

CCSE Checkpoint



IT EDUCATION CENTRE

Upgrading

Taking backup of a Security Gateway and Management Server

Explain the differences between backups, snapshots,
& upgrade-exports.

Perform Upgrade and troubleshoot a Management Server
using a database migration.

Upgrade and troubleshoot a clustered Security Gateway deployment.

Backup and Restore Security Gateways and Management Servers

Managing Snapshots

Upgrade Tools

Backup Schedule Recommendations

Upgrade Tools

Performing Upgrades

Support Contract

Advanced Firewall

Check Point Firewall Infrastructure

GUI Clients

Management

Security Gateway

User and Kernel Mode Processes

CPC Core Process

FWM

FWD

CPWD

Inbound and Outbound Packet Flow

Inbound FW CTL Chain Modules

Outbound Chain Modules

Columns in a Chain

Stateful Inspection

Kernel Tables

Connections Table

Connections Table Format



IT EDUCATION CENTRE

Check Point Firewall Key Features

- Packet Inspection Flow
- Policy Installation Flow
- Policy Installation Process
- Policy Installation Process Flow

Network Address Translation

- How NAT Works
- Hide NAT Process
- Security Servers
- How a Security Server Works
- Basic Firewall Administration
- Common Commands

FW Monitor

- What is FW Monitor
- C2S Connections and S2C Packets fw monitor

Clustering and Acceleration

VRRP

- VRRP vs ClusterXL
- Monitored Circuit VRRP
- Troubleshooting VRRP

Clustering and Acceleration

- Clustering Terms
- ClusterXL
- Cluster Synchronization
- Synchronized-Cluster Restrictions
- Securing the Sync Interface
- To Synchronize or Not to Synchronize

ClusterXL: Load Sharing

- Multicast Load Sharing
- Unicast Load Sharing
- How Packets Travel Through a Unicast
- LS Cluster
- Sticky Connections

Maintenance Tasks and Tools

- Perform a Manual Failover of the FW Cluster
- Advanced Cluster Configuration



IT EDUCATION CENTRE

Management HA

The Management High Availability Environment

Active vs. Standby

What Data is Backed Up?

Synchronization Modes

Synchronization Status

SecureXL: Security Acceleration

What SecureXL Does

Packet Acceleration

Session Rate Acceleration

Masking the Source Port

App Layer Protocol - e.g with HTTP HTTP 1.1

Factors that Preclude Acceleration

Factors that Preclude Templating (Session Acceleration)

Packet Flow

VPN Capabilities

CoreXL: Multicore Acceleration

Supported Platforms and Features

Default Configuration

Processing Core Allocation

Allocating Processing Cores

Adding Processing Cores to the Hardware

Allocating an Additional Core to the SND

Allocating a Core for Heavy Logging

Packet Flows with SecureXL Enabled

Advanced User Management

User Management

Active Directory OU Structure

Using LDAP Servers with Check Point

LDAP User Management with User Directory

Defining an Account Unit

Configuring Active Directory Schemas

Multiple User Directory (LDAP) Servers

Authentication Process Flow

Limitations of Authentication Flow

User Directory (LDAP) Profiles



IT EDUCATION CENTRE

Troubleshooting User Authentication and User Directory (LDAP)

- Common Configuration Pitfalls
- Some LDAP Tools
- Troubleshooting User Authentication
- Identity Awareness
- Enabling AD Query
- AD Query Setup
- Identifying users behind an HTTP Proxy
- Verification of a log-on AD user at the source IP
- Checking the source computer OS
- Using SmartView Tracker

Advanced IPsec VPN and Remote Access

Advanced VPN Concepts and Practices

- IPsec
- Internet Key Exchange (IKE)
- IKE Key Xchange – P1/ P2

Remote Access VPNs

- Connection Initiation
- Link Selection

Multiple Entry Point VPNs

- How Does MEP Work
- Explicit MEP
- Implicit MEP

Tunnel Management

- Permanent Tunnels
- Tunnel Testing
- VPN Tunnel Sharing
- Tunnel-Management Configuration
- Permanent-Tunnel Configuration
- Tracking Options
- Advanced Permanent-Tunnel configuration
- VPN Tunnel Sharing Configuration

Troubleshooting-VPN Encryption Issues



IT EDUCATION CENTRE

VPN Debugging commands
vpn debug Command
vpn debug on | off
vpn debug ikeon |ikeoff
vpn Log Files
vpn debug trunc
VPN Environment Variables
vpn Command
vpn tu
Compare Sas

Auditing and Reporting

Standards for Auditing and Reporting
Introduction to SmartEvent
SmartEvent Arch
Process of Component Communication
Event Policy User-Interface
Concept of SmartReporter

