Configure and Examine SOCKS Proxy on Secure Web Appliance

Contents

Introduction

This document describes how the SOCKS proxy works on Cisco SWA and provides an overview of how it routes traffic between a client and the end server

How SOCKS proxy works at a high level

Socket Secure (SOCKS) is a network protocol that facilitates communication with servers through a SOCKS proxy (here, it is SWA/WSA) by routing network traffic to the actual server on behalf of a client. SOCKS is designed to route any type of application-layer traffic generated by any program.
The SWA by default uses TCP port 1080 to listen to the client SOCKS traffic. The clients can configure to send the socks traffic to WSA on TCP port 1080. You can add additional port numbers if needed.

SOCKS version 5 also supports UDP tunneling so the client can use the UDP port as well to send the traffic to the proxy. By default, it is 16000-16100.

When you want to relay a UDP traffic over the SOCKS5 proxy, the client makes a UDP associate request over the TCP control port 1080. SOCKS5 server (SWG/WSA) then returns an available UDP port to the client to send UDP packages to. By default, it is 16000-16100. You can modify the port numbers.

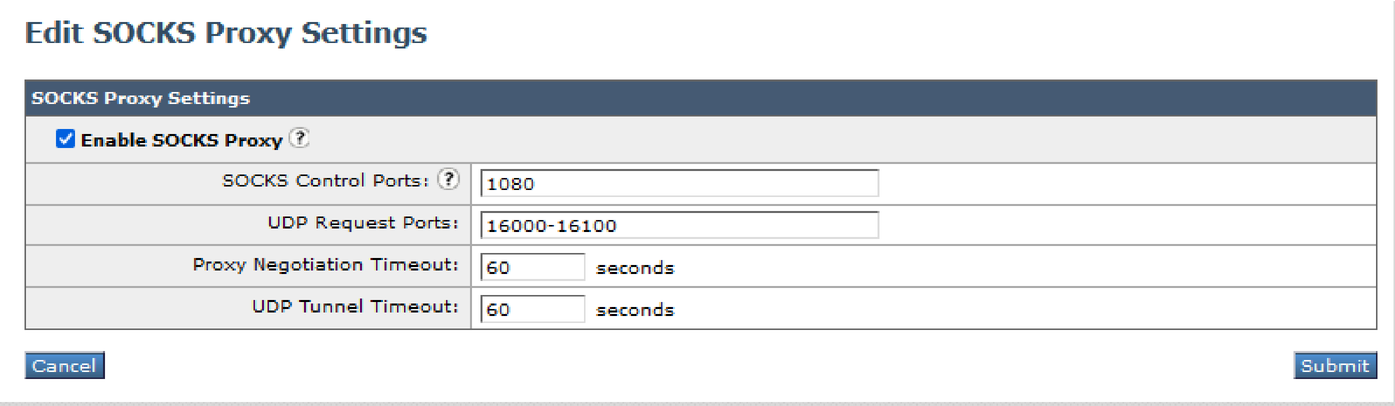
The client then starts sending the UDP packages that need to be relayed to the new UDP port that is available on the SOCKS5 server. SOCKS5 server redirects these UDP packages to the remote server and redirects the UDP packages coming from the remote server back to the PC.

When you want to terminate the connection, the PC sends a FIN package over the TCP. The SOCKS5 server then terminates the UDP connection created for the client and then terminates the TCP connection.

Caution: The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

SOCKS Proxy Configuration on SWA/WSA

You can navigate to **Security services > SOCKS proxy** to configure the SOCKS control port and UDP request ports. This also allows configuring the timeouts.



Edit SOCKS Proxy Settings

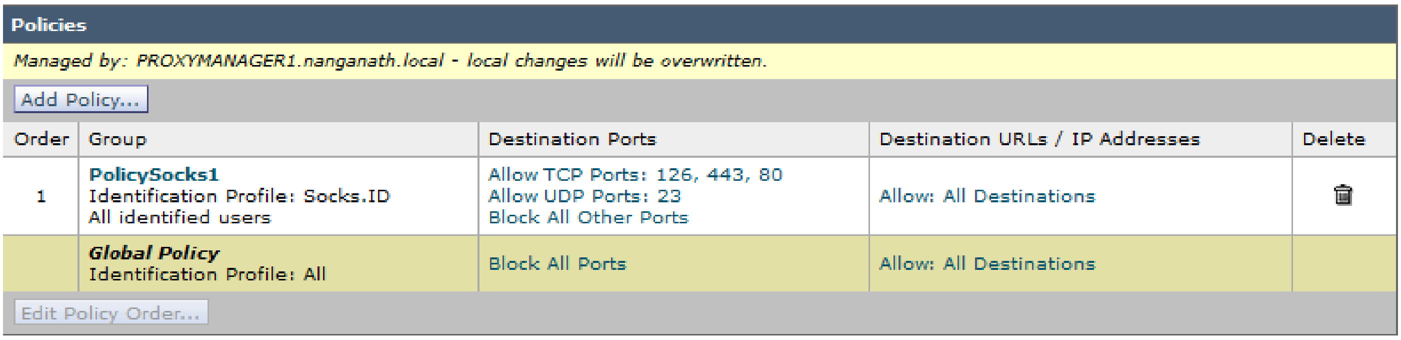
SOCKS Proxy Settings

☑ Enable SOCKS Proxy

SOCKS Control Ports:	1080
UDP Request Ports:	16000-16100
Proxy Negotiation Timeout:	60 seconds
UDP Tunnel Timeout:	60 seconds

SOCKS policies can be configured by navigating to **Web Security Manager > SOCKS Proxy**.

You can configure the policies as required and you can allow specific TCP/UDP ports as needed



Policies

Managed by: PROXYMANAGER1.nanganath.local - local changes will be overwritten.

Order	Group	Destination Ports	Destination URLs / IP Addresses	Delete
1	**PolicySocks1** Identification Profile: Socks.ID All identified users	Allow TCP Ports: 126, 443, 80 Allow UDP Ports: 23 Block All Other Ports	Allow: All Destinations	🗑
	Global Policy Identification Profile: All	Block All Ports	Allow: All Destinations	

Troubleshoot the SOCKS proxy-related issues

You can view the logs via Web tracking on the WSA reporting module SOCKS section or through the access logs.

```
1652931442.472 0 10.106.37.183 SOCKS_TCP_MISS/200 0 SOCKS_HELLO/ - NONE/- -
ALLOW_ADMIN_SOCKS_ALL_CONNECTIONS_11-PolcySocks1-Socks.ID-NONE-NONE-NONE-
NONE-NONE <"-",-,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,"-",-,"-","-","-","-","-","-","-",0.00,0,-,"-","-",-,"-",-,-
,"-","-",-,-,"-",-,-> - - [ Request Details: ID = 2428020, User Agent = -, AD Group Memberships = ( NONE )
- ] ; "19/May/2022:09:07:22 +0530"
```

```
1652931442.488 16 10.106.37.183 SOCKS_TCP_MISS/200 338 SOCKS_CONNECT
tunnel://151.101.130.219:80/ - DIRECT/151.101.130.219 -
ALLOW_ADMIN_SOCKS_ALL_CONNECTIONS_11-PolcySocks1-Socks.ID-NONE-NONE-NONE-
NONE-NONE <"-",-,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,"-",-,"-","-","-","-","-","-","-",169.00,0,-,"-","-",-,"-
",-,-,"-","-",-,-,"-",-,-> - - [ Request Details: ID = 2428030, User Agent = -, AD Group Memberships = (
NONE ) - ]; "19/May/2022:09:07:22 +0530", Server IP = 151.101.130.219
```

Unsupported in SWA SOCKS implementation

1. SOCKS version 5 is supported. Version 4 is not supported.
2. The SOCKS protocol only supports direct forward connections so it can not support redirections.
3. The SOCKS proxy does not support upstream proxies so you cannot send the WSA socks traffic to another upstream proxy. You must always use the Direct connection routing policy.

4. You can not utilise the WSA functionalities such as scanning, AVC, DLP and malware detection.
5. Policy trace cannot work with socks proxy.
6. No SSL decryption support is available as the traffic tunnels from client to server.
7. Socks proxy only supports basic authentication.

Additional Information

By default, when try sending SOCKS traffic via Firefox, the DNS resolution is made locally, hence the WSA does not see any hostname in reporting or access logs. If we enable Remote DNS on Firefox then WSA can do DNS resolution and we can view the hostname in reporting/access logs. The Remote DNS option is available in the latest Firefox versions. If it is not available, try these steps.

about:config
Search Preference name : proxy, find **network.proxy.socks_remote_dns** and set it to **True**.

Google Chrome browser by default performs DNS resolution on the SOCKS proxy so no changes are needed.

As per the Google chrome Proxy support document, SOCKSv5 is only used to proxy TCP-based URL requests. It cannot be used to relay UDP traffic.

Reference

https://www.rfc-editor.org/rfc/rfc1928#section-4

https://chromium.googlesource.com/chromium/src/+/HEAD/net/docs/proxy.md#SOCKSv5-proxy-scheme