Cisco TrustSec How-To Guide: Closed Mode

For Comments, please email: howtoguides@external.cisco.com

Current Document Version: 3.0

August 27, 2012

Table of Contents

Introduction

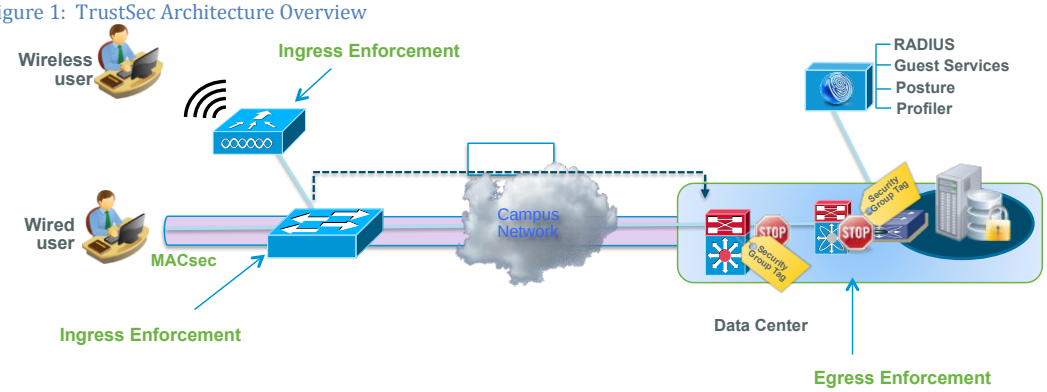
What Is the Cisco TrustSec System?

Cisco TrustSec®, a core component of the Cisco SecureX Architecture™, is an intelligent access control solution. TrustSec mitigates security risks by providing comprehensive visibility into who and what is connecting across the entire network infrastructure, and exceptional control over what and where they can go.

TrustSec builds on your existing identity-aware access layer infrastructure (switches, wireless controllers, and so on). The solution and all the components within the solution are thoroughly vetted and rigorously tested as an integrated system.

In addition to combining standards-based identity and enforcement models, such as IEEE 802.1X and VLAN control, the TrustSec system it also includes advanced identity and enforcement capabilities such as flexible authentication, Downloadable Access Control Lists (dACLs), Security Group Tagging (SGT), device profiling, posture assessments, and more.

Figure 1: TrustSec Architecture Overview

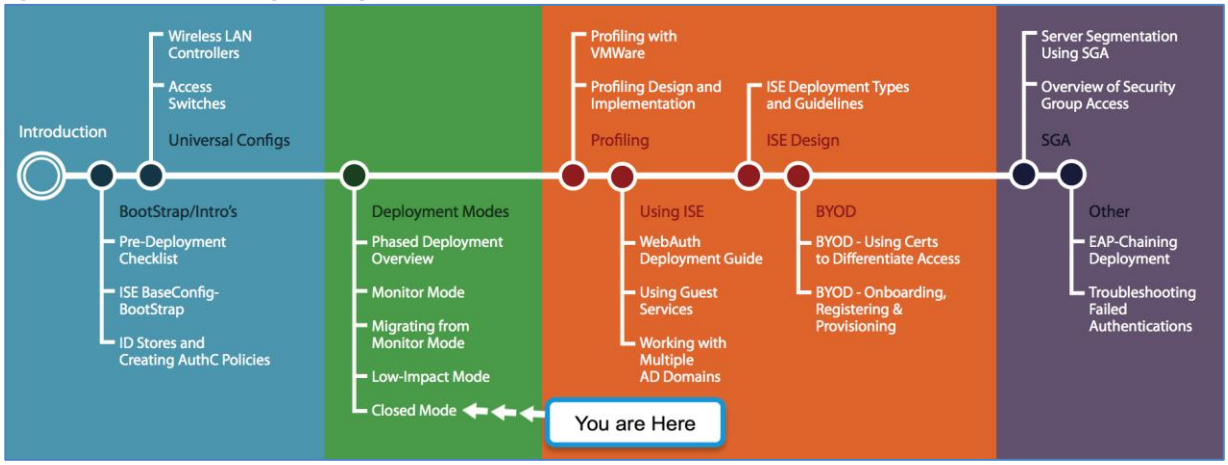


About the TrustSec How-To Guides

The TrustSec team is producing this series of How-To documents to describe best practices for TrustSec deployments. The documents in the series build on one another and guide the reader through a successful implementation of the TrustSec system. You can use these documents to follow the prescribed path to deploy the entire system, or simply pick the single use-case that meets your specific need.

Each guide is this series comes with a subway-style "You Are Here" map to help you identify the stage the document addresses and pinpoint where you are in the TrustSec deployment process (Figure 2).

Figure 2: How-To Guide Navigation Map



What does it mean to be 'TrustSec Certified'?

Each TrustSec version number (for example, TrustSec Version 2.0, Version 2.1, and so on) is a certified design or architecture. All the technology making up the architecture has undergone thorough architectural design development and lab testing. For a How-To Guide to be marked "TrustSec certified," all the elements discussed in the document must meet the following criteria:

- Products incorporated in the design must be generally available.
- Deployment, operation, and management of components within the system must exhibit repeatable processes.
- All configurations and products used in the design must have been fully tested as an integrated solution.

Many features may exist that could benefit your deployment, but if they were not part of the tested solution, they will not be marked as "TrustSec "certified". The TrustSec team strives to provide regular updates to these documents that will include new features as they become available, and are integrated into the TrustSec test plans, pilot deployments, and system revisions. (i.e., TrustSec 2.2 certification).

Additionally, many features and scenarios have been tested, but are not considered a best practice, and therefore are not included in these documents. As an example, certain IEEE 802.1X timers and local web authentication features are not included.

Note: Within this document, we describe the recommended method of deployment, and a few different options depending on the level of security needed in your environment. These methods are examples and step-by-step instructions for TrustSec deployment as prescribed by Cisco best practices to help ensure a successful project deployment.

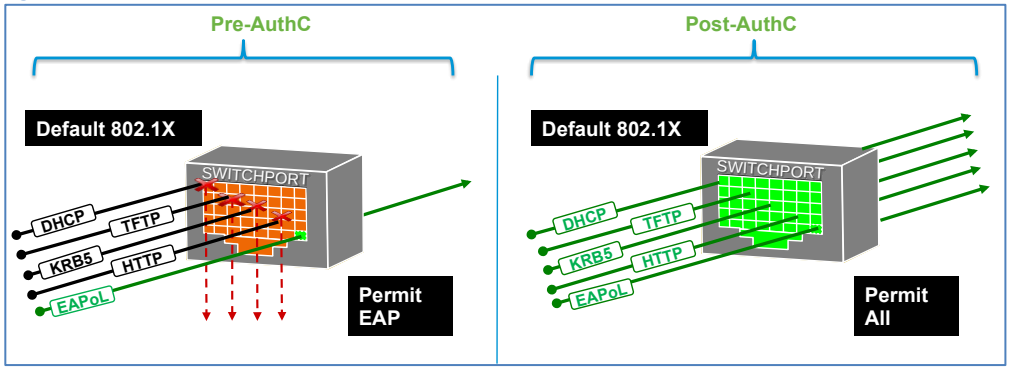
Closed Mode

Overview of Closed Mode

Closed Mode is a more traditional deployment model of 802.1X. In a properly prepared network, Closed Mode provides total control over switch-level (Layer 2) network access. This type of deployment is recommended only for environments that are experienced with 802.1X deployments and have considered all the nuances that go along with it. Think of this mode as a "deploy with caution" mode.

Cisco recommends deploying TrustSec and 802.1X in a staged approach. The stages begin with Monitor Mode as the initial stage, and the end state will be either Low-Impact Mode or Closed Mode. This document focuses on Closed-Mode deployments (Figure 3).

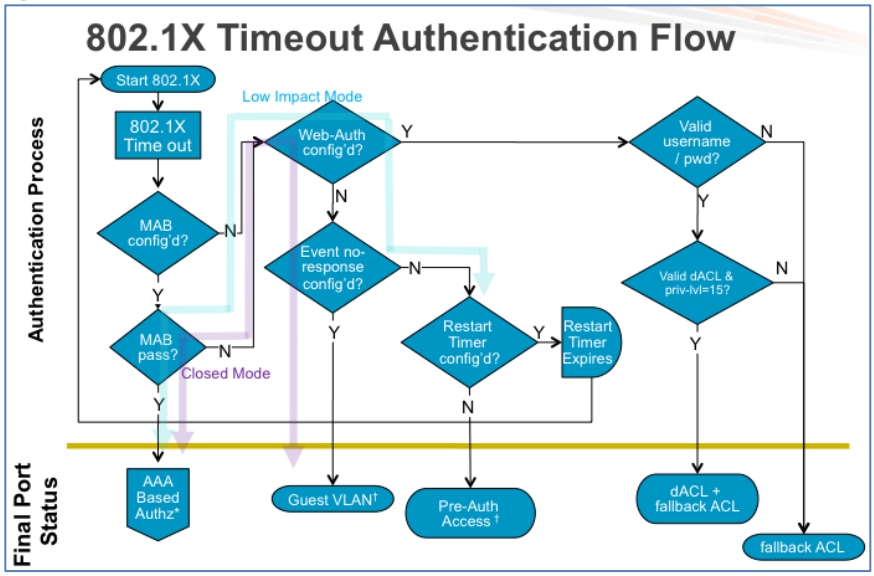
Figure 3 Closed Mode Default 802.1X Port Behavior



In Closed Mode, the switchport does not allow any traffic except EAP over LAN (EAPoL) until a successful authentication takes place. There is no concept of pre-authentication access, which means that no access is allowed—such as Dynamic Host Configuration Protocol (DHCP), HTTP, and Domain Name System (DNS)—while authentication is in progress. Closed Mode can be useful for VLAN-based enforcement since the client does not get an IP address until they have been successfully authenticated.

For users and devices that successfully complete 802.1X authentication, this is not typically an issue, since that authentication usually happens quickly. For devices that cannot perform 802.1X, there may be a significant delay in network access. Because the switch is configured to attempt the most secure authentication method first, non-802.1X-capable devices must wait until the authentication timer runs out and the switchport falls back to MAC Authentication Bypass (MAB) and/or Web Authentication as a secondary authentication method. As suggested in HowTo-Universal_Switch_Configuration guide, one practice is to change the 802.1X tx-timer from 30 seconds to 10 seconds, which will speed up the total time before a non-802.1X-capable device accesses the network from 90 seconds to 30 seconds. One common reason to change this timer is to allow a device to receive an IP address before its DHCP timer expires. Figure 4 illustrates the 802.1X timeout authentication flow.

Figure 4 Timeout Authentication Flow



To add more granular access control, Closed Mode uses dynamic VLAN assignment to isolate different classes of users into different broadcast domains. By isolating traffic from different classes of users into separate VLANs, Closed Mode provides the foundation for virtualized network services. Devices that can't authenticate or fail to authenticate retain the same level of access that they had before authentication: in other words, no access to the network because denying access is not as desirable as providing limited access or guest access. The deployment recommendation is to configure secondary authentication mechanisms such as Centralized Web Authentication (CWA) with the Cisco Identity Services Engine (ISE).

Note: By default, wireless follows this same Closed Mode logic, but instead of permitting all traffic after authentication, it is recommended to add the authentication and enforcement mode logic of using a wireless access control list (wACL) or dynamic VLAN (dVLAN) with the wireless connection.

Use Cases of Closed Mode

Closed Mode deployment with wired and wireless networks provides users with a full network access after a successful authentication and assigns the VLAN to the authenticated user. For wireless, a failed authentication results in no network access (as that is inherently how wireless works), but a failed authentication in wired connection results in the next-method of authentication being used. So non-802.1X authentications in a wired environment try MAB and WebAuth (CWA) for interactive users. Below, please find a few more use-cases for Closed Mode.

- No access before authentication
- Rapid access for non-802.1X capable corporate assets
- Logical isolation of traffic at the access edge

Deployment Considerations

Deploying Closed Mode with VLAN assignment can have a significant impact on network architecture. Understanding these potential impacts is essential to a successful deployment of this mode. Therefore, the deployment of Closed Mode requires strategic planning and a variety of considerations. The following procedures outline several practices to help you plan before deployment.

VLAN Considerations

Dynamic VLAN assignment requires that every dynamic VLAN be supported on every access switch to which a user might connect and authenticate. This requirement has several repercussions. For instance, suppose you have three user groups to which you wish to assign unique VLANs: Engineering, Finance, and HR. In this case, every access switch must have those three VLANs defined by name (the number of the VLAN does not have to be the same). The User Distribution feature allows you to map multiple VLANs to a VLAN group name. This can be useful in large-campus LANs because it allows the switch to load balance users in the same group across different VLANs, thus reducing the size of the broadcast domain for any single VLAN. The User Distribution feature was originally developed for this use case, hence the name.

If the switch attempts to apply a nonexistent VLAN to a port, the authorization will fail and users will not be able to gain access (even if they presented valid credentials and passed authentication).

Using the Minimum Number of VLANs Necessary

Supporting multiple VLANs per access switch is nontrivial from an IP addressing perspective. Good campus design principles dictate a single subnet per VLAN with no VLAN spanning more than one switch. Your IP addressing scheme should support multiple subnets per switch in such a way that that does not overburden the control and data planes of the campus distribution block.

In reality, the fewer VLANs you assign, the more manageable and scalable your solution will be. Indeed, some customers have found that, upon analysis, their security policy requirements could be met with very few VLANs (for example, Employee, Guest/Fail, and Voice).

MAB Configuration Consideration

If you choose to change the order of authentication to perform MAB before 802.1X**,** be aware that this will mean that every device (even those capable of 802.1X) will be subject to MAB. This could significantly increase the amount of control-plane traffic in your network.

Granting Limited Access Based on the Type of Authentication Method That Failed

If some level of access is needed for devices that fail 802.1X authentication (for example, to allow employees with expired certificates to download a new certificate), it is possible to configure the solution to grant limited access based on the type of authentication method that failed. If 802.1X fails, the switch can be configured to open the port into a special VLAN (the Auth-Fail VLAN) for this purpose.

Handling Devices That Cannot Perform 802.1X and FAIL MAB

There may be devices on your network that cannot perform 802.1X and cannot pass MAB (for example, contractors without a properly configured supplicant that need to have some form of network access). For unknown MAC addresses that fail MAB, the default policy will be WebAuth (CWA). If the device is profiled and matched any defined authorization policies, the policy will apply; else, the device will be limited to WebAuth mode.

Implementing Closed Mode

Procedure 1 Ensure All Identity Store Databases Are Up to Date and Online

Before transitioning to Closed Mode, you should ensure that all endpoints can authenticate. All identity store databases should be up to date and online.

Note: From Low-Impact Mode to Closed Mode, users can choose either dACL or dVLAN to enforce the authorization policies. The key to Closed Mode is to understand how Closed Mode works and to choose a deployment method that meets the requirements. Therefore, no specific ISE configuration will be provided in this section. However, the required switch configuration is provided.

Procedure 2 Configuring the Switch

Closed Mode represents the default 802.1X behavior. With this mode, a switchport will not permit any traffic other than EAP over LAN (EAPoL) prior to an authorization result from the authentication, authorization, and accounting (AAA) server. This is often the desired end state for a deployment because it provides very strong security. Like Low-Impact Mode, Closed Mode is also capable of using all the enforcement mechanisms available in a TrustSec deployment (including dVLAN, downloadable ACL [dACL], Security Group Access (SGA), and so on), but Closed Mode may have some impact on the operational models of an IT deployment.

Step 1 Verify that all VLANs that can be assigned are defined by name on the access switch and that each VLAN has the expected connectivity. Use the User Distribution feature to map existing VLAN names if necessary.

Step 2 Verify that the switch has been configured to accept authorization instructions from Cisco ISE.

Step 3 Remove any ingress port ACLs from the switch, as follows:

```
C3750X(config-if-range)# no ip access-group ACL-DEFAULT in
```

Note: This deployment scenario does not require ACLs.

Step 4 Disable the Open Authentication feature on all ports.

```
C3750X(config-if-range)# no authentication open
```

Note: If desired, configure the authentication order to perform MAB before 802.1X and modify the authentication priority so that 802.1X can pre-empt a successful MAB authentication.

Step 5 Unless you have a specific need to support multiple data devices on a single port, configure all access ports for single host-mode (for non-IP-Telephony deployments) or multi-domain host-mode (for IP Telephony deployments).

Appendix A: References

Cisco TrustSec System:

- http://www.cisco.com/go/trustsec
- http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

Device Configuration Guides:

Cisco Identity Services Engine User Guides:
http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

For more information about Cisco IOS Software, Cisco IOS XE Software, and Cisco NX-OS Software releases, please refer to following URLs:

- For Cisco Catalyst 2900 series switches:
  http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 3000 series switches:
  http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 3000-X series switches:
  http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 4500 series switches:
  http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html
- For Cisco Catalyst 6500 series switches:
  http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html
- For Cisco ASR 1000 series routers:
  http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html

For Cisco Wireless LAN Controllers: http://www.cisco.com/en/US/docs/wireless/controller/7.2/configuration/guide/cg.html