

Websense Certified Engineer

Web Security Professional Examination Specification

Introduction

This is an exam specification for the Websense Certified Engineer - Web Security Professional examination. The specification defines the test framework, content coverage of the examination, and the relevant background and experience needed to become a Websense Certified Engineer in Web Security at the Professional level.

Exam Purpose

This examination will certify that the successful candidate has the important knowledge, skills and competencies necessary to ensure the proper design, architecture, planning, installation and configuration of Websense Enterprise/Web Security Suite Software. In addition, a certified examinee will be able to implement and administer policy and reporting features related to identifying spyware, malicious mobile code, and phishing attacks, as well as bots and other network and security threats.

Audience

The examination is available to Websense sales engineers, customers, partners and others interested in becoming certified as a Websense Certified Engineer at a Professional level in the state-of-the-art technology of Websense Enterprise/Web Security Suite software solutions.

Candidate Background and Experience

Experience

Successful candidates for this certification should have extensive industry experience with information technologies and Web security, and must be knowledgeable about networking topologies, operating systems, system administration and enterprise database systems. It is recommended that candidates hold other certifications or completed training in one or more of the following areas but are not required.

Related certifications recommended in this field are:

Security

- Check Point CCSA/CCSE
- CISA (Certified Information Systems Auditor)
- CISSP (Certified Information Systems Security Professional)
- CompTIA Security+ and TICSIA Bootcamp

Networking

- CompTIA Network + Certification
- Networking Specialist Certificate
- Cisco CCNA/CCNP/CCIE

Operating System Certifications

- MCSA (Microsoft Certified Systems Administrator)
- MCSE (Microsoft Certified Systems Engineer)
- Linux certification
- Sun Solaris certification

Recommended Training

- Websense Certified Engineer - Web Security training
- Websense University
- Websense Webinars
- Websense tutorials
- Channel Booster Presentations
- Websense documentation, white papers, KnowledgeBase (KB) articles, and guides
- Other External security and network certification training
- Network Security Specialist training
- Security Management training
- Networking Specialist training

Background Education

Generally, highly successful candidates have undergraduate or graduate degrees in computer science, information security or software engineering but are not required to have these degrees.

Prerequisite Skills for Certification

A successful candidate:

- Can independently design, architect, plan, install and configure Websense Enterprise/Web Security Suite software, choosing the right model based on network topology and server configurations.
- Can apply policy controls to address primary network and application security issues.
- Can advise customers about Websense Enterprise/Web Security Suite software.
- Can analyze user needs and Web security requirements to determine feasibility of design implementation.

Examination Structure

The knowledge domains measured by this examination and the extent to which they are represented in the examination are shown in the table below.

Note: This examination blueprint includes weighting, test objectives, and example content. Enabling sub-skills are included to clarify the test objectives and should not be construed as a comprehensive listing of the examination content.

The table below lists the high level domains measured by this examination and the extent to which they are represented in the examination. These are the main activity areas of a Websense Certified Engineer with a Web Security Professional specialty.

Weighting for Exam Content Areas

Domain	Percent (%) of Examination
1.0 Architecture and Capabilities	5%
2.0 Pre-Deployment Planning	10%
3.0 Installation and Configuration	20%
4.0 Policy Configuration and Administration	25%
5.0 Reporting	20%
6.0 Troubleshooting	20%
Total	100%

Response Limits

The examinee selects, from three (3) or more response options, the option(s) that best completes the statement or answers the question. Distracters or wrong answers are response options that examinees with incomplete knowledge or skill would likely choose, but are generally plausible responses fitting into the content area defined by the test objective.

Test item formats used in this examination are:

Multiple-choice (single answer): The examinee selects one option that best answers the question or completes a statement.

Multiple-response (multiple answers): The examinee selects more than one option that best answers the question or completes a statement. The question will state how many options are correct, i.e.,– (Choose TWO).

Sample Directions: Read the statement or question and from the response options, select only the option(s) that represent the most correct or best answer(s) given the information provided.

Domain 1 - Architecture and Capabilities

This domain serves as the foundation and addresses general knowledge of Websense, Websense Enterprise/Web Security Suite software as well as the features and capabilities of the Websense Security Labs.

1.1. Recognize what makes Websense a leader in Intelligent Content Protection.

Enabling sub-skills:

- Websense Product Offerings and the value they bring to an organization
- Websense addresses issues with Web Security, Bandwidth, Productivity, and Legal Liability

1.2. Identify Websense Enterprise/Web Security Suite software Architecture.

Enabling sub-skills:

- Websense Services and purposes
- Websense Deployment options for multiple server environments
- Backend architecture and design required to enable Websense Components

1.3. Recognize the features and capabilities of Websense Security Labs and the Websense ThreatSeeker Web threat detection technology as well as Protection Services.

Enabling sub-skills:

- Identify Websense ThreatSeeker technology and how it delivers 0 day protection against 0 day exploits

1.4. Identify key capabilities of Websense Enterprise/Web Security Suite software and describe key features such as Reporting Tools.

Enabling sub-skills:

- Identify Websense Administration and configuration options
- Identify Websense reporting and capabilities
- Identify additional features & product add-ons for Websense Enterprise/Web Security Suite software.

1.5. Identify Websense Product Options.

Enabling sub-skills:

- Websense Security Filtering
- Websense Security Suite
- Websense CPM
- Websense Remote Filtering

Domain 1 Sample Item

On what platform(s) is the Websense User Service supported?

- a) Linux Only
- b) Solaris Only
- c) Windows Only
- d) Windows and Linux

Domain 2 - Pre-Deployment Planning

This domain addresses knowledge of core and secondary product features and proficiency to recognize how to assess, plan and install Websense Enterprise/Web Security Suite solutions.

2.1. Recognize core and secondary software components, features and benefits when planning the installation of Websense Enterprise/Web Security Suite software.

Enabling sub-skills:

- Identify purpose, features and functions of core components.
 - Filtering Service
 - Websense Manager
 - Websense Master database
 - Policy Server
 - User Service
 - Network Agent
- Identify purpose, features and functions of secondary components.
 - Real Time Analyzer (RTA)
 - Transparent ID (XID) Agents
 - Usage Monitor

2.2. Identify implications of installation and configuration with various integrations and Firewalls, Proxies, and VPNs to determine how they will affect the other functions of Websense Enterprise/Web Security Suite software.

2.3. Recognize Websense Security Labs Protection services, capabilities and features as it applies to planning deployment.

Enabling sub-skills:

- Websense BrandWatcher
- Websense ThreatWatcher
- Websense SiteWatcher
- WebCatcher

Domain 2 Sample Item

What component is the definitive source of configuration information within the Websense environment?

- a) Subscription key
- b) Websense Filtering Service
- c) Websense Policy Server
- d) Websense Master Database

Domain 3 - Installation and Configuration

This domain addresses the proficiency to successfully install and configure Websense Enterprise/Web Security Suite solutions.

3.1. Recognize how to properly execute an implementation plan for installing a Websense solution in complex network topologies.

Enabling sub-skills:

- Identify Operating System, Server and Hardware requirements
- Identify network topology
- Plan which components are necessary for a successful installation
- Verify components that communicate with the Policy Server

3.2. Recognize how to navigate the Websense Manager.

Enabling sub-skills:

- Navigation tree
- Policy Window
 - Yes Lists
 - Category Set
 - Protocol Set

3.3. Recognize how to configure Websense Server Settings.

Enabling sub-skills:

- Configuring Network Agent
- Customizing Block Pages
- Starting and Stopping Websense components

Domain 3 Sample Item

When using DC Agent for transparent authentication, where is the service required to be installed?

- a) On any operating system with connectivity to domain controllers that require to be polled.
- b) On the same server as the Websense User service, with secure communication to the domain controllers on port 40000.
- c) On a Windows 2000/2003 server with NetBios enabled between the DC Agent and Domain Controller.

Domain 4 – Policy Configuration and Administration

This domain covers the activity of configuring and administering Websense Enterprise/Web Security Suite software to enable Web traffic filtering and optimizing network performance and security.

4.1. Identify the important application areas to configure Web traffic.

Enabling sub-skills:

- Content Page
 - Policy Window
 - Category Set
 - Protocol Set
- Server Configuration
 - Category and Protocol Sets
 - Policy Timing
 - Network Agent
- Recognize how to start and stop components for all operating systems.
- Identify the three different methods for identifying users.
- Identify the various transparent identification (XID) agents available.
 - Websense DC Agent
 - Websense Logon Agent
 - Websense E-Directory Agent
 - Websense Radius Agent

4.2. Recognize how to create, apply and customize web filtering policies, classify Web traffic, and to apply optimum web security practices.

Enabling sub-skills:

- Create, modify and apply filtering structures (category and protocol sets)
- Identify, apply and customize basic and advanced filters
- Integrating with different directory services
- Identify when to apply Web traffic policies and know the available criteria
- Determine whether defined policies are working properly
- Tailor policies for certain people within organizations
- Apply policies to individual IP addresses or individuals
- Basic Regular Expressions

4.3. Identify Policy Types.

Enabling sub-skills:

- User
- IP
- Network
- Group
- Global and how these are applied in order
- Less Restrictive Blocking vs. More Restrictive blocking

Domain 4 Sample Item

To what file type can the contents of the audit log be exported?

- a) Text file
- b) PDF file
- c) HTML file

Domain 5 - Reporting

This domain covers Websense Enterprise/Web Security Suite reporting functions and activities.

5.1. Recognize how to properly use Websense Reporting Components.

Enabling sub-skills:

- Websense Log Server
- Websense Log Database
- Websense Reporting Tools Portal
- Access Web-based Reporting Tools using the Websense Reporting Tools.
 - Real Time Analyzer
 - Enterprise Explorer
 - Database Administration Tool

- Use Database Administration Tool to manage:
 - Database Partition Rollover Options
 - Internet Browse Time Configuration (IBT)
 - Full URL logging
 - Maintenance configuration
 - Database Partitions
 - Error Logs
 - MSDE differences
 - SQL requirements

- View and schedule favorite reports.
- Filter reports by users.

Domain 5 Sample Item

"Consolidation" decreases the size of your Log Database by combining internet requests that share what elements?

- a) Domain, Duration, Disposition
- b) Domain, Date/Time, Disposition
- c) Domain, Browse Time, Disposition
- d) Domain, Username/IP Address, Disposition

Domain 6 - Troubleshooting

This domain addresses how to utilize critical Websense troubleshooting utilities and techniques to determine causes of filtering problems, network communications and authentication issues.

6.1. Recognize how to properly use Websense Diagnostic Tools.

Enabling sub-skills:

- Identify when and how to use:
 - TestLogServer
 - WebsensePing
 - Block Page 'More Information'
 - ConsoleClient

6.2. Identify and recognize when and how to properly use Websense Component Service Debugging mode.

Enabling sub-skills:

- Network Agent
- User Service
- Log Server
- Websense Explorer
- Websense Real-Time Analyzer

6.3. Identify the important problems and issues and recognize when and how to use other diagnostic troubleshooting tools to determine the causes and resolve problems.

Enabling sub-skills:

- Use Errors logs.
 - Websense Log File
 - Windows Event Viewer
- Use 3rd Party Diagnostic Tools important for assisting in diagnostics
 - Ethereal/Wireshark
 - SysInternals -TCP View
 - SysInternals – FileMon
- Use other tools and utilities such as LDAP browsers.
- Use operating system commands such as:
 - telnet
 - ping
 - net view
 - netstat
 - net session (Used by DC Agent to pick up usernames on domain controllers)

6.4. Identify the important problems and issues in troubleshooting database downloads, (disk space, process) copying databases, and understanding licensing.

Domain 6 Sample Item

What file must be deleted after all configuration files are recovered from backup?

- a) config.xml
- b) eimserver.ini
- c) websense.ini
- d) config.xml.bak
- e) eimserver.ini.bak