Cisco Cloud Web Security

ISR G2 Deployment Guide

October 2014

Contents

Introduction

Integrating CWS with the ISR G2 appliance saves bandwidth, money and resources by intelligently redirecting internet traffic from branch offices directly to the cloud to enforce security and control policies.

This document provides directions to redirect network traffic to CWS through the ISR G2.

*Note: we refer to our cloud proxies as towers. You will see the terms “proxy” and “tower” used interchangeably throughout the document.

Cloud Deployment

Deployment is divided into the following three sections

Additional Redirect Methods

There are 4 additional redirection methods that have corresponding deployment guides. Deployment guides for each redirection methods can be found here, under Technical Collateral.

Redirection Method	Overview
Next Generation Firewall (ASA/ASAv with CWS Connector)	Capitalize ASA investments by offloading content scanning to Cisco’s cloud through CWS. Apply acceptable use policy to the company, groups or individual users.
Web Security Appliance (WSA/WSAv with CWS Connector)	Integrate CWS and WSA to enable identity information to the cloud and extend other on-premises enterprise features to Cloud Web Security customers
Cisco AnyConnect Secure Mobility Client (AnyConnect)	Authenticate and redirect web traffic securely whenever the end user is off the corporate network. CWS leverages cached user credentials and directory information when they are away from the office or VPN, ensuring that exactly the same web-usage policies are applied.
Standalone Deployment	Deploy a simple web security solution that does not require any additional hardware. Connect to Cisco’s Cloud Web Security service using existing browser settings and PAC/WPAD files.

Prepare

Verify proper IOS image

The recommended version at the time of this writing is 15.3.3M3 or later. However, CWS is supported is IOS version 15.2(1) T1 and later. For up-to-date information, please reference this link: https://supportforums.cisco.com/document/12110031/cisco-cloud-web-security-cws-isr-g2-faq

*Note: For images earlier than 15.3.3M3, all references to “cws” in the CLI please use “content-scan” instead.

Verify connection to a tower

Site-to-tower communication is accomplished over TCP port 8080. HTTP and HTTPS requests are sent to a cloud scanning tower in this method. Therefore, TCP port 8080 outbound is required to be open for all users within the organization. For security reasons, Cisco recommends that port 8080 outbound destinations be limited to the scanning towers provisioned for the customer’s account.

Reference video: Verify connection to a tower

Step 1: Log on to a client computer inside the customer’s network.

Step 2: Click on the Control Panel and go to Programs and Features.

Step 3: Click Turn on Windows features on or off. Scroll down the list of available features until you find the Telnet Client. Check the box and click OK. Now that the Telnet Client is installed, we can resume our test.

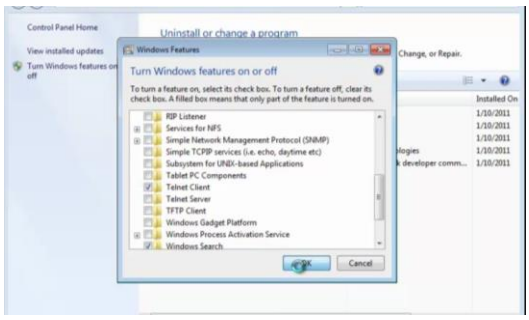

Figure 1.1

Step 4: Open the command line window and type command ‘telnet [tower IP address] 8080.” A successful connection is noted by a blank screen and blinking cursor.

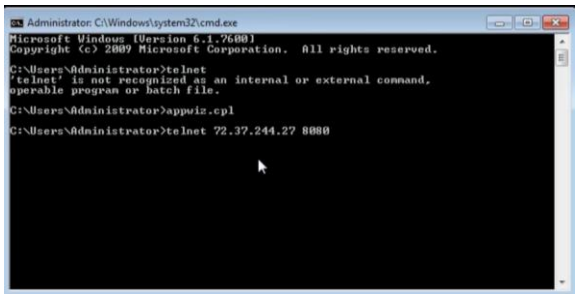

Figure 1.2

Create authentication license key

Reference video: [Authentication license key creation and management]

Step 1: Log on to the Cisco Cloud Web Security portal at https://scancenter.scansafe.com/.

Step 2: From the *Admin* tab, mouse over *Authentication*, and select the key that you would like to generate. The options are Company Key to have a single key for all users in the company (can be used in various Connectors), AnyConnect, or a mixture of them all.

Step 3: Notice that no Company Key currently exists in this account. Click the *Create Key* button to create the Company Key. If one already exists and you don't know the whole string (only the last four characters will be seen), then you will have to revoke it before you can create a new one, but then if it is in use anywhere (Connectors or AnyConnect) then it will have to be replaced with the new one

Step 4: The key is active immediately. The email option below is only for the admin to have a backup of the key. **Note:** Once you navigate away from the page you'll no longer see the complete string of the key (only the last 4 characters).

Figure 1.3

Step 5: Copy the entire alphanumeric string in the *Authentication Key* field and record it in a document that will be backed up.

*Note: The second option is to create a group key by selecting *Group Key* under *Authentication*. To create a group key you may either use an existing directory group or you may create a custom group under → Admin → Management → Groups.

Step 6: Click on the *Create Key* button which corresponds to the group for which you are creating a key.

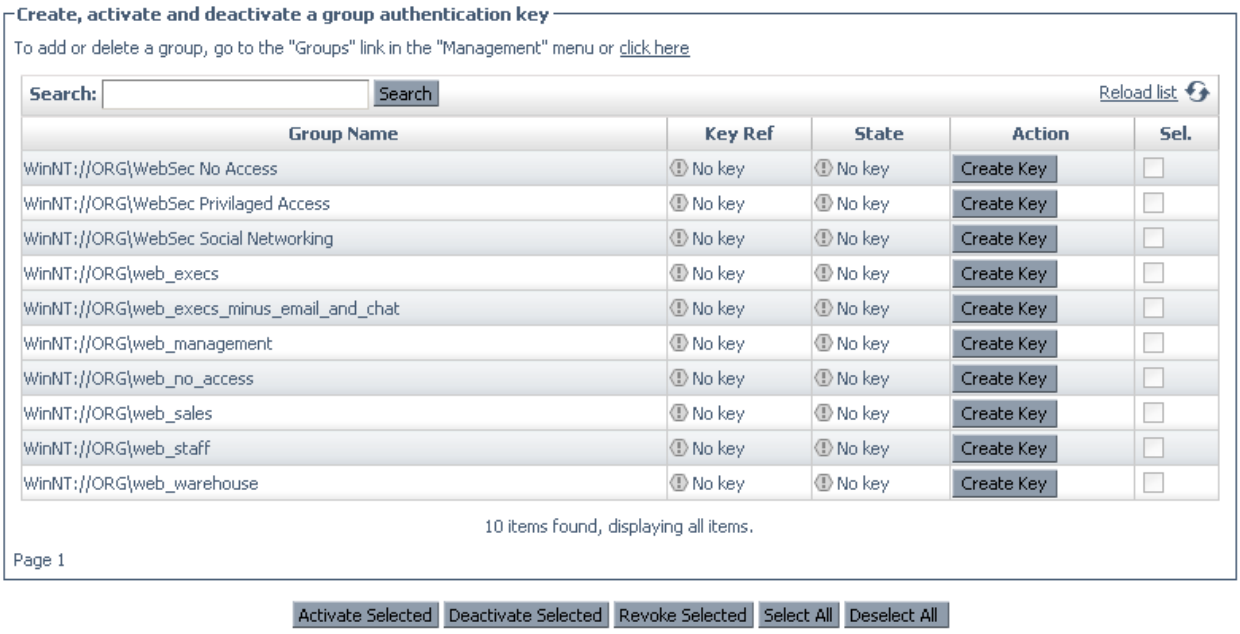

Figure 1.4

*Note: It is the same UI and process for creating a Company Key

Deploy

Configure an ISR G2 connection

This document is intended to provide an overview of the deployment process. For more detailed information and troubleshooting, please refer to the Admin Guide.

Cisco ISR-G2 routers enables you to easily connect branch office networks to CWS. Connector functionality integrated into the ISR G2 device software intelligently redirects web traffic to CWS to enforce security and control policies. With this integrated routing and web security solution, branch offices can be controlled centrally. ISR G2 routers also serve as a cost-effective solution for delivering CWS on public WiFi networks.

Redirect web traffic

```
parameter-map type content-scan global
server scansafe primary ipv4 <primary tower ip> port http 8080 https 8080
server scansafe secondary ipv4 <secondary tower ip> port http 8080 https 8080
license 0 <license key generated above>
source interface GigabitEthernet0/1
timeout server 30
server scansafe on-failure block-all

interface GigabitEthernet0/1
cws out
```

Note the following:

`license` – this is where you apply the license key you generated above. Using 0 will be in clear text, using 7 will be encrypted

`source interface`- this command configures an interface or an IP address as the source from which packets to Cloud Web Security will originate from the device. The IP address that is configured in this command must be the IP addresses that is associated with the interface on which "`cws out`" command is configured.

`cws out`- this command enables web filtering and should be applied to the outside interface.

Configure ACL whitelisting – By Host

```
parameter-map type regex allowed_hosts
pattern *.cisco.com
cws whitelisting
whitelist header host regex allowed_hosts
```

Configure ACL whitelisting – By User Agent

```
parameter-map type regex allowed_user-agents
pattern Mozilla/5.0
cws whitelisting
```

```
whitelist header user-agent regex allowed_user-agents
```

Configuring LDAP Server

```
aaa new-model
aaa group server ldap scansafe
server ss-ldap
ldap server ss-ldap
ipv4 <ldap server ip>
transport port 3268
bind authenticate root-dn "<service account distinguished name>" password
   <server account password>
base-dn "<search base distinguished name>"
search-filter user-object-type user
authentication bind-first
```

Configure user identity

```
aaa authentication login ss-aaa group scansafe
aaa authorization network ss-aaa group scansafe
aaa accounting network ss-aaa none
ip admission virtual-ip 1.1.1.1 virtual-host proxy
ip admission name ssauth ntlm passive inactivity-time 60
ip admission name ssauth order ntlm
ip admission name ssauth method-list authentication ss-aaa authorization ss-
aaa accounting ss-aaa

interface GigabitEthernet0/0
ip admission ssauth
ip http server
aaa authentication login default none
aaa authorization exec default none
```

For user authentication to work, the client must be able to resolve "proxy" to the IP address 1.1.1.1. For testing purposes, edit the hosts file on a client to include an entry for this IP address. In production, create an A record in DNS.

Troubleshooting commands

```
sh cws statistics
sh cws summary
sh cws session active
sh cws session history <1-512>
```

Bypass ip admission (auth)

```
ip admission name ntlm-rule ntlm list ssauth
ip access-list extended ssauth
permit ip <corporate ip> <wildcard mask> any any
```

Bypass HTTPS filtering:

```
ip access-list extended matchHTTPS
permit ip any any eq 443
cws whitelisting
whitelist acl name matchHTTPS
```

Test

Verify web redirection to the cloud

Step 1: From a client machine, browse to whoami.scansafe.net. If a message is displayed, “User is not currently using the service,” then the traffic is not redirected to the Cisco cloud. This can be useful in determining if the user is being resolved correctly, any groups being discovered, the internal/external IP of the user/location, and what Connector is in use.

This is an example of a successful whoami.scansafe.net output:

```
authUserName: "WinNT://CISCO\\user"
authenticated: true
companyName: Cisco
connectorGuid: ABC012345AB
connectorVersion: "AP-ISR-x.x(x)x,"
countryCode: US
externalIp: 12.34.56.78
groupNames:
  - "LDAP://Group"
internalIp: 1.2.3.4
logicalTowerNumber: 1782
staticGroupNames:
  - "LDAP://Group"
userName: "WinNT://CISCO\\user"
```

Step 2: From a client machine, browse to policytrace.scansafe.net and enter a URL to see how the web request is processed against the current web filtering policy.

Step 3: With *SearchAhead* enabled in ScanCenter (the CWS admin portal), browse to Google, Bing, or Yahoo and search for something. The *SearchAhead* data should be prepended to each search result in the form of a green, yellow, or red dot. Mouse over the dot to see what information is contained within.

*Note: For additional options on authentication methods reference this link.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-727200-00 04/13