

Adirondack Internet

/Public Access

Visitor Internet Systems

Security and Liability Considerations

Summary

Providing public Internet access opens a provider to multiple security issues, potential theft of service, and liability for negligence if the network is abused by end users.

As with any Internet service provider, a public access service requires implementation of common sense safeguards at a minimum. Additional management functions can mitigate charges of negligence, and assist law enforcement with investigating network abuse originating from a provider's network.

Minimum Provider Responsibilities

Connection Provider Permission

Before offering public access through another providers Internet connection, be sure such usage is permitted by the upstream provider. Most residential service offerings specifically prohibit the sharing of a residential connection, especially Wi-Fi connections that extend beyond the property.

In most cases a commercial service offering is required at greater expense, and may still include limitations regarding extending service beyond the property. Carefully review the contract terms and upstream provider Acceptable Use Policy (AUP) to avoid termination of service or criminal theft of service charges.

Acceptable Use Policy and End User Acknowledgment

Whether free or paid, all public Internet access providers include a legally binding Acceptable Use Policy (AUP). The AUP should at a minimum include all elements of the upstream provider's AUP.

The AUP is often presented as an initial screen before Internet access is enabled, requiring the end user to accept the terms before using the service. This is a function of the gateway hardware. Alternatively a copy of the AUP may be provided for the end user's signature; or at a minimum posted in one or more conspicuous location(s) on the premises.

Egress Filtering

Prevents outbound connections and denial-of-service attacks which make use of spoofed source addresses. Only legitimate local addresses are permitted egress to the Internet.

Basic Provider Functions

Public / Private Network Isolation

Under no circumstances should the private network be accessible from the public access network. Any path from public to private networks, including default routes, can result in compromise of private computers and data contained therein.

The reverse is also true. The public access network should not be accessible from the private network. Any path from private to the public access networks, including default routes, can result in compromise of end user machines. Such compromise of public end user machines from the private network is clearly negligent, and may serve as the basis for liability claims.

End User Identity Management

Public access Hot Spots that allow anonymous connections are the preferred connection points for launching attacks on other networks; releasing malicious code into the wild; unlawfully sharing copyrighted material; originating UCE (spam); and other criminal communications.

All professionally configured public access networks include some form of end user identity management. The mechanisms may be as simple as a recording end user MAC addresses; a hotel providing a name and password while recording the data in a guest folio; or authentication using credit card authorization.

The more obvious and detailed the identification method, the less desirable the public network is to those that would use it for illegal activities.

Network Usage Records and Audit Trails

A public access Internet provider is responsible for all network activity originating from their connection. If such activity violates the upstream provider's AUP the connection may be terminated without warning.

Additionally, unlawful activity may be traced back to the originating public IP address, and in turn the public access provider. In those situations the provider may be asked, or instructed by court order, to provide documentation and records identifying the users of the service at a particular time.

Generally providers maintain such records for a minimum of thirty days. The records may take the form of syslog entries, RADIUS accounting records, and/or firewall logs. Maintaining such records aids law enforcement investigations; and as they are common practice also mitigate claims of negligence.