**Site-to-Site Preparation**

|  |  |  |
| --- | --- | --- |
| **1.** | Enter the protocol and port that must be specified within an interface ACL to allow a management connection to be terminated on the router: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. | [*    The protocol and port that must be specified within an interface ACL to allow a management connection to be terminated on the router is UDP 500.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=839117335&rowid=1877&noteMenuToggle=0&hitSectionMenuToggle=0&leftMenuState=1#answer.N27) |

**Answers**

|  |  |
| --- | --- |
| **1.** | *  The protocol and port that must be specified within an interface ACL to allow a management connection to be terminated on the router is UDP 500. |

**ISAKMP/IKE Phase 1 Configuration**

|  |  |  |
| --- | --- | --- |
| **2.** | If you omit a parameter in an ISAKMP/IKE Phase 1 policy, a default value is used. Which of the following is not a default value?   1. MD5 2. DES 3. DH group 1 4. RSA signatures | [*     A. SHA-1 is the default, not MD5, if the HMAC function is omitted from a Phase 1 policy.  *    Answers B , C , and D are default values, if omitted.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=839117335&rowid=1877&noteMenuToggle=0&hitSectionMenuToggle=0&leftMenuState=1#answer.N52) |
| **3.** | You need to create an ISAKMP/IKE Phase 1 policy that uses the following parameters: preshared keys, using a preshared key of abc123 for peer 192.1.1.1, 3DES, MD5, DH key group 2, and a lifetime of one hour. Use a policy number of 100. Enter the commands to accomplish this: \_\_\_\_\_\_\_\_\_\_\_. | [*    Here is the configuration to set up the policy:   Router(config)# crypto isakmp policy 100 Router(config-isakmp)# authentication pre-share Router(config-isakmp)# encryption 3des Router(config-isakmp)# group 2 Router(config-isakmp)# hash md5 sha Router(config-isakmp)# lifetime 3600 Router(config-isakmp)# exit Router(config)# crypto isakmp key 0 abc123 address 192.1.1.1](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=839117335&rowid=1877&noteMenuToggle=0&hitSectionMenuToggle=0&leftMenuState=1#answer.N108) |

**Answers**

|  |  |
| --- | --- |
| **2.** | *  **A.** SHA-1 is the default, not MD5, if the HMAC function is omitted from a Phase 1 policy. *  Answers **B**, **C**, and **D** are default values, if omitted. |
| **3.** | *  Here is the configuration to set up the policy: * Router(config)# **crypto isakmp policy 100** * Router(config-isakmp)# **authentication pre-share** * Router(config-isakmp)# **encryption 3des** * Router(config-isakmp)# **group 2** * Router(config-isakmp)# **hash md5 sha** * Router(config-isakmp)# **lifetime 3600** * Router(config-isakmp)# **exit** * Router(config)# **crypto isakmp key 0 abc123 address 192.1.1.1** |

**ISAKMP/IKE Phase 2 Configuration**

|  |  |  |
| --- | --- | --- |
| **4.** | What is the default lifetime of data SAs, if not overridden?   1. 300 seconds 2. 600 seconds 3. 3,600 seconds 4. 86,400 seconds | [*     C. The default lifetime of data SAs, if not overridden, is 3,600 seconds.  *     A and B are too small. D is the default value for the management connection.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=839117335&rowid=1877&noteMenuToggle=0&hitSectionMenuToggle=0&leftMenuState=1#answer.N171) |
| **5.** | What is the default mode for a transform set, if omitted?   1. Transport 2. Transform 3. Symmetrical 4. Tunnel | [*     D. The default mode for a transform set, if omitted, is tunnel mode.  *     A is used for host-to-host connections and is not the default. B and C are nonexistent transform set modes.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=839117335&rowid=1877&noteMenuToggle=0&hitSectionMenuToggle=0&leftMenuState=1#answer.N227) |
| **6.** | Which of the following is not required in a crypto map entry?   1. Crypto ACL 2. Router's local IP address 3. Transform set name 4. Connection method: manual or dynamic (ISAKMP/IKE) | [*     B. The remote peer's IP address, not the local router's address, must be specified in a crypto map entry.  *    Answers A , C , and D are required.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=839117335&rowid=1877&noteMenuToggle=0&hitSectionMenuToggle=0&leftMenuState=1#answer.N288) |
| **7.** | Which of the following traffic is dropped when using static crypto maps and IPSec?   1. Inbound traffic that is protected and matches a crypto ACL entry 2. Inbound traffic that doesn't match a crypto ACL entry 3. Inbound traffic that matches a crypto ACL entry and is in clear text 4. Outbound traffic that matches a crypto ACL and is already protected by IPSec | [*     C. Inbound traffic that matches a crypto ACL entry and is in clear text is dropped by the router.  *     A is verified and decrypted by the router. B is not processed by IPSec. D is protected by IPSec again.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=839117335&rowid=1877&noteMenuToggle=0&hitSectionMenuToggle=0&leftMenuState=1#answer.N345) |

**Answers**

|  |  |
| --- | --- |
| **4.** | *  **C.** The default lifetime of data SAs, if not overridden, is 3,600 seconds. *  **A** and **B** are too small. **D** is the default value for the management connection. |
| **5.** | *  **D.** The default mode for a transform set, if omitted, is tunnel mode. *  **A** is used for host-to-host connections and is not the default. **B** and **C** are nonexistent transform set modes. |
| **6.** | *  **B.** The remote peer's IP address, not the local router's address, must be specified in a crypto map entry. *  Answers **A**, **C**, and **D** are required. |
| **7.** | *  **C.** Inbound traffic that matches a crypto ACL entry and is in clear text is dropped by the router. *  **A** is verified and decrypted by the router. **B** is not processed by IPSec. **D** is protected by IPSec again. |

**Examining and Troubleshooting Connections**

|  |  |  |
| --- | --- | --- |
| **8.** | What state will a management connection be in if it is successfully set up?   1. MM\_NO\_STATE 2. QM\_IDLE 3. MM\_SA\_SETUP 4. MM\_KEY\_AUTH | [*     B. QM_IDLE indicates that the management connection has completed successfully.  *     A indicates that the tunnel has been initialized but nothing has been negotiated. C indicates that the IPSec peers have negotiated the ISAKMP/IKE Phase 1 policies. D indicates that the management SA has been authenticated.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=839117335&rowid=1877&noteMenuToggle=0&hitSectionMenuToggle=0&leftMenuState=1#answer.N411) |
| **9.** | Which output from the **debug crypto isakmp** command indicates a failed policy negotiation?   1. %CRYPTO-6-IKMP\_SA\_NOT\_OFFERED: Remote peer % 15i responded with attribute [chars] not offered or changed. 2. %CRYPTO-6-IKMP\_SA\_NOT\_AUTH: Cannot accept Quick Mode exchange from %15i if SA is not authenticated! 3. IPSec(validate\_transform\_proposal): proxy identities not supported; ISAKMP: IPSec policy invalidated proposal 4. IPSEC(validate\_proposal): invalid local address *IP\_address* | [*     A. The ` %CRYPTO-6-IKMP_SA_NOT_OFFERED: Remote peer % 15i responded with attribute [chars] not offered or changed. ` message in the output of the debug crypto isakmp command indicates a failed policy negotiation.  *     B indicates Phase 1 authentication failure. C indicates a mismatched crypto ACL in Phase 2. D indicates an invalid remote peer IP address in Phase 1.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=839117335&rowid=1877&noteMenuToggle=0&hitSectionMenuToggle=0&leftMenuState=1#answer.N467) |

**Answers**

|  |  |
| --- | --- |
| **8.** | *  **B.** QM\_IDLE indicates that the management connection has completed successfully. *  **A** indicates that the tunnel has been initialized but nothing has been negotiated. **C** indicates that the IPSec peers have negotiated the ISAKMP/IKE Phase 1 policies. **D** indicates that the management SA has been authenticated. |
| **9.** | *  **A.** The "%CRYPTO-6-IKMP\_SA\_NOT\_OFFERED: Remote peer % 15i responded with attribute [chars] not offered or changed." message in the output of the **debug crypto isakmp** command indicates a failed policy negotiation. *  **B** indicates Phase 1 authentication failure. **C** indicates a mismatched crypto ACL in Phase 2. **D** indicates an invalid remote peer IP address in Phase 1. |

**Classic Method Site-to-Site Example**

|  |  |  |
| --- | --- | --- |
| **10.** | What crypto map command is used to specify the crypto ACL to use?   1. **set transform-set** 2. **match address** 3. **set address** 4. **set crypto-acl** | [*     B. The match address crypto map command is used to specify the crypto ACL to use.  *     A defines the transform set to use. C and D are invalid commands.](http://www.books24x7.com/assetviewer.aspx?bookid=33002&chunkid=839117335&rowid=1877&noteMenuToggle=0&hitSectionMenuToggle=0&leftMenuState=1#answer.N555) |

**Answers**

|  |  |
| --- | --- |
| **10.** | *  **B.** The **match address** crypto map command is used to specify the crypto ACL to use. *  **A** defines the transform set to use. **C** and **D** are invalid commands. |