

Information Technology Resource Management Council (ITRMC)

ENTERPRISE STANDARDS S3000 – NETWORK AND TELECOMMUNICATIONS

Category: S3220 – SECURITY – VIRTUAL PRIVATE NETWORK

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. [Procedural Reference](#)
- IX. [Review Cycle](#)
- X. [Time Line](#)
- XI. [Revision History](#)

I. DEFINITION

A Virtual Private Network (VPN) is a set of hardware, software, and procedures that create a secure logical network. VPNs provide functions such as access control, authentication, tunneling, and encryption and are often implemented in Intranet, Extranet, or Secure Remote Access applications.

II. RATIONALE

There are many business requirements that justify providing logical access to network resources, independent of physical topology or location. A VPN implementation can be used to fulfill these business requirements while maintaining security standards. Any VPN solution must have an architecture that can be implemented within the enterprise security policy, including passwords, smart cards, token-based products, directory systems (LDAP, etc.), remote access services, and X.509 digital certificates.

III. APPROVED STANDARD(S)

1. Internet Protocol (IP);
2. IP Security Protocol (IPSec); and,
3. Secure Sockets Layer (SSL).

IV. APPROVED PRODUCT(S)

1. Check Point VPN-1;
2. Check Point VPN-1 SecureClient;
3. Cisco VPN Products (VPN 3000 Family, IOS, Adaptive Security Appliances, and Security Router Bundles); and,
4. F5 FirePass SSL VPN.

V. JUSTIFICATION

Check Point, Cisco, and F5 are recognized as industry leaders in VPN products and solutions. Significant technical expertise is available within the State to support these products.

VI. TECHNICAL AND IMPLEMENTATION CONSIDERATIONS

The deployment, configuration and management of a VPN service is a complex task requiring skilled resources. IPSec VPN solutions are best used to secure site-to-site connections over an untrusted network. IPSec VPNs are also frequently used to provide secure, remote access to managed workstations that require persistent connections to the state's network. Interoperability of IPSec VPNs between various vendors can be challenging or non-existent; however, interoperability between Check Point and Cisco VPN products has been proven and is available for site-to-site IPSec VPN architectures. IPSec VPN client software is typically not compatible between vendors.

SSL VPN solutions can provide more flexible, remote access for mobile employees, extranet partners, and telecommuters. SSL VPNs leverage the remote user's web browser, easing the IT management burden typically encountered with IPSec VPN client software. Since SSL VPNs are typically used with unmanaged systems (e.g. home systems, kiosks, conference systems, etc), extreme care must be taken to ensure end point security of these remote systems is sufficient. As agencies evaluate options for new (or to replace existing) remote access technologies, they should first consider SSL VPN solutions due to simplified administration and provisioning of user accounts, as well as a less complicated user experience.

The Department of Administration provides centralized VPN management services to any interested agency. Due to limited resources, this service is only provided for Check Point VPN-1 products. Any agency deploying or maintaining a Cisco or F5 VPN product will assume all responsibility and costs for such systems.

VII. EMERGING TRENDS AND ARCHITECTURAL DIRECTIONS

SSL VPN solutions will continue to grow in popularity and will replace many IPSec VPN deployments for secure, remote user access. However, IPSec VPNs will continue to be used as the de facto protocol for secure, site-to-site communications.

VIII. PROCEDURAL REFERENCE

VPN solutions used on the State of Idaho's Wide Area Network must comply with the Department of Administration's "VPN Connectivity and Management Policy."

IX. REVIEW CYCLE

Six (6) Months

X. TIME LINE

Last Reviewed: October 10, 2007

Last Revised: March 7, 2007

Effective Date: October 2, 2001

XI. REVISION HISTORY

3/7/07 – Added additional considerations regarding new or replacement remote access solutions.

9/13/06 – Added SSL as an approved standard. Added F5 FirePass as an approved SSL product. Updated technical considerations and procedural reference.

4/25/05 – Added Cisco VPN products.

8/25/04 – Acknowledged emerging trend of SSL-based VPNs.