TABLE OF CONTENTS

I. INTRODUCTION

1.1 SSL VPNs: Three Common Denominators
1.2 SSL VPNs at Work
1.3 SSL vs. IPSec
1.4 Advantage: IPSec
1.5 A Brief History of SSL

II. TECHNOLOGY AND MARKET OVERVIEW

2.1 Sizing Up the Players
2.2 SSL VPN Gateway Form Factors: Size Does Matter

III. PRODUCT DETAILS

3.1 Modus Operandi
3.2 Secret Agents: Extending Application Access
3.3 Which Applications?
3.4 Securing Access to the Enterprise
3.5 No Secrets: The Benefits of URL Rewriting
3.6 Objects of Desire: File Systems and Access Control
3.7 Lower-Layer Access Control
3.8 Who Goes There? SSL VPNs and Authentication
3.9 Log Handling
3.10 Redundancy and High Availability
3.11 Management Methods
3.12 Service and Support

APPENDICES

A Test Results

I. Capacity Tests
II. Maximum Concurrent Users
III. Outlook Web Access
IV. The Waiting Game
V. OWA and DOS
VI. Forwarding Rates
VII. Security Assessment

B Lab Test Methodology

I. Executive Summary
II. The Test Bed
2.1 Test Considerations
   IP Configuration
   Username and Passwords

III. Test Procedures

3.1 SSL Setup/Teardown Rates
    Objective
    Configuration
    Procedure
    Metrics

3.2 Maximum Concurrent Users
    Objective
    Configuration
    Procedure
    Metrics

3.3 Outlook Web Access (OWA) Performance
    Objective
    Configuration
    Procedure
    Metrics

3.4 Outlook Web Access Performance While Under DDOS Attack (Optional)
    Objective
    Configuration
    Procedure
    Metrics

3.5 HTTP Goodput
    Objective
    Configuration
    Procedure
    Metrics

3.6 Security Assessment
    Objective
    Configuration
    Procedure
    Metrics

IV. Change History

B1 OWA LoginBox URL List
C OWA Performance Under Load
D Bibliography
E Author Biography
F Legal Disclaimer