

Log File: 10.176.194.164\_0205.txt

Execution Count: 7

## DashBoard

CPU Utilization	%
5 sec utilization	10%
1 min utilization	10%
5 min utilization	10%

Memory Utilization	Total	Used	Free
Memory utilization	8.00 GB	1.71 GB	6.29 GB

Device Summary	
Hostname	BAT-WER-SFPLB03-ASA-01
Device info	Cisco Adaptive Security Appliance Software Version 9.2(2)4
Image version	"disk0:/asa922-4-smp-k8.bin"
Uptime	37 days 23 hours
Config Register	0x1
Hardware	ASA5555

## Policy Findings

The total device-wide Access Control List (ACL) count is ACL1 0 1208Top ACLs, by size, on this Firewall:

ACL_list	rule
CORPORATE	338
SF685GRDWEB	99
SF891RDVDI	61
SF695LIMS01	52
SF696LIMS02	51
SF550GRD-CINFOSDI	50

SF600GRDPORTAL3	50
SF689GRDPORTAL2	47
SF687GRDPORTAL	43
SF688GRDLIVELINK	40

#### Medium

access-list CORPORATE extended permit ip any object Z2T3GBSFPLS04 log disable

access-list CORPORATE extended permit ip any object-group SF710BLD8and12MGMT01 log disable

access-list CORPORATE extended permit tcp any object Z2T3GBSFVLA31 object-group DM\_INLINE\_TCP\_5

access-list nat-0 extended permit ip any any

#### Medium

port-object eq smtp

access-list SF600GRDPORTAL3 extended permit tcp object-group SFGRANDD object-group PARITYMONITORS eq ftp-data

access-list SF689GRDPORTAL2 extended permit tcp object-group SFGRANDD object-group PARITYMONITORS eq ftp-data

access-list SF689GRDPORTAL2 extended permit tcp object-group SFGRANDD object-group PARITYMONITORS eq ftp

port-object eq ftp

port-object eq ftp-data

access-list SF685GRDWEB extended permit tcp object-group Portal-Servers object-group PARITYMONITORS eq ftp

access-list SF685GRDWEB extended permit tcp object-group Portal-Servers object-group PARITYMONITORS eq ftp-data

access-list SF687GRDPORTAL extended permit tcp object-group SFGRANDD object-group PARITYMONITORS eq ftp log disable

access-list SF687GRDPORTAL extended permit tcp object-group SFGRANDD object-group PARITYMONITORS eq ftp-data log disable

port-object eq smtp

access-list SF520GR&D-ENV extended permit tcp object-group SFGRANDD object-group PARITYMONITORS eq ftp-data

port-object eq telnet

access-list SF689GRDPORTAL2 extended permit tcp object-group Portal-Servers object-group PARITYMONITORS eq ftp-data

access-list SF697LIMS03 extended permit tcp object-group SF697LIMS03 object-group PARITYMONITORS eq ftp log disable

access-list CORPORATE extended permit tcp 10.176.247.0 255.255.255.240 10.16.8.0 255.255.248.0 eq ftp

access-list CORPORATE extended permit tcp object Z2T3GBGLVTA37 object AZGLGBNEVLA20 eq ftp

service tcp destination eq ftp

access-list SF697LIMS03 extended permit tcp object-group SF697LIMS03 object HVW2KDWH1-HAMBURG eq ftp

access-list SF697LIMS03 extended permit tcp object-group DM\_INLINE\_NETWORK\_3 object DEFMLDWH01 eq ftp

access-list SF697LIMS03 extended permit tcp object-group DM\_INLINE\_NETWORK\_4 object DEFMLDWH01 eq ftp-data

access-list CORPORATE extended permit tcp object-group BATLANS object BLM-FTP eq ftp

port-object eq ftp-data

port-object eq ftp
service tcp destination eq ftp
port-object eq telnet
access-list CORPORATE extended permit tcp object HVW2KDWH1-HAMBURG object-group SF697LIMS03 eq ftp log disable
port-object eq smtp
access-list SF520GR&D-ENV extended permit tcp object-group SFGRANDD object-group PARITYMONITORS eq ftp
access-list SF688GRDLIVELINK extended permit tcp object-group SFGRANDD object-group PARITYMONITORS eq ftp
port-object eq smtp
access-list SF689GRDPORTAL2 extended permit tcp object-group Portal-Servers object-group PARITYMONITORS eq ftp
access-list SF600GRDPORTAL3 extended permit tcp object-group SFGRANDD object-group PARITYMONITORS eq ftp
access-list SF530GRD-Development extended permit tcp object-group SF530GRD-Development object-group PARITYMONITORS eq ftp-data
access-list SF697LIMS03 extended permit tcp object-group SF697LIMS03 object-group PARITYMONITORS eq ftp-data log disable
port-object eq ftp
port-object eq telnet
access-list SF530GRD-Development extended permit tcp object-group SF530GRD-Development object-group PARITYMONITORS eq ftp
port-object eq ftp
access-list SF688GRDLIVELINK extended permit tcp object-group SF688GRDLIVELINK object-group PARITYMONITORS eq ftp-data log disable
access-list SF688GRDLIVELINK extended permit tcp object-group SF688GRDLIVELINK object-group PARITYMONITORS eq ftp log disable
port-object eq smtp
access-list CORPORATE extended permit tcp object Z2T3GBGHVLI04 object PLANON_FTP_SRV eq ftp
port-object eq telnet
port-object eq ftp
port-object eq ftp-data
port-object eq telnet
access-list CORPORATE extended permit tcp object-group BATLANS object ADAPCOFTP eq ftp
access-list SF600GRDPORTAL3 extended permit tcp object-group Portal-Servers object-group PARITYMONITORS eq ftp-data
access-list SF600GRDPORTAL3 extended permit tcp object-group Portal-Servers object-group PARITYMONITORS eq ftp
port-object eq telnet
port-object eq ftp-data
port-object eq ftp
port-object eq ftp
access-list CORPORATE extended permit tcp object-group BATLANS object cdg1.sme.zscaler.net eq ftp
access-list SF686GRDWEBDEV extended permit tcp object-group SFGRANDD object-group PARITYMONITORS eq ftp-data
access-list SF686GRDWEBDEV extended permit tcp object-group SFGRANDD object-group PARITYMONITORS eq ftp
access-list CORPORATE extended permit tcp object-group INTERNAL_SERVERS object FTP100_RJRT_COM eq ftp

access-list SF891RDVDI extended permit tcp object-group SF891RDVDI object-group PARITYMONITORS eq ftp	
access-list SF891RDVDI extended permit tcp object-group SF891RDVDI object-group PARITYMONITORS eq ftp-data	
access-list SF688GRDLIVELINK extended permit tcp object-group SFGRANDD object-group PARITYMONITORS eq ftp-data	
access-list CORPORATE extended permit tcp object-group BATLANS object lon3d2-sme.gateway.zscaler.net eq ftp	
access-list SF656PRIMEDB_access_in extended permit tcp object Z2T3GBSFPLA14 object DEFMLMEEG01 eq smtp	
access-list CORPORATE extended permit tcp object-group BATLANS object DAGWOODSFTP eq ftp	

Critical

access-list nat-0 extended permit ip any any

## Interfaces

Interface_name	Interface_description	Interface_state	Duplex_state
GigabitEthernet0/0	CORPORATE	UP	Auto-Duplex(Full-duplex)
GigabitEthernet0/1		DOWN	Auto-Duplex
GigabitEthernet0/2		UP	Auto-Duplex(Full-duplex)
GigabitEthernet0/2.201	SF201CITRIXOUTSIDE	UP	NA
GigabitEthernet0/2.301	SF301CITRIXINSIDE	UP	NA
GigabitEthernet0/2.399	SF399MGMT	UP	NA
GigabitEthernet0/3		UP	Auto-Duplex(Full-duplex)
GigabitEthernet0/3.12	SF12EX90	UP	NA
GigabitEthernet0/3.21	SF21GLOBALGUEST	UP	NA
GigabitEthernet0/3.22	SF22ICONNECTCLIENTS	UP	NA
GigabitEthernet0/3.500	SF500DHCP-DMZ	UP	NA
GigabitEthernet0/3.510	SF510BMS-DMZ	UP	NA
GigabitEthernet0/3.520	SF520GR&D-ENV	UP	NA
GigabitEthernet0/3.530	SF530GRD-Development	UP	NA
GigabitEthernet0/3.541	SF541FACILITIES	UP	NA
GigabitEthernet0/3.545	SF545VMCDMZ	UP	NA
GigabitEthernet0/3.550	SF550GRD-CINFOSDI	UP	NA
GigabitEthernet0/3.560	SF560RDCMSERVERS	UP	NA
GigabitEthernet0/3.591	SF591EX90	UP	NA
GigabitEthernet0/3.595	SF595GR&DFactory	UP	NA
GigabitEthernet0/3.600	SF600GRDPORTAL3	UP	NA
GigabitEthernet0/3.655	SF655PRIMEWEB	UP	NA
GigabitEthernet0/3.656	SF656PRIMEDB	UP	NA

GigabitEthernet0/3.685	SF685GRDWEB	UP	NA
GigabitEthernet0/3.686	SF686GRDWEBDEV	UP	NA
GigabitEthernet0/3.687	SF687GRDPORTAL	UP	NA
GigabitEthernet0/3.688	SF688GRDLIVELINK	UP	NA
GigabitEthernet0/3.689	SF689GRDPORTAL2	UP	NA
GigabitEthernet0/3.694	SF694GRDCAD	UP	NA
GigabitEthernet0/3.695	SF695LIMS01	UP	NA
GigabitEthernet0/3.696	SF696LIMS02	UP	NA
GigabitEthernet0/3.697	SF697LIMS03	UP	NA
GigabitEthernet0/3.698	SF698GRDMAN	UP	NA
GigabitEthernet0/3.797	SF797GRDLABSWIFI	UP	NA
GigabitEthernet0/3.891	SF891RDVDIUSER	UP	NA
GigabitEthernet0/4		UP	Auto-Duplex(Full-duplex)
GigabitEthernet0/4.460	FOLINK	UP	NA
GigabitEthernet0/4.465	STATELINK	UP	NA
GigabitEthernet0/5		DOWN	Auto-Duplex
GigabitEthernet0/6		DOWN	Auto-Duplex
GigabitEthernet0/7	SF100INTERNET	UP	Auto-Duplex(Full-duplex)
Management0/0	management	UP	NA

## Observation

Interface_name	Subnet
GigabitEthernet0/0	The subnet mask of the IP address 10.176.194.164 is 255.255.255.240
GigabitEthernet0/1	NA
GigabitEthernet0/2	NA
GigabitEthernet0/2.201	The subnet mask of the IP address 10.184.193.225 is 255.255.255.240
GigabitEthernet0/2.301	The subnet mask of the IP address 10.184.193.209 is 255.255.255.240
GigabitEthernet0/2.399	The subnet mask of the IP address 10.184.193.193 is 255.255.255.240
GigabitEthernet0/3	NA
GigabitEthernet0/3.12	The subnet mask of the IP address 192.168.11.1 is 255.255.255.0
GigabitEthernet0/3.21	The subnet mask of the IP address 172.30.16.1 is 255.255.248.0
GigabitEthernet0/3.22	The subnet mask of the IP address 172.30.32.1 is 255.255.224.0
GigabitEthernet0/3.500	The subnet mask of the IP address 192.168.12.1 is 255.255.255.0
GigabitEthernet0/3.510	The subnet mask of the IP address 10.184.201.3 is 255.255.255.0

GigabitEthernet0/3.520	The subnet mask of the IP address 10.184.197.129 is 255.255.255.224
GigabitEthernet0/3.530	The subnet mask of the IP address 10.184.197.1 is 255.255.255.128
GigabitEthernet0/3.541	The subnet mask of the IP address 10.178.223.177 is 255.255.255.248
GigabitEthernet0/3.545	The subnet mask of the IP address 10.176.200.193 is 255.255.255.224
GigabitEthernet0/3.550	The subnet mask of the IP address 10.184.192.1 is 255.255.255.0
GigabitEthernet0/3.560	The subnet mask of the IP address 10.184.193.241 is 255.255.255.240
GigabitEthernet0/3.591	The subnet mask of the IP address 10.184.255.193 is 255.255.255.224
GigabitEthernet0/3.595	The subnet mask of the IP address 10.176.194.49 is 255.255.255.240
GigabitEthernet0/3.600	The subnet mask of the IP address 10.184.197.162 is 255.255.255.224
GigabitEthernet0/3.655	The subnet mask of the IP address 10.184.194.193 is 255.255.255.248
GigabitEthernet0/3.656	The subnet mask of the IP address 10.184.194.201 is 255.255.255.248
GigabitEthernet0/3.685	The subnet mask of the IP address 10.176.193.129 is 255.255.255.224
GigabitEthernet0/3.686	The subnet mask of the IP address 10.176.193.161 is 255.255.255.240
GigabitEthernet0/3.687	The subnet mask of the IP address 10.176.193.177 is 255.255.255.248
GigabitEthernet0/3.688	The subnet mask of the IP address 10.176.193.185 is 255.255.255.248
GigabitEthernet0/3.689	The subnet mask of the IP address 10.176.200.225 is 255.255.255.240
GigabitEthernet0/3.694	The subnet mask of the IP address 10.184.194.129 is 255.255.255.224
GigabitEthernet0/3.695	The subnet mask of the IP address 10.176.207.1 is 255.255.255.0
GigabitEthernet0/3.696	The subnet mask of the IP address 10.176.200.1 is 255.255.255.128
GigabitEthernet0/3.697	The subnet mask of the IP address 10.176.194.209 is 255.255.255.248
GigabitEthernet0/3.698	The subnet mask of the IP address 10.184.194.65 is 255.255.255.224
GigabitEthernet0/3.797	The subnet mask of the IP address 10.184.203.1 is 255.255.255.0
GigabitEthernet0/3.891	The subnet mask of the IP address 10.178.157.1 is 255.255.255.0
GigabitEthernet0/4	NA
GigabitEthernet0/4.460	The subnet mask of the IP address 172.16.0.1 is 255.255.255.252
GigabitEthernet0/4.465	The subnet mask of the IP address 172.16.0.5 is 255.255.255.252
GigabitEthernet0/5	NA
GigabitEthernet0/6	NA
GigabitEthernet0/7	The subnet mask of the IP address 62.7.71.226 is 255.255.255.240
Internal-Control0/0	The subnet mask of the IP address 127.0.1.1 is 255.255.0.0
Internal-Data0/0	NA
Internal-Data0/1	NA
Internal-Data0/2	NA
Management0/0	NA

not\_monitored

All Interfaces are currently monitored

from_state	to_state	Reason
Sync Config	Sync File System	Configuration mismatch due to wr standby in active
Standby Ready	Cold Standby	Configuration mismatch due to wr standby in active
Failed	Standby Ready	Interface check
Active Drain	Active Applying Config	Set by the config command
Active Config Applied	Active	No Active unit found
Sync File System	Bulk Sync	Configuration mismatch due to wr standby in active
Standby Ready	Just Active	Set by the config command
Active Config Applied	Active	Set by the config command
Cold Standby	Sync Config	Configuration mismatch due to wr standby in active
Active	Failed	Interface check
Negotiation	Just Active	No Active unit found
Bulk Sync	Standby Ready	Configuration mismatch due to wr standby in active
Active Applying Config	Active Config Applied	No Active unit found
Not Detected	Negotiation	No Error
Active Drain	Active Applying Config	No Active unit found
Just Active	Active Drain	Set by the config command
Active Applying Config	Active Config Applied	Set by the config command
Just Active	Active Drain	No Active unit found

process

run\_time

CP

3863131

Interface_name	Overruns	Underruns	
GigabitEthernet0/0	0 Input errors	0 overrun	326 underruns
GigabitEthernet0/3	248350 input errors	248350 overrun	2409565 underruns
GigabitEthernet0/7	431 input errors	427 overrun	0 underruns

