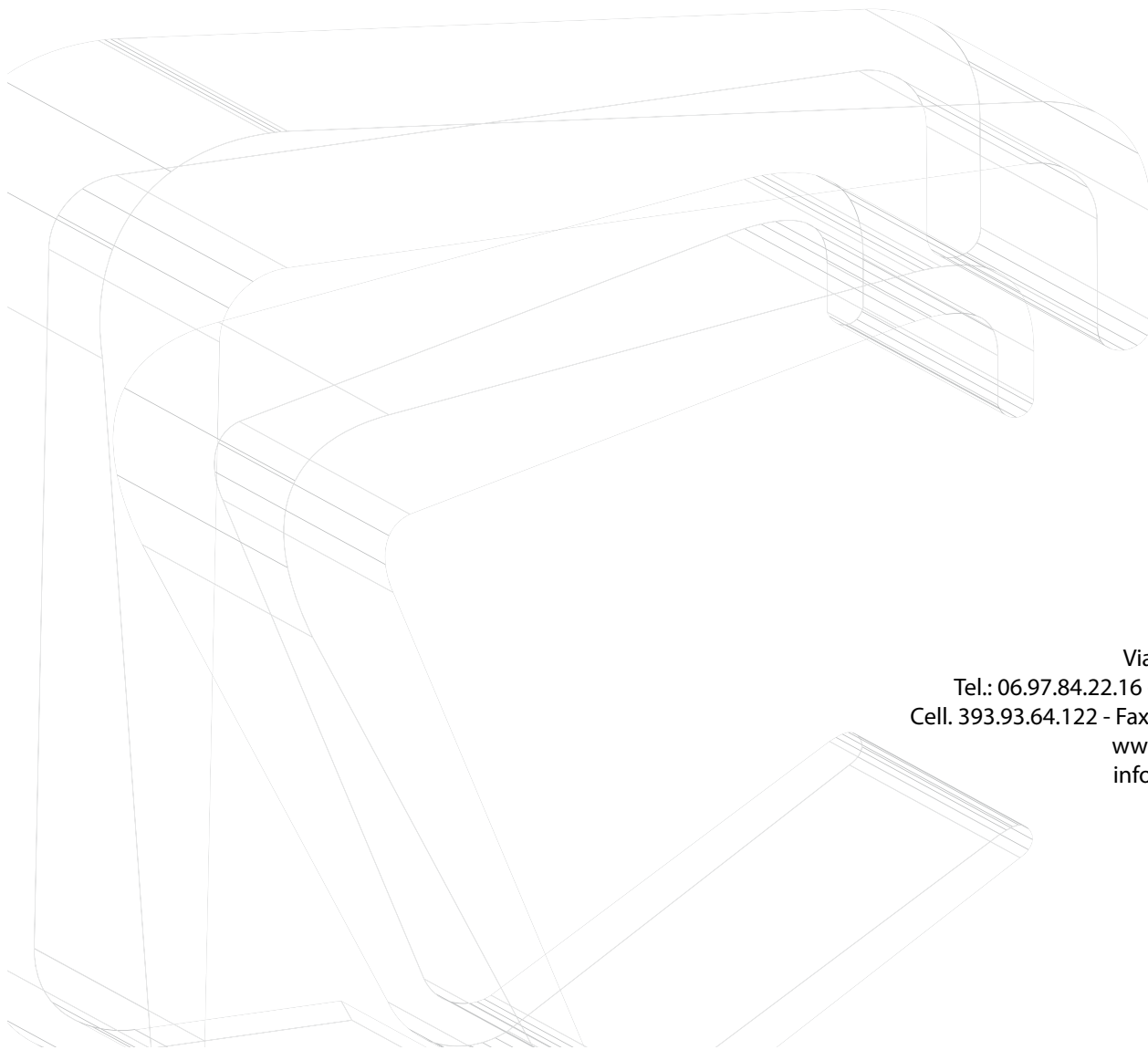




Programma corso Cisco CCNP - ISCW



PCAcademy  
Via Capodistria 12  
Tel.: 06.97.84.22.16 • 06.85.34.44.76  
Cell. 393.93.64.122 - Fax: 06.91.65.92.92  
[www.pcademy.it](http://www.pcademy.it)  
[info@pcacademy.it](mailto:info@pcacademy.it)

### **Informazioni generali**

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.

**Are e obiettivi per la certificazione CCNP**

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).

**Implement Cisco Device Hardening**

- :: Describe, Configure, and verify AutoSecure/One-Step Lockdown implementations (i.e., CLI and SDM).
- :: Describe, configure, and verify AAA for Cisco Routers.
- :: Describe and configure threat and attack mitigation using ACLs.
- :: Describe and configure IOS secure management features (e.g., SSH, SNMP, SY SLOG, NTP, Role-Based CLI, etc.)

**Implement Cisco IOS firewall**

- :: Describe the functions and operations of Cisco IOS Firewall (e.g., Stateful Firewall, CBAC, etc.).
- :: Configure Cisco IOS Firewall with SDM.
- :: Verify Cisco IOS Firewall configurations (i.e., IOS CLI configurations, SDM Monitor).

**Describe and configure Cisco IOS IPS**

- :: Describe the functions and operations of IDS and IPS systems (e.g., IDS/IPS signatures, IPS Alarms, etc.)
  - :: Configure Cisco IOS IPS using SDM
-