



## Secure Wireless Solutions for the Government

### SECURITY SOLUTION

#### Government Directives for Information Sharing Among Agencies

In the new era of the war to combat terrorism, government agencies are mandated to open their doors and share information with other like-minded agencies who serve to protect U.S. interests both at home and abroad. These mandates put an increased emphasis on information sharing with local and federal agencies that were previously outside the normal channels of classified information processing. In turn, these Local and Federal agencies have greater responsibilities for handling national security information.

Historically, agencies have maintained unique computing infrastructures for each level of security classification. This often resulted in data with lower security classifications being replicated on networks with the highest. Because of the very nature of agencies storing secret data, it will always be the case that an individual agency is entirely accountable for ensuring the security of its data until it becomes declassified.

The challenge government agencies face today centers on how to implement better IT solutions that provide secure information sharing with other agencies. Individuals need access to more data than ever, and agencies need to include security controls that:

- Prevent users from accessing information at a higher classification level than their authorization level permits
- Prevent unauthorized users from declassifying information
- Provide NIST/NSA validated confidentiality for data in transit

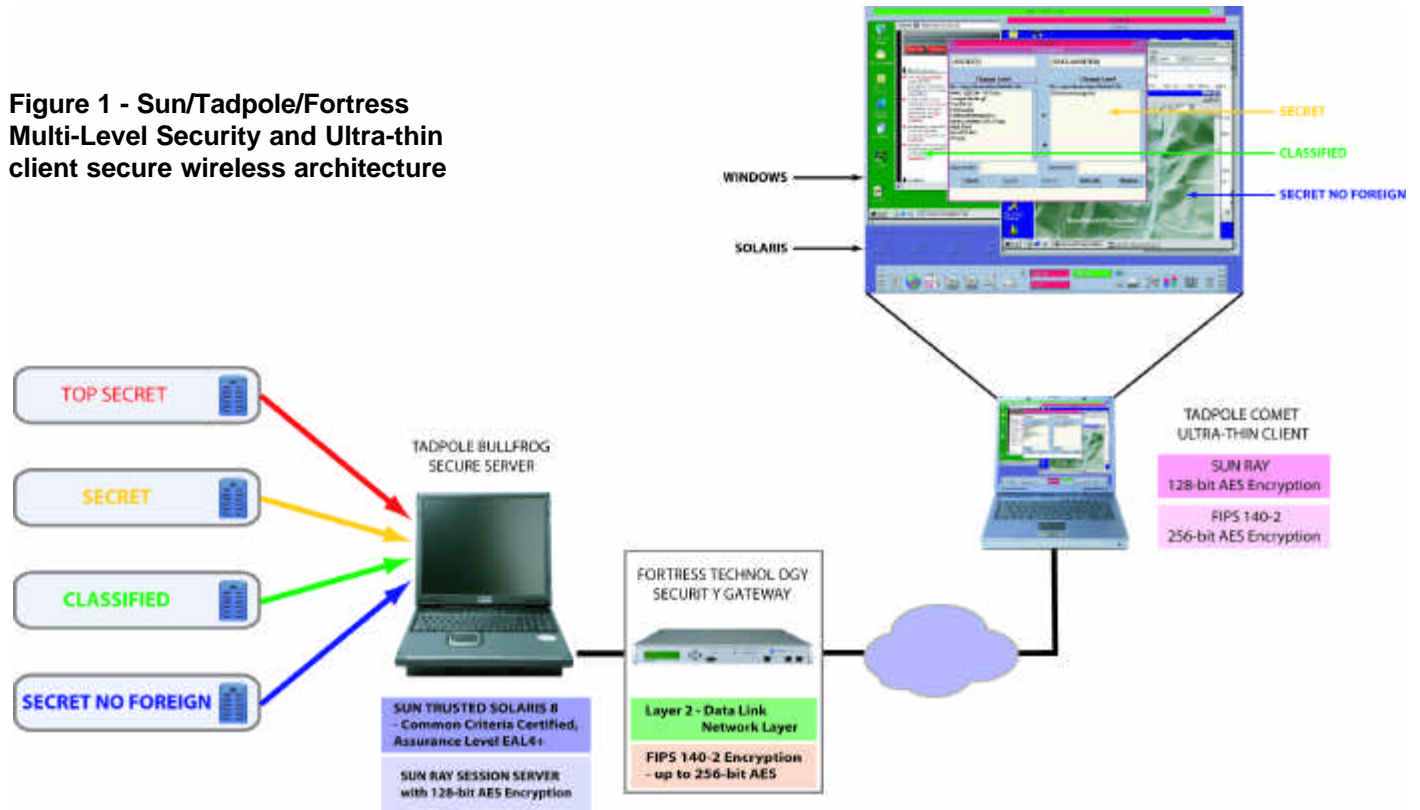
#### Simplicity For Government Agencies Seeking Deployable Multi-Level Security Solutions Now

The thought of disseminating national security information outside a specific agency has previously been a taboo subject with agencies doing their utmost to protect and secure this information. These disparate networks all share one thing in common though, and that is that they are networks, albeit disconnected networks.

Many vendors will propose complex software solutions to provide web-based access control privileges across these networks. These solutions, as well as being very complex and time consuming to implement, may have limitations. They may also present other security concerns.

There is a better and much simpler solution that can be implemented and managed at a low cost today without any new software architectures. This solution centers on secure ultra-thin client desktops and ultra-secure network gateway servers that provide secure access to multiple security domains over wired and wireless networks.

**Figure 1 - Sun/Tadpole/Fortress Multi-Level Security and Ultra-thin client secure wireless architecture**



**TADPOLE COMET  
SECURE ULTRA-THIN  
CLIENT DESKTOPS WITH  
FORTRESS FIPS 140-2,  
256-bit AES ENCRYPTION**

**FORTRESS TECHNOLOGIES  
SECURE GATEWAYS WITH  
FIPS 140-2 ENCRYPTION  
AT LAYER 2 OF THE  
NETWORK STACK**

**TADPOLE BULLFROG  
SECURE GATEWAY  
SERVERS RUNNING  
TRUSTED SOLARIS  
PROVIDE GATEWAYS  
TO MULTIPLE SECURITY  
DOMAINS**

Secure ultra-thin clients have no operating system, applications or resident data. This presents a number of benefits for securing data and controlling access to data and applications including:

- Eliminates security compromises resulting from data theft from the desktop client
- Allows the desktop client to be virtually immune from network intrusion threats
- Prevents network intrusion by providing strong 256-bit AES encryption at Layer 2 of the network stack
- Authenticates users via CAC card, user name/password and/or optional bio-metric devices
- Integrates secure wireless options
- Provides desktop terminal access to any back-office application and data, with the ability to open Windows, UNIX, Linux and mainframe applications simultaneously on the same device Requires ZERO administration for the desktop client (ALL administration is on the server)

The Multi-level Secure network gateway servers comprise Secure Gateways from Fortress Technologies and small form-factor secure servers from Tadpole Computer. The Fortress Secure Gateways provide the high assurance link between the Tadpole Comet ultra-thin clients and the secure network server. Tadpole Bullfrog users the ability to access applications and data on multiple security network domains. Together they provide:

- Policy management for user authentication and access control privileges
- Administration for individuals and groups of users that let new users or groups of users be established or disabled instantly
- Secure gateways to multiple networks at different classification levels
- Policy controls that allow authorized users to view multiple classification labels simultaneously
- Access to community networks, allowing users to browse various classified networks from the same window
- Centrally located and tightly managed secure server(s) for simplicity of administration and optimum security
- A solution that works with existing infrastructure solutions
- In-transit Layer 2 security

## Designed for Simple Deployment and Ease of Use

As well as providing true Multi-Level-Security the solution is designed for deployable applications. The secure network server is the Tadpole Bullfrog, a powerful small form-factor, portable server running Sun's Trusted Solaris Operating System. Sun Ray Server software 3.0 running on the Tadpole Bullfrog acts as the communication protocol to the Tadpole Comet ultra-thin clients and provides user authentication and encryption between the server and clients. User computing sessions are managed by the Sun Ray Server software on Tadpole Bullfrog's to provide users with access to applications and data on multiple security networks.

The Tadpole Comet ultra-thin clients are highly portable notebook implementations of a Sun Ray ultra-thin client. Tadpole Comet's are battery powered and for optimum mobility come with the option of Fortress FIPS 140-2 certified secure wireless networking to meet NIST/NSA mandates for wireless networking in government applications.

With Tadpole Comet ultra-thin clients, users can be given complete portability of their computer sessions. With simple but secure authentication protocols users can move seamlessly from one Tadpole ultra-thin client to another without losing any state of the application. This can be as simple as removing the users CAC card from one system and inserting it into another. More likely though, additional authentication from username/password and/or biometric devices will be used to securely authenticate users.

With centralized management, users no longer need local system administration for their personal mobile computers. Ultra-thin clients provide zero-administration locally and move the system administration to a Network Operations Center (NOC) that can be hundreds or thousands of miles away.

For example, First Responders can set-up local networks quickly and efficiently without needing expert technical support in emergency situations. And centralized management with ultra-thin client technology benefits medical personnel by providing a common operating environment to doctors or nurses regardless of location.

## Delivering a Deployable Multi-Level Security Solution

Tadpole Computer and Fortress Technologies have joined their strengths and experience to offer a simple, robust solution for the complex problem of MLS. The solution combines Tadpole's award winning ultra-thin client technology with Fortress Technologies FIPS-certified network security products and services for U.S. government agencies.

The combined components work together seamlessly in a MLS solution that is mobile, secure and affordable. As well as being ideally suited to First Responders, Command & Control, Criminal Justice, Public Safety, Military Intelligence and a whole host of other deployable applications, the solution easily scales for use in any government agency that has a requirement for affordable MLS based on readily available Commercial-Off-The-Shelf technology (COTS).

## Key Components for a Multi-Level-Security solution:

### DESKTOP CLIENTS

#### TADPOLE COMET ULTRA-THIN CLIENTS

No local operating system, applications or data:

- Eliminates threat of security compromises through loss or theft of desktop hardware
- Eliminates threat of network intrusion attacks on desktop hardware

#### 802.11A/B/G WIRELESS AND/OR 10/100 ETHERNET

Secure wireless networking provides optimum mobility.  
Wired networking option for situations where wireless is not an option.

#### FORTRESS FIPS 140-2 SECURITY



Secure ultra-thin clients with strong 256-bit AES

- Encryption at Layer 2 eliminates threat of network intrusion/denial of service attacks.
- Meets NSA mandated requirements for wireless SBU (sensitive but unclassified) networks

#### BATTERY POWERED

Long battery life provides optimum mobility. Ultra-thin client technology means battery failures do not cause loss of state on the client. Replace the battery or connect DC power to continue work from where you left off.

### SECURE GATEWAYS

#### FORTRESS TECHNOLOGIES AF8500

Provides end-to-end FIPS 140-2 security. Tadpole Comet ultra-thin clients communicate over 802.11a/b/g or wired networks through the Fortress Secure Gateway to the Sun Ray Server.

### SECURE NETWORK SERVER

#### TADPOLE BULLFROG MOBILE SERVER

Single or dual processor UltraSPARC IIIi mobile server:

- Approximately 22lb
- Up to 16GB memory
- Up to 200GB disk storage
- Integrated full-length PCI slot
- Integrated graphics display

#### TRUSTED SOLARIS 8 OPERATING SYSTEM

Common Criteria certification, Assurance Level EAL4+  
Orange Book B1 Certified out of the box  
Supports client naming services including NIS and NIS+  
Scales to handle heavy traffic  
Superior availability through small kernel & load balancing between cpus  
Configurable Security Functionality  
Multilevel File System allows segregation of different classes of users with strictly enforced data access controls and privileges  
Role-based Access Controls  
Execution Profiles limit users to specific sets of commands & actions to perform specific jobs

#### SUN RAY SERVER SESSION SOFTWARE

Provides User Authentication and encryption between server and client  
Provides user session management  
Provides enhanced security and reduces complexity and administration  
Seamlessly integrates access to applications running on any platform  
Leverages investment in existing back-end infrastructure  
Enhanced security with data & applications centralized where they can be:

- Easily backed up
- Made redundant
- Secured against theft and attacks



4023 Tampa Road, Ste. 2000 Oldsmar, FL 34677  
Tel: 1.888.4PRIVACY  
[www.fortresstech.com](http://www.fortresstech.com)  
© 2005 Fortress Technologies, Inc. All rights reserved.

46050 Manekin Plaza, Dulles, VA 20166  
Tel: 1-888TADPOLE6 +1 703-433-1157 Fax +1 703-433-9561  
[govsales@tadpole.com](mailto:govsales@tadpole.com) <http://www.tadpole.com>  
© 2005 Tadpole Computer Inc. All rights reserved.

