**Aerohive Firewall Test Plan & Test Case**

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Description |
| **0.1** | **8/07/2009** | **Xin Sheng** | **Initial version** |
| **0.2** | **8/21/2009** | **Xin Sheng** | **Add IP-policy cases, and modify by Ligang’s comments** |
| **0.3** | **9/01/2009** | **Xin Sheng** | **Modify cases by Ligang’s comments** |
| **0.4** | **10/14/2009** | **Xin Sheng** | **Add cases which check access ethx** |
| **0.5** | **11/09/2010** | **Xin Sheng** | **Add cases about session syn** |
| **0.6** | **1/24/2011** | **Xin Sheng** | **Add cases 8.11 about support hostname** |
| **0.7** | **1/26/2011** | **Xin Sheng** | **Add and modify cases 8.11 by the reviewed comment** |
| **0.8** | **8/25/2011** | **Wei Cai** | **Modify accept cases to automation form** |
| **0.9** | **8/25/2011** | **Wei Cai** | **Add priority and automation flag** |
| **1.0** | **9/14/2011** | **Wei Cai** | **Add 8.2 priority and automation flag** |
| **1.1** | **11/11/2011** | **Wei Cai** | **Update case 11.2&5** |
| **1.2** | **07/18/2011** | **Wei Cai** | **Update case and priority** |

Version 0.7

1. add step in case 8.11.3.2 to check “the overwirte id's order”

2. add case 8.11.3.3 to check “while moving id's order”

3. add case 8.11.3.4, “compability with configure tv's policy”

4. add step in cases 8.11.5.1/8.11.5.2 to check “set ip-policy rule to FE after configuring correct dns server”

5. add step in cases 8.11.6.1 to check “dns response timeout”

6. add case 8.11.2.2 to check “make sure resolve hostname after ap gets ip”

7. add step in cases 8.11.4.3 to check “check the internal id can be reuse”

8. add case 8.11.6.2 to do “create/delete ip-policy continuously” stress test

9. add case 8.11.6.3 to do “change the order of rule continuously” stress test

10. add case 8.11.6.4 to do “reboot ap with full configuration” test

Table of Contents

[1. Introduction 4](#_Toc302996157)

[2. Aerohive solution 4](#_Toc302996158)

[3. Test Topologies 4](#_Toc302996159)

[4. Test Points and Strategies 5](#_Toc302996160)

[5. Software Tools Requirements 6](#_Toc302996161)

[6 Hardware Requirements 6](#_Toc302996162)

[7. Mac-policy TestCase 6](#_Toc302996163)

[7.1 Single “from || to” policy test 6](#_Toc302996164)

[7.2 “From & To” policy simultaneous test 23](#_Toc302996165)

[7.3 Order of rules test 32](#_Toc302996166)

[7.4 Regular session test 37](#_Toc302996167)

[7.5 Session syn test 48](#_Toc302996168)

[7.6 Group Mac-Address test 49](#_Toc302996169)

[7.7 Change policy or binding while traffic is on-going 51](#_Toc302996170)

[7.8 Performance/Stress test 84](#_Toc302996171)

[8. IP-policy Testcase 93](#_Toc302996172)

[8.1 Single “from || to” policy test 93](#_Toc302996173)

[8.2 “From & To” policy simultaneous test 111](#_Toc302996174)

[8.3 Order of rules test 119](#_Toc302996175)

[8.4 Regular session test 124](#_Toc302996176)

[8.5 Session syn test 137](#_Toc302996177)

[8.6 Group IP-Address test 141](#_Toc302996178)

[8.7 Change policy or binding while traffic is on-going 143](#_Toc302996179)

[8.8 Fragment test 176](#_Toc302996180)

[8.9 Services test 186](#_Toc302996181)

[8.10 Performance/Stress test 196](#_Toc302996182)

[8.11 Support Hostname test 209](#_Toc302996183)

[8.11.1 Basic function test 210](#_Toc302996184)

[8.11.2 Hostname resolve test 211](#_Toc302996185)

[8.11.3 Compatibility test 212](#_Toc302996186)

[8.11.4 Capability test 216](#_Toc302996187)

[8.11.5 Negative test 220](#_Toc302996188)

[8.11.6 Stress test 224](#_Toc302996189)

# 1. Introduction

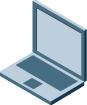
Firewall policy includes L2(Mac-policy) & L3 (IP-policy). Each policy is a rule for how to process the received packets. Policy can be bound to user profiles, not to SSIDs. This will make the usage more flexible. The binding policies will be used for checking the packets received from access interfaces, or sent to the access interfaces (it is called “from-access” and “to-access” respectively) and not used for backhaul interfaces in the current implementation.

# 2. Aerohive solution

Please refer to document AH-Essential-WLAN-Config-Rev-3.2.

# 3. Test Topologies

Topology 1



**Station1**



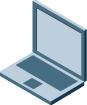
SW

**AP1**



**AP2**

Topology 2



**Station1**

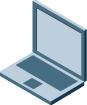


SW

**AP1**



**AP2**



**Station2**

# 4. Test Points and Strategies

* **Mac-policy test**
* **Single “from || to” policy test**
* **“From & To” policy simultaneous test**
* **Order of rules test**
* **Regular session parameters test**
* **Session syn test**
* **Group Mac-Address test**
* **Add/Delete policy, binding/unbinding user-profile while is traffic on-going**
* **Performance/Stress test**
* **IP-policy test**
* **Single “from || to” policy test**
* **“From & To” policy simultaneous test**
* **Order of rules test**
* **Regular session parameters test**
* **Session syn test**
* **Group IP-Address test**
* **Add/Delete policy, binding/unbinding user-profile while is traffic on-going**
* **Fragment test**
* **Services test**
* **Performance/Stress test**

# 5. Software Tools Requirements

# 6 Hardware Requirements

* **PC**
* **2 APs**
* **Server**

# 7. Mac-policy TestCase

## 7.1 Single “from || to” policy test

* Case ID FW\_Mac\_Policy\_Fun\_1

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.1 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config single “from” policy(permit) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop ping gateway of SW 2. Laptop ping Server 3. Laptop ping AP1 4. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop mac addr> action permit”  “user-profile FW security mac-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1-3 | | |
| Expect result | - Laptop ping successfully on step 1), 2) and 3)  - Laptop ping successfully on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.2 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config single “from” policy(deny) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop ping gateway of SW 2. Laptop ping Server 3. Laptop ping AP1 4. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop mac addr> action deny”  “user-profile FW security mac-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1-3 | | |
| Expect result | - Laptop ping successfully on step 1), 2) and 3)  - Laptop ping unsuccessfully on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.3 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Delete a config-single “from” policy(deny/permit) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop ping gateway of SW 2. Laptop ping Server 3. Laptop ping AP1 4. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop mac addr> action [deny/permit]”  “user-profile FW security mac-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Delete the config policy   “no user-profile FW security mac-policy from-access”  “no mac-policy FW id [num]”   1. Repeat step 1-3. | | |
| Expect result | -Laptop ping successfully on step 1), 2) and 3)  -If action is deny, Laptop ping unsuccessfully on step 5),else Laptop ping successfully on step 5)  - Laptop ping successfully on step 6) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.4 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config single “to” policy(permit) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Gateway of SW ping Laptop 2. Server ping Laptop 3. AP1 ping Laptop 4. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop mac addr> action permit”  “user-profile FW security mac-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1-3 | | |
| Expect result | - Devices ping successfully on step 1), 2) and 3)  - Devices ping successfully on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.5 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server | | |
| Description | Config single “to” policy(deny) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Gateway of SW ping Laptop 2. Server ping Laptop 3. AP1 ping Laptop 4. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop mac addr> action deny”  “user-profile FW security mac-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1-3 | | |
| Expect result | - Devices ping successfully on step 1), 2) and 3)  - Devices ping unsuccessfully on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.6 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Delete a config-single “to” policy(deny/permit) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Gateway of SW ping Laptop 2. Server ping Laptop 3. AP1 ping Laptop 4. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop mac addr> action [deny/permit]”  “user-profile FW security mac-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Delete the config policy   “no user-profile FW security mac-policy to-access”  “no mac-policy FW id [num]”   1. Repeat step 1-3. | | |
| Expect result | - Devices ping successfully on step 1), 2) and 3)  - If action is deny, Devices ping unsuccessfully on step 5),else Devices ping successfully on step 5)  - Devices ping successfully on step 6) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.7 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Config single “from” policy(permit) on AP1, one Laptop ping another through AP1 | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 ping Laptop2 2. Configure a L2 policy and bind it to user-profile:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 2. Clear mac-session table, then Laptop2 ping Laptop1 | | |
| Expect result | - Laptop1 ping successfully on step 1)  - Laptop1 ping successfully on step 3)  - Laptop2 ping unsuccessfully on step 4) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.8 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Config single “from” policy(deny) on AP1, one Laptop ping another through AP1 | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 ping Laptop2 2. Configure a L2 policy and bind it to user-profile:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 2. Laptop2 ping Laptop1 | | |
| Expect result | - Laptop1 ping successfully on step 1)  - Laptop1 ping unsuccessfully on step 3)  - Laptop2 ping unsuccessfully on step 4) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.9 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Delete a config-single “from” policy(deny/permit) on AP1, one Laptop ping another through AP1 | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 ping Laptop2 2. Configure a L2 policy and bind it to user-profile:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action deny/permit”  “user-profile FW security mac-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 2. Delete the config policy   “no user-profile FW security mac-policy from-access”  “no mac-policy FW id [num]”   1. Repeat step 1 2. Laptop2 ping Laptop1 | | |
| Expect result | - Laptop1 ping successfully on step 1)  - If action is deny,Laptop1 ping unsuccessfully on step 3),else Laptop1 ping successfully on step 3)  - Laptop1 ping successfully on step 5)  - Laptop2 ping successfully on step 6) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.10 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Config single “to” policy(permit) on AP1, one Laptop ping another through AP1 | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 ping Laptop2 2. Configure a L2 policy and bind it to user-profile:   “mac-policy FW”  “mac-policy FW to <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 2. Laptop2 ping Laptop1 | | |
| Expect result | - Laptop1 ping successfully on step 1)  - Laptop1 ping unsuccessfully on step 3)  - Laptop2 ping unsuccessfully on step 4) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.11 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Config single “to” policy(deny) on AP1, one Laptop ping another through AP1 | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 ping Laptop2 2. Configure a L2 policy and bind it to user-profile:   “mac-policy FW”  “mac-policy FW to <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 2. Laptop2 ping Laptop1 | | |
| Expect result | - Laptop1 ping successfully on step 1)  - Laptop1 ping unsuccessfully on step 3)  - Laptop2 ping unsuccessfully on step 4) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.12 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Delete a config-single “to” policy(deny/permit) on AP1, one Laptop ping another through AP1 | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 ping Laptop2 2. Configure a L2 policy and bind it to user-profile:   “mac-policy FW”  “mac-policy FW to <Laptop1 mac addr> action [deny/permit]”  “user-profile FW security mac-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 2. Laptop2 ping Laptop1 3. Delete the config policy   “no user-profile FW security mac-policy to-access”  “no mac-policy FW id [num]”   1. Repeat step 1 2. Laptop2 ping Laptop1 | | |
| Expect result | - Laptop1 ping successfully on step 1)  - Laptop1 ping successfully on step 3)  - Laptop2 ping unsuccessfully on step 4)  - Laptop1 ping successfully on step 6)  - Laptop2 ping successfully on step 7) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.13 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Change the policy from permit to deny (“from-access”) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop ping gateway of SW 2. Laptop ping Server 3. Laptop ping AP1 4. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop mac addr> action permit”  “user-profile FW security mac-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1-3 2. Change the policy from permit to deny   “mac-policy FW from <Laptop mac addr> action deny”   1. Repeat step 1-3 | | |
| Expect result | - Laptop ping successfully on step 1), 2) and 3)  - Laptop ping successfully on step 5)  - Laptop ping unsuccessfully on step 7) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.14 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Change the policy from deny to permit (“from-access”) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop ping gateway of SW 2. Laptop ping Server 3. Laptop ping AP1 4. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop mac addr> action deny”  “user-profile FW security mac-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1-3 2. Change the policy from permit to deny   “mac-policy FW from <Laptop mac addr> action permit”   1. Repeat step 1-3 | | |
| Expect result | - Laptop ping successfully on step 1), 2) and 3)  - Laptop ping unsuccessfully on step 5)  - Laptop ping successfully on step 7) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.15 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Change the policy from permit to deny (“to-access”) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. gateway of SW ping Laptop 2. Server ping Laptop 3. AP1 ping Laptop 4. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop mac addr> action permit”  “user-profile FW security mac-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1-3 2. Change the policy from permit to deny   “mac-policy FW to <Laptop mac addr> action deny”   1. Repeat step 1-3 | | |
| Expect result | - Devices ping successfully on step 1), 2) and 3)  - Devices ping successfully on step 5)  - Devices ping unsuccessfully on step 7) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.16 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Change the policy from deny to permit (“to-access”) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. gateway of SW ping Laptop 2. Server ping Laptop 3. AP1 ping Laptop 4. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop mac addr> action deny”  “user-profile FW security mac-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1-3 2. Change the policy from permit to deny   “mac-policy FW to <Laptop mac addr> action permit”   1. Repeat step 1-3 | | |
| Expect result | - Devices ping successfully on step 1), 2) and 3)  - Devices ping unsuccessfully on step 5)  - Devices ping successfully on step 7) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.17 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ MP ------ Laptop2  |  SW | | |
| Description | Config single “from” policy(permit, through MP) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 ping Laptop2 each other 2. Configure a L2 policy on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | - All ping are successful on step 1)  - All ping are successful on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.18 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ MP ------ Laptop2  |  SW | | |
| Description | Config single “from” policy(deny, through MP) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 ping Laptop2 each other 2. Configure a L2 policy on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | - All ping are successful on step 1)  - Laptop1 ping unsuccessfully, Laptop2 ping successfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.19 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ MP ------ Laptop2  |  SW | | |
| Description | Delete a config-single “from” policy(deny/permit,through MP) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 ping Laptop2 each other 2. Configure a L2 policy on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action [permit/deny]”  “user-profile FW security mac-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 2. Delete the config policy   “no user-profile FW security mac-policy from-access”  “no mac-policy FW id [num]”   1. Repeat step 1. | | |
| Expect result | -All ping are successful on step 1)  -If action is deny, Laptop1 ping unsuccessfully, Laptop2 ping successful ; else All ping are successful on step 3)  - All ping are successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.20 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ MP ------ Laptop2  |  SW | | |
| Description | Config single “to” policy(permit, through MP) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 ping Laptop2 each other 2. Configure a L2 policy on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | - All ping are successful on step 1)  - All ping are successful on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.21 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ MP ------ Laptop2  |  SW | | |
| Description | Config single “to” policy(deny, through MP) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 ping Laptop2 each other 2. Configure a L2 policy on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | - All ping are successful on step 1)  - Laptop1 ping successfully, Laptop2 ping unsuccessfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.22 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ MP ------ Laptop2  |  SW | | |
| Description | Delete a config-single “to” policy(deny/permit,through MP) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 ping Laptop2 each other 2. Configure a L2 policy on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop1 mac addr> action [permit/deny]”  “user-profile FW security mac-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 2. Delete the config policy   “no user-profile FW security mac-policy to-access”  “no mac-policy FW id [num]”   1. Repeat step 1. | | |
| Expect result | -All ping are successful on step 1)  -If action is deny, Laptop2 ping unsuccessfully, Laptop1 ping successful ; All ping are successful on step 3)  - All ping are successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.23 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ MP (eth0)------ Laptop2  |  SW | | |
| Description | Set eth port access,check the mac-policy(“from-permit”, through MP) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Configure a L2 policy which permit Laptop2’s mac-address on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop2 mac addr> action permit”  “user-profile FW security mac-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop2 ping Laptop1 2. Check the mac-session table on MP | | |
| Expect result | - Laptop2 ping successfully on step 2)  - There is a mac-session between Laptop2 and Laptop1 on MP on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.24 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ MP (eth0)------ Laptop2  |  SW | | |
| Description | Set eth port access,check the mac-policy(“from-deny”, through MP) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Configure a L2 policy which deny Laptop2’s mac-address on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop2 mac addr> action deny”  “user-profile FW security mac-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop2 ping Laptop1 2. Check the mac-session table on MP | | |
| Expect result | - Laptop2 ping unsuccessfully on step 2)  - There is no mac-session between Laptop2 and Laptop1 on MP on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.25 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ MP (eth0)------ Laptop2  |  SW | | |
| Description | Set eth port access,check the mac-policy(“to-permit”, through MP) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Configure a L2 policy which permit Laptop2’s mac-address on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop2 mac addr> action permit”  “user-profile FW security mac-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop1 ping Laptop2 2. Check the mac-session table on MP | | |
| Expect result | - Laptop1 ping successfully on step 2)  - There is a mac-session between Laptop2 and Laptop1 on MP on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.26 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ MP (eth0)------ Laptop2  |  SW | | |
| Description | Set eth port access,check the mac-policy(“to-deny”, through MP) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Configure a L2 policy which deny Laptop2’s mac-address on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop2 mac addr> action deny”  “user-profile FW security mac-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop1 ping Laptop2 2. Check the mac-session table on MP | | |
| Expect result | - Laptop1 ping unsuccessfully on step 2)  - There is no mac-session between Laptop2 and Laptop1 on MP on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.27 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config single “from” policy(related mgt0) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop and AP1 ping each other 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop mac addr> action [permit/deny]”  “user-profile FW security mac-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | - All pings are successful on step 1)  - If policy is deny, Laptop pings unsuccessfully, AP1 pings successfully; else all pings are successful on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.28 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config single “to” policy(related mgt0) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop and AP1 ping each other 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop mac addr> action [permit/deny]”  “user-profile FW security mac-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | - All pings are successful on step 1)  - If policy is deny, Laptop pings successfully, AP1 pings unsuccessfully; else all pings are successful on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.29 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop ------ (eth0)AP1 ------ SW ------ Server | | |
| Description | Config single “from” policy(related mgt0, through eth0) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop and AP1 ping each other 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop mac addr> action [permit/deny]”  “user-profile FW security mac-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | - All pings are successful on step 1)  - If policy is deny, Laptop pings unsuccessfully, AP1 pings successfully; else all pings are successful on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.30 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop ------(eth0) AP1 ------ SW ------ Server | | |
| Description | Config single “to” policy(related mgt0, through eth0) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop and AP1 ping each other 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop mac addr> action [permit/deny]”  “user-profile FW security mac-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | - All pings are successful on step 1)  - If policy is deny, Laptop pings successfully, AP1 pings unsuccessfully; else all pings are successful on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.31 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | PC1+++++(eth0) AP1 (eth1)+++++ SW ++++ PC2 | | |
| Description | Config single “from” policy from ethx to ethx | | |
| Pre-condition | -PC1 has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. PC1 and PC2 ping each other 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <pc1 mac addr> action [permit/deny]”  “user-profile FW security mac-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | - All pings are successful on step 1)  - If policy is deny, pc2 pings successfully, pc1 pings unsuccessfully; else all pings are successful on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_1.32 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | PC1+++++(eth0) AP1 (eth1)+++++ SW ++++ PC2 | | |
| Description | Config single “to” policy from ethx to ethx | | |
| Pre-condition | -PC1 has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. PC1 and PC2 ping each other 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW to <pc1 mac addr> action [permit/deny]”  “user-profile FW security mac-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | - All pings are successful on step 1)  - If policy is deny, pc1 pings successfully, pc2 pings unsuccessfully; else all pings are successful on step 3) | | |
| Test result |  | | |

## 7.2 “From & To” policy simultaneous test

* Case ID FW\_Mac\_Policy\_Fun\_2

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_2.1 | | |
| **Priority** | Accept | **Automation Flag** | Yes |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config “from & to” simultaneous policy(permit) | | |
| Pre-condition | -Configure AP1  *“security-object FWtest”*  *“security-object FWtest default-user-profile-attr 1”*  *“ssid FWtest”*  *“ssid FWtest security-object FWtest”*  *“interface wifi0 ssid FWtest”*  *“interface wifi1 ssid FWtest”*  *“user-profile FW qos-policy def-user-qos vlan-id <mgt0 vlan> attribute 1”*  -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1) Laptop and gateway of SW ping each other through AP1  2) Laptop and Server ping each other through AP1  3) Laptop and AP1 ping each other  4) Configure a L2 policy and bind it to FW:  ***“mac-policy FW”***  ***“mac-policy FW from <Laptop mac addr> action permit”***  ***“mac-policy FW to <Laptop mac addr> action permit”***  ***“user-profile FW security mac-policy from-access FW to-access FW***  ***“clear forwarding-engine mac-sessions”***  5)Repeat step 1-3 | | |
| Expect result | -All ping successfully on step 1), 2) and 3)  -All ping successfully on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_2.2 | | |
| **Priority** | Accept | **Automation Flag** | Yes |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config “from & to” simultaneous policy(deny) | | |
| Pre-condition | -Configure AP1  *“security-object FWtest”*  *“security-object FWtest default-user-profile-attr 1”*  *“ssid FWtest”*  *“ssid FWtest security-object FWtest”*  *“interface wifi0 ssid FWtest”*  *“interface wifi1 ssid FWtest”*  *“user-profile FW qos-policy def-user-qos vlan-id <mgt0 vlan> attribute 1”*  -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop and gateway of SW ping each other through AP1 2. Laptop and Server ping each other through AP1 3. Laptop and AP1 ping each other 4. Configure a L2 policy and bind it to FW:   ***“mac-policy FW”***  ***“mac-policy FW from <Laptop mac addr> action deny”***  ***“mac-policy FW to <Laptop mac addr> action deny”***  ***“mac-policy FW action permit”***  ***“user-profile FW security mac-policy from-access FW to-access FW***  ***“clear forwarding-engine mac-sessions”***   1. Repeat step 1-3 | | |
| Expect result | -All ping are successful on step 1), 2) and 3)  -All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_2.3 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config “from & to” simultaneous policy(“from” permit, “to” deny) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop and gateway of SW ping each other through AP1 2. Laptop and Server ping each other through AP1 3. Laptop and AP1 ping each other 4. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop mac addr> action permit”  “mac-policy FW to <Laptop mac addr> action deny”  “user-profile FW security mac-policy from-access FW to-access FW  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1-3 | | |
| Expect result | -All ping are successful on step 1), 2) and 3)  -Laptop’s ping are all successful; Devices’ ping to Laptop are all unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_2.4 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config “from & to” simultaneous policy(“from” deny, “to” permit) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop and gateway of SW ping each other through AP1 2. Laptop and Server ping each other through AP1 3. Laptop and AP1 ping each other 4. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop mac addr> action deny”  “mac-policy FW to <Laptop mac addr> action permit”  “user-profile FW security mac-policy from-access FW to-access FW  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1-3 | | |
| Expect result | -All ping are successful on step 1), 2) and 3)  -Laptop’s ping are all unsuccessful; Devices’ ping to Laptop are all successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_2.5 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Config “from & to” simultaneous policy(permit, two Laptops) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other through AP1 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action permit”  “mac-policy FW to <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy from-access FW to-access FW  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | -All ping successfully on step 1)  -All ping successfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_2.6 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Config “from & to” simultaneous policy(deny, two Laptops) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other through AP1 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action deny”  “mac-policy FW to <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy from-access FW to-access FW  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | -All ping successfully on step 1)  -All ping unsuccessfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_2.7 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Config “from & to” simultaneous policy(“from” permit, “to” deny, two Laptops) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other through AP1 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action permit”  “mac-policy FW to <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy from-access FW to-access FW  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | -All ping successfully on step 1)  -Laptop1 ping successfully, Laptop2 ping unsuccessfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_2.8 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Config “from & to” simultaneous policy(“from” deny, “to” permit, two Laptops) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other through AP1 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action deny”  “mac-policy FW to <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy from-access FW to-access FW  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | -All ping successfully on step 1)  -Laptop1 ping unsuccessfully, Laptop2 ping successfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_2.9 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ MP ------ Laptop2  |  SW | | |
| Description | Config “from & to” simultaneous policy(permit, through MP) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other through MP 2. Configure a L2 policy on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action permit”  “mac-policy FW to <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy from-access FW to-access FW  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | -All ping successfully on step 1)  -All ping successfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_2.10 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ MP ------ Laptop2  |  SW | | |
| Description | Config “from & to” simultaneous policy(deny, through MP) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other through MP 2. Configure a L2 policy on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action deny”  “mac-policy FW to <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy from-access FW to-access FW  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | -All ping successfully on step 1)  -All ping unsuccessfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_2.11 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ MP ------ Laptop2  |  SW | | |
| Description | Config “from & to” simultaneous policy(“from” permit, “to” deny, through MP) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other through MP 2. Configure a L2 policy on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action permit”  “mac-policy FW to <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy from-access FW to-access FW  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | -All ping successfully on step 1)  - Laptop1 ping successfully, Laptop2 ping unsuccessfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_2.12 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ MP ------ Laptop2  |  SW | | |
| Description | Config “from & to” simultaneous policy(“from” deny, “to” permit, through MP) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other through MP 2. Configure a L2 policy on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action deny”  “mac-policy FW to <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy from-access FW to-access FW  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | -All ping successfully on step 1)  - Laptop1 ping unsuccessfully, Laptop2 ping successfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_2.13 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ Laptop2  |  SW | | |
| Description | Config “from & to” simultaneous policy(config “from” policy but bind it to “to” direction) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other through AP1 2. Configure a L2 policy on AP1 and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | -All ping successfully on step 1)  - Laptop1 ping successfully, Laptop2 ping unsuccessfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_2.14 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ Laptop2  |  SW | | |
| Description | Config “from & to” simultaneous policy(config “to” policy but bind it to “from” direction) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other through AP1 2. Configure a L2 policy on AP1 and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | -All ping successfully on step 1)  - Laptop1 ping unsuccessfully, Laptop2 ping successfully on step 3) | | |
| Test result |  | | |

## 7.3 Order of rules test

* Case ID FW\_Mac\_Policy\_Fun\_3

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_3.1 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Mac-policy “after” attribute, using “from” policy. | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 ping Laptop2 2. Configure multi-policy in a mac-policy and bind it to user-profile:   “mac-policy FW”  “mac-policy FW id 1 from <Laptop1 mac addr> action permit”  “mac-policy FW id 2 from <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 2. Laptop2 ping Laptop1 3. Use the after attribute to change the sequence of id 1 and id 2   “mac-policy FW id 1 after id 2”   1. Show the running config 2. Repeat step 1 3. Laptop2 ping Laptop1 | | |
| Expect result | - Laptop1 ping successfully on step 1)  - Laptop1 ping successfully on step 3)  - Laptop2 ping successfully on step 4)  -The running config shows that the id 2 policy is before id 1 in mac-policy FW.  - Laptop1 ping unsuccessfully on step 7)  - Laptop2 ping successfully on step 8) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_3.2 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Mac-policy “after” attribute, using “to” policy. | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 ping Laptop2 2. Configure multi-policy in a mac-policy and bind it to user-profile:   “mac-policy FW”  “mac-policy FW id 1 to <Laptop1 mac addr> action permit”  “mac-policy FW id 2 to <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 2. Laptop2 ping Laptop1 3. Use the after attribute to change the sequence of id 1 and id 2   “mac-policy FW id 1 after id 2”   1. Show the running config 2. Repeat step 1 3. Laptop2 ping Laptop1 | | |
| Expect result | - Laptop1 ping successfully on step 1)  - Laptop1 ping successfully on step 3)  - Laptop2 ping successfully on step 4)  -The running config shows that the id 2 policy is before id 1 in mac-policy FW.  - Laptop1 ping successfully on step 7)  - Laptop2 ping unsuccessfully on step 8) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_3.3 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Mac-policy “after” attribute, using coveraged policy. | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 ping Laptop2 2. Configure multi-policy in a mac-policy and bind it to user-profile:   “mac-policy FW”  “mac-policy FW id 1 from <Laptop1 mac addr> action permit”  “mac-policy FW id 2 to <Laptop1 mac addr> action permit”  “mac-policy FW id 3 action deny”  “user-profile FW security mac-policy from-access FW to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 2. Laptop2 ping Laptop1 3. Use the after attribute to change the sequence of id 1 and id 3   “mac-policy FW id 1 after id 3”   1. Show the running config 2. Repeat step 1 3. Laptop2 ping Laptop1 4. Use the after attribute to change the sequence of id 2 and id 3   “mac-policy FW id 2 after id 3”   1. Show the running config 2. Repeat step 1 3. Laptop2 ping Laptop1 | | |
| Expect result | - Laptop1 ping successfully on step 1)  - Laptop1 ping successfully on step 3)  - Laptop2 ping successfully on step 4)  -The running config shows that the id 3 policy is before id 1 in mac-policy FW. And the id 2 policy is on the top on step 6).  - Laptop1 ping unsuccessfully on step 7)  - Laptop2 ping successfully on step 8)  - The running config shows that the id 3 policy is before id 2 in mac-policy FW. And the id 3 policy is on the top on step 10).  - Laptop1 ping unsuccessfully on step 11)  - Laptop2 ping unsuccessfully on step 12) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_3.4 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Mac-policy “before” attribute, using “from” policy. | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 ping Laptop2 2. Configure multi-policy in a mac-policy and bind it to user-profile:   “mac-policy FW”  “mac-policy FW id 1 from <Laptop1 mac addr> action permit”  “mac-policy FW id 2 from <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 2. Laptop2 ping Laptop1 3. Use the after attribute to change the sequence of id 1 and id 2   “mac-policy FW id 2 before id 1”   1. Show the running config 2. Repeat step 1 3. Laptop2 ping Laptop1 | | |
| Expect result | - Laptop1 ping successfully on step 1)  - Laptop1 ping successfully on step 3)  - Laptop2 ping successfully on step 4)  -The running config shows that the id 2 policy is before id 1 in mac-policy FW.  - Laptop1 ping unsuccessfully on step 7)  - Laptop2 ping successfully on step 8) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_3.5 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Mac-policy “before” attribute, using “to” policy. | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 ping Laptop2 2. Configure multi-policy in a mac-policy and bind it to user-profile:   “mac-policy FW”  “mac-policy FW id 1 to <Laptop1 mac addr> action permit”  “mac-policy FW id 2 to <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 2. Laptop2 ping Laptop1 3. Use the after attribute to change the sequence of id 1 and id 2   “mac-policy FW id 2 before id 1”   1. Show the running config 2. Repeat step 1 3. Laptop2 ping Laptop1 | | |
| Expect result | - Laptop1 ping successfully on step 1)  - Laptop1 ping successfully on step 3)  - Laptop2 ping successfully on step 4)  -The running config shows that the id 2 policy is before id 1 in mac-policy FW.  - Laptop1 ping successfully on step 7)  - Laptop2 ping unsuccessfully on step 8) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_3.6 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Mac-policy “before” attribute, using coveraged policy. | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 ping Laptop2 2. Configure multi-policy in a mac-policy and bind it to user-profile:   “mac-policy FW”  “mac-policy FW id 1 from <Laptop1 mac addr> action permit”  “mac-policy FW id 2 to <Laptop1 mac addr> action permit”  “mac-policy FW id 3 action deny”  “user-profile FW security mac-policy from-access FW to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 2. Laptop2 ping Laptop1 3. Use the after attribute to change the sequence of id 2 and id 3   “mac-policy FW id 3 before id 2”   1. Show the running config 2. Repeat step 1 3. Laptop2 ping Laptop1 4. Use the after attribute to change the sequence of id 1 and id 3   “mac-policy FW id 3 before id 1”   1. Show the running config 2. Repeat step 1 3. Laptop2 ping Laptop1 | | |
| Expect result | - Laptop1 ping successfully on step 1)  - Laptop1 ping successfully on step 3)  - Laptop2 ping successfully on step 4)  -The running config shows that the id 3 policy is before id 2 in mac-policy FW. And the id 1 policy is on the top on step 6).  - Laptop1 ping successfully on step 7)  - Laptop2 ping unsuccessfully on step 8)  - The running config shows that the id 3 policy is before id 1 in mac-policy FW. And the id 3 policy is on the top on step 10).  - Laptop1 ping unsuccessfully on step 11)  - Laptop2 ping unsuccessfully on step 12) | | |
| Test result |  | | |

## 7.4 Regular session test

* Case ID FW\_Mac\_Policy\_Fun\_4

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_4.1 | | |
| **Priority** | Accept | **Automation Flag** | Yes |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Mac-session setup. | | |
| Pre-condition | -Configure AP1  *“security-object FWtest”*  *“security-object FWtest default-user-profile-attr 1”*  *“ssid FWtest”*  *“ssid FWtest security-object FWtest”*  *“interface wifi0 ssid FWtest”*  *“interface wifi1 ssid FWtest”*  *“user-profile FW qos-policy def-user-qos vlan-id <mgt0 vlan> attribute 1”*  -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1) Server ping Laptop  2) Check the mac-session table on AP1  ***“show forwarding-engine mac-sessions”***  3) Clear mac-session table and config mac-policy deny the traffic from and to Laptop  ***“mac-policy FW”***  ***“mac-policy FW from <Laptop mac addr> action deny”***  ***“user-profile FW security mac-policy from-access FW”***  ***“clear forwarding-engine mac-sessions”***  4) Server ping Laptop  5) Check the mac-session table on AP1  ***“show forwarding-engine mac-sessions”*** | | |
| Expect result | - Server ping successfully on step 1)  - There is a mac-session established between Server and Laptop on AP1 on step 2)  - Server ping unsuccessfully on step 4)  - There is no mac-session between Server and Laptop on step 5) | | |
| Test result | Id:12; Ageout:294225; Up:2 min 27 sec; Flag: 0x84; UPID: 1  0019:7781:b740->2477:035d:afd4,eth0; Tun:0; Flg: (0xe1210); Vlan:1; Paks:12; Bytes: 894  2477:035d:afd4->0019:7781:b740,wifi1.2; Tun:0; Flg: (0x65000); Vlan:1; Paks:11; Bytes:812 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_4.2 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Mac-session delete.(timeout) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Server ping Laptop 2. Check the mac-session table on AP1 3. Config mac-policy deny the traffic from and to Laptop   “mac-policy FW”  “mac-policy FW from/to <Laptop mac addr> action deny”  “user-profile FW security mac-policy from/to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Server ping Laptop 2. After the default age out time, check the mac-session table on AP1 | | |
| Expect result | - Server ping successfully on step 1)  - There is a mac-session established between Server and Laptop on AP1 on step 2)  - Server ping unsuccessfully on step 4)  - The mac-session is age out on step 5) | | |
| Test result | 2012-07-13 09:17:35 debug kernel: [fe]: invalidate MAC sess (10) for (5) seconds, reason (ageout)  2012-07-13 09:17:36 debug kernel: [fe]: delete MAC sess id [10] | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_4.3 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Mac-session delete.(eth port [which links Server] down) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Server ping Laptop 2. Check the mac-session table on AP1 3. Config the eth port down or unplug the cable   “int eth[X] shutdown”   1. Check the mac-session table on AP1 | | |
| Expect result | - Server ping successfully on step 1)  - There is a mac-session established between Server and Laptop on AP1 on step 2)  - The mac-session is deleted on step 4) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_4.4 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Mac-session delete.(eth port [which links Server] mode change) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Server ping Laptop 2. Check the mac-session table on AP1 3. Change the eth port mode AP1   “intface eth[X] mode [backhaul|bridge-access]”   1. Check the mac-session table on AP1 | | |
| Expect result | - Server ping successfully on step 1)  - There is a mac-session between Server and Laptop on AP1 on step 2)  - The mac-session is deleted on step 4) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| ~~Case ID~~ | ~~FW\_Mac\_Policy\_Fun\_4.5~~ | | |
| **~~Priority~~** | ~~Low~~ | **~~Automation Flag~~** | ~~NA~~ |
| ~~Topology to use~~ | ~~Laptop ------ AP1 ------ SW ------ Server~~ | | |
| ~~Description~~ | ~~Mac-session delete.(wifi port [which links Laptop] mode change)~~ | | |
| ~~Pre-condition~~ | ~~-Laptop has been associated with AP1 and assigned an ip address~~  ~~-Laptop uses user-profile “FW”~~ | | |
| ~~Test procedure~~ | 1. ~~Server ping Laptop~~ 2. ~~Check the mac-session table on AP1~~ 3. ~~Change the wifi port mode AP1~~   ~~“intface wifi[X] mode backhaul”~~   1. ~~Check the mac-session table on AP1~~ | | |
| ~~Expect result~~ | ~~- Server ping successfully on step 1)~~  ~~- There is a mac-session between Server and Laptop on AP1 on step 2)~~  ~~- The mac-session is deleted on step 4)~~ | | |
| ~~Test result~~ |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_4.6 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Mac-session delete.(Laptop go away) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Server ping Laptop 2. Check the mac-session table on AP1 3. Move the Laptop out range of the AP1 4. Check the mac-session table on AP1 | | |
| Expect result | - Server ping successfully on step 1)  - There is a mac-session between Server and Laptop on AP1 on step 2)  - The mac-session is deleted on step 4) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_4.7 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Mac-session delete.(using cmd) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Server ping Laptop 2. Check the mac-session table on AP1 3. Delete the mac-session by cmd   “clear forward-engine mac-session id [X]”   1. Check the mac-session table on AP1 | | |
| Expect result | - Server ping successfully on step 1)  - There is a mac-session between Server and Laptop on AP1 on step 2)  - The mac-session is deleted on step 4) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_4.8 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Mac-session delete.(ssid shutdown) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Server ping Laptop 2. Check the mac-session table on AP1 3. Shutdown the ssid by cmd   “intface wifi[num] ssid <ssid\_name> shutdown”   1. Check the mac-session table on AP1 | | |
| Expect result | - Server ping successfully on step 1)  - There is a mac-session between Server and Laptop on AP1 on step 2)  - The mac-session is deleted on step 4) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_4.9 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Mac-session delete.(modify policy conflict with the address in the exsit session) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Server ping Laptop 2. Check the mac-session table on AP1 3. Modify the policy which conflict with the address in the exsit session 4. Check the mac-session table on AP1 | | |
| Expect result | - Laptop ping successfully on step 1)  - There is a mac-session between Server and Laptop on AP1 on step 2)  - The mac-session is deleted on step 4) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_4.10 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | MP ------ AP1 ------ SW ------ Server  | |  Laptop1 Laptop2 | | |
| Description | Mac-session setup/delete.(through MP) | | |
| Pre-condition | -Laptop2 has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 ping Laptop2 2. Check the mac-session table on MP 3. Shutdown the wifi backhoul of AP1   “intface wifi[num] shutdown”   1. Check the mac-session table on MP 2. Up the wifi backhaul of AP1, repeat step 1 3. Check the mac-session table on MP 4. Shutdown the wifi backhaul of MP   “intface wifi[num] shutdown”   1. Check the mac-session table on MP 2. Up the wifi backhoul of MP, repeat step 1 3. Check the mac-session table on MP 4. Change the wifi backhaul to access on AP1   “intface wifi[num] mode access”   1. Check the mac-session table on MP 2. Change the wifi to backhaul on AP1, repeat step 1 3. Check the mac-session table on MP 4. Change the wifi backhaul to access on MP   “intface wifi[num] mode access”   1. Check the mac-session table on MP | | |
| Expect result | - Laptop1 ping successfully on step 1)  - There is a mac-session between Laptop1 and Laptop2 on MP on step 2)  - The mac-session is deleted on step 4)  - There is a mac-session between Laptop1 and Laptop2 on MP on step 6)  - The mac-session is deleted on step 8)  - There is a mac-session between Laptop1 and Laptop2 on MP on step 10)  - The mac-session is deleted on step 12)  - There is a mac-session between Laptop1 and Laptop2 on MP on step 14)  - The mac-session is deleted on step 16) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_4.11 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Mac-session correlative mgt0 test(change mgt0’s vlan). | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop ping AP1 2. Check the mac-session table on AP1 3. Change the mgt0’s vlan attribute   “intface mtg0 vlan [num]”   1. Check the mac-session table on AP1 | | |
| Expect result | - Laptop ping successfully on step 1)  - There is a mac-session between AP1(mgt0) and Laptop on AP1 on step 2)  - The mac-session is deleted on step 4) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_MAC\_Policy\_Fun\_4.12 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Mac-session correlative mgt0 test (packet with error vlan). | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop ping AP1 2. Check the mac-session table on AP1 3. Send packet to AP1 which is corresponding the session between AP1 and Laptop but the vlan using tools 4. Check the packet information on AP1 | | |
| Expect result | - Laptop ping successfully on step 2)  - There is a mac-session between AP1(mgt0) and Laptop on AP1 on step 3)  - The packet should be dropped cause the wrong vlan on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_4.13 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Mgt0 communicates device through backhaul | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. AP1 and gateway of SW ping each other | | |
| Expect result | - Laptop ping successfully, and there is a mac-session between AP1 and gateway of SW on AP1 on step 1) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_4.14 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Mac-session parameters test.(upid) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config a new upid and radius-server   “user-group <group\_name>”  “user-group <group\_name> user-attribute [num]”  “aaa radius-server local user-group <group\_name>”  “aaa radius-server local db-type local”  “aaa radius-server local enable”  “ssid <ssid\_name> security aaa radius-server primary <ip\_address>”  “ssid <ssid\_name> security protocol-suite wpa-auto-8021x”  “user-profile <user-profile\_string> qos-policy def-user-qos vlan-id [num] attribute [num]”   1. Laptop ping Server 2. Check the mac-session table on AP1 | | |
| Expect result | - Laptop ping successfully on step 2)  - There is a mac-session between Server and Laptop on AP1 on step 2), and the upid attribute is the config user-attribute | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_4.15 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Mac-session parameters test.(upid, Laptop with AP) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config a mac-policy, binding it to a user-profile, and config a upid on AP1   “mac-policy MAC-0”  “mac-policy MAC-0 [from/to] <Laptop mac\_addr> action permit”  “user-profile FW”  “user-profile FW security mac-policy from-access MAC-0 to-access MAC-0”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop ping AP1 2. Check the mac-session table on AP1 | | |
| Expect result | - Laptop ping successfully on step 2)  - There is a mac-session between AP1 and Laptop on AP1 on step 3), and the upid attribute (Laptop->AP1) is 4096, the the upid attribute (AP1->Laptop) is the config user-attribute. | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_4.16 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Mac-session parameters test.(upid, Laptop1 with Laptop2) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address  -Laptops uses user-profile “FW” | | |
| Test procedure | 1. Config two mac-policy, binding them to different user-profiles, and config two different upid   “mac-policy MAC-0”  “mac-policy MAC-0 [from/to] <Laptop1 mac\_addr> action permit”  “user-profile FW1”  “user-profile FW1 security mac-policy from-access MAC-0 to-access MAC-0”  “ssid <ssid1\_name> default-user-profile-attr [num1]”  “mac-policy MAC-1”  “mac-policy MAC-1 [from/to] <Laptop2 mac\_addr> action permit”  “user-profile FW2”  “user-profile FW2 security mac-policy from-access MAC-1 to-access MAC-1”  “ssid <ssid2\_name> default-user-profile-attr [num2]”   1. Laptop1 ping Laptop2 2. Check the mac-session table on AP1 3. Clear the mac-session 4. Laptop1 ping Laptop2 5. Check the mac-session table on AP1 | | |
| Expect result | - Laptop1 ping successfully on step 2)  - There is a mac-session between Laptop1 and Laptop2 on AP1 on step 3), and the upid attribute (Laptop1-> Laptop2) is num2, the the upid attribute (Laptop 2->Laptop1) is the config num1. And the primary upid is num2.  - Laptop2 ping successfully on step 5)  - There is a mac-session between Laptop1 and Laptop2 on AP1 on step 6), and the upid attribute (Laptop1-> Laptop2) is num2, the the upid attribute (Laptop 2->Laptop1) is the config num1. And the primary upid is num1. | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_4.17 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------MP ------ Laptop2  |  SW | | |
| Description | Mac-session parameters test.(upid, through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address  -Laptops uses user-profile “FW” | | |
| Test procedure | 1. Config two mac-policy, binding them to different user-profiles, and config two different upid on AP1 and MP   “mac-policy MAC-0”  “mac-policy MAC-0 [from/to] <Laptop1 mac\_addr> action permit”  “user-profile FW1”  “user-profile FW1 security mac-policy from-access MAC-0 to-access MAC-0”  “ssid <ssid1\_name> default-user-profile-attr [num1]”  “mac-policy MAC-1”  “mac-policy MAC-1 [from/to] <Laptop2 mac\_addr> action permit”  “user-profile FW2”  “user-profile FW2 security mac-policy from-access MAC-1 to-access MAC-1”  “ssid <ssid2\_name> default-user-profile-attr [num2]”   1. Laptop1 ping Laptop2 2. Check the mac-session table on AP1, MP 3. Clear the mac-session 4. Laptop2 ping Laptop1 5. Check the mac-session table on AP1, MP | | |
| Expect result | - Laptop1 ping successfully on step 2)  - There is a mac-session between Laptop1 and Laptop2 on AP1 and MP on step 3), and the upid attribute (Laptop1-> Laptop2) is num2, the the upid attribute (Laptop 2->Laptop1) is the config num1. And the primary upid is num1 on AP1, num2 on MP  - Laptop2 ping successfully on step 5)  - There is a mac-session between Laptop1 and Laptop2 on AP1 and MP on step 6), and the upid attribute (Laptop1-> Laptop2) is num2, the the upid attribute (Laptop 2->Laptop1) is the config num1. And the primary upid is num1 on AP1, num2 on MP | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_4.18 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Mac-session parameters test.(vlan) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Using default vlan 2. Laptop ping Server 3. Check the mac-session table on AP1 4. Change the Mgt-vlan and native-vlan and their values are the same 5. Laptop ping Server 6. Check the mac-session table on AP1 7. Change the Mgt-vlan and native-vlan and their values are the different, config the SW that ensure the conmmunication between Laptop and Server is successful. 8. Laptop ping Server 9. Check the mac-session table on AP1 | | |
| Expect result | - Laptop ping successfully on step 2)  - There is a mac-session between Server and Laptop on AP1 on step 3), and the vlan attribute is the default value 1  - Laptop ping successfully on step 5)  - There is a mac-session between Server and Laptop on AP1 on step 6), and the vlan attribute is the changed value  - Laptop ping successfully on step 8)  - There is a mac-session between Server and Laptop on AP1 on step 9), and the vlan attribute is the changed Mgt-vlan | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_4.19 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop-------AP1 ------ SW ------ Server | | |
| Description | Mac-session correlative binding test. | | |
| Pre-condition | -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop ping Server 2. Check the mac-session table on AP1 3. Config mac-policy on AP1 and binding it to an user-profile   “mac-policy MAC-0”  “mac-policy MAC-0 [from/to] <Laptop mac\_addr> action [permit/deny]”  “user-profile FW”  “user-profile FW security mac-policy from-access MAC-0 to-access MAC-0”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Check the mac-session table on AP1 | | |
| Expect result | - Laptop ping successfully on step 1)  - There is a mac-session between server and Laptop on AP1 on step 2)  - The mac-session is deleted on AP1 on step 4) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_4.20 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop-------AP1 ------ SW ------ Server | | |
| Description | Mac-session correlative unbinding test. | | |
| Pre-condition | -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config mac-policy on AP1 and binding it to an user-profile   “mac-policy MAC-0”  “mac-policy MAC-0 [from/to] <Laptop mac\_addr> action permit”  “user-profile FW”  “user-profile FW security mac-policy from-access MAC-0 to-access MAC-0”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop ping Server 2. Check the mac-session table on AP1 3. Unbinding the mac-policy   “no user-profile FW security mac-policy from-access MAC-0 to-access MAC-0”   1. Check the mac-session table on AP1 | | |
| Expect result | - Laptop ping successfully on step 2)  - There is a mac-session between server and Laptop on AP1 on step 3)  - The mac-session is deleted on AP1 on step 5) | | |
| Test result |  | | |

## 7.5 Session syn test

* Case ID FW\_Mac\_Policy\_Fun\_5

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_5.1 | | |
| **Priority** | Accept | **Automation Flag** | No |
| Topology to use | Laptop-------AP1 ------ SW ------ Server  |  AP2 | | |
| Description | Mac-session correlative L2 roaming test. | | |
| Pre-condition | -AP1 and AP2 are in the same vlan  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Make sure AP1 and AP2 with same configures 2. Change the radio power max on AP1   “intface wifi[num] radio power 20”   1. Laptop ping Server 2. Check the mac-session table on AP1 and AP2 3. Change the wifi radio power down on AP1, and Change the radio power max on AP1   “intface wifi[num] radio power [num]”   1. Check the mac-session table on AP1 and AP2 | | |
| Expect result | - Laptop ping successfully on step 3)  - There is a mac-session between server and Laptop on AP1 on step 4)  - The mac-session is deleted on AP1, and there is a mac-session between server and Laptop on AP2 on step 6) | | |
| Test result |  | | |

## 7.6 Group Mac-Address test

* Case ID FW\_Mac\_Policy\_Fun\_6

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_6.1 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Group mac-address test (permit) | | |
| Pre-condition | -Laptop1 and Laptop2’s mac-address should be in the same address range, for example their addresses are all in 0019:770e:xxxx range | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other 2. Laptops and Server ping each other 3. Configure a L2 policy using group mac-address which coveraged Laptop1 and Laptop2 and bind it to user-profile:   “mac-policy FW”  “mac-policy FW from <group mac addr> action permit”  “user-profile FW security mac-policy from-access FW to-access FW”   1. Show the config 2. Repeat step 1 3. Repeat step 2 4. Configure a L2 policy using group mac-address which coveraged Laptop1 and Laptop2 and bind it to user-profile:   “no mac-policy FW id 1”  “mac-policy FW to <group mac addr> action permit”   1. Show the config 2. Repeat step 1 3. Repeat step 2 | | |
| Expect result | - All ping are successfully on step 1)  - The config shows the mac-policy correctly on step 3)  - All ping are successfully on step 4) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_6.2 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Group mac-address test (deny) | | |
| Pre-condition | -Laptop1 and Laptop2’s mac-address should be in the same address range, for example their addresses are all in 0019:770e:xxxx range | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other 2. Laptops and Server ping each other 3. Configure a L2 policy using group mac-address which coveraged Laptop1 and Laptop2 and bind it to user-profile:   “mac-policy FW”  “mac-policy FW [from/to] <group mac addr> action deny”  “user-profile FW security mac-policy from-access FW to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Show the config 2. Repeat step 1-2 | | |
| Expect result | - All ping are successfully on step 1),2)  - The config shows the mac-policy correctly on step 4)  - All ping are unsuccessfully on step 5) | | |
| Test result |  | | |

## 7.7 Change policy or binding while traffic is on-going

* Case ID FW\_Mac\_Policy\_Fun\_7

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.1 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Add/Delete policy while traffic is on-going(from-access permit) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop and gateway of SW ping each other continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop mac addr> action permit”  “user-profile FW security mac-policy from-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the policy config   ~~“no user-profile FW security mac-policy from-access”~~  “no mac-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  1)All ping are successful  ~~- All ping are successful on step 3)~~  3) Laptop1 ping gateway successfully, gateway ping Laotop1 unsuccessfully  ~~- All ping are successful on step 5)~~  5) All ping are unsuccessful | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.2 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Add/Delete policy while traffic is on-going(from-access deny) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop and gateway of SW ping each other continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop mac addr> action deny”  “user-profile FW security mac-policy from-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the policy config   ~~“no user-profile FW security mac-policy from-access”~~  “no mac-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- Laptop ping unsuccessfully, SW ping successfully on step 3)~~  ~~- All ping are successfu on step 5)~~  1) All ping are successful  3) All ping are unsuccessful  5) All ping are unsuccessful | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.3 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Add/Delete policy while traffic is on-going(from-access permit+deny) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop and gateway of SW ping each other continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop mac addr> action permit”  “user-profile FW security mac-policy from-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Add the deny policy   “mac-policy FW from <Laptop mac addr> action deny”   1. Check the ping pkt 2. Delete the permit policy   ~~“no user-profile FW security mac-policy from-access”~~  “no mac-policy FW id [num=permit policy num]”   1. Check the ping pkt 2. Delete the deny policy   ~~“no user-profile FW security mac-policy from-access”~~  “no mac-policy FW id [num=deny policy num]”   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- All ping are successful on step 3)~~  ~~- All ping are successful on step 5)~~  ~~- Laptop ping unsuccessfully, SW ping successfully on step 7)~~  ~~- All ping are successful on step 9)~~  1) All ping are successful  3) Laptop1 ping gateway successfully, gateway ping Laotop1 unsuccessfully  5) Laptop1 ping gateway successfully, gateway ping Laotop1 unsuccessfully  7) All ping are unsuccessful  9) All ping are unsuccessful | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.4 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Add/Delete policy while traffic is on-going(to-access permit) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop and gateway of SW ping each other continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop mac addr> action permit”  “user-profile FW security mac-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the policy config   ~~“no user-profile FW security mac-policy from-access”~~  “no mac-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - Laptop unsuccessful/Server successful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.5 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Add/Delete policy while traffic is on-going(to-access deny) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop and gateway of SW ping each other continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop mac addr> action deny”  “user-profile FW security mac-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the policy config   ~~“no user-profile FW security mac-policy from-access”~~  “no mac-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.6 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Add/Delete policy while traffic is on-going(to-access permit+deny) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop and gateway of SW ping each other continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop mac addr> action permit”  “user-profile FW security mac-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Add the deny policy   “mac-policy FW to <Laptop mac addr> action deny”   1. Check the ping pkt 2. Delete the permit policy   ~~“no user-profile FW security mac-policy to-access”~~  “no mac-policy FW id [num=permit policy num]”   1. Check the ping pkt 2. Delete the deny policy   ~~“no user-profile FW security mac-policy to-access”~~  “no mac-policy FW id [num=deny policy num]”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - Laptop unsuccessful/Server successful on step 3)  - Laptop unsuccessful/Server successful on step 3)  - All ping are unsuccessful on step 7)  - All ping are unsuccessful on step 9) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.7 | | |
| **Priority** | Accept | **Automation Flag** | Yes |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Add/Delete policy while traffic is on-going(from+to permit) | | |
| Pre-condition | -Configure AP1  *“security-object FWtest”*  *“security-object FWtest default-user-profile-attr 1”*  *“ssid FWtest”*  *“ssid FWtest security-object FWtest”*  *“interface wifi0 ssid FWtest”*  *“interface wifi1 ssid FWtest”*  *“user-profile FW qos-policy def-user-qos vlan-id <mgt0 vlan> attribute 1”*  -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop and gateway of SW ping each other continuance 2. Configure a L2 policy and bind it to FW:   ***“mac-policy FW”***  ***“mac-policy FW from <Laptop mac addr> action permit”***  ***“mac-policy FW to <Laptop mac addr> action permit”***  ***“user-profile FW security mac-policy from-access FW to-access FW”***  ***“clear forwarding-engine mac-sessions”***   1. Check the ping pkt 2. Delete the policy 1   ***“no mac-policy FW id 1”***   1. Check the ping pkt 2. Delete the policy 2   ***“no mac-policy FW id 2”***   1. Check the ping pkt 2. Unbind the policy   ***“user-profile FW security mac-policy from-access FW”***  ***“user-profile FW security mac-policy to-access FW”***   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- All ping are successful on step 3)~~  ~~- All ping are successful on step 5)~~  ~~- All ping are successful on step 7)~~  ~~- All ping are successful on step 9)~~  1) All ping are successful  3) All ping are successful  5) Laptop ping gateway unsuccessfully(from-access default deny), gateway ping laptop successfully(to-access id 1 permit)  7) All ping are unsuccessful  9) All ping are successful | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.8 | | |
| **Priority** | Accept | **Automation Flag** | Yes |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Add/Delete policy while traffic is on-going(from+to deny) | | |
| Pre-condition | -Configure AP1  *“security-object FWtest”*  *“security-object FWtest default-user-profile-attr 1”*  *“ssid FWtest”*  *“ssid FWtest security-object FWtest”*  *“interface wifi0 ssid FWtest”*  *“interface wifi1 ssid FWtest”*  *“user-profile FW qos-policy def-user-qos vlan-id <mgt0 vlan> attribute 1”*  -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1) Laptop and gateway of SW ping each other continuance  2) Configure a L2 policy and bind it to FW:  ***“mac-policy FW”***  ***“mac-policy FW from <Laptop mac addr> action deny”***  ***“mac-policy FW to <Laptop mac addr> action deny”***  ***“user-profile FW security mac-policy from-access FW to-access FW”***  ***“clear forwarding-engine mac-sessions”***  3) Check the ping pkt  4) Delete the policy 1  ***~~“no user-profile FW security mac-policy from-access”~~***  ***“no mac-policy FW id 1”***  5) Check the ping pkt  6) Delete the policy 2  ***~~“no user-profile FW security mac-policy from-access”~~***  ***“no mac-policy FW id 2”***  7) Check the ping pkt  8) Unbind the policy  ***“user-profile FW security ip-policy from-access FW”***  ***“user-profile FW security ip-policy to-access FW”***  9) Check the packet | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5)  - All ping are unsuccessful on step 7)  - All ping are successful on step 9) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.9 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Add/Delete policy while traffic is on-going(from+to, one direction permit, one deny) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop and gateway of SW ping each other continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop mac addr> action permit”  “mac-policy FW to <Laptop mac addr> action deny”  “user-profile FW security mac-policy from-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the from policy   ~~“no user-profile FW security mac-policy [from/to]-access”~~  “no mac-policy FW id [num]”   1. Check the ping pkt 2. Delete the to policy   ~~“no user-profile FW security mac-policy [from/to]-access”~~  “no mac-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - Laptop successful/Server unsuccessful on step 3)  - All ping are unsuccessful on step 5)  - All ping are unsuccessful on step 7) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.10 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Add/Delete policy while traffic is on-going(from-access permit, two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy from-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the policy config   ~~“no user-profile FW security mac-policy from-access”~~  “no mac-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- All ping are successful on step 3)~~  ~~- All ping are successful on step 5)~~  1) All ping are successful  3) All ping are unsuccessful(Laptop1 to-access default/Laptop2 from-access default)  5) All ping are unsuccessful | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.11 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Add/Delete policy while traffic is on-going(from-access deny, two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy from-access FW”  “~~ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the policy config   ~~“no user-profile FW security mac-policy from-access”~~  “no mac-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- Laptop1 ping unsuccessfully, Laptop2 ping successfully on step 3)~~  ~~- All ping are successful on step 5)~~  1) All ping are successful  3) All ping are unsuccessful(Laptop1 from-access id 1/Laptop2 from-access default)  5) All ping are unsuccessful | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.12 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Add/Delete policy while traffic is on-going(from-access permit+deny, two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy from-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Add the deny policy   “mac-policy FW to <Laptop1 mac addr> action deny”   1. Check the ping pkt 2. Delete the permit policy   ~~“no user-profile FW security mac-policy from-access”~~  “no mac-policy FW id [num=permit policy num]”   1. Check the ping pkt 2. Delete the deny policy   ~~“no user-profile FW security mac-policy from-access”~~  “no mac-policy FW id [num=deny policy num]”   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- All ping are successful on step 3)~~  ~~- All ping are successful on step 5)~~  ~~- Laptop1 ping unsuccessfully, Laptop2 ping successfully on step 7)~~  ~~- All ping are successful on step 9)~~  1) All ping are successful  3) All ping are unsuccessful  5) All ping are unsuccessful  7) All ping are unsuccessful  9) All ping are unsuccessful | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.13 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Add/Delete policy while traffic is on-going(to-access permit, two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the policy config   ~~“no user-profile FW security mac-policy to-access”~~  “no mac-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.14 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Add/Delete policy while traffic is on-going(to-access deny, two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the policy config   ~~“no user-profile FW security mac-policy to-access”~~  “no mac-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- Laptop2 ping unsuccessfully, Laptop1 ping successfully on step 3)~~  ~~- All ping are successful on step 5)~~  1) All ping are successful  3) All ping are unsuccessful(Laptop1 from-access default/Laptop2 from-access default)  5) All ping are unsuccessful(Laptop1 from-access default/Laptop2 from-access default) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.15 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Add/Delete policy while traffic is on-going(to-access permit+deny, two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Add the deny policy   “mac-policy FW to <Laptop1 mac addr> action deny”   1. Check the ping pkt 2. Delete the permit policy   ~~“no user-profile FW security mac-policy to-access”~~  “no mac-policy FW id [num=permit policy num]”   1. Check the ping pkt 2. Delete the deny policy   ~~“no user-profile FW security mac-policy to-access”~~  “no mac-policy FW id [num=deny policy num]”   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- All ping are successful on step 3)~~  ~~- All ping are successful on step 5)~~  ~~- Laptop2 ping unsuccessfully, Laptop1 ping successfully on step 7)~~  ~~- All ping are successful on step 9)~~  1) All ping are successful  3) All ping are unsuccessful(Laptop1 from-access default/Laptop2 from-access default)  5) All ping are unsuccessful(Laptop1 from-access default/Laptop2 from-access default)  7) All ping are unsuccessful | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.16 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Add/Delete policy while traffic is on-going(from+to permit, two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action permit”  “mac-policy FW to <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy from-access FW to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the from policy   ~~“no user-profile FW security mac-policy [from/to]-access”~~  “no mac-policy FW id [num]”   1. Check the ping pkt 2. Delete the to policy   ~~“no user-profile FW security mac-policy [from/to]-access”~~  “no mac-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- All ping are successful on step 3)~~  ~~- All ping are successful on step 5)~~  1) All ping are successful  3) All ping are successful  5) Laptop1 cannot ping Laptop2 successfully, Laptop2 can ping Laptop1 successfully  7) All ping are unsuccessful | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.17 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Add/Delete policy while traffic is on-going(from+to deny, two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action deny”  “mac-policy FW to <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy from-access FW to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the from policy   ~~“no user-profile FW security mac-policy [from/to]-access”~~  “no mac-policy FW id [num]”   1. Check the ping pkt 2. Delete the to policy   ~~“no user-profile FW security mac-policy [from/to]-access”~~  “no mac-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- All ping are unsuccessful on step 3)~~  ~~- All ping are successful on step 5)~~  1) All ping are successful  3) All ping are unsuccessful  5) All ping are unsuccessful  7) All ping are unsuccessful | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.18 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Add/Delete policy while traffic is on-going(from+to, one direction permit, one deny ,two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action permit”  “mac-policy FW to <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy from-access FW to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the permit policy   ~~“no user-profile FW security mac-policy [from/to]-access”~~  “no mac-policy FW id [num]”   1. Check the ping pkt 2. Delete the deny policy   ~~“no user-profile FW security mac-policy [from/to]-access”~~  “no mac-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- If from-policy permit, Laptop1 ping successfully, Laptop2 ping unsuccessfully; else Laptop1 ping unsuccessfully, Laptop2 ping successfully on step 3)~~  ~~- All ping are successful on step 5)~~  1) All ping are successful  3) Laptop1 can ping Laptop2 successfully, Laptop2 cannot ping Laptop1 successfully  5) All ping are unsuccessful  7) All ping are unsuccessful | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.19 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP ------ Laptop2  |  SW | | |
| Description | Add/Delete policy while traffic is on-going(from-access permit, through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a L2 policy on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy from-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the policy config   ~~“no user-profile FW security mac-policy from-access”~~  “no mac-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.20 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP ------ Laptop2  |  SW | | |
| Description | Add/Delete policy while traffic is on-going(from-access deny, through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a L2 policy on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy from-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the policy config   ~~“no user-profile FW security mac-policy from-access”~~  “no mac-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- Laptop1 ping unsuccessfully, Laptop2 ping successfully on step 3)~~  ~~- All ping are successful on step 5)~~  - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.21 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP ------ Laptop2  |  SW | | |
| Description | Add/Delete policy while traffic is on-going(from-access permit+deny, through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a L2 policy on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy from-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Add the deny policy   “mac-policy FW to <Laptop1 mac addr> action deny”   1. Check the ping pkt 2. Delete the permit policy   ~~“no user-profile FW security mac-policy from-access”~~  “no mac-policy FW id [num=permit policy num]”   1. Check the ping pkt 2. Delete the deny policy   ~~“no user-profile FW security mac-policy from-access”~~  “no mac-policy FW id [num=deny policy num]”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5)  - All ping are unsuccessful on step 7)  - All ping are unsuccessful on step 9) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.22 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP ------ Laptop2  |  SW | | |
| Description | Add/Delete policy while traffic is on-going(to-access permit, through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a L2 policy on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the policy config   ~~“no user-profile FW security mac-policy to-access”~~  “no mac-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - Laptop1 unsuccessful/Laptop2 successful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.23 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP ------ Laptop2  |  SW | | |
| Description | Add/Delete policy while traffic is on-going(to-access deny, through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a L2 policy on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the policy config   ~~“no user-profile FW security mac-policy to-access”~~  “no mac-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.24 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP ------ Laptop2  |  SW | | |
| Description | Add/Delete policy while traffic is on-going(to-access permit+deny, through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a L2 policy on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Add the deny policy   “mac-policy FW to <Laptop1 mac addr> action deny”   1. Check the ping pkt 2. Delete the permit policy   ~~“no user-profile FW security mac-policy to-access”~~  “no mac-policy FW id [num=permit policy num]”   1. Check the ping pkt 2. Delete the deny policy   ~~“no user-profile FW security mac-policy to-access”~~  “no mac-policy FW id [num=deny policy num]”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5)  - All ping are unsuccessful on step 7)  - All ping are unsuccessful on step 9) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.25 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP ------ Laptop2  |  SW | | |
| Description | Add/Delete policy while traffic is on-going(from+to permit, through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a L2 policy on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action permit”  “mac-policy FW to <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy from-access FW to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the from policy   ~~“no user-profile FW security mac-policy [from/to]-access”~~  “no mac-policy FW id [num]”   1. Check the ping pkt 2. Delete the to policy   ~~“no user-profile FW security mac-policy [from/to]-access”~~  “no mac-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are successful on step 3)  - Laptop1 unsuccessful/Laptop2 successful on step 5)  - All ping are unsuccessful on step 7) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.26 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP ------ Laptop2  |  SW | | |
| Description | Add/Delete policy while traffic is on-going(from+to deny, through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a L2 policy on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action deny”  “mac-policy FW to <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy from-access FW to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the from policy   ~~“no user-profile FW security mac-policy [from/to]-access”~~  “no mac-policy FW id [num]”   1. Check the ping pkt 2. Delete the to policy   ~~“no user-profile FW security mac-policy [from/to]-access”~~  “no mac-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5)  - All ping are unsuccessful on step 7) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.27 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP ------ Laptop2  |  SW | | |
| Description | Add/Delete policy while traffic is on-going(from+to, one direction permit, one deny , through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a L2 policy on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action permit”  “mac-policy FW to <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy from-access FW to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the from policy   ~~“no user-profile FW security mac-policy [from/to]-access”~~  “no mac-policy FW id [num]”   1. Check the ping pkt 2. Delete the to policy   ~~“no user-profile FW security mac-policy [from/to]-access”~~  “no mac-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - Laptop1 successful/Laptop2 unsuccessful on step 3)  - All ping are unsuccessful on step 5)  - All ping are unsuccessful on step 7) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.28 | | |
| **Priority** | Accept | **Automation Flag** | Yes |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Binding/Unbinding user-profile while traffic is on-going(from-access permit) | | |
| Pre-condition | -Configure AP1  *“security-object FWtest”*  *“security-object FWtest default-user-profile-attr 1”*  *“ssid FWtest”*  *“ssid FWtest security-object FWtest”*  *“interface wifi0 ssid FWtest”*  *“interface wifi1 ssid FWtest”*  *“user-profile FW qos-policy def-user-qos vlan-id <mgt0 vlan> attribute 1”*  -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop and SW ping each other continuance 2. Configure a L2 policy and bind it to FW:   ***“mac-policy FW”***  ***“mac-policy FW from <Laptop mac addr> action permit”***  ***“user-profile FW security mac-policy from-access FW”***  ***“clear forwarding-engine mac-sessions”***   1. Check the ping pkt 2. Unbinding the policy to user-profile   ***“no user-profile FW security mac-policy from-access”***   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - Laptop successful/Server unsuccessful on step 3)  - All ping are successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.29 | | |
| **Priority** | Accept | **Automation Flag** | Yes |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Binding/Unbinding user-profile while traffic is on-going(from-access deny) | | |
| Pre-condition | -Configure AP1  *“security-object FWtest”*  *“security-object FWtest default-user-profile-attr 1”*  *“ssid FWtest”*  *“ssid FWtest security-object FWtest”*  *“interface wifi0 ssid FWtest”*  *“interface wifi1 ssid FWtest”*  *“user-profile FW qos-policy def-user-qos vlan-id <mgt0 vlan> attribute 1”*  -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop ping gateway of SW continuance 2. Configure a L2 policy and bind it to FW:   ***“mac-policy FW”***  ***“mac-policy FW from <Laptop mac addr> action deny”***  ***“mac-policy FW to <Laptop mac addr> action deny”***  ***“user-profile FW security mac-policy from-access FW”***  ***“clear forwarding-engine mac-sessions”***   1. Check the ping pkt 2. Unbinding the policy to user-profile   ***“no user-profile FW security mac-policy from-access”***   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.30 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Binding/Unbinding user-profile while traffic is on-going(to-access permit) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop ping gateway of SW continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop mac addr> action permit”  “user-profile FW security mac-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Laptop ping gateway of SW continuance 2. Unbinding the policy to user-profile   “no user-profile FW security mac-policy to-access”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - Laptop unsuccessful/Server successful on step 3)  - All ping are successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.31 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Binding/Unbinding user-profile while traffic is on-going(to-access deny) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop ping gateway of SW continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop mac addr> action deny”  “user-profile FW security mac-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Laptop ping gateway of SW continuance 2. Unbinding the policy to user-profile   “no user-profile FW security mac-policy to-access”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.32 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Binding/Unbinding user-profile while traffic is on-going(from-access permit, two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy from-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Unbinding the policy to user-profile   “no user-profile FW security mac-policy from-access”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are successful on step 3)  - All ping are successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.33 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Binding/Unbinding user-profile while traffic is on-going(from-access deny, two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Check the ping pkt 2. Unbinding the policy to user-profile   “no user-profile FW security mac-policy from-access”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - Laptop1 ping unsuccessfully, Laptop2 ping successfully on step 3)  - All ping are successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.34 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Binding/Unbinding user-profile while traffic is on-going(to-access permit, two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Check the ping pkt 2. Unbinding the policy to user-profile   “no user-profile FW security mac-policy to-access”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are successful on step 3)  - All ping are successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.35 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Binding/Unbinding user-profile while traffic is on-going(to-access deny, two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 ping Laptop1 continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop2 ping Laptop1 continuance 2. Unbinding the policy to user-profile   “no user-profile FW security mac-policy to-access”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - Laptop1 ping successfully, Laptop2 ping unsuccessfully on step 3)  - All ping are successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.36 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP ------ Laptop2  |  SW | | |
| Description | Binding/Unbinding user-profile while traffic is on-going(from-access permit, through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping continuance 2. Configure a L2 policy on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Check the ping pkt 2. Unbinding the policy to user-profile   “no user-profile FW security mac-policy from-access”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are successful on step 3)  - All ping are successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.37 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP ------ Laptop2  |  SW | | |
| Description | Binding/Unbinding user-profile while traffic is on-going(from-access deny, through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping continuance 2. Configure a L2 policy on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Check the ping pkt 2. Unbinding the policy to user-profile   “no user-profile FW security mac-policy from-access”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - Laptop1 ping unsuccessfully, Laptop2 ping successfully on step 3)  - All ping are successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.38 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP ------ Laptop2  |  SW | | |
| Description | Binding/Unbinding user-profile while traffic is on-going(to-access permit, through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping continuance 2. Configure a L2 policy on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Check the ping pkt 2. Unbinding the policy to user-profile   “no user-profile FW security mac-policy to-access”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are successful on step 3)  - All ping are successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.39 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP ------ Laptop2  |  SW | | |
| Description | Binding/Unbinding user-profile while traffic is on-going(to-access deny, through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping continuance 2. Configure a L2 policy on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Check the ping pkt 2. Unbinding the policy to user-profile   “no user-profile FW security mac-policy to-access”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - Laptop1 ping successfully, Laptop2 ping unsuccessfully on step 3)  - All ping are successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.40 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop------ AP1 ------ SW ------ Server | | |
| Description | Change the Binding user-profile while traffic is on-going(from-access)(permit->deny) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop and gateway of SW ping each other continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop mac addr> action permit”  “user-profile FW security mac-policy from-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Configure an new L2 policy and bind it to FW   “mac-policy FW2”  “mac-policy FW2 from <Laptop mac addr> action deny”  “user-profile FW security mac-policy from-access FW2”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - Laptop successful/Sever unsuccessful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.41 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop------ AP1 ------ SW ------ Server | | |
| Description | Change the Binding user-profile while traffic is on-going(from-access)(deny->permit) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop and gateway of SW ping each other continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop mac addr> action deny”  “user-profile FW security mac-policy from-access FW”  “~~ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Configure an new L2 policy and bind it to FW   “mac-policy FW2”  “mac-policy FW2 from <Laptop mac addr> action permit”  “user-profile FW security mac-policy from-access FW2”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - Laptop successful/Sever unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.42 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop------ AP1 ------ SW ------ Server | | |
| Description | Change the Binding user-profile while traffic is on-going(to-access)(permit->deny) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop and gateway of SW ping each other continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop mac addr> action permit”  “user-profile FW security mac-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Configure an new L2 policy and bind it to FW   “mac-policy FW2”  “mac-policy FW2 to <Laptop mac addr> action deny”  “user-profile FW security mac-policy to-access FW2”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - Laptop unsuccessful/Sever successful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.43 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop------ AP1 ------ SW ------ Server | | |
| Description | Change the Binding user-profile while traffic is on-going(to-access)(deny->permit) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop and gateway of SW ping each other continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop mac addr> action deny”  “user-profile FW security mac-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Configure an new L2 policy and bind it to FW   “mac-policy FW2”  “mac-policy FW2 to <Laptop mac addr> action permit”  “user-profile FW security mac-policy to-access FW2”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - Laptop unsuccessful/Sever successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.44 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop------ AP1 ------ SW ------ Server | | |
| Description | Change the Binding user-profile while traffic is on-going (from/to-access) (permit->deny->permit) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1)Laptop and gateway of SW ping each other continuance  2)Configure a ip-policy and bind it to FW:  “mac-policy FW”  “mac-policy FW from <Laptop mac addr> action permit”  “user-profile FW security mac-policy from-access FW to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~  3)Check the ping pkt  4)Configure an new ip-policy and bind it to FW  “mac-policy FW2”  “mac-policy FW2 from <Laptop mac addr> action deny”  “user-profile FW security mac-policy from-access FW2 to-access FW2”  5)Check the ping pkt  6) Recover  “user-profile FW security mac-policy from-access FW to-access FW”  7)Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - Laptop successful/Server unsuccessful on step 3)  - All ping are unsuccessful on step 5)  - Laptop successful/Server unsuccessful on step 7) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.45 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Change the Binding user-profile while traffic is on-going(from-access)(permit->deny)(two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy from-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Configure an new L2 policy and bind it to FW   “mac-policy FW2”  “mac-policy FW2 from <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy from-access FW2”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.46 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Change the Binding user-profile while traffic is on-going(from-access)(deny->permit)(two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy from-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Configure an new L2 policy and bind it to FW   “mac-policy FW2”  “mac-policy FW2 from <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy from-access FW2”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.47 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Change the Binding user-profile while traffic is on-going(to-access)(permit->deny) (two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Configure an new L2 policy and bind it to FW   “mac-policy FW2”  “mac-policy FW2 to <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy to-access FW2”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.48 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Change the Binding user-profile while traffic is on-going(to-access)(deny->permit) (two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other continuance 2. Configure a L2 policy and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Configure an new L2 policy and bind it to FW   “mac-policy FW2”  “mac-policy FW2 to <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy to-access FW2”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.49 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Change the Binding user-profile while traffic is on-going (from/to-access) (permit->deny->permit) (two Laptops) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1)Laptop1 and laptop2 ping each other continuance  2)Configure a ip-policy and bind it to FW:  “mac-policy FW”  “mac-policy FW from <Laptop mac addr> action permit”  “user-profile FW security mac-policy from-access FW to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~  3)Check the ping pkt  4)Configure an new ip-policy and bind it to FW  “mac-policy FW2”  “mac-policy FW2 from <Laptop mac addr> action deny”  “user-profile FW security mac-policy from-access FW2 to-access FW2”  5)Check the ping pkt  6) Recover  “user-profile FW security mac-policy from-access FW to-access FW”  7)Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - Laptop1 successful/Laptop2 unsuccessful on step 3)  - All ping are unsuccessful on step 5)  - Laptop1 successful/Laptop2 unsuccessful on step 7) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.50 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP------ Laptop2  |  SW | | |
| Description | Change the Binding user-profile while traffic is on-going (from-access) (permit->deny) (through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other continuance 2. Configure a L2 policy on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy from-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Configure an new L2 policy and bind it to FW   “mac-policy FW2”  “mac-policy FW2 from <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy from-access FW2”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.51 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP------ Laptop2  |  SW | | |
| Description | Change the Binding user-profile while traffic is on-going(from-access)(deny->permit)(through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other continuance 2. Configure a L2 policy on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW from <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy from-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Configure an new L2 policy and bind it to FW   “mac-policy FW2”  “mac-policy FW2 from <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy from-access FW2”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.52 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP------ Laptop2  |  SW | | |
| Description | Change the Binding user-profile while traffic is on-going(to-access)(permit->deny) (through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other continuance 2. Configure a L2 policy on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Configure an new L2 policy and bind it to FW   “mac-policy FW2”  “mac-policy FW2 to <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy to-access FW2”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.53 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP------ Laptop2  |  SW | | |
| Description | Change the Binding user-profile while traffic is on-going(to-access)(deny->permit) (through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other continuance 2. Configure a L2 policy on MP and bind it to FW:   “mac-policy FW”  “mac-policy FW to <Laptop1 mac addr> action deny”  “user-profile FW security mac-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Configure an new L2 policy and bind it to FW   “mac-policy FW2”  “mac-policy FW2 to <Laptop1 mac addr> action permit”  “user-profile FW security mac-policy to-access FW2”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Fun\_7.54 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP------ Laptop2  |  SW | | |
| Description | Change the Binding user-profile while traffic is on-going (from/to-access) (permit->deny->permit) (through MP) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1)Laptop1 and laptop2 ping each other continuance  2)Configure a ip-policy and bind it to FW:  “mac-policy FW”  “mac-policy FW from <Laptop mac addr> action permit”  “user-profile FW security mac-policy from-access FW to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~  3)Check the ping pkt  4)Configure an new ip-policy and bind it to FW  “mac-policy FW2”  “mac-policy FW2 from <Laptop mac addr> action deny”  “user-profile FW security mac-policy from-access FW2 to-access FW2”  5)Check the ping pkt  6) Recover  “user-profile FW security mac-policy from-access FW to-access FW”  7)Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - Laptop1 successful/Laptop2 unsuccessful on step 3)  - All ping are unsuccessful on step 5)  - Laptop1 successful/Laptop2 unsuccessful on step 7) | | |
| Test result |  | | |

## 7.8 Performance/Stress test

* Case ID FW\_Mac\_Policy\_Perf\_8

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Perf\_8.1 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config full policy in one mac-policy(permit,from-access)(32 id per mac-policy) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config full policy in one mac-policy by script and bind it to FW:   “mac-policy FW”  “mac-policy FW id 1 from <Laptop mac addr> action permit”  “mac-policy FW id 2 from <Laptop mac addr> action permit”  “mac-policy FW id 3 from <Laptop mac addr> action permit”  “…..”  ~~“user-profile FW security mac-policy from-access FW”~~  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Show the running config 2. Add the id 33 rule in policy FW | | |
| Expect result | ~~- Laptop ping successfully on step 1), 2) and 3)~~  ~~- Config full policy successfully, and the running config shows the config-policies correctly on step 5).~~  ~~- Laptop ping successfully on step 6)~~  2) Configure is shown correctly  3) May show error info | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Perf\_8.2 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config full policy in one mac-policy(deny,from-access)(32) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config full policy in one mac-policy by script and bind it to FW:   “mac-policy FW”  “mac-policy FW id 1 from <Laptop mac addr> action deny”  “mac-policy FW id 2 from <Laptop mac addr> action deny”  “mac-policy FW id 3 from <Laptop mac addr> action deny”  “…..”  ~~“user-profile FW security mac-policy from-access FW”~~  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Show the running config 2. Add the id 33 rule in policy FW | | |
| Expect result | ~~- Laptop ping successfully on step 1), 2) and 3)~~  ~~- Config full policy successfully, and the running config shows the config-policies correctly on step 5).~~  ~~- Laptop ping unsuccessfully on step 6)~~  2) Configure is shown correctly  3) May show error info | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Perf\_8.3 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config full policy in one mac-policy(permit, to-access)(32) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config full policy in one mac-policy by script and bind it to FW:   “mac-policy FW”  “mac-policy FW id 1 to <Laptop mac addr> action permit”  “mac-policy FW id 2 to <Laptop mac addr> action permit”  “mac-policy FW id 3 to <Laptop mac addr> action permit”  “…..”  ~~“user-profile FW security mac-policy to-access FW”~~  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Show the running config 2. Add the id 33 rule in policy FW | | |
| Expect result | ~~- Devices ping Laptop successfully on step 1), 2) and 3)~~  ~~- Config full policy successfully, and the running config shows the config-policies correctly on step 5).~~  ~~- Devices ping Laptop successfully on step 6)~~  2) Configure is shown correctly  3) May show error info | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Perf\_8.4 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config full policy in one mac-policy(deny, to-access)(32) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config full policy in one mac-policy by script and bind it to FW:   “mac-policy FW”  “mac-policy FW id 1 to <Laptop mac addr> action deny”  “mac-policy FW id 2 to <Laptop mac addr> action deny”  “mac-policy FW id 3 to <Laptop mac addr> action deny”  “…..”  ~~“user-profile FW security mac-policy to-access FW”~~  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Show the running config 2. Add the id 33 rule in policy FW | | |
| Expect result | ~~- Devices ping Laptop successfully on step 1), 2) and 3)~~  ~~- Config full policy successfully, and the running config shows the config-policies correctly on step 5).~~  ~~- Devices ping Laptop unsuccessfully on step 6)~~  2) Configure is shown correctly  3) May show error info | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Perf\_8.5 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config full policy in one mac-policy(deny/permit, from/to-access)(32) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config full policy in one mac-policy by script and bind it to FW:   “mac-policy FW”  “mac-policy FW id 1 from <Laptop mac addr> action permit”  “mac-policy FW id 2 from <Laptop mac addr> action deny”  “mac-policy FW id 3 to <Laptop mac addr> action permit”  “mac-policy FW id 4 to <Laptop mac addr> action deny”  “…..”  ~~“user-profile FW security mac-policy [from/to]-access FW”~~  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Show the running config 2. Add the id 33 rule in policy FW | | |
| Expect result | ~~- Devices ping successfully on step 1), 2) and 3)~~  ~~- Config full policy successfully, and the running config shows the config-policies correctly on step 5).~~  ~~- If match the deny-policy, ping should be unsuccessful on step 6), else should be successful on step 6)~~  2) Configure is shown correctly  3) May show error info | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Perf\_8.6 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config full policy in one mac-policy(deny/permit, from/to-access)(32), and using before/after attributes | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config full policy in one mac-policy by script and bind it to FW:   “mac-policy FW”  “mac-policy FW id 1 from <Laptop mac addr> action permit”  “mac-policy FW id 2 from <Laptop mac addr> action deny”  “mac-policy FW id 3 to <Laptop mac addr> action permit”  “mac-policy FW id 4 to <Laptop mac addr> action deny”  “…..”  ~~“user-profile FW security mac-policy [from/to]-access FW”~~  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Show the running config 2. Add the id 33 rule in policy FW 3. Using before/after to change the policy’s sequence   “mac-policy FW id 32 before id 1”  “mac-policy FW id 31 after id 2”  “…..”   1. Show the running config | | |
| Expect result | ~~- Devices ping successfully on step 1), 2) and 3)~~  ~~- Config full policy successfully, and the running config shows the config-policies correctly on step 5).~~  ~~- If match the deny-policy, ping should be unsuccessful on step 6), else should be successful on step 6)~~  ~~- Change the policy’s sequence successfully, and the running config should be show the sequences correctly on step 8)~~  ~~- If match the deny-policy, ping should be unsuccessful on step 6), else should be successful on step 9)~~  2) Configure is shown correctly  3) May show error info  5) The rule order is 32-1-2-31-3-4… | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Perf\_8.7 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config maximum mac-policy, and config full policy in every mac-policy (config&resource check)(32\*32) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config full policy by script and bind one of them to FW:   “mac-policy FW-0”  “mac-policy FW-0 id 1 [from/to] <Laptop mac addr> action [permit/deny]”  “mac-policy FW-0 id 2 [from/to] <Laptop mac addr> action [permit/deny]”  “mac-policy FW-0 id 3 [from/to] <Laptop mac addr> action [permit/deny]”  “…..”  “mac-policy FW-32”  “mac-policy FW-32 id 1 [from/to] <Laptop mac addr> action [permit/deny]”  “mac-policy FW-32 id 2 [from/to] <Laptop mac addr> action [permit/deny]”  “mac-policy FW-32 id 3 [from/to] <Laptop mac addr> action [permit/deny]”  ~~“user-profile FW security mac-policy [from/to]-access FW[N]”~~  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Show the running config, show the AP1’s resource using 2. Add any MAC policy or rule | | |
| Expect result | ~~- Config full policy successfully, and the running config shows the config-policies correctly , the cpu & mem’s using are normal on step 2).~~  2) CPU&Memery is normal, config is correct  3) May show error info | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Perf\_8.8 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config maximum mac-policy, and config full policy in every mac-policy, binding it to an user-profile(32\*32) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config full policy by script and bind one of them to FW:   “mac-policy FW-1”  “mac-policy FW-1 id 1 [from/to] <Laptop mac addr> action [permit/deny]”  “mac-policy FW-1 id 2 [from/to] <Laptop mac addr> action [permit/deny]”  “mac-policy FW-1 id 3 [from/to] <Laptop mac addr> action [permit/deny]”  “…..”  “mac-policy FW-32”  “mac-policy FW-32 id 1 [from/to] <Laptop mac addr> action [permit/deny]”  …  “mac-policy FW-32 id 32 [from/to] <Laptop mac addr> action [permit/deny]”  ~~“user-profile FW security mac-policy [from/to]-access FW[N]”~~  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Binding userprofile   “user-profile 1”  …  “user-profile 16”  “user-profile 1 security mac-policy from-access FW1 to-access FW2”  …  “user-profile 16 security mac-policy from-access FW31 to-access FW32”   1. Show running config, show the AP1’s resource using 2. Add any MAC rule or policy | | |
| Expect result | ~~- Laptop ping successfully on step 1), 2) and 3)~~  ~~- Config full policy successfully, and the running config shows the config-policies correctly on step 5).~~  ~~- If match the deny-policy, ping should be unsuccessful on step 6), else should be successful on step 6)~~  3) CPU&Memery is normal, config is correct  4) May show error info | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Perf\_8.9 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config maximum mac-policy, and config full policy in every mac-policy, using before/after attributes | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config full policy by script and bind one of them to FW:   “mac-policy FW-1”  “mac-policy FW-1 id 1 [from/to] <Laptop mac addr> action [permit/deny]”  “mac-policy FW-1 id 2 [from/to] <Laptop mac addr> action [permit/deny]”  “mac-policy FW-1 id 3 [from/to] <Laptop mac addr> action [permit/deny]”  “…..”  “mac-policy FW-32”  “mac-policy FW-32 id 1 [from/to] <Laptop mac addr> action [permit/deny]”  …  “mac-policy FW-32 id 32 [from/to] <Laptop mac addr> action [permit/deny]”  ~~“user-profile FW security mac-policy [from/to]-access FW[N]”~~  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Bind the user-profile   “user-profile 1”  …  “user-profile 16”  “user-profile 1 security mac-policy from-access FW1 to-access FW2”  …  “user-profile 16 security mac-policy from-access FW31 to-access FW32”   1. Add any Mac rule or policy 2. Using before/after to change the policy’s sequence which is binding to FW   “mac-policy FW-[N] id X1 before/after id Y1”  “mac-policy FW-[N] id X2 before/after id Y2”  “…..”   1. Show the running config and CPU&Memery using | | |
| Expect result | ~~- Laptop ping successfully on step 1), 2) and 3)~~  ~~- Config full policy successfully, and the running config shows the config-policies correctly on step 5).~~  ~~- If match the deny-policy, ping should be unsuccessful on step 6), else should be successful on step 6)~~  ~~- Change the policy’s sequence successfully, and the running config should be show the sequences correctly on step 8)~~  ~~- If match the deny-policy, ping should be unsuccessful on step 6), else should be successful on step 9)~~  3) May show error info  5) CPU&Memery is normal | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_Mac\_Policy\_Perf\_8.10 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config maximum mac-policy, and config full policy in every mac-policy, change the binding relation. | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Gateway of SW ping Laptop each other 2. Server ping Laptop each other 3. AP1 ping Laptop each other 4. Config full policy by script and bind one of them to FW:   “mac-policy FW-0”  “mac-policy FW-0 id 1 [from/to] <Laptop mac addr> action [permit/deny]”  “mac-policy FW-0 id 2 [from/to] <Laptop mac addr> action [permit/deny]”  “mac-policy FW-0 id 3 [from/to] <Laptop mac addr> action [permit/deny]”  “…..”  “mac-policy FW-X”  “mac-policy FW-X id 1 [from/to] <Laptop mac addr> action [permit/deny]”  “mac-policy FW-X id 2 [from/to] <Laptop mac addr> action [permit/deny]”  “mac-policy FW-X id 3 [from/to] <Laptop mac addr> action [permit/deny]”  “user-profile FW security mac-policy [from/to]-access FW-[N]”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Show the running config 2. Repeat step 1-3 3. Binding another mac-policy to FW   “user-profile FW security mac-policy [from/to]-access FW-[M]”   1. Show the running config 2. Repeat step 1-3 | | |
| Expect result | - Laptop ping successfully on step 1), 2) and 3)  - Config full policy successfully, and the running config shows the config-policies correctly on step 5).  - If match the deny-policy, ping should be unsuccessful on step 6), else should be successful on step 6)  - Change binding relation successfully, and the running config should be show the binding relation correctly on step 8)  - If match the deny-policy, ping should be unsuccessful on step 6), else should be successful on step 9) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_MAC\_Policy\_Perf\_8.11 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Establish maximum mac-session (config&resource check) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Establish maximum mac-session by using script to send packets   “#!/usr/bin/tclsh  #Filename: Macsession\_max.tcl  #Fuction: Test maximum of the macsession(8191)  #Test topo: LinuxPc+++L2sw+++(eth0)AP(wifix.x)-----Laptop  package require Expect  package require Tclx  for { set a 1 } { $a < 9 } { incr a } {  for { set b 1 } { $b < 9 } { incr b } {  for { set c 1 } { $c < 9 } { incr c } {  for { set d 1 } { $d < 9 } { incr d } {  puts "nohup pkt -i eth1 -d 10.2.2.11 -m 10.2.2.29 -N ff:ff:ff:ff:ff:ff -M 00:11:0${a}:0${b}:0${c}:0${d} -p arpreq \n"  exec pkt -i eth1 -d 10.2.2.11 -m 10.2.2.29 -N ff:ff:ff:ff:ff:ff -M 00:11:0${a}:0${b}:0${c}:0${d} -p arpreq &  }  }  }  }”   1. Show the running config and the mac-session, show the AP1’s resource using | | |
| Expect result | - Establish maximum mac-session successfully, and the running config shows the mac-session correctly , the cpu & mem’s using are normal on step 2). | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_MAC\_Policy\_Perf\_8.12 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config maximum mac-policy, and config full policy in every mac-policy, and every mac-policy to an user-profile, using one SSID(config&resource check) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Config full policy by script and bind every mac-policy to an user-profile:   “mac-policy FW-0”  “mac-policy FW-0 id 1 [from/to] <Laptop mac addr> action [permit/deny]”  “mac-policy FW-0 id 2 [from/to] <Laptop mac addr> action [permit/deny]”  “mac-policy FW-0 id 3 [from/to] <Laptop mac addr> action [permit/deny]”  “…..”  “mac-policy FW-X”  “mac-policy FW-X id 1 [from/to] <Laptop mac addr> action [permit/deny]”  “mac-policy FW-X id 2 [from/to] <Laptop mac addr> action [permit/deny]”  “mac-policy FW-X id 3 [from/to] <Laptop mac addr> action [permit/deny]”  “user-profile FW-[N] security mac-policy [from/to]-access FW-[N]”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Show the running config and check the resource consuming | | |
| Expect result | - Config full policy,and bind to user-pofile successfully, and the running config shows the config-policies and binding-relation correctly , the cpu & mem’s using are normal on step 2). | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_MAC\_Policy\_Perf\_8.13 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config maximum mac-policy, and config full policy in every mac-policy, and every mac-policy to an user-profile, using multi-SSID(config&resource check) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Config full policy by script and bind every mac-policy to an user-profile:   “mac-policy FW-0”  “mac-policy FW-0 id 1 [from/to] <Laptop mac addr> action [permit/deny]”  “mac-policy FW-0 id 2 [from/to] <Laptop mac addr> action [permit/deny]”  “mac-policy FW-0 id 3 [from/to] <Laptop mac addr> action [permit/deny]”  “…..”  “mac-policy FW-X”  “mac-policy FW-X id 1 [from/to] <Laptop mac addr> action [permit/deny]”  “mac-policy FW-X id 2 [from/to] <Laptop mac addr> action [permit/deny]”  “mac-policy FW-X id 3 [from/to] <Laptop mac addr> action [permit/deny]”  ~~“user-profile FW-[N] security mac-policy [from/to]-access FW-[N]”~~  ~~“ssid ssid[N] default-user-profile-attr [num]”~~   1. Show the running config and check the resource consuming | | |
| Expect result | - Config full policy,and bind to user-pofile successfully, and the running config shows the config-policies and binding-relation correctly , the cpu & mem’s using are normal on step 2). | | |
| Test result |  | | |

# 8. IP-policy Testcase

## 8.1 Single “from || to” policy test

* Case ID FW\_IP\_Policy\_Fun\_1

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.1 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config single “from” policy(permit) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop ping gateway of SW 2. Laptop ping Server 3. Laptop ping AP1 4. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop ip addr> action permit”  “user-profile FW security ip-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1-3 | | |
| Expect result | - Laptop ping successfully on step 1), 2) and 3)  - Laptop ping successfully on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.2 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config single “from” policy(deny) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop ping gateway of SW 2. Laptop ping Server 3. Laptop ping AP1 4. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop ip addr> action deny”  “user-profile FW security ip-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1-3 | | |
| Expect result | - Laptop ping successfully on step 1), 2) and 3)  - Laptop ping unsuccessfully on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.3 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Delete a config-single “from” policy(deny/permit) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop ping gateway of SW 2. Laptop ping Server 3. Laptop ping AP1 4. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop ip addr> action [deny/permit]”  “user-profile FW security ip-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Delete the config policy   “no user-profile FW security ip-policy from-access”  “no ip-policy FW id [num]”   1. Repeat step 1-3. | | |
| Expect result | -Laptop ping successfully on step 1), 2) and 3)  -If action is deny, Laptop ping unsuccessfully on step 5),else Laptop ping successfully on step 5)  - Laptop ping successfully on step 6) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.4 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config single “to” policy(permit) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Gateway of SW ping Laptop 2. Server ping Laptop 3. AP1 ping Laptop 4. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop ip addr> action permit”  “user-profile FW security ip-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1-3 | | |
| Expect result | - Devices ping successfully on step 1), 2) and 3)  - Devices ping successfully on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.5 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server | | |
| Description | Config single “to” policy(deny) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Gateway of SW ping Laptop 2. Server ping Laptop 3. AP1 ping Laptop 4. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop ip addr> action deny”  “user-profile FW security ip-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1-3 | | |
| Expect result | - Devices ping successfully on step 1), 2) and 3)  - Devices ping unsuccessfully on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.6 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Delete a config-single “to” policy(deny/permit) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Gateway of SW ping Laptop 2. Server ping Laptop 3. AP1 ping Laptop 4. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop ip addr> action [deny/permit]”  “user-profile FW security ip-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Delete the config policy   “no user-profile FW security ip-policy to-access”  “no ip-policy FW id [num]”   1. Repeat step 1-3. | | |
| Expect result | - Devices ping successfully on step 1), 2) and 3)  - If action is deny, Devices ping unsuccessfully on step 5),else Devices ping successfully on step 5)  - Devices ping successfully on step 6) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.7 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Config single “from” policy(permit) on AP1, one Laptop ping another through AP1 | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 ping Laptop2 2. Configure a ip-policy and bind it to user-profile:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 2. Clear ip-session table, then Laptop2 ping Laptop1 | | |
| Expect result | - Laptop1 ping successfully on step 1)  - Laptop1 ping successfully on step 3)  - Laptop2 ping unsuccessfully on step 4) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.8 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Config single “from” policy(deny) on AP1, one Laptop ping another through AP1 | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 ping Laptop2 2. Configure a ip-policy and bind it to user-profile:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 2. Laptop2 ping Laptop1 | | |
| Expect result | - Laptop1 ping successfully on step 1)  - Laptop1 ping unsuccessfully on step 3)  - Laptop2 ping successfully on step 4) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.9 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Delete a config-single “from” policy(deny/permit) on AP1, one Laptop ping another through AP1 | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 ping Laptop2 2. Configure a ip-policy and bind it to user-profile:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action deny/permit”  “user-profile FW security ip-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 2. Delete the config policy   “no user-profile FW security ip-policy from-access”  “no ip-policy FW id [num]”   1. Repeat step 1 2. Laptop2 ping Laptop1 | | |
| Expect result | - Laptop1 ping successfully on step 1)  - If action is deny,Laptop1 ping unsuccessfully on step 3),else Laptop1 ping successfully on step 3)  - Laptop1 ping successfully on step 5)  - Laptop2 ping successfully on step 6) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.10 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Config single “to” policy(permit) on AP1, one Laptop ping another through AP1 | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 ping Laptop2 2. Configure a ip-policy and bind it to user-profile:   “ip-policy FW”  “ip-policy FW to <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy to-access FW”   1. Repeat step 1 2. Laptop2 ping Laptop1 | | |
| Expect result | - Laptop1 ping successfully on step 1)  - Laptop1 cannot ping successfully on step 3)  - Laptop2 ping successfully on step 4) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.11 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Config single “to” policy(deny) on AP1, one Laptop ping another through AP1 | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 ping Laptop2 2. Configure a ip-policy and bind it to user-profile:   “ip-policy FW”  “ip-policy FW to <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 2. Laptop2 ping Laptop1 | | |
| Expect result | - Laptop1 ping successfully on step 1)  - Laptop1 ping successfully on step 3)  - Laptop2 ping unsuccessfully on step 4) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.12 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Delete a config-single “to” policy(deny/permit) on AP1, one Laptop ping another through AP1 | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 ping Laptop2 2. Configure a ip-policy and bind it to user-profile:   “ip-policy FW”  “ip-policy FW to <Laptop1 ip addr> action [deny/permit]”  “user-profile FW security ip-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 2. Laptop2 ping Laptop1 3. Delete the config policy   “no user-profile FW security ip-policy to-access”  “no ip-policy FW id [num]”   1. Repeat step 1 2. Laptop2 ping Laptop1 | | |
| Expect result | - Laptop1 ping successfully on step 1)  - Laptop1 ping successfully on step 3)  - Laptop2 ping unsuccessfully on step 4)  - Laptop1 ping successfully on step 6)  - Laptop2 ping successfully on step 7) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.13 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Change the policy from permit to deny (“from-access”) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop ping gateway of SW 2. Laptop ping Server 3. Laptop ping AP1 4. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop ip addr> action permit”  “user-profile FW security ip-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1-3 2. Change the policy from permit to deny   “ip-policy FW from <Laptop ip addr> action deny”   1. Repeat step 1-3 | | |
| Expect result | - Laptop ping successfully on step 1), 2) and 3)  - Laptop ping successfully on step 5)  - Laptop ping unsuccessfully on step 7) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.14 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Change the policy from deny to permit (“from-access”) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop ping gateway of SW 2. Laptop ping Server 3. Laptop ping AP1 4. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop ip addr> action deny”  “ip-profile FW security ip-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1-3 2. Change the policy from permit to deny   “ip-policy FW from <Laptop ip addr> action permit”   1. Repeat step 1-3 | | |
| Expect result | - Laptop ping successfully on step 1), 2) and 3)  - Laptop ping unsuccessfully on step 5)  - Laptop ping successfully on step 7) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.15 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Change the policy from permit to deny (“to-access”) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. gateway of SW ping Laptop 2. Server ping Laptop 3. AP1 ping Laptop 4. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop ip addr> action permit”  “user-profile FW security ip-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1-3 2. Change the policy from permit to deny   “ip-policy FW to <Laptop ip addr> action deny”   1. Repeat step 1-3 | | |
| Expect result | - Devices ping successfully on step 1), 2) and 3)  - Devices ping successfully on step 5)  - Devices ping unsuccessfully on step 7) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.16 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Change the policy from deny to permit (“to-access”) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. gateway of SW ping Laptop 2. Server ping Laptop 3. AP1 ping Laptop 4. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop ip addr> action deny”  “user-profile FW security ip-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1-3 2. Change the policy from permit to deny   “ip-policy FW to <Laptop ip addr> action permit”   1. Repeat step 1-3 | | |
| Expect result | - Devices ping successfully on step 1), 2) and 3)  - Devices ping unsuccessfully on step 5)  - Devices ping successfully on step 7) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.17 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ MP ------ Laptop2  |  SW | | |
| Description | Config single “from” policy(permit, through MP) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 ping Laptop2 each other 2. Configure a ip-policy on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action permit”  “ip-profile FW security ip-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | - All ping are successful on step 1)  - All ping are successful on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.18 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ MP ------ Laptop2  |  SW | | |
| Description | Config single “from” policy(deny, through MP) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 ping Laptop2 each other 2. Configure a ip-policy on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action deny”  “ip-profile FW security ip-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | - All ping are successful on step 1)  - Laptop1 ping unsuccessfully, Laptop2 ping successfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.19 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ MP ------ Laptop2  |  SW | | |
| Description | Delete a config-single “from” policy(deny/permit,through MP) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 ping Laptop2 each other 2. Configure a ip-policy on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action [permit/deny]”  “user-profile FW security ip-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 2. Delete the config policy   “no user-profile FW security ip-policy from-access”  “no ip-policy FW id [num]”   1. Repeat step 1. | | |
| Expect result | -All ping are successful on step 1)  -If action is deny, Laptop1 ping unsuccessfully, Laptop2 ping successful ; else All ping are successful on step 3)  - All ping are successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.20 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ MP ------ Laptop2  |  SW | | |
| Description | Config single “to” policy(permit, through MP) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 ping Laptop2 each other 2. Configure a ip-policy on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | - All ping are successful on step 1)  - All ping are successful on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.21 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ MP ------ Laptop2  |  SW | | |
| Description | Config single “to” policy(deny, through MP) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 ping Laptop2 each other 2. Configure a L2 policy on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | - All ping are successful on step 1)  - Laptop1 ping successfully, Laptop2 ping unsuccessfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.22 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ MP ------ Laptop2  |  SW | | |
| Description | Delete a config-single “to” policy(deny/permit,through MP) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 ping Laptop2 each other 2. Configure a ip-policy on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop1 ip addr> action [permit/deny]”  “user-profile FW security ip-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 2. Delete the config policy   “no user-profile FW security ip-policy to-access”  “no ip-policy FW id [num]”   1. Repeat step 1. | | |
| Expect result | -All ping are successful on step 1)  -If action is deny, Laptop2 ping unsuccessfully, Laptop1 ping successful ; All ping are successful on step 3)  - All ping are successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.23 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ MP (eth0)------ Laptop2  |  SW | | |
| Description | Set eth port access,check the ip-policy(“from-permit”, through MP) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Configure a ip-policy which permit Laptop2’s ip-address on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop2 ip addr> action permit”  “user-profile FW security ip-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop2 ping Laptop1 2. Check the ip-session table on MP | | |
| Expect result | - Laptop2 ping successfully on step 2)  - There is a ip-session between Laptop2 and Laptop1 on MP on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.24 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ MP (eth0)------ Laptop2  |  SW | | |
| Description | Set eth port access,check the ip-policy(“from-deny”, through MP) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Configure a ip-policy which deny Laptop2’s ip-address on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop2 ip addr> action deny”  “user-profile FW security ip-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop2 ping Laptop1 2. Check the ip-session table on MP | | |
| Expect result | - Laptop2 ping unsuccessfully on step 2)  - There is no ip-session between Laptop2 and Laptop1 on MP on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.25 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ MP (eth0)------ Laptop2  |  SW | | |
| Description | Set eth port access,check the ip-policy(“to-permit”, through MP) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Configure a ip-policy which permit Laptop2’s ip-address on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop2 ip addr> action permit”  “user-profile FW security ip-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop1 ping Laptop2 2. Check the ip-session table on MP | | |
| Expect result | - Laptop1 ping successfully on step 2)  - There is a ip-session between Laptop2 and Laptop1 on MP on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.26 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ MP (eth0)------ Laptop2  |  SW | | |
| Description | Set eth port access,check the ip-policy(“to-deny”, through MP) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Configure a ip-policy which deny Laptop2’s ip-address on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop2 ip addr> action deny”  “user-profile FW security ip-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop1 ping Laptop2 2. Check the ip-session table on MP | | |
| Expect result | - Laptop1 ping unsuccessfully on step 2)  - There is no ip-session between Laptop2 and Laptop1 on MP on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.27 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config single “from” policy(related mgt0) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Configure a ip-policy which deny Laptop2’s ip-address on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop2 ip addr> action [permit/deny]”  “user-profile FW security ip-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop and AP1 ping each other | | |
| Expect result | - All pings are successful on step 1)  - If policy is deny, Laptop pings unsuccessfully, AP1 pings successfully; else all pings are successful on step 2) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.28 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config single “to” policy(related mgt0) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Configure a ip-policy which deny Laptop2’s ip-address on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop2 ip addr> action [permit/deny]”  “user-profile FW security ip-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop and AP1 ping each other | | |
| Expect result | - All pings are successful on step 1)  - If policy is deny, Laptop pings successfully, AP1 pings unsuccessfully; else all pings are successful on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.29 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ (eth0)AP1 ------ SW ------ Server | | |
| Description | Config single “from” policy(related mgt0, through eth0) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Configure a ip-policy which deny Laptop2’s ip-address on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop2 ip addr> action [permit/deny]”  “user-profile FW security ip-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop and AP1 ping each other | | |
| Expect result | - All pings are successful on step 1)  - If policy is deny, Laptop pings unsuccessfully, AP1 pings successfully; else all pings are successful on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.30 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ (eth0)AP1 ------ SW ------ Server | | |
| Description | Config single “to” policy(related mgt0, through eth0) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Configure a ip-policy which deny Laptop2’s ip-address on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop2 ip addr> action [permit/deny]”  “user-profile FW security ip-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop and AP1 ping each other | | |
| Expect result | - All pings are successful on step 1)  - If policy is deny, Laptop pings successfully, AP1 pings unsuccessfully; else all pings are successful on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.31 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | PC1+++++(eth0) AP1 (eth1)+++++ SW ++++ PC2 | | |
| Description | Config single “from” policy from ethx to ethx | | |
| Pre-condition | -PC1 has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. PC1 and PC2 ping each other 2. Configure a ip policy and bind it to FW:   “ip-policy FW”  “ip-policy FW from <pc1 ip addr> action [permit/deny]”  “user-profile FW security ip-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | - All pings are successful on step 1)  - If policy is deny, pc2 pings successfully, pc1 pings unsuccessfully; else all pings are successful on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_1.32 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | PC1+++++(eth0) AP1 (eth1)+++++ SW ++++ PC2 | | |
| Description | Config single “to” policy from ethx to ethx | | |
| Pre-condition | -PC1 has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. PC1 and PC2 ping each other 2. Configure a ip policy and bind it to FW:   “ip-policy FW”  “ip-policy FW to <pc1 ip addr> action [permit/deny]”  “user-profile FW security ip-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | - All pings are successful on step 1)  - If policy is deny, pc1 pings successfully, pc2 pings unsuccessfully; else all pings are successful on step 3) | | |
| Test result |  | | |

## 8.2 “From & To” policy simultaneous test

* Case ID FW\_IP\_Policy\_Fun\_2

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_2.1 | | |
| **Priority** | Accept | **Automation Flag** | Yes |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config “from & to” simultaneous policy(permit) | | |
| Pre-condition | -Configure AP1  *“security-object FWtest”*  *“security-object FWtest default-user-profile-attr 1”*  *“ssid FWtest”*  *“ssid FWtest security-object FWtest”*  *“interface wifi0 ssid FWtest”*  *“interface wifi1 ssid FWtest”*  *“user-profile FW qos-policy def-user-qos vlan-id <mgt0 vlan> attribute 1”*  -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop and gateway of SW ping each other through AP1 2. Laptop and Server ping each other through AP1 3. Laptop and AP1 ping each other 4. Configure a ip-policy and bind it to FW:   ***“ip-policy FW”***  ***“ip-policy FW from <Laptop ip addr> action permit”***  ***“ip-policy FW to <Laptop ip addr> action permit”***  ***“user-profile FW security ip-policy from-access FW to-access FW***  ***“clear forwarding-engine ip-sessions”***   1. Repeat step 1-3 | | |
| Expect result | -All ping successfully on step 1), 2) and 3)  -All ping successfully on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_2.2 | | |
| **Priority** | Accept | **Automation Flag** | Yes |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config “from & to” simultaneous policy(deny) | | |
| Pre-condition | -Configure AP1  *“security-object FWtest”*  *“security-object FWtest default-user-profile-attr 1”*  *“ssid FWtest”*  *“ssid FWtest security-object FWtest”*  *“interface wifi0 ssid FWtest”*  *“interface wifi1 ssid FWtest”*  *“user-profile FW qos-policy def-user-qos vlan-id <mgt0 vlan> attribute 1”*  -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop and gateway of SW ping each other through AP1 2. Laptop and Server ping each other through AP1 3. Laptop and AP1 ping each other 4. Configure a ip-policy and bind it to FW:   ***“ip-policy FW”***  ***“ip-policy FW from <Laptop ip addr> action deny”***  ***“ip-policy FW to <Laptop ip addr> action deny”***  ***“ip-policy FW action permit”***  ***“user-profile FW security ip-policy from-access FW to-access FW***  ***“clear forwarding-engine ip-sessions”***   1. Repeat step 1-3 | | |
| Expect result | -All ping are successful on step 1), 2) and 3)  -All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_2.3 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config “from & to” simultaneous policy(from permit, to deny) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop and gateway of SW ping each other through AP1 2. Laptop and Server ping each other through AP1 3. Laptop and AP1 ping each other 4. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop ip addr> action permit”  “ip-policy FW to <Laptop ip addr> action deny”  “user-profile FW security ip-policy from-access FW to-access FW  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1-3 | | |
| Expect result | -All ping are successful on step 1), 2) and 3)  -Laptop’s ping are all successful; Devices’ ping to Laptop are all unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_2.4 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config “from & to” simultaneous policy(from deny, to permit) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop and gateway of SW ping each other through AP1 2. Laptop and Server ping each other through AP1 3. Laptop and AP1 ping each other 4. Configure a ip- policy and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop ip addr> action deny”  “mac-policy FW to <Laptop ip addr> action permit”  “user-profile FW security ip-policy from-access FW to-access FW  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1-3 | | |
| Expect result | -All ping are successful on step 1), 2) and 3)  -Laptop’s ping are all unsuccessful; Devices’ ping to Laptop are all successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_2.5 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Config “from & to” simultaneous policy(permit, two Laptops) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other through AP1 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action permit”  “ip-policy FW to <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy from-access FW to-access FW  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | -All ping successfully on step 1)  -All ping successfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_2.6 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Config “from & to” simultaneous policy(deny, two Laptops) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other through AP1 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action deny”  “ip-policy FW to <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy from-access FW to-access FW  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | -All ping successfully on step 1)  -All ping unsuccessfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_2.7 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Config “from & to” simultaneous policy(from permit, to deny, two Laptops) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other through AP1 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action permit”  “ip-policy FW to <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy from-access FW to-access FW  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | -All ping successfully on step 1)  -Laptop1 ping successfully, Laptop2 ping unsuccessfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_2.8 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Config “from & to” simultaneous policy(from deny, to permit, two Laptops) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other through AP1 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action deny”  “ip-policy FW to <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy from-access FW to-access FW  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | -All ping successfully on step 1)  -Laptop1 ping unsuccessfully, Laptop2 ping successfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_2.9 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ MP ------ Laptop2  |  SW | | |
| Description | Config “from & to” simultaneous policy(permit, through MP) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other through MP 2. Configure a ip-policy on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action permit”  “ip-policy FW to <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy from-access FW to-access FW  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | -All ping successfully on step 1)  -All ping successfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_2.10 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ MP ------ Laptop2  |  SW | | |
| Description | Config “from & to” simultaneous policy(deny, through MP) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other through MP 2. Configure a ip-policy on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action deny”  “ip-policy FW to <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy from-access FW to-access FW  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | -All ping successfully on step 1)  -All ping unsuccessfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_2.11 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ MP ------ Laptop2  |  SW | | |
| Description | Config “from & to” simultaneous policy(from permit, to deny, through MP) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other through MP 2. Configure a ip-policy on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action permit”  “ip-policy FW to <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy from-access FW to-access FW  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | -All ping successfully on step 1)  - Laptop1 ping successfully, Laptop2 ping unsuccessfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_2.12 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ MP ------ Laptop2  |  SW | | |
| Description | Config “from & to” simultaneous policy(from deny, to permit, through MP) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other through MP 2. Configure a ip-policy on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action deny”  “ip-policy FW to <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy from-access FW to-access FW  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | -All ping successfully on step 1)  - Laptop1 ping unsuccessfully, Laptop2 ping successfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_2.13 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ Laptop2  |  SW | | |
| Description | Config “from & to” simultaneous policy(config “from” policy but bind it to “to” direction) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other through AP1 2. Configure a L3 policy on AP1 and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | -All ping successfully on step 1)  - Laptop1 ping successfully, Laptop2 ping unsuccessfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_2.14 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ Laptop2  |  SW | | |
| Description | Config “from & to” simultaneous policy(config “to” policy but bind it to “from” direction) | | |
| Pre-condition | -Laptop1 has been associated with AP1 and assigned an ip address  -Laptop1 uses user-profile “FW” | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other through AP1 2. Configure a L3 policy on AP1 and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 | | |
| Expect result | -All ping successfully on step 1)  - Laptop1 ping unsuccessfully, Laptop2 ping successfully on step 3) | | |
| Test result |  | | |

## 8.3 Order of rules test

* Case ID FW\_IP\_Policy\_Fun\_3

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_3.1 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | IP-policy “after” attribute, using from policy. | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 ping Laptop2 2. Configure multi-policy in a IP-policy and bind it to user-profile:   “ip-policy FW”  “ip-policy FW id 1 from <Laptop1 ip addr> action permit”  “ip-policy FW id 2 from <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 2. Laptop2 ping Laptop1 3. Use the after attribute to change the sequence of id 1 and id 2   “ip-policy FW id 1 after id 2”   1. Show the running config 2. Repeat step 1 3. Laptop2 ping Laptop1 | | |
| Expect result | - Laptop1 ping successfully on step 1)  - Laptop1 ping successfully on step 3)  - Laptop2 ping successfully on step 4)  -The running config shows that the id 2 policy is before id 1 in ip-policy FW.  - Laptop1 ping unsuccessfully on step 7)  - Laptop2 ping successfully on step 8) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_3.2 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | IP-policy “after” attribute, using to policy. | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 ping Laptop2 2. Configure multi-policy in a ip-policy and bind it to user-profile:   “ip-policy FW”  “ip-policy FW id 1 to <Laptop1 ip addr> action permit”  “ip-policy FW id 2 to <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 2. Laptop2 ping Laptop1 3. Use the after attribute to change the sequence of id 1 and id 2   “ip-policy FW id 1 after id 2”   1. Show the running config 2. Repeat step 1 3. Laptop2 ping Laptop1 | | |
| Expect result | - Laptop1 ping successfully on step 1)  - Laptop1 ping successfully on step 3)  - Laptop2 ping successfully on step 4)  -The running config shows that the id 2 policy is before id 1 in ip-policy FW.  - Laptop1 ping successfully on step 7)  - Laptop2 ping unsuccessfully on step 8) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_3.3 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | IP-policy “after” attribute, using coveraged policy. | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 ping Laptop2 2. Configure multi-policy in a ip-policy and bind it to user-profile:   “ip-policy FW”  “ip-policy FW id 1 from <Laptop1 ip addr> action permit”  “ip-policy FW id 2 to <Laptop1 ip addr> action permit”  “ip-policy FW id 3 action deny”  “user-profile FW security ip-policy from-access FW to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 2. Laptop2 ping Laptop1 3. Use the after attribute to change the sequence of id 1 and id 3   “ip-policy FW id 1 after id 3”   1. Show the running config 2. Repeat step 1 3. Laptop2 ping Laptop1 4. Use the after attribute to change the sequence of id 2 and id 3   “ip-policy FW id 2 after id 3”   1. Show the running config 2. Repeat step 1 3. Laptop2 ping Laptop1 | | |
| Expect result | - Laptop1 ping successfully on step 1)  - Laptop1 ping successfully on step 3)  - Laptop2 ping successfully on step 4)  -The running config shows that the id 3 policy is before id 1 in ip-policy FW. And the id 2 policy is on the top.  - Laptop1 ping unsuccessfully on step 7)  - Laptop2 ping successfully on step 8)  - The running config shows that the id 3 policy is before id 2 in ip-policy FW. And the id 3 policy is on the top.on step 10)  - Laptop1 ping unsuccessfully on step 11)  - Laptop2 ping unsuccessfully on step 12) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_3.4 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | IP-policy “before” attribute, using from policy. | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 ping Laptop2 2. Configure multi-policy in a ip-policy and bind it to user-profile:   “ip-policy FW”  “ip-policy FW id 1 from <Laptop1 ip addr> action permit”  “ip-policy FW id 2 from <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 2. Laptop2 ping Laptop1 3. Use the after attribute to change the sequence of id 1 and id 2   “ip-policy FW id 2 before id 1”   1. Show the running config 2. Repeat step 1 3. Laptop2 ping Laptop1 | | |
| Expect result | - Laptop1 ping successfully on step 1)  - Laptop1 ping successfully on step 3)  - Laptop2 ping successfully on step 4)  -The running config shows that the id 2 policy is before id 1 in ip-policy FW.  - Laptop1 ping unsuccessfully on step 7)  - Laptop2 ping successfully on step 8) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_3.5 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | IP-policy “before” attribute, using to policy. | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 ping Laptop2 2. Configure multi-policy in a ip-policy and bind it to user-profile:   “ip-policy FW”  “ip-policy FW id 1 to <Laptop1 ip addr> action permit”  “ip-policy FW id 2 to <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 2. Laptop2 ping Laptop1 3. Use the after attribute to change the sequence of id 1 and id 2   “ip-policy FW id 2 before id 1”   1. Show the running config 2. Repeat step 1 3. Laptop2 ping Laptop1 | | |
| Expect result | - Laptop1 ping successfully on step 1)  - Laptop1 ping successfully on step 3)  - Laptop2 ping successfully on step 4)  -The running config shows that the id 2 policy is before id 1 in ip-policy FW.  - Laptop1 ping successfully on step 7)  - Laptop2 ping unsuccessfully on step 8) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_3.6 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | IP-policy “before” attribute, using coveraged policy. | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 ping Laptop2 2. Configure multi-policy in a ip-policy and bind it to user-profile:   “ip-policy FW”  “ip-policy FW id 1 from <Laptop1 ip addr> action permit”  “ip-policy FW id 2 to <Laptop1 ip addr> action permit”  “ip-policy FW id 3 action deny”  “user-profile FW security ip-policy from-access FW to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Repeat step 1 2. Laptop2 ping Laptop1 3. Use the after attribute to change the sequence of id 2 and id 3   “ip-policy FW id 3 before id 2”   1. Show the running config 2. Repeat step 1 3. Laptop2 ping Laptop1 4. Use the after attribute to change the sequence of id 1 and id 3   “ip-policy FW id 3 before id 1”   1. Show the running config 2. Repeat step 1 3. Laptop2 ping Laptop1 | | |
| Expect result | - Laptop1 ping successfully on step 1)  - Laptop1 ping successfully on step 3)  - Laptop2 ping successfully on step 4)  -The running config shows that the id 3 policy is before id 2 in ip-policy FW. And the id 1 policy is on the top on step 6).  - Laptop1 ping successfully on step 7)  - Laptop2 ping unsuccessfully on step 8)  - The running config shows that the id 3 policy is before id 1 in ip-policy FW. And the id 3 policy is on the top on step 10).  - Laptop1 ping unsuccessfully on step 11)  - Laptop2 ping unsuccessfully on step 12) | | |
| Test result |  | | |

## 8.4 Regular session test

* Case ID FW\_IP\_Policy\_Fun\_4

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_4.1 | | |
| **Priority** | Accept | **Automation Flag** | Yes |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | IP-session setup. | | |
| Pre-condition | -Configure AP1  *“security-object FWtest”*  *“security-object FWtest default-user-profile-attr 1”*  *“ssid FWtest”*  *“ssid FWtest security-object FWtest”*  *“interface wifi0 ssid FWtest”*  *“interface wifi1 ssid FWtest”*  *“user-profile FW qos-policy def-user-qos vlan-id <mgt0 vlan> attribute 1”*  -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config ip-policy which permit Laptop’s ip\_address   ***“ip-policy FW”***  ***“ip-policy FW to <Laptop ip addr> action permit”***  ***“user-profile FW security ip-policy to-access FW”***  ***“clear forwarding-engine ip-sessions”***   1. Server ping Laptop 2. Check the ip-session table on AP1   ***“show forwarding-engine ip-sessions”***   1. Clear ip-session table, delete the ip-policy and reconfig ip-policy deny the traffic from and to Laptop   ***“no ip-policy FW”***  ***“ip-policy FW”***  ***“ip-policy FW to <Laptop ip addr> action deny”***  ***“user-profile FW security ip-policy to-access FW”***  ***“clear forwarding-engine ip-sessions”***   1. Server ping Laptop 2. Check the ip-session table on AP1   ***“show forwarding-engine ip-sessions”*** | | |
| Expect result | - Server ping successfully on step 2)  - There is a ip-session established between Server and Laptop on AP1 on step 3)  - Server ping unsuccessfully on step 5)  - There is no ip-session between Server and Laptop on step 6) | | |
| Test result | AH-958280#show forwarding-engine ip-sessions  IP session table:  Ageout time (in ms)  Total entries: 2/8191  Id:2; Ageout:4800; Flags:0x24200; QOS:2; Up: 0 min 2 sec; InPol:fw/2;  10.2.2.12/4112 -> 10.2.2.10/4112; Proto 1; Flg:0x122; Pkts:3 Bytes:252 Parent-MAC-Sess: 12  10.2.2.10/4112 -> 10.2.2.12/3; Proto 1; Flg:0x100; Pkts:3 Bytes:252 | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_4.2 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | IP-session delete.(timeout) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config ip-policy which permit Laptop’s ip\_address   “ip-policy FW”  “ip-policy FW from/to <Laptop ip addr> action permit”  “user-profile FW security ip-policy from/to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Server and Laptop ping each other 10 times 2. Check the ip-session table on AP1 during pinging 3. After the default age out time, check the ip-session table on AP1 | | |
| Expect result | -We can see ip-session between Laptop and server in step 3)  - The ip-session is age out on step 4) | | |
| Test result | 2012-07-13 09:17:30 debug kernel: [fe]: invalidate IP sess (2) for (2) seconds, reason (ageout)  2012-07-13 09:17:32 debug kernel: [fe]: delete IP sess id [2] | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_4.3 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | IP-session delete.(eth port [which links Server] down) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config ip-policy which permit Laptop’s ip\_address   “ip-policy FW”  “ip-policy FW from/to <Laptop ip addr> action permit”  “user-profile FW security ip-policy from/to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Server ping Laptop 2. Check the ip-session table on AP1 3. Config the eth port down or unplug the cable   “int eth[X] shutdown”   1. Check the ip-session table on AP1(after aging-time) | | |
| Expect result | - Server ping successfully on step 2)  - There is a ip-session established between Server and Laptop on AP1 on step 3)  - The ip-session is deleted on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_4.4 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | IP-session delete.(eth port [which links Server] mode change) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config ip-policy which permit Laptop’s ip\_address   “ip-policy FW”  “ip-policy FW from/to <Laptop ip addr> action permit”  “user-profile FW security ip-policy from/to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Server ping Laptop 2. Check the ip-session table on AP1 3. Change the eth port mode AP1   “intface eth[X] mode [backhaul|bridge-access]”   1. Check the ip-session table on AP1 | | |
| Expect result | - Server ping successfully on step 2)  - There is a ip-session between Server and Laptop on AP1 on step 3)  - The ip-session is deleted on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| ~~Case ID~~ | ~~FW\_IP\_Policy\_Fun\_4.5~~ | | |
| **~~Priority~~** | ~~High~~ | **~~Automation Flag~~** | ~~NA~~ |
| ~~Topology to use~~ | ~~Laptop ------ AP1 ------ SW ------ Server~~ | | |
| ~~Description~~ | ~~IP-session delete.(wifi port [which links Laptop] mode change)~~ | | |
| ~~Pre-condition~~ | ~~-Laptop has been associated with AP1 and assigned an ip address~~  ~~-Laptop uses user-profile “FW”~~ | | |
| ~~Test procedure~~ | 1. ~~Config ip-policy which permit Laptop’s ip\_address~~   ~~“ip-policy FW”~~  ~~“ip-policy FW from/to <Laptop ip addr> action permit”~~  ~~“user-profile FW security ip-policy from/to-access FW”~~  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. ~~Server ping Laptop~~ 2. ~~Check the ip-session table on AP1~~ 3. ~~Change the wifi port mode AP1~~   ~~“intface wifi[X] mode backhaul”~~   1. ~~Check the ip-session table on AP1~~ | | |
| ~~Expect result~~ | ~~- Server ping successfully on step 2)~~  ~~- There is a ip-session between Server and Laptop on AP1 on step 3)~~  ~~- The ip-session is deleted on step 5)~~ | | |
| ~~Test result~~ |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_4.6 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | IP-session delete.(Laptop go away) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config ip-policy which permit Laptop’s ip\_address   “ip-policy FW”  “ip-policy FW from/to <Laptop ip addr> action permit”  “user-profile FW security ip-policy from/to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Server ping Laptop 2. Check the ip-session table on AP1 3. Move the Laptop out range of the AP1 4. Check the ip-session table on AP1 | | |
| Expect result | - Server ping successfully on step 2)  - There is a ip-session between Server and Laptop on AP1 on step 3)  - The ip-session is deleted on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_4.7 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | IP-session delete.(using cmd) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config ip-policy which permit Laptop’s ip\_address   “ip-policy FW”  “ip-policy FW from/to <Laptop ip addr> action permit”  “user-profile FW security ip-policy from/to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Server ping Laptop 2. Check the ip-session table on AP1 3. Delete the ip-session by cmd   “clear forward-engine ip-session id [X]”   1. Check the ip-session table on AP1 | | |
| Expect result | - Server ping successfully on step 2)  - There is a ip-session between Server and Laptop on AP1 on step 3)  - The ip-session is deleted on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_4.8 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | IP-session delete.(ssid shutdown) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config ip-policy which permit Laptop’s ip\_address   “ip-policy FW”  “ip-policy FW from/to <Laptop ip addr> action permit”  “user-profile FW security ip-policy from/to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Server ping Laptop 2. Check the ip-session table on AP1 3. Shutdown the ssid by cmd   “intface wifi[num] ssid <ssid\_name> shutdown”   1. Check the ip-session table on AP1 | | |
| Expect result | - Server ping successfully on step 2)  - There is a ip-session between Server and Laptop on AP1 on step 3)  - The ip-session is deleted on step 5) | | |
| Test result | “invalidate MAC sess (1) for (35) seconds, reason (station-deletion)”  "invalidate IP sess (2) for (32) seconds, reason (MAC-session-ageout)" | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_4.9 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | IP-session delete.(modify policy conflict with the address in the exsit session) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config ip-policy which permit Laptop’s ip\_address   “ip-policy FW”  “ip-policy FW from/to <Laptop ip addr> action permit”  “user-profile FW security ip-policy from/to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Server ping Laptop 2. Check the ip-session table on AP1 3. Modify the policy which conflict with the address in the exsit session 4. Check the ip-session table on AP1 | | |
| Expect result | - Laptop ping successfully on step 2)  - There is a ip-session between Server and Laptop on AP1 on step 3)  - The ip-session is deleted on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_4.10 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | IP-session delete.(icmp replay packet) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config ip-policy which permit Laptop’s ip\_address   “ip-policy FW”  “ip-policy FW from/to <Laptop ip addr> action permit”  “user-profile FW security ip-policy from/to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Server ping Laptop 2. Check the ip-session table on AP1 3. Check the debug log | | |
| Expect result | - Server ping successfully on step 2)  - There is a ip-session between Server and Laptop on AP1 on step 2)  - The ip-session is deleted after AP1 sees the icmp reply packet on step 4) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_4.11 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | IP-session delete.(tcp 4-way handshake) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config ip-policy which permit Laptop’s ip\_address   “ip-policy FW”  “ip-policy FW from/to <Laptop ip addr> action permit”  “user-profile FW security ip-policy from/to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop accesses server by tcp 2. Check the ip-session table on AP1 3. Laptop logout from server 4. Check the debug log and ip-session | | |
| Expect result | - Laptop accesses Server successfully on step 2)  - There is a ip-session between Server and Laptop on AP1 on step 2)  - The ip-session is deleted after AP1 sees the tcp 4-way handshake on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_4.12 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | IP-session delete.(tcp RST packet) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config ip-policy which permit Laptop’s ip\_address   “ip-policy FW”  “ip-policy FW from/to <Laptop ip addr> action permit”  “user-profile FW security ip-policy from/to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop accesses server by tcp 2. Check the ip-session table on AP1 3. Laptop sends tcp RST packet to server corresponding the former tcp session 4. Check the debug log and ip-session | | |
| Expect result | - Laptop accesses Server successfully on step 2)  - There is a ip-session between Server and Laptop on AP1 on step 2)  - The ip-session is deleted after AP1 sees the tcp RST packet on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_4.13 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | MP ------ AP1 ------ SW ------ Server  | |  Laptop1 Laptop2 | | |
| Description | IP-session setup/delete.(through MP) | | |
| Pre-condition | -Laptop2 has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Config ip-policy on MP which permit Laptop’s ip\_address   “ip-policy FW”  “ip-policy FW from/to <Laptop ip addr> action permit”  “user-profile FW security ip-policy from/to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop1 ping Laptop2 2. Check the ip-session table on MP 3. Shutdown the wifi backhoul of AP1   “intface wifi[num] shutdown”   1. Check the ip-session table on MP 2. Up the wifi backhaul of AP1, repeat step 1 3. Check the ip-session table on MP 4. Shutdown the wifi backhaul of MP   “intface wifi[num] shutdown”   1. Check the ip-session table on MP 2. Up the wifi backhoul of MP, repeat step 1 3. Check the ip-session table on MP 4. Change the wifi backhaul to access on AP1   “intface wifi[num] mode access”   1. Check the ip-session table on MP 2. Change the wifi to backhaul on AP1, repeat step 1 3. Check the ip-session table on MP 4. Change the wifi backhaul to access on MP   “intface wifi[num] mode access”   1. Check the ip-session table on MP | | |
| Expect result | - Laptop1 ping successfully on step 2)  - There is a ip-session between Laptop1 and Laptop2 on MP on step 3)  - The ip-session is deleted on step 5)  - There is a ip-session between Laptop1 and Laptop2 on MP on step 7)  - The ip-session is deleted on step 9)  - There is a ip-session between Laptop1 and Laptop2 on MP on step 11)  - The ip-session is deleted on step 13)  - There is a ip-session between Laptop1 and Laptop2 on MP on step 15)  - The ip-session is deleted on step 17) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_4.14 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | IP-session correlative mgt0 test. (change mgt0’s vlan)(vlan is not the factor of the ip-sessions) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config ip-policy which permit Laptop’s ip\_address   “ip-policy FW”  “ip-policy FW from/to <Laptop ip addr> action permit”  “user-profile FW security ip-policy from/to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Laptop ping AP1 2. Check the ip-session table on AP1 3. Change the mgt0’s vlan attribute   “intface mgt0 vlan [num]”   1. Check the ip-session table on AP1 | | |
| Expect result | - Laptop ping successfully on step 2)  - There is a ip-session between AP1(mgt0) and Laptop on AP1 on step 3)  - The ip-session is deleted on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_4.15 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | IP-session correlative mgt0 test (change mgt0’s ip). | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config ip-policy which permit Laptop’s ip\_address   “ip-policy FW”  “ip-policy FW from/to <Laptop ip addr> action permit”  “user-profile FW security ip-policy from/to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop ping AP1 2. Check the ip-session table on AP1 3. Change the mgt0’s ip   “intface mgt0 ip <ip\_address>”   1. Check the ip-session table on AP1 | | |
| Expect result | - Laptop ping successfully on step 2)  - There is a ip-session between AP1(mgt0) and Laptop on AP1 on step 3)  - The ip-session is deleted on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_4.16 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | IP-session correlative mgt0 test (delete mgt0’s ip). | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config ip-policy which permit Laptop’s ip\_address   “ip-policy FW”  “ip-policy FW from/to <Laptop ip addr> action permit”  “user-profile FW security ip-policy from/to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop ping AP1 2. Check the ip-session table on AP1 3. Delete the mgt0’s ip   “no intface mgt0 ip”   1. Check the ip-session table on AP1 | | |
| Expect result | - Laptop ping successfully on step 2)  - There is a ip-session between AP1(mgt0) and Laptop on AP1 on step 3)  - The ip-session is deleted on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_4.17 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | IP-session correlative mgt0 test (packet with error vlan). | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config ip-policy which permit Laptop’s ip\_address   “ip-policy FW”  “ip-policy FW from/to <Laptop ip addr> action permit”  “user-profile FW security ip-policy from/to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop ping AP1 2. Check the ip-session table on AP1 3. Send packet to AP1 which is corresponding the session between AP1 and Laptop but the vlan using tools 4. Check the packet information on AP1 | | |
| Expect result | - Laptop ping successfully on step 2)  - There is a ip-session between AP1(mgt0) and Laptop on AP1 on step 3)  - The packet should be dropped cause the wrong vlan on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_4.18 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | IP-session parameters(Proto) test. | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config ip-policy which permit Laptop’s ip\_address   “ip-policy FW”  “ip-policy FW from/to <Laptop ip addr> action permit”  “user-profile FW security ip-policy from/to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop ping AP1 2. Check the ip-session table on AP1 3. Laptop telnet Server 4. Check the ip-session table on AP1 5. Laptop get a file from Server by tftp 6. Check the ip-session table on AP1 | | |
| Expect result | - Laptop ping successfully on step 2)  - There is a ip-session between AP1(mgt0) and Laptop on AP1 on step 3), and the proto value is 1 (icmp)  - There is a ip-session between Server and Laptop on AP1 on step 5), and the proto value is 6 (telnet/tcp)  - There is a ip-session between Server and Laptop on AP1 on step 7), and the proto value is 17 (tftp/udp) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_4.19 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | IP-session parameters(InPol/OutPol) test. | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config ip-policy which permit Laptop’s ip\_address   “ip-policy FW”  “ip-policy FW from/to <Laptop ip addr> action permit”  “user-profile FW security ip-policy from/to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop ping AP1 2. Check the ip-session table on AP1 3. Laptop get/put a file from Server by ftp 4. Check the ip-session table on AP1 | | |
| Expect result | - Laptop ping successfully on step 2)  - There is a ip-session between AP1(mgt0) and Laptop on AP1 on step 3), and the InPol/OutPol value is correct corresponding with the policy id  - There is a ip-session between Server and Laptop on AP1 on step 5), and the InPol/OutPol value is correct corresponding with the policy id | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_4.20 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop-------AP1 ------ SW ------ Server | | |
| Description | IP-session correlative unbinding test. | | |
| Pre-condition | -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config ip-policy which permit Laptop’s ip\_address   “ip-policy FW”  “ip-policy FW from/to <Laptop ip addr> action permit”  “user-profile FW security ip-policy [from/to]-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop ping Server 2. Check the ip-session table on AP1 3. Unbinding the ip-policy   “no user-profile FW security ip-policy [from/to]-access FW”   1. Check the ip-session table on AP1 | | |
| Expect result | - Laptop ping successfully on step 2)  - There is a ip-session between server and Laptop on AP1 on step 3)  - The ip-session is deleted on AP1 on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_4.21 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop-------AP1 ------ SW ------ Server | | |
| Description | IP-session and mac-seesion’s timeout should be the same. | | |
| Pre-condition | -Laptop uses user-profile “FW”  -Make sure Laptop’s ip is different from the subnet of mgt0’s | | |
| Test procedure | 1. Config ip-policy which permit Laptop’s ip\_address   “ip-policy FW”  “ip-policy FW from <Laptop ip addr> to <server ip addr> action nat”  “user-profile FW security ip-policy [from/to]-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop accesses Server by services (telnet,ftp…) 2. Check the timeout of mac-session and ip-session on AP1 3. Define a service using different timeout value 4. Laptop accesses Server by the new define service 5. Check the timeout of mac-session and ip-session on AP1 | | |
| Expect result | - Mac-session and ip-session's timeout should be both corresponding to service's timeout on step 3)  - Mac-session and ip-session's timeout should be both corresponding to service's timeout on step 6) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_4.22 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop-------AP1 ------ SW ------ Server | | |
| Description | IP-session correlative nat. | | |
| Pre-condition | -Laptop uses user-profile “FW”  -Make sure Laptop’s ip is different from the subnet of mgt0’s | | |
| Test procedure | 1. Config ip-policy which permit Laptop’s ip\_address, and action is nat to server   “ip-policy FW”  “ip-policy FW from <Laptop ip addr> to <server ip addr> action nat”  “user-profile FW security ip-policy [from/to]-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop accesses Server by tcp or udp (telnet,ftp…) 2. Check the ip-session table on AP1 | | |
| Expect result | - There is a ip-session which describes between Laptop and server, one direction is Laptop to server, another is server to mgt0 (AP1) on step 3) | | |
| Test result |  | | |

## 8.5 Session syn test

* Case ID FW\_IP\_Policy\_fun\_5

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_5.1 | | |
| **Priority** | Accept | **Automation Flag** | No |
| Topology to use | Laptop-------AP1 ------ SW ------ Server  |  AP2 | | |
| Description | IP-session correlative L2 roaming test. | | |
| Pre-condition | -AP1 and AP2 are in the same vlan  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Make sure AP1 and AP2 with same configures, configure ip-policy permit laptop “from” direction but deny “to” direction 2. Change the radio power max on AP1   “intface wifi[num] radio power 20”   1. Laptop ping Server 2. Check the ip-session table on AP1 and AP2 3. Change the wifi radio power down on AP1, and Change the radio power max on AP1   “intface wifi[num] radio power [num]”   1. Check the ip-session table on AP1 and AP2 | | |
| Expect result | - Laptop ping successfully on step 3)  - There is an ip-session between server and Laptop on AP1 on step 4)  - The ip-session is deleted on AP1, and there is a ip-session between server and Laptop on AP2 on step 6), and make sure it is not a new create session but sync from AP1, through CLI \_kdebug fe sync to see it | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_5.2 | | |
| **Priority** | Accept | **Automation Flag** | No |
| Topology to use | Laptop-------AP1 ------ SW ------ Server  |  AP2 | | |
| Description | IP-session sync with application (ftp/alg) do L2 roaming | | |
| Pre-condition | -AP1 and AP2 are in the different vlan  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Make sure AP1 and AP2 with same configures and in the same vlan, configure ip-policy permit laptop “from” direction but deny “to” direction, and enable ftp alg on both aps 2. Change the radio power max on AP1   “intface wifi[num] radio power 20”   1. Laptop gets large files from Server through ftp 2. Check the ip-session table on AP1 and AP2 3. Change the wifi radio power down on AP1, and Change the radio power max on AP1   “intface wifi[num] radio power [num]”   1. Check the ip-session table on AP1 and AP2 | | |
| Expect result | - Laptop gets files successfully on step 3)  - There are two ip-sessions about ftp and ftp-data between server and Laptop on AP1 on step 4)  - The ip-sessions are deleted on AP1, and there are two ip-sessions about ftp and ftp-data between server and Laptop on AP2 on step 6), and make sure they are not new create sessions but sync from AP1, through CLI \_debug amrp sync to see it, and laptop’s ftp service is ok | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_5.3 | | |
| **Priority** | Accept | **Automation Flag** | No |
| Topology to use | Laptop-------AP1 ------ SW ------ Server  |  AP2 | | |
| Description | IP-session correlative L3 roaming test. | | |
| Pre-condition | -Configure AP1  *security-object cw-330-1*  *security-object cw-330-1 default-user-profile-attr 1*  *ssid cw-330-1*  *ssid cw-330-1 security-object cw-330-1*  *hive caiw*  *interface mgt0 hive caiw*  *interface mgt0 vlan 27*  *interface wifi0 ssid cw-330-1*  *interface wifi1 ssid cw-330-1*  *mobility-policy roaming dnxp*  *user-profile cw-330-1 qos-policy def-user-qos vlan-id 27 mobility-policy roaming attribute 1*  *ip-policy fw*  *ip-policy fw id 1 action permit*  *user-profile cw-330-1 security ip-policy from-access fw to-access fw*  -Configure AP2  *security-object cw-330-1*  *security-object cw-330-1 default-user-profile-attr 1*  *ssid cw-330-1*  *ssid cw-330-1 security-object cw-330-1*  *hive caiw*  *interface mgt0 hive caiw*  *interface mgt0 vlan 28*  *interface wifi0 ssid cw-330-1*  *interface wifi1 ssid cw-330-1*  *mobility-policy roaming dnxp*  *user-profile cw-330-1 qos-policy def-user-qos vlan-id 28 mobility-policy roaming attribute 1*  *ip-policy fw*  *ip-policy fw id 1 action permit*  *user-profile cw-330-1 security ip-policy from-access fw to-access fw* | | |
| Test procedure | 1. Confirm station state on AP1   ***“show station”***   1. Turn on debug on AP1/AP2,Clear session   ***“\_kdebug fe sync”***  ***“clear forwarding-engine ip-sessions”***   1. Laptop ssh to server 2. Check the ip-session table on AP1 and AP2   ***“show forwarding-engine ip-sessions”***   1. Shutdown SSID on AP1   ***“interface wifi0 ssid cw-330-1 shutdown”***  ***“interface wifi1 ssid cw-330-1 shutdown”***   1. Check the ip-session table on AP1 and AP2, look up logs   ***“show forwarding-engine ip-sessions”***   1. Use laptop ssh server to ping ap1 or any other reachable IPaddr | | |
| Expect result | 1.Confirm station is connected to AP1  CW340#show station  Ifname=wifi0.1, Ifindex=13, SSID=cw-330-1:  Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release  -------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------  Ifname=wifi1.2, Ifindex=15, SSID=cw-330-1:  Mac Addr IP Addr Chan Tx Rate Rx Rate Pow(SNR) A-Mode Cipher A-Time VLAN Auth UPID Phymode SM-PS Chan-width Release  -------------- --------------- ---- ------- ------- --- ---------- -------- -------- ---- ---- ---- ------- --------- ---------- -------  2477:0312:d9c0 172.16.118.148 165 52M 6M -104(11) open none 00:04:29 27 Yes 1 11na disabled 20MHz No  You can find the station’mac in this area either wifi0 or wifi1  4.We can find this ip-session as below  AP1  CW320#show forwarding-engine ip-sessions  Id:1; Ageout:7199060; Flags:0x20440; QOS:2; Up: 0 min 1 sec; InPol:fw/1;  172.16.118.148/57596 -> 172.16.130.120/22; Proto 6; Flg:0x102; Pkts:6 Bytes:396 Parent-MAC-Sess: 30  172.16.130.120/22 -> 172.16.118.148/57596; Proto 6; Flg:0x100; Pkts:6 Bytes:600  Id:2; Ageout:99777; Flags:0x20440; QOS:2; Up: 0 min 0 sec; InPol:fw/1;  172.16.118.148/137 -> 172.16.118.255/137; Proto 17; Flg:0x102; Pkts:2 Bytes:156 Parent-MAC-Sess: 22  172.16.118.255/137 -> 172.16.118.148/137; Proto 17; Flg:0x0; Pkts:0 Bytes:0  172.16.118.148 is Laptop’s IPaddr ;172.16.130.120 is Serv’s IPaddr,and you should careful of the Id num(1),we will use it to check logs  AP2 has no Laptop to serv IP-session  6.We can find laptop to serv IP-session in AP2,not AP1  ***AP1 log***  2011-11-15 07:27:42 debug [fe]: send sess sync msg, instance 1 mac 2477:0312:d9c0  2011-11-15 07:27:42 debug [fe]: send ip session from sync 172.16.118.148/137 <-> 172.16.118.255/137, 17, mac sess dir (same)  2011-11-15 07:27:42 debug [fe]: send ip-session (id 2) 172.16.118.148/137 <-> 172.16.118.255/137, proto 17 qos 2, mac-sess dir (same) flag 0x40  2011-11-15 07:27:42 debug [fe]: send mac-session (id 30) 2477:0312:d9c0 (zone backhaul) <-> 3ce5:a64a:768f (zone backhaul), ageout 2 ms  2011-11-15 07:27:42 debug [fe]: send mac sess 2477:0312:d9c0 (zone backhaul) -> 3ce5:a64a:768f (zone backhaul)  2011-11-15 07:27:42 debug [fe]: send ip session from sync 172.16.118.148/57596 <-> 172.16.130.120/22, 6, mac sess dir (same)  2011-11-15 07:27:42 debug [fe]: send ip-session (id 1) 172.16.118.148/57596 <-> 172.16.130.120/22, proto 6 qos 2, mac-sess dir (same) flag 0x40  2011-11-15 07:27:42 debug [fe]: send sess sync of size 240, instance 1  ***AP2 log***  2011-11-15 07:28:46 debug [fe]: recv session sync msg, size 240  2011-11-15 07:28:46 debug [fe]: receive mac sess from sync 2477:0312:d9c0 (zone backhaul) -> ffff:ffff:ffff  2011-11-15 07:28:46 debug [fe]: receive ip session from sync 172.16.118.148/57596 -> 172.16.130.120/22, 6, mac sess dir (same) flag 0x40  2011-11-15 07:28:46 debug [fe]: created ip session from sync 172.16.118.148/57596 <-> 172.16.130.120/22, 6, mac sess dir (reverse) flag 0x420  7.Ping successfully | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_5.4 | | |
| **Priority** | Accept | **Automation Flag** | No |
| Topology to use | Laptop-------AP1 ------ SW ------ Server  |  AP2 | | |
| Description | IP-session sync with application (ftp/alg) do L3 roaming | | |
| Pre-condition | -AP1 and AP2 are in the different vlan  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Make sure AP1 and AP2 with same configures but different vlan, configure ip-policy permit laptop “from” direction but deny “to” direction, and enable ftp alg on both aps 2. Change the radio power max on AP1   “intface wifi[num] radio power 20”   1. Laptop gets large files from Server through ftp 2. Check the ip-session table on AP1 and AP2 3. Change the wifi radio power down on AP1, and Change the radio power max on AP1   “intface wifi[num] radio power [num]”   1. Check the ip-session table on AP1 and AP2 | | |
| Expect result | - Laptop gets files successfully on step 3)  - There are two ip-sessions about ftp and ftp-data between server and Laptop on AP1 on step 4)  - The ip-sessions are deleted on AP1, and there are two ip-sessions about ftp and ftp-data between server and Laptop on AP2 on step 6), and make sure they are not new create sessions but sync from AP1, through CLI \_debug amrp sync to see it, and laptop’s ftp service is ok | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_5.5 | | |
| **Priority** | Accept | **Automation Flag** | No |
| Topology to use | Laptop-------AP1 ------ SW ------ Server  |  AP2 | | |
| Description | IP-session sync with application (TV) do L3 roaming | | |
| Pre-condition | -AP1 and AP2 are in the different vlan  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Make sure AP1 and AP2 with same configures but different vlan, and configure service about TV (default http(tcp 80) on HM), and enable TV alg on both aps, configure TV parameters (class, student and teacher) through HM or hidden CLI, and laptop is a student 2. Change the radio power max on AP1   “intface wifi[num] radio power 20”   1. Laptop accesses web page 2. Check the ip-session table on AP1 and AP2 3. Change the wifi radio power down on AP1, and Change the radio power max on AP1   “intface wifi[num] radio power [num]”   1. Check the ip-session table on AP1 and AP2 | | |
| Expect result | - There is an ip-policy which is created by TV configuration automatically  - Laptop accesses successfully on step 3)  - There are is an ip-sessions about http (tcp 80) between server and Laptop on AP1 on step 4)  - The ip-session is deleted on AP1, and there is an ip-sessions about http (tcp 80) between server and Laptop on AP2 on step 6), and make sure it is not a new create session but sync from AP1, through CLI \_debug amrp sync to see it | | |
| Test result |  | | |

## 8.6 Group IP-Address test

* Case ID FW\_IP\_Policy\_fun\_6

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_6.1 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Group ip-address test (permit) | | |
| Pre-condition | -Laptop1 and Laptop2’s ip-address should be in the same address range, for example their addresses are all in 10.155.30.xx/24 range | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other 2. Laptops and server ping each other 3. Configure a ip-policy using group ip-address which coveraged Laptop1 and Laptop2 and bind it to user-profile:   “ip-policy FW”  “ip-policy FW from <group ip addr> action permit”  “user-profile FW security ip-policy from-access FW to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Show the config 2. Repeat step 1 3. Repeat step 2 4. Configure a ip-policy using group ip-address which coveraged Laptop1 and Laptop2 and bind it to user-profile:   “no ip-policy FW id 1”  “ip-policy FW to <group ip addr> action permit”   1. Show the config 2. Repeat step 1 3. Repeat step 2 | | |
| Expect result | - All ping are successfully on step 1) and 2)  - All ping are successfully on step 5)  - Laptops successful/Server unsuccessfully on step 6)  - All ping are successfully on step 9)  - Laptops unsuccessful/Server successfully on step 6) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_6.2 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Group ip-address test (deny) | | |
| Pre-condition | -Laptop1 and Laptop2’s ip-address should be in the same address range, for example their addresses are all in 10.155.30.xx/24 range | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other 2. Laptops and Server ping each other 3. Configure a ip-policy using group ip-address which coveraged Laptop1 and Laptop2 and bind it to user-profile:   “ip-policy FW”  “ip-policy FW from <group ip addr> action deny”  “user-profile FW security ip-policy from-access FW to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Show the config 2. Repeat step 1-2 3. Configure a ip-policy using group ip-address which coveraged Laptop1 and Laptop2 and bind it to user-profile:   “no ip-policy FW id 1”  “ip-policy FW to <group ip addr> action deny”   1. Show the config 2. Repeat step 1-2 | | |
| Expect result | - All ping are unsuccessfully on step 1) and 2)  - All ping are unsuccessfully on step 5)  - All ping are unsuccessfully on step 8) | | |
| Test result |  | | |

## 8.7 Change policy or binding while traffic is on-going

* Case ID FW\_IP\_Policy\_fun\_7

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.1 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Add/Delete policy while traffic is on-going(from-access permit) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop and gateway of SW ping each other continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop ip addr> action permit”  “user-profile FW security ip-policy from-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the policy config   ~~“no user-profile FW security mac-policy ip-access”~~  “no ip-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- All ping are successful on step 3)~~  ~~- All ping are successful on step 5)~~  1) All ping are successful  3) Laptop ping gateway successfully(from-access id 1 permit), gateway ping laptop unsuccessfully(to-access default deny)  5) All ping are unsuccessful | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.2 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Add/Delete policy while traffic is on-going(from-access deny) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop and gateway of SW ping each other continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop ip addr> action deny”  “user-profile FW security ip-policy from-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the policy config   ~~“no user-profile FW security ip-policy from-access”~~  “no ip-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- Laptop ping unsuccessfully, SW ping successfully on step 3)~~  ~~- All ping are successfu on step 5)~~  1) All ping are successful  3) All ping are unsuccessful  5) All ping are unsuccessful | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.3 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Add/Delete policy while traffic is on-going(from-access permit+deny) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop and gateway of SW ping each other continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop ip addr> action permit”  “user-profile FW security ip-policy from-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Add the deny policy   “ip-policy FW from <Laptop ip addr> action deny”   1. Check the ping pkt 2. Delete the permit policy   ~~“no user-profile FW security ip-policy from-access”~~  “no ip-policy FW id [num=permit policy num]”   1. Check the ping pkt 2. Delete the deny policy   ~~“no user-profile FW security ip-policy from-access”~~  “no ip-policy FW id [num=deny policy num]”   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- All ping are successful on step 3)~~  ~~- All ping are successful on step 5)~~  ~~- Laptop ping unsuccessfully, SW ping successfully on step 7)~~  ~~- All ping are successful on step 9)~~  1) All ping are successful  3) Laptop ping gateway successfully(from-access id 1 permit), gateway ping laptop unsuccessfully(to-access default deny)  5) Laptop ping gateway successfully(from-access id 1 permit), gateway ping laptop unsuccessfully(to-access default deny)  7) All ping are unsuccessful  9) All ping are unsuccessful | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.4 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Add/Delete policy while traffic is on-going(to-access permit) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop and gateway of SW ping each other continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop ip addr> action permit”  “user-profile FW security ip-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the policy config   ~~“no user-profile FW security ip-policy from-access”~~  “no ip-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- All ping are successful on step 3)~~  ~~- All ping are successful on step 5)~~  1) All ping are successful  3) Laptop ping gateway unsuccessfully(from-access default deny), gateway ping laptop successfully(to-access id 1 permit)  5) All ping are unsuccessful | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.5 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Add/Delete policy while traffic is on-going(to-access deny) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop and gateway of SW ping each other continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop ip addr> action deny”  “user-profile FW security ip-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the policy config   ~~“no user-profile FW security ip-policy from-access”~~  “no ip-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- Laptop ping successfully, SW ping unsuccessfully on step 3)~~  ~~- All ping are successful on step 5)~~  1) All ping are successful  3) All ping are unsuccessful  5) All ping are unsuccessful | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.6 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Add/Delete policy while traffic is on-going(to-access permit+deny) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop and gateway of SW ping each other continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop ip addr> action permit”  “user-profile FW security ip-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Add the deny policy   “ip-policy FW to <Laptop ip addr> action deny”   1. Check the ping pkt 2. Delete the permit policy   ~~“no user-profile FW security ip-policy to-access”~~  “no ip-policy FW id [num=permit policy num]”   1. Check the ping pkt 2. Delete the deny policy   ~~“no user-profile FW security ip-policy to-access”~~  “no ip-policy FW id [num=deny policy num]”   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- All ping are successful on step 3)~~  ~~- All ping are successful on step 5)~~  ~~- Laptop ping successfully, SW ping unsuccessfully on step 7)~~  ~~- All ping are successful on step 9)~~  1) All ping are successful  3) Laptop ping gateway unsuccessfully(from-access default deny), gateway ping laptop successfully(to-access id 1 permit)  5) All ping are unsuccessful  7) All ping are unsuccessful  9) All ping are unsuccessful | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.7 | | |
| **Priority** | Accept | **Automation Flag** | Yes |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Add/Delete policy while traffic is on-going(from+to permit) | | |
| Pre-condition | -Configure AP1  *“security-object FWtest”*  *“security-object FWtest default-user-profile-attr 1”*  *“ssid FWtest”*  *“ssid FWtest security-object FWtest”*  *“interface wifi0 ssid FWtest”*  *“interface wifi1 ssid FWtest”*  *“user-profile FW qos-policy def-user-qos vlan-id <mgt0 vlan> attribute 1”*  -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop and gateway of SW ping each other continuance 2. Configure a ip-policy and bind it to FW:   ***“ip-policy FW”***  ***“ip-policy FW from <Laptop ip addr> action permit”***  ***“ip-policy FW to <Laptop ip addr> action permit”***  ***“user-profile FW security ip-policy from-access FW to-access FW”***  ***“clear forwarding-engine ip-sessions”***   1. Check the ping pkt 2. Delete the policy 1   ***“no ip-policy FW id 1”***   1. Check the ping pkt 2. Delete the policy 2   ***“no ip-policy FW id 2”***   1. Check the ping pkt 2. Unbind the policy   ***“user-profile FW security ip-policy from-access FW”***  ***“user-profile FW security ip-policy to-access FW”***   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- Laptop ping gateway successful, gateway ping Laptop unsuccessful on step 3)~~  ~~- All ping are successful on step 5)~~  ~~- Laptop ping gateway unsuccessful, gateway ping Laptop successful on step 3)~~  ~~- All ping are successful on step 9)~~ | | |
| Test result | 1) All ping are successful  3) All ping are successful  5) Laptop ping gateway unsuccessfully(from-access default deny), gateway ping laptop successfully(to-access id 1 permit)  7) All ping are unsuccessful  9) All ping are successful | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.8 | | |
| **Priority** | Accept | **Automation Flag** | Yes |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Add/Delete policy while traffic is on-going(from+to deny) | | |
| Pre-condition | -Configure AP1  *“security-object FWtest”*  *“security-object FWtest default-user-profile-attr 1”*  *“ssid FWtest”*  *“ssid FWtest security-object FWtest”*  *“interface wifi0 ssid FWtest”*  *“interface wifi1 ssid FWtest”*  *“user-profile FW qos-policy def-user-qos vlan-id <mgt0 vlan> attribute 1”*  -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1) Laptop and gateway of SW ping each other continuance  2) Configure a ip-policy and bind it to FW:  ***“ip-policy FW”***  ***“ip-policy FW from <Laptop ip addr> action deny”***  ***“ip-policy FW to <Laptop ip addr> action deny”***  ***“user-profile FW security ip-policy from-access FW to-access FW”***  ***“clear forwarding-engine ip-sessions”***  3) Check the ping pkt  4) Delete the policy 1  ***“no ip-policy FW id 1”***  5) Check the ping pkt  6) Delete the policy 2  ***“no ip-policy FW id 2”***  7) Check the ping pkt  8) Unbind the policy  ***“user-profile FW security ip-policy from-access FW”***  ***“user-profile FW security ip-policy to-access FW”***  9) Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- All ping are unsuccessful on step 3)~~  ~~- All ping are successful on step 5)~~  ~~- All ping are unsuccessful on step 7)~~  ~~- All ping are successful on step 9)~~  1) All ping are successful  3) All ping are unsuccessful  5) All ping are unsuccessful  7) All ping are unsuccessful  9) All ping are successful | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.9 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Add/Delete policy while traffic is on-going(from+to, one direction permit, one deny) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop and gateway of SW ping each other continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop ip addr> action permit”  “ip-policy FW to <Laptop ip addr> action deny”  “user-profile FW security ip-policy from-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the policy 1   ~~“no user-profile FW security ip-policy [from/to]-access”~~  “no ip-policy FW id 1”   1. Check the ping pkt 2. Delete the policy 2   ~~“no user-profile FW security ip-policy [from/to]-access”~~  “no ip-policy FW id 2”   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- If from-policy permit, Laptop ping successfully, SW ping unsuccessfully; else Laptop ping unsuccessfully, SW ping successfully on step 3)~~  ~~- All ping are successful on step 5)~~  1) All ping are successful  3) Laptop ping gateway successfully(from-access id 1), gateway ping laptop unsuccessfully(to-access id 2)  5) All ping are unsuccessful  7) All ping are unsuccessful | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.10 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Add/Delete policy while traffic is on-going(from-access permit, two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy from-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the policy config   ~~“no user-profile FW security ip-policy from-access”~~  “no ip-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- All ping are successful on step 3)~~  ~~- All ping are successful on step 5)~~  1) All ping are successful  3) All ping are unsuccessful(Laptop1 to-access default/Laptop2 from-access default)  5) All ping are unsuccessful | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.11 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Add/Delete policy while traffic is on-going(from-access deny, two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy from-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the policy config   ~~“no user-profile FW security ip-policy from-access”~~  “no ip-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- Laptop1 ping unsuccessfully, Laptop2 ping successfully on step 3)~~  ~~- All ping are successful on step 5)~~  1) All ping are successful  3) All ping are unsuccessful(Laptop1 from-access id 1/Laptop2 from-access default)  5) All ping are unsuccessful | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.12 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Add/Delete policy while traffic is on-going(from-access permit+deny, two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action permit”  “ip-policy FW to <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy from-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the permit policy   ~~“no user-profile FW security ip-policy from-access”~~  “no ip-policy FW id [num=permit policy num]”   1. Check the ping pkt 2. Delete the deny policy   ~~“no user-profile FW security ip-policy from-access”~~  “no ip-policy FW id [num=deny policy num]”   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- All ping are successful on step 3)~~  ~~- All ping are successful on step 5)~~  ~~- Laptop1 ping unsuccessfully, Laptop2 ping successfully on step 7)~~  ~~- All ping are successful on step 9)~~  1) All ping are successful  3) All ping are unsuccessful(Laptop1 to-access default/Laptop2 from-access default)  5) All ping are unsuccessful(Laptop1 from-access default/Laptop2 from-access default)  7) All ping are unsuccessful | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.13 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Add/Delete policy while traffic is on-going(to-access permit, two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the policy config   ~~“no user-profile FW security ip-policy to-access”~~  “no ip-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- All ping are successful on step 3)~~  ~~- All ping are successful on step 5)~~  1) All ping are successful  3) All ping are unsuccessful(Laptop1 from-access default/Laptop2 from-access default)  5) All ping are unsuccessful(Laptop1 from-access default/Laptop2 from-access default) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.14 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Add/Delete policy while traffic is on-going(to-access deny, two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the policy config   ~~“no user-profile FW security ip-policy to-access”~~  “no ip-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- Laptop2 ping unsuccessfully, Laptop1 ping successfully on step 3)~~  ~~- All ping are successful on step 5)~~  1) All ping are successful  3) All ping are unsuccessful(Laptop1 from-access default/Laptop2 from-access default)  5) All ping are unsuccessful(Laptop1 from-access default/Laptop2 from-access default) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.15 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Add/Delete policy while traffic is on-going(to-access permit+deny, two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop1 ip addr> action permit”  “ip-policy FW to <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the permit policy   ~~“no user-profile FW security ip-policy to-access”~~  “no ip-policy FW id [num=permit policy num]”   1. Check the ping pkt 2. Delete the deny policy   ~~“no user-profile FW security ip-policy to-access”~~  “no ip-policy FW id [num=deny policy num]”   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- All ping are successful on step 3)~~  ~~- All ping are successful on step 5)~~  ~~- Laptop2 ping unsuccessfully, Laptop1 ping successfully on step 7)~~  ~~- All ping are successful on step 9)~~  1) All ping are successful  3) All ping are unsuccessful(Laptop1 from-access default/Laptop2 from-access default)  5) All ping are unsuccessful(Laptop1 from-access default/Laptop2 from-access default)  7) All ping are unsuccessful | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.16 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Add/Delete policy while traffic is on-going(from+to permit, two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action permit”  “ip-policy FW to <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy from-access FW to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the from policy   ~~“no user-profile FW security ip-policy [from/to]-access”~~  “no ip-policy FW id [num]”   1. Check the ping pkt 2. Delete the to policy   ~~“no user-profile FW security ip-policy [from/to]-access”~~  “no ip-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- All ping are successful on step 3)~~  ~~- All ping are successful on step 5)~~  1) All ping are successful  3) All ping are successful  5) Laptop1 cannot ping Laptop2 successfully, Laptop2 can ping Laptop1 successfully  7) All ping are unsuccessful | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.17 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Add/Delete policy while traffic is on-going(from+to deny, two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action deny”  “ip-policy FW to <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy from-access FW to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the from policy   ~~“no user-profile FW security ip-policy [from/to]-access”~~  “no ip-policy FW id [num]”   1. Check the ping pkt 2. Delete the to policy   ~~“no user-profile FW security ip-policy [from/to]-access”~~  “no ip-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- All ping are unsuccessful on step 3)~~  ~~- All ping are successful on step 5)~~  1) All ping are successful  3) All ping are unsuccessful  5) All ping are unsuccessful  7) All ping are unsuccessful | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.18 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Add/Delete policy while traffic is on-going(from+to, one direction permit, one deny ,two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action permit”  “ip-policy FW to <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy from-access FW to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the permit policy   ~~“no user-profile FW security ip-policy [from/to]-access”~~  “no ip-policy FW id [num]”   1. Check the ping pkt 2. Delete the deny policy   ~~“no user-profile FW security ip-policy [from/to]-access”~~  “no ip-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | ~~- All ping are successful on step 1)~~  ~~- If from-policy permit, Laptop1 ping successfully, Laptop2 ping unsuccessfully; else Laptop1 ping unsuccessfully, Laptop2 ping successfully on step 3)~~  ~~- All ping are successful on step 5)~~  1) All ping are successful  3) Laptop1 can ping Laptop2 successfully, Laptop2 cannot ping Laptop1 successfully  5) All ping are unsuccessful  7) All ping are unsuccessful | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.19 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP ------ Laptop2  |  SW | | |
| Description | Add/Delete policy while traffic is on-going(from-access permit, through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a ip-policy on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy from-access FW to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the policy config   ~~“no user-profile FW security ip-policy from-access”~~  “no ip-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.20 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP ------ Laptop2  |  SW | | |
| Description | Add/Delete policy while traffic is on-going(from-access deny, through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a ip-policy on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy from-access FW to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the policy config   ~~“no user-profile FW security ip-policy from-access”~~  “no ip-policy FW id [num]”   1. Check the pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.21 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP ------ Laptop2  |  SW | | |
| Description | Add/Delete policy while traffic is on-going(from-access permit+deny, through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a ip-policy on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy from-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Add the deny policy   “ip-policy FW to <Laptop1 ip addr> action deny”   1. Check the ping pkt 2. Delete the permit policy   ~~“no user-profile FW security ip-policy from-access”~~  “no ip-policy FW id [num=permit policy num]”   1. Check the ping pkt 2. Delete the deny policy   ~~“no user-profile FW security ip-policy from-access”~~  “no ip-policy FW id [num=deny policy num]”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5)  - All ping are unsuccessful on step 7)  - All ping are unsuccessful on step 9) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.22 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP ------ Laptop2  |  SW | | |
| Description | Add/Delete policy while traffic is on-going(to-access permit, through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a ip-policy on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy from-access FW to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the policy config   ~~“no user-profile FW security ip-policy to-access”~~  “no ip-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - Laptop1 unsuccessful Laptop2 successful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.23 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP ------ Laptop2  |  SW | | |
| Description | Add/Delete policy while traffic is on-going(to-access deny, through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a ip-policy on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy from-access FW to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the policy config   ~~“no user-profile FW security ip-policy to-access”~~  “no ip-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.24 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP ------ Laptop2  |  SW | | |
| Description | Add/Delete policy while traffic is on-going(to-access permit+deny, through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a ip-policy on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Add the deny policy   “ip-policy FW to <Laptop1 ip addr> action deny”   1. Check the ping pkt 2. Delete the permit policy   ~~“no user-profile FW security ip-policy to-access”~~  “no ip-policy FW id [num=permit policy num]”   1. Check the ping pkt 2. Delete the deny policy   ~~“no user-profile FW security ip-policy to-access”~~  “no ip-policy FW id [num=deny policy num]”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5)  - All ping are unsuccessful on step 7)  - All ping are unsuccessful on step 9) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.25 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP ------ Laptop2  |  SW | | |
| Description | Add/Delete policy while traffic is on-going(from+to permit, through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a ip-policy on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action permit”  “ip-policy FW to <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy from-access FW to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the from policy   ~~“no user-profile FW security ip-policy [from/to]-access”~~  “no ip-policy FW id [num]”   1. Check the ping pkt 2. Delete the to policy   ~~“no user-profile FW security ip-policy [from/to]-access”~~  “no ip-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are successful on step 3)  - Laptop1 unsuccessful/Laptop2 successful on step 5)  - All ping are unsuccessful on step 7) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.26 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP ------ Laptop2  |  SW | | |
| Description | Add/Delete policy while traffic is on-going(from+to deny, through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a ip-policy on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action deny”  “ip-policy FW to <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy from-access FW to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the from policy   ~~“no user-profile FW security ip-policy [from/to]-access”~~  “no ip-policy FW id [num]”   1. Check the ping pkt 2. Delete the to policy   ~~“no user-profile FW security ip-policy [from/to]-access”~~  “no ip-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5)  - All ping are unsuccessful on step 7) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.27 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP ------ Laptop2  |  SW | | |
| Description | Add/Delete policy while traffic is on-going(from+to, one direction permit, one deny , through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping each other continuance 2. Configure a ip-policy on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action permit”  “ip-policy FW to <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy from-access FW to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Delete the permit policy   ~~“no user-profile FW security ip-policy [from/to]-access”~~  “no ip-policy FW id [num]”   1. Check the ping pkt 2. Delete the deny policy   ~~“no user-profile FW security ip-policy [from/to]-access”~~  “no ip-policy FW id [num]”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - Laptop1 successful/Laptop2unsuccessful on step 3)  - All ping are unsuccessful on step 5)  - All ping are unsuccessful on step 7) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.28 | | |
| **Priority** | Accept | **Automation Flag** | Yes |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Binding/Unbinding user-profile while traffic is on-going(from-access permit) | | |
| Pre-condition | -Configure AP1  *“security-object FWtest”*  *“security-object FWtest default-user-profile-attr 1”*  *“ssid FWtest”*  *“ssid FWtest security-object FWtest”*  *“interface wifi0 ssid FWtest”*  *“interface wifi1 ssid FWtest”*  *“user-profile FW qos-policy def-user-qos vlan-id <mgt0 vlan> attribute 1”*  -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop and SW ping each other continuance 2. Configure a ip-policy and bind it to FW:   ***“ip-policy FW”***  ***“ip-policy FW from <Laptop ip addr> action permit”***  ***“user-profile FW security ip-policy from-access FW”***   1. Check the ping pkt 2. Unbinding the policy to user-profile   ***“no user-profile FW security ip-policy from-access”***   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - Laptop successful/Server unsuccessful on step 3)  - All ping are successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.29 | | |
| **Priority** | Accept | **Automation Flag** | Yes |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Binding/Unbinding user-profile while traffic is on-going(from-access deny) | | |
| Pre-condition | -Configure AP1  *“security-object FWtest”*  *“security-object FWtest default-user-profile-attr 1”*  *“ssid FWtest”*  *“ssid FWtest security-object FWtest”*  *“interface wifi0 ssid FWtest”*  *“interface wifi1 ssid FWtest”*  *“user-profile FW qos-policy def-user-qos vlan-id <mgt0 vlan> attribute 1”*  -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop ping gateway of SW continuance 2. Configure a ip-policy and bind it to FW:   ***“ip-policy FW”***  ***“ip-policy FW from <Laptop ip addr> action deny”***  ***“user-profile FW security ip-policy from-access FW”***   1. Check the ping pkt 2. Unbinding the policy to user-profile   ***“no user-profile FW security ip-policy from-access”***   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessfully on step 3)  - All ping are successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.30 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Binding/Unbinding user-profile while traffic is on-going(to-access permit) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop ping gateway of SW continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop ip addr> action permit”  “user-profile FW security ip-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop ping gateway of SW continuance 2. Unbinding the policy to user-profile   “no user-profile FW security ip-policy to-access”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - Laptop unsuccessful/Server successful on step 3)  - All ping are successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.31 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Binding/Unbinding user-profile while traffic is on-going(to-access deny) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Laptop ping gateway of SW continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop ip addr> action deny”  “user-profile FW security ip-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop ping gateway of SW continuance 2. Unbinding the policy to user-profile   “no user-profile FW security ip-policy to-access”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.32 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Binding/Unbinding user-profile while traffic is on-going(from-access permit, two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Check the ping pkt 2. Unbinding the policy to user-profile   “no user-profile FW security ip-policy from-access”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are successful on step 3)  - All ping are successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.33 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Binding/Unbinding user-profile while traffic is on-going(from-access deny, two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Check the ping pkt 2. Unbinding the policy to user-profile   “no user-profile FW security ip-policy from-access”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - Laptop1 ping unsuccessfully, Laptop2 ping successfully on step 3)  - All ping are successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.34 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Binding/Unbinding user-profile while traffic is on-going(to-access permit, two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Check the ping pkt 2. Unbinding the policy to user-profile   “no user-profile FW security ip-policy to-access”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are successful on step 3)  - All ping are successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.35 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Binding/Unbinding user-profile while traffic is on-going(to-access deny, two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 ping Laptop1 continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop2 ping Laptop1 continuance 2. Unbinding the policy to user-profile   “no user-profile FW security ip-policy to-access”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - Laptop1 ping successfully, Laptop2 ping unsuccessfully on step 3)  - All ping are successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.36 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP ------ Laptop2  |  SW | | |
| Description | Binding/Unbinding user-profile while traffic is on-going(from-access permit, through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping continuance 2. Configure a ip-policy on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Check the ping pkt 2. Unbinding the policy to user-profile   “no user-profile FW security ip-policy from-access”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are successful on step 3)  - All ping are successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.37 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP ------ Laptop2  |  SW | | |
| Description | Binding/Unbinding user-profile while traffic is on-going(from-access deny, through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping continuance 2. Configure a ip-policy on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy from-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Check the ping pkt 2. Unbinding the policy to user-profile   “no user-profile FW security ip-policy from-access”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - Laptop1 ping unsuccessfully, Laptop2 ping successfully on step 3)  - All ping are successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.38 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP ------ Laptop2  |  SW | | |
| Description | Binding/Unbinding user-profile while traffic is on-going(to-access permit, through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping continuance 2. Configure a ip-policy on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Check the ping pkt 2. Unbinding the policy to user-profile   “no user-profile FW security ip-policy to-access”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are successful on step 3)  - All ping are successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.39 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP ------ Laptop2  |  SW | | |
| Description | Binding/Unbinding user-profile while traffic is on-going(to-access deny, through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop2 and Laptop1 ping continuance 2. Configure a ip-policy on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Unbinding the policy to user-profile   “no user-profile FW security ip-policy to-access”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - Laptop1 ping successfully, Laptop2 ping unsuccessfully on step 3)  - All ping are successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.40 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop------ AP1 ------ SW ------ Server | | |
| Description | Change the Binding user-profile while traffic is on-going (from-access) (permit->deny) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop and gateway of SW ping each other continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop ip addr> action permit”  “user-profile FW security ip-policy from-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Configure an new ip-policy and bind it to FW   “ip-policy FW2”  “ip-policy FW2 from <Laptop ip addr> action deny”  “user-profile FW security ip-policy from-access FW2”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - Laptop successful/Sever unsuccessful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.41 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop------ AP1 ------ SW ------ Server | | |
| Description | Change the Binding user-profile while traffic is on-going (from-access) (deny->permit) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop and gateway of SW ping each other continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop ip addr> action deny”  “user-profile FW security ip-policy from-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Configure an new ip-policy and bind it to FW   “ip-policy FW2”  “ip-policy FW2 from <Laptop ip addr> action permit”  “user-profile FW security ip-policy from-access FW2”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - Laptop successful/Sever unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.42 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop------ AP1 ------ SW ------ Server | | |
| Description | Change the Binding user-profile while traffic is on-going (to-access) (permit->deny) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop and gateway of SW ping each other continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop ip addr> action permit”  “user-profile FW security ip-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Configure an new ip-policy and bind it to FW   “ip-policy FW2”  “ip-policy FW2 to <Laptop ip addr> action deny”  “user-profile FW security ip-policy to-access FW2”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - Laptop unsuccessful/Sever successful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.43 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop------ AP1 ------ SW ------ Server | | |
| Description | Change the Binding user-profile while traffic is on-going (to-access) (deny->permit) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop and gateway of SW ping each other continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop ip addr> action deny”  “user-profile FW security ip-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Configure an new ip-policy and bind it to FW   “ip-policy FW2”  “ip-policy FW2 to <Laptop ip addr> action permit”  “user-profile FW security ip-policy to-access FW2”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - Laptop unsuccessful/Sever successful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.44 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop------ AP1 ------ SW ------ Server | | |
| Description | Change the Binding user-profile while traffic is on-going (from/to-access) (permit->deny->permit) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1)Laptop and gateway of SW ping each other continuance  2)Configure a ip-policy and bind it to FW:  “ip-policy FW”  “ip-policy FW from <Laptop ip addr> action permit”  “user-profile FW security ip-policy from-access FW to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~  3)Check the ping pkt  4)Configure an new ip-policy and bind it to FW  “ip-policy FW2”  “ip-policy FW2 from <Laptop ip addr> action deny”  “user-profile FW security ip-policy from-access FW2 to-access FW2”  5)Check the ping pkt  6) Recover  “user-profile FW security ip-policy from-access FW to-access FW”  7)Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - Laptop successful/Server unsuccessful on step 3)  - All ping are unsuccessful on step 5)  - Laptop successful/Server unsuccessful on step 7) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.45 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Change the Binding user-profile while traffic is on-going (from-access) (permit->deny) (two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy from-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Configure an new ip-policy and bind it to FW   “ip-policy FW2”  “ip-policy FW2 from <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy from-access FW2”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.46 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Change the Binding user-profile while traffic is on-going (from-access) (deny->permit) (two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy from-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Configure an new ip-policy and bind it to FW   “ip-policy FW2”  “ip-policy FW2 from <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy from-access FW2”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.47 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Change the Binding user-profile while traffic is on-going (to-access) (permit->deny) (two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Configure an new ip-policy and bind it to FW   “ip-policy FW2”  “ip-policy FW2 to <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy to-access FW2”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.48 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Change the Binding user-profile while traffic is on-going (to-access) (deny->permit) (two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other continuance 2. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Configure an new ip-policy and bind it to FW   “ip-policy FW2”  “ip-policy FW2 to <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy to-access FW2”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.49 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Change the Binding user-profile while traffic is on-going (from/to-access) (permit->deny->permit) (two Laptops) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1) Laptop1 and Laptop2 ping each other continuance  2) Configure a ip-policy and bind it to FW:  “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy from-access FW to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~  3) Check the ping pkt  4) Configure an new ip-policy and bind it to FW  “ip-policy FW2”  “ip-policy FW2 from <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy from-access FW2 to-access FW2”  5) Check the ping pkt  6) Recover  “user-profile FW security ip-policy from-access FW to-access FW”  7) Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - Laptop1 successful/Laptop2 unsuccessful on step 3)  - All ping are unsuccessful on step 5)  - Laptop1 successful/Laptop2 unsuccessful on step 7) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.50 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP------ Laptop2  |  SW | | |
| Description | Change the Binding user-profile while traffic is on-going(from-access)(permit->deny)(through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other continuance 2. Configure a ip-policy on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy from-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Configure an new ip-policy and bind it to FW   “ip-policy FW2”  “ip-policy FW2 from <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy from-access FW2”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.51 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP------ Laptop2  |  SW | | |
| Description | Change the Binding user-profile while traffic is on-going(from-access)(deny->permit)(through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other continuance 2. Configure a ip-policy on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy from-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Configure an new ip-policy and bind it to FW   “ip-policy FW2”  “ip-policy FW2 from <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy from-access FW2”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.52 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP------ Laptop2  |  SW | | |
| Description | Change the Binding user-profile while traffic is on-going(to-access)(permit->deny) (through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other continuance 2. Configure a ip-policy on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Configure an new ip-policy and bind it to FW   “ip-policy FW2”  “ip-policy FW2 to <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy to-access FW2”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.53 | | |
| **Priority** | Middle | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP------ Laptop2  |  SW | | |
| Description | Change the Binding user-profile while traffic is on-going(to-access)(deny->permit) (through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Laptop1 and Laptop2 ping each other continuance 2. Configure a ip-policy on MP and bind it to FW:   “ip-policy FW”  “ip-policy FW to <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Check the ping pkt 2. Configure an new ip-policy and bind it to FW   “ip-policy FW2”  “ip-policy FW2 to <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy to-access FW2”   1. Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - All ping are unsuccessful on step 3)  - All ping are unsuccessful on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_7.54 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1------ AP1 ------MP------ Laptop2  |  SW | | |
| Description | Change the Binding user-profile while traffic is on-going (from/to-access) (permit->deny->permit) (through MP) | | |
| Pre-condition | -Laptops has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1) Laptop1 and Laptop2 ping each other continuance  2) Configure a ip-policy and bind it to FW:  “ip-policy FW”  “ip-policy FW from <Laptop1 ip addr> action permit”  “user-profile FW security ip-policy from-access FW to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~  3) Check the ping pkt  4) Configure an new ip-policy and bind it to FW  “ip-policy FW2”  “ip-policy FW2 from <Laptop1 ip addr> action deny”  “user-profile FW security ip-policy from-access FW2 to-access FW2”  5) Check the ping pkt  6) Recover  “user-profile FW security ip-policy from-access FW to-access FW”  7) Check the ping pkt | | |
| Expect result | - All ping are successful on step 1)  - Laptop1 successful/Laptop2 unsuccessful on step 3)  - All ping are unsuccessful on step 5)  - Laptop1 successful/Laptop2 unsuccessful on step 7) | | |
| Test result |  | | |

## 8.8 Fragment test

* Case ID FW\_IP\_Policy\_Serv\_8

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_8.1 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Fragments are sent in order | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW [from/to] <Laptop ip addr> action permit”  “user-profile FW security ip-policy [from/to]-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Server sends all the fragment packets to Laptop in order by using hping2 or other tools 2. Check the the packets on AP1 and Laptop | | |
| Expect result | - AP1 should process the fragment packets, AP1 sends the fragments to Laptop if them can be reassembled a complete packets while receives all fragments; Laptop should receive the fragment packets. | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_8.2 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Fragments are sent in disorder | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW [from/to] <Laptop ip addr> action permit”  “user-profile FW security ip-policy [from/to]-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Server sends all the fragment packets to Laptop in disorder by using hping2 or other tools 2. Check the the packets on AP1 and Laptop | | |
| Expect result | - AP1 should process the fragment packets, AP1 sends the fragments to Laptop if them can be reassembled a complete packets while receives all fragments; Laptop should receive the fragment packets. | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_8.3 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Fragments are sent, but miss one or more fragments | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW [from/to] <Laptop ip addr> action permit”  “user-profile FW security ip-policy [from/to]-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Server sends the fragment packets to Laptop in order/disorder by using hping2 or other tools, but one or more fragments are not sent. 2. Check the the packets on AP1 and Laptop | | |
| Expect result | - AP1 should process the fragment packets, but couldn’t reassemble the fragments cause miss some fragments, so AP1 don’t transmit the fragment packets; Laptop should dont’t receive the fragments. | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_8.4 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Fragments are sent, using different protocol(TCP/UDP) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW [from/to] <Laptop ip addr> action permit”  “user-profile FW security ip-policy [from/to]-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Server sends all the fragment packets to Laptop in order/disorder by using hping2 or other tools, and using different protocol. 2. Check the the packets on AP1 and Laptop | | |
| Expect result | - AP1 should process the fragment packets, AP1 sends the fragments to Laptop if them can be reassembled a complete packets while receives all fragments; Laptop should receive the fragment packets. | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_8.5 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Fragments are sent in order(two Laptops) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW [from/to] <Laptops ip addr> action permit”  “user-profile FW security ip-policy [from/to]-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop1 sends all the fragment packets to Laptop2 in order by using hping2 or other tools 2. Check the the packets on AP1 and Laptop2 | | |
| Expect result | - AP1 should process the fragment packets, AP1 sends the fragments to Laptop2 if them can be reassembled a complete packets while receives all fragments; Laptop2 should receive the fragment packets. | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_8.6 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Fragments are sent in disorder(two Laptops) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW [from/to] <Laptops ip addr> action permit”  “user-profile FW security ip-policy [from/to]-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop1 sends all the fragment packets to Laptop2 in disorder by using hping2 or other tools 2. Check the the packets on AP1 and Laptop2 | | |
| Expect result | - AP1 should process the fragment packets, AP1 sends the fragments to Laptop2 if them can be reassembled a complete packets while receives all fragments; Laptop2 should receive the fragment packets. | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_8.7 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Fragments are sent, but miss one or more fragments(two Laptops) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW [from/to] <Laptops ip addr> action permit”  “user-profile FW security ip-policy [from/to]-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop1 sends the fragment packets to Laptop2 in order/disorder by using hping2 or other tools, but one or more fragments are not sent. 2. Check the the packets on AP1 and Laptop2 | | |
| Expect result | - AP1 should process the fragment packets, but couldn’t reassemble the fragments cause miss some fragments, so AP1 don’t transmit the fragment packets; Laptop2 should dont’t receive the fragments. | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_8.8 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------ SW ------ Server  |  Laptop2 | | |
| Description | Fragments are sent, using different protocol(TCP/UDP)(two Laptops) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW [from/to] <Laptops ip addr> action permit”  “user-profile FW security ip-policy [from/to]-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop1 sends all the fragment packets to Laptop2 in order/disorder by using hping2 or other tools, and using different protocol. 2. Check the the packets on AP1 and Laptop2 | | |
| Expect result | - AP1 should process the fragment packets, AP1 sends the fragments to Laptop2 if them can be reassembled a complete packets while receives all fragments; Laptop2 should receive the fragment packets. | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_8.9 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------MP------ Laptop2  |  SW | | |
| Description | Fragments are sent in order(through MP) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Configure a ip-policy on AP1 and MP, and bind it to FW:   “ip-policy FW”  “ip-policy FW [from/to] <Laptops ip addr> action permit”  “user-profile FW security ip-policy [from/to]-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop1 sends all the fragments which could be reassembled a large packet to Laptop2 in order by using hping2 or other tools 2. Check the the packets on AP1, MP and Laptop2 | | |
| Expect result | - AP1 should process the fragment packets, AP1 sends the fragments to Laptop2 through MP if them can be reassembled a complete packets while receives all fragments; MP transmits the fragment packets to Laptop2; Laptop2 should receive the fragment packets. | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_8.10 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------MP------ Laptop2  |  SW | | |
| Description | Fragments are sent in disorder(through MP) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Configure a ip-policy on AP1 and MP, and bind it to FW:   “ip-policy FW”  “ip-policy FW [from/to] <Laptops ip addr> action permit”  “user-profile FW security ip-policy [from/to]-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop1 sends all the fragment packets to Laptop2 in disorder by using hping2 or other tools 2. Check the the packets on AP1, MP and Laptop2 | | |
| Expect result | - AP1 should process the fragment packets, AP1 sends the fragments to Laptop2 through MP if them can be reassembled a complete packets while receives all fragments; MP transmits the fragment packets to Laptop2; Laptop2 should receive the fragment packets. | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_8.11 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------MP------ Laptop2  |  SW | | |
| Description | Fragments are sent, but miss one or more fragments(through MP) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Configure a ip-policy on AP1 and MP, and bind it to FW:   “ip-policy FW”  “ip-policy FW [from/to] <Laptops ip addr> action permit”  “user-profile FW security ip-policy [from/to]-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop1 sends the fragment packets to Laptop2 in order/disorder by using hping2 or other tools, but one or more fragments are not sent. 2. Check the the packets on AP1 ,MP and Laptop2 | | |
| Expect result | - AP1 should process the fragment packets, but couldn’t reassemble the fragments cause miss some fragments, so AP1 don’t transmit the fragment packets; MP and Laptop2 dont’t receive the fragment packets | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_8.12 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------MP------ Laptop2  |  SW | | |
| Description | Fragments are sent, using different protocol(TCP/UDP)( through MP) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Configure a ip-policy on AP1 and MP, and bind it to FW:   “ip-policy FW”  “ip-policy FW [from/to] <Laptops ip addr> action permit”  “user-profile FW security ip-policy [from/to]-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop1 sends all the fragment packets to Laptop2 in order/disorder by using hping2 or other tools, and using different protocol. 2. Check the the packets on AP1, MP and Laptop2 | | |
| Expect result | - AP1 should process the fragment packets, AP1 sends the fragments to Laptop2 through MP if them can be reassembled a complete packets while receives all fragments; MP transmits the fragment packets to Laptop2; Laptop2 should receive the fragment packets. | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_8.13 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------MP(eth)------ Laptop2  |  SW | | |
| Description | Set eth port access, fragments are sent in order(through MP) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Configure a ip-policy on AP1 and MP, and bind it to FW:   “ip-policy FW”  “ip-policy FW [from/to] <Laptops ip addr> action permit”  “user-profile FW security ip-policy [from/to]-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop1 sends all the fragment packets to Laptop2 in order by using hping2 or other tools 2. Check the the packets on AP1, MP and Laptop2 | | |
| Expect result | - AP1 should process the fragment packets, AP1 sends the fragments to Laptop2 through MP if them can be reassembled a complete packets while receives all fragments; MP transmits the fragment packets to Laptop2; Laptop2 should receive the fragment packets. | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_8.14 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------MP(eth)------ Laptop2  |  SW | | |
| Description | Set eth port access, fragments are sent in disorder(through MP) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Configure a ip-policy on AP1 and MP, and bind it to FW:   “ip-policy FW”  “ip-policy FW [from/to] <Laptops ip addr> action permit”  “user-profile FW security ip-policy [from/to]-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop1 sends all the fragment packets to Laptop2 in disorder by using hping2 or other tools 2. Check the the packets on AP1, MP and Laptop2 | | |
| Expect result | - AP1 should process the fragment packets, AP1 sends the fragments to Laptop2 through MP if them can be reassembled a complete packets while receives all fragments; MP transmits the fragment packets to Laptop2; Laptop2 should receive the fragment packets. | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_8.15 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------MP------ Laptop2  |  SW | | |
| Description | Set eth port access, fragments are sent, but miss one or more fragments(through MP) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Configure a ip-policy on AP1 and MP, and bind it to FW:   “ip-policy FW”  “ip-policy FW [from/to] <Laptops ip addr> action permit”  “user-profile FW security ip-policy [from/to]-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop1 sends the fragment packets to Laptop2 in order/disorder by using hping2 or other tools, but one or more fragments are not sent. 2. Check the the packets on AP1 ,MP and Laptop2 | | |
| Expect result | - AP1 should process the fragment packets, but couldn’t reassemble the fragments cause miss some fragments, so AP1 don’t transmit the fragment packets; MP and Laptop2 dont’t receive the fragment packets | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_8.16 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop1 ------ AP1 ------MP------ Laptop2  |  SW | | |
| Description | Set eth port access, fragments are sent, using different protocol(TCP/UDP)( through MP) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Configure a ip-policy on AP1 and MP, and bind it to FW:   “ip-policy FW”  “ip-policy FW [from/to] <Laptops ip addr> action permit”  “user-profile FW security ip-policy [from/to]-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Laptop1 sends all the fragment packets to Laptop2 in order/disorder by using hping2 or other tools, and using different protocol. 2. Check the the packets on AP1, MP and Laptop2 | | |
| Expect result | - AP1 should process the fragment packets, AP1 sends the fragments to Laptop2 through MP if them can be reassembled a complete packets while receives all fragments; MP transmits the fragment packets to Laptop2; Laptop2 should receive the fragment packets. | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_8.17 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Fragments are sent to mgt0 | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW [from/to] <Laptop ip addr> action permit”  “user-profile FW security ip-policy [from/to]-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Server sends the fragment packets to mgt0 of AP1 by using hping2 or other tools 2. Check the the packets on AP1 | | |
| Expect result | - AP1 should process the fragment packets, sends it to mgt0 if them can be reassembled to a complete packets while receives all fragments; else drop the fragment after timeout | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_8.18 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Send two similar fragments except port different | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW [from/to] <Laptop ip addr> action permit”  “user-profile FW security ip-policy [from/to]-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Server sends two fragment packets to Laptop which are the same except the src or dst port   “pkt1 (src\_ip1, dst\_ip1, src\_port1, dst\_port1)”  “pkt2 (src\_ip2, dst\_ip2, src\_port2, dst\_port2)”   1. Check the the packets on AP1 | | |
| Expect result | - AP1 should process the fragment packets, the second packet should be dropped | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Fun\_8.19 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Send fragments with error offset | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW [from/to] <Laptop ip addr> action permit”  “user-profile FW security ip-policy [from/to]-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Server sends fragment packets to Laptop which the offset is error or offset value+data length>ip maximum length 2. Check the the packets on AP1 | | |
| Expect result | - AP1 should process the fragment packets, the packet should be dropped | | |
| Test result |  | | |

## 8.9 Services test

* Case ID FW\_IP\_Policy\_Serv\_9

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Serv\_9.1 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Session setup for ping traffic | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config the ip-policy that permit L3 traffic between Laptop and Server   “ip-policy FW-0”  “ip-policy FW-0 [from/to] <Laptop ip addr> action permit”   1. Laptop ping Server 2. Show the ip-session | | |
| Expect result | - Laptop ping successfully on step 2)  - Establish the ip-session between Laptop and Server successfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Serv\_9.2 | | |
| **Priority** | Accept | **Automation Flag** | Yes |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Session setup for ftp/ftp-data traffic | | |
| Pre-condition | -Configure AP1  *“security-object FWtest”*  *“security-object FWtest default-user-profile-attr 1”*  *“ssid FWtest”*  *“ssid FWtest security-object FWtest”*  *“interface wifi0 ssid FWtest”*  *“interface wifi1 ssid FWtest”*  *“user-profile FW qos-policy def-user-qos vlan-id <mgt0 vlan> attribute 1”*  -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config the ip-policy FTP permit   ***“ip-policy FW”***  ***“ip-policy FW service ftp action permit”***  ***“user-profile FW security ip-policy from-access FW ”***  ***“clear forwarding-engine ip-sessions”***   1. Laptop uses ftp to connect Server, and download/upload files, check the result 2. Show the ip-session   ***“show forwarding-engine ip-sessions”***   1. Enable FTP-alg   ***“alg ftp enable”***  ***“clear forwarding-engine ip-sessions”***   1. Laptop uses ftp to connect Server, and download/upload files, check the result 2. Show the ip-session   ***“show forwarding-engine ip-sessions”***   1. Clear alg configure   ***“no alg ftp enable”***   1. Config the ip-policy FTP/FTPData permit   ***“ip-policy FW”***  ***“ip-policy FW service ftp action permit”***  ***“ip-policy FW service ftp-data action permit”***  ***“user-profile FW security ip-policy from-access FW to-access FW”***  ***“clear forwarding-engine ip-sessions”***   1. Laptop uses ftp to connect Server, and download/upload files, check the result 2. Show the ip-session   ***“show forwarding-engine ip-sessions”***   1. Config the ip-policy that deny ftp/ftp-data traffic between Laptop and Server   ***“ip-policy FW”***  ***“ip-policy FW service ftp action deny”***  ***“ip-policy FW service ftp-data action deny”***  ***“ip-policy FW action permit”***  ***“user-profile FW security ip-policy from-access FW to-access FW”***  ***“clear forwarding-engine ip-sessions”***   1. Laptop uses ftp to connect Server, and download/upload files, check the result 2. Show the ip-session   ***“show forwarding-engine ip-sessions”*** | | |
| Expect result | 2.Laptop can connect server,but cannot download/upload files;  3.We should check IP-session such as  Id:15; Ageout:1792409; Flags:0x24400; QOS:2; Up: 2 min 22 sec; InPol:fw/1;  172.29.10.51/58402 -> 10.155.30.43/21; Proto 6; Flg:0x112; Pkts:16 Bytes:761 Parent-MAC-Sess: 7  10.155.30.43/21 -> 172.29.10.51/58402; Proto 6; Flg:0x110; Pkts:9 Bytes:656  172.29.10.51 is Laptop’s IPaddr,10.155.30.43 is Server’s IPaddr, 21 is FTP port  5. Laptop can connect server and download/upload files successfully;  6.The same as step 3;  9. Laptop can connect server, but cannot download/upload files;  10. The same as step 3;  12. Laptop can neither connect server nor download/upload files;  13.We cannot see the session such as step3; | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Serv\_9.3 | | |
| **Priority** | Accept | **Automation Flag** | Yes |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Session setup for http/https traffic | | |
| Pre-condition | -Configure AP1  *“security-object FWtest”*  *“security-object FWtest default-user-profile-attr 1”*  *“ssid FWtest”*  *“ssid FWtest security-object FWtest”*  *“interface wifi0 ssid FWtest”*  *“interface wifi1 ssid FWtest”*  *“user-profile FW qos-policy def-user-qos vlan-id <mgt0 vlan> attribute 1”*  -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config the ip-policy that permit http/https traffic between Laptop and Server   ***“ip-policy FW-0”***  ***“ip-policy FW-0 service [http/https] [from/to] <Laptop ip addr> action permit”***  ***“user-profile FW security ip-policy from-access FW”***   1. Using Server as a http/https Server, Laptop accesses Server by http/https 2. Show the ip-session   ***“show forwarding-engine ip-sessions”*** | | |
| Expect result | - Laptop can access Server successfully by http/https, and get pages successfully on step 2)  - Establish the ip-session(http/https) between Laptop and Server successfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Serv\_9.4 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Session setup for telnet traffic | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config the ip-policy that permit telnet traffic between Laptop and Server   “ip-policy FW-0”  “ip-policy FW-0 service [telnet] [from/to] <Laptop ip addr> action permit”   1. Laptop accesses Server by telnet 2. Show the ip-session | | |
| Expect result | - Laptop can login Server successfully by telnet on step 2)  - Establish the ip-session(telnet) between Laptop and Server successfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Serv\_9.5 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Session setup for tftp traffic | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config the ip-policy that permit tftp traffic between Laptop and Server   “ip-policy FW-0”  “ip-policy FW-0 service [tftp] [from/to] <Laptop ip addr> action permit”   1. Laptop accesses Server and get/put files by tftp 2. Show the ip-session | | |
| Expect result | - Laptop can link Server successfully by tftp, and get/put files successfully on step 2)  - Establish the ip-session(tftp) between Laptop and Server successfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Serv\_9.6 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Session setup for dns traffic | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config the ip-policy that permit dns traffic between Laptop and Server   “ip-policy FW-0”  “ip-policy FW-0 service [dns] [from/to] <Laptop ip addr> action permit”   1. Laptop using command “nslookup” to request Server 2. Show the ip-session | | |
| Expect result | - Laptop can get data from Server successfully by dns on step 2)  - Establish the ip-session(dns) between Laptop and Server successfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Serv\_9.7 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Session setup for smtp traffic | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config the ip-policy that permit smtp traffic between Laptop and Server   “ip-policy FW-0”  “ip-policy FW-0 service [smtp] [from/to] <Laptop ip addr> action permit”   1. Laptop accesses Server through smtp, and writes/sends mail 2. Show the ip-session | | |
| Expect result | - Laptop can login Server successfully by smtp, and write/send mail successfully on step 2)  - Establish the ip-session(smtp) between Laptop and Server successfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Serv\_9.8 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Session setup for pop3 traffic | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config the ip-policy that permit pop3 traffic between Laptop and Server   “ip-policy FW-0”  “ip-policy FW-0 service [pop3] [from/to] <Laptop ip addr> action permit”   1. Laptop accesses Server through pop3, and receives mail 2. Show the ip-session | | |
| Expect result | - Laptop can login Server successfully by pop3, and receive mail successfully on step 2)  - Establish the ip-session(pop3) between Laptop and Server successfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Serv\_9.9 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Session setup for imap traffic | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config the ip-policy that permit imap traffic between Laptop and Server   “ip-policy FW-0”  “ip-policy FW-0 service [imap] [from/to] <Laptop ip addr> action permit”   1. Laptop accesses Server through imap, and receives mail 2. Show the ip-session | | |
| Expect result | - Laptop can login Server successfully by imap, and receive mail successfully on step 2)  - Establish the ip-session(imap) between Laptop and Server successfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Serv\_9.10 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Session setup for sip traffic | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config the ip-policy that permit sip traffic between Laptop and Server   “ip-policy FW-0”  “ip-policy FW-0 service [sip] [from/to] <Laptop ip addr> action permit”   1. Laptop uses tool call Server 2. Show the ip-session | | |
| Expect result | - Laptop call server successfully on step 2)  - Establish the ip-session(sip) between Laptop and Server successfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Serv\_9.11 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Session setup for ssh traffic | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config the ip-policy that permit ssh traffic between Laptop and Server   “ip-policy FW-0”  “ip-policy FW-0 service [ssh] [from/to] <Laptop ip addr> action permit”   1. Laptop accesses Server by ssh 2. Show the ip-session | | |
| Expect result | - Laptop can login Server successfully by ssh on step 2)  - Establish the ip-session(ssh) between Laptop and Server successfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Serv\_9.12 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Session setup for dhcp-server traffic | | |
| Pre-condition | -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config the ip-policy that permit dhcp-server traffic between Laptop and Server   “ip-policy FW-0”  “ip-policy FW-0 service [dhcp-server] [from/to] <Laptop ip addr> action permit”   1. Config AP1 as a dhcp-server   “interface mgt0 dhcp-server enable”  “interface mgt0 dhcp-server ip-pool <first\_ip\_addr> <last\_ip\_addr>”   1. Laptop can get ip\_address in the ip\_pool range from AP1 2. Laptop ping AP1 3. Show the ip-session | | |
| Expect result | - Laptop ping successfully on step 4)  - Establish the ip-session(dhcp-server) between Laptop and AP1 successfully on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Serv\_9.13 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Session setup for dhcp-client traffic | | |
| Pre-condition | -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config the ip-policy that permit dhcp-client traffic between Laptop and Server   “ip-policy FW-0”  “ip-policy FW-0 service [dhcp-client] [from/to] <Laptop ip addr> action permit”   1. Config AP1 as a dhcp-client   “interface mgt0 dhcp client”   1. Laptop can get ip\_address from dhcp Server through AP1 2. Laptop ping AP1, Server 3. Show the ip-session | | |
| Expect result | - Laptop ping successfully on step 4)  - Establish the ip-session(dhcp-client) between Laptop and AP1 successfully on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Serv\_9.14 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Session setup for snmp traffic | | |
| Pre-condition | -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config the ip-policy that permit snmp traffic between Laptop and Server   “ip-policy FW-0”  “ip-policy FW-0 service [snmp] [from/to] <Laptop ip addr> action permit”   1. Laptop connects to AP1, and uses MIB tool to operate AP1 2. Show the ip-session | | |
| Expect result | - Laptop ping successfully on step 4)  - Establish the ip-session(snmp) between Laptop and AP1 successfully on step 5) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Serv\_9.15 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Session setup for snmp-trap traffic | | |
| Pre-condition | -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config the ip-policy that permit snmp-trap traffic between Laptop and Server   “ip-policy FW-0”  “ip-policy FW-0 service [snmp-trap] [from/to] <Laptop ip addr> action permit”   1. Config the snmp-trap   “snmp trap-host <ip\_addr>”  “snmp trap-info over-snmp”  “\_test trap-case <level> <trap\_event>”   1. Show the ip-session | | |
| Expect result | - Establish the ip-session(snmp-trap) between Laptop and AP1 successfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Serv\_9.16 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Session setup for vocera-control traffic | | |
| Pre-condition | -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config the ip-policy that permit vocera-control traffic between Laptop and Server   “ip-policy FW-0”  “ip-policy FW-0 service [vocera-control] [from/to] <Laptop ip addr> action permit”   1. Using vocera client connect to AP1 2. Show the ip-session | | |
| Expect result | - Establish the ip-session(vocera-control) between vocera client and AP1 successfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Serv\_9.17 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Session setup for vocera-media traffic | | |
| Pre-condition | -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config the ip-policy that permit vocera-media traffic between Laptop and Server   “ip-policy FW-0”  “ip-policy FW-0 service [vocera-media] [from/to] <Laptop ip addr> action permit”   1. Using vocera clients connect to AP1, and communicate each other through AP1 2. Show the ip-session | | |
| Expect result | - Establish the ip-session(vocera-media) between vocera clients successfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Serv\_9.18 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Session setup for voip\_svp traffic | | |
| Pre-condition | -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config the ip-policy that permit voip\_svp traffic between Laptop and Server   “ip-policy FW-0”  “ip-policy FW-0 service [voip\_svp] [from/to] <Laptop ip addr> action permit”   1. Using voip\_svp clients connect to AP1, and communicate each other 2. Show the ip-session | | |
| Expect result | - Establish the ip-session(voip\_svp) between voip\_svp clients successfully on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Serv\_9.19 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Radius service. | | |
| Pre-condition | -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config a radius-server on AP1   “user-group <group\_name>”  “user-group <group\_name> user-attribute [num]”  “aaa radius-server local user-group <group\_name>”  “aaa radius-server local db-type local”  “aaa radius-server local enable”  “ssid <ssid\_name> security aaa radius-server primary <AP1\_ip>”  “ssid <ssid\_name> security protocol-suite wpa-auto-8021x”  “user-profile <user-profile\_string> qos-policy def-user-qos vlan-id [num] attribute [num]”   1. Laptop ping server | | |
| Expect result | - Laptop get a ip\_address from AP1(radius server) and ping successfully on step 2)- | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Serv\_9.20 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Radius acct service. | | |
| Pre-condition | -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config a radius acct on AP1   “user-group <group\_name>”  “user-group <group\_name> user-attribute [num]”  “aaa radius-server local user-group <group\_name> shared-secret <string> acct-port 1813 ”  “aaa radius-server local db-type local”  “aaa radius-server local enable”  “ssid <ssid\_name> security aaa radius-server primary <server\_ip>”  “ssid <ssid\_name> security protocol-suite wpa-auto-8021x”  “user-profile <user-profile\_string> qos-policy def-user-qos vlan-id [num] attribute [num]”   1. Laptop ping server | | |
| Expect result | - Laptop get a ip\_address from server(radius server) through AP1 and ping successfully on step 2)- | | |
| Test result |  | | |

## 8.10 Performance/Stress test

* Case ID FW\_IP\_Policy\_Perf\_10

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Perf\_10.1 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config full rule in one ip-policy(permit,from-access) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config full policy in one ip-policy by script and bind it to FW:   “ip-policy FW”  “ip-policy FW id 1 from <Laptop ip addr> action permit”  “ip-policy FW id 2 from <Laptop ip addr> action permit”  “ip-policy FW id 3 from <Laptop ip addr> action permit”  “…..”  “ip-policy FW id 64 from <Laptop ip addr> action permit”  ~~“user-profile FW security ip-policy from-access FW”~~   1. Show the running config 2. Add the id 33 rule in policy FW | | |
| Expect result | ~~- Laptop ping successfully on step 1), 2) and 3)~~  ~~- Config full policy successfully, and the running config shows the config-policies correctly on step 5).~~  ~~- Laptop ping successfully on step 6)~~  2) Configure is shown correctly  3) May show error info | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Perf\_10.2 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config full policy in one ip-policy(deny,from-access) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config full policy in one ip-policy by script and bind it to FW:   “ip-policy FW”  “ip-policy FW id 1 from <Laptop ip addr> action deny”  “ip-policy FW id 2 from <Laptop ip addr> action deny”  “ip-policy FW id 3 from <Laptop ip addr> action deny”  “…..”  ~~“user-profile FW security ip-policy from-access FW”~~  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Show the running config 2. Add the id 33 rule in policy FW | | |
| Expect result | ~~- Laptop ping successfully on step 1), 2) and 3)~~  ~~- Config full policy successfully, and the running config shows the config-policies correctly on step 5).~~  ~~- Laptop ping unsuccessfully on step 6)~~  2) Configure is shown correctly  3) May show error info | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Perf\_10.3 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config full policy in one ip-policy(permit, to-access) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config full policy in one ip-policy by script and bind it to FW:   “ip-policy FW”  “ip-policy FW id 1 to <Laptop ip addr> action permit”  “ip-policy FW id 2 to <Laptop ip addr> action permit”  “ip-policy FW id 3 to <Laptop ip addr> action permit”  “…..”  ~~“user-profile FW security ip-policy to-access FW”~~  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Show the running config 2. Add the id 33 rule in policy FW | | |
| Expect result | ~~- Devices ping Laptop successfully on step 1), 2) and 3)~~  ~~- Config full policy successfully, and the running config shows the config-policies correctly on step 5).~~  ~~- Devices ping Laptop successfully on step 6)~~  2) Configure is shown correctly  3) May show error info | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Perf\_10.4 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config full policy in one ip-policy(deny, to-access) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config full policy in one mac-policy by script and bind it to FW:   “ip-policy FW”  “ip-policy FW id 1 to <Laptop ip addr> action deny”  “ip-policy FW id 2 to <Laptop ip addr> action deny”  “ip-policy FW id 3 to <Laptop ip addr> action deny”  “…..”  ~~“user-profile FW security ip-policy to-access FW”~~  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Show the running config 2. Add the id 33 rule in policy FW | | |
| Expect result | ~~- Devices ping Laptop successfully on step 1), 2) and 3)~~  ~~- Config full policy successfully, and the running config shows the config-policies correctly on step 5).~~  ~~- Devices ping Laptop unsuccessfully on step 6)~~  2) Configure is shown correctly  3) May show error info | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Perf\_10.5 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config full policy in one ip-policy(deny/permit, from/to-access) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config full policy in one ip-policy by script and bind it to FW:   “ip-policy FW”  “ip-policy FW id 1 from <Laptop ip addr> action permit”  “ip-policy FW id 2 from <Laptop ip addr> action deny”  “ip-policy FW id 3 to <Laptop ip addr> action permit”  “ip-policy FW id 4 to <Laptop ip addr> action deny”  “…..”  “ip-policy FW id 64 to <Laptop ip addr> action deny”  ~~“user-profile FW security ip-policy from-access FW to-access FW”~~  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Show the running config 2. Add the id 33 rule in policy FW | | |
| Expect result | ~~- Devices ping successfully on step 1), 2) and 3)~~  ~~- Config full policy successfully, and the running config shows the config-policies correctly on step 5).~~  ~~- If match the deny-policy, ping should be unsuccessful on step 6), else should be successful on step 6)~~  2) Configure is shown correctly  3) May show error info | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Perf\_10.6 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config full rule in one ip-policy(deny/permit, from/to-access), and using before/after attributes | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config full policy in one ip-policy by script and bind it to FW:   “ip-policy FW”  “ip-policy FW id 1 from <Laptop ip addr> action permit”  “ip-policy FW id 2 from <Laptop ip addr> action deny”  “ip-policy FW id 3 to <Laptop ip addr> action permit”  “ip-policy FW id 4 to <Laptop ip addr> action deny”  “…..”  “ip-policy FW id 64 to <Laptop ip addr> action deny”  “user-profile FW security ip-policy from-access FW to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Show the running config 2. Add the id 33 rule in policy FW 3. Using before/after to change the policy’s sequence   “ip-policy FW id 64 before id 1”  “ip-policy FW id 63 after id 2”   1. Show the running config | | |
| Expect result | ~~- Devices ping successfully on step 1), 2) and 3)~~  ~~- Config full policy successfully, and the running config shows the config-policies correctly on step 5).~~  ~~- If match the deny-policy, ping should be unsuccessful on step 6), else should be successful on step 6)~~  ~~- Change the policy’s sequence successfully, and the running config should be show the sequences correctly on step 8)~~  ~~- If match the deny-policy, ping should be unsuccessful on step 6), else should be successful on step 9)~~  2) Configure is shown correctly (The order is 1->64)  3) May show error info(ERROR: Invalid parameter(s))  5) Configure is shown correctly (The order id 64,1,2,63,3,4,5,6…) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Perf\_10.7 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config maximum ip-policy, and config full policy in every ip-policy (config&resource check)(32\*64) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config full policies and full rules FW:   “ip-policy FW-1”  “ip-policy FW-1 id 1 [from/to] <Laptop ip addr> action [permit/deny]”  “ip-policy FW-1 id 2 [from/to] <Laptop ip addr> action [permit/deny]”  “ip-policy FW-1 id 3 [from/to] <Laptop ip addr> action [permit/deny]”  “…..”  “ip-policy FW-32”  “ip-policy FW-32 id 1 [from/to] <Laptop ip addr> action [permit/deny]”  “ip-policy FW-32 id 2 [from/to] <Laptop ip addr> action [permit/deny]”  “ip-policy FW-32 id 3 [from/to] <Laptop ip addr> action [permit/deny]”  …  “ip-policy FW-32 id 64 [from/to] <Laptop ip addr> action [permit/deny]”  ~~“user-profile FW security ip-policy from-access FW[N]”~~  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Show the running config, show the AP1’s resource using 2. Add the FW-33 group on AP | | |
| Expect result | ~~- Config full policy successfully, and the running config shows the config-policies correctly , the cpu & mem’s using are normal on step 2).~~  2) Configure is shown correctly, cpu and mermory is in normal status  3) May show error info(exceed max groups, can't add any more!) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Perf\_10.8 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config maximum ip-policy, and config full policy in every ip-policy, binding it to 16 user-profiles | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config full policies and full rules   “ip-policy FW-1”  “ip-policy FW-1 id 1 [from/to] <Laptop ip addr> action [permit/deny]”  “ip-policy FW-1 id 2 [from/to] <Laptop ip addr> action [permit/deny]”  “ip-policy FW-1 id 3 [from/to] <Laptop ip addr> action [permit/deny]”  “…..”  “ip-policy FW-32”  “ip-policy FW-32 id 1 [from/to] <Laptop ip addr> action [permit/deny]”  “ip-policy FW-32 id 2 [from/to] <Laptop ip addr> action [permit/deny]”  “ip-policy FW-32 id 3 [from/to] <Laptop ip addr> action [permit/deny]”  …  “ip-policy FW-32 id 64 [from/to] <Laptop ip addr> action [permit/deny]”  “user-profile 1”  …  “user-profile 16”   1. Bind firewall policies to user-profiles   “user-profile 1 security ip-policy from-access FW-1 to-access FW-2”  …  “user-profile 16 security ip-policy from-access FW-31 to-access FW-32”   1. Show the running config show the AP1’s resource using 2. Add the FW-33 group on AP | | |
| Expect result | ~~- Laptop ping successfully on step 1), 2) and 3)~~  ~~- Config full policy successfully, and the running config shows the config-policies correctly on step 5).~~  ~~- If match the deny-policy, ping should be unsuccessful on step 6), else should be successful on step 6)~~  3) Configure is shown correctly, cpu and mermory is in normal status  4) May show error info(exceed max groups, can't add any more!) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Perf\_10.9 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config maximum ip-policy, and config full policy in every ip-policy, using before/after attributes | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Config full policy by script and bind one of them to FW:   “ip-policy FW-1”  “ip-policy FW-1 id 1 [from/to] <Laptop ip addr> action [permit/deny]”  “ip-policy FW-1 id 2 [from/to] <Laptop ip addr> action [permit/deny]”  “ip-policy FW-1 id 3 [from/to] <Laptop ip addr> action [permit/deny]”  “…..”  “ip-policy FW-32”  “ip-policy FW-32 id 1 [from/to] <Laptop ip addr> action [permit/deny]”  “ip-policy FW-32 id 2 [from/to] <Laptop ip addr> action [permit/deny]”  “ip-policy FW-32 id 3 [from/to] <Laptop ip addr> action [permit/deny]”  …  “ip-policy FW-32 id 64 [from/to] <Laptop ip addr> action [permit/deny]”   1. Show the running config 2. Using before/after to change the policy’s sequence which is binding to FW   “ip-policy FW-[N] id X1 before/after id Y1”  “ip-policy FW-[N] id X2 before/after id Y2”  “…..”   1. Show the running config | | |
| Expect result | ~~- Laptop ping successfully on step 1), 2) and 3)~~  ~~- Config full policy successfully, and the running config shows the config-policies correctly on step 5).~~  ~~- If match the deny-policy, ping should be unsuccessful on step 6), else should be successful on step 6)~~  ~~- Change the policy’s sequence successfully, and the running config should be show the sequences correctly on step 8)~~  ~~- If match the deny-policy, ping should be unsuccessful on step 6), else should be successful on step 9)~~  2) Configure is shown correctly (The order is 1->64)  3) May show error info(ERROR: Invalid parameter(s))  5) Configure is shown correctly | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Perf\_10.10 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config maximum ip-policy, and config full policy in every ip-policy, change the binding relation. | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Gateway of SW ping Laptop each other 2. Server ping Laptop each other 3. AP1 ping Laptop each other 4. Config full policy by script and bind one of them to FW:   “ip-policy FW-0”  “ip-policy FW-0 id 1 [from/to] <Laptop ip addr> action [permit/deny]”  “ip-policy FW-0 id 2 [from/to] <Laptop ip addr> action [permit/deny]”  “ip-policy FW-0 id 3 [from/to] <Laptop ip addr> action [permit/deny]”  “…..”  “ip-policy FW-X”  “ip-policy FW-X id 1 [from/to] <Laptop ip addr> action [permit/deny]”  “ip-policy FW-X id 2 [from/to] <Laptop ip addr> action [permit/deny]”  “ip-policy FW-X id 3 [from/to] <Laptop ip addr> action [permit/deny]”  “user-profile FW security ip-policy [from/to]-access FW-[N]”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Show the running config 2. Repeat step 1-3 3. Binding another mac-policy to FW   “user-profile FW security ip-policy [from/to]-access FW-[M]”   1. Show the running config 2. Repeat step 1-3 | | |
| Expect result | - Laptop ping successfully on step 1), 2) and 3)  - Config full policy successfully, and the running config shows the config-policies correctly on step 5).  - If match the deny-policy, ping should be unsuccessful on step 6), else should be successful on step 6)  - Change binding relation successfully, and the running config should be show the binding relation correctly on step 8)  - If match the deny-policy, ping should be unsuccessful on step 6), else should be successful on step 9) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Perf\_10.11 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Establish maximum ip-session (config&resource check) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Configure ip-policy   ***“ip-policy fw”***  ***“ip-policy fw id 1 action permit”***  ***“user-profile {user-profile name} security ip-policy from-access fw to-access fw”***   1. Establish maximum ip-session by using script to send packets(such as Hping)   ***“hping3 192.168.30.225 -2 -c 10000 -I eth1 -i u1000”***   1. Show ip-session   ***AH-958280#show forwarding-engine ip-sessions | include entries***  ***Total entries: 8191/8191*** | | |
| Expect result | ~~- Establish maximum ip-session successfully, and the running config shows the ip-session correctly , the cpu & mem’s using are normal on step 2).~~  3)Total entries:8191/8191 | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Perf\_10.12 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Establish maximum ip-session & mac-session (config&resource check) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Configure mac-policy&ip-policy   ***“ip-policy fw”***  ***“ip-policy fw id 1 action permit”***  ***“user-profile {user-profile name} security ip-policy from-access fw to-access fw”***   1. Establish maximum Mac&IP-session by using script to send packets(such as pkt and Hping) 2. Show ip/mac session   ***AH-8c6f80#show forwarding-engine ip-sessions | include entries***  ***Total entries: 8191/8191***  ***AH-8c6f80#show forwarding-engine mac-sessions | include entries***  ***Total entries: 8191/8191*** | | |
| Expect result | ~~- Establish maximum ip-session & mac-session successfully, and the running config shows the ip-session & mac-session correctly , the cpu & mem’s using are normal on step 2).~~  3) ***Total entries: 8191/8191*** | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Perf\_10.13 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config maximum ip-policy, and config full policy in every ip-policy, and every ip-policy to an user-profile, using one SSID(config&resource check) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Config full policy by script and bind every ip-policy to an user-profile:   “ip-policy FW-0”  “ip-policy FW-0 id 1 [from/to] <Laptop ip addr> action [permit/deny]”  “ip-policy FW-0 id 2 [from/to] <Laptop ip addr> action [permit/deny]”  “ip-policy FW-0 id 3 [from/to] <Laptop ip addr> action [permit/deny]”  “…..”  “ip-policy FW-X”  “ip-policy FW-X id 1 [from/to] <Laptop ip addr> action [permit/deny]”  “ip-policy FW-X id 2 [from/to] <Laptop ip addr> action [permit/deny]”  “ip-policy FW-X id 3 [from/to] <Laptop ip addr> action [permit/deny]”  “user-profile FW-[N] security ip-policy [from/to]-access FW-[N]”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Show the running config and check the resource consuming | | |
| Expect result | - Config full policy,and bind to user-pofile successfully, and the running config shows the config-policies and binding-relation correctly , the cpu & mem’s using are normal on step 2). | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Perf\_10.14 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config maximum ip-policy, and config full policy in every ip-policy, and every ip-policy to an user-profile, using multi-SSID(config&resource check) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Config full policy by script and bind every ip-policy to an user-profile:   “ip-policy FW-0”  “ip-policy FW-0 id 1 [from/to] <Laptop ip addr> action [permit/deny]”  “ip-policy FW-0 id 2 [from/to] <Laptop ip addr> action [permit/deny]”  “ip-policy FW-0 id 3 [from/to] <Laptop ip addr> action [permit/deny]”  “…..”  “ip-policy FW-X”  “ip-policy FW-X id 1 [from/to] <Laptop ip addr> action [permit/deny]”  “ip-policy FW-X id 2 [from/to] <Laptop ip addr> action [permit/deny]”  “ip-policy FW-X id 3 [from/to] <Laptop ip addr> action [permit/deny]”  “user-profile FW-[N] security ip-policy [from/to]-access FW-[N]”  “ssid ssid[N] default-user-profile-attr [num]”   1. Show the running config and check the resource consuming | | |
| Expect result | - Config full policy,and bind to user-pofile successfully, and the running config shows the config-policies and binding-relation correctly , the cpu & mem’s using are normal on step 2). | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Perf\_10.15 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config maximum ip-policy & mac-policy, and config full policy in every ip-policy & mac-policy, and every ip-policy & mac-policy to an user-profile, using one SSID(config&resource check) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Config full policy by script and bind every ip-policy & mac-policy to an user-profile:   “[ip/mac]-policy FW-0”  “[ip/mac]-policy FW-0 id 1 [from/to] <Laptop [ip/mac] addr> action [permit/deny]”  “[ip/mac]-policy FW-0 id 2 [from/to] <Laptop [ip/mac] addr> action [permit/deny]”  “[ip/mac]-policy FW-0 id 3 [from/to] <Laptop [ip/mac] addr> action [permit/deny]”  “…..”  “[ip/mac]-policy FW-X”  “[ip/mac]-policy FW-X id 1 [from/to] <Laptop [ip/mac]addr> action [permit/deny]”  “[ip/mac]-policy FW-X id 2 [from/to] <Laptop [ip/mac]addr> action [permit/deny]”  “[ip/mac]-policy FW-X id 3 [from/to] <Laptop [ip/mac]addr> action [permit/deny]”  “user-profile FW-[N] security [ip/mac]-policy [from/to]-access FW-[N]”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Show the running config and check the resource consuming | | |
| Expect result | - Config full policy,and bind to user-pofile successfully, and the running config shows the config-policies and binding-relation correctly , the cpu & mem’s using are normal on step 2). | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Perf\_10.16 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Config maximum ip-policy & mac-policy, and config full policy in every ip-policy & mac-policy, and every ip-policy & mac-policy to an user-profile, using multi-SSID(config&resource check) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address | | |
| Test procedure | 1. Config full policy by script and bind every ip-policy & mac-policy to an user-profile:   “[ip/mac]-policy FW-0”  “[ip/mac]-policy FW-0 id 1 [from/to] <Laptop [ip/mac] addr> action [permit/deny]”  “[ip/mac]-policy FW-0 id 2 [from/to] <Laptop [ip/mac] addr> action [permit/deny]”  “[ip/mac]-policy FW-0 id 3 [from/to] <Laptop [ip/mac] addr> action [permit/deny]”  “…..”  “[ip/mac]-policy FW-X”  “[ip/mac]-policy FW-X id 1 [from/to] <Laptop [ip/mac]addr> action [permit/deny]”  “[ip/mac]-policy FW-X id 2 [from/to] <Laptop [ip/mac]addr> action [permit/deny]”  “[ip/mac]-policy FW-X id 3 [from/to] <Laptop [ip/mac]addr> action [permit/deny]”  “user-profile FW-[N] security [ip/mac]-policy [from/to]-access FW-[N]”  “ssid ssid[N] default-user-profile-attr [num]”   1. Show the running config and check the resource consuming | | |
| Expect result | - Config full policy,and bind to user-pofile successfully, and the running config shows the config-policies and binding-relation correctly , the cpu & mem’s using are normal on step 2). | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Perf\_10.17 | | |
| **Priority** | High | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Maximum fragments are sent in one FCB(config&resource check) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW”(32) | | |
| Test procedure | 1. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW from<Laptop ip addr> action permit”  “user-profile FW security ip-policy [from/to]-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Server sends Maximum fragments in one FCB to Laptop using hping2 or other tools(laptop send pkt size 1500\*32) 2. Check the the fragment packets on AP1 | | |
| Expect result | ~~- AP1 should process the fragment packets, and show the maximum fragments in one FCB correctly, if the fragments are integrity, AP1 should reassemble the fragments to a complete packets, then sends it to Laptop; Laptop should receive the complete packet.~~  ~~- The cpu & mem’s using are normal on step 3)~~  3) AP can receive the pkt successfully | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Perf\_10.18 | | |
| **Priority** | Low | **Automation Flag** | No |
| Topology to use | Laptop ------ AP1 ------ SW ------ Server | | |
| Description | Maximum fragments are sent in maximum FCBs(config&resource check) | | |
| Pre-condition | -Laptop has been associated with AP1 and assigned an ip address  -Laptop uses user-profile “FW” | | |
| Test procedure | 1. Configure a ip-policy and bind it to FW:   “ip-policy FW”  “ip-policy FW [from/to] <Laptop ip addr> action permit”  “user-profile FW security ip-policy [from/to]-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Server sends Maximum fragments in maximum FCBs to Laptop using hping2 or other tools 2. Check the the fragment packets on AP1 | | |
| Expect result | - AP1 should process the fragments, and show the maximum fragments in every FCB correctly, if the fragments are integrity, AP1 should reassemble the fragments to a complete packets, then sends it to Laptop; Laptop should receive the complete packet.  - The cpu & mem’s using are normal on step 3) | | |
| Test result |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| ~~Case ID~~ | ~~FW\_IP\_Policy\_Perf\_10.19~~ | | |
| **~~Priority~~** | ~~Low~~ | **~~Automation Flag~~** | ~~NA~~ |
| ~~Topology to use~~ | ~~Laptop ------ AP1 ------ SW ------ Server~~ | | |
| ~~Description~~ | ~~Maximum Mac sessions on a AP~~ | | |
| ~~Pre-condition~~ | ~~-Configure AP1~~  *~~“security-object FWtest”~~*  *~~“security-object FWtest default-user-profile-attr 1”~~*  *~~“ssid FWtest”~~*  *~~“ssid FWtest security-object FWtest”~~*  *~~“interface wifi0 ssid FWtest”~~*  *~~“interface wifi1 ssid FWtest”~~*  *~~“user-profile FW qos-policy def-user-qos vlan-id <mgt0 vlan> attribute 1”~~*  ~~-Laptop has been associated with AP1 and assigned an ip address~~  ~~-Laptop uses user-profile “FW”~~ | | |
| ~~Test procedure~~ | ~~1.Laptop uses tool (such as pkt) send (random source mac)packets to AP1~~  ~~2.Show total entries of the mac-sessions~~  ***~~“show forwarding-engine mac-sessions | include total”~~*** | | |
| ~~Expect result~~ | ~~2.~~~~CW350#show forwarding-engine mac-sessions | include total~~  ~~Total entries:8191/8191~~ | | |
| ~~Test result~~ |  | | |

|  |  |  |  |
| --- | --- | --- | --- |
| ~~Case ID~~ | ~~FW\_IP\_Policy\_Perf\_10.20~~ | | |
| **~~Priority~~** | ~~Low~~ | **~~Automation Flag~~** | ~~NA~~ |
| ~~Topology to use~~ | ~~Laptop ------ AP1 ------ SW ------ Server~~ | | |
| ~~Description~~ | ~~Maximum IP sessions on a AP~~ | | |
| ~~Pre-condition~~ | ~~-Configure AP1~~  *~~“security-object FWtest”~~*  *~~“security-object FWtest default-user-profile-attr 1”~~*  *~~“ssid FWtest”~~*  *~~“ssid FWtest security-object FWtest”~~*  *~~“interface wifi0 ssid FWtest”~~*  *~~“interface wifi1 ssid FWtest”~~*  *~~“user-profile FW qos-policy def-user-qos vlan-id <mgt0 vlan> attribute 1”~~*  ~~-Laptop has been associated with AP1 and assigned an ip address~~  ~~-Laptop uses user-profile “FW”~~ | | |
| ~~Test procedure~~ | ~~1.Config IP policy rules~~  ***~~“ip-policy FW”~~***  ***~~“ip-policy FW from <Laptop ip addr> action permit”~~***  ***~~“ip-policy FW to <Laptop ip addr> action permit”~~***  ***~~“user-profile FW security ip-policy from-access FW to-access FW~~***  ***~~“clear forwarding-engine ip-sessions”~~***  ~~2.Laptop uses tool (such as hping) send (random port UDP)packets to AP1~~  ~~“hping3 <server IP> -2 –p 69 –i u100 –c 9000”~~  ~~3.Show total entries of the mac-sessions~~  ***~~“show forwarding-engine ip-sessions | include total”~~*** | | |
| ~~Expect result~~ | ~~3.~~~~CW350#show forwarding-engine ip-sessions | include total~~  ~~Total entries:8191/8191~~ | | |
| ~~Test result~~ |  | | |

## 8.11 Support Hostname test

### Basic function test

#### 8.11.1.1 Single “from” policy permit test

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Host\_11.1 | | |
| Priority | High | Automation Flag | No |
| Topology to use | Laptop (hostname1) ------ AP1 ------ SW ------ Server (hostname2) | | |
| Description | Config single “from” policy(permit) | | |
| Pre-condition | Configure the dns server right which can resolve the hostname in ip-policy | | |
| Test procedure | 1. Laptop ping gateway of SW 2. Laptop ping Server 3. Laptop ping AP1 4. Configure a L3 policy and bind it to FW:   ***“ip-policy FW”***  ***“ip-policy FW from < hostname1> action permit”***  ***“user-profile FW security ip-policy from-access FW to-access FW”***   1. Repeat step 1-3 | | |
| Expect result | - Laptop ping successfully on step 1), 2) and 3)  - Laptop ping successfully on step 5) | | |

#### 8.11.1.2 Single “to” policy deny test

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Host\_11.2 | | |
| Priority | Accept | Automation Flag | No |
| Topology to use | Laptop (hostname1) ------ AP1 ------ SW ------ Server (hostname2) | | |
| Description | Config single “to” policy(deny) | | |
| Pre-condition | **-Configure the dns server right which can resolve the hostname in ip-policy**  -Configure AP1  *“security-object FWtest”*  *“security-object FWtest default-user-profile-attr 1”*  *“ssid FWtest”*  *“ssid FWtest security-object FWtest”*  *“interface wifi0 ssid FWtest”*  *“interface wifi1 ssid FWtest”*  *“user-profile FW qos-policy def-user-qos vlan-id <mgt0 vlan> attribute 1”*  -Laptop has been associated with AP1 and assigned an ip address  **-Laptop uses user-profile “FW”** | | |
| Test procedure | 1. Laptop ping www.google.com.hk 2. Configure a L3 policy and bind it to FW:   ***“ip-policy FW”***  ***“ip-policy FW to www.google.com.hk action deny”***  ***“ip-policy FW action permit”***  ***“user-profile FW security ip-policy from-access FW to-access FW”***  ***“clear forwarding-engine ip-sessions”***   1. Repeat step 1 | | |
| Expect result | - Laptop ping successfully on step 1)  - Laptop ping unsuccessfully on step 3) | | |

### Hostname resolve test

#### 8.11.2.1 Hosname resolve test

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Host\_11.3 | | |
| Priority | High | Automation Flag | No |
| Topology to use | Laptop (hostname1) ------ AP1 ------ SW ------ Server (hostname2) | | |
| Description | Hostname resolve in normal condition | | |
| Pre-condition | Configure the dns server right which can resolve the hostname in ip-policy, and 4 items maximum | | |
| Test procedure | 1. Configure a L3 policy with hostname which can be resolved many ips:   “ip-policy FW”  “ip-policy FW from/to < www.163.com> action permit/deny”  “user-profile FW security ip-policy from/to-access FW”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Show ip-policy, result 1 2. Show ip-policy by internal cli “Show ip-policy FW \_”, result 2 | | |
| Expect result | - there is ip-policy about the configured hostname, such as “ip-policy FW from/to < www.163.com> action permit/deny”.  - there are several ip policy rules set to FE, suppose [www.163.com](http://www.163.com) resolve to 10.10.10.11---10.10.10.14, there are will be 4 rules in FE, such as  Ip-policy FW id 10 from 10.10.10.11 255.255.255.255 action permit/deny  Ip-policy FW id 11 from 10.10.10.12 255.255.255.255 action permit/deny  Ip-policy FW id 12 from 10.10.10.13 255.255.255.255 action permit/deny Ip-policy FW id 14 from 10.10.10.14 255.255.255.255 action permit/deny | | |

#### 8.11.2.2 Hosname resolve with ap’s ip test

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Host\_11.4 | | |
| Priority | High | Automation Flag | No |
| Topology to use | Laptop (hostname1) ------ AP1 ------ SW ------ Server (hostname2) | | |
| Description | Hostname resolve with ap’s ip test | | |
| Pre-condition | Configure the dns server right which can resolve the hostname in ip-policy, and 4 items maximum | | |
| Test procedure | 1. Configure a L3 policy with hostname which can be resolved many ips:   “ip-policy FW”  “ip-policy FW from/to < www.163.com> action permit/deny”  “user-profile FW security ip-policy from/to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Show ip-policy, result 1 2. Show ip-policy by internal cli “Show ip-policy FW \_”, result 2 3. Reboot ap, show fe debug info, result 3 | | |
| Expect result | - There is ip-policy about the configured hostname, such as “ip-policy FW from/to < www.163.com> action permit/deny”.  - There are several ip policy rules set to FE, suppose [www.163.com](http://www.163.com) resolve to 10.10.10.11---10.10.10.14, there are will be 4 rules in FE, such as  Ip-policy FW id 10 from 10.10.10.11 255.255.255.255 action permit/deny  Ip-policy FW id 11 from 10.10.10.12 255.255.255.255 action permit/deny  Ip-policy FW id 12 from 10.10.10.13 255.255.255.255 action permit/deny Ip-policy FW id 14 from 10.10.10.14 255.255.255.255 action permit/deny  - While ap brings up, make sure it should not send the dns request for hostname if doesn’t get ip; after getting ip, ap will send the request to dns server | | |

### Compatibility test

#### 8.11.3.1 Mix configuration test

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Host\_11.5 | | |
| Priority | Accept | Automation Flag | No |
| Topology to use | Laptop (hostname1) ------ AP1 ------ SW ------ Server (hostname2) | | |
| Description | Mix configuration ip-policy with hostname and ip | | |
| Pre-condition | **-Configure the dns server right which can resolve the hostname in ip-policy**  -Configure AP1  *“security-object FWtest”*  *“security-object FWtest default-user-profile-attr 1”*  *“ssid FWtest”*  *“ssid FWtest security-object FWtest”*  *“interface wifi0 ssid FWtest”*  *“interface wifi1 ssid FWtest”*  *“user-profile FW qos-policy def-user-qos vlan-id <mgt0 vlan> attribute 1”*  -Laptop has been associated with AP1 and assigned an ip address  **-Laptop uses user-profile “FW”** | | |
| Test procedure | 1. Laptop ping www.google.com.hk, result 1 2. Configure a L3 policy with ip and hostname and action is deny:   ***“ip-policy FW”***  ***“ip-policy FW from <laptop\_ip> to www.google.com.hk action deny”***  ***“ip-policy FW action permit”***  ***“user-profile FW security ip-policy from-access FW to-access FW”***  ***“clear forwarding-engine ip-sessions”***   1. Show ip-policy, result 1   ***“show ip-policy FW \_”***   1. Laptop ping www.google.com.hk, result 2 | | |
| Expect result | - Laptop ping successfully on step 1)  - Hostname can be resolved to 4 IP addresses on step 3)  - Laptop ping unsuccessfully on step 4) | | |

#### 8.11.3.2 Configuration overwrite test

##### 8.11.3.2.1 Configuration overwrite with hostname to ip

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Host\_11.6 | | |
| Priority | High | Automation Flag | No |
| Topology to use | Laptop (hostname1) ------ AP1 ------ SW ------ Server (hostname2) | | |
| Description | Configuration overwrite with hostname to ip | | |
| Pre-condition | Configure the dns server right which can resolve the hostname in ip-policy, and 4 items maximum | | |
| Test procedure | 1. Laptop ping www.google.com.hk, result 1 2. Configure a L3 policy with ip and action is deny:   ***“ip-policy FW”***  ***“ip-policy FW id 1 from <laptop\_ip> action deny”***  ***“user-profile FW security ip-policy from-access FW to-access FW”***   1. Show ip-policy, result 1 2. Laptop ping www.google.com.hk, result 2 3. Overwrite configuration ip-policy by hostname and action is permit:   ***“ip-policy FW id 1 from <hostname1> action permit”***   1. Check the overwrite id’s order, result 3 2. Laptop ping Server, result 4 | | |
| Expect result | - Laptop ping successfully on step 1)  - There is ip-policy about the configured ip, such as “ip-policy FW from <laptop\_ip> action deny”.  - Laptop ping unsuccessfully on step 4)  - There is ip-policy about the configured hostname, such as “ip-policy FW from < hostname1> action permit”  - The new overwrite id’s order is the same as former’s on step 6)  - Laptop ping successfully on step 7) | | |

##### 8.11.3.2.2 Configuration overwrite with ip to hostname

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Host\_11.7 | | |
| Priority | High | Automation Flag | No |
| Topology to use | Laptop (hostname1) ------ AP1 ------ SW ------ Server (hostname2) | | |
| Description | Configuration overwrite with ip to hostname | | |
| Pre-condition | Configure the dns server right which can resolve the hostname in ip-policy, and 4 items maximum | | |
| Test procedure | 1. Laptop ping Server, result 1 2. Configure a L3 policy with hostname and action is deny:   “ip-policy FW”  “ip-policy FW id 1 from <hostname1> action deny”  “user-profile FW security ip-policy from-access FW ***to-access FW***”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Show ip-policy, result 1 2. Laptop ping Server, result 2 3. Overwrite configuration ip-policy by ip and action is permit:   “ip-policy FW id 1 from <laptop\_ip> action permit”   1. Check the overwrite id’s order, result 3 2. Laptop ping Server, result 4 | | |
| Expect result | - Laptop ping successfully on step 1)  - There is ip-policy about the configured hostname, such as “ip-policy FW from < hostname1> action deny”.  - Laptop ping unsuccessfully on step 4)  - There is ip-policy about the configured ip, such as “ip-policy FW from <laptop\_ip> action permit”  - The new overwrite id’s order is the same as former’s on step 6)  - Laptop ping successfully on step 7) | | |

#### 8.11.3.3 “Before” and “After” operation test

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Host\_11.8 | | |
| Priority | High | Automation Flag | No |
| Topology to use | Laptop (hostname1) ------ AP1 ------ SW ------ Server (hostname2) | | |
| Description | “Before” and “After” operation test | | |
| Pre-condition | Configure the dns server right which can resolve the hostname in ip-policy, and 4 items maximum | | |
| Test procedure | 1. Laptop ping Server, result 1 2. Configure a L3 policy with hostname and ip, including many ID:   “ip-policy FW”  “ip-policy FW id 1 from <hostname1> action deny”  “ip-policy FW id 2 from <hostname1> action permit”  “ip-policy FW id 3 from <laptop\_ip> action permit”  “user-profile FW security ip-policy from-access FW ***to-access FW***”  ~~“ssid <ssid\_name> default-user-profile-attr [num]”~~   1. Show ip-policy, result 1 2. Laptop ping Server, result 2 3. Show ip-policy by internal cli “Show ip-policy FW \_”, result 3 4. Change the id’s order by “Before” and “After” operation 5. Check the rules by internal cli “Show ip-policy FW \_”, result 4 | | |
| Expect result | - Laptop ping successfully on step 1)  - There is ip-policy about the configured hostname, such as  “ip-policy FW id 1 from <hostname1> action deny”  “ip-policy FW id 2 from <hostname1> action permit”  “ip-policy FW id 3 from <laptop\_ip> action permit”  - There is ip-policy about the configured ip, and configured with hostname id includes several rules, all rules are ordered by configuration on step 5)  - All rules’ order are identical to the operation, iid will be moded as together on step 7) | | |

#### 8.11.3.4 Compatibility with TV ip-policy test

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Host\_11.9 | | |
| Priority | Low | Automation Flag | No |
| Topology to use | Laptop (hostname1) ------ AP1 ------ SW ------ Server (hostname2) | | |
| Description | Compatibility with TV ip-policy test | | |
| Pre-condition | Configure the dns server right which can resolve the hostname in ip-policy, and 4 items maximum | | |
| Test procedure | 1. Laptop ping Server, result 1 2. Configure maximum L3 policies with hostname and action is deny:   “ip-policy FW1”  “ip-policy FW1 id 1 from <hostname1> to <hostname2> action deny”  “ip-policy FW1 id 2 from <hostname3> to <hostname4> action deny”  ….  “ip-policy FW1 id n from <hostnameN> to <hostnameM> action deny”  “user-profile FW1 security ip-policy from/to-access FW1”  “ip-policy FW2”  “ip-policy FW2 id 1 from <hostname1> to <hostname2> action permit”  “ip-policy FW2 id 2 from <hostname3> to <hostname4> action permit”  ….  “ip-policy FW2 id n from <hostnameN> to <hostnameM> action permit”  “user-profile FW2 security ip-policy from/to-access FW1”   1. Show ip-policy, result 1 2. Laptop ping Server, result 2 3. Configure TV maximum ip-policy to ap 4. Laptop ping Server, result 3 | | |
| Expect result | - Laptop ping successfully on step 1)  - There is ip-policy about the configured ip, such as  “ip-policy FW1 id 1 from <hostname1> to <hostname2> action deny”  “ip-policy FW1 id 2 from <hostname3> to <hostname4> action deny”  ….  “ip-policy FWN id n from <hostnameN> to <hostnameM> action deny”  - Laptop ping unsuccessfully on step 4)  - There is ip-policy about the configured hostname, such as “ip-policy FW from < hostname1> action permit”  - Laptop ping unsuccessfully on step 6), and no abnormal occurs on ap | | |

### Capability test

#### 8.11.4.1 Maximum resolved items in one rule

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Host\_11.10 | | |
| Priority | Low | Automation Flag | No |
| Topology to use | Laptop (hostname1) ------ AP1 ------ SW ------ Server (hostname2) | | |
| Description | Maximum resolved items in one rule test | | |
| Pre-condition | Configure the dns server right which can resolve the hostname in ip-policy, and every hostname can be resolved at least 4 items | | |
| Test procedure | 1. Configure a L3 policy both from and to with hostname:   “ip-policy FW”  “ip-policy FW id 1 from <hostname1> to <hostname2> action deny”  “user-profile FW security ip-policy from/to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Show ip-policy, result 1 2. Show ip-policy by internal cli “Show inter-ip-policy FW to display”, result 2 | | |
| Expect result | - There is ip-policy about the configured hostname, such as “ip-policy FW from <hostname1> to <hostname2> action deny”.  - There is ip-policy about the configured ip, and there are 16 rule in FE, Suppose hostname1 resolve to 10.10.10.11---10.10.10.14 hostname2 resolve to  [20.20.20.11](http://www.google.com)---[20.20.20.14](http://www.google.com)) Set to FE:  Ip-policy policy-name id 10 from 10.10.10.11 255.255.255.255 to [20.20.20.11](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 11 from 10.10.10.12 255.255.255.255 to [20.20.20.11](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 12 from 10.10.10.13 255.255.255.255 to [20.20.20.11](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 13 from 10.10.10.14 255.255.255.255 to [20.20.20.11](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 14 from 10.10.10.11 255.255.255.255 to [20.20.20.12](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 15 from 10.10.10.12 255.255.255.255 to [20.20.20.12](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 16 from 10.10.10.13 255.255.255.255 to [20.20.20.12](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 17from 10.10.10.14 255.255.255.255 to [20.20.20.12](http://www.google.com) 255.255.255.255  ……….  Ip-policy policy-name id 22 from 10.10.10.11 255.255.255.255 to [20.20.20.14](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 23 from 10.10.10.12 255.255.255.255 to [20.20.20.14](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 24 from 10.10.10.13 255.255.255.255 to [20.20.20.14](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 25 from 10.10.10.14 255.255.255.255 to [20.20.20.14](http://www.google.com) 255.255.255.255 | | |

#### 8.11.4.2 Maximum resolved items in one policy

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Host\_11.11 | | |
| Priority | Low | Automation Flag | No |
| Topology to use | Laptop (hostname1) ------ AP1 ------ SW ------ Server (hostname2) | | |
| Description | Maximum resolved items in one policy test | | |
| Pre-condition | Configure the dns server right which can resolve the hostname in ip-policy, and every hostname can be resolved, maximum is 1023 rules in one policy | | |
| Test procedure | 1. Configure a L3 policy both from and to with hostname:   “ip-policy FW1”  “ip-policy FW1 id 1 from <hostname1> to <hostname2> action deny”  “ip-policy FW1 id 2 from <hostname3> to <hostname4> action deny”  ….  “ip-policy FW1 id n from <hostnameN> to <hostnameM> action deny”  “user-profile FW1 security ip-policy from/to-access FW1”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Show ip-policy, result 1 2. Show ip-policy by internal cli “Show inter-ip-policy FW to display”, result 2 | | |
| Expect result | - There is ip-policy about the configured hostname, such as  “ip-policy FW id 1 from <hostname1> to <hostname2> action deny”  “ip-policy FW id 2 from <hostname3> to <hostname4> action deny”  ….  “ip-policy FW id n from <hostnameN> to <hostnameM> action deny”  - There is ip-policy about the configured hostname, and there are 1023 rules in FE, others will be invalid.  Suppose hostname1 resolve to 10.10.10.11---10.10.10.14 hostname2 resolve to  [20.20.20.11](http://www.google.com)---[20.20.20.14](http://www.google.com)) Set to FE:  Ip-policy policy-name id 10 from 10.10.10.11 255.255.255.255 to [20.20.20.11](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 11 from 10.10.10.12 255.255.255.255 to [20.20.20.11](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 12 from 10.10.10.13 255.255.255.255 to [20.20.20.11](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 13 from 10.10.10.14 255.255.255.255 to [20.20.20.11](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 14 from 10.10.10.11 255.255.255.255 to [20.20.20.12](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 15 from 10.10.10.12 255.255.255.255 to [20.20.20.12](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 16 from 10.10.10.13 255.255.255.255 to [20.20.20.12](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 17from 10.10.10.14 255.255.255.255 to [20.20.20.12](http://www.google.com) 255.255.255.255  ……….  Ip-policy policy-name id 22 from 10.10.10.11 255.255.255.255 to [20.20.20.14](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 23 from 10.10.10.12 255.255.255.255 to [20.20.20.14](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 24 from 10.10.10.13 255.255.255.255 to [20.20.20.14](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 25 from 10.10.10.14 255.255.255.255 to [20.20.20.14](http://www.google.com) 255.255.255.255 | | |

#### 8.11.4.3 Maximum resolved items on ap

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Host\_11.12 | | |
| Priority | Low | Automation Flag | No |
| Topology to use | Laptop (hostname1) ------ AP1 ------ SW ------ Server (hostname2) | | |
| Description | Maximum resolved items on ap test | | |
| Pre-condition | Configure the dns server right which can resolve the hostname in ip-policy, and every hostname can be resolved, maximum is 1023\*32 rules on ap | | |
| Test procedure | 1. Configure a maximum L3 policies both from and to with hostname:   “ip-policy FW1”  “ip-policy FW1 id 1 from <hostname1> to <hostname2> action deny”  “ip-policy FW1 id 2 from <hostname3> to <hostname4> action deny”  ….  “ip-policy FW1 id n from <hostnameN> to <hostnameM> action deny”  “user-profile FW1 security ip-policy from/to-access FW1”  “ip-policy FW2”  “ip-policy FW2 id 1 from <hostname1> to <hostname2> action permit”  “ip-policy FW2 id 2 from <hostname3> to <hostname4> action permit”  ….  “ip-policy FW2 id n from <hostnameN> to <hostnameM> action permit”  “user-profile FW2 security ip-policy from/to-access FW1”   1. Show ip-policy, result 1 2. Show ip-policy by internal cli “Show inter-ip-policy FW to display”, result 2 3. Delete one hostname ID in a ip-policy, the add it again, result 3 | | |
| Expect result | - There are ip-policies on ap about the configured hostname, such as  “ip-policy FW1 id 1 from <hostname1> to <hostname2> action deny”  “ip-policy FW1 id 2 from <hostname3> to <hostname4> action deny”  ….  “ip-policy FWN id n from <hostnameN> to <hostnameM> action deny”  - There are ip-policies about the configured hostname, and there are 32736 rules in FE, others will be invalid.  Suppose hostname1 resolve to 10.10.10.11---10.10.10.14 hostname2 resolve to  [20.20.20.11](http://www.google.com)---[20.20.20.14](http://www.google.com)) Set to FE:  Ip-policy policy-name id 10 from 10.10.10.11 255.255.255.255 to [20.20.20.11](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 11 from 10.10.10.12 255.255.255.255 to [20.20.20.11](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 12 from 10.10.10.13 255.255.255.255 to [20.20.20.11](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 13 from 10.10.10.14 255.255.255.255 to [20.20.20.11](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 14 from 10.10.10.11 255.255.255.255 to [20.20.20.12](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 15 from 10.10.10.12 255.255.255.255 to [20.20.20.12](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 16 from 10.10.10.13 255.255.255.255 to [20.20.20.12](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 17from 10.10.10.14 255.255.255.255 to [20.20.20.12](http://www.google.com) 255.255.255.255  ……….  Ip-policy policy-name id 22 from 10.10.10.11 255.255.255.255 to [20.20.20.14](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 23 from 10.10.10.12 255.255.255.255 to [20.20.20.14](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 24 from 10.10.10.13 255.255.255.255 to [20.20.20.14](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 25 from 10.10.10.14 255.255.255.255 to [20.20.20.14](http://www.google.com) 255.255.255.255  -Through internal cli “Show inter-ip-policy FW to display” can see the the hostname ID is deleted includes the iid rules, then both the ID and iid are created again, make sure the iid is can be reuse | | |

### Negative test

#### 8.11.5.1 Configure hostname without DNS server

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Host\_11.13 | | |
| Priority | Low | Automation Flag | No |
| Topology to use | Laptop (hostname1) ------ AP1 ------ SW ------ Server (hostname2) | | |
| Description | Config ip-policy with hostname but no DNS server | | |
| Pre-condition | No dns server configuration | | |
| Test procedure | 1. Configure a L3 policy with hostname:   “ip-policy FW”  “ip-policy FW to < www.163.com> action permit”  “user-profile FW security ip-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Show ip-policy, result 1 2. Show ip-policy by internal cli “Show inter-ip-policy FW to display”, result 2 3. Laptop ping [www.163.com](http://www.163.com), result 3 4. Configure dns server make sure it can resolve the hostname item, result 4 5. Laptop ping [www.163.com](http://www.163.com), result 5 | | |
| Expect result | - there is ip-policy about the configured hostname, such as “ip-policy FW to <www.163.com> action permit”.  - There is no ip policy rules set to FE because there is no dns server configuration.  - Laptop ping unsuccessfully on step 4), and error info about dns configuration will be shown on ap  - ap resolves the hostname successfully, through internal cli “Show inter-ip-policy FW to display” can see the hostname is convert to ip and be set to FE  - Laptop ping unsuccessfully on step 6) | | |

#### 8.11.5.2 Configure DNS server but it can’t resolve the hostname

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Host\_11.14 | | |
| Priority | Low | Automation Flag | No |
| Topology to use | Laptop (hostname1) ------ AP1 ------ SW ------ Server (hostname2) | | |
| Description | Config ip-policy with hostname but they can’t be resolved by the dns server | | |
| Pre-condition | Configure dns server but it can’t resolve the hostname in ip-policy | | |
| Test procedure | 1. Configure a L3 policy with hostname:   “ip-policy FW”  “ip-policy FW to < www.163.com> action permit”  “user-profile FW security ip-policy to-access FW”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Show ip-policy, result 1 2. Show ip-policy by internal cli “Show inter-ip-policy FW to display”, result 2 3. Laptop ping [www.163.com](http://www.163.com), result 3 4. Configure dns server make sure it can resolve the hostname item, result 4 5. Laptop ping [www.163.com](http://www.163.com), result 5 | | |
| Expect result | - There is ip-policy about the configured hostname, such as “ip-policy FW to <www.163.com> action permit”.  - There is no ip policy rules set to FE because hostname can’t be resolved by dns server.  - Laptop ping unsuccessfully on step 4), info about dns resolve timeout will be shown on ap, and ap will send dns request periodly. (1 min?)  - ap resolves the hostname successfully, through internal cli “Show inter-ip-policy FW to display” can see the hostname is convert to ip and be set to FE  - Laptop ping unsuccessfully on step 6) | | |

#### 8.11.5.3 Configure hostname resolved items exceed the maximum in one policy

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Host\_11.15 | | |
| Priority | Low | Automation Flag | No |
| Topology to use | Laptop (hostname1) ------ AP1 ------ SW ------ Server (hostname2) | | |
| Description | Configure hostname resolved items exceed the maximum in one policy | | |
| Pre-condition | Configure the dns server right which can resolve the hostname in ip-policy, and every hostname can be resolved, maximum is 1023 rules in one policy | | |
| Test procedure | 1. Configure a L3 policy both from and to with hostname:   “ip-policy FW1”  “ip-policy FW1 id 1 from <hostname1> to <hostname2> action deny”  “ip-policy FW1 id 2 from <hostname3> to <hostname4> action deny”  ….  “ip-policy FW1 id n from <hostnameN> to <hostnameM> action deny”  “user-profile FW1 security ip-policy from/to-access FW1”  “ssid <ssid\_name> default-user-profile-attr [num]”   1. Show ip-policy, result 1 2. Show ip-policy by internal cli “Show inter-ip-policy FW to display”, result 2 3. Configure more hostname rule in the same policy, make sure the total rules exceed the maximum in one policy, result 3 | | |
| Expect result | - There are ip policies about the configured hostname, such as  “ip-policy FW1 id 1 from <hostname1> to <hostname2> action deny”  “ip-policy FW1 id 2 from <hostname3> to <hostname4> action deny”  ….  “ip-policy FWN id n from <hostnameN> to <hostnameM> action deny”  - There are ip-policies about the configured hostname, and there are nearly 1023 (1000?) rules in FE  Suppose hostname1 resolve to 10.10.10.11---10.10.10.14 hostname2 resolve to  [20.20.20.11](http://www.google.com)---[20.20.20.14](http://www.google.com)) Set to FE:  Ip-policy policy-name id 10 from 10.10.10.11 255.255.255.255 to [20.20.20.11](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 11 from 10.10.10.12 255.255.255.255 to [20.20.20.11](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 12 from 10.10.10.13 255.255.255.255 to [20.20.20.11](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 13 from 10.10.10.14 255.255.255.255 to [20.20.20.11](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 14 from 10.10.10.11 255.255.255.255 to [20.20.20.12](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 15 from 10.10.10.12 255.255.255.255 to [20.20.20.12](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 16 from 10.10.10.13 255.255.255.255 to [20.20.20.12](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 17from 10.10.10.14 255.255.255.255 to [20.20.20.12](http://www.google.com) 255.255.255.255  ……….  Ip-policy policy-name id 22 from 10.10.10.11 255.255.255.255 to [20.20.20.14](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 23 from 10.10.10.12 255.255.255.255 to [20.20.20.14](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 24 from 10.10.10.13 255.255.255.255 to [20.20.20.14](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 25 from 10.10.10.14 255.255.255.255 to [20.20.20.14](http://www.google.com) 255.255.255.255  - There is ip-policy about the configured hostname, and there are 1023 rules in FE, others will be invalid | | |

#### 8.11.5.4 Configure hostname resolved items exceed the maximum on ap

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Host\_11.16 | | |
| Priority | Low | Automation Flag | No |
| Topology to use | Laptop (hostname1) ------ AP1 ------ SW ------ Server (hostname2) | | |
| Description | Configure hostname resolved items exceed the maximum on ap | | |
| Pre-condition | Configure the dns server right which can resolve the hostname in ip-policy, and every hostname can be resolved, maximum is 1023\*32 rules in one policy | | |
| Test procedure | 1. Configure many L3 policies both from and to with hostname, but don’t exceed the maximum of ap:   “ip-policy FW1”  “ip-policy FW1 id 1 from <hostname1> to <hostname2> action deny”  “ip-policy FW1 id 2 from <hostname3> to <hostname4> action deny”  ….  “ip-policy FW1 id n from <hostnameN> to <hostnameM> action deny”  “user-profile FW1 security ip-policy from/to-access FW1”  “ip-policy FW2”  “ip-policy FW2 id 1 from <hostname1> to <hostname2> action permit”  “ip-policy FW2 id 2 from <hostname3> to <hostname4> action permit”  ….  “ip-policy FW2 id n from <hostnameN> to <hostnameM> action permit”  “user-profile FW2 security ip-policy from/to-access FW1”   1. Show ip-policy, result 1 2. Show ip-policy by internal cli “Show inter-ip-policy FW to display”, result 2 3. Configure more hostname rule in the same policy, make sure the total rules exceed the maximum of ap, result 3 | | |
| Expect result | - There are ip policies about the configured hostname, such as  “ip-policy FW1 id 1 from <hostname1> to <hostname2> action deny”  “ip-policy FW1 id 2 from <hostname3> to <hostname4> action deny”  ….  “ip-policy FWN id n from <hostnameN> to <hostnameM> action deny”  - There are ip-policies about the configured hostname, and there are nearly 32736 (32700?) rules in FE  Suppose hostname1 resolve to 10.10.10.11---10.10.10.14 hostname2 resolve to  [20.20.20.11](http://www.google.com)---[20.20.20.14](http://www.google.com)) Set to FE:  Ip-policy policy-name id 10 from 10.10.10.11 255.255.255.255 to [20.20.20.11](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 11 from 10.10.10.12 255.255.255.255 to [20.20.20.11](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 12 from 10.10.10.13 255.255.255.255 to [20.20.20.11](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 13 from 10.10.10.14 255.255.255.255 to [20.20.20.11](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 14 from 10.10.10.11 255.255.255.255 to [20.20.20.12](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 15 from 10.10.10.12 255.255.255.255 to [20.20.20.12](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 16 from 10.10.10.13 255.255.255.255 to [20.20.20.12](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 17from 10.10.10.14 255.255.255.255 to [20.20.20.12](http://www.google.com) 255.255.255.255  ……….  Ip-policy policy-name id 22 from 10.10.10.11 255.255.255.255 to [20.20.20.14](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 23 from 10.10.10.12 255.255.255.255 to [20.20.20.14](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 24 from 10.10.10.13 255.255.255.255 to [20.20.20.14](http://www.google.com) 255.255.255.255  Ip-policy policy-name id 25 from 10.10.10.14 255.255.255.255 to [20.20.20.14](http://www.google.com) 255.255.255.255  - There are ip-policies about the configured hostname, and there are 32736 rules in FE, others will be invalid | | |

### Stress test

#### 8.11.6.1 Maximum dns request stress test

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Host\_11.17 | | |
| Priority | Low | Automation Flag | No |
| Topology to use | Laptop (hostname1) ------ AP1 ------ SW ------ Server (hostname2) | | |
| Description | Config many ip-policies with hostname but they can’t be resolved by the dns server | | |
| Pre-condition | Configure dns server but it can’t resolve the hostname in ip-policy | | |
| Test procedure | 1. Configure many L3 policies items with hostname:   “ip-policy FW1”  “ip-policy FW1 id 1 from <hostname1> to <hostname2> action deny”  “ip-policy FW1 id 2 from <hostname3> to <hostname4> action deny”  ….  “ip-policy FW1 id n from <hostnameN> to <hostnameM> action deny”  “user-profile FW1 security ip-policy from/to-access FW1”  “ip-policy FW2”  “ip-policy FW2 id 1 from <hostname1> to <hostname2> action permit”  “ip-policy FW2 id 2 from <hostname3> to <hostname4> action permit”  ….  “ip-policy FW2 id n from <hostnameN> to <hostnameM> action permit”  “user-profile FW2 security ip-policy from/to-access FW1”   1. Show ip-policy, result 1 2. Show ip-policy by internal cli “Show inter-ip-policy FW to display”, result 2 3. Laptop ping the configured hostname in ip-policy, result 3 | | |
| Expect result | - There is ip-policy about the configured hostname, such as  “ip-policy FW1 id 1 from <hostname1> to <hostname2> action deny”  “ip-policy FW1 id 2 from <hostname3> to <hostname4> action deny”  ….  “ip-policy FWN id n from <hostnameN> to <hostnameM> action deny”  - There is no ip policy rules set to FE because hostname can’t be resolved by dns server.  - Laptop ping unsuccessfully on step 4), info about dns resolve timeout will be shown on ap, and ap will send dns request about all hostname items periodly (1 min?), and the dns’ timeout is acceptable. | | |

#### 8.11.6.2 Create/delete ip-policy with hostname test

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Host\_11.18 | | |
| Priority | Low | Automation Flag | No |
| Topology to use | Laptop (hostname1) ------ AP1 ------ SW ------ Server (hostname2) | | |
| Description | Create/delete ip-policy with hostname repeatedly test | | |
| Pre-condition | Configure dns server and it can resolve the hostname in ip-policy | | |
| Test procedure | 1. Use script to create/delete ip-policy with hostname repeatedly at least overnight 2. Check ap’s info, result 1 3. Configure a rule with hostname with action is deny, result 2 4. Laptop ping the configured hostname in ip-policy, result 3 | | |
| Expect result | - Make sure there is no abnormal info on ap, such as memory leak, crash and etc  - There is ip policy rules set to FE with the configured hostname.  - Laptop ping unsuccessfully on step 4) | | |

#### 8.11.6.3 Change the rule’s order stress test

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Host\_11.19 | | |
| Priority | Low | Automation Flag | No |
| Topology to use | Laptop (hostname1) ------ AP1 ------ SW ------ Server (hostname2) | | |
| Description | Change the rule’s order overnight test | | |
| Pre-condition | Configure dns server and it can resolve the hostname in ip-policy | | |
| Test procedure | 1. Configure a L3 policy includes many rule with hostname and ip 2. Use script to change the rule’s order overnight 3. Check ap’s info, result 1 4. Change a rule with hostname with action is deny, and make it as the first rule, result 2 5. Laptop ping the configured hostname in ip-policy, result 3 | | |
| Expect result | - Make sure there is no abnormal info on ap, such as memory leak, crash and etc  - There is ip policy rules set to FE with the configured hostname.  - Laptop ping unsuccessfully on step 5) | | |

#### 8.11.6.4 Reboot ap with full configuration ip-policy

|  |  |  |  |
| --- | --- | --- | --- |
| Case ID | FW\_IP\_Policy\_Host\_11.20 | | |
| Priority | Low | Automation Flag | No |
| Topology to use | Laptop (hostname1) ------ AP1 ------ SW ------ Server (hostname2) | | |
| Description | Reboot ap with full configuration ip-policy | | |
| Pre-condition | Configure dns server and it can resolve the hostname in ip-policy | | |
| Test procedure | 1. Configure maximum L3 policies includes many rule with hostname and ip 2. Save it then reboot 3. Check ap’s info, result 1 | | |
| Expect result | - Make sure there is no abnormal info on ap, such as memory leak, crash and etc | | |