LANCOM Techpaper
Public Spot

Die Aufgabe eines Public Spots ist es, den Internet-Zugang in einem Umfeld mit temporären Nutzern zu kontrollieren. Ein typisches Beispiel ist ein WLAN, welches jedem Client eine direkte Verbindung ins Internet ermöglichen würde. Um dies zu unterbinden und den Zugang zu kontrollieren, wird ein Public Spot eingesetzt, an dem sich Anwender erst authentifizieren müssen, bevor sie den Internetzugang nutzen können.

Anwendungsbereiche

Es gibt diverse Szenarien, in denen ein Public Spot eingesetzt werden kann. Hotels sind ein typisches Beispiel, hier möchte der Hotelbetreiber seinen Gästen einen zeitlich abhängigen Zugang zum Internet ermöglichen und auch entsprechend abrechnen. Allerdings möchte er auch sicherstellen, dass keine anderen Personen den Zugang nutzen können. Ein weiteres Beispiel ist ein Unternehmen, das seinen Besuchern über WLAN den Zugang zum Internet ermöglichen will, aber auch sicherstellen möchte, dass nicht jeder den Zugang nutzen kann. Hierbei ist auch zu beachten, dass die Einsatzmöglichkeiten der Public Spot Option auch davon abhängen, auf welchem Gerät sie freigeschaltet wurde. Wird sie auf einem einzelnen Access Point genutzt (Abb. 1), kann der Public Spot lediglich den

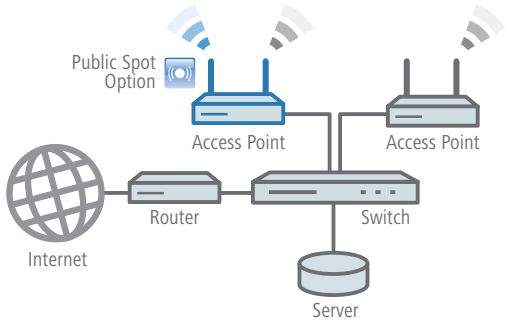

Abb. 1: Access Point mit Public Spot Option

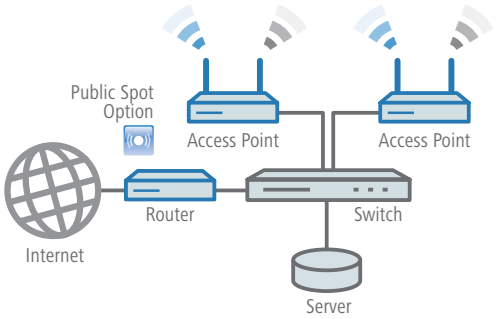

Abb. 2: Router mit Public Spot Option

Zugang der WLAN-Clients kontrollieren, die sich auf diesem Access Point anmelden. Im Gegensatz hierzu können ein Router (Abb. 2), Central Site Gateway und WLAN-Controller ein ganzes IP-Netzwerk inklusive mehrerer Access Points und deren WLAN-Clients oder Ethernet-Clients durch den Public Spot authentifizieren. Mit einem WLAN-Controller (Abb. 3) können zusätzlich die einzelnen Access Points des

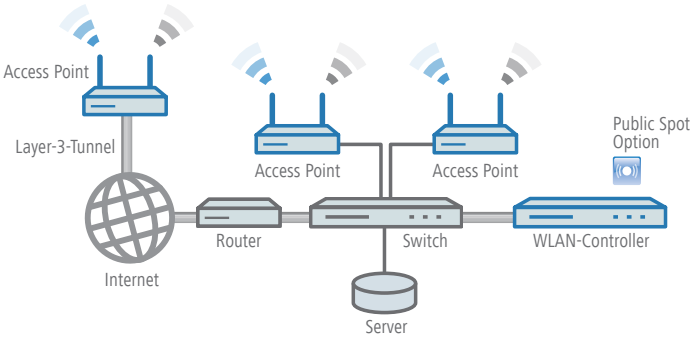

Abb. 3: WLAN-Controller mit Public Spot Option

LANCOM Systems

Netzwerkes verwaltet werden, hierbei verteilt der WLAN-Controller die nötigen Konfigurationsparameter an Access Points, so dass keine Konfiguration der einzelnen Geräte notwendig ist. Zudem kann mit Hilfe von Layer-3-Tunneling der Public Spot auch über WAN-Grenzen hinweg eingesetzt werden.

Sicherheit

Das Thema Sicherheit lässt sich beim Public Spot in vier Untergruppen aufteilen, die Trennung des Public Spot-Netzwerks vom internen Netzwerk, Authentifizierung, Authorisierung und Accounting (AAA).

Der erste wichtige Punkt zum Thema Sicherheit ist die Separierung des Public Spots von anderen internen Diensten und Daten. Eine entsprechende Trennung kann über VLANs (Virtual Local Area Networks) erreicht werden, so dass die bestehende Infrastruktur weiterhin genutzt werden kann. Das VLAN selbst wird dabei, wie die Bezeichnung sagt, als eigenes virtuelles LAN behandelt, inklusive eines eigenen IP-Adressbereiches, eine direkte Kommunikation zwischen den einzelnen VLANs ist nicht möglich. Eine weitere Möglichkeit die Netze zu trennen besteht im Layer-3-Tunneling. Hierbei kann eine SSID an einem Access Point in einen Layer-3-Tunnel geleitet werden; dies bewirkt, dass die Daten nicht direkt am Access Point in ein VLAN geschoben werden, sondern erst am WLAN-Controller, der für diese Methode notwendig ist. Der Vorteil ist, dass die Netzwerkstruktur erst vom WLAN-Controller an VLAN-fähig sein muss und auch eine bestehende VLAN-Konfiguration zwischen Access Point und WLAN-Controller keiner erneuten Konfiguration bedarf. Diese Art der Konfiguration ermöglicht es auch den Public Spot über diverse WAN-Verbindungen bereitzustellen, vorausgesetzt der Access Point kann ein Profil vom WLAN-Controller beziehen. Für die Authentisierung am Public Spot gibt es unterschiedliche Methoden. Die gängige Methode nutzt Benutzername und Kennwort zur Authentisierung am Public Spot. Hier muss der Benutzer zum Nutzen des Internets die erhaltenen Zugangsdaten zunächst in einem Web-Login eingeben, bevor das Internet zugänglich ist. Diese Login-Webseite kann nach Belieben vom Betreiber angepasst werden, um zum Beispiel die AGB zur Nutzung des Hotspots anzuzeigen. Die Option, eine Authentifizierung durch Benutzername, Kennwort und MAC-Adresse durchzuführen, wird nur selten eingesetzt, hauptsächlich wenn die Zugangsdaten auch an ein bestimmtes Endgerät gekoppelt werden sollen. Die notwendigen Daten zur Authentifizierung liegen entweder auf einem externen oder auf dem internen RADIUS-Server des Gerätes. Die Anmeldung selbst läuft über einen Browser in HTTPS ab um die Sicherheit zu gewährleisten, dass Benutzerinformationen nicht mitgeschnitten und missbraucht werden können.

Der Betreiber des Hotspots kann bei der Definition des Zeitrahmens festlegen, ob die Zugangsberechtigung für einen gewissen Zeitraum nach der ersten Aktivierung gültig ist oder inkrementell von einem Zeitbudget abgebaut wird (Abb. 4). Der Zeitrahmen und die Zugangsdaten können einfach in Form einen Vouchers ausgedruckt und an den Kunden herausgegeben werden. Zudem ist es möglich, eine interne und beliebig viele externe Webseiten in einem sogenannten „Walled Garden“ anzubieten, für die keine Authentifikation am Public Spot nötig ist. So kann zum

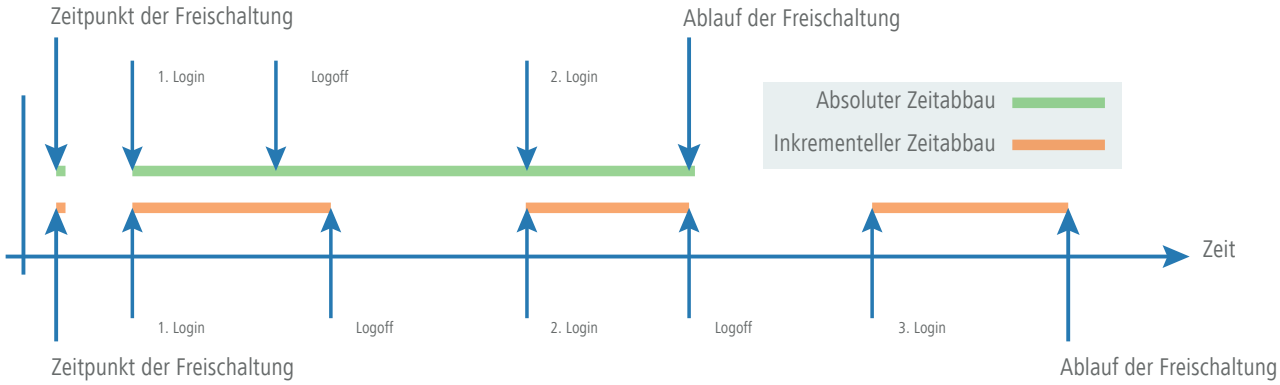

Abb. 4: Absolute und inkrementelle Internet Zugangsbeschränkung

Beispiel ein Hotel die Webseiten für Sehenswürdigkeiten, zu denen es Ausflüge anbietet, freischalten.

Protokollierung und Filterung

Zusätzlich können sowohl Login als auch Logout eines Benutzers im Public Spot protokolliert werden. Hierbei wird auch die MAC-Adresse beim Login gespeichert. Desweiteren kann der Start jeder IP-Session protokolliert werden. Diese Informationen können über SYSLOG ausgegeben werden.

Eine weitere Maßnahme ist das Filtern des Angebots im Internet. Hier kann auf zwei verschiedene Mechanismen zurückgegriffen werden. Zum einen die Stateful Inspection Firewall, in der unter anderem Ports geblockt werden können, um so die Verbindung zu gewissen Diensten zu unterbinden, und zum anderen kann ein optionaler Content Filter eingesetzt werden um durch Kategorieprofile den Zugriff auf Webseiten zu kontrollieren (HTTP und HTTPS).

Fazit

Der Public Spot ist eine vielseitige und sichere Lösung für Szenarien, in denen Gästen oder Kunden ein temporärer Internetzugang zur Verfügung gestellt werden soll, sei es über Funk oder Kabel.