

# JUTM-604 Junos Unified Threat Management (JUTM)

## Course Overview

This one-day course includes detailed coverage of Web filtering, antivirus (AV), antispam, and content filtering. Through demonstrations and hands-on labs, students will gain experience in configuring and monitoring the Unified Threat Management (UTM) features of the Junos operating system.

This course is based on the Junos OS Release 11.4R1.6.

## Objectives

After successfully completing this course, you should be able to:

- Describe the challenges that branch offices present to network managers.
- List the major features that UTM offers.
- Explain how each major feature addresses the challenges of the branch office.
- List the SRX Series Services Gateways hardware devices on which UTM is available.
- Describe the UTM features that require specific licenses.
- Define terms used in the creation of effective antispam UTM policies.
- Describe the process by which UTM examines traffic for spam.
- Describe the overall process of configuring an antispam UTM policy.
- Describe the kinds of information available from the device when it has detected spam.
- Describe how the AV process examines traffic.
- Describe the differences between full file-based AV versus express AV.
- Describe the settings that are required for configuring AV protection.
- Explain how these settings affect scanning performance and effectiveness.
- Describe options available for scanning supported protocols.
- List the general steps required to configure AV.
- Describe the statistical information available to verify AV functionality.
- Describe content and Web filtering and their purpose.
- List and describe each of the parameters used when configuring Web and content filtering.
- Describe in general terms the steps necessary to configure web and content filtering.
- Monitor Web and content filtering.

## Intended Audience

This course benefits individuals responsible for implementing and monitoring the UTM features available on branch SRX Services Gateways and J Series Services Routers.

## Course Level

JUTM is an intermediate-level course.

## Prerequisites

Students should have basic networking knowledge and an understanding of the Open Systems Interconnection (OSI) model and the TCP/IP protocol suite. Students should also have working knowledge of security policies. Students should also attend the *Introduction to the Junos Operating System (IJOS)*, *Junos Routing Essentials (JRE)*, and *Junos Security (JSEC)* courses prior to attending this class.

## Course Contents

### Chapter 1: Course Introduction

### Chapter 2: UTM Overview

- Branch Office Challenges
- UTM Feature Overview
- Design Basics
- Hardware Support

- Licensing of Features
- Lab 1: Connecting to the Lab Equipment and Testing Connectivity

**Chapter 3: Antispam**

- Antispam Terminology
- Overview of Antispam Process
- UTM Policy Overview
- Configuration Steps
- Monitoring Antispam
- Lab 2: Configuring an Antispam Policy

**Chapter 4: Full File-Based and Express Antivirus**

- Antivirus Terminology
- Overview of Antivirus Process
- AV Operation
- Full File-based AV Configuration
- Express AV Configuration
- Monitoring AV
- Lab 3: Antivirus Configuration and Testing

**Chapter 5: Content and Web Filtering**

- Overview and Terminology
- Configuration
- Verification and Monitoring
- Lab 4: Configuring Content and Web Filtering