Secure Access Application Protocol Blocking Prevents Internet Connectivity

Contents

- Issue
- Environment
- Resolution
  - Step 1: Identify the Blocking Rule
  - Step 2: Modify Application Settings
  - Step 3: Apply and Verify Changes
- Cause
- Related Content

Issue

After migrating to Cisco Secure Access, users experienced blocked internet connectivity when attempting to access web services. The specific symptom involved HTTP traffic being blocked by the security policy, preventing access to legitimate websites and applications.

The blocking event details showed these characteristics:

- Action: Blocked
- Event Block Reason: AC_RULE_MATCH_BLOCK
- Destination: http://www.bing.com/api/shopping/v1/user/shoppingsettings
- Destination Port: 443
- Categories: Uncategorized
- Application Category: Search

- Application Protocol: Hypertext Transfer Protocol
- Protocol: TCP

Environment

- Cisco Secure Access deployment
- Active security policy with application protocol restrictions

Resolution

The resolution involves modifying the security rule configuration to allow HTTP application protocol traffic while maintaining security posture for truly untrusted applications.

Step 1: Identify the Blocking Rule

Locate the specific rule causing the block in the Secure Access management interface:

- **Rule Name**: Test
- **Current Configuration**: Using Application Settings Block as a Destination.

Step 2: Modify Application Settings

Access the rule configuration and check the name of the Application Settings in Destination:

- Navigate to **Resources > Internet and SaaS resources > Application Lists**. Then, click on the application.
- Locate the **Application Protocol** settings.
- Uncheck or remove **HTTP** from the blocked application protocols list.
- Ensure other security controls remain in place for actual untrusted applications.

Step 3: Apply and Verify Changes

Save the rule modifications and test connectivity:

1.- Apply the configuration changes to the active policy.

2.- Test internet connectivity to previously blocked destinations.

3.- Monitor security logs to ensure legitimate HTTP traffic is now allowed.

4.- Verify that other security protections remain effective.

Cause

The root cause was an overly restrictive security rule configuration in Cisco Secure Access. The rule was configured to block all HTTP application protocol traffic, which prevented legitimate web browsing and application access. The broad application of HTTP protocol blocking affected normal internet connectivity for users accessing legitimate web services and applications that utilize HTTP/HTTPS protocols.

Related Content

- Cisco Technical Support & Downloads