

Project Specification

Analysis of VPN Protocols

Version 2.0
Touhid Satiar
Tamer Mabrouk

1. VPN protocols to be evaluated:

- a. IPSec
- b. PPTP
- c. L2TP
- d. L2F
- e. MPLS

2. Description of Problem:

The objective of this project is to describe a framework for Virtual Private Networks (VPN's), compare and contrast various VPN protocols, their respective requirements, and the process specific attributes that encompasses each.

3. Tentative topics of comparison

We hope to discuss the following comparison topics in the course of this project:

- a. Security Issues
 - i. Authentication
 - ii. Encryption
 - iii. Digital Signature
 - iv. Key management
 - v. Vulnerability
- b. Deployment considerations
 - i. Cost
 - ii. Availability of protocol
 - iii. Vendors
- c. Flexibility
 - i. Scalability
 - ii. Compatibility
- d. Performance
 - i. Speed vs. Security
 - ii. Security overhead
- e. IP Service Capability
 - i. Dynamic tunnel IP address assignment
 - ii. IP multicast support
 - iii. NAT capability
- f. Multi-protocol Support

4. Procedure of Verification:

The research in this project will be verified by:

- a. RFC's
- b. White papers
- c. Industry recognized vendor technical documents
- d. Technical books

5a. Format of Final report:

IEEE Transaction and Journal Format.

5b) Tentative Table of Contents for Final report:

1. Introduction

2. Emergence of VPN

- a. Background of networking
- b. Inception of Virtual Private Network
- c. VPN Application

3. VPN Tunneling protocols

I) Concept of Tunnels in Virtual Private Network

II) Different types of Tunneling Protocols:

Customer Premise Equipment (CPE) based VPN

- a. IPsec
- b. Layer 2 Tunneling Protocol (L2TP)
- c. Point to point Tunneling Protocol (PPTP)
- d. Layer 2 forwarding Protocol (L2F)

Provider Provisioned VPN

- a. Multi protocol label switching VPN
- b. MPLS/BGP VPN

4. Comparison of Protocols:

- i. Security Issues
 1. Authentication
 2. Encryption
 3. Digital Signature
 4. Key management
 5. Vulnerability
- ii. Deployment considerations
 1. Cost

- 2. Availability of protocol
- 3. Vendors
- iii. Flexibility
 - 1. Scalability
 - 2. Compatibility
- iv. Performance
 - 1. Speed vs. Security
 - 2. Security overhead
- v. IP Service Capability
 - 1. Dynamic tunnel IP address assignment
 - 2. IP multicast support
 - 3. NAT capability
- vi. Multi-protocol Support

5. Future of VPN

6. Conclusion

7. References

6. Project Development timeline:

Date	Day	Project Goal
10/04/03	Saturday	Final Project Specification submit date
10/15/03	Wednesday	1st Progress Report: Introduction and finalized table of contents.
10/29/03	Wednesday	2nd Progress Report: Concepts of VPN and VPN tunneling
11/12/03	Wednesday	3rd Progress Report Comparison of Protocols and Future of VPN
12/03/03	Wednesday	Final Progress Report Draft version of the final Viewgraph presentation
12/06/03	Saturday	Project reports submit date.
12/12/03	Friday	Final Oran Presentation and Final Report submit date.

7. Possible areas where the Specification can be altered

- 1. Structural analysis of chosen VPN protocols

2. Emphasis on comparison criteria. Possible add or deletion of them.
3. New important and relevant topics might be added.

8. List of Literature

- i) S. Kent , R. Atkinson, "Security Architecture for the Internet Protocol", RFC : 2401, November 1998
- ii) S. Kent, R. Atkinson, " IP Authentication Header" , RFC: 2402, Nov, 1998.
- iii) W. Townsley, A. Valencia, " Layer Two Tunneling Protocol L2TP" RFC: 2661 . Aug 1999.
- iv) B. Gleason, A. Lin, " A Framework for IP Based Virtual Private Networks" RFC: 2764. Feb 2000.
- v) R K. Hamzeh, G. Pall, J. Taarud, W. Little; " Point-to-Point Tunneling Protocol (PPTP)" RFC: 2637; July 1999
- vi) VPNs: Virtually Anything?" White paper. Core Competance, Inc.,
- vii) <http://www.corecom.com/html/vpn.html>
- viii) Virtual Private Network Consortium, <http://www.vpnc.org>.
- ix) Smith, Richard, Internet Cryptography, Reading, MA: Addison-
- x) Wesley, 1997. ISBN 0201-92480-3.
- xi) www.Nortelnetwork.com
- xii) www.cisco.com
- xiii) www.microsoft.com
- xiv) www.intel.com