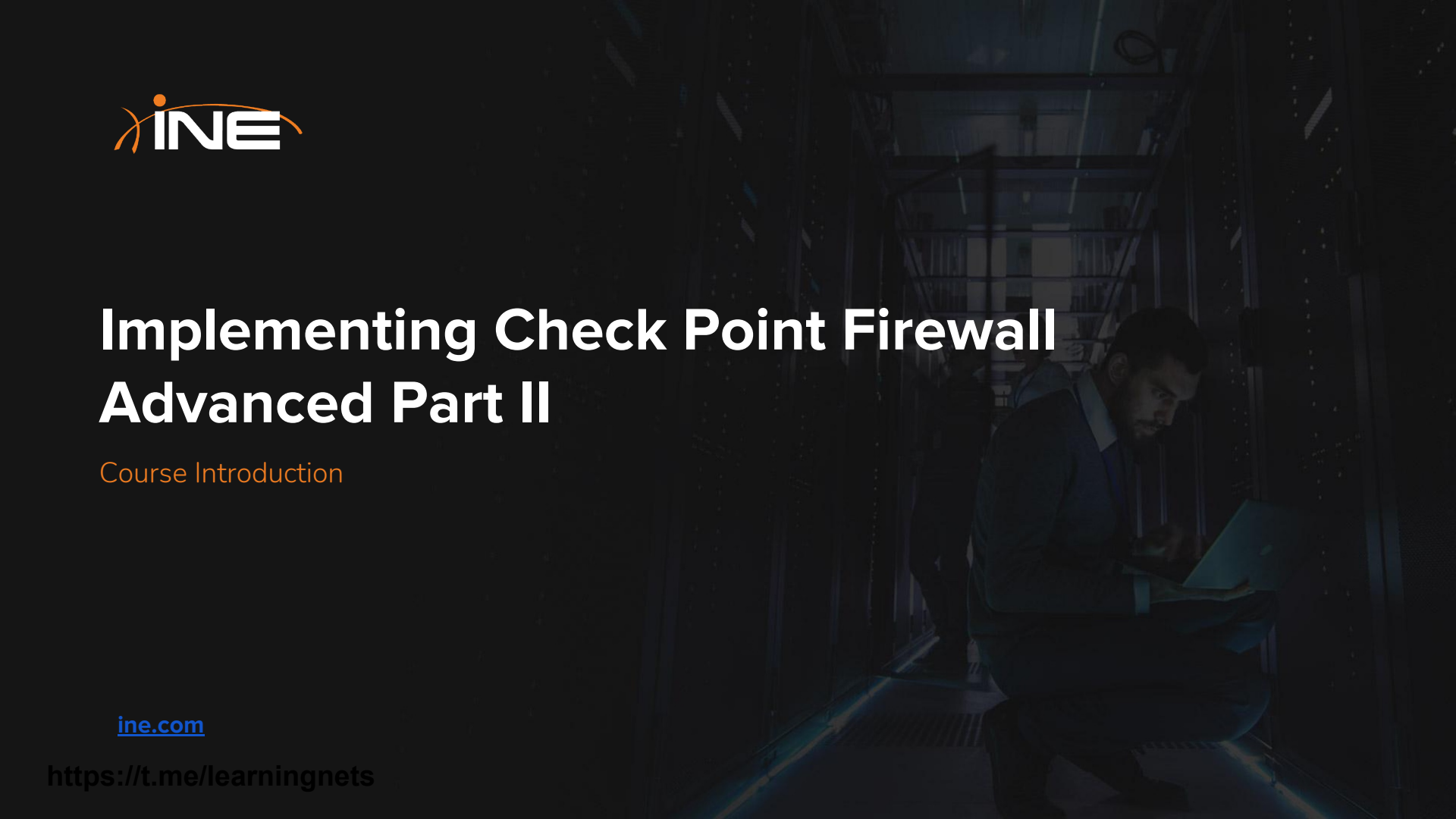


Implementing Check Point Firewall Advanced Part II

Course Introduction

ine.com

Piotr Kaluzny

CCIE #25665

pkaluzny@ine.com

linkedin.com/in/piotrkaluzny

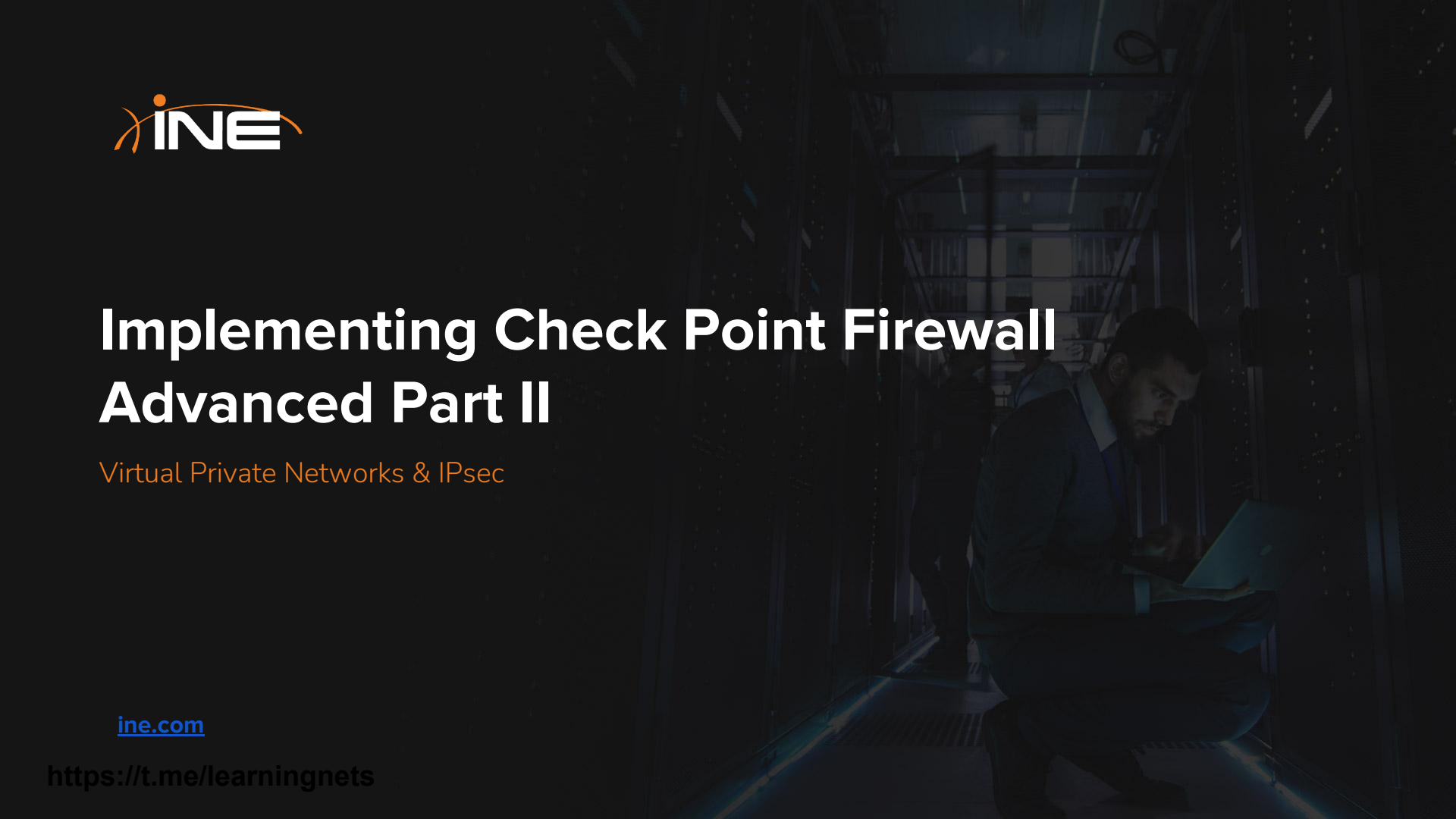
CCIE Security

+ Check Point Fundamentals

Course Prerequisites

Course Overview

- Module 1 Virtual Private Networks & IPsec
- Module 2 Check Point VPN Features
- Module 3 Site-Site VPN
- Module 4 Remote Access VPN
- Module 5 Introduction to SmartEvent



Implementing Check Point Firewall Advanced Part II

Virtual Private Networks & IPsec

ine.com

Module Overview

- What is VPN?
- IPsec overview, components & operations

Virtual Private Network (VPN) Overview

- Virtual Private Network (VPN) serves as a logical connection
  - Its primary function is to provide end-to-end connectivity
    - Usually built over an unsecured network, such as the Internet
- VPNs rely on Tunneling
  - A process of encapsulating the original packet into a new header
  - Relies on three protocols :
    - Carrier, Encapsulating & Passenger
- Not all VPN implementations are secure

IP Security (IPsec) Overview

- The most common implementation of VPNs
  - RFC 4301 „Security Architecture for the Internet Protocol”
  - Layer 3

- IPsec Security Services
  - Authentication
  - Data Confidentiality
  - Data Integrity
  - Anti-replay

IPsec Components

- IPsec consists of multiple protocols & standards
  - Internet Security Association & Key Management Protocol (ISAKMP)
    - A framework describing core IPsec functions for secure communication (RFC 2408)
      - Specifies that keying & authentication should occur
      - Describes the procedures to establish, negotiate, modify & delete tunnel information
  - Internet Key Exchange (IKE) is an implementation of ISAKMP
    - Performs main Control Plane functions, like key exchange, authentication, etc.
    - IKEv1 (RFC 2409) & IKEv2 (RFC 7296)

IPsec Components

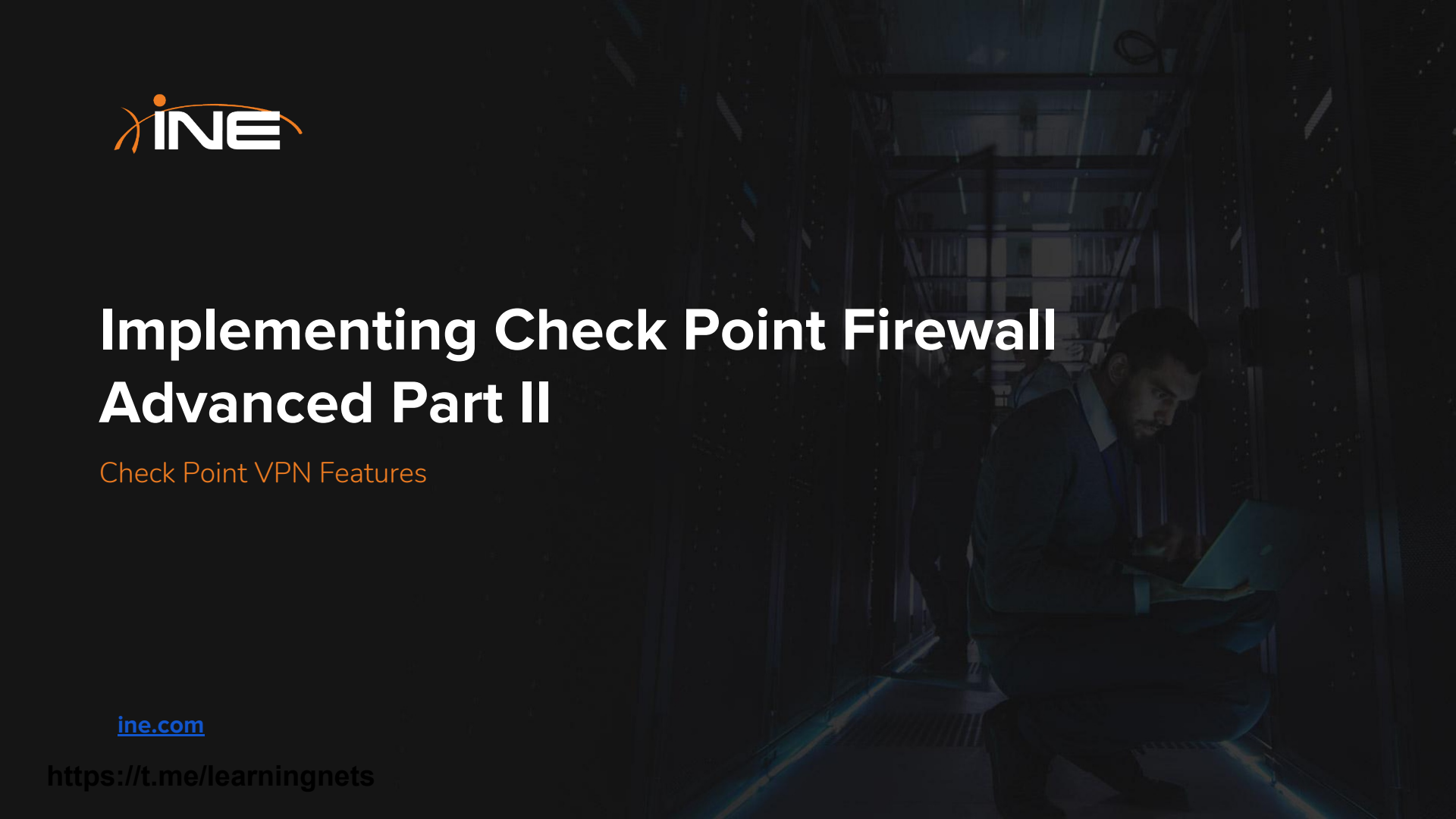
- IPsec heavily relies on Cryptography
  - Control Plane
    - Key Management : DH, ECDH
    - Authentication : PSK, RSA, ECDSA
  - Data Plane
    - Security Protocols : ESP, AH
    - Confidentiality : DES, 3DES, AES, SEAL
    - Data Integrity and Origin Authentication : MD5, SHA-1, SHA-2

- IPsec is a framework of open standards
  - Obsolete technologies can be replaced without changing the framework

IPsec Operations

- Negotiation Goals
  - Policy agreement
  - Key establishment
  - Authentication
  - Data protection
  - Maintenance

- IPsec VPNs are negotiated (UDP 500/4500) in phases
  - Management/Control Connection
    - IKEv1 "Phase I" or IKEv2 "IKE_SA_INIT"
  - Data Channels
    - IKEv1 "Phase II" or IKEv2 "IKE_AUTH"



Implementing Check Point Firewall Advanced Part II

Check Point VPN Features

ine.com

Module Overview

+ VPN features
+ Documentation

VPN Features

- VPN Topologies
  - Star vs Meshed
- VPN Types
  - Domain-based
    - VPN Domain
  - Route-based
    - VPN Tunnel Interface (VTI)
    - Supports Dynamic Routing
- VPN Community
  - Represents tunnels & their attributes

VPN Features

- Link Selection
  - VPN Interface
  - Route Probing
  - Load Sharing
    - Regular
    - Service-based

VPN Features - Remote Access

- Remote Access Solutions
  - Clientless
  - On demand client
    - SSL Network Extender
  - Client-based
    - Including Endpoint Security
- Office Mode
  - VPN address assignment
- Visitor Mode
  - TCP Tunneling

Documentation

- Site to Site VPN Administration Guide
  - https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_SitetoSiteVPN_AdminGuide/Default.htm
- Remote Access VPN Administration Guide
  - https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_RemoteAccessVPN_AdminGuide/Default.htm

Implementing Check Point Firewall Advanced Part II

Site-Site VPN

ine.com

Module Overview

+ Configuration steps
+ Example

Configuration

- Define/edit Security Gateways
  - Local Security Gateway
    - Enable the IPsec blade
      - Gateways & Servers -> General Properties
        - Network Security -> IPSec VPN
  - External Security Gateway
    - Check Point
      - Network Object > Gateways and Servers > More > Externally Managed VPN Gateway
    - Third-party
      - Network Object -> More -> Interoperable Device

Configuration

- Link Selection
  - Gateways & Servers -> IPSec VPN
    - Link Selection
- VPN Domain
  - Gateways & Servers > Network Management
    - VPN Domain
  - Third Party
    - Topology

Configuration

- VPN Community
  - Security Policies -> Access Tools
    - VPN Communities
- ACP Rules
  - Security Policies -> Access Control
    - Policy
      - Local/remote VPN subnets, VPN community, Accept
- Verification
  - Logs & Monitor
  - vpn tu (CLI)

Implementing Check Point Firewall Advanced Part II

Remote Access VPN

ine.com

Module Overview

+ Configuration steps
+ Example

Configuration

- Blades
  - Gateways & Servers -> General Properties -> Network Security
    - IPSec VPN
    - Identity Awareness
      - Remote Access
    - Mobile Access

- Authentication
  - Gateways & Servers -> General Properties > VPN Clients > Authentication
    - Authentication Method

Configuration

- User Settings
  - User Object
    - User
    - Group
    - Access Role
- VPN Community
  - Security Policies -> Access Tools
    - VPN Communities

Configuration

- ACP Rules
  - Security Policies -> Access Control
    - Policy
      - Access Role (Source), VPN community, Accept
- Verification
  - Logs & Monitor

Implementing Check Point Firewall Advanced Part II

Introduction to SmartEvent

ine.com

Module Overview

- Overview
- Event Correlation
- Documentation

SmartEvent Overview

- Unified solution for security event management & analysis
  - Consolidates logs and shows them as prioritized security events
    - Minimizes the amount of data to be reviewed
  - Provides a centralized display of aggregated data
    - Views & Reports
  - Provides log correlation

SmartEvent Installation

- SmartEvent is a licensed software blade
  - Single server vs multiple servers
    - https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_Installation_and_Upgrade_Guide/Topics-IUG/Getting-Started.htm?tocpath=_____3
  - Open server vs Smart-1
    - https://www.checkpoint.com/quantum/event-management/

Event Correlation

- SmartEvent correlates logs from all Check Point enforcement points
  - Correlation Unit performs log analysis and event extraction
    - Event Policy

- Basic Event Policy Workflow
  - Logs & Monitor -> SmartEvent Settings & Policy
    - Initial Settings
    - Event Configuration
    - Policy installation

Documentation

- Logging and Monitoring Administration Guide
  - https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_LoggingAndMonitoring_AdminGuide/Default.htm

Implementing Check Point Firewall Advanced Part II

ine.com

Course Conclusion

- IPsec is a secure standard for data communication
- Check Point supports Site-to-Site & Remote Access VPN solutions
- VPN implementation is not a one-step process - the main components include gateways, VPN communities & ACP rules
- SmartEvent provides unified event management & correlation

Thank You