Route Analytics Management Software Security

Software Version: 9.20

Route Analytics Management Software Security

Introduction

This document addresses several topics related to the system and network security of the HP Route Analytics Management Software (RAMS). It describes the network-visible services exported by the RAMS unit, the various means by which the units can be accessed, expected forms of network activity initiated by RAMS.

The information in this document is generally applicable to earlier versions of RAMS; differences between various versions and release trains are noted where applicable. Unless otherwise noted, the comments in this document apply to all RAMS product brandings and variants, such as RAMS Traffic.

This document assumes that the reader has a basic familiarity with the RAMS architecture.

General Remarks

RAMS uses a reduced version of CentOS Linux with some kernel modifications and package changes. Therefore, it shares many of the strengths of Linux- and UNIX-based systems with respect to security. In particular, RAMS is generally unaffected by worms, viruses, and other forms of malware commonly associated with personal computer systems.

In general, principles and techniques used for improving the security of Linux and UNIX based systems on a network can be (and have been) used on RAMS. These include (but are not limited to) keeping the number of network-visible services to a minimum, the use of passwords and strong passphrases, and the encryption of network communications where possible.

Exported Services

The RAMS appliance exports only a minimal set of services that are accessible from other hosts on the network, as shown in the following table. A port scan, for example, using nmap (1), would reveal these ports. On a system with multiple network interfaces enabled, these services are accessible only on the designated administrative network interface (commonly referred to as the “admin port”), except as noted. By default, this is the first built-in network interface, although this can be changed on the Network web administration page. All other interfaces are used for data collection only. In addition, several of the services on the admin port, such as MySQL and NTP, incorporate access control mechanisms at the application level.

Protocol	Port	Notes
TCP	21	FTP (File Transfer Protocol). Used primarily for uploading data files to the appliance, to be used by the “Correlate Time Series” feature of the RAMS GUI, uploading backup images for restoration, or for certain software upgrade scenarios. FTP access is only granted to a subset of user accounts as configured by the administrator. Note that the FTP server is disabled by default unless explicitly enabled from the Administration web pages.

Protocol	Port	Notes
TCP	22	SSH (Secure Shell). Used for access to the RAMS GUI. Normal access to the GUI uses X Windows over SSH. May also be used for SFTP access as an alternative to FTP by those users configured to have FTP access.
TCP	23	Telnet, an unencrypted remote login protocol. RAMS does not allow logins via telnet, but has a daemon listening to the telnet port that prints the message “This host does not accept telnet connections” and closes the connection. The EIGRP topology exploration feature uses this behavior as a performance optimization to avoid retrying unnecessary connections. In theory, multiple RAMSs running in a single network could use this behavior to identify each other.
TCP	49	TACACS+, an authentication, authorization and accounting (AAA) protocol. The master unit in a distributed system can provide user authentication service to the client units in the system. The interactions are encrypted by a shared secret.
TCP	80	HTTP (Hypertext Transfer Protocol). Used for initial web access to the RAMS. Most access to the appliance is encrypted (HTTPS) and is restricted to authorized (password-authenticated) users only.
TCP	179	While technically not a service, RAMS boxes that are configured to record BGP data will have this TCP port open to allow connections from potential BGP peers. This port is open on any interface configured for BGP recording.
TCP	443	HTTPS (Secure Hypertext Transfer Protocol). Used for encrypted access to the RAMS's administration and reporting web pages. Almost all web-based interaction with RAMS units (including authentication) is encrypted.
TCP	646	LDP (Label Distribution Protocol). This port will be open when configured on a Flow Collector unit for collection of MPLS label information in a VPN service provider's network. Not encrypted.
TCP	1020	Raw Flow Server. This port is open on a Flow Collector to allow the Modeling Engine to fetch information from the database of raw traffic flows using a proprietary protocol. Not encrypted.
TCP	2000	XML-RPC, used for the query API. This functionality is disabled by default and, if desired, must be enabled explicitly through the Queries web page. Queries are password-protected. The password can be encrypted or

Protocol	Port	Notes
		sent as plaintext.
TCP	3306	MySQL. Various “distributed configuration” setups (with multiple units being partially configured and operated in a coordinated fashion) need to allow each other remote access to each other's databases. This access is protected by the use of public-key pairs for access and authentication. MySQL's access control tables prevent unauthorized access within the application level. Inter-unit MySQL communication is protected by SSL encryption.
TCP	5000-5000+n (number of Route Recorder units)	MySQL. When database replication is enabled in a distributed RAMS system with n Route Recorder units, multiple MySQL servers are running, each with its own port, to create the replicates from each recorder and allow access to those replicates. Inter-unit MySQL communication is protected by SSL encryption.
TCP	5801	VNC (Virtual Network Computing). Used to access a single, shared instance of the RAMS GUI using a Java VNC viewer. This form of VNC access is an optional feature that is disabled by default. Access is controlled by a password configured when the service is enabled.
TCP	5897	Route / RAMS Traffic status daemon. This port is open on each unit of a Route / RAMS Traffic distributed configuration system. The application listening on this port allows the master unit to display the status and licensing information regarding the other units.
TCP	5901	VNC (Virtual Network Computing). Used to access a single, shared instance of the RAMS GUI through a VNC viewer. This form of VNC access is an optional feature that is disabled by default. Access is controlled by a password configured when the service is enabled.
TCP	5902-5910	VNC (Virtual Network Computing). Used to access multiple instances of the RAMS GUI through a VNC viewer. This form of VNC access is an optional feature that is disabled by default. Access is controlled by the same set of usernames and passwords as configured for X/SSH and web access.
TCP	6101	Flow Collector Configuration Manager, an internal component of the RAMS Traffic appliance to allow configuration changes to the Flow Collector daemon from the Master Modeling Engine unit. Open only if the Flow Collector daemon is running. DES-CBC encrypted with a fixed secret.

Protocol	Port	Notes
TCP	6501-6501+n (number of Collector instances)	The Collector recorder process listens for a connection from the RouteAnalyzer daemon on the Master Modeling Engine unit if the RSVP-TE feature is licensed and IGP-triggered exploration is configured. Not encrypted.
TCP	7890	Flow Analyzer Configuration Manager, an internal component of the RAMS Traffic appliance to allow configuration changes to the Flow Analyzer daemon from the Master Modeling Engine unit. Open only if the Flow Analyzer daemon is running. DES-CBC encrypted with a fixed secret.
TCP	32768-65535	XDMCP (X Display Manager Control Protocol) opens a single port in this range. This port is opened when VNC displays 2 through 10 are enabled; however, access control within the xdm(1) configuration disallows any access from remote machines.
UDP	123	NTP (Network Time Protocol). It is strongly recommended that RAMS use NTP to synchronize its clock with time sources on the network. Although this requires that the NTP daemon listen for packets on the NTP network port, the daemon ignores all requests to query or change its operating state.
UDP	161	SNMP (Simple Network Management Protocol). SNMP is used for querying various aspects of the REX unit's operation. This functionality is disabled by default until a read-only community string (for SNMPv2) or security profile (for SNMPv3) is set.
UDP	162	SNMP traps. Reception of SNMP traps is enabled if configured as part of the RSVP-TE feature to learn about changes in tunnels. The port number is configurable.
UDP	177	XDMCP (X Display Manager Control Protocol). This port is opened when VNC displays 2 through 10 are enabled; however, access control within the xdm(1) configuration disallows any access from remote machines.
UDP	514	Syslog. Reception of Syslog messages from routers is enabled if configured as part of the RSVP-TE feature to learn about changes in tunnels. The port number is configurable.
UDP	646	LDP (Label Distribution Protocol). This port will be open when configured on a Flow Collector unit for collection of MPLS label information in a VPN service provider's network. Not encrypted.

Accessing the RAMS

There are several means of accessing the RAMS. You can access the RAMS GUI using X Windows tunneled over SSH. All traffic (including the initial password-based authentication exchange and the tunneled X Windows data) is encrypted using one of several strong encryption algorithms.[1] The SSH server process on the appliance requires SSH protocol version 2.

The GUI can also be accessed using the Virtual Network Computing (VNC) family of remote desktop access applications or X Windows over SSH.

RAMS supports multiple VNC sessions per unit, with one user per independent session. You can log in using your normal passwords on a customized version of the xdm(1) login manager, running inside a VNC instance. The VNC display number is used to select the screen size. This functionality opens TCP ports 5902 through 5910 inclusive. This service is disabled by default. A single shared session on VNC display :1 is also available if enabled. Access to the shared session is controlled by a password that is configured at the time the session is enabled.

Most configuration functions of the RAMS (beyond the initial network setup on the serial console) are performed through the web administration interface. All web traffic is all encrypted using HTTPS and ciphers with keys at least 128 bits in length. Authentication and authorization to all of the administration functions is protected by a username and password login (again this transaction is encrypted). Cookies are used to maintain login session state, as well as to transfer authentication credentials between different units in a distributed configuration setup.

In its initial configuration, the RAMS web server uses a self-signed certificate to authenticate itself to users. Consequently, users accessing the web administration interface will see warnings from their web browsers that they might not see when accessing web sites that have certificates signed by well-known certificate authorities (e.g. web commerce sites). To avoid these warnings, the RAMS can generate a Certificate Signing Request so that a certificate signed by a well-known certificate authority may be obtained and installed into the web server on the RAMS.

User Authentication and Authorization

RAMS can be configured to perform authentication and authorization of users either through a remote TACACS+ or RADIUS server or through its own internal TACACS+ server. If remote authentication is configured but authentication through the remote server fails, then authentication is attempted using the internal server as a backup. In a distributed configuration with multiple RAMS units, the client units can be configured to authenticate using the TACACS+ server on the master unit so that user accounts need be configured only once.

In all cases, communication between a RAMS unit and the authentication server is protected using a shared secret configured on both the RAMS and the server.

[1] The version of OpenSSH used on the RAMSs supports AES, 3DES, BlowFish, CAST128, or Arcfour. The actual encryption algorithm used by any particular session is selected by the end user's SSH client software.

Serial Console

Initial setup of the RAMS is done through a serial port console interface. This interface initially does not require any authentication on the assumption that using it requires physical access to the unit. However, a password can be configured so that subsequent access is not allowed without the password. If the serial port console is to be made remotely accessible (for example, using a network-accessible console server), encryption and authentication for the remote access is strongly recommended.

Most of the functions of the serial port console interface can also be accessed via SSH if a user account is configured to have “CLI Access” privilege. Such accounts do not invoke the usual X-based application GUI when the SSH connection is established, and instead run the same text-based CLI that is presented on the serial port console. This CLI provides access to several diagnostic functions such as ping and traceroute.

SNMP Queries

Each RAMS unit runs an SNMP daemon. It supports SNMPv2 and SNMPv3 queries of various aspects of the RAMS's operation. Queries are supported to the system, interfaces, SNMPv2, TCP, IP, UDP, view-based access control model, and tunnel MIBs. No application-specific MIB is supported. SNMP queries are disabled by default until a read-only community string (for SNMPv2) or security profile (for SNMPv3) is set.

Application Programming Interface (XML RPC API)

External systems can access various kinds of data stored in the appliances by sending queries to the XML RPC API. This functionality is disabled by default and, if desired, must be enabled explicitly through the Queries web page. Queries are password-protected. The password can be encrypted or sent as plaintext.

In a multi-unit system, most queries would be sent to the Master Modeling Engine or a secondary Modeling Engine if there is one. For example, a summary of the status of all units in the system is returned from an api_system_health query to the Master unit. Alternatively, that query may be sent directly to an individual unit to obtain the status of that unit alone. Queries for routing data can be served by the Route Recorder unit that records the requested topologies. Queries for raw flow records must be sent to the Flow Collector unit recording the desired traffic.

The XML RPC API is also used internally by the Collector recorder to obtain a list of all routers in the IGP and BGP topologies. That query can be served by the Collector's own unit if the system includes only one Route Recorder, but usually it is served by the Master Modeling Engine.

RAMS Network Usage

RAMS has a number of reasons for sending data over the network, either between units in a distributed system or to external routers or servers. These uses are briefly described here to characterize the expected behavior of RAMSs that could be visible from parts of a customer's network infrastructure (for example, intrusion detection systems, network monitoring, etc.).

Routing and Topology Discovery

RAMS needs to establish peerings with neighbor routers; towards this end it emits and responds to protocol messages for any IGPs being recorded, including OSPF, ISIS, or EIGRP. If a BGP topology is being recorded, RAMS will accept TCP connections from neighboring BGP routers that are included in the configured list of peers.

In order to do EIGRP topology discovery, a RAMS will perform telnet or SSH logins as configured in order to query all the EIGRP-speaking routers within each EIGRP AS that is configured to be recorded. These logins use authentication parameters entered and stored as part of the recorder configuration. Enabled access is not required.

If recording of “Collector” information is also configured, queries will be sent to the routers within the recorded network using one or more of the access methods SNMP, SSH or telnet for CLI, and SSH for NETCONF, as configured, to collect configuration and status information from the routers. The collected information includes router vendor, software version, hardware type and serial number, and interface details. Static routes can be collected in addition from some or all of the routers if configured. For VPN networks additional information such as VRF routing tables will be collected. If the RSVP-TE feature is licensed, then the configuration of tunnels will be collected both during the initial topology exploration and dynamically based on triggers from IGP changes, syslog messages, or SNMP traps. See the Appendix of the Administrator's Guide for a full description of the information collected.

Alerts

RAMS may send alerts to notify the user / administrator of notable conditions in the network such as excessive network churn. These alerts can take the form of SNMP traps sent from a REX unit to an SNMP management station, or syslog events sent to a syslog server, or email messages sent to configured recipients. By default, this functionality is disabled until enabled by the user from the Alerts configuration dialog in the GUI.

Software Updates

Updates to the software images on the unit are typically transferred from Packet Design's update server using the File Transfer Protocol (FTP). Although this protocol offers neither authentication nor encryption, the update images themselves are encrypted and cryptographically signed before being placed on the update server. The RAMS software will not install an update image unless the user supplies the correct update key, the update image is successfully decrypted, and the attached signature is correctly verified.

RAMS supports upgrades from USB “key chain” flash memory devices. This feature is intended primarily for use by support personnel upgrading units that cannot reach the Packet Design update server. The same mechanisms used to protect the integrity of FTP transfers are also used for USB-based updates.

Technical Support Callback

The Technical Support Callback feature (currently enabled through the serial port console interface or the System web page) provides a way for HP support personnel to access a unit in some circumstances where the unit may not be directly accessible from the outside. In brief, this feature initiates an SSH connection from a RAMS Appliance to a restricted account on a dedicated machine at Packet Design (rextarget.packetdesign.com); it is configured in such a way that new login sessions can be tunneled through the SSH connection back to the RAMS Appliance. This feature is disabled by default, and requires an explicit action on the part of the customer to enable it. If technical support callback is enabled and a unit is rebooted (or if network communication is otherwise interrupted), then the RAMS Appliance will try to re-establish the callback connection. Note that this mechanism provides a means (albeit limited) of bypassing a customer's firewall and opens up an avenue of access to the customer's RAMS Appliance. Customers should be cautioned not to enable technical support callback except when requested by HP support personnel.

Access to appliances connected via the technical support callback mechanism requires an account on the appropriate callback host, as well as possession of a shared SSH private key file. The key file and its unlocking passphrase are only given to authorized HP personnel with “need to know” access. This key is changed periodically in conjunction with major software releases.

Network Time Protocol

A RAMS unit can use the Network Time Protocol (NTP) to synchronize its clock with time sources on the network. Enabling this feature will result in NTP packets being sent to and from time servers configured on the Time and Date web administration page. As with any other NTP client, customers should use reasonably trusted NTP servers. Configuring multiple NTP servers is recommended for reliability; up to 3 servers may be specified. The NTP daemon is configured not to provide time service to any other hosts, and it ignores any request over the network to query or change its operating state.

Note that NTP time synchronization of RAMS units is strongly recommended. NTP time synchronization of routers exporting NetFlow data to RAMS Traffic Flow Collectors is also strongly recommended.

Distributed Configuration

Multiple RAMS or RAMS Traffic units may be connected in a “distributed configuration” environment, whereby the multiple units can be configured and operated (at least in some respects) from a single “master” unit. As of this writing, operations on licenses and recorder configuration are performed on the master unit, while other configuration and administration functions are performed separately on each unit.

In each distributed configuration setup, one unit is designated to be the “master”. Users access the master unit for all license and recorder configuration operations. A unit can only become a master if it is so licensed and if the user has explicitly performed the “Make Master” operation on the Units web page. In typical RAMS Traffic deployments, the Modeling Engine will be the master.

“Client” units are added from the master's Units page. The master is authenticated to the clients using a shared secret called the “Master Access Password”. To prevent rogue or misconfigured masters from adding unauthorized clients, the Master Access Password can be changed on the serial port configuration menu of each unit. The Master Access Password is only used for authentication during the initial client binding operation; subsequent access is authenticated by keys deposited as a part of the initial binding operation. Clients require this protection because the master has the ability to perform configuration actions (such as applying licenses or starting recording) on bound clients without further authentication.

Control actions between the master and its associated clients take place over encrypted (HTTPS) network connections.

Distributed configuration systems have the ability to to access each other's databases. For example, a RAMS Traffic Flow Analyzer needs to access the routing databases on a Route Recorder and the traffic databases on a Flow Collector. Normally this access is provided by replicating the databases from one unit to the other. Both remote access and replication take place over MySQL connections that are encrypted using public-key mechanisms. Each unit in the distributed configuration setup is given an X.509 certificate signed by the master unit when it added to the master. The unit must present the certificate in order to access databases stored on another unit. Each unit also possesses the certificate of the master unit in order to verify the authenticity of any units trying to access its databases remotely.

User Authentication Service

RAMS will contact a remote TACACS+ or RADIUS server if configured for remote authentication and authorization. In a distributed configuration of multiple units, if the client units are configured to authenticate via the master unit, then the client unit will contact the master unit using the TACACS+ protocol. For all cases, the exchange between the RAMS unit and the server is protected with a shared secret entered on the unit and on the server.

If local authentication is selected on all units, then authentication will be performed by a TACACS+ server running inside each unit so no external communication is required.

Database Archival

The user can configure RAMS to periodically archive the recorded databases to a storage server provided by the user. The server is accessed via the Common Internet File System (CIFS) protocol, successor to the Microsoft® SMB protocol. This protocol operates between a dynamically assigned port number on each RAMS unit configured for archiving and TCP port 445 on the storage server. If a firewall separates the RAMS unit from the storage server, this protocol must be allowed to pass between these systems.

Domain Name Service

For a variety of reasons, a RAMS may need to perform name resolution using the Domain Name Service. These may include (but are not limited to): DNS resolution performed on the part of the RAMS GUI, finding the update or technical support callback servers at Packet Design, finding time servers, and sending email.

For a variety of reasons, a RAMS Appliance may need to perform name resolution using the Domain Name Service. These may include (but are not limited to): DNS resolution performed on the part of the RAMS GUI, finding the update or technical support callback servers at HP or Packet Design, finding time servers, and sending email.

The table below lists hosts at Packet Design, Inc. that might be accessed by a RAMS Appliance. These entries may be useful for inserting into a customer's private DNS server or helping to verify the identity of a host. The IP addresses in this table are current as of this writing, but are subject to change.

Host	IP Address	Use
rextarget.packetdesign.com	65.192.41.14	SSH server for technical support callback connections.

Email

RAMS has had the ability to send periodic email reports about the state of networks being monitored, as well as the general health of the appliance. These are sometimes referred to as “Batch Emails” or “Daily Reports”. Currently, a single report is generated once a day at a user-selectable time. Email may also be configured as a delivery method for alerts generated by RAMS.

RAMS uses the Simple Mail Transfer Protocol (SMTP) to transmit the email message, usually to a customer's mail server. SMTP is the standard protocol used for sending mail to Internet mail servers (other protocols, such as POP3 or IMAP, are used by mail clients to retrieve messages from servers, and do not enter into this discussion). RAMS relies on the sendmail mail transfer daemon for the actual transfer of messages.

The customer's mail server is typically one that can accept messages from workstations or other end-user systems. It frequently is referred to as an “outbound mail relay”, “outgoing mail server”, or some similar term. If the outbound mail relay is unreachable or cannot process the message, sendmail will queue the mail and re-attempt delivery once per hour. If the message cannot be sent for five days, it will be silently dropped.

If the “Mail Server” field on the Mail configuration page is left blank, RAMS will attempt to send mail messages directly to the recipients' mail servers.

RAMS will never accept mail messages, and in fact does not even accept inbound connections on TCP ports 25 or 587, which are usually used for accepting mail messages. Users with internal firewalls will need to permit traffic from the RAMS to TCP port 25 on the configured mail server in order for periodic email reports to be delivered correctly.

RAMS Traffic and Traffic

RAMS Traffic extends the capabilities underlying RAMS to include analysis of network traffic. Traffic information is gathered from via NetFlow[2] and analyzed with respect to the routing model. The Flow Collector units in a Traffic Explore deployment are passive receivers of NetFlow data. They send no data to the exporting routers; they only receive a stream of UDP packets. Note that NetFlow data is unencrypted and may reveal (at various levels of detail) information about end user network traffic. The contents of network conversations are not exposed, but NetFlow can provide information about the sources and destinations of flows, protocol and port numbers, and traffic volume.

To prevent a rogue or misconfigured router from overwhelming (or corrupting) the FRs, each FR has an access list of routers from which it will accept NetFlow packets (the access list is specified on the Flow Collector configuration web pages). This provides a simple form of access control. Note that because NetFlow (in currently-supported formats) is carried over UDP, it would be possible for an attacker to send packets that spoof the sending address of a permitted router.

Firewall Passage Requirements

The previous sections described the forms of communication utilized to, from and among RAMS and Traffic Explore units. A distributed configuration generally requires IP connectivity among all of the different REX units. The presence of internal firewalls could interfere with this communication.

This section summarizes the network access that must be allowed if a firewall is interposed between any two units in a RAMS system or between that system and its users or the servers that it accesses. For example, remote database access requires that customers' internal firewalls (if any) allow TCP connections to port 3306 (the default MySQL port) and to ports in the range 5000-5000+N (for MySQL replication) among some of the communicating units. Connectivity between units is tested using the “ping” utility that transmits ICMP Echo Request packets and looks for ICPM Echo Reply packets in return.

[2] NetFlow is originally a Cisco feature but is implemented by a number of vendors and open source operating systems. On Juniper routers, this feature is called “cflow”. NetFlow v9 is the basis for the IPFIX standard.

These must not be blocked by a customer's firewall.

The following tables list the specific ports and protocols that must be allowed to pass through a firewall interposed between two units of a particular type. The “to” unit is the one that is listening on the specified port, and the “from” unit establishes the connection.

The FTP connection from a unit to an FTP server or to the Master unit to transfer a software update image is requested in passive mode (PASV). This means that the data transfer connection will be opened by the unit and will use a dynamically allocated port number on the server that is communicated over the control connection on port 21.

From users or servers to any unit

Service	Protocol	Port
FTP for backups, etc.	TCP	21
SSH (for CLI Access privilege)	TCP	22
HTTP for web UI (just redirects to HTTPS)	TCP	80
HTTPS for web UI	TCP	443
NTP for time sync	UDP	123
SNMP (if desired for polling)	UDP	161
XML RPC API (if using direct queries)	TCP	2000

From any unit to servers

Service	Protocol	Port
FTP for software update	TCP	21 (passive)
SSH (for Technical Support Callback)	TCP	22
SMTP for alerts & reports (if configured)	TCP	25
TACACS+ (if selected for remote AAA)	TCP	49
NTP for time sync	UDP	123
SNMP for traps (if configured)	UDP	162
RADIUS (if selected for remote AAA)	UDP	1812

From routers to Route Recorder or RAMS

Service	Protocol	Port
SNMP traps (if configured for RSVP-TE)	UDP	162
BGP (if recording BGP)	TCP	179
Syslog (if configured for RSVP-TE)	UDP	514

IGPs (if tunnels are configured)	GRE (protocol 47)	--

From routers to Flow Collector

Service	Protocol	Port
LDP (if configured for MPLS VPN)	TCP	646
LDP (if configured for MPLS VPN)	UDP	646
NetFlow	UDP	any (9991 default)

From Route Recorder or RAMS to routers

Service	Protocol	Port
SSH (if configured for CLI collection)	TCP	22
Telnet (if configured for CLI collection)	TCP	23
SNMP (if configured for info collection)	UDP	161
SSH (if configured for NETCONF)	TCP	830
IGPs (if tunnels are configured)	GRE (protocol 47)	--

From Flow Collector to routers

Service	Protocol	Port
LDP (if configured for MPLS VPN)	TCP	646
LDP (if configured for MPLS VPN)	UDP	646

From users to RAMS or Modeling Engine (Master or Secondary)

(See also “From users or servers to any unit”)

Service	Protocol	Port
SSH/X for GUI	TCP	22
HTTP for web UI (just redirects to HTTPS)	TCP	80
HTTPS for web UI (primarily to Master)	TCP	443
XML RPC API	TCP	2000
VNC for GUI	TCP	5901-5910

From Master Modeling Engine to Route Recorder or RAMS

Service	Protocol	Port

HTTPS	TCP	443
XML RPC API (if using api_system_health)	TCP	2000
MySQL	TCP	3306
Status Daemon	TCP	5897
IGP Triggers (if multiple RR or REX units)	TCP	6501-6501+n
Ping	ICMP Echo	--

From Master Modeling Engine to Flow Analyzer

Service	Protocol	Port
HTTPS	TCP	443
XML RPC API (if using api_system_health)	TCP	2000
MySQL	TCP	3306
Status Daemon	TCP	5897
Ping	ICMP Echo	--

From Master Modeling Engine to Flow Collector

Service	Protocol	Port
HTTPS	TCP	443
Raw Flow Server	TCP	1020
XML RPC API (if using api_system_health)	TCP	2000
MySQL	TCP	3306
Status Daemon	TCP	5897
Configuration Manager (flowaggd)	TCP	6101
Configuration Manager (trs)	TCP	7890
Ping	ICMP Echo	--

From Master Modeling Engine to Secondary Modeling Engine

Service	Protocol	Port
HTTPS	TCP	443
XML RPC API (if using api_system_health)	TCP	2000
Status Daemon	TCP	5897

Ping	ICMP Echo	--

From Secondary Modeling Engine to Master Modeling Engine

Service	Protocol	Port
FTP (for Update All Units)	TCP	21 (passive)
TACACS+ (if authenticating via Master)	TCP	49
MySQL	TCP	3306
MySQL (if data source is Master)	TCP	5000-5000+n
Ping	ICMP Echo	--

From Secondary Modeling Engine to Route Recorder or RAMS

Service	Protocol	Port
MySQL (unless data source is Master)	TCP	3306

From Secondary Modeling Engine to Flow Analyzer

Service	Protocol	Port
MySQL	TCP	3306

From Secondary Modeling Engine to Flow Collector

Service	Protocol	Port
Raw Flow Server	TCP	1020
MySQL	TCP	3306

From Route Recorder to Master Modeling Engine

Service	Protocol	Port
FTP (for Update All Units)	TCP	21 (passive)
TACACS+ (if authenticating via Master)	TCP	49
XML RPC API (for Collector recorder)	TCP	2000
MySQL	TCP	3306
Ping	ICMP Echo	--

From Route Recorder to Flow Collector, Flow Analyzer, or Secondary ME

Service	Protocol	Port

None		

From Flow Collector to Master Modeling Engine

Service	Protocol	Port
FTP (for Update All Units)	TCP	21 (passive)
TACACS+ (if authenticating via Master)	TCP	49
MySQL	TCP	3306
Ping	ICMP Echo	--

From Flow Collector to Route Recorder

Service	Protocol	Port
MySQL	TCP	3306

From Flow Collector to Flow Analyzer or Secondary Modeling Engine

Service	Protocol	Port
None		

From Flow Analyzer to Master Modeling Engine

Service	Protocol	Port
FTP (for Update All Units)	TCP	21 (passive)
TACACS+ (if authenticating via Master)	TCP	49
MySQL	TCP	3306
Ping	ICMP Echo	--

From Flow Analyzer to Flow Collector

Service	Protocol	Port
MySQL	TCP	3306

From Flow Analyzer to Route Recorder or Secondary Modeling Engine

Service	Protocol	Port
None		

Licensing

The primary method of controlling access to the RAMS features relies on licenses issued by HP. Various product features check for valid license attributes (and license expiration dates) when they are invoked.

The license-checking stores the raw, cryptographically-signed licenses in the license database, exactly as applied by the user on the License web page. Multiple licenses (with different expiration times) can be installed at once; composing the license features and verifying checksums is performed with every license check. Every license is locked to a particular unit based on its Unit ID or serial number. This implementation is designed to prevent subversion of the contents of the license database; an attacker trying to modify the license database would also need to correctly modify the digital signature on the stored license.

In all software releases to date, it should be noted that licenses are preserved across a “Reset to Factory Default” (RTFD) operation. While this technically means that RTFD does not truly return the unit to a completely known state, it was felt that this disadvantage was acceptable in exchange for user convenience.

In distributed configuration setups, users apply licenses using the master unit's web pages. The licenses relevant to each client unit are automatically propagated out to that unit (depending on the Unit ID or serial number encoded in each license).

Security Components

RAMS uses a number of widely-deployed packages for security and cryptographic functions, some of which are listed in the table below. Unless otherwise noted, all version numbers refer to RPM archive files issued by the CentOS Project as a part of CentOS Linux 5.2 or subsequent updates.

Name	Version	Notes
httpd	2.2.3	The Apache web server.
mod_ssl	2.2.3	The Secure Sockets Library (SSL) module for the Apache web server.
openssh	4.3p2	Secure Shell (SSH) implementation with backported security fixes, common files used by both client and server programs.
openssh-clients	4.3p2	Secure Shell (SSH) implementation with backported security fixes, client programs.
openssh-server	4.3p2	Secure Shell (SSH) implementation with backported security fixes, server programs.
openssl	0.9.8e	Secure Sockets Library implementation with backported security fixes.

June 2012