International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 10
June 2016

Guest Traffic Isolation Using Ignition Guest Tunneling

Shwetha N M
M. Tech Student, Dept. of IS&E,
Sri Jayachamarajendra College of Engineering,
Autonomous under VTU, Mysore, Karnataka, India

Vani H Y
Assistant Professor, Dept. of IS&E,
Sri Jayachamarajendra College of Engineering,
Autonomous under VTU, Mysore, Karnataka, India

ABSTRACT: Providing guest Wi-Fi access has become a must-have capability for companies in nearly every industry. Today, free Wi-Fi is ubiquitous in highly trafficked areas such as airports, coffee shops and hotels. However, guest Wi-Fi is not limited to retail environments; businesses in other sectors such as finance and healthcare also need to offer guest Wi-Fi to vendors and customers. However, these industries must ensure a high level of security and enforce company-specific acceptable use policies.

Visitors, customers, business partners, suppliers, temporary workers and a variety of professionals who come into your office to do business now expect you to offer access to Internet. However, granting guests access poses security risks. If you allow access, they also connect to enterprise network. To avoid access to enterprise network and to provide only Internet access we can use Guest tunneling virtual appliance.

Enterprise WLAN service for Non-employees or visitors should be isolated from corporate network for security reason and tunneling technology is one of the simplest way to provide "WLAN Guest Isolation". This paper discusses isolation of

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 10
June 2016

guest traffic using ignition guest tunneling (IGT) virtual appliance.

KEY WORDS: Ignition Guest Tunneling (IGT), WLAN 9100 Access Point, GRE protocol, Access Portal.

INTRODUCTION:

IT departments today are faced with a growing challenge: to maintain network security while facilitating access via wired, wireless and VPN networks for employees, contractors, guests and others who may be on or off premise. They're being asked to provide only as much access as each user requires, to ensure that user devices are healthy and in compliance with the chosen security policy, and to provide that access in real time. Managing these demands is a critical element of your success.

Ignition Guest Tunneling virtual appliance is a product which provides WLAN guest user traffic isolation solution using GRE (Generic Routing Encapsulation) tunneling technology. Network security is the first priority for any company looking to offer guest Wi-Fi access. Isolation keeps guest users away from the Enterprise LAN. That is, a guest user cannot see any Ethernet connected devices, nor can they see any Wi-Fi devices that are logged on to a Enterprise Wi-Fi network. This prevents guests from being able to access files on a NAS (Network Attached Storage) device or print to a network printer. Isolated guests can get to the Internet; they just can't get to any device on the Enterprise LAN.

Common Guest Network Isolation Methods:

Guest Network Isolation is security requirement for network access control to separate the guest traffic out of intranet and vice-versa.

Common Guest Network Isolation method includes:

- Mapping Service Set Identifier (SSID) and VLAN
- Tunneling from WLAN controller to Demilitarized Zone (DMZ)
- Enforcing through security policy and Firewall

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 10
June 2016

- VIP and source NAT from WLAN controller
- The problem becomes complicated especially in large enterprise network where provisioning guest VLAN in every switches and external captive portal is being used to support larger number of guests instead of switch embedded captive portal.
- Statistics shows that more than 80% of security breach or outages were caused by misconfiguration. Hence, it is desirable to achieve the guest network isolation in a simple and non-disruptive way.

LITERATURE SURVEY:

Avaya Identity Engines:

Avaya Identity Engines Portfolio solutions enable businesses to control who accesses a network, when, where, and how the network is accessed, and which devices will be allowed on the network. Identity management software from Avaya helps ensure secure network access for employees, guests, and partners, even when they are using personal devices at work. In supporting the Bring-Your-Own-Device—BYOD—trend, securing network access is paramount. You must define and enforce who gets on, with what, to go where.

Avaya Identity Engines gives you granular control of both users and devices. Set the policies you need: For example, a user connects wirelessly to the corporate network via a work-provided laptop and is granted full access. However, the same user connecting via a personal iPad device is granted restricted access.

METHODOLOGY:

In order to accomplish this, the following method is carried on:

Guest Network Isolation using IGT

IGT uses Guest Network Isolation to separate the guest traffic from intranet and to separate intranet from guest traffic.

Guest Network Isolation method for IGT includes:

- Mapping SSID and VLAN
- Tunneling to IGT through the SSID and GRE tunneling

GRE-based Guest Isolation Deployment

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 10
June 2016

GRE-based Guest Isolation Deployment deals with isolating guest traffic by making use of IGT virtual appliance and Access Portal that acts as an external captive portal. Create three interfaces such as management interface, IN interface and OUT interface in IGT. The IGT's IN-interface is configured as the remote end point on the Access Point (AP) 9100. The AP tunnels the guest traffic to the IGT appliance. The appliance on receiving client traffic, decapsulates the packets and forwards it to the Access Portal. The Access Portal OVA can be deployed as virtual appliance on the same server that host IGT appliance. In this situation, the OUT interface of IGT is connected to the IN interface of the Access Portal. A Dynamic Host Configuration Protocol (DHCP) server can reside on the IN interface of the Access Portal. The OUT interface of Access Portal will be connected to the Internet or DMZ. Hence, guest traffic is tunneled from the AP to the guest tunneling appliance and later through the access portal.

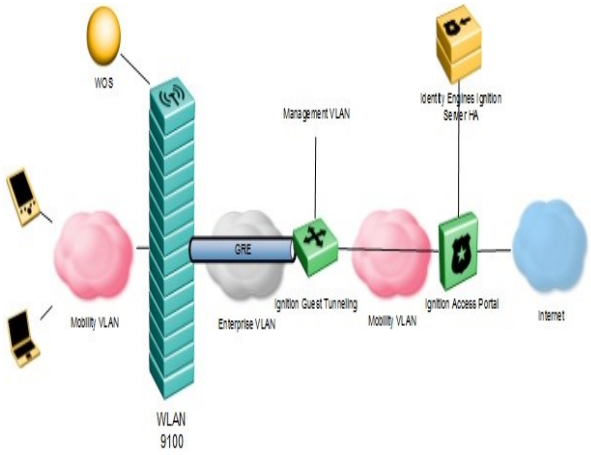


Figure 1: Architecture of Ignition Guest Tunneling

This figure represents the architecture of Ignition Guest Tunneling.

IMPLEMENTATION:

Installation and Configuration

Install Ignition Guest Tunneling and Access portal on the same ESXi server.

WLAN 9100 Orchestration Server

Create SSID and Tunnel Configuration in WLAN 9100 AP or WOS (WLAN Orchestration Server):

Tunnel configuration on WLAN 9100 access points can be done through two interfaces. The WLAN Orchestration Server

(WOS) is a management application through which multiple access points can be managed. The Access Point Web Management Interface (WMI) is a GUI used to manage a single access point.

WLAN Orchestration Server (WOS) is a management application, using this application we can create SSID for Guest or Employee. This web application also provides option for configuring GRE Tunnel. To create tunnel between WLAN 9100 and Ignition guest tunneling we have to mention Local Endpoint is AP IP address, Primary remote Endpoint is Ignition Guest Tunneling Inbound interface IP. Associate the GRE tunnel created to SSID.

Access Portal

Access Portal is a virtual machine based captive portal and firewall application that controls the access of client devices to the network. Access Portal blocks all traffic from client devices and allow network access only after successful authentication. Access Portal allows Enterprises to provide Guest users to connect the Internet using their own devices.

Access Portal has three network interfaces:

• OUT - The OUT interface provides connectivity to the Internet.

• ADMIN - The ADMIN interface provides connectivity to the portal to perform administrative tasks.

• IN - The IN interface provides connectivity to the client network. This is the guest or unauthenticated client VLAN / network.

GRE protocol

Tunneling technology is one of the simplest way to provide "WLAN Guest Isolation". Generic Routing Encapsulation (GRE) is a tunneling protocol**.** It can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network. OVS can use GRE tunnels between hosts as a way of encapsulating traffic and creating an overlay network. IGT uses GRE with TEB payload so that the entire L2 frame is tunneled.

Configuring GRE Tunnels:

Step1: Create a tunnel interface

Interface tunnel number

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 10
June 2016

Step2: Assign an IP address to the tunnel interface

IP address address mask

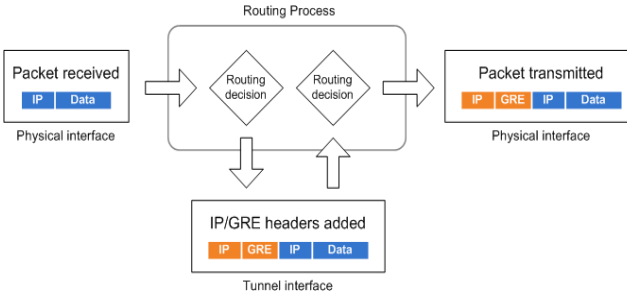
Step3: Configure the tunnel's source IP address in the public part of the network.

Tunnel source interface or the tunnel source IP-address

Step4: Configure the tunnel's destination IP address in the public part of the network.

Tunnel destination IP-address

Step5: Configure the routes to use the tunnel with IP routes



When client connect to WLAN 9100 AP using wireless device, when an Employee connects, after successful authentication will be placed in an employee VLAN. When a Guest user connects and gets registered successfully, he will be placed in a Guest VLAN. Then it sends traffic through Access portal. Access portal provides captive portal web page, only successful authentication of guests, this page will allow to access Internet. This Product is very useful wherever Wi-Fi feature is used.

Using Management IP address launch IGT web user interface. Through which administrator can able to manage all tunnel related configurations.

CONCLUSION:

Offering guests access to your network services is essential. Today, the Avaya Identity Engines Ignition Guest Tunneling enables organizations to securely provide network access to guests and visitors without compromising the security of the network.

REFERENCES:

1. https://www.avaya.com/usa/documents/avaya-WLAN-9100-series-dn7647.pdf, Avaya WLAN 9100 series
2. https://www.avaya.com/usa/documents/identity_engines_ignition_access

_portal_dn7082.pdf, Identity Engines Ignition Access portal

3. http://www.avaya.com/usa/product/identity-engines/, Avaya Identity Engines

4. https://en.wikipedia.org/wiki/Generic_Routing_Encapsulation, Generic Routing Encapsulation –Wikipedia

5. http://archive.openflow.org/wk/index.php/Tunneling_-_GRE/L2TP, Tunneling –GRE/L2TP