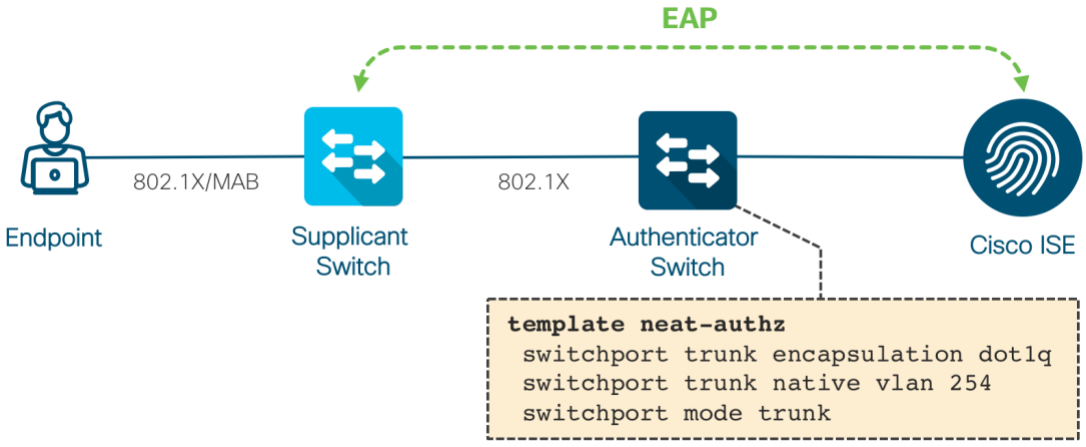
NEAT with Interface Templates

Overview

Network Edge Authentication Topology offers secure extension of the Layer 2 network beyond the wiring closet. It ensures that a supplicant switch (compact switch outside the wiring closet) is allowed access to the network only if it authenticates successfully. For more information on the NEAT click here. This document covers the NEAT configurations with IOS Interface-templates. This method may be considered as a "neater" way of doing NEAT.

Topology



Why interface-template for NEAT?

To understand the need for using the IOS Interface-templates for NEAT, it is important to know how the NEAT system functions. The principle of NEAT is that a supplicant switch connecting to the Authenticator switch (ASw) must first authenticate prior to any access being given to the devices connecting to it. The switchport configuration on the NEAT authenticator switch will have the generic "access-mode" configuration along with the 802.1X related commands. When the Supplicant Switch (SSw) successfully authenticates, the RADIUS Server sends down Cisco AV Pair **"device-traffic-class=switch"** along with ACCESS-ACCEPT to the Authenticator switch. The authenticator switch then changes the port configuration from access to "trunk-mode" with the help of a built-in macro.

ASw port configuration connecting to SSw (with Macro based NEAT)

Before SSw authentication	After SSw authentication
interface GigabitEthernet0/12 description ** To SSw 0/12 ** **switchport access vlan 254** **switchport mode access** authentication port-control auto dot1x pae authenticator !	interface GigabitEthernet0/12 description ** To SSw 0/12 ** **switchport trunk native vlan 254** **switchport mode trunk** authentication port-control auto dot1x pae authenticator !

Hariprasad Holla, Technical Marketing Engineer, Cisco

The current macro based NEAT has two limitations:

1. **The macros modify the interface configuration in the running-config.** When an SSw is authenticated, if a script or someone saves the running-config on the ASw, then on a power cycle the default port configuration would be lost.
2. **If the admin prefers to make modifications to the default macro, it can't be done.** For this purpose, an ASP macro must be configured on the ASw and ISE must be configured to authorize the supplicant with the "ASP macro name" along with the custom Cisco AVP for NEAT.

The solution to this problem is to use the interface-templates instead of macros for port configuration related changes.

Interface templates

Interface template is a port configuration container that can be applied to a specific interface or a user's network access session. Almost all the interface specific commands can be configured under the **"template"** and then either manually applied on the port (with **"source template"** interface command) or can be applied dynamically on the port, based on either device discovery (AutoConf, similar to AutoSmartPorts) or via RADIUS authorization. One of the major advantages of interface templates is that the running-configuration will have a fixed configuration, where the interface specific (active) configuration will be placed under a separate runtime memory. The configuration that is currently applied on a physical interface can be seen with the **"show derived-config interface <interface>"** exec command. Interface templates are supported from Cisco IOS 15.2(2)E / XE 03.06.00E.

Configuring NEAT with Interface templates

The following configurations are necessary for NEAT to function:

Authenticator Switch:

(1) AAA configuration for RADIUS transactions
(2) Global 802.1X configurations
(3) 802.1X authentication configuration on the port
(4) Enable NEAT globally
(5) Configure the interface-template to be authorized for NEAT supplicant switch

Supplicant Switch:

(1) AAA configuration for RADIUS transactions
(2) Global 802.1X configurations (for client authentication)
(3) 802.1Q Trunk configuration on the uplink port connecting the Authenticator switch
(4) 802.1X authentication configuration on the client side ports
(5) Enable NEAT globally

Note *In this configuration example EAP-MD5 is used as the EAP method between the supplicant switch and ISE. However NEAT supplicants support many other EAP methods. **"show eap registrations"** EXEC command tells the EAP support on the supplicant switch*

Supplicant Switch	Authenticator Switch
aaa new-model aaa authentication login default group radius aaa authentication login console none aaa authentication dot1x default group radius aaa authorization network default group radius aaa session-id common ! dot1x system-auth-control ! ip radius source-interface Vlan254 !	aaa new-model aaa authentication login default group radius aaa authentication login console none aaa authentication dot1x default group radius aaa authorization network default group radius aaa session-id common ! dot1x system-auth-control ! ip radius source-interface Vlan254 !

```
radius server ise01
 address ipv4 172.20.254.4 auth-port 1645 acct-
port 1646
 key xxxxxx
```

```
radius server ise01
 address ipv4 172.20.254.4 auth-port 1645 acct-
port 1646
 key xxxxxx
```

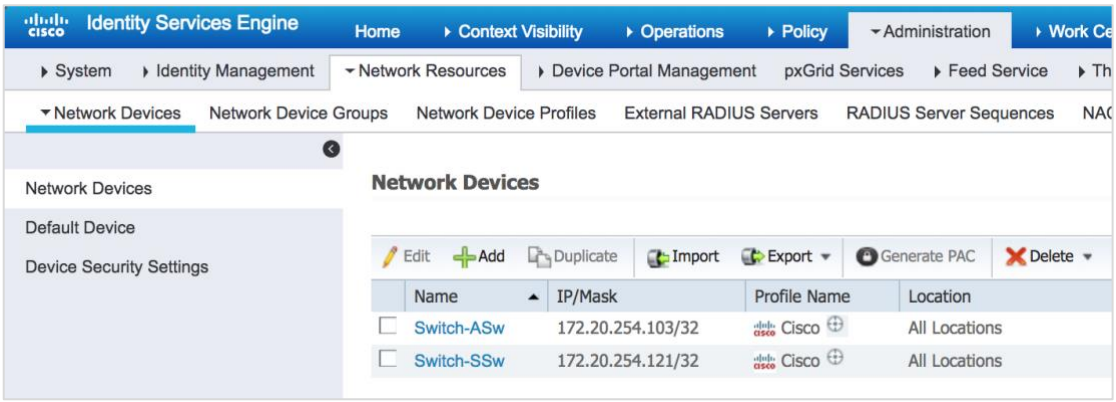
```
cisp enable
!
eap profile eap-md5
 description PEAP-MD5 Supplicant
 method md5
!
dot1x credentials eap-md5-cred
 username ssw01
 password 0 cisco123
 anonymous-id ssw01
!
interface GigabitEthernet0/12
 description ** To ASw Gi0/12 **
 switchport trunk native vlan 254
 switchport mode trunk
 dot1x pae supplicant
 dot1x credentials eap-md5-cred
 dot1x supplicant eap profile eap-md5
 ip dhcp snooping trust
```

```
cisp enable
!
template neat-authz
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 254
 switchport mode trunk
!
interface GigabitEthernet0/12
 description ** To SSw 0/12 **
 switchport access vlan 254
 switchport mode access
 authentication host-mode multi-host
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast
!
```

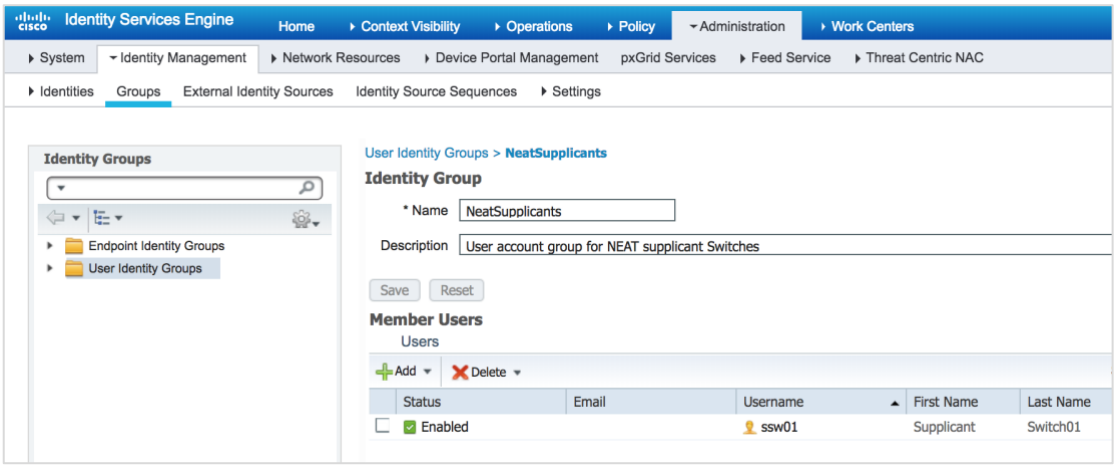
ISE configuration for NEAT with Interface-template

ISE needs to be configured with the user identity and policies to authenticate and authorize the NEAT supplicant. Follow these steps:

ASw and SSw Definition:

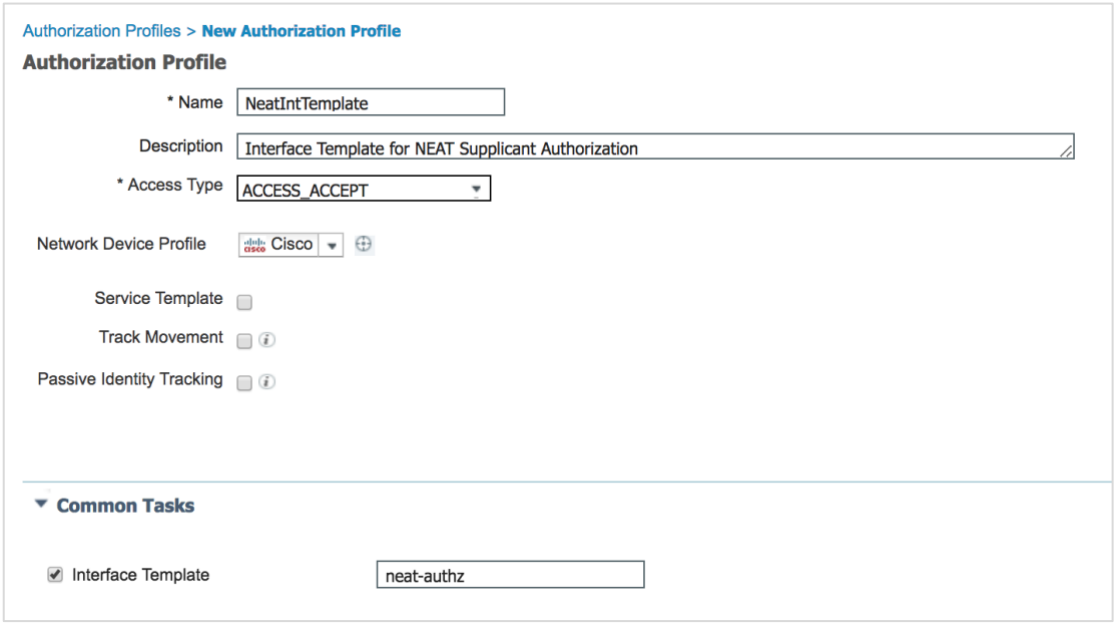


NEAT Switch User account:

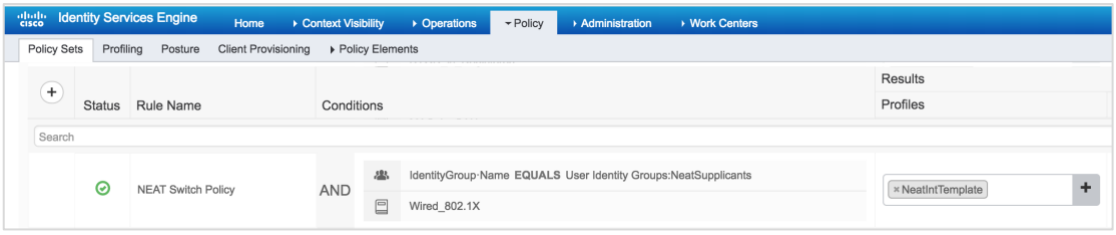


NEAT Switch Authorization Profile

Note *On ISE, one major difference between traditional NEAT and "NEAT with Interface-template" configuration, is that the authorization profile for the former is Cisco AVP "device-traffic-class=switch", whereas for the later it is "interface-template-name=<name>"*



Authorization Policy:
[Policy → Policy Sets → [Policy Set] → Authorization Policy]



Validating NEAT with Interface-template

```
ASw#show cisp summary

CISP is running on the following interface(s):
---------------------------------------------
  Gi0/12 (authenticator)


ASw#show dot1x interface gigabitEthernet 0/12 details

Dot1x Info for GigabitEthernet0/12
----------------------------------
PAE                       = AUTHENTICATOR
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30

Dot1x Authenticator Client List
```

```
------------------------------
EAP Method               = MD5
Supplicant               = 5c50.1562.368c
Session ID               = AC14FE67000000BD3DCC54AC
    Auth SM State        = AUTHENTICATED
    Auth BEND SM State   = IDLE

ASw#show authentication sessions interface gigabitEthernet 0/12 details
           Interface:  GigabitEthernet0/12
         MAC Address:  5c50.1562.368c
        IPv6 Address:  Unknown
        IPv4 Address:  Unknown
           User-Name:  ssw01
         Device-type:  Cisco-Switch
              Status:  Authorized
              Domain:  DATA
      Oper host mode:  multi-host
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  AC14FE67000000BD3DCC54AC
      Acct Session ID:  Unknown
              Handle:  0x140000B2
       Current Policy:  POLICY_Gi0/12

Local Policies:
        Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
      Security Policy:  Should Secure
      Security Status:  Link Unsecure

Server Policies:
   Interface Template:  neat-authz

Method status list:
       Method           State
       dot1x            Authc Success

ASw#show running-config interface gigabitEthernet 0/12
Building configuration...

Current configuration : 240 bytes
!
interface GigabitEthernet0/12
 description ** To SSw 0/12 **
 switchport access vlan 254
 switchport mode access
 authentication host-mode multi-host
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast
end

ASw#show derived-config interface gigabitEthernet 0/12
Building configuration...

Derived configuration : 240 bytes
!
interface GigabitEthernet0/12
 description ** To SSw 0/12 **
 switchport access vlan 254
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 254
 switchport mode trunk
 dot1x pae authenticator
 spanning-tree portfast
end


SSw#show cisp summary

CISP is running on the following interface(s):
---------------------------------------------
  Gi0/1 (authenticator)
  Gi0/12 (supplicant)

SSw#show dot1x interface gigabitEthernet 0/12 details

Dot1x Info for GigabitEthernet0/12
```

```
---------------------------------
PAE                       = SUPPLICANT
StartPeriod               = 30
AuthPeriod                = 30
HeldPeriod                = 60
MaxStart                  = 3
Credentials profile       = eap-md5-cred
EAP profile               = eap-md5
Dot1x Supplicant Client List
-------------------------------
Authenticator             = f0f7.55db.7d8c
        Supp SM State       = AUTHENTICATED
        Supp Bend SM State  = IDLE
Port Status               = AUTHORIZED
```

ASw Interface configurations

Before SSw Authentication	After SSw Authentication
ASw#show run interface Gi 0/12 Building configuration... Current configuration : 250 bytes ! interface GigabitEthernet0/12 description ** To SSw 0/12 ** **switchport access vlan 254** **switchport mode access** authentication host-mode multi-host authentication port-control auto dot1x pae authenticator spanning-tree portfast ! **ASw#show derived-config int Gi0/12** Building configuration... Derived configuration : 179 bytes ! interface GigabitEthernet0/12 description ** To SSw 0/12 ** **switchport access vlan 254** **switchport mode access** dot1x pae authenticator spanning-tree portfast !	**ASw#show run interface Gi 0/12** Building configuration... Current configuration : 250 bytes ! interface GigabitEthernet0/12 description ** To SSw 0/12 ** **switchport access vlan 254** **switchport mode access** authentication host-mode multi-host authentication port-control auto dot1x pae authenticator spanning-tree portfast ! **ASw#show derived-config int Gi0/12** Building configuration... Derived configuration : 240 bytes ! interface GigabitEthernet0/12 description ** To SSw 0/12 ** switchport access vlan 254 **switchport trunk encapsulation dot1q** **switchport trunk native vlan 254** **switchport mode trunk** dot1x pae authenticator spanning-tree portfast !

Client Information Signaling Protocol (CISP)

Upon connecting an endpoint to the supplicant switch, authentications and authorizations takes place with ISE. The Client Information Signaling Protocol (CISP) on the supplicant switch signals the endpoint-supplicant's MAC address to the authenticator switch for forwarding. The authenticator switch installs the clients MAC address in its forwarding table and grants access to the upstream network.

```
SSw#show cisp clients

Authenticator Client Table is empty

Supplicant Client Table:
------------------------
  MAC Address     VLAN    Interface
  --------------------------------
  000c.293c.8dca   200    Gi0/1

<output truncated>
SSw#show authentication sessions interface gigabitEthernet 0/1 details
            Interface:  GigabitEthernet0/1
          MAC Address:  000c.293c.8dca
```

```
         IPv6 Address:  Unknown
         IPv4 Address:  172.20.200.2
            User-Name:  harips
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  single-host
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  050F142C0000002704A2188E
      Acct Session ID:  Unknown
               Handle:  0xA000001B
       Current Policy:  POLICY_Gi0/1

Local Policies:
        Template: DEFAULT LINKSEC POLICY SHOULD SECURE (priority 150)

Server Policies:
           Vlan Group:  Vlan: 200

Method status list:
       Method           State
       dot1x            Authc Success
```

```
ASw#show cisp clients

Authenticator Client Table:
---------------------------
  MAC Address     VLAN    Interface
  ---------------------------------
  5c50.1562.36c1   254    Gi0/12
  000c.293c.8dca   200    Gi0/12
```

Note *These configurations can be done in the policy-mode as well. The ports can have static default interface-templates applied on them with "source template" interface command and the template for supplicant switch authorization can be activated after an authentication success.*

ISE Live Logs
[Operations → RADIUS → Live Logs]

Identity	Endpoint ID	Endpoint Profile	IP Address	Authorization Profiles	Network Device
Identity	Endpoint ID	Endpoint Profile	IP Address	Authorization Profiles	Network Device
ssw01	5C:50:15:62:36:8C	Cisco-Device	172.20.254.121	NeatIntTemplate	Switch-ASw

"Macro NEAT" and "NEAT with Interface-template" comparison

Particulars	NEAT with Macros	NEAT with Interface Template
Supplicant EAP Methods	All methods (MD5, PEAP, EAP-TLS)	All methods (MD5, PEAP, EAP-TLS)
CISP for MAC notification	Yes	Yes
Cisco AVP	device-traffic-class=switch	interface-template-name=<name>
Supplicant switch authorization modifies running-config on ASw	Yes	No
Modifying post-authc interface configuration	With additional ASP Macro	Modify the original authorization template referenced by ISE