Systems & Network Training

# Total IPsec for engineers

A 3 day Hands on training course

Save on expenses. This course is also available on your premises.

## Description

This hands on course focuses on IPsec VPNs. Rather than focusing on one implementation this course concentrates on the technologies and protocols of IPsec. Starting with an overview of the complete IPsec architecture the course then moves onto ESP packet analysis along with encryption and authentication provided. IKEv1 and IKEv2 are both covered in detail. Having covered IPsec with pre shared keys the course then moves onto IPsec with certificates followed by IPsec issues. The course is vendor neutral with hands on with both Cisco and Microsoft implementations.

## Key outcomes

By the end of the course delegates will be able to:

- ✔ Explain how IPsec works.
- ✔ Explain the role of AH, ESP and IKE.
- ✔ Configure IPsec.
- ✔ Troubleshoot IPsec.

## Training approach

This structured course uses Instructor Led Training to provide the best possible learning experience. Small class sizes ensure students benefit from our engaging and interactive style of teaching with delegates encouraged to ask questions throughout the course. Quizzes follow each major section allowing checking of learning. Hands on sessions are used throughout to allow delegates to consolidate their new skills.

## Details

**Who will benefit?**
Technical staff working with IPsec.

**Prerequisites**
Definitive IP VPNs for engineers.

**Duration:** 3 days

**Customer rating:** ★★★★★

| Generic training | Small class sizes | Hands On training | Our courseware | Customise your course |
|---|---|---|---|---|
| Generic training compliments product specific courses covering the complete picture of all relevant devices including the protocols "on the wire". | We limit our maximum class size to 8 delegates; often we have less than this. This ensures optimal interactivity between delegates and instructor. | The majority of our courses use hands on sessions to reinforce the theory. | We write our own courses; courseware does not just consist of slides and our slides are diagrams not bullet point text. | Please contact us if you would like a course to be customised to meet your specific requirements. Have the course your way. |
| "*Friendly environment with expert teaching that teaches the why before the how.*" G.C. Fasthosts | *"Excellent course. The small class size was a great benefit..."* M.B. IBM | *"Not many courses have practice added to it. Normally just the theoretical stuff is covered."* J.W. Vodafone | *"Comprehensive materials that made the course easy to follow and will be used as a reference point."* V.B. Rockwell Collins | *"I was very impressed by the combination of practical and theory. Very informative. Friendly approachable environment, lots of hands on."* S.R. Qinetiq |

# Total IPsec for engineers

## Course content

**What is IPsec?**

How to spell IPsec, IPsec is IP security, confidentiality, integrity, authenticity, replay protection, what is a VPN? Network layer security, IPsec and IPv4, IPsec and IPv6, the suite of protocols, the standard, IPsec RFCs, IPsec history. Hands on: Analysis of “normal” IP packets.

**IPsec architecture**

The IPsec protocols, AH vs ESP, Why two headers? transport mode, tunnel mode, Remote access VPNs, site to site VPNs, security associations, SA database, Security Parameters Index, implementations: Host tack, Bump in the Stack, Bump in the Wire. Hands on: Configuring IPsec.

**AH**

What AH does, the stack, The AH header, What is authenticated? Device authentication. AH in transport mode, AH in tunnel mode. Hands on: AH packet analysis.

**ESP**

What ESP does, the ESP header, ESP in transport mode, ESP in tunnel mode, ESP and SA, ESP and SPI. Hands on: ESP packet analysis, policy configuration.

**IPsec encryption**

IPsec is a framework, standard algorithms, ESP keys, the role of IKE, key lifetimes, how IKE generates the keys, DES, 3DES, AES, cipher block chaining, counter mode, other encryption. Hands on: Encryption configuration.

**IPsec authentication**

Authentication types, IPsec authentication, Authentication algorithms: MD5, keyed SHA-1, HMAC-MD5, HMAC-SHA-1, HMAC-RIPEMD, other authentication algorithms. Hands on: Authentication configuration.

**IKE**

Internet Key Exchange, IKE and the SAD, the two phase negotiation, ISAKMP, ISAKMP header, pre shared keys, digital signatures, public key encryption, Diffie Hellman, proposals, counter proposals, nonces, identities, phase 1 negotiation: main mode, aggressive mode, base mode. Phase 2 negotiation: quick mode, new group mode. Hands on: IKE packet analysis.

**More IKE**

PFS, IKE and dynamic addresses, XAUTH, hybrid authentication, CRACK, ULA, PIC. User level authentication. IKE renegotiation, heartbeats. Hands on: Troubleshooting IPsec.

**IKEv2**

The IKEv2 exchange, IKE_SA_INIT, IKE_AUTH, CREATE_CHILD_SA, IKEv2 packets, the informational exchange. Comparing IKev1 vs IKE v2. Hands on: IKEv2 configuration and analysis.

**PKI**

What is PKI?, Digital certificates, Certificate authorities, CA servers, RA, VA, certificates, CA hierarchy, CRLs, certificate formats. Hands on: installing and configuring certificate servers.

**IPsec issues**

NAT, IPsec overhead and fragmentation.

**Summary**

IPsec strengths and weaknesses. Where to get further information.