



RSA Ready Implementation Guide for RSA Security Analytics

Last Modified: August 5th 2015

Partner Information

Product Information	
Partner Name	Interface Masters
Web Site	www.InterfaceMasters.com
Product Name	Niagara 2299
Version & Platform	3.14-33
Product Description	Bypass and TAP switch



Solution Summary

The Interface Masters Series delivers performance and intelligence as a Traffic Visibility Fabric™ node, with port density and speeds that scale to your needs from 1Gb to 100Gb. With an intuitive web-based GUI and a powerful CLI, the Visibility Fabric is able to replicate, selectively forward network traffic to monitoring, management, and security tools such as RSA Security Analytics.

By combining Interface Masters with RSA Security Analytics, you empower network forensic and packet capture devices by providing customized data streams aggregated from multiple points on the production network. Advantages of such a solution include preventing data loss, collecting more relevant data per packet capture device, de-duplication for tool optimization and masking to address compliance

RSA Security Analytics Tested Features	
Interface Masters 2299	
Flow / Traffic Mapping	Yes
Failover (bypass fail open or fail close)	Yes
Health check via hart beat packet	Yes
Dual power supplies	Yes
AC and DC support	Yes
Ability to be in TAP (passively look at the traffic)	Yes
High availability (support active passive)	Yes
Management capabilities: GUI, CLI, TACACS, SSH, SNMP, Syslog, e-mail notification, NTP	Yes
Filtering	No ¹
De-duplication	No ²

1. Next software release filtering will be supported
2. De-duplication can be performed by using the Niagara a5002

Interface Masters

TECHNOLOGIES

Innovative Network Solutions

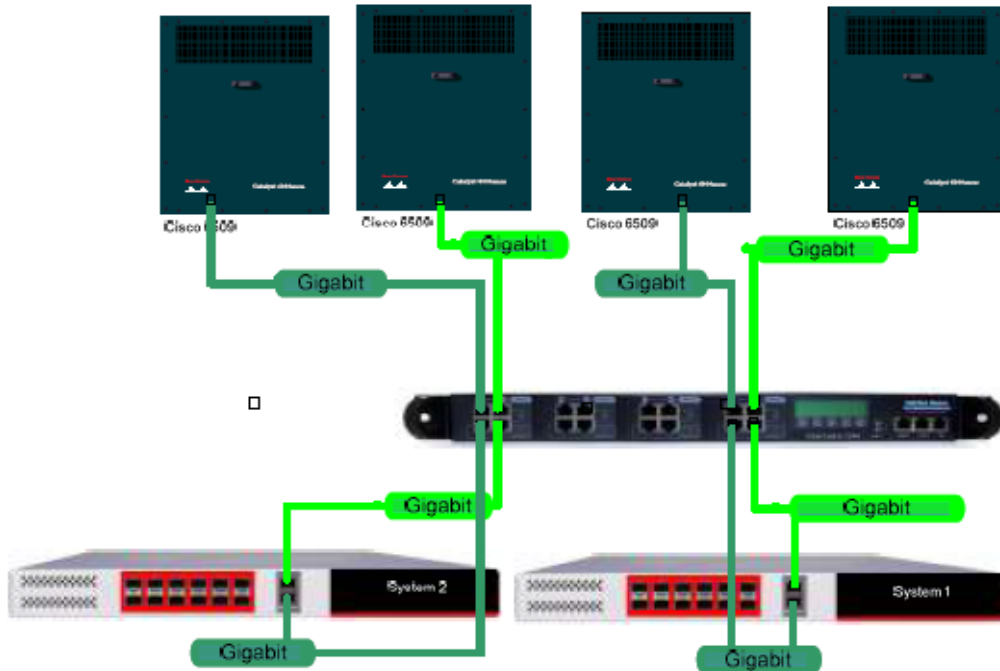


Figure 1 Connectivity example, Niagara 2299 can connect up to 4 network segments

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Niagara with RSA Security Analytics. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Interface Master components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

! > Important: The configuration shown in this Implementation Guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure the Product is properly configured and secured before deploying to a production environment. For more information, please refer to the Product documentation or website.

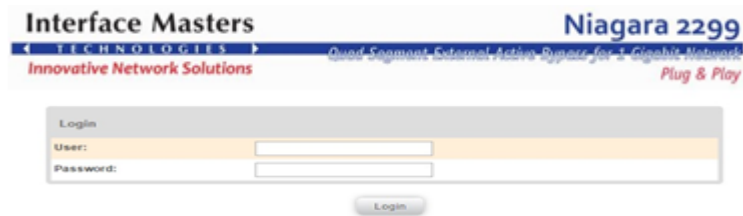
Niagara 2299 Configuration

The Niagara 2299 possesses active bypass functionality for seamless failover, TAP functionality for traffic monitoring, and extensive management capabilities. It is available with four independent segments with various media combinations including copper, single-mode fiber, multi-mode fiber, multi-mode fiber to single-mode fiber conversion and copper to fiber conversion options. The intelligent bypass also enables plug-and-play connectivity, includes an auto heartbeat and requires no additional drivers to be installed on connected appliances. Below is a sample use case for the 2299.

The Niagara 2299 can be set to mirror traffic from a Network port N1 for example, to A1. This is configured in the bottom tap section.

If you want to use the “TAP” port on the right to mirror you will need use the Analyzer section. All ports can be mirrored for transmit, receive or both on the TAP port.

1. Log into the Niagara 2299 GUI



The screenshot shows the login interface for the Niagara 2299 GUI. At the top left, it says "Interface Masters" and "TECHNOLOGIES". At the top right, it says "Niagara 2299" and "Plug & Play". Below the header, there is a "Login" section with two input fields: "User:" and "Password:". A "Login" button is located below the input fields.

2. Click on a segments on the left and in the analyzer section you want to configure.

- Status
- Segments
- Ports
- Advanced
- Management Port
- Notification
- Time
- Authentication
- System

Bypass				
	Segment 1	Segment 2	Segment 3	Segment 4
Bypass mode	Internal	Internal	Internal	Internal
Operation mode	Normal active bypass	Normal active bypass	Normal active bypass	Manual active bypass
Operation mode at boot	Auto	Auto	Auto	Auto
Heartbeat Frame	ETH	ETH	ETH	ETH
Heartbeat Ethernet Type	0x88b5	0x88b5	0x88b5	0x88b5
Heartbeat Source MAC	00:0c:bd:00:00:00	00:0c:bd:00:00:00	00:0c:bd:00:00:00	00:0c:bd:00:00:00
Heartbeat Destination MAC	00:0c:bd:00:00:ff	00:0c:bd:00:00:ff	00:0c:bd:00:00:ff	00:0c:bd:00:00:ff
Heartbeat Source IP	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Heartbeat Destination IP	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Heartbeat Source Port	0	0	0	0
Heartbeat Destination Port	0	0	0	0
Source Network Mask	0x012234aa	0x012234aa	0x012234aa	0x012234aa
Destination Network Mask	0x022234aa	0x022234aa	0x022234aa	0x022234aa
Heartbeat interval (ms)	100	100	100	100
Heartbeat timeout (ms)	100	100	100	100
Bypass heartbeat threshold	2	2	2	2
Active heartbeat threshold	3	3	3	3
Bidirectional Heartbeat	No	No	No	No

Link Fault Detection				
	Segment 1	Segment 2	Segment 3	Segment 4
Link Fault Detection	Enabled	Enabled	Enabled	Enabled

Analyzer				
	Segment 1	Segment 2	Segment 3	Segment 4
Analyzer state	Disabled	Disabled	Disabled	Enabled
N1 tap mode	DISABLED	DISABLED	DISABLED	RXTX
N2 tap mode	DISABLED	DISABLED	DISABLED	RXTX
A1 tap mode	DISABLED	DISABLED	DISABLED	DISABLED
A2 tap mode	DISABLED	DISABLED	DISABLED	DISABLED

Tap				
	Segment 1	Segment 2	Segment 3	Segment 4
Tap state	Disabled	Disabled	Disabled	Enabled
Tap segment mode	Split	Split	Split	Aggregation and packet injection
Tap segment boot mode	Auto	Auto	Auto	Auto

- Click on the Analyzer and using the pull down menus, enable and select what ports you want to mirror to the TAP port.

Segment 4 > Bypass

Bypass mode	Internal
Operation mode	Manual active bypass
Operation mode at boot	Auto
Heartbeat Frame	ETH
Heartbeat Source MAC	00:0c:bd:00:00:00
Heartbeat Destination MAC	00:0c:bd:00:00:ff
Heartbeat interval (ms)	100
Heartbeat timeout (ms)	100
Bypass heartbeat threshold	2
Active heartbeat threshold	3
Bidirectional Heartbeat	No

Segment 4 > Link Fault Detection

Link Fault Detection	Enabled
----------------------	---------

Segment 4 > Analyzer

Analyzer state	Enabled ▼
N1 tap mode	RXTX ▼
N2 tap mode	RXTX ▼
A1 tap mode	DISABLED ▼
A2 tap mode	DISABLED ▼

Save Cancel

Segment 4 > Tap

Tap state	Enabled
Tap segment mode	Aggregation and packet injection
Tap segment boot mode	Auto

Certification Checklist for RSA Security Analytics

Date Tested: July 30 2015

Certification Environment		
Product Name	Version Information	Operating System
RSA Security Analytics	10.5	Virtual Appliance
Nigiars 2299	3.14-33	Linux

Security Analytics Test Cases	Result
Packet Loss	
Syslog TCP data consumed by the SA Log Decoder	<input checked="" type="checkbox"/>
Syslog UDP data consumed by the SA Log Decoder	<input checked="" type="checkbox"/>
Various packet data consumed by the SA Packet Decoder	<input checked="" type="checkbox"/>
De-duplication	
Replaying data files to the SA Packet Decoder	<input type="checkbox"/> N/A
Traffic Mapping	
Mapping network service ports to dedicated ports	<input checked="" type="checkbox"/>
Performance	
SA Log Decoder minimal EPS performance	<input checked="" type="checkbox"/>
SA Packet Decoder minimal EPS performance	<input checked="" type="checkbox"/>

INIT / FAL

✓ = Pass ✗ = Fail N/A = Non-Available Function