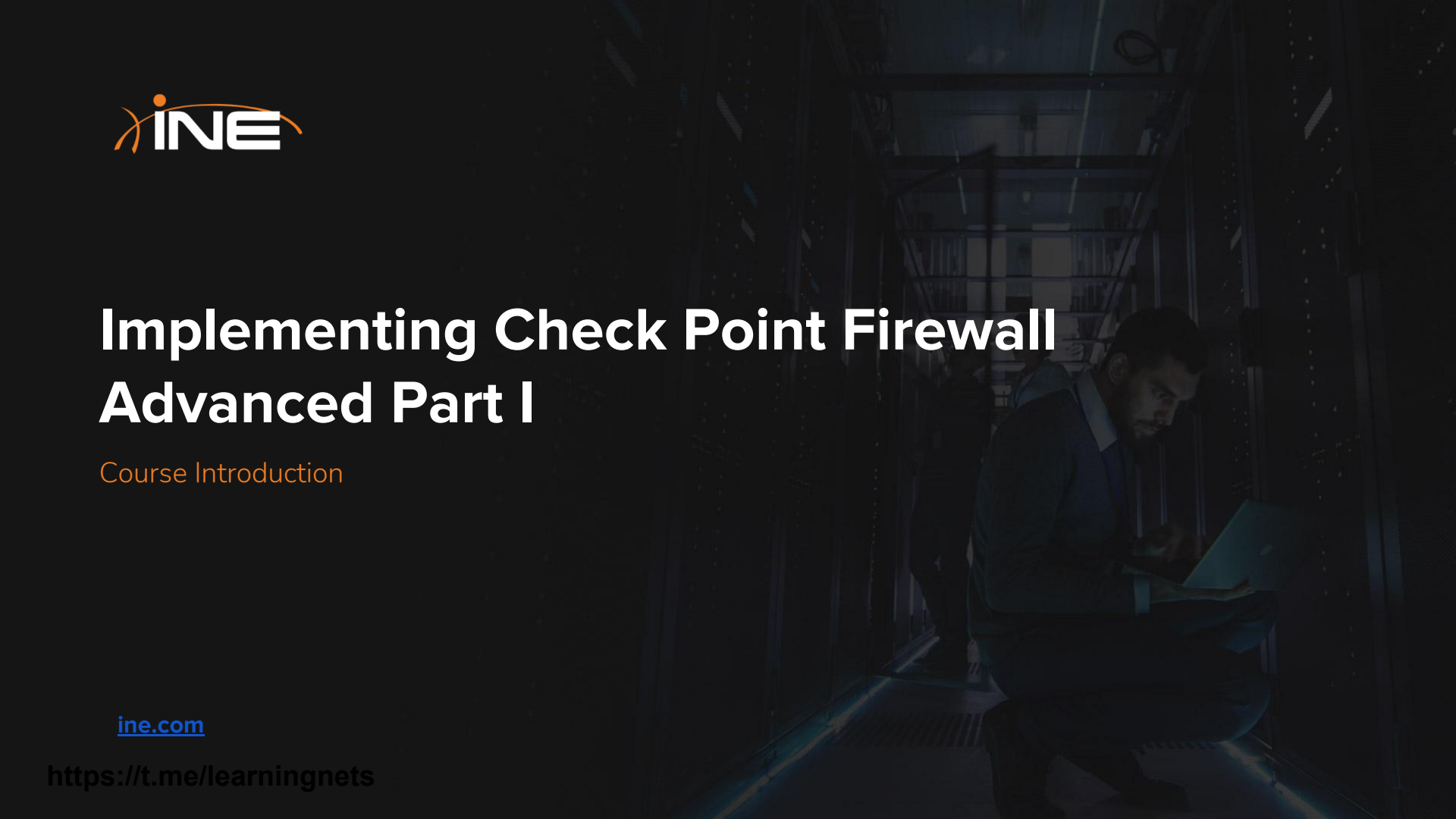


Implementing Check Point Firewall Advanced Part I

Course Introduction

ine.com

Piotr Kaluzny

CCIE #25665

pkaluzny@ine.com

linkedin.com/in/piotrkaluzny

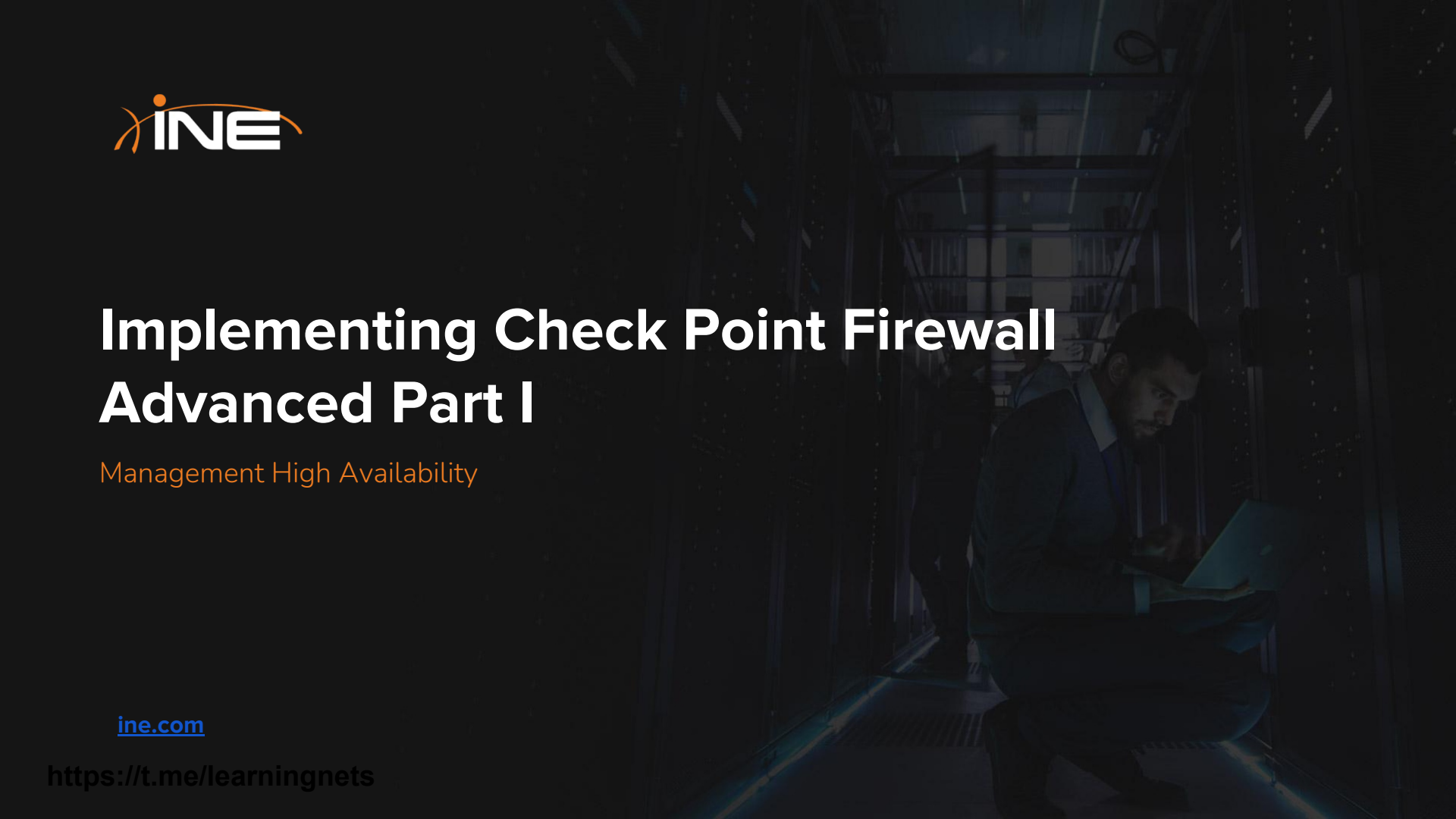
CCIE Security

+ Check Point Fundamentals

Course Prerequisites

Course Overview

- Module 1 Management High Availability
- Module 2 Clustering
- Module 3 Implementing Clustering
- Module 4 SecureXL
- Module 5 CoreXL
- Module 6 Multi-Queue
- Module 7 Check Point APIs



Implementing Check Point Firewall Advanced Part I

Management High Availability

ine.com

Module Overview

- Overview
- Terminology
- Operations
- Configuration

Management High Availability Overview

- High Availability (HA) allows a system to function in case of a failure
  - Typically requires Redundancy

- Management High Availability requires more than one SMS
  - The main management station is used for administration
  - Additional management station acts as a backup
    - There can be more than one backup unit

Management High Availability Terminology

- Primary vs Secondary
  - The first-installed management station becomes the Primary server
  - Additional unit acts as a Secondary server
- Active vs Standby
  - Active server refers to the "live" system
  - Standby server refers to the "backup" system

Management High Availability Operations

- Active server synchronizes a Standby server (configuration overwrite)
  - Regular intervals
  - Session publish
    - Unpublished changes are not synced
- Active <-> Standby changeover is not automatic
  - A standby system should be manually promoted to Active
    - Triggers a re-sync
- Servers enter Collision Mode when there is more than one Active system
  - Puts synchronization on hold

Configuration

- Prerequisites
  - Install a Secondary SMS
- Primary Server
  - Create an object for the Secondary SMS
    - Objects -> New Network Object -> Gateways and Servers
      - Check Point Host
  - Configure object settings (**General Properties**)
    - Hostname and IP address
    - Management blade
      - Management -> Network Policy Management
  - Specify a SIC key for secure communication (**Communication**)

Configuration

- Primary Server
  - Initialize a sync
    - **Publish**
  - Check out & manage the HA status
    - **Menu -> Management High Availability**

Implementing Check Point Firewall Advanced Part I

Clustering

ine.com

Module Overview

- Technology overview
- Cluster Control Protocol
- Synchronization

Clustering Overview

- Grouping two or more units to run in parallel as one
  - Provides redundancy and extends computing power
- Check Point's ClusterXL is a software-based clustering technology
  - Transparent failover
  - Enhanced throughput
    - Load Sharing
  - Zero downtime
    - Synchronization

Clustering Overview

- ClusterXL Types
  - High Availability
    - Active-Standby
    - Active-Active
      - See "Active-Active Mode in ClusterXL"
  - Load Sharing
    - Active-Active

Clustering Overview

- Prerequisites
  - Identical hardware
    - CPU
    - Interfaces
    - Underlying OS
  - Identical Check Point software
  - Identical Software Blades

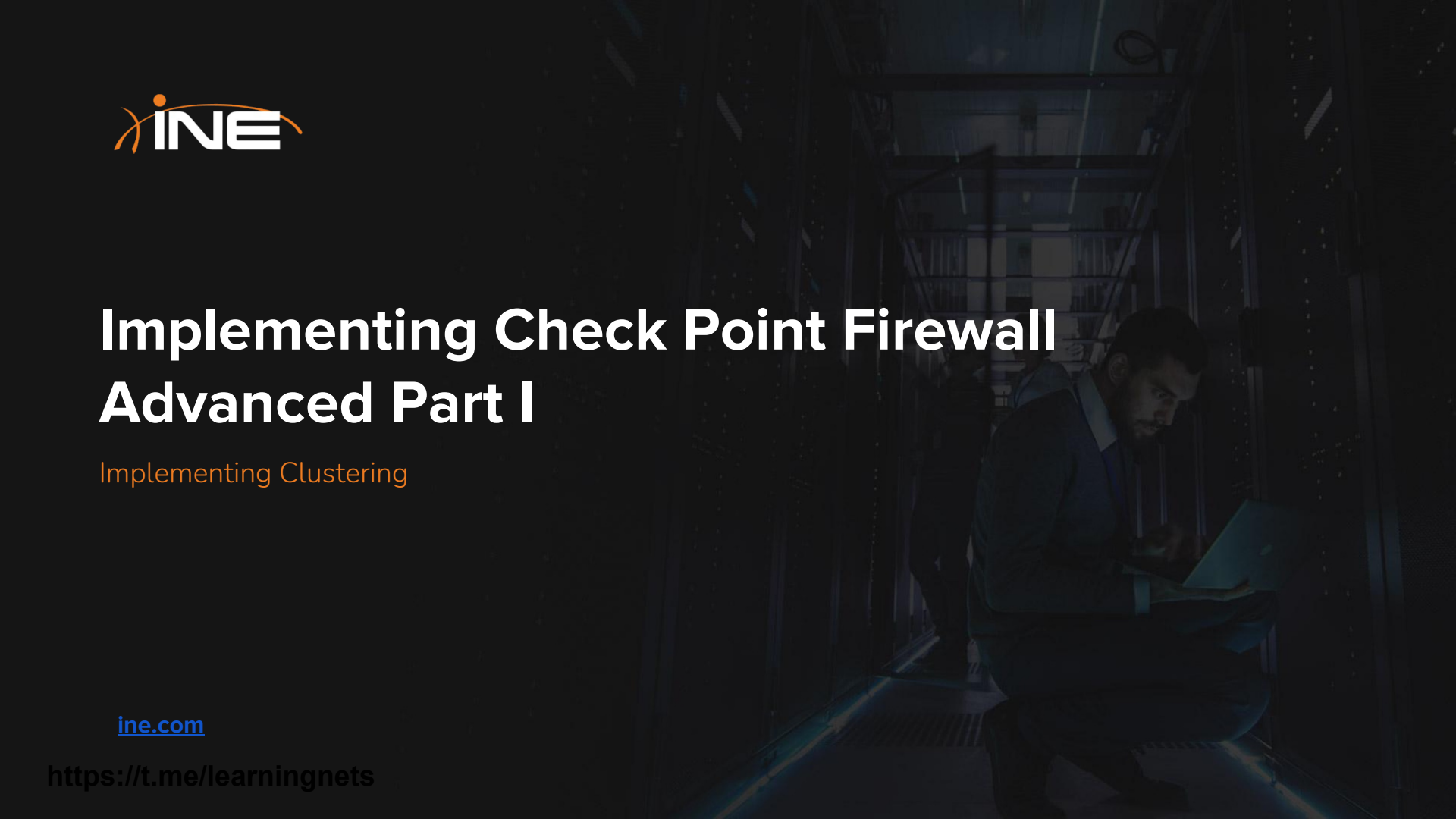
Cluster Control Protocol (CCP)

- Communicates cluster members with each other over UDP port 8116
  - State reporting
  - Keepalives
  - Synchronization
- CCP traffic does not require explicit Security Policy rules

Synchronization

- Cluster members can exchange connection data & state during Synchronization
  - Full Sync
    - Initial transfer and recovery over TCP port 256
  - Delta Sync
    - Kernel table changes over UDP port 8116

- Synchronization Considerations
  - Dedicated synchronization network and/or encryption
  - Performance impact
    - "Long" vs "short" connections



Implementing Check Point Firewall Advanced Part I

Implementing Clustering

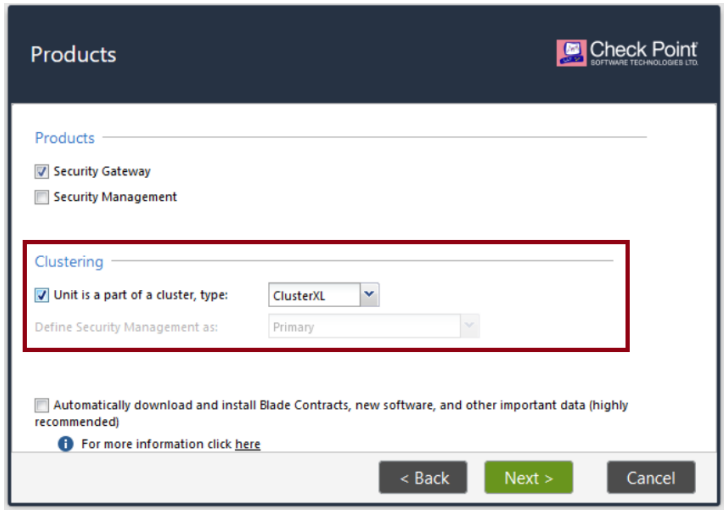
ine.com

Module Overview

+ Configuration steps
+ Example

Configuration

- Pre-requisites
  - Enable gateways for Clustering



Configuration

- Cluster Wizard
  - Objects -> New Network Object -> Gateways and Servers
    - Cluster

- Configuration Items
  - Name & IP address
  - Cluster Type
  - Cluster Members
    - SIC (gateway installation)
  - Cluster Properties
    - Tune Topology Settings
  - Security Policy & Routing

Documentation

- ClusterXL Administration Guide
  - https://sc1.checkpoint.com/documents/R80.40/WebAdminGuides/EN/CP_R80.40_ClusterXL_AdminGuide/Default.htm

Implementing Check Point Firewall Advanced Part I

SecureXL

ine.com

Module Overview

+ Overview
+ Configuration

SecureXL Overview

- Check Point Firewall processes traffic in a few ways ("paths")
  - Slow Path (F2F)
  - Medium Path (PXL)
  - Accelerate Path (SXL)
    - SecureXL

- SecureXL is a performance-enhancing technology
  - Access Control, NAT, Software Blades, ClusterXL
  - Encryption
  - Connection/session rate
  - Policy installation

SecureXL Overview

- SecureXL adds another layer between the connection table and ACP
  - A connection table "miss" normally indicates F2F (Slow Path) processing
  - Accept Template Table allows for a rule base lookup bypass

- Accept Template Table
  - Source/destination IP address
  - Source/destination port number
  - IP protocol number

Configuration

- SecureXL is enabled by the First Time Configuration Wizard
  - You can temporarily disable it for troubleshooting (all cluster members)
    - **fwaccel [off | on] [-a]**
  - Verification
    - **fwaccel stat**
    - **fwaccel stats**

Implementing Check Point Firewall Advanced Part I

CoreXL

ine.com

Module Overview

+ Overview
+ Configuration

CoreXL Overview

- The ability of the firewall to utilize multiple CPU cores simultaneously
  - Replicates the firewall kernel into multiple instances (one per core)
    - Increases available throughput
    - Decreases processing latency

- Core Types
  - Firewall Worker
  - Secure Network Dispatcher (SND)
    - Software Interrupt Request (SoftIRQ)
    - Accelerated processing (SecureXL)
    - Traffic-to-core distribution

CoreXL Overview

- The default core split is static
  - Example (8-core hardware)
    - 2x SND
    - 6x Firewall Worker
  - Use **top** before adjusting

- R80.40 and above supports Dynamic Split
  - Not enabled by default

Configuration

- Enabled by default on hardware with at least 2 cores
  - A change to CPU cores requires adjustments to be made
    - **cpconfig**
- Dynamic Split
  - **dynamic_split -o enable** (needs a reboot)
  - Verify with **cpview**
    - **SysInfo**
- Remember to keep the same configuration on all cluster members

Implementing Check Point Firewall Advanced Part I

Multi-Queue

ine.com

Module Overview

+ Overview
+ Configuration

Multi-Queue Overview

- A mechanism used to alleviate "receive drop" (RX-DRP)
  - Also known as "buffering miss"
    - Ring buffer fill up (NIC > ring buffer > SoftIRQ)
      - netstat -ni
- The original system architecture limits CPU allocation to a single SND core per interface
  - Multi-Queue permits all SND cores to handle a port
    - Effectively results in multiple SoftIRQ "queues"
    - Prevents packet loss

Multi-Queue Overview

- Prerequisites
  - SecureXL
  - 2+ CPU cores
  - Interface drivers (**ethtool -i**)
    - Intel PCIe 1Gbps (igb)
    - Intel PCIe 10Gbps (ixgb)
    - Intel PCIe 40Gbps (i40e)
    - Mellanox ConnectX 40Gbps (mlx5_core)

Configuration

- Enabled by default on all supported interfaces
  - mq_mng
    - -- show
    - --set-mode auto
    - -s
    - --reconf
- Remember to keep the same configuration on all cluster members

Implementing Check Point Firewall Advanced Part I

Check Point APIs

ine.com

Module Overview

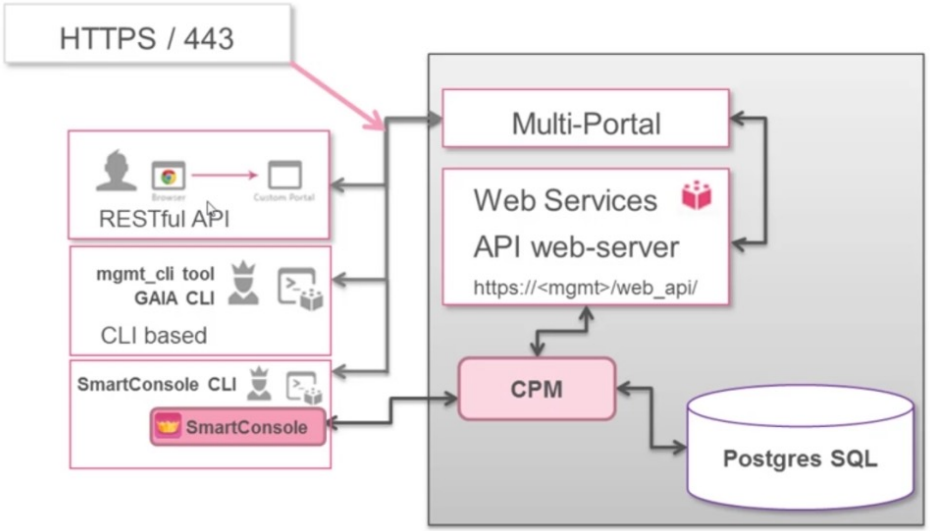
- Overview
- Architecture
- Management API
- Documentation

Check Point API Overview

- Check Point provides several different RESTful APIs
  - Help automate product administration/management

- API Examples
  - Management
  - GAiA
  - Threat Prevention
  - IoT

The Architecture



*source: https://community.checkpoint.com/

Documentation

- API Reference
  - https://sc1.checkpoint.com/documents/latest/api_reference/index.html
- Management API
  - Direct access
    - https://*SMS_IP_address*/api_docs/

Management API

- Provides read/write access to the SMS
  - Scripting and/or integration
- API Interfaces
  - SmartConsole CLI
  - GAIA CLI
  - mgmt_cli
  - Web Services
- Prerequisites
  - Manage & Settings -> Blades -> Management API -> Advanced Settings

Management API

- SmartConsole CLI
  - No need to authenticate
  - Example
    - *add host name PC1 ip-address 10.1.12.11*
    - *add network name LAN5 subnet 10.5.5.0 mask-length 255.255.255.0*

- GAIA CLI (clish)
  - Similar to SmartConsole, but commands start with **mgmt**
  - Requires authentication (**mgmt login**)
  - Example
    - *mgmt add host name PC2 ip-address 10.1.12.12*

Management API

- mgmt_cli
  - Commands start with **mgmt_cli**
    - Assumes SMS is local by default
  - Requires authentication or session-id
    - **mgmt_cli login [-r]**
      - Returns a session-id (can be "saved" in a file)
  - Example
    - *mgmt_cli login user api-admin password api-pw > sid.txt*
    - *mgmt_cli add host name PC3 ip-address 10.1.12.13 –s sid.txt*
    - *mgmt_cli publish –s sid.txt*
    - *mgmt_cli logout –s sid.txt*

Management API

- Web Services
  - HTTP POST calls
    - https://<*mgmt* >:<*port* >/web_api/<*command* >
  - JSON format

*source: https://community.checkpoint.com/

- Mandates "X-chkp-sid" in all API calls except **login**

Management API

- Web Services
  - Example (Request)

    HTTP POST to https://192.0.2.10/web_api/add-host
    content-Type: application/json
    X-chkp-sid:8478V00sYHvH_nBvIhDI203eu3clauAuB1iCEWOw_YY

```
{
   "name":"PC4",
   "ip-address":"10.1.12.14"
}
```

  - Example (Response)

    Status: 200 OK

```
{
   "sid": "8478V00sYHvH_nBvIhDI203eu3clauAuB1iCEWOw_YY",
   "url": "https://192.0.2.10:443/web_api",
   ... <truncated> ...
}
```

Implementing Check Point Firewall Advanced Part I

ine.com

Course Conclusion

- Redundant management systems include a Primary & Secondary unit
- Clustering allows to combine firewalls to run as a single system
- SecureXL enhances firewall's performance by reducing CPU usage
- CoreXL allows a firewall to utilize multiple CPU cores simultaneously
- Multi-queue alleviates "receive drop"
- Check Point offers several different APIs including Management API for scripting and easy integration

Thank You