SY0-601 Q&As

CompTIA Security+

Pass CompTIA SY0-601 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/sy0-601.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A security analyst is investigating suspicious traffic on the web server located at IP address 10.10.1.1. A search of the WAF logs reveals the following output:

Source IP	Destination IP	Requested URL	Action Taken
172.16.1.3	10.10.1.1	/web/cgi-bin/contact? category=custname'--	permit and log
172.16.1.3	10.10.1.1	/web/cgi-bin/contact? category=custname+OR+1=1--	permit and log

Which of the following is MOST likely occurring?

A. XSS attack

B. SQLi attack

C. Replay attack

D. XSRF attack

Correct Answer: B

SQL injection, also known as SQLI, is a common attack vector that uses malicious SQL code for backend database manipulation to access information that was not intended to be displayed. The giveaway here is the 1=1 in the query which is

essentially creating a condition that will automatically be true.

==========

Helpful Info:

XSS (Cross-Site Scripting) attacks -a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. Replay Attack - a kind of man-in-the-middle attack in which an attacker sniffs messages being sent on a

channel to intercept them and resend them under the cloak of authentic messages. CSRF (Cross Sit Request Forgery)- attacks that target functionality that causes a state change on the server, such as changing the victim\\'s email address or

password, or purchasing something.

QUESTION 2

SIMULATION

A company recently added a DR site and is redesigning the network. Users at the DR site are having issues browsing websites.

INSTRUCTIONS

Click on each firewall to do the following:

1.

Deny cleartext web traffic.

2.

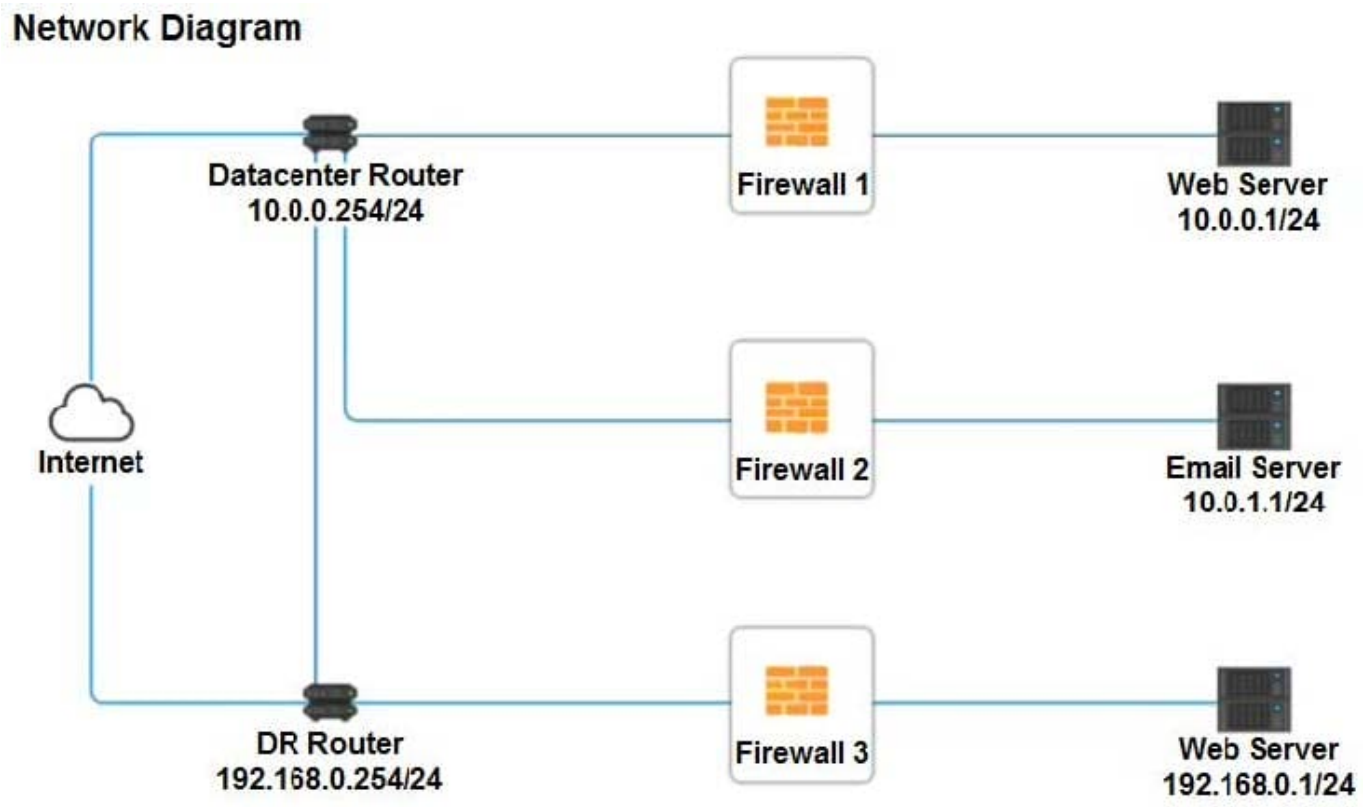
Ensure secure management protocols are used.

3.

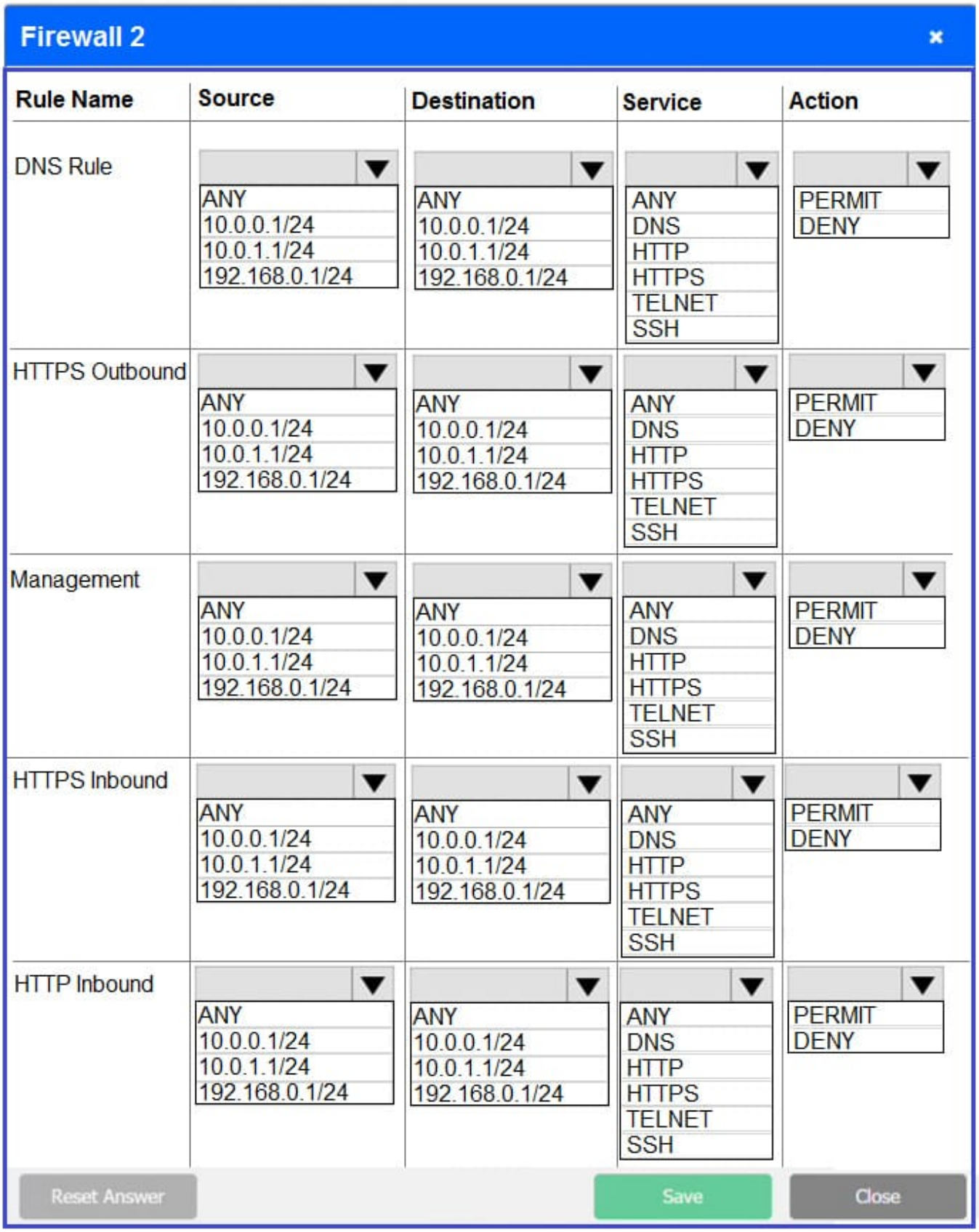
Resolve issues at the DR site.

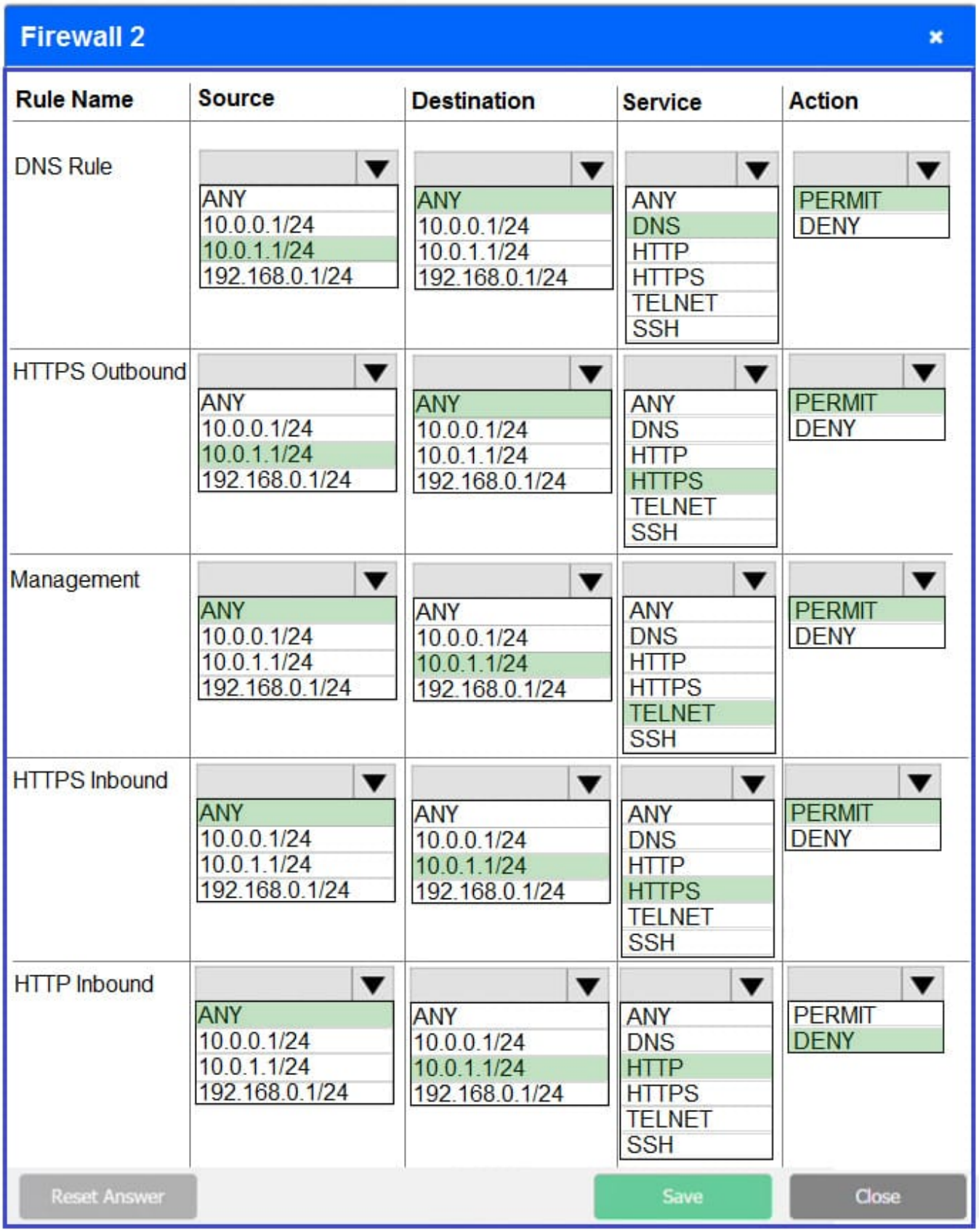
The ruleset order cannot be modified due to outside constraints.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



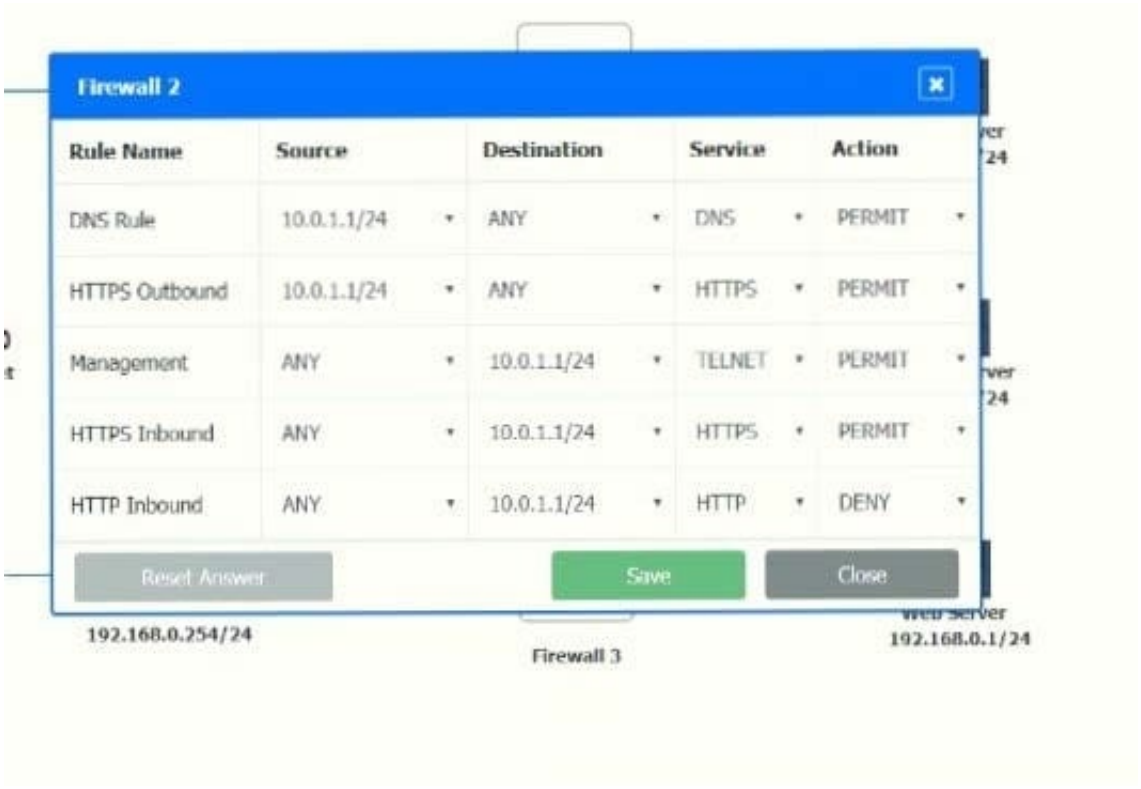
Firewall 2 Hot Area:


Firewall 2
Rule Name
Source
Destination
Service
Action
DNS Rule
HTTPS Outbound
Management
HTTPS Inbound
HTTP Inbound
ANY
10.0.0.1/24
10.0.1.1/24
192.168.0.1/24
ANY
DNS
HTTP
HTTPS
TELNET
SSH
PERMIT
DENY
Reset Answer
Save
Close



Correct Answer:

Firewall 2: No changes should be made to this firewall



QUESTION 3

A company was recently breached. Part of the company\\'s new cybersecurity strategy is to centralize the logs from all security devices. Which of the following components forwards the logs to a central source?

A. Log enrichment

B. Log queue

C. Log parser

D. Log collector

Correct Answer: D

A log collector can collect logs from various sources, such as servers, devices, applications, or network components, and forward them to a central source for analysis and storage23.

QUESTION 4

Which of the following best describes the risk that is present once mitigations are applied?

A. Control risk

B. Residual risk

C. Inherent risk

D. Risk awareness

Correct Answer: B

The residual risk is the amount of risk or danger associated with an action or event remaining after natural or inherent risks have been reduced by risk controls.

QUESTION 5

Server administrators want to configure a cloud solution so that computing memory and processor usage is maximized most efficiently across a number or virtual servers. They also need to avoid potential dental-of-service situations caused by availability. Which of the following should administrators configure to maximize system availability while efficiently utilizing available computing power?

A. Dynamic resource allocation

B. High availably

C. Segmentation

D. Container security

Correct Answer: A

To maximize system availability and efficiently utilize available computing power, administrators should configure dynamic resource allocation. Dynamic resource allocation is a technique that allows a system to automatically adjust the allocation of resources, such as memory and processing power, to different applications or processes in response to changing workloads or conditions. This can help to ensure that computing resources are used efficiently and that the system is able to respond to changes in demand without encountering performance issues or becoming unavailable.