Aerohive Networks Inc.

Network Firewall TestCase

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **rsion** | **Date** | **Author** | **Description** |
| 0.1 | 07/22/2011 | Wei Cai | First version |
| 0.2 | 07/26/2011 | Wei Cai | Modify cases based on review suggestion |
| 0.3 | 07/27/2011 | Wei Cai | Modify cases based on Ligang’s suggestion |
| 0.3 | 07/27/2011 | Ligang Zhang | Approved |
| 0.4 | 08/19/2011 | Wei Cai | Modify cases based on CLI commands update |
| 0.5 | 08/19/2011 | Wei Cai | Modify cases based on Ligang’s suggestion |
| 0.6 | 08/22/2011 | Wei Cai | Modify cases based on hardening firewall rule changed |
| 0.7 | 11/18/2011 | Wei Cai | Add topology 9&10,case Services8&Negative10 |

The explanation of version 0.2（Case review suggestion）:

1. Modify priority;

2. Modify Topology3, add Topology4, add related cases;

3. Add network-firewall order and logic cases;

4. Add negative cases;

5. Add stress-logs cases;

The explanation of version 0.3（Ligang’s suggestion）:

1. Add mesh topology and cases;

4. Add IP/Mask cases;

5. Add ap self to gateway and gateway to ap self cases;

The explanation of version 0.4（CLI commands update）:

1. Delete “start-session” cases;

2. Add CVG/BR input chain firewall cases (6.2.7);

The explanation of version 0.5（Ligang’s suggestion）:

1. Add topology8;

2. Modify CVG/BR input chain firewall cases (lan mode), add changing port mode case;

The explanation of version 0.5（Ligang’s suggestion）:

1. Modify topology8;

2. Modify CVG/BR input chain firewall cases;

[1. Introduction 6](#_Toc302982819)

[2. Test Objectives 6](#_Toc302982820)

[3. Test Acceptance Criterion from Development 6](#_Toc302982821)

[4. Product Pass Criterion 6](#_Toc302982822)

[5. Test Bed/Topo Design 6](#_Toc302982823)

[Topology1 6](#_Toc302982824)

[Topology2 6](#_Toc302982825)

[Topology3 6](#_Toc302982826)

[Topology4 7](#_Toc302982827)

[Topology5 7](#_Toc302982828)

[Topology6 7](#_Toc302982829)

[Topology7 7](#_Toc302982830)

[Topology8 7](#_Toc302982831)

[6. TestCase 7](#_Toc302982832)

[6.1. Key Scenarios 7](#_Toc302982833)

[6.2. Function Test Case 8](#_Toc302982834)

[6.2.1. Network Firewall direction test case 8](#_Toc302982835)

[6.2.2. Network Firewall parameters test 38](#_Toc302982836)

[6.2.3. Network Firewall services test case 62](#_Toc302982837)

[6.2.4. Network Firewall log test case 68](#_Toc302982838)

[6.2.5. Network firewall fragment test case 76](#_Toc302982839)

[6.2.6. Network firewall order test case 78](#_Toc302982840)

[6.2.7. Hardening firewall test case 80](#_Toc302982841)

[6.3. Negative test case 81](#_Toc302982842)

[6.4. Stress Test Case 88](#_Toc302982843)

[6.4.1. Firewall rules maximum test case 88](#_Toc302982844)

[6.4.2. Firewall logs Maximum test 93](#_Toc302982845)

[6.5. Duration Test Case 94](#_Toc302982846)

[6.6. Performance Test Case 94](#_Toc302982847)

[6.7. Scalability Test Case 94](#_Toc302982848)

[6.8. Compatibility Test Case 96](#_Toc302982849)

[6.9. CLI Management (Automation Status: No) 96](#_Toc302982850)

[6.10. GUI Management-HiveManager 99](#_Toc302982851)

[6.11. GUI Management-HiveUI 99](#_Toc302982852)

Glossary and Abbreviations

# Introduction

The network firewall will be implemented entirely via iptables. There is only a single, global network firewall configuration (unlike the L2 firewall which can be configured per user profile).

An admin can choose to configure an L2 firewall (implemented in the FE) in addition to an network firewall, but this is an advanced use case and not expected to be used.

# Test Objectives

This test case includes 4 test points:

1.Cli commands of network firewall

2.Direction of network firewall

3.The parameters of network firewall

4.Maximum network firewall rules

Note: All of this info should come from requirement/spec, if has not this info in requirement/spec, pls ask dev and get the expected info/number. If no expected number, we try to give out the QA’s expected number.

# Test Acceptance Criterion from Development

* Approved – Functional Specifications
* Approved – Unit Test Plans

# Product Pass Criterion

Meet all objects in marketing requirement or function spec which may include key function objectives, scalability objectives, performance objectives and so on.

# Test Bed/Topo Design

## Topology1

Laptop1------AP------Laptop2

## Topology2

Laptop1------AP1-------SW-------AP2--------Laptop2

## Topology3

Laptop1------AP1(WAN)------(tunnel1)-------------Gateway1------L3SW------Laptop3

| |

| |

Laptop2------AP2(WAN)------(tunnel2)------------------- Laptop4

## Topology4

Laptop1--------AP1(WAN)-----(tunnel1)------ Gateway1------L3SW------Laptop2

| |

| |

----------- ---(tunnel2)-------Gateway2 Laptop4

|

|

L3SW

|

|

Laptop3

## Topology5

Laptop1------AP------Laptop2

|

|

|

Laptop3

## Topology6

Laptop1------AP------SW------Server(hostname1)

## Topology7

Laptop1------MP---(mesh)--- AP1------Laptop2

## Topology8

Laptop1--------(wifi)AP1(eth0)-----L3switch------(eth0) Gateway1

|

|

Laptop2

## Topology9

Laptop------AP----(VPN)----CVG-----------------

| www.sina.com

|-----------------------------------------

## Topology10

SIP server

|

|

Laptop1------AP------Laptop2

底层查看session的方法

cat /proc/net/nf\_conntrack

# TestCase

## Key Scenarios

## Function Test Case

### Network Firewall direction test case

#### “From” direction test case

##### Case ID Network-Firewall\_Direction\_1

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Direction\_1 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Configure single “From” rule(permit) , 2 Laptops is in the same AP , wifi connection | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (wifi)  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 (wifi) | | |
| **Test procedure** | 1) Laptop1 ping Laptop2  2) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 ping Laptop2 | | |
| **Expect result** | 2) Laptop1 ping Laptop2 successfully  3) Laptop1 ping Laptop2 successfully | | |

##### Case ID Network-Firewall\_Direction\_2

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Direction\_2 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Configure single “From” rule(deny) , 2 Laptops is in the same AP , wifi connection | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (wifi)  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 (wifi) | | |
| **Test procedure** | 1) Laptop1 ping Laptop2  2) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 ping Laptop2 | | |
| **Expect result** | 2) Laptop1 ping Laptop2 successfully  3) Laptop1 ping Laptop2 unsuccessfully | | |

##### Case ID Network-Firewall\_Direction\_3

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Direction\_3 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Delete network-firewall ”From” rule(permit/deny) , 2 Laptops is in the same AP , wifi connection | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (wifi)  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 (wifi) | | |
| **Test procedure** | 1) Laptop1 ping Laptop2  2) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 ping Laptop2  4) Delete network firewall config  ***“no network-firewall”***  5) Show network firewall  ***“show network-firewall”***  6) Laptop1 ping Laptop2  7) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  8) Laptop1 ping Laptop2  9) Delete network firewall config  ***“no network-firewall”***  10) Show network firewall  ***“show network-firewall”***  11) Laptop1 ping Laptop2 | | |
| **Expect result** | 1) Laptop1 ping Laptop2 successfully  3) Laptop1 ping Laptop2 successfully  5) No network firewall information can be displayed  6) Laptop1 ping Laptop2 successfully  8) Laptop1 ping Laptop2 unsuccessfully  10) No network firewall information can be displayed  11) Laptop1 ping Laptop2 successfully | | |

##### Case ID Network-Firewall\_Direction\_4

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Direction\_4 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Configure single network-firewall “From” rule(permit/deny) , 2 Laptops is in the same AP , eth connection | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (eth)  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 (wifi) | | |
| **Test procedure** | 1) Laptop1 ping Laptop2  2) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 ping Laptop2  4) Delete network firewall config  ***“no network-firewall”***  5) Show network firewall  ***“show network-firewall”***  6) Laptop1 ping Laptop2  7) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  8) Laptop1 ping Laptop2  9) Delete network firewall config  ***“no network-firewall”***  10) Show network firewall  ***“show network-firewall”***  11) Laptop1 ping Laptop2 | | |
| **Expect result** | 1) Laptop1 ping Laptop2 successfully  3) Laptop1 ping Laptop2 successfully  5) No network firewall information can be displayed  6) Laptop1 ping Laptop2 successfully  8) Laptop1 ping Laptop2 unsuccessfully  10) No network firewall information can be displayed  11) Laptop1 ping Laptop2 successfully | | |

##### Case ID Network-Firewall\_Direction\_5

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Direction\_5 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy2 | | |
| **Description** | Configure single network-firewall “From” rule(permit/deny) , 2 Laptops is in different AP , wifi connection | | |
| **Pre-condition** | -Configure AP1  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (wifi)  -Configure AP2  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop2 connect to Mgt0.1 IPaddr 10.1.20.2 (wifi) | | |
| **Test procedure** | 1) Laptop1 ping Laptop2  2) Configure network firewall rule on AP1  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 ping Laptop2  4) Delete network firewall config on AP1  ***“no network-firewall”***  5) Show network firewall on AP1  ***“show network-firewall”***  6) Laptop1 ping Laptop2  7) Configure network firewall rule on AP1  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  8) Laptop1 ping Laptop2  9) Delete network firewall config  ***“no network-firewall”***  10) Show network firewall  ***“show network-firewall”***  11) Laptop1 ping Laptop2 | | |
| **Expect result** | 1) Laptop1 ping Laptop2 successfully  3) Laptop1 ping Laptop2 successfully  5) No network firewall information can be displayed  6) Laptop1 ping Laptop2 successfully  8) Laptop1 ping Laptop2 unsuccessfully  10) No network firewall information can be displayed  11) Laptop1 ping Laptop2 successfully | | |

##### Case ID Network-Firewall\_Direction\_6

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Direction\_6 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy2 | | |
| **Description** | Configure single network-firewall “From” rule(permit/deny) , 2 Laptops is in different AP , eth connection | | |
| **Pre-condition** | -Configure AP1  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (eth)  -Configure AP2  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop2 connect to Mgt0.1 IPaddr 10.1.20.2 (wifi) | | |
| **Test procedure** | 1) Laptop1 ping Laptop2  2) Configure network firewall rule on AP1  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 ping Laptop2  4) Delete network firewall config on AP1  ***“no network-firewall”***  5) Show network firewall on AP1  ***“show network-firewall”***  6) Laptop1 ping Laptop2  7) Configure network firewall rule on AP1  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  8) Laptop1 ping Laptop2  9) Delete network firewall config on AP1  ***“no network-firewall”***  10) Show network firewall on AP1  ***“show network-firewall”***  11) Laptop1 ping Laptop2 | | |
| **Expect result** | 1) Laptop1 ping Laptop2 successfully  3) Laptop1 ping Laptop2 successfully  5) No network firewall information can be displayed  6) Laptop1 ping Laptop2 successfully  8) Laptop1 ping Laptop2 unsuccessfully  10) No network firewall information can be displayed  11) Laptop1 ping Laptop2 successfully | | |

##### Case ID Network-Firewall\_Direction\_7

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Direction\_7 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy7 | | |
| **Description** | Configure single network-firewall “From” rule(permit/deny) ,Laptop1 connect to MP | | |
| **Pre-condition** | -Configure AP1  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  MP’mgt0 got IP from mgt0.1(vlan 10), IPaddr is 10.1.10.2  Laptop1 connect to MP IPaddr 10.1.10.3  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 | | |
| **Test procedure** | 1) Laptop1 ping Laptop2  2) Configure network firewall rule on AP1  ***“network-firewall name 1001 from network 10.1.10.3 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 ping Laptop2  4) Delete network firewall config on AP1  ***“no network-firewall”***  5) Laptop1 ping Laptop2  6) Configure network firewall rule on AP1  ***“network-firewall name 1001 from network 10.1.10.3 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  7) Laptop1 ping Laptop2  8) Delete network firewall config on AP1  ***“no network-firewall”***  9) Laptop1 ping Laptop2 | | |
| **Expect result** | 1) Laptop1 ping Laptop2 successfully  3) Laptop1 ping Laptop2 successfully  5) Laptop1 ping Laptop2 successfully  7) Laptop1 ping Laptop2 unsuccessfully  9) Laptop1 ping Laptop2 successfully | | |

##### Case ID Network-Firewall\_Direction\_8

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Direction\_8 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy7 | | |
| **Description** | Configure single network-firewall “From” rule(permit/deny) ,Laptop1 connect to MP DHCP server | | |
| **Pre-condition** | -Configure AP1  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Laptop2 connect to Mgt0.1 IPaddr 10.1.10.2  -Configure MP  Enable 1 dhcp server (mgt0.1)  Mgt0.1 vlan 10 IPaddr 100.1.10.1 gateway 100.1.10.1  Laptop1 connect to Mgt0.1 IPaddr 100.1.10.2 | | |
| **Test procedure** | 1) Laptop1 ping Laptop2  2) Configure network firewall rule on AP1  ***“network-firewall name 1001 from network 100.1.10.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 ping Laptop2  4) Delete network firewall config on AP1  ***“no network-firewall”***  5) Laptop1 ping Laptop2  6) Configure network firewall rule on AP1  ***“network-firewall name 1001 from network 100.1.10.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  7) Laptop1 ping Laptop2  8) Delete network firewall config on AP1  ***“no network-firewall”***  9) Laptop1 ping Laptop2 | | |
| **Expect result** | 1) Laptop1 ping Laptop2 successfully  3) Laptop1 ping Laptop2 successfully  5) Laptop1 ping Laptop2 successfully  7) Laptop1 ping Laptop2 unsuccessfully  9) Laptop1 ping Laptop2 successfully | | |

#### “To” direction test case

##### Case ID Network-Firewall\_Direction\_9

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Direction\_9 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Configure single “To” rule(permit) , 2 Laptops is in the same AP , wifi connection | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (wifi)  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 (wifi) | | |
| **Test procedure** | 1) Laptop2 ping Laptop1  2) Configure network firewall rule  ***“network-firewall name 1001 to network 10.1.10.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop2 ping Laptop1 | | |
| **Expect result** | 2) Laptop2 ping Laptop1 successfully  3) Laptop2 ping Laptop1 successfully | | |

##### Case ID Network-Firewall\_Direction\_10

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Direction\_10 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Configure single “To” rule(deny) , 2 Laptops is in the same AP , wifi connection | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (wifi)  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 (wifi) | | |
| **Test procedure** | 1) Laptop2 ping Laptop1  2) Configure network firewall rule  ***“network-firewall name 1001 to network 10.1.10.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop2 ping Laptop1 | | |
| **Expect result** | 2) Laptop2 ping Laptop1 successfully  3) Laptop2 ping Laptop1 unsuccessfully | | |

##### Case ID Network-Firewall\_Direction\_11

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Direction\_11 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Delete network-firewall “To” rule(permit/deny) , 2 Laptops is in the same AP , wifi connection | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (wifi)  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 (wifi) | | |
| **Test procedure** | 1) Laptop2 ping Laptop1  2) Configure network firewall rule  ***“network-firewall name 1001 to network 10.1.10.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop2 ping Laptop1  4) Delete network firewall config  ***“no network-firewall”***  5) Show network firewall  ***“show network-firewall”***  6) Laptop2 ping Laptop1  7) Configure network firewall rule  ***“network-firewall name 1001 to network 10.1.10.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  8) Laptop2 ping Laptop1  9) Delete network firewall config  ***“no network-firewall”***  10) Show network firewall  ***“show network-firewall”***  11) Laptop2 ping Laptop1 | | |
| **Expect result** | 1) Laptop2 ping Laptop1 successfully  3) Laptop2 ping Laptop1 successfully  5) No network firewall information can be displayed  6) Laptop2 ping Laptop1 successfully  8) Laptop2 ping Laptop1 unsuccessfully  10) No network firewall information can be displayed  11) Laptop2 ping Laptop1 successfully | | |

##### Case ID Network-Firewall\_Direction\_12

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Direction\_12 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Configure single network-firewall “To” rule(permit/deny) , 2 Laptops is in the same AP , eth connection | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (eth)  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 (wifi) | | |
| **Test procedure** | 1) Laptop2 ping Laptop1  2) Configure network firewall rule  ***“network-firewall name 1001 to network 10.1.10.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop2 ping Laptop1  4) Delete network firewall config  ***“no network-firewall”***  5) Show network firewall  ***“show network-firewall”***  6) Laptop2 ping Laptop1  7) Configure network firewall rule  ***“network-firewall name 1001 to network 10.1.10.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  8) Laptop2 ping Laptop1  9) Delete network firewall config  ***“no network-firewall”***  10) Show network firewall  ***“show network-firewall”***  11) Laptop2 ping Laptop1 | | |
| **Expect result** | 1) Laptop2 ping Laptop1 successfully  3) Laptop2 ping Laptop1 successfully  5) No network firewall information can be displayed  6) Laptop2 ping Laptop1 successfully  8) Laptop2 ping Laptop1 unsuccessfully  10) No network firewall information can be displayed  11) Laptop2 ping Laptop1 successfully | | |

##### Case ID Network-Firewall\_Direction\_13

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Direction\_13 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy2 | | |
| **Description** | Configure single network-firewall “To” rule(permit/deny) , 2 Laptops is in different AP , wifi connection | | |
| **Pre-condition** | -Configure AP1  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (wifi)  -Configure AP2  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop2 connect to Mgt0.1 IPaddr 10.1.20.2 (wifi) | | |
| **Test procedure** | 1) Laptop2 ping Laptop1  2) Configure network firewall rule on AP1  ***“network-firewall name 1001 to network 10.1.10.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop2 ping Laptop1  4) Delete network firewall config on AP1  ***“no network-firewall”***  5) Show network firewall on AP1  ***“show network-firewall”***  6) Laptop2 ping Laptop1  7) Configure network firewall rule on AP1  ***“network-firewall name 1001 to network 10.1.10.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  8) Laptop2 ping Laptop1  9) Delete network firewall config  ***“no network-firewall”***  10) Show network firewall  ***“show network-firewall”***  11) Laptop2 ping Laptop1 | | |
| **Expect result** | 1) Laptop2 ping Laptop1 successfully  3) Laptop2 ping Laptop1 successfully  5) No network firewall information can be displayed  6) Laptop2 ping Laptop1 successfully  8) Laptop2 ping Laptop1 unsuccessfully  10) No network firewall information can be displayed  11) Laptop2 ping Laptop1 successfully | | |

##### Case ID Network-Firewall\_Direction\_14

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Direction\_14 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy2 | | |
| **Description** | Configure single network-firewall “To” rule(permit/deny) , 2 Laptops is in different AP , eth connection | | |
| **Pre-condition** | -Configure AP1  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (eth)  -Configure AP2  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop2 connect to Mgt0.1 IPaddr 10.1.20.2 (wifi) | | |
| **Test procedure** | 1) Laptop2 ping Laptop1  2) Configure network firewall rule on AP1  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop2 ping Laptop1  4) Delete network firewall config on AP1  ***“no network-firewall”***  5) Show network firewall on AP1  ***“show network-firewall”***  6) Laptop2 ping Laptop1  7) Configure network firewall rule on AP1  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  8) Laptop2 ping Laptop1  9) Delete network firewall config on AP1  ***“no network-firewall”***  10) Show network firewall on AP1  ***“show network-firewall”***  11) Laptop2 ping Laptop1 | | |
| **Expect result** | 1) Laptop2 ping Laptop1 successfully  3) Laptop2 ping Laptop1 successfully  5) No network firewall information can be displayed  6) Laptop2 ping Laptop1 successfully  8) Laptop2 ping Laptop1 unsuccessfully  10) No network firewall information can be displayed  11) Laptop2 ping Laptop1 successfully | | |

##### Case ID Network-Firewall\_Direction\_15

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Direction\_15 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy7 | | |
| **Description** | Configure single network-firewall “To” rule(permit/deny) ,Laptop1 connect to MP | | |
| **Pre-condition** | -Configure AP1  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  MP’mgt0 got IP from mgt0.1(vlan 10), IPaddr is 10.1.10.2  Laptop1 connect to MP IPaddr 10.1.10.3  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 | | |
| **Test procedure** | 1) Laptop1 ping Laptop2  2) Configure network firewall rule on AP1  ***“network-firewall name 1001 to network 10.1.20.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 ping Laptop2  4) Delete network firewall config on AP1  ***“no network-firewall”***  5) Laptop1 ping Laptop2  6) Configure network firewall rule on AP1  ***“network-firewall name 1001 to network 10.1.20.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  7) Laptop1 ping Laptop2  8) Delete network firewall config on AP1  ***“no network-firewall”***  9) Laptop1 ping Laptop2 | | |
| **Expect result** | 1) Laptop1 ping Laptop2 successfully  3) Laptop1 ping Laptop2 successfully  5) Laptop1 ping Laptop2 successfully  7) Laptop1 ping Laptop2 unsuccessfully  9) Laptop1 ping Laptop2 successfully | | |

##### Case ID Network-Firewall\_Direction\_16

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Direction\_16 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy7 | | |
| **Description** | Configure single network-firewall “To” rule(permit/deny) ,Laptop1 connect to MP DHCP server | | |
| **Pre-condition** | -Configure AP1  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Laptop2 connect to Mgt0.1 IPaddr 10.1.10.2  -Configure MP  Enable 1 dhcp server (mgt0.1)  Mgt0.1 vlan 10 IPaddr 100.1.10.1 gateway 100.1.10.1  Laptop1 connect to Mgt0.1 IPaddr 100.1.10.2 | | |
| **Test procedure** | 1) Laptop1 ping Laptop2  2) Configure network firewall rule on AP1  ***“network-firewall name 1001 to network 10.1.10.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 ping Laptop2  4) Delete network firewall config on AP1  ***“no network-firewall”***  5) Laptop1 ping Laptop2  6) Configure network firewall rule on AP1  ***“network-firewall name 1001 to network 10.1.10.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  7) Laptop1 ping Laptop2  8) Delete network firewall config on AP1  ***“no network-firewall”***  9) Laptop1 ping Laptop2 | | |
| **Expect result** | 1) Laptop1 ping Laptop2 successfully  3) Laptop1 ping Laptop2 successfully  5) Laptop1 ping Laptop2 successfully  7) Laptop1 ping Laptop2 unsuccessfully  9) Laptop1 ping Laptop2 successfully | | |

#### “From&To” direction test case

##### Case ID Network-Firewall\_Direction\_17

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Direction\_17 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Configure “From&To”(permit) rule, 2 Laptops is in the same AP ,Laptop1 wifi connection Laptop2 wifi connection. | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (wifi)  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 (wifi) | | |
| **Test procedure** | 1) Laptop1 ping Laptop2  2) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 10.1.20.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 ping Laptop2 | | |
| **Expect result** | 2) Laptop1 ping Laptop2 successfully  3) Laptop1 ping Laptop2 successfully | | |

##### Case ID Network-Firewall\_Direction\_18

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Direction\_18 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Configure single “From&To” rule(deny) , 2 Laptops is in the same AP , Laptop1 wifi connection Laptop2 wifi connection. | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (wifi)  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 (wifi) | | |
| **Test procedure** | 1) Laptop1 ping Laptop2  2) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 10.1.20.2 255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 ping Laptop2 | | |
| **Expect result** | 2) Laptop1 ping Laptop2 successfully  3) Laptop1 ping Laptop2 unsuccessfully | | |

##### Case ID Network-Firewall\_Direction\_19

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Direction\_19 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Delete network-firewall ”From&To” rule(permit/deny) , 2 Laptops is in the same AP , Laptop1 wifi connection Laptop2 wifi connection. | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (wifi)  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 (wifi) | | |
| **Test procedure** | 1) Laptop1 ping Laptop2  2) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 10.1.20.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 ping Laptop2  4) Delete network firewall config  ***“no network-firewall”***  5) Show network firewall  ***“show network-firewall”***  6) Laptop1 ping Laptop2  7) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 10.1.20.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  8) Laptop1 ping Laptop2  9) Delete network firewall config  ***“no network-firewall”***  10) Show network firewall  ***“show network-firewall”***  11) Laptop1 ping Laptop2 | | |
| **Expect result** | 1) Laptop1 ping Laptop2 successfully  3) Laptop1 ping Laptop2 successfully  5) No network firewall information can be displayed  6) Laptop1 ping Laptop2 successfully  8) Laptop1 ping Laptop2 unsuccessfully  10) No network firewall information can be displayed  11) Laptop1 ping Laptop2 successfully | | |

##### Case ID Network-Firewall\_Direction\_20

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Direction\_20 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Configure network-firewall “From&To” rule(permit/deny) , 2 Laptops is in the same AP , Laptop1 eth connection Laptop2 wifi connection. | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (eth)  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 (wifi) | | |
| **Test procedure** | 1) Laptop1 ping Laptop2  2) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 10.1.20.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 ping Laptop2  4) Delete network firewall config  ***“no network-firewall”***  5) Show network firewall  ***“show network-firewall”***  6) Laptop1 ping Laptop2  7) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 10.1.20.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  8) Laptop1 ping Laptop2  9) Delete network firewall config  ***“no network-firewall”***  10) Show network firewall  ***“show network-firewall”***  11) Laptop1 ping Laptop2 | | |
| **Expect result** | 1) Laptop1 ping Laptop2 successfully  3) Laptop1 ping Laptop2 successfully  5) No network firewall information can be displayed  6) Laptop1 ping Laptop2 successfully  8) Laptop1 ping Laptop2 unsuccessfully  10) No network firewall information can be displayed  11) Laptop1 ping Laptop2 successfully | | |

##### Case ID Network-Firewall\_Direction\_21

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Direction\_21 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Configure network-firewall “From&To” rule(permit/deny) , 2 Laptops is in the same AP , Laptop1 wifi connection Laptop2 eth connection. | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (wifi)  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 (eth) | | |
| **Test procedure** | 1) Laptop1 ping Laptop2  2) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 10.1.20.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 ping Laptop2  4) Delete network firewall config  ***“no network-firewall”***  5) Show network firewall  ***“show network-firewall”***  6) Laptop1 ping Laptop2  7) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 10.1.20.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  8) Laptop1 ping Laptop2  9) Delete network firewall config  ***“no network-firewall”***  10) Show network firewall  ***“show network-firewall”***  11) Laptop1 ping Laptop2 | | |
| **Expect result** | 1) Laptop1 ping Laptop2 successfully  3) Laptop1 ping Laptop2 successfully  5) No network firewall information can be displayed  6) Laptop1 ping Laptop2 successfully  8) Laptop1 ping Laptop2 unsuccessfully  10) No network firewall information can be displayed  11) Laptop1 ping Laptop2 successfully | | |

##### Case ID Network-Firewall\_Direction\_22

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Direction\_22 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Configure network-firewall “From&To” rule(permit/deny) , 2 Laptops is in the same AP , Laptop1 eth connection Laptop2 eth connection. | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (eth)  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 (eth) | | |
| **Test procedure** | 1) Laptop1 ping Laptop2  2) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 10.1.20.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 ping Laptop2  4) Delete network firewall config  ***“no network-firewall”***  5) Show network firewall  ***“show network-firewall”***  6) Laptop1 ping Laptop2  7) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 10.1.20.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  8) Laptop1 ping Laptop2  9) Delete network firewall config  ***“no network-firewall”***  10) Show network firewall  ***“show network-firewall”***  11) Laptop1 ping Laptop2 | | |
| **Expect result** | 1) Laptop1 ping Laptop2 successfully  3) Laptop1 ping Laptop2 successfully  5) No network firewall information can be displayed  6) Laptop1 ping Laptop2 successfully  8) Laptop1 ping Laptop2 unsuccessfully  10) No network firewall information can be displayed  11) Laptop1 ping Laptop2 successfully | | |

##### Case ID Network-Firewall\_Direction\_23

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Direction\_23 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy2 | | |
| **Description** | Configure network-firewall “From&To” rule(permit/deny) , 2 Laptops is in different AP , wifi connection | | |
| **Pre-condition** | -Configure AP1  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (wifi)  -Configure AP2  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop2 connect to Mgt0.1 IPaddr 10.1.20.2 (wifi) | | |
| **Test procedure** | 1) Laptop1 ping Laptop2  2) Configure network firewall rule on AP1  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 10.1.20.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 ping Laptop2  4) Delete network firewall config on AP1  ***“no network-firewall”***  5) Show network firewall on AP1  ***“show network-firewall”***  6) Laptop1 ping Laptop2  7) Configure network firewall rule on AP1  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 10.1.20.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  8) Laptop1 ping Laptop2  9) Delete network firewall config  ***“no network-firewall”***  10) Show network firewall  ***“show network-firewall”***  11) Laptop1 ping Laptop2 | | |
| **Expect result** | 1) Laptop1 ping Laptop2 successfully  3) Laptop1 ping Laptop2 successfully  5) No network firewall information can be displayed  6) Laptop1 ping Laptop2 successfully  8) Laptop1 ping Laptop2 unsuccessfully  10) No network firewall information can be displayed  11) Laptop1 ping Laptop2 successfully | | |

##### Case ID Network-Firewall\_Direction\_24

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Direction\_24 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy2 | | |
| **Description** | Configure single network-firewall “From&To” rule(permit/deny) , 2 Laptops is in different AP , eth connection | | |
| **Pre-condition** | -Configure AP1  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (eth)  -Configure AP2  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop2 connect to Mgt0.1 IPaddr 10.1.20.2 (wifi) | | |
| **Test procedure** | 1) Laptop1 ping Laptop2  2) Configure network firewall rule on AP1  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 10.1.20.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 ping Laptop2  4) Delete network firewall config on AP1  ***“no network-firewall”***  5) Show network firewall on AP1  ***“show network-firewall”***  6) Laptop1 ping Laptop2  7) Configure network firewall rule on AP1  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 10.1.20.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  8) Laptop1 ping Laptop2  9) Delete network firewall config on AP1  ***“no network-firewall”***  10) Show network firewall on AP1  ***“show network-firewall”***  11) Laptop1 ping Laptop2 | | |
| **Expect result** | 1) Laptop1 ping Laptop2 successfully  3) Laptop1 ping Laptop2 successfully  5) No network firewall information can be displayed  6) Laptop1 ping Laptop2 successfully  8) Laptop1 ping Laptop2 unsuccessfully  10) No network firewall information can be displayed  11) Laptop1 ping Laptop2 successfully | | |

##### Case ID Network-Firewall\_Direction\_25

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Direction\_25 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy7 | | |
| **Description** | Configure single network-firewall “From&To” rule(permit/deny) ,Laptop1 connect to MP | | |
| **Pre-condition** | -Configure AP1  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  MP’mgt0 got IP from mgt0.1(vlan 10), IPaddr is 10.1.10.2  Laptop1 connect to MP IPaddr 10.1.10.3  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 | | |
| **Test procedure** | 1) Laptop1 ping Laptop2  2) Configure network firewall rule on AP1  ***“network-firewall name 1001 from network 10.1.10.3 255.255.255.255 to network 10.1.20.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 ping Laptop2  4) Delete network firewall config on AP1  ***“no network-firewall”***  5) Laptop1 ping Laptop2  6) Configure network firewall rule on AP1  ***“network-firewall name 1001 from network 10.1.10.3 255.255.255.255 to network 10.1.20.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  7) Laptop1 ping Laptop2  8) Delete network firewall config on AP1  ***“no network-firewall”***  9) Laptop1 ping Laptop2 | | |
| **Expect result** | 1) Laptop1 ping Laptop2 successfully  3) Laptop1 ping Laptop2 successfully  5) Laptop1 ping Laptop2 successfully  7) Laptop1 ping Laptop2 unsuccessfully  9) Laptop1 ping Laptop2 successfully | | |

##### Case ID Network-Firewall\_Direction\_26

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Direction\_26 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy7 | | |
| **Description** | Configure single network-firewall “From&To” rule(permit/deny) ,Laptop1 connect to MP DHCP server | | |
| **Pre-condition** | -Configure AP1  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Laptop2 connect to Mgt0.1 IPaddr 10.1.10.2  -Configure MP  Enable 1 dhcp server (mgt0.1)  Mgt0.1 vlan 10 IPaddr 100.1.10.1 gateway 100.1.10.1  Laptop1 connect to Mgt0.1 IPaddr 100.1.10.2 | | |
| **Test procedure** | 1) Laptop1 ping Laptop2  2) Configure network firewall rule on AP1  ***“network-firewall name 1001 from network 100.1.10.2 255.255.255.255 to network 10.1.10.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 ping Laptop2  4) Delete network firewall config on AP1  ***“no network-firewall”***  5) Laptop1 ping Laptop2  6) Configure network firewall rule on AP1  ***“network-firewall name 1001 from network 100.1.10.2 255.255.255.255 to network 10.1.10.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  7) Laptop1 ping Laptop2  8) Delete network firewall config on AP1  ***“no network-firewall”***  9) Laptop1 ping Laptop2 | | |
| **Expect result** | 1) Laptop1 ping Laptop2 successfully  3) Laptop1 ping Laptop2 successfully  5) Laptop1 ping Laptop2 successfully  7) Laptop1 ping Laptop2 unsuccessfully  9) Laptop1 ping Laptop2 successfully | | |

### Network Firewall parameters test

#### VPN test case

##### Case ID Network-Firewall\_Parameter\_1

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Parameter\_1 | | |
| **Priority** | Accept | **Automation Flag** | No |
| **Topology to use** | Topolopy3 | | |
| **Description** | Network firewall “From” VPN test | | |
| **Pre-condition** | -Configure AP1  Enable tunnel1 between AP1 and Gateway1  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (wifi)  -Configure AP2  Enable tunnel2 between AP2 and Gateway1  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 20.1.10.1 gateway 20.1.10.1  Laptop2 connect to Mgt0.1 IPaddr 20.1.10.2 (wifi) | | |
| **Test procedure** | 1) Laptop2 and Laptop3 ping Laptop1  2) Configure network firewall rule  ***“network-firewall name 1001 from vpn to network 10.1.10.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop2 and Laptop3 ping Laptop1  4) Delete network firewall config on AP1  ***“no network-firewall”***  5) Laptop2 and Laptop3 ping Laptop1  6) Configure network firewall rule on AP1  ***“network-firewall name 1001 from vpn to network 10.1.10.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  7) Laptop2 and Laptop3 ping Laptop1  8) Delete network firewall config on AP1  ***“no network-firewall”***  9) Laptop2 and Laptop3 ping Laptop1 | | |
| **Expect result** | 1) Laptop2 and Laptop3 ping Laptop1 successfully  3) Laptop2 and Laptop3 ping Laptop1 successfully  5) Laptop2 and Laptop3 ping Laptop1 successfully  7) Laptop2 and Laptop3 ping Laptop1 unsuccessfully  9) Laptop2 and Laptop3 ping Laptop1 successfully | | |
|  |  | | |

##### Case ID Network-Firewall\_Parameter\_2

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Parameter\_2 | | |
| **Priority** | Accept | **Automation Flag** | No |
| **Topology to use** | Topolopy3 | | |
| **Description** | Network firewall “To” VPN test | | |
| **Pre-condition** | -Configure AP1  Enable tunnel1 between AP1 and Gateway1  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (wifi)  -Configure AP2  Enable tunnel2 between AP2 and Gateway1  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 20.1.10.1 gateway 20.1.10.1  Laptop2 connect to Mgt0.1 IPaddr 20.1.10.2 (wifi) | | |
| **Test procedure** | 1) Laptop1 ping Laptop2 and Laptop3  2) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to vpn action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 ping Laptop2 and Laptop3  4) Delete network firewall config on AP1  ***“no network-firewall”***  5) Laptop1 ping Laptop2 and Laptop3  6) Configure network firewall rule on AP1  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to vpn action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  7) Laptop1 ping Laptop2 and Laptop3  8) Delete network firewall config on AP1  ***“no network-firewall”***  9) Laptop1 ping Laptop2 and Laptop3 | | |
| **Expect result** | 1) Laptop1 ping Laptop2 and Laptop3 successfully  3) Laptop1 ping Laptop2 and Laptop3 successfully  5) Laptop1 ping Laptop2 and Laptop3 successfully  7) Laptop1 ping Laptop2 and Laptop3 unsuccessfully  9) Laptop1 ping Laptop2 and Laptop3 successfully | | |
|  | **To vpn permit**  2012-05-14 15:27:48 debug kernel: L\*: (i) wifi0.2 172.17.107.2->172.32.1.241(950) ttl(128) icmp-echo-req(1/58) 60 bytes  2012-05-14 15:27:48 debug kernel: [fe]: MAC session (id [2]) found  2012-05-14 15:27:48 debug kernel: [fe]: fflow 2477:035d:afd4->0019:7722:1180 flag 0x41002, rflow 0019:7722:1180->2477:035d:afd4 flag 0xe1210  2012-05-14 15:27:48 debug kernel: [fe]: fflow acl 0x0/0x0, rflow acl 0x0/0x0  2012-05-14 15:27:48 debug kernel: [fe]: update from-access counters 74 bytes  2012-05-14 15:27:48 debug kernel: [fe]: QoS: ingress pkt fwd(wifi0.2) profile=16 qos=2  2012-05-14 15:27:48 debug kernel: [fe]: set pkt to self  2012-05-14 15:27:48 debug kernel: [fe]: swap incoming dev wifi0.2 -> mgt0.9  2012-05-14 15:27:48 debug kernel: [fe]: allow to self-pak, dst-ip 172.32.1.241,allow-arp 0 allow-dhcp 0 allow-forwarding 1  2012-05-14 15:27:48 debug kernel: [fe]: ip forward: ip pkt with dst-ip 172.32.1.241 received on wifi0.2  2012-05-14 15:27:48 debug kernel: [fe]: deliver pak to self on mgt0.9 with fw mark 1  2012-05-14 15:27:48 debug kernel: L\*: (u) mgt0.9 172.17.107.2->172.32.1.241(950) ttl(128) icmp-echo-req(1/58) 60 bytes  2012-05-14 15:27:48 debug kernel: [kernel]: iptables PRE\_ROUTING pkt 172.17.107.2(mgt0.9)->172.32.1.241(<NULL>) proto(1) 60 bytes: ACCEPT  2012-05-14 15:27:48 debug kernel: [kernel]: routing done, 172.17.107.2 -> 172.32.1.241 ttl(128) proto(1) mark(1) 60 bytes, found route in table:Main(Split)  2012-05-14 15:27:48 debug kernel: [kernel]: create routing cache:172.17.107.2 -> 172.32.1.241 fwmark 1 dev tunnel0  2012-05-14 15:27:48 debug kernel: [kernel]: iptables FORWARD pkt 172.17.107.2(mgt0.9)->172.32.1.241(tunnel0) proto(1) 60 bytes: ACCEPT  2012-05-14 15:27:48 debug kernel: [kernel]: iptables POST\_ROUTING pkt 172.17.107.2(<NULL>)->172.32.1.241(tunnel0) proto(1) 60 bytes: ACCEPT  2012-05-14 15:27:48 debug kernel: L\*: (o) tunnel0 172.17.107.2->172.32.1.241(950) ttl(127) mtu(1476) icmp-echo-req(1/58) 60 bytes  2012-05-14 15:27:48 debug kernel: [fe]: QoS: pkt forwarded (tunnel0) qos=2 profile=16  2012-05-14 15:27:48 debug kernel: [kernel]: GRE-encap packet: 172.17.107.2->172.32.1.241 ttl(127) proto(1) mark(1) 60 bytes mtu 1476  2012-05-14 15:27:48 debug kernel: [kernel]: update mtu to 1398 clamp tcp mss flag: 1  2012-05-14 15:27:48 debug kernel: [kernel]: GRE-encap packet done =>172.32.1.225->10.3.3.200 ttl(127) proto(47) mark(1) 84 bytes  2012-05-14 15:27:48 debug kernel: [kernel]: iptables LOCAL\_OUT pkt 172.32.1.225(<NULL>)->10.3.3.200(eth0) proto(47) 84 bytes: ACCEPT  2012-05-14 15:27:48 debug kernel: [kernel]: iptables POST\_ROUTING pkt 172.32.1.225(<NULL>)->10.3.3.200(eth0) proto(47) 84 bytes: ACCEPT  2012-05-14 15:27:48 debug kernel: [kernel]: encap outgoing packet 172.32.1.225->10.3.3.200 ttl(127) proto(47) 84 bytes  2012-05-14 15:27:48 debug kernel: [kernel]: encap(ESP, SPI:a460f3d) packet successfully(rc=0) =>10.2.2.14->10.155.32.172 ttl(64) proto(17) mark(1) 160 bytes  2012-05-14 15:27:48 debug kernel: [kernel]: iptables LOCAL\_OUT pkt 10.2.2.14(<NULL>)->10.155.32.172(eth0) proto(17) 160 bytes: ACCEPT  2012-05-14 15:27:48 debug kernel: [kernel]: iptables POST\_ROUTING pkt 10.2.2.14(<NULL>)->10.155.32.172(eth0) proto(17) 160 bytes: ACCEPT  2012-05-14 15:27:48 debug kernel: L\*: (o) eth0 10.2.2.14->10.155.32.172(46108) ttl(64) mtu(1500) UDP 4500->4500 174 bytes  2012-05-14 15:27:48 debug kernel: [fe]: bypass fe egress procesing and deliver packet to stack on eth0  CW-BR200WP#show logging buffered | include ipfw  2012-05-14 09:06:04 info ah\_ipfw: ACCEPT PACKET: SRC=172.18.252.1 DST=172.29.10.35 PROTO=ICMP TYPE=8 CODE=0 (RULE=2)  **To vpn deny**  2012-05-14 15:41:50 debug kernel: L\*: (i) wifi0.2 172.17.107.2->172.32.1.241(2235) ttl(128) icmp-echo-req(1/75) 60 bytes  2012-05-14 15:41:50 debug kernel: [fe]: MAC session (id [2]) found  2012-05-14 15:41:50 debug kernel: [fe]: fflow 2477:035d:afd4->0019:7722:1180 flag 0x41002, rflow 0019:7722:1180->2477:035d:afd4 flag 0xe1210  2012-05-14 15:41:50 debug kernel: [fe]: fflow acl 0x0/0x0, rflow acl 0x0/0x0  2012-05-14 15:41:50 debug kernel: [fe]: update from-access counters 74 bytes  2012-05-14 15:41:50 debug kernel: [fe]: QoS: ingress pkt fwd(wifi0.2) profile=16 qos=2  2012-05-14 15:41:50 debug kernel: [fe]: set pkt to self  2012-05-14 15:41:50 debug kernel: [fe]: swap incoming dev wifi0.2 -> mgt0.9  2012-05-14 15:41:50 debug kernel: [fe]: allow to self-pak, dst-ip 172.32.1.241,allow-arp 0 allow-dhcp 0 allow-forwarding 1  2012-05-14 15:41:50 debug kernel: [fe]: ip forward: ip pkt with dst-ip 172.32.1.241 received on wifi0.2  2012-05-14 15:41:50 debug kernel: [fe]: deliver pak to self on mgt0.9 with fw mark 1  2012-05-14 15:41:50 debug kernel: L\*: (u) mgt0.9 172.17.107.2->172.32.1.241(2235) ttl(128) icmp-echo-req(1/75) 60 bytes  2012-05-14 15:41:50 debug kernel: [kernel]: iptables PRE\_ROUTING pkt 172.17.107.2(mgt0.9)->172.32.1.241(<NULL>) proto(1) 60 bytes: ACCEPT  2012-05-14 15:41:50 debug kernel: [kernel]: routing done, 172.17.107.2 -> 172.32.1.241 ttl(128) proto(1) mark(1) 60 bytes, found route in table:Main(Split)  2012-05-14 15:41:50 debug kernel: [kernel]: create routing cache:172.17.107.2 -> 172.32.1.241 fwmark 1 dev tunnel0  2012-05-14 15:41:50 debug kernel: [kernel]: iptables FORWARD pkt 172.17.107.2(mgt0.9)->172.32.1.241(tunnel0) proto(1) 60 bytes: DROP  2012-05-14 15:41:50 debug kernel: L\*: (!) tunnel0 172.17.107.2->172.32.1.241(2235) ttl(127) mtu(1476) icmp-echo-req(1/75) 60 bytes  CW-BR200WP#show logging buffered | include ipfw  2012-05-14 08:46:06 info ah\_ipfw: DROP PACKET: SRC=172.17.107.2 DST=172.32.1.241 PROTO=ICMP TYPE=8 CODE=0 (RULE=1) | | |

##### Case ID Network-Firewall\_Parameter\_3

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Parameter\_3 | | |
| **Priority** | Accept | **Automation Flag** | No |
| **Topology to use** | Topolopy4 | | |
| **Description** | Network firewall “From” 2 different VPNs test | | |
| **Pre-condition** | -Configure AP1  Enable tunnel1 between AP1 and Gateway1  Enable tunnel2 between AP1 and Gateway2  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (wifi) | | |
| **Test procedure** | 1) Laptop2 and Laptop3 ping Laptop1  2) Configure network firewall rule  ***“network-firewall name 1001 from vpn to network 10.1.10.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop2 and Laptop3 ping Laptop1  4) Delete network firewall config on AP1  ***“no network-firewall”***  5) Laptop2 and Laptop3 ping Laptop1  6) Configure network firewall rule on AP1  ***“network-firewall name 1001 from vpn to network 10.1.10.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  7) Laptop2 and Laptop3 ping Laptop1  8) Delete network firewall config on AP1  ***“no network-firewall”***  9) Laptop2 and Laptop3 ping Laptop1 | | |
| **Expect result** | 1) Laptop2 and Laptop3 ping Laptop1 successfully  3) Laptop2 and Laptop3 ping Laptop1 successfully  5) Laptop2 and Laptop3 ping Laptop1 successfully  7) Laptop2 and Laptop3 ping Laptop1 unsuccessfully  9) Laptop2 and Laptop3 ping Laptop1 successfully | | |

##### Case ID Network-Firewall\_Parameter\_4

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Parameter\_4 | | |
| **Priority** | Accept | **Automation Flag** | No |
| **Topology to use** | Topolopy4 | | |
| **Description** | Network firewall “To” 2 different VPNs test | | |
| **Pre-condition** | -Configure AP1  Enable tunnel1 between AP1 and Gateway1  Enable tunnel2 between AP1 and Gateway2  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (wifi) | | |
| **Test procedure** | 1) Laptop1 ping Laptop2 and Laptop3  2) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to vpn action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 ping Laptop2 and Laptop3  4) Delete network firewall config on AP1  ***“no network-firewall”***  5) Laptop1 ping Laptop2 and Laptop3  6) Configure network firewall rule on AP1  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to vpn action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  7) Laptop1 ping Laptop2 and Laptop3  8) Delete network firewall config on AP1  ***“no network-firewall”***  9) Laptop1 ping Laptop2 and Laptop3 | | |
| **Expect result** | 1) Laptop1 ping Laptop2 and Laptop3 successfully  3) Laptop1 ping Laptop2 and Laptop3 successfully  5) Laptop1 ping Laptop2 and Laptop3 successfully  7) Laptop1 ping Laptop2 and Laptop3 unsuccessfully  9) Laptop1 ping Laptop2 and Laptop3 successfully | | |

#### IP/Mask test case

##### Case ID Network-Firewall\_Parameter\_5

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Parameter\_5 | | |
| **Priority** | High | **Automation Flag** | No |
| **Topology to use** | Topolopy5 | | |
| **Description** | Network firewall “From” IP/Mask test | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2  Laptop3 connect to Mgt0.1 IPaddr 10.1.10.3 | | |
| **Test procedure** | 1) Laptop1 and Laptop3 ping Laptop2  2) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.0 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 and Laptop3 ping Laptop2  4) Delete network firewall config  ***“no network-firewall”***  5) Laptop1 and Laptop3 ping Laptop2  6) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.0 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  7) Laptop1 and Laptop3 ping Laptop2  8) Delete network firewall config on AP1  ***“no network-firewall”***  9) Laptop1 and Laptop3 ping Laptop2 | | |
| **Expect result** | 1) Laptop1 and Laptop3 ping Laptop2 successfully  3) Laptop1 and Laptop3 ping Laptop2 successfully  5) Laptop1 and Laptop3 ping Laptop2 successfully  7) Laptop1 and Laptop3 ping Laptop2 unsuccessfully  9) Laptop1 and Laptop3 ping Laptop2 successfully | | |

##### Case ID Network-Firewall\_Parameter\_6

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Parameter\_6 | | |
| **Priority** | High | **Automation Flag** | No |
| **Topology to use** | Topolopy5 | | |
| **Description** | Network firewall “To” IP/Mask test | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2  Laptop3 connect to Mgt0.1 IPaddr 10.1.10.3 | | |
| **Test procedure** | 1) Laptop2 ping Laptop1 and Laptop3  2) Configure network firewall rule  ***“network-firewall name 1001 to network 10.1.10.2 255.255.255.0 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop2 ping Laptop1 and Laptop3  4) Delete network firewall config  ***“no network-firewall”***  5) Laptop2 ping Laptop1 and Laptop3  6) Configure network firewall rule  ***“network-firewall name 1001 to network 10.1.10.2 255.255.255.0 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  7) Laptop2 ping Laptop1 and Laptop3  8) Delete network firewall config on AP1  ***“no network-firewall”***  9) Laptop2 ping Laptop1 and Laptop3 | | |
| **Expect result** | 1) Laptop2 ping Laptop1 and Laptop3 successfully  3) Laptop2 ping Laptop1 and Laptop3 successfully  5) Laptop2 ping Laptop1 and Laptop3 successfully  7) Laptop2 ping Laptop1 and Laptop3 unsuccessfully  9) Laptop2 ping Laptop1 and Laptop3 successfully | | |

##### Case ID Network-Firewall\_Parameter\_7

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Parameter\_7 | | |
| **Priority** | Accept | **Automation Flag** | No |
| **Topology to use** | Topolopy3 | | |
| **Description** | Network firewall “From” IP/Mask test when the packets are from VPN | | |
| **Pre-condition** | -Configure AP1  Enable tunnel1 between AP1 and Gateway1  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (wifi)  -Configure AP2  Enable tunnel2 between AP2 and Gateway1  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 20.1.10.1 gateway 20.1.10.1  Laptop2 connect to Mgt0.1 IPaddr 20.1.10.2 (wifi)  -Laptop3 get IPaddr 192.168.10.10  -Laptop4 get IPaddr 192.168.20.20 | | |
| **Test procedure** | 1) Laptop3 and Laptop4 ping Laptop1  2) Configure network firewall rule  ***“network-firewall name 1001 from network 192.168.10.1 255.255.255.0 to network 10.1.10.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop3 and Laptop4 ping Laptop1  4) Delete network firewall config on AP1  ***“no network-firewall”***  5) Laptop3 and Laptop4 ping Laptop1  6) Configure network firewall rule on AP1  ***“network-firewall name 1001 from network 192.168.10.1 255.255.255.0 to network 10.1.10.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  7) Laptop3 and Laptop4 ping Laptop1  8) Delete network firewall config on AP1  ***“no network-firewall”***  9) Laptop3 and Laptop4 ping Laptop1 | | |
| **Expect result** | 1) Laptop3 ping Laptop1 successfully, Laptop4 ping Laptop1 successfully  3) Laptop3 ping Laptop1 successfully, Laptop4 ping Laptop1 unsuccessfully  5) Laptop3 ping Laptop1 successfully, Laptop4 ping Laptop1 successfully  7) Laptop3 ping Laptop1 unsuccessfully, Laptop4 ping Laptop1 unsuccessfully  9) Laptop3 ping Laptop1 successfully, Laptop4 ping Laptop1 successfully | | |

##### Case ID Network-Firewall\_Parameter\_8

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Parameter\_8 | | |
| **Priority** | Accept | **Automation Flag** | No |
| **Topology to use** | Topolopy3 | | |
| **Description** | Network firewall “To” IP/Mask test when the packets are to VPN | | |
| **Pre-condition** | -Configure AP1  Enable tunnel1 between AP1 and Gateway1  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (wifi)  -Configure AP2  Enable tunnel2 between AP2 and Gateway1  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 20.1.10.1 gateway 20.1.10.1  Laptop2 connect to Mgt0.1 IPaddr 20.1.10.2 (wifi)  -Laptop3 get IPaddr 192.168.10.10  -Laptop4 get IPaddr 192.168.20.20 | | |
| **Test procedure** | 1) Laptop1 ping Laptop3 and Laptop4  2) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 192.168.10.1 255.255.255.0 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 ping Laptop3 and Laptop4  4) Delete network firewall config on AP1  ***“no network-firewall”***  5) Laptop1 ping Laptop3 and Laptop4  6) Configure network firewall rule on AP1  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 192.168.10.1 255.255.255.0 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  7) Laptop1 ping Laptop3 and Laptop4  8) Delete network firewall config on AP1  ***“no network-firewall”***  9) Laptop1 ping Laptop3 and Laptop4 | | |
| **Expect result** | 1) Laptop1 ping Laptop3 successfully, Laptop1 ping Laptop4 successfully  3) Laptop1 ping Laptop3 successfully, Laptop1 ping Laptop4 unsuccessfully  5) Laptop1 ping Laptop3 successfully, Laptop1 ping Laptop4 successfully  7) Laptop1 ping Laptop3 unsuccessfully, Laptop1 ping Laptop4 unsuccessfully  9) Laptop1 ping Laptop3 successfully, Laptop1 ping Laptop4 successfully | | |

##### Case ID Network-Firewall\_Parameter\_9

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Parameter\_9 | | |
| **Priority** | High | **Automation Flag** | No |
| **Topology to use** | Topolopy3 | | |
| **Description** | Network firewall IP/Mask test when the packets are from VPN to VPN | | |
| **Pre-condition** | -Configure AP1  Enable tunnel1 between AP1 and Gateway1  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (wifi)  -Configure AP2  Enable tunnel2 between AP2 and Gateway1  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 20.1.10.1 gateway 20.1.10.1  Laptop2 connect to Mgt0.1 IPaddr 20.1.10.2 (wifi)  -Laptop3 get IPaddr 192.168.10.10  -Laptop4 get IPaddr 192.168.20.20 | | |
| **Test procedure** | 1) Laptop1 and Laptop2 ping each other  2) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 20.1.10.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from network 20.1.10.2 255.255.255.255 to network 10.1.10.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1003 from any to any action deny logging off”***  3) Laptop1 and Laptop2 ping each other  4) Delete network firewall config on AP1  ***“no network-firewall”***  5) Laptop1 and Laptop2 ping each other  6) Configure network firewall rule on AP1  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 20.1.10.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from network 20.1.10.2 255.255.255.255 to network 10.1.10.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1003 from any to any action deny logging off”***  7) Laptop1 and Laptop2 ping each other  8) Delete network firewall config on AP1  ***“no network-firewall”***  9) Laptop1 and Laptop2 ping each other | | |
| **Expect result** | 1) Laptop1 and Laptop2 ping each other successfully  3) Laptop1 and Laptop2 ping each other successfully  5) Laptop1 and Laptop2 ping each other successfully  7) Laptop1 and Laptop2 ping each other unsuccessfully  9) Laptop1 and Laptop2 ping each other successfully | | |

##### Case ID Network-Firewall\_Parameter\_10

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Parameter\_10 | | |
| **Priority** | High | **Automation Flag** | No |
| **Topology to use** | Topolopy4 | | |
| **Description** | Network firewall IP/Mask test when the packets are to 2 vpn | | |
| **Pre-condition** | -Configure AP1  Enable tunnel1 between AP1 and Gateway1  Enable tunnel2 between AP1 and Gateway2  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (wifi)  -Laptop2 get IPaddr 192.168.10.10  -Laptop3 get IPaddr 192.168.20.20 | | |
| **Test procedure** | 1) Laptop1 ping Laptop2 and Laptop3  2) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 192.168.1.1 255.255.0.0 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 ping Laptop2 and Laptop3  4) Delete network firewall config on AP1  ***“no network-firewall”***  5) Laptop1 ping Laptop2 and Laptop3  6) Configure network firewall rule on AP1  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 192.168.1.1 255.255.0.0 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  7) Laptop1 ping Laptop2 and Laptop3  8) Delete network firewall config on AP1  ***“no network-firewall”***  9) Laptop1 ping Laptop2 and Laptop3 | | |
| **Expect result** | 1) Laptop1 ping Laptop2 and Laptop3 successfully  3) Laptop1 ping Laptop2 and Laptop3 successfully  5) Laptop1 ping Laptop2 and Laptop3 successfully  7) Laptop1 ping Laptop2 and Laptop3 unsuccessfully  9) Laptop1 ping Laptop2 and Laptop3 successfully | | |

#### IP range test case

##### Case ID Network-Firewall\_Parameter\_11

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Parameter\_11 | | |
| **Priority** | Middle | **Automation Flag** | No |
| **Topology to use** | Topolopy5 | | |
| **Description** | Network firewall “From” IP range test | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2  Laptop3 connect to Mgt0.1 IPaddr 10.1.10.3 | | |
| **Test procedure** | 1) Laptop1 and Laptop3 ping Laptop2  2) Configure network firewall rule  ***“network-firewall name 1001 from ip-range 10.1.10.2 10.1.10.254 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 and Laptop3 ping Laptop2  4) Delete network firewall config  ***“no network-firewall”***  5) Laptop1 and Laptop3 ping Laptop2  6) Configure network firewall rule  ***“network-firewall name 1001 from ip-range 10.1.10.2 10.1.10.254 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  7) Laptop1 and Laptop3 ping Laptop2  8) Delete network firewall config on AP1  ***“no network-firewall”***  9) Laptop1 and Laptop3 ping Laptop2 | | |
| **Expect result** | 1) Laptop1 and Laptop3 ping Laptop2 successfully  3) Laptop1 and Laptop3 ping Laptop2 successfully  5) Laptop1 and Laptop3 ping Laptop2 successfully  7) Laptop1 and Laptop3 ping Laptop2 unsuccessfully  9) Laptop1 and Laptop3 ping Laptop2 successfully | | |

##### Case ID Network-Firewall\_Parameter\_12

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Parameter\_12 | | |
| **Priority** | Middle | **Automation Flag** | No |
| **Topology to use** | Topolopy5 | | |
| **Description** | Network firewall “To” IP range test | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2  Laptop3 connect to Mgt0.1 IPaddr 10.1.10.3 | | |
| **Test procedure** | 1) Laptop2 ping Laptop1 and Laptop3  2) Configure network firewall rule  ***“network-firewall name 1001 to ip-range 10.1.10.2 10.1.10.254 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop2 ping Laptop1 and Laptop3  4) Delete network firewall config  ***“no network-firewall”***  5) Laptop2 ping Laptop1 and Laptop3  6) Configure network firewall rule  ***“network-firewall name 1001 to ip-range 10.1.10.2 10.1.10.254 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  7) Laptop2 ping Laptop1 and Laptop3  8) Delete network firewall config on AP1  ***“no network-firewall”***  9) Laptop2 ping Laptop1 and Laptop3 | | |
| **Expect result** | 1) Laptop2 ping Laptop1 and Laptop3 successfully  3) Laptop2 ping Laptop1 and Laptop3 successfully  5) Laptop2 ping Laptop1 and Laptop3 successfully  7) Laptop2 ping Laptop1 and Laptop3 unsuccessfully  9) Laptop2 ping Laptop1 and Laptop3 successfully | | |

##### Case ID Network-Firewall\_Parameter\_13

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Parameter\_13 | | |
| **Priority** | High | **Automation Flag** | No |
| **Topology to use** | Topolopy3 | | |
| **Description** | Network firewall IP range test when the packets are from VPN | | |
| **Pre-condition** | -Configure AP1  Enable tunnel1 between AP1 and Gateway1  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (wifi)  -Configure AP2  Enable tunnel2 between AP2 and Gateway1  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 20.1.10.1 gateway 20.1.10.1  Laptop2 connect to Mgt0.1 IPaddr 20.1.10.2 (wifi)  -Laptop3 get IPaddr 192.168.10.10  -Laptop4 get IPaddr 192.168.20.20 | | |
| **Test procedure** | 1) Laptop3 and Laptop4 ping Laptop1  2) Configure network firewall rule  ***“network-firewall name 1001 from ip-range 192.168.10.1 192.168.10.254 to network 10.1.10.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop3 and Laptop4 ping Laptop1  4) Delete network firewall config on AP1  ***“no network-firewall”***  5) Laptop3 and Laptop4 ping Laptop1  6) Configure network firewall rule on AP1  ***“network-firewall name 1001 from ip-range 192.168.10.1 192.168.10.254 to network 10.1.10.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  7) Laptop3 and Laptop4 ping Laptop1  8) Delete network firewall config on AP1  ***“no network-firewall”***  9) Laptop3 and Laptop4 ping Laptop1 | | |
| **Expect result** | 1) Laptop3 ping Laptop1 successfully, Laptop4 ping Laptop1 successfully  3) Laptop3 ping Laptop1 successfully, Laptop4 ping Laptop1 unsuccessfully  5) Laptop3 ping Laptop1 successfully, Laptop4 ping Laptop1 successfully  7) Laptop3 ping Laptop1 unsuccessfully, Laptop4 ping Laptop1 unsuccessfully  9) Laptop3 ping Laptop1 successfully, Laptop4 ping Laptop1 successfully | | |

#### IP/wildcard test case

##### Case ID Network-Firewall\_Parameter\_14

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Parameter\_14 | | |
| **Priority** | Middle | **Automation Flag** | No |
| **Topology to use** | Topolopy5 | | |
| **Description** | Network firewall “From” IP/wildcard test | | |
| **Pre-condition** | -Configure AP  Enable 3 dhcp server（mgt0.1 mgt0.2 mgt0.3）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.2.20.1 gateway 10.2.20.1  Mgt0.3 vlan30 IPaddr 10.1.30.1 gateway 10.1.30.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.2.20.2  Laptop3 connect to Mgt0.3 IPaddr 10.1.30.2 | | |
| **Test procedure** | 1) Laptop1 and Laptop3 ping Laptop2  2) Configure network firewall rule  ***“network-firewall name 1001 from wildcard 10.1.10.2 255.255.0.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 and Laptop3 ping Laptop2  4) Delete network firewall config  ***“no network-firewall”***  5) Laptop1 and Laptop3 ping Laptop2  6) Configure network firewall rule  ***“network-firewall name 1001 from wildcard 10.1.10.2 255.255.0.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  7) Laptop1 and Laptop3 ping Laptop2  8) Delete network firewall config on AP1  ***“no network-firewall”***  9) Laptop1 and Laptop3 ping Laptop2 | | |
| **Expect result** | 1) Laptop1 and Laptop3 ping Laptop2 successfully  3) Laptop1 and Laptop3 ping Laptop2 successfully  5) Laptop1 and Laptop3 ping Laptop2 successfully  7) Laptop1 and Laptop3 ping Laptop2 unsuccessfully  9) Laptop1 and Laptop3 ping Laptop2 successfully | | |

##### Case ID Network-Firewall\_Parameter\_15

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Parameter\_15 | | |
| **Priority** | Middle | **Automation Flag** | No |
| **Topology to use** | Topolopy5 | | |
| **Description** | Network firewall “To” IP/wildcard test | | |
| **Pre-condition** | -Configure AP  Enable 3 dhcp server（mgt0.1 mgt0.2 mgt0.3）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.2.20.1 gateway 10.2.20.1  Mgt0.3 vlan30 IPaddr 10.1.30.1 gateway 10.1.30.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.2.20.2  Laptop3 connect to Mgt0.3 IPaddr 10.1.30.2 | | |
| **Test procedure** | 1) Laptop2 ping Laptop1 and Laptop3  2) Configure network firewall rule  ***“network-firewall name 1001 to wildcard 10.1.10.2 255.255.0.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop2 ping Laptop1 and Laptop3  4) Delete network firewall config  ***“no network-firewall”***  5) Laptop2 ping Laptop1 and Laptop3  6) Configure network firewall rule  ***“network-firewall name 1001 to wildcard 10.1.10.2 255.255.0.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  7) Laptop2 ping Laptop1 and Laptop3  8) Delete network firewall config on AP1  ***“no network-firewall”***  9) Laptop2 ping Laptop1 and Laptop3 | | |
| **Expect result** | 1) Laptop2 ping Laptop1 and Laptop3 successfully  3) Laptop2 ping Laptop1 and Laptop3 successfully  5) Laptop2 ping Laptop1 and Laptop3 successfully  7) Laptop2 ping Laptop1 and Laptop3 unsuccessfully  9) Laptop2 ping Laptop1 and Laptop3 successfully | | |

##### Case ID Network-Firewall\_Parameter\_16

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Parameter\_16 | | |
| **Priority** | High | **Automation Flag** | No |
| **Topology to use** | Topolopy3 | | |
| **Description** | Network firewall IP/Wildcard test when the packets are from VPN | | |
| **Pre-condition** | -Configure AP1  Enable tunnel1 between AP1 and Gateway1  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (wifi)  -Configure AP2  Enable tunnel2 between AP2 and Gateway1  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 20.1.10.1 gateway 20.1.10.1  Laptop2 connect to Mgt0.1 IPaddr 20.1.10.2 (wifi)  -Laptop3 get IPaddr 192.168.10.10  -Laptop4 get IPaddr 192.168.20.20 | | |
| **Test procedure** | 1) Laptop3 and Laptop4 ping Laptop1  2) Configure network firewall rule  ***“network-firewall name 1001 from wildcard 192.168.10.10 255.255.0.255 to network 10.1.10.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop3 and Laptop4 ping Laptop1  4) Delete network firewall config on AP1  ***“no network-firewall”***  5) Laptop3 and Laptop4 ping Laptop1  6) Configure network firewall rule on AP1  ***“network-firewall name 1001 from wildcard 192.168.10.10 255.255.0.255 to network 10.1.10.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  7) Laptop3 and Laptop4 ping Laptop1  8) Delete network firewall config on AP1  ***“no network-firewall”***  9) Laptop3 and Laptop4 ping Laptop1 | | |
| **Expect result** | 1) Laptop3 ping Laptop1 successfully, Laptop4 ping Laptop1 successfully  3) Laptop3 ping Laptop1 successfully, Laptop4 ping Laptop1 unsuccessfully  5) Laptop3 ping Laptop1 successfully, Laptop4 ping Laptop1 successfully  7) Laptop3 ping Laptop1 unsuccessfully, Laptop4 ping Laptop1 unsuccessfully  9) Laptop3 ping Laptop1 successfully, Laptop4 ping Laptop1 successfully | | |

#### User-profile test case

##### Case ID Network-Firewall\_Parameter\_17

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Parameter\_17 | | |
| **Priority** | Accept | **Automation Flag** | No |
| **Topology to use** | Topolopy5 | | |
| **Description** | Network firewall “From” user-profile test | | |
| **Pre-condition** | -Configure AP  Enable 3 dhcp server（mgt0.1 mgt0.2 mgt0.3）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Mgt0.3 vlan30 IPaddr 10.1.30.1 gateway 10.1.30.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (user-profile name up10)  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 (user-profile name up20)  Laptop3 connect to Mgt0.3 IPaddr 10.1.30.2 (user-profile name up30) | | |
| **Test procedure** | 1) Laptop1 and Laptop3 ping Laptop2  2) Configure network firewall rule  ***“network-firewall name 1001 from user-profile up10 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 and Laptop3 ping Laptop2  4) Delete network firewall config  ***“no network-firewall”***  5) Laptop1 and Laptop3 ping Laptop2  6) Configure network firewall rule  ***“network-firewall name 1001 from user-profile up10 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  7) Laptop1 and Laptop3 ping Laptop2  8) Delete network firewall config on AP1  ***“no network-firewall”***  9) Laptop1 and Laptop3 ping Laptop2 | | |
| **Expect result** | 1) Laptop1 ping Laptop2 successfully, Laptop3 ping Laptop2 successfully  3) Laptop1 ping Laptop2 successfully, Laptop3 ping Laptop2 unsuccessfully  5) Laptop1 ping Laptop2 successfully, Laptop3 ping Laptop2 successfully  7) Laptop1 ping Laptop2 unsuccessfully, Laptop3 ping Laptop2 unsuccessfully  9) Laptop1 ping Laptop2 successfully, Laptop3 ping Laptop2 successfully | | |

##### Case ID Network-Firewall\_Parameter\_18

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Parameter\_18 | | |
| **Priority** | Accept | **Automation Flag** | No |
| **Topology to use** | Topolopy5 | | |
| **Description** | Network firewall the same user-profile but not the same attribute test | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2 (attribute 1)  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 (attribute 3)  Laptop3 connect to Mgt0.1 IPaddr 10.1.10.3 (attribute 2)  User-profile Upid10 binds attribute 1-2 vlan10  User-profile Upid20 binds attribute 3 vlan 20 | | |
| **Test procedure** | 1) Laptop1 and Laptop3 ping Laptop2  2) Configure network firewall rule  ***“network-firewall name 1001 from user-profile upid10 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 and Laptop3 ping Laptop2  4) Delete network firewall config  ***“no network-firewall”***  5) Laptop1 and Laptop3 ping Laptop2  6) Configure network firewall rule  ***“network-firewall name 1001 from user-profile upid10 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  7) Laptop1 and Laptop3 ping Laptop2  8) Delete network firewall config on AP1  ***“no network-firewall”***  9) Laptop1 and Laptop3 ping Laptop2 | | |
| **Expect result** | 1) Laptop1 and Laptop3 ping Laptop2 successfully  3) Laptop1 and Laptop3 ping Laptop2 successfully  5) Laptop1 and Laptop3 ping Laptop2 successfully  7) Laptop1 and Laptop3 ping Laptop2 unsuccessfully  9) Laptop1 and Laptop3 ping Laptop2 successfully | | |

#### Hostname test case

##### Basic function test case

##### Case ID Network-Firewall\_Parameter\_19

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Parameter\_19 | | |
| **Priority** | Accept | **Automation Flag** | No |
| **Topology to use** | Topolopy6 | | |
| **Description** | Network firewall “To” hostname test | | |
| **Pre-condition** | -Configure AP  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  AP get IPaddr(interface wan) <IP1> from server  The server’s hostname is <hostname1> | | |
| **Test procedure** | 1) Laptop1 ping Server  2) Configure network firewall rule  ***“network-firewall name 1001 to hostname <hostname1> action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 ping Server  4) Delete network firewall config  ***“no network-firewall”***  5) Laptop1 ping Server  6) Configure network firewall rule  ***“network-firewall name 1001 to hostname <hostname1> action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  7) Laptop1 ping Server  8) Delete network firewall config on AP1  ***“no network-firewall”***  9) Laptop1 ping Server | | |
| **Expect result** | 1) Laptop1 ping Server successfully  3) Laptop1 ping Server successfully  5) Laptop1 ping Server successfully  7) Laptop1 ping Server unsuccessfully  9) Laptop1 ping Server successfully | | |

##### Hostname resolve test case

##### Case ID Network-Firewall\_Parameter\_20

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Parameter\_20 | | |
| **Priority** | High | **Automation Flag** | No |
| **Topology to use** | Topolopy6 | | |
| **Description** | Hostname is resolved in normal situation | | |
| **Pre-condition** | -Configure AP  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  AP get IPaddr(interface wan) <IP1> from server  The server’s hostname is <hostname1> | | |
| **Test procedure** | 1) Configure network firewall rule  ***“network-firewall name 1001 to hostname www.google.com action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  2) Show network firewall rules in shell  ***“\_shell”***  ***“iptables -nL”*** | | |
| **Expect result** | 2) We can see several IP address in destination IP frame , not “www.google.com” | | |

### Network Firewall services test case

##### Case ID Network-Firewall\_Services\_1

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Services\_1 | | |
| **Priority** | Middle | **Automation Flag** | No |
| **Topology to use** | Topolopy5 | | |
| **Description** | Network firewall user-define service test | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2  Laptop3 connect to Mgt0.1 IPaddr 10.1.10.3 | | |
| **Test procedure** | 1) Configure user-define service  ***“service service1 protocol 200 port 521”***  ***“service service2 protocol svp port 8000”***  ***“service service3 protocol tcp port 8001”***  ***“service service4 protocol udp port 8002”***  2) Configure network firewall rule  ***“network-firewall name 1001 service service1 action permit logging off”***  ***“network-firewall name 1002 service service2 action permit logging off”***  ***“network-firewall name 1003 service service3 action permit logging off”***  ***“network-firewall name 1004 service service4 action permit logging off”***  ***“network-firewall name 1005 from any to any action deny logging off”***  3) Show iptables rules in shell and contrast the protocol and port with service defined above  ***“\_shell”***  ***“iptables -nL”***  4) Laptop1 uses tools (such as hping) send packets as above to Laptop2  5) Look up the packets captured by Laptop2  6) Delete network firewall configure  ***“no network-firewall”***  7) Configure network firewall rule  ***“network-firewall name 1001 service service1 action deny logging off”***  ***“network-firewall name 1002 service service2 action deny logging off”***  ***“network-firewall name 1003 service service3 action deny logging off”***  ***“network-firewall name 1004 service service4 action deny logging off”***  ***“network-firewall name 1005 from any to any action permit logging off”***  8) Show iptables rules in shell and contrast the protocol and port with service defined above  ***“\_shell”***  ***“iptables -nL”***  9) Laptop1 uses tools (such as hping) send packets as above to Laptop2  10) Look up the packets captured by Laptop2 | | |
| **Expect result** | 3) Iptables rules’ protocol and port is the same as the services defined by user  5) We can see all services packets  7) Iptables rules’ protocol and port is the same as the services defined by user  10) We cannot see any services packets | | |

##### Case ID Network-Firewall\_Services\_2

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Services\_2 | | |
| **Priority** | High | **Automation Flag** | No |
| **Topology to use** | Topolopy6 | | |
| **Description** | FTP(port mode) enable alg influence on network Firewall rules | | |
| **Pre-condition** | -Configure AP  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  AP get IPaddr(interface wan) <IP1> from server  -Configure Server  Enable FTP function port mode | | |
| **Test procedure** | 1) Configure network firewall rule  ***“network-firewall name 1001 to network 192.168.1.1 255.255.255.255 service ftp action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  2) Laptop1 uses FTP connect to server and download/upload files | | |
| **Expect result** | 2) Laptop1 can connect to server and download/upload files successfully | | |

##### Case ID Network-Firewall\_Services\_3

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Services\_3 | | |
| **Priority** | High | **Automation Flag** | No |
| **Topology to use** | Topolopy6 | | |
| **Description** | FTP(passive mode) enable alg influence on network Firewall rules | | |
| **Pre-condition** | -Configure AP  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  AP get IPaddr(interface wan) <IP1> from server  -Configure Server  Enable FTP function passive mode | | |
| **Test procedure** | 1) Configure network firewall rule  ***“network-firewall name 1001 to network 192.168.1.1 255.255.255.255 service ftp action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  2) Laptop1 uses FTP connect to server and download/upload files | | |
| **Expect result** | 2) Laptop1 can connect to server and download/upload files successfully | | |

##### Case ID Network-Firewall\_Services\_4

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Services\_4 | | |
| **Priority** | Middle | **Automation Flag** | No |
| **Topology to use** | Topolopy6 | | |
| **Description** | FTP(EPRT mode) enable alg influence on network Firewall rules | | |
| **Pre-condition** | -Configure AP  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  AP get IPaddr(interface wan) <IP1> from server  -Configure Server  Enable FTP function EPRT mode | | |
| **Test procedure** | 1) Configure network firewall rule  ***“network-firewall name 1001 to network 192.168.1.1 255.255.255.255 service ftp action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  2) Laptop1 uses FTP connect to server and download/upload files | | |
| **Expect result** | 2) Laptop1 can connect to server and download/upload files successfully | | |

##### Case ID Network-Firewall\_Services\_5

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Services\_5 | | |
| **Priority** | Middle | **Automation Flag** | No |
| **Topology to use** | Topolopy6 | | |
| **Description** | FTP(EPSV mode) enable alg influence on network Firewall rules | | |
| **Pre-condition** | -Configure AP  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  AP get IPaddr(interface wan) <IP1> from server  -Configure Server  Enable FTP function EPSV mode | | |
| **Test procedure** | 1) Configure network firewall rule  ***“network-firewall name 1001 to network 192.168.1.1 255.255.255.255 service ftp action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  2) Laptop1 uses FTP connect to server and download/upload files | | |
| **Expect result** | 2) Laptop1 can connect to server and download/upload files successfully | | |

##### Case ID Network-Firewall\_Services\_6

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Services\_6 | | |
| **Priority** | High | **Automation Flag** | No |
| **Topology to use** | Topolopy6 | | |
| **Description** | TFTP(RRQ mode) enable alg influence on network Firewall rules | | |
| **Pre-condition** | -Configure AP  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  AP get IPaddr(interface wan) <IP1> from server  -Configure Server  Enable TFTP function RRQ mode | | |
| **Test procedure** | 1) Configure network firewall rule  ***“network-firewall name 1001 to network 192.168.1.1 255.255.255.255 service ftp action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  2) Laptop1 uses TFTP connect to server and download/upload files | | |
| **Expect result** | 2) Laptop1 can connect to server and download files successfully, cannot modify | | |

##### Case ID Network-Firewall\_Services\_7

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Services\_7 | | |
| **Priority** | High | **Automation Flag** | No |
| **Topology to use** | Topolopy6 | | |
| **Description** | TFTP(WRQ mode) enable alg influence on network Firewall rules | | |
| **Pre-condition** | -Configure AP  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  AP get IPaddr(interface wan) <IP1> from server  -Configure Server  Enable TFTP function WRQ mode | | |
| **Test procedure** | 1) Configure network firewall rule  ***“network-firewall name 1001 to network 192.168.1.1 255.255.255.255 service ftp action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  2) Laptop1 uses Ftp connect to server and download/upload files | | |
| **Expect result** | 2) Laptop1 can connect to server successfully, can modify files | | |

##### Case ID Network-Firewall\_Services\_8

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Services\_8 | | |
| **Priority** | High | **Automation Flag** | No |
| **Topology to use** | Topolopy10 | | |
| **Description** | SIP enable alg influence on network Firewall rules | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 | | |
| **Test procedure** | 1.Laptop2 use tools such as x-lite to call Laptop1  2.Config Firewall  ***"network-firewall name 1 service sip action permit logging on"***  ***"network-firewall name 2 logging on"***  ***"clear network-firewall session all"***  3.Laptop2 call Laptop1 | | |
| **Expect result** | 1.Laptop2 can call Laptop1 and transmit voice data successfully  2.Laptop2 can call Laptop1 and transmit voice data successfully(sip alg is always on) | | |

### Network Firewall log test case

##### Case ID Network-Firewall\_Log\_1

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_log\_1 | | |
| **Priority** | Middle | **Automation Flag** | No |
| **Topology to use** | Topolopy4 | | |
| **Description** | Network firewall log “logging on” test | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2  Laptop3 connect to Mgt0.1 IPaddr 10.1.10.3 | | |
| **Test procedure** | 1) Laptop1 and Laptop3 ping Laptop2 100 packets  2) Show logging and look up the network firewall logs  ***“show logging buffered | include l3-fw”***  3) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 10.1.20.2 255.255.255.255 action permit logging on”***  ***“network-firewall name 1002 from any to any action deny logging off”***  4) Laptop1 and Laptop3 ping Laptop2 100 packets  5) Show logging and look up the network firewall logs  ***“show logging buffered | include l3-fw”***  6) Delete network firewall config  ***“no network-firewall”***  7) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 10.1.20.2 255.255.255.255 action deny logging on”***  ***“network-firewall name 1002 from any to any action deny logging off”***  8) Laptop1 and Laptop3 ping Laptop2 100 packets  9) Show logging and look up the network firewall logs  ***“show logging buffered | include l3-fw”***  10) Delete network firewall config on AP1  ***“no network-firewall”***  11) Laptop1 and Laptop3 ping Laptop2 100 packets  12) Show logging and look up the network firewall logs  ***“show logging buffered | include l3-fw”*** | | |
| **Expect result** | 2) We cannot see any logs  5) We can only see the logs of packets from Laptop1 (total 100 entries)  9) We can only see the logs of packets from Laptop1 (total 100 entries)  12) We cannot see any logs | | |

##### Case ID Network-Firewall\_Log\_2

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_log\_2 | | |
| **Priority** | Middle | **Automation Flag** | No |
| **Topology to use** | Topolopy4 | | |
| **Description** | Network firewall log “logging off” test | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2  Laptop3 connect to Mgt0.1 IPaddr 10.1.10.3 | | |
| **Test procedure** | 1) Laptop1 and Laptop3 ping Laptop2 100 packets  2) Show logging and look up the network firewall logs  ***“show logging buffered | include l3-fw”***  3) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 10.1.20.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  4) Laptop1 and Laptop3 ping Laptop2 100 packets  5) Show logging and look up the network firewall logs  ***“show logging buffered | include l3-fw”***  6) Delete network firewall config  ***“no network-firewall”***  7) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 10.1.20.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  8) Laptop1 and Laptop3 ping Laptop2 100 packets  9) Show logging and look up the network firewall logs  ***“show logging buffered | include l3-fw”***  10) Delete network firewall config on AP1  ***“no network-firewall”***  11) Laptop1 and Laptop3 ping Laptop2 100 packets  12) Show logging and look up the network firewall logs  ***“show logging buffered | include l3-fw”*** | | |
| **Expect result** | 2) We cannot see any logs  5) We cannot see any logs  9) We cannot see any logs  12) We cannot see any logs | | |

##### Case ID Network-Firewall\_Log\_3

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_log\_3 | | |
| **Priority** | Middle | **Automation Flag** | No |
| **Topology to use** | Topolopy4 | | |
| **Description** | Network firewall log “logging on” , FTP normally exit clear session test | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2  Laptop3 connect to Mgt0.1 IPaddr 10.1.10.3  Laptop2 enable FTP server | | |
| **Test procedure** | 1) Laptop1 and Laptop3 connects to Laptop2 by FTP, exit normally, repeat 5 times  2) Show logging and look up the network firewall logs  ***“show logging buffered | include l3-fw”***  3) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 10.1.20.2 255.255.255.255 action permit logging on”***  ***“network-firewall name 1002 from any to any action deny logging off”***  4) Laptop1 and Laptop3 connects to Laptop2 by FTP, exit normally, repeat 5 times  5) Show logging and look up the network firewall logs  ***“show logging buffered | include l3-fw”***  6) Delete network firewall config  ***“no network-firewall”***  7) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 10.1.20.2 255.255.255.255 action deny logging on”***  ***“network-firewall name 1002 from any to any action deny logging off”***  8) Laptop1 and Laptop3 connects to Laptop2 by FTP, exit normally, repeat 5 times  9) Show logging and look up the network firewall logs  ***“show logging buffered | include l3-fw”***  10) Delete network firewall config on AP1  ***“no network-firewall”***  11) Laptop1 and Laptop3 connects to Laptop2 by FTP, exit normally, repeat 5 times  12) Show logging and look up the network firewall logs  ***“show logging buffered | include l3-fw”*** | | |
| **Expect result** | 2) We cannot see any logs  5) We can only see the session created logs of Laptop1 (total 5 entry?)  9) We cannot see any logs  12) We cannot see any logs | | |

##### Case ID Network-Firewall\_Log\_4

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_log\_4 | | |
| **Priority** | Middle | **Automation Flag** | No |
| **Topology to use** | Topolopy4 | | |
| **Description** | Network firewall log “logging on” , session aging test | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2  Laptop3 connect to Mgt0.1 IPaddr 10.1.10.3 | | |
| **Test procedure** | 1) Laptop1 and Laptop3 uses tool (such as hping) send 10 Udp packets to Laptop2  2) Clear session and configure network firewall rule  ***“no network-firewall”***  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 10.1.20.2 255.255.255.255 action permit logging on”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 and Laptop3 uses tool (such as hping) send 10 Udp packets to Laptop2  4) Show logging and look up the network firewall logs  ***“show logging buffered | include l3-fw”***  5) After session aging time  6) Laptop1 and Laptop3 uses tool (such as hping) send 10 Udp packets to Laptop2 | | |
| **Expect result** | 3) We can only see the session created logs of Laptop1 (total 1 entry)  6) We can only see the session created logs of Laptop1 (total 2 entry) | | |

##### Case ID Network-Firewall\_Log\_5

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_log\_5 | | |
| **Priority** | Middle | **Automation Flag** | No |
| **Topology to use** | Topolopy4 | | |
| **Description** | Network firewall log “logging on” , clear session manually test | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2  Laptop3 connect to Mgt0.1 IPaddr 10.1.10.3 | | |
| **Test procedure** | 1) Laptop1 and Laptop3 uses tool (such as hping) send 10 Udp packets to Laptop2  2) Clear session and configure network firewall rule  ***“no network-firewall”***  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 10.1.20.2 255.255.255.255 action permit logging on”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Laptop1 and Laptop3 uses tool (such as hping) send 10 Udp packets to Laptop2  4) Show logging and look up the network firewall logs  ***“show logging buffered | include l3-fw”***  5) Clear session and configure network firewall rule  ***“no network-firewall”***  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 10.1.20.2 255.255.255.255 action permit logging on”***  ***“network-firewall name 1002 from any to any action deny logging off”***  6) Laptop1 and Laptop3 uses tool (such as hping) send 10 Udp packets to Laptop2 | | |
| **Expect result** | 3) We can only see the session created logs of Laptop1 (total 1 entry)  6) We can only see the session created logs of Laptop1 (total 1 entry) | | |

##### Case ID Network-Firewall\_Log\_6

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_log\_6 | | |
| **Priority** | Middle | **Automation Flag** | No |
| **Topology to use** | Topolopy4 | | |
| **Description** | Modify network firewall log “logging on” to “logging off” | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2  Laptop3 connect to Mgt0.1 IPaddr 10.1.10.3 | | |
| **Test procedure** | 1) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 10.1.20.2 255.255.255.255 action permit logging on”***  ***“network-firewall name 1002 from any to any action deny logging off”***  2) Laptop1 and Laptop3 ping Laptop2 continuously  3) Show logging and look up the network firewall logs  ***“show logging buffered | include l3-fw”***  4) Delete network firewall config  ***“no network-firewall”***  5) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 10.1.20.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  6) Show logging and look up the network firewall logs  ***“show logging buffered | include l3-fw”***  10) Delete network firewall config on AP1  ***“no network-firewall”***  7) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to network 10.1.20.2 255.255.255.255 action permit logging on”***  ***“network-firewall name 1002 from any to any action deny logging off”***  8) Show logging and look up the network firewall logs  ***“show logging buffered | include l3-fw”*** | | |
| **Expect result** | 3) We can only see the logs of packets from Laptop1  6) We cannot see any logs  8) We can only see the session created logs of Laptop1 | | |

### Network firewall fragment test case

##### Case ID Network-Firewall\_Fragment\_1

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Fragment\_1 | | |
| **Priority** | Middle | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Fragments are sent in order(permit) | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 | | |
| **Test procedure** | 1) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  2) Laptop1 sends fragments to Laptop2 in order  3) Check the packets in Laptop2 | | |
| **Expect result** | 3) Laptop2 should receive all fragments and resume the packet successfully | | |

##### Case ID Network-Firewall\_Fragment\_2

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Fragment\_2 | | |
| **Priority** | Middle | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Fragments are sent in order(deny) | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 | | |
| **Test procedure** | 1) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  2) Laptop1 sends fragments to Laptop2 in order  3) Check the packets in Laptop2 | | |
| **Expect result** | 3) Laptop2 receive all fragments but the first one, so cannot resume the packet | | |

##### Case ID Network-Firewall\_Fragment\_3

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Fragment\_3 | | |
| **Priority** | Middle | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Fragments are sent disorder | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 | | |
| **Test procedure** | 1) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  2) Laptop1 sends fragments to Laptop2 in disorder  3) Check the packets captured by Laptop2  4) Delete network firewall configure  ***“no network-firewall”***  5) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 action deny logging on”***  ***“network-firewall name 1002 from any to any action deny logging off”***  6) Laptop1 sends fragments to Laptop2 in disorder  7) Check the packets captured by Laptop2 | | |
| **Expect result** | 3) Laptop2 receives all fragments, can resume the packet?(need confirm)  7) Laptop2 receives nothing, cannot resume the packet | | |

### Network firewall order test case

##### Case ID Network-Firewall\_Order\_1

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Order\_1 | | |
| **Priority** | Middle | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Order of network firewall rules influence | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 | | |
| **Test procedure** | 1) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from network 10.1.10.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1003 from network 10.1.20.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1004 from network 10.1.20.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1005 from any to any action deny logging off”***  2) Laptop1 ping Laptop2  3) Laptop2 ping Laptop1 | | |
| **Expect result** | 2) Laptop1 ping Laptop2 unsuccessfully  3) Laptop2 ping Laptop1 successfully | | |

##### Case ID Network-Firewall\_Order\_2

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Order\_2 | | |
| **Priority** | Middle | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Different mask rules’ order influence | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 | | |
| **Test procedure** | 1) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.0 action permit logging on”***  ***“network-firewall name 1002 from network 10.1.10.2 255.255.255.255 action deny logging on”***  ***“network-firewall name 1003 from any to any action deny logging off”***  2) Laptop1 ping Laptop2 | | |
| **Expect result** | 2) Laptop1 ping Laptop2 successfully, match rule 1001 | | |

### Hardening firewall test case

#### BR test case

##### Case ID Hardening Firewall\_BR\_1

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Hardening\_Firewall\_BR\_1 | | |
| **Priority** | Middle | **Automation Flag** | No |
| **Topology to use** | Topolopy8 | | |
| **Description** | Hardening Firewall Influence on the packets to BR self(Wan) | | |
| **Pre-condition** | -Configure AP1  Configure interface eth0&eth1 mode wan | | |
| **Test procedure** | 1.Laptop2 ping mgt0(ICMP)  2.Enable vpn to Gateway1(IKE) and show vpn ike  ***“show vpn ike sa”***  3.Gateway1 ping mgt0(IPsec-ESP)  4.Send any other service packets to AP1(such as telnet and ssh…) | | |
| **Expect result** | 1.Laptop2 can ping mgt0.1 successfully  2.AP can establish vpn to Gateway1 successfully  3.Gateway1 can ping mgt0.1 successfully  4.We cannot telnet or ssh to AP | | |

#### CVG test case

##### Case ID Hardening Firewall\_CVG\_1

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Hardening\_Firewall\_CVG\_1 | | |
| **Priority** | Middle | **Automation Flag** | No |
| **Topology to use** | Topolopy8 | | |
| **Description** | Hardening Firewall Influence on the packets to CVG self(wan) | | |
| **Pre-condition** | - Configure Gateway1  Configure interface eth0&eth1 mode wan | | |
| **Test procedure** | 1.Laptop2 ping Gateway1(ICMP)  2.Enable vpn to AP1(IKE) and show vpn ike  ***“show vpn ike sa”***  3.AP1 ping Gateway1(IPsec-ESP)  4.Enable OSPF both sides and show ip route on Gateway1  5.Enable RIP both sides and show ip route on Gateway1  6.Enable BGP both sides and show ip route on Gateway1  7. Send any other service packets to AP1(such as telnet and ssh…) | | |
| **Expect result** | 1.Laptop2 can ping mgt0.1 successfully  2.AP can establish vpn to Gateway1 successfully  3.Gateway1 can ping mgt0.1 successfully  4.Gateway1 can get OSPF neighbor info successfully  5.Gateway1 can get RIP neighbor info successfully  6.Gateway1 can get BGP neighbor info successfully  7.We cannot telnet or ssh to AP | | |

## Negative test case

##### Case ID Network-Firewall\_Negative\_1

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Negative\_1 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Network Firewall rules influence on Laptop to AP self | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 | | |
| **Test procedure** | 1) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  2) Laptop1 ping Mgt0.1  3) Laptop1 ping Mgt0.2 | | |
| **Expect result** | 2) Laptop1 ping Mgt0.1 successfully  3) Laptop1 ping Mgt0.2 successfully | | |

##### Case ID Network-Firewall\_Negative\_2

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Negative\_2 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Network Firewall rules influence on AP self to Laptop | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 | | |
| **Test procedure** | 1) Configure network firewall rule  ***“network-firewall name 1001 to network 10.1.10.1 255.255.0.0 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  2) AP ping Laptop1  3) AP ping Laptop2 | | |
| **Expect result** | 2) AP ping Laptop1 successfully  3) AP ping Laptop2 successfully | | |

##### Case ID Network-Firewall\_Negative\_3

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Negative\_3 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy4 | | |
| **Description** | Network Firewall rules influence on gateway to AP self | | |
| **Pre-condition** | -Configure AP1  Enable tunnel1 between AP1 and Gateway1  Enable tunnel2 between AP1 and Gateway2  Laptop2 IPaddr 192.168.10.2  Laptop3 IPaddr 192.168.30.2  Laptop4 IPaddr 192.168.20.2 | | |
| **Test procedure** | 1) Configure network firewall rule  ***“network-firewall name 1001 from vpn action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  2) Laptop2 and Laptop4 ping AP1  3) Laptop3 ping Ap1 | | |
| **Expect result** | 2) Laptop2 and Laptop4 ping AP1 successfully  3) Laptop3 ping AP1 successfully | | |

##### Case ID Network-Firewall\_Negative\_4

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Negative\_4 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy4 | | |
| **Description** | Network Firewall rules influence on AP self to gateway | | |
| **Pre-condition** | -Configure AP1  Enable tunnel1 between AP1 and Gateway1  Enable tunnel2 between AP1 and Gateway2  Laptop2 IPaddr 192.168.10.2  Laptop3 IPaddr 192.168.30.2  Laptop4 IPaddr 192.168.20.2 | | |
| **Test procedure** | 1) Configure network firewall rule  ***“network-firewall name 1001 from vpn action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  2) AP1 ping Laptop2 and Laptop4  3) AP1 ping Laptop3 | | |
| **Expect result** | 2) AP1 ping Laptop2 and Laptop4 successfully  3) AP1 ping Laptop2 and Laptop4 successfully | | |

##### Case ID Network-Firewall\_Negative\_5

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Negative\_5 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Network Firewall rules influence on layer 2 switch | | |
| **Pre-condition** | -Configure AP  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.1 IPaddr 10.1.10.3 | | |
| **Test procedure** | 1) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.1 255.255.255.0 to network 10.1.10.1 255.255.255.0 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  2) Laptop1 ping Laptop2  3) Laptop2 ping Laptop1 | | |
| **Expect result** | 2) Laptop1 ping Laptop2 successfully  3) Laptop2 ping Laptop1 successfully | | |

##### Case ID Network-Firewall\_Negative\_6

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Negative\_6 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Network Firewall rules influence on IP-policy | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 | | |
| **Test procedure** | 1) Configure L2 firewall rule,Laptop1 connect to ssid\_name\_1  ***“ip-policy FW”***  ***“ip-policy FW from 10.1.10.1 action permit”***  ***“user-profile FW security ip-policy from-access FW”***  ***“ssid <ssid\_name\_1> default-user-profile-attr [num]”***  2) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.1 255.255.255.0 to network 10.1.10.1 255.255.255.0 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  2) Laptop1 ping Laptop2 | | |
| **Expect result** | 2) Laptop1 ping Laptop2 successfully | | |

##### Case ID Network-Firewall\_Negative\_7

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Negative\_7 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Overwrite network firewall rules | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 | | |
| **Test procedure** | 1) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1003 from network 10.1.20.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  2) Overwrite 2 rules  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1003 from network 10.1.20.2 255.255.255.255 action deny logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Show network firewall  ***“show network-firewall”***  4) Laptop1 ping Laptop2  5) Laptop2 ping Laptop1 | | |
| **Expect result** | 3) We can see 4 rules on the table, not 2, because it cannot support overwrite now  2) Laptop1 ping Laptop2 unsuccessfully  3) Laptop2 ping Laptop1 successfully | | |

##### Case ID Network-Firewall\_Negative\_8

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Negative\_8 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy6 | | |
| **Description** | Hostname resolve situation when the network is abnormal | | |
| **Pre-condition** | -Configure AP  Enable 1 dhcp server（mgt0.1）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  AP get IPaddr(interface wan) <IP1> from server  The server’s hostname is <hostname1> | | |
| **Test procedure** | 1) Cut off the connection of dns and internet  2) Configure network firewall rule  ***“network-firewall name 1001 to hostname www.google.com action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  3) Show network firewall rules in shell  ***“\_shell”***  ***“iptables -nL”***  4) Resume the connection  5) Show network firewall rules in shell  ***“\_shell”***  ***“iptables -nL”*** | | |
| **Expect result** | 3) We cannot see anything  5) We can see several IP address in destination IP frame , not “www.google.com” | | |

##### Case ID Network-Firewall\_Negative\_9

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Negative\_9 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy5 | | |
| **Description** | Network firewall situation when the process ah\_l3fw is killed | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2  Laptop3 connect to Mgt0.1 IPaddr 10.1.10.3 | | |
| **Test procedure** | 1) Configure network firewall rule  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 to 10.1.20.2 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from any to any action deny logging off”***  ***“save running config”***  2) Kill process ah\_l3fw  ***“\_shell”***  ***“killall -9 ah\_l3fw”***  3) Wait for a moment  4)Show process  ***“\_shell”***  ***“ps”***  5)Show network firewall  ***“show network-firewall”***  6) Laptop1 and Laptop3 ping Laptop2 | | |
| **Expect result** | 3) We can see process ah\_l3fw  5) We can see network firewall correctly  6) Laptop1 ping Laptop2 successfully, Laptop3 ping Laptop3 unsuccessfully | | |

##### Case ID Network-Firewall\_Negative\_10

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Negative\_10 | | |
| **Priority** | High | **Automation Flag** | No |
| **Topology to use** | Topolopy9 | | |
| **Description** | Switch the path between vpn and nat | | |
| **Pre-condition** | Laptop connected to AP can ping [www.sina.com](http://www.sina.com) both by nat and tunnel | | |
| **Test procedure** | 1.Laptop ping www.sina.com continuously by default route (eth0)  2.Add route on CVG,and push to AP  ***"routing internal-sub-network 61.172.201.0/24"(sina IPaddr)***  3.~~Clear all sessions~~ Waite the CVG put the route to BR(about 90s)  4.Cut off vpn connect by delete vpn configure | | |
| **Expect result** | 1.Laptop ping www.sina.com successfully by default route;  2.Laptop ping www.sina.com successfully by vpn;  3.Laptop ping www.sina.com successfully by vpn;  4.Laptop ping www.sina.com successfully by default route; | | |

## Stress Test Case

### Firewall rules maximum test case

##### Case ID Network-Firewall\_Stress-Rules\_1

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Rules\_1 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy5 | | |
| **Description** | Network firewall work status when reach the maximum | | |
| **Pre-condition** | -Configure AP  Enable 3 dhcp server（mgt0.1 mgt0.2 mgt0.3）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Mgt0.3 vlan39 IPaddr 10.1.30.1 gateway 10.1.30.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2  Laptop3 connect to Mgt0.3 IPaddr 10.1.30.2 | | |
| **Test procedure** | 1) Use script configure 1023 network firewall rules  ***“network-firewall name 1001 from network 10.1.10.1 255.255.255.255 action permit logging on”***  ***“network-firewall name 1002 from network 10.1.10.2 255.255.255.255 action permit logging on”***  ***…***  ***“network-firewall name 2022 from network 10.1.14.6 255.255.255.255 action permit logging on”***  ***“network-firewall name 2023 action deny logging on”***  2) Laptop1 ping Laptop2  3) Laptop3 ping Laptop2  4) Delete network firewall configure  ***“no network-firewall”***  5) Use script configure 1023 network firewall rules  ***“network-firewall name 1001 from network 10.1.10.1 255.255.255.255 action deny logging on”***  ***“network-firewall name 1002 from network 10.1.10.2 255.255.255.255 action deny logging on”***  ***…***  ***“network-firewall name 2022 from network 10.1.14.7 255.255.255.255 action deny logging on”***  ***“network-firewall name 2023 action deny logging on”***  6) Laptop1 ping Laptop2  7) Laptop3 ping Laptop2 | | |
| **Expect result** | 2) Laptop1 ping Laptop2 successfully, match the rule 1002 in the logs  3) Laptop3 ping Laptop2 unsuccessfully, match the rule 2023 in the logs  6) Laptop1 ping Laptop2 unsuccessfully, match the rule 1002 in the logs  7) Laptop3 ping Laptop2 unsuccessfully, match the rule 2023 in the logs | | |

##### Case ID Network-Firewall\_Stress-Rules\_2

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Rules\_2 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy5 | | |
| **Description** | Influence on memory when firewall rules cleared by manually | | |
| **Pre-condition** | -Configure AP  Enable 3 dhcp server（mgt0.1 mgt0.2 mgt0.3）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Mgt0.3 vlan39 IPaddr 10.1.30.1 gateway 10.1.30.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2  Laptop3 connect to Mgt0.3 IPaddr 10.1.30.2 | | |
| **Test procedure** | 1) Show AP memory  ***“show memory”***  2) Use script configure 1023 network firewall rules  ***“network-firewall name 1001 from network 10.1.10.1 255.255.255.255 action permit logging on”***  ***“network-firewall name 1002 from network 10.1.10.2 255.255.255.255 action permit logging on”***  ***…***  ***“network-firewall name 2022 from network 10.1.14.6 255.255.255.255 action permit logging on”***  ***“network-firewall name 2023 action deny logging on”***  3) Delete network firewall configure  ***“no network-firewall”***  4) Show AP memory  ***“show memory”***  5) Repeat step 10 times | | |
| **Expect result** | 4) The value of step 4 should be close to step1, and repeat 10 times  5) No abnormal status, such as CPU, memory and so on | | |

##### Case ID Network-Firewall\_Stress-Rules\_3

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Rules\_3 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy5 | | |
| **Description** | Reboot AP when network firewall rules reach the maximum | | |
| **Pre-condition** | -Configure AP  Enable 3 dhcp server（mgt0.1 mgt0.2 mgt0.3）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Mgt0.3 vlan39 IPaddr 10.1.30.1 gateway 10.1.30.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2  Laptop3 connect to Mgt0.3 IPaddr 10.1.30.2 | | |
| **Test procedure** | 1) Use script configure 1023 network firewall rules  ***“network-firewall name 1001 from network 10.1.10.1 255.255.255.255 action permit logging on”***  ***“network-firewall name 1002 from network 10.1.10.2 255.255.255.255 action permit logging on”***  ***…***  ***“network-firewall name 2022 from network 10.1.14.6 255.255.255.255 action permit logging on”***  ***“network-firewall name 2023 action deny logging on”***  2) Save configure  ***“save config”***  3) Reboot AP  ***“Reboot”***  4) Check AP status | | |
| **Expect result** | 4)No abnormal status, such as CPU, memory and so on | | |

##### Case ID Network-Firewall\_Stress-Rules\_4

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Rules\_4 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy6 | | |
| **Description** | Hostname maximum resolve ip addresses in a network firewall rule should be 4?(need be confirmed by Tuming shen) | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2 mgt0.3）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2  -Configure on dns server  Set hostname [www.aerohive.com](http://www.aerohive.com) correspond 5 different IP addresses | | |
| **Test procedure** | 1) Configure network firewall rules  ***“network-firewall name 1001 from network 10.1.10.1 255.255.255.255 to hostname www.aerohive.com action permit logging on”***  2) Show network firewall  ***“show network-firewall”*** | | |
| **Expect result** | 2) We can see 4?(need be confirmed by Tuming shen) resolved IP in rule 1001 | | |

##### Case ID Network-Firewall\_Stress-Rules\_5

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Rules\_5 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy6 | | |
| **Description** | Hostname maximum resolve ip addresses in a AP should be 1024\*4?(need be confirmed by Tuming shen) | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2 mgt0.3）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 | | |
| **Test procedure** | 1) Use script configure 1024 network firewall rules  ***“network-firewall name 1001 from network 10.1.10.1 255.255.255.255 to hostname www.google.com action permit logging on”***  ***“network-firewall name 1002 from network 10.1.10.1 255.255.255.255 to hostname www.sina.com action permit logging on”***  ***…***  ***“network-firewall name 1003 from network 10.1.10.1 255.255.255.255 to hostname www.163.com action permit logging on”*** | | |
| **Expect result** | ? | | |

### Firewall logs Maximum test

##### Case ID Network-Firewall\_Stress-Logs\_1

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Logs\_1 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy5 | | |
| **Description** | Influence on system when firewall print logs all the time | | |
| **Pre-condition** | -Configure AP  Enable 3 dhcp server（mgt0.1 mgt0.2 mgt0.3）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Mgt0.3 vlan39 IPaddr 10.1.30.1 gateway 10.1.30.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2  Laptop3 connect to Mgt0.3 IPaddr 10.1.30.2 | | |
| **Test procedure** | 1) Configure network firewall rules  ***“network-firewall name 1001 from network 10.1.10.2 255.255.255.255 action permit logging on”***  ***“network-firewall name 1002 from network 10.1.20.2 255.255.255.255 action permit logging on”***  ***“network-firewall name 1003 from network 10.1.30.2 255.255.255.255 action permit logging on”***  ***“network-firewall name 2023 action deny logging on”***  2) Laptop1 ping Laptop2 all the time  3) Laptop2 ping Laptop3 all the time  4) Laptop3 ping Laptop1 all the time | | |
| **Expect result** | 2) No abnormal status, such as CPU, memory and so on  3) No abnormal status, such as CPU, memory and so on  4) No abnormal status, such as CPU, memory and so on | | |

## Duration Test Case

## Performance Test Case

## Scalability Test Case

##### Case ID Network-Firewall\_Scalability\_1

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Scalability\_1 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Maximum of network firewall rules should be 1024 | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 | | |
| **Test procedure** | 1) Use script configure 1024 network firewall rules  ***“network-firewall name 1001 from network 10.1.10.1 255.255.255.255 action permit logging off”***  ***“network-firewall name 1002 from network 10.1.10.2 255.255.255.255 action permit logging off”***  ***…***  ***“network-firewall name 2024 from network 10.1.14.8 255.255.255.255 action permit logging off”***  2) Add a network firewall rule  ***“network-firewall name 2025 from network 10.1.14.9 255.255.255.255 action permit logging off”***  3) Show network-firewall rules and look up the rules number  ***“show network-firewall”*** | | |
| **Expect result** | 2) We can see a error info network firewall rules reach the maximum, cannot add new rule  3) We can see 1024 network firewall rules | | |

##### Case ID Network-Firewall\_Scalability\_2

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_Scalability\_2 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Maximum of network firewall sessions should be 15940 ?(need be confirmed by Tuming shen ) | | |
| **Pre-condition** | -Configure AP  Enable 2 dhcp server（mgt0.1 mgt0.2）  Mgt0.1 vlan10 IPaddr 10.1.10.1 gateway 10.1.10.1  Mgt0.2 vlan20 IPaddr 10.1.20.1 gateway 10.1.20.1  Laptop1 connect to Mgt0.1 IPaddr 10.1.10.2  Laptop2 connect to Mgt0.2 IPaddr 10.1.20.2 | | |
| **Test procedure** | 1) Configure network firewall rules  ***“network-firewall name 1001 from any to any action permit”***  2) Laptop1 uses tool send 1024 different UDP packets to Laptop2  3) Look up the packets captured by Laptop2  4) Laptop1 send others UDP packets to Laptop2 | | |
| **Expect result** | 3) We can see 1024 network firewall packets  4) We cannot see any new packets | | |

## Compatibility Test Case

## CLI Management (Automation Status: No)

CLI commands

1. network-firewall name <string> from {any | vpn |{network <ip\_addr> <mask>} | {ip-range <ip\_addr> <ip\_addr>} | {user-profile <string>} | {wildcard <ip\_addr> <mask>}} to {any | vpn | {network <ip\_addr> <mask>} | {ip-range <ip\_addr> <ip\_addr>} | {hostname <string>} | {wildcard <ip\_addr> <mask>}} service <string> action {permit | deny} logging {on | off }
2. no network-firewall
3. show network-firewall

##### Case ID Network-Firewall\_CLI\_1

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_CLI\_1 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | By default, there is no network firewall | | |
| **Pre-condition** | None | | |
| **Test procedure** | 1) show default network firewall  ***“show network-firewall”***  2) show default network firewall configure  ***“show running config”*** | | |
| **Expect result** | 1) No information is displayed  2) No network firewall config is displayed | | |

##### Case ID Network-Firewall\_CLI\_2

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_CLI\_2 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Normal network firewall config | | |
| **Pre-condition** | -Configure AP  ***“network-firewall name 1001 from any to network 10.0.0.0 255.0.0.0 action deny logging on”***  ***“network-firewall name 1002 from user-profile 4 to vpn action permit logging off”*** | | |
| **Test procedure** | 1) show network firewall  ***“show network-firewall”***  2) show network firewall configure  ***“show running config”*** | | |
| **Expect result** | 1) Information can be displayed correctly  2) Network firewall config can be displayed correctly | | |

##### Case ID Network-Firewall\_CLI\_3

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_CLI\_3 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Delete network firewall config | | |
| **Pre-condition** | -Configure AP  ***“network-firewall name 1001 from any to network 10.0.0.0 255.0.0.0 action deny logging on”***  ***“network-firewall name 1002 from user-profile 4 to vpn action permit logging off”*** | | |
| **Test procedure** | 1) Delete network firewall  ***“no network-firewall”***  2) show network firewall  ***“show network-firewall”***  3) show network firewall configure  ***“show running config”*** | | |
| **Expect result** | 2) No information is displayed  3) No network firewall config is displayed | | |

##### Case ID Network-Firewall\_CLI\_4

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_CLI\_4 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Overwrite network firewall config | | |
| **Pre-condition** | -Configure AP  ***“network-firewall name 1001 from any to network 10.0.0.0 255.0.0.0 action deny logging on”***  ***“network-firewall name 1002 from user-profile 4 to vpn service any action permit logging off”*** | | |
| **Test procedure** | 1) Overwrite network firewall config  ***“network-firewall name 1001 from network 10.0.0.0 255.0.0.0 to any action deny logging on”***  2) show network firewall  ***“show network-firewall”***  3) show network firewall configure  ***“show running config”*** | | |
| **Expect result** | 2) You can see 3 network-firewall rules displayed on CLI, network-firewall cannot be overwritten even the name is the same  3) You can see 3 network-firewall config-rules displayed on CLI | | |

##### Case ID Network-Firewall\_CLI\_5

|  |  |  |  |
| --- | --- | --- | --- |
| **Case ID** | Network\_firewall\_CLI\_5 | | |
| **Priority** | Low | **Automation Flag** | No |
| **Topology to use** | Topolopy1 | | |
| **Description** | Network firewall IP range config | | |
| **Pre-condition** | None | | |
| **Test procedure** | 1) Config network firewall rule  ***“network-firewall name 1001 from ip-range 10.0.0.1 10.0.0.254 action deny logging on”***  2) Show network firewall  ***“show network-firewall”***  3) Delete network firewall  ***“no network-firewall”***  4) Config network firewall rule  ***“network-firewall name 1001 from ip-range 10.0.0.254 10.0.0.1 action deny logging on”***  5) Show network firewall  ***“show network-firewall”*** | | |
| **Expect result** | 2) Network firewall information can be displayed correctly  4) Error info should be displayed on the AP  5) No network firewall rule is displayed on the AP | | |

## GUI Management-HiveManager

**<List HM test case or test log>**

## GUI Management-HiveUI

**<List HiveUI test case or test log>**