UNDERSTANDING THE

WEB PROTECTION

Protection And Control Beyond The Router (Including The Possibilities Of DNS Filtering)

An Informational eBook

CORE6+

UNDERSTANDING THE

WEB PROTECTION

Protection And Control Beyond The Router (Including The Possibilities Of DNS Filtering)

An Informational eBook

Table of Contents: Web Protection & DNS Filtering

Chapter 4: A Complete, Layered Defense

- **4.1** How Web Protection and DNS Filtering Work Together
- **4.2** The Symbiotic Relationship: Two Layers of Protection for a Resilient Network
- **4.3** Seamless Protection: Safeguarding Your Users On and Off-Site

Chapter 5: Conclusion

- **5.1** A Summary of What Matters Most
- **5.2** The Peace of Mind: A Final Look at the Ultimate Benefit
- **5.3** A Strategic Advantage: How a Layered Solution Protects Your Future

---

Chapter 1: The Internet as a Double-Edged Sword

1.1 Beyond the Firewall: Why Your Users are Still Exposed Online

In today's digital world, every business, regardless of size, relies on the internet. But the internet is a double-edged sword: it is a tool for productivity and growth, and also a playground for cyber threats.

You have a firewall, a security guard at your digital front door, but that's not always enough. In today’s world, threats don’t always come knocking at the front door; they come from within, through your users. A single click on a malicious link, an email with a virus-laden attachment, or a visit to a dangerous website can bypass the firewall and compromise your entire network.

1.2 The New Threats: Why Phishing, Malware, and Dangerous Websites are a Constant Risk

The world of cyber threats has evolved beyond the simple virus. Hackers are using sophisticated methods to trick your users into giving them access to your network.

- **Phishing:** This is a scam that uses fraudulent emails to trick you into revealing personal information or clicking on a malicious link. It is one of the most common ways that hackers gain access to a network.
- **Malware:** This is a broad term for malicious software that can damage your computer or steal your data. It can be delivered through an email attachment, a website, or a malicious link.
- **Dangerous Websites:** Many websites contain hidden malware or viruses that can infect your computer just by visiting them. Even a seemingly legitimate website can be compromised and used to deliver a virus.

1.3 The Cost of the Click: What Happens When an Employee Visits a Malicious Site

The cost of a single careless click can be catastrophic for a business. The problem isn't just the time and money it takes to fix the infected computer; it's the fact that a single computer can be used as a gateway to infect your entire network.

A single click can lead to:

- **Data Breach:** An attacker can steal sensitive client information, financial records, and other valuable data.
- **Ransomware Attack:** A single infected computer can be used to encrypt all of your files and hold them hostage until you pay a ransom.
- **Operational Shutdown:** A single click can shut down your entire business, leading to weeks of downtime and lost productivity.

The reality is that your users are your greatest vulnerability. And in today’s world, a security strategy that doesn't include a comprehensive plan for protecting them when they are online is no longer a viable defense.

Chapter 2: The Solution - Web Protection

2.1 What is Web Protection? Your Network's Traffic Director

In the last chapter, we talked about how a single malicious website can pose a serious threat. **Web Protection** is your solution. Think of it as your network's traffic director, giving you granular control over all the web access and policy management for your team.

Web Protection is a security layer that acts as a safeguard for all your users while they are surfing the internet. It goes beyond a simple firewall by allowing you to set specific content-filtering policies and to create website blacklists. This is a powerful tool for improving productivity and ensuring your team is not exposed to hidden malware or other online threats.

2.2 The Power of Policy: Content-Based Filtering for Safety and Productivity

The great thing about Web Protection is that it gives you the freedom to choose your own security policy. You can block or manage your users' access to certain types of websites, or even specifically identified URLs.

For example, you could set a policy that prevents your accounting team from accessing social media sites like Facebook or Instagram during business hours. This not only protects them from the security risks that are common on these sites but also helps to improve productivity.

Web Protection offers more targeted control over the user’s web access and allowable content. It is a way of ensuring that every user on your network is on a safe and productive path.

2.3 The Time-Block Advantage: How Time-Based Policies Align with Your Business

Web Protection also gives you the power to set **time-based browsing policies**. This is a great feature for businesses that want to allow their employees to access certain websites during specific times.

For example, you could set a policy that allows your accounting team to visit Facebook and Instagram, but only from 10:00 AM to 10:30 AM, 12:00 PM to 1:00 PM, and 2:30 PM to 3:00 PM. This is a way of saying that you trust your employees, but you also want to make sure that they are being as productive as possible.

You can have as much specific control over site URLs and time-blocks per PC as you see best suits your business and users. This ensures your network bandwidth is used for business-critical functions and provides a higher level of security and control.

Chapter 3: The Add-On Solution - DNS Filtering

3.1 What is DNS Filtering? The Internet's Security Guard

To understand DNS Filtering, you first have to know what DNS is. The

Domain Name System (DNS) is like the internet's phonebook. It translates human-readable website addresses (like

google.com) into a numerical IP address that computers use to connect to those sites.

DNS Filtering is a security measure that uses this system to **block access to malicious websites** and inappropriate content online. It works by filtering the DNS request

before the site is ever reached. Think of it as a security guard who has a list of known dangerous neighborhoods. When your computer asks for directions to one of those places, the guard immediately puts up a roadblock, preventing you from ever reaching the malicious site. This is an essential first line of defense for every user on your network.

3.2 The Initial Barrier: Why Filtering Threats at the DNS Level is a Critical First Step

DNS Filtering acts as the

initial barrier, blocking access to malicious websites at the DNS level. This is a critical first step in your security because it stops threats before a user can even access them, and before the threat can reach the user's device.

For example, a user might receive a phishing email with a malicious link. Even if they were to click that link, DNS Filtering would intercept the connection request and block it. This is a crucial defense against threats that originate from malicious websites, like phishing attacks and malware. It uses AI and machine learning to identify and block threats in real-time.

3.3 The "Add-On" Advantage: Choosing to Fortify Your Network at the Core

While Web Protection provides a powerful layer of security, DNS Filtering is an **add-on** that fortifies your network at its core. It is a separate security layer that works in concert with your Web Protection to provide a more comprehensive defense.

The "Add-On" advantage is that it gives you the freedom to choose your own security policy. You can choose to fortify your network with DNS Filtering, which will provide a critical first line of defense, or you can choose to stick with Web Protection alone. DNS Filtering is a powerful tool for blocking malicious websites, but Web Protection offers a broader range of features for managing and controlling the user’s web access.

Chapter 4: A Complete, Layered Defense

4.1 How Web Protection and DNS Filtering Work Together

In today's digital world, a single security solution is not enough. The most effective security plans are built on layers of protection, with each layer designed to back up the others. Your Web Protection and DNS Filtering are two complimentary security layers that work together to enhance your overall protection.

Think of it like a security checkpoint. The

DNS Filtering is the initial barrier, blocking access to malicious websites at the DNS level. It's like a guard at the entrance who has a list of every known troublemaker. They check everyone who tries to enter and prevent the bad ones from ever getting close.

The **Web Protection**, on the other hand, is the security team inside the building. It provides more granular control over web access, including content filtering and policy management. The Web Protection can address other types of threats like inappropriate content that may have been specifically banned by the company. Together, these two layers provide a comprehensive, multi-layered defense that is much stronger than either one alone.

4.2 The Symbiotic Relationship: Two Layers of Protection for a Resilient Network

The reason these two layers are so effective is because they have a symbiotic relationship. DNS Filtering acts as the first line of defense, stopping threats before the user can access them and/or before the threat can reach the user's device. This prevents a huge number of threats from ever reaching your network.

Web Protection then offers additional and different layers of protection, allowing for more targeted control over the user’s web access and allowable content. For example, Web Protection can even monitor and/or restrict excessive bandwidth usage. This two-part approach is what creates a resilient network.

In essence, DNS Filtering is a powerful tool for blocking malicious websites, but Web Protection offers a broader range of features for managing and controlling the user's web access.

4.3 Seamless Protection: Safeguarding Your Users On and Off-Site

One of the greatest benefits of this combined security solution is that it provides seamless protection for both on-network and remote users. Whether an employee is working from the office, from a coffee shop, or from a home office, their web traffic is subject to the same security policies. The combined features enhance online security, improve productivity, and help manage internet access for all of your users.

This is a crucial point in today's mobile world. The protection is not just limited to your office; it travels with your users. The Core 6+ Web Protection and DNS Filtering can protect your users in real-time, on and off-site, with full roaming endpoint protection for Windows, MacOS, iOS, and Android. This ensures that your entire organization, and all of its devices, are protected from today's web-based threats.

Chapter 5: Conclusion

5.1 A Summary of What Matters Most

We've covered a lot of ground in this guide, moving from the dangers of the internet to the power of a layered defense. As we bring this guide to a close, let's quickly recap the most important takeaways:

1. **Your Firewall is Not Enough:** The internet is a double-edged sword. While your firewall protects you from outside threats, your users are still exposed to phishing, malware, and dangerous websites.
2. **DNS Filtering is Your Digital Security Guard:** It's a critical first line of defense that blocks access to malicious websites at the DNS level, stopping threats before a user can ever access them.
3. **Web Protection is Your Traffic Director:** It provides a broader range of features, including content filtering and policy management, that protect your users from unproductive and dangerous websites.
4. **A Layered Approach is the Most Effective:** DNS Filtering and Web Protection are two complimentary security layers that work together to enhance your overall protection.
5. **Protection Goes Beyond the Office:** This layered solution provides seamless protection for your users both on and off-site, safeguarding all of your devices.

5.2 The Peace of Mind: A Final Look at the Ultimate Benefit

The ultimate benefit of a layered Web and DNS Protection solution is the peace of mind that comes with knowing your users are safe when they're online. As a business owner or a nonprofit director, you have a partner who is proactively working to prevent a single careless click from turning into a major disruption. You can operate with the confidence that your users are on a safe and productive path.

This protection goes beyond just security. It enhances online security, improves productivity, and helps manage internet access for both on-network and remote users. It is a way of saying that you are taking your security seriously, and you are leaving nothing to chance.

5.3 A Strategic Advantage: How a Layered Solution Protects Your Future

In the end, a layered Web and DNS Protection solution is more than just a security tool; it's a strategic investment in a resilient security stance. It's a commitment to a proactive defense that protects your business from the threats of today and tomorrow. It's a way of saying that you are taking your security seriously, and you are not going to leave your business vulnerable. It's the new standard for small business and nonprofit cybersecurity.

Visit https://Core6Plus.com to learn more.

Your Strategic CyberSecurity Provider (SCP)

Core 6+ is your Strategic CyberSecurity Provider (SCP) — a partner focused exclusively on protecting your organization from today's ever-evolving cyber threats. Unlike traditional MSPs that primarily handle IT labor and computer fixes, Core 6+ delivers the world's best, proactive cybersecurity protection applications and defense tools through layered solutions like Gateway Protection, SOC-managed EDR, NOC-managed Daily Patching and Preventative Maintenance, Web Protection and DNS Filtering, Data Backups, and more. Core 6+ augments and works directly with your trusted IT support – whether that be internal staff or external contractor. Core 6+ wants to help augment your team by providing 24/7 real-time, all-the-time protection, Where You Want It Most — giving you the freedom to choose only what you need, at a price you can actually afford.

Traditional MSPs tend to - and often want to - live on one end of the service spectrum with fully "Done For You" services option, which always include high fees and retainers. Whereas, at the other end of that spectrum, where most small businesses and nonprofits are, the only option for cybersecurity protection seems to be: (Pay Way Too Much, or) "Do It Yourself" - literally leaving small businesses and nonprofits on their own, with no professional guidance, and with no real safety net.

Core 6+, as your SCP, bridges that gap. Giving organizations - of every size - the freedom to handle as much of their own IT and computer support as they want and have been doing for years. Core 6+ works with whoever your trusted IT support person is… And, if need be, Core 6+ can help you find local IT Partners to provide complete, hands-on service when needed.

With Core 6+, as your SCP, partnering with your trusted IT support you can get the perfect blend of CyberSecurity Protection, IT independence and the expert (augmented) backup support if, or whenever needed.