

# **NETWORK SECURITY ARCHITECTURES**

Foreword.

Preface.

## **I. NETWORK SECURITY FOUNDATIONS.**

### **1. Network Security Axioms.**

Network Security Is a System. Business Priorities Must Come First. Network Security Promotes Good Network Design. Everything Is a Target. Everything Is a Weapon. Strive for Operational Simplicity. Good Network Security Is Predictable. Avoid Security Through Obscurity. Confidentiality and Security Are Not the Same. Summary. Reference. Applied Knowledge Questions.

### **2. Security Policy and Operations Life Cycle.**

You Can't Buy Network Security. What Is a Security Policy? Security System Development and Operations Overview. Summary. References. Applied Knowledge Questions.

### **3. Secure Networking Threats.**

The Attack Process. Attacker Types. Vulnerability Types. Attack Results. Attack Taxonomy. Summary. References. Applied Knowledge Questions.

### **4. Network Security Technologies.**

The Difficulties of Secure Networking. Security Technologies. Emerging Security Technologies. Summary. References. Applied Knowledge Questions.

## **II. DESIGNING SECURE NETWORKS.**

### **5. Device Hardening.**

Components of a Hardening Strategy. Network Devices. Host Operating Systems. Applications. Appliance-Based Network Services. Rogue Device Detection. Summary. References. Applied Knowledge Questions.

### **6. General Design Considerations.**

Physical Security Issues. Layer 2 Security Considerations. IP Addressing Design Considerations. ICMP Design Considerations. Routing Considerations. Transport Protocol Design Considerations. DoS Design Considerations. Summary. References. Applied Knowledge Questions.

### **7. Network Security Platform Options and Best Deployment Practices.**

Network Security Platform Options. Network Security Device Best Practices. Summary. Reference. Applied Knowledge Questions.

### **8. Common Application Design Considerations.**

E-Mail. DNS. HTTP/HTTPS. FTP. Instant Messaging. Application Evaluation. Summary. References. Applied Knowledge Questions.

### **9. Identity Design Considerations.**

Basic Foundation Identity Concepts. Types of Identity. Factors in Identity. Role of Identity in Secure Networking. Identity Technology Guidelines. Identity Deployment Recommendations. Summary. References. Applied Knowledge Questions.

### **10. IPsec VPN Design Considerations.**

VPN Basics. Types of IPsec VPNs. IPsec Modes of Operation and Security Options. Topology Considerations. Design Considerations. Site-to-Site Deployment Examples. IPsec Outsourcing. Summary. References. Applied Knowledge Questions.

**BUY ONLINE AT: <http://www.itgovernance.co.uk/products/722>**

### **11. Supporting-Technology Design Considerations.**

Content. Load Balancing. Wireless LANs. IP Telephony. Summary. References. Applied Knowledge Questions.

### **12. Designing Your Security System.**

Network Design Refresher. Security System Concepts. Impact of Network Security on the Entire Design. Ten Steps to Designing Your Security System. Summary. Applied Knowledge Questions.

## **III. SECURE NETWORK DESIGNS.**

### **13. Edge Security Design.**

What Is the Edge? Expected Threats. Threat Mitigation. Identity Considerations. Network Design Considerations. Small Network Edge Security Design. Medium Network Edge Security Design. High-End Resilient Edge Security Design. Provisions for E-Commerce and Extranet Design. Summary. References. Applied Knowledge Questions.

### **14. Campus Security Design.**

What Is the Campus? Campus Trust Model. Expected Threats. Threat Mitigation. Identity Considerations. Network Design Considerations. Small Network Campus Security Design. Medium Network Campus Security Design. High-End Resilient Campus Security Design. Summary. References. Applied Knowledge Questions.

### **15. Teleworker Security Design.**

Defining the Teleworker Environment. Expected Threats. Threat Mitigation. Identity Considerations. Network Design Considerations. Software-Based Teleworker Design. Hardware-Based Teleworker Design. Design Evaluations. Summary. Reference. Applied Knowledge Questions.

## **IV. NETWORK MANAGEMENT, CASE STUDIES, AND CONCLUSIONS.**

### **16. Secure Network Management and Network Security Management.**

Utopian Management Goals. Organizational Realities. Protocol Capabilities. Tool Capabilities. Secure Management Design Options. Network Security Management Best Practices. Summary. References. Applied Knowledge Questions.

### **17. Case Studies.**

Introduction. Real-World Applicability. Organization. NetGamesRUs.com. University of Insecurity. Black Helicopter Research Limited. Summary. Reference. Applied Knowledge Questions.

### **18. Conclusions.**

Introduction. Management Problems Will Continue. Security Will Become Computationally Less Expensive. Homogeneous and Heterogeneous Networks. Legislation Should Garner Serious Consideration. IP Version 6 Changes Things. Network Security Is a System. Summary. References.

Appendix A: Glossary of Terms.

Appendix B: Answers to Applied Knowledge Questions.

Chapters 1-16.

Appendix C: Sample Security Policies.

Index.

**BUY ONLINE AT:** <http://www.itgovernance.co.uk/products/722>