DNS Content Filtering Explained

1

When you type a website name (URL) in your browser or click a website link, your browser immediately contacts a server.

2

This is called a DNS server. Your browser sends the website name to this server over the internet.

A DNS server is like your neighborhood directory. Each home belongs to someone. To find your neighbor's home, you search the directory by his name and find his address.

The DNS server looks at the website name you sent and finds the unique IP address for the website.

3

What is an IP address? It is a unique number assigned to a device on the internet or a local network. It allows other devices to find and connect with it on the internet.

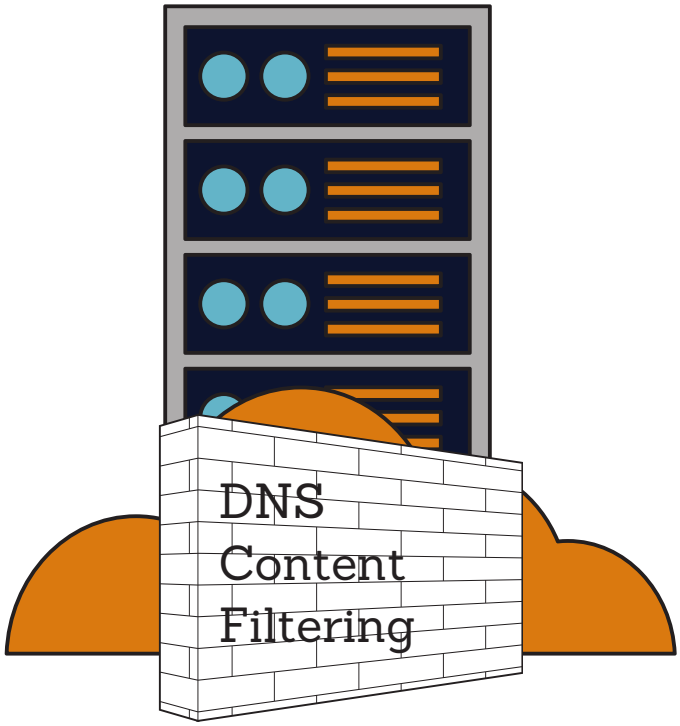
Example: You entered https://www.gohere.com. The DNS server finds this name with an IP address of 199.250.45.2. Now we know which server on the internet has (hosts) gohere.com.

If the IP address isn't found, then your browser displays a message that the website could not be found.

4

Before you can see the website's content in your browser, we need to learn more about this website. This is known as DNS content (or web) filtering.

A request to check this website is sent from the DNS server to a DNS content filtering server.



The DNS content filter server goes through a series of checks:

- Is this website on the list of known potential risk sites?
- Is it a website your company allows?
- Are you allowed to visit this site?
- Does the site contain content that is on the list of blocked categories?
- What rules has your company defined to manage website access?

When the DNS content filtering check approves your website, the content filtering server sends the IP address for your website to your browser.

The website is displayed on your browser.

If the website does not pass all the tests, then your browser displays a message that the website is not allowed.

The entire trip has been completed in a matter of milliseconds!

How Will This Help Your Company?

When someone hears website blocking, it's only natural to think of it as heavy-handed and controlling. The reality is, when properly implemented and explained to everyone, responsible internet activity becomes a positive, shared commitment.

A Few Simple Everyday Wins for Everyone

- Malware can impact the performance of your devices. Malware is continuously working in the background to find valuable information, track your activities, and send your stolen data to their internet servers.

How much time do your employees waste every day waiting for their desktops and laptops to do what they need to do?

- Malware can secretly use one of your computers to stream unacceptable content across the internet.

What would happen if one of your company's computers became the new favorite internet destination for some really unsavory content?

How Will This Help Your Company?

- Stolen email addresses and login credentials make sending unauthorized emails on behalf of your company too easy.

One often overlooked outcome with the unauthorized use of your domain is the potential for being blacklisted. This means that your entire company can be prevented from sending or receiving emails.

What would no emails mean to your day-to-day business? What would happen if you rely on e-commerce or website transactions?

- The damage that results from your company's stolen information extends far beyond your company.

Consider the immediate impact to your reputation and clients' trust. You will have to quickly let them know there has been a breach.

Your clients' data has also been compromised. The impact now reaches their customers as well. It's like a rapidly growing hurricane eye.

The benefits to your company are substantial. Employees don't intentionally do anything wrong. They just need the right knowledge and defenses. Remember --- you, not your employees, are ultimately responsible for your company's internet activities.

Tech Terms Translated Into Plain English

Blacklist:

A blacklist is a list of domains, email addresses or IP address that are blocked from internet access. These may be identified as inappropriate sites by internet servers or through users' spam reporting.

Cloud:

The cloud is the internet. It's everything you can access through the internet.

When your company is in the cloud, it means that your files and possibly the software you use to access them are stored on an internet server instead of on-premises.

Device:

In technology a device is the general term for any piece of hardware such as server, firewall, router, desktop, laptop, tablet, keyboard, mouse, monitor, camera, microphone, speakers.

These are sometimes referred to as peripherals.

Tech Terms Translated Into Plain English

DNS:

The Domain Name System (DNS) is like the master directory of the internet. It converts the website names into numbers (IP addresses). These numbers identify the internet (cloud) server on which each website resides.

Domain:

The unique name that is your company's internet address. It's the character part of the longer text you type in your search box or see in the address bar..

For example, https://www.yourcompanyname.com is the full text. The highlighted portion is the domain name.

Malware:

Malware is an abbreviation for "malicious software." It is a type of computer program designed to infect and intentionally harm a person's computer, server or network.

There are many types of malware such as viruses, Trojan horses, worms, ransomware, spyware, and keyloggers.

Tech Terms Translated Into Plain English

Server:
A piece of computer hardware or a software application that provides the functionality another piece of hardware or software needs to do its job.

Example:
A mail server sends and receives all the email from your email account. It is both a software application that knows how to handle each email and a piece of hardware where the software lives.

Ready to Learn More?

Contact Us Anytime

Quest Technology Group
315 E. Robinson Street, Suite 525
Orlando, FL 32801

407.843.6603

learning@quest-technology-group.com

www.quest-technology-group.com