Release 10.3 for Secure Router 2330 & 4134 General Availability

Revision History

Date	Revision #	Summary of Changes
19 Nov 2010	1.0	This is the original publication

Introduction

Avaya is pleased to announce general availability of the Release 10.3 for the Secure Router 2330 and 4134 effective November 3rd, 2010. This release extends the resiliency, scalability and performance of IPSec VPN services, as well as enhances the core security features of the Secure Router 2330 and 4134. It also provides the basis for Federal Information Processing Standard (FIPS) 140-2 Level 2 test certification for these Secure Router platforms which is scheduled for completion in late 2011.

Product Description/Solution Overview

Release 10.3 delivers new features that enable more robust security solutions based on the Secure Router 2330 and 4134. Key enhancements have been made in the following areas:

Resiliency – IPSec VPN tunnel back-up services on the Secure Router 2330 and 4134 have been significantly strengthened with Release 10.3. VPN tunnel back-up (or fail-over) is the ability to use an alternative VPN tunnel path if a primary VPN tunnel is no longer available. Key features include the ability to define "nailed-up" VPN tunnels over IP static links. Nailed-up tunnels can more quickly detect VPN tunnel failure and establish a back-up path. Also, back-up tunnel mechanisms have been expanded to provide more efficient operation over both static-routed and dynamically-routed VPN connections.

Scalability and Performance – Significant improvements in VPN performance and scalability have been achieved. Most notably, Release 10.3 delivers a three-fold increase (and more) in the number of dynamically routed VPN tunnels on the Secure Router 2330 and 4134. This helps Secure Router IPSec VPN performance over both OSPF and RIP connections. VPN tunnel establishment (or start-up) rates have also been greatly improved in Release 10.3 – valuable when running multiple VPN tunnel connections to one or more remote system. Additional scaling improvements include support for multiple IP sub-nets on a single VPN tunnel and a more efficient mechanism for handling RIP updates (i.e., triggered RIP) over IPSec.

Core Security – Enhancements have also been made in the core security functionality of the Secure Router 2330 and 4134 – both to increase these platforms' base security and to make them more conformant with industry-standards. These include support for larger RSA certificate key sizes, two-factor authentication for the management interface and branch office "split-tunneling" support.

Foundation for FIPS 140-2 Level 2 certification – Release 10.3 will be the foundation release used to take both the Secure Router 2330 and 4134 through FIPS 140-2 Level 2 certification. FIPS (or Federal Information Processing Standard) 140-2 is the US Federal security standard used to accredit cryptographic devices. Acquiring this certification will facilitate Avaya Government Solution sales of Secure Router 2330 and 4134

sales to US Federal agencies, but also will help in sales to state and local government as well as enterprise customers, who often require this certification. Since FIPs accreditation is an intensive process requiring the 3rd-party testing, the goal is to achieve FIPS 140-2 Level 2 accreditation in 2nd Half of Calendar 2011.

Release 10.3 Feature Details:

The following is a brief description of key features in the 10.3 release. For a list and description of all the new 10.3 features, please refer to the *Avaya Secure Router 10.3 Release Notes (NN47263-400).*

IPSec Nailed-Up Tunnels. New in Release 10.3, IPSec nailed-up tunnels enable an "always-available" tunnel to be set up on the Secure Router, even if no data is being transmitted across the tunnel. Data can be more quickly forwarded across the tunnel, since it is "nailed-up" and does not require VPN tunnel establishment. Previously on the Secure Router, a VPN tunnel was only established "on-demand" when data was ready to be forwarded across the tunnel. Nailed-up tunnels are particularly useful when configuring VPN tunnels over statically routed links, since IP route updates are not transmitted across the link to keep the VPN tunnel open.

Periodic Tunnel Health-Checks (aka Periodic Dead Peer Detection). In Release 10.3, the ability to periodically send a keep-alive message through the VPN tunnel to check tunnel status has been added. If the Secure Router 2330/4134 does not receive a response to the keep-alive, the remote system (or peer) is deemed unreachable and the Secure Router can take appropriate action to tear down the VPN tunnel and re-route traffic. In previous releases, tunnel status was only checked when data was ready to be transmitted across the tunnel (i.e., on-demand health checking). Periodic health checking is important in situations where consistent tunnel availability is a high priority (for example over nailed-up tunnels), as well as to more quickly detect connectivity failures and re-route data to secondary paths.

Tunnel Fail-over using Round-Robin DNS. With Release 10.3, the Secure Router 2330 and 4134 has added the ability to configure (or use) a Domain Name Server (DNS) name for an IPSec VPN peer. With this capability, the Secure Router can use DNS "round-robin" replies to establish a back-up VPN tunnel when the primary VPN tunnel fails. This capability is especially useful over broadband connections – where DHCP-assigned addresses are used in conjunction with a DNS server to connect to the Internet.

Tunnel Fail-over using Static Weighted Tunnels. Static weighted tunnels have been added in Release 10.3. This feature enables "weighting" of VPN tunnels, which can be used to configure primary and back-up VPN tunnels over static IP routes. Each tunnel (or path) can be given a relative weight and the Secure Router 2330/4134 will forward traffic accordingly. This feature provides an efficient way to configure VPN tunnel back-up options over static IP links.

Increase in Dynamically Routed Tunnels. VPN tunnel capacity over dynamically routed RIP and OSPF connections has greatly increased in Release 10.3 – in some cases more than a three-fold increase. The Secure Router 2330 now can handle up to 100 VPN tunnels over RIP and 50 VPN tunnels over OSPF; the Secure Router 4134 now can run 500 RIP tunnels and 150 OSPF tunnels. The increased VPN tunnel capacity will help the Secure Router within large and/or highly-meshed site-to-site network deployments.

Multiple IP Subnets on a Single VPN Tunnel. With Release 10.3, multiple IP sub-networks can be configured on a single IPSec VPN tunnel. This is done by defining an IP address range for both source and destination IP address associated with each tunnel. In previous releases, only a single source and destination subnet could be associated with a VPN tunnel. This enhancement not only simplifies Secure Router VPN tunnel configuration, but minimizes the number of IPSec VPN tunnels needed on the Secure Router to securely connect multiple IP subnets.

Triggered RIP. The Secure Router 2330/4134 now supports triggered RIP (Routing Information Protocol) as an extension for on-demand circuits (e.g., ISDN). Based on RFC 2091, triggered RIP improves RIP efficiency by transmitting route updates only when an update to the routing database occurs. This feature is particular useful when configuring back-up VPN tunnels over on-demand circuits, like ISDN, since it suppresses RIP route updates over the on-demand circuit.

IPSec VPN Bypass Policy. The Secure Router 2330 and 4134 can now explicitly exclude network traffic from traversing a VPN tunnel in Release 10.3. This capability can be used to enable "split-tunneling" on the Secure Router – the ability for some traffic to access the Internet instead of going through the VPN tunnel. It also allows IP traffic to traverse between two "secure" subnets without going through a Secure Router VPN tunnel. This feature provides additional flexibility for handling VPN tunnel traffic within the branch.

Key Certificate Improvements. Release 10.3 introduces several enhancements to certificate key operation. These include an increase in the RSA certificate key size to 4096 bits from 2048 bits. Enhancements have also been made to X.509 digital certificates, including support for "key usage extension checking" as well as special character support in the Distinguished Name (DN) attribute (as specified in RFC 2253). Beyond improved security, these enhancements provide greater interoperability with Avaya/Nortel VPN Router environments where these certificate key features were supported.

Two-Factor Authentication for Device Management. The Secure Router 2330 and 4134 previously supported single-factor authentication (User ID and password) for telnet and console based access to the device. With Release 10.3, two-factor authentication has been added for both telnet and console-based access. Two-factor authentication supported in Release 10.3 is based on RSA Secure ID and includes both PIN and token-based mechanisms.

Target Customers / Positioning

Release 10.3 enhances the secure site-to-site VPN operation of the Secure Router 2330/4134 and adds to their positioning as converged branch routers for enterprise remote sites. Beyond the new security functionality, a key goal of Release 10.3 was to improve interoperability with the Avaya VPN Router (aka Contivity) products. In fact, many 10.3 features mirror capabilities that exist on Avaya's VPN Router family. By making the Secure Router more interoperable with the VPN Router, Release 10.3 will help ease migration of VPN Router customers to the Secure Router 2330/4134 platforms.

Another purpose of Release 10.3 is to establish the baseline for US Federal security (i.e., FIPS 140-2 Level 2) certification for the Secure Router 2330 and 4134. 10.3 will be the foundation release for taking these two platforms through FIPS certification testing during Calendar Year 2011 with the goal of achieving certification by year-end. FIPS certification for the Secure Router 2330 and 4134 will not only help in positioning the Secure Router within US Federal government opportunities, but also within state and local governments and industry verticals, like financial services, who use FIPS certification as a check list item when evaluating security devices.

System Requirements

Release 10.3 runs only on the Secure Router 2330 and 4134 and is the base operating system for these Secure Router platforms. (Release 10.3 is not supported on the Secure Router 1000 Series, 3120 or 8000 Series platforms.) **NOTE:** IPSec VPN features on the Secure Router 2330/4134 are enabled only through an optional IPSec VPN encryption module. The VPN Encryption module must be purchased separately from the Secure Router 2330/4134 chassis.

Compatibility

IPSec VPN features in Release 10.3 have been extensively tested and validated for interoperability with Avaya's VPN Router family. A key goal of Release 10.3 was to improve Secure Router 2330 and 4134 interoperability with customer's existing VPN Router networks.

The Secure Router 2330 and 4134 with Release 10.3 has also been extensively tested with Secure Router 1000 and 3120 platforms running Release 9.4.

Product Availability

Release 10.3 for the Secure Router 2330 and 4134 is generally available worldwide as of November 3rd, 2010. **NOTE**: The Secure Router IPSec VPN module employs secure encryption technology that may be restricted from export to certain countries (i.e., Iran).

Ordering Information/Packaging

Secure Router customers with an existing support contract can download Release 10.3 from the support site. Otherwise, no new ordering codes have been created. Customers can order Secure Router 2330 and 4134 hardware and associated software licenses using standard ordering procedures. For more information, contact your Avaya Sales/Channel Account Manager or distributor.

Training

Sales training on the Secure Router 2330 and 4134 is available through an Avaya Professional Sales Specialist (APSS) module on Avaya's Unified Branch portfolio (Course #ASC00633OEN) This sales training module can be accessed through on the Avaya University web site at: https://www.avaya-learning.com/.

Documentation and Sales Collaterals

General information on the Secure Router 2330 and 4134 can be found on the Global Sales Portal for each site. Each site hosts a variety of product resources including Knowledge Transfer Kits (KTKs), product brochures, Customer Presentations, and other marketing and support materials. The Secure Router 2330 Sales Portal can be directly accessed at: https://enterpriseportal.avaya.com/ptlWeb/gs/products/P0617/AllCollateral. Partners can access the Secure Router 2330 Partner portal page at: https://enterpriseportal.avaya.com/ptlWeb/bp/products/P0617/AllCollateral

Contacts for additional information

Mike Fitzgerald, Secure Router Lead Product Manager, E-mail: mifitzge@avaya.com

Dave Passamonte, Secure Router R10.3 Product Manager, E-mail: dpassamo@avaya.com

Bob Reason, Unified Branch Marketing Manager, E-mail: rreason@avaya.com