

1 - Encryption

Objectives

- Understand how the Firewall uses symmetric encryption
- Understand how the Firewall uses asymmetric encryption
- Understand the requirement for integrity & authenticity
- Understand the function of the Certificate Authority
- Understand the two phases of IKE
- Know the ports & protocol numbers used by IKE and IPSEC
- Understand the process of establishing a VPN tunnel

Prerequisites

- Complete all 'Check Point Essentials - Management 1' Modules
- VMWare Server or Workstation
- Virtual machines configured
- Base firewalls installed and under SmartCenter control

Approximate time for completing each section

Section 1	Securing Communications	30 minutes
Section 2	IKE and IPSec	40 minutes
	Total	1Hr 10 Min

Contents

1	Securing Communications	3
1.1	Symmetric Encryption	3
1.1.1	Encryption Key & Algorithms	3
1.1.2	Symmetric Key Problems	3
1.2	Asymmetric Encryption	4
1.2.1	Asymmetric Keys	4
1.2.2	Asymmetric Key Problems	4
1.3	Diffie-Hellman (DH)	5
1.3.1	DH Special Asymmetric Algorithm	5
1.4	Integrity and Authenticity	6
1.4.1	Integrity Using Hashing Algorithms – MD5/SHA-1	6
1.4.2	Sending a Message using MD5	7
1.4.3	Authenticity Using Digital Signatures - RSA	8
1.5	Certificate Authorities	8
1.5.1	Central & Distributed Authorities	8
1.5.2	Check Point Internal Certificate Authority - ICA	9
1.5.3	Certificate Revocation Lists - CRLs	10
2	IKE and IPSEC	11
2.1	ISAKMP/Oakley - IKE	11
2.1.1	IKE Phase 1	11
2.1.2	IKE Phase 2	11
2.1.3	Encryption & Authentication Algorithms	11
2.1.4	Perfect Forward Secrecy	12
2.1.5	'vpn debug' & IKEView	12
2.2	IPSec	14
2.2.1	Process of Building a VPN Tunnel	14
2.2.2	Encryption Mode - Tunnel or Transport	14
2.2.3	Encryption and Authentication (Packet Integrity)	15
2.2.4	Packet Integrity Problems & NAT	16