Nortel VPN Router

Software Patch V8_05.455

1. Release Summary

Release Date: August 9, 2012
Purpose: Software Maintenance Release to address customer found software issues.

Note:
As of August 2010 the Nortel VPN Router defect reporting tool Clarify is being replaced with the Avaya Clear Quest defect reporting tool. Defects are reported in Work Items (WI) not in Correction Reports (CR) as was done in Clarify. For any defect originally reported in Clarify, the new WI number will be followed by the corresponding CR number for clarity.

2. Important Notes Before Upgrading to This Release

None

3. Platforms Supported

Nortel VPN Router (formerly known as Contivity Secure IP Services Gateway) software Release V08_05.455 supports the following hardware platforms

600
1010
1050
1100
1600
1700
1740
1750
2600
2700
2750
4600
5000

4. Notes for Upgrade

For details on how to upgrade your VPN Router (formerly known as the Contivity Secure IP Services Gateway), see the *VPN Router Release Notes* (NN46110-403 03.01, part no. 315000-U Rev 01. Release notes are

available at http://www.avaya.com/support; Select Documentation and Release Notes & Software Update Notes, click on the letter "V" for VPN Router Portfolio and select your product for available Release Notes.

5. Version of Previous Release

Software Version 8_05.450

6. Compatibility

In order to take full advantage of this Release the following versions are recommended for the related products.
This is only a recommendation; this Release is compatible with all supported versions.

Contivity VPN Client	8.01.100
Avaya VPN Client	10.06.022
Contivity VPN Localized Client	6.02.040
Nortel Tunnel Guard Agent	4.5.0.0_014
Avaya VPN Gateway	6.0.1

NOTE: Contivity VPN Client version 5_01.103 and above is required to get the full benefit of Entrust Roaming Profiles and Entrust Link Certificates.

7. Changes in This Release

New Features in This Release

None

Old Features Removed From This Release

None

Problems Resolved in This Release

Nortel VPN Router sustaining Release Version 8.05.455 resolves the following issues:

wi00994731-
Avaya VPN Router may core in task tRipTimer with ECMP enabled.

Nortel VPN Router sustaining Release Version 8.05.454 resolves the following issues:

wi00946115 –
Avaya VPN Router does not perform sufficient validity checking on the Isakmp Informational Frame. This may lead to the ISAKMP task hanging for periods of time affecting new incoming sessions.

Nortel VPN Router sustaining Release Version 8.05.453 resolves the following issues:

wi00527953 –
Avaya VPN Router does not provide detail information for the source of a LAND Denial of Service attack. Information regarding the interface and IP protocol is now logged.

wi00873464 –
The Avaya VPN Router may core in the Journal Update environment.

wi00924705 –
The Avaya VPN Router may core in the HTTP server process while under heavy load.

wi00955284 –
The fix for WI00653592 did not account for a second condition and would therefore continue to process the invalid Hash payloads from a VPNC Client. In addition it was discovered that a non Avaya VPN Client may attempt to negotiate an encryption proposal for AES 128 Group1 and that the Avaya VPN Router incorrectly accepted this leading to the recognition of an invalid hash payload. This specific scenario has been resolved in this release and the non Avaya VPN Client connection will not be dropped. The protection against invalid hash payloads that may be caused by unknown factors remains in the code.

Nortel VPN Router sustaining Patch Version 8.05.451 resolves the following issues:

wi00525867 –
The Nortel VPN Router may lose memory when a BGP MIB Table Update fails.

wi00871157 –
The Nortel VPN Router returns invalid values for the TunnelConfig MIBs when an SNMP Query is performed.

8. Outstanding Issues

1. After installing a new CA certificate to replace an expiring CA certificate and with both CA certificates still on the VPN Router (AVR), VPN Client (AVC) users are not able to login.

The AVR will not allow remote certificate AVC users login access with two CA certificates installed with the same Subject DN. The following log message is seen in the Event Log:

08/07/2012 05:28:54 0 Security [05] ISAKMP Verify Signature: peer certificate validation failed, Matching CA certificate was not found

Workaround:

Remove the expiring same Subject DN CA certificate allowing only the new same Subject DN CA certificate to remain. AVC users can then login.

---

2. An issue has been identified with the V08_0X.XXX version software. When a certificate PKCS#10 request is made on the VPN Router (AVR), the AVR adds a space to each line of the output resulting in what appears like a diagonal line running down the entire request output. When the request is imported to the certificate server the certificate request is denied. This issue has only been identified with Verisign CA servers.

Workaround:

Open the certificate PKCS#10 request in Notepad and edit the request by eliminating the space in each line. Save the output and submit the edited version to the Verisign CA server for certificate generation.

9. Known Limitations:

When QOS Classifiers are configured on GUI page (QOS->Classifiers) or using CLI Commands "qos mf-class XXX":

1. A classifier or rule name containing the “?” character cannot be configured using the CLI; it must be configured from the GUI.
2. The backslash cannot be used as part of a classifier or rule name.
3. If you create a rule or classifier name, the “show running config” command will display the rule or name within double quotes.

10. Documentation Corrections

None

For known issues, please refer to the product release notes and technical documentation available from the Avaya Technical Support web site at: http://www.avaya.com/support.