

Information Technology Resource Management Council (ITRMC)

ENTERPRISE STANDARDS – S3000 NETWORK AND TELECOMMUNICATIONS

Category: S3200 – SECURITY – FIREWALL

CONTENTS:

- I. [Definition](#)
- II. [Rationale](#)
- III. [Approved Standard\(s\)](#)
- IV. [Approved Product\(s\)](#)
- V. [Justification](#)
- VI. [Technical and Implementation Considerations](#)
- VII. [Emerging Trends and Architectural Directions](#)
- VIII. [Review Cycle](#)
- IX. [Time Line](#)
- X. [Revision History](#)

I. DEFINITION

A firewall is a system of server hardware and software that monitors data passing between two networks and uses an access control policy to make decisions about what data is shared between the two networks. Firewall services provide the ability to determine who can access resources on a network based upon these policies. It also provides monitoring and auditing of network traffic.

II. RATIONALE

Use of LAN/WAN networking has increased the opportunity for foreign access within the network, as well as unapproved use of networking resources by internal staff. A coordinated firewall approach is necessary to monitor, track, and restrict access to portions of the network. In addition, any firewall solution must have an architecture that permits a variety of authentication solutions to be implemented within the enterprise-side security policy, including passwords, smart cards, token-based products, directory services (LDAP, etc.), remote access services, and X.509 digital certificates.

III. APPROVED STANDARD(S)

Internet Protocol (IP)

IV. APPROVED PRODUCTS(S)

1. Check Point Firewall-1; and

2. Cisco Firewall Products (PIX, Blades, IOS, and Security Router Bundles).

V. JUSTIFICATION

Check Point's Firewall-1 and Cisco's Firewall products are recognized as industry leader in firewall solutions. Through this standard, the State is able to achieve a stronger level of security by providing various product options which allow for enhanced integration of firewall technologies into the State's network infrastructure. By maintaining a set of defined products, the State can continue to leverage its buying power and position itself for the future possibility of an enterprise security architecture and shared infrastructure.

VI. TECHNICAL AND IMPLEMENTATION CONSIDERATIONS

The deployment, configuration and management of a firewall is a complex task requiring skilled resources. Agencies should ensure the appropriate skill sets are available to implement and maintain a firewall system.

The Department of Administration provides centralized firewall management services to any interested agency. Due to limited resources, this service is only provided for Check Point Firewall-1 Products. Any agency deploying or maintaining a Cisco Firewall product will assume all responsibility and costs for such systems.

VII. EMERGING TRENDS AND ARCHITECTURAL DIRECTIONS

The industry is evolving towards a layered "defense in depth" approach to the firewall architecture. Desktop, remote PC, laptop, and local office/agency firewalls are a few of the components being more broadly implemented as part of enterprise security systems.

VIII. REVIEW CYCLE

Six (6) Months

IX. TIME LINE

Last Reviewed: March 7, 2007
Last Revised: April 25, 2005
Effective Date: October 2, 2001

X. REVISION HISTORY

4/25/05 - Added Cisco Firewall products.