

Business Policy Switch (BPS) Increases Security Capability with Software Version 2.5 – Now Available

Introduction

This bulletin announces the availability of Business Policy Switch software v2.5. This software version includes two new features described in the main topic section. The software is available for free download from the web; the instructions to download it are explained in the Ordering Guidelines and Procedures section.

Main Topic

Secure Shell Access

Secure Shell (SSH) Access is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. Basically, it's an internet protocol that allows a user to connect to a remote host via an encrypted link. It provides strong authentication and secure communications over unsecured channels. It provides an encrypted terminal session with strong authentication of both the server and client, using public-key cryptography. It is intended as a replacement for telnet, rlogin (remote login), rsh (remote shell), and rcp (remote copy).

SSH in the BPS protects against:

- IP spoofing, where a remote host sends out packets which pretend to come from another, trusted host
- IP source routing, where a host can pretend that an IP packet comes from another, trusted host
- DNS spoofing, where an attacker forges name server records
- Interception of clear text passwords and other data by intermediate hosts

SSH will be used to replace telnet and provide a secure access to user console menu and CLI interface. There are two distinct versions of SSH protocols (SSH version 1 and SSH version 2):

- SSH1 and SSH2 encrypt different parts of the packet.
- SSH2 does not use the same network implementation as SSH1.
- SSH2 uses a different key exchange protocol.
- MAC calculation of SSH2 is more secure.

Business Policy Switch will support only SSH2 because:

- It is the most popular version on the market and all major client software supports it.

SSH2 is a protocol for secure remote login and other secure network services over an insecure network. It consists of three major components:

1. The Transport Layer Protocol [SSH-TRANS] provides server authentication, confidentiality, and integrity. It may optionally also provide compression. The

transport layer will typically be run over a TCP/IP connection, but might also be used on top of any other reliable data stream.

2. The User Authentication Protocol [SSH-USERAUTH] authenticates the client-side user to the server. It runs over the transport layer protocol.
3. The Connection Protocol [SSH-CONNECT] multiplexes the encrypted tunnel into several logical channels. It runs over the user authentication protocol.

Features:

1. The SSH implementation supports both password and DSA public key authentication.
2. 3DES are supported for symmetric key exchange and data encryption.
3. The Diffie-Hellman algorithm is implemented for SSH2 key exchange.
4. SSH server provides user interface to allow DSA public key being managed by user.
5. Secure Shell can be configured through CLI interface, Web interface and SNMP interface. The management objects are:
 1. SSH enable/disable.
When SSH is enabled, it can chose to disable other non-secured interfaced. This is so called SSH secured mode. Otherwise is SSH in unsecured mode.
 2. DSA authentication enable or disable
SSH server (which is running in BayStack) can be configured to allow or disallow the DSA authentication. Other authentication method BayStack SSH supports is password authentication.
 3. Password authentication enable or disable
If there is none authentication enabled, user will not be allowed to make any connection.
 4. DSA public key upload/download.
 5. SSH information dump – shows all the SSH related information
 6. Max SSH session allowed is 2.
This will limit the number of SSH session user can open simultaneously.

Note: Due to export control restrictions, two images must be produced: one with SSH and without SSH. The image with SSH will have its console menus disabled.

Per VLAN tagging on egress

Some customers would like to have more control on VLAN tagging. Specifically, they need such a feature that a port can transmit frames tagged on some VLANs, and untagged on other VLANs. A port on the BPS currently has two tagging modes: tagged or untagged. If it is tagged, outgoing frames in all VLANs will be transmitted tagged from this port; if it is untagged, outgoing frames in all VLANs will be transmitted untagged. There are some exceptions to this rule; for example, BPDUs for Spanning Tree Group 1 are always transmitted untagged.

QoS Enhancements to permit use of all 24 global filters

Past releases allowed only 14 Layer 2 global filter definitions. Version 2.5 will allow users to specify up to 24 Layer 2 global filters and install them as policies. Also,

References and Related Documents

Release Notes Download

The Release Notes for v2.5 are available for download from the web by visiting:

www.nortelnetworks.com

Click on **Support**.

Click on **Business Series**.

Click on **Documentation** under **Business Series Portfolio: Business Policy Switch**.

Download the Release Notes.

Ordering Guidelines and Procedures

Software Download

Version 2.5 software release is available now and can be downloaded from the web by visiting:

www.nortelnetworks.com

Click on **Support**.

Click on **Business Series**.

Click on **Software** under **Business Series Portfolio: Business Policy Switch**.

Download the agent code.

It is also recommended that you download the updated version of the diagnostic code.

For more information, please contact your Nortel Networks account representative.

Nortel Networks, the Nortel Networks logo, and BayStack are trademarks of Nortel Networks. All other trademarks are property of their respective owners. Information subject to change. Product capabilities and availability dates described in this document pertain solely to Nortel Networks marketing activities in the United States and Canada.

© 2003 Nortel Networks Inc. ALL RIGHTS RESERVED.