Configuring Endpoint Admission Control

Revised: May 28, 2010

This chapter contains the following sections:

Information About Endpoint Admission Control

In TrustSec networks, packets are filtered at the egress, not the ingress to the network. In TrustSec endpoint authentication, a host accessing the TrustSec domain (endpoint IP address) is associated with a Security Group Tag (SGT) at the access device through DHCP snooping and IP device tracking. The access device transmits that association (binding) through SXP-to-TrustSec hardware-capable egress devices, which maintain a continually updated table of Source IP to SGT bindings. Packets are filtered on egress by the TrustSec hardware-capable devices by applying security group ACLS (SGACLs).

Endpoint Admission Control (EAC) access methods for authentication and authorization can include the following:

- 802.1X port-based Authentication
- MAC Authentication Bypass (MAB)
- Web Authentication (WebAuth)

All port-based authentication can be enabled with the **authentication** command. Each access method must be configured individually per port. The flexible authentication sequence and failover features permit the administrator to specify the failover and fallback sequence when multiple authentication modes are configured and the active method fails. The 802.1X host mode determines how many endpoint hosts can be attached per 802.1X port.

Basic EAC Configuration Sequence

1. Configure the Cisco Secure ACS to provision SGTs to authenticated endpoint hosts.
2. Enable SXP on access switches. See the chapter, "Configuring SGT Exchange Protocol."
3. Enable any combination of 802.1X, MAB, or WebAuth authentication methods on the access switch.
4. Enable DHCP and IP device tracking on access switches.

802.1X Authentication Configuration

The following example shows the basic 802.1x configuration on a Gigabit Ethernet port:

```
Switch(config)# dot1x system-auth-control
Switch(config)# interface GigabitEthernet2/1
Switch(config-if)# authentication port-control auto
Switch(config-if)# dot1x pae authenticator
```

Verifying the 802.1X Configuration

To verify 802.1X authentication configuration, use the **show authentication interface** command.

```
Switch# show authentication interface gigabitEthernet 2/1
*May  7 11:22:06: %SYS-5-CONFIG_I: Configured from console by console

Client list:
  Interface  MAC Address     Domain   Status         Session ID
  Gi2/1      000c.293a.048e  DATA     Authz Success  AC1AD01F0000000904BBECD8

Available methods list:
  Handle  Priority  Name
    3        0      dot1x
Runnable methods list:
  Handle  Priority  Name
    3        1      dot1x
```

And to verify the port has successfully authenticated:

```
Switch# show dot1x interface gigabitEthernet 2/1 details

Dot1x Info for GigabitEthernet2/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = SINGLE_HOST
QuietPeriod               = 60
ServerTimeout             = 30
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 2
TxPeriod                  = 30

Dot1x Authenticator Client List
-------------------------------
Supplicant                = 000c.293a.048e
Session ID                = AC1AD01F0000000904BBECD8
    Auth SM State         = AUTHENTICATED
```

```
    Auth BEND SM State    = IDLE
Port Status               = AUTHORIZED
```

MAC Authentication Bypass Configuration

MAC Authentication Bypass (MAB) enables hosts or clients that are not 802.1X capable to join 802.1X-enabled networks. It is not required to enable 802.1X authentication prior to enabling MAB.

The following example is a basic MAB configuration on a Catalyst switch:

```
switch(config)# interface GigabitEthernet2/1
switch(config-if)# authentication port-control auto
switch(config-if)# mab
```

For additional information on configuring MAB authentication, see the configuration guide for your access switch.

Verifying the MAB Configuration

To verify the MAC Authentication Bypass configuration, use the **show authentication interface** command.

```
switch# show authentication interface gigabitEthernet 2/1

Client list:
  Interface  MAC Address     Domain   Status         Session ID
  Gi2/1      000c.293a.048e  DATA     Authz Success  AC1AD01F0000000A04CD41AC

Available methods list:
  Handle  Priority  Name
    2        1      mab
Runnable methods list:
  Handle  Priority  Name
    2        0      mab
```

To verify that the port has successfully authenticated, use the **show mab interface** command.

```
switch# show mab interface gigabitEthernet 2/1 details
MAB details for GigabitEthernet2/1
-------------------------------------
Mac-Auth-Bypass           = Enabled

MAB Client List
---------------
Client MAC                = 000c.293a.048e
Session ID                = AC1AD01F0000000A04CD41AC
MAB SM state              = ACQUIRING
Auth Status               = UNAUTHORIZED
```

Web Authentication Proxy Configuration

Web Authentication Proxy (WebAuth) allows the user to use a web browser to transmit their login credentials to the Cisco Secure ACS though a Cisco IOS web server on the access device. WebAuth can be enabled independently. It does not require 802.1X or MAB to be configured.

The following example shows a basic WebAuth configuration on a Gigabit Ethernet port:

```
switch(config)# ip http server
switch(config)# ip access-list extended POLICY
switch(config-ext-nacl)# permit udp any any eq bootps
switch(config-ext-nacl)# permit udp any any eq domain
switch(config)# ip admission name HTTP proxy http
switch(config)# fallback profile FALLBACK_PROFILE
switch(config-fallback-profile)# ip access-group POLICY in
switch(config-fallback-profile)# ip admission HTTP
switch(config)# interface GigabitEthernet2/1
switch(config-if)# authentication port-control auto
switch(config-if)# authentication fallback FALLBACK_PROFILE6500(config-if)#ip access-group
POLICY in
```

Verifying Web Authentication Proxy Configuration

To verify the Web Authentication Proxy configuration, access the interface IP address with a web browser. If configured correctly, the access device generates a challenge and accepts valid login information.

To verify the Web Authentication proxy configuration with the CLI, use the **show authentication interface** command.

```
switch# show authentication interface gigabitEthernet 2/1

Client list:
  Interface  MAC Address     Domain   Status         Session ID
  Gi2/1      000c.293a.048e  DATA     Authz Success  AC1AD01F0000000904BBECD8

Available methods list:
  Handle  Priority  Name
    1        2      webauth
Runnable methods list:
  Handle  Priority  Name
    1        0      webauth
```

Flexible Authentication Sequence and Failover Configuration

Flexible Authentication Sequence (FAS) allows the access port to be configured for 802.1X, MAB, and WebAuth authentication methods, specifying the fallback sequence if one or more of the authentication methods are not available. The default failover sequence is as follows:

- 802.1X port-based Authentication
- MAC Authentication Bypass
- Web Authentication

Layer 2 authentications always occur before Layer 3 authentications. That is, 802.1X and MAB must occur before WebAuth.

The following example specifies the authentication sequence as MAB, dot1X, and then WebAuth.

```
switch(config)# interface gigabitEthernet 2/1
switch(config-if)# authentication order mab dot1x webauth
switch(config-if)^Z
```

For additional information on FAS, see the Cisco document, *Flexible Authentication Order, Priority, and Failed Authentication* at the following URL:

http://www.ciscosystems.com.pe/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6638/application_note_c27-573287_ps6638_Products_White_Paper.html

802.1X Host Modes

Four host classification modes can be configured per port:

- Single Host —Interface-based session with one MAC address
- Multi Host—Interface-based session with multiple MAC addresses per port
- Multi Domain—MAC + Domain (VLAN) session
- Multi Auth—MAC-based session with multiple MAC address per port

Pre-Authentication Open Access

The Pre-Authentication Open Access feature allows clients and devices to gain network access before port authentication is performed. This process is primarily required for the PXE boot scenario, where a device needs to access the network before PXE times out and download a bootable image that may contain a supplicant.

DHCP Snooping and SGT Assignment

After the authentication process, authorization of the device occurs (for example, dynamic VLAN assignment, ACL programming, etc.). For TrustSec networks, a Security Group Tag (SGT) is assigned per the user configuration in the Cisco ACS. The SGT is bound to traffic sent from that endpoint through DHCP snooping and the IP device tracking infrastructure.

The following example enables DHCP snooping and IP device tracking on an access switch:

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ip dhcp snooping
switch(config)# ip dhcp snooping vlan 10
switch(config)# no ip dhcp snooping information option
switch(config)# ip device tracking
```

Verifying the SGT to Endpoint Host Binding

To verify that hosts are visible to DHCP Snooping and IP Device Tracking, use the **show ip dhcp snooping binding** and **show ip device tracking** commands.

```
switch# show ip dhcp snooping binding

MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:0C:29:3A:04:8E   10.252.10.10     84814       dhcp-snooping   10    GigabitEthernet2/1
Total number of bindings: 1


switch# show ip device tracking all

IP Device Tracking = Enabled
IP Device Tracking Probe Count = 3
IP Device Tracking Probe Interval = 30
-----------------------------------------------------------
  IP Address     MAC Address       Interface          STATE
-----------------------------------------------------------
10.252.10.10    000c.293a.048e GigabitEthernet2/1     ACTIVE
```

To verify that the correct SGT is bound to an endpoint IP address, use the **show cts role-based sgt-map** command.

```
switch# show cts role-based sgt-map all

Active IP-SGT Bindings Information
IP Address   SGT Source
============================================
1.1.1.1       7 INTERNAL
10.252.10.1   7 INTERNAL
10.252.10.10  3 LOCAL
10.252.100.1  7 INTERNAL
172.26.208.31 7 INTERNAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 1
Total number of INTERNAL bindings = 4
Total number of active   bindings = 5
```

Cisco TrustSec Endpoint Access Control Feature Histories

For a list of supported platforms, supported features, and the minimum required IOS releases, see the *Cisco TrustSec Platform Support Matrix* at the following URL:

http://www.cisco.com/en/US/solutions/ns170/ns896/ns1051/trustsec_matrix.html

Otherwise, see product release notes for detailed feature introduction information.