

Technical Requirements

Recommended Hardware Specifications (min.) & Supported Operating Systems

Windows NT Platform - (NT 4.0)

Pentium II 300MHz, 64MB of RAM (Min.), 4GB HDD

Windows 2000 - Coming Soon

Sun Solaris Platform - Solaris 2.6 (2.7 Coming Q4)

Sun SPARC or UltraSparc
sbus or PCI bus
128MB RAM

HP- UX UNIX Platform

HP 9000, A, D & R class servers, 128MB RAM

Tru64 UNIX Platform

Alpha Processor, 256MB RAM, 8GB HDD

With AXENT's exclusive *Smart Security Architecture* product direction, our goal is to implement integrated security solutions. With common repositories and administrative and monitoring consoles, AXENT enables you to configure the 'right' level of trusted e-security for your business.

Raptor Firewall integrates with other AXENT products including:

- PowerVPN®
- Intruder Alert™
- NetRecon™
- NetProwler™

Corporate Headquarters

2400 Research Blvd.
Rockville, MD 20850
301-258-5043
301-330-5756 (fax)
info@axent.com

International Headquarters

Apex House
4A-10 West Street
Epsom, Surrey KT18 7RG
United Kingdom
44-1372-729655
44-1372-749965 (fax)

1-888-44-AXENT

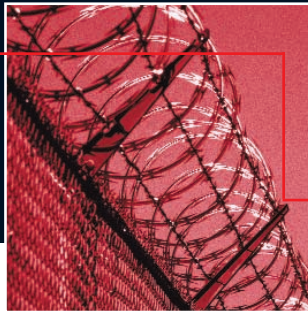
www.axent.com

About AXENT

AXENT Technologies, Inc., a global leader in information security, provides e-security solutions that maximize its customers' business advantage. AXENT delivers integrated products and expert services to assess, protect, enable and manage business processes and information assets, as well as to facilitate trust level management within its customers' environments. Through its unique Lifecycle Security™ Methodology, combined with *Smart Security Architecture*, AXENT delivers the 'right' level of trusted e-security for customers. Award-winning solutions offer assessment and policy compliance, firewall, intrusion detection, authentication and authorization technology, virtual private networking, Web access and single sign-on for enterprises and e-businesses.

©2000 AXENT Technologies, Inc. All rights reserved. AXENT, AXENT Technologies, the AXENT logo, Lifecycle Security, Raptor, Raptor Firewall, PowerVPN and Defender are trademarks or registered trademarks of AXENT Technologies, Inc., and its subsidiaries in the U.S.A. and certain other countries. Windows and Windows NT are trademarks or registered trademarks of Microsoft Corporation. Names of other products and trademarks mentioned are property of their respective holders. Printed in the U.S.A.





RAPTOR FIREWALL

PERIMETER SECURITY WITH UNCOMPROMISED PERFORMANCE

Overview

Organizations embracing new business models to leverage the Internet are connecting customers, partners and suppliers to IT resources in order to conduct e-commerce and e-business. This new electronic environment affords organizations with new opportunities, but not without its associated risks and responsibilities to safeguard corporate assets. The Raptor® Firewall provides the industry's maximum perimeter security solution without compromising network performance. It is the strongest protection against unwanted intrusion, while allowing approved business traffic to traverse the enterprise network.

Product Description

AXENT's Raptor Firewall provides the required protection for the enterprise, including the corporate/Internet perimeter interface, the corporate Intranets, the private subnets and branch offices. Its award-winning architecture and functionality combine to secure organizations' networks, delivering full-featured security and ensuring complete control of information entering and leaving the corporate network. The Raptor Firewall employs application level proxies to validate information at all levels of the protocol stack.

Developed for Windows NT®, Tru64™, UNIX®, Solaris®, and HP-UX® platforms, the Raptor Firewall provides complete protection by integrating application level proxies, network circuits and packet filtering into its unique architecture. More than just protocol protection, the Raptor Firewall also contains intuitive management, high-performance characteristics and multi-threaded services which work together, establishing it as the most secure, manageable and flexible solution for enterprise protection needs.

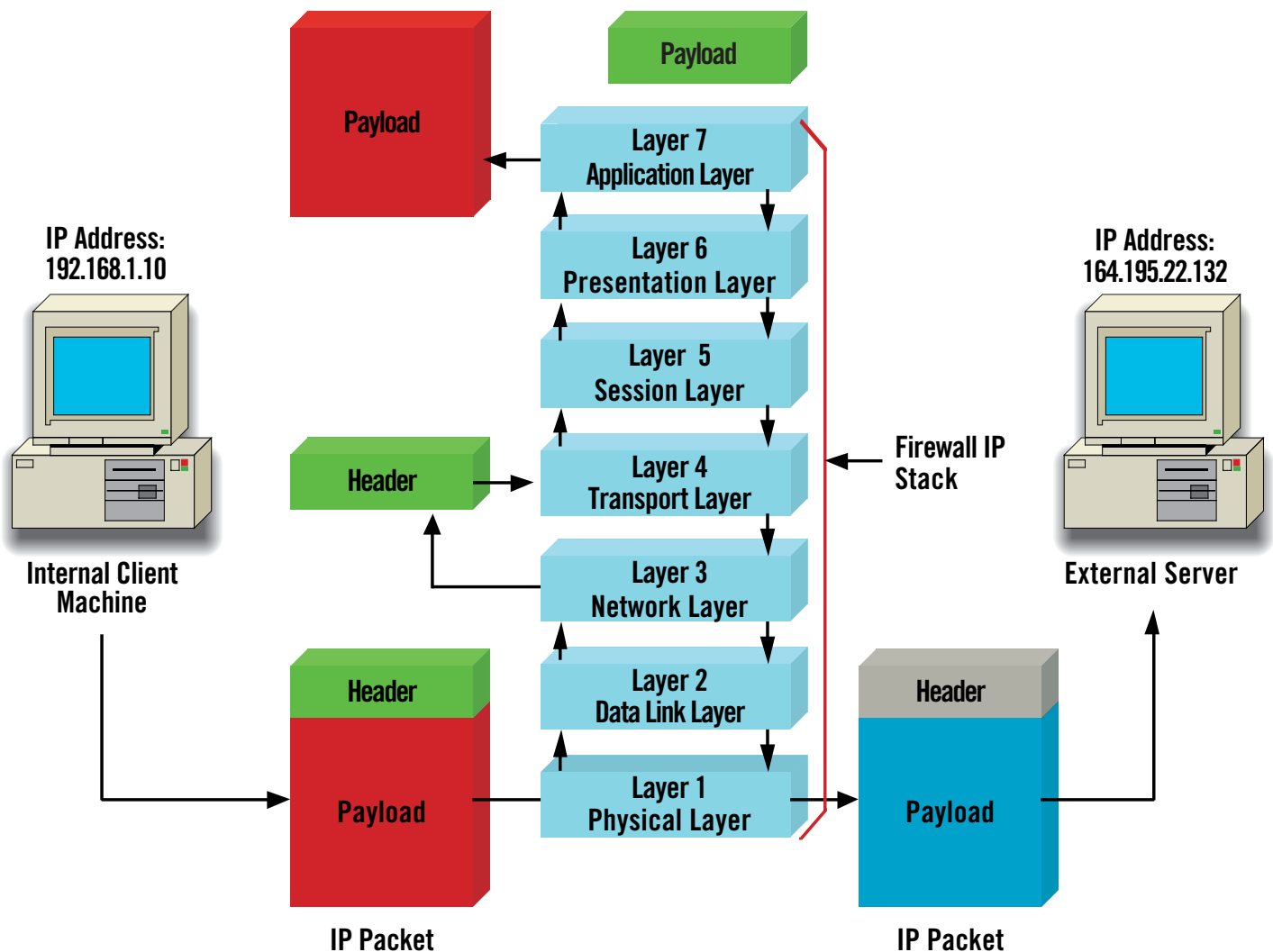
HIGHLIGHTS

- Delivers easy management of local and remote firewalls with the Raptor Management Console (RMC)
- AXENT's ProxySecured PowerVPN Server Upgrade integrates seamlessly with the Raptor Firewall to securely connect to remote offices and users
- Offers a comprehensive selection of strong user authentication alternatives, providing the flexibility to choose depending on the repository that already exists
- Enables firewall-integrated content blockers for filtering WWW and Internet Usenet groups
- Provides High Availability and Load Balancing with the use of Radware hardware "Fireproof" or High Availability with the use of Microsoft Cluster Server software (for Windows NT) and Veritas software (for Solaris)
- Delivers comprehensive architecture for Security Policy Management, allowing administrators to create rules in any order without inadvertently creating security holes
- Possesses extensive Logging and Reporting Capabilities to enable the generation of detailed statistical and session trend reports or custom analyses
- Meets stringent interoperability requirements among products of different vendors and is ICSA certified
- Extends enterprise networks with encryption and authentication

Technical Features

- **Application Proxy Technology** –The diagram below illustrates the packet flow through the Raptor Firewall. It shows packets entering the TCP/IP Stack of the device on the left-hand side. Various scanning techniques are then applied via the seven layers of the protocol (TCP/IP) stack and completed. After all tests are completed, if there are no problems, the packets are allowed to flow out of the firewall to the next network segment.
- **Centralized Management** – The Raptor Management Console (RMC) simplifies policy configuration and management by implementing Microsoft's Management Console (MMC) technology.

The Raptor Firewall utilizes the Microsoft Management Console for administration under Windows NT platforms. A specific Raptor Management Console (RMC) "snap in" allows the administrator to install the RMC on as many machines as desired. The security device can be configured for management from selected machines. The RMC allows for centralized management, connecting to multiple security devices simultaneously. For UNIX operating systems, management is performed via the use of a native UNIX GUI. Additionally, command line tools allow the user to log in remotely and securely to the security device and display current sessions.



- **ProxySecured PowerVPN Server Upgrade Integration** – Standards-based PowerVPN® Server (IPSec, X.509, LDAP, Triple DES encryption) allows connection to remote offices and users securely.
- **User Authentication** – Offers comprehensive selection of strong user authentication alternatives (i.e. NT Domain, Radius, etc.) and provides the flexibility to choose, depending on the repository already existing in the user's environment. The Raptor Firewall supports many different authentication schemes, including:
 - ❑ OOBA (Out of Band Authentication) - Allows the administrator to set up authentication schemes for any protocol required to pass through the firewall. OOBA is performed using the browser to open a channel for the client to access the required server.
 - ❑ Windows NT Domain - The Raptor Firewall can authenticate users based on their domain credentials.
 - ❑ AXENT Defender™ (either hard or soft token), LDAP (Lightweight Directory Access Protocol), BellCore Skey, Gateway Password, CryptoCard or SecureID.
 - ❑ Two authentication protocols also supported are TACAS and Radius®.
- **Content Blockers, WebNOT and NewsNOT** - The Raptor Firewall utilizes URL filtering technology to filter out access to objectionable Web sites. The administrator can set various rules for certain users to limit or restrict access to sites that contain nudity, violence, etc. This content blocking can also be applied to news groups. Additionally, this URL filtering technology is customizable to administrator preferences. WebNOT™ and NewsNOT™ are the only firewall-integrated content blockers for filtering WWW and Internet Usenet groups.
- **High Availability and Load Balancing** – The choice is yours – Veritas FirstWatch (for Solaris) or Microsoft Cluster Server (for NT) or MCS Service Guard (for HP-UX) software-enabled high availability, enabling system failover for maximum security uptime and productivity or Radware hardware-enabled firewall high availability and load balancing. Additionally, utilizing Radware's hardware "Fireproof" will load balance the Raptor Firewall, providing the user the ability to share traffic loads among multiple security devices.
- **Security Policy Management** – This unique architecture allows the administrator to build network policies that are consistent with corporate policies. And with its unique, best-fit algorithm for matching access rules to connection attempts, the administrator can create rules in any order without inadvertently creating security holes. The Raptor Firewall contains configurable items for both users and user groups. As users become members of specific user groups, they will immediately inherit the policies that apply to that specific user group. Some examples of policies include (1) access to certain servers, (2) access to certain file shares and (3) access limited to certain time schemes, etc.
- **Logging and Reporting** – Raptor Firewall log files contain information such as session duration, byte counts, full URLs, user names and authentication methods that can be used to generate detailed statistical and session trend reports. An ASCII log file is dynamically represented in the RMC, giving the administrator the opportunity to view the log in real time. Log files are rotated each 24-hour period (configurable) and can be imported to other reporting products, such as Telemate.Net (for graphical illustration of network usage).
- **ICSA Certification** – Meets stringent interoperability requirements among products of different vendors. ICSA uses the Raptor Firewall as a reference product for all other product certification testing.
- **Network Address Translation** – The Raptor Firewall contains specific NAT (Network Address Translation) features that allow the administrator to create access lists so that requests leaving or entering the secured network appear to originate at predetermined addresses, rather than the address of the security device. The administrator can choose the address to be the internal client machine (if routable addresses are chosen for the internal network) or the real address can be that of the server (if located on the Internet), or the address can be just an extra address that belongs to the organization's official IP range.
- **Wizards** – The Raptor Firewall contains many new wizards to aid the security administrator in the completion of cumbersome and complicated installation and configuration tasks.