

# ***KillTest***

Higher Quality, Better Service!



## **Q&A**

<http://www.killtest.com>

We offer free update service for one year.

**Exam** : **830-01**

**Title** : RCPE Certified Professional  
WAN Optimization

**Version** : DEMO

- 1.What do you need to ensure when connecting a SteelHead to a Hardware Security Module?
- A. Access is required for both server-side and client side SteelHead appliances to the HSM
  - B. The in-path interface must be at least 10Gbps
  - C. The HSM and the in-path interfaces must share the same default gateway
  - D. The latency between the in-path interfaces and the HSM must be kept to a minimum
  - E. The latency between the auxiliary or Primary interfaces and the HSM must be kept to a minimum

**Answer:** E

- 2.For optimized encrypted MAPI, is the inner channel encrypted by default?

- A. Yes, always
- B. No
- C. Only for MS Exchange 2003 and later
- D. Yes, but this is configured on the server

**Answer:** B

**Explanation:**

Reference:

[https://support.riverbed.com/bin/support/static/d6j3tb1i55ni1erbjp6e3fln9v/html/mhmppa9t9gq3laicvt0r91b1n7/sh\\_cx\\_9.2\\_ug\\_html/index.html#page/sh\\_cx\\_9.2\\_ug/setupServiceProtocolsMAPI.html](https://support.riverbed.com/bin/support/static/d6j3tb1i55ni1erbjp6e3fln9v/html/mhmppa9t9gq3laicvt0r91b1n7/sh_cx_9.2_ug_html/index.html#page/sh_cx_9.2_ug/setupServiceProtocolsMAPI.html)

- 3.Which report displays the rate of established SSL connections?

- A. WAN Throughput
- B. Traffic Summary
- C. SSL
- D. Current Connections

**Answer:** C

**Explanation:**

Reference:

[https://support.riverbed.com/bin/support/static/d6j3tb1i55ni1erbjp6e3fln9v/html/mhmppa9t9gq3laicvt0r91b1n7/sh\\_cx\\_9.2\\_ug\\_html/index.html#page/sh\\_cx\\_9.2\\_ug/reportSSLStatistics.html](https://support.riverbed.com/bin/support/static/d6j3tb1i55ni1erbjp6e3fln9v/html/mhmppa9t9gq3laicvt0r91b1n7/sh_cx_9.2_ug_html/index.html#page/sh_cx_9.2_ug/reportSSLStatistics.html)

- 4.A customer is complaining that all optimized connections to their internal website cause a splash screen indicating an untrusted certificate. If the users click to accept the risks and add a security exception in their browsers, it all works fine.

What is a likely cause?

- A. The proxy certificate in the server-side SteelHead appliance is not trusted by the client browser
- B. The SteelHead Peering Certificates have expired
- C. The proxy certificate on the client-side SteelHead appliance is not trusted by the client browser
- D. The server-side SteelHead does not trust the server certificate
- E. The server-side SteelHead appliance has not joined the Domain properly

**Answer:** A

- 5.Authentication fails for certain users after configuring the joining of the server-side SteelHead appliance to the domain as a read-only domain controller (RODC).

What is the most likely issue?

- A. The users have local branch file servers
- B. There is an incorrect Short Domain Name (NETBIOS name)
- C. There's an incorrect domain controller
- D. These users exclusively make use of Kerberos authentication

**Answer: B**