts to reach external servers to determine if a WAN interface is successfully connected. The connectivity check proceeds in three phases:

1. Resolving connectivity check addresses

2. Pinging connectivity check addresses

3. Simultaneously pinging and attempting HTTP connections to connectivity check addresses

The maximum duration (in seconds) of each phase may be adjusted by clicking **Settings** in the **Index** column of the **Connectivity Check Settings** configuration table. If desired, to immediately check HTTP in addition to ICMP, the time for the ping phase may be reduced to zero. Be aware, though, of the bandwidth overhead of retrieving HTTP responses on very limited lines.

The Exinda SD-WAN internally manages a list of active server IPs that is used for these checks, which are automatically updated as long as the Exinda SD-WAN maintains a connection to the internet. Additional servers may be added manually by clicking **Add** next to **Additional Remote Servers for Connectivity Check** on the **Advanced** tab and entering the server's IP address. These servers should be responsive to ICMP or HTTP requests, or both, and be available with high reliability.

List of DHCP leases

A list of all dynamic IP addresses leased out by the Exinda SD-WAN DHCP server can be viewed on the **Status** tab. The MAC address, IP address, and possibly the machine name are listed for each IP address lease.

Remote syslog

A log of Exinda SD-WAN system events appears in the Status tab. The IP address of a Remote Syslog Server can be specified which is to be the recipient of log messages generated by the Exinda SD-WAN. After the IP address of the

Remote Syslog Server has been specified, click Apply to configure this feature.

Domain Name Blocking / DNS Redirection

Screenshot 17: The Domain Name Blocking / DNS Redirection Menu

Domain name blocking / DNS redirection is used to block a site or used to redirect to a particular IP for a site. For the DNS redirection to work, the Exinda SD-WAN device should be configured the same as the DNS server in the local network.

VLAN setup

Screenshot 18: The VLAN Setup menu

The VLAN setup can be used for creating 802.11q format frames with a particular tag. The "Device Type" would be WAN, LAN, or Cellular, followed by the "Device Index" which would be the index number. For WAN 1, you would enter '1' here. The "VLAN Tag" field contains the tag number, and "Bridge Index" contains the bridge index.

Netflow settings

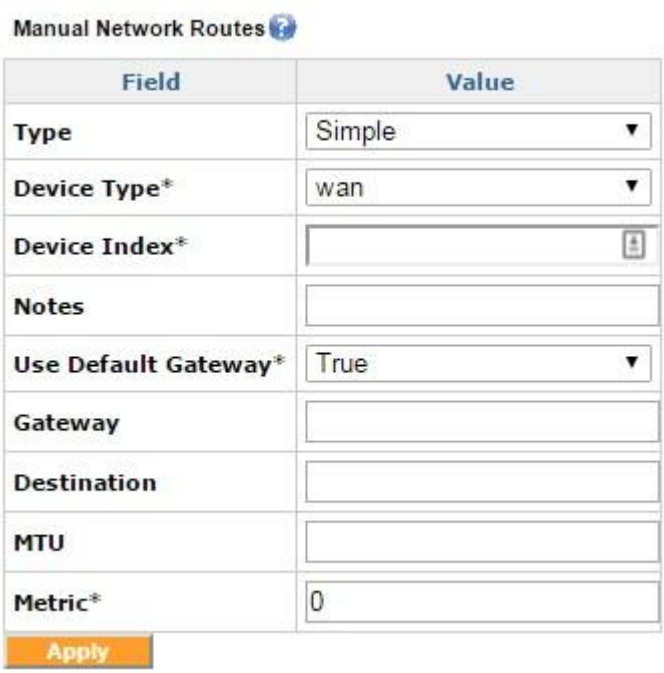
Screenshot 19: The Netflow Settings menu

The netflow settings are used to configure sending netflow data to a netflow server on the local area network of the Exinda device. The required parameters are the **Netflow Server IP** and the **Netflow Server Port**. The Netflow Version supports versions 1, 5, and 9.

Manual network routes

Manual routes are used in scenarios where you have multiple subnets on the LAN segment, or you want to specify certain subnet traffic to use a specific Remote LAN, or WAN, link. This feature can be configured by going to the Advanced tab on the Exinda SD-WAN Management Interface and clicking Add next to the Manual Network Routes

section:

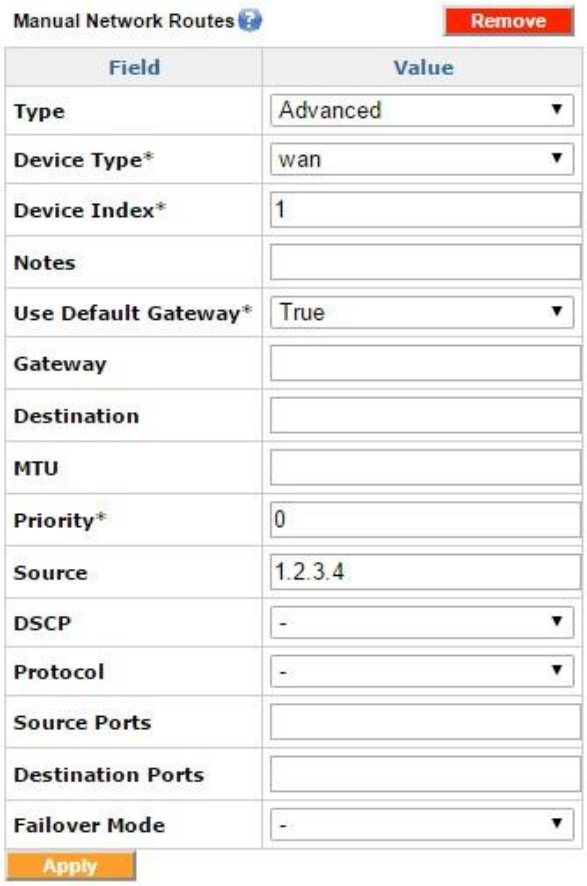


Screenshot 20: Manual Network Routes, Simple

This generates a pop-up window where the information specifying a manual route rule can be entered. The **Type** field specifies **Simple Route** or **Advanced Route**. **Device Type** identifies the interface/tunnel type for the traffic we are setting the route for. As an example, WAN or LAN subnets or VLL if the traffic is destined for a VLL tunnel. The **Destination** field specifies the destination IP address subnet to which the packets are routed to. This can be accomplished either through a device route or through a VLL route, based on the option chosen previously.

Choosing the **Advanced Route** as the **Type** exposes additional configuration options to identify the traffic including **Source IP/Subnet**, **DSCP**, **Protocol**, **Source Ports**, and **Destination Ports**. You can also modify the **Priority** and the Maximum Transmission Unit (**MTU**) size of the traffic.

The failover mode is used to configure the failover action in case of primary interface failure. It has 2 modes: "sticky mode" and "available mode". In case of a primary interface failure, the sticky mode transfers the traffic on to the secondary interface, and when the primary line comes back up, transfers the traffic back to the primary interface. With the "available mode", after the primary interface recovers, the traffic that failed- over earlier continues to use the failover interface. The newer sessions is routed over the primary interface as usual.



Screenshot 21: Manual Network Routes, Advanced

Interface groups

An "interface group" is an abstraction of a set of real interfaces that the user can manage with finer control. The user can define what interfaces (WAN, Cellular, VLL) are to be associated with a particular interface group, what percentage of each interface is to be used and if the group requires failover interfaces. The user can also define what type of traffic would traverse this bundled virtual interface.

Components of interface groups

Interface groups

This block gives the user the functionality to create a group which could then have filters and the outgoing interfaces associated with it.

Screenshot 22: Adding interface groups

Interface group interfaces

Once an interface group is created, the group's specific interfaces can be configured and added to the interface group. For instance the user can add WAN 1 and Cellular WAN 2 to a particular interface group.

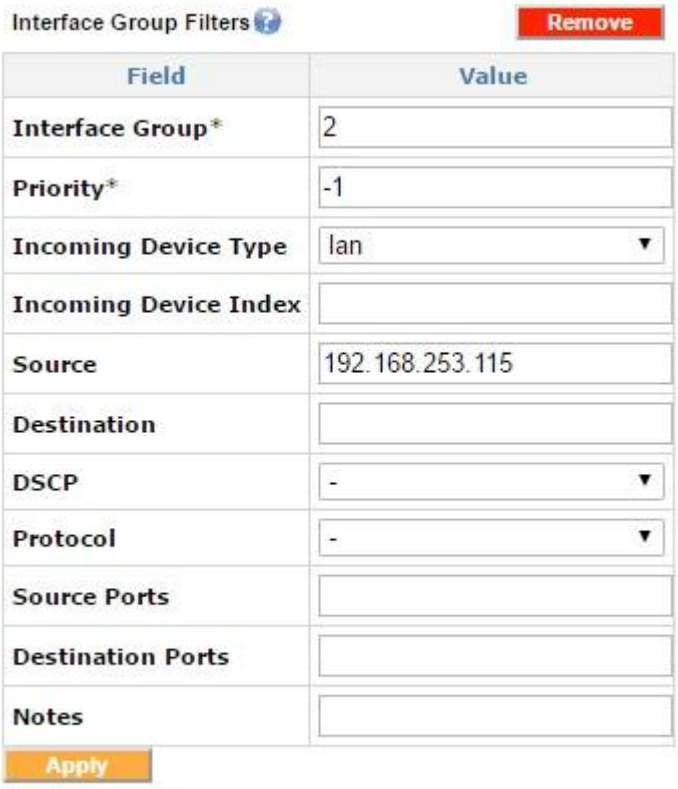
Index	Interface Group	Device Type	Device Index	Weight
1	1	wan	1	1.0
2	1	cellular	2	1.0

Screenshot 23: Interface group interfaces

In this example only WAN1 and Cellular WAN2 is included in this group.

Interface group filter

The interface group filter is used to filter the desired traffic types on a particular Interface Group.



Screenshot 24: Adding interface group filters

This sample filter directs all traffic from `192.168.253.115` onto Interface Group 2.

> The default Interface Group with index 1 should not be modified. Any additional desired Interface Groups should be added as new Interface Groups.

Interface Groups

Add

Index	Type	Notes
1	Hash	

Interface Group Interfaces

Add

Index	Interface Group	Device Type	Device Index	Weight
1	1	wan	-	0.0
2	1	cellular	-	0.0

Interface Group Filters

Add

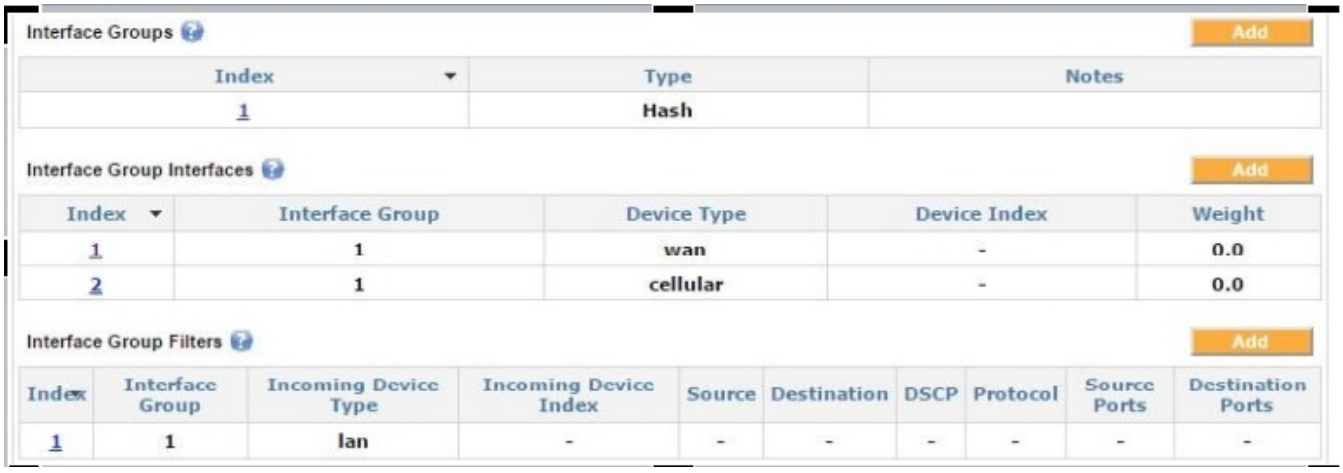
Index	Interface Group	Incoming Device Type	Incoming Device Index	Source	Destination	DSCP	Protocol	Source Ports	Destination Ports
1	1	lan	-	-	-	-	-	-	-

Screenshot 25: Interface Groups

The blank **Device Index** in this example indicates that all device type indexes should be selected.

The distribution of traffic within this interface group can be customized by using **Weights**. The "weight" indicates the proportion of traffic desired for a particular interface. A weight of 0.0 for all interfaces selected indicates an equalized distribution of the traffic. This would match all the incoming traffic on the LAN. These weights can be customized to load balance by changing the weights as desired.

Enable Capture All with group interfaces



Interface Groups

Add

Index	Type	Notes
1	Hash	

Interface Group Interfaces

Add

Index	Interface Group	Device Type	Device Index	Weight
1	1	wan	-	0.0
2	1	cellular	-	0.0

Interface Group Filters

Add

Index	Interface Group	Incoming Device Type	Incoming Device Index	Source	Destination	DSCP	Protocol	Source Ports	Destination Ports
1	1	lan	-	-	-	-	-	-	-

Screenshot 26: Enabling Capture All with interface groups

In this example, the weight of 1.0 for the VLL tunnel ensures all the traffic goes over the VLL interface. The other interfaces have weights of 0.0, which makes them a failover interface and only activate them in case the primary interface (in this example, the VLL interface) goes down.

Load balancing by using the interface groups

Interface Groups

Add

Index	Type	Notes
1	Hash	

Interface Group Interfaces

Add

Index	Interface Group	Device Type	Device Index	Weight
1	1	wan	1	0.7
2	1	wan	2	0.3

Interface Group Filters

Add

Index	Interface Group	Incoming Device Type	Incoming Device Index	Source	Destination	DSCP	Protocol	Source Ports	Destination Ports
1	1	lan	-	-	-	-	-	-	-

Screenshot 27: Load balancing with interface groups

Load balancing weights can be defined for each interface contained in the interface group interfaces. These weights indicate the proportion of traffic desired for the given interface.

In this example, the weights are set to 0 . 7 for WAN1 and 0 . 3 for WAN2, which results in 70% of the traffic being directed to WAN1 and 30% of the traffic being directed to WAN2.

Random group

Interface Groups

Add

Index	Type	Notes
1	Random	

Interface Group Interfaces

Add

Index	Interface Group	Device Type	Device Index	Weight
2	1	wan	-	1.0

Interface Group Filters

Add

Index	Interface Group	Incoming Device Type	Incoming Device Index	Source	Destination	DSCP	Protocol	Source Ports	Destination Ports
1	1	lan	-	-	-	-	-	-	-

Screenshot 28: Random interface group

In this example, the traffic matching the filter is randomly distributed across all interfaces that are included in the interface group interfaces for that group. Note that since the **Device Index** is left blank, then all WAN interfaces are included in this group. This load-balancing algorithm is essentially a round-robin algorithm.

> Advanced routes take precedence over the interface group filters, and therefore advanced routes can be used to create exceptions to the interface group filters.

VLAN tagging

Screenshot 29: VLAN tagging

The VLAN tags can be set for both WAN and LAN interfaces. The **Device Type** can be WAN or LAN, the **Device Index** here is the index number. The **VLAN Tag** field contains the tag number.

Bridge alias

Screenshot 30: A Bridge alias

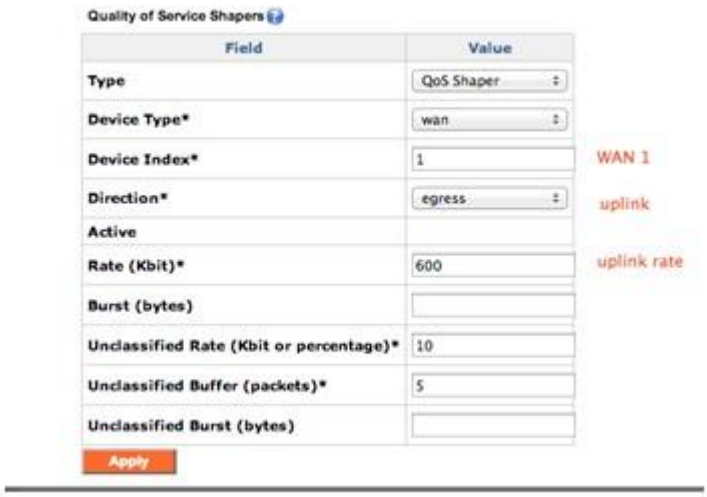
The Bridge alias is used to add a subnet alias to the LAN interface. This feature can be useful if there is more than one subnet in the local network.

QoS (Quality of Service)

The QoS feature can be configured through the **Advanced** tab on the Exinda SD-WAN Management Interface. This feature is used to guarantee a certain bandwidth for an application or to prioritize certain traffic, such as Citrix or SIP.

Quality of Service shapers

In order to use the QoS feature, a user must first create the WAN Shaper rule (**Quality of Service Shaper**) on the **Advanced** tab. A rate that is 85% of the rate provided by the ISP should be used as the shaper rule both for uplink (egress) and downlink (ingress).

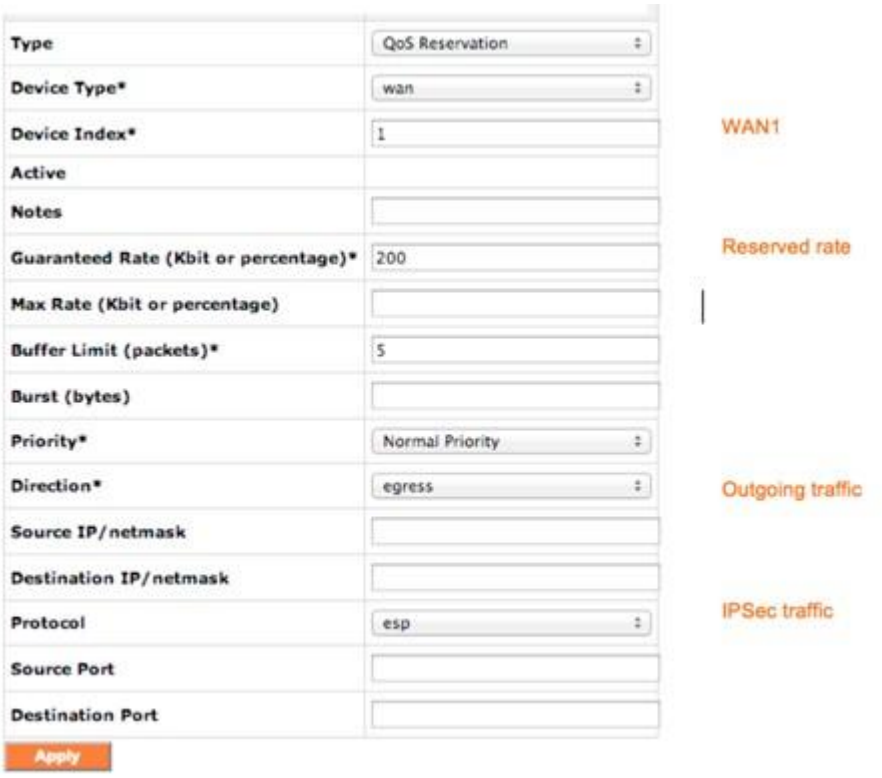


Screenshot 31: Quality of Service shaper example

In this example, the ISP uplink rate is 705 kbps, so the egress shaper for WAN1 is set to 85% of the available bandwidth, or 600 Kbps.

Quality of Service reservations

After creating the shaper rule for both ingress and egress, the application traffic reservation and prioritization can be created using **Quality of Service Reservations**. The following example illustrates how to reserve 200 Kbps uplink for IPSec traffic:



Screenshot 32: Quality of Service reservation example

For prioritizing real time traffic, the **Priority** field can be changed from **Normal Priority** to **High Priority**. Advanced application specific QoS can be achieved with Exinda Network Orchestrator. For more information, see www.gfi.com/exinda.

Prioritization of VLL traffic (example)

1. On the **Advanced** tab, add a new QoS reservation rule with the destination port as 9899 for the UDP protocol .

2. Create another rule using port 9899 in case your remote LAN has both client and server configured on the same GFI device:

Screenshot 33: Example of prioritization of VLL traffic

Virtual leased line

The Exinda SD-WAN can be configured to peer/mate with another Exinda SD-WAN device that has a server license to create a data communication tunnel between the pair of Exinda SD-WAN units. By virtue of combining the capacity of multiple resources, the capacity of the tunnel created can be close to the sum of the capacities of the individual resources. Moreover, the reliability of the communication tunnel is increased since the communication tunnel remains operational as long as there is at least one active communication path between the Exinda SD-WAN devices.

It is also possible for each Exinda SD-WAN to peer with multiple Exinda SD-WAN devices. A bi-directional tunnel can be set up between each pair of Exinda SD-WAN devices as long as one Exinda SD-WAN has the server license activated. For each bidirectional tunnel, one Exinda SD-WAN device is designated as a “server” and the other is designated as a “client”. For example, one Exinda SD-WAN device might act as a server for several other Exinda SD-WAN devices, each of which acts as a client.

A tunnel can be configured in two possible modes, “default” and “proxy”. For each end of the tunnel, there is an associated LAN address. In the default mode, traffic that appears at one Exinda SD-WAN that matches the associated LAN address of the remote Exinda SD-WAN is forwarded to the remote Exinda SD-WAN through the tunnel. In the proxy mode, all traffic that appears at the Exinda SD-WAN on the client side that does not match the local LAN address is sent to the remote Exinda SD-WAN device over the tunnel. Also, in proxy mode, traffic appearing at the Exinda SD-WAN on the server side that matches the LAN address of the Exinda SD-WAN on the client side is forwarded to the Exinda SD-WAN device on the client side over the tunnel. LAN addresses are specified by an IP address and associated network mask.

The VLL feature is configured on the **Home** tab of the Exinda SD-WAN Management Interface, in the **Remote LAN** table. It looks similar to the following:

Screenshot 34: Remote LAN example

To create a tunnel, two Exinda SD-WAN devices are required. A tunnel is configured by creating an instance of a server connection at one Exinda SD-WAN and creating a matching instance of a client connection at the other Exinda SD-WAN. For security purposes, each bi-directional tunnel has an associated connection name and password, which must be specified identically at each end of the tunnel when the tunnel is configured.

By default, packets that are sent over the tunnel are encapsulated in UDP packets in order to provide robustness against certain types of packet filtering that may be commonly present in ISP access networks.

To create an instance of a server connection or a client connection at a Exinda SD-WAN device:

1. Go to the **Home** tab of the Exinda SD-WAN Management Interface for that Exinda SD-WAN device.

2. Click **Add Remote LAN** at the top of the Remote LAN table.

3. Set the **Connection Mode** as **Client** or **Server** in the menu at the top of the pop-up.

To configure the device in the **Server** mode:

1. Select **Server** for the **Connection Mode**.

2. Enter a text string for the **Connection Name** field, and an associated password in the **Password** field. To provide security, these fields must exactly match the corresponding fields for the associated connection at the other Exinda SD-WAN device in order for the tunnel to become operational.

3. Specify the network address of the LAN associated with the remote Exinda SD-WAN device in the **Remote LAN Network** and the **Remote LAN Netmask** fields.

4. After the parameters for the connection are entered, click **Add** to add the corresponding connection.

After a connection is added, the parameters can be edited by clicking on the corresponding entry in the **Remote LAN** table, modifying the entries in the pop-up menu, and clicking **Edit**. You can also remove a connection by deleting it.

To configure the device in the **Client** mode:

1. Select **Client** for the **Connection Mode**.

2. Specify which WAN ports on the Exinda SD-WAN are used for the tunnel by selecting or clearing each listed interface as appropriate, or selecting **ALL** to use all available interfaces for the tunnel.

3. The specification of which WAN ports is used on the remote side of the tunnel (that is, the server side) is done by providing a list of IP addresses (separated by commas) of these WAN ports in the **Remote IP/Name** field. Alternatively, instead of a list of IP address, a DNS domain name can be entered. The domain name should resolve to the list of IP addresses associated with the server that is used for the tunnel.

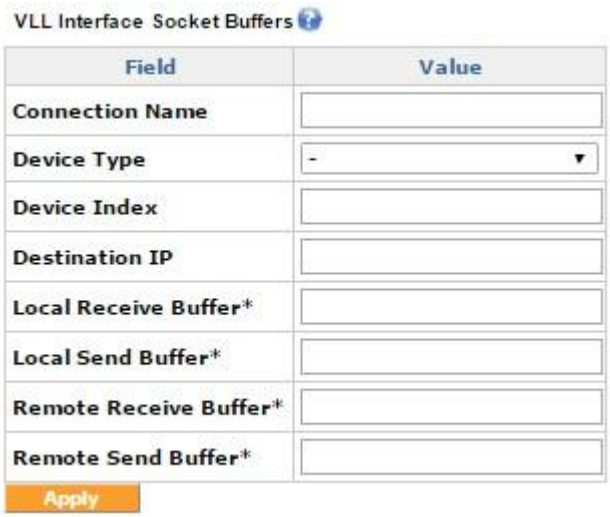
4. Specify the network address of the remote LAN in the **Remote LAN Network** and the **Remote LAN Netmask** fields.

5. The **Connection Name** and **Password** fields should contain text strings which exactly match the associated connection entries at the remote Exinda SD-WAN.

6. After the parameters for the connection are entered, click **Add** to add the corresponding connection.

The order in which the server and client are configured is arbitrary. Currently, the Exinda SD-WAN does not support overlapping LAN addresses on each Exinda SD-WAN; the network addresses for the Exinda SD-WAN devices at each end of the VLL tunnel must be distinct and non-overlapping. Once both the client and server devices are configured, the **Status** field of the **Remote LAN** table is appropriately updated on the Exinda SD-WAN Management Interface for each device. The entries in the **Status** column can be clicked on, and a pop-up menu appears that provides additional information regarding the state of the tunnel.

VLL Interface Socket buffers



Screenshot 35: VLL Interfaces Sockets buffers

The VLL interface socket buffers are required in scenarios where the lines bonded by the VLL have huge difference in the latencies (for example, combining a DSL and a satellite line). In these cases, fine-tuning the VLL socket buffers leads to an optimized performance.

Interface binding support

The Exinda SD-WAN supports binding of specific outbound traffic to a specific WAN interface or VLL data tunnel (with the optional VLL feature). This is sometimes useful for some applications or users that require certain traffic to be routed over the same WAN interface or over a certain tunnel.

To configure the interface binding feature, go to the **Advanced** tab. To configure an interface binding rule, click **Add Interface Binding Rule**. This generates a pop-up window where the information specifying an interface binding rule can be specified. The rule action is specified by an Interface which can be either `WIRED WAN 1`,`WIRED WAN 2`, `WIRED WAN 3`,`WIRED WAN 4`, or possibly `Cellular WAN 1` if a cellular broadband data modem is plugged into the Exinda SD-WAN. If a remote LAN connection has been defined (with the optional VLL feature), that can also be specified as an `interface`.

The specified traffic is preferentially routed over the WAN interface with the index that is selected for the rule, or to the corresponding remote LAN connection.

The traffic specification for the rule consists of a protocol designation, a port number, and an IP address or IP subnet. Only packets which match the corresponding protocol designation, port number, and IP address or IP subnet is affected by the rule (that is, the "and" of these three conditions). A match for the port number occurs when either the **Source Port** field or the **Destination Port** field matches with the port numbers specified. A port number specification can be a single integer, but it can also be a range. For example, `56-59` would be the range that includes `56`, `57`, `58`, and `59`. Values and ranges can also be separated by commas. For example, `56,59` corresponds to the set containing the values `56` and `59`. If the **Port Number** field is left blank, there is no match condition applied to the **Source Port** or **Destination Port** fields, that is, all ports match.

A match for the IP address occurs when either the source IP address of the packet or the destination IP address of the packet matches the given IP address. If an IP subnet is given, a match occurs when the source IP address or the destination IP address of the packet is within the IP subnet. If the **IP address / subnet** field is left blank then there is no match condition applied to the IP address field, that is, all IP address / subnet values matches.

The protocol designation can be `ANY`, `TCP`, `UDP`, `IPSEC`, `PPTP`, or `Other`. The `ANY` choice means any protocol matches. With the `Other` protocol designation, the corresponding protocol number is also specified.

All of the match conditions, if any, for the port number, the IP address or subnet, and the protocol designation must be met in order to trigger the port forwarding rule. When the port forwarding rule is triggered, the traffic is routed in the manner specified, for example, `WIRED WAN 1`, `WIRED WAN 2`, `WIRED WAN 3`, `WIRED WAN 4`, `Cellular WAN 1` if a cellular broadband data modem is plugged into the Exinda SD-WAN, and `Remote LAN 1` if a VLL connection has been configured (with the optional VLL feature).

There are two port numbers that need special consideration for interface binding. Specifically, traffic on port `80 (HTTP)` and port `443 (SSL)` should be selected for interface binding only with extreme care. Nominally, traffic for these ports should be handled by the same WAN interface.

An optional **Note** field is provided for convenience and typically is used to document what the interface binding rule is used for (for example, for a particular application or user). Once all the information for an interface binding rule has been entered, click **Add** to enable the rule.

Multiple interface binding rules can be added in order to provide more flexible binding of traffic. If an interface binding rule that was added previously needs to be deleted, click **Delete** next to the listed binding rule. If an interface binding rule needs to be edited, the rule can first be deleted and the modified rule can then be entered as before. The Exinda SD-WAN processes outgoing traffic by sequential application of the interface binding rules specified. This means if there are conflicts in the interface binding rules, the rule nearest the top of the list takes precedence. By default, the list of rules is such that rules entered earlier is lower in the list.

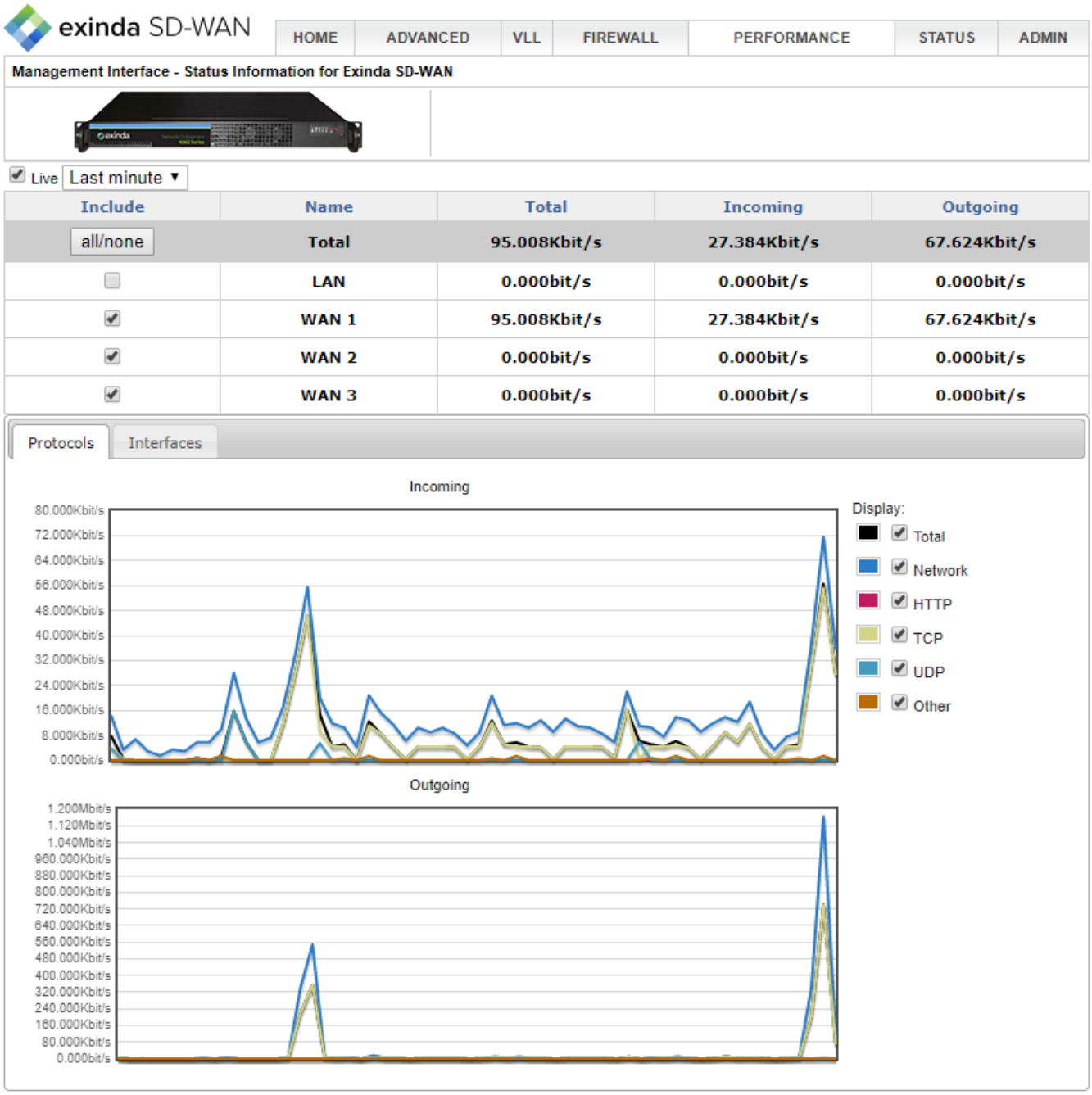
VLL Cloud Relay

Each Exinda SD-WAN subscription can have up to 1 VLL connected to our Cloud Relay service. The Cloud Relay Service connects the Exinda SD-WAN device to another GFI hosted Exinda SD-WAN device, hosted on Amazon AWS. The Cloud Relay service utilizes the VLL feature explained above. To set it up, you should contact Support.

0.8 Performance tab

The **Performance** tab displays graphical performance metrics. A history of your traffic usage based on protocol, including total, network, HTTP, TCP, UDP, other, or interface, such as LAN or WAN1, are presented with multicolor graphs with a time scale from seconds, minutes, hours, days and months. There is also a check-box for live, realtime performance.

A typical example is shown below:

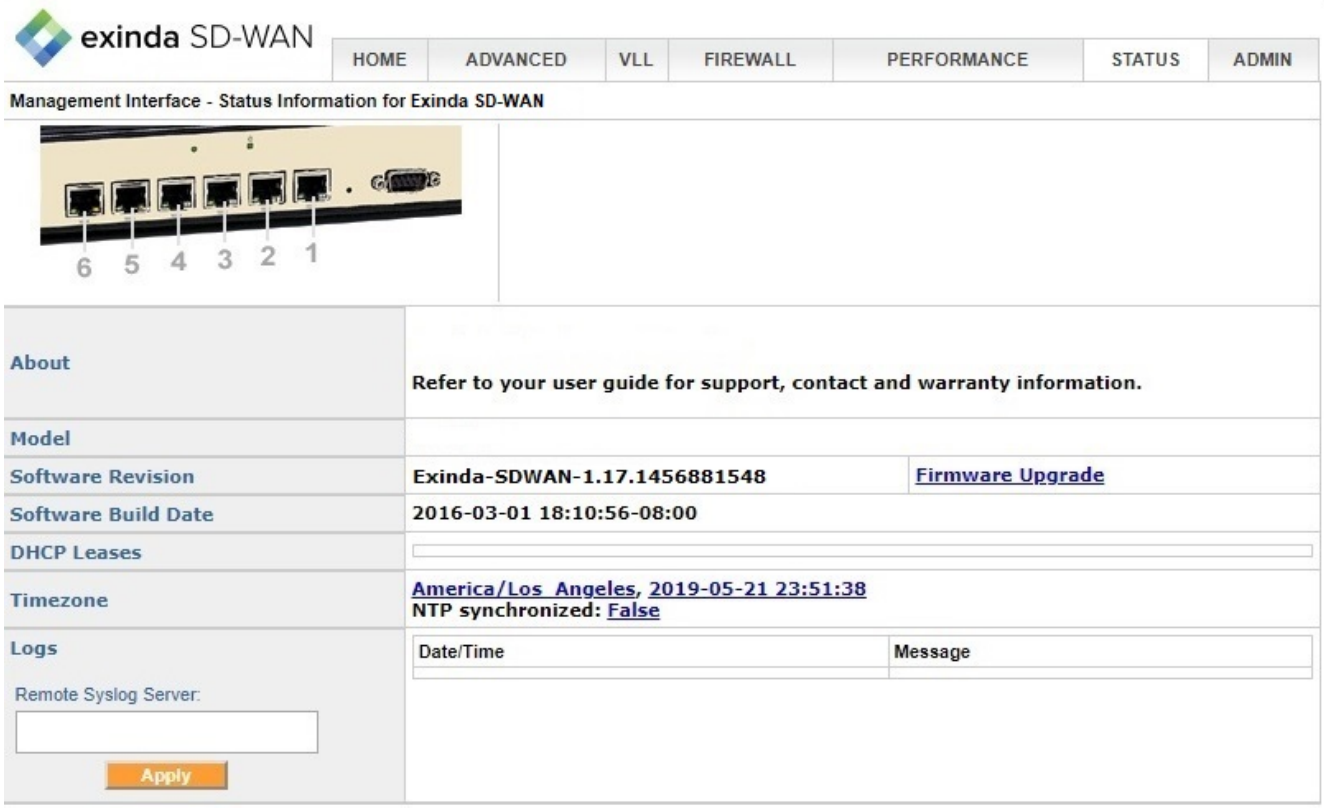


Screenshot 36: The Performance tab

0.9 Status tab

The **Status** tab displays auxiliary information about the Exinda SD-WAN, including the software revision number, as well as links to a menu to upgrade the software version.

A log of system events is displayed. The Remote Syslog feature can be configured, as described in For more information, refer to Remote syslog (page 27).. A list of DHCP leases is also displayed.



Screenshot 37: The Status tab

0.10 Administrative features

In this section, the administrative features of the Exinda SD-WAN are described.

Web interface password

The Exinda SD-WAN Management Interface can be configured so that it can be accessed only with the entry of a username and password. With the default factory settings, entry of a password is not required.

The Exinda SD-WAN Management Interface password can be configured on the **Admin** tab so that it would require a password to access it.

> The password should be changed with extreme care — if it is forgotten or mistyped it is not possible to access the Exinda SD-WAN Management Interface.

To configure the feature:

1. Go to the **Admin** tab.

2. Click the status under **Web Interface Password** and set it to **Enabled**. The default username is `admin`.

3. Set the password by entering it in the **Web Interface Password** field. Type in the password twice to ensure it is accurately recorded, then click **Apply**.

Configuration of this feature causes the Exinda SD-WAN to restart.

Allow web IPs

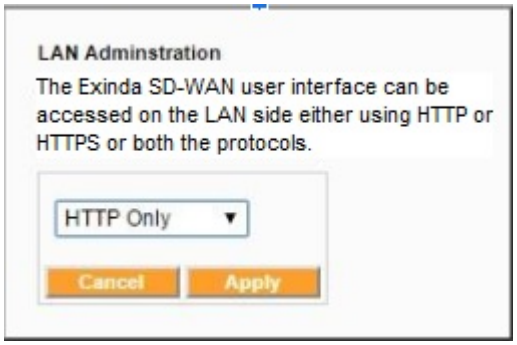
This feature allows restricting the access to the Exinda SD-WAN Management Interface to only the IPs provided in this field. For example, if the administrator for the device wants to access the device remotely from the IP `76.211.117.87`, the **Web Allow IPs** field can be configured accordingly, which would restrict the access to the

Exinda SD-WAN Management Interface to only this particular IP.

Screenshot 38: Allowing web IPs

LAN user interface

The LAN user interface defines the protocol used to access the Exinda SD-WAN Management Interface from the LAN side. By default this would be set to HTTP.



Screenshot 39: LAN user interface

WAN HTTP Port (Remote web interface port)

The Exinda SD-WAN Management Interface can be configured so that it can be accessed externally from the internet via the Exinda SD-WAN WAN ports. To enable this feature, go to the **Admin** tab and click on the status indicator of the **WAN HTTP Port** entry in the displayed status table. The pop-up window allows configuration of the feature. If the feature is enabled, a port number must be specified.

If the feature is enabled, the Exinda SD-WAN Management Interface can be remotely accessed from the internet through any of the public IP addresses for the Exinda SD-WAN. These public IP addresses can be obtained from the **External IP** column in the WAN status table on the **Home** tab of the Exinda SD-WAN Management Interface. The URL through which the Exinda SD-WAN Management Interface can be accessed is given by the external IP address appended with the assigned port number. For example, if one of the external IP addresses for the Exinda SD-WAN is `76.211.117.87` and the Remote Web Interface is enabled through port 8080, then the Exinda SD-WAN Management Interface can be accessed through the URL `http://76.211.117.87:8080`.

If Pass Through mode is enabled on WAN interface 1, the Exinda SD-WAN Management Interface can be accessed externally from the internet through the IP address of the router/firewall that is connected to the LAN port of the Exinda SD-WAN. For example, if the IP address of this router is `76.37.181.2` and the WAN HTTP Port is accessed through port `8080`, then the Exinda SD-WAN Management Interface can be externally accessed through the URL `http://76.37.181.2:8080`. Note that in this example from a host on the LAN of the Exinda SD-WAN, packets addressed to `76.37.181.2` are forwarded to the router/firewall and not the Exinda SD-WAN. To access the Exinda SD-WAN Management Interface from the Exinda SD-WAN LAN, the Exinda SD-WAN LAN address should be used (for example, the default Exinda SD-WAN LAN address `192.168.254.99`).

If the WAN HTTP Port is enabled, then it is highly recommended that a web interface password be configured to prevent unauthorized access to the Exinda SD-WAN from the public Internet.

WAN HTTPS Port

The WAN HTTPS Port `8081` allows remote access of the Exinda SD-WAN Management Interface by using HTTPS. The URL through which the Exinda SD-WAN Management Interface can be accessed is given by the external IP address appended with the assigned port number. For example, if one of the external IP addresses for the Exinda SD-WAN is `76.211.117.87` and the Remote Web Interface is enabled through port `8081`, then the Exinda SD-WAN Management Interface can be accessed through the URL `http://76.211.117.87:8081`.

If Pass Through mode is enabled on WAN interface 1, the Exinda SD-WAN Management Interface can be accessed externally from the Internet through the IP address of the router/firewall connected to the LAN port of the Exinda SD-WAN. For example, if the IP address of this router is `76.37.181.2` and the WAN HTTP Port is accessed through port `8081`, then the Exinda SD-WAN Management Interface can be externally accessed through the URL `http://76.37.181.2:8081`. Note that in this example from a host on the LAN of the Exinda SD-WAN, packets addressed to `76.37.181.2` is forwarded to the router/firewall and not the Exinda SD-WAN. To access the Exinda SD-WAN Management Interface from the Exinda SD-WAN LAN, the Exinda SD-WAN LAN address should be used (e.g. the default Exinda SD-WAN LAN address `192.168.254.99`).

Maintenance mode

The Exinda SD-WAN has a maintenance mode for remote troubleshooting by GFI Support. This allows external access to the Exinda SD-WAN by GFI Support over the internet. Normally this mode should be disabled, and it is disabled in the default factory settings.

To configure the feature:

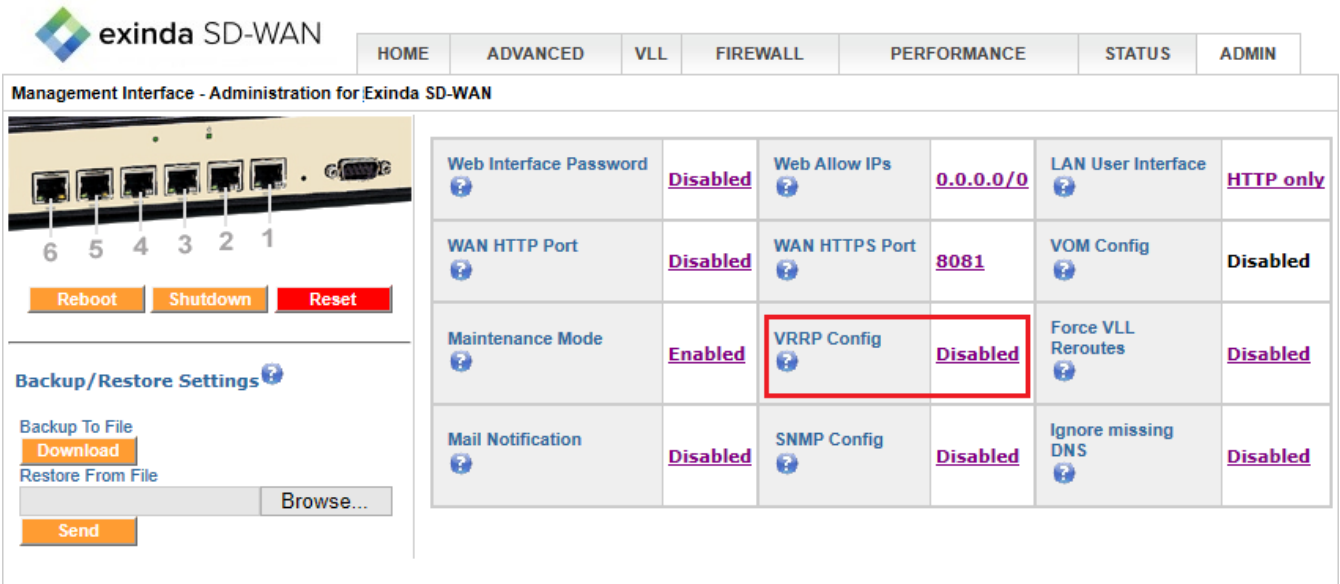
1. Go to the **Admin** tab.

2. Click the status for **Maintenance Mode**, then set it to **Disabled** or **Enabled**. This generates a pop-up window to prompt the user to configure the feature.

3. Click **Apply** to make the changes.

VRRP configuration

The Exinda SD-WAN has an option to configure VRRP (Virtual Router Redundancy Protocol), which is designed to increase the availability of the default gateway-servicing hosts on the same subnet. By default this feature is disabled but can be enabled on the Admin tab.



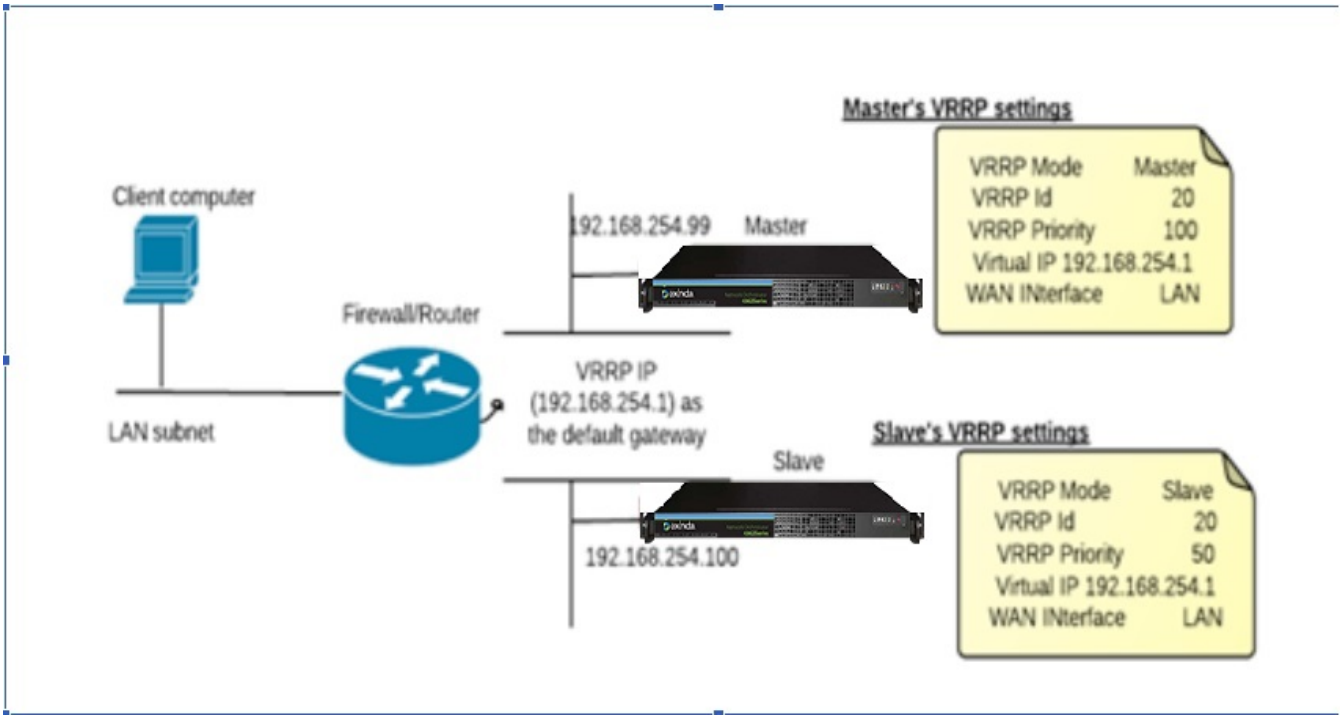
Screenshot 40: VRRP configuration

VRRP mode can be configured to be either as master or slave depending on which physical router is doing the actual routing. In case of failure of the master router, the slave router which was configured as a virtual router automatically

replaces it. **VRRP ID** is the Virtual Router Identifier (VRID), which uniquely identifies each virtual router in the subnet. This is a configurable item in the range 1-255 (decimal) and has no default value.

VRRP Priority is an 8-bit unsigned integer field with higher value indicating higher priority. The master should be given the highest priority. Care should be taken in configuring this field as the master should always be given highest priority compared to the slaves or this could cause instability in the network. **Virtual IP** is the IP address of the Exinda SD-WAN device depending on which interface is connected to the subnet.

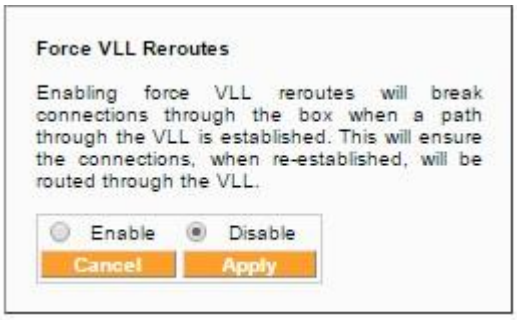
Here is an example setup:



Screenshot 41: Example of VRRP setup

Force VLL reroutes

Enabling force VLL reroutes break connections through the box when a path through the VLL is established. This ensures the connections, when re-established, is routed through the VLL.



Screenshot 42: Force VLL reroutes configuration

Mail notification (E-mail alarms)

The Exinda SD-WAN supports sending of email alarms to a specified address when a serious event occurs. A "serious" event is defined by a WAN interface going down or coming back up without manually enabling or disabling the WAN interface.

To configure email alarms:

1. Go to the **Admin** tab.

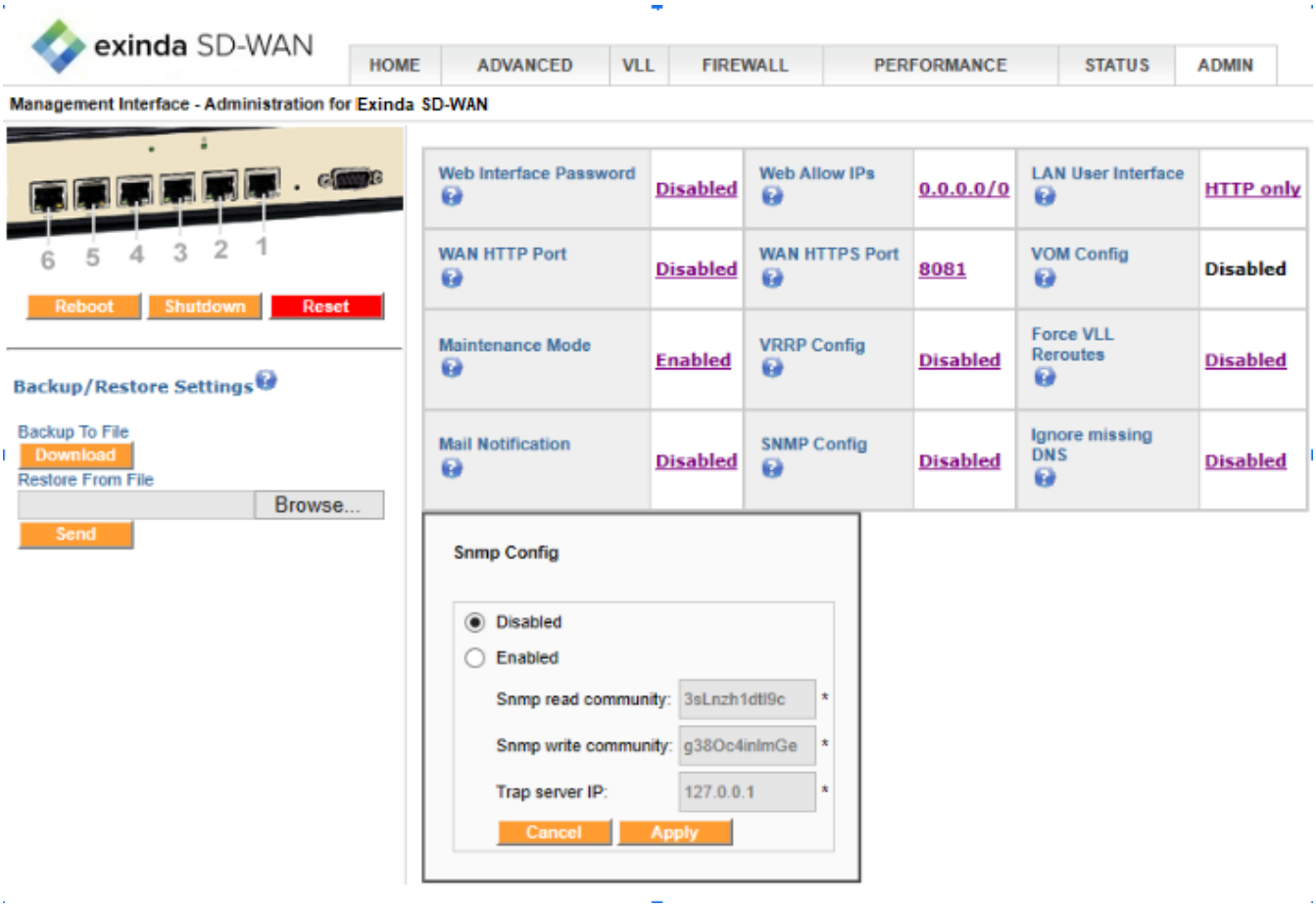
2. Click the status for **Mail Notification**, which is either **Disabled** or **Enabled**.

3. Enter the email address and the IP address of the SMTP server in the pop-up window to receive the alarms. Typically, this is the SMTP server on the Exinda SD-WAN LAN.

In order to test the configuration, a WAN interface can be manually brought down and up again by disconnecting the cable from an active WAN interface which triggers an email alarm to be sent to the designated address and server.

SNMP configuration

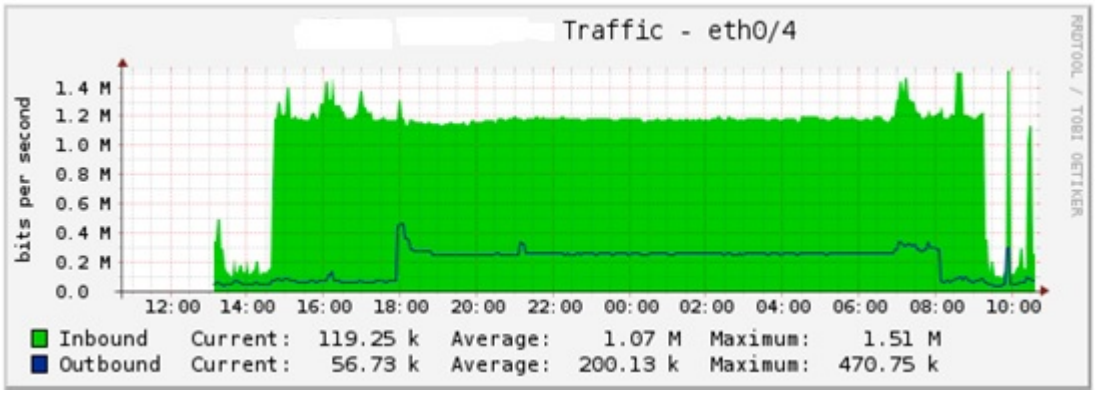
The Exinda SD-WAN has a built in SNMP (Simple Network Management Protocol) agent running on the device which can be accessed by any SNMP browser or SNMP client application. The Exinda SD-WAN supports MIB2 (RFC 1213) management information base (MIB). You can enable the SNMP feature on the **Admin** tab.



Screenshot 43: SNMP configuration

Asynchronous notification by using SNMP traps for WAN links getting **Connected** and **Disconnected** can also be pushed to a **Trap server IP** .

By using external SNMP management and graphing tools you can retrieve interface statistics from the GFI Exinda SD-WAN device. The following is an example graph for one of the WAN statistics using MRTG grapher:



Screenshot 44: Example Graph of WAN Statistic

Note that any host on the Exinda SD-WAN LAN can access the SNMP interface. For external network access to the SNMP interface the Exinda SD-WAN firewall needs to be configured to allow SNMP traffic from the outside that uses port 161. To do this, go to the **Firewall** tab in the Exinda SD-WAN Management Interface and add a rule that permits inbound traffic on port 161 for UDP protocol. In rare cases it may be necessary to also add a rule that permits inbound traffic on port 161 for TCP protocol.

Ignore missing DNS

If this option is disabled, if your DHCP server fails to provide DNS servers the device attempts to re-DHCP onto the network. This handles cases where the DHCP server is in a bad state, but can prevent accessing an unconfigured server to configure it.

Screenshot 45: Ignore Missing DNS configuration

0.11 Assigning a static IP address to a PC

It is likely that a search on the Internet easily yield instructions on how to configure the management computer (PC) with a static IP address. For convenience, instructions on how to do this for a Windows XP-based PC are given below.

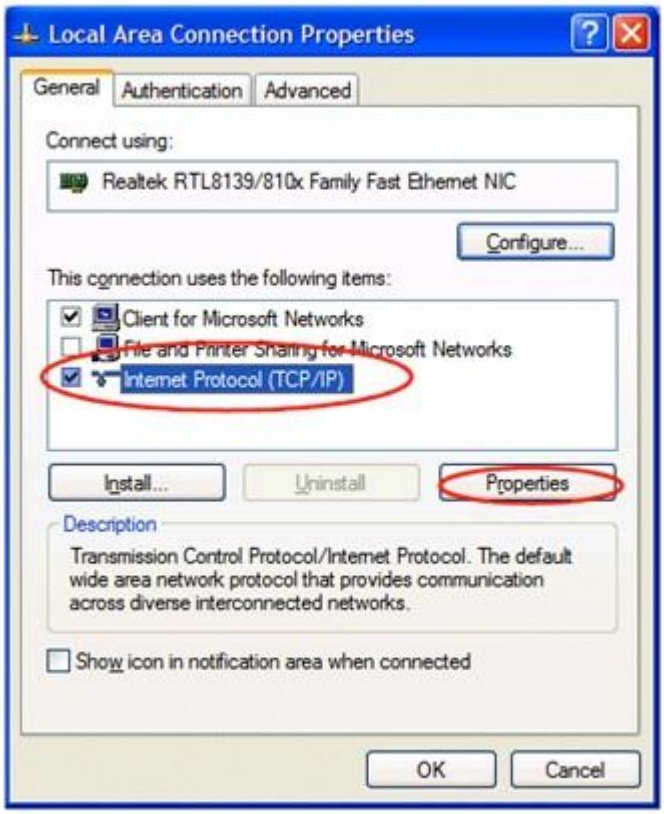
To set a static IP address:

1. Open the Windows **Start** menu.
2. Open the **Control Panel**.
3. Classic view: Open **Network Connections**.

Category view: Open **Network and Internet Connections**, and then **Network Connections**.

4. Double-click on the active **LAN or Internet connection**.
5. Click **Properties**. This opens the Local Area Connection Properties window.

6. In the General tab, highlight the **Internet Protocol (TCP/IP)**, and click **Properties**.



This opens the Internet Protocol (TCP/IP) Properties window.

7. In the General tab, click **Use the following IP address**, and enter:

» IP address. The static IP address to be assigned to this computer (it is recommended that `192.168.254.10` be used unless changed the IP address of the Exinda SD-WAN has been reconfigured).

» Subnet mask. Subnet mask used by the Exinda SD-WAN (usually this is `255.255.255.0`).

» Default gateway. IP address of the Exinda SD-WAN (usually this is `192.168.254.99`).

8. In **Use the following DNS server addresses**, enter all the IP addresses for the DNS servers the Exinda SD-WAN uses (the address `192.168.254.99` can be used, or this can be left blank to configure the Exinda SD-WAN).

9. Click **OK**.

10. Click **OK** again to close each window.

11. Restart the computer.

12. Then, check the IP address again, to make sure that the changes were applied.

To check the IP address:

1. Open Windows **Start** menu.

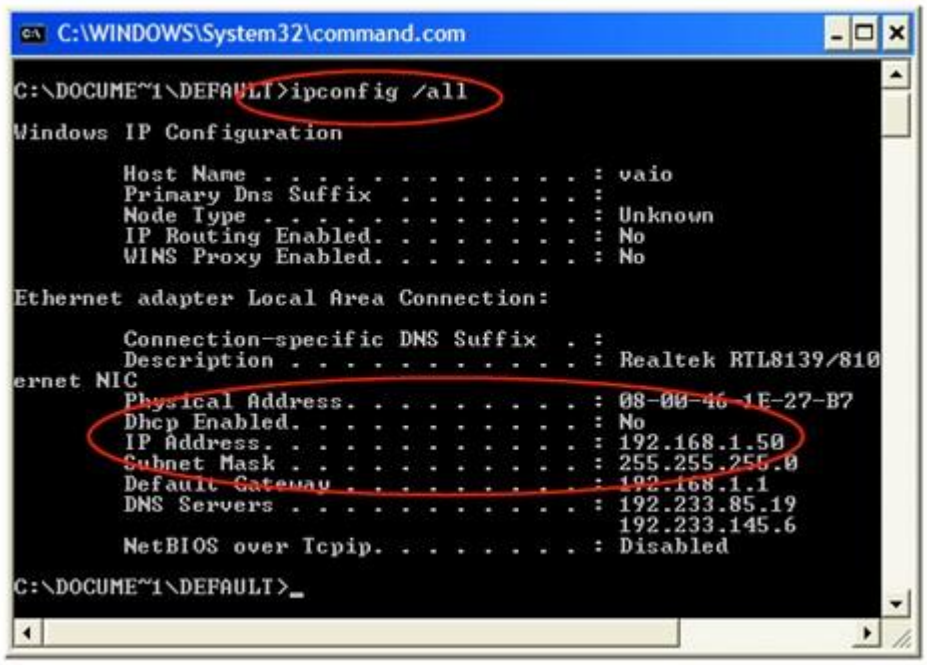
2. Select **Run**. Type: command and click **OK**.

3. At the blinking cursor, type: **ipconfig /all** and press Enter.

4. Look for these entries near the end of the list:

- **DHCP Enabled**. "No" means the IP address is static. "Yes" means it is dynamic.
- **IP Address**. This is the current IP address.

5. To exit, at the blinking cursor, type: exit and press Enter.



Maintenance and usage

The Exinda SD-WAN is an appliance that is designed to run at all times. It does not need to be powered off or restarted for normal usage. For moving or storage, the Exinda SD-WAN may be powered off at any time, but it is recommended that the **SHUTDOWN** option be used on the Admin tab. Note that this puts the Exinda SD-WAN in a state whereby the power to the unit can be safely interrupted.

In addition to the **SHUTDOWN** option on the Admin tab, there are the **REBOOT** and **RESET** options. The **REBOOT** option causes the Exinda SD-WAN to reboot. The **RESET** option resets all configuration data in the Exinda SD-WAN Management Interface to their factory defaults.

The Exinda SD-WAN should be placed on a flat and dry surface in a well-ventilated area. Overheating shortens the life of the Exinda SD-WAN.

> Opening the case of the Exinda SD-WAN, except under instruction of GFI, Inc., voids the warranty.

0.12 Software upgrade

You can find the latest software version on the **Status** tab of the Exinda SD-WAN Management Interface and upgrade the software if required.

To determine the latest software version,

1. Go to the **Status** tab of the Exinda SD-WAN Management Interface.

2. Click **Firmware Upgrade** located next to the current **Software Revision**.

This causes the Exinda SD-WAN to access the internet and determine the latest software version available for the Exinda SD-WAN and display it at the top of the list.

3. Select the latest software version in the list and click **Update**.

A status bar is displayed indicating the progress of the software upgrade to the device. It may take several minutes for the upgrade to complete.

4. To apply the upgrade, click **Finalize** after the progress bar has completed.

The upgrade is effective upon the next device reboot.

After upgrading the system software, you can verify that the software has been upgraded by checking the version number in the **Status** tab. You should clear your browser cache to make sure that you are not viewing a cached page.

0.13 Firmware reset with USB key

A USB key for resetting the software and settings is included with each unit. It is recommended that you keep the USB key in a safe and secure place, since it is needed to restore the unit to factory default condition, when necessary.

> You should use the appropriate procedure as indicated to reset or reload the software into the Exinda SD-WAN unit.

When resetting the Exinda SD-WAN system software, it is possible to do only a software reset without resetting the factory defaults, if the USB key is removed at the appropriate time during the upgrade process. Alternatively, to avoid the USB key resetting the Exinda SD-WAN to factory settings and only reset the firmware, a file named `noreset` can be added to the USB key where the file can be of any type.

Firmware Reset with or without restore to factory default settings

1. Power off the device.

2. Unplug all USB attached devices from the Exinda SD-WAN, and insert the USB key that came with the unit into any USB slot on the front panel.

3. Power on the device.

4. The device loads the firmware from the USB key. When the firmware upload is complete, the Exinda SD-WAN beeps three times.

> To avoid resetting to factory default settings, the Exinda SD-WAN may safely be powered off following the 3 beeps.

5. To reset to factory default settings, continue to wait for 1 minute after the beeps and the device powers itself off.

6. Remove the USB key and power the unit back on. It is now fully reset.

Abbreviations and acronyms

Term	Description
ADSL	Asymmetric Digital Subscriber Line
APN	Access Point Network
ARP	Address Resolution Protocol
CDMA	Code Division Multiple Access
CIDR	Classless Inter-Domain Routing
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DDNS	Dynamic DNS
DNS	Domain Name Server
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
GSM	Global System for Mobile Communications
HSPA	High Speed Packet Access
ICMP	Internet Control Message Protocol
IP	Internet protocol
IPSec	Internet Protocol Security
LAN	Local area network
MAC	Media Access Control
MIB	Management Information Base
MIBv2	Management Information Base, version 2
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NTP	Network Time Protocol
PPPoE	Point-to-Point Protocol over Ethernet
PPTP	Point-to-Point Tunneling Protocol
QoS	Quality of Service
SD-WAN	Software-Defined Wide Area Network
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

Term	Description
UPnP	Universal Plug and Play
USB	Universal Serial Bus
VDSL	Very High Bitrate Digital Subscriber Line
VOIP	Voice over Internet Protocol
VOIP/SIP	Voice over Internet Protocol / Session Initiation Protocol
VPN	Virtual Private Network
VRID	Virtual Router Identifier
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network