Janus FAQ

By: cuculan
Revision: 1.0

Please reach us at contact@cuculan.com if you cannot find an answer to your question.

Cryptography

Q - What encryption/decryption type does Janus use?
A- Janus Management application for Janus and Janus to Janus connections use TLS 1.3.

Q – Does Janus rotate the resource data path cryptographic key periodically?
A – Yes, key rotation is automatic and does not interrupt resource data path communications.

Q – Does each Janus-to-Janus connection use a unique cryptographic key?
A – Yes, every Janus-to-Janus connection uses a unique key.

Q – Do Janus connections use AEAD (Authenticated Encryption with Associated Data)?
A – Yes, as defined in RFC 8446 TLS 1.3 specification.

Q – Does Janus have resource data path packet replay protection?
A – Yes, Janus has resource data path packet replay protection.

Q – Can I use my own cryptographic keys?
A – No, Janus cryptographic key management is fully automated, the Janus devices automatically generate keys as needed.

Management

Q – What type of communications does Janus Management application use?
A – Janus has a REST API interface; the Janus Management application uses this interface.

Q – Do you publish the Janus REST API details?
A – Yes, the details are in the Janus Instruction Manual.

Q – Can I log into Janus with a local console connection?
A – No, for security reasons Janus's only management access is through the REST API accessible by the Janus WAN Ethernet interface.

Q – Can I export Janus configuration data for my use?
A – Yes, it is a text .CSV file intended to be easily exported.

Janus FAQ

Q – Can I manage Janus devices remotely over the WAN?
A – Yes, the management REST API is accessible by the Janus WAN Ethernet interface.

Q – Why is there an Inactive mode in addition to an Active mode?
A – During system setup when Janus devices are being deployed a Janus device may only be installed at one end of a connection. Inactive mode allows existing communications to continue to take place until both Janus devices are deployed. Both Janus devices can then be set to Active mode protecting the resources at each end of the connection.

Q – How do I get status of a Janus device?
A – Janus devices report status through the syslog protocol. Janus supports up to 2 syslog servers. One intended to be the Janus Management application that is operational when running the application and the second intended for a user supplied syslog server that is always available. Status is also available directly through the Janus REST API.

Network

Q – How many Ethernet interfaces are on Janus?
A – There are 2 Ethernet interfaces, LAN for the protected resource and WAN for general Network.

Q – What are the supported protocols?
A - TCP, UDP, DNS, and NTP packet support.

Q – My resource needs to reach the internet for DNS and NTP updates, how does that work?
A – When a protected resource is making DNS or NTP requests these requests are not encrypted but are masqueraded (IP hidden by substituting Janus management IP) to the WAN.

Q – What is the throughput of Janus-10 in Active mode (encryption/decryption enabled)?
A – Percent of baseline is 90% for a 1G connection and 46% for a 10G connection. Obtained using 1 - ((baseline – result) / baseline) formula. Baseline is first measured without Janus and then result is measured with 2 Janus devices in-line. For example, a 1G Network with 941Mbs baseline and 850Mbs result will have 90% throughput of baseline. Measurements were obtained using iperf3 with client command of “iperf3 -c <target IP> -w 400K -4 -t 30”.

Janus FAQ

Q – How much of the protected resource packet is hidden on the WAN?
A – 100%, the entire packet including the headers is encapsulated and encrypted before being sent to the WAN. The packet on the WAN will use the management IPs of the source and destination Janus devices.

Q – Will Janus work with my TCP or UDP custom application protocol?
A – Yes, it will work with both. Janus does not interpret the application-level data. All TCP or UDP protocol requests/responses are sent end to end. For example, a SYN request and ACK response are sent/received resource to resource securely.

Q – Does Janus support multiple Janus to Janus connections?
A – Yes, Janus supports one to one or one to many topologies.