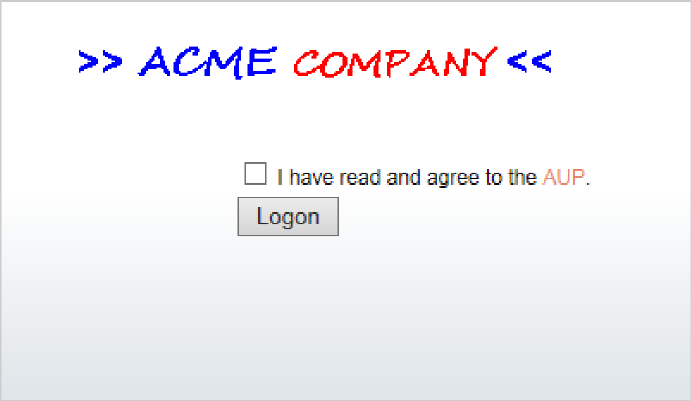
Wavecrest

Securing Your Guest Network

Introduction

Have you recently logged on to a public Wi-Fi network in a hotel, a coffee shop, an airport, or another venue that offers free Internet access? If so, you may have seen a logon page otherwise known as a captive portal page. It looks like a regular Web page, and most people click through the logon process without giving it much thought. But there are some important aspects to a captive portal that organizations need to understand if they are the ones offering free wireless guest access.

When a user first logs on to a network with a captive portal, a Web page is presented that requires certain actions before Internet access is granted. A simple captive portal forces the user to at least look at, if not read, an Acceptable Use Policy (AUP) page, and then click or tap a button indicating agreement to the terms of the policy. The captive portal page is customizable, which allows for organizations to add their company logo and own message or policy text to the logon page.



>> ACME COMPANY <<

□ I have read and agree to the AUP.

Captive Portal Page

A captive portal provides the ability to set day and time limits to the guest access so that they automatically expire after a certain amount of time. Organizations do not want to give guest users indefinite access because they will then be able to log on whenever they want. With a captive portal, IT administrators can track and report on guest account activity. They can get high-level usage and trend reports along with detailed reports to meet management requirements.

In some organizations, usage reports on where the Web traffic is coming from in the network, that is, wired or wireless, reveal that more than 75% of all Internet bandwidth being consumed is from wireless users. This may be true in college systems and hospitals that have a large number of mobile device users, but similar trends have been seen in the enterprise and even retail environment.

Many times, small businesses or even hospitals will provide their guests with free access to their wireless networks without using a captive portal solution. This can have many negative consequences for both their guest users and their business. From legal issues to your bottom line, implementing a captive portal should be a fundamental part of your overall business strategy.

Benefits of a Captive Portal

The benefits of a captive portal are many and include the ability to monitor unmanaged devices, implement bandwidth throttling, separate Web traffic, and reduce legal liability.

With free guest access, your guests' unmanaged devices are completely in their control, and the enterprise is unable to enforce any device policies. This means no configuration profiles to enforce device settings increasing the probability of security threats. For instance, smartphones can be infected by malware from personal e-mail accounts over the cellular connection and then forward the contents inside the network through the internal wireless connection. A captive portal can block this security threat as well as other inappropriate Web use to protect the network.

Even when a simple captive portal is used in a free public network, certain individuals may repeatedly connect, using the network on an almost continuous basis to download music, videos, or other large files. This activity, called bandwidth hogging, can be minimized by managing bandwidth using the captive portal. Bandwidth throttling can control the speed at which large files are downloaded, limit the size of files that can be downloaded, or block connections to cloud apps commonly used for downloading large files.

A captive portal allows for the separation of guest traffic from corporate traffic. This has tons of security benefits including keeping untrusted users away from confidential resources. Guest users should have limited access inside the corporate network. To ensure the health and well-being of the corporate network as well as the security of the organization's information assets, it is imperative to restrict guest access.

Providing free Internet service does not mean that you are always providing secure Internet service. An AUP on your captive portal ensures that users understand just that. It can contain a statement outlining the conditions that guests must agree to before they are granted access to the Wi-Fi network. This relieves your company of some of the liability if a guest user is the offender or victim of illegal activity on your Wi-Fi network.

To help secure your guest network, Wavecrest offers CyBlock Appliance—a turnkey, Web-security hardware solution that blocks Web sites, malware, IM, P2P, streaming, file sharing, and more. Some of the product's features are summarized below.

The CyBlock Appliance Approach

Advanced Web Filtering

With 70-plus standard content categories including cloud service categories and an unlimited number of custom categories, CyBlock Appliance provides threat protection for your guest network. IT administrators are able to block malicious Web sites as well as cloud applications and services that threaten the health of the corporate network.

Direct Traffic Management

With CyBlock Appliance inline in your network, you can filter all Web traffic flowing through both private and public Wi-Fi networks, that is, monitor managed as well as unmanaged devices. With the Direct Traffic feature enabled, policy settings can be applied to all direct traffic including guest network traffic. The proxy will see all Web traffic regardless if a proxy port is set in the browser. This is a necessary feature to redirect traffic from unmanaged devices in your guest network in order for the proxy to monitor and filter the Web traffic.

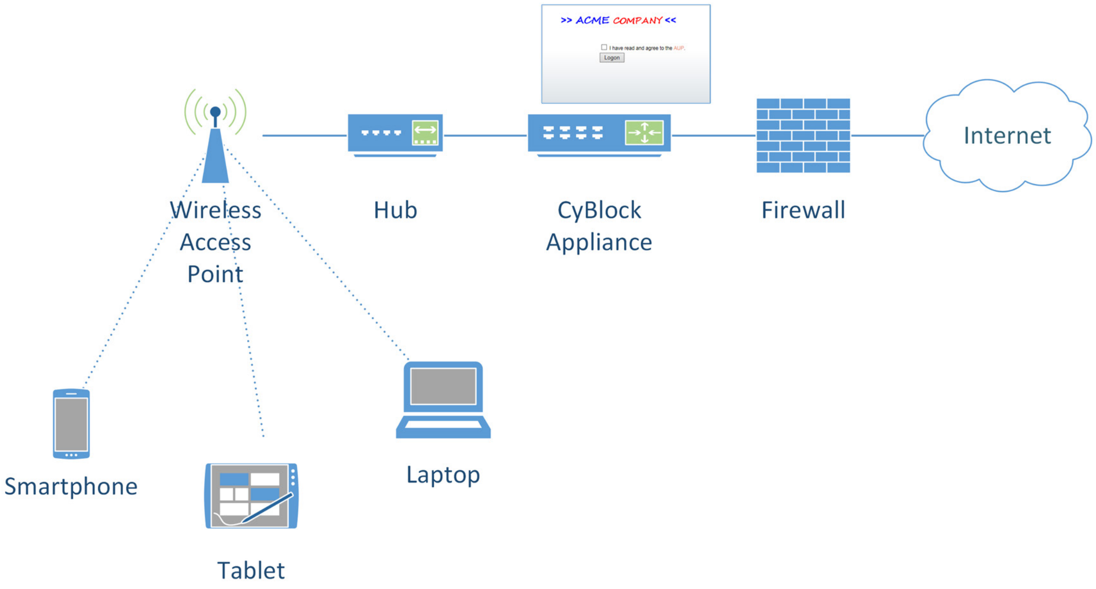
Bandwidth Management

With CyBlock's Bandwidth Management feature, IT administrators can throttle guest network traffic by content category or group to optimize bandwidth usage, keeping important business operations running smoothly for the organization. A cloud service category detected as hogging bandwidth, such as Video

Streaming or Audio Streaming, can be blocked, or its bandwidth can be capped, limiting noncritical data usage. With tiered-threshold capability, the enterprise is able to implement several policies being as restrictive as necessary based on the amount of bandwidth being consumed.

User Authentication

Using a captive portal with CyBlock Appliance, guests are identified with a guest ID. The captive portal can be set up so that guests can access the corporate network by accepting the AUP. A wider range of devices in the organization, such as laptops, tablets, and smartphones, can be supported. With AUP Only authentication, guests will not be prompted to accept the AUP again until one hour after idle time or one day from AUP acceptance. The captive portal supports authenticating users who are filtered in transparent proxy mode as mentioned earlier with CyBlock Appliance inline.



Captive Portal in Your Guest Network With CyBlock Appliance

Summary

With its easy setup, a captive portal is a feasible solution to secure your organization's guest network. A captive portal works well for users who want to access your guest network with devices, such as laptops, tablets, and smartphones. It requires guest users to accept an AUP before they can browse the Internet. A good captive portal has the ability to provide a myriad of benefits to your guest network, such as monitoring unmanaged devices, throttling bandwidth, reducing legal liability, and much more.

CyBlock Appliance minimizes the complexity of delivering guest access to the Internet for a broad range of mobile devices, helping to increase the productivity of both guest users and IT staff. CyBlock Appliance may be just the solution you need in deploying or updating your captive portal to secure your wireless guest network.

About Wavecrest Computing

Since 1996, Wavecrest Computing has provided business and government clients with reliable, accurate employee Web-access security, monitoring, and analytics solutions. IT specialists, HR professionals, and business managers trust Wavecrest's Cyfin and CyBlock products to manage employee Internet usage with today's distributed workforce in mind–monitoring VPN use, following roaming and remote users, managing and monitoring Web usage for hybrid work environments, comprehensive reporting on Microsoft 365 use, and more. Focused on our customer's needs–reducing liability risks, improving productivity, managing cloud services, saving bandwidth, and controlling costs.

Wavecrest has clients worldwide, including Canadian National Railway, Johns Hopkins, Goodyear, USPS Office of Inspector General, Chevron, Health Choice Network, and a growing list of enterprises and government agencies. For more information on our company, products, and partners,visit www.wavecrest.net.

Wavecrest

Wavecrest Computing
904 East New Haven Avenue
Melbourne, FL 32901
toll-free: 877-442-9346
voice: 321-953-5351

All specifications subject to change without notice.