

# Advanced Troubleshooting R71

## Custom training solutions for advanced performance

The course addresses numerous techniques to troubleshoot and debug Check Point based security systems. It provides new tools and information about troubleshooting, thus allowing for faster resolution of Service Requests.

During the three<sup>1</sup> day course, participants will acquire in-depth knowledge of Firewall-1/VPN-1 architecture, technologies used, and the methodologies and tools to troubleshoot most security system elements. The course includes various examples from actual Check Point support cases and Professional Services field experience along with numerous hands-on practical labs.

### TARGET AUDIENCE

The course is intended for firewall administrators and managers, security engineers, security consultants, integrators and support partners to improve troubleshooting capabilities and get “under the hood”.

### REQUIRED KNOWLEDGE

It is highly recommended that course participants have experience in planning, implementing and managing network security systems based on Check Point products.

Check Point Certified Security Administrator (CCSA) and Check Point Certified Security Expert (CCSE) courses or equivalent knowledge is recommended before taking this course.

### COURSE AGENDA (3 DAYS)

#### 1. General concepts

- Firewall-1 architecture
- Main user mode processes
- Firewall-1 kernel infrastructure
- Policy installation
- Configuration files

#### 2. User space debug

- Isolating the problem
- How to run user mode debug
- Analyzing debug output
- Core dump

#### 3. Kernel debug

- Kernel debug mechanism
- Debugging flags
- Debugging tips

#### 4. FW Monitor

- What is ‘fw monitor’?
- Client to server connection
- Server to client connection
- Expressions and Tips
- Analyzing ‘fw monitor’ output
- Examples

#### 5. NAT technology

- General explanation
- How NAT works
- How to Debug NAT issues
- Debug example of Hide NAT
- Other cases of NAT

#### 6. Clustering solutions<sup>2</sup>

- Understanding the Cluster Elements
- Check Point Solutions:  
ClusterXL (HA ,Load Sharing)
- Advanced features and problematic scenarios
- 3rd party clusters
- Troubleshooting for clusters

#### 7. VPN solutions

- General
- Kernel and User Mode functions
- IKE and IPSec
- Logs and tools
- Troubleshooting techniques

#### 8. Acceleration

- What is acceleration
- Acceleration infrastructure
- Acceleration templates
- Drop templates
- Forensics
- Debugging

Please contact Professional Services at [ps@checkpoint.com](mailto:ps@checkpoint.com) for more information about this course.

<sup>1</sup> There is option for additional modules as add-on to the course baseline (requires more days):

- Provider-1
- VSX
- Edge
- GX
- VoIP

<sup>2</sup> Clustering can be focused either on ClusterXL or VRRP/IP Clustering

