Check Point
SOFTWARE TECHNOLOGIES LTD

CHECK POINT SECURITY MASTER
STUDY GUIDE

WELCOME TO THE FUTURE OF CYBER SECURITY

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page (http://www.checkpoint.com/copyright.html) for a list of our trademarks.
Refer to the Third Party copyright notices
(http://www.checkpoint.com/3rd_party_copyright.html)
for a list of relevant copyrights and third-party licenses.

International Headquarters:	5 Ha'Solelim Street Tel Aviv 67897, Israel Tel: +972-3-753 4555
U.S. Headquarters:	959 Skyway Road, Suite 300 San Carlos, CA 94070 Tel: 650-628-2000 Fax: 650-654-4233
Technical Support, Education & Professional Services:	6330 Commerce Drive, Suite 120 Irving, TX 75063 Tel: 972-444-6612 Fax: 972-506-7913 E-mail any comments or questions about our courseware to courseware@us.checkpoint.com. For questions or comments about other Check Point documentation, e-mail CP_TechPub_Feedback@checkpoint.com.
Document #:	CPTS-DOC-CCSM-SG-R77

Preface

The Check Point Certified Security Master Course

The *Check Point Security Master* course provides a review and practice on a sample of the core troubleshooting and advanced configuration skills the Certified Security Master is expected to demonstrate.

The *Check Point Security Master Study Guide* supplements knowledge you have gained from the Security Master course, and is not a sole means of study.

The Check Point Certified Security Master #156-115.xx exam covers the following topics:

CCSM Objectives

Topic: Troubleshoot security problems

- Given a specific internal or client problem, replicate the issues in a test environment.
- Given a specific internal or client problem, troubleshoot and correct the issue.

Topic: Chain Modules

- Use command `fw ctl chain` to study chain module behavior. Observe how policy changes impact the chain.
- Use the command `fw debug fwm on` and review the file `fwm.elg` to find such issues as SIC, mis-configured rules, GUI client connectivity problems, and improperly entered information.
- Given a specific internal or client need, analyze and apply the appropriate hot fix and evaluate its effectiveness.
- Use Check Point Debugging Tools
  a. Reading and identifying fwmonitor outputs
  b. Generating and interpreting kernel debugs

Topic: NAT

- Use commands `fw ctl debug` and `fw monitor` to troubleshoot the NAT stages of Automatic Hide NAT and Automatic Static NAT.
- Configure Manual NAT to define specific rules in unique NAT environments.

Topic: ClusterXL

- Using commands `fw ctl debug` and `fw ctl kdebug` troubleshoot ClusterXL connections from information displayed in debug file.
- Use commands `fw tab -t connections` and `fw tab -t connections -x` to review and clear connections table.
- Modify file `table.def` to allow traffic through a specific cluster member.

Topic: VPN Troubleshooting

- Use command `vpn debug` to locate source of encryption failures.
- Use command `fw monitor` to verify VPN connectivity and identify potentially mis-configured VPN's.

Topic: SecureXL Acceleration debugging

- Use commands `fw accel` and `kernel debug` to view acceleration tables and verify accelerated connections.

Topic: Hardware Optimization

- Identify the correct Check Point Hardware/Appliances for a given scenario
- Performance tuning and evaluation of complex networks and technologies
- Scope proper sizing of hardware based on customer requirements
- Use command `ethtool` to tune NIC performance.
- Edit `arp cache` table to increase size to improve performance.
- Use command `fw ctl pstat` to improve load capacity.
- Use the `fwaccel stat` and `fwaccel stats` outputs to tune the firewall rule base.

Topic: Software Tuning

- Deploy NAT templates to reduce load on Rule Base application.
- Configure cluster synchronization planning to improve network performance.
- Identify performance limiting configurations
- Correct and tune different scenarios
- Identify the causes of performance limiting factors (internal and external factors)

Topic: Enable CoreXL

- Configure CoreXL for specific cpu task assignment.

Topic: IPS

- Configure IPS to reduce false positives.
- Use command `fw ctl zdebug` to improve logging efficiency.
- Use IPS Bypass to improve performance.

Topic: IPV6

- Deploy IPV6 in a local environment

Topic: Advanced VPN

- Identify differences between route-based VPNs and domain-based VPNs.
- Configure VTI for route-based VPN gateways.
- Configure OSPF for Dynamic VPN routing in a Community.
- Identify the Wire Mode function by testing a VPN failover.
- Configure Directional VPN Rule Match for Route-Based VPN.

Topic: Dynamic Routing

- Diagnose and solve specific routing issues in a network environment.
- Multicast Design and troubleshooting PIM Sparse mode and Dense mode based on GateD and IPSRD
- Design/troubleshoot OSPF/BGP in GateD and IPSO IPSRD environments
- Static routing and network topologies

Section 1: Troubleshoot security problems

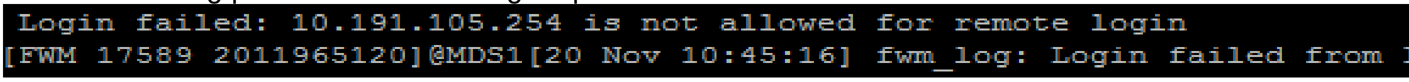
Check Point technology is designed to address network exploitation, administrative flexibility and critical accessibility. This Section introduces the basic concepts of network security and management based on Check Point's three-tier structure, and provides the foundation for technologies involved in the Check Point Architecture. These objectives and study questions provide a review of important concepts, but is not all inclusive.

Objectives

1. Given a specific internal or client problem, replicate the issues in a test environment.
2. Given a specific internal or client problem, troubleshoot and correct the issue.

Do you know ...

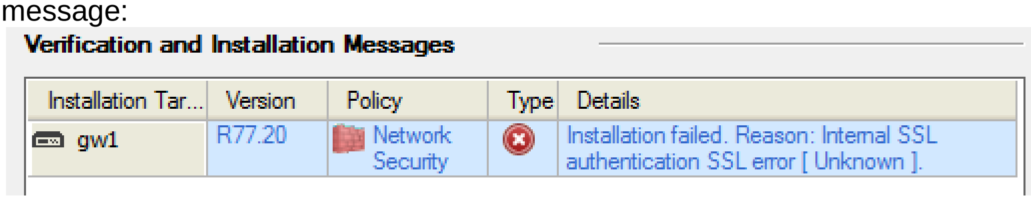
- What command you would use for a packet capture on an absolute position for TCP streaming (out) `1ffffe0`?
- What type of information the command `fw monitor -p all` displays?
- What command lists the firewall kernel modules on a Security Gateway?
- What command would give you a summary of all the tables available to the firewall kernel?
- What flag option(s) you would use to dump the complete table in a user-friendly format, assuming the connections in the table are more than 100?
- The command functions of `fw ctl kdebug <params>` ?
- Which command to use to generate a detailed status of your Threat Emulation quota in a specific Security Gateway?
- The fastest way to troubleshoot silent drops, i.e. don't see any drops in the logs?
- What behavior results from enabling the "Match for any" setting on more than one service with the same destination port?
- The issue that would cause connections to be dropped "because the connections table is full" on a firewall under VSX mode when the connections table is big enough?
- Which gateway directory first receives the new policy files when pushing policy to a security gateway?
- Which debug produces the following output and to which file?



```
 Login failed: 10.191.105.254 is not allowed for remote login
[FWM 17589 2011965120]@MDS1[20 Nov 10:45:16] fwm_log: Login failed from
```

- Which process you should suspect when a Policy installation fails with the following error message: F*ailed to load Policy on Module*? Especially when you find that –
  - You are able to push policy successfully to other gateways from the same management.
  - That the policy installation files are not getting updated to the gateway.

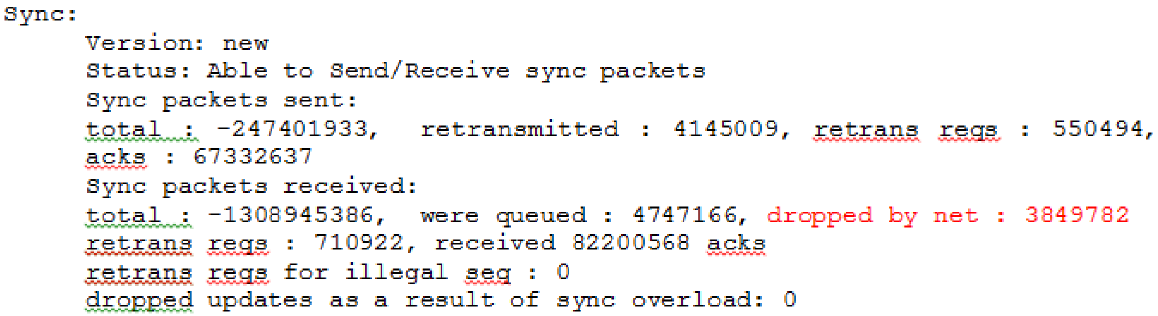
- The MOST LIKELY root cause when Policy installation to a gateway fails with the following error message:



Verification and Installation Messages

Installation Tar...	Version	Policy	Type	Details
gw1	R77.20	Network Security	⊗	Installation failed. Reason: Internal SSL authentication SSL error [Unknown].

- What *dropped by net* indicates in the following output?



```
Sync:
      Version: new
      Status: Able to Send/Receive sync packets
      Sync packets sent:
      total  : -247401933,   retransmitted : 4145009, retrans reqs : 550494,
      acks : 67332637
      Sync packets received:
      total  : -1308945386,  were queued : 4747166, dropped by net : 3849782
      retrans reqs : 710922, received 82200568 acks
      retrans reqs for illegal seq : 0
      dropped updates as a result of sync overload: 0
```

- Which blade do you investigate when you see high CPU caused by the pdpd process?

Section 2: Chain Modules

Check Point technology is designed to address network exploitation, administrative flexibility and critical accessibility. This Section introduces the basic concepts of network security and management based on Check Point's three-tier structure, and provides the foundation for technologies involved in the Check Point Software Blade Architecture, as discussed in the introduction. This course is lab-intensive, and in this Section, you will begin your hands-on approach with a first-time installation using standalone and distributed topologies.

Objectives

1. Use command `fw ctl chain` to study chain module behavior. Observe how policy changes impact the chain.
2. Use the command `fw debug fwm on` and review the file `fwm.elg` to find such issues as SIC, mis-configured rules, GUI client connectivity problems, and improperly entered information.
3. Given a specific internal or client need, analyze and apply the appropriate hot fix and evaluate its effectiveness.
4. Use Check Point Debugging Tools

Do you know ...

- What the `IP Options Strip` represents under the `fw chain` output?
- How to explain the command `fw ctl chain` function?
- What command shows which firewall chain modules are active on a gateway.
- Why `fw debug` commands should always be followed with an "off" parameter after capturing troubleshooting data?
- What flag option(s) must be useed to dump the complete table in friendly format, assuming the connections in the table are more than 100?
- Which directory contains the URL Filtering engine update info?
- What table is used to contain the URLF cache values for URL Filtering in the Cloud in R75 and above?
- What command would you issue in order to show all the chains through which traffic passed?
- Which commands will properly set the debug level to maximum and then run a policy install in debug mode for the policy Standard on gateway A-GW from an R77 Gaia Management Server?
- Which commands obtain information about the mis-configuration issues that point to the rule base.
- What following command would help you understand which chain is causing a problem on the Security Gateway, you use?
- Which process should you debug when SmartDashboard authentication is rejected?
- Where fwm debug logs are written?

Section 3: Network Address Translation

Check Point technology is designed to address network exploitation, administrative flexibility and critical accessibility. This Section introduces the basic concepts of network security and management based on Check Point's three-tier structure, and provides the foundation for technologies involved in the Check Point Architecture. These objectives and study questions provide a review of important concepts.

Objectives

1. Use commands `fw ctl debug` and `fw monitor` to troubleshoot the NAT stages of Automatic Hide NAT and Automatic Static NAT.
2. Configure Manual NAT to define specific rules in unique NAT environments.

Do you know ...

- How to confirm if traffic is actually being dropped by the gateway when unsuccessfully attempting to establish an FTP session between your computer and a remote server?

- What this `fw ctl zdebug drop` output tells while troubleshooting a DHCP relay issue?

  ```
  ;[cpu_1];[fw_0];fw_log_drop: Packet proto=17 10.216.14.108:67 ->
  172.31.2.1:67 dropped by fw_handle_first_packet Reason:
  fwconn_init_links (INBOUND) failed;
  ```

  Where `10.216.14.108` is the IP address of the DHCP server and `172.31.2.1` is the VIP of the Cluster.

- What flags to use for the kernel debug when trying to troubleshoot a NAT issue on your network, and you need to verify that a connection is correctly translated to its NAT address?

- Which FW-1 kernel flags should be used to properly debug and troubleshoot NAT issues?

- Which file should be edited to modify ClusterXL VIP hide NAT rules? Where is it located?

- What `table.def` file should you edit to hide FTP traffic behind the virtual IP of a cluster? Where would it be located?

- What does a `tcpdump` on the external interface of the gateway, that only shows ARP requests coming from the upstream router, tell you about a connectivity issue with an internal web server? You know that packets are getting to the upstream router.

Section 4: ClusterXL

Objectives

1. Using commands `fw ctl debug` and `fw ctl kdebug` troubleshoot ClusterXL connections from information displayed in debug file.
2. Use commands `fw tab -t connections` and `fw tab -t connections -x` to review and clear connections table.
3. Modify file `table.def` to allow traffic through a specific cluster member.

Do you know ...

- What the state of an active gateway will be using the command `clusterXL_admin` up with default ClusterXL settings?
- Which command you should use to stop kernel module debugging (excluding SecureXL)?
- Which command you should run to debug the VPN-1 kernel module?
- Which command can be used to see all active modules on the Security Gateway?
- What command you should invoke to change from multicast to broadcast.
- What must be done to ensure proxy arps for both manual and automatic NAT rules function when you have edited the local.arp configuration, to support a manual NAT?
- What command clears all the connection table entries on a security gateway
- How you can see a dropped connection and the cause from the kernel?
- The elements of the 6-tuple when viewing connections using the '*fw tab -t connections*' command?
- How the symbolic link entries point back to the real entry?
- How you would prevent outgoing NTP traffic from being hidden behind a Cluster IP?
- Which command would be best suited for viewing the connections table on a gateway?

- What this `cphaprob -i list` output tells you about clustering issues?

```
Clusterb> cphaprob -i list
Built-in Devices:
Device Name: Interface Active Check Current state: OK
Device Name: HA Initialization Current state: OK
Device Name: Recovery Delay Current state: OK
Registered Devices:
Device Name: Synchronization Registration number: 0 Timeout:
none Current state: OK Time since last report: 3651.5 sec
Device Name: Filter Registration number: 1 Timeout: none Current
state: problem Time since last report: 139 sec
Device Name: routed Registration number: 2 Timeout: none Current
state: OK Time since last report: 3651.9 sec
Device Name: cphad Registration number: 3 Timeout: none Current
state: OK Time since last report: 3696.5 sec
Device Name: fwd Registration number: 4 Timeout: none Current
state: OK Time since last report: 3696.5 sec
```

- Which command you would use to verify table connection info (peak, concurrent) and verify information about cluster synchronization state?

- The functions of the file `table.def`?

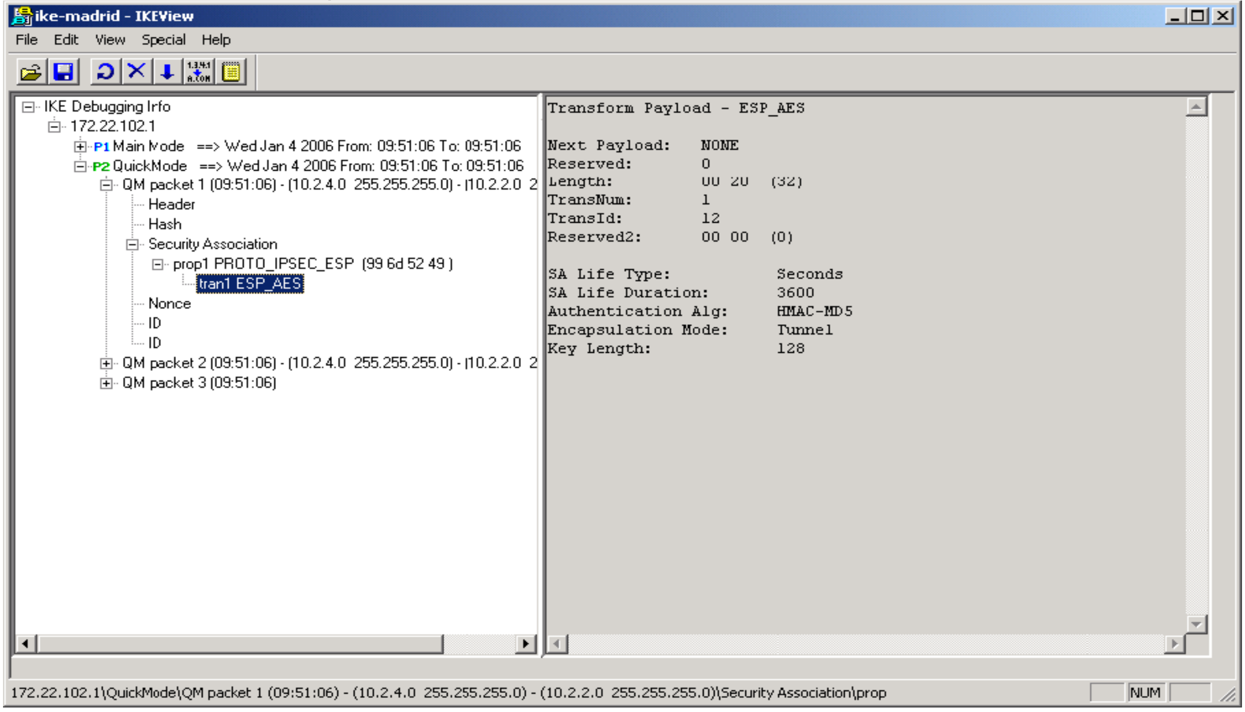
Section 5: VPN Troubleshooting

Objectives

1. Use command `vpn debug` to locate source of encryption failures.
2. Use command `fw monitor` to verify VPN connectivity and identify potentially mis-configured VPN's.

Do you know ...

- Which command you run to list established VPN tunnels?
- Where the log file used to log IKE negotiations during VPN tunnel establishment is located?
- Which command displays compression/decompression statistics?
- What debug file you would look at to see what IKE version is being used?
- What file contains IKEv2 debug messages?
- What log file shows the keep alive packets during the debug process?
- What log file shows the processes that participate in the tunnel initiation stage?
- Which program you use to analyze Phase I and Phase II packet exchanges?
- What this IKEView output tells us about QuickMode Packet 1?



```
⊟ IKE Debugging Info
   ⊟ 172.22.102.1
      ⊞ P1 Main Mode   ==> Wed Jan 4 2006 From: 09:51:06 To: 09:51:06
      ⊟ P2 QuickMode   ==> Wed Jan 4 2006 From: 09:51:06 To: 09:51:06
         ⊟ QM packet 1 (09:51:06) - (10.2.4.0  255.255.255.0) - (10.2.2.0  2
               Header
               Hash
            ⊟ Security Association
               ⊟ prop1 PROTO_IPSEC_ESP  (99 6d 52 49 )
                     tran1 ESP_AES
               Nonce
               ID
               ID
         ⊞ QM packet 2 (09:51:06) - (10.2.4.0  255.255.255.0) - (10.2.2.0  2
         ⊞ QM packet 3 (09:51:06)
```

```
Transform Payload - ESP_AES

Next Payload:   NONE
Reserved:       0
Length:         00 20   (32)
TransNum:       1
TransId:        12
Reserved2:      00 00   (0)

SA Life Type:           Seconds
SA Life Duration:       3600
Authentication Alg:     HMAC-MD5
Encapsulation Mode:     Tunnel
Key Length:             128
```

```
172.22.102.1\QuickMode\QM packet 1 (09:51:06) - (10.2.4.0  255.255.255.0) - (10.2.2.0  255.255.255.0)\Security Association\prop     NUM
```

- What files you want to analyze after running a VPN debug on a problematic gateway?
- What mode in a VPN configuration, can be used to increase throughput by bypassing firewall enforcement?

- Which of the following debug logs is essential When VPN user-based authentication fails?

- The most likely cause when you get a drop log that states “No proposal chosen”?
- What is never affected by incorrect OS time and date configuration when troubleshooting VPNs?

- The issue when you notice on the output of "fw monitor -e "host(172.21.1.10), accept;"" that packets are going through the inbound chain (i -> I) and then disappearing after the outbound chain (o -> __), while you were expecting to see the packet leave on O.

- What is the best solution for site-to-site-VPN connections when you see the SmartLog error message: *Encryption failure: Clear text packet should be encrypted*

- How to completely shut down a VPN between two security gateways?

- The things that can be done with the command `vpn tu`?

- How to generate the vpn.elg file to troubleshoot VPN related issues?

- Which folder contains the VPN debug files?

Section 6: SecureXL Acceleration debugging

Objectives

1. Use commands `fw accel` and `kernel debug` to view acceleration tables and verify accelerated connections.

Do you know ...

- What command you should run to determine if Accept, Drop and NAT templating is enabled?
- What command should be used to determine on what rule templates are disabled?
- What effect a TIME object has on the following rules?
- What information the command `fwaccel stat` displays?
- How you initialize the debug buffer to 48000 when running a SecureXL debug?
- What command you would use to determine if a particular connection is being accelerated by SecureXL?
- What process the firewall starts when a new packet has arrived to the interface and finds no match when compared with the connection table?
- How to check the overall SecureXL statistics?
- When rules, that include identity awareness access roles, are accelerated through SecureXL?
- Why the command `fw monitor -e accept dport = 443` would NOT show the TCP ack packet when engaged in connection troubleshooting?
- When rules including Identity Awareness Access (IDA) roles are accelerated through SecureXL?
- The BEST way to start the analysis for optimizing a customer firewall rule base?
- The F flag's meaning in the output of "fwaccel conns"?
- What command displays a summary of connections accelerated versus those that are not?
- The principle theory behind the SecureXL function?
- How SecureXL can be enabled or disabled?

Section 7: Hardware Optimization

Objectives

1. Identify the correct Check Point Hardware/Appliances for a given scenario
2. Performance tuning and evaluation of complex networks and technologies
3. Scope proper sizing of hardware based on customer requirements

4. Use command `ethtool` to tune NIC performance.
5. Edit `arp cache` table to increase size to improve performance.
6. Use command `fw ctl pstat` to improve load capacity.
7. Use the `fwaccel stat` and `fwaccel stats` outputs to tune the firewall rule base.

Do you know ...

- The expected ClusterXL status in an HA cluster, when you modify the number of cores given to CoreXL, on only one member using `cpconfig` and then reboot?

- Which information CANNOT be displayed by using the command `cat /proc/cpuinfo?`

- What happens to manual changes in the $FWDIR/conf/local.arp file when adding Proxy ARP entries through the GAiA portal or Clish?

- What causes the kernel message: `kernel: neighbor table overflow`?

- Which of the following commands would show you the current and peak connection counts in Smart Dashboard?

- What does `the` command `fwaccel templates` do?

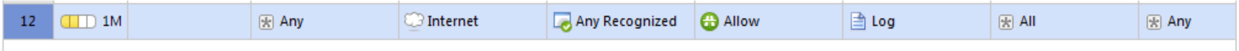
- Running the command `fw ctl pstat -l` would return what information?

- The best way to find which physical interface matches to interface names (eth1, eth2 etc.)?

- What information the command fw ctl pstat shows ?

- How to check which firewall module causes the latency when a client from IP address 168.128.10.11 tries to access the DMZ server going through the firewall?

- What problems this rule could potentially create in a customer's Application Control/URL filtering policy?



12	1M		Any	Internet	Any Recognized	Allow	Log	All	Any

Section 8: Software Tuning

Objectives

1. Deploy NAT templates to reduce load on Rule Base application.
2. Configure cluster synchronization planning to improve network performance.
3. Identify performance limiting configurations
4. Correct and tune different scenarios
5. Identify the causes of performance limiting factors (internal and external factors)

Do you know ...

- How Check Point security administrator enables NAT Templates?
- What you should do after editing `fwkern.conf` to enable NAT templates?
- How you would determine the value of 'Maximum concurrent connections' of the NAT Table?
- Which commands you would use to enable NAT Templates “on the fly”?
- What `cphwd_nat_templates_enabled=1` does when entered into `fwkern.conf`?
- How to check cluster status on two gateways running in HA mode?
- Which command displays FireWall internal statistics about memory and traffic?
- What command checks what is currently set in the Firewall kernel debug?
- What commands sync the connections table with the Active member?
- The best way to see how a firewall is performing while processing packets in the firewall path, including resource usage?
- the best way to see how much traffic went through the firewall that was TCP, UDP and ICMP?
- Which file holds global Kernel values to survive reboot in a Check Point R77 gateway?
- What file determines how NAT acceleration templates are deployed?

Section 9: Enable CoreXL

Objectives

1. Configure CoreXL for specific cpu task assignment.

Do you know ...

- The responsibilities of the Secure Network Dispatcher (SND)?

- The method to change the number of cores that CoreXL will use?

- The command to verify what core each gateway interface and firewall instance is currently running on?

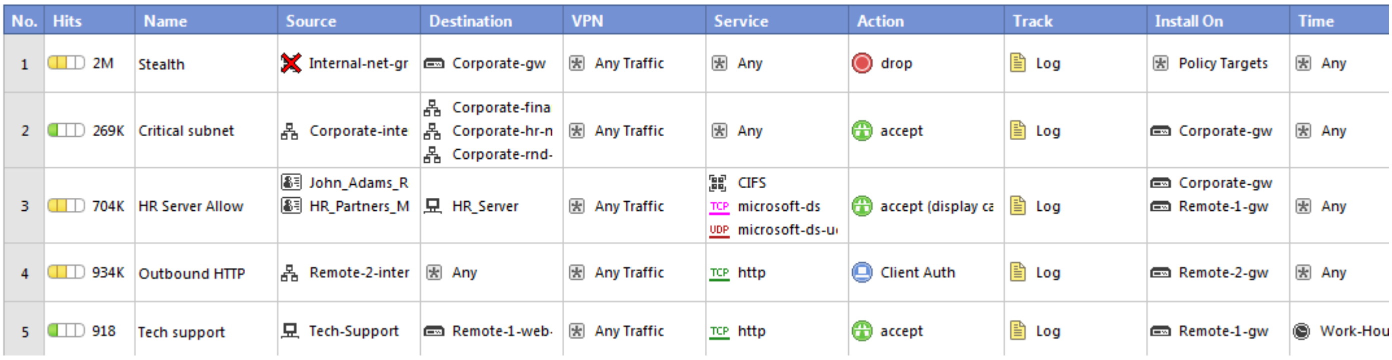
- The correct process to increase the number of processing cores on a Check Point security gateway and the number of kernel instances?

- What command displays the Connections Table for specified CoreXL FW instance

- Why would you not see a CoreXL configuration option in `cpconfig`?

- Where would you go to adjust the number of Kernels in CoreXL?

- Which rule disables SecureXL in the policy below?



No.	Hits	Name	Source	Destination	VPN	Service	Action	Track	Install On	Time
1	2M	Stealth	☒ Internal-net-gr	Corporate-gw	Any Traffic	Any	● drop	Log	Policy Targets	Any
2	269K	Critical subnet	Corporate-inte	Corporate-fina Corporate-hr-n Corporate-rnd-	Any Traffic	Any	accept	Log	Corporate-gw	Any
3	704K	HR Server Allow	John_Adams_R HR_Partners_M	HR_Server	Any Traffic	CIFS TCP microsoft-ds UDP microsoft-ds-u	accept (display ca	Log	Corporate-gw Remote-1-gw	Any
4	934K	Outbound HTTP	Remote-2-inter	Any	Any Traffic	TCP http	Client Auth	Log	Remote-2-gw	Any
5	918	Tech support	Tech-Support	Remote-1-web-	Any Traffic	TCP http	accept	Log	Remote-1-gw	Work-Hou

- What is the command to check the number of connections each core is processing when troubleshooting a performance problem on multicore firewall that is using CoreXL?

- What command you would use to check if CoreXL is enabled?

- Which command will allow you to change firewall affinity and survive a reboot with no further modification?

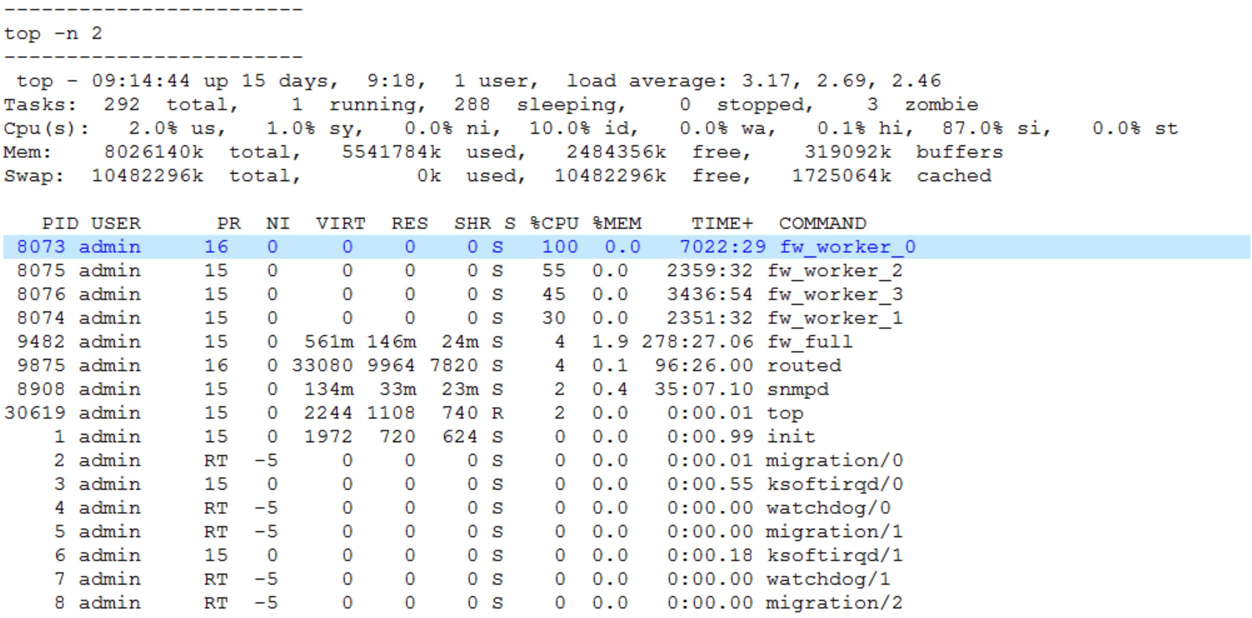
- What command you could run if you suspect that the number of cores are not matched on both cluster members.

- What the following command and output tell you about system performance problems?

```
fw affinity -l -a -v
Output:
Interface eth0 (irq 154): CPU 0
Interface eth1 (irq 178): CPU 1
Interface eth2 (irq 202): CPU 2
Interface eth4 (irq 59): CPU 3
Interface eth5 (irq 83): CPU 4
Interface eth6 (irq 107): CPU 5
Interface eth7 (irq 131): CPU 6
Kernel fw_0: CPU 7
Kernel fw_1: CPU 3
Kernel fw_2: CPU 6
Kernel fw_3: CPU 2
Kernel fw_4: CPU 5
Kernel fw_5: CPU 1
```

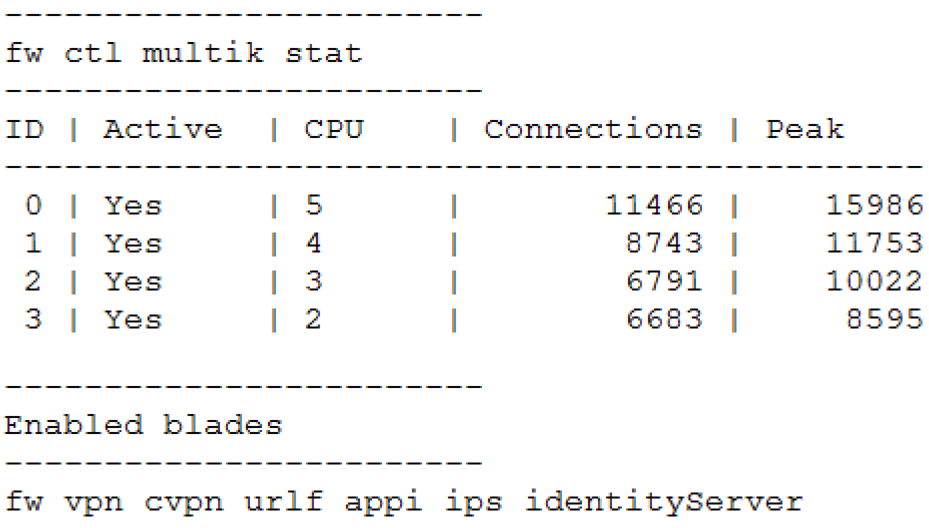
- What the command `fw ctl multik stat` shows?

- What do these commands/output tell you about system performance?



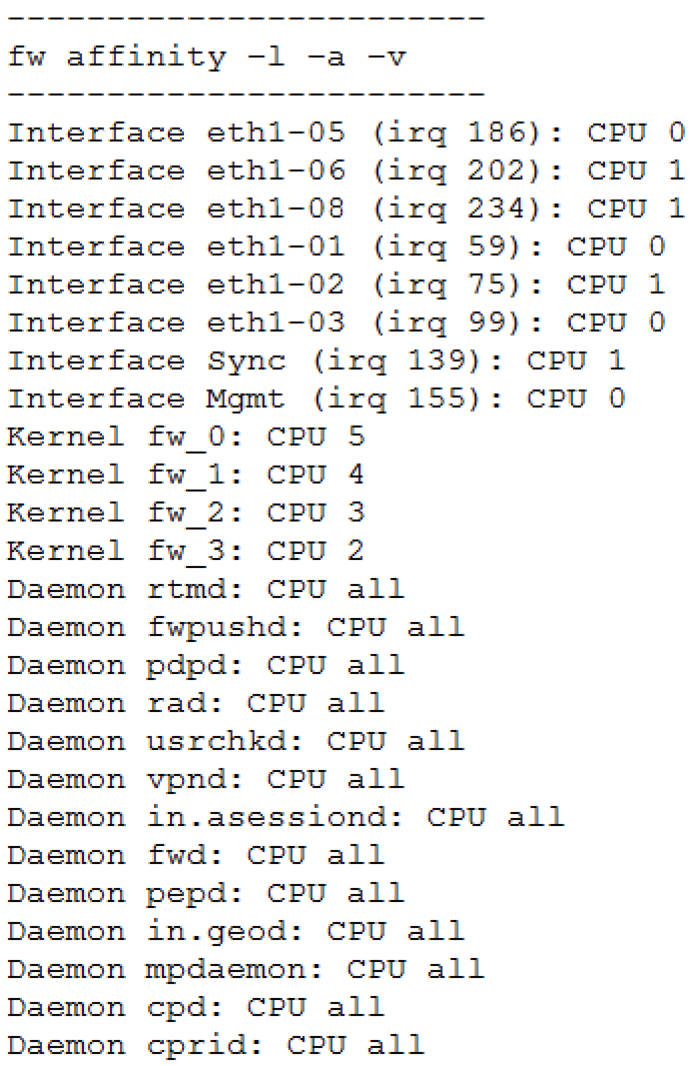
```
------------------------
top -n 2
------------------------
 top - 09:14:44 up 15 days,  9:18,  1 user,  load average: 3.17, 2.69, 2.46
Tasks:  292  total,    1  running,  288  sleeping,    0  stopped,    3  zombie
Cpu(s):   2.0% us,   1.0% sy,   0.0% ni,  10.0% id,   0.0% wa,   0.1% hi,  87.0% si,   0.0% st
Mem:    8026140k  total,   5541784k  used,   2484356k  free,    319092k  buffers
Swap:  10482296k  total,         0k  used,  10482296k  free,   1725064k  cached

   PID USER      PR  NI  VIRT  RES   SHR S %CPU %MEM    TIME+  COMMAND
  8073 admin     16   0     0    0     0 S  100  0.0   7022:29 fw_worker_0
  8075 admin     15   0     0    0     0 S   55  0.0   2359:32 fw_worker_2
  8076 admin     15   0     0    0     0 S   45  0.0   3436:54 fw_worker_3
  8074 admin     15   0     0    0     0 S   30  0.0   2351:32 fw_worker_1
  9482 admin     15   0  561m 146m   24m S    4  1.9 278:27.06 fw_full
  9875 admin     16   0 33080 9964  7820 S    4  0.1  96:26.00 routed
  8908 admin     15   0  134m  33m   23m S    2  0.4  35:07.10 snmpd
 30619 admin     15   0  2244 1108   740 R    2  0.0   0:00.01 top
     1 admin     15   0  1972  720   624 S    0  0.0   0:00.99 init
     2 admin     RT  -5     0    0     0 S    0  0.0   0:00.01 migration/0
     3 admin     15   0     0    0     0 S    0  0.0   0:00.55 ksoftirqd/0
     4 admin     RT  -5     0    0     0 S    0  0.0   0:00.00 watchdog/0
     5 admin     RT  -5     0    0     0 S    0  0.0   0:00.00 migration/1
     6 admin     15   0     0    0     0 S    0  0.0   0:00.18 ksoftirqd/1
     7 admin     RT  -5     0    0     0 S    0  0.0   0:00.00 watchdog/1
     8 admin     RT  -5     0    0     0 S    0  0.0   0:00.00 migration/2
```



```
------------------------
fw ctl multik stat
------------------------
ID | Active  | CPU    | Connections | Peak
----------------------------------------------
 0 | Yes     | 5      |       11466 |   15986
 1 | Yes     | 4      |        8743 |   11753
 2 | Yes     | 3      |        6791 |   10022
 3 | Yes     | 2      |        6683 |    8595

------------------------
Enabled blades
------------------------
fw vpn cvpn urlf appi ips identityServer
```



```
------------------------
fw affinity -l -a -v
------------------------
Interface eth1-05 (irq 186): CPU 0
Interface eth1-06 (irq 202): CPU 1
Interface eth1-08 (irq 234): CPU 1
Interface eth1-01 (irq 59): CPU 0
Interface eth1-02 (irq 75): CPU 1
Interface eth1-03 (irq 99): CPU 0
Interface Sync (irq 139): CPU 1
Interface Mgmt (irq 155): CPU 0
Kernel fw_0: CPU 5
Kernel fw_1: CPU 4
Kernel fw_2: CPU 3
Kernel fw_3: CPU 2
Daemon rtmd: CPU all
Daemon fwpushd: CPU all
Daemon pdpd: CPU all
Daemon rad: CPU all
Daemon usrchkd: CPU all
Daemon vpnd: CPU all
Daemon in.asessiond: CPU all
Daemon fwd: CPU all
Daemon pepd: CPU all
Daemon in.geod: CPU all
Daemon mpdaemon: CPU all
Daemon cpd: CPU all
Daemon cprid: CPU all
```

Section 10: IPS

Objectives

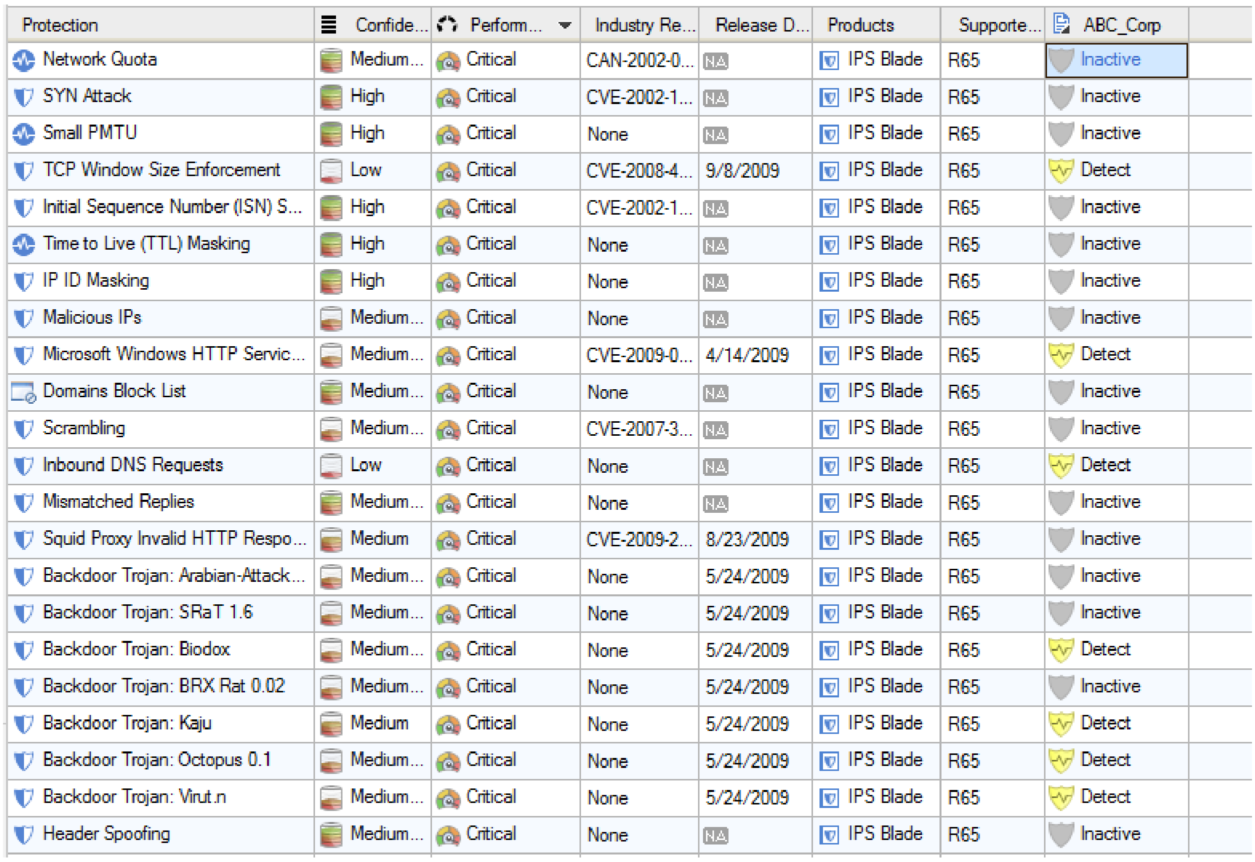
1. Configure IPS to reduce false positives.
2. Use command `fw ctl zdebug` to improve logging efficiency.
3. Use IPS Bypass to improve performance.

Do you know ...

- Which actions prevent TCP-ACK packets continuing indefinitely back and forth and thus creating an "ACK storm"?

- Where you enable INSPECT debugging?

- What we can understand from this IPS profile output regarding the performance of the environment?



Protection	Confide...	Perform...	Industry Re...	Release D...	Products	Supporte...	ABC_Corp
Network Quota	Medium...	Critical	CAN-2002-0...	N/A	IPS Blade	R65	Inactive
SYN Attack	High	Critical	CVE-2002-1...	N/A	IPS Blade	R65	Inactive
Small PMTU	High	Critical	None	N/A	IPS Blade	R65	Inactive
TCP Window Size Enforcement	Low	Critical	CVE-2008-4...	9/8/2009	IPS Blade	R65	Detect
Initial Sequence Number (ISN) S...	High	Critical	CVE-2002-1...	N/A	IPS Blade	R65	Inactive
Time to Live (TTL) Masking	High	Critical	None	N/A	IPS Blade	R65	Inactive
IP ID Masking	High	Critical	None	N/A	IPS Blade	R65	Inactive
Malicious IPs	Medium...	Critical	None	N/A	IPS Blade	R65	Inactive
Microsoft Windows HTTP Servic...	Medium...	Critical	CVE-2009-0...	4/14/2009	IPS Blade	R65	Detect
Domains Block List	Medium...	Critical	None	N/A	IPS Blade	R65	Inactive
Scrambling	Medium...	Critical	CVE-2007-3...	N/A	IPS Blade	R65	Inactive
Inbound DNS Requests	Low	Critical	None	N/A	IPS Blade	R65	Detect
Mismatched Replies	Medium...	Critical	None	N/A	IPS Blade	R65	Inactive
Squid Proxy Invalid HTTP Respo...	Medium	Critical	CVE-2009-2...	8/23/2009	IPS Blade	R65	Inactive
Backdoor Trojan: Arabian-Attack...	Medium...	Critical	None	5/24/2009	IPS Blade	R65	Inactive
Backdoor Trojan: SRaT 1.6	Medium...	Critical	None	5/24/2009	IPS Blade	R65	Inactive
Backdoor Trojan: Biodox	Medium...	Critical	None	5/24/2009	IPS Blade	R65	Detect
Backdoor Trojan: BRX Rat 0.02	Medium...	Critical	None	5/24/2009	IPS Blade	R65	Inactive
Backdoor Trojan: Kaju	Medium	Critical	None	5/24/2009	IPS Blade	R65	Detect
Backdoor Trojan: Octopus 0.1	Medium...	Critical	None	5/24/2009	IPS Blade	R65	Detect
Backdoor Trojan: Virut.n	Medium...	Critical	None	5/24/2009	IPS Blade	R65	Detect
Header Spoofing	Medium...	Critical	None	N/A	IPS Blade	R65	Inactive

- Which of the two initial IPS profiles is the more resource intensive?

- What does a high confidence rating mean in IPS?

- Under what circumstances IPS bypass would be enforced?

- What feature you would configure to disable inspection if a high cpu usage develops when your Customer enables IPS inspection in his Corporate Cluster?

- The best process for making changes on the Enterprise gateway only in the following scenario?
    - You have created a number of profiles and activated the relevant protections.
    - Afterwards, you decide that the ‘Enterprise gateway’ should allow instant messaging.
    - The current profile enabled for Enterprise gateway blocks instant messaging.
    - The profile for the Enterprise gateway is currently being used on the Voyager gateway and the Bird of Prey gateway.

Section 11: IPV6

Objectives

1. Deploy IPV6 in a local environment

Do you know ...

- What command displays the IPV6 routes?

- What command displays the IPV6 status?

- How to erase all IPV6 connection tables?

- How to configure the sync interface in a ClusterXL that uses IPV6 Addressing?

- The command to monitor IPV6 packets in a kernel module?

- If it is possible to operate a security gateway entirely with IPV6 addressing?

Section 12: Advanced VPN

Objectives

1. Identify differences between route-based VPNs and domain-based VPNs.
2. Configure VTI for route-based VPN gateways.
3. Configure OSPF for Dynamic VPN routing in a Community.
4. Identify the Wire Mode function by testing a VPN failover.
5. Configure Directional VPN Rule Match for Route-Based VPN.

Do you know ...

- What features are supported with *unnumbered* and *numbered* VTI's?

- Why information would be missing in the following scenario? Under the gateway object topology you select "Get All Members Interfaces with Topology". Upon checking, you find your newly configured unnumbered VTIs are not populated.

- Whether unnumbered VTIs support load sharing clustering?

- How you can enable the required gated daemon when you want to enable OSPF on Secure Platform?

- How you add the route entry for the "Enforcement Point Gateway" on the management server?

- How to describe the way the "Directional Enforcement" rule manages subsequent packet inspections?

- Why the route-based tunnel would NOT come up in the following scenario? You configure VTIs in a clustered environment. On peer A the VTI name is VT_Cluster_GWA and on peer B the VTI name is VT_Cluster_GWB.

- Why the command `show running-config` would NOT list your OSPF configuration when you -
  - configure OSPF on your Secure Platform firewall.
  - run the following commands in expert mode:
    ```
    interface vt-Gateway_C
    IP ospf 1 area 0.0.0.0
    exit
    ```

- Whether the firewall will perform Stateful inspection in wire mode if a packet from a trusted source reaches the gateway and is going to a trusted destination,?

- How you designate the *Enforcement Point Gateway* for the peers involved in *VPN Directional Enforcement*?

- How you can restrict access based on destination in an IPV6 environment when you have two additional requirements?

  - access control
  - new directional VPN rules.

- Why the “Directional Match Condition” option is missing when you enable “VPN Directional Match” on the VPN column?

Section 13: Dynamic Routing

Objectives

1. Diagnose and solve specific routing issues in a network environment.
2. Multicast Design and troubleshooting PIM Sparse mode and Dense mode based on GateD and IPSRD
3. Design/troubleshoot OSPF/BGP in GateD and IPSO IPSRD environments
4. Static routing and network topologies

Do you know ...

You are having issues with dynamic routing after a failover. The traffic is now coming from the backup and is being dropped as out of state. What is the best configuration to avoid stateful inspection dropping your dynamic routing traffic?

Why a Check Point Certified Security Master would choose to combine dynamic routing protocols and VPNs?

Why OSPF adjacencies would not establish when you are configuring dynamic VPN routing using OSPF? You have:

- defined the gateways,
- created a fully meshed VPN Community that includes all participating Gateways;
- created a rule to accept OSPF, and
- configured dynamic routing.

What issues could prevent the dynamic routing daemon from starting while configuring dynamic routing on SecurePlatform? You run the command `pro enable` and reboot.

Conclusion

You knew all that?

Already have your CCSE R7X?

Does your Pearson VUE profile email address match your User Center profile email address?

Then you are ready. Go to Pearson VUE and request exam 156-115.77.

Good testing!