

The logo features the letters 'CEH' in a large, bold, white sans-serif font. A vertical white line separates the 'C' from the 'EH'. To the right of the 'EH' is a small 'TM' trademark symbol. Behind the text is a stylized globe composed of glowing blue lines and dots, resembling a network or orbital system. Below the 'CEH' text, the words 'CERTIFIED ETHICAL HACKER' are written in a smaller, white, all-caps sans-serif font. The entire logo is set against a dark blue background with subtle light effects and bokeh.

[illegible]

000000 0000 00000 .0000000 00000000 00000 00 0000000 00000 00 00000 00000 000000000 00000
 0000000 00000 00 .000 000000 OC3 Optical Carrier-3 0 ISDN 00 0000000 0000 00 00 00 000000 00000000
 0 0000000000 000 0000000 00000000 0 000000 00000 00 000000000 00000 000000 00000 00 00 00000 00000000 00000000
 000000 000000 0000 00000000 00000000 00000000 00000 00 00000000 0 000 00 00000000 00000 00 000000000
 000000000 000000 0000 00 0000000000 00000 0000000000 0000000000 000000000 000000 00 00000000 .000
 0000 00 00000000 0000 0000 .000 00000 000000000 000000000 00000000 00000 00 .000000000 000 000000000000
 00 00000 00 000000000 00 000 0000000 00 000000000 00 000000000 000000 00000000 00 0000000000 00 000000000 00000000

0000000000 00 00 0000 000000 000000 0000 000 000000 000000 000000 00 00000000 0 0000 00 0000
 00000000 0000 00 .0000 00000000 000000 00000000 000000 000000 0000000000 00 0000 000000
 00000000 0000 00 00000000 0000000 0 000 000 00 0000 0000000 00 0000000 0000 0000 00 00 000000
 000000 0000000 00 00 **Leased** 00000 00000 000000 0000 00 00000000 000 00 0000000 000 000 .000000 00000000
 .0000000 000000000 000000000 0000 000000 00000 000000000 00

☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

[illegible]

0000 00000000000000 00 000000 000000 0000 0000000000 00 0000000000 00 00 00000000 00 000000 000 000000
 000000000000000000 00000000 00000000 0000 00 000000 0000 00 00000000 000000 .000 000000 0000 00 0000000000
 0000 000000000000 00 0000000 0 00000000 000000000000 00 00 **FTP** 00000000 000000000000 .000 000000 000000
 00 0000 0000000000 00 00000000 000000 0000000000 00 000 .0000 0000 00 0000 0000 00000000 000 00000000
Remote 000000000000 000000 00 0000000000 0000000000 000000 00 000000 00 000000 00 00 000 0000 000
 00 000 000 .000 0000 00 0000 0000 000 000 000000 00000000 000000 000000 00000000 .000 0000 **Access Service**
 000000 0000 00 00 000000 0000 0000 0000 000 000000 0000 00000000 00 000000 0000 00 00 00000000
 000 0000 00 0000000000 00000000 000000 000 00 .000 000000 00 000000 000000 00 0000 0000000000000000
 000000 0000 000 00 000000 0 000000 000000 000000 000000 0000000000 000 0000 000000 0000 000000000000
 000000 0000 .000000 00000000 000000 0000 000000 00 0000 000000 0000 00000000 .000000 0000 000000
 0000000000 00 000000 0000 0 000000 000000 0000 0000 00 00000000 0000 00000000 0000000000 000 00 000000
 .000000 0000 00 0000 00 0000 000000 000000 00 00000000 0 0000

000000 0000 00 00000 00000000 .00000000 000000000 00000 00000000 00 0000000 0000000 0 000000000
 000000 00000000 00 .000 000000 00 00 00 0000000 00000000 0000 00000000 0 000000 0000
 0000000 000 0000000 00000000 00 000000 000000 000000 000 0000000 00 0000000 00 000 00 0000000
 000000 00000000 000000 00000 000000000000 000000 00 000000 000000000 00000 0000 00 000000000000
 .000000 000000 000 00 0000000 000000 0000000 0000000

□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □

00 000000 00 000000 000 000000 00 000000 0 00000 00 0000 000 00000 00000000 00000000 00 000000 00 00000 00
 00 00 00000 00000 00000 00 000000000000 00 000000 000000 00000 000000 00 000000 000000 00000000 00000000
 000000 00000 000000 00000 000000000 .00000 00000 00000000 00000000 00 000000 00 00000000 000000 00 00000000
 AAA 00000 0IPsec 0000000000 00000 000000 000000 00000000 000000 00000000 00 00 00000 000000
 .00000000 0000000000 .00000000 0000000000

100 101

00 .000000 000000 00000000 0 00000000 00000000 0000 00 0000 00000000 0000 00 0000000000 000 000000
00000 0000000 00 0000000 0000000000 000000 0000 00 00 00000000 0000000 0000000 0000000000 00 00000000
000000 0000 00000000000 00 000000 00 00000000 000000 000000 00000000 00000 00 00000000 000000 .000
00 00 00000000 00 00000000 00 000 00000000 00 00000 000000 ...] 0000000000 0000000000 000 00 00000000

. □□□ □□□□□ □□□□□□□□

□□□□□□□

.000000 000000 00000 000 00 00000 0000000000 00 00 000 0000000000 00000 00000000 00000000 00000000 0000000000
00 00 000000 00000 .000000 00000000 0000000000 00 00000 00000 00000000000000 00000 00000 000 00
00 0000000 0000000000 00000 0000000000 00 0000000000 00 0000 0000000000000000 0000000000 00000 00000000 000000
.0000000 0000000000 00000000 0000000 0000000000 00000000 00 00 0000000000 0000000000 .0000 0000000000

□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □

[illegible]

□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □

00000 00000 00000 00000 .00000 000000000 000000 00000 00 0 000000 00000 00 000000 00 000000 00 0000000000 00
 00000 00000000 00 0000 00000000000 00000 000000 00000 .000 000000000 0 000000000 00000 00000000000 0000000000
 000 00000 00 0000000000 00000 .000000 0000000 000000 00 00 00 0000000 000 00 000000 0000000000000000
 00000 0 000 000000 00000000000 0000000000 00000 00 000000 00000 00 00000000 00 0000 0000000000 00 0000
 .000000 0000000 0000 00000000000 00 000000 000 00 000000 000000

IPSec

IPSec Tunnel, :transport transport tunnel .Transport

IP-Sec □□□□□ □□□□□□□□□

[illegible]

IPsec □□ □□□□□□ □□□□□□□□

Authentication Header (AH) 是 IPsec 协议族中用于提供数据完整性和认证性的协议。它通过计算数据摘要（如 MD5 或 SHA-1）并附加数字签名来验证数据的来源和完整性。AH 协议不加密数据，只负责认证。

IPsec 的 AH 和 ESP 协议头。AH 协议头提供数据完整性、数据源认证和防重放保护。ESP 协议头提供数据机密性、数据完整性、数据源认证和防重放保护。IPsec 隧道模式（Tunneling）和传输模式（Transport）是两种主要的部署模式。隧道模式将整个 IP 数据包封装在 IPsec 保护的数据包中，而传输模式只对数据包的有效载荷进行保护。IPsec 使用多种加密算法，如 DES、3DES、AES、MD5 和 SHA-1。IPsec 还使用多种认证算法，如 HMAC-MD5、HMAC-SHA-1 和 RSA。IPsec 的部署和管理通常通过 IKE（Internet Key Exchange）协议进行。

IPsec 隧道模式

IPsec 隧道模式（Tunneling）是一种将整个 IP 数据包封装在 IPsec 保护的数据包中的部署模式。在这种模式下，原始数据包的所有信息（包括源 IP 地址、目的 IP 地址和有效载荷）都被封装在 IPsec 保护的数据包中。接收方收到数据包后，会先验证其完整性，然后解密有效载荷，最后再验证其完整性。隧道模式通常用于保护整个网络流量，特别是在远程访问和站点到站点的连接中。隧道模式的优点是能够提供端到端的保护，缺点是会增加网络延迟和带宽消耗。

IPsec 传输模式

IPsec 传输模式（Transport）是一种只对数据包的有效载荷进行保护的部署模式。在这种模式下，只有数据包的有效载荷被封装在 IPsec 保护的数据包中，而源 IP 地址和目的 IP 地址保持不变。接收方收到数据包后，会先验证其完整性，然后解密有效载荷，最后再验证其完整性。传输模式通常用于保护特定的应用程序流量，特别是在局域网内的通信中。传输模式的优点是能够提供点对点的保护，缺点是只能保护特定的流量，而不能保护整个网络流量。

IPsec 隧道模式的部署

IPsec 隧道模式的部署通常涉及以下几个步骤：1. 配置 IPsec 隧道：在两端设备上配置 IPsec 隧道，包括指定源 IP 地址、目的 IP 地址和隧道名称。2. 配置加密和认证：在两端设备上配置加密算法和认证算法。3. 配置 IKE 协议：在两端设备上配置 IKE 协议，用于建立和管理 IPsec 隧道。4. 配置路由：在两端设备上配置路由，确保数据包能够通过隧道传输。

ike 协议

Internet Key Exchange (IKE) 协议是 IPsec 隧道模式部署的关键协议。它用于在两端设备之间建立和管理 IPsec 隧道。IKE 协议分为两个版本：IKEv1 和 IKEv2。IKEv1 是较早的版本，而 IKEv2 是较新的版本，提供了更多的功能和更好的性能。IKE 协议的主要功能是协商加密和认证参数，并建立 IPsec 隧道。IKE 协议还支持多种认证方式，包括预共享密钥（Pre shared keys）和数字证书。

IPsec 隧道模式的部署和管理通常通过 IKE 协议进行。

CEH 认证考试中的 IPsec 隧道模式部署和管理是重点内容。

[CEH 认证考试中的 IPsec 隧道模式部署和管理](#)

:□□□□ □□□□

□□□□□

:□□□□□□ □□□□□

13:15 - 05/06/1399

:□□□□□

□□□□□ - [CEH v10 □□□□□](#) - □□□□ □□□□ □□□ - [CEH □□□□ □□□□□□ □□□□□](#) - [CEH □□□□□□ □□□□□](#) - [CEH □□□□□](#)
□□□□□ □□□□□ □□□□ - □□□□□□ □□ - [CEH10 □□□□□□□](#)

□□□□□

<https://www.shabakeh-mag.com/security/17314/%D8%A2%D9%85%D9%88%D8%B2%D8%B4-c:eh-%D9%87%DA%A9%D8%B1-%DA%A9%D9%84%D8%A7%D9%87-%D8%B3%D9%81%DB%8C%D8%AF-%DA%86%DA%AF%D9%88%D9%86%D9%87-%DB%8C%DA%A9-%D8%B4%D8%A8%DA%A9%D9%87-%D8%AE%D8%B5%D9%88%D8%B5%DB%8C-%D8%B3%D8%A7%D8%B2%D9%85%D8%A7%D9%86%DB%8C-%D8%A7%DB%8C%D9%85%D9%86-%D9%BE%DB%8C%D8%A7%D8%AF%D9%87%E2%80%8C%D8%B3%D8%A7%D8%B2%DB%8C-%DA%A9%D9%86%DB%8C%D9%85%D8%9F>