Citrix

Exam Questions 1Y0-341

Citrix ADC Advanced Topics - Security-Management and Optimization

NEW QUESTION 1
Scenario: A Citrix Engineer is monitoring the environment with Citrix Application Management (ADM). Management has asked lota report of high-risk traffic to protected internal websites.
Which dashboard can the engineer use to generate the requested report?

A. Transactions
B. APP
C. APP Security
D. Users & Endpoints

Answer: C

NEW QUESTION 2
Scenario: A Citrix Engineer has configured Citrix Application Delivery Management (ADM) to monitor applications presented by Citrix ADC appliances. When reviewing the App Security Dashboard, the engineer finds no data.
What must the engineer do to ensure data is being collected from the applications?

A. Enable AppFlow for Security Insight on the instances in Citrix ADM.
B. Update the password stored in the instance profile on Citrix ADM.
C. Point the default route on Citrix ADM to the subnet with the NSIPs of the Citrix ADC appliances.
D. Enable the Web App Firewall feature on the Citrix ADC appliances.

Answer: A

NEW QUESTION 3
Which security model should a Citrix Engineer implement to ensure that only appropriate traffic that matches the expected application behavior is permitted to pass through to the web application?

A. Dynamic
B. Hybrid
C. Positive
D. Negative

Answer: C

NEW QUESTION 4
Which syntax is used to write a StyleBook?

A. JSON
B. LISP
C. YAML
D. XML

Answer: C

NEW QUESTION 5
Scenario: A Citrix Engineer implements Application-level Quality of Experience (AppQoE) to protect a web application. Shortly after that, users call to complain that nearly every request is being met with a Captcha.
What can the engineer do to improve the user experience?

A. Disable the Captcha.
B. Increase the DOS Attack Threshold.
C. Increase the Policy Queue Depth.
D. Increase the Session Life.

Answer: B

NEW QUESTION 6
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

Answer: C

NEW QUESTION 7
Scenario: A Citrix Engineer is reviewing the log files for a protected application. The engineer discovers a lot of errors pertaining to invalid data being supplied by users.
Which protection can the engineer implement at the Citrix Web App Firewall to reduce these errors?

A. Field Format

B. Cross-Site Request Forgeries (CSRF)
C. Form Field Consistency
D. HTML SQL Injection

Answer: C

NEW QUESTION 8
Statistics for which three types of violations are presented on the App Security Dashboard? (Choose three.)

A. Web App Firewall protection
B. IP Reputation
C. SSL Enterprise Policy
D. Signature
E. AAA

Answer: ABD

NEW QUESTION 9
Scenario: A Citrix Engineer reviewed the log files of a web application and found the error message below: "Unable to complete request Unrecognized field cext2_price>" Which protection can the engineer implement to prevent this error from happening?

A. Form Field Consistency
B. Cross-Site Request Forgeries (CSRF)
C. HTML SQL Injection
D. HTML Cross-Site Scripting (XSS)

Answer: A

NEW QUESTION 10
Which license must be present on the Citrix ADC for the Citrix Application Delivery Management (ADM) Service to generate HDX Insight reports that present one year's worth of data?

A. Advanced
B. Premium Plus
C. Premium
D. Standard

Answer: C

NEW QUESTION 10
Scenario: A Citrix Engineer has enabled the Learn function for a Citrix Web App Firewall profile. After a period of time, the engineer notices that Citrix Web App Firewall is no longer learning any new rules.
What would cause Citrix Web App Firewall to stop learning?

A. The Citrix Web App Firewall has reached its capacity of 500 Learn transactions.
B. The Citrix Web App Firewall feature is NOT licensed.
C. The Citrix Web App Firewall Learn database has reached its capacity of 20 MB.
D. The Citrix Web App Firewall profile was unbound from the application.

Answer: C

NEW QUESTION 12
A Citrix Engineer wants the Citrix Web App Firewall to respond with a page stored on the Citrix ADC when a violation is detected.
Which profile setting accomplishes this?

A. Redirect URL
B. RFC Profile
C. Default Request
D. HTML Error Object

Answer: D

NEW QUESTION 16
Which Citrix Application Delivery Management (ADM) Analytics page allows an engineer to measure the ICA Round Trip Time for user connections?

A. Security Insight
B. Gateway Insight
C. TCP Insight
D. HDX Insight
E. Web Insight

Answer: B

NEW QUESTION 21
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

Answer: A

NEW QUESTION 22
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
B. Make Inline
C. Extend Page Cache
D. Minify

Answer: A

NEW QUESTION 25
Which Citrix Web App Firewall engine setting can a Citrix Engineer use to ensure that protections are applied in the event that an advanced policy expression cannot be evaluated as either 'True' or 'False'?

A. Undefined profile
B. Session Limit
C. Default profile
D. Entity Decoding

Answer: B

NEW QUESTION 27
Scenario: A Citrix Engineer wants to configure the Citrix ADC for 0Auth Authentication. The engineer uploads the required certificates, configures the actions, and creates all the necessary policies. After binding the authentication policy to the application, the engineer is unable to authenticate.

A. The log files are full
B. The policy bindings were assigned incorrect priorities
C. The Redirect URL is incorrect
D. The certificates have expired

Answer: C

NEW QUESTION 29
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.aspx Administrative users are permitted to the path /login.aspx.

Answer: A

NEW QUESTION 34
In which order is a client request to a protected web application processed?

A. CitrixWebApp Firewall, Load Balancing, Caching, Rewrite
B. Caching, Citrix Web App Firewall, Load Balancing, Rewrite
C. Citrix Web App Firewall, Caching, Load Balancing, Rewrite
D. Load Balancing, Citrix Web App Firewall, Caching, Rewrite

Answer: C

NEW QUESTION 39
Scenario: A Citrix Engineer is implementing Integrated Caching to increase performance of a web application. The Application Engineer replaces a small logo on the main page with a new one. Later on, when the engineer attempts to access the page, the old logo is displayed. Which enabled setting in the Content Group would cause this to happen?

A. Ignore browser's reload request
B. Do not cache—if size exceeds 500 KB
C. Expire content after 60 seconds
D. Do not cache—if hits are less than 1

Answer: A

NEW QUESTION 43
Which Citrix Web App Firewall profile setting can a Citrix Engineer configure to provide a response when a violation occurs?

A. Default Request
B. Redirect URL
C. Return URL
D. Default Response

Answer: B

NEW QUESTION 45
Scenario : A Citrix Engineer needs to forward the Citrix Web App Firewall log entries to a central management service. This central management service uses an open log file standard. Which log file format should the engineer use in the Citrix Web App Firewall engine settings to designate the open log file standard?

A. CEF
B. TLA
C. IIS
D. W3C

Answer: A

NEW QUESTION 49
A Citrix Engineer observes that the servers hosting a critical application are crashing on a regular basis. Which protection could the engineer implement on a Citrix Web App Firewall in front of the application?

A. Buffer Overflow Check
B. HTML Cross-Site Scripting (XSS)
C. Start URL
D. HTML SQL Injection

Answer: A

NEW QUESTION 50
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

Answer: B

NEW QUESTION 53
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

Answer: A

NEW QUESTION 55
A Citrix Engineer is reviewing the log files for a sensitive web application and notices that someone accessed the application using the engineer's credentials while the engineer was out of the office for an extended period of time.
Which production can the engineer implement to protect against this vulnerability?

A. Deny URL
B. Buffer Overflow
C. Form Field Consistency
D. Cookie Consistency

Answer: D

NEW QUESTION 59
Scenaho: A Citrix Engineer needs to block requests from a list of IP addresses in a database maintained by the Security team. The Security team has built a web application that will send a response of either "Blocked" or "Allowed," based on whether the given IP address is on the list. Which expression should the engineer use to extract the status for policy processing?

A. HTTP.RES.STATUS

B. HTTP.RES.HEADERfConnection")
C. HTTP.RES.BODY(1000)
D. HTTP.RES.CONTENT LENGTH.GT(0)

Answer: B

NEW QUESTION 61
Which build-in TCP profile can a Citrix Engineer assign to a virtual server to improve performance for users who access an application from a secondary campus building over a fiber optic connection?

A. nstcp_default_tcp_lfp
B. nstcp_default_tcp_lan
C. nstcp_default_tcp_interactive_stream
D. nstcp_default_tcp_lnp

Answer: A

NEW QUESTION 64
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)

Answer: AD

NEW QUESTION 65
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

Answer: D

NEW QUESTION 68
Which protection can a Citrix Engineer implement to prevent a hacker from extracting a customer list from the company website?

A. Cross-Site Request Forgeries (CSRF)
B. Form Field Consistency
C. HTML Cross-Site Scripting (XSS)
D. HTML SQL Injection

Answer: D

NEW QUESTION 69
Scenario: A Citrix Engineer has a pair of Citrix ADC VPX appliances configured as a High-Availability (HA) pair and hosted on a Citrix Hypervisor. The engineer wants to use Citrix Application Delivery Management (ADM) to monitor and manage the 35 web applications on the appliances. The engineer has imported Citrix ADM virtual appliance to Citrix Hypervisor. The engineer has also configured the management IP address settings and has added the 35 instances. However, some of the instances are NOT reporting any data.
Which two areas can the engineer check to determine the cause of the issue? (Choose two.)

A. A Premium platform license must be configured on each instance.
B. AppFlow must be enabled on each instance.
C. The Citrix ADM license must be installed.
D. An SSL certificate must be installed on the Citrix ADM appliance.

Answer: CD

NEW QUESTION 71
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

Answer: A

NEW QUESTION 74
Scenario: A Citrix Engineer needs to forward the Citrix Web App Firewall log entries to a central management service. This central management service uses an

open log file standard.
Which log file format should the engineer use in the Citrix Web App Firewall engine settings to designate the open log file standard?

A. CEF
B. IIS
C. W3C
D. TLA

Answer: A

NEW QUESTION 79
A manager for a hospital billing system wants to display the last four digits of a credit card number when printing invoices.
Which credit card security action does this?

A. X-Out
B. Log
C. Transform
D. Block

Answer: A

NEW QUESTION 84
Scenario: A Citrix Engineer has established protections for web applications using Citrix Web App Firewall. One of the application owners is concerned that some negative traffic is passing through to the application servers. The owner wants confirmation that Citrix Web App Firewall is blocking negative traffic. Which CLI command can the engineer use to display statistics on a per-protection basis for the enabled protections?

A. stat appfw policyjabel <policy_label_name>
B. stat appfw policy <policy_name>
C. stat appfw profile <profile_name>
D. stat appfw signature <signature_object>

Answer: C

NEW QUESTION 85
Which Application-level Quality of Experience (AppQoE) Action setting modifies the communication characteristics of the connections established with the associated web application?

A. Priority
B. TCP Profile
C. Action Type
D. DOS Action

Answer: C

NEW QUESTION 89
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")

Answer: D

NEW QUESTION 94
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

Answer: A

NEW QUESTION 95
......

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

1Y0-341 Practice Exam Features:

* 1Y0-341 Questions and Answers Updated Frequently

* 1Y0-341 Practice Questions Verified by Expert Senior Certified Staff

* 1Y0-341 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 1Y0-341 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The 1Y0-341 Practice Test Here