Cisco Integrated Services Routers Generation 2 with Cisco Cloud Web Security Solution

The Cisco Integrated Services Routers Generation 2 (ISR G2) with Cloud Web Security solution enables branch offices to intelligently redirect web traffic to the cloud to enforce granular security and acceptable use policies over user web traffic. With this solution, you can deploy a market-leading web security quickly and easily to protect branch office users from web-based threats such as viruses, while saving bandwidth, money, and resources.

This module explains how to configure Cloud Web Security on ISR G2.

- Information About Cisco Integrated Services Routers Generation 2 and Cisco Cloud Web Security Solution, page 1
- Configuring Cloud Web Security on Integrated Services Routers Generation 2 , page 6
- Sample Configuration of Cloud Web Security on ISR G2s, page 28
- Cloud Web Security Troubleshooting Tips, page 29
- Additional References for Cisco Cloud Web Security and Integrated Services Routers Solution, page 32

Information About Cisco Integrated Services Routers Generation 2 and Cisco Cloud Web Security Solution

Overview of Cisco ISR G2 and Cloud Web Security Solution

The Cisco Integrated Services Router Generation 2 (ISR G2) family delivers numerous security services, including firewall, intrusion prevention, and VPN. These security capabilities are extended with Cisco Cloud Web Security for a web security and web filtering solution that does not require any additional hardware or client software.

The Cisco ISR G2 with Cloud Web Security solution can enable branch offices to intelligently redirect web traffic to the cloud to enforce granular security and acceptable use policies over user web traffic. With this

solution, you can deploy web security quickly and easily to protect branch office users from web-based threats such as viruses, and save bandwidth and resources.

Cisco ISR G2 integration with Cloud Web Security provides the following features:

- Enforces granular security and acceptable use policies for branch office users without using on-premise hardware or without backhauling all branch office traffic to the headquarters.
- Provides a zero-day threat protection that is driven by Cisco Outbreak Intelligence, which uses dynamic reputation- and behavior-based analysis of web pages to stop malware from entering a network.

After configuring the ISR G2 router with Cloud Web Security, use the Cloud Web Security portal to create, edit, and manage Cloud Web Security accounts and policies.

Benefits of Using the Cisco ISR G2 with Cloud Web Security

The following benefits apply to the Cisco Integrated Service Routers Generation 2 (ISR G2) and Cisco Cloud Web Security solution:

- Lower total cost of ownership: Helps customers avoid costs associated with deployment and maintenance of on-premise software and hardware.
- Leading security: Real-time cloud-based scanning blocks malware and inappropriate content before it enters the network.
- Scalability and availability: The global network processes high volumes of web content at high speeds.
- Integration with other Cisco security products: Cisco ISR G2 with Cloud Web Security integrates Cisco AnyConnect to offer a web security solution for users both on and off the network.
- Consistent, unified policy: Acceptable use policy (AUP) that can be applied to all users regardless of their location, simplifying management.

For more information on configuring and using the Cloud Web Security Portal, see the Cisco CWS Portal Administrator Guide.

Cloud Web Security Licensing

The Cloud Web Security feature on the Cisco Integrated Services Routers Generation 2 (ISR G2) is available with the Security SECK9 license bundle. For more information on configuring the Security SECK9 license bundle, refer to the Cisco ISR G2 Licensing and Packaging white paper.

Cloud Web Security Supported Platforms

The following table lists the Cisco Integrated Services Routers Generation 2 (ISR G2) platforms compatible with Cloud Web Security:

Table 1: Supported Platforms

Product	Supported Platforms
Cisco 800 Series Integrated Service Routers	Cisco 819, 860VAE, 880VA, 881, 881W, 887V, 888E, 888EA, 888, 888W, 891, 891W, 892, 892F, 892FW, 892W
Cisco 1900 Series Integrated Service Routers	Cisco 1905, 1921, 1941, 1941W
Cisco 2900 Series Integrated Service Routers	Cisco 2901, 2911, 2921, 2951
Cisco 3900 Series Integrated Service Routers	Cisco 3925, 3925E, 3945, 3945E

The *Cisco ISR G2 and Cloud Web Security Design Guide* provides details of supported architectures and best practices.

How Cloud Web Security Works with an ISR G2

When Cisco Cloud Web Security is enabled on a Cisco Integrated Services Routers Generation 2 (ISR G2) and the router is configured to redirect web traffic to the Cloud Web Security server, the ISR G2 router transparently redirects HTTP and secure HTTP (HTTPS) traffic to the Cloud Web Security proxy servers based on the destination IP address and port number. The Cloud Web Security proxy servers scan the content and either allow or block the traffic based on the configured policies, to enforce an acceptable use and protect clients from malwares.

The ISR G2 router authenticates and identifies users who make web traffic requests using the configured authentication and authorization methods. The router encrypts user information and includes the information (user name and user groups) in the traffic that it redirects to the Cloud Web Security server. Cloud Web Security uses user credentials to determine the web policies to apply to users and for user-based reporting.

You can configure the ISR G2 router to direct web traffic directly to the originally requested web server and avoid the scanning of web traffic by Cloud Web Security. For more information, see the section “Bypassing Cisco Cloud Web Security Scanning”.

You can configure a primary and a backup Cloud Web Security proxy servers. The ISR G2 router polls each server regularly to check for their availability.

Communication Between Cloud Web Security, ISR G2, and Clients

Clients are any devices that can connect to a Cisco Integrated Services Routers Generation 2 (ISR G2), either directly or indirectly. When a client sends an HTTP or secure HTTP (HTTPS) request, the ISR G2 router receives the request and forwards it to the Cloud Web Security proxy server. If authentication is configured, the ISR G2 router first authenticates the user, and then retrieves the group name from the authentication server. The router maintains the IP address-to-user-name mapping for future reference. After identifying the user (if applicable), the ISR G2 router determines whether to send the HTTP or HTTPS client request to the Cloud Web Security server by checking the Cisco IOS Firewall Port to Application Mapping (PAM) and whitelist database.

For information about PAM, see the “Configuring Port to Application Mapping" chapter in the *Context-Based Access Control Firewall* configuration Guide.

When the ISR G2 router sends a client request to Cloud Web Security servers, the router acts as an intermediary between the client and Cloud Web Security by creating a separate connection with the Cloud Web Security proxy server. When the ISR G2 router communicates with Cloud Web Security, it changes the destination IP address and destination port in the client request. It also adds Cloud Web Security-specific HTTP headers, which includes information about the username and user group, and then sends the modified request to Cloud Web Security.

You can configure how the ISR G2 router handles web traffic when it cannot reach either the primary or backup Cloud Web Security proxy server. It can either block or allow all web traffic. By default, it blocks web traffic.

When Cloud Web Security receives an HTTP or HTTPS request from an ISR G2 router, it uses the information in the request and user credentials in the Cloud Web Security HTTP headers to apply the appropriate policies to the user. After applying the configured policies, Cloud Web Security allows, blocks, or presents a warning message before allowing the client request:

- Allow—When Cloud Web Security allows a client request, it contacts the originally requested server and retrieves data. Cloud Web Security forwards the server response to the ISR G2 router, which then forwards the response to the client. The ISR G2 changes the source and destination IP addresses and ports in the response.
- Block—When Cloud Web Security blocks a client request, it sends an HTTP 302 “Moved Temporarily” response that redirects the client application to a web page hosted by Cloud Web Security. This page notifies the user that access has been blocked. The ISR G2 router forwards the 302 response to the client changing the source and destination IP addresses and port numbers.

  Note Administrators can customize the block page by using the Cloud Web Security portal.

- Warn—Sometimes, web sites that do not fully comply with a company's policies are not completely blocked. In these cases, Cloud Web Security first presents a page hosted by Cloud Web Security with a warning message and an “accept” button. Users who click the accept button, is allowed access to these sites.

Note ISR G2 routers do not have the ability to detect apps on mobile devices, even if the apps are web-based. As a result, traffic from apps launched on mobile devices and tablets may not be blocked/warned by the configured Cloud Web Security policies. However, if the content is accessed through a web browser, the content is blocked/warned according to specified policies. For example, Facebook access is blocked by the configured Cloud Web Security policies of a company. Employees of this company will not be able to access Facebook through Safari on an Apple iPad; however, they may be able to access Facebook through the Facebook app that is installed on the Apple iPad.

Cisco Cloud Web Security Headers

A device that forwards web traffic to Cisco Cloud Web Security proxy servers includes additional HTTP headers in each HTTP and HTTPS request. Cisco Cloud Web Security uses these headers to obtain information about customer deployments, including information about the user who had originally made the client request and the device that sent the request. For security purposes, the information in the headers is encrypted and then hexadecimal encoded.

Cisco Cloud Web Security headers provide both asymmetric cryptography and symmetric cryptography by using industry standard algorithms. Asymmetric encryption is done by using the RSA/ECB/PKCS1Padding algorithm that uses key pairs of 512 bits. Symmetric encryption is done by using the triple "DESede" algorithm with a randomly generated triple Data Encryption Standard (DES) key of 168 bits.

The ISR adds the following CWS HTTP headers:

- X-ScanSafe—This contains a session key that is encrypted using a CWS public key (embedded in the ISR operating system).
- X-ScanSafe-Data—This contains the data CWS needs. It is encrypted with the session key from the X-CWS header.

For example, the headers in a message might look like the following text:

- X-ScanSafe: 35A9C7655CF259C175259A9B980A8DFBF5AC934720BE9374D344F7E584780ECDB9236FF90DF562A79DC4C754C3782E7C3D38C76566F0377D5689E25BD62FC5F
- X-ScanSafe-Data: 8D57AEE5D76432ACAB184AA807D94A7392986FA0D3ED9BEB

Bypassing Cloud Web Security Scanning

You can configure Cisco Integrated Services Routers Generation 2 (ISR G2) to bypass Cloud Web Security scanning of approved web traffic. When Cloud Web Security scanning is bypassed, the ISR G2 router retrieves the content directly from the originally requested web server without contacting Cloud Web Security. When the router receives a response from the web server, it sends the data directly to the client.

You can bypass Cloud Web Security scanning based on the following client web traffic properties:

- IP address—Bypass the scanning of traffic that matches a numbered or named access control list (ACL) that is configured in the global parameter map on the ISR G2 router. Configure Cloud Web Security traffic for trusted sites, such as intranet servers.
- HTTP header fields—Bypass the scanning of web traffic that matches an HTTP header field that is configured in a global parameter map on the ISR G2 router. You can configure a match based on Host or User-Agent header fields for user agents that do not function properly when scanned. Or, you can bypass scanning traffic that is intended for trusted hosts, such as third- party partners.
  Note: When HTTP header-based whitelisting is enabled, the ISR G2 router automatically disables/removes TCP options such as windows scaling and timestamps.
- Username or User group—Bypass the scanning for web traffic that matches a username or the user group a user belongs to. You can bypass scanning for a subset of trusted users.

Use the commands**content-scan whitelisting** and **whitelist** to create a whitelist database for traffic that can bypass scanning.

Working with Multiple ISRs

A typical branch office uses one Cisco Integrated Services Routers Generation 2 (ISR G2) to route network traffic to the headquarter and redirect web traffic to Cloud Web Security for security scanning. Some organizations can have multiple branch offices with one ISR G2 router in each office.

These ISR G2 routers may force users to authenticate before granting access to the network. The ISR G2 authentication sends user-group information about the user who makes the web request from an authentication server. When the ISR G2 router do not enforce authentication, no user group information is sent from the authentication server. Use the command **user-group** to configure a default user-group name for all web traffic, while configuring Cloud Web Security on the ISR G2 router. All ISR G2 routers must be configured with a license (authentication key) in the Cloud Web Security portal. The Cloud Web Security portal supports company and group authentication keys.

If your network has multiple ISR G2 routers, you can choose the type of Cloud Web Security authentication key the you need to create and use when you configure each ISR G2 router. Configure the authentication key based on whether the ISR G2 router enforces authentication or not.

- No authentication on the ISR G2 router—Cloud Web Security applies the same web policies to all traffic originating from a single ISR G2 router. To apply different web policies for traffic from different ISR G2 routers, generate a group key in the Cloud Web Security portal for each ISR G2 router. Configure a different group key as the license in each ISR G2 router configuration. To apply the same web policies for traffic from all ISR G2 routers, generate a company key in the Cloud Web Security portal and configure it as the license in each ISR G2 router configuration. A company key is a key used by an organization.
- Authentication on the ISR G2 router—When an ISR G2 router enforces authentication, it sends user-group information from an authentication server in the redirected web traffic. Cloud Web Traffic enables you to apply different web policies for different user groups. Generate a company key in the Cloud Web Security portal and configure the key as the license in each ISR G2 router configuration. You can apply either the same Cloud Web Security policy or different policies to different user groups.

Configuring Cloud Web Security on Integrated Services Routers Generation 2

In Cisco IOS Release 15.4(2)T release, some Cloud Web Security commands were replaced. The releases prior to Cisco IOS Release 15.4(2)T still use the old commands.

This section consists of tasks that use the commands existing prior to Cisco IOS Release 15.4(2)T and a corresponding task that uses the commands introduced or modified in the Cisco IOS Release 15.4(2)T.

To use Cisco Cloud Web Security with Cisco Integrated Services Routers Generation 2 (ISR G2), you must configure the following products:

- Cisco ISR G2 router that uses Cisco IOS Release 15.3(3)M or later releases.

Note The recommend image is Cisco IOS Release15.3(3)M or later releases, however, Cloud Web Security works on Cisco IOS Releases 15.2(1)T1 and later releases.

- Cisco Cloud Web Security Portal.
- Before you enable Cloud Web Security on an ISR G2 router, create a company or group key in the Cloud Web Security portal.

To configure Cloud Web Security on an ISR G2 router, perform the following tasks:

- Configuring Cisco Cloud Web Security Features

- Enabling Cisco Cloud Web Security on the ISR G2
- Configuring Whitelisting
- Configuring a Default-User Group
- Configuring Authentication with Cloud Web Security
- Configuring NTLM or HTTP Basic Authentication
- Transparent Authentication with NTLM
- Domain and Non-Domain Users
- Configuring the Cisco Cloud Web Security Portal

Configuring Cloud Web Security in Cisco IOS Release 15.4(2)T and Later Releases

Note This task applies to Cisco IOS Release 15.4(2)T and later releases.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type cws global**
4. **server primary ipv4** *ip-address* **port http** *port-number* **https** *port-number*
5. **server secondary ipv4** *ip-address* **port http** *port-number* **https** *port-number*
6. **license 7** *license-key*
7. **source interface** *type number*
8. **timeout server** *seconds*
9. **timeout session-inactivity** *seconds*
10. **user-group** *group-name* **username** *username*
11. **server on-failure block-all**
12. **user-group exclude** *username*
13. **exit**
14. **interface** *type number*
15. **cws out**
16. **ip virtual-reassembly in**
17. **ip virtual-reassembly out**
18. **end**
19. **show cws**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**parameter-map type cws global** **Example:** `Device(config)# parameter-map type cws global`	Configures a global Cloud Web Security parameter map and enters parameter-map type inspect configuration mode.
Step 4	**server primary ipv4** *ip-address* **port http** *port-number* **https** *port-number* **Example:** `Device(config-profile)# server primary ipv4 10.12.34.23 port http 8080 https 8080`	Configures a Cisco Cloud Web Security primary server for content scanning. • The default Cisco Cloud Web Security port for the proxied HTTP and HTTPS traffic is 8080. • You can use either the HTTP port or the HTTPS port or both.
Step 5	**server secondary ipv4** *ip-address* **port http** *port-number* **https** *port-number* **Example:** `Device(config-profile)# server secondary ipv4 10.21.34.21 port http 8080 https 8080`	Configures a Cisco Cloud Web Security secondary server for content scanning. • The default Cisco Cloud Web Security port for the proxied HTTP and HTTPS traffic is 8080. • You can use either the HTTP port or the HTTPS port or both.
Step 6	**license 7** *license-key* **Example:** `Device(config-profile)# license 7 D5D4A545D7A53222E706D1A5D3B5D4E345E5B25737A737B6613724257425A507`	Configures an encrypted license key that is sent to Cisco Cloud Web Security for authentication.
Step 7	**source interface** *type number* **Example:** `Device(config-profile)# source interface fastethernet 0/2`	Configures the source interface for content scan redirection.

	Command or Action	Purpose
Step 8	**timeout server** *seconds* **Example:** `Device(config-profile)# timeout server 5`	Specifies a server keepalive time in seconds.
Step 9	**timeout session-inactivity** *seconds* **Example:** `Device(config-profile)# timeout session-inactivity 3600`	Specifies the session inactivity time in seconds.
Step 10	**user-group** *group-name* **username** *username* **Example:** `Device(config-profile)# user-group marketing username superuser`	Specifies a default usergroup.
Step 11	**server on-failure block-all** **Example:** `Device(config-profile)# server on-failure block-all`	Blocks all traffic to a web server when communication between the web server and the Cisco Cloud Web Security server fails.
Step 12	**user-group exclude** *username* **Example:** `Device(config-profile)# user-group exclude marketing`	Excludes the specified user group.
Step 13	**exit** **Example:** `Device(config-profile)# exit`	Exits parameter-map type inspect configuration mode and enters global configuration mode.
Step 14	**interface** *type number* **Example:** `Device(config)# interface ethernet 0/0`	Configures an interface and enters interface configuration mode.
Step 15	**cws out** **Example:** `Device(config-if)# cws out`	Configures the egress interface for Cloud Web Security content scanning.
Step 16	**ip virtual-reassembly in** **Example:** `Device(config-if)# ip virtual-reassembly in`	Enables Virtual Fragment Reassembly (VFR) on the ingress.
Step 17	**ip virtual-reassembly out** **Example:** `Device(config-if)# ip virtual-reassembly out`	Enables VFR on the egress.

	Command or Action	Purpose
Step 18	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and enters privileged EXEC mode.
Step 19	**show cws** **Example:** `Device# show cws`	Displays content scanning information.

Example

The following is sample output from the **show cws history** command:

```
Device# show cws history 6

 Protocol  Source              Destination           Bytes          URI
Time
 HTTP      192.168.100.2:1347  209.165.201.4:80    (102:45)       www.google.com
00:01:13
 HTTP      192.168.100.2:1326  209.165.201.6:80    (206:11431)    www.google.com
00:12:55
 HTTP      192.168.100.2:1324  209.165.201.5:80    (206:11449)    www.google.com
00:15:20
 HTTP      192.168.100.2:1318  209.165.201.5:80    (206:11449)    www.google.com
00:17:43
 HTTP      192.168.100.2:1316  209.165.201.4:80    (206:11449)    www.google.com
00:20:04
 HTTP      192.168.100.2:1315  10.254.145.107:80   (575:1547)     alert.scansafe.net
00:21:32
```

Configuring Cisco Cloud Web Security

Note This task applies to releases prior to Cisco IOS Release 15.4(2)T.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type content-scan global**
4. **server scansafe primary ipv4** *ip-address* **port http** *port-number* **https** *port-number*
5. **server scansafe secondary ipv4** *ip-address* **port http** *port-number* **https** *port-number*
6. **license 7** *license-key*
7. **source interface** *type number*
8. **timeout server** *seconds*
9. **timeout session-inactivity** *seconds*
10. **user-group** *group-name* **username** *username*
11. **server scansafe on-failure block-all**
12. **user-group exclude** *username*
13. **exit**
14. **interface** *type number*
15. **content-scan out**
16. **ip virtual-reassembly in**
17. **ip virtual-reassembly out**
18. **end**
19. **show content-scan**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**parameter-map type content-scan global** **Example:** `Device(config)# parameter-map type content-scan global`	Configures a global content-scan parameter map and enters parameter-map type inspect configuration mode.

	Command or Action	Purpose
Step 4	**server scansafe primary ipv4** *ip-address* **port http** *port-number* **https** *port-number* **Example:** `Device(config-profile)# server scansafe primary ipv4 10.12.34.23 port http 8080 https 8080`	Configures a Cisco Cloud Web Security primary server for content scanning. • The default Cisco Cloud Web Security port for the proxied HTTP and HTTPS traffic is 8080. • You can use either the HTTP port or the HTTPS port or both.
Step 5	**server scansafe secondary ipv4** *ip-address* **port http** *port-number* **https** *port-number* **Example:** `Device(config-profile)# server scansafe secondary ipv4 10.21.34.21 port http 8080 https 8080`	Configures a Cisco Cloud Web Security secondary server for content scanning. • The default Cisco Cloud Web Security port for the proxied HTTP and HTTPS traffic is 8080. • You can use either the HTTP port or the HTTPS port or both.
Step 6	**license 7** *license-key* **Example:** `Device(config-profile)# license 7 D5D4A545D7A53222E706D1A5D3B5D4E345E5B25737A737B66137242574 25A507`	Configures an encrypted license key that is sent to Cisco Cloud Web Security for authentication.
Step 7	**source interface** *type number* **Example:** `Device(config-profile)# source interface fastethernet 0/2`	Configures the source interface for content scan redirection.
Step 8	**timeout server** *seconds* **Example:** `Device(config-profile)# timeout server 5`	Specifies a server keepalive time in seconds.
Step 9	**timeout session-inactivity** *seconds* **Example:** `Device(config-profile)# timeout session-inactivity 3600`	Specifies the session inactivity time in seconds.
Step 10	**user-group** *group-name* **username** *username* **Example:** `Device(config-profile)# user-group marketing username superuser`	Specifies a default usergroup.
Step 11	**server scansafe on-failure block-all** **Example:** `Device(config-profile)# server scansafe on-failure block-all`	Blocks all traffic to a web server when communication between the web server and the Cisco Cloud Web Security server fails.

	Command or Action	Purpose
Step 12	**user-group exclude** *username* **Example:** `Device(config-profile)# user-group exclude marketing`	Excludes the specified user group.
Step 13	**exit** **Example:** `Device(config-profile)# exit`	Exits parameter-map type inspect configuration mode and enters global configuration mode.
Step 14	**interface** *type number* **Example:** `Device(config)# interface ethernet 0/0`	Configures an interface and enters interface configuration mode.
Step 15	**content-scan out** **Example:** `Device(config-if)# content-scan out`	Configures the egress interface for content scanning.
Step 16	**ip virtual-reassembly in** **Example:** `Device(config-if)# ip virtual-reassembly in`	Enables Virtual Fragment Reassembly (VFR) on the ingress.
Step 17	**ip virtual-reassembly out** **Example:** `Device(config-if)# ip virtual-reassembly out`	Enables VFR on the egress.
Step 18	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and enters privileged EXEC mode.
Step 19	**show content-scan** **Example:** `Device# show content-scan`	Displays content scanning information.

Example

The following is sample output from the **show content-scan history** command:

```
Device# show content-scan history 6

 Protocol  Source              Destination           Bytes          URI
Time
 HTTP      192.168.100.2:1347  209.165.201.4:80    (102:45)       www.google.com
```

```
00:01:13
 HTTP      192.168.100.2:1326  209.165.201.6:80    (206:11431)    www.google.com
00:12:55
 HTTP      192.168.100.2:1324  209.165.201.5:80    (206:11449)    www.google.com
00:15:20
 HTTP      192.168.100.2:1318  209.165.201.5:80    (206:11449)    www.google.com
00:17:43
 HTTP      192.168.100.2:1316  209.165.201.4:80    (206:11449)    www.google.com
00:20:04
 HTTP      192.168.100.2:1315  10.254.145.107:80   (575:1547)     alert.scansafe.net
00:21:32
```

Configuring Whitelisting in Cisco IOS Release 15.4(2)T and Later Releases

Note This task applies to Cisco IOS Release 15.4(2)T and later releases.

User and user-group-based whitelisting is initially done during a TCP synchronization (SYN). No content-scan sessions are created when a session is whitelisted based on an username or user group. The order of whitelisting is: acl, user, user group, header user-agent, header host.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cws whitelisting**
4. **whitelist** {**acl** {*aclist* | *extended-acl-list* | *acl-name*} | **header** {**host** | **user-agent**} **regex** *regex-host* | **notify-tower**}
5. **whitelist** {**acl** {*aclist* | *extended-acl-list* | *acl-name*} | **header** {**host** | **user-agent**} **regex** *regex-host* | **notify-tower**}
6. **whitelist** {**acl** {*aclist* | *extended-acl-list* | *acl-name*} | **header** {**host** | **user-agent**} **regex** *regex-host* | **notify-tower**}
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**cws whitelisting** **Example:** `Device(config)# cws whitelisting`	Enables whitelisting of incoming traffic and enters Cloud Web Security whitelisting configuration mode.

	Command or Action	Purpose
Step 4	**whitelist** {**acl** {*aclist* | *extended-acl-list* | *acl-name*} | **header** {**host** | **user-agent**} **regex** *regex-host* | **notify-tower**} **Example:** `Device(config-cws-wl)# whitelist acl name whitelistedSubnets`	Configures whitelisting of traffic based on the access control list (ACL) or the HTTP request whose header matches the configured regular expression.
Step 5	**whitelist** {**acl** {*aclist* | *extended-acl-list* | *acl-name*} | **header** {**host** | **user-agent**} **regex** *regex-host* | **notify-tower**} **Example:** `Device(config-cws-wl)# whitelist header host regex whitelistedPatterns`	Configures whitelisting of traffic based on the access control list (ACL) or the HTTP request whose header matches the configured regular expression.
Step 6	**whitelist** {**acl** {*aclist* | *extended-acl-list* | *acl-name*} | **header** {**host** | **user-agent**} **regex** *regex-host* | **notify-tower**} **Example:** `Device(config-cws-wl)# whitelist user regex whitelistedUsers`	Configures whitelisting of traffic based on the access control list (ACL) or the HTTP request whose header matches the configured regular expression.
Step 7	**end** **Example:** `Device(config-cws-wl)# end`	Exits Cloud Web Security whitelisting configuration mode and returns to privileged EXEC mode.

Configuring Whitelisting

Note This task applies to releases prior to Cisco IOS Release 15.4(2)T.

User and user-group-based whitelisting is initially done during a TCP synchronization (SYN). No content-scan sessions are created when a session is whitelisted based on an username or user group. The order of whitelisting is: acl, user, user group, header user-agent, header host.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **content-scan whitelisting**
4. **whitelist** {**acl** {*aclist* | *extended-acl-list* | *acl-name*} | **header** {**host** | **user-agent**} **regex** *regex-host* | **notify-tower**}
5. **whitelist** {**acl** {*aclist* | *extended-acl-list* | *acl-name*} | **header** {**host** | **user-agent**} **regex** *regex-host* | **notify-tower**}
6. **whitelist** {**acl** {*aclist* | *extended-acl-list* | *acl-name*} | **header** {**host** | **user-agent**} **regex** *regex-host* | **notify-tower**}
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**content-scan whitelisting** **Example:** `Device(config)# content-scan whitelisting`	Enables whitelisting of incoming traffic and enters content-scan whitelisting configuration mode.
Step 4	**whitelist** {**acl** {*aclist* | *extended-acl-list* | *acl-name*} | **header** {**host** | **user-agent**} **regex** *regex-host* | **notify-tower**} **Example:** `Device(config-cont-scan-wl)# whitelist acl name whitelistedSubnets`	Configures whitelisting of traffic based on the access control list (ACL) or the HTTP request whose header matches the configured regular expression.
Step 5	**whitelist** {**acl** {*aclist* | *extended-acl-list* | *acl-name*} | **header** {**host** | **user-agent**} **regex** *regex-host* | **notify-tower**} **Example:** `Device(config-cont-scan-wl)# whitelist header host regex whitelistedPatterns`	Configures whitelisting of traffic based on the access control list (ACL) or the HTTP request whose header matches the configured regular expression.

	Command or Action	Purpose
Step 6	**whitelist** {**acl** {*aclist* | *extended-acl-list* | *acl-name*} | **header** {**host** | **user-agent**} **regex** *regex-host* | **notify-tower**} **Example:** `Device(config-cont-scan-wl)# whitelist user regex whitelistedUsers`	Configures whitelisting of traffic based on the access control list (ACL) or the HTTP request whose header matches the configured regular expression.
Step 7	**end** **Example:** `Device(config-cont-scan-wl)# end`	Exits content-scan whitelisting configuration mode and returns to privileged EXEC mode.

Whitelisting HTTP Traffic

By default, Cloud Web Security forwards both HTTP and secure HTTP (HTTPS) traffic to the Cloud Web Security server. However, you can use whitelisting to bypass HTTPS traffic from Cloud Web Security redirection.

To whitelist HTTPS traffic, first create an access control list (ACL) that matches the HTTPS traffic, and add this ACL to the Cloud Web Security whitelist

```
ip access-list extended matchHTTPS
 permit ip any any eq 443
!
content-scan whitelisting
 whitelist acl name matchHTTPS
!
```

Or you can remove the HTTPS port configuration in the Cloud Web Security parameter map.

```
parameter-map type content-scan global
 server scansafe primary ipv4 72.37.244.147 port http 8080
 server scansafe secondary ipv4 80.254.145.147 port http 8080
!
```

Example: Configuring Whitelisting

Note This example applies to releases prior to Cisco IOS Release 15.4(2)T.

```
Device# configure terminal
Device(config)# content-scan whitelisting
Device(config-cont-scan-wl)# whitelist header host regex whitelistedPatterns
Device(config-cont-scan-wl)# whitelist acl name whitelistedSubnets
Device(config-cont-scan-wl)# whitelist user regex whitelistedUsers
Device(config-cont-scan-wl)# whitelist user-group regex whitelistedUserGroups
Device(config-cont-scan-wl)# end
```

Configuring Default User Groups

You can configure a default user group on the egress interface to assign to clients when Integrated Services Routers Generation 2 (ISR G2) cannot determine the credentials users. Define a default user group using the following commands:

```
interface GigabitEthernet 0/1
 user-group default user-group1
```

The ISR G2 uses the default user-group name to identify all clients who are connected to an interface, when it cannot determine the user credentials. Define a default user group so that all traffic that is redirected to the Cloud Web Security proxy servers are assigned a user group to ensure that Cloud Web Security policies are appropriately applied. Only one user group can be defined per interface.

The order of user groups is as follows:

1. User group information from authentication methods (example, AD group information)
2. Interface default user group
3. Parameter-map default user group

If no user group information is gathered during authentication, the default-user group information configured on the interface is used. If a default-user group is not configured on the interface, the ISR G2 router uses the default user group information configured in a parameter map to forward traffic to the Cloud Web Security tower.

Cloud Web Security Authentication Types

Cloud Web Security on Integrated Services Routers Generation 2 (ISR G2) supports three types of authentication—NT LAN Manager (NTLM), HTTP Basic, and Web authentication. The following tables provides a list of authentication types supported in various Cisco IOS Releases:

Cisco IOS Release	Authentication Type Supported
15.2(1)T1, 15.2(1)T2, 15.2(2)T1	Web and HTTP Basic authentication
15.2(4)M and later	NTLM, HTTP Basic, Web Auth

To configure web authentication, refer to the “Configuring Authentication Proxy” module of the *Authentication Proxy Configuration Guide*.

NTLM or HTTP Basic Authentication

Cisco Integrated Services Routers Generation 2 (ISR-G2) uses Windows NT Lan Manager (NTLM) to retrieve user credentials transparently from the client application without prompting end users for authentication. If the client application cannot send user credentials transparently, ISR G2 prompts users to enter credentials.

When using NTLM authentication, you can choose two modes: active or passive. The default mode for NTLM authentication is active. To enable passive mode, configure the command **ip admission name rule1 ntlm passive**.

In NTLM active mode, ISR G2 routers gather both the username and password from the client during the TCP handshake process and verify these against the Active Directory domain controller. In NTLM passive mode, ISR G2 routers only query for the user group information and do not verify the password, which reduces the number of transactions between ISR G2 routers and the domain controller.

During HTTP basic authentication, client applications always prompt users to enter their credentials.

Configuring NTLM or HTTP Basic Authentication

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **ldap server** *name*
5. **ipv4** *ip-address*
6. **bind authenticate root-dn password** [**0** *string* | **7** *string*] *string*
7. **base-dn** *string*
8. **authentication bind-first**
9. **exit**
10. **ldap attribute-map** *map-name*
11. **map type** *ldap-attr-type aaa-attr-type*
12. **exit**
13. **aaa group server ldap** *group-name*
14. **aaa authentication login** *list-name*
15. **ip admission** *admission-name*
16. **ip admission virtual-ip** *ip-address* **virtual-host** *hostname*
17. **interface** *type number*
18. **ip admission** *admission-name*
19. **exit**
20. **ip http server**
21. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** **Example:** `Device(config)# aaa new-model`	Enables the authentication, authorization, and accounting (AAA) functionality on the device. • **Note** Once you enable the **aaa new-model** command, it cannot be disabled.
Step 4	**ldap server** *name* **Example:** `Device(config)# ldap server server1`	Defines a Lightweight Directory Access Protocol (LDAP) server and enters LDAP server configuration mode.
Step 5	**ipv4** *ip-address* **Example:** `Device(config-ldap-server)# ipv4 10.1.1.1`	Specifies the LDAP server IP address using IPv4.
Step 6	**bind authenticate root-dn password** [**0** *string* | **7** *string*] *string* **Example:** `Device(config-ldap-server)# bind authenticate root-dn “cn=administrator,cn=users,dc=nac-blr2,dc=example,dc=com password”`	Specifies a shared secret text string used between the device and an LDAP server. • Use the 0 line option to configure an unencrypted shared secret. • Use the 7 line option to configure an encrypted shared secret. • **Note** If passive NTLM authentication is used, this command is mandatory.
Step 7	**base-dn** *string* **Example:** `Device(config-ldap-server)#  base-dn "dc=sns,dc=example,dc=com"`	(Optional) Configures the base distinguished name to use for search operations in the LDAP server.
Step 8	**authentication bind-first** **Example:** `Device(config-ldap-server)# authentication bind-first`	Configures the sequence of search and bind operations for an authentication request.
Step 9	**exit** **Example:** `Device(config-ldap-server)# exit`	Exits mode and returns to global configuration mode.
Step 10	**ldap attribute-map** *map-name* **Example:** `Device(config)# ldap attribute-map map1`	Configures a dynamic LDAP attribute map and enters attribute-map configuration mode.

	Command or Action	Purpose
Step 11	**map type** *ldap-attr-type aaa-attr-type* **Example:** `Device(config-attr-map)# map type department hr-group`	Defines an attribute map.
Step 12	**exit** **Example:** `Device(config-attr-map)# exit`	Exits attribute-map configuration mode and returns to global configuration mode.
Step 13	**aaa group server ldap** *group-name* **Example:** `Device(config)# aaa group server ldap name1`	Defines the AAA server group with a group name and enters LDAP server group configuration mode. All members of a group must be the of same type, that is, RADIUS, LDAP, or TACACS+.
Step 14	**aaa authentication login** *list-name* **Example:** `Device(config)# aaa authentication login userauthen`	Sets AAA authentication at login. The default keyword uses the listed authentication methods that follow this keyword as the default list of methods when a user logs in.
Step 15	**ip admission** *admission-name* **Example:** `Device(config)# ip admission webauth`	Creates a global policy that can be applied on a network access device.
Step 16	**ip admission virtual-ip** *ip-address* **virtual-host** *hostname* **Example:** `Device(config)# ip admission virtual-ip 10.2.2.2 virtual-host webproxy`	Configures a web-based proxy authentication virtual IP address. • This command is required only for transparent authentication with NTLM. • The IP address should not correspond to an existing device on the network and should not have the same IP as any interface on the Cisco Integrated Service Routers Generation 2 (ISR G2). The virtual proxy hostname is a single-word, non-qualified domain name.
Step 17	**interface** *type number* **Example:** `Device(config)# interface gigabitethernet 0/0`	Configures an interface and enters interface configuration mode.
Step 18	**ip admission** *admission-name* **Example:** `Device(config-if)# ip admission webproxy`	Creates a Layer 3 network admission control rule to be applied to the interface.
Step 19	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 20	**ip http server** **Example:** `Device(config)# ip http server`	Enables the HTTP server on your IP system. • Credentials can be passed using HTTPS instead of HTTP with the command **ip http secure-server**. With HTTPS, clients may encounter SSL certificate errors as the ISR G2 routers use a test certificate server. To avoid SSL certificate errors, replace the certificate on ISR G2 routers with a certificate signed by a trusted certificate authority.
Step 21	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Transparent Authentication with NTLM

An Integrated Services Routers Generation 2 (ISR G2) that uses Windows NT LAN Manager (NTLM) to authenticate users tries to retrieve user credentials transparently from the client application without prompting users for authentication. If the client application cannot send user credentials transparently, then the ISR G2 prompts users to enter their username and password.

During NTLM authentication, an ISR G2 router redirects the client browser from the originally requested URL to a virtual proxy URL (either by using the configured IP address or hostname) configured on the ISR G2 router. After the browser redirects users to the virtual proxy URL, the users are prompted for authentication credentials. Successfully authenticated users are redirected to the requested URL.

Users are transparently authenticated by using NTLM when they access the web using a web browsers on the Windows operating system. For example, users are transparently authenticated through Microsoft Internet Explorer, Mozilla Firefox, and Google Chrome on Windows; however, the users are prompted for authentication credentials when using Apple Safari on an Apple Macintosh or Opera on any operating system.

To ensure that users are transparently authenticated using Microsoft Internet Explorer, Mozilla Firefox, and Chrome on the Windows operating system, perform the following steps:

1 Define a virtual proxy URL on the ISR G2 router using the **ip admission command**.
```
ip admission virtual-ip 10.1.1.1 virtual-host webproxy
```

Note You can specify a single-word hostname as the virtual proxy hostname. The virtual proxy IP address must not be used by any other device or configured on the ISR G2 router.

2 Configure the third-party authentication software to transparently authenticate users by using the virtual proxy URL.

• If you are using Microsoft Internet Explorer or Google Chrome, perform the following step:

- If a virtual proxy hostname is defined, create a Domain Name System (DNS) record that resolves the virtual proxy hostname to the virtual proxy IP address specified in Step 1 (10.1.1.1). Microsoft Internet Explorer and Google Chrome consider a single word hostname as a local intranet server.

- Microsoft Internet Explorer: Add the virtual proxy URL to the Microsoft Internet Explorer Local Intranet Zone. If only the virtual proxy IP address is defined, add the IP address (for example, http://10.1.1.1) to the Local Intranet Zone. If the virtual proxy hostname is defined, add it (for example, http://webproxy) to the Local Intranet Zone.
  For more information on adding a URL to the Internet Explorer Local Intranet Zone, see the Internet Explorer documentation.
- Mozilla Firefox: Edit the Mozilla Firefox preferences that determines the sites that are automatically authenticated by using NTLM and add the virtual proxy URL configured in Step 1. The "network.automatic-ntlm-auth.trusted-uris" is the configuration setting that you have to edit. For more information on editing the Firefox configuration, see the Mozilla Firefox documentation.

Bypassing Authentication

Use network/IP-based authentication or browser-based authentication bypass to disable the authentication to users.

Network/IP-Based Authentication Bypass

To configure Cisco Integrated Services Routers Generation 2 (ISRvG2) to bypass authentication for certain subnets and users, you must either know the IP addresses of the users you do want to authenticate, or the IP addresses of users you do not want to authenticate. Create an access control list (ACL) that permits users who are authenticated and denies users who bypasses authentication access to the network. The ACL rule must associated with the **ip admission** command.

The following example shows how to authenticate users whose IP addresses are known:

```
ip access-list extended authenticationACL
 permit ip 10.0.0.0 0.0.0.255 any any  !! users in this IP range will be asked to authenticate
 first. everyone else bypasses authentication [implicit deny for all others]
!
ip admission name ntlm-rule ntlm list authenticationACL
```

The following example shows how not to authenticate users whose IP addresses are known:

```
ip access-list extended authenticationACL
 deny ip 10.0.0.0 0.0.0.255 any any  !! users in this IP range will be NOT be asked to
authenticate. everyone else must authenticate first
 permit ip any any
!
ip admission name ntlm-rule ntlm list authenticationACL
```

Note This configuration is mostly used only in proof-of-concept or pilot phases where only a subset of users access Cisco Cloud Web Security. For production deployments, typically all corporate users are asked for authentication. For guest users, it is recommended to have a separate VLAN or a network that does not apply authentication. The bypass authentication configuration should only be used if a separate guest VLAN/network is not possible.

Browser-Based Authentication Bypass

Transparent authentication can be done through NTLM authentication. However, some web browsers that do not support transparent NTLM authentication, such as Mozilla Firefox or Apple Safari, will use authentication prompts.

The Browser-Based Authentication Bypass features uses the user agent string sent by the web browser to bypass authentication. A list of user agent strings can be configured on the web browser. Before the authentication, the Cisco Integrated Services Routers Generation 2 (ISR G2) checks if the user agent string from a user's device matches the configured list. If there is a match, authentication is bypassed, and the user can access the Internet with guest Cloud Web Security policies. If there is no match, user authentication is required. Web browsers that support transparent NTLM authentication, the authentication happens in the background, and users are not prompted for credentials.

The ISR G2 router does a match on the user agent string configured on the router with the user agent string sent by the web browser. Web browsers may change the user agent string that is used to identify the browser. A best practice is for the Network administrators to periodically update the list of user agent strings on the ISR G2 router. To find the user agent string that your web browser is sending, go to *http://whatsmyuseragent.com*. A list of user agent strings is also available at *http://techpatterns.com/forums/about304.html*

A sample user agent string for an iPad 3 would be the following: "Mozilla/5.0 (iPad; CPU OS 5_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B176 Safari/7534.48.3"

Typically most smartphones or tablets have the following user agent strings:

```
Mobile =
iphone|ipod|android|blackberry|opera|mini|windows\sce|palm|smartphone|iemobile
 Tablet =
ipad|android|android|xoom|sch-i800|playbook|tablet|kindle
```

The following is a sample parameter map (to match common bring-your-own devices) that uses the user agent strings given above:

```
parameter-map type regex byod
 pattern .*iPad*
 pattern .*andriod*
 pattern .*kindle*
```

Authentication Failure

Prior to the Cisco IOS Release 15.2(4)M3, if a user failed authentication, the default behavior was to block all Internet access for that IP address. In Cisco IOS Release 15.2(4)M3 and later release, if a user fails authentication, the configured guest access policies are applied.

Note The following are the causes of user authentication failures:

- Username, password, or both are incorrect in active NTLM authentication mode.
- Username is incorrect in passive NTLM authentication mode.
- LDAP server is not reachable and the user must make 5 attempts or the configured number of login attempts, before the authentication fails.

Default guest access is enabled by default. However, you can configure the maximum number of login attempts that are required before a user can fall back to the default guest access policy. The default maximum login attempt value is 5. This means that a user must fail five consecutive login attempts before falling back to the default access policy.

To change the maximum login attempt value, configure the following command:

```
ip admission max-login-attempt 2
```

While determining the maximum login attempt value, understand the risks of corporate users entering wrong username and password. If the value is too less, some corporate users may be moved to the default guest policy with the multiple authentication pop-up messages. We recommend that you configure a maximum login attempt value of at least two to prevent corporate users from being authenticated as guests very often.

Session States and Time Between Sessions

If a user fails authentication, that user is authenticated as a guest user by using the configured default guest policy; however the session state will show SERVICE_DENIED. The session will remain in SERVICE_DENIED state for a default of 2 minutes, after which the session is moved to the initialized (INIT) state and the user will be prompted for credentials.

To adjust the time between authentication prompts, enable a watch list and configure watch-list timeout:

```
ip admission watch-list enable
ip admission watch-list expiry-time 1440
```

We recommend not to set the watch-list expiry timer to a very high value so that users are not prompted for credentials frequently. Setting zero (time of forever) is also not recommended as the user is never prompted for authentication and will have granular user policies applied.

Domain and Non-Domain Users

Domain users who use transparent Windows NT Lan Manager (NTLM) authentication with supported browsers cannot login to the domain with invalid credentials. Because the device/domain will not let a user login to a network with invalid credentials, the domain will always have the correct username and user group, which ensures that the user always receives the granular user policies defined in the Cloud Web Security portal. If the password of a user expires, the user must log off and relogin to the domain with the new password.

The default guest access policy is available to users who use non-transparent NTLM authentication methods and fail authentication.

The following users are considered as non-domain users:

- Domain users who do not use either Microsoft Internet Explorer or Google Chrome (These web browsers supports transparent NTLM by default.).
- A user who locally logs into a device (for example, workgroup machines that support local sign-on).
- Guest users

During authentication, non-domain users must specify the domain name (cisco\user1) and the password. If a user enters only the username and password, the client PC considers the hostname/computer name as the domain name and the user may not be authenticated, even when proper credentials were given.

For example, a corporate user User1 who uses a Mozilla Firefox web browser (that does not support transparent NTLM authentication by default) belongs to the “humanresources” domain. User1 must log into the domain with the username “humanresources\user1” to be recognized as a corporate user who has access to corporate

policies configured on Cloud Web Security. If User1 logs in as just "user1", the user is authenticated as a guest user and only the default policy is applied.

Acceptable Use Policy Aggrement

You can configure the Cisco Integrated Services Routers Generation 2 (ISR G2) to authenticate users who access the web to agree to an acceptable use policy before browsing the web. This authentication helps warn users that their web traffic is scanned by Cisco Cloud Web Security.

Acceptable use policy (AUP) agreement enforcement works with and without authentication. However, the only authentication type supported with AUP on ISR G2 routers is web authentication. NTLM or HTTP basic authentication is not supported.

For users to agree to the acceptable use policy agreement use the Consent feature. For more information, see the Consent Feature for Cisco IOS Routers.

Enabling Nested LDAP for Cloud Web Security

In Cisco IOS Release 15.3(3)M and later releases, nested Lightweight Directory Access Protocol (LDAP) is supported with HTTP basic, Web, and NTLM authentication. With this support, the LDAP client module can fetch both direct and nested user-group information for a user.

An LDAP search query retrieves the authorization profile of a user from an LDAP server to find direct user group members. Each of these direct user groups can be part of multiple groups and thus form a nested-user group.

Perform the following task to enable nested LDAP search:

```
Device(config)# ldap server server1
Device(config-lap-server)# search-type nested
```

Configuring the Cisco Cloud Web Security Portal

To configure Cisco Cloud Web Security to work with Cisco Integrated Services Routers Generation 2 (ISR G2), you must complete the following steps in the Cloud Web Security web-based GUI portal:

1. Create a Cloud Web Security authentication key.
   In the Cloud Web Security portal, navigate to the Admin page and create either a company or a group authentication key. The type of key that you create depends on your network environment. For more information on the type of key to create, see the section “Working with Multiple ISRs”.

   For more information on how to create keys in the Cloud Web Security portal, see the “Authentication” section in the “Administration” chapter of the Cloud Web Security Portal Administrator Guide.

2. Define Cloud Web Security user groups.
   If ISR G2 routers enforce authentication and you need to create different web policies for each user group, or configure a different group key for different ISR routers, you must define user groups in the Cloud Web Security portal. You can define the following groups:

   - Directory—Directory groups can be Windows Active Directory (AD) groups or LDAP groups.
   - Custom—Custom groups enable you to create a group containing any users, regardless of their AD or LDAP group.

In the Cloud Web Security Admin page, create user groups. For more information, see the "User Management" section in the "Administration" chapter of the *Cloud Web Security Portal Administrator Guide*.

3 Create Cloud Web Security web policies.
The Web Filtering Service of the Cloud Web Security portal enables you to create different web policies to enforce acceptable use policies for web traffic. To create a policy, you must first configure web filters and schedules that apply to policies. Web filters control the content coming into a network and schedules determine when policy rules are applied. For more information on configuring web filters, see the "Web Filtering Service" chapter in the *Cloud Web Security Portal Administrator Guide*

4 Configure the Malware Service options in the Cloud Web Security portal.
For more information, see the Malware Service chapter in the *Cloud Web Security Portal Administrator Guide*.

5 View reports.
For more information, see the Reporting chapter in the *Cloud Web Security Portal Administrator Guide*.

Cloud Web Security Logging Messages

To enable the logging of Cloud Web Security messages, configure the **logging** command under the **parameter-map type content-scan global** command.

The following table displays the Cloud Web Security syslog messages:

Table 2: Cloud Web Security Syslog Messages

Message	Description
%CONT_SCAN-6-START_SESSION	Indicates that a flow is created by the content-scanning process. This syslog message is rate-limited.
%CONT_SCAN-6-STOP_SESSION	Indicates that a flow is removed by the content-scanning process. This syslog message is rate-limited.
%CONT_SCAN-3-CONNECTIVITY	Indicates that the primary or secondary Cloud Web Security proxy server is up or down. When the server is up, the "is up" message only appears after the configured timeout value, which by default is 300 seconds.
%CONT_SCAN-3-UNREACHABLE	Indicates that both the primary and secondary Cloud Web Security proxy servers are down and the content scanning process is disabled.
%CONT_SCAN-3-TOWER-CHANGE	Indicates that a new Cloud Web Security proxy server is selected as the primary server.

Message	Description
%CONT_SCAN-6-WHITE_LIST	Indicates that a flow is scanned by Cloud Web Security because the original client request matched the configured whitelist. The message includes the reason for the client request matching the whitelist. This syslog message is rate-limited.

Sample Configuration of Cloud Web Security on ISR G2s

The following is a sample Cloud Web Security configuration on Cisco Integrated Services Routers Generation 2 (ISR G2) with NTLM authentication:

```
!Configuring Cloud Web Security parameter-map features
parameter-map type content-scan global
 server scansafe primary ipv4 209.165.201.1 port http 8080 https 8080
 server scansafe secondary ipv4 209.165.202.129 port http 8080 https 8080
 license 0 5D22AA983ABC544AF92F83A51A507262 ---! Enter your license. This is a sample.
 source interface GigabitEthernet0/0
 timeout server 30
 user-group cisco username ciscouser
 server scansafe on-failure block-all
!
!Enabling Cloud Web Security on the outbound interface.
interface GigabitEthernet 0/0
 description outbound interface
 content-scan out
!
!Enabling content-scan whitelisting.
content-scan whitelisting
 whitelist acl name whitelistedSubnets
 whitelist header host regex whitelist
!
!Enabling a whitelist pattern parameter-map.
parameter-map type regex whitelist
 pattern google
 pattern cisco
!
!Enabling a whitelist access control list.
ip access-list standard whitelistedSubnets
 permit 10.1.0.0 0.0.0.255
!
!Defining an LDAP attribute map.
ldap attribute-map ad-map
 map type sAMAccountName username
!
!Configuring an LDAP server
ldap server ss
 ipv4 10.0.0.1
 attribute map ad-map
 bind authenticate root-dn CN=CiscoScansafe,OU=Global, DC=Cisco,DC=com password 0
secretpassword ! optional
 base-dn DC=Cisco,DC=com
!
! Enabling authentication.
aaa new-model
!
!Defining AAA group and adding LDAP server to the group.
aaa group server ldap ss-grp
 server ss
!
!Defining AAA authentication and authentication groups.
aaa authentication login aaa-ss group ss-grp
aaa authorization network aaa-ss group ss-grp
```

```
!
!Defining ip admission rules. Here, NTLM authentication and specific subnet of IPs subject
 to authentication only are defined.
ip admission name ntlm-rule ntlm absolute-timer 60 list authlist
ip admission name ntlm-rule method-list authentication aaa-ss authorization aaa-ss
!
!Enabling authentication on inbound interface.
interface GigabitEthernet0/1
 description inbound interface
 ip admission ntlm-rule
!
!Defining  maximum login attempts. A user must fail login 2x attempts before falling back
to the default guest policy.
ip auth-proxy max-login-attempts 2
!
!Enabling the ip admission watch-list.
ip admission watch-list enable
!
!Defining a watch-list timer. Users on a watch-list are not prompted again for authentication
 within 24 hours.
ip admission watch-list expiry-time 1440
!
!Defining a virtual IP address and a virtual hostname for NTLM transparent authentication.
ip admission virtual-ip 10.5.5.1 virtual-host CWSwebproxy
!
!Configuring Cloud Web Security authentication bypass. ACL bypasses defined subnets for
authentication only. Cloud Web Security is still applied for these networks.
ip access-list extended authlist
 permit ip 10.0.1.0 0.0.0.255 any any ! these subnets have to do authentication
 [implicit deny for all others] ! all other IPs bypassed
!
```

Cloud Web Security Troubleshooting Tips

Packet Drops with Small MTU Value on Interfaces

When you configure a smaller Maximum Transmission Unit (MTU) value size using the **ip mtu** *mtu-value* command on an interface in the network, it may prevent web browsing. If the packet size is greater than the MTU size configured on an interface, packets may drop, which prevents web browsing, and the packets are sent with a Do Not Fragment (DF) bit set. This issue happens rarely.

As a workaround for this issue, configure **ip tcp adjust-mss** *segment-size* command on the interface along with the **ip mtu** *mtu-value*. The value for the segment size must be less than the configured MTU value.

Example:

```
interface FastEthernet 4
 ip mtu 100
 ip tcp adjust-mss 55
!
```

Cloud Web Security Tower is Located in a Different Location

The Cisco Cloud Web Security usually chooses the tower nearest to your geographical location, sometimes a tower may not exist in the same country as the user. In this case, web pages that use localization features or have a local server may not display these features properly.

For example, if a user is located in the United States but the tower is located in the United Kingdom, when the user enters www.yahoo.com, the user is redirected to www.yahoo.co.uk because the returning traffic from the Cloud Web Security tower originates in the United Kingdom.

The workaround for this issue is to enter the county-specific URL. For example, in the above situation, enter www.us.yahoo.com to open the local Yahoo! web site.

Host and User Agent-Based Whitelisting Inconsistencies with Asymmetric Routing

The host and user agent-based whitelisting may not work properly with asymmetrical routing because the returning synchronize (SYN) and acknowledge (ACK) messages take a different path than the initiating SYN message.

As a workaround, use IP-based whitelisting instead of header-based whitelisting.

Page Loads Differently After Cloud Web Security Warning Page

When the Warning option is used, the destination page may load differently than normal after the user clicks "Accept."

This is a known issue. The functionality of the page is not lost; only the appearance is affected.

Virtual Hostname Resolves to Open DNS Server

If you configure the virtual hostname incorrectly, the virtual hostname is resolved to the open Domain Name System (DNS) server. This issue does not impact the Cloud Web Security functionality, this is a security risk in some circumstances.

To avoid this issue, ensure that the virtual IP address and virtual hostname is correctly configured.

NTLM Authentication and Browser-Based Authentication Bypass Supports only GET Requests

Windows NT Lan Manager (NTLM) authentication and browser-based authentication bypass on Cisco Integrated Services Routers Generation 2 (ISR G2) currently supports only the GET method in the HTTP request. Other methods like POST, PUT, and so on are not supported. The ISR G2 router will close connections if one of the unsupported methods are received prior to the authentication of a user. If the authentication timer expires while a user is completing a form, the form may not be submitted correctly.

To avoid this issue, open another page or link by using the GET method.

Clearing the Cache Results in Credential Requests

When a network administrator configures the **clear ip admission cache** command on the Cisco Integrated Services Router Generation 2 (ISR G2), all established sessions are cleared for a particular user or for everyone, depending on the configuration. In this case, if NTLM authentication is configured, some users may see

additional pop-up messages that requests for authentication credentials. This issue is more noticeable when authentication timers are configured for longer periods of time.

To reduce the number of users getting pop-up message requests for credentials, configure the **clear ip admission cache** command during non-peak hours. To clear the sessions of specific users, configure their IP address using the **clear ip admission cache** *ip-address* command to avoid clearing all other sessions.

Multiple NTLM Authentication Requests

If a virtual IP address is not configured, the NTLM authentication may not appear transparent to users. In such cases, users may get multiple authentication requests.

To avoid this issue, configure a virtual IP address and virtual hostname, and ensure that they are resolvable through the Domain Name System (DNS).

Root Bind in LDAP Configuration

You must configure the root bind command,**bind authenticate root-dn** *attributes* available in the LDAP server configuration mode for NTLM passive authentication to work. With NTLM active authentication, the root bind configuration is optional.

Protecting ISR G2s from Layer 4 Forwarding Attacks

The Cloud Web Security connector on Cisco Integrated Services Routers Generation 2 (ISR G2) is prone to Layer 4 TCP attacks.

To protect ISR G2 routers from Layer 4 attacks, configure features like the Zone-Based Policy Firewall or Intrusion Prevention System.

ACL Logging not Supported with Whitelisting

The access control list (ACL) for Cloud Web Security IP-based whitelisting does not support ACL logging. For example, you cannot configure an ACL statement such as the following:

```
permit ip host 10.1.1.1 any log
```

Configure ACL statements without the **log** keyword.

Cloud Web Security and Multipath TCP

Cloud Web Security currently do not support multipath TCP. Devices that use multipath TCP such as Apple devices running iOS 7, the multipath TCP feature may be disabled.

Additional References for Cisco Cloud Web Security and Integrated Services Routers Solution

Related Documents

Related Topic	Document Title
IOS commands	Cisco IOS Master Command List, All Releases
Security commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z
Cloud Web Security: FAQs	Cisco Cloud Web Security On ISR-G2 - FAQ
Cisco ScanCenter administrator guide	Cisco ScanCenter Administrator Guide

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support