

Opleiding : CCSA, Check Point Certified Security Administrator R82, certificering

Praktijkcursus - 4d - 28u00 - Ref. CPH

Prijs : 2460 € V.B.

NEW

Het doel van de cursus is om je te leren hoe je Check Point R82 installeert en configureert, beveiligingsbeleid implementeert, licenties en beheerders beheert, logs en verkeer monitort, HTTPS-decodering implementeert, toepassingen controleert en URL's filtert, back-ups en upgrades uitvoert, site-to-site VPN's beheert en standalone bedreigingspreventie begrijpt. De cursus bevat ook voorbereiding op het CCSA certificeringsexamen en de implementatie van een high-availability cluster.

Pedagogische doelstellingen

Aan het einde van de training is de deelnemer in staat om:

- ✓ Check Point R82 installeren en configureren
- ✓ Beveiligingsbeleid implementeren en beheren
- ✓ Adresomzetting (NAT) implementeren
- ✓ Licenties en contracten beheren
- ✓ Omgevingen met meerdere sites beheren
- ✓ Administratieve toegang beheren
- ✓ Logboeken en netwerkverkeer monitoren
- ✓ HTTPS-inspectie en HTTP/3-ondersteuning configureren
- ✓ Applicatiebeheer en URL-filtering toepassen
- ✓ VPN's en bedreigingspreventie implementeren

Doelgroep

Systeem-/netwerk-/beveiligingstechnici, -beheerders en -ingenieurs.

Voorafgaande vereisten

Goede kennis van TCP/IP. Basiskennis van IT-beveiliging.

DEELNEMERS

Systeem-/netwerk-/beveiligingstechnici, -beheerders en -ingenieurs.

VOORAFGAANDE VEREISTEN

Goede kennis van TCP/IP.
Basiskennis van IT-beveiliging.

VAARDIGHEDEN VAN DE CURSUSLEIDER

De deskundigen die de cursus leiden zijn specialisten op het betreffende vakgebied. Zij werden geselecteerd door onze pedagogische teams zowel om hun vakkennis als hun pedagogische vaardigheden voor elke cursus die zij geven. Zij hebben minstens vijf tot tien jaar ervaring in hun vakgebied en oefenen of oefenden verantwoordelijke bedrijfsfuncties uit.

BEOORDELINGSMODALITEITEN

De cursusleider beoordeelt de pedagogische vooruitgang van de deelnemer gedurende de gehele cursus aan de hand van meerkeuzevragen, praktijksituaties, praktische opdrachten, ...
De deelnemer legt ook van tevoren en naderhand een test af ter bevestiging van de verworven kennis.

Praktische modaliteiten

Praktisch werk

Praktische oefeningen: Installatie van Check Point R82. SmartConsole installeren. Objecten aanmaken. Aanmaken van een beveiligingsbeleid.

Opleidingsprogramma

1 Inleiding tot de Check Point R82 architectuur: Initiële configuratie

- Check Point-producten en R82-nieuws.
- Maak kennis met Gaia OS.
- Drietrapsarchitectuur, Software Blades en Check Point Infinity.
- Standalone vs. gedistribueerde modi.
- Presentatie van het SIC-protocol.
- CLI: opdrachtregelinterface.
- Web SmartConsole.

Oefening

Installatie van Gaia in R82 op de beheerserver en de hoofdgateway.

2 Beheer van beveiligingsbeleid

- Aan de slag met SmartConsole R82.
- Pakketinspectie.
- Objecten en regels maken.
- Inline lagen" beleid (onder regels).

Oefening

SmartConsole installeren. Objecten aanmaken. Een beveiligingsbeleid aanmaken.

3 Adresomzetting (NAT)

- Statische, dynamische en handmatige NAT.
- ARP en routeringsproblemen.
- Implementatie van NAT-regels.

Oefening

Implementatie van automatische statische NAT, Hide en handmatige transactieregels.

4 Beheer van licenties en locaties op afstand

- Licentietypen en beheer via SmartUpdate.
- Multi-site implementatie en beleidspakketten.
- Geordende lagen en beleidsdeling.

Oefening

Installation d'une passerelle distante, création d'une politique de sécurité (Policy Pack), et de règles de base pour le site distant. Création et partage d'une « Ordered Layer ».

PEDAGOGISCHE EN TECHNISCHE MIDDELEN

- De gebruikte pedagogische middelen en cursusmethoden zijn voornamelijk: audiovisuele hulpmiddelen, documentatie en cursusmateriaal, praktische oefeningen en correcties van de oefeningen voor praktijkstages, casestudies of reële voorbeelden voor de seminars.
- Na afloop van de stages of seminars verstrekt ORSYS de deelnemers een evaluatievragenlijst over de cursus die vervolgens door onze pedagogische teams wordt geanalyseerd.
- Na afloop van de cursus wordt een presentielijst per halve dag verstrekt, evenals een verklaring van de afronding van de cursus indien de stagiair alle sessies heeft bijgewoond.

TOEGANGSMODALITEITEN EN TERMIJNEN

De inschrijving dient 24 uur voor aanvang van de cursus plaatsgevonden te hebben.

TOEGANKELIJKHEID VOOR MINDERVALIDEN

Is voor u speciale toegankelijkheid vereist? Neem contact op met mevr. FOSSE, contactpersoon voor mindervaliden, via het adres psh-accueil@ORSYS.fr om uw verzoek en de haalbaarheid daarvan zo goed mogelijk te bestuderen.

5 Beheerder

- Toestemmingsprofielen.
- Gelijktijdige sessies en beheer van beheerders.

Oefening

Aanmaken van een nieuw "Permissieprofiel" met beperkte autorisaties.

6 Logboeken, bewaking en probleemoplossing

- Verbindingstracering en waarschuwingen.
- Bewakingstools (CPView, SmartView Monitor).
- Inleiding tot probleemoplossing (tcpdump, zdebug).

7 HTTPS-inspectie. Applicatiecontrole, URL-filtering en onderhoud

- Uitgaande/Ingaande regels.
- Beheer van certificaten en SNI's.
- Geavanceerde HTTPS-inspectiefuncties.
- App-controle, URL-filtering, DNS-filtering. Gebruikerscontrole.
- Back-ups (lokaal en in de cloud), CPUSE, updates. Het commando cpconfig.

Oefening

Mise en oeuvre de l'inspection HTTPS. Filtrage Web et Applications : créer et partager la politique de « Filtrage Web et Applications » en tant que « Inline Layer » et « Ordered Layer ». Restauration de la configuration d'une passerelle.

8 Site-to-site VPN, preventie van bedreigingen en hoge beschikbaarheid

- VPN-architectuur, IKE/IPSec, VPN-routing.
- ClusterXL en redundantie (bonus).

Oefening

Utilisation de VPN-IPSec Inter-sites (Shared Secret) et VPN-IPSec Inter-sites (Certificats).

9 Bedreigingspreventie

- Autonome preventie van bedreigingen (AI, ThreatCloud).

Oefening

Implementatie van autonome preventie van bedreigingen.

10 Clustering

- ClusterXL en redundantie.

Oefening

Implementatie van ClusterXL in HA-modus.

Opties

: 300 € HT

De certificering wordt uitgegeven door Check Point Software Technologies. Het valideert de fundamentele vaardigheden die nodig zijn om Check Point beveiligingsoplossingen te beheren. Het duurt 90 minuten en is gebaseerd op een MCQ van 90 vragen in het Engels.

De certificeringsoptie wordt aangeboden in de vorm van een voucher of een uitnodiging waarmee u na afloop van de opleiding het examen kunt afleggen.

Data en plaats

KLAS OP AFSTAND

2026 : 24 maa., 16 juni, 29 sep., 8 dec.

PARIS LA DÉFENSE

2026 : 24 maa., 16 juni, 29 sep., 8 dec.