Secure Access Client-Based ZTA Posture Configuration and Behavior Specifications

Contents

Issue

Questions arose regarding the specific behavior and configuration capabilities of Cisco Secure Access client-based Zero Trust Access (ZTA) posture functionality when used for internet access. The specific concerns included:

- Whether Operating System posture requirements support a configurable grace period of up to 365 days during which devices can still use the ZTA module to access internet destinations even if they do not meet the required OS version.
- Whether posture requirements other than Operating System, such as Firewall, System Password, among others, result in immediate blocking of destination access when not met.
- Whether custom warning messages or actions other than blocking (such as monitoring) can be configured for posture requirement failures through the Secure Access GUI interface.

Environment

- Cisco Secure Access with Zero Trust Access (ZTNA) functionality
- Client-based ZTA posture implementation
- Internet access use case scenario
- Posture requirements including Operating System, Firewall, and System Password conditions

Resolution

The clarifications described in the next sections were provided regarding Secure Access client-based ZTA posture behavior and configuration capabilities.

Operating System Posture Grace Period

The Operating System posture requirement behavior described is correct. When an Operating System posture condition is configured, it supports a configurable grace period of up to 365 days. During this grace period, devices that do not meet the required OS version can still use the ZTA module to access internet destinations while they upgrade to the target version.

Non-Operating System Posture Requirements

For posture conditions other than Operating System (such as Firewall, System Password, and other security controls), access to destinations is immediately blocked when these requirements are not met. These posture types do not support the grace period functionality that is available for Operating System requirements.

Posture Failure Actions and Custom Messages

Actions for posture requirement failures are controlled through the Access Policy configuration.

The Access Policy supports multiple action types including:

- Allow
- Block
- Warn
- Isolate

Custom warning messages and notification pages for posture failures can be configured through the Access Policy Security profile settings. The warning and notification page management is handled via the **Manage Notification Pages** documentation and configuration interface.

This means that actions other than blocking (such as monitoring through the Warn action) are available and can be configured, contrary to the initial assessment that only blocking actions were possible.

Cause

The questions arose from the need to understand the specific behavioral differences between Operating System posture requirements and other posture types, as well as clarification on the available configuration options for posture failure handling that cannot be immediately apparent in the Secure Access GUI interface.

Related Content

- Manage Notification Pages documentation for Secure Access
- Cisco Technical Support & Downloads