Dhansham - Engineer's Notebook Checkpoint Firewalls Gaia

Over three decades of Information Technology experience, specializing in High Performance Networks, Security Architecture, E-Commerce Engineering, Data Center Design, Implementation and Support

Thursday, April 6, 2017

Checkpoint R80.10 - Command Line Cheat sheet

Check Point Environment variables (most common ones)
$FWDIR FW-1 ---installation directory, with f.i. the conf, log, lib, bin and spool directories. You will mostly work in this tree.
$CPDIR ---SVN Foundation / cpshared tree.
$CPMDIR ---Management server installation directory.
$FGDIR ---FloodGate-1 installation directory.
$MDSDIR ---MDS installation directory. Same as $FWDIR on MDS level.
$FW_BOOT_DIR ---Directory with files needed at boot time.

Basic starting and stopping
cpstop ---Stop all Check Point services except cprid. You can also stop specific services by issuing an option with cpstop.
cpstart ---Start all Check Point services except cprid. cpstart works with the same options as cpstop.
cprestart ---Combined cpstop and cpstart. Complete restart.
cpridstop ---Stop cprid, the Check Point Remote installation Daemon.
cpridstart ---Start cprid, the Check Point Remote installation Daemon.
cpridrestart ---Combined cpridstop and cpridstart.
fw kill [-t sig] proc_name ---Kill a Firewall process. PID file in $FWDIR/tmp/ must be present. Per default sends signal 15 (SIGTERM).
Example: fw kill -t 9 fwm
fw unloadlocal ---Uninstall local security policy and disables forwarding.

Basic firewall information gathering

fw ver ---Check FW-1/VPN-1 major and minor version as well as build number and latest installed hotfix.
fwm ver ---Check management module major and minor version as well as build number and latest installed hotfix.
vpn ver ---Check VPN-1 major and minor version as well as build number and latest installed hotfix. Use the switch -k for additional kernel version.
cpshared_ver ---Show the version of the SVN Foundation.
fw stat ---Show the name of the currently installed policy as well as a brief interface list. Can be used with the -long or -short switch for more information.
cpwd_admin list ---Display process information about CP processes monitored by the CP WatchDog.
fw ctl iflist ---Display interface list.
fw ctl arp [-n] ---Display proxy arp table. -n disables name resolution.

Modems
MPLS
MST
Multicast
Multicast (routing)
NAT & PAT
NetFlow
NTP
OSPF
PfR & OER
Port Channels
PPP
PPPoE
Prefix Lists
QoS
Redistribution
RIPv2
RITE
RMON
Route Maps
RSTP
SCP
Security
SNMP
SPAN & RSPAN
SSH
STP
Summarization
Switching Paths
Virtual LANs

fw ctl pstat ---Display internal statistics including information about memory, inspect, connections and NAT.
fw ctl chain ---Displays in and out chain of CP Modules. Useful for placing fw monitor into the chain with the -p option.
fw ctl zdebug drop ---Real time listing of dropped packets.
cp_conf sic state ---Display current SIC trust state.
cp_conf lic get ---View licenses.
cp_conf finger get ---Display fingerprint on the management module.
cp_conf client get ---Display GUI clients list.
cp_conf admin get ---Display admin accounts and permissions. Also fwm -p
---

Basic firewall information gathering
cp_conf auto get all ---Display auto state of all products. Also works with fw1, fg1 and rm instead of all.
cpstat <app_flag> [-f flavour] ---Display status of the CP applications. Command has to be used with a application flag app_flag and an optional flavour. Issue cpstat without any options to see all possible application flags and corresponding flavours.
Examples:
cpstat fw -f policy —-verbose policy info
cpstat fw -f sync —-Synchronisation statistics
cpstat os -f cpu —-CPU utilization statistics
cpstat os -f memory —-Memory usage info
cpstat os -f ifconfig —-Interface table
fgate stat ---Status and statistics of Flood-Gate-1.
fwaccel <stat|stats|conns> ---Status and statistics or connection table of SecureXL.
cpinfo -z -o <file> ---Create a compressed cpinfo file to open with the InfoView utility or to send to Check Point support.
fw hastat ---View HA state of local machine.
cphaprob state ---View HA state of all cluster members.
vpn overlap_encdom ---Show, if any, overlapping VPN domains.
fw tab –t <tbl> [–s] ---View kernel table contents. Make output short with -s switch. List all available tables with fw tab -s. E.g.
fw tab -t connections -s ---Connections table.
avsu_client [-app <app>] get_version ---Get local signature version and status of content security <app> where <app> can be “Edge AV”, “URL Filtering” and “ICS”. Without the -app <app> option “Anti Virus” is used by default.
avsu_client [-app <app>] fetch_remote -fi ---Check if signature for <app> is up-to-date. See previous command for the possible values of <app>.
show asset hardware View hw info like serial numbers in Nokia clish. See also ipsctl -a and cat /var/etc/.nvram.
info device View Edge Appliance information (hw, fwl, license..)
info computers List active devices behind Edge Appliance.

View and manage logfiles
fw lslogs ---View a list of available fw logfiles and their size.
fwm logexport ---Export/display current fw.log to stdout.
fw logswitch [-audit] ---Write the current (audit) logfile to YY-MM-DDHHMMSS. log and start a new fw.log.
fw log -c <action> ---Show only records with action <action>, e.g. accept, drop, reject etc. Starts from the top of the log, use -t to start a tail at the end.
fw log -f -t ---Tail the actual log file from the end of the log. Without the -t switch it starts from the beginning.

► March (3)
► February (2)
► 2016 (52)

fw log -b <starttime> <endtime> ---View today's log entries between <starttime> and <endtime>.
Example:
fw log -b 09:00:00 09:15:00.
fw fetchlogs -f <file> module ---Fetch a logfile from a remote CP module. NOTICE: The log will be moved, hence deleted from the remote module. Does not work with current fw.log.
fwm logexport -i in.log -o out.csv -d ',' -p -n ---Export logfile in.log to file out.csv, use , (comma) as delimiter (CSV) and do not resolve services or hostnames.

Display and manage licenses
cp_conf lic get ---View licenses.
cplic print ---Display more detailed license information.
fw lichosts ---List protected hosts with limited hosts licenses. dtps lic SecureClient Policy Server license summary.
cplic del <sig> <obj> ---Delete CP license with signature sig from object obj.
cplic get <ip host|-all> ---Retrieve all licenses from a certain gateway or all gateways in order to synchronize license repository on the SmartCenter server with the gateway(s).
cplic put <-l file> ---Install local license from file to an local machine.
cplic put <obj> <-l file> ---Attach one or more central or local licenses from file remotely to obj.
cprlic ---Remote license management tool.

ClusterXL
ATRG -- sk93306
cp_conf ha enable|disable [norestart] ---Enable or disable HA.
cphastop ---Disable ClusterXL on the cluster member. Issued on a cluster member running in HA Legacy Mode cphastop might stop the entire cluster.
cphastart ---Activate ClusterXL on this cluster member.
fw hastat ---View HA state of local machine.
cphaprob state ---View HA state of all cluster members.
cphaprob -a if ---View interface status.
cphaprob -ia list ---View list and state of critical cluster devices.
cphaprob syncstat ---View sync transport layer statistics. Reset with -reset.
cphaconf set_ccp <broadcast|multicast> ---Configure Cluster Control Protocol (CCP) to use unicast or multicast messages. By default set to multicast. Setting survives reboot.
clusterXL_admin <up|down> ---Perform a graceful manual failover by registering a faildevice.
Note: DO NOT run any cphaconf commands other than set_ccp

SecureXL
ATRG --sk98722
fwaccel on
fwaccel off ---"-q" flag suppresses the output
"-a" flag means to start acceleration on all Virtual Systems
fwaccel ver
fwaccel stat
fwaccel stats -s Prints the acceleration statistics for Network Access Control (NAC)
fwaccel stats -d Prints the acceleration statistics for dropped packets
fwaccel stats -n
fwaccel stats -p Prints the acceleration statistics for SecureXL violations (F2F packets)

fwaccel stats -l Prints all acceleration statistics in Legacy mode (output is not divided into sections)

fwaccel stats -m Prints the acceleration statistics for multicast traffic
fwaccel stats -r Resets all acceleration statistics
fwaccel conns Prints the SecureXL Connections Table ('cphwd_db')

CoreXL
ATRG: CoreXL --sk98737
fw ctl multik --Controls CoreXL FW instances
fw ctl multik ---Prints the general help message with available parameters
fw ctl multik stat ---Prints the summary table for CPU cores and CoreXL FW instances
fw ctl multik start ---Starts CoreXL
fw -i Instance_ID ctl multik start ----Starts specific CoreXL FW instance
fw ctl multik stop ---Stops CoreXL
fw -i Instance_ID ctl multik stop ---Stops specific CoreXL FW instance
fw ctl affinity <options> ---Controls CoreXL affinities of interfaces / processes / CoreXL FW instances to CPU cores
fw ctl affinity ---Prints the help message with available options
fw -d ctl affinity -corelicnum ---Prints the number of system CPU cores allowed by CoreXL license
fw ctl affinity -l ---Prints the current CoreXL affinities - output shows affinities of interfaces/processes/CoreXL FW instances to CPU cores
fw ctl affinity -l -r ---Prints the current CoreXL affinities in reverse order - output shows CPU cores and which interface/process/CoreXL FW instance is affined to each CPU core
fw ctl affinity -l -a ---Prints all current CoreXL affinities - output shows affinities of interfaces/processes/CoreXL FW instances to CPU cores, and also shows targets without specific affinity
fw ctl affinity -l -v ---Prints the current CoreXL affinities - verbose output shows affinities of interfaces/processes/CoreXL FW instances to CPU cores (targets are shown as 'Interface' (with IRQ), 'Kernel', 'Process'
fw ctl affinity -l -q ---Prints the current CoreXL affinities - output shows affinities of interfaces/processes/CoreXL FW instances to CPU cores, and suppresses errors
fw ctl affinity -l -r -a -v ---Prints the current CoreXL affinities - verbose output that combines all possible outputs (shows all targets in reverse order) fw ctl affinity -l -p PID [-r] [-a] [-v] Prints the current CoreXL affinity of the specified process (by PID) to CPU cores
fw ctl affinity -l -n Daemon_Name [-r] [-a] [-v] ---Prints the current CoreXL affinity of the specified process (by name [maximal length = 255 characters]) to CPU cores
fw ctl affinity -l -k Instance_ID [-r] [-a] [-v] ---Prints the current CoreXL affinity of the specified CoreXL FW instance to CPU cores
fw ctl affinity -l -i Interface_Name [-r] [-a] [-v] ---Prints the current CoreXL affinity of the specified interface to CPU cores
fw ctl affinity -s <target> { CPU_ID [CPU_ID ...] | all } ---Sets CoreXL Affinity
fw ctl affinity -s -p PID { CPU_ID [CPU_ID ...] | all } ---Sets CoreXL affinity of the specified process (by PID) to CPU cores
fw ctl affinity -s -n Daemon_Name { CPU_ID [CPU_ID ...] | all } ---Sets CoreXL affinity of the specified process (by name [maximal length = 255 characters]) to CPU cores
fw ctl affinity -s -k Instance_ID { CPU_ID [CPU_ID ...] | all } ---Sets CoreXL affinity of the specified CoreXL FW instance to CPU cores
fw ctl affinity -s -i Interface_Name { CPU_ID [CPU_ID ...] | all } ---Sets CoreXL affinity of the specified interface to CPU cores

---
Traffic Gathering /monitoring

TCPdump
ATRG -sk40072
tcpdump -i <int name> host <ip> -w filename
tcpdump -i <int name> tcp port <port number>
tcpdump -i <int name> udp port <port number>
tcpdump -i <int name> proto ospf
FW Monitor
ATRG - 41045
Functionality
There are four inspection points when a packet passes through a Security Gateway:
Pre-Inbound - marked as 'i'
Post-Inbound - marked as 'I'
Pre-Outbound - marked as 'o'
Post-Outbound - marked as 'O'
Note:
The direction (inbound/outbound) relates to each specific packet, and not to the connection.
fw monitor -e 'accept src=x.x.x.x or dst=v.v.v.v;' -o filename.cap
fw monitor -e "accept;" -o /var/log/fw_mon.cap
fw monitor -e "((src=x.x.x.x , dst=y.y.y.y) or (src=y.y.y.y , dst=x.x.x.x)), accept;" -o /var/log/fw_mon.cap
fw monitor Examples:
packets with IP 192.168.1.12 as SRC or DST
fw monitor -e 'accept host(192.168.1.12);'
all packets from 192.168.1.12 to 192.168.3.3
fw monitor -e 'accept src=192.168.1.12 and dst=192.168.3.3;'
UDP port 53 (DNS) packets, pre-in position is before 'ippot_strip'
fw monitor -pi ipopt_strip -e 'accept udpport(53);'
UPD traffic from or to unprivileged ports, only show post-out
fw monitor -m O -e 'accept udp and (sport>1023 or dport>1023);'
Windows traceroute (ICMP, TTL<30) from and to 192.168.1.12
fw monitor -e 'accept host(192.168.1.12) and tracert;'
Capture web traffic for VSX virtual system ID 23
fw monitor -v 23 -e 'accept tcpport(80);'
Capture traffic on a SecuRemote/SecureClient client into a file.
srfw.exe in $SRDIR/bin (C:\Program Files\CheckPoint\SecuRemote\bin)
srfw monitor -o output_file.cap

Kernel debug 'fw ctl debug'
Usage:
fw ctl debug -h ---Default (clear) all current kernel debugging options:
fw ctl debug 0 ---Disable all kernel debugging options (de-allocates the buffer automatically kills "fw ctl debug"
process):
fw ctl debug -x ---Allocate the debugging buffer (to catch debug messages):
fw ctl debug -buf 32000 ---Enable desired debug flags (in addition to the default flags):
fw ctl debug -m MODULE_NAME + FLAG1 FLAG2 FLAG3 ---Enable only the specified debug flags (all other
flags will be overwritten):
file:///C|/Users/kwinfiel/Desktop/CCSE%20ADV%20TS/CLI%20Command%20line%20cheat%20sheet.txt[5/11/2015 9:26:32 AM]
fw ctl debug -m MODULE_NAME - FLAG6 FLAG7 ---Disable undesired debug flags:
fw ctl debug ---Display all kernel modules and their flags that Security Gateway "understands":

fw ctl debug -m ---Display the flags for specific module that were turned on:
fw ctl debug -m MODULE_NAME ---Print the timestamp in debug output (t = seconds ; T = microseconds):
fw ctl kdebug -t or fw ctl kdebug -T
fw ctl kdebug -T -f > /var/log/debug.txt ---Save the debug messages from debugging buffer into a file:
To stop the debug - press CTRL+C

Zdebug drop
Fw ctl Zdebug drop > filename.out

61000/41000 CLI commands
Information
asg stat [-v] ---Blade and policy status for all chassis
asg monitor ---Monitor blade and policy status
asg resource [-v] ---SGM resource use
asg if ---Chassis interface information
asg_route ---Routing tables for all SGMs
asg perf [-v -a -p -k] ---Continously monitor performance
asg conns [-b <blade>] ---Show connections per blade
asg config show ---Show gclish configuration for all blades
asg cores_stat ---CoreXL information for all blades
asg_info -w ---Asg Info Diagnostic File
asg_auditlog ---Chassis audit log
asg_blade_config is_in_security_group ---Check if SMG is in security group
asg_blade_config get_smo_ip ---Get SMO ip address
asg dxl stat ---Blade Distribution Stats
asg dxl dist_mode verify [-v] ---Blade Distribution Mode
g_all mpstat ---CPU use for all blades
asg if -p ---Interface Performance Information
Navigation
blade 1_02 ---to change to chassis 1 blade 2
Security Switch Module (SSM)
asg_chassis_ctrl start_ssm <SSM> ---Start SSM
asg_chassis_ctrl shutdown_ssm <SSM> ---Stop SSM
asg_chassis_ctrl restart_ssm <SSM> ---Restart SSM
asg_chassis_ctrl active_ssm ---Get active SSMs
asg_chassis_ctrl get_ssm_firmware <SSM> ---SSM Firmware version
asg_chassis_ctrl get_ssm_type <SSM> ---SSM Hardware version

asg_chassis_ctrl get_bmac <SSM> ---MAC Addresses on SSM
show chassis id 1 module <SSM1|SSM2> ip ---Show SSM's CIN Address
Configuration and Policy
asg_ntp_sync_config ---Configure NTP on all blades
asg security_group ---Configure SGM security group
asg_blade_config pull_config all <bladeIP> ---Pull config from another blade
asg_blade_config fetch_smc ---Fetch policy for all blades from smc
asg_policy fetch ---Fetch the policy for all SGMs
asg_policy unload ---Unload policy for all SGMs
asg policy verify ---View installed policy for each SGM
g_all <command> ---Return command from all blades

gexec -a -c <Command> ---Execute command on blades
asg_cp2blades <SrcFile> [<DstFile>] ---Copy file to all blades
asg alert Configure ---Chassis Alerts (SNMP/SMS)
asg_sync_manager ---Chassis Syncronization Wizard
fwaccel <on|off|stat> ---SecureXL control
g_update_conf_file fwkern.conf <Kernel Parameter> ---Set kernel parameter for all blades
View available kernel parameters by ruinning modinfo against the kernel file
modinfo $FWDIR/boot/modules/fwmod.2.6.18.cp.i686.o
Chassis
asg_sgm_serial ---SGM Serial Numbers
asg_serial_info ---CMM,SSM and Chassis Serial Numbers
asg diag verify ---Chassis diagnostic and results
asg_version ---Version information for all blades
asg stat -i tasks ---Used to identify the SMO blade
asg chassis_admin -c <chassis> [down|up] ---Administratively down/up a chassis
asg sgm_admin -b <blade> <up|down> ---Administratively down/up a blade
asg_reboot -b <Blade> ---Reboot blade(s) or Chassis
asg_reboot -b chassis1
asg_reboot -b 1_01
asg_reboot -b 1_01,1_03
asg_chassis_ctrl get_psu_status ---Chassis PUS status
asg_chassis_ctrl get_cpus_temp <Blade> ---SGM CPU Temeperature
asg_chassis_ctrl get_power_type ---Returns AC/DC
asg hw_monitor ---Chassis Hardware Stats
set chassis high-availability primary-chassis <0-2> ---Set chassis priority
set chassis high-availability factors <x> ---Change chassis component score(s)
See cli guide for additional syntax
Chassis Control Module (CMM)
asg_chassis_ctrl restart_cmm <CMM#> Restart CMM
asg_chassis_ctrl get_cmm_status Get CMM status and firmware version
Active CMM CIN address 198.51.100.33
Standby CMM CIN address 198.51.100.233
GCLISH Commands
gclish ---enter global clish shell
show configuration ---List gclish text configuration

set bonding group <ID> lacp_rate slow ---Configure bonding rate
verify bonding rate by running: cat /proc/net/bonding/bond<ID>
asg_config save -t <File> ---Save Gclish config to a text file
save config ---Save Gclish configuration
Packet Captures and Troubleshooting
tcpdump -mcap -w <outfile> -nnei <IF> ---Packet capture from all blades
asg search ---Search blades for specific connection
g_fw ctl zdebug drop ---Dropped packet debug across all blades
g_fw ctl zdebug -m cluster + correction ---Kernel debug across all blades
dxl calc <> ---Determine the blade a connection will use. Based on the src and dst pair
asg log <audit|smd|ports> {-b <blade string>} ---View messages from blade(s) or chassis
Image Management
show snapshots ---List current snapshots (gclish)
add snapshot <name> ---Create new snapshot (gclish)
delete snapshot <name> ---Delete snapshot from respoitory (gclish)

set snapshot import <name> path <path to snapshot> ---Add snapshot to respoitory (gclish)
set global-mode off/on ---Disable global mode for gclish
set snapshot export <name> path <path to export to> ---Export snapshot from repository (shell)
Note: The snapshot cannot contain .tgz in the name
g_snapshot -b <blade string> revert <snapshot name> ---Revert snapshot on blade(s) (shell)
backup_system backup <name> ---Create backup package
Note this creates 4 separate files
watch -d "g_all dbget snap:show:progress" ---View snapshot revert progress
Gaia Interface and Routes
set interface <IF Name> ipv4-address <IP Address> mask-length <Bit Length> ---Configure Address on
Interface (Physical/VLAN/Bond)
set interface <IF Name> state on/off ---Enable/Disable Interface
(Physical/VLAN/Bond)
add interface <IF NAME> vlan <VLAN ID> ---Add VLAN Interface
add bonding group <Bond ID> interface <IF Name> ---Create and Enslave Bonded
Interface(s)
add interface <IF Name> alias <Address>/<Mask Length> ---Create Interface Alias
set static-route <Network>/<Netmask> nexthop gateway address <Gateway> on ---Configure Static
Route
set static-route default nexthop gateway address <Gateway> on ---Configure Default Route
---

VSX
vsx stat [-v] [-l] [id] ---Display VSX status. Verbose output with -v, interface list with -l or status of single
system with VS ID <id>.
vsx get ---View current shell context.
vsx set <id> ---Set context to VS with the ID <id>.
vsx sic reset <id> ---Reset SIC for VS ID <id>.
file:///C|/Users/kwinfiel/Desktop/CCSE%20ADV%20TS/CLI%20Command%20line%20cheat%20sheet.txt[5/11/2015 9:26:32 AM]
cpinfo -x <vs> ---Start cpinfo collecting data for VS ID <vs>.
fw -vs <id> getifs ---View driver interface list for a VS. You can also use the VS name instead of -vs <id>.
fw tab -vs <id> -t <table> ---View state tables for virtual system <id>.
fw monitor -v <id> -e 'accept;' ---View traffic for virtual system with ID <id>.
Attn: with fw monitor use -v instead of -vs
In general, a lot of Check Point's commands do understand the -vs <id> switch.

Provider-1
mdsenv [cma_name] ---Set the environment variables for MDS oder CMA level.
mdsstart [-m|-s] Starts the MDS and all CMAs (10 at a time). ---Start only the MDS with -m or the CMAs
subsequently with -s.
mdsstop [-m] ---Stop MDS and all CMAs or with -m just the MDS.
mdsstat [cma_name]|[-m] ---Show status of the MDS and all CMAs or a certain customer's
CMA. Use -m for only MDS status.
cpinfo -c <cma> (Remember to run mdsenv <cma> in advance.) ---Create a cpinfo for the customer cma <cma>.
mcd <directory> ---Quick cd to $FWDIR/<directory> of the current CMA.
mdsstop_customer <cma> Stop CMA. ---Run mdsenv <cma> in advance.
mdsstart_customer <cma> Start CMA. ---Run mdsenv <cma> in advance
mdsconfig MDS replacement for cpconfig. ---mds_backup Backup binaries and data to current directory.
You can exclude files by specifying them in $MDSDIR/conf/mds_exclude.dat.
mds_restore <file> ---Restore MDS backup from file. Notice: you may need to copy

mds_backup from $MDSDIR/scripts/ as well as gtar and gzip from $MDS_SYSTEM/shared/ to the directory with the backup file. Normally, mds_backup does this during backup

---

VPN & VPN Debugging
vpn ver [-k] ---Check VPN-1 major and minor version as well as build number and latest hotfix. Use -k for kernel version.
vpn tu ---Start a menu based VPN TunnelUtil program where you can list and delete Security Associations (SAs) for peers. vpn shell Start the VPN shell.
vpn debug ikeon|ikeoff ---Debug IKE into $FWDIR/log/ike.elg.
vpn debug on|off ---Debug VPN into $FWDIR/log/vpnd.elg.
vpn debug trunc ---Truncate and stamp logs, enable IKE & VPN debug.
vpn drv stat ---Show status of VPN-1 kernel module.
vpn overlap_encdom ---Show, if any, overlapping VPN domains.
vpn macutil <user> ---Show MAC for Secure Remote user <user>.

Site to site VPN troubleshooting
1. Turn on debugs
vpn debug trunc
vpn debug on TDERROR_ALL_ALL=5
file:///C|/Users/kwinfiel/Desktop/CCSE%20ADV%20TS/CLI%20Command%20line%20cheat%20sheet.txt[5/11/2015 9:26:32 AM]
2. Run the following command to reset the tunnel
(not needed if you are testing a Remote Access VPN):
vpn tu
Then select the option that reads,
"Delete all IPsec+IKE SAs for a given peer (GW)"
enter your remote GW ip address
exit the utility
3. Try to build the tunnel back up again, in both directions,
attempt to connect from YOUR NETWORK to a device in
the remote encryption domain and then attempt to connect
from THE REMOTE NETWORK to a device in the local
encryption domain.
4. Turn off debugs
vpn debug ikeoff
vpn debug off
debug file location:
SecurePlatform - $FWDIR/log/ike.elg*
$FWDIR/log/vpnd.elg*
Windows - %FWDIR%\log\ike.elg*
%FWDIR%\log\vpnd.elg*

FWD -- Logging/Policy debug
1. Turn on debug
fw debug fwd on TDERROR_ALL_ALL=5
2. Recreate issue
3. Turn off debug
fw debug fwd off TDERROR_ALL_ALL=0
debug file location:

SecurePlatform - $FWDIR/log/fwd.elg
Windows - %FWDIR%\log\fwd.elg

FWM -- policy/Dashboard/Mgt HA Sync debug
Debug it!
1. Turn on debug
fw debug fwm on TDERROR_ALL_ALL=5
2. Recreate issue
3. Turn off debug
fw debug fwm off TDERROR_ALL_ALL=0
debug file location:
SecurePlatform - $FWDIR/log/fwm.elg
Windows - %FWDIR%\log\fwm.elg

CPD --- SIC debug
Debug it!
1. Turn on debug
cpd_admin debug on TDERROR_ALL_ALL=5
2. Recreate issue
3. Turn off debug
cpd_admin debug off TDERROR_ALL_ALL=0
debug file location:
SecurePlatform - $CPDIR/log/cpd.elg
Windows - %CPDIR%\log\cpd.elg

Posted by Shyam's Engineering Notes at 5:46 AM

Newer Post Home Older Post

Followers (5)

Follow

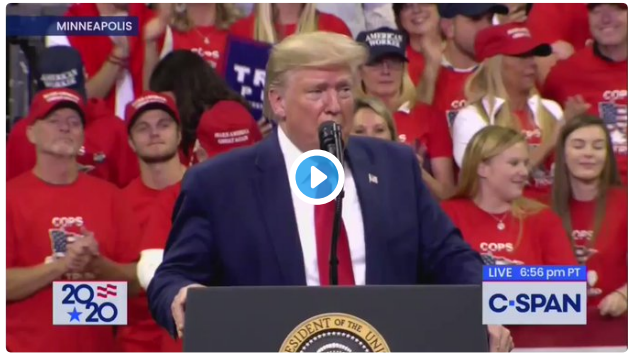
Live Feed

Tweets by @DannySriSai

Shyam Retweeted

Aaron Rupar ✓
@atrupar
Replying to @atrupar

Trump vows to crack down on Somali refugees in a city with one of the largest Somali populations in the country



Oct 11, 2019

Embed View on Twitter