Configure SSE Do Not Decrypt for IPS and SWG Decryption Bypass

Contents

Issue

HTTPS traffic to finance-category destinations continues to present a Cisco SSE certificate instead of the origin website certificate, even after adding the Finance category or specific domains to a Do Not Decrypt (DND) list and applying the relevant access rule. This behavior is observed when accessing sites over Zero Trust Access Client (TIA), specifically impacting access to finance-related websites such as https://onlinesbi.sbi.bank.in/ where end-to-end certificate visibility is required.

The expected behavior is that when a site or content category is added to the DND list, the origin website certificate can be presented to the browser instead of the Cisco SSE certificate. However, the Cisco SSE certificate continues to be presented, indicating that traffic decryption is still occurring despite the DND configuration.

Environment

- Cisco Secure Service Edge (SSE)
- Zero Trust Access Client (TIA) connectivity
- Global IPS decryption enabled
- IPS active on access policies
- Finance category configured in Do Not Decrypt list within security profile
- Access rules applied with corresponding security profiles

Resolution

The resolution involves understanding that Cisco SSE performs two distinct types of decryption and configuring the appropriate Do Not Decrypt settings for both decryption types.

Understanding SSE Decryption Types

Cisco SSE performs two separate decryption processes:

- **SWG (Secure Web Gateway) decryption** - Web proxy decryption
- **IPS decryption** - Intrusion Prevention System decryption

Do Not Decrypt entries configured inside a security profile apply only to SWG decryption and do not prevent IPS decryption. When global IPS decryption is enabled and IPS is active on any access policy, IPS decryption still occurs, resulting in the Cisco SSE certificate being presented to the browser.

Configuration Steps

Step 1: Add **sites** or **content categories** to the System Provided Do Not Decrypt List.

The System Provided Do Not Decrypt List is applied across all IPS profiles. Adding a site or content category to this System Provided list results in the origin website certificate being presented, effectively bypassing IPS decryption.

Step 2: Verify that no additional policy changes are required.

There is no need to reference the System Provided Do Not Decrypt List inside access policies. The list is automatically applied to all IPS profiles.

Validation Testing

These validation methods can be used to confirm proper configuration:

Method 1: Add Domain to System Provided Do Not Decrypt List

Adding the specific domain to the System Provided Do Not Decrypt List can result in the origin website certificate being presented instead of the Cisco SSE certificate.

Method 2: Temporarily Disable Global IPS Decryption (for testing only)

Temporarily disabling global IPS decryption also causes the origin certificate to be seen for the tested site, confirming that IPS decryption was the cause of the Cisco SSE certificate presentation.

Expected Results

After proper configuration:

- Sites or content categories added to the System Provided Do Not Decrypt List present their origin website certificates.
- Both SWG and IPS decryption are bypassed for the specified sites or categories.
- The browser displays the actual website certificate instead of the Cisco SSE certificate.

Cause

The issue occurs because Cisco SSE performs two distinct decryption processes: SWG decryption and IPS decryption. Do Not Decrypt entries configured within security profiles only bypass SWG decryption. When global IPS decryption is enabled and IPS is active on access policies, IPS decryption continues to occur independently, causing the Cisco SSE certificate to be presented to the browser even when sites are included in security profile DND lists.

To fully bypass both types of decryption, sites or content categories must be added to the System Provided Do Not Decrypt List, which applies to all IPS profiles and prevents both SWG and IPS decryption from occurring.

Related Content

- Create Effective Do Not Decrypt List for Secure Access
- Troubleshoot and Collect Basic Information for Secure Access
- Cisco Technical Support & Downloads