Citrix ADC 12.x Advanced Concepts – Secure Web Applications

Certification: None | **Course Length:** 3 Days | **Instructional Method:** Classroom or Virtual w/ hands-on labs

Course overview

Citrix Web App Firewall protects web apps and sites from known and unknown attacks. This three-day course will teach you how to address application services security requirements with Web App Firewall. After studying Citrix Web App Firewall, you'll learn about many different types of web attacks and vulnerabilities, such as SQL injection and cookie tampering, and how to protect against them. The course also covers policies, profiles and expressions; monitoring, management and reporting; and troubleshooting techniques. Highlighted features include the Adaptive Learning Engine and Secure Insight. This advanced course is designed for IT professionals with previous Citrix Networking experience.

What you'll learn

- Identify common web attacks and vulnerabilities
- Understand PERL compatible regular expressions
- Understand how to operate the adaptive learning engine
- Configure Citrix Web App Firewall to protect web applications
- Utilize Citrix ADC Secure Insight to monitor, manage, and report on Application Services security
- Troubleshoot Citrix Web App Firewall

Versions covered

This course is currently on Citrix ADC version 12.x, but is still applicable for learners of previous versions of the product.

Prereq. knowledge

Citrix recommends students prepare for this course by taking the following course/courses: **CNS-220** Citrix ADC 12.x Essentials and Traffic Management, or **CNS-222** Citrix ADC 12.x Essentials and Citrix Gateway.

Is this course for me?

Designed for students with previous Citrix Networking experience, this course is best suited for individuals who will be deploying and/or managing Citrix Web App Firewall in Citrix Networking environments.

Learning Path

1. **CNS-220** Citrix ADC 12.x Essentials and Traffic Management
   OR
   CNS-222 Citrix ADC 12.x Essentials and Citrix Gateway
2. **CNS-318** Citrix ADC 12.x Advanced Concepts – Secure Web Applications
3. **CNS-420** Citrix Networking Assessment, Design, and Advanced Configuration

Citrix ADC 12.x Advanced Concepts – Secure Web Applications

Module 1: Citrix Web App Firewall Overview

- The Business Problem
- Industry Standards
- Protection Methodologies
- Introducing Citrix Web App Firewall

Module 2: Citrix Web App Firewall Profiles and Policies

- Citrix Web App Firewall Policies
- Citrix Web App Firewall Profiles
- Citrix Web App Firewall Learning
- Citrix Web App Firewall Engine Settings

Module 3: Implementing Citrix Web App Firewall Protections

- Security Checks and Data Flow
- Rules and Adaptive Learning
- Signatures and Comment Stripping
- Top-Level Protections

Module 4: Additional Citrix Web App Firewall Protections

- Cookie Consistency
- Advanced Form Protection Checks
- URL Protections
- Protecting Sensitive Data

Module 5: Monitoring and Troubleshooting Citrix Web App Firewall

- Web App Firewall and Web Applications
- Logging and Reporting
- Customizing Errors
- Troubleshooting

Module 6: Security and Filtering

- Application level Quality of Experience (AppQoE)
- IP Reputation
- Rate Limiting
- HTTP Callout

Module 7: Authentication with Security Assertion Markup Language (SAML)

- What is SAML?
- Configuring SAML on Citrix ADC

Module 8: Authentication with OAuth, OpenID, and nFactor

- OAuth and OpenID
- Configuring OAuth on Citrix ADC
- Multi-Factor Authentication with nFactor
- Configuring nFactor