FastNAC

SWITCH CONFIGURATIONS

CONTENTS;

1. Switch Configurations

FastNAC operates based on MAC address notification traps. Before adding switches to FastNAC, the necessary SNMP configuration must be done on the switches. In addition to configuring the SNMP trap on the switches, a user with SNMP read/write permissions must be created.

If you enable the Auto-Config feature when adding a switch, the configurations described above will be automatically performed by FastNAC. For the Auto-Config feature to work, you only need to create an SNMPv2c community or SNMPv3 user with Read/Write permissions on the switch. If the switch's SSH information is also entered, the relevant configuration will be performed automatically via SSH even if there is no SNMP configuration on the switch. Auto-configuration processes are performed via TFTP and SSH. UDP port 69 (TFTP) and TCP port 22 (SSH) must be open on the switches to connect to FastNAC.

Note: *If the Auto-Config feature is enabled when adding a switch, the following configurations are automatically performed by FastNAC.*

Note: *For the Auto-Config feature to work;*

- The switch's IP address needs to be made accessible to the FastNAC's IP address via the TFTP port (UDP Port 69).
- On the switch, an SNMP configuration with write permissions must also be entered. (If SSH is not provided)

1.1. Cisco Switches

To configure SNMP settings on Cisco switches after entering “Global Configuration Mode” (config terminal or conf t), the following configuration is required.

```
config terminal
```

1.1.1. SNMPv2c

- Creating an SNMP community with read/write permissions;

```
snmp-server community AAAA RW
```

Notes: *The SNMP Community password should be entered in the places marked* ***AAAA . This password must be the same as the one entered in " Settings*** *->* ***General Settings*** *->* ***Connection Settings*** *->* ***SNMP Settings*** *". If the SNMP community is different for each switch, a different community can be specified on the switch adding screen.*

- For SNMP traps to reach FastNAC;

```
snmp-server host AAAA version 2c BBBB
```

Notes: *The IP address of FastNAC should be entered in place of* ***AAAA . The SNMP Community password should be entered in place of BBBB*** *. The password entered here must match the password entered in “* ***Settings*** *->* ***General Settings*** *->* ***Connection Settings*** *->* ***SNMP Trap Settings ”.***

1.1.2. SNMPv3

fastnac_view is created to enable SNMP-related operations , and the necessary SNMP OIDs for FastNAC are allowed;

```
snmp-server view fastnac_view iso included
snmp-server view fastnac_view system included
snmp-server view fastnac_view interface included
```

- An SNMP group is then created that has access permissions to the view that was subsequently created;

```
snmp-server group fastnac_group v3 priv read fastnac_view write fastnac_view notify fastnac_view
```

Note: *In the example above, an SNMP group named* ***fastnac_group has been created and granted fastnac_view*** *access.*

- Cisco switches do not have access to the VLAN table via SNMPv3. Therefore, VLAN Match Prefix must be configured.

```
snmp-server group fastnac_group v3 priv context vlan- match prefix read fastnac_view notify fastnac_view
```

- On Cisco switches with older iOS versions, if the VLAN Match Prefix command is not available, a separate context must be created for each VLAN on the switch;

```
snmp-server group fastnac_group v3 priv context vlan- CCCC read fastnac_view notify fastnac_view
```

Notes: *The VLAN number is entered in place of* ***CCCC*** *. Each VLAN on the switch must be defined separately. If the VLAN Match Prefix command is working, these settings are not necessary.*

- After these steps, a user is created for SNMPv3;

```
snmp-server user fastnac fastnac_group v3 auth md5 ***** priv des *****
```

Note: *In the example above, a user named* ***fastnac has been created and added to the fastnac_group . MD5 is used*** *as the Authentication Mode and* ***DES*** *as the Privacy Mode . You must enter your SNMP passwords in the* ******** fields. The information created here must match the information entered in the " Settings*** *->* ***General Settings*** *->* ***Connection Settings*** *->* ***SNMP Settings*** *" section. If the SNMP connection information is different for each switch, different SNMP information can be specified on the switch addition screen.*

- For SNMP traps to reach FastNAC;

```
snmp-server host AAAA traps version 3 priv fastnac
```

Notes: *The IP address of FastNAC should be entered in place of* ***AAAA . In the example above, " fastnac*** *" is used as the user for the Trapler. The SNMP information for the " **fastnac** " user must also be entered in the " **Settings** -> **General Settings** -> **Connection Settings** -> **SNMP Trap Settings** " section.*

1.1.3. Other Settings

- To enable MAC address change notifications:

```
snmp-server enable traps mac-notification change move threshold
mac address-table notification changed
```

```
mac address-table notification move
mac address-table notification threshold
```

Note: *Some iOS versions may use `mac-move` instead of `move`. If the `move` commands don't work, try the above commands using `mac-move`.*

- The following configurations must be made for the ports that are desired to be included in FastNAC protection on the switch.

```
interface GigabitEthernet1/0/1
 snmp trap mac-notification change added
 snmp trap mac-notification change removed
```

Note: It is not recommended to enter *commands under the ports into the* ***uplink*** *ports (AP ports, other switch connection ports, etc.).*

1.2. Huawei Switches

To configure SNMP settings on Huawei switches after accessing "System View," the following configuration is required.

```
system-view
```

Next, the snmp-agent feature needs to be enabled;

```
snmp-agent
```

First, to enable SNMP-related operations, a view named **fastnac_view** is created and permissions are granted for the SNMP OIDs that FastNAC needs;

```
snmp-agent mib-view included fastnac_view iso
snmp-agent mib-view included fastnac_view system
snmp-agent mib-view included fastnac_view interfaces
```

1.2.1. SNMPv2c

- Creating an SNMP community with read/write permissions and granting access permissions to the necessary SNMP OIDs for FastNAC;

```
snmp-agent community write AAAA mib-view fastnac_view
```

Notes: *The SNMP Community password should be entered in the places marked* ***AAAA . This password must be the same as the one entered in " Settings -> General Settings -> Connection***

Settings *->* ***SNMP Settings*** *". If the SNMP community is different for each switch, a different community can be specified on the switch adding screen.*

- If you only want SNMPv2c to be used on the switch;

```
snmp-agent sys-info version v2c
```

1.2.2. SNMPv3

- Subsequently, an SNMP group is created that has access privileges to the fastnac_view that was created;

```
snmp-agent group v3 fastnac_group privacy read-view fastnac_view write-view
fastnac_view notify-view fastnac_view
```

Note: *In the example above, an SNMP group named* ***fastnac_group has been created and granted fastnac_view*** *access.*

- Next, a user is created to join the group established above;

```
snmp-agent usm-user v3 fastnac
snmp-agent usm-user v3 fastnac group fastnac_group
```

Note: *In the example above, an SNMP user named fastnac has been created and assigned to the fastnac_group group.*

- The authentication-mode property is then added for the user created later;

```
snmp-agent usm-user v3 fastnac authentication-mode md5
```

Note: *In the example above,* ***MD5 is set*** *as the Authentication Mode for the* ***fastnac user*** *. When you confirm the command, you will be prompted for a password. Keep this password safe. The information created here must match the information entered in the "* ***Settings*** *->* ***General Settings*** *->* ***Connection Settings*** *->* ***SNMP Settings*** *" section. If the SNMP connection information is different for each switch, different SNMP information can also be specified on the switch adding screen.*

- The privacy-mode feature is then added for the user created later;

```
snmp-agent usm-user v3 fastnac privacy-mode des56
```

Note: *In the example above,* ***DES is set*** *as the Privacy Mode for the* ***fastnac user*** *. When you confirm the command, you will be asked for a password. Keep this password safe. The information created here must match the information entered in the "* ***Settings*** *->* ***General Settings*** *->* ***Connection Settings*** *->* ***SNMP Settings*** *" section. If the SNMP connection information is different for each switch, different SNMP information can also be specified on the switch adding screen.*

- For SNMP traps to reach FastNAC;

```
snmp-agent target-host trap address udp-domain AAAA params securityname fastnac v3
privacy
```

Notes: *The IP address of FastNAC should be entered in the* ***AAAA section. In the example above, " fastnac " is used*** *as the user for the Trapler . The SNMP information for the " **fastnac** " user must also be entered in the " **Settings** -> **General Settings** -> **Connection Settings** -> **SNMP Trap Settings** " section.*

- If you only want to use SNMPv3 on the switch;

```
snmp-agent sys-info version v3
```

1.2.3. Other Settings

- To send MAC address change notifications to FastNAC;

```
snmp-agent trap enable feature-name L2IFPPI trap-name hwMacTrapAlarm
```

- The following configurations must be made for the ports that are desired to be included in FastNAC protection on the switch.

```
interface GigabitEthernet1/0/1
 mac-address trap notification all
```

Note: It is not recommended to enter commands under the ports into the **uplink** ports (AP ports, other switch connection ports, etc.).

- Source settings need to be configured on Huawei switches.

```
snmp-agent protocol source-interface Vlanif AAAA
```

Notes: *Instead of* ***AAAA,*** *the source-interface VLAN number that will handle SNMP operations should be entered. If no VLAN is to be defined, the command " **snmp-agent protocol source-status all-interface** " can be used.*

- The auto-save feature needs to be activated on the Switch;

```
set save-configuration interval 30
```

- If you want to use all SNMP versions on the switch;

```
snmp-agent sys-info version all
```

You can type the command.

1.3. Aruba Switches

To configure SNMP settings on Aruba switches after entering "Global Configuration Mode" (config terminal or conf t), the following configuration is required.

```
config terminal
```

1.3.1. SNMPv2c

- Creating an SNMP community with read/write permissions;

```
snmp-server community AAAA unrestricted
```

Notes: *The SNMP Community password should be entered in the places marked* ***AAAA . This password must be the same as the one entered in " Settings*** *->* ***General Settings*** *->* ***Connection Settings*** *->* ***SNMP Settings*** *". If the SNMP community is different for each switch, a different community can be specified on the switch adding screen.*

- For SNMP traps to reach FastNAC;

```
snmp-server host AAAA community BBBB trap-level critical
```

Notes: *The IP address of FastNAC should be entered in place of* ***AAAA . The SNMP Community password should be entered in place of BBBB*** *. The password entered here must match the password entered in "*
Settings *->* ***General Settings*** *->* ***Connection Settings*** *->* ***SNMP Trap Settings ".***

1.3.2. SNMPv3

- SNMP v3 is enabled on the switch;

```
snmpv3 enable
snmpv3 restricted-access
```

- To enable trap notifications, a notification named **FastNAC** is created and **the FastNAC_tag** tag is specified;

```
snmpv3 notify "FastNAC" tagvalue "FastNAC_tag"
```

- After these steps, a user is created for SNMPv3;

```
snmpv3 user “fastnac” auth md5 ***** priv des *****
```

Note: *In the example above, a user named* ***fastnac has been created. MD5 is used*** *as the Authentication Mode and* ***DES*** *as the Privacy Mode for encryption . You need to enter your SNMP passwords in the* ******** fields. The information created here must match the information entered in the " Settings*** *->* ***General Settings*** *->* ***Connection Settings*** *->* ***SNMP Settings*** *" section. If the SNMP connection information is different for each switch, different SNMP information can be specified on the switch adding screen.*

- The created user is granted managerauth privileges;

```
snmpv3 group managerauth user "fastnac" sec-model ver3
```

- To send SNMP traps using the fastnac user, the following configuration must be entered:

```
snmpv3 params "FastNAC_params" user "fastnac" sec-model ver3 message-processing ver3 priv
```

- For SNMP traps to reach FastNAC;

```
snmpv3 targetaddress "CT_FastNAC" params "FastNAC_params" AAAA taglist "FastNAC_tag"
```

Note: *The IP address of FastNAC should be entered in place of AAAA. In the example above, “* **FastNAC_params** *” is used for the Trap. The SNMP information for the “* ***fastnac ” user*** *in “* **FastNAC_params ” must also be entered in the** *“* ***Settings*** *->* ***General Settings*** *->* ***Connection Settings*** *->* ***SNMP Trap Settings*** *” section.*

- To enable SNMP MAC notifications, the following configurations are made in global settings:

```
snmp-server enable traps mac-notify
snmp-server enable traps mac-notify mac-move
snmp-server enable traps mac-notify trap-interval 2
```

1.3.3. Other Settings

- To enable SNMP MAC notifications, the following configurations are made in global settings:

```
interface 1
  mac-notify traps learnt
  mac-notify traps removed
  mac-notify traps aged
```

***Note: It is not recommended to enter** commands under the ports into the **uplink** ports (AP ports, other switch connection ports, etc.).*

1.4. Juniper Switches

To configure SNMP settings on Juniper switches after entering configuration mode, the following configuration is required.

```
cli
edit
```

1.4.1. SNMPv2c

- Creating an SNMP community with read/write permissions;

```
set snmp view fastnac_view oid .1
set snmp community AAAA view fastnac_view
set snmp community AAAA authorization read-write
set snmp trap-group fastnac
set groups fastnac_group snmp community AAAA authorization read-write
```

***Notes:** The SNMP Community password should be entered in the places marked **AAAA . This password must be the same as the one entered in " Settings** -> **General Settings** -> **Connection Settings** -> **SNMP Settings** ". If the SNMP community is different for each switch, a different community can be specified on the switch adding screen.*

- For SNMP traps to reach FastNAC;

```
set groups fastnac_group snmp trap-options
set groups fastnac_group snmp trap-group fastnac version v2
set groups fastnac_group snmp trap-group fastnac targets AAAA
set groups fastnac_group snmp traceoptions file fastnac
set groups fastnac_group snmp traceoptions flag all
set groups fastnac_group
set apply-groups fastnac_group
set switch-options mac-notification notification-interval
```

Notes: *The IP address of FastNAC should be entered in place of* ***"AAAA"*** *.*

1.4.2. SNMPv3

- First, to perform SNMP-related operations, a view named fastnac_view is opened, an SNMPv3 user and group are created, and permissions are granted for the necessary SNMP OIDs for FastNAC;

```
set snmp v3 usm local-engine user fastnac authentication-md5 authentication-password
*****
set snmp v3 usm local-engine user fastnac privacy-des privacy-password *****
set snmp v3 vacm security-to-group security-model usm security-name fastnac group
admin
set snmp v3 vacm access group admin default-context-prefix security-model any
security-level privacy read-view fastnac_view
set snmp v3 vacm access group admin default-context-prefix security-model any
security-level privacy write-view fastnac_view
set snmp view fastnac_view oid .1 include
```

Note: *In the example above,* ***MD5*** *is set as the Authentication Mode and* ***DES*** *is set as the Privacy Mode for* ***the fastnac user.*** *You need to enter the SNMP passwords in the* ******** fields. The information created here must match the information entered in the " Settings*** *->* ***General Settings*** *->* ***Connection Settings*** *->* ***SNMP Settings*** *" section. If the SNMP connection information is different for each switch, different SNMP information can also be specified on the switch adding screen.*

- For SNMP traps to reach FastNAC;

```
set snmp v3 target-address FastNAC address AAAA
set snmp v3 target-address FastNAC target-parameters FastNAC_Params
set snmp v3 target-parameters FastNAC_Params parameters message-processing-model
v3
set snmp v3 target-parameters FastNAC_Params parameters security-model usm
set snmp v3 target-parameters FastNAC_Params parameters security-level privacy
set snmp v3 target-parameters FastNAC_Params parameters security-name fastnac
```

Notes: *The IP address of FastNAC should be entered in place of* ***AAAA . In the example above, the user used is " fastnac "****. The SNMP information for the "* ***fastnac " user must also be entered in the " Settings*** *->* ***General Settings*** *->* ***Connection Settings*** *->* ***SNMP Trap Settings*** *" section.*

1.4.3. Other Settings

- To enable MAC address change notifications:

```
set switch-options mac-notification notification-interval 1
```

- The following configurations must be made for the ports that are desired to be included in FastNAC protection on the switch;

```
set interfaces ge-0/0/1 traps
set interfaces ge-0/0/1 enable
```

Note: It is not recommended to enter *commands under the ports into the* ***uplink*** *ports (AP ports, other switch connection ports, etc.).*

- If trap sending is enabled under Uplinks, you can disable trap sending with the following command;

```
set interfaces ge-0/0/0 no-trap
```