

Module Flow

1

**Understand Different
Types of Network
Segmentation**

2

**Understand Different
Types of Firewalls
and their Role**

3

**Understand Different
Types of IDS/IPS and
their Role**

4

**Understand Different
Types of Honeypots**

5

**Understand Different
Types of Proxy Servers
and their Benefits**

6

**Discuss Fundamentals
of VPN and its
importance in Network
Security**

7

**Discuss Security Incident
and Event Management
(SIEM)**

8

**Discuss User Behavior
Analytics (UBA)**

9

**Understand Various
Antivirus/Anti-
malware Software**

Honeypot



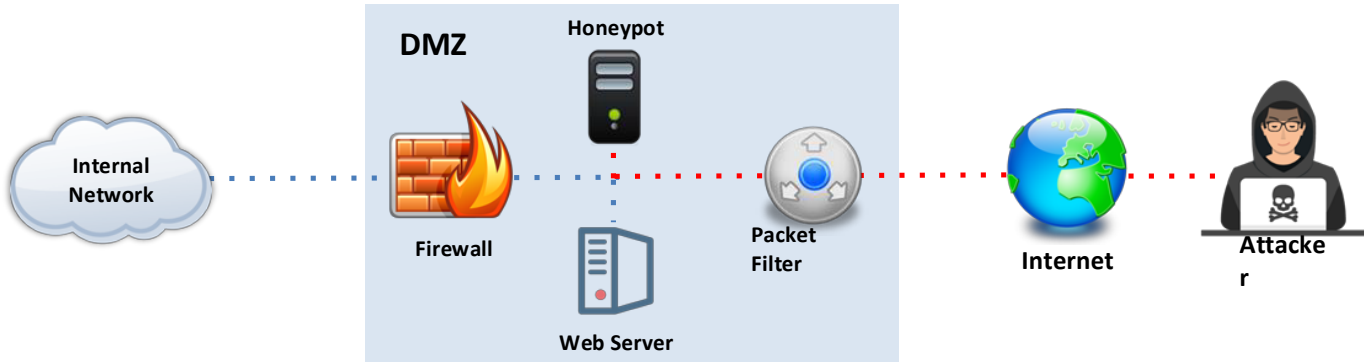
A honeypot is an information system resource that is expressly **set up to attract and trap people** who attempt to penetrate an **organization's network**



It has no authorized activity, does not have any **production value**, and any traffic to it is likely to be a **probe**, **attack**, or **compromise**



A honeypot can **log port access** attempts or monitor an **attacker's keystrokes**. These could be **early warnings** of a more concerted attack



Types of Honeypots

Classification of Honeypots based on their design criteria

Low-interaction Honeypots

- ❑ These honeypots simulate only a **limited number of services** and applications of a target system or network



Medium-interaction Honeypots

- ❑ These honeypots simulate a **real operating system**, applications, and services of a target network



High-interaction Honeypots

- ❑ These honeypots **simulate all services** and applications of a target network



Pure Honeypots

- ❑ These honeypots emulate the **real production network** of a target organization



Types of Honeypots (Cont'd)

Classification of honeypots based on their deployment strategy



Production Honeypots

- ❑ Are deployed inside the production network of the organization along with other production servers
- ❑ As they are deployed internally, they also help to find out internal flaws and attackers within an organization



Research Honeypots

- ❑ Are high-interaction honeypots primarily deployed by research institutes, governments, or military organizations to gain detailed knowledge about the actions of intruder

Types of Honeypots (Cont'd)



Classification of honeypots based on their deception technology



Malware Honeypots

- ☐ Are used to trap malware campaigns or malware attempts over the network infrastructure



Database Honeypots

- ☐ Employ fake databases that are vulnerable to perform database-related attacks such as SQL injection and database enumeration



Spam Honeypots

- ☐ Specifically target spammers who abuse vulnerable resources such as open mail relays and open proxies



Email Honeypots

- ☐ Fake email addresses that are specifically used to attract fake and malicious emails from adversaries



Spider Honeypots

- ☐ Specifically designed to trap web crawlers and spiders



Honeynets

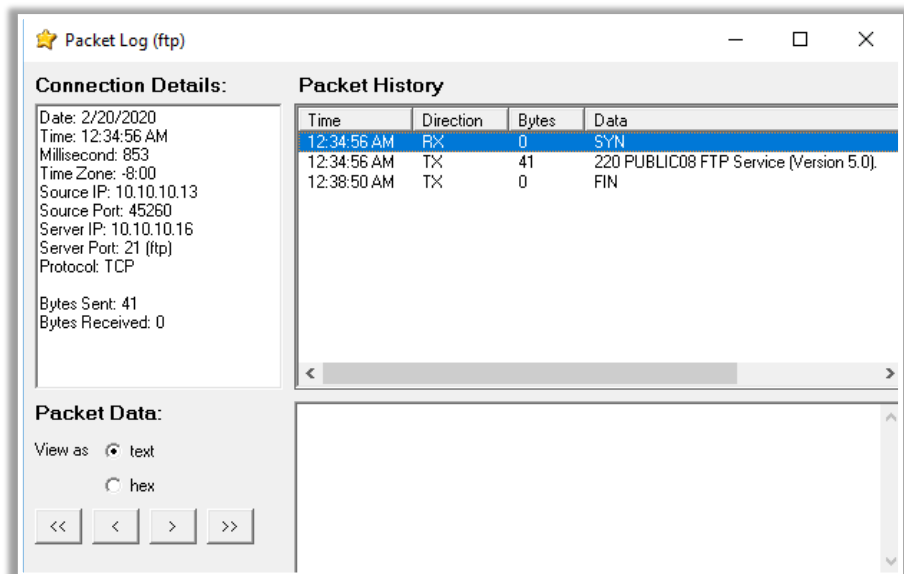
- ☐ Networks of honeypots which are very effective in determining the entire capabilities of the adversaries

HoneyPot Tools



HoneyBOT

HoneyBOT is a medium interaction honeypot for windows. It is an easy-to-use solution that is ideal for network security research



<https://www.atomicsoftwareolutions.com>



KFSensor

<http://www.keyfocus.net>



MongoDB-HoneyProxy

<https://github.com>



Modern Honey Network

<https://github.com>



ESPot

<https://github.com>



HoneyPy

<https://github.com>

Module Flow

1

**Understand Different
Types of Network
Segmentation**

2

**Understand Different
Types of Firewalls
and their Role**

3

**Understand Different
Types of IDS/IPS and
their Role**

4

**Understand Different
Types of Honeypots**

5

**Understand Different
Types of Proxy Servers
and their Benefits**

6

**Discuss Fundamentals
of VPN and its
importance in Network
Security**

7

**Discuss Security
Incident and Event
Management
(SIEM)**

8

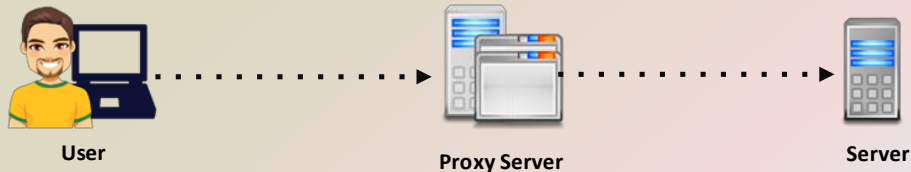
**Discuss User Behavior
Analytics (UBA)**

9

**Understand Various
Antivirus/Anti-
malware Software**

What are Proxy Servers?

- 01 A proxy server is a **dedicated computer**, or a software system virtually located between a client and the actual server
- 02 It is a **sentinel** between an internal network and the open internet
- 03 It serves **clients requests** on behalf of actual servers, thereby preventing actual servers from exposing themselves to the outside world
- 04 It provides an additional **layer of defense** to the network and can protect against certain operating system (OS) and web server specific attacks
- 05 Security professionals should deploy a proxy server to **intercept** malicious, offensive web content, computer viruses, etc., hidden in the client requests



Benefits of Proxy Server

1

Acts as a **security protector** between the user devices and a server

2

Enhances the security and **privacy of client devices**

3

Improves the **browsing speed**

4

Provides **advanced logging capabilities** for user activities

5

Controls access to specific types of restricted services

6

Hides internal IP addresses and filters requests from external sites

7

Reduces the chances of modifying cookies in the **browser configuration**

8

Enables authentication for the proxy servers before handling user requests

Functioning of a Proxy Server



01

Internal host requests to access a **web site**

02

The request enters the proxy server which examines the **header** and **packet** content based on the rule base

03

Server **reconstructs** the data packet with a **different source IP address**

04

Proxy server transmits the packet to **target address** that conceals the actual end user who made the request

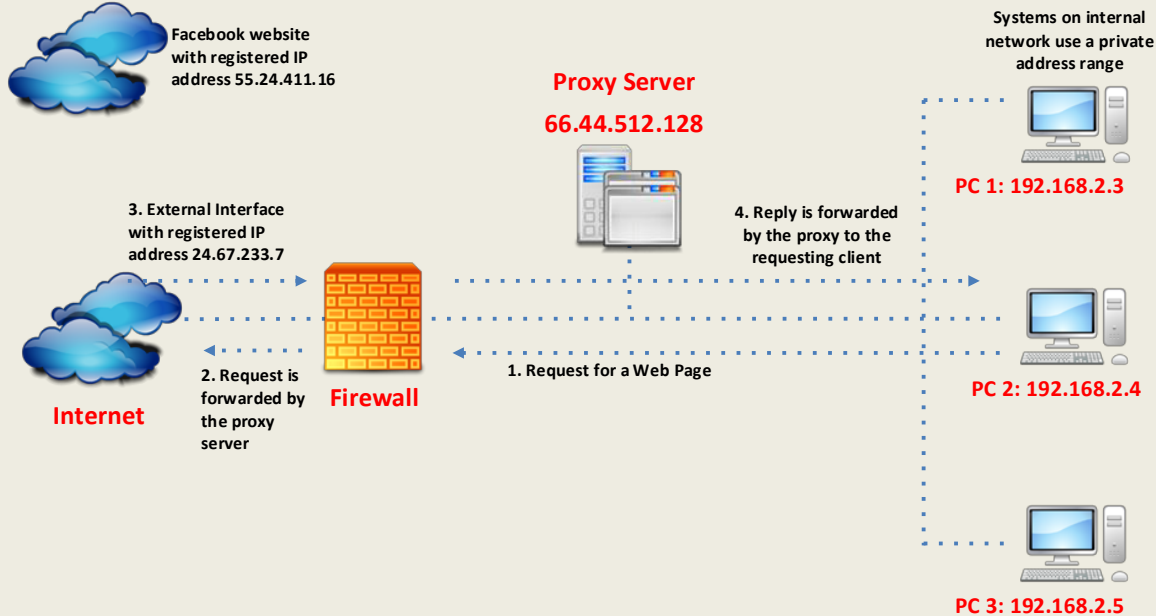
05

If the data packet is returned, it is again sent to the **proxy server** to check with the rule base

06

The returned packet is **reconstructed** by the proxy server and is sent to the source computer

Functioning of a Proxy Server (Cont'd)



Proxy Servers vs Packet Filters

Proxy Servers	Packet Filters
❑ Proxy server examines the data payload of the packet	❑ Packet filters examine the routing information of the packet
❑ Creates detailed log file listings, since they scan the entire data of IP packets	❑ Logs only the header information of the IP packets
❑ Restructures the packet with new source IP data	❑ Allows or blocks the data depending on the packet filter rules
❑ In the case of failure of a proxy server, all network communications would cease	❑ In the case of failure of a packet filter, all packets may be allowed to pass through the internal network



Types of Proxy Servers



**Transparent
Proxy**



**Non Transparent
Proxy**



SOCKS Proxy



Anonymous Proxy



Reverse Proxy



Transparent Proxy



01

A transparent proxy is a proxy through which a **client system connects** to a server without its knowledge

02

It is configured to be entirely **invisible** to an end user

03

With a transparent proxy, all the web clients must be **configured manually**

Non-transparent Proxy

- ☐ Require **client software to be configured** to use the proxy server
- ☐ The **client** is made aware of the **proxy's existence**
- ☐ They are difficult to configure, as each client program must be set up to route all requests to a single port



01

Group Annotation
Services

02

Media Type
Transformation

03

Protocol Reduction

04

Anonymity
Filtering

SOCKS Proxy

- ☐ The SOCKS is an **Internet Engineering Task Force (IETF)** standard
- ☐ It is a proxy server that does not have the special caching abilities of a caching HTTP proxy server
- ☐ The SOCKS proxy server does not allow **external network components** to collect information on the client that generated the request

The **SOCKS** package includes or contains the following components



A SOCK server for the specified operating system (OS)



A client program such as FTP, Telnet, or an Internet browser



A client library for SOCKS

Anonymous Proxy

- ❑ An anonymous proxy does not transfer information about the IP address of its user, thereby **hiding information** about the user and their **surfing interests**



Pros

- ❑ A user can surf the Internet **privately** by using an anonymous proxy
- ❑ With the help of an anonymous proxy server, a user can access even **censored websites**



Cons

- ❑ Using this type of proxy server may **decrease the speed** of loading a web page on to the browser
- ❑ Using anonymous proxy servers to **bypass Internet censorship is illegal** in some countries



Reverse Proxy

01

A reverse proxy is usually **situated closer to the server(s)** and will only return a configured set of resources

02

It can **optimize content** by compressing it to speed up loading

03

The client is **unaware of the presence** of a reverse proxy

04

A reverse proxy server is an **intermediate server** that is located between a client and the actual web server

How to Configure Proxy Server

Configuring Automatic Proxy Setup in Windows 10

Step 1

Open Windows Settings by pressing the **Windows key** and **I** together

Step 2

Click **Network & Internet** > **Proxy**

Step 3

Check if the “**Automatically detect settings**” toggle button is **On**

Step 4

Windows runs an automatic check by default

Step 5

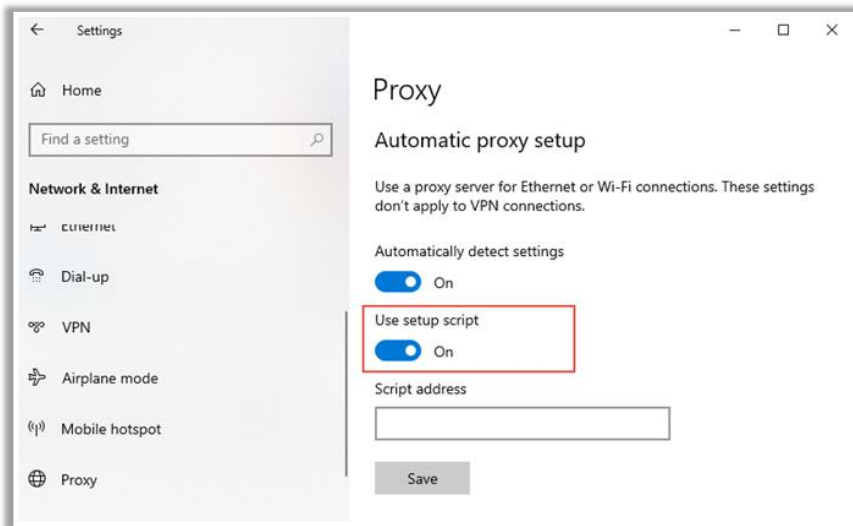
If Windows detects PAC file, set the “**Use Setup Script**” toggle button to **On**

Step 6

Type **proxy.certifiedhacker.com** in the “**Script Address**” field

Step 7

Click **Save** to implement the changes and use the Internet through the proxy



How to Configure Proxy Server (Cont'd)

Step 1

Open the Windows settings menu by pressing the **Windows key** and **I** together

Step 2

Click **Network & Internet** > **Proxy**

Step 3

Automatic proxy setup window opens. Scroll down to "**Manual proxy setup**" and set the "**Use a Proxy Server**" toggle button to **On**

Step 4

Type **proxy.certifiedhacker.com** in the address field and **8888** in the port field

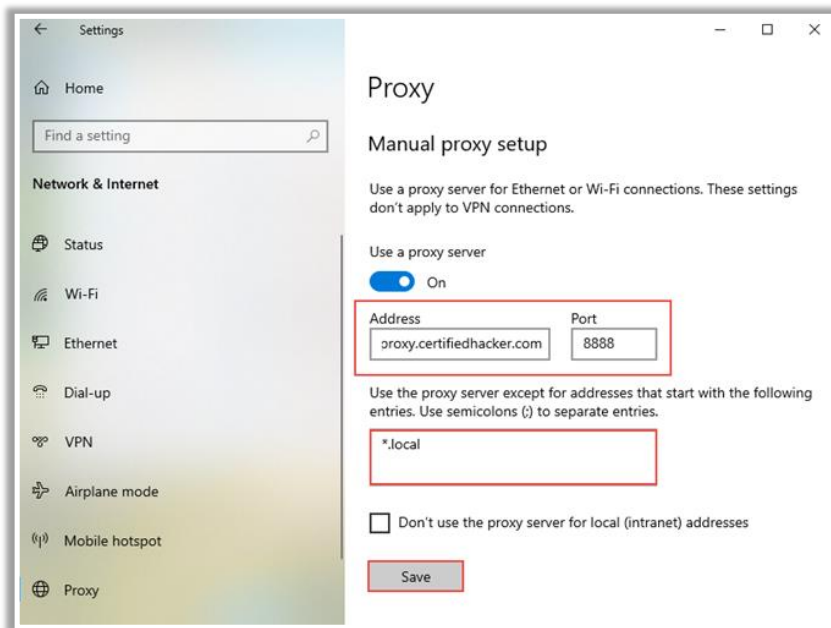
Step 5

Type ***.local** in the field below the address and port fields to exempt the use of a proxy server

Step 6

Click **Save** to implement the changes and use the proxy in Windows 10

Configuring Manual Proxy Setup in Windows 10



How to Configure Proxy Server (Cont'd)

Configuring Proxy Setup in Google Chrome

Step 1

Open the Google Chrome browser and select "**Settings**" in the toolbar

Step 2

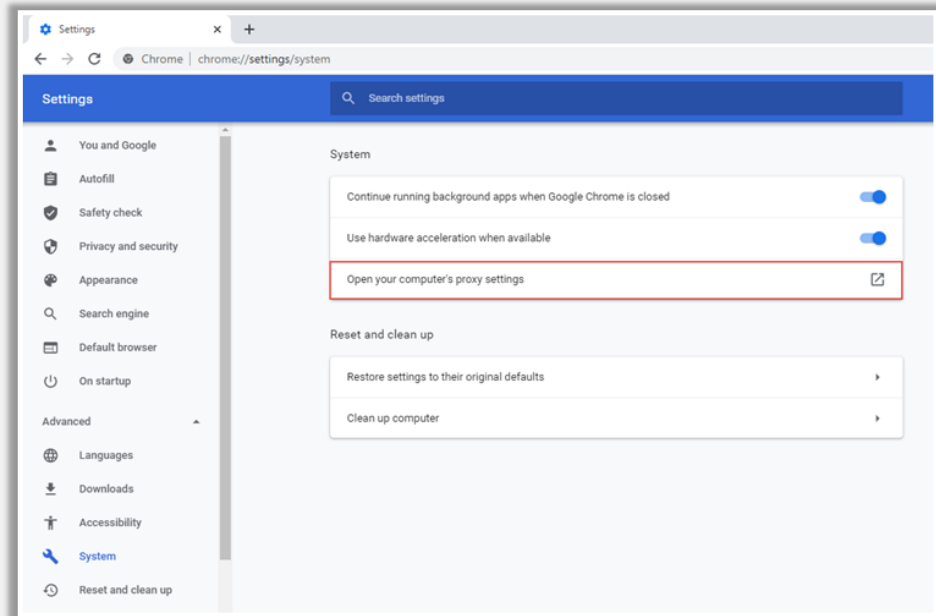
Scroll down on the page and Click **Advanced**
System

Step 3

The **System** window opens. Click "**Open your computer's proxy settings**"

Step 4

The proxy server settings window opens. Follow the instructions to configure the proxy



How to Configure Proxy Server (Cont'd)

Configuring Proxy Setup in Microsoft Edge

Step 1

Open the Microsoft Edge browser and click "**Settings**" from the menu displayed on the top-right corner

Step 3

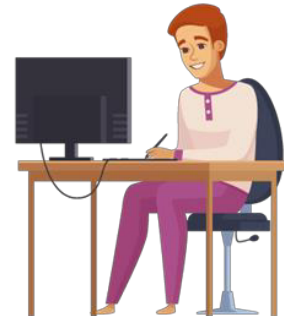
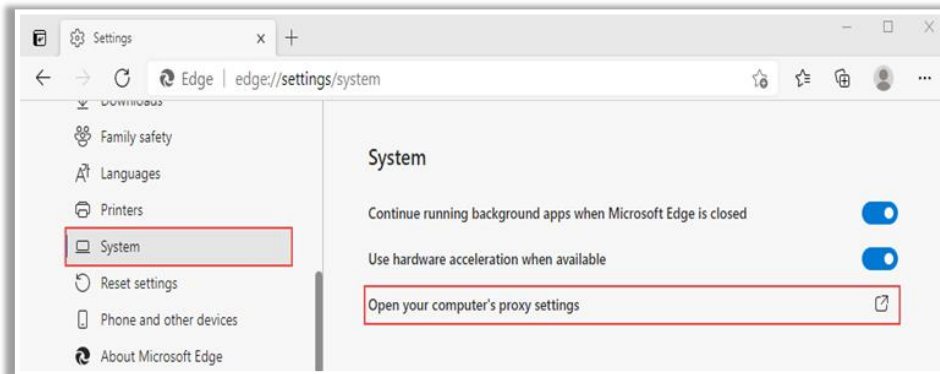
The **System** window opens. Click "**Open your computer's proxy settings**"

Step 2

Scroll down on the page and click "**System**"

Step 4

The proxy server setup window opens. Follow the instructions to configure the proxy server



Limitations of Proxy Server

1

If proxy is **not properly secured**, then it may become point of failure in an event of attack

2

Increase in workload since proxy must be configured for each and every service it provides

3

If we attempt to change the **default settings**, the proxy server might not function properly

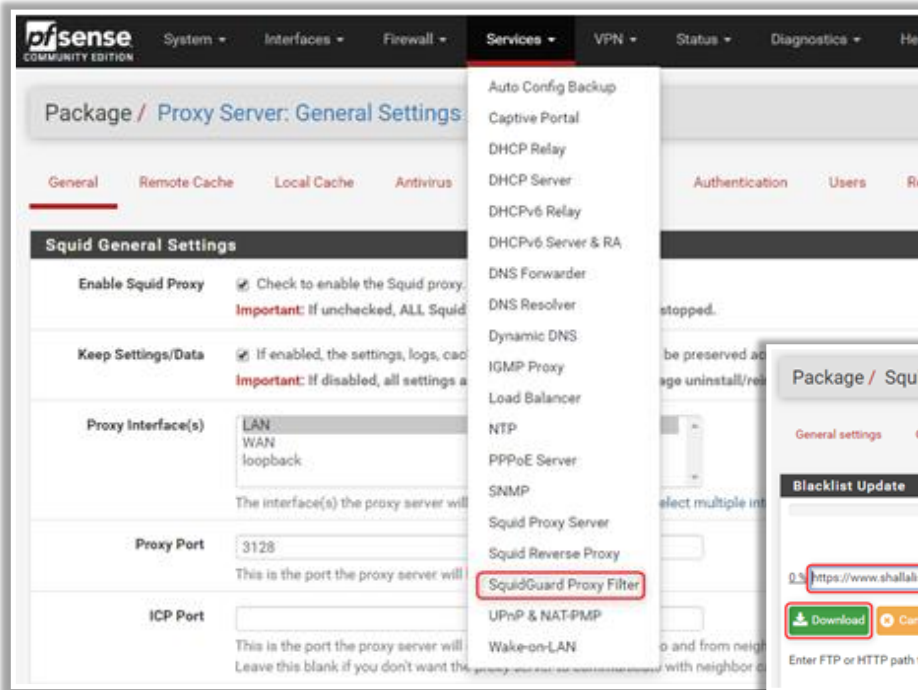
4

Proxy servers have to **reroute information**, thus web pages can sometimes load slowly

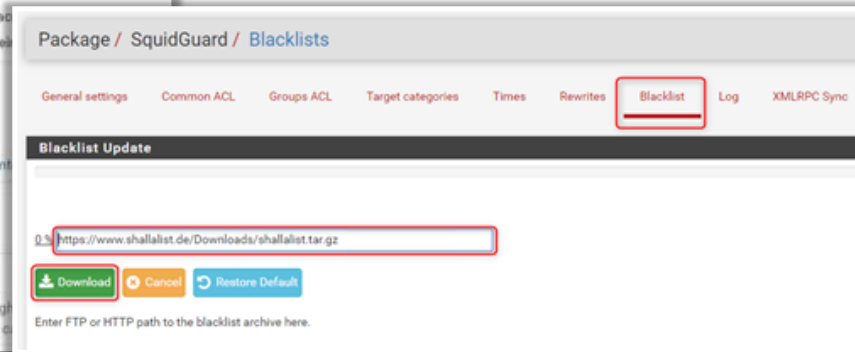
5

If the proxy server is attempting to **bypass suspicious software**, some elements of a page may not load

Example of a Proxy Server: Squid Proxy



- ☐ Squid is a **caching proxy for the web** and supports HTTP, HTTPS, FTP, and more
- ☐ It **reduces the bandwidth** and **improves the response time** by caching and reusing frequently-requested web pages



List of Proxy Tools



Whonix

<https://www.whonix.org>



Psiphon

<https://psiphon.ca>



FoxyProxy

<https://getfoxyproxy.org>



GeoSurf

<https://www.geosurf.com>



JonDo

<https://anonymous-proxy-servers.net>



Proxify

<https://proxify.com>



Guardster

<http://www.guardster.com>



Global Proxy Network

<https://infatica.io>



Anonym8

<https://github.com>



ProxySite

<https://www.proxysite.com>



ProxyCap

<https://www.proxycap.com>



CCProxy

<https://www.youngzsoft.net>



Fiddler

<https://www.telerik.com>



BlackArch Proxy

<https://blackarch.org>



Artica Proxy

<https://artica-proxy.com>