PaloAlto Configuration Report

Hostname: PA-VM

Firmware Version 8.0.0

Report printed on DESKTOP-R0JBCCS at 09/26/18 16:22:25 with autodoc Version 10.00

Table of Contents

1. Policies	**1**
1.1 Security	1
1.1.1 Policy Overview	1
1.1.2 Policy Detail	1
1.2 NAT	2
1.3 QoS	2
1.4 Policy based Forwarding	3
1.5 Decryption	3
1.6 DoS Protection	3
2. Objects	**4**
2.1 Addresses	4
2.2 Address Groups	4
2.3 Applications	4
2.4 Tags	4
2.5 Security Profiles	5
2.5.1 AntiVirus	5
2.5.2 URL-Filtering	5
2.6 Schedules	6
3. Network	**7**
3.1 Interfaces	7
3.1.1 Ethernet	7
3.1.1.1 Additional information on Ethernet Interfaces	7
3.1.2 VLAN	7
3.1.2.1 Additional information on VLANs	7
3.1.3 Loopback	8
3.1.3.1 Additional information on Loopbacks	8
3.1.4 Tunnel	8
3.1.4.1 Additional information on Tunnels	8
3.2 Zones	9
3.3 Virtual Routers	9
3.3.1 Profile: default	9
3.3.1.1 Router Settings	9
3.4 IPSec Tunnels	10
3.5 GlobalProtect	10
3.5.1 Gateways	11
3.5.1.1 Profile: gp_gw01	11
3.5.1.1.1 General	11
3.5.1.1.2 Authentication	11
3.5.1.1.3 Agent	11
3.5.1.2 Profile: gp_gw02	11
3.5.1.2.1 General	11
3.5.1.2.2 Authentication	11
3.5.1.2.3 Agent	11

3.5.1.3 Profile: gp_gw03 11
3.5.1.3.1 General 11
3.5.1.3.2 Authentication 11
3.5.1.3.3 Agent 11
3.6 Network Profiles 13
3.6.1 GlobalProtect IPSec Crypto 13
3.6.2 IKE Gateways 13
3.6.3 IPSec Crypto 13
3.6.4 IKE Crypto 13
3.6.5 Monitor 13
3.6.6 QoS Profile 14

4. Device **15**
4.1 Password Profiles 15
4.2 Administrators 15
4.3 Admin Roles 16
4.4 Certificate Management 16
4.4.1 Certificates 16
4.4.2 SSL/TLS Service Profile 16
4.5 Server Profiles 17
4.5.1 LDAP 17
4.6 Local User Database 17
4.7 Users 17
4.8 User Groups 17

1. Policies

1.1 Security

1.1.1 Policy Overview

Name	Source Zone	Address	Destination Zone	Address	Application	Service	Action
trust-untrust	trust	any	untrust	any	any	application-default	allow
addr1_allow	trust	addr1	untrust	any	any	application-default	allow
addr2_allow	trust	addr2	untrust	any	any	application-default	allow
LAN_allow	trust	LAN	untrust	any	any	application-default	allow

1.1.2 Policy Detail

trust-untrust

Rule Type	universal
Source User	any
HIP Profiles	any
URL Category	any
Profile Type	Profiles
Antivirus	strict
Vulnerability Protection	
Anti-Spyware	
URL Filtering	social_media
File Blocking	
Data Filtering	
WildFire Analysis	
Log at Session Start	yes
Log at Session End	yes
Log Forwarding	
Schedule	working-hours
QoS Marking	ip-dscp
Disable Server Response Inspection	

addr1_allow

Rule Type	universal
Source User	any
HIP Profiles	any
URL Category	any
Profile Type	None
Log at Session Start	no
Log at Session End	yes
Log Forwarding	
Schedule	
QoS Marking	ip-dscp
Disable Server Response Inspection	

addr2_allow

Rule Type	universal
Source User	any
HIP Profiles	any
URL Category	any
Profile Type	None
Log at Session Start	no
Log at Session End	yes

Log Forwarding	
Schedule	
QoS Marking	ip-dscp
Disable Server Response Inspection	

LAN_allow

Rule Type	universal
Source User	any
HIP Profiles	any
URL Category	any
Profile Type	Profiles
Antivirus	default
Vulnerability Protection	default
Anti-Spyware	
URL Filtering	
File Blocking	basic file blocking
Data Filtering	
WildFire Analysis	
Log at Session Start	yes
Log at Session End	yes
Log Forwarding	
Schedule	
QoS Marking	ip-dscp
Disable Server Response Inspection	

1.2 NAT

Name	Src Zone	Dst Zone	Dst Interface	Src Address	Dst Address	Service	Src Translation	Dst Translation
trust_untrust	trust	untrust	any	any	any	any	none	none

1.3 QoS

Name	Zone	Source Address	User	Zone	Destination Address	Application	Service
addr1_class	trust	addr1	any	untrust	any	any	any

addr1_class1

DSCP / ToS	any
Class	1
Schedule	

1.4 Policy based Forwarding

Name	Source Zone/Intf	Address	User	Destination Address	Application	Service
pbf_01		LAN	any	any	any	any

pbf_01

Action	forward
Egress Interface	ethernet1/6
Next Hop	
Monitor	
Profile	
Disable this rule if nexthop/monitor ip is unreachable	
IP Address	
Enforce Symmetric Return	no
Schedule	

1.5 Decryption

Name	Source Zone	Address	User	Destination Zone	Address	URL Cat	Service	Action	Type	Decr Profile

1.6 DoS Protection

Name	Source Zone/Intf	Address	User	Destination Zone/Intf	Address	Service	Action
wordpress		wordpress	any		any	any	protect

wordpress

Protection Aggregate	
Classified Profile	:
Schedule	
Log Forwarding	

2. Objects

2.1 Addresses

Name	Description	Type	Address	Tags
addr1	fasdf	IP Netmask	10.10.10.5/32	
addr2		IP Netmask	10.10.10.10/32	
LAN		IP Netmask	192.168.100.0/24	
wordpress		IP Netmask	1.1.1.1	

2.2 Address Groups

Name	Members Count	Addresses	Tags
addr1-2	2	addr1, addr2	

2.3 Applications

Profile: hjkl

Description	instant-messaging
Properties	
Category	collaboration
Parent App	acronis-cloud-backup
Subcategory	instant-messaging
Risk	1
Technology	client-server
Characteristics	
Capable of File Transfer	no
Excessive Bandwidth Use	no
Tunnels Other Applications	no
Has Known Vulnerabilities	no
Used by Malware	
Evasive	no
Prevasive	no
Prone to Misuse	no
Continue scanning for other Applications	yes

2.4 Tags

Name	Comments
intern	

2.5 Security Profiles

2.5.1 AntiVirus

Profile: alert

Packet Capture	no

Decoders

Name	Action	WildFire Action
ftp	alert	default
http	alert	default
imap	alert	default
pop3	alert	default
smb	alert	default
smtp	alert	default

Application Exceptions

Name	Action

Profile: strict

Packet Capture	no

Decoders

Name	Action	WildFire Action
smtp	drop	default
smb	default	default
pop3	drop	default
imap	drop	default
http	default	default
ftp	drop	default

Application Exceptions

Name	Action

2.5.2 URL-Filtering

Profile: social_media

URL Filtering Settings

Log container page only	yes
Safe Search Enforcement	no

HTTP Header Logging

User-Agent	no
Referer	no
X-Forwarded-For	no

User Credential Detection

User Credential Detection	Disabled
Valid Username Detected Log Severity	medium

Categories

blocked Categories	social-networking, streaming-media
allowed Categories	all other

2.6 Schedules

Name	Recurrence	Times
working-hours	Daily	08:00-12:00

3. Network

3.1 Interfaces

3.1.1 Ethernet

	Interface	IP Address	Virtual Router	VLAN / VWire	Security Zone
Virtual Wire					
	ethernet1/8	none	none	none	none
	ethernet1/9	none	none	none	none
Layer 3					
	ethernet1/6	Dynamic-DHCP Client	none	none	Zone2
	ethernet1/7	192.168.55.5/24	none	none	Zone1
	ethernet1/1	192.168.66.6/24	none	none	Zone1

3.1.1.1 Additional information on Ethernet Interfaces

ethernet1/6

Link Speed	auto
DAD Attempts	1
Reachable Time (sec)	30
NS Interval (sec)	1
Enable Duplicate Address Detection	no
Enable NDP Monitoring	no

ethernet1/7

Link Speed	auto
DAD Attempts	1
Reachable Time (sec)	30
NS Interval (sec)	1
Enable Duplicate Address Detection	no
Enable NDP Monitoring	no

ethernet1/1

Link Speed	auto
DAD Attempts	1
Reachable Time (sec)	30
NS Interval (sec)	1
Enable Duplicate Address Detection	no
Enable NDP Monitoring	no

3.1.2 VLAN

Interface	IP Address	Virtual Router	VLAN	Security Zone
vlan.30	10.30.0.0/16		none	none
vlan.40	10.40.0.0/16		none	none
vlan.50	10.50.0.0/16		none	none

3.1.2.1 Additional information on VLANs

vlan.30

DAD Attempts	1
Reachable Time (sec)	30
NS Interval (sec)	1
Enable Duplicate Address Detection	no
Enable NDP Monitoring	no
Management Profile	

MTU	
Untagged Subinterface	

vlan.40

DAD Attempts	1
Reachable Time (sec)	30
NS Interval (sec)	1
Enable Duplicate Address Detection	no
Enable NDP Monitoring	no
Management Profile	
MTU	
Untagged Subinterface	

vlan.50

DAD Attempts	1
Reachable Time (sec)	30
NS Interval (sec)	1
Enable Duplicate Address Detection	no
Enable NDP Monitoring	no
Management Profile	
MTU	
Untagged Subinterface	

3.1.3 Loopback

Interface	Management Profile	IP Address	Virutal Router	Security Zone	Comment
loopback.5		192.168.20.20/32			

3.1.3.1 Additional information on Loopbacks

loopback.5

IPv4	192.168.20.20/32

3.1.4 Tunnel

Interface	Management Profile	IP Address	Virutal Router	Security Zone	Comment
tunnel.10		10.10.55.5/24			

3.1.4.1 Additional information on Tunnels

tunnel.10

IPv4	192.168.20.20/32, 10.10.55.5/24

3.2 Zones

Profile: Zone1

Type	layer3
Interfaces / Virutal Systems	ethernet1/1, ethernet1/7
Zone Protection Profile	-
Packet Buffer Protection	no
Log Setting	None
User-ID Enabled	no

Profile: Zone2

Type	layer3
Interfaces / Virutal Systems	ethernet1/6
Zone Protection Profile	-
Packet Buffer Protection	no
Log Setting	None
User-ID Enabled	no

Profile: trust

Type	layer3
Interfaces / Virutal Systems	
Zone Protection Profile	-
Packet Buffer Protection	no
Log Setting	None
User-ID Enabled	no

Profile: untrust

Type	layer3
Interfaces / Virutal Systems	
Zone Protection Profile	-
Packet Buffer Protection	no
Log Setting	None
User-ID Enabled	no

3.3 Virtual Routers

3.3.1 Profile: default

3.3.1.1 Router Settings

Interfaces	none

Administrative Distances

Static	10
Static IPv6	10
OSPF Int	30
OSPF Ext	110
OSPFv3 Int	30
OSPFv3 Ext	110
IBGP	200
EBGP	20
RIP	120

3.4 IPSec Tunnels

Profile: remote_tunnel

Tunnel Interface	tunnel
Type	Auto Key
Address Type	ipv4
IKE Gateway	remote-users
IPSec Crypto Profile	None
Enable Replay Protection	yes
Copy TOS Header	no
Tunnel Monitor	disabled

3.5 GlobalProtect

3.5.1 Gateways

3.5.1.1 Profile: gp_gw01

3.5.1.1.1 General

Network Settings

Interface
ethernet1/7

3.5.1.1.2 Authentication

Server Authentication

SSL/TLS Service Profile	ssl_prof01

3.5.1.1.3 Agent

Tunnel Settings	**disabled**

Timeout Settings

Login Lifetime	days:
Inactivity Logout	:
Disconnect On Idle	minutes:

3.5.1.2 Profile: gp_gw02

3.5.1.2.1 General

Network Settings

Interface
ethernet1/6

3.5.1.2.2 Authentication

Server Authentication

SSL/TLS Service Profile	ssl_prof01

3.5.1.2.3 Agent

Tunnel Settings	**disabled**

Timeout Settings

Login Lifetime	days:
Inactivity Logout	:
Disconnect On Idle	minutes:

3.5.1.3 Profile: gp_gw03

3.5.1.3.1 General

Network Settings

Interface	IP Address Type	IPv4 Address
ethernet1/7	IPv4	192.168.55.5/24

3.5.1.3.2 Authentication

Server Authentication

SSL/TLS Service Profile	ssl_prof01

3.5.1.3.3 Agent

Tunnel Settings	**disabled**

Timeout Settings

Login Lifetime	days:
Inactivity Logout	:
Disconnect On Idle	minutes:

3.6 Network Profiles

3.6.1 GlobalProtect IPSec Crypto

Profile: default

Encryption

aes-128-cbc

Authentication

sha1

3.6.2 IKE Gateways

Profile: remote-users

General	
Version	ipv4
Address Type	ikev1
Interface	ethernet1/1
Local IP Address	None
Peer IP Type	Static
Peer IP Address	2.2.2.2
Authentication	Pre-Shared Key
Local Identification	None
Peer Identification	None

Advanced Options	
Common Options	
Enable Passive Mode	no
Enable NAT Traversal	no
IKEv1	
Exchange Mode	
IKE Crypto Profile	
Dead Peer Detection	yes
Interval	
Retry	

3.6.3 IPSec Crypto

Name	IPSec Protocol	Encryption	Authentication	DH Grop	Lifetime	Lifesize
default	ESP	aes-128-cbc, 3des	sha1	group2	hours: 1	disabled
Suite-B-GCM-128	ESP	aes-128-gcm	none	group19	hours: 1	disabled
Suite-B-GCM-256	ESP	aes-256-gcm	none	group20	hours: 1	disabled

3.6.4 IKE Crypto

				Timers	
Name	DH Group	Encryption	Authentication	Key Lifetime	IKEv2 Authentication Multiple
default	group2	aes-128-cbc, 3des	aes-128-cbc, 3des	time: 8	0
Suite-B-GCM-128	group19	aes-128-cbc	aes-128-cbc	time: 8	0
Suite-B-GCM-256	group20	aes-256-cbc	aes-256-cbc	time: 8	0

3.6.5 Monitor

Name	Action	Interval (sec)	Threshold
default	wait-recover	3	5

3.6.6 QoS Profile

Profile: default

Egress Max	0
Egress Guaranteed	0

Class	Priority	Egress Max	Egress Guaranteed
class1	real-time	0	0
class2	high	0	0
class3	high	0	0
class4	medium	0	0
class5	medium	0	0
class6	low	0	0
class7	low	0	0
class8	low	0	0

4. Device

4.1 Password Profiles

Name	**strict**
Required Password Change Period (days)	120
Expiration Warning Period (days)	10
Post Expiration Admin Login Count	2
Post Expiration Grace Period (days)	10

4.2 Administrators

User: admin

Role	superuser
Public Key Authentication (SSH)	Enabled

User: read_only

Role	custom
Profile	read_only
Public Key Authentication (SSH)	Enabled

4.3 Admin Roles

read_only	Access Control		Rights
Web UI			
	Dashboard		
	ACC		
	Monitor		disable
	Policies		enable
		Security	read-only
		NAT	read-only
		QoS	read-only
		Policy Based Forwarding	read-only
		Decryption	read-only
		Tunnel Inspection	read-only
		Application Override	read-only
		Authentication	read-only
		DoS Protection	read-only
	Objects		disable
		Network	disable
	Device		disable
	Privacy		disable
	Validate		
	Save		disable
	Commit		disable
	Tasks		
	Global		disable
	XML API		
	Report		disable
	Log		disable
	Configuration		disable
	Operational Requests		disable
	Commit		disable
	User-ID Agent		disable
	Export		disable
	Import		disable
	CLI		
			None

4.4 Certificate Management

4.4.1 Certificates

Name	Subject	Issuer	CA	Expires	Algorithm
192.168.1.100	/CN=192.168.1.100	/CN=192.168.1.100	yes	Sep 3 10:03:25 2019 GMT	RSA

4.4.2 SSL/TLS Service Profile

Name	Certificate	Min Version	Max Version
ssl_prof01	SSL-Decrypt	tls1-0	max

4.5 Server Profiles

4.5.1 LDAP

Profile: LDAP_01

Administrator Use Only	no

Server Settings

Type	other
Base DN	None
Bind DN	CN=Administrator,CN=Users,DC=test,DC=com
Bind Timeout	30
Search Timeout	30
Retry Interval	60
Require SSL/TLS secured connection	yes
Verify Server Certificate for SSL sessions	

Name	LDAP Server	Port
dc01	192.168.1.115	389
dc02	192.168.1.116	389

4.6 Local User Database

4.7 Users

Name	Enable
user01	yes
user02	yes
user03	yes
user04	yes
user05	yes

4.8 User Groups

Name	Local Users
users	user01, user02, user03, user04, user05