Oracle® SD-WAN

How to Configure Third-Party Firewalls

Original Publication Date: Nov 1, 2019

Table of Contents

About This Document

This document discusses how to configure third-party firewalls on a network with Talari appliances. For information on configuring the built-in Talari firewall, please see the *Talari Firewall Configuration Guide*.

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with My Oracle Support registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select 2 for New Service Request.
2. Select 3 for Hardware, Networking, and Solaris Operating System Support.
3. Select one of the following options:
    - For technical issues such as creating a new Service Request (SR), select 1.
    - For non-technical issues such as registration or assistance with My Oracle Support, select 2.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration

- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click Industries.
3. Click the Oracle Communications link.

   Under the SD-WAN header, select a product.
4. Select the Release Number.

   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the PDF link, select Save target as (or similar command based on your browser), and save to a local folder.

References

The following documents are available: *Talari Glossary*

Firewall Configuration

In a Talari WAN, a WAN Path is a logical, one-way, UDP encapsulated flow of data between two Talari Appliances and a constituent part of a Conduit. Conduits use Talari Reliable Protocol (TRP) on UDP Port 2156 by default, but the UDP Port number can be manually configured for each Conduit.

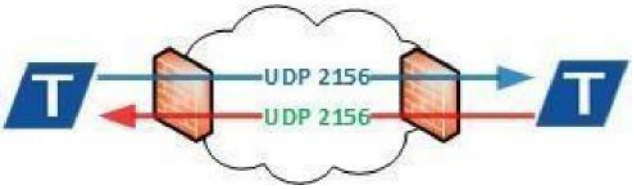

Figure 1: UDP Ports

UDP Port Mapping and Forwarding

When a Talari Appliance is installed behind a firewall or NAT device it is necessary to ensure the TRP traffic is permitted in each direction and mapped to the corresponding internal WAN Link Virtual IP Address (VIP).

Firewall Access Rules

Firewall vendors often employ associative object-based components to create service rules for access to the private network. These guidelines are listed below, however, consult your firewall vendor documentation for specific configuration instruction.

1. **Service Object**: By default, TRP uses UDP 2156. If the port number is changed in the configuration, the service object should match.
2. **Host Object:** The WAN Link VIP as it appears to the firewall from the private network.
3. **NAT Policy:** Apply NAT to the outbound TRP traffic referencing the Service and Host Objects.
4. **Security Policy:** Allow inbound TRP traffic from the remote Talari Appliance. Depending on the firewall make and model this may be implicitly allowed through the NAT Policy.

Objects and Policies	Properties
Service Object	UDP Port 2156
Host Object	WAN Link VIP
NAT Policy	NAT Host and Service
Security Policy	Permit or Forward UDP 2156 to WAN Link VIP

Figure 2: Configuring the Firewall

Troubleshooting

Incorrect firewall configuration may result in a DEAD Path in one or both directions. A Path is DEAD when no TRP packets are received for 1500ms or longer.

1. Verify that the firewall configuration matches the configured WAN Link VIPs and UDP ports.
2. Are TRP packets being received on the sending firewall from the LAN?
3. Inspect packet flow on the sending firewall:
    a. Are TRP packets using the expected NAT Policy and have the correct public IP Address?
    b. Are TRP packets forwarded from the correct public facing interface?
4. Inspect packet flow on the receiving firewall:
    c. Are TRP packets arriving on the public facing interface?
    d. Are TRP packets forwarded to the LAN on the correct private facing interface?
5. Inspect the packet flow on the receiving Talari Appliance:
    a. Are TRP packets arriving on the associated WAN Link Interface Group?