



BorderWare Firewall Server

Roadmap for BorderWare Firewall Server
V6.5, BWClient and the IPSec VPN Option

Version 1.0
August 8th 2001

Introduction

Version 6.5 of the Firewall Server is nearing completion and a beta release is planned for August/September 2001. This updated road map details the new features in V6.5 and maps out the enhancements planned after this release.

The Feature Packs released for Version 6.1.2 have proved very successful, so the same mechanism will be used to deliver enhancements after the release of Version 6.5.

This roadmap includes planned release dates for Feature Packs and version upgrades. These dates are based on our current development plans and on our best estimates of the length of time required to implement and thoroughly test each of the documented features. It does not represent a firm commitment by BorderWare Technologies Inc to a release date. As always, we will endeavour to meet the published schedule and will of course update this document should there be any significant changes. BorderWare Technologies reserves the right to change the release schedule and the contents of any of the planned updates.

Comments about this roadmap may be sent to feedback@borderware.com

V6.5 New Features

Version 6.5 of the BorderWare Firewall Server will include all the new features released in Feature Packs A and B for V6.1.2 plus the following additional features.

Operating System Upgrade

The underlying operating system will be upgraded to FreeBSD 4.2. This will provide numerous security and performance enhancements.

Additional Hardware Support

Support will be added for newer hardware technologies including a number of new network cards and ATA-66 disk controllers. Some specific platforms that will now be supported include the Compaq DL320 and DL360 rack mount servers.

RAID support

Various disk array controllers are now fully supported, including the integrated SmartArray controller available on the Compaq DL360 server.

Buffer and Stack Overflow Protection

Many known vulnerabilities rely on exploiting stack and buffer overflows. These occur as a result of software code that does not properly check the size of its input

data. The result is that the data overwrites memory used by another part of the application.

Stack and buffer overflows are a particular problem in network application servers as by sending carefully formatted data, an attacker can force a target application server to execute arbitrary code and may be able to take control of that system.

The S-Core operating system and the BorderWare Firewall Server have been carefully designed and tested to avoid buffer overflows, and any known vulnerabilities have been eliminated. However it is always possible that new buffer overflow vulnerabilities may be discovered in the future.

In V6.5 an additional level of buffer overflow protection has been added. Critical modules, including the full set of application servers, have been re-built using compiler technology that traps buffer and stack overflows and immediately terminates execution. This means that if in the future buffer and stack overflow vulnerabilities are discovered in any of the application servers or other modules used by the Firewall, then protection will be in place to prevent the vulnerability being exploited. This represents a major competitive advantage for the Firewall and all of BTI's S-Core based products.

Additional Network Interfaces

V6.5 will support up to 6 network interfaces. The first three interfaces correspond to the existing External, Internal, and SSN interfaces. The additional interfaces are called Auxiliary interfaces, and are named AUX1, AUX2, and AUX3. They will operate exactly like the current SSN interface: proxies may be defined to and from the External and Internal network and all interfaces will have access to the internal DNS. Initially, it will not be possible to define proxies between pairs of SSN/AUX interfaces.

Import/Export of Cryptocard Programming details

Many BorderWare partners offer an outsourced Firewall Management Service. These partners currently need to use a separate Cryptocard (or other authentication token) for each Firewall that they manage via BWClient.

To address this inconvenience, V6.5 will allow the Cryptocard programming details to be transferred between Firewalls, making it possible for organisations offering outsourced management to use a single Cryptocard (or set of Cryptocards) for BWClient authentication.

Remote Installation of Patches

V6.5 will allow patches and service packs to be installed remotely using BWClient. (A system reboot will still be necessary).

Office Gateway Replaced with New 10-User Firewall License

The Office Gateway license will be replaced with a new 10-User Firewall license. The current restriction that limits the Office Gateway to two interfaces will be lifted. There will be no price changes and end-users with a current Office Gateway Support contract will receive a new 10-User Firewall License.

Graphical Console Support

The graphical console introduced on the Document Gateway and Mail Gateway products will be added to V6.5.

Bug Fixes and Minor Enhancements

A large number of minor bug fixes and enhancements have been made to the product.

V6.5 Migration

Migrating from existing 6.x releases will be straightforward: V6.5 will be able to restore configuration files generated from release 6.0.2 and higher, including the XML backup format available with 6.1.2 [B].

V6.5 Feature Pack A

Feature Pack A for BorderWare Firewall Server V6.5 is scheduled for release in December 2001, and will include the following capabilities:

High Availability for 2 Parallel Firewalls

The new high-availability feature will allow two firewalls to be connected in parallel to provide a redundant connection. This feature will be implemented using an enhanced version of the VRRP protocol.

In the case of a failure of the primary firewall, the secondary firewall will automatically assume the primary role, allowing connections passing through the Firewall to be quickly re-established with no manual intervention. Both firewalls will need to be properly licensed (the existing cold-standby serial number cannot be used). More details will be provided on this feature as development progresses.

Access Rules in SMTP Server

This feature will permit the definition of access rules for the SMTP Servers on the Internal, External and SSN/AUX interfaces. These access rules may be used to ensure that outbound e-mail may be sent via a Mail Filtering product only or to reject inbound messages from a known source.

Support for SmartFilter V3.0

V3.0 is the latest version of SmartFilter incorporating many new features. Feature Pack A will update the SmartFilter option offered with the BorderWare Firewall Server to V3.0.

Support for Oracle 8i¹

The Oracle*SQLnet proxy included in the BorderWare Firewall Server currently does not support Oracle 8i. Feature Pack A will enable support for this version of Oracle.

Patch Management

Feature Pack A will improve the management of patches by permitting the simultaneous application of multiple patches.

V6.5 Feature Pack B

Feature Pack B is scheduled for release in Q2/Q3 2002.

Improved facilities for handling disk failure.

The BorderWare Firewall Server currently does not allow the system to boot if an unrecoverable disk error is found. This is a deliberate design decision to guard against the possibility of system operating with corrupt application files or configuration inconsistencies that could result in serious security failures. Disk failures of this kind can be caused by hardware problems or by transient power spikes or power supply failures. The problem manifests itself when the Firewall fails to boot and displays the message, "Please run fsck manually".

Currently, manually running fsck is not permitted. Feature Pack B will prompt the administrator (via the console) to confirm if manual fsck should be run. If this option is chosen and if the system then successfully boots, a permanent warning will be displayed on the console indicating that the system is in an unknown state

¹ The availability of this feature is dependent on satisfactory completion of functional and security tests on a Toolkit provided by Oracle Corporation

and should be re-installed as soon as possible. This new feature is designed only to allow dynamic data such as queued e-mail to be recovered and is not intended to enable continued normal operation.

New “bundled” proxy for setting up NT Trust Relationships

Users frequently need to set up NT Trust relationships through the Firewall (e.g. to enable a system on the SSN to connect to an Internal NT server). This requires the definition of a number of TCP and UDP user-defined proxies. The new NT Trust proxy will combine these into a single system-defined proxy.

Built-in Load Balancing for dual parallel Firewalls

This feature enhances the built-in redundancy feature introduced in V6.5 Feature Pack A to allow dynamic load balancing between dual parallel Firewalls.

Extended support for DNS CNAMEs (Aliases)

The Internal and External Domain Name servers currently allow CNAMEs (Aliases) to be defined within a domain, so for example www.borderware.com may be aliased to gateway.borderware.com, but it is not possible to alias www.borderware.dk to www.borderware.com. This enhancement removes that restriction.

Alarms generate SNMP Traps

As an enhancement to the SNMP support introduced in V6.1.2 Feature Pack B, Alarms will now be able to trigger SNMP traps in addition to the current alerting mechanism of logging, generating a console alert and sending an e-mail.

PPPOE Support

The Firewall server currently supports DHCP for dynamic allocation of the external IP address. This feature was added to simplify use of the Firewall on Cable Modem, DSL and other low-cost Internet links where static IP addresses are not available. Many ISPs use PPPoE (Point-to-Point Protocol over Ethernet) as an alternative to DHCP. Adding this support will enable dynamic allocation of the external IP address using PPPoE and will simplify connection to ISPs that do not offer DHCP.

Firewall Future Plans

Detailed plans for Firewall development after Version 6.5 have yet to be finalised, but these plans will include enabling more flexible use of the additional interfaces introduced in V6.5 and enabling traffic flow between pairs of SSN/AUX interfaces.

BWClient Enhancements

A number of enhancements to BWClient are planned; the first (V1.6) which will allow management of a V6.5 Firewall with more than 3 interfaces will be available to support the release of V6.5. Further planned releases include BWClient V2.0 (planned for December 2001) and V2.1 planned for Q1 2002.

BWClient V1.6

Firewall Management

BWClient V1.6 will include the ability to manage a V6.5 Firewall configured with up to 6 interfaces and will be required to manage a V6.5 Firewall.

BWClient V2.0

Firewall Monitoring

BWClient will be enhanced to include a Firewall monitoring option, this will utilise the SNMP support added in V6.1.2 Feature Pack B.

Improved Ability to Manage Multiple Firewalls

BWClient can currently support the simultaneous management of multiple Firewalls, each Firewall is displayed in a separate window. This enhancement will introduce a new top-level in the BWClient menu tree. The top level menu items will display the list of Firewalls that the administrator is authorised to manage. Each Firewall will then have its own menu hierarchy to configure DNS, Servers, Proxies etc.

BWClient V2.1

New VPN Wizard

The VPN wizard will automate the process of setting up a server-server VPN between two Firewalls managed by a single instance of BWClient. To use the Wizard, users will simply select any two Firewalls appearing in the new BWClient Firewall Menu (new in V2.0) and confirm which interfaces are to participate in the VPN. The Wizard will then handle all the details of configuring the VPN link.

Distributed Policy Management

In addition to managing multiple Firewalls, BWClient will be enhanced to enable the creation of policies which can be applied to a group of Firewalls.

Tiered Administration

This enhancement will enable administrators to be assigned different rights, so a local administrator will be able to carry out routine administration of the Firewall but will be blocked from over-riding policy defined by a central administrator.

IPSec Enhancements

A number of significant enhancements are planned to the Firewall's IPSec VPN Server option. These include full support for PKI (Public Key Infrastructure) as a mechanism for identifying and authenticating VPN peers (both IPSec clients and other Firewalls running the server option). PKI support will considerably simplify the deployment of VPNs. The latest VPN Client (V6.0.0) already includes the PKI facilities required to the planned enhancements, so development will focus on the IPSec server option. Two releases are planned, V3.0 scheduled for November 2001 and V3.1 scheduled for Q1/Q2 2002. Further information on BTI's plans for PKI support is available in the white paper *Managing VPNs with PKI*.

IPSec Version 3.0

Wider choice of encryption algorithms.

Blowfish (key length up to 448 bits) and Rijndael the new AES algorithm will be added. Rijndael supports key lengths of 128, 192 or 256 bits.

Additional Password Required for IPSec Client Authentication

An enhancement to the IPSec server option will enable a Client-Server VPN connection to be configured so that an additional password is needed in order to establish a security association. This password will be configured and maintained on the server. This feature provides additional security when IPSec is used to secure connections from mobile users and guards against the risk associated with loss or theft of laptops.

PKI Authentication of Client-Server and Server-Server VPN

The Firewall will be able to import a certificate generated by most popular CA products such as Entrust, Verisign and Baltimore. This will enable certificates

signed by the CA to be used to identify and authenticate connecting IPSec clients and other BorderWare Firewalls running the IPSec server option.

IPSec Version 3.1

Extended Authentication for IPSec Client Connections

This enhancement will enable IPSec client connections to be configured to require strong authentication (e.g. SecureID) before the security association is established. The authentication settings will be configured and managed on the Firewall.

Certificate Authority in Firewall Server

IPSec V3.1 will enable the Firewall Server to run a certificate authority. The Firewall hosted CA will be capable of signing certificates generated locally, by other Firewalls and by BTI's IPSec client. This facility will enable users to set up and use PKI services for managing complex VPNs without incurring the cost of a commercial CA product.