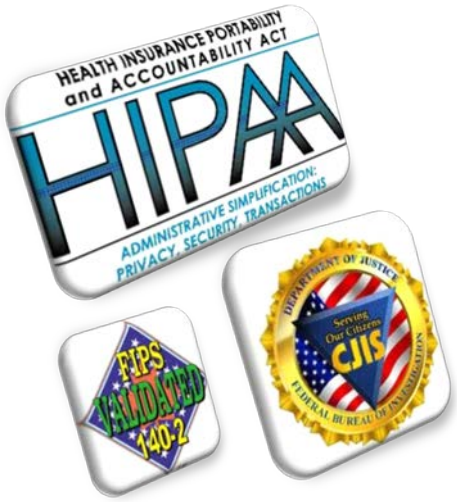
The expansion of mobile workforces across mission-critical environments such as public safety, home care, and hospital settings is challenging IT administrators to ensure quick, reliable, and seamless wireless communications without sacrificing security measures.

From municipal, to state, to federal environments, first responders of every kind need timely and secure access to highly confidential information, such as criminal histories and healthcare files. The inherent sensitivity of the information demands security policies that protect the data wherever and however it is being accessed.

Advanced Mobile VPN Security

Designed specifically for organizations transmitting sensitive, mission critical data over mobile VPN connections, Mult-IP delivers seamless and persistent device and user security even when roaming over disparate networks. Mult-IP supports the highest encryption standards while remaining flexible enough to allow agencies to adjust their security programs according to their needs, budgets and resources.



Benefits

- Protect the integrity of mobile data being transmitted wirelessly
- Validate client devices and users accessing the network
- Simplify authentication processes without creating security breaches
- Track and save all security events to a centralized server

RSA SECURED

Mobile Security

Mult-IP is a mobile VPN solution that allows mobile workforces to access application servers and other resources with a level of security that rivals that of the corporate LAN.

Authentication

Mult-IP integrates into established Windows, RADIUS, RSA or 802.1x (single sign on) authentication environments, providing full validation protection without forcing administrators to redefine access rights for each user. Furthermore, if the client device falls out of wireless coverage, the user will remain authenticated for a configurable amount of time delivering session persistence.

Multi Agency Authentication

Mult-IP enables IT administrators from multiple agencies to share one Mult-IP system and create their own unique client groups and associated authentication procedures tailored to their distinct needs and budget. Administrators can be assigned to one or more functional groups, controlling access to their associated data via permission-based access rights. This intelligent partitioning of resources empowers each agency to configure which network will carry specific application data based on priority, operational parameters, and/or security requirements — independent of other groups within a single agency and across other agencies.

Microsoft® Windows	RADIUS	RSA®	802.1x
• charges the local machine with the task of prompting users to enter their username/password upon connection. • Windows Domain Logon; validates credentials against those contained in the corporate Active Directory accessible to the Mult-IP gateway via the corporate LAN	• uses Network Access Service (NAS) to validate user credentials against a centralized database. • provides authentication, authorization and accounting capabilities • supports various authentication protocols, including EAP, PEAP, CHAP, PAP, etc.	• two-factor hardware or software token authentication via RSA Authentication Manager (also known as the RSA appliance) • embedded RADIUS server interfaces with the gateways acting as client devices	• port-based client device authentication via EAP (Extensible Authentication Protocol) • three-tier authentication mechanism composed of the client (supplicant), access controller (authenticator), and authentication server • Mult-IP behaves as an access point that opens and closes the communication channels independently for each virtual port (client connection) • Single-sign-on support; enables a user to log in once and gain access to multiple systems without being prompted to log in again at each of them

Encryption

Mult-IP is a FIPS 140-2 certified mobile VPN software that provides system-wide end-to-end encryption using single DES, 3DES, or AES (128,192,256) cryptographic algorithms. The software uses integrated cryptographic modules which have been certified by the National Institute of Standards and Technology of the United States of America and the Communications Security Establishment of the Government of Canada. Mult-IP ensures a secure connection right from the start by applying a handshake protocol between the gateway and client device to ensure both parties agree on the rules of further transmission. Encryption is a system-wide setting which cannot be segregated among functional groups. The choice of which encryption method (or level) best applies to an environment depends on application robustness and availability may be subject to export rights outside the US and Canada.

OS Platform	FIPS 140-2 Certificates
Windows XP SP3	989
Windows 7	1330
Windows 8.1	1894
Window 10	2606
Windows Server 2008 r2	1337
Windows Server 2012 r2	2357
Android 4.x, IMOS	1747

Radio IP
Redefining Secure Mobility

Government Policy Compliance

Mult-IP conforms to all regulations outlined in draft version 5 of the U.S. Department of Justice – FBI Criminal Justice Information Services (CJIS) security policy, and the latest versions of the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) policies. Mult-IP exceeds the FBI CJIS, HIPAA and HITECH requirements, providing FIPS 140-2, AES (128, 192, 256) and 3DES encryption, supporting 2-factor authentication.

FBI CJIS

Mult-IP addresses applicable sections of the CJIS policy version 5.0 (draft). The policy provides appropriate controls to protect the full lifecycle of Criminal Justice Information (CJI), whether at rest or in transit.

Encryption (Section 5.10.1.2)	User Identification (Section 5.6.1)	Advanced Authentication (Section 5.6.2.2)
"When CJIS is transmitted outside the boundary of the physically secure location; the data shall be immediately protected via cryptographic mechanisms (encryption)".	*"Each person who is authorized to (…) transmit CJI shall be uniquely identified. A unique identification shall also be required for all persons who administer and maintain the system(s) that access CJI or networks leveraged for CJI transit".*	*"Advanced Authentication provides for additional security to the typical user identification and authentication of login IP and password".*
→ Mult-IP supports the requested usage of FIPS 140-2 certified encryption, at a minimum level of 128 bit. → The symmetric key is encrypted by a FIPS 140-2 Certified RSA 2048 bit encryption algorithm as recommended by the NIST (National Institute of Standards and Technology, Special Publication 800-56B and 800-131A).	→ Mult-IP supports Windows authentication, RADIUS, 802.1x, and RSA as authentication methods for client devices.	→ Mult-IP supports two-factor authentication to ensure the legitimacy of a user. Two-factor authentication is a security protocol through which a user is identified using two (2) sources of identification from the following approved methods: • a token/key is automatically generated by the software/hardware device • a password/security code is defined and entered by the user • a biometric reading (i.e. a fingerprint, iris scan, etc.) → Mult-IP provides the flexibility to apply any combination of RADIUS, Smart Cards, PKI (Public Key Infrastructure) and biometric methods.

HIPAA & HITECH

HIPAA and HITECH define privacy and security rules protecting healthcare data - Electronic Protected Health Information (EPHI).

Access Control	Audit Controls	Integrity	Person or Entity Authentication	Transmission Security
§ 164.312(a)(1): *"the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource."* **§ 164.312(a)(2)(i):** *"Assign a unique name and/or number for identifying and tracking user identity."* **§ 164.312(a)(2)(iii):** *"Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity."* **§ 164.312(a)(2)(iv):** *"Implement a mechanism to encrypt and decrypt electronic protected health information."*	**§ 164.312(b):** *"Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."*	**§ 164.312(c)(1):** *"the property that data or information have not been altered or destroyed in an unauthorized manner."* *"Implement policies and procedures to protect electronic protected health information from improper alteration or destruction."* **§ 164.312(c)(2):** *"Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner."*	**§ 164.312(d):** *"Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."*	**§ 164.312(e)(1):** *"Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."* **§ 164.312(e)(2)(i):** *"Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of."* **§ 164.312(e)(2)(ii):** *"Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate."*
Mult-IP Clients and Administrators are uniquely identified and authenticated Session persistence: ensures that client devices reconnecting outside a pre-set duration are forced to register. Mult-IP supports single DES, 3DES, or AES (128,192,256) cryptographic algorithms using FIPS 140-2 for encryption.	The Mult-IP system log tracks events related to mobile client device activities and changing statuses as well as miscellaneous system-wide conditions. Mult-IP Analytics provides 25 Excel™-based reporting templates delivering comprehensive insight into network and application usage.	Mult-IP guarantees data integrity and protects against unauthorized alteration or destruction, through authentication, encryption and multi-agency. As a mobile VPN, the cryptographic tunneling protocols of Mult-IP provide confidentiality by blocking intercepts and packet sniffing, allowing sender authentication to block identity spoofing, and provide message integrity by preventing message alteration.	Mult-IP offers secure, two-factor authentication (password, token, biometrics, etc.) to provide proof of identity for authentication.	Mult-IP encrypts all data to protect EPHI integrity and prevent unauthorized access over communication networks. As a mobile VPN, the cryptographic tunneling protocols of Mult-IP provide confidentiality by blocking intercepts and packet sniffing, allowing sender authentication to block identity spoofing, and provide message integrity by preventing message alteration. Mult-IP is using FIPS 140-2 certified encryption using 3DES, or AES cryptographic algorithms.