WIPRO HOLMES
ARTIFICIAL INTELLIGENCE PLATFORM

Firewall Analysis Bot

Log File: innovation_2may.txt

Execution Count: 27

DashBoard

CPU Utilization	%
5 sec utilization	9%
1 min utilization	9%
5 min utilization	10%

Memory Utilization	Total	Used	Free
Memory utilization	6.00 GB	1.70 GB	4.30 GB

Device Summary	
Hostname	BAT-WER-GHPDB01-ASA-01
Device info	Cisco Adaptive Security Appliance Software Version 9.0(2)
Image version	"disk0:/asa902-smp-k8.bin"
Uptime	23 days 23 hours
Config Register	0x1
Hardware	ASA5585-SSP-10

Policy Findings

Low
Filter Drop Rules Were Configured Without Logging. It is recommended to enable logging

Low
There is no ip verify reverse-path

Medium
access-list GH457ICONNECT_access_in extended permit ip any4 any4
access-list GH590INTRANS_access_in extended permit ip any4 any4

access-list Internet extended permit tcp any host 10.179.1.156 object-group Office365_tcp
access-list Internet extended permit tcp any object Z2T3GBGHVDHSS01-VmSecServer-INT object-group VMWare-Sec-Server-Internet-TCP
access-list Internet extended permit tcp any4 object tvr201-External object-group TVR201
access-list global_access extended permit ip any any
access-list prod-app-230 extended permit tcp any host 10.176.226.121
access-list zscaler-acl extended permit tcp any4 object-group zscaler-interesting object-group iConnect

Medium
service-object tcp destination eq smtp
service tcp destination eq ftp
service-object tcp destination eq smtp
port-object eq smtp
access-list GH310CSIDMZ extended permit tcp object-group Google-Servers host 10.176.227.69 eq smtp
access-list prod-web-ext-220 extended permit tcp object CTXMDM-Internal object mail.batgen.com eq smtp
service-object tcp destination eq telnet
access-list GH310CSIDMZ extended permit tcp host 10.179.1.201 host 10.94.40.4 eq smtp

Critical
access-list global_access extended permit ip any any

Interfaces

Interface_name	Interface_description	Interface_state	Duplex_state
GigabitEthernet0/0	Arrow_Internet	UP	Full-Duplex(Full-duplex)
GigabitEthernet0/1		DOWN	Auto-Duplex
GigabitEthernet0/2		UP	Auto-Duplex(Full-duplex)
GigabitEthernet0/2.210	GH210CSEDMZ	UP	NA
GigabitEthernet0/2.220	prod-web-ext-220	UP	NA
GigabitEthernet0/2.221	prod-web-int-221	UP	NA
GigabitEthernet0/2.229	prod-web-mgmt-229	UP	NA
GigabitEthernet0/2.298	GH298PSMGMT	UP	NA
GigabitEthernet0/2.299	GH299MGMT	UP	NA
GigabitEthernet0/3		UP	Auto-Duplex(Full-duplex)
GigabitEthernet0/3.305	GH305WLCMGMT	UP	NA
GigabitEthernet0/3.306	GH306GLOBALWIFICLIENTS	UP	NA
GigabitEthernet0/3.307	GH307GLOBALIPTCLIENTS	UP	NA

GigabitEthernet0/3.309	GH309ICONNECTCLIENTS	UP	NA
GigabitEthernet0/3.310	GH310CSIDMZ	UP	NA
GigabitEthernet0/3.311	Gwan-Test-311	UP	NA
GigabitEthernet0/3.315	GH315ICONNECTGUEST	UP	NA
GigabitEthernet0/3.320	GH320GLOBALGUEST	UP	NA
GigabitEthernet0/3.399	GH399MGMT	UP	NA
GigabitEthernet0/4		UP	Auto-Duplex(Full-duplex)
GigabitEthernet0/4.21	GH21GLOBALGUEST	UP	NA
GigabitEthernet0/4.22	GH22ICONNECTCLIENTS	UP	NA
GigabitEthernet0/4.400	GH400DHCPDMZ	UP	NA
GigabitEthernet0/4.457	GH457ICONNECT	UP	NA
GigabitEthernet0/4.590	GH590INTRANS	UP	NA
GigabitEthernet0/4.591	GH591TPEX90	UP	NA
GigabitEthernet0/5		UP	Auto-Duplex(Full-duplex)
GigabitEthernet0/5.230	prod-app-230	UP	NA
GigabitEthernet0/5.239	prod-app-mgmt-239	UP	NA
GigabitEthernet0/5.630	dev-app-630	UP	NA
GigabitEthernet0/5.639	dev-app-mgmt-639	UP	NA
GigabitEthernet0/6	prod-sbc-transit	DOWN	Full-Duplex
GigabitEthernet0/7	Internet	UP	Full-Duplex(Full-duplex)
Management0/0		DOWN	Auto-Duplex
Management0/1		DOWN	Auto-Duplex
TenGigabitEthernet0/8		DOWN	NA
TenGigabitEthernet0/9		DOWN	NA

Observation

Interface_name	Subnet
GigabitEthernet0/0	The subnet mask of the IP address 89.197.68.130 is 255.255.255.224
GigabitEthernet0/1	NA
GigabitEthernet0/2	NA
GigabitEthernet0/2.210	The subnet mask of the IP address 10.179.1.161 is 255.255.255.224
GigabitEthernet0/2.220	The subnet mask of the IP address 10.187.1.129 is 255.255.255.224
GigabitEthernet0/2.221	The subnet mask of the IP address 10.187.1.161 is 255.255.255.224
GigabitEthernet0/2.229	The subnet mask of the IP address 10.187.0.225 is 255.255.255.240

GigabitEthernet0/2.298	The subnet mask of the IP address 10.179.1.217 is 255.255.255.248
GigabitEthernet0/2.299	The subnet mask of the IP address 10.179.1.225 is 255.255.255.240
GigabitEthernet0/3	NA
GigabitEthernet0/3.305	The subnet mask of the IP address 10.179.1.209 is 255.255.255.248
GigabitEthernet0/3.306	The subnet mask of the IP address 10.179.0.1 is 255.255.255.128
GigabitEthernet0/3.307	The subnet mask of the IP address 10.187.0.1 is 255.255.255.128
GigabitEthernet0/3.309	The subnet mask of the IP address 172.30.32.1 is 255.255.224.0
GigabitEthernet0/3.310	The subnet mask of the IP address 10.179.1.129 is 255.255.255.224
GigabitEthernet0/3.311	The subnet mask of the IP address 10.187.1.249 is 255.255.255.248
GigabitEthernet0/3.315	The subnet mask of the IP address 172.29.33.1 is 255.255.255.0
GigabitEthernet0/3.320	The subnet mask of the IP address 172.30.16.1 is 255.255.248.0
GigabitEthernet0/3.399	The subnet mask of the IP address 10.179.1.241 is 255.255.255.240
GigabitEthernet0/4	NA
GigabitEthernet0/4.21	The subnet mask of the IP address 172.16.16.1 is 255.255.248.0
GigabitEthernet0/4.22	The subnet mask of the IP address 172.16.32.1 is 255.255.224.0
GigabitEthernet0/4.400	The subnet mask of the IP address 192.168.12.1 is 255.255.255.0
GigabitEthernet0/4.457	The subnet mask of the IP address 172.29.16.5 is 255.255.248.0
GigabitEthernet0/4.590	The subnet mask of the IP address 10.176.224.161 is 255.255.255.240
GigabitEthernet0/4.591	The subnet mask of the IP address 10.184.236.129 is 255.255.255.128
GigabitEthernet0/5	NA
GigabitEthernet0/5.230	The subnet mask of the IP address 10.187.0.129 is 255.255.255.192
GigabitEthernet0/5.239	The subnet mask of the IP address 10.187.1.33 is 255.255.255.224
GigabitEthernet0/5.630	The subnet mask of the IP address 10.187.1.1 is 255.255.255.224
GigabitEthernet0/5.639	The subnet mask of the IP address 10.187.1.113 is 255.255.255.240
GigabitEthernet0/6	The subnet mask of the IP address 10.187.1.241 is 255.255.255.248
GigabitEthernet0/7	The subnet mask of the IP address 188.39.10.162 is 255.255.255.224
Internal-Data0/0	NA
Internal-Data0/1	NA
Internal-Data0/2	NA
Internal-Data0/3	NA
Management0/0	NA
Management0/1	NA
TenGigabitEthernet0/8	NA
TenGigabitEthernet0/9	NA

from_state	to_state	Reason
Not Detected	Disabled	No Error

process	run_time
bcmCNTR.0	4878065