Verifying IPS Decryption in Cisco Secure Access

Contents

Issue

When using Cisco Secure Access with RAVPN (Remote Access VPN) through Secure Client, organizations need to verify whether IPS (Intrusion Prevention System) decryption and inspection are being correctly performed for traffic to specific websites. The primary challenge is confirming that TLS decryption and inspection processes are functioning properly through methods other than the standard management UI logs such as Activity Search. Specific verification requirements include identifying client-side certificate checks or debug/reporting mechanisms that can support test validation and provide additional confirmation of IPS operation beyond the management interface.

Environment

- Cisco Secure Access (CSA) with RAVPN functionality
- Cisco Secure Client for remote access VPN connections
- IPS decryption and inspection capabilities enabled
- TLS/SSL traffic requiring decryption for security inspection
- Web traffic from RAVPN clients to external websites

Resolution

There are two methods to verify that IPS decryption and inspection are functioning correctly for Remote Access VPN traffic in Cisco Secure Access:

Method 1: Management UI Activity Search (Primary Method)

The Activity Search feature in the Cisco Secure Access management interface provides the most reliable method to confirm IPS decryption and inspection operations. This interface displays detailed logs and analytics showing when traffic has been decrypted and inspected by the security services.

To access Activity Search:

Navigate to the Cisco Secure Access management dashboard and locate the Activity Search functionality to review traffic inspection logs and decryption status for specific user sessions and destination websites.

To Enable Decryption Logs, this setting can be enabled on global settings:

Dashboard -> Secure -> Access Policy -> Rule Defaults and Global Settings -> Global Settings -> Decryption Logging.

Method 2: Client-Side Certificate Verification

As an additional verification method, you can perform client-side certificate checks to confirm that traffic decryption is occurring.

When Cisco Secure Access successfully decrypts and inspects TLS traffic, it presents its own certificate to the client instead of the original website certificate.

To verify decryption through certificate inspection:

1. Check the Website Certificate
Open the certificate details in the browser and review the issuer and validity period.

If the certificate is issued by Cisco Secure Access Root CA with a validity period of ~10 days, it indicates Intrusion Prevention System decryption at the firewall level.

If the certificate validity is approximately 5 days, it indicates Secure Web Gateway-based decryption.

2. Validate the Certificate Issuer (DC Naming)

This client-side certificate verification method serves as a supplementary confirmation technique alongside the primary Activity Search method, providing additional assurance that IPS decryption processes are functioning as expected.

Intrusion Prevention System Do Not Decrypt:

Decryption for Intrusion Prevention System is going to take place if -

• It is enabled under global settings AND

• Intrusion Prevention System is enabled for at least one of the Access policy rules (i believe even though the rule is disabled, this condition still applies)

Want to bypass a domain from Intrusion Prevention System decryption

Use system provided do not decrypt list and add domain in the system provided do not decrypt list.

or

Utilize source based decryption under Global Settings on Cisco Secure access -

NOTE:This will work if there is NO Outbound NAT configured on the Network tunnel configuration on Secure Access.

Cause

The need for multiple verification methods arises from the requirement to validate security policy enforcement in enterprise environments. While management UI logs provide comprehensive visibility, client-side verification methods offer additional confirmation points that can be useful for compliance testing, troubleshooting, and validation scenarios where direct access to management interfaces may be limited or when multiple verification points are required for thorough testing procedures.

Related Content

- Cisco Technical Support & Downloads