

Access Defender™

Version 2.4

The inherent nature of Internet communications on IP-based wireless networks puts IT Managers at unnecessary risk with intruders attempting to access their LAN.

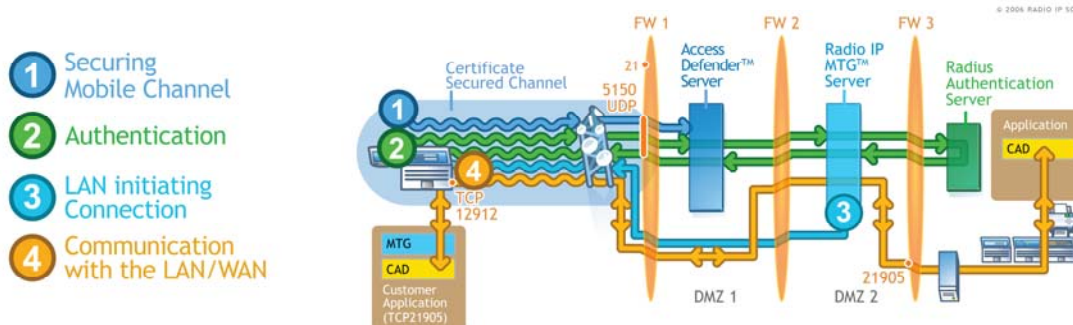
While mobile communication is pivotal to mission-critical organizations' bottom lines, ensuring high standards of emergency response and customer service, while denying unauthorized access to the system, becomes a "must-have". A typical wireless set-up requires a server and firewall that is configured to let specific communication ports open to your mobile workers. Even though you have done everything to ensure limited access, there is always an open door from which intruders can pass through, attacking your sensitive back-office data by employing methods such as "denial of service" or "buffer overrun". Access Defender is an additional security gate that removes the vulnerability associated with using IP networks. By residing between two firewalls, Access Defender scrutinizes and quarantines all incoming communication

attempts, allowing the LAN to give access to your mobiles rather than the mobiles initiating the access to the LAN.

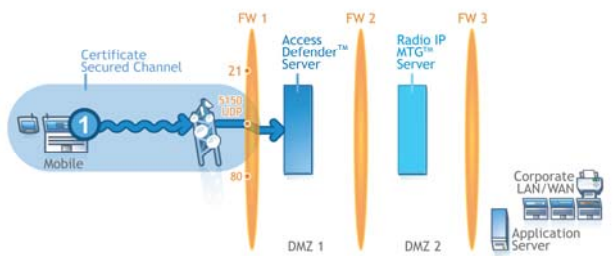
Principal Features

- ➔ Intruder-proof technology keeps intruders out by closing all open doors to the corporate LAN. Eliminates threats such as "denial of service" and "buffer overrun" attacks.
- ➔ Reduces recurring costs and saves money by leveraging your Internet communications to the fullest extent, bypassing the need for a dedicated line.
- ➔ Event Notification: Receive alarms (text message, email...) triggered by pre-defined events.
- ➔ Real-time communications dashboard lets your IT Managers view all attempted communications live, allowing them to take immediate action towards intruders and giving them an active role in defending the LAN.
- ➔ Historical communications dashboard logs all communication attempts for future analysis, empowering you to pursue your perpetrators or to even view connection profiles of authorized users.

Access Defender™ - Four Step Process

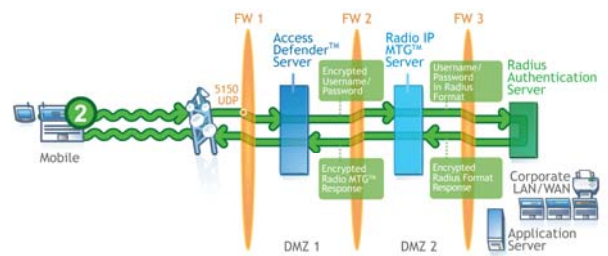


1 Securing Mobile Channel



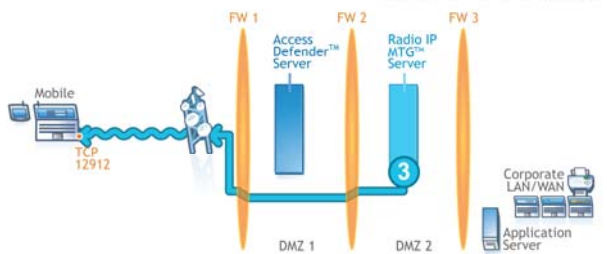
This first step makes use of a hardware certificate, preventing unauthorized mobiles from accessing the Access Defender server. The mobile can only pass to Step 2 if the machine's certificate is validated.

2 Authentication



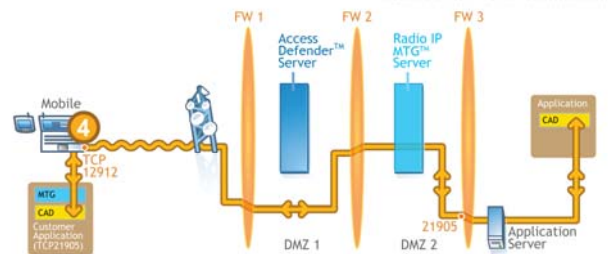
Access Defender now initiates the user authentication process. With optional two-factor authentication, the user's identity can be confirmed in tandem with their device authenticity. All non-authorized communications attempts will be quarantined, not allowed to go further.

3 LAN Initiating Connection



Once the authentication process is complete, Radio IP MTG will initiate a connection with the mobile on behalf of the LAN. In other words, Radio IP MTG allows the LAN to give access to your mobiles rather than the mobiles initiating access to the LAN.

4 Communication with the LAN/WAN



The final step demonstrates the two-way communications between the mobile unit and the application server residing on the LAN. Designed to safeguard your IT infrastructure, Access Defender's security architecture extends between three firewalls and two demilitarized zones.

Technical Specifications

Operates on:

- ➔ Windows Server 2003 SP1
- ➔ Windows Server Cluster-Friendly environments

Supports:

- ➔ All IP-based wireless networks (Networks Address Translation process not supported)
- ➔ Radio IP MTG version 2.5

Compliance with:

- ➔ FIPS 140-2 for key encryption
- ➔ ITU X.509 v3 for digital certificates
- ➔ FBI's CJIS security policy v 4.5

For more information on our security options, email us at: info@radio-ip.com