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 anmelden müssen, bevor sie den Internetzugang nutzen können.

Anwendungsbereiche

Es gibt diverse Szenarien, in denen ein Public Spot eingesetzt werden kann. Ein typisches Beispiel sind Hotels. Hier möchte der Hotelbetreiber seinen Gästen einen zeitlich befristeten Zugang zum Internet ermöglichen und auch unter Umständen 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.

Die Einsatzmöglichkeiten der LANCOM Public Spot Option sind davon abhängig, auf welchem Gerät sie freigeschaltet wurde. Wird sie auf einem einzelnen Access Point genutzt (Abb. 1), kann der Public Spot lediglich den Zugang der WLAN-Clients kontrollieren, die sich auf diesem Access Point anmelden. Im Gegensatz hierzu sind Router (Abb. 2), Central Site Gateways und WLAN-Controller in der Lage, ein ganzes IP-Netzwerk inklusive mehrerer Access Points und deren WLAN- oder Ethernet-Clients durch den Public Spot zu authentifizieren. Mit einem WLAN-Controller (Abb. 3) können zusätzlich die einzelnen Access Points des Netzwerkes verwaltet werden. Hierbei verteilt der WLAN-Controller die nötigen Konfigurationsparameter an die Access Points, so dass diese nicht separat konfiguriert werden müssen.

Zudem kann mit Hilfe von Layer-3-Tunneling der Public Spot auch über WAN-Grenzen hinweg eingesetzt werden. Informationen zum Layer-3-Tunneling finden Sie im LCOS Referenzhandbuch, welches Sie kostenlos auf der LANCOM Webseite herunterladen können.

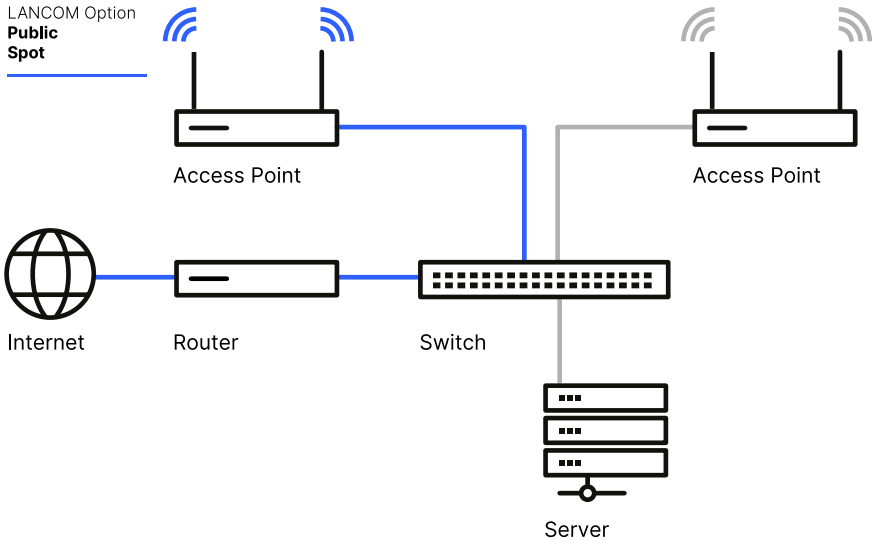

Abbildung 1:
Access Point mit
Public Spot Option

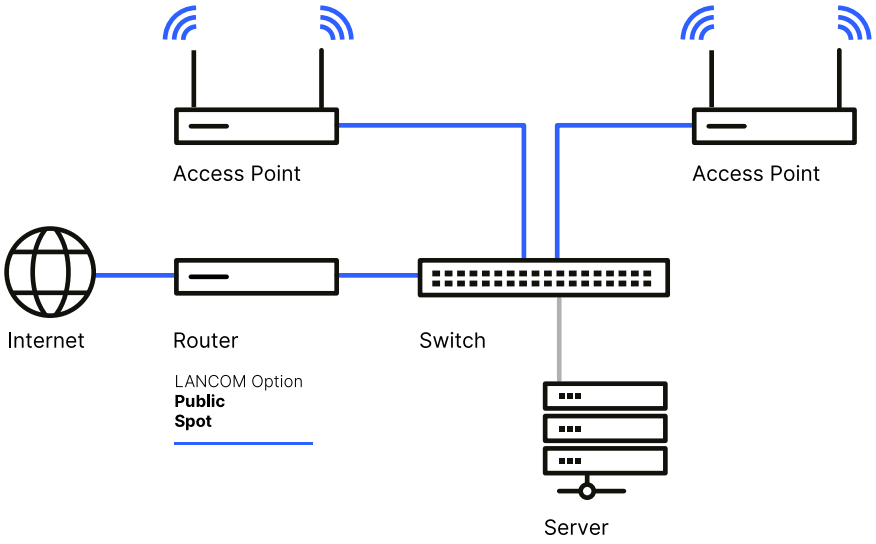

Abbildung 2:
Router mit
Public Spot Option

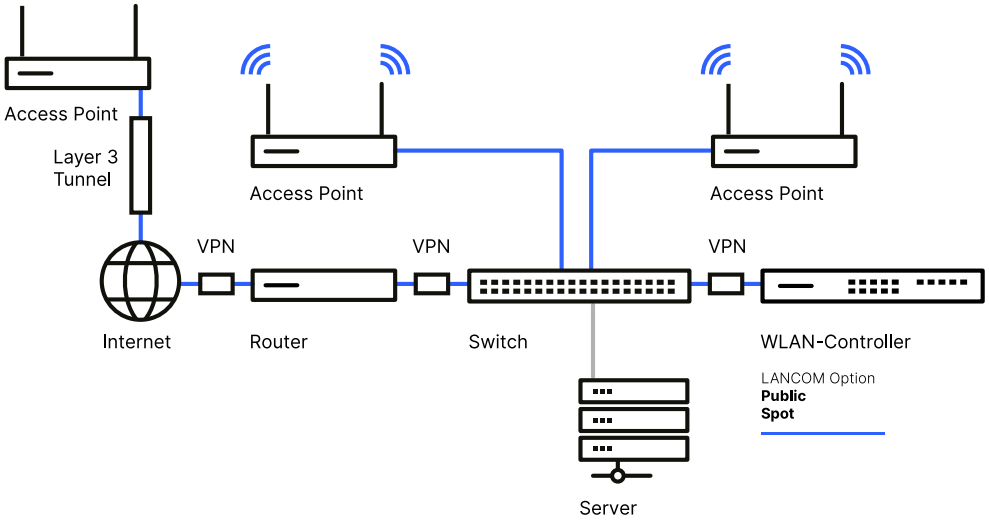

Abbildung 3:
WLAN-Controller mit
Public Spot Option

Sicherheit

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

Der erste wichtige Punkt zum Thema Sicherheit ist die Trennung des Public Spots von anderen internen Diensten und Daten. Diese kann über VLANs (Virtual Local Area Networks) erreicht werden, so dass die bestehende Infrastruktur weiterhin genutzt werden kann. Das VLAN selbst wird dabei wie ein 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 dafür notwendigen WLAN-Controller. 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, den Public Spot über diverse WAN-Verbindungen bereitzustellen, sofern der betroffene Access Point ein Profil vom WLAN-Controller beziehen kann.

Für die Authentifizierung am Public Spot gibt es unterschiedliche Methoden. Die gängigste nutzt Benutzername und Kennwort. Hier muss der Benutzer 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 Nutzungsbedingungen des Hotspots anzuzeigen.

Die Option, eine Authentifizierung durch Benutzername, Kennwort und MAC-Adresse durchzuführen, wird nur selten eingesetzt, hauptsächlich wenn die Zugangsdaten an ein bestimmtes Endgerät gekoppelt werden sollen. Die notwendigen Authentifizierungsdaten liegen entweder auf einem externen oder auf dem internen RADIUS-Server des Gerätes (Autorisierung). Die Anmeldung selbst läuft über das HTTPS-Protokoll in einen Browser ab, um die Sicherheit zu gewährleisten, dass Benutzerinformationen nicht mitgeschnitten und missbraucht werden können.

Der Betreiber des Hotspots kann bei der Definition des erlaubten Zeitrahmens festlegen, ob die Zugangsberechtigung für einen gewissen Zeitraum nach der ersten Aktivierung

gültig ist oder inkrementell über ein 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 Authentifizierung am Public Spot nötig ist. So kann zum Beispiel ein Hotel die Webseiten für Sehenswürdigkeiten, zu denen es Ausflüge anbietet, freischalten.

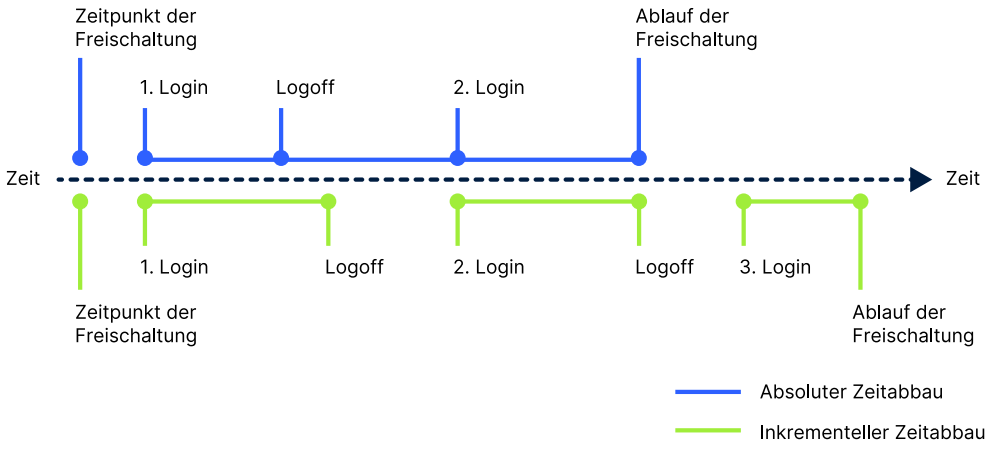

Abbildung 4:
Absolute und inkrementelle Internet-Zugangsbeschränkung

Protokollierung und Filterung

Es 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 (Accounting).

Eine weitere Maßnahme ist das Filtern des Angebots im Internet. Hier kann auf zwei verschiedene Mechanismen zurückgegriffen werden. Zum einen auf die Stateful Inspection Firewall, in der unter anderem Ports geblockt werden können, um so die Verbindung zu gewissen Diensten zu unterbinden. 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.

LANCOM Systems GmbH
A Rohde & Schwarz Company
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info@lancom.de | lancom-systems.de