4ipnet®

WI-FI ACCESS CONTROL, REINVENTED

FEATURE GUIDE

SUMMARY OF FEATURES

- ROLE-BASED POLICY ASSIGNMENT
- TIME-DEPENDENT & LOCATION-WARY POLICIES
- BANDWIDTH LIMITATIONS
- TRAFFIC CLASSIFICATION
- INDIVIDUAL FIREWALL RULE SCHEDULES
- SPECIFIC ROUTING RULES
- MULTIPLE LOGINS PER WI-FI ACCOUNT
- CONCURRENT SESSIONS LIMITATIONS
- CHANGE PASSWORD PRIVILEGE
- IP ADDRESS REASSIGNMENT

CURRENT STATE OF PUBLIC WI-FI

Gone are the days when Wi-Fi in public areas could be left uncontrolled and unmanaged. Whether it be airports, hotels, or hospitals, users are becoming increasingly frustrated by slow and unreliable Wi-Fi connections. The primary cause is the rapid adoption of smartphones and tablets – everyone is using Wi-Fi on these handheld devices to stay connected, everywhere and anywhere. Since Wi-Fi operates on a shared medium, network congestion naturally follows. The situation is then further exacerbated by individuals who abuse the wireless freedom given to them, running bandwidth hungry applications that bog down an entire network. As a result, organizations and network operators alike are finding it more and more difficult to offer open, public Wi-Fi while maintaining an acceptable connection quality for each user.

You may be wondering – what about the password that can be set on Wi-Fi networks? It may be enough to prevent people walking by your coffee shop or office building from leeching off of your Wi-Fi service, but when it comes to guaranteeing network quality, it is far from sufficient. Users who know the password are still given free rein on the Internet, and as most Internet users are, for a lack of a better word, "selfish", it is highly unlikely that you will find individuals who will refrain from watching their YouTube videos in 1080p HD out of concern for the Internet needs of others.

Many Internet providers today offer households broadband connectivity surpassing 100M on both the uplink and downlink end. As a result, we have grown numb to the bandwidth needs of applications we use. Therefore, when we open our laptop computers at the airport terminal while waiting for our flight, we instantly begin streaming our favorite TV show without even considering that all the other people sitting next to us are also using the same Wi-Fi. When this kind of behavior has become so natural and reflexive, the network and IT personnel at the airport simply cannot expect all the passengers to respect each other and use Wi-Fi moderately.

SOLVING THE PROBLEM

So how does the airport reduce complaints regarding its Wi-Fi service?

In this scenario, 4ipnet's managed Wi-Fi solution is an ideal solution for helping the airport reduce its Wi-Fi complaints. The 4ipnet WHG-series wireless LAN controllers enable fine-grained user access control by

segregating Wi-Fi users into **ROLES**. Each role can then be assigned a **POLICY** with traffic shaping **PROFILES** based on the time and day of the week. The primary advantage over unmanaged Wi-Fi networks is that IT personnel can now ensure appropriate usage of Wi-Fi access, guaranteeing the quality of the network without relying on users to curb their own usage.

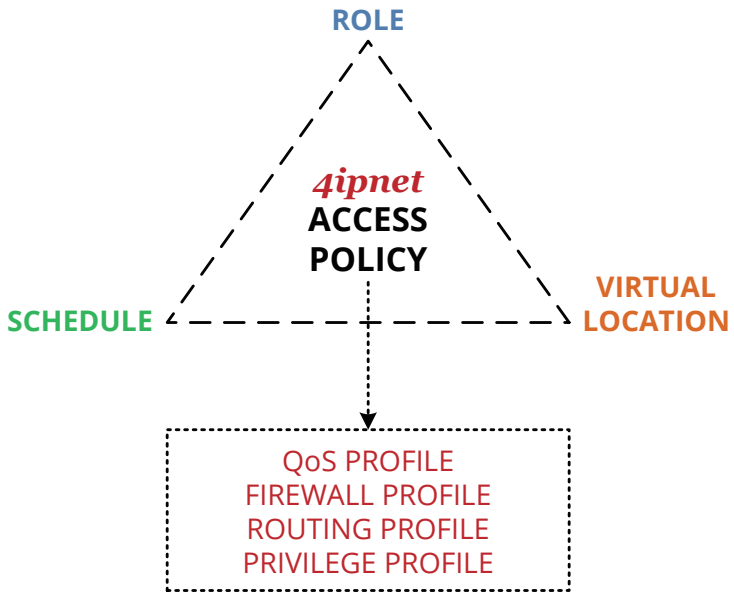
This feature guide introduces 4ipnet's Wi-Fi access control features, from bandwidth control to specific routes and multiple logins per account. The goal is to offer a clear picture of the benefits provided by 4ipnet's solution, regardless of when compared with unmanaged Wi-Fi solutions or other managed Wi-Fi offerings.

ROLES, POLICIES, & PROFILES

Whether you are providing Wi-Fi in a hotel, a hospital, an office building, or even a warehouse, it usually makes sense to divide potential users into various roles with differentiated services. For example, hotel staff may not be allowed to use Facebook during work hours, while guests may not be allowed to exceed a certain amount of bandwidth.

In a 4ipnet-based WLAN deployment, access restrictions can be accomplished by defining roles with different policies that take effect at different times. Each policy is then associated with various profiles. Returning to the example above, the hotel staff role is defined with two schedules, one for work hours and one for after-work hours. During work hours, a policy with a firewall profile prevents the staff from accessing Facebook. After work, a separate policy with a separate firewall profile enables the access. Similarly, for the hotel guests there is a single schedule (i.e. all day, every day of the week) that limits each user's bandwidth through a policy with a QoS profile.

The following is an illustration of the different factors that affect 4ipnet's user access policies:



TIME-DEPENDENT, LOCATION-WARY

With scheduling, enterprises and organizations are able to assign different policies to each role based on the time of the day or the day of the week. This feature is especially beneficial for businesses, where management do not want staff and employees accessing certain Internet sites or network resources during work hours. Without a scheduling capability, IT teams would be faced with the arduous task of creating multiple roles just to assign different policies. This is also counterintuitive, as these users' "roles" have not actually changed – an employee is still an employee, even if it's not during the work day.

In order to fully understand how schedules and policies function, we must first introduce the concept of a Service Zone. 4ipnet WHG controllers have the ability to segment a physical network into multiple virtual networks, each of which is a **SERVICE ZONE**. The most obvious difference between a Service Zone and a VLAN is that a Service Zone can contain multiple VLAN IDs. Users who connect to the network are automatically associated to a Service Zone based on the physical LAN port or VLAN that they are connecting from.

So what is the relationship between scheduling of roles and Service Zones? Not only can a schedule define which profiles to apply to a role at a given time, it can also define which profiles to apply to a role at a given time **and** a given Service Zone. In other words, the profiles applied to a user role can be both time-dependent and location-wary.

Armed a basic understanding of how access policies are determined in a 4ipnet system, we can proceed to explain the different profiles and how they allow network administrators to perform fine-grained management of Wi-Fi users.

QOS PROFILE: ENSURING NETWORK PERFORMANCE

The most common and direct method to prevent users from consuming the entire bandwidth of a network is to apply **BANDWIDTH LIMITATIONS**. The QoS Profile on 4ipnet WHG controllers allows administrators to specify two types of bandwidth limitation:

1. Per Role Downlink & Uplink Limitation
2. Per User Downlink & Uplink Limitation

Not only can network administrators limit individual users, they can also limit the total bandwidth consumed by all users of the same role. Both limitations can work simultaneously, and if so, only one needs to be satisfied for the system to begin curbing usage. For example, although you may not have reached the defined per user maximum downlink, your usage may be capped due to others who have the same role (i.e. per role maximum downlink has been reached). Despite the per user limitation being the more intuitive of the two, per role limitation still has applications for many Wi-Fi service providers. For instance, network administrators can use the per role limitation to control the distribution of bandwidth between different roles. This may be critical in environments such as hospitals, where Wi-Fi reliability and uninterrupted access for visitors is trivial when compared to that of for doctors and physicians.

In addition to assigning bandwidth limitations, the 4ipnet WHG controller can also perform **TRAFFIC CLASSIFICATION** – the assigning of different priorities to network traffic belonging to each user role. In many deployments, it is imperative to have certain roles take on a higher priority than others. For example, SIP-based devices (which in this case can be viewed as "users") need to be configured with a higher priority so that when the network becomes congested, calls will not be interrupted. Similarly, hospitals have many devices and equipment that are very sensitive and mission critical, all of which must take the highest priority when transmitting data wirelessly over the hospital network.

FIREWALL PROFILE: BLOCKING THAT UNWANTED TRAFFIC

Sometimes, it is just not enough to only limit the quantity of traffic. Schools may want to prevent its students from surfing the Internet during class time. A coffee shop may want to block specific websites that are known to be illegal. Businesses may need to ban Facebook access during work hours. There are a multitude of potential scenarios, but the requirements are the same – network administrators need a method for blocking or allowing certain network usage.

With the Firewall Profile on 4ipnet WHG controllers, applications using specific ports can be blocked, and access

to specific websites can be prevented. Initially this may sound very unimpressive, as many network devices can perform similar functionality. However, dig deeper and you will find that the real value behind 4ipnet's Firewall Profile is its ability to perform double-layer scheduling, with an **INDIVIDUAL FIREWALL RULE SCHEDULE** on top of the overall access policy schedule.

Assume that a business wishes to have a specific access policy take effect for employees from 9 in the morning until 5 in the afternoon – this access policy will only contain one Firewall Profile. However, with the second layer of scheduling, network administrators gain additional flexibility, allowing them to block IP addresses on one day and allowing the same IP addresses on another day. Most importantly, all of this can be accomplished without having to configure multiple policies, which greatly simplifies the lives of network personnel.

SPECIFIC ROUTE PROFILE: MAKING TRAFFIC MOVE THE WAY YOU WANT

For security and network management purposes, or for deployments that have unique topologies and requirements, network administrators may wish to assign **SPECIFIC ROUTING RULES** for users of different roles. On the 4ipnet WHG controllers, this is accomplished through the Specific Route Profile. These rules override the default routing of the network, which is sometimes a necessity to guarantee that the network works as intended.

For example, users may need to specify a route for servers that are located on the second WAN port of a WHG controller, instead of the default first WAN port. Or a user may need a defined route to allow communication between different Service Zones under the same WHG controller. Although not as common, these applications still exist, and with a 4ipnet solution IT teams do not need to worry about encountering any limitations when deplying wireless network infrastructure.

PRIVILEGE PROFILE: MANAGING USE BEHAVIOR

When you walk around on the streets today, it is not uncommon to see a large variety of devices being used – smartphones, tablets, or even small-sized laptop computers. The explosion of handheld devices in recent years has drastically altered Internet usage behavior. Specifically, it is becoming more and more common for a single Wi-Fi user to have multiple devices that need to be online at the same time. For example, a businessman may be connected back to the office network using VPN on his laptop, while at the same time checking e-mails on his BlackBerry.

Traditional Wi-Fi accounts that only allow a single login per account can no longer fulfill the evolving market demands. To address this phenomena, 4ipnet WHG controllers support **MULTIPLE LOGINS PER WI-FI ACCOUNT**, such that a user can use the same username and password for all of his/her handheld devices. As part of a user role's Privilege Profile, network administrators can configure different roles to have different multiple login thresholds. For instance, staff members may only be allowed to login with one device at a time, while guests may be allowed to have up to 3 devices simultaneously connected.

Not only can the 4ipnet WHG controllers allow network administrators to configure the simultaneous device login limit, it can also define the number of **CONCURRENT SESSIONS ALLOWED PER USER** for a given role. Naturally, one thinks about this feature working in conjunction with QoS profiles to prevent individual users from congesting the entire WHG-managed network. And with the **CHANGE PASSWORD PRIVILEGE**, organizations can reduce operational overhead by allowing Wi-Fi users of a specific role to modify their own login password.

Lastly, the **IP ADDRESS REASSIGNMENT** function allows users to switch IP addresses after successfully authenticating on the network. In specific deployments, it may be necessary for authenticated users to obtain public IP addresses. For example, when VPN with NAT traversal is not available, business travelers staying at hotels may need public IP addresses in order to establish concurrent VPN connections back to their office network. The function can also allow users to switch to other private IP addresses after authentication, which caters to organizations with specific security and network topology needs.

CONCLUSION

The combination of roles, scheduling, and profiles makes the 4ipnet Wi-Fi user access control truly unique, and able to fulfill the needs of all different types of deployments. Network administrators can control each user's bandwidth, traffic priorities, routing, and much more. More importantly, this can be individually configured for users of different roles. Even within the same role, users can be assigned different policies depending on the current day & time, and which Service Zone they belong to.

There are numerous possibilities - organizations and businesses looking to enforce proper Wi-Fi usage and ensure network quality need to look no further than 4ipnet's solution.