COMMON CRITERIA CONFIGURATION GUIDANCE

ARUBA OS 8.6 SUPPLEMENTAL GUIDANCE

Target of Evaluation: Aruba Mobility Controllers with ArubaOS 8.6-FIPS

Version 1.10
February 2021

aruba
a Hewlett Packard Enterprise company

3333 SCOTT BLVD | SANTA CLARA, CA 95054
info@arubanetworks.com

www.arubanetworks.com

CONTENTS

Aruba OS 8.6 Supplemental Guidance 1
1 Introduction 4
1.1 Evaluated Platforms 4
1.2 Version Information 5
1.3 Aruba Firewall high-level concepts 5
1.4 Restrictions for Virtual Controller VMM 6
2 Configuration 6
2.1 Security Audit (FAU) 7
2.1.1 FAU_GEN.1 7
2.2 Security Audit (FAU) 7
2.2.1 FAU_GEN.1 7
2.2.2 FAU_GEN.2 20
2.2.3 FAU_STG.1 20
2.2.4 FAU_STG_EXT.1 20
2.3 Cryptographic Support (FCS) 22
2.3.1 FCS_CKM.1 22
2.3.2 FCS_CKM.4 22
2.3.3 FCS_COP.1 22
2.3.4 FCS_HTTPS_EXT.1 22
2.3.5 FCS_IPSEC_EXT.1 22
2.3.6 FCS_RBG_EXT.1 29
2.3.7 FCS_SSHS_EXT.1 29
2.3.8 FCS_TLSS_EXT.1 29
2.4 User Data Protection (FDP) 30
2.4.1 FDP_RIP.2 30
2.5 Firewall (FFW) 30
2.5.1 FFW_RUL_EXT.1 30
2.6 Identification and Authentication (FIA) 37
2.6.1 FIA_802X_EXT.1 37
2.6.2 FIA_AFL.1 38
2.6.3 FIA_AFL.1 (WLAN) 39
2.6.4 FIA_PMG_EXT.1 39
2.6.5 FIA_PSK_EXT.1 (VPNGW) 39
2.6.6 FIA_PSK_EXT.1 (WLAN) 40
2.6.7 FIA_ UAU.6 40
2.6.8 FIA_UAU.7 40
2.6.9 FIA_UAU_EXT.2 40
2.6.10 FIA_UIA_EXT.1 40
2.6.11 FIA_X509_EXT.1 41
2.6.12 FIA_X509_EXT.3 44
2.6.13 FIA_X509_EXT.4 44

2.7 Security Management (FMT) 45
2.7.1 FMT_MOF.1/ManualUpdate 45
2.7.2 FMT_MOF.1/Functions 45
2.7.3 FMT_MOF.1/Services 45
2.7.4 FMT_MTD.1/CoreData 45
2.7.5 FMT_MTD.1/CryptoKeys 45
2.7.6 FMT_SMF.1 45
2.7.7 FMT_SMR.1 45
2.7.8 FMT_SMR.2 45
2.8 Packet Filtering (FPF) 45
2.8.1 FPF_RUL_EXT.1 45
2.9 Protection of the TSF (FPT) 46
2.9.1 FPT_APW_EXT.1 46
2.9.2 FPT_FLS.1 (VPNGW/WLAN) 47
2.9.3 FPT_SKP_EXT.1 47
2.9.4 FPT_STM_EXT.1 47
2.9.5 FPT_TST_EXT.1 47
2.9.6 FPT_TST_EXT.3 47
2.9.7 FPT_TUD_EXT.1 47
2.10 TOE Access (FTA) 48
2.10.1 FTA_SSL.3 48
2.10.2 FTA_SSL.4 48
2.10.3 FTA_SSL_EXT.1 49
2.10.4 FTA_TAB.1 49
2.10.5 FTA_TSE.1 (VPNGW/WLAN) 49
2.10.6 FTA_VCM_EXT.1 54
2.11 Trusted Path/Channels (FTP) 54
2.11.1 FTP_ITC.1 54
2.11.2 FTP_TRP.1/Admin 54
3 Reference Documents 54

1 Introduction

This document serves as a supplement to the official Aruba user guidance (documentation), consolidating configuration information specific to the collaborative Protection Profile for Network Devices, Version 2.1, 24 September 2018, PP-Module for Virtual Private Network (VPN) Gateways, Version 1.0, 2019-09-17, PP-Module for Stateful Traffic Filter Firewalls, Version 1.3, 27 September 2019 and Network Device collaborative Protection Profile (NDcPP) Extended Package Wireless Local Area Network (WLAN) Access Systems, Version 1.0, May 29 2015.

This document contains configuration "snippets" from an ArubaOS configuration file. For the sake of simplicity, only command-line interface (CLI) commands are included. When configuring an Aruba controller, a graphical user interface (WebUI) is also available; this document does not include screenshots from the WebUI. Refer to the official ArubaOS User Guide for WebUI instructions, if needed.

https://asp.arubanetworks.com/downloads/documents/RmlsZTo1MTliMTJhNC00MjJlLTExZWEtYTQ3MS0zYjJhMzUzYmI4NDU%3D

The ordering of items in this document is based on the ordering of items in the Protection Profiles and Security Target. Configuration guidance in this document is provided so that specific test activities within the PP may be completed.

1.1 Evaluated Platforms

The following platforms are covered under the evaluated configuration:

Mobility Controller Hardware Appliances

Product Model	Part Number(s)	CPU
Aruba 9004 Mobility Controller	R1B25A	Intel Atom C3508
Aruba 7005 Mobility Controller	JW636A	Broadcom XLP208
Aruba 7008 Mobility Controller	JX932A	Broadcom XLP208
Aruba 7010 Mobility Controller	JW703A	Broadcom XLP208
Aruba 7024 Mobility Controller	JW707A	Broadcom XLP208
Aruba 7030 Mobility Controller	JW711A	Broadcom XLP208
Aruba 7205 Mobility Controller	JW740A	Broadcom XLP316
Aruba 7210 Mobility Controller	JW746A	Broadcom XLP416
Aruba 7220 Mobility Controller	JW754A	Broadcom XLP432
Aruba 7240 Mobility Controller	JW762A	Broadcom XLP432
Aruba 7240XM Mobility Controller	JW830A	Broadcom XLP432
Aruba 7280 Mobility Controller	JX914A	Broadcom XLP780

Mobility Controller Virtual Appliances (deployed on ESXi v6.5)

- MC-VA-50
- MC-VA-250
- MC-VA-1k

The Mobility Controller Virtual Appliances are deployed on ESXi version 6.5. The following virtual machine platforms are included in the evaluated configuration:

Name	CPU	Memory
HPE EdgeLine EL8000	Intel Xeon Gold 6212U	128GB
DTECH M3-SE-SVR4	Intel Xeon E3-1505L	32GB
DTECH M3x	Intel Core i5	32GB
Klas Telecom TDC Blade	Intel Xeon D	128GB
Klas Telecom VoyagerVMm	Intel Corei5	32GB
Pacstar 451/3	Intel Xeon D	32GB
Pacstar 451/3	Intel Xeon E3	32GB
IAS VPN Gateway Module NANO-VM	Intel Atom E3	4GB
IAS VPN Gateway Module Classic Plus	Intel Core i7	32GB

1.2 Version Information

This document covers Aruba Mobility Controllers running ArubaOS 8.6. Customers are advised to use the newest available 8.6 release in order to take advantage of defect fixes, which may include fixes for security vulnerabilities.

1.3 Aruba Firewall high-level concepts

In an Aruba mobility controller, firewall rules may be applied in multiple ways:

1. To traffic entering a physical port (Ethernet interface) or logical port (VLAN or tunnel) which has been labeled in the configuration as “trusted”. The notion of “trusted” does not mean that the interface necessarily connects to a trusted network. The “trusted” marking in the configuration means that no user-focused processing takes place on traffic entering this interface. That is, the concept of users and user-roles is not applied, and IP addresses learned through this interface will not appear in the user table. This configuration of the mobility controller corresponds to the traditional view of a firewall as a physical device sitting between two networks. The examples used in this configuration guidance will focus on this mode of operation.
2. To traffic entering from an untrusted user. The concept of a “user” can be described as “an IP address learned through an untrusted interface”. Wi-Fi users connecting through Access Points (APs) are automatically untrusted. VPN users connecting to the mobility controller with a VPN client are automatically untrusted. Physical ports and logical ports (VLAN or tunnel) may be configured as “untrusted”, in which case every source IP address learned through that interface will appear in the user table and will have a role/firewall policy assigned to it.

3. To traffic directed to the mobility controller itself (i.e. management traffic). Management traffic may be filtered using the two methods previously described, or it may be filtered through a special “service ACL” configuration which applies universally to all interfaces.

See the ArubaOS User Guide and CLI Reference Guide for full details on roles, firewall policies, authentication, and user management.

https://asp.arubanetworks.com/downloads/documents/RmlsZTo1MTliMTJhNC00MjJlLTExZWEtYTQ3MS0zYjJhMzUzYmI4NDU%3D

https://support.hpe.com/hpesc/public/docDisplay?docId=a00100140en_us&docLocale=en_US

1.4 Restrictions for Virtual Controller VMM

For the Virtual Controllers running on ESXi (the VMM permitted under the evaluated configuration), the administrator of the TOE should ensure the following prior to configuration of the TOE:

1. The only virtual machine installed upon the VMM is the Aruba AOS 8.6 Virtual Mobility Controller image. No other VMs may be installed on the VMM in the evaluated configuration in compliance of Common Criteria.
2. The TOE should *only* be configured to run on the ESXi version claimed within the Security Target.
3. No other instances of the TOE or other virtual TFFW may be present on the same hardware platforms.

2 Configuration

The purpose of this section is to provide the commands and information necessary to configure the device to be compliant with the government approved protection profile. The following Requirement classes are covered within this document:

- Security Audit (FAU)
- Cryptographic Support (FCS)
- User Data Protection (FDP)
- Firewall (FFW)
- Identification and Authentication (FIA)
- Security Management (FMT)
- Packet Filtering (FPF)
- Protection of the TSF (FPT)
- TOE Access (FTA)
- Trusted Path/Channels (FTP)

2.1 Security Audit (FAU)

2.1.1 FAU_GEN.1

All required audit logs are generated by default. Note that for compliance with FPF_RUL_EXT.1, the "log" keyword must be used on any firewall rules that should be logged. In the event that a TOE network interface is overwhelmed by traffic, the TOE will drop packets and generate an audit event for every packet that is denied and dropped. These statistics are also available through the "show interface" command.

2.2 Security Audit (FAU)

2.2.1 FAU_GEN.1

All required audit logs are generated by default. Note that for compliance with FPF_RUL_EXT.1, the "log" keyword must be used on any firewall rules that should be logged. In the event that a TOE network interface is overwhelmed by traffic, the TOE will drop packets and generate an audit event for every packet that is denied and dropped. These statistics are also available through the "show interface" command.

Logging should be configured without the bsd-standard format to ensure that the logs include all required information in the timestamp including year, month, day, hour, minute, and seconds.

(config) #logging 192.168.215.253 source-interface 215
(config) #write mem
Saving Configuration...
Configuration Saved.
(config) #

Note that the sample audit records in the table below do not contain the year, however, when configured as described above, the audit records will contain the full timestamp. For example:

Jan 14 16:17:38 2021 Aruba7220 localdb[3763]: <133112> <3763> <DBUG> <Aruba7220 192.168.144.200> |db| DELETE FROM cpsec_whitelist WHERE enable=2 and sequence_num <= 0;

Requirement	Auditable Events	Additional Content
NDcPP21:FAU_GEN.1	Startup and Shutdown of the Audit function	None
Oct 10 23:58:11 cli[32430]: USER:admin@serial NODE:"/mm/mynode" COMMAND:<no logging 1.1.1.249 > -- command executed successfully Oct 10 23:58:20 cli[32430]: USER:admin@serial NODE:"/mm/mynode" COMMAND:<logging 1.1.1.249 severity debugging> -- command executed successfully		
NDcPP21:FAU_GEN.2	None	None
NDcPP21:FAU_STG.1	None	None
NDcPP21:FAU_STG_EXT.1	None	None
NDcPP21:FCS_CKM.1	None	None
VPNGW10:FCS_CKM.1/IKE	None	None
WLANASEP10:FCS_CKM.1(2)	None	None
NDcPP21:FCS_CKM.2	None	None

WLANASEP10:FCS_CKM.2(2)	None	None
WLANASEP10:FCS_CKM.2(3)	None	None
NDcPP21:FCS_CKM.4	None	None
VPNGW10:FCS_COP.1/DataEncryption	None	None
WLANASEP10:FCS_COP.1/DataEncryption	None	None
NDcPP21:FCS_COP.1/DataEncryption	None	None
NDcPP21:FCS_COP.1/Hash	None	None
NDcPP21:FCS_COP.1/KeyedHash	None	None
NDcPP21:FCS_COP.1/SigGen	None	None
NDcPP21:FCS_HTTPS_EXT.1	Failure to establish a HTTPS Session.	Reason for failure.
Jul 28 19:28:24 httpd[5853]: [ssl:error] [pid 5853:tid 870642864] [client 192.168.144.249:53892] AH02039: Certificate Verification: Error (19): self signed certificate in certificate chain, referer: Aug 19 12:56:01 Aruba7030 httpd[6598]: <350008> <6603> <ERRS> <Aruba7030 192.168.144.201> |webserver| SSL Library Error: error:1408C095:SSL routines:SSL3_GET_FINISHED:digest check failed Aug 19 14:10:24 Aruba7220 httpd[7470]: <350008> <7490> <ERRS> <Aruba7220 192.168.144.200> |webserver| SSL Library Error: error:1408A0C1:SSL routines:SSL3_GET_CLIENT_HELLO:no shared cipher Too restrictive SSLCipherSuite or using DSA server certificate? Aug 19 12:55:25 Aruba9004LTE httpd[12094]: <350008> <12104> <ERRS> <Aruba9004LTE 192.168.144.202> |webserver| SSL Library Error: error:1408B010:SSL routines:SSL3_GET_CLIENT_KEY_EXCHANGE:EC lib Aug 19 13:50:03 ArubaVMC-DTech httpd[20783]: <350008> <20797> <ERRS> <ArubaVMC-DTech 192.168.144.204> |webserver| SSL Library Error: error:1408A10B:SSL routines:SSL3_GET_CLIENT_HELLO:wrong version number		
NDcPP21:FCS_IPSEC_EXT.1	Failure to establish an IPsec SA.	Reason for failure.
Oct 6 11:30:23 Aruba7030 isakmpd[3520]: <103063> <3520> <DBUG> <Aruba7030 192.168.144.201> 192.168.144.154:4500-> I <-- Notify: NO_PROPOSAL_CHOSEN spi={f2caa917e13078bd 0000000000000000} np=SA Dec 17 08:24:30 Aruba7220 isakmpd[3616]: <103054> <3616> <INFO> <Aruba7220 192.168.144.200> Dropping IKE message drop from 192.168.144.154 500 due to notification type:NO_PROPOSAL_CHOSEN		
VPNGW10:FCS_IPSEC_EXT.1	Session Establishment with peer	Entire packet contents of packets transmitted/received during session establishment Reason for failure
Oct 14 14:20:17 Aruba7030 isakmpd[3519]: <103077> <3519> <INFO> <Aruba7030 192.168.144.201> IKEv2 IKE_SA succeeded for peer 192.168.144.154:4500		

24B2F056.log

WLANASEP10:FCS_IPSEC_EXT.1	Protocol failures. Establishment/Termination of an IPsec SA. Negotiation “down” from an IKEv2 to IKEv1 exchange.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
Feb 27 14:46:53 isakmpd[3949]: <103063> <3949> <DBUG> |ike| exchange_start_ikev2 initiate for peer:192.168.145.249 Feb 27 14:46:53 isakmpd[3949]: <103063> <3949> <DBUG> |ike| exchange_start_ikev2 ipsecsa is NULL Feb 27 14:46:53 isakmpd[3949]: <103102> <3949> <INFO> |ike| IKE SA deleted for peer 192.168.145.249 See NDcPP21:FTP_ITC.1 for protocol establishment, termination and failure.		
NDcPP21:FCS_NTP_EXT.1	Configuration of a new time server Removal of configured time server	Identity of new/removed time server
Oct 26 12:27:22 Aruba7220 <Aruba7220 192.168.144.200> cli[29443]: USER:admin@172.16.16.100 NODE:"/mm/mynode" COMMAND:<ntp server 192.168.144.100 > -- command executed successfully Oct 26 12:38:02 Aruba7220 <Aruba7220 192.168.144.200> cli[29443]: USER:admin@172.16.16.100 NODE:"/mm/mynode" COMMAND:<no ntp server 192.168.144.100 > -- command executed successfully		
NDcPP21:FCS_RBG_EXT.1	None	None
NDcPP21:FCS_SSHS_EXT.1	Failure to establish an SSH session.	Reason for failure.
Oct 11 01:59:46 sshd[7305]: <199801> <7305> <INFO> |sshd| Failed password for admin from 192.168.144.249 port 36920 ssh2		
NDcPP21:FCS_TLSS_EXT.1	Failure to establish a TLS Session.	Reason for failure.
Feb 25 08:02:01 httpd[5131]: [ssl:warn] [pid 5131:tid 715980496] AH01909: ECC certificate configured for webui.securelogin.arubanetworks.com:443 does NOT include an ID which matches the server name, referer:		
NDcPP21:FDP_RIP.2	None	None
STFFW13:FFW_RUL_EXT.1	Application of rules configured with the 'log' operation.	Source and destination addresses. Source and destination ports. Transport Layer Protocol. TOE Interface.

		TOE interface that is unable to process packets. Identifier of rule causing packet drop.
Application of rules: Feb 28 00:08:11 cli[31763]: USER:admin@serial NODE:"/mm/mynode" COMMAND:<ip access-list session test_log> -- command executed successfully Feb 28 00:08:22 cli[31763]: USER:admin@serial NODE:"/mm/mynode" COMMAND:<any any any permit log> -- command executed successfully Feb 28 00:08:48 cli[31763]: USER:admin@serial NODE:"/mm/mynode" COMMAND:<host 192.168.144.1 any 22 deny log> -- command executed successfully Feb 28 00:11:58 cli[31763]: USER:admin@serial NODE:"/mm/mynode" COMMAND:<any host 192.168.145.1 icmp echo permit > -- command executed successfully Feb 28 00:13:50 cli[31763]: USER:admin@serial NODE:"/mm/mynode" COMMAND:<any host 192.168.145.1 icmp echo permit log> -- command executed successfully ACL logs: Feb 20 17:42:53 authmgr[3957]: <124006> <3957> <WARN> |authmgr| {944} UDP srcip=2001:192:168:144::254 srcport=32000 dstip=2001:172:16:8::15 dstport=21, action=permit, policy=ffw_1_5 Feb 20 17:43:03 authmgr[3957]: <124006> <3957> <WARN> |authmgr| {4562} UDP srcip=192.168.144.6 srcport=32000 dstip=172.16.8.15 dstport=21, action=deny, policy=ffw_1_5 Feb 20 21:08:08 authmgr[3957]: <124006> <3957> <WARN> |authmgr| {5693} ICMP srcip=192.168.144.2 dstip=192.168.144.251, type=8, code=0, sequence=256, id=40206, action=deny, policy=ffw_1_5 Feb 20 17:34:43 authmgr[3957]: <124006> <3957> <WARN> |authmgr| {914} ICMPv6 srcip=2001:192:168:144::254 dstip=fe80::b:8600:1b4:b347, type=136, code=0, action=permit, policy=ffw_1_5		
WLANASEP10:FIA_8021X_EXT.1	Attempts to access the 802.1X controlled port prior to successful completion of the authentication exchange.	Provided client identity (MAC address).
Feb 27 23:22:47 ucm[4350]: <347003> <5384> <DBUG> |ucm| ucm_handle_user_add_channel_events: GSM USER channel event received for mac: b8:d7:af:8d:1a:05, event_type: add		
NDcPP21:FIA_AFL.1	Unsuccessful login attempts limit is met or exceeded.	Origin of the attempt (e.g., IP address).
Nov 6 14:01:10 Aruba7030 aaa[3483]: <125027> <3483> <DBUG> <Aruba7030 192.168.144.201> mgmt-auth: admin, failure, , 0 Nov 6 14:01:10 Aruba7030 aaa[3483]: <125050> <3483> <DBUG> <Aruba7030 192.168.144.201> [aaaMsg.c:1316] Determining the existing sessions for user: admin with configured max_sessions 0		
WLANASEP10:FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions	None

	taken (e.g., disabling of an account) and the subsequent, if appropriate, restoration to the normal state (e.g., re-enabling of a terminal).	
Nov 6 14:01:10 Aruba7030 aaa[3483]: <125027> <3483> <DBUG> <Aruba7030 192.168.144.201> mgmt-auth: admin, failure, , 0 Nov 6 14:01:10 Aruba7030 aaa[3483]: <125050> <3483> <DBUG> <Aruba7030 192.168.144.201> [aaaMsg.c:1316] Determining the existing sessions for user: admin with configured max_sessions 0 Nov 11 16:40:54 Aruba7030 stm[3609]: <501103> <3609> <WARN> <Aruba7030 192.168.144.201> Blacklist add: 74:9e:f5:ff:a5:e9: Reason: auth-failure		
NDcPP21:FIA_PMG_EXT.1	None	None
VPNGW10:FIA_PSK_EXT.1	None	None
WLANASEP10:FIA_PSK_EXT.1	None	None
WLANASEP10:FIA_UAU.6	Attempts to re-authenticate.	Origin of the attempt (e.g., IP address).
Nov 16 12:00:39 Aruba7030 dot1x-proc: 2[4207]: <138086> <4207> <INFO> <Aruba7030 192.168.144.201> WPA 2 Key exchange failed to complete, de-authenticating the station 74:9e:f5:ff:a5:e9 associated with AP b4:5d:50:6f:7b:90 ap225 Nov 16 12:00:43 Aruba7030 authmgr[3586]: <124004> <5408> <DBUG> <Aruba7030 192.168.144.201> Adding station for this user: 74:9e:f5:ff:a5:e9 Nov 16 12:00:43 Aruba7030 authmgr[3586]: <124004> <5408> <DBUG> <Aruba7030 192.168.144.201> User (74:9e:f5:ff:a5:e9) found aaa profile 7220-Test_aaa_prof		
NDcPP21:FIA_UAU.7	None	None
NDcPP21:FIA_UAU_EXT.2	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
Tested as part of FIA_UIA_EXT.1		
NDcPP21:FIA_UIA_EXT.1	All use of identification and authentication mechanism.	Origin of the attempt (e.g., IP address).
Oct 11 00:09:18 sshd[24685]: <199801> <24685> <DBUG> |sshd| debug1: userauth-request for user admin service ssh-connection method password Oct 11 00:09:18 sshd[24685]: <199801> <24685> <INFO> |sshd| Accepted password for admin from 192.168.144.249 port 36904 ssh2 Feb 28 02:11:41 authmgr[3950]: <522038> <3950> <NOTI> |authmgr| username=user1 MAC=b8:d7:af:8d:1a:05 IP=0.0.0.0 Authentication result=Authentication Successful method=802.1x server=rad1		

Feb 28 02:13:30 authmgr[3950]: <522274> <3950> <ERRS> |authmgr| Mgmt User Authentication failed. username=admin userip=0.0.0.0 servername=rad1 serverip=192.168.144.249 Feb 28 01:37:53 webui[3800]: USER: admin has logged in from 192.168.144.253. Feb 28 01:34:15 cli[29241]: USER: admin has logged in using serial. Feb 28 01:48:27 cli[30967]: USER: admin connected using serial has logged out. Feb 28 01:50:15 cli[32640]: USER: admin has logged in using serial.		
NDcPP21:FIA_X509_EXT.1/Rev	Unsuccessful attempt to validate a certificate. Any addition, replacement or removal of trust anchors in the TOE's trust store	Reason for failure of certificate validation Identification of certificates added, replaced or removed as trust anchor in the TOE's trust store
Oct 26 08:55:55 Aruba7030 isakmpd[3524]: <103063> <3524> <DBUG> <Aruba7030 192.168.144.201> 192.168.144.154:4500-> Notify: 16417ike2_state.c (7683): errorCode = ERR_CERT_EXPIRED Oct 27 09:49:37 Aruba7030 <Aruba7030 192.168.144.201> webui[3408]: USER:admin@192.168.144.153 NODE:"/mm/mynode" COMMAND:<crypto pki-import pem TrustedCA rootca-unacceptable-rsa rootca-unacceptable-rsa.pem ****** > -- command executed successfully Oct 27 09:49:37 Aruba7030 <Aruba7030 192.168.144.201> profmgr[3559]: USER:admin@192.168.144.153 NODE:"/mm/mynode" COMMAND:<crypto-local pki TrustedCA rootca-unacceptable-rsa rootca-unacceptable-rsa.pem > -- command executed successfully		
NDcPP21/VPNGW10:FIA_X509_EXT.2	None	None
NDcPP21/VPNGW10:FIA_X509_EXT.3	None	None
NDcPP21:FMT_MOF.1/Functions	None	None
NDcPP21:FMT_MOF.1/ManualUpdate	Any attempt to initiate a manual update.	None
Dec 14 16:17:04 Aruba7030 <Aruba7030 192.168.144.201> cli[6558]: USER:admin@serial NODE:"/mm/mynode" COMMAND:<copy tftp: 172.16.16.153 ArubaOS_70xx_8.6.0.7-FIPS_78216 system: partition 0 > -- command executed successfully		
NDcPP21:FMT_MOF.1/Services	Starting and stopping of services.	None
Dec 15 15:13:49 Aruba7030 <Aruba7030 192.168.144.201> profmgr[3582]: USER:admin@172.16.16.153 NODE:"/mm/mynode" COMMAND:<no logging 1.1.1.1> -- command executed successfully Nov 13 09:22:56 Aruba7030 <Aruba7030 192.168.144.201> cli[24718]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<logging 172.16.16.154 format bsd-standard severity debugging > -- command executed successfully		
NDcPP21:FMT_MTD.1/CoreData	None	None
NDcPP21:FMT_MTD.1/CryptoKeys	Management of cryptographic keys.	None

Jan 8 09:57:06 Aruba7030 profmgr[3568]: <334000> <3568> <DBUG> <Aruba7030 192.168.144.201> profmgr_np_config_commit_working_entry: new objtype_buffer added , CMD: crypto-local pki TrustedCA ROOT_TEST rootca-rsa.pem

Jan 8 12:41:31 Aruba7220 profmgr[3671]: <334000> <3671> <DBUG> <Aruba7220 192.168.144.200> profmgr_np_config_gen_partial_cfg: cmd (crypto-local pki rcp ROOT_TEST), rev_for_del=0 rev_for_del_pend=0 rev_for_del_parent=0 inc_in_partial_for_del=0

VPNGW10:FMT_MTD.1/CryptoKeys	None	None
NDcPP21:FMT_SMF.1	All management activities of TSF data	None

Ability to administer the TOE locally and remotely
See audit records for NDcPP21:FIA_UIA_EXT.1 where successful login audits are recorded for each method of administration (both local and remote)

Ability to configure the access banner
Jan 7 13:46:10 cli[8523]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<banner motd | THIS IS THE BANNER |> -- command executed successfully

Ability to configure the session inactivity time before session termination
Jan 7 14:16:20 Aruba7030 <Aruba7030 192.168.144.201> cli[21465]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<loginsession timeout 0> -- command executed successfully

Ability to update the TOE, and to verify the updates using digital signature and [no other] capability prior to installing those updates
Dec 14 16:17:04 Aruba7030 <Aruba7030 192.168.144.201> cli[6558]: USER:admin@serial NODE:"/mm/mynode" COMMAND:<copy tftp: 172.16.16.153 ArubaOS_70xx_8.6.0.7-FIPS_78216 system: partition 0 > -- command executed successfully

Ability to configure the authentication failure parameters for FIA_AFL.1
Jan 7 16:17:05 Aruba7030 <Aruba7030 192.168.144.201> cli[14808]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<aaa password-policy mgmt> -- command executed successfully

Jan 7 16:17:05 Aruba7030 <Aruba7030 192.168.144.201> cli[14808]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<enable> -- command executed successfully

Jan 7 16:17:05 Aruba7030 <Aruba7030 192.168.144.201> cli[14808]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<password-lock-out 3> -- command executed successfully

Jan 7 16:17:05 Aruba7030 <Aruba7030 192.168.144.201> cli[14808]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<password-lock-out-time 1> -- command executed successfully

Ability to start and stop services
Dec 15 15:13:49 Aruba7030 <Aruba7030 192.168.144.201> profmgr[3582]: USER:admin@172.16.16.153 NODE:"/mm/mynode" COMMAND:<no logging 1.1.1.1> -- command executed successfully

Nov 13 09:22:56 Aruba7030 <Aruba7030 192.168.144.201> cli[24718]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<logging 172.16.16.154 format bsd-standard severity debugging > -- command executed successfully

Ability to manage the cryptographic keys
Jan 8 09:57:06 Aruba7030 profmgr[3568]: <334000> <3568> <DBUG> <Aruba7030 192.168.144.201> profmgr_np_config_commit_working_entry: new objtype_buffer added , CMD: crypto-local pki TrustedCA ROOT_TEST rootca-rsa.pem

Ability to configure the cryptographic functionality
Jan 8 09:14:15 Aruba7030 <Aruba7030 192.168.144.201> cli[20633]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<crypto isakmp policy 111> -- command executed successfully

Jan 8 09:14:27 Aruba7030 <Aruba7030 192.168.144.201> cli[20633]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<authentication pre-share> -- command executed successfully

Jan 8 09:15:14 Aruba7030 <Aruba7030 192.168.144.201> cli[20633]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<encryption aes128> -- command executed successfully

Jan 8 09:15:27 Aruba7030 <Aruba7030 192.168.144.201> cli[20633]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<hash sha> -- command executed successfully

Jan 8 09:15:42 Aruba7030 <Aruba7030 192.168.144.201> cli[20633]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<group 20> -- command executed successfully

Ability to configure the lifetime for IPsec SAs
Jan 7 15:37:33 Aruba7030 <Aruba7030 192.168.144.201> cli[6821]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<crypto-local ipsec-map gss 111> -- command executed successfully

Jan 7 15:37:33 Aruba7030 <Aruba7030 192.168.144.201> cli[6821]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<set security-association lifetime seconds 86400> -- command executed successfully

Jan 7 15:37:33 Aruba7030 <Aruba7030 192.168.144.201> cli[6821]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<crypto isakmp policy 111 > -- command executed successfully

Jan 7 15:37:33 Aruba7030 <Aruba7030 192.168.144.201> cli[6821]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<lifetime 86400> -- command executed successfully

Ability to import X.509v3 certificates to the TOE's trust store
Oct 27 09:49:37 Aruba7030 <Aruba7030 192.168.144.201> webui[3408]: USER:admin@192.168.144.153 NODE:"/mm/mynode" COMMAND:<crypto pki-import pem TrustedCA rootca-unacceptable-rsa rootca-unacceptable-rsa.pem ****** > -- command executed successfully

Oct 27 09:49:37 Aruba7030 <Aruba7030 192.168.144.201> profmgr[3559]: USER:admin@192.168.144.153 NODE:"/mm/mynode" COMMAND:<crypto-local pki TrustedCA rootca-unacceptable-rsa rootca-unacceptable-rsa.pem > -- command executed successfully

Ability to configure the list of TOE-provided services available before an entity is identified and authenticated, as specified in FIA_UIA_EXT.1

Jan 9 14:34:30 Aruba7030 <Aruba7030 192.168.144.201> profmgr[3568]: USER:admin@172.16.16.153 NODE:"/mm/mynode" COMMAND:<banner motd ~ THIS IS THE BANNER! ~> -- command executed successfully **Ability to set the time which is used for time-stamps** Jan 8 08:54:53 Aruba7030 <Aruba7030 192.168.144.201> cli[13685]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<clock timezone America/New_York 8 55> -- command executed successfully **Ability to configure NTP** Jan 20 20:00:46 Aruba7030 <Aruba7030 192.168.144.201> cli[6558]: USER:admin@serial NODE:"/mm/mynode" COMMAND:<ntp server 1.1.1.1 > -- command executed successfully **Ability to configure the reference identifier for the peer** Jan 8 09:13:02 Aruba7030 <Aruba7030 192.168.144.201> cli[20147]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<peer-cert-dn testing> -- command executed successfully		
VPNGW10:FMT_SMF.1	None	None
WLANASEP10:FMT_SMR.1	None	None
STFFW13:FMT_SMF.1/FFW	All management activities of TSF data (including creation, modification and deletion of firewall rules).	None
Jan 7 15:18:44 Aruba7030 <Aruba7030 192.168.144.201> cli[3054]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<ip access-list session test_log> -- command executed successfully Jan 6 13:09:40 Aruba7030 authmgr[3604]: <124590> <3604> <DBUG> <Aruba7030 192.168.144.201> Sending insert acl fau_gen.1.2:110 to fpapps. Jan 6 13:09:40 Aruba7030 authmgr[3604]: <124332> <3604> <DBUG> <Aruba7030 192.168.144.201> Add rule in policy fau_gen.1.2 with action 1 Jan 6 13:11:16 Aruba7030 authmgr[3604]: <124556> <3604> <DBUG> <Aruba7030 192.168.144.201> {ACL} Free ace entries: (acl 110).		
NDcPP21:FMT_SMR.2	None	None
VPNGW10:FPF_RUL_EXT.1	Application of rules configured with the 'log' operation	Source and destination addresses Source and destination ports Transport Layer Protocol
See logs: STFFW13:FFW_RUL_EXT.1		
NDcPP21:FPT_APW_EXT.1	None	None
VPNGW10:FPT_FLS.1	None	None
WLANASEP10:FPT_FLS.1	Failure of the TSF.	Indication that the TSF has failed with the type of failure that occurred.

[123.028000] 2:apsd_porf_getdmamem: physical address 0xB4E10000, virtual address 0xc0000000b4e10000, size 8192 openssl crng for rngd failed [DONE] [05:14:08]:Initializing FPAPPs [149.219000] 0:<4>hrtimer: interrupt took 3000963 ns [151.025000] 0:<3>MTD get_chip(): chip not ready after erase suspend Starting OpenSSL FIPS KAT test		
NDcPP21:FPT_SKP_EXT.1	None	None
NDcPP21:FPT_STM_EXT.1	Discontinuous changes to time - either Administrator actuated or changed via an automated process. (Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1)	For discontinuous changes to time: The old and new values for the time. Origin of the attempt to change time for success and failure (e.g., IP address).
Aug 26 10:28:58 Aruba7030 <Aruba7030 192.168.144.201> ctrlmgmt: USER:admin: clock changed from Wed Aug 26 10:29:02 EDT 2020 to Wed Aug 26 10:28:58 EDT 2020 Aug 26 10:28:58 Aruba7030 <Aruba7030 192.168.144.201> cli[18263]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<clock set 2020 august 26 10 28 58 > -- command executed successfully		
NDcPP21:FPT_TST_EXT.1	None	None
WLANASEP10:FPT_TST_EXT.1	Execution of this set of TSF self-tests. Detected integrity violations.	For integrity violations, the TSF code file that caused the integrity violation.
[151.793000] 6:apsd_porf_getdmamem: physical address 0x15E7C0000, virtual address 0xc00000015e7c0000, size 8192 openssl sha1 failed [14:51:18]:Initializing FPAPPs [240.364000] 3:apsd_controller_vlan_device_set::Vlanid sent from user space : 1 __controller_vlan_id set in APSD driver : 1 [240.611000] 2:apsd_controller_vlan_device_set::Vlanid sent from user space : 1 __controller_vlan_id set in APSD driver : 1 Starting OpenSSL FIPS KAT test openssl sha1 failed openssl sha1 failed openssl sha1 failed OpenSSL FIPS KAT test FAILED!! Restarting System		
VPNGW10:FPT_TST_EXT.3	None	None
NDcPP21:FPT_TUD_EXT.1	Initiation of update; result of the update attempt (success or failure).	None

Dec 11 16:39:02 Aruba7030 <Aruba7030 192.168.144.201> cli[31503]: USER:admin@192.168.144.154 NODE:"/mm/mynode" COMMAND:<copy tftp: 172.16.16.153 ArubaOS_70xx_8.6.1.0-FIPS.fcs86x_fips_no_sig system: partition 1 > -- command executed successfully		
VPNGW10:FPT_TUD_EXT.1	None	None
NDcPP21:FTA_SSL.3	The termination of a remote session by the session locking mechanism.	None
Feb 27 10:52:23 webui[3800]: USER: admin connected from 192.168.144.3 has timed out. Sep 8 10:52:44 Aruba7030 <Aruba7030 192.168.144.201> cli[14459]: USER: admin connected from 172.16.16.154 has logged out. Reason: Idle timeout		
NDcPP21:FTA_SSL.4	The termination of an interactive session.	None
Feb 28 02:26:52 webui[3800]: USER: admin connected from 192.168.144.253 has logged out. Feb 28 02:57:47 sshd[15323]: <199801> <15323> <INFO> |sshd| Close session: user admin from 192.168.144.253 port 51968 id 0 Sep 8 11:30:05 Aruba7030 sshd[10027]: <199801> <10027> <INFO> <Aruba7030 192.168.144.201> Received disconnect from 172.16.16.154 port 40676:11: disconnected by user		
NDcPP21:FTA_SSL_EXT.1	(if 'lock the session' is selected) Any attempts at unlocking of an interactive session. (if 'terminate the session' is selected) The termination of a local session by the session locking mechanism.	None
Sep 8 11:33:34 Aruba7030 <Aruba7030 192.168.144.201> cli[10822]: USER: admin connected using serial has logged out. Reason: Idle timeout		
NDcPP21:FTA_TAB.1	None	None
VPNGW10:FTA_TSE.1	None	None
WLANASEP10:FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism.	Reason for denial, origin of establishment attempt.
Dec 10 15:13:09 Aruba7030 stm[3609]: <304003> <3609> <DBUG> <Aruba7030 192.168.144.201> Sending Time Range Monitor message to Auth denywifi_periodic-1 Dec 10 15:13:09 Aruba7030 authmgr[3583]: <124004> <3583> <DBUG> <Aruba7030 192.168.144.201> Start monitoring time-range 'denywifi_periodic' for remote notification Dec 10 15:13:15 Aruba7030 authmgr[3583]: <124039> <3583> <INFO> <Aruba7030 192.168.144.201> Time-range denywifi_periodic activated		
VPNGW10:FTA_VCM_EXT.1	None	None

<table>
<tr><td>NDcPP21:FTP_ITC.1</td><td>Initiation of the trusted channel.

Termination of the trusted channel.

Failure of the trusted channel functions.</td><td>Identification of the initiator and target of failed trusted channels establishment attempt.</td></tr>
<tr><td colspan="3">Initiation:

Oct 11 01:52:12 isakmpd[3922]: <103076> <3922> <DBUG> |ike| IKEv2 IPSEC Tunnel created for peer 192.168.144.243:50750

Oct 14 14:20:17 Aruba7030 isakmpd[3519]: <103077> <3519> <INFO> <Aruba7030 192.168.144.201> IKEv2 IKE_SA succeeded for peer 192.168.144.154:4500

Termination:

Feb 27 14:46:53 isakmpd[3949]: <103102> <3949> <INFO> |ike| IKE SA deleted for peer 192.168.145.249

Failure:

Oct 11 01:36:37 isakmpd[3922]: <103060> <3922> <DBUG> |ike| 192.168.144.243:50750-> ike_phase_1.c:attribute_unacceptable:2850 Proposal match failed in auth algo, configured=RSA_SIG, peer using=unknown</td></tr>
<tr><td>VPNGW10:FTP_ITC.1</td><td>None</td><td>None</td></tr>
<tr><td>WLANASEP10:FTP_ITC.1</td><td>Failed attempts to establish a trusted channel (including IEEE 802.11).

Detection of modification of channel data.</td><td>Identification of the initiator and target of channel.</td></tr>
<tr><td colspan="3">Nov 16 12:00:39 Aruba7030 dot1x-proc: 2[4207]: <138086> <4207> <INFO> <Aruba7030 192.168.144.201> WPA 2 Key exchange failed to complete, de-authenticating the station 74:9e:f5:ff:a5:e9 associated with AP b4:5d:50:6f:7b:90 ap225</td></tr>
<tr><td>NDcPP21:FTP_TRP.1/Admin</td><td>Initiation of the trusted path.

Termination of the trusted path.

Failure of the trusted path functions.</td><td>None</td></tr>
<tr><td colspan="3">Initiation:

Oct 15 09:17:20 Aruba7030 sshd[4976]: <199801> <4976> <INFO> <Aruba7030 192.168.144.201> Connection from 192.168.144.154 port 44596 on 192.168.144.201 port 22</td></tr>
</table>

Jul 28 11 01:59:46 sshd[7305]: <125032> <7305> <info> |sshd| Authentication Succeeded for User admin, Logged in from 192.167.144.253 port 22, Connecting to 192.168.144.5 port 22 connection type SSH

Oct 26 12:16:28 Aruba7030 <Aruba7030 192.168.144.201> webui[3408]: TLS connection with client 192.168.144.153 is established.

Feb 28 01:37:53 webui[3800]: USER: admin has logged in from 192.168.144.253.

Termination:

Oct 14 13:41:04 Aruba7030 <Aruba7030 192.168.144.201> webui[3403]: TLS connection with client 192.168.144.153 is terminated.

Feb 27 10:52:23 webui[3800]: USER: admin connected from 192.168.144.3 has timed out.

Oct 15 12:11:08 Aruba7030 sshd[6100]: <199801> <6100> <INFO> <Aruba7030 192.168.144.201> Received disconnect from 192.168.144.154 port 44802:11: disconnected by user

Oct 15 12:11:08 Aruba7030 sshd[6100]: <199801> <6100> <INFO> <Aruba7030 192.168.144.201> Disconnected from user admin 192.168.144.154 port 44802

Feb 28 02:57:47 sshd[15323]: <199801> <15323> <INFO> |sshd| Close session: user admin from 192.168.144.253 port 51968 id 0

Failure:

Jul 28 19:28:24 httpd[5853]: [ssl:error] [pid 5853:tid 870642864] [client 192.168.144.249:53892] AH02039: Certificate Verification: Error (19): self signed certificate in certificate chain, referer:

Oct 8 10:07:05 Aruba7030 sshd[22714]: <199801> <22714> <INFO> <Aruba7030 192.168.144.201> Failed password for admin from 192.168.144.154 port 33902 ssh2

All Administrative actions are audited by the TOE. As noted within the Syslog Guide for 8.X (https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-c05321932), the controller creates syslog entries for all commands and configuration changes that alter system behavior, the user name of the user making the change, and the location of the user. This information appears in the output of the syslog, with the keyword COMMAND. This same information also appears in the output of the CLI command **show audit-trail**.

The syslog information in the example below shows that a user with the username **admin** logged in to the controller through the serial port, changed logging levels, loaded new software onto partition 1, then updated the system clock.

Oct 2 18:50:00 cli[19855]: USER:admin@serial NODE:"/mm/mynode" COMMAND:<clock set 2018 october 2 18 50 00> -- command executed successfully

Sep 1 01:26:34 nanny[5174]: <399814> <5174> <DBUG> |nanny| PROCESS_RUNNING Process ntpwrap marked as PROCESS_RUNNING Timeout value : 240 Time updated: 56 sec

Oct 2 20:55:43 nanny[5174]: <399814> <5174> <DBUG> |nanny| PROCESS_RUNNING Process ntpwrap marked PROCESS_NOT_RESPONDING Timeout value : 240 Time since not updated : 2748544 sec

By default, the controller does not generate a log entry for **show** commands issued using the CLI, as these commands display existing settings but do not change system behavior. To create a log entry for all commands issued, (including show commands) access the CLI in config mode and issue the command **audit-trail all**.

A full record of audit records generated by the controller can be found at the following link:

https://support.hpe.com/hpesc/public/docDisplay?docId=emr_na-c05321932

2.2.2 FAU_GEN.2

No configuration required.

2.2.3 FAU_STG.1

No configuration required.

2.2.4 FAU_STG_EXT.1

Local storage space for audit logs is limited on a mobility controller. The local protected log storage operates using the first in, first out (FIFO) method, therefore audit logs are overwritten when the available space is exhausted.To operate in the evaluated configuration, an external syslog server **must** be used. All audit logs are simultaneously written to both the local audit log and the syslog server. The local audit logs and logs sent to a remote server are identical.

To configure an external syslog server:

```
(config)# logging <ip address>
```

The connection between the mobility controller and the syslog server must be protected using IPsec. Configure a site-to-site VPN tunnel to carry this traffic. The syslog server must use a different IP address for the syslog receiver process than it uses for IPsec termination. Alternatively, a VPN gateway (such as an Aruba mobility controller) may front-end the syslog server to provide the IPsec tunnel. The following is an example of an IPsec tunnel which assumes that the syslog receiver process listens on 192.168.1.1, and the IPsec tunnel terminates on 192.168.2.1 – these IP addresses may be on the same server, or on different systems.

```
crypto-local ipsec-map <name> 10
  version v2
  set ikev2-policy <policy>
  peer-ip <ip address>
  src-net <ip address> <subnet>
  dst-net <ip address> <subnet>
  set transform-set "<transform-set>"
  set security-association lifetime seconds <seconds>
  set security-association lifetime kilobytes <kilobytes>
```

```
pre-connect enable
trusted enable
uplink-failover disable
force-natt disable
set ca-certificate root-ca
set server-certificate server-cert
```

Adjust the above ipsec-map as appropriate, following instructions in the ArubaOS User Guide. The peer-ip and dst-net addresses cannot be the same. Note that bi-directional communication is not necessary – syslog is sent using UDP, so the only requirement is that packets are able to flow from the mobility controller to the syslog server.

2.3 Cryptographic Support (FCS)

2.3.1 FCS_CKM.1

No configuration required. Ensure the controller has FIPS mode enabled so that cryptographic requirements are met.

(config)# fips enable

During regular operation of the TOE, key generation is invoked during session establishment between the TOE and external IT entities for user sessions. An administrator can invoke the use of RSA and ECDSA during generation of certificates used for X.509. Information on configuration X.509 can be found in Section 2.5.10 through Section 2.5.12.

2.3.2 FCS_CKM.4

No configuration required. During runtime, all CSPs will be zeroized automatically when no longer needed. To erase all CSPs stored in flash memory (as well as software images and configuration files), issue the command ‘zeroize-tpm-keys’ (for hardware) and ‘wipe out flash’ (for virtual). This command will overwrite the entire flash with an alternating pattern. The controller must be restored through TFTP after this process. In addition, files in the flash can be zeroized using the ‘write erase all’ command. There are no configurations or circumstances that do not strictly conform to the key destruction requirement.

For further details on sanitizing systems, request the document “Identification of Non-Volatile Storage and Sanitization of System Components” from Aruba Networks.

2.3.3 FCS_COP.1

Ensure that the Advanced Cryptography License is installed in order for all required cryptographic algorithms to be enabled. Ensure the controller has FIPS mode enabled so that cryptographic requirements are met.

(config)# fips enable

2.3.4 FCS_HTTPS_EXT.1

No configuration is required. The TOE will function over HTTPS, compliant to RFC 2818, when operation under FIPS mode.

2.3.5 FCS_IPSEC_EXT.1

2.3.5.1 FCS_IPSEC_EXT.1.1/2

RFC 4301 references an explicit Security Policy Database (SPD) with rules for DISCARD, BYPASS, and PROTECT. ArubaOS does not implement an explicit SPD, but equivalent behavior may be obtained through the use of firewall policies and “routing” ACLs.

The access-list in the following configuration defines the behavior with rules for PROTECT BYPASS and DISCARD. Note that the traffic that is to be protected is defined in an ipsec-map (see Section 2.3.5.2 FCS_IPSEC_EXT.1.3). The ipsec-map defines traffic that will be encrypted in an IPsec connection. The access-list determines whether traffic will be permitted or denied. If traffic is permitted, it is then processed to see if the traffic is encrypted in IPsec. If the traffic

matches the rules defined in the ipsec-map, then the traffic will be encrypted. Otherwise, it will bypass the tunnel and proceed in plaintext.

```
ip access-list session spd-test
      host 192.168.144.153 any icmp echo permit log
      host 192.168.144.153 any tcp 22 deny log
      network 1.1.1.0 255.255.255.0 any any permit log
      any network 1.1.1.0 255.255.255.0 any permit log
      host 192.168.144.154 any any permit log
      any host 192.168.144.154 any permit log
      any any any deny log
```

The 1st rule is a BYPASS rule using the ICMP echo-request which allows plaintext traffic from 192.168.144.153. The 2nd rule is a DISCARD (deny) rule to discard SSH traffic from 192.168.144.153. The 3rd, 4th, 5th and 6th rules are PROTECT (permit) rules to allow encrypted traffic to flow through the IPsec tunnel. The final rule is a default deny rule.

Section 2.5.1.2 FFW_RUL_EXT.1.5 describes how the access list is assigned to an interface.

These rules can be modified as needed for explicit control over tunneled and non-tunneled traffic. Note: Most deployments will not make use of this feature, as ALL traffic to a specific destination will typically be tunneled. The sample config file at the end of this document does NOT contain examples from this section.

The configuration above provides SPD control for inbound wired traffic. For wireless or VPN client users (not tested as part of the Common Criteria evaluation), multiple ACLs may be sequenced with a user-role container, simplifying this configuration.)

The access control lists used by the TOE are read in hierarchical order. When traffic enters or exits the TOE, the first applicable rule in the ACL is applied. Any rule below the initially triggered rule is not applied. Note that if an access rule is applied, a duplicate cannot be entered. If the administrator applied a permit rule and then enters a deny rule with the same parameters, the deny rule will replace the permit rule and vice versa.

2.3.5.2 FCS_IPSEC_EXT.1.3

ArubaOS supports both IPsec in tunnel mode and transport mode. The following configuration shows an example of a site-to-site IPsec VPN tunnel:

```
crypto-local ipsec-map 10.10.20.1 100
  version v2
  set ikev2-policy 10009
  peer-ip 192.168.2.1
  vlan 2
```

```
  src-net 172.16.1.0 255.255.255.0
  dst-net 10.10.20.0 255.255.255.0
  set transform-set "default-gcm256"
  set pfs group20
  set security-association lifetime seconds 420
  set security-association lifetime kilobytes 30000
  pre-connect enable
  trusted enable
  uplink-failover disable
  force-natt disable
  set ca-certificate root-ca
  set server-certificate server-cert
```

Running the following command will show that both transport and tunnel mode can be used in negotiation:

```
show crypto ipsec transform-set
Transform set default-transform: { esp-aes128 esp-sha-hmac }
    will negotiate = { Transport, Tunnel }
```

Additionally, the following command can be used under the crypto-local ipsec-map to force tunnel mode to be the only option offered. However, it is not necessary with the above configuration.

```
  force-tunnel-mode
```

With this command present, the crypto map would show the following:

```
Transform set transform-tunnel: { esp-aes128 esp-sha-hmac }
    will negotiate = { Tunnel }
```

2.3.5.3 FCS_IPSEC_EXT.1.4

IPsec cipher suites are configured using transform-sets. These are ordered lists of ciphers - the controller will attempt each one in order until one is successfully negotiated with the peer. The command "show crypto ipsec transform-set" will display the configured transform sets.

ArubaOS provides pre-configured transforms that meet three of the Common Criteria requirements. Note that the Advanced Cryptography License must be installed in order to have access to AES-GCM. The default transforms are:

```
Transform set default-gcm256: { esp-aes256-gcm  }
Transform set default-gcm128: { esp-aes128-gcm  }
Transform set default-aes: { esp-aes256 esp-sha-hmac }
```

Note: The TOE's IPsec ESP protocol implementation supports only HMAC-SHA-1. The IKE protocol supports HMAC-SHA-1, HMAC-SHA-256 and HMAC-SHA-384 (see section 2.3.5.5 FCS_IPSEC_EXT.1.6 below).

To configure AES-CBC-128, add a new transform set:

```
(config) #crypto ipsec transform-set aes128 esp-aes128 esp-sha-hmac
```

The transform sets above are referenced directly by name when creating a site-site IPsec tunnel, as shown in FCS_IPSEC_EXT.1.2. For IPsec VPN clients (non site-to-site), dynamic-maps are used to order the list of transform sets. The command "show crypto dynamic-map" will list these. The number assigned to the dynamic-map indicates the priority - a lower number will be matched before a higher number. To create a single dynamic-map which incorporates all required transform sets for evaluation, configure the following:

```
(config) #crypto dynamic-map cc-required 1
(config-dynamic-map)#  set transform-set default-gcm256 default-gcm128
default-aes aes128
```

The resulting dynamic-map:

```
Crypto Map Template"cc-required" 1
         IKE Version: 2
         IKEv2 Policy: DEFAULT
         Security association lifetime seconds : [300 -86400]
         Security association lifetime kilobytes: N/A
         PFS (Y/N): Y (Use the 384-bit Diffie Hellman elliptic curve
group
         Transform sets={ default-gcm256, default-gcm128, default-aes,
aes128 }
```

This dynamic-map will be revisited in future sections. Note that SA lifetimes have not yet been set in this example; this will be done further in this document.

PFS has been enabled in this example. Although the VPNGW PP-Module does not mandate the use of Perfect Forward Secrecy, it is a security best-practice. To enable PFS:

```
(config-dynamic-map)#  set pfs group20
```

2.3.5.4 FCS_IPSEC_EXT.1.5

IKEv1 and IKEv2 are both supported, and both may be configured simultaneously. NAT Traversal (NAT-T) is supported for both. NAT-T transports packets over UDP port 4500 rather than using IPsec native encapsulation.

For inbound connections where the controller is the IKE responder, NAT-T is supported by default. To disable, install a firewall rule that blocks UDP 4500.

For outbound connections in a site-to-site VPN tunnel, NAT-T is configured in the ipsec-map described in FCS_IPSEC_EXT.1.2. To force NAT-T rather than allowing it to be negotiated, issue the following command:

```
(config) #crypto-local ipsec-map 10.10.20.1 100
(config-ipsec-map)#  force-natt enable
```

To specify the IKEv1 or IKEv2 policy:

```
(config) #crypto isakmp policy <priority>
(config-isakmp) #version <v1 | v2>
```

2.3.5.5 FCS_IPSEC_EXT.1.6

IKE policies are matched in numerical order, with lower numbers having higher priority. A number of IKE policies are pre-configured - to view these, issue the command "show crypto isakmp policy".

Default policies may not be deleted, but may be disabled. To disable a policy:

```
(config) #crypto isakmp policy <policy>
(config-isakmp)# disable
```

It is recommended that when deployed as a VPN gateway, **all** default IKE policies be disabled, and only user-defined policies configured for use.

To configure an IKEv2 policy that uses AES-256, issue the following commands:

```
(config) # crypto isakmp policy 100
(config-isakmp)# encryption aes256
(config-isakmp)# hash sha
(config-isakmp)# version v2
```

To configure IKEv1 or AES128, adjust the version to ‘v1’ and the encryption to ‘encryption aes128’. Similarly, to configure AES192 adjust the encryption to ‘aes192’. To configure HMAC-SHA-256 or HMAC-SHA-384, adjust the hash to ‘sha2-256-128’ or ‘sha2-384-192’.

2.3.5.6 FCS_IPSEC_EXT.1.7/8

Disable IKEv1 aggressive mode using the following command:

```
(config) #crypto-local isakmp disable-aggressive-mode
```

Note that with aggressive mode disabled, master-local communication (if used) must be authenticated using certificates, and not pre-shared keys.

For IKEv1 Phase 1 SA and IKEv2 SA, lifetimes are configured in the IKE policies in seconds (300-86400 seconds). Thus, the lifetime can be set within 1-24 hours. To adjust a previously-created IKE policy for a 24-hour lifetime (this is the default value), issue the following commands:

```
(config) # crypto isakmp policy 100
(config-isakmp)# lifetime 86400
```

For IKEv1 Phase 2 SA and IKEv2 Child SA, lifetimes are configured in the ipsec-map (for site-to-site). The lifetime for the security association (SA) is configured in seconds (300-28800 seconds). Thus, the lifetime can be set within 1-8 hours. The lifetime is configured using the following commands:

```
(config) #crypto-local ipsec-map 10.10.20.1 100
(config-ipsec-map)#  set security-association lifetime seconds 28800
```

or the dynamic-map (for client VPN):

```
(config) #crypto dynamic-map cc-required 1
(config-dynamic-map)#  set security-association lifetime seconds 28800
```

2.3.5.7 FCS_IPSEC_EXT.1.9/10

No configuration required to meet these requirements.

2.3.5.8 FCS_IPSEC_EXT.1.11

ArubaOS supports DH groups 14, 19, and 20. To configure, modify the IKE policy:

```
(config) # crypto isakmp policy 100
(config-isakmp)# group 20
```

2.3.5.9 FCS_IPSEC_EXT.1.13

ArubaOS supports both RSA and ECDSA certificates. Note that the Advanced Cryptography License must be installed to make use of ECDSA.

Loading of certificates onto the controller for both authentication to peers and for verification of other peers is described in the “Managing Certificates” section of the ArubaOS User Guide. Minimally, both a "server certificate" and a "trusted root CA" certificate must be loaded onto the controller in order to perform IPsec operations. Once these certificates are loaded on the controller, configure them for use in IPsec. For use with dynamic VPN clients:

```
(config) #crypto-local isakmp server-certificate "server-cert"
(config) #crypto-local isakmp ca-certificate "trusted-root-ca-cert"
```

For a site-to-site VPN tunnel:

```
(config) #crypto-local ipsec-map 10.10.20.1 100
```

```
(config-ipsec-map)#  set server-certificate server-cert
(config-ipsec-map)#  set ca-certificate root-ca
```

To configure an IKE policy to authenticate RSA certificates sent by peers, use the following command:

```
(config) #crypto isakmp policy 100
(config-isakmp)# authentication rsa-sig
```

To configure an IKE policy for ECDSA-384 authentication, use the following command:

```
(config) #crypto isakmp policy 100
(config-isakmp)# authentication ecdsa-384
```

ECDSA-256 may be supported by replacing "384" with "256".

Administrators should take care to configure IKE/IPsec policies so that the strength of the IKE association is greater than or equal to the strength of the IPsec tunnel (for example, by always using AES-256). However, if a misconfiguration is made, the controller will reject the security association along with generating an audit log message.

When the IPsec connection is configured to use pre-shared keys, the administrator can follow the following steps to configure a pre-shared key on the TOE:

To configure the key, pick one of the following options:

```
(config) #crypto-local isakmp key DEADBEEF01010202abc!@# address 0.0.0.0
netmask 0.0.0.0
```

When configuring the pre-shared key, the administrator must ensure that the PSK is at least 22 characters, contains at least one uppercase character, one lowercase character, one special character, and one digit. If the PSK is configured as a bit-based key, the ‘key-hex’ field should be used instead.

```
(config) #crypto-local isakmp key-hex DEADBEEF01010202ABA010 address
0.0.0.0 netmask 0.0.0.0
```

2.3.5.10 FCS_IPSEC_EXT.1.14

The TOE does not support SAN extension.

To configure the TOE reference identifier for the distinguished name of the peer, an administrator may use the following commands:

```
(config) #crypto-local ipsec-map testmap 1
(config-submode)#peer-cert-dn
     <peer-dn>       Subject-Name DN string of the Peer's Certificate
```

To ensure appropriate compliance within the evaluated configuration, the administrator should generate a CA chain with one Root CA and two Intermediate CAs. The OCSP configuration and information on this can be found under Sections 2.5.10 through 2.5.12.

2.3.6 FCS_RBG_EXT.1

No configuration required.

2.3.7 FCS_SSHS_EXT.1

Telnet or SSH access requires that you configure an IP address and a default gateway. No configuration is needed to specify the permitted algorithms after ‘fips enable’ has been set. The controller will attempt negotiations using AES128-CBC, AES256-CBC, AES128-CTR, and AES256-CTR in conjunction with HMAC-SHA-1 and HMAC-SHA1-96 and RSA using the following key exchange method: diffie-hellman-group14-sha1.

To view configuration for SSH, the following command can be used:

```
show ssh
```

To configure the SSH server, the following commands can be used:

```
ssh disable_dsa
```

```
ssh mgmt-auth {public-key [username/password]|username/password [public-key]}
```

To configure authentication for SSH using public key (SSH-RSA), the following commands can be used:

```
ssh mgmt-auth public-key
```

```
mgmt-user ssh-pubkey client-cert ssh-pubkey cli-admin root
```

SSH rekey intervals are non-configurable and are set to a maximum time interval of one (1) hour or 512M, whichever occurs first.

2.3.8 FCS_TLSS_EXT.1

No configuration is required to set the permitted cipher suites or the associated key agreement parameters once ‘fips enable’ has been entered on the controller. The TOE performs RSA key establishment with key sizes 2048 bits and generates DH parameters over NIST curve secp256r1. The controller negotiates using TLSv1.2 and the following ciphersuites:

- RSA:
    - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
    - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
    - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
    - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- ECDSA:
    - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
    - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
    - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
    - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

To view configuration for TLS, the following command can be used:

```
show web-server profile
show web-server statistics
```

The following commands can be used to configure the TLS web-server profile:

```
web-server profile
absolute-session-timeout <30-3600>
ciphers high
mgmt-auth username/password
session-timeout <30-3600>
ssl-protocol tlsv1.2
web-max-clients <25-320>
web-https-port-443
switch-cert <name>
```

2.4 User Data Protection (FDP)

2.4.1 FDP_RIP.2

No configuration required.

2.5 Firewall (FFW)

2.5.1 FFW_RUL_EXT.1

2.5.1.1 FFW_RUL_EXT.1.2/3/4

ArubaOS supports standard, extended, and session ACLs. Only session ACLs are stateful. Do not configure other types of ACLs.

By default, ArubaOS does not enforce a full three-way TCP handshake before permitting traffic – this is an optimization for Wi-Fi mobility. To enable enforcement of a full TCP handshake, configure the system as follows:

```
(config) #firewall enforce-tcp-handshake
```

To enable enforcement of TCP sequence numbers:

```
(config) #firewall enforce-tcp-sequence
```

To process ICMP packets statefully, enable stateful ICMP processing:

```
(config) #firewall enable-stateful-icmp
```

To statefully follow TCP session teardown, enable the following feature:

```
(config) #firewall prohibit-rst-replay
```

Perform similar configuration for IPv6:

```
(config) #ipv6 firewall enforce-tcp-handshake
(config) #ipv6 firewall prohibit-rst-replay
```

```
(config) #ipv6 firewall enable-stateful-icmp
```

The ArubaOS User Guide contains a full description of how firewall rules are configured. This guidance provides a summary. Firewall rules are configured according to a common general pattern:

```
(config) #ip access-list session <name>
```

```
(config-sess-<name>)# <source> <destination> <service> <action> <extended action> <position>
```

Rules should be configured in order from highest priority to lowest; enforcement is based on a first-match principle where the first rule that matches a traffic flow is applied, and further rules are not processed. The <position> field may be used to insert new rules somewhere other than at the end of a policy.

The following shows several examples of different rules that may be configured, which should give the reader a flavor of what is possible. Context-sensitive help is available in the ArubaOS CLI at any time by typing the ? character.

The following examples demonstrate the use of these commands.

ICMPv4:

```
(config) #ip access-list session FFW_RUL_EXT_1_3
```

```
(config-sess-FFW_RUL_EXT_1_3)#any any icmp echo deny
```

```
(config-sess-FFW_RUL_EXT_1_3)#any network 10.0.0.0 255.0.0.0 icmp port-unreachable permit
```

```
(config-sess-FFW_RUL_EXT_1_3)#host 172.16.52.1 any icmp traceroute permit
```

```
(config-sess-FFW_RUL_EXT_1_3)#any any icmp 3 permit
```

```
(config-sess-FFW_RUL_EXT_1_3)#any any svc-icmp deny log
```

Note: In the final example, the alias “svc-icmp” was used. This is a firewall *alias* which is defined using the keyword “netservice”. In the standard ArubaOS config file, *svc-icmp* is defined as follows:

```
netservice svc-icmp 1
```

This indicates that it is IP protocol 1 (ICMP). The “netservice” definition does NOT indicate network services (listeners) that are enabled on the mobility controller – they are used only for convenience when defining firewall rules.

ICMPv6:

```
(config-sess-FFW_RUL_EXT_1_3)#ipv6 any any icmpv6 echo-request deny
(config-sess-FFW_RUL_EXT_1_3)#ipv6 any network 2004:10:09::0/64 icmpv6 port-unreachable permit
(config-sess-FFW_RUL_EXT_1_3)#ipv6 host 2006:03:23::123 any icmpv6 hop-limit-exceeded permit
(config-sess-FFW_RUL_EXT_1_3)#ipv6 any any icmpv6 nb-adv permit
(config-sess-FFW_RUL_EXT_1_3)#ipv6 any any icmpv6 nb-solicitation permit
```

IPv4:

```
(config-sess-FFW_RUL_EXT_1_3)#any network 10.2.3.0 255.255.255.0 any permit
(config-sess-FFW_RUL_EXT_1_3)#host 1.2.3.4 any any deny log
(config-sess-FFW_RUL_EXT_1_3)#any network 10.2.4.0 255.255.255.0 17 permit
```

IPv6:

```
(config-sess-FFW_RUL_EXT_1_3)#ipv6 any network 2001:42:65::0/64 any permit
(config-sess-FFW_RUL_EXT_1_3)#ipv6 any network 2001:42:66::0/64 17 deny log
```

TCP:

```
(config-sess-FFW_RUL_EXT_1_3)#any any tcp source 53 dest 65 permit
(config-sess-FFW_RUL_EXT_1_3)#any any tcp 80 permit
```

UDP:

```
(config-sess-FFW_RUL_EXT_1_3)#any any udp source 1234 dest 5678 permit
(config-sess-FFW_RUL_EXT_1_3)#any any udp 53 permit
```

The TOE can be configured to restrict the distinct interface (ie. the external port where the applicable network traffic was received or will be sent) and the.following protocols and associated attributes:

- ICMPv4
    - Source address
    - Destination Address
    - Type
    - Code
- ICMPv6
    - Source address

    - Destination Address
    - Type
    - Code
- IPv4
    - Source address
    - Destination Address
    - Transport Layer Protocol
- IPv6
    - Source address
    - Destination Address
    - Transport Layer Protocol
    - IPv6 Extension header type
- TCP
    - Source address
    - Destination Address
    - Source Port
    - Destination Port
- UDP
    - Source address
    - Destination Address
    - Source Port
    - Destination Port

2.5.1.2 FFW_RUL_EXT.1.5

Once a firewall policy is defined, it may be assigned to an interface. The following examples show a firewall policy being applied to a physical Ethernet port, and to a VLAN interface.

```
(config) #interface gigabitethernet 1/3
(config-if)#ip access-group FFW_RUL_EXT_1_3 session
(config-if)#interface gigabitethernet 1/2
(config-if)#ip access-group FFW_RUL_EXT_1_3 session vlan 2
```

The following commands can be used to ensure TCP sequencing is properly enforced:

```
firewall enforce-tcp-handshake
firewall enforce-tcp-sequence
```

```
firewall prohibit-rst-replay
ipv6 firewall enforce-tcp-handshake
ipv6 firewall enforce-tcp-sequence
ipv6 firewall prohibit-rst-replay
```

The TOE provides stateful session firewalls for communication sent through its interfaces. The Aruba Policy Enforcement Firewall (PEF) provides context-based controls to enforce application-layer security and prioritization. With PEF, IT can enforce network access policies that specify who may access the network, with which mobile devices and which areas of the network they may access.

The TOE implements a full stateful firewall instance around every user, tightly controlling what the user is permitted to do and providing separation between user classes.

For the highest level of network security, Mobility Controllers support client-to-data center encryption, whether providing Wi-Fi services or VPN tunneling. The TOE provides a unified point for authentication, encryption and policy enforcement. When session access control lists are configured with logging specified, traffic sent through the session will be logged in syslog and recorded within statistical counters that can be viewed by an administrator.

2.5.1.3 FFW_RUL_EXT.1.6

The following commands can be used to ensure proper handling of traffic with addresses identified as ‘reserved for future use’.

```
firewall deny-reserved-ip
ipv6 firewall deny-reserved-ip
```

The TOE blocks the following protocols by default:

- IPv4
  - Protocol 2
  - Protocol 47
- ICMPv4
  - Code 134
- IPv6
  - Protocol 61
  - Protocol 93
  - Protocol 97
  - Protocol 135
  - Protocol 140

To ensure logging is captured, follow the guidance in Section 2.5.1.4 below.

2.5.1.4 FFW_RUL_EXT.1.7

The Mobility Controller should be configured with a default Access Control List to ensure that traffic identified under FFW_RUL_EXT.1.7 is dropped. To ensure logging of traffic, the following rule should be applied as the last rule of an ACL to drop and log all unwanted traffic:

```
(config-sess-ACL)#any any any deny log
```

All rules should contain 'log' as shown above to ensure all traffic is properly captured. Below is additional information on configuration of access controls for the traffic sent through the TOE:

1. The firewall will automatically drop invalid fragments. If logging of these packet drops is needed, configure "`firewall log-ip-error`" and "`ipv6 firewall log-ip-error`".
2. ArubaOS does not automatically determine which packets should be allowed through an interface. Configure a firewall rule with a source containing the network's address, and apply it to the inbound interface.
3. ArubaOS, because it may operate as a router, does not automatically determine which source addresses are acceptable to pass through an interface. Configure firewall rules appropriately to determine which source addresses are accepted through an interface.
4. Define a firewall rule to reject traffic with a source of a local broadcast address. This rule is useful only for local subnets, since the mobility controller has no knowledge of the broadcast address for remote networks.
5. Define a firewall rule to reject traffic with a source address that falls within the multicast range of 224.0.0.0 through 239.255.255.255. This can be done using the following rule:

   ```
   network <IP address> <Subnet> any any deny log
   ipv6 network <IPv6 address> any any deny log
   ```

6. Define a firewall rule to reject traffic with a source address that is defined as a loopback address. This can be done using the following rule:

   ```
   network <IP address> <Subnet> any any deny log
   ```

7. Define a firewall rule to reject traffic with a source address that is defined as a link-local address. This can be done using the following rule:

   ```
   ipv6 network <IPv6 address> any any deny log
   ```

   ```
   ipv6 any network <IPv6 address> any deny log
   ```

   Note: This will prevent other devices on the same subnet from communicating with the mobility controller through link-local addressing.

8. To configure the firewall to reject traffic that is using reserved IPv4 address space, configure the following:

   ```
   firewall deny-reserved-ip
   ```

9. To configure the firewall to reject traffic that is using reserved IPv6 address space, configure the following:

   ```
   ipv6 firewall deny-reserved-ip
   ```

10. Please note that for each internal interface, external network addresses should be configured to be blocked from the internal network interface. For each external network interface, the internal network addresses should be blocked from communicating with the interface. This can be done by explicitly permitting communication between internal network subnets and applying a deny rule on each external network interface for communication to an internal network address (an example is shown below):

    ```
    Internal Rule:

    ipv6 network 2001:192:168:144::/112 2001:192:168:124::/112 any
    permit

    ipv6 network 2001:192:168:144::/112 any any deny

    External Interface:

    ipv6 network any 2001:192:168:144::/112 any deny
    ```

2.5.1.5 FFW_RUL_EXT.1.8

The TOE access control lists function in a hierarchical structure. If a rule is applied at the beginning of the ACL, it will take priority over any rule following it. For instance, if an access rule denies a specific IP address and a later rule permits a subnet that contains the specific host, the initial rule denying that specific IP will be applied and traffic from that IP address will be dropped.

Note: If a rule is applied permitting or denying traffic, applying the inverse of this rule will overwrite the pre-existing rule. The TOE will not allow inverse rules to be applied. Additional information for access rule lists can be found within the Aruba AOS 8.6 CLI Reference Guide.

2.5.1.6 FFW_RUL_EXT.1.9

An access control list must be applied to all in-use interfaces in the evaluated configuration. If traffic is sent to an interface and no rule within the ACL applied to that interface matches the packet in-transit, the packet will be dropped.

To ensure logging of traffic, the following rule should be applied as the last rule of an ACL to drop and log all unwanted traffic:

```
(config-sess-ACL)#any any any deny log
```

All unsolicited messages are dropped by default. This can be tracked within “authmgr” warning logs.

2.5.1.7 FFW_RUL_EXT.1.10

By default, TCP sequence numbers are ignored. The following commands can be used to ensure TCP sequencing is properly enforced:

```
firewall enforce-tcp-handshake
```

The command ‘enforce-tcp-handshake’ prevents data from passing between two clients until the three-way TCP handshake has been performed, at a upper limit of 8 half-open TCP connections.

```
firewall enforce-tcp-sequence
```

The command ‘enforce-tcp-sequence’ enforces the TCP sequence numbers for all packets.

When applied, the TOE will monitor traffic sent through the TOE and drop half-open TCP connections.To monitor if traffic has been dropped, an administrator can enter the following command:

```
Show datapath frame
```

This will identify a counter next to the entry “Drop due to max half syns.”

2.5.1.8 Default Port Restrictions

ICMPv4 Code 134 is an unsolicited router advertisement which is discarded/dropped by the controller. All other traffic is handled based upon access control lists configured on the TOE.

2.6 Identification and Authentication (FIA)

2.6.1 FIA_802X_EXT.1

The configuration of 802.1X can be performed by following the guidance information found within the ArubaOS 8.6 CLI Reference Guide on Page 20 (“aaa authentication dot1x”). The commands are provided below for reference.

```
aaa authentication dot1x {<profile>|countermeasures}
     ca-cert <certificate>
     cert-cn-lookup
     clear
     clone <profile>
     delete-keycache
     eapol-logoff
     enforce-suite-b-128
     enforce-suite-b-192
     framed-mtu <mtu>
     heldstate-bypass-counter <number>
     ignore-eap-id-match
     ignore-eapolstart-afterauthentication
     key-cache clear
     machine-authentication blacklist-on-failure|{cache-timeout
     <hours>}|enable|
     {machine-default-role <role>}|{user-default-role <role>}
     max-authentication-failures <number>
     max-requests <number>
     multicast-keyrotation
     no ...
```

```
opp-key-caching
reauth-max <number>
reauth-server-termination-action
reauthentication
reload-cert
server {server-retry <number>|server-retry-period <seconds>}
server-cert <certificate>
termination {eap-type <type>}|enable|enable-token-caching|{inner-
eap-type (eap- gtc|eapmschapv2)}|{
token-caching-period <hours>}
timer {idrequest_period <seconds>}|{keycache-tmout <kc-
tmout>}|{mkey-rotation-period
<seconds>}|{quiet-period <seconds>}|{reauth-period <seconds>}|{ukey-
rotation-period
<seconds>}|{wpa- groupkey-delay <seconds>}|{wpa-key-period
<milliseconds>}|wpa2-key-delay
<milliseconds>
tls-guest-access
tls-guest-role <role>
unicast-keyrotation
use-session-key
use-static-key
validate-pmkid
wep-key-retries <number>
wep-key-size {40|128}
wpa-fast-handover
wpa-key-retries <number>
xSec-mtu <mtu>
```

2.6.2 FIA_AFL.1

All configuration related to administrative login is configured using "aaa password-policy mgmt". Note that if the remote authentication server locks out a user, the local account with the same name will not be marked as locked. However, the local user will not be able to authenticate when configured authenticate against the remote authentication server. To configure failed authentication lockout that will lock an administrative account for five minutes, when five failed login attempts occur in a three minute period, use the following commands:

```
(config) #aaa password-policy mgmt
(Mgmt Password Policy) #password-lock-out 5
(Mgmt Password Policy) #password-lock-out-time 5
(Mgmt Password Policy) #enable
```

2.6.3 FIA_AFL.1 (WLAN)

Refer to Section **2.10 FTA_TSE.1 (VPNGW/WLAN)** for instructions on how to configure blacklisting of clients after failed authentication attempts.

2.6.4 FIA_PMG_EXT.1

Administrative password policies are configured under “aaa password-policy mgmt”.

```
(config) #aaa password-policy mgmt
(Mgmt Password Policy) #password-min-length 8
(Mgmt Password Policy) #password-min-lowercase-characters 1
(Mgmt Password Policy) #password-min-uppercase-characters 1
(Mgmt Password Policy) #password-min-special-characters 1
(Mgmt Password Policy) #password-min-digit 1
(Mgmt Password Policy) #enable
```

The following special characters can be used when configuring passwords: !, @, #, $, %, ^, &, *, <, >, {, }, [,], :, ., comma, |, +, ~, `

Once configured, the TOE only permits the use of strong passwords.

2.6.5 FIA_PSK_EXT.1 (VPNGW)

ArubaOS supports IKE pre-shared keys, when certificates are not used for authentication. To use these, create an IKE policy that uses pre-shared keys, then enter the pre-shared key mapped by client IP address. If the client address is unknown, use a key mapped to 0.0.0.0 to cover the "default" IP address.

Both text-based and hex-based pre-shared keys are supported. Use the corresponding command:

```
(config) #crypto isakmp policy 101
(config-isakmp)# authentication pre-share
(config-isakmp)# exit
```

To configure the key, pick one of the following options:

```
 (config) #crypto-local isakmp key DEADBEEF01010202abc!@# address 0.0.0.0
netmask 0.0.0.0
```

When configuring the pre-shared key, the administrator must ensure that the PSK is at least 22 characters, contains at least one uppercase character, one lowercase character, one special character, and one digit. Allowable special characters are: '!', '@', '#', '$', '%', '^', '&', '*', '(', and ')'.

If the PSK is configured as a bit-based key, the 'key-hex' field should be used instead.

```
(config) #crypto-local isakmp key-hex DEADBEEF01010202ABA010 address
0.0.0.0 netmask 0.0.0.0
```

2.6.6 FIA_PSK_EXT.1 (WLAN)

Configuration of the pre-shared key for 802.1X can be performed by following the guidance on Page 2656 of the ArubaOS 8.6 CLI Reference Guide ("wlan ssid-profile"). The commands are provided below for reference.

```
Wlan ssid-profile <profile-name>

wpa2-psk-aes
```

To configure a text-based PSK or bit-based PSK, the administrator should use one of the following two options after the command above:

```
wpa-hexkey <psk>

wpa-passphrase <string>

The same character and length restrictions as shown under Section 2.6.4
should be followed by the administrator.
```

2.6.7 FIA_ UAU.6

No configuration required.

2.6.8 FIA_UAU.7

No configuration required.

2.6.9 FIA_UAU_EXT.2

Configure administrative users with "mgmt-user". For example, to add a read-only user with the username "ops", use the following command:

```
(config) # mgmt-user ops read-only

Password:***************

Re-Type password:***************
```

2.6.10 FIA_UIA_EXT.1

A warning banner may be configured as follows. Ensure that no line is longer than 255 characters.

```
#configure terminal

Enter Configuration commands, one per line. End with CNTL/Z
```

```
(config) #banner motd =
Enter TEXT message [maximum of 4095 characters].
Each line in the banner message should not exceed 255 characters.
End with the character '='.


You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only. By using this IS (which includes
any device attached to this IS), you consent to the following conditions:
-The USG routinely intercepts and monitors communications on this IS for
purposes including, but not limited to, penetration testing, COMSEC
monitoring, network operations and defense, personnel misconduct (PM),
law enforcement (LE), and counterintelligence (CI) investigations.
-At any time, the USG may inspect and seize data stored on this IS.
-Communications using, or data stored on, this IS are not private, are
subject to routine monitoring, interception, and search, and may be
disclosed or used for any USG-authorized purpose.
-This IS includes security measures (e.g., authentication and access
controls) to protect USG interests -- not for your personal benefit or
privacy.
-Notwithstanding the above, using this IS does not constitute consent to
PM, LE or CI investigative searching or monitoring of the content of
privileged communications, or work product, related to personal
representation or services by attorneys, psychotherapists, or clergy, and
their assistants. Such communications and work product are private and
confidential. See User Agreement for details
=
```

The TOE permits authentication by an administrator through SSH or Web UI over TLS or via a serial console (direct) connection to the CLI. Authentication is permitted through username/password and public key authentication (for SSH) via local authentication or by a remote authentication server (RADIUS/TACACS+). Authentication to the TOE through a wireless connection does not permit administration by default.

No user can perform any actions prior to successful authentication to the TOE outside of viewing the warning banner as defined under FTA_TAB.1 and above.

2.6.11 FIA_X509_EXT.1

Certificate Signing Requests (CSRs) may be generated by the controller. This process is described in the ArubaOS User Guide. Best practice is to generate the CSR on the controller, then load the resulting certificate after issuance by the CA. This protects the private key from

disclosure. If the private key is generated externally, the controller can also accept a certificate/key combination in the form of a PKCS#12 file.

ArubaOS supports certificate revocation checking using either an installed CRL, or using OCSP. CRLs support a maximum of 512 entries, and the controller does not support automatic retrieval of new CRLs through a distribution point. OCSP is the recommended method of revocation checking.

When a root CA or intermediate CA certificate is loaded on the controller, an automatic Revocation Check Point (RCP) section is created in the configuration file. These may be shown using "show crypto-local pki rcp". For each RCP, the revocation check method may be configured, and may be set to none, crl, or ocsp. If set for CRL, a CRL filename must be specified. This corresponds to a CRL file that has been uploaded to the controller using one of the file copy methods. If OCSP has been specified, then an OCSP responder URL and OCSP responder certificate must be specified. In addition, an administrator may configure the behavior if an OCSP responder is unreachable - treat the certificate as valid or treat the certificate as revoked.

For the purpose of verifying OCSP responses, ArubaOS requires that the responses be signed, and requires that the nonce extension be supported by the OCSP responder. Signed responses are verified using the "OCSP Responder" certificate. Two methods are supported: direct trust and delegated trust. For direct trust, the signing certificate of the OCSP responder must be loaded onto the controller through the WebUI Certificate Management section, and its name configured in the relevant RCP. When used, the controller makes a direct comparison between the signer certificate included in the OCSP response, and the OCSP responder certificate that was loaded - they must be exactly the same certificate. Direct Trust is cumbersome in environments where the OCSP responder certificate expires frequently. An alternative is Delegated Trust. In this method, the "OCSP Responder" type certificate must still be loaded into the controller, in the same way just described. However, the certificate should be the *Issuing CA certificate* for the CA that issues a signing certificate to the OCSP responder. When this type of configuration is performed, ArubaOS will examine the certificate in the OCSP response, then chain one level up to see if that certificate was issued by the CA configured in the RCP. Note, OCSP does not support multiple levels of certificate chaining for delegated trust, so the direct issuer of the OCSP responder's signing certificate must be configured In the RCP. If multiple levels of certificate checking will be performed (e.g. for a peer's IPsec certificate and one level up to an Intermediate CA) then a separate RCP must be configured for each, along with an appropriate OCSP responder certificate.

The following configuration demonstrates revocation checking against a three-level PKI. Delegated trust is in use for validating OCSP responses. The OCSP responder is the same for both levels, and the OCSP responder's signing certificate is issued directly by the root CA, as shown in the example below.

```
crypto-local pki TrustedCA intermediate-ca ecdsa-intermediate.cer
crypto-local pki TrustedCA root-ca ecdsa-root-ca.cer
crypto-local pki OCSPResponderCert ocsp-root ecdsa-root-ca.cer
crypto-local pki rcp "intermediate-ca"
```

```
  ocsp-url "http://ocsp.domain.com/ocsp"
  ocsp-responder-cert "ocsp-root"
  revocation-check ocsp
!
crypto-local pki rcp "root-ca"
  ocsp-url "http://ocsp.domain.com/ocsp"
  ocsp-responder-cert "ocsp-root"
  revocation-check ocsp
```

For site-to-site IPsec tunnels, the peer certificate DN is configured in the ipsec-map, as shown in the example below:

```
crypto-local ipsec-map 10.10.20.1 100
     peer-cert-dn
"/C=US/ST=CA/L=Sunnyvale/O=ArubaNetworks/OU=TestLab/CN=192.168.2.1/emailA
ddress=nobody@arubanetworks.com"
```

Note: It may be difficult to determine the exact DN to configure, simply by looking at a peer's certificate. Attempting to establish an IPsec tunnel while examining the log file (possibly after enabling "logging level debugging security") will generally show the exact DN string that must be configured, once it is received from the peer.

For client VPN: ArubaOS will extract the User Principal Name field from the client certificate, and will pass it through an authentication/authorization process when this functionality has been enabled. Configuring authentication servers is described in the ArubaOS User Guide. VIA clients will be authenticated according to configuration found under "`aaa authentication via auth-profile`". Third-party VPN clients will be authenticated according to configuration found under "`aaa authentication vpn`". Both types of profiles are configured in a similar way. The following configuration allows the controller to perform authentication for VIA clients against a RADIUS server. After a client certificate has been validated, including revocation checking, the controller will pass the User Principal Name to a configured RADIUS server using an "authorize-only" transaction.

```
(config) #aaa authentication via auth-profile VIA_CERT_AUTH
(VIA Authentication Profile "VIA_CERT_AUTH") #cert-cn-lookup
(VIA Authentication Profile "VIA_CERT_AUTH") #server-group CPPM_CLUSTER
```

If authentication is not desired, set "cert-cn-lookup" to disabled.

To configure the behavior in the event an OCSP responder cannot be reached, use the "server-unreachable" keyword under the RCP configuration. As an example, to permit peers to connect even when an OCSP responder cannot be reached, perform the following configuration:

```
(config) #crypto-local pki rcp intermediate-ca
(RCP-intermediate-ca) #server-unreachable allow-cert
```

To configure delegated trust on the TOE for OCSP verification of each CA, ensure that CA certificates are uploaded as bundles. The following procedures should be followed:

1. Create a full CA bundle, from the leaf's issuing CA to the rootca.
2. Upload that as a trustedCA bundle.
3. Upload the same CA bundle as an OCSP responder cert.
4. Click on the RCP for the full CA bundle.
5. Ensure that the correct OCSP responder cert is selected.
6. Input the OCSP responder URL for the top most intermediary CA in the bundle.
7. For the next CA bundle, remove the top most intermediary CA and save it as a new bundle.
8. Repeat above steps until you're left with just the rootca.

2.6.12 FIA_X509_EXT.3

An example of the commands that can be used to generate a certificate sign request are provided below:

```
crypto pki
csr rsa
key_len 2048
common_name <common_val>
country <country>
organization <org>
unit <org_unit>
```

To export the request, you may show the CSR with the follow command:

```
Show crypto pki csr
```

Before creating a CSR, the administrator must ensure that the CN, country, O, and OU have been set as identified above.

2.6.13 FIA_X509_EXT.4

Removed by TD0329

2.7 Security Management (FMT)

2.7.1 FMT_MOF.1/ManualUpdate

See FPT_TUD_EXT.1 for information. No configuration is required to restrict updates to administrator role.

2.7.2 FMT_MOF.1/Functions

An administrator with the management role of “root” has full privileges to modify, add, and delete configuration settings on the TOE. The “root” role maps to the Security Administrator role.

2.7.3 FMT_MOF.1/Services

An administrator with the management role of “root” has full privileges to enable or disable services on the TOE. The “root” role maps to the Security Administrator role.

2.7.4 FMT_MTD.1/CoreData

An administrator with the management role of “root” has full privileges to modify, add, and delete configuration and user accounts. The “root” role maps to the Security Administrator role.

2.7.5 FMT_MTD.1/CryptoKeys

An administrator with the management role of “root” has full privileges to modify, add, and delete configuration and user accounts. The “root” role maps to the Security Administrator role.

2.7.6 FMT_SMF.1

No additional configuration required. Please reference the Aruba OS CLI Reference Guide and Aruba OS User Guide for a full list of configuration instructions through the CLI and Web GUI.

2.7.7 FMT_SMR.1

No additional configuration required.

2.7.8 FMT_SMR.2

No additional configuration required.

2.8 Packet Filtering (FPF)

2.8.1 FPF_RUL_EXT.1

For information specific to each protocol, ordering of rules, and behavior when no matching rule is found, please see Section 2.4.1 (FFW_RUL_EXT.1).

The EP lists several requirements to test packet filtering behavior. All configuration for these tests is performed using the "ip access-list session" command. The ArubaOS User Guide contains extensive documentation on how firewall rules are configured. To summarize:

For a wired interface: Configure a single ACL and apply it to a physical interface or VLAN interface. For example, to block ICMP "ping" on an Ethernet port:

```
(config) #ip access-list session block-icmp
(config-sess-block-icmp)#any any icmp echo deny log
```

```
(config-sess-block-icmp)#exit
(config) #interface gigabitethernet 1/2
(config-if)#ip access-group block-icmp session
```

Use the "log" keyword In the firewall rule to ensure that hits against this rule appear in the audit log.

For a user (Wi-Fi or VPN): Any user session that appears in "show user-table" has a role and firewall policy associated with it, as long as the PEF-NG or PEF-V license is installed. Configuration of user roles is described extensively in the ArubaOS User Guide. Mapping a user into a particular role is normally performed at the time of authentication, through one of the "aaa" policies, and may be based on a default role or may be based on attributes returned from an authentication server. Once a user session is placed into a role, firewall policies (one or more) are applied. Firewall policies contain one or more firewall rules. The following is an example of a role/policy configuration:

```
(config) #ip access-list session filter_http
(config-sess-filter_http)#user network 172.16.1.0 255.255.255.0 svc-http
permit
(config-sess-filter_http)#user network 172.16.2.0 255.255.255.0 svc-http
permit
(config-sess-filter_http)#user any svc-http deny log
(config-sess-filter_http)#exit
(config) #ip access-list session filter_smtp
(config-sess-filter_smtp)#user any svc-smtp deny log
(config-sess-filter_smtp)#exit
(config) #user-role example_role
(config-role) #session-acl filter_http
(config-role) #session-acl filter_smtp
(config-role) #session-acl allowall
```

To see the resulting policy, issue the command "`show rights example_role`".

2.9 Protection of the TSF (FPT)

2.9.1 FPT_APW_EXT.1

No additional configuration required.

2.9.2 FPT_FLS.1 (VPNGW/WLAN)

No configuration required.

2.9.3 FPT_SKP_EXT.1

No additional configuration required.

2.9.4 FPT_STM_EXT.1

Mobility controllers require clock synchronization using NTPv4 in order to generate reliable timestamps. To specify an NTP server:

```
(config) # ntp server <IP address>
(config) # ntp server <IP address>
(config) # ntp server <IP address>
```

Additionally, an administrator can configure a manual system time with the following command:

```
(config) # clock set <year> <month> <day> <HH:MM:SS>
```

The TOE supports configuration of 3 NTP time sources. Multiple time servers can be configured with the use of the 'ntp server' command shown above.

If a remote NTP server is used, the administrator must ensure that the connection is protected via IPsec. The TOE, by default, does not accept broadcast and multicast NTP packets.

2.9.5 FPT_TST_EXT.1

No configuration required.

If a self-test fails, the TOE will immediately halt operation and enter an error state thereby preventing potentially insecure operations (i.e., maintaining a secure state). The controller will reboot after a self-test failure. During reboot, memory is re-initialized, which wipes all keys and user data. If a self-test failure continues to occur, the controller will continue to reboot repeatedly and will require return to manufacturer. The error output of a failed self-test will appear as follows: "FIPS Aruba Cryptographic asymmetric key KAT failure, main: FIPS_powerupSelfTest failed." If a firmware image fails its integrity check, the TOE will load the previous image (if one is present). An error will be output during boot in this instance stating that the firmware validation failed.

If the issue continues, the administrator should contact support at http://support.arubanetworks.com.

2.9.6 FPT_TST_EXT.3

No configuration required.

2.9.7 FPT_TUD_EXT.1

Use the command "show version" and "show image version" to view the firmware version.

Use the "copy" command to download new firmware images from an FTP or TFTP server and to select the system partition to which the image file is copied. Note that the administrator should first ensure that the `boot system partition <partition_id>` command is correctly set to

specify the system partition number that the controller should use during the next reboot. The following CLI commands transfer the ArubaOS image file:

```
copy tftp:<tftphost><filename>system:partition[0|1]}
copy ftp:<ftphost><user><filename>system:partition{0|1}
```

An option is provided to reboot the device with the transferred image file.

From the WebUI, navigate to Maintenance>Software Management>Upgrade page to upload an ArubaOS image from a local filesystem. Specify the system partition to which the image file is copied and choose whether the device should be rebooted when the image file is transferred. Click Upgrade.

ArubaOS images are integrity-protected through three methods:

1. When downloading a firmware image from http://support.arubanetworks.com, a file may be found in the download directory that contains SHA256 hashes of each file. This hash may be checked manually after downloading an image.
2. ArubaOS images are digitally signed using RSA 2048-bit signature validation. The mobility controller will check the digital signature immediately after downloading a new firmware image, and will refuse to install an image whose digital signature does not match.
3. Mobility controllers also check the digital signature of an ArubaOS image when booting. The controller will refuse to boot a corrupted ArubaOS image file.

If digital signature verification fails, the TOE will enter into an error state. The TOE's error state will allow direct console access only, where an administrator can change to a new file partition or TFTP a new image and re-boot.

2.10 TOE Access (FTA)

2.10.1 FTA_SSL.3

For both local and remote administrative sessions, an idle timeout may be set to disconnect idle sessions. The timeout value can be set from 5- 60 minutes, or 1- 3600 seconds. To disable, set to 0. The default value is 15 minutes. To configure the timer value, use the following command:

```
(config) #loginsession timeout <minutes>
```

The idle timeout value can be configured in the Web UI by navigating to Configuration>System>Admin>Admin Authentication Options and setting the 'Idle session timeout' value.

2.10.2 FTA_SSL.4

No configuration required. An administrator can terminate their own session by exiting the SSH session or logging out from the Web UI session. To enforce a timeout interval, please see Section 2.10.1 above.

2.10.3 FTA_SSL_EXT.1

For both local and remote administrative sessions, an idle timeout may be set to disconnect idle sessions. The timeout value can be set from 5- 60 minutes, or 1- 3600 seconds. To disable, set to 0. The default value is 15 minutes. To configure the timer value, use the following command:

```
(config) #loginsession timeout <minutes>
```

The idle timeout value can be configured in the Web UI by navigating to Configuration>System>Admin>Admin Authentication Options and setting the 'Idle session timeout' value.

2.10.4 FTA_TAB.1

See FIA_UIA_EXT.1.1 above for a description of how to configure a notice and consent banner message.

2.10.5 FTA_TSE.1 (VPNGW/WLAN)

The TOE can deny establishment of a VPN client session and a wireless client session as follows:

- VPN client sessions can be restricted based on location (IP address), time, day, and blacklist state.
- Wireless client sessions can be restricted based on TOE interface, time, day and blacklist state.

To configure blacklisting of clients after failed authentication attempts, the following command must be set:

```
aaa authentication vpn <profile-name>
max-authentication-failures <number>
```

Configuring the above field sets the maximum number of authentication failures before the user is blacklisted. The supported range is 1-10 failures.

A client will be blacklisted until an administrator configured time period has expired. To configure the blacklist time period, the following command can be used:

```
ap ap-blacklist-time <time in seconds>
```

The default blacklist time period is 3600 seconds. The blacklist time can be viewed via the following command:

```
show ap blacklist-time
```

To blacklist a user via address, the following command can be used:

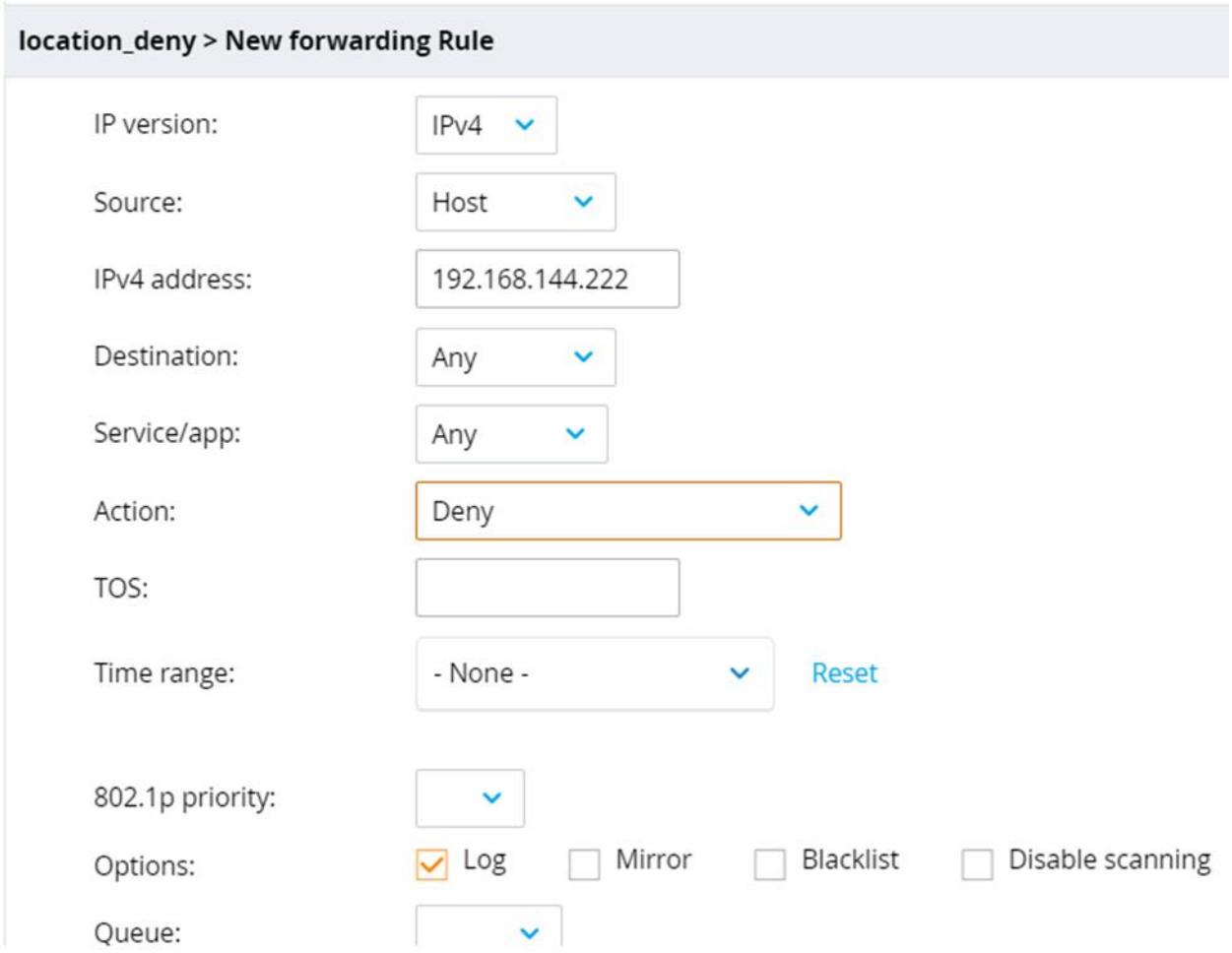
```
stm add-blacklist-client <mac address>
```

To remove a user from blacklisting, the following command can be used:

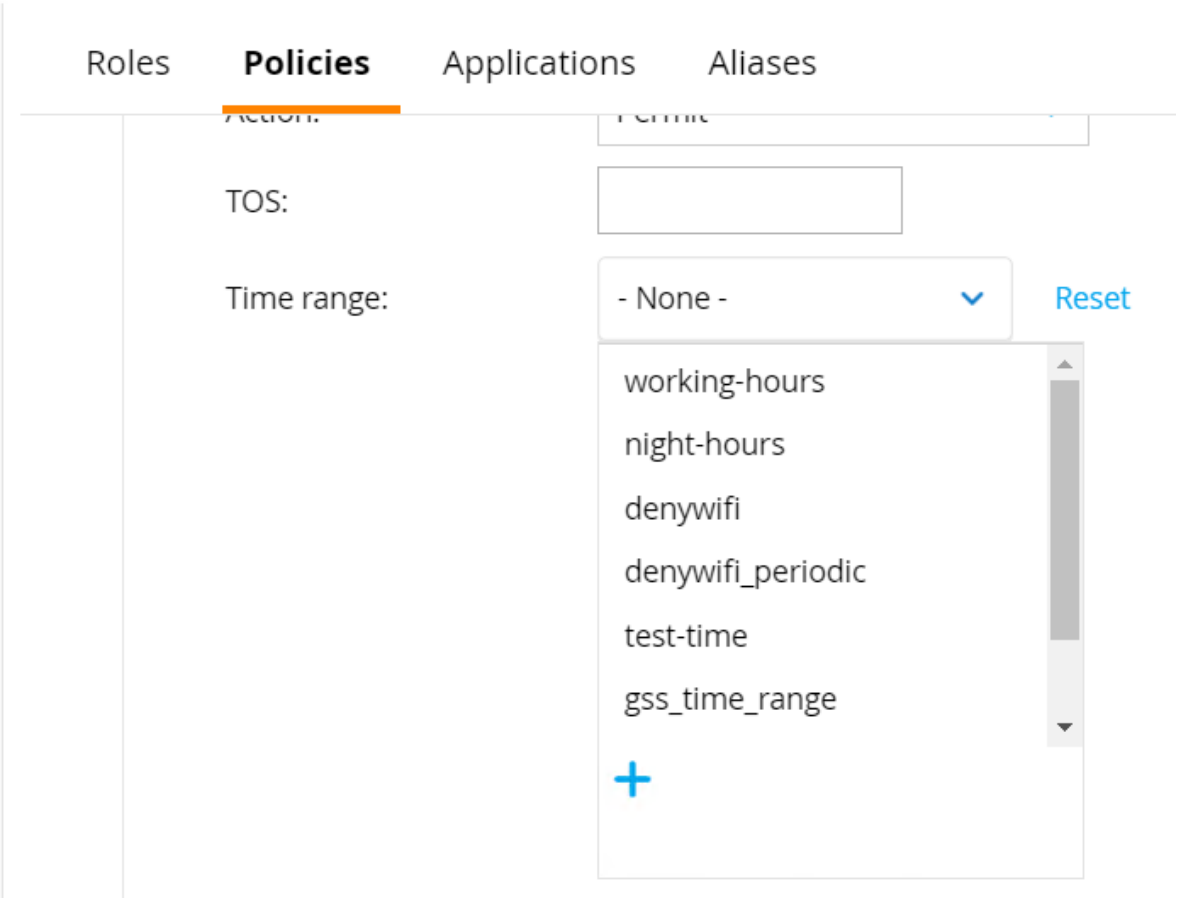
```
stm remove-blacklist-client <mac address>
```

To configure VPN client restrictions based on location, time and day, the administrator can navigate to the Web UI and go to Configuration > Roles & Policies > Policies to add a new policy

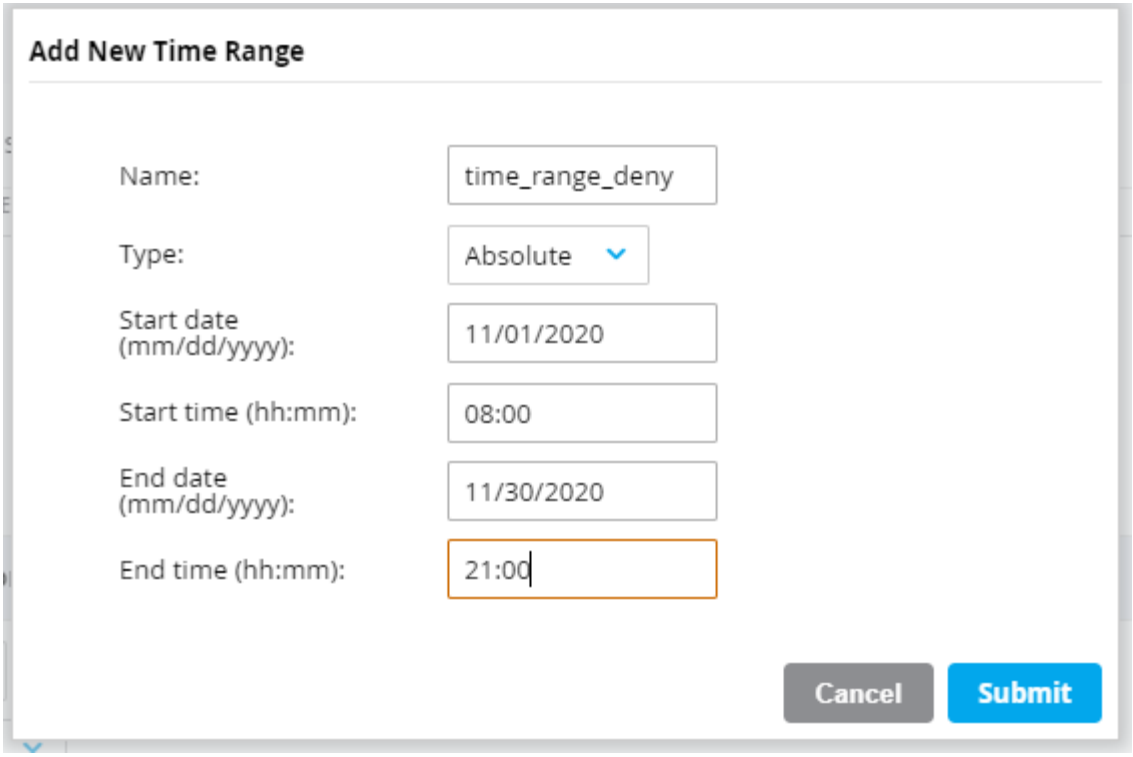
and create a firewall rule to deny clients based on location (IP address) and time range as shown in the screenshots below:



To configure the time-range, click the drop down menu in the Time Range field shown above. A list of time ranges that were previously defined will be displayed.



- Click the '+' button to add a new time range.



- Enter a name for the new time range
- Select the type (Periodic or Absolute)
- Enter the Start time and End time.
- Click Submit.

To configure Wireless client restrictions based on time and day, the administrator should use the following command:

```
time-range
absolute<name>[end<mm/dd/yyyy><hh:mm>][start<mm/dd/yyyy><hh:mm>]
no
periodic <name>
Daily<hh:mm>to<hh:mm>
Friday<hh:mm>to<hh:mm>
Monday<hh:mm>to<hh:mm>
Saturday<hh:mm>to<hh:mm>
Sunday<hh:mm>to<hh:mm>
Thursday<hh:mm>to<hh:mm>
```

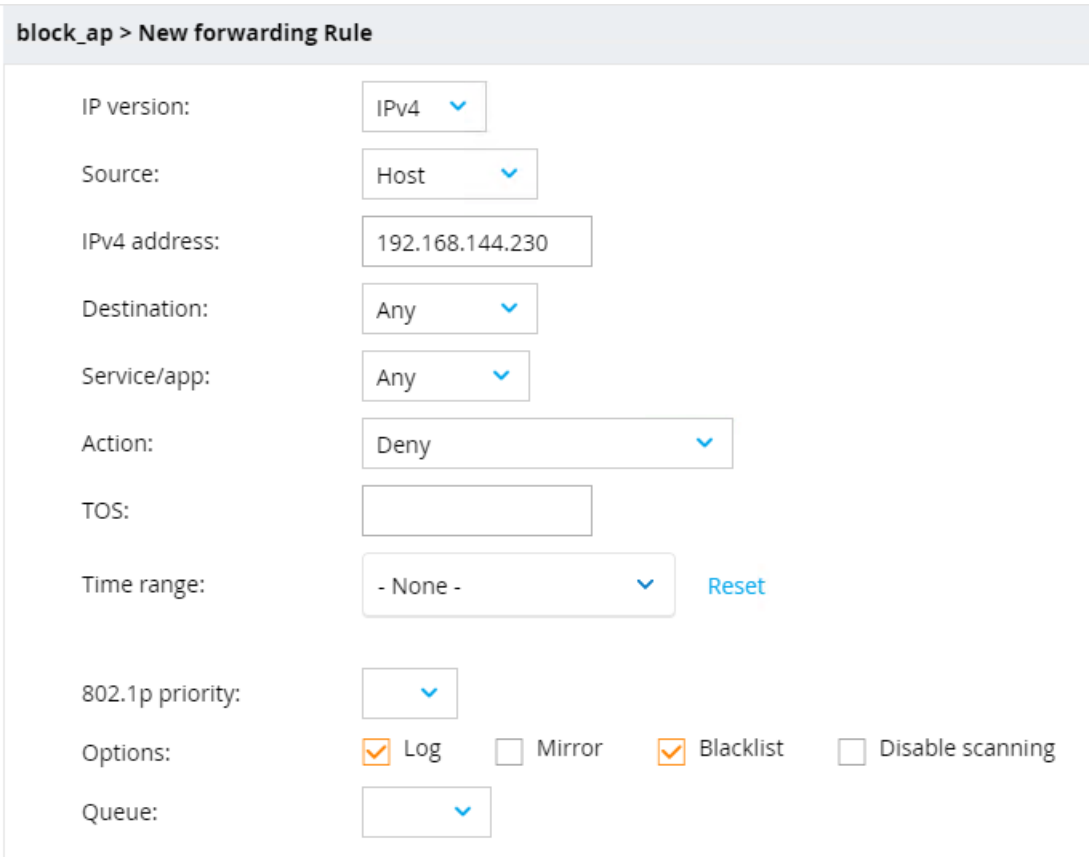
```
Tuesday<hh:mm>to<hh:mm>
Wednesday<hh:mm>to<hh:mm>
Weekday<hh:mm>to<hh:mm>
Weekend<hh:mm>to<hh:mm>
```

Once configured, the administrator should apply the time-range to each wlan virtual-AP profile.

To configure Wireless client restrictions based on location (MAC address), the administrator should use the following command:

```
stm add-blacklist-client <macaddr>
```

When an Access Point (AP) is connected to the TOE, it will have its own IP address. To configure wireless client restrictions based on TOE interface, the administrator can navigate to the Web UI and go to Configuration > Roles & Policies > Policies to add a new policy and create a firewall rule to block all traffic from the AP as shown below.



2.10.6 FTA_VCM_EXT.1

IP address pools assigned to VPN clients are, by default, configured through an address pool. Clients will be assigned the next available address from the pool. To configure the address pool, use the following command:

```
(config) #ip local pool "pool1" <IP Address pool start> <IP address Pool start>
```

With no further configuration, VPN clients will obtain their address from this pool, and any other pool that is configured. If desired, user-roles may also reference IP (L2TP) pools. When this is done, users matching a particular user-role will be assigned an address only from the referenced address pool.

VPN client IP addresses may also be assigned through the authentication process, either by looking them up in the internal user database or through a RADIUS server sending a Framed-IP-Address attribute during an authorization response.

2.11 Trusted Path/Channels (FTP)

2.11.1 FTP_ITC.1

ArubaOS supports IPsec as the inter-TSF trusted channel. This channel is to be used between a Mobility Controller and a) a syslog server, b) a RADIUS or TACACS server, c) an 802.1x authentication server d) an NTP server, e) remote VPN Gateways/Peers and f)WLAN clients. For WLAN clients operating in a Robust Security Network (RSN), IEEE 802.11-2012 (WPA2) and IEEE 802.1X are used to provide a trusted channel between the TOE and wireless clients.

When the Mobility Controller acts as a Wireless LAN controller, IPsec is also used between multiple controllers and between controllers and APs.

If for any reason a connection is unintentionally broken, the TOE will re-establish the connection once connectivity is restored. If the timeout period has expired, re-authentication/re-negotiation is required.

2.11.2 FTP_TRP.1/Admin

Communication between a Mobility Controller and a remote administrator may be protected by TLS/HTTPS (when using the Web-based interface) or SSH (when using the command-line interface). All remote administration must take place over one of these interfaces.

3 Reference Documents

The Guidance documentation for ArubaOS can be found in its entirety at the link below:

https://asp.arubanetworks.com/downloads;pageIndex=1;search=8.6;fileTypes=DOCUMENT;products=Aruba%20Mobility%20Controllers%20%28AOS%29