

# CC Computers 2019 Focus

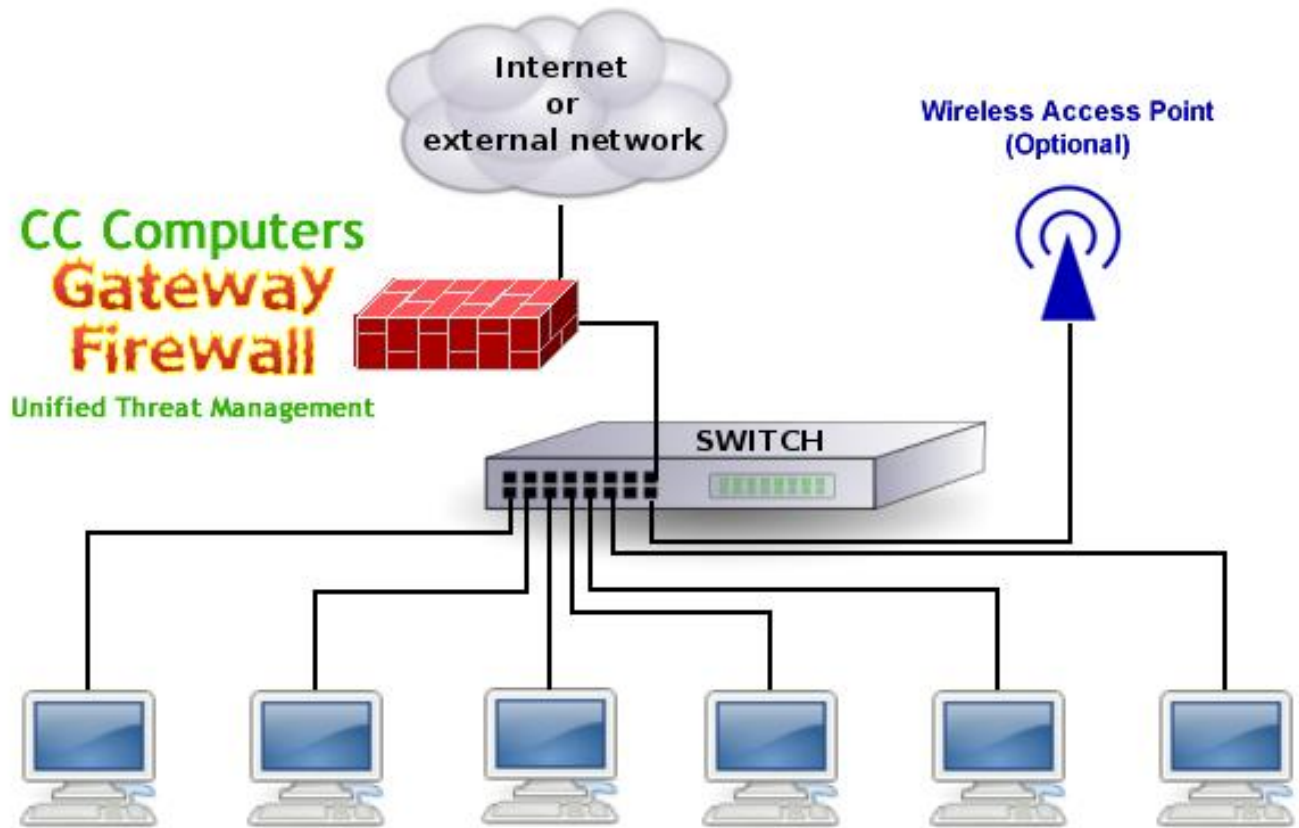


As IT specialists we evaluate the trends we have seen in technology over the last 2-3 years and decide if any of those trends involve anything we should be concerned with for our clients. This year we have determined that we need to present a better option than most of our clients have in place to combat cyber malware and cyber crime at the gateway level of their networks.

We have been seeing an uptrend of activity over the last few years, and it is past time to take actions that will help to isolate your network from cyber criminals. A gateway firewall appliance is one of the best ways to accomplish this. We will discuss with you what a firewall is, what it can do for you, and why you need it.

## What is a Gateway Firewall?

A **gateway** is a machine or appliance (think of a router) through which data packets flow. It is responsible for linking together two networks (e.g. an internal network, and an external network - The Internet). A **firewall** is a filtering system through which data packets are sent or received; the **firewall** decides to let some of the packets pass through, while it blocks or diverts others. A gateway firewall is one appliance that can do both, and is the most efficient method of deployment. The firewall portion can have many rules in place that determine what is or is not allowed to pass through the network in either direction.



## What can a Gateway Firewall do for me?

The rules that can be created and activated in the firewall are unlimited and may include such things as web content filtering either by category or individual website. Virus blocking scans are performed as well as email phishing scans, ad blocking scans, intrusion prevention, and more.

Intrusion Prevention blocks hacking attempts before they reach internal servers and desktops. Over 34,000 signature detections, including heuristic signatures for port scans, enable you to effectively monitor and block most suspicious requests.



Identity thieves are becoming increasingly sophisticated with email and website spoofs that are nearly impossible to discern from the real thing. Phish Blocker protects users from email phishing attacks and fraudulent pharming websites. Protection for SMTP protocols ensures that signatures are always current with automatic updates.

Don't wait until viruses infect your devices—block them at the gateway. Modern malware threats target servers, appliances, laptops, tablets, even mobile phones. While it is important that all of these devices have end-point protection—with the latest versions of software and virus signatures—you may struggle with control over these devices as they connect offsite to unsecured networks, then return to your network with malware onboard. You need a first line of defense.



Bad guys are working tirelessly to develop malware that they let loose on the Internet. That's why you need a team of anti-malware experts working around the clock to defend you against the latest threats. Virus Blocker leverages signatures from Bitdefender, the leader in speed and efficacy, whose threat lab experts work 24-hours a day, 365-days a year to identify emerging threats. Heuristic models provide an additional layer of protection against zero-day threats, and real-time updates with no system downtime ensure that your network is always protected. Virus Blocker identifies and blocks zero-day threats, viruses, worms, Trojan horses, botnets, unknown malware, and new infections.

Virus Blocker also does a cloud scan concurrently with the local scan. The cloud scan leverages the current threat intelligence in our partner's cloud platform and checks the known information about the file, the URL, and other metadata. If either the local scan or the cloud scan determines that a file is malicious, it is blocked.

### **What about Ransomware?**

Ransomware is malware that installs itself on your computer or server, and blocks access to your files via encryption until a ransom is paid. The most common method of ransomware distribution is by end users opening a file either from email or downloaded from a non-reputable site that has ransomware attached. The file could even come from a known or reputable source, and be infected unknowingly by the sender. Once on a workstation, ransomware can easily migrate into a server across the network affecting company data.

Our Unified Threat Management not only leverages the award winning Bitdefender cloud scans, but also ScoutIQ cloud scans. ScoutIQ is the native anti-malware cloud scanner specific found only on our partner Gateway Firewall software. It is designed specifically just for the purpose of combating ransomware. If that isn't enough protection, we also activate a third scanner which utilizes CLAM Anti Virus scanning signatures for detecting malware.

All three scanners run concurrently looking for anything that tries to infiltrate your systems. As we may have already mentioned, stacking protection is always the best defense against malware and malicious activity software. We feel that having all of these protection products constantly working for you is your best defense against future ransomware.



Eliminate annoying advertisements and decrease page load times with Ad Blocker. AD Blocker lets you easily block ads at the gateway without installing browser plugins. Prevent malware and scam links through banner ads while reducing traffic on the network.

Application Control helps you wrangle productivity drains, bandwidth hogs and protocol-agile apps used for filter bypass. Make sure that your users can access mission-critical, cloud-based apps (like CRM, ERP) while keeping recreational or inappropriate apps off the network.

Application Control performs deep packet (DPI) and deep flow (DFI) inspection of network traffic, enabling it to accurately identify thousands of common applications such as social networking, P2P, instant messaging, video streaming, file sharing, enterprise applications and much more. We help you determine anything you want to stop, and Application Control will take care of the rest.


Web Filter can block porn, gambling, videos, social networks, shopping sites and other inappropriate content or applications from entering your network. If users turn off safe search, you can have Web Filter turn it right back on, automatically. Just as Application Control manages access based on the application type, Web Filter manages access based on the type of content on the site.

The screenshot shows a dark grey web page with the following content:


**CC Computers Gateway Firewall**  
Unified Threat Management

---

**Web Filter**

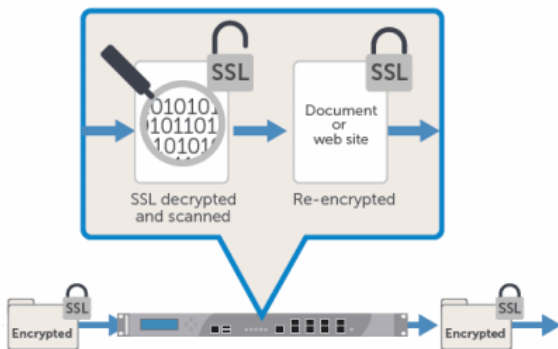
 **This web page is blocked because it violates network policy.**  
If you have any questions, Please contact [CC Computers - 618-252-0914](tel:618-252-0914).

---

 **Host:** www.pornhub.com  
**URL:** http://www.pornhub.com/  
**Reason:** Pornography - Web pages which contain images or videos depicting sexual acts, sexual arousal, or explicit nude imagery intended to be sexual in nature.

There are more than 1 billion websites on the Internet, so how can you realistically evaluate each one to filter out offensive or inappropriate content? No worries, we do that for you! Flexible access can also be allowed based on user groups by combining Web Filter with Policy Manager. Allowing access to inappropriate content can reduce productivity, create distractions or even lead to legal action. Web Filter is a fast, easy, and effective way to ensure that your users are not abusing your network use policies.

More and more Internet traffic is being encrypted using HTTPS, which creates a huge blind spot for firewalls. It compromises their ability to analyze traffic, identify threats or handle policy violations.



SSL Inspector solves this problem. Whether it is driven by concerns about personal privacy, or the rise of web applications like Salesforce, Netflix and Facebook, the amount of encrypted Internet traffic has exploded. SSL Inspector puts our Firewall in the middle of the encrypted traffic, with the ability to decrypt and analyze the data as it passes through.

SSL Inspector creates a specialized certificate on each client. This certificate communicates directly with the gateway which is then able to decrypt HTTPS and SMTP traffic, process, and re-encrypt it on the fly all from within our Firewall—without ever exposing the decrypted traffic to the network. This enables HTTPS traffic to be inspected in the same way as regular HTTP traffic, meaning that all our Firewall apps and their rules can be applied.

## Why do I need a Gateway Firewall?

More than likely, the only thing between your workstations and the internet is whatever anti-malware software you have installed on those machines. While that is a necessary part of any cyber security program, do you know for a fact right this moment if all those machines currently have that software in place? Do you also know if any user has turned off or disabled that protection for some reason? Do you know if each machine has software definitions that are up to date for that software? Do you know when the software scanned for infections last, or when it trapped malicious activity last?

If you answered NO to most of those questions, do not be alarmed as most of our clients will fall into that category. Unless you have an IT department that works FULL TIME you could not possibly be expected to know those things. Our clients are all small or medium sized businesses that simply do not have resources for full time IT people.

Besides not being able to constantly monitor individual anti malware installations, having just one line of defense these days just simply not enough. If a threat reaches just one workstation it has already infiltrated your network. It may or may not be malicious, but why let it penetrate your network in the first place if it can be stopped at the door? By stacking protection with a gateway defense and individual workstation defense your chances of surviving a serious attack are greatly increased.

Think of your Gateway Firewall as a fortress. Would you rather have your enemies on the outside of the fortress walls, or on the inside? It becomes much more difficult to fight them once they are on the inside.

The firewall also has extensive reporting features. Not only can we monitor your firewall remotely, but we can make any necessary changes and see if there are any unusual activity that needs attention. Reporting can isolate issues to an individual machine on your network and allow us to take any appropriate actions.

Here are some key reasons why you would benefit from a Gateway Firewall:

1. You can't monitor your whole network, but your firewall can
2. We can monitor your firewall remotely and alert you to any issues
3. The Gateway Firewall can't be turned off or disabled like local WS protection
4. A high percentage of threats can be stopped at the door before entering your network
5. Gateway Firewall appliance software is automatically kept up to date against new threats
6. Firewall filtering can increase productivity and decrease necessary bandwidth
7. A Gateway Firewall increases your compliance with data security protection policies

## About our Partner

There are many companies out there that offer a wide range of firewall appliances and software protection. Those companies range from offerings to end user to the largest of corporate settings requiring high end firewall capabilities and management. After reviewing and testing several of these, we have chosen to partner with a company called Untangle.



Untangle has been around since 2003 and their product offerings have evolved as changes in technology demand increased security. The last several years Untangle has shown steady growth. We chose Untangle because they focus on small & medium size businesses and understand the special needs of those businesses because of the lack of full time IT security departments.

We wanted a company that understands those needs as we do, and offers a product appropriate for that setting with the security of corporate level performance. We wanted a company that has exceptional customer service as well as a superb product. We wanted a company that offers flexible deployment options. Finally, we wanted a company that communicates well with its customers and has an efficient platform to monitor and administer their product.

After testing products and talking with several companies, we found that only Untangle met all those criteria. While we could make other products 'fit' in small & medium business settings, Untangle makes a product FOR small and medium business. Our faith and confidence in Untangle is why we trust them to protect our own business with a product exactly like what we recommend to you.

## **What about cost?**

We will provide you with a quote that will include both an appliance and the Untangle software that will run on that appliance. The software cost is based on the number of users on your network, and which services are needed to effectively protect your particular network. The advanced features that secure your network most effectively are subscription based, which is the same model used on other business and enterprise class firewall protection programs.

A subscription based program insures that your appliance stays up to date with the latest technology and definitions to protect your network. An unmanaged and outdated program and appliance lends itself to weakened security for your business. There simply are NO free options that will do what this Gateway Firewall system will do for you. If someone suggests otherwise, they simply do NOT have all their facts together.

## **What we, CC Computers, specifically do for you**

We provide you with a quote that will include the cost of the appliance and software for the first year. We will also provide you with a proposed schedule to help you budget the cost of renewal for subsequent years. There are discounts for multiple year renewals, and will give you an idea of savings.

If you decide to go forward, we will install your Firewall, which replaces your current router, and configure it with the settings we agree on based on your individual business needs. If you currently have a wireless router and need wireless, we will reconfigure your current router to be a wireless access point that runs under your new firewall. Installation normally takes less than an hour, so there is minimal downtime. Once installed, we help you test your network to make sure everything works as expected. Adjustments are easily made later, which we can do remotely without having to come to your location.

We will monitor reports at regular intervals to check for alerts or potential issues within your network. We see daily reports via email, and investigate any issue that is particularly alarming. Subscription renewals will be taken care of by our office, at your direction, so your network does not have any protection lapse.

Thank you for taking the time to consider us for your cyber security needs. We look forward to becoming your partner in the effort to stop cyber security breaches and criminals.