



Implementing Secure Converged Wide Area Networks (ISCW) v1.0

Associated Certifications : CCDP / CCNP
Duration : 5 days, Classroom

Prerequisites

- Introduction to Cisco Networking Technologies (INTRO)
- Interconnecting Cisco Network Devices (ICND)

Course Content

Learners will be able to secure and expand the reach of their enterprise network to teleworkers and remote sites. Focus is on securing remote access and VPN client configuration.

Course Objectives

After completing this course the student should be able to:

- Explain the Cisco hierarchical network model as it pertains to the WAN Describe and implement teleworker configuration and access
- Implement and verify frame mode MPLS
- Describe and configure a site-to-site IPSEC VPN
- Describe and configure Cisco EZVPN
- Explain the strategies used to mitigate network attacks
- Describe and configure Cisco device hardening
- Describe and configure IOS firewall features

Course Outline

- Describe Network Requirements
- Connect Teleworks
- Implement Frame Mode MPLS
- IPsec VPNs
- Cisco Device Hardening
- Cisco IOS Threat Defense Features

Who Should Attend

- Channel Partner / Reseller
- Customer
- Employee



642-825 ISCW: Implementing Secure Converged Wide Area Networks

Exam Number	: 642-825
Associated Certifications	: CCNP
Duration	: 90 minutes
Available Languages	: English
Register for Exam	: Pearson VUE

Exam Description

The Implementing Secure Converged Wide Area Networks (ISCW 642-825) is a qualifying exam for the Cisco Certified Network Professional CCNP®. The ISCW 642-825 exam will certify that the successful candidate has important knowledge and skills necessary to secure and expand the reach of an enterprise network to teleworkers and remote sites with focus on securing remote access and VPN client configuration. The exam covers topics on Cisco hierarchical network model as it pertains to the WAN, teleworker configuration and access, frame mode MPLS, site-to-site IPSEC VPN, Cisco EZVPN, strategies used to mitigate network attacks, Cisco device hardening and IOS firewall features.

Exam Topics

The following information provides general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. In order to better reflect the contents of the exam and for clarity purposes the guidelines below may change at any time without notice.

Implement basic teleworker services

- Describe Cable (HFC) technologies.
- Describe xDSL technologies.
- Configure ADSL (i.e., PPPoE or PPPoA).
- Verify basic teleworker configurations.

Implement Frame-Mode MPLS

- Describe the components and operation of Frame-Mode MPLS (e.g., packet-based MPLS VPNs).
- Configure and verify Frame-Mode MPLS.

Implement a site-to-site IPSec VPN

- Describe the components and operations of IPSec VPNs and GRE Tunnels.
- Configure a site-to-site IPSec VPN/GRE Tunnel with SDM (i.e., preshared key).
- Verify IPSec/GRE Tunnel configurations (i.e., IOS CLI configurations).
- Describe, configure, and verify VPN backup interfaces.
- Describe and configure Cisco Easy VPN solutions using SDM.

Describe network security strategies

- Describe and mitigate common network attacks (i.e., Reconnaissance, Access, and Denial of Service).
- Describe and mitigate Worm, Virus, and Trojan Horse attacks.
- Describe and mitigate application-layer attacks (e.g., management protocols).