

Citrix Application Firewall 8.0: Administration

700 Exam

Preparation Guide

Citrix Education

4.0

24 August 2009

Notice**NOTICE**

Citrix® Systems, Inc. (Citrix) makes no representations or warranties with respect to the content or use of this publication. Citrix specifically disclaims any expressed or implied warranties, merchantability or fitness for any particular purpose. Citrix reserves the right to make any changes in specifications and other information contained in this publication without prior notice and without obligation to notify any person or entity of such revisions or changes.

© Copyright 2007 Citrix Systems, Inc. All Rights Reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or information storage and retrieval systems, for any purpose other than the purchaser's personal use, without express written permission of:

Citrix Systems, Inc.
851 W. Cypress Creek Road
Ft. Lauderdale, FL 33309
<http://www.citrix.com>

Marks

The following marks are service marks, trademarks or registered trademarks of their respective owners in the United States and other countries.

Mark	Owner
Apache®	Apache Micro Peripherals, Inc.
DES™ Encryption	Practical Peripherals, Inc.
DSA™	Data Science Automation, Inc.
Access Gateway®, Application Firewall™, Citrix®, NetScaler®, NetScaler® Application Delivery Systems	Citrix Systems, Inc.
Java®, JavaScript®	Sun Microsystems, Inc.
PCI SM	PCI Security Standards Council, LLC
RSA™	RSA Security, Inc.
Windows®	Microsoft Corporation
PERL™	Yet Another Society
SafeWord®	Enigma Logic, Inc.
UNIX®	The Open Group

Disclaimer

This Exam Preparation Guide is designed to allow you to assess the types of questions that may be asked during the subject Citrix certification exam. Please be aware that your review of the content of this guide in no way ensures a passing score on the certification exam.

Author Alejandra Amador, Exam Developer

Item Development Team Alejandra Amador, Exam Developer, Citrix Systems
Patrick Quinlan, Experienced Courseware Developer, Citrix Systems
Meghan Myers, Courseware Developer, Citrix Systems
James Hsu, Vice-President, THConsultants Inc.

Subject Matter Experts Lena Yarovaya, Manager of Application Networking Group Engineering, Citrix Systems
Kit Wetzler, Product Manager, Citrix Systems
Arvind Bangari, Manager of World Wide Escalation Services, Citrix Systems
Rajiv Mirani, Director of Engineering, Citrix Systems
Ajay Kapase, Principal Product Marketing Manager, Citrix Systems
Guy Rosefelt, Manager of Application Firewall International Technical Operations, Citrix Systems

Table of Contents

1	The Exam	5
	1.1 Purpose of Exam	5
	1.2 Beta Testing an Exam	5
	1.3 Number of Questions	5
	1.4 Passing Score	5
	1.5 Time Limit	5
	1.6 Registration and Administration	6
	1.7 Registering with Pearson VUE	6
	1.8 Citrix Exam Policies	6
	1.9 Commenting During Live Exam	6
2	The Intended Audience	7
	2.1 Intended Audience	7
	2.2 Defining the Role Being Tested	7
3	Preparatory Recommendations for the Exam	8
	3.1 Introduction	8
	3.2 Recommended Knowledge and Skills	8
	3.3 Recommended Product Experience	8
	3.4 Recommended Course	8
4	Exam Sections and Weights	9
	4.1 Introduction	9
	4.2 Section Titles and Weights	9
	4.3 How Section Weights Relate to Questions on the Exam	9
5	Exam Objectives and Resources for the Exam	10
	5.1 Introduction	10
	5.2 Obtaining Hands-on Experience with Citrix Application Firewall 8.0	10
	5.3 Resources Used to Develop the Exam	10
	5.4 Exam Objectives	11
	5.5 How Objectives Relate to Questions on the Exam	14
6	Appendix: Practice	15

1 The Exam

1.1 Purpose of Exam This exam certifies that successful exam-takers have the knowledge and skills necessary to install, administer and support Citrix Application Firewall 8.0 implementations in an enterprise environment.

1.2 Beta Testing an Exam Once all the questions are developed for an exam, it is offered at no charge to individuals who have expressed interest in it.

The beta exam contains the complete pool of questions. Beta exam-takers take this exam and complete a survey regarding background experience with the exam's subject matter. A professional and credentialed Psychometrician analyzes the exams and surveys in order to determine which questions will be kept in the final version of the exam; the Psychometrician also determines the passing score and the timing for the exam.

After the analysis is complete and the passing score has been determined, if an exam-taker gets a passing score on the beta exam, their exam score will be posted and the exam-taker will not have to take the live exam for credit.

The Citrix Application Firewall 8.0: Administration (700) exam was beta-tested from 06/07 to 08/07.

If you are interested in participating in future beta exams, please e-mail us at training@citrix.com to be added to the beta exam mailing list.

1.3 Number of Questions The 700 exam is a 58-question exam written in English.

1.4 Passing Score The passing score for this exam is 55%.

The passing score for CCIs in this exam is 66%.

The passing score is based on a statistical analysis of beta exam scores. The beta exam participants answered a survey that helped determine their skill level with the product. Their skill level and their score, as a group, are analyzed to determine the final passing score.

1.5 Time Limit The timing for each exam is determined by a statistical analysis that compares the time of all beta exam-takers with that of those who passed the beta exam.

Native English speakers have 90 minutes to complete the exam. Non-native English speakers who take the exam in English have 120 minutes to complete the exam.

If a non-native English speaker wishes to have the time extension when registering for the exam in English, they must ask for it; it will not be given as a default. Exam takers should verify the specific policies with the test provider they choose.

1.6 Registration and Administration

This exam is administered through Pearson VUE. For details on the rules and procedures associated with registering for and taking the exam, please visit the Exams section of www.CitrixEducation.com.

1.7 Registering with Pearson VUE

In the United States and Canada, call 1-800-931-4084. Worldwide, visit the Pearson VUE website (www.VUE.com) to locate a testing center in your area and register for an exam with Pearson VUE.

1.8 Citrix Exam Policies

If an exam-taker fails an exam, they must wait 24 hours to register for a second attempt of any Citrix exam and 14 days after a second attempt to register for a third or any subsequent attempt of any Citrix exam.

Each beta exam can only be taken once.

Citrix Education monitors retake activity for breaches of this policy. Breach of this policy can result in sanctions up to and including temporary ban from taking Citrix exams and/or decertification.

1.9 Commenting During Live Exam

Citrix Education is committed to continually monitoring and updating our exams as needed. As a practice, Citrix Education regularly reviews and refreshes exams and exam items even after the beta exam period is over. Comments made by exam takers during beta and live exams are used as anecdotal feedback and considered when making decisions about the exam and specific exam questions.

2 The Intended Audience

2.1 Intended Audience

The 700 exam is a rigorous examination of subjects that are critical to an administrator's role as defined by Citrix Systems' subject matter experts (SMEs). This role includes, but is not limited to:

- Network Administrators/Engineers
 - Web Security Administrators/Engineers
 - Access Partners
 - Web Application Developers
-

2.2 Defining the Role Being Tested

The intended audience is determined by subject matter experts (SMEs) for the product through a Job Task Analysis (JTA) procedure. The SMEs defined the exam audience by discussing which job functions require use of the Citrix Application Firewall product.

3 Preparatory Recommendations for the Exam

3.1 Introduction

It is recommended that exam-takers have the knowledge, skills and abilities necessary to install, administer and support Citrix Application Firewall 8.0 prior to taking this exam.

3.2 Recommended Knowledge and Skills

Exam-takers should have the following knowledge and skills prior to taking this exam:

- Basic network administration skills, including knowledge of:
 - Network Operating Systems
 - Network Protocols
 - Internet Software
 - Network Management
 - Network Monitoring
 - Load Balancing
 - Encryption
 - Data Compression
 - Basic knowledge of UNIX
 - Basic understanding of network security
 - Basic understanding of NetScaler Application Accelerator
 - Thorough knowledge of network and communication protocols specifically TCP and HTTP
 - Previous knowledge of the Citrix NetScaler
-

3.3 Recommended Product Experience

It is recommended that exam-takers have at least six to eight (6-8) months of experience with the product, Citrix Application Firewall 8.0

3.4 Recommended Course

It is also recommended that exam-takers attend or self-study the CTX-1734AI Citrix Application Firewall 8.0: Basic Operations and Administration course.

4 Exam Sections and Weights

4.1 Introduction

The Citrix Application Firewall 8.0: Administration exam (700) is divided into five (5) sections. Each section of the exam is weighted as follows, totaling 100%.

4.2 Section Titles and Weights

Sections	Weight
Pre-deployment Planning	24%
Configuring Initial Settings	10%
Creating a Profile	47%
Creating and Configuring Initial Policies	10%
Administering the Application Firewall	9%
Total	100%

4.3 How Section Weights Relate to Questions on the Exam

Section Weights correlate directly to the number of questions on the exam. For example, if an exam has 60 questions, and Section 1 is weighted as 50%, then 30 of the questions on the exam will relate to Section 1. ($60 * 50\% = 30$).

Section weights are NOT used to calculate an exam-taker's score. Section weights are meant to give exam-takers an idea of the percentage of coverage on certain content. Because some questions may have different point values assigned to them, section weights and exam scores do not always have a one-to-one correlation.

5 Exam Objectives and Resources for the Exam

5.1 Introduction

The questions for the exam were developed directly from the exam objectives. The exam objectives are used to test exam-takers' knowledge, skills and abilities related to each section of the exam.

Some of the exam objectives will correspond, or map, to field experience. Exam-takers are expected to have at least six to eight months of experience with Citrix implementations of Citrix Application Firewall 8.0 to increase their likelihood of passing this exam.

For optimal performance on this exam, Citrix recommends that exam-takers attend the CTX-1734AI Citrix Application Firewall 8.0: Basic Operations and Administration course and obtain field experience.

5.2 Obtaining Hands-on Experience with Citrix Application Firewall 8.0

Exam-takers can get hands-on experience by attending the CTX-1734AI Citrix Application Firewall 8.0: Basic Operations and Administration course.

5.3 Resources Used to Develop the Exam

The following resources were used to develop this exam:

Resource	How to Obtain
Citrix Application Firewall 8.0 Administrator's Guide	Available with the purchase of the Citrix Application Firewall 8.0 module on the Citrix NetScaler 8.0 appliance
CTX-1734AI Citrix Application Firewall 8.0: Basic Operations and Administration	This course is available at Citrix Authorized Learning Centers (CALCs) worldwide. To find the CALC nearest you, please visit the http://www.citrix.com/English/SS/education/feature.asp?contentID=24019&ntref=edu_training .
Citrix NetScaler 8.0 Administrator's Guide	Available with the purchase of the Citrix NetScaler 8.0 appliance

5.4 Exam Objectives

For each exam objective, the chart below lists the corresponding Citrix course and/or available technical publications.

For all sections, at least six to eight months of experience administering a Citrix Application Firewall 8.0 implementation is recommended.

Section	Objectives	Citrix Course and/or Technical Publication
Pre-deployment Planning	<ul style="list-style-type: none"> • Identify how the positive security model works in relation to Citrix Application Firewall. • Based on a description of the environment which includes relevant information about capacity and data details, determine the amount and content type of the data passing through the Application Firewall. • Based on a scenario about capacity planning or stated requirements, determine whether the application firewall appliances should be deployed integrated or as stand-alone. • Given a description of an enterprise environment and/or a network diagram, determine the appropriate placement of Application Firewall appliance(s) in the network. • Given a description of the corporate security policy or a set of requirements, decide the SSL termination point. • Given a description of a web application, decide which parts of the application can access 	<ul style="list-style-type: none"> • Citrix Application Firewall 8.0 Administrator's Guide • CTX-1734AI Citrix Application Firewall 8.0: Operations and Administration • Citrix NetScaler 8.0 Administrator's Guide • Field Experience

	<p>sensitive data.</p> <ul style="list-style-type: none"> • Given a scenario or a description of a web application, decide how many profiles will be needed for optimal configuration and flexibility. • Given a description of the network or a network diagram, determine the appropriate network configuration of the devices for proper functionality. 	
Configuring Initial Settings	<ul style="list-style-type: none"> • Given requirements for Application Firewall appliances and web servers, select the correct step(s) to create servers and/or configure service by name based services and type and/or create vserver. • Given a scenario describing whether a certificate is self-signed or requiring signature via Certificate Authority, select the correct step(s) to create and upload SSL certificates. • Based on a description of how the Application Firewall will be deployed, decide the type of vserver deployment needed. • Based on the needs of a described environment, determine how the session cookie name and/or session timeout value should be set. 	<ul style="list-style-type: none"> • Citrix Application Firewall 8.0 Administrator's Guide • CTX-1734AI Citrix Application Firewall 8.0: Basic Operations and Administration • Citrix NetScaler Administrator's Guide • Field Experience
Creating a Profile	<ul style="list-style-type: none"> • Given a profile on the Application Firewall appliance determine which 	<ul style="list-style-type: none"> • CTX-1734AI Citrix Application Firewall 8.0: Basic

	<p>RegEx would meet the stated requirement or given a RegEx, determine which (URL/Requests) would be allowed.</p> <ul style="list-style-type: none"> • Based on security, fail-over and/or performance requirements, determine whether to add a basic or advanced profile to an Application Firewall deployment. • Given a protection or combination of protections, determine the risk(s) of not using the protection(s) or mis-configuring the protection(s) • Based on a scenario and/or requirements, select the protection(s) and/or configuration settings to meet the needs of the environment • Based on a scenario and/or a screenshot, decide which learned suggestions for relaxation to implement and/or whether or not the suggestion should be modified or not • Given a configuration (which includes protections and their actions/settings), determine how the Application Firewall affects the web application. 	<p>Operations and Administration</p>
<p>Creating and Configuring Initial Policies</p>	<ul style="list-style-type: none"> • Based on a described environment and/or described applications, determine whether or not traffic needs to be protected. 	<ul style="list-style-type: none"> • CTX-1734AI Citrix Application Firewall 8.0: Basic Operations and Administration • Field experience

	<ul style="list-style-type: none"> • Based on the traffic that should go to a profile, determine which policy is appropriate (using named expressions or policy engine). 	
Administering the Application Firewall	<ul style="list-style-type: none"> • Given a description of a log or a screen shot of a log, identify the protection and profile being logged and/or if it is set to block. • Based on a scenario including the security policy and a description of logs or a screenshot of a log for a protection, determine whether to configure a protection or modify a configuration. 	<ul style="list-style-type: none"> • CTX-1734AI Citrix Application Firewall 8.0: Basic Operations and Administration

5.5 How Objectives Relate to Questions on the Exam

All questions in a Citrix exam are based on objectives. Exam Developers and SMEs developed objectives based on the Job Task Analysis, which identified tasks related to performing the job of administrator using the Citrix Application Firewall 8.0. SMEs defined the key activities required to successfully administer the Application Firewall. This definition ensures that the test content is proportional to actual job requirements and describes what the test is designed to measure.

6 Appendix: Practice

Question 1

Scenario: A banking institution just purchased a stand-alone Citrix Application Firewall system to increase security of the online banking functions. To comply with industry regulations, all the traffic coming from and going to the web servers of the bank must be encrypted. An administrator has already created the necessary certificate and key pair.

Which three specific entities must the administrator create for this scenario? (Choose three.)

- A. A vserver of type SSL for the web servers
- B. Servers that point to the back-end web server
- C. Services of type SSL associated with the web server
- D. Services of type HTTP associated with the web server
- E. Services of type SSL bridged associated with the web server

Answers: A, B and C

Question 2

Scenario: On the ordering page of a company's web site, there is a field for entering Canadian postal codes, which always follow this format: Letter Number Letter Space Number Letter Number. For example: B1Y 3X7.

How many of these regular expressions will match this pattern?

- `^[0-9a-zA-Z]{3}.[0-9a-zA-z]{3}$`
- `^[0-9][a-zA-Z][0-9] [0-9][a-zA-Z][0-9]$`
- `^[a-zA-Z][0-9][a-zA-Z] [0-9][a-zA-Z][0-9]$`
- `^{alphanumeric} {alphanumeric}$`

- A. One
- B. Two
- C. Three
- D. Four

Answer: C

Question 3

Scenario: A web application displays images of a company's products as well as text describing the products. The web site also contains an online survey that customers can complete to provide feedback. The feedback is e-mailed to the designated marketing employee who then analyzes the responses and enters them into a Microsoft SQL database.

Which profile types should an administrator configure for this web site?

- A. A basic profile for all the pages
- B. An advanced profile for all the pages
- C. A basic profile for the pages containing only text and images and an advanced profile for the feedback page
- D. A basic profile for the pages containing only text and an advanced profile for the feedback page and pages containing images

Answer: A

Question 4

Which Citrix Application Firewall protection guards against a hacker gaining access to another user's account by modifying a cookie on a web application and sending it to the web server?

- A. Field Formats
- B. Sessionization
- C. Cookie Consistency
- D. Form Field Consistency

Answer: C

Question 5

Scenario: The administrator is using an Application Firewall with a start URL configured for the index page. The environment has a web site, www.site.com, with the page index.htm. There is a link on the index page to contact.htm and register.htm. Clicking the submit button in the form on the register.htm page takes the user to login/index.com. The error page is set to blocked.htm. Users need to be able to bookmark and go directly to http://www.site.com/login/index.htm.

What must the administrator configure to meet the needs of this environment?

- A. URL closure for http://www.site.com/login/index.htm
- B. Sessionization for http://www.site.com/login/index.htm URL
- C. The start URL check to include http://www.site.com/login/index.htm
- D. The deny URL check to include http://www.site.com/login/index.htm

Answer: C

Question 6

Scenario: A company hires a new administrator and tasks the administrator with deploying a Citrix Application Firewall in the company's network environment. Since the administrator is new to the company and does not know much about the web traffic that will be passing through the Application Firewall for a specific web application, the administrator decides to configure a basic profile and plans to review the information from the Application Firewall to modify the protections as needed.

For which two protections can the administrator configure learning? (Choose two.)

- A. Deny URL
- B. Field Formats
- C. Buffer Overflow
- D. Cross-Site Scripting

Answers: B and D

Question 7

Scenario: An administrator recently deployed a Citrix Application Firewall to protect against malicious attacks such as cross-site scripting to the web servers and to users on the site. The administrator wants to prevent users from entering potentially harmful code into fields that request information such as phone numbers, emails and user names.

The administrator is now reviewing a Syslog to determine if the current settings of the Application Firewall profile for a web application are appropriate. Since deploying the Application Firewall, the web application has not had any more successful cross-site scripting attacks. The web application allows users to post blogs and images and contains Javascript in HTML comments. The company requires that web traffic be dropped only when absolutely necessary for security.

The administrator saw these errors in the Syslog:

```
Field format check failed for field email notAnEmailAddress
Cross-site script check failed for
comments=<script>alert('Hello')</script><blocked>
Field format check failed for field phone notAPhoneNumber
Cross-site script check failed for comments=(script>alert('Smile')</script><blocked>
```

Should the administrator modify the current profile configurations, and if so, how?

- A. No, the current settings are appropriately blocking attacks.
- B. No, the learning feature will modify the settings as necessary.
- C. Yes, the administrator should enable HTML comment stripping.
- D. Yes, the administrator should deselect block and select transform on the Cross-Site Script check

Answer: D

Question 8

An administrator wants to ensure that .JHTML files are inspected by a particular profile.

Which two qualifier and operator pairs should an administrator use in an expression to include .JHTML files? (Choose two.)

- A. URL !=
- B. URL ==
- C. URL CONTAINS
- D. URL NOTCONTAINS

Answers: B and C

Question 9

Scenario: An IT Administrator at a bank has configured an Application Firewall profile to protect the web site of the bank and user account information. Bank executives previewed the new protections and were concerned that customers might become anxious if they see a page with their information begin to load and stop loading midway through.

In which way can the administrator set the SAFE Object check to prevent this from happening while still protecting the user information?

- A. x-out
- B. block
- C. transform
- D. Set the Safe Commerce check to x-out
- E. Set the Safe Commerce check to transform

Answer: A
