Exam Code: 1Y0-341

Exam A

QUESTION 1
Scenario: A Citrix Engineer is reviewing the Citrix Web App Firewall log files using the GUI. Upon further analysis, the engineer notices that legitimate application traffic is being blocked.
What can the engineer do to allow the traffic to pass through while maintaining security?

A. Note the protection blocking the traffic in the log entry. Edit the profile and deselect the Block action for the protection.

B. Select the check box in the log entry. Choose Dismiss to allow the traffic to pass through from the Action menu.

C. Note the protection blocking the traffic in the log entry. Create a new profile and policy and bind it with a larger priority number.

D. Select the check box in the log entry. Choose Edit & Deploy to create a relaxation rule from the Action menu.

Correct Answer: A
Section:

QUESTION 2
Scenario: A Citrix Engineer is asked to implement multi-factor authentication for Citrix Gateway. The engineer creates the authentication policies and binds the policies to the appropriate bind points. The engineer creates a custom form using Notepad++ to format the page which will capture the user's credentials.
What is the first step the engineer must perform to assign this form to the authentication process?

A. Create a login schema policy and bind it to the authentication virtual server.

B. Bind the authentication policy to the primary authentication bank of the Citrix Gateway

C. Create a login schema profile and select the uploaded file.

D. Create an authentication policy label and bind it to an authentication policy.

Correct Answer: D
Section:

QUESTION 3
What should a Citrix Engineer do when using the Learn feature for Start URL relaxation?

A. Ensure that only valid or correct traffic is directed to the protected web application while in Learn mode.

B. Invite at least 10 test users to collect sufficient data for the Learn feature.

C. Create a Web App Firewall policy that blocks unwanted traffic.

D. Ensure that the /var file system has at least 10 MB free.

Correct Answer: A
Section:

QUESTION 4
Scenario: A Citrix Engineer notices that a web page takes a long time to display. Upon further investigation, the engineer determines that the requested page consists of a table of high-resolution pictures which are being displayed in table cells measuring 320 by 180 pixels.
Which Front End Optimization technique can the engineer enable on the Citrix ADC to improve time to display? A.
Shrink to Attributes

A. Make Inline

B. Extend Page Cache

C. Minify

Correct Answer: D
Section:
Explanation:
Reference: https://docs.citrix.com/en-us/netscaler/11-1/optimization/front-end-optimization.html

QUESTION 5
A Web Application Engineer is reviewing log files and finds that a large number of bad HTTP requests are being sent to the web application servers.
What can the Citrix ADC Engineer to do prevent bad HTTP requests from getting to the web application?

A. Create an HTTP profile and select 'Drop invalid HTTP requests'.Assign the HTTP profile to the virtual server.

B. Create an HTTP profile and select 'Drop invalid HTTP requests'.Assign the HTTP profile to the Web App Firewall policy.

C. Modify the default HTTP profile and select 'Drop invalid HTTP requests'.Bind the default HTTP profile globally.

D. Select 'Change HTTP Parameters' under System > Settings.Select 'Drop invalid HTTP requests'.

Correct Answer: D
Section:
Explanation:
Reference: https://support.citrix.com/article/CTX121149

QUESTION 6
Which syntax is used to write a StyleBook?

A. JSON

B. LISP

C. YAML

D. XML

Correct Answer: C
Section:
Explanation:
Reference: https://docs.citrix.com/en-us/citrix-application-delivery-management-service/stylebooks.html

QUESTION 7
Scenario: A Citrix Engineer wants to protect a web application using Citrix Web App Firewall. After the Web App Firewall policy afweb_protect is bound to the virtual server, the engineer notices that pages are displaying in plain text with graphics included.
What is the likely cause of this?

A. The Safe Objects protection is NOT properly configured.

B. The Start URL list does NOT include CSS files.

C. The Web App Firewall feature is disabled.

D. The policy expression allows for HTML files only.

Correct Answer: B
Section:

QUESTION 8
Which two protections ensure that the correct data is returned by the client?
(Choose two.)

A. Form Field Consistency.

B. Field Formats

C. HTML Cross-Site Scripting (XSS)

D. Cross-Site Request Forgeries (CSRF)

Correct Answer: A, D
Section:
Explanation:
Reference: https://docs.citrix.com/en-us/citrix-adc/citrix-adc-secure-deployment/secure-deployment-guide.html

QUESTION 9
Scenario: A Citrix Engineer is asked to implement multi-factor authentication for Citrix Gateway. The engineer creates the authentication policies and binds the policies to the appropriate bind points. The engineer creates a custom form using Notepad++ to format the page which will capture the user's credentials.
To which folder on the Citrix ADC will the engineer need to upload this form?

A. /flash/nsconfig/loginschema/LoginSchema

B. /var/netscaler

C. /flash/nsconfig/loginschema

D. /var

Correct Answer: A
Section:
Explanation:
Reference: https://docs.citrix.com/en-us/citrix-adc/current-release/system/authentication-and-authorization-for-system-user/two-factor-authentication-for-system-users-and-external-users.html

QUESTION 10
Scenario: A Citrix Engineer used Learning to establish the HTML SQL Injection relaxations for a critical web application. The engineer now wishes to begin working on the protections for a different web application. The name of the Web App Profile is appfw_prof_customercare.
Which CLI command can the engineer use to empty the Learn database?

A. set appfw learningsettings appfw_prof_customercare -SQLInjectionMinThreshold 0

B. set appfw learningsettings appfw_prof_customercare -startURLMinThreshold 0

C. reset appfw learningdata

D. export appfw learningdata appfw_prof_customercare

Correct Answer: C
Section:

QUESTION 11
Which Citrix Application Delivery Management (ADM) Analytics page allows a Citrix Engineer to monitor web application traffic?

A. Web Insight
B. WAN Insight
C. HDX Insight
D. Gateway Insight

Correct Answer: C
Section:
Explanation:
Reference: https://docs.citrix.com/en-us/citrix-application-delivery-management-service/analytics/hdx-insight.html

QUESTION 12
Which report can a Citrix Engineer review to ensure that the Citrix ADC meets all PCI-DSS requirements.

A. Generate Application Firewall Configuration

B. PCI-DSS Standards

C. Application Firewall Violations Summary

D. Generate PCI-DSS

Correct Answer: D
Section:
Explanation:
Reference: https://docs.citrix.com/en-us/citrix-adc/current-release/application-firewall/stats-and-reports.html

QUESTION 13
Scenario: A Citrix Engineer manages Citrix Application Delivery Management (ADM) for a large holding company. Each division maintains its own ADC appliances. The engineer wants to make Citrix ADM features and benefits available to each group independently.
What can the engineer create for each division to achieve this?

A. A site

B. A role

C. A tenant

D. A dashboard

E. A group

Correct Answer: A
Section:

QUESTION 14
Scenario: During application troubleshooting, a Citrix Engineer notices that response traffic received from a protected web application is NOT matching what the web server is sending out. The engineer is concerned that someone is trying to disrupt caching behavior.
Which action is the Citrix Web App Firewall performing that would trigger this false positive?

A. Removing the Last-Modified header

B. Inserting a hidden form field

C. Removing the Accept-Encoding header

D. Modifying and adding cookies in the response

Correct Answer: C
Section:

QUESTION 15
Scenario: A Citrix Engineer configures Citrix Web App Firewall to protect an application. Users report that they are NOT able to log on. The engineer enables a Start URL relaxation for the path //login.aspx.
What is the effect of the Start URL relaxation on the application?

A. Access to the path /login.aspx is unblocked.

B. Access to the path /login.aspx is blocked.

C. External users are blocked from the path /login.aspx.Internal users are permitted to the path /login.aspx.

D. Non-administrative users are blocked from the path /login.aspxAdministrative users are permitted to the path /login.aspx.

Correct Answer: A
Section:

QUESTION 16
Which setting in the Cookie Consistency protection feature does a Citrix Engineer need to configure to ensure that all a cookie is sent using TLS only?

A. Encrypt Server Cookies > Encrypt All

B. Flags to Add in Cookies > Secure

C. Encrypt Server Cookies > Encrypt Session Only

D. Proxy Server Cookies > Session Only

Correct Answer: B
Section:
Explanation:
Reference: https://docs.citrix.com/en-us/citrix-adc/current-release/application-firewall/cookie-protection/cookie-consistency-check.html

QUESTION 17
Which security model should a Citrix Engineer implement to make sure that no known attack patterns pass through Citrix Web App Firewall?

A. Hybrid

B. Static

C. Positive

D. Negative

Correct Answer: A
Section:
Explanation:
Reference: https://docs.citrix.com/en-us/citrix-adc/current-release/application-firewall/introduction-to-citrix-web-app-firewall.html

QUESTION 18
Scenario: A Citrix Engineer has configured Integrated Caching to improve application performance. Within hours, the Citrix ADC appliance has run out of memory.
Which Content Group setting can the engineer configure to show the caching process until a need is demonstrated?

A. Maximum memory usage limit

B. Quick Abort Size

C. Do not cache – if hits are less than

D. Do not cache – if size exceeds

Correct Answer: A
Section:
Explanation:
Reference: https://docs.citrix.com/en-us/citrix-adc/current-release/optimization/integrated-caching.html

QUESTION 19
A Citrix Engineer reviews the App Dashboard and notices that three of the monitored applications have an App Score of less than 50.
The engineer can interpret the App Score as a metric of application _____. (Choose the correct option to complete the sentence.)

A. security, with a lower score indicating better security

B. performance and availability, with a higher score indicating better health

C. performance and availability, with a lower score indicating better health

D. security, with a higher score indicating better security

Correct Answer: B
Section:

QUESTION 20
Which Front End Optimization technique causes the Citrix ADC to resize images before sending them to the client?

A. Minify

B. Shrink to Attributes

C. Compression

D. Inlining

Correct Answer: B
Section:
Explanation:
Reference: https://docs.citrix.com/en-us/citrix-adc/current-release/optimization/front-end-optimization.html

QUESTION 21
A review of purchases made at an online retailer shows that several orders were processed for items at an unpublished price.
Which protection can a Citrix Engineer implement to prevent a site visitor from modifying the unit price of a product on the shopping cart page?

A. Cross-Site Request Forgeries (CSRF)

B. Form Field Consistency

C. HTML Cross-Site Scripting (XSS)

D. HTML SQL Injection

Correct Answer: B
Section:

QUESTION 22
Scenario: A Citrix Engineer configures Citrix Web App Firewall to protect an application. Upon reviewing the log files, the engineer notices a pattern of forceful browsing toward the configuration page for the application. To protect against this, the engineer enforces Start URL and enables Enforce URL Closure.
What is the effect of enforcing Start URL and enabling Enforce URL Closure on the application?

A. Access to the path /config.aspx is unblocked when a user clicks a referring link elsewhere on the website.

B. Non-administrative users are blocked from the path /config.aspx.Administrative users are permitted to the path /config.aspx.

C. External users are blocked from the path /config.aspx.Internal users are permitted to the path /config.aspx. D. Access to the path /config.aspx is blocked.

Correct Answer: D
Section:

QUESTION 23
A Citrix Engineer needs to set up access to an internal application for external partners.
Which two entities must the engineer configure on the Citrix ADC to support this? (Choose two.)

A. SAML Policy

B. SAML IdP Profile

C. SAML IdP Policy

D. SAML Action

Correct Answer: A, C
Section:
Explanation:
Reference: https://www.citrix.com/blogs/2015/04/09/how-to-use-saml-authentication-with-storefront-2-6/

QUESTION 24
Scenario: A Citrix Engineer implements Application-level Quality of Experience (AppQoE) to protect a web application. The engineer configures the AppQoE action to deliver a custom response from a backup server once the maximum number of concurrent connection is reached.
To achieve this, the engineer should set the Acton Type to _____ and specify the _____. (Choose the correct option to complete the sentence.)

A. NS; Alternate Content Server Name

B. ACS; Custom File

C. ACS; Alternate Content Server Name

D. NS; Custom File

Correct Answer: D
Section:

QUESTION 25
Scenario: A Citrix Engineer wants to configure the Citrix ADC for OAuth authentication. The engineer uploads the required certificates, configure the actions, and creates all the necessary policies. After binding the authentication policy to the application, the engineer is unable to authenticate.
What is the most likely cause of this failure?

A. The log files are full.

B. The Redirect URL is incorrect.

C. The certificates have expired.

D. The policy bindings were assigned incorrect priorities.

Correct Answer: D
Section:
Explanation:

Reference: https://docs.citrix.com/en-us/citrix-adc/current-release/aaa-tm/entities-of-authentication-authorization-auditing/authentication-policies.html

QUESTION 26
What is required for connecting a data center to the Citrix Application Delivery Management (ADM) Service?

A. Instance
B. Configuration Job
C. Agent
D. Syslog

Correct Answer: C
Section:
Explanation:
Reference: https://docs.citrix.com/en-us/citrix-application-delivery-management-service/citrix-application-delivery-management-service.html

QUESTION 27
A Citrix Engineer needs to create a configuration job to clone a configuration from an existing Citrix ADC to a new Citrix ADC.
Which configuration source can the engineer use to accomplish this?

A. Master Configuration
B. Inbuilt Template
C. Instance
D. Configuration Template

Correct Answer: D
Section:
Explanation:
Reference: https://docs.citrix.com/en-us/citrix-application-delivery-management-software/current-release/stylebooks/migrate-citirx-adc-application-configuration-using-stylebooks.html

QUESTION 28
Scenario: A Citrix Engineer is asked to help improve the performance of a web application. After capturing and analyzing a typical session, the engineer notices a large number of user requests for the stock price of the company.
Which action can the engineer take to improve web application performance for the stock quote?

A. Enable the Combine CSS optimization.
B. Create a static content group.
C. Create a dynamic content group.
D. Enable the Minify JavaScript optimization.

Correct Answer: D
Section:

QUESTION 29
Which Citrix Application Delivery Management (ADM) Analytics page allows a Citrix Engineer to monitor the metrics of the optimization techniques and congestion control strategies used in Citrix ADC appliances?

A. Gateway Insight
B. TCP Insight
C. HDX Insight

D. Web Insight

Correct Answer: B
Section:
Explanation:
Reference: https://docs.citrix.com/en-us/tech-zone/design/reference-architectures/citrix-adm.html

QUESTION 30
What can a Citrix Engineer implement to protect against the accidental disclosure of personally identifiable information (PII)?

A. Form Field Consistency

B. HTML Cross-Site Scripting

C. Safe Object

D. Cookie Consistency

Correct Answer: A
Section:
Explanation:
Reference: https://docs.citrix.com/en-us/citrix-adc/current-release/application-firewall/form-protections/form-field-consistency-check.html

QUESTION 31
Which Front End Optimization technique can a Citrix Engineer enable on the Citrix ADC to remove all excess whitespace from a file?

A. Shrink to Attributes

B. Minify

C. Lazy Load

D. Inlining

Correct Answer: B
Section:
Explanation:
Reference: https://docs.citrix.com/en-us/citrix-adc/current-release/optimization/front-end-optimization.html

QUESTION 32
Which data populates the
Events Dashboard?

A. Syslog messages

B. SNMP trap messages

C. API calls

D. AppFlow IPFIX records

Correct Answer: D
Section:

QUESTION 33
Scenario: A Citrix Engineer is notified that improper requests are reacting the web application. While investigating, the engineer notices that the Citrix Web App Firewall policy has zero hits. What are two possible causes for this within the Citrix Web App Firewall policy? (Choose two.)

A. The expression is incorrect.
B. It has been assigned an Advanced HTML profile.
C. It is NOT bound to the virtual server.
D. It has been assigned the built-in APPFW_RESET profile.

Correct Answer: A, C
Section:

QUESTION 34
Which feature of Learning should a Citrix Engineer configure to direct Citrix Web App Firewall to learn from specific sessions?

A. Advanced policy expression filter
B. Default policy expression filter
C. Trusted Learning Clients list
D. Manage Content Types for Safe Commerce

Correct Answer: C
Section:
Explanation:
Reference: https://docs.citrix.com/en-us/citrix-adc/current-release/application-firewall/profiles/learning.html

QUESTION 35
A Citrix Engineer has defined an HTTP Callout, hc_authorized_location, to return the value "Authorized" if client's IP address is on a list of authorized external locations.
Which advanced expression should the engineer use in a policy for testing this condition?

A. SYS.HTTP_CALLOUT(hc_authorized_location).IS_TRUE
B. SYS.HTTP_CALLOUT(hc_authorized_location).EQ("Authorized")
C. SYS.HTTP_CALLOUT(hc_authorized_location).IS_VALID
D. SYS.HTTP_CALLOUT(hc_authorized_location).EQUALS_ANY("Authorized")

Correct Answer: D
Section:

QUESTION 36
Scenario: A Citrix Engineer configured signature protections for Citrix Web App Firewall. Signature Auto-Update has been enabled. Upon reviewing the log files, the engineer notices that the auto update process has an error.
In the settings for Signature Auto Update the engineer notices that the URL is blank.
Which URL should the engineer enter to restore the update process?

A. https://s3.amazonaws.com/NSAppFwSignatures/SignaturesMapping.xml
B. https://download.citrix.com/NSAppFwSignatures/SignaturesMapping.xml
C. https://www.citrix.com/NSAppFwSignatures/SignaturesMapping.xml
D. https://citrix.azure.com/NSAppFwSignatures/SignaturesMapping.xml

Correct Answer: A
Section:
Explanation:
Reference: https://support.citrix.com/article/CTX138858

QUESTION 37
Scenario: A Citrix Engineer creates a Responder policy to redirect users attempting to access an application protected with Citrix Web App Firewall. Instead of being redirected, users are seeing an 'Access Denied' page. This is happening because Citrix Web App Firewall is processed _____. (Choose the correct option to complete the sentence.)

A. before Responder, and the redirection is invalid

B. after Responder, but the violation is applied to prevent access

C. before Responder, and a violation is occurring

D. after Responder, and the redirection is invalid

Correct Answer: B
Section:

QUESTION 38
A Citrix Engineer enabled Cookie Consistency protection on a web application and wants to verify that it is working.
Which cookie name can the engineer look for in the HTTP headers sent from the client to verify the protection?

A. Citrix_ns_id

B. Citrix_waf_id

C. Citrix_adc_id

D. Citrix_sc_id

Correct Answer: D
Section:

QUESTION 39
Which protection is applied on a server response from a protected application?

A. Cross-Site Request Forgeries (CSRF)

B. Form Field Consistency

C. HTML Cross-Site Scripting (XSS)

D. Safe Object

Correct Answer: A
Section:

QUESTION 40

Which variable will display the client's source IP address when added to an HTML Error Object page?

A. $[CLIENT.IP.SRC]
B. ${CLIENT.IP.SRC}
C. $<CLIENT.IP.SRC>
D. $(CLIENT.IP.SRC)

Correct Answer: B
Section:
Explanation:
Reference: https://support.citrix.com/article/CTX140292

QUESTION 41
Scenario: A Citrix Engineer wants to protect a web application using Citrix Web App Firewall. After the Web App Firewall policy afweb_protect is bound to the virtual server, the engineer notices that Citrix Web App Firewall is NOT properly displaying the page.
A positive number for the Policy Hits counter for afweb_protect, tells the engineer the number of times Citrix Web App Firewall _____. (Choose the correct option to complete the sentence.)

A. received a request that matched the policy expression for afweb_protect
B. blocked traffic for web applications assigned the afweb_protect policy
C. logged a request matching the expression defined in the afweb_protect policy
D. forwarded users to the Redirect URL specified in the profile assigned to afweb_protect

Correct Answer: C
Section: