RG-SMP

Программное обеспечение управления безопасностью

Ruijie Networks Co., Ltd.
For further information, please visit our website http://www.ruijienetworks.com

Обзор

Ruijie RG-SMP (Платформа управления безопасностью) является платформой промышленного класса, которая обеспечивает наблюдение и контроль за сетевыми устройствами и устройствами безопасности Ruijie. Ruijie RG-SMP предлагает комплексное управление безопасностью с широким набором устройств, включая интеллектуальные коммутаторы и беспроводные решения Ruijie. Ruijie RG-SMP также совместим с другими сторонними сетевыми устройствами с использованием протокола 802.1 x, позволяющего AAУ (аутентификацию, авторизацию и учет) управление сетевым доступом (NAC) в соответствии с требованиями пользователя.

Ruijie RG-SMP позволяет пользователям управлять офисными сетями любых размеров в широком спектре отраслей промышленности, соответствуя требованиям безопасности идентификации пользователя, поддержки работоспособности и безопасности сетевого взаимодействия.

Основные черты

Объединенный проводной и беспроводной контроль сетевого доступа

Ruijie RG-SMP предлагает единую интегрированную безопасную платформу для всех проводных, беспроводных и VPN устройств. Он поддерживает не только динамическую аутентификацию для различных смарт устройств, но и интеграцию с устройствами третьей стороны RADIUS и LDAP.

Эксклюзивное решение End-to-End NAC

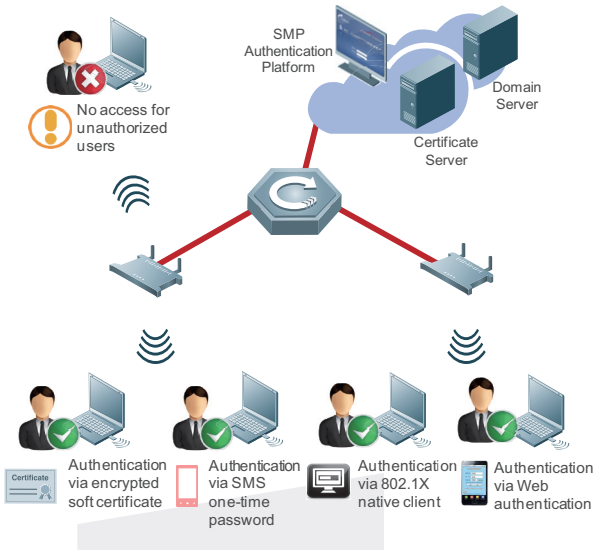
Решение поддержки BYOD

Ruijie RG-SMP поддерживает динамическую политику контроля Wireless Guest Account, основанную на идентификации пользователя и используемой мобильной платформы. Он также поддерживает гостевые аккаунты при помощи SMS аутентификации на всех последних платформах смарт устройств – планшетах, смартфонах и т.д.

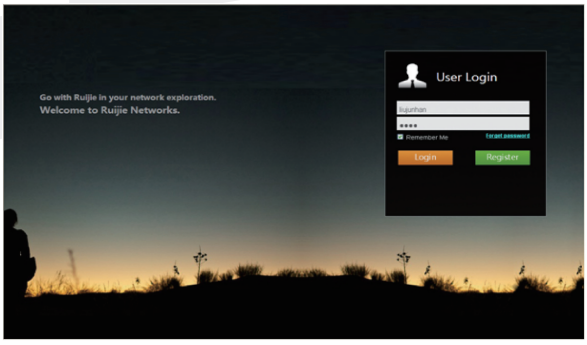
RG-SMP для объединенного управления BYOD

Комплексная проверка подлинности

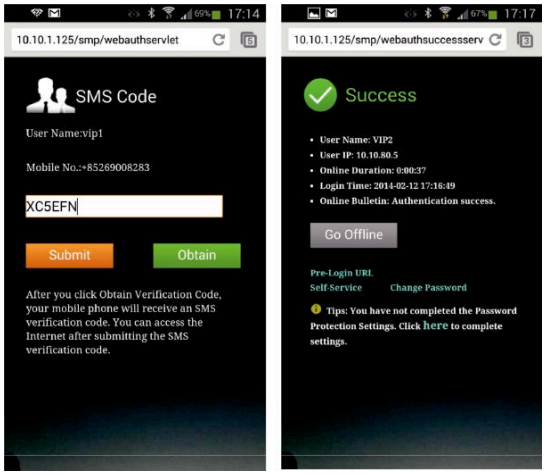
Ruijie RG-SMP поддерживает веб-аутентификации и идентификации беспроводной сети на базе протокола 802.1X. Через гибкую связь учетных данных пользователя, IP-адрес, MAC-адрес, IP-адрес коммутатора, порт коммутатора и серийный номер жесткого диска, может быть проверен идентификатор пользователя. Он обеспечивает сетевой контроль доступа, запись пользователя онлайн/оффлайн и проверку учетной записи обычного пользователя. С помощью Ruijie RG-SMP может быть также составлен чёрный список пользователей. RG-SMP обеспечивает обширную библиотеку режимов аутентификации, включая веб-портал аутентификации, двухфакторную аутентификацию для персонала, QR-код аутентификации и SMS-авторизацию. Следующая схема иллюстрирует отображение интерфейса и принципы четырех методов аутентификации.



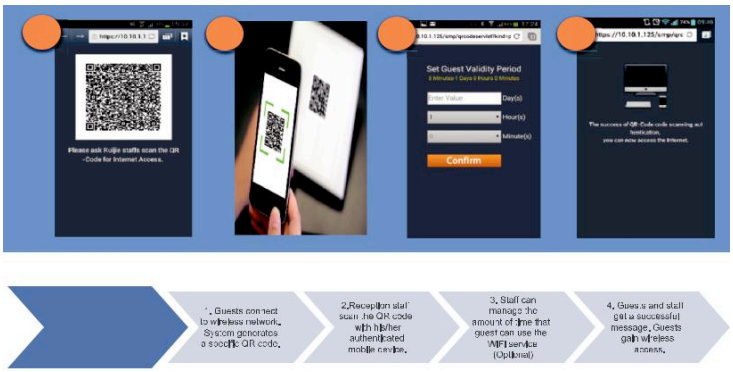
RG-SMP комплексный режим авторизации



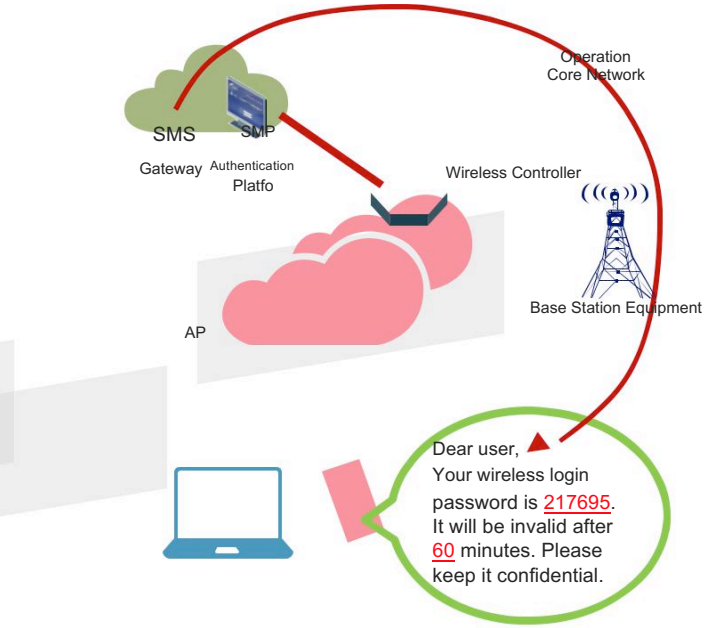
Настроенный веб-портал аутентификации



Двухфакторная аутентификация для персонала (Пароль + SMS)



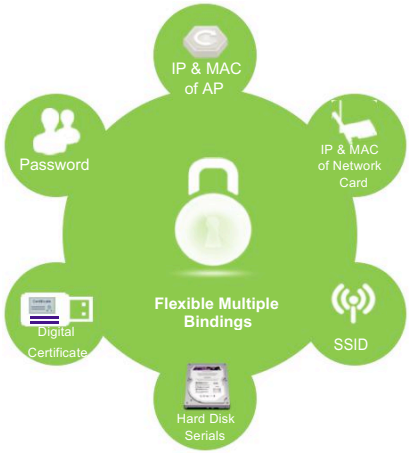
QR код аутентификация



SMS аутентификация

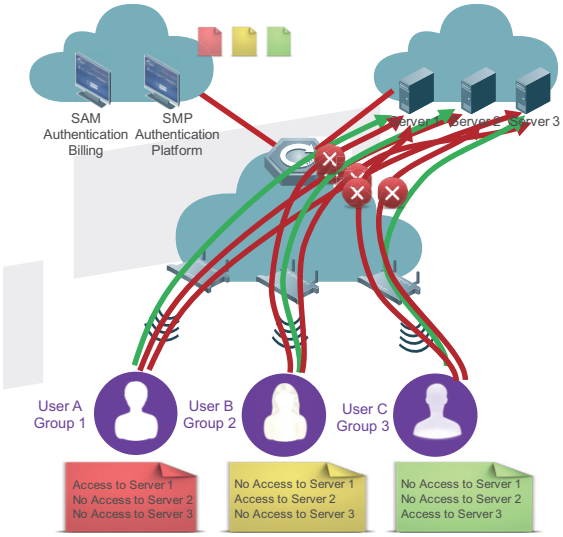
Поддержка узла защиты конечных точек

Получая обновления от Microsoft WSUS, Ruijie RG-SMP позволяет администраторам развертывать последние обновления операционной системы для компьютеров под управлением Windows. Антивирусное программное обеспечение также поддерживается, чтобы защитить систему от вредоносных атак. Черными и белыми списками можно управлять на ПО конечных устройств для блокирования нежелательных и рискованных пользователей. Кроме того, Ruijie RG-SMP предотвращает несанкционированный доступ и спуфинг с MAC адреса, обеспечивая сетевую и сервисную доступность и стабильность бизнеса. ПО Ruijie RG-SMP предлагает несколько привязок к пользовательским экземплярам для обеспечения высокого уровня безопасности пароля, конечных устройств и сети доступа. Функции обеспечивают быстрое определение местоположения пользователей и конечных устройств для немедленного устранения неисправностей.



Гибкость привязок пользовательской информации

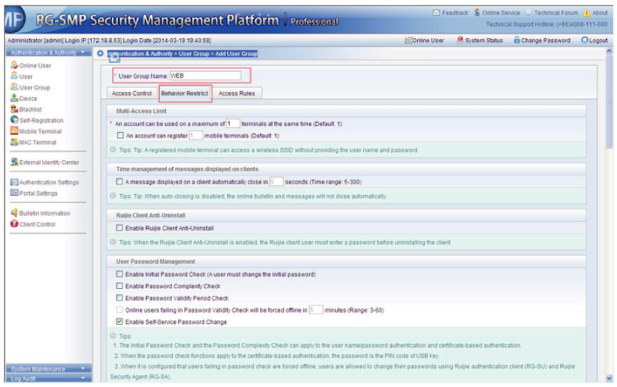
RG-SMP предлагает расширенную безопасность с гибким управлением. Решение позволяет осуществлять правила динамического контроля доступа с гибким Role/User/IP VLAN карантином. Решение гарантирует, что пользователю разрешается доступ к сети через заданную сеть через гибкий доступ с ограничением прав доступа на основе различных групп пользователей, доменов, логином, конечных устройств и др.



Множество связанной пользовательской информации

Простые Web операции

Ruijie RG-SMP поддерживает дружественный пользователям графический Web GUI интерфейс, для выполнения всех относящихся к SMP безопасности конфигураций и управления статусом пользовательского доступа.



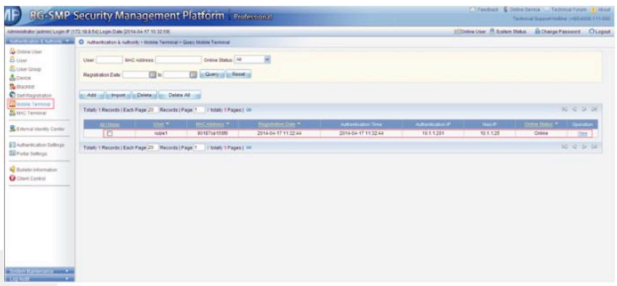
Web GUI интерфейс

Детальное документирование записей безопасности

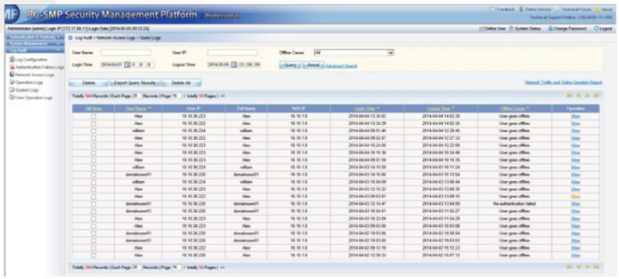
RG-SMP предоставляет широкий спектр отчетов и анализа для упрощения управления безопасностью. Решение предоставляет подробную онлайн информацию о пользователе, включая имя пользователя, IP, MAC, VLAN ID, NAS IP, время входа, метод аутентификации, беспроводной SSID, Upstream/Downstream трафик (требуется RG-ACE) тип клиента и т.д.

Ruijie RG-SMP предлагает различные типы журналов для простого управления:

- Журнал сбоя проверки подлинности
- Журнал доступа к сети
- Журнал операций
- Системные журналы
- Журналы операций пользователя
- 360-дней записи



Управление мобильным устройством



Log Generation и управление

Техническая спецификация

Спецификация	Техническая спецификация
Контроль сетевого доступа	Support wired, wireless and VPN network access control (NAC)
	Support IEEE 802.1x access authentication, without the need for any client agent installation
	Support MAC address authentication, without the need for any client agent installation
	Support Web Portal authentication for staff Support two-factor authentication using user credentials as well as one-time password via SMS to verify user's pre-registered mobile phone number
	Support Web Portal authentication for visitors Support Web Self-Service Platform for visitors to establish temporary/ one-time user accounts (via SMS)
	Support QR-Code authentication for visitors Visitors require QR-Code authorization by any authenticated user before network access
	Support different QoS bandwidth policies application to different users based on their role within the organization and the device type currently in use
	Support per user, per device, and per application/TCP-port prioritization (require integration with Ruijie RG-ACE Internet Application Security Gateway)
	Support web-based management interface
	Support report and analysis generation to show details and correlation of user, authentication and device information for troubleshooting and locating problems
	Support AAA framework providing complete separation of Authentication and Authorization sources
	Support authorization for LDAP, AD, Kerberos, Token Server, SQL compliant database
	Support integrated, network based, device profiler utilizing collection via SNMP, DHCP, HTTP, AD and ActiveSync
	Support complex PKI deployment and AAA server certificate signed by external CA whilst validating internal PKI signed client certificates
	Support NAC health check allowing both agent and agentless methods and the solution acts as a permanent or dissolvable health agent for Windows, Linux, and Macintosh platforms
Сертификат системы интеграции 3-й стороны	Support 3rd party RADIUS authentication integration Support user data collection of 3rd party certification information from Java / web service based interface
	Support Microsoft Windows Active Directory (AD) domain integration, including seamless Single-Sign-On integration for a complete 802.1X authentication and Windows AD authentication

Спецификация	Техническая спецификация
Сертификат системы интеграции 3-й стороны	Support the integration with LDAP server to obtain user identity information to achieve unified authentication
Изучение и поддержка связи мульти-элементов	Support terminal hard drive serial number, SSID, user name, password, terminal IP, terminal MAC, network access control device (NAS) IP, NAS port active learning as well as multi-element flexible combination of binding elements (May require agent installation)
Пользовательское управление	Support account creation, cancellation and user group management Support customized user information fields, such as department, age, etc. Support Self-Service Platform (Web) for visitors to establish temporary/ one-time user accounts Support dynamic user blacklist which prohibits user to login in specified period of time Support for setting account usage period and auto account cancellation when expired, with user notification in advance
	Support users login broadcast messages pop up, or web page pop up Support Disclaimer Acceptance message pop up and visitors need to click “Accept” before accessing the network Support authentication suspension period, during that period the user disabled cannot authenticate or access the Internet
	Support online user management, including message broadcast, online users status review, forced offline as well as online user re-authentication, information gathering and remote assistance
	Support maximum user password attempts before user account is locked
	Support direct access to the user's physical NIC MAC address, to prevent tampering of the MAC address
	Support limited number of devices, quota or bandwidth per user
	Support caching of MAC address for post guest authentication and guests do not need to re-authenticate during the valid access period
	Support bulk import of guest accounts and enable notification of credentials via email
	Support sponsored approval workflow for guest self-registration which the new SSID registration requires approval from internal staff
	Support display of post login session statistics page for users to review and monitor usage or quota assigned
	Support network-based devices ACL, VLAN, and host ACL network access control
Аутентификация пользователей	Support seamless 802.1x authentication, without the need for any client agent installation and multi-vendor network access
	Support Web Portal authentication for staff Optionally support two-factor authentication using user credentials as well as one-time password via SMS to verify user’s pre-registered mobile phone number
	Support Web Portal authentication for visitors Support Web Self-Service Platform for visitors to establish temporary/ one-time user accounts (via SMS or e-mail)

Спецификация	Техническая спецификация
Аутентификация пользователей	Support QR-Code authentication for visitors Visitors require QR-Code authorization by any authenticated user before network access
	Support MAC Address Bypass (MAB) authentication for devices which cannot support IEEE 802.1x protocol
	Support auto-login for self-registration workflow
Совместимость конечной точки	Support the latest Windows, Mac desktops and support for Apple, Android mobile device platform
	Support device-based portal page and automatic screen fit feature for various screen resolution mobile device platform
Управление хостом безопасности (Требуется установка агента)	Support 3rd party antivirus software integration, allowing software installation detection, operation, and updates patches can be pushed remotely
	Support integration with Windows Security Center
	Support the installation program to detect and repair software that must be installed to force the download and installation, prohibit the installation software prompts to uninstall; support processes running, registry keys, Windows service entry inspection and repair; support external connection port for management, prohibiting the use of USB, CD-ROM loaded with connectors; support Windows patch updates the mandatory or non-mandatory; support switch-based ACL, the switch VLAN, ACL implementation of quarantine host
Управление активом (Требуется установка агента)	Support the collection of the user's software and hardware information, hardware information when the user changes, CPU, memory, motherboards, hard drives and other information for logging
Управление сетевой безопасностью	Support ARP spoofing prevention features that enable trusted gateway ARP entries to prevent ARP spoofing gateway device, the client also supports static binding ARP information
	Support role-based user security management
	Support dynamic, stateful access rights into the network once authenticated based on source, destination, and/or ports
	Support defining rules for access rights based on any combination of time, location, user identity, device identity, and extended attributes from the authentication database
	Support defining policies for users who can access the network, with which mobile device and which parts of the network they can access
	Support users to allow traffic, deny traffic, reject traffic, route traffic, and blacklist (remove from the network)
	Support blacklisting of wireless devices once firewall / ACL access rule violations are detected or revocated (Ruijie RG-SMP Client installation is required)

Спецификация	Техническая спецификация
Управление сетевой безопасностью	Support the automatic recognition of operating system and product type of the end devices
	Support display of users' internet usage (integration with RG-ACE Internet Application Security Gateway required)
	Support integration with RG-IDS devices that can collect IDS devices reported security incidents and the source of the attack for direct processing; critical server's IP address configuration for more sensitive event handling and protection
Контроль интернет приложений на базе пользователя	Support integration with RG-ACE Internet Application Security Gateway; the gateway supports real-time analysis on the L7 Internet Application that the authenticated users are using; the gateway supports user-based application control which the user can be selected from the Authentication System
Надежность системы	Support Microsoft Windows and SQL Server cluster hot standby
	Support over 50,000 users by license extension
	Support backup cluster node with uninterrupted authentication traffic when node failure occurs
	Support high availability redundancy design for resiliency

Требования к оборудованию и ПО:

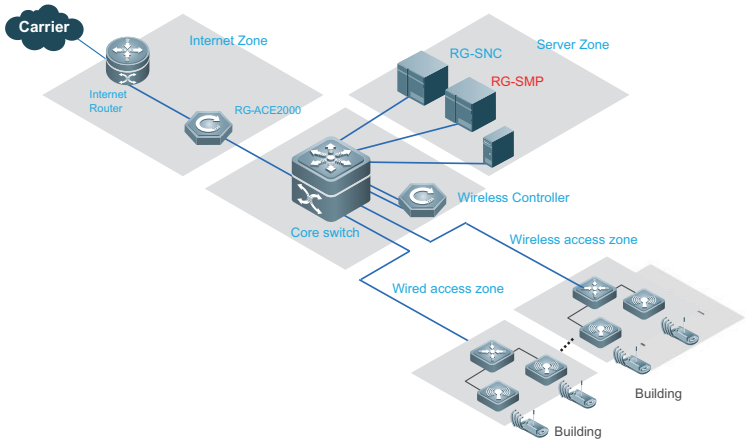
■ Минимальная спецификация

Требования к платформе оборудования	
Процессор	Intel Xeon 2.8GHz Quad Core x 2 or above
Память	4G or above
Хранилище	160G or above
Сетевая карта	3 x Gigabit Ports
ОС и БД	
ОС	Windows Server 2003 Enterprise Edition SP2 or above
База данных	SQL Server 2005 Enterprise Edition SP2 or above

■ Рекомендованная спецификация для широкого развёртывания (более 15,000 чел.):

Требования к платформе оборудования	
Процессор	Intel Xeon 2.8GHz Quad Core x 2 or above
Память	16G or above
Хранилище	500G or above
Сетевая карта	3 x Gigabit Ports
ОС и БД	
ОС	Windows Server 2008 Enterprise Edition SP1 or above (x64)
База данных	SQL Server 2008 Enterprise Edition SP1 or above (x64)

Типовое применение



Управление сетевым доступом для проводных и беспроводных пользователей предприятий

Благодоря Ruijie RG-SMP достигается управления доступа и безопасности учета и управления аутентификацией единой сети:

1. Единая система пользовательского управления: Единый портал, способных идентифицировать разных пользователей. Все проводные, беспроводные и VPN пользователи централизованно управляются с помощью платформы RG-SMP. RG-SMP объединяют карты с Microsoft Windows Active Directory и достигают настоящей унификации. Windows AD это главный контроллер по управлению всеми учетными записями пользователей. Все изменения одновременно обновляются в веб аккаунте. Каждому пользователю требуется только один логин и пароль.

2. Гостевое управление: QR-код проверки подлинности развертывается для удовлетворения растущего спроса со стороны гостей. QR-код размещен в общественной зоне, где автоматически дается ID и пароль для доступа к Wi-Fi. IT администраторы могут легко настраивать срок действия QR-кода пароля. Эта мера эффективно уменьшает нагрузку на гостевую сеть управления.

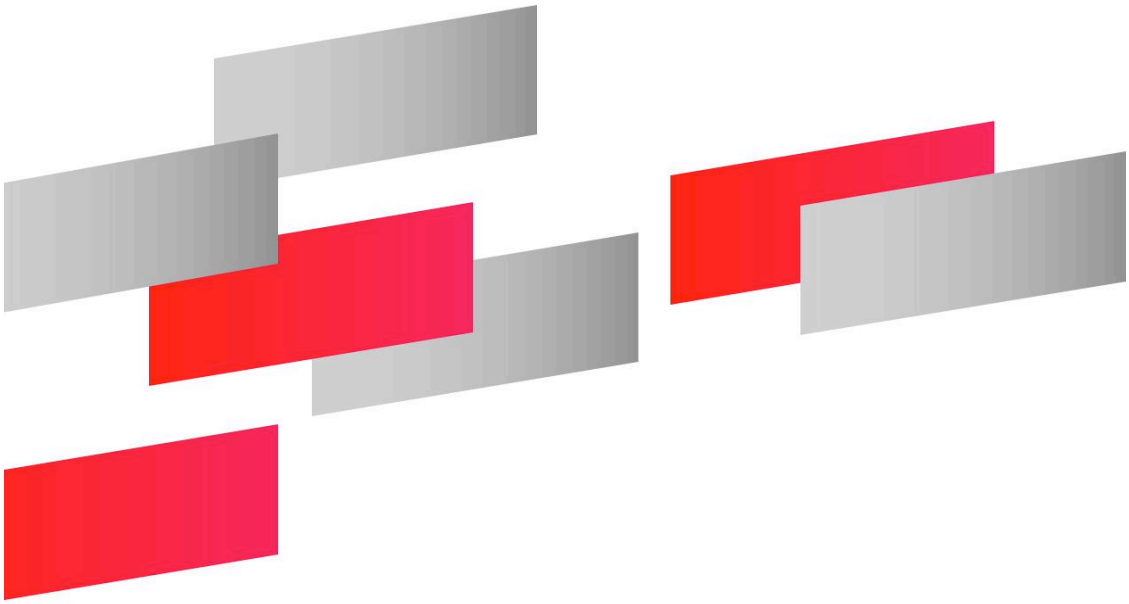
3. Расширенное гостевое управление: RG-SMP предлагает QR код аутентификации. Авторизованный персонал компании может предоставлять гостевой доступ. Это объединяет гостевую активность входов и аккаунты персонала, упрощая журналирование для управления. Гость сначала подключается к беспроводной сети, где будет показан QR код. Гость может попросить авторизованный персонал отсканировать QR-код и сразу получает право доступа.

4. Авторизации пользователя: Возможны специфические ограничения пользователя. Управленческий персонал имеет бесплатный доступ к сети. Гости могут заходить только в интернет.

Информация для заказа

Модель	Описание
RG-SMP-Pro-EN	RG-SMP 2.X professional edition, supports RADIUS identity authentication, including BYOD and NAC features. Software requirement for SMP: • Windows Server 2003 or above • SQL Server 2000 or above
RG-SMP-Pro-EN-license-50	Concurrent User License for RG-SMP 2.X professional edition, includes permission for 50 concurrent users edition,

Innovation Beyond Networks



Ruijie Networks Co., Ltd.

Headquarter in Beijing

Address: Floor 11, East Wing, ZhongYiPengAo Plaza, No.29 Fuxing Road, Haiddian District, Beijing 100036,China
Email: info@ruijie.com.cn
Tel: (8610) 5171-5961
Fax: (8610) 5171-5997

Supply Chain in Fuzhou

Address: JuYuan Star-net Ruijie Technology Park, No. 618 JinShan road, Fuzhou City, 350002, China
Tel: (86591) 83057888
(86591) 83057000

Regional Office in Hong Kong

Address: Unit 09,20/F, Millennium City 2, 378 Kwun Tong Road, Kowloon,Hong Kong
Email: sales-hk@ruijienetworks.com
Tel: (852) 3620-3460
Fax: (852) 3620-3470

Regional Office in Malaysia

Address: Office Suite 19-12-3A, Level 12, UOA Center, No.19 Jalan Pinang, 50450 Kuala Lumpur
Email: sales-my@ruijienetworks.com
Tel: (603) 21811071

For further information, please visit our website http://www.ruijienetworks.com