

Actualtests.com

The Power of Knowing



Exam : 156-515

Title : Check Point Certified Security Expert Plus NGX

Ver : 11-24-2008

QUESTION 1:

The fw ctl debug command is used primarily to troubleshoot _____ problems.

- A. Kernel
- B. Secure Internal Communications (SIC)
- C. Policy-load
- D. Logging
- E. OPSEC

Answer: A

QUESTION 2:

Which file provides the data for the host_table output and is responsible for keeping a record of all internal IPs passing through the internal interfaces of a restricted hosts licensed Security Gateway?

- A. external.if
- B. fwconn.h
- C. hosts
- D. hosts.h
- E. fwd.h

Answer: E

QUESTION 3:

What does it indicate when a cluster state is "Active Attention"?

- A. Traffic is being passed, but a problem has been detected: There are no other active members in the cluster
- B. The cluster member is booting: CluserXL is running, but VPN-1/NGX is not yet ready
- C. Cluster members are running different versions: The newer version member is in the ready state, which the older version member is in the active state
- D. Both cluster members are up and ready

Answer: A

QUESTION 4:

Which type of routing relies on a VPN Tunnel interface (VTI) to route traffic?

- A. Host-based VPN
- B. Subnet-based VPN

- C. Route-Based VPN
- D. All VPN types
- E. Domain-based VPN

Answer: C

QUESTION 5:

In some circumstances, adjusting the number of Security Servers spawned may help in troubleshooting performance issues. Which of the following files would you edit to achieve this?

- A. fwssd.conf
- B. fwx.conf
- C. fwauthd.conf
- D. fwd.conf
- E. fwm.conf

Answer: C

QUESTION 6:

You have implemented a Check Point High Availability solution. You have defined a Gateway Cluster and a group of Security Gateways with synchronized state tables. If the active Security Gateway fails, what happens?

- A. Clear text connections survive the failure. Encrypted connections must be re-established
- B. All connections must be re-established with the security Gateway that assumes control
- C. Encrypted and clear text connections fail over to the Security Gateway that assumes control
- D. The remaining Security Gateway force an election to determine who takes over
- E. The control network is flooded with synchronization packets

Answer: C

QUESTION 7:

To Stop the sr_service debug process, you must first stop VPN-1 SecureClient, delete which of the following files and restart SecureClient?

- A. sr_users.all
- B. sr_service.dll
- C. sr_topo.all
- D. sr_auth.all
- E. sr_tde.all

Answer: E

QUESTION 8:

Setting snaplen to 0 will capture host much of the packet data?

- A. None of the packet
- B. The first octet of the packet header
- C. The whole packet
- D. The first protocol level of the packet

Answer: C

QUESTION 9:

Which of the following types of information should an Administrator use tcpdump to view?

- A. VLAN trunking analysis
- B. DeCnet traffic analysis
- C. AppleTalk Traffic analysis
- D. Packet-header analysis
- E. NAT traffic analysis

Answer: D

QUESTION 10:

When network address translation is used:

- A. It is not necessary to add a static route to the Gateway's routing table
- B. It is necessary to add a static route to the Gateway's routing table
- C. VLAN tagging can't be defined for any hosts protected by the Gateway
- D. The Security Gateway's ARP file must be modified
- E. The Gateway's lmhosts file must be modified

Answer: A

QUESTION 11:

When you run the fw monitor -e "accept" command, what type of traffic is captured?

- A. Only inbound traffic, before and after inbound and outbound kernels
- B. Only inbound traffic, before and after the inbound kernel
- C. All traffic coming in all directions, before and after inbound and outbound kernels

- D. All traffic accepted by the Rule Base
- E. Only outbound traffic, before and after the outbound kernel

Answer: C

QUESTION 12:

You use fwm to input the following command: fwm lock_admin a. What does this command do?

- A. Sets the access level of administrators to "all-access"
- B. Uninstalls all administrators, except the default administrator
- C. Locks all administrator accounts
- D. Unlocks all administrator accounts

Answer: D

QUESTION 13:

Which native UNIX utility displays fw monitor output on Solaris?

- A. Snoop -I (lowercase)
- B. Ethereal
- C. Soop (lowercase)
- D. tcpdump
- E. CapView

Answer: A

QUESTION 14:

If you run only fw monitor without any parameters, where does the output display?

- A. In /tmp/log/monitor.out
- B. On the console
- C. In /var/log/monitor.out
- D. In \$FWDIR/bin
- E. In /var/adm/monitor.out

Answer: B

QUESTION 15:

Which of the following commands shows full synchronization status?

- A. fw hastat

- B. cphaprob -l list
- C. cphastop
- D. fw ctl stat
- E. cphaprob -a if

Answer: B

QUESTION 16:

To troubleshoot SmartDashboard issues. You run the command: fw debug fwm on TDERRR_ALL_ALL=4. What does this command do?

- A. Sets the fwm to debug on the fly
- B. Nothing, fwm is not the correct process to debug any known SmartDashboard issues
- C. Includes special debugging options for FW1_LOG
- D. Appends the process-identifier number to the core filename
- E. Captures traffic, including UUID

Answer: A

QUESTION 17:

When collecting information relating to the perceived problem, what is the most important question to ask?

- A. What action or state am I trying to achieve?
- B. Under what circumstances does this problem occur?
- C. Is this problem software or hardware related?
- D. Does the problem appear random or can you establish a pattern?
- E. Is this problem repeatable?

Answer: B

QUESTION 18:

Which of the following commands would you run to debug a VPN connection?

- A. vpn debug ike
- B. debug vpn ike
- C. debug vpn ikeon
- D. debug vpn ike on
- E. vpn debug ikeon

Answer: E

QUESTION 19:

If fwauth.NDB or fwauth.NDB# are corrupt, what will be the result?

- A. SIC will fail
- B. You will not be able to authenticate to the SmartDashboard using the cpconfig created administrator user
- C. You will not be able to find any users in the SmartDashboard
- D. You will not be able to push a policy

Answer: C

QUESTION 20:

Setting snaplen to 0 will capture host much of the packet data?

- A. None of the packet
- B. The whole packet
- C. The first protocol level of the packet
- D. The first octet of the packet header

Answer: B

QUESTION 21:

How can you view cpinfo on a SecurePlatform Pro Machine?

- A. infotab
- B. tcpdump
- C. Infoview
- D. snoop -l
- E. Text Editor, such vi

Answer: E

QUESTION 22:

Which statement is true for route based VPNs?

- A. Route-based VPNs replace domain-based VPNs
- B. Route-Based VPNs are a form of partial overlap VPN Domain
- C. IP Pool Nat must be configured on each gateway
- D. Dynamic-routing protocols are not required
- E. Packets are encrypted or decrypted automatically

Answer: D

QUESTION 23:

The following is part of a fw ctl pstat output. How much kernel memory is assigned to this system?

```
Hash kernel memory (hmem) statistics:
Total memory allocated: 20971520 bytes in 5114 4KB blocks using 6 pools
Initial memory allocated: 6291456 bytes (Hash memory extended by 14680064 bytes)
Memory allocation limit: 83886080 bytes using 512 pools

Total memory bytes used: 886580 unused: 20084940 <95.77%> peak: 1438396
Total memory blocks used: 318 unused: 4796 <93%> peak: 471

Allocations: 249736 alloc, 0 failed alloc, 235423 free

System kernel memory (smem) statistics:
Total memory bytes used: 37502884 peak: 37513740
Blocking memory bytes used: 1385116 peak: 1395972
Non-Blocking memory bytes used: 36117768 peak: 36117768

Allocations: 4367790 alloc, 0 failed alloc, 4367353 free, 0 failed free

Kernel memory (kmem) statistics:
Total memory bytes used: 17385056 peak: 19164776

Allocations: 251977 alloc, 0 failed alloc, 237441 free, 0 failed free
```

- A. 5MB
- B. 20MB
- C. 37MB
- D. 6MB
- E. 12MB

Answer: B

QUESTION 24:

If fwauth.NDB or fwauth.NDB# are corrupt, what will be the result?

- A. You will not be able to find any users in the SmartDashboard
- B. You will not be able to push a policy
- C. You will not be able to authenticate to the SmartDashboard using the cpconfig created administrator user
- D. SIC will fail

Answer: A

QUESTION 25:

Which of the following vpn debug options purges ike.elg and vpnd.elg and creates a time stamp before starting ike debug and vpn debug at the same time?

- A. mon
- B. trunk
- C. timeon
- D. ikedfail

E. ike on

Answer: B

QUESTION 26:

The list below provides all the actions check point recommends to troubleshoot a problem with an NGX product.

- A. List possible causes
- B. Identify the problem
- C. Collect Related Information
- D. Consult Various Reference Sources
- E. Test Causes Individually and Logically

Select the answer that shows order of the recommended actions that make up check point's troubleshooting guidelines?

- A. B,C,A,E,D
- B. A,E,B,D,C
- C. A,B,C,D,E
- D. B,A,D,E,C
- E. D,B,A,C,E

Answer: A

QUESTION 27:

Gus is troubleshooting a problem with SMTP. He has enabled debugging on his security Gateway and needs to copy the *.elg files into an archive to send to Check Point Support. Which of the following files does Gus NOT need to send?

- A. asmtpd.elg
- B. mdq.elg
- C. diffserv.elg
- D. fwd.elg

Answer: C

QUESTION 28:

What can you do in the advanced mode of GuiDbEdit Query that you can't do in the simple mode?

- A. Query by object name
- B. Log when medications are made
- C. Run a CPMI Query
- D. Query by table name

Answer: C

QUESTION 29:

When setting up a High Availability solution using ClusterXL, on which network objects do you define VPN properties?

- A. On the networks
- B. On the Synchronization Interface
- C. On the gateway cluster
- D. On the Management Server
- E. On each Security Gateway in the Gateway cluster

Answer: C

QUESTION 30:

Where should you run the cpinfo command in a distributed environment?

- A. SmartCenter Server and Security Gateways only
- B. Security Gateonly
- C. SmartConsole only
- D. Client behind the Security Gateway
- E. SmartCenter server only

Answer: A

QUESTION 31:

You have installed SecurePlatform R60 as Security Gateway operating system. As company requirements changed, you need the VTI features of NGX. What should you do?

- A. In SmartDashboard click on the OS drop down menu and choose SecurePlatform Pro. You have to reboot the Security Gateway in order for the change to take effect
- B. You have to re-install your Security Gateway with SecurePlatform Pro R60, as SecurePlatform R60 does not support VTIs
- C. Only IPSO 3.9 supports VTI feature, so you have to replace your Security Gateway with Nokia appliances
- D. Nothing, because SPLAT R60 does support VTIs
- E. Type "pro enable" on your Security Gateway and reboot it

Answer: E

QUESTION 32:

Which of the following processes is responsible for Policy related functions and communication between a SmartConsole and SmartCenter Server?

- A. fwd
- B. cpd
- C. fw monitor
- D. fw sam
- E. fwm

Answer: E

QUESTION 33:

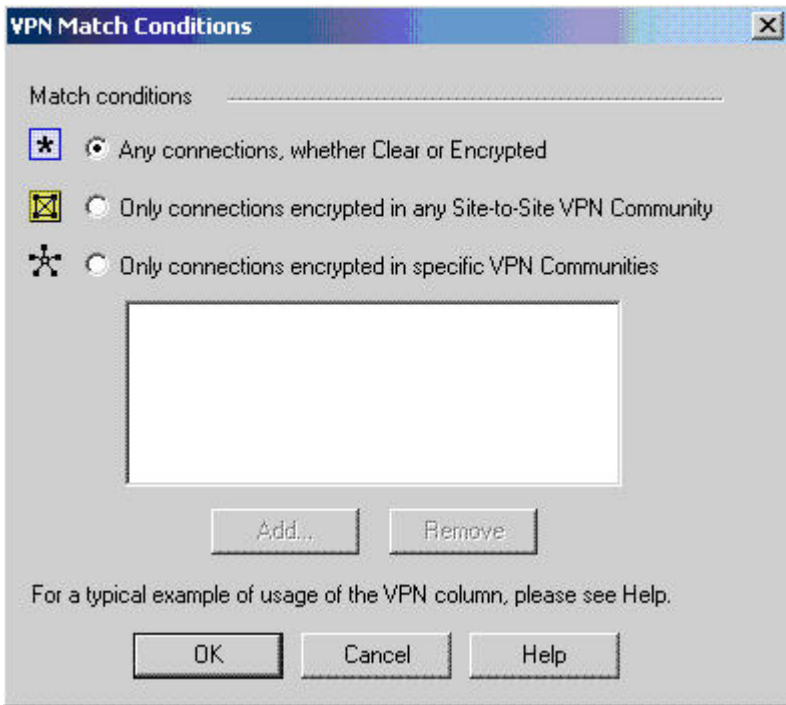
To cross-reference sr fw monitor output what should you do?

- A. Run fw monitor on the client
- B. Restart the client and run sr fw monitor a second time
- C. Run fw monitor and compare against a known good baseline
- D. Run fw monitor from the Gateway
- E. Run sr fw monitor a second time

Answer: D

QUESTION 34:

Steve tries to configure directional VPN Rule match in the rule base. However, the match column does not have the option to see the Directional Match. Steve sees the following screen. What is the problem?



- A. Steve must enable Advanced Routing on each Security Gateway
- B. Steve must enable VPN Directional Match on the VPN advanced screen, in Global properties
- C. Steve must enable `directional_match` (true) in the `objects_5_0.C` file on SmartCenter server
- D. Steve must enable VPN Directional Match on the gateway object's VPN tab
- E. Steve must enable a dynamic-routing protocol, such as OSPF, on the Gateway's

Answer: B

QUESTION 35:

Which of the following fw monitor commands only captures traffic between IP addresses 192.168.11.1 and 10.10.10.1?

- A. `fw monitor -e "accept src=192.168.11.1 or dst=192.168.11.1 or src=10.10.10.1 or dst=10.10.10.1;"`
- B. `fw monitor -e "accept src=192.168.11.11 or dst=192.168.11.1;src=10.10.10.1 or dst=10.10.10.1;"`
- C. `fw monitor -e "accept (src=192.168.11.1 and dst=10.10.10.1) or (src=10.10.10.1 and dst=192.168.11.1);"`
- D. `fw monitor -e "accept src=192.168.11.1 and dst=192.168.11.1;src=10.10.10.1 and dst=10.10.10.1;"`
- E. `fw monitor -e "accept src=192.168.11.1 or dst=192.168.11.1 and src=10.10.10.1 or dst=10.10.10.1;"`

Answer: C

QUESTION 36:

You modified the *.def file on your Security Gateway, but the changes were not applied. Why?

- A. There is more than one *.def file on the Gateway
- B. *.def files must be modified on the SmartCenter Server
- C. You did not have the proper authority
- D. The *.def file on the Gateway is read-only

Answer: B

QUESTION 37:

After configuring ClusterXL, where do you install the Security Policy?

- A. On each Security Gateway in the Gateway Cluster
- B. On the Gateway Cluster
- C. Policy installation is not required after configuring ClusterXL. This automatic in NGX
- D. On the management Server
- E. On the backup Security Gateway

Answer: B

QUESTION 38:

If you save the fw monitor output with option, how do you view the output file afterwards?

- A. SmartView Tracker
- B. The output file is ASCII, so you can use your preferred ASCII editor
- C. SmartView Monitor
- D. WINWORD.EXE or openoffice
- E. Ethereal

Answer: E

QUESTION 39:

Each Module within the NGX kernel contains specific debugging flags. Which of the statements is true concerning kernel-debug flags?

- A. Debug flags require an administrator to set them
- B. Each flag is generic and can't be modified to produce varying levels of information
- C. Debugging flags can be configured to produce varying levels of information

- D. Debug flags can't be disabled
- E. Debugging flags are universal across all modules

Answer: C

QUESTION 40:

A SecureRemote/SecureClient tunnel test uses which port?

- A. UDP 18233
- B. UDP 2746
- C. TCP 18231
- D. UDP 18321
- E. UDP 18234

Answer: E

QUESTION 41:

Assume you have a rule allowing HTTP traffic, on port 80, to a specific web server in a Demilitarized Zone (DMZ). If an external host port scans the web server's IP address, what information will be revealed?

- A. Port 80 is open on the web server
- B. All ports are open on the web server
- C. The web server's file structure is revealed
- D. All ports are open on the Security Server
- E. Nothing, the NGX Security Server Automatically block all ports scans

Answer: A

QUESTION 42:

Which of the following commands identifies whether or not a Security Policy is installed or the Security Gateway is operating with the initial Policy?

- A. fw stat
- B. fw policy
- C. cp stat
- D. fw monitor
- E. cp policy

Answer: A

QUESTION 43:

Policy Server login and Desktop Policy installation will kill which of the following processes on the client machine?

- A. fw monitor
- B. srfw monitor
- C. fwm
- D. fwd
- E. cpd

Answer: B

QUESTION 44:

What does it indicate when a cluster state is "Active Attention"?

- A. Both cluster members are up and ready
- B. Cluster members are running different versions: The newer version member is in the ready state, which the older version member is in the active state
- C. Traffic is being passed, but a problem has been detected: There are no other active members in the cluster
- D. The cluster member is booting: CluserXL is running, but VPN-1/NGX is not yet ready

Answer: C

QUESTION 45:

When you verify IP Forwarding on SecurePlatform Pro using the command more /proc/sys/net/ipv4/ip_forward, what value should be stored in the resulting file?

- A. 0
- B. Y
- C. P
- D. 1
- E. 4

Answer: D

QUESTION 46:

VPN debugging information is written to which of the following files?

- A. FWDIR/log/fw.elg
- B. FWDIR/log/ahttpd.elg
- C. FWDIR/log/vpn.elg
- D. FWDIR/log/authd.elg
- E. \$FWDIR/log/ike.elg

Answer: E

QUESTION 47:

Gill Bates is in charge of a large enterprise, which requires VPN connections between offices around the world. To achieve this Gill decides to use a dynamic routing protocol to make sure all offices are connected through the VPN community using tunnel interfaces among all peers. Nothing is configured in `vpn_route.conf`. However, Gill is experiencing connectivity problems and when examining the logs he discovers multiple "out of state" drops. What is the most likely cause of and solution to this problem?

- A. Asymmetric routing will happen if nothing has been configured in `vpn_route.conf`. The `vpn_route.conf` should be configured to prevent asymmetric routing
- B. The dynamic routing protocol introduces asymmetric routing in Gill's VPN community. Gill should use wire mode on the VPN tunnel interfaces
- C. In this configuration, NAT is necessary for traffic to be routed correctly. IP pool NAT should be configured on each gateway
- D. The firewall security policy drops the traffic. Gill should introduce a Directional VPN rule to allow the VPN traffic

Answer: B

QUESTION 48:

Gill Bates is in charge of a large enterprise, which requires VPN connections between offices around the world. To achieve this Gill decides to use a dynamic routing protocol to make sure all offices are connected through the VPN community using tunnel interfaces among all peers. Nothing is configured in `vpn_route.conf`. However, Gill is experiencing connectivity problems and when examining the logs he discovers multiple "out of state" drops. What is the most likely cause of and solution to this problem?

- A. The firewall security policy drops the traffic. Gill should introduce a Directional VPN rule to allow the VPN traffic
- B. The dynamic routing protocol introduces asymmetric routing in Gill's VPN community. Gill should use wire mode on the VPN tunnel interfaces
- C. In this configuration, NAT is necessary for traffic to be routed correctly. IP pool NAT should be configured on each gateway
- D. Asymmetric routing will happen if nothing has been configured in `vpn_route.conf`. The `vpn_route.conf` should be configured to prevent asymmetric routing

Answer: B

QUESTION 49:

Which files should be acquired from a Windows 2003 Server System crash with a Dr.

Watson Error?

- A. drwtsn32.log
- B. core.log
- C. vmcore.log
- D. memory.log
- E. info.log

Answer: A

QUESTION 50:

fw monitor packets are collected from the kernel in a buffer. What happens if the buffer becomes full?

- A. Packet capture stops
- B. The information in the buffer is saved and packet capture continues, what new data stored in the buffer
- C. All packets in it are deleted and the buffer begins filling from the beginning
- D. Older packet information is dropped as new packet information is added

Answer: C

QUESTION 51:

Which of the following is a consequence of using the fw ctl debug all option?

- A. No debug output will be collected since this is an invalid flag
- B. Writes limited amounts of data to the console
- C. Options is not recommended because it fills the log buffer with likely irrelevant information
- D. Provides state information for all ports
- E. Loads step-by-step firewall data to a user-defined log file

Answer: C

QUESTION 52:

Which of the following commands is used to read messages in the debug buffer?

- A. fw ctl debug
- B. fw ctl kdebug
- C. fw ctl debug uf

Answer: B

QUESTION 53:

After a sudden spike in traffic, you receive this system log file message: "Kernel: FW-1: Log Buffer is full". Which is NOT a solution?

- A. Reconfigure the minimum disk space "stop logging" threshold
- B. Decrease the amount of logging
- C. Increase the log buffer size
- D. Disable logging

Answer: A

QUESTION 54:

Which statement is true for route based VPNs?

- A. Route-based VPNs replace domain-based VPNs
- B. Route-Based VPNs are a form of partial overlap VPN Domain
- C. IP Pool Nat must be configured on each gateway
- D. Dynamic-routing protocols are not required
- E. Packets are encrypted or decrypted automatically

Answer: D

QUESTION 55:

To start both vpnd.elg and ike.elg, which single vpn debug command would you use?

- A. vpn tu
- B. vpn debug ikeon
- C. vpn debug trunc
- D. vpn debug vpnd.elg + ike
- E. vpn debug ikeinit

Answer: C

QUESTION 56:

Which of the following types of information should an Administrator use tcpdump to view?

- A. Packet-header analysis
- B. AppleTalk Traffic analysis
- C. NAT traffic analysis
- D. DECnet traffic analysis
- E. VLAN trunking analysis

Answer: A

QUESTION 57:

How does fw monitor differ from the INSPECT filter?

- A. Fw monitor allows Administrators to view how traffic would be filtered through a specific Rule Base, if implemented. The INSPECT filter implements the Rule Base
- B. Fw monitor is a command-line utility that can be used for packet-header analysis, while the INSPECT filter implements the Rule Base
- C. fw monitors traffic passing through a security Gateway's interfaces. The INSPECT filter implements the Rule Base.
- D. Fw monitor captures all packets on the network segment to which an interface is attached. The INSPECT filter implements the Rule Base
- E. Fw monitor tracks changes made to the Rule base. The INSPECT filter implements the Rule Base

Answer: C

QUESTION 58:

Which of these issues would you use fw debug fwm as the primary debugging command for troubleshooting?

- A. Alerts
- B. Policy save issues
- C. Blocked Port Issues
- D. Logging issues
- E. Kernel communication issues

Answer: B

QUESTION 59:

Which of the following explanations best describes the audit log file xx.adtloginitial_ptr?

- A. Pointers to the beginning of each log chain
- B. Additional temporary pointer file
- C. Pointers to the begging of each log record
- D. Audit log records
- E. Pointers to the beginning of each accounting record

Answer: A

QUESTION 60:

Resource rules that accept HTTP, FTP and SMTP must:

- A. Replace rules that accept these services
- B. Be placed after rules that accept these services
- C. Be placed before rules that accept these services
- D. Be placed before rules that deny these services
- E. Be placed after rules that deny these services

Answer: C

QUESTION 61:

Which of the following explanations best describes the active log file
\$FWDIR/log/xx.logptr?

- A. Real log records
- B. Pointers to the beginning of each log record
- C. Pointers to the beginning of each log chain
- D. Pointers to the beginning of each accounting record
- E. Additional temporary pointer file

Answer: B

QUESTION 62:

You create a FTP resource and select the Get check box. Which of the following actions are denied to users, on net-detroit, when using FTP to an external host when the rule action is "accept" and no other permissive ftp rule exists lower in the rule base?

NO.	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK
1		Net_Detroit	Tech-Support	Any Traffic	FTP ftp->External	accept	Log

- A. Put
- B. Change
- C. List
- D. mget
- E. Directory

Answer: A

QUESTION 63:

Which of the following explanations best describes the active log file
\$FWDIR/log/xx.logptr?

- A. Pointers to the beginning of each accounting record

- B. Pointers to the beginning of each log record
- C. Pointers to the beginning of each log chain
- D. Additional temporary pointer file
- E. Real log records

Answer: B

QUESTION 64:

Which of the following explanations best describes the command fw lslogs?

- A. Control kernel
- B. Display protected hosts
- C. Send signal to a daemon
- D. Create a new log file. The old log has moved
- E. Display a remote machine's log-file list

Answer: E

QUESTION 65:

Which of the following commands can you run to view packet flow of a VPN-1 SecuRemote/SecureClient connection?

- A. sc monitor
- B. fw monitor
- C. srfw monitor
- D. cpd monitor
- E. vpn monitor

Answer: C

QUESTION 66:

The output of tcpdump is a binary file. Which of the following commands will write the tcpdump file into an ASCII file through std_out?

- A. tcpdump <file_name> > <file_name>
- B. tcpdump <file_name> %> <file_name>
- C. tcpdump <file_name> ?> <file_name>
- D. tcpdump <file_name> &> <file_name>
- E. tcpdump <file_name> *> <file_name>

Answer: D

QUESTION 67:

Joey downloads the following Desktop Security Policy to his laptop and successfully logs in to the policy server. Joey then disconnects from the VPN-1 Policy server. What happens to Joey's laptop?

Inbound Rules					
NO.	SOURCE	DESKTOP	SERVICE	ACTION	TRACK
1	* Any	SC_Users@Any	* Any	Encrypt	Log
2	* Any	All Users@Any	* Any	Block	Log

Outbound Rules					
NO.	DESKTOP	DESTINATION	SERVICE	ACTION	TRACK
3	SC_Users@Any	localnet	* Any	Encrypt	Log
4	SC_Users@Any	* Any	* Any	Block	Log
5	All Users@Any	* Any	* Any	Accept	Log

- A. A default desktop security policy is loaded on Joey's laptop, which allows Joey to connect to the Internet. Joey can't receive any inbound traffic
- B. A default Desktop Security Policy is loaded on Joey's laptop, which opens up inbound and outbound connections
- C. There is no default Desktop Security Policy, unless the client connects to the security gateway
- D. A default desktop security policy is loaded on Joey's laptop, which allows Joey to connect to anywhere, except the policy server site's VPN Domain

Answer: A

QUESTION 68:

Pulling Certificates from an ICA uses which port?

- A. Port 18209
- B. Port 18212
- C. Port 18210
- D. Port 18211

Answer: C

QUESTION 69:

user.C is populated on the SecuRemote/SecureClient during what stage of the SecuRemote/SecureClient packet flow.

- A. When creating a site
- B. When connecting/resolving Gateway IP
- C. When connecting/IKE negotiation
- D. When connecting/encrypting data

Answer: A

QUESTION 70:

Which one of these is a temporary pointer log file?

- A. \$FWDIR/log/xx.logLuuidDB
- B. \$FWDIR/log/xx.logaccount_ptr
- C. \$FWDIR/log/xx.logptr
- D. \$FWDIR/log/xx.log

Answer: A