Checkpoint 156-515

156-515 Check Point Security Administration NGX III

Practice Test

Version 1.0

QUESTION NO: 1

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

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

Answer: A

QUESTION NO: 2

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

A. lw 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. lw monitor-e accept src=192.168.11.1 or dst=192.168.11.1; src=10.10.10.1 or dst=10.10.10.1;"
C. fw monitor-e accept src=192.168.111 and dst=192.168.11.1; src=10.10.10.1 and dst=10.10.10.1;"
D. tw 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;"
E. lw 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);"

Answer: E

QUESTION NO: 3

How do you run fw ctl debug, to see all information about a cluster?

A. tw ct debug cluster all tw ct debug > output twct debug uf1024
B. tw ct pstat
tw ct debug all
tw ct debug > out
C. twct debug uf1024 lw ct debug cluster all tw ct kdebug > output
D. lw ct debug on
lw ct debug cluster all
lw ct kdebug > output
E. lw ct debug on fwct debug uf1024 tw ct debug cluster all tw ct kdebug > output

Answer: C

QUESTION NO: 4

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

Answer: C

QUESTION NO: 5

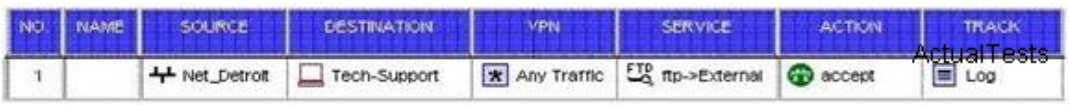
To stop the sr_service debug process, you must first stop VPN-1 SecureClient, delete which of the following files, and restart SecureClient?

A. sr_auth.all
B. sr_topo.all
C. srjde.all
D. sr_service.all
E. sr users.all

Answer: C

QUESTION NO: 6

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?



A. mget
B. change
C. put
D. directory

E. list

Answer: C

QUESTION NO: 7

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

Answer: C

QUESTION NO: 8

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

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

Answer: E

QUESTION NO: 9

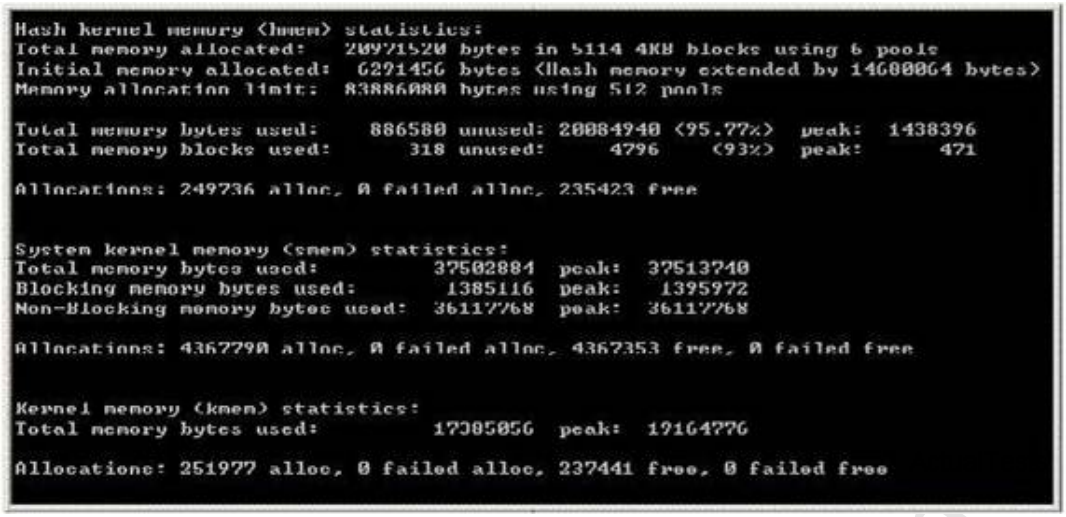
Which of the following processes controls Secure Internal Communications, Policy installation, and shared-management capabilities between Check Point products and OPSEC-partner products?

A. cpd
B. fwd
C. fwsam
D. fw monitor
E. fwm

Answer: A

QUESTION NO: 10

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



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

Answer: B

QUESTION NO: 11

How do you disable all fw debug logging?

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

Answer: C

QUESTION NO: 12

The virtual machine inspects each packet at the following points:
-Before the virtual machine, in the inbound direction (i or PREIN) -After the virtual machine, in the inbound direction (I or POSTIN) -Before the virtual machine, in the outbound direction (o or PREOUT) -After the virtual machine, in the outbound direction (0 or POSTOUT)
If Ethereal displays a packet with i, I, o, and 0 entries, what does that likely indicate?

A. The packet was rejected by the Rule Base.

B. The packet was destined for the Gateway.
C. Nothing unusual; the o and 0 entries only appear if there is a kernel-level error.
D. The packet was rerouted by the Gateway's OS.
E. The packet arrived at the kernel and left the Security Gateway successfully.

Answer: E

QUESTION NO: 13

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. twm.conf
B. twssd.conf
C. twauthd.conf
D. twd.conf
E. lwx.conf

Answer: C

QUESTION NO: 14

Which statement is true for route based VPNs?

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

Answer: E

QUESTION NO: 15

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

A. On the synchronization interface
B. On the Management Server
C. On each Security Gateway in the Gateway Cluster
D. On the networks

E. On the Gateway Cluster

Answer: E

QUESTION NO: 16

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

A. All traffic coming in all directions, before and after inbound and outbound kernels.
B. Only inbound traffic, before and after inbound and outbound kernels.
C. Only outbound traffic, before and after the outbound kernel.
D. All traffic accepted by the Rule Base.
E. Only inbound traffic, before and after the inbound kernel.

Answer: A

QUESTION NO: 17

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 monitor
B. cp policy
C. cp stat
D. fw policy
E. fwstat

Answer: E

QUESTION NO: 18

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. The control network is flooded with synchronization packets.
D. Encrypted and clear text connections fail over to the Security Gateway that assumes control
E. The remaining Security Gateway force an election to determine who takes over.

Answer: D

QUESTION NO: 19

To cross-reference sriw monitor output what should you do?

A. run tw monitor on the client.
B. run sriw monitor a second time.
C. run lw monitor from the Gateway.
D. restart the client and run sriw monitor a second time.
E. run lw monitor and compare against a known good baseline.

Answer: C

QUESTION NO: 20

The fw ctl debug command is used primarily to troubleshoot_____problems.

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

Answer: A

QUESTION NO: 21

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. Only IPSO 3.9 supports VTI feature, so you have to replace your Security Gateway with Nokia appliances
C. You have to re-install your Security Gateway with SecurePlatform Pro R60, as Secure Platform R60 does not support VTIs
D. Nothing, because SPLAT R60 does support VTIs
E. Type "pro enable" on your Security Gateway and reboot it

Answer: E

QUESTION NO: 22

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

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

Answer: E

QUESTION NO: 23

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. Nothing; the NGX Security Server automatically block all port scans.
B. All ports are open on the Security Server.
C. All ports are open on the Web server.
D. The Web server's file structure is revealed.
E. Port 80 is open on the Web server.

Answer: E

QUESTION NO: 24

NGX Wire Mode allows:

A. Peer gateways to establish a VPN connection automatically from predefined preshared secrets.
B. Administrators to verify that each VPN-1 Secure Client is properly configured, before allowing it access to the protected domain.
C. Peer gateways to fail over existing VPN traffic, by avoiding Stateful Inspection.
D. Administrators to monitor VPN traffic for troubleshooting purposes.
E. Administrators to limit the number of simultaneous VPN connections, to reduce the traffic load passing through a Security Gateway.

Answer: C

QUESTION NO: 25

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

A. Policy save issues
B. Logging issues
C. Kernel communication issues
D. Alerts
E. Blocked port issues

Answer: A

QUESTION NO: 26

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: A

QUESTION NO: 27

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

A. stfw monitor
B. fwm
C. fw monitor
D. fwd
E. cpd

Answer: A

QUESTION NO: 28

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. ike on
B. timeon
C. trunc
D. ikefail
E. mon

Answer: C

QUESTION NO: 29

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

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

Answer: C

QUESTION NO: 30

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

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

Answer: A

QUESTION NO: 31

Which native UNIX utility displays fw monitor output on Solaris?

A. tcpdump
B. Ethereal

C. snoop -i (lowercase)
D. CapView
E. snoop (lowercase)

Answer: C

QUESTION NO: 32

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

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

Answer: D

QUESTION NO: 33

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

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

Answer: A

QUESTION NO: 34

How does fw monitor differ from the INSPECT filter?

A. fw monitor monitors traffic passing through a Security Gateway's interfaces. The INSPECT filter implements the Rule Base.
B. 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.
C. fw monitor tracks changes made to the Rule Base. 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 is a command-line utility that can be used for packet-header analysis, while the INSPECT filter implements the Rule Base.

Answer: A

QUESTION NO: 35

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 the order of the recommended actions that make up Check Point's troubleshooting guidelines?
F. B C A, E, D
G. AE B.D.C
H. A B C.D.E
I. B A D.E.C
J. D B A, C, E

Answer: A

QUESTION NO: 36

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

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

Answer: C

QUESTION NO: 37

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

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

Answer: B

QUESTION NO: 38

A SecuRemote/SecureClient tunnel test uses which port?

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

Answer: C

QUESTION NO: 39

You use -0 to set the number of processes to be spawned when troubleshooting Security Server. How many will be spawned?

A. The parent process will spawn up to 10000 child processes.
B. No processes will be spawned.
C. The parent process will not spawn the child processes.
D. The parent process will now spawn the child processes as needed.

Answer: D

QUESTION NO: 40

Which one of these is a temporary pointer log file?

A. $FWDIR/log/xx.logptr
B. $FWDIR/log/xx.log
C. $FWDIR/log/xx.logaccount_ptr
D. $FWDIR/log/xx.logl_uuidDB

Answer: D

QUESTION NO: 41

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

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

Answer: D

QUESTION NO: 42

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

A. FWDIR/log/ahttpd.elg
B. FWDIR/log/lw.elg
C. $FWDIR/log/ike.elg
D. FWDIR/log/authd.elg
E. FWDIR/log/vpn.elg

Answer: C

QUESTION NO: 43

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

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

Answer: C

QUESTION NO: 44

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

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

Answer: D

QUESTION NO: 45

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 NO: 46

Pulling Certificates from an ICA uses which port?

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

Answer: D

QUESTION NO: 47

When VPN-1 NGX starts after reboot, with no installed Security Policy, which of these occurs?

A. All traffic except HTTP connections is blocked.
B. All traffic except Smart Defense Console connections is blocked.
C. All traffic is blocked.
D. All traffic except Smart Console/Smart Center Server connections is blocked.
E. All traffic is allowed.

Answer: D

QUESTION NO: 48

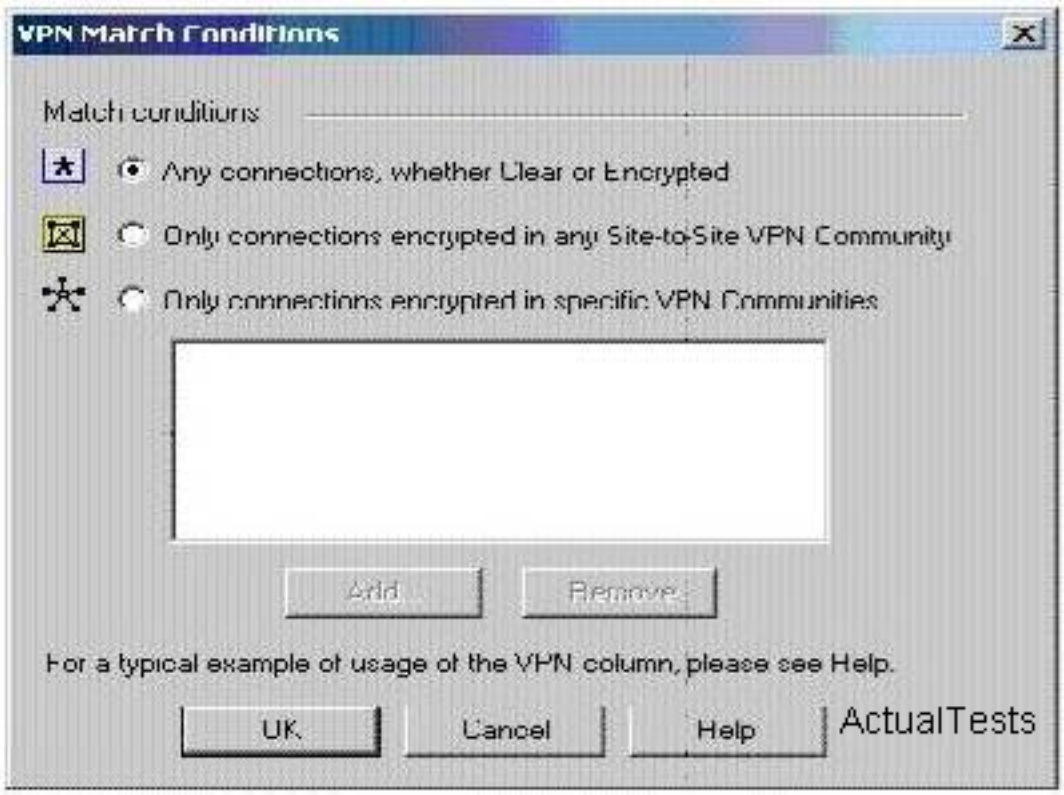
After a sudden spike in traffic, you receive this system log file message: "kernel: FW-1: Log buffer is full". Which is NOT a solution?

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

Answer: C

QUESTION NO: 49

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 directional_match(true) in the objects_5_0.C file on Smart Center Server.
B. Steve must enable Advanced Routing on each Security Gateway.
C. Steve must enable VPN Directional Match on the gateway object's VPN tab.
D. Steve must enable VPN Directional Match on the VPN advanced screen, in Global properties.

E. Steve must enable a dynamic-routing protocol, such as OSPF, on the Gateways.

Answer: D

QUESTION NO: 50

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

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

Answer: C

QUESTION NO: 51

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

A. Client behind the Security Gateway
B. Smart Center Server and Security Gateways only
C. Security Gateway only
D. Smart Console only
E. Smart Center Server only

Answer: B

QUESTION NO: 52

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

A. Debugging flags are universal across all modules.
B. Debug flags cannot be disabled.
C. Debugging flags can be configured to produce varying levels of information.
D. Debug flags require an administrator to set them.
E. Each flag is generic and cannot be modified to produce varying levels of information.

Answer: C

QUESTION NO: 53

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

A. Host-based VPN
B. Subnet-based VPN
C. Domain-based VPN
D. Route-based VPN
E. All VPN types

Answer: D

QUESTION NO: 54

Which of the following commands shows full synchronization status?

A. cphaprob -I list
B. fw hastat
C. cphaprob -a if
D. fw ctl stat
E. cphastop

Answer: A

QUESTION NO: 55

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

A. DECnet traffic analysis
B. VI.AN trunking analysis
C. NAT traffic analysis
D. Packet-header analysis
E. AppleTalk traffic analysis

Answer: D

QUESTION NO: 56

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

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

Answer: A

QUESTION NO: 57

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

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

Answer: D

QUESTION NO: 58

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?

A. A default Desktop Security Policy is loaded on Joey's laptop, which opens up inbound and outbound connections.

B. There is no default Desktop Security Policy, unless the client connects to the Security Gateway.
C. A default Desktop Security Policy is loaded on Joey's laptop, which allows Joey to connect to the Internet. Joey cannot receive any inbound traffic.
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.
E. A default Desktop Security Policy is loaded on Joey's laptop, which allows everyone from the Internet access to Joey's machine. Joey cannot connect to the Internet.

Answer: C

QUESTION NO: 59

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

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

Answer: C

QUESTION NO: 60

When Network Address Translation is used:

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

Answer: B

QUESTION NO: 61

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

A. Smart View Tracker
B. The output file is ASCII, so you can use your preferred ASCII editor.

C. Smart View Monitor
D. Ethereal
E. WINWORD.EXE or Open Office

Answer: D

QUESTION NO: 62

userc. C is populated on the Secu Remote/Secure Client during what stage of the Secu Remote/Secure Client packet flow.

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

Answer: B

QUESTION NO: 63

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

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

Answer: D

QUESTION NO: 64

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. hosts, h
B. external, if
C. hosts
D. fwd.h

E. fwconn.h

Answer: D

QUESTION NO: 65

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 firewall security policy drops the traffic. Gill should introduce a Directional VPN rule to allow the VPN traffic
C. The dynamic routing protocol introduces asymmetric routing in Gill's VPN community. Gill should use wire mode on the VPN tunnel interfaces
D. In this configuration, NAT is necessary for traffic to be routed correctly. IP pool NAT should be configured on each gateway

Answer: C

QUESTION NO: 66

How can you view cpinfo on a SecurePlatform Pro machine?

A. snoop -i
B. infotab
C. tcpdump
D. Text editor, such as vi
E. infoview

Answer: D

QUESTION NO: 67

If flwauth.NDB or1wauth.NDB#are corrupt, what will be the result?

A. You will not be able to push a policy.

B. SIC will fail.
C. You will not be able to authenticate to the SmarlDashboard using the cpconfig created Administrator user.
D. You will not be able to find any users in the SmarlDashboard.

Answer: D

QUESTION NO: 68

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

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

Answer: C

QUESTION NO: 69

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

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

Answer: C

QUESTION NO: 70

Which files should be acquired from a Windows 2003 Server system crash with a Dr. Watson error?

A. drwtsn32.log
B. vmcore.log
C. core.log
D. memory.log

E. info, log

Answer: A