

# IA for the deployed

Basic tools of boundary protection, misuse detection and internal system controls allow comm to flow

By Mr. Jim Taratino  
Air Combat Command

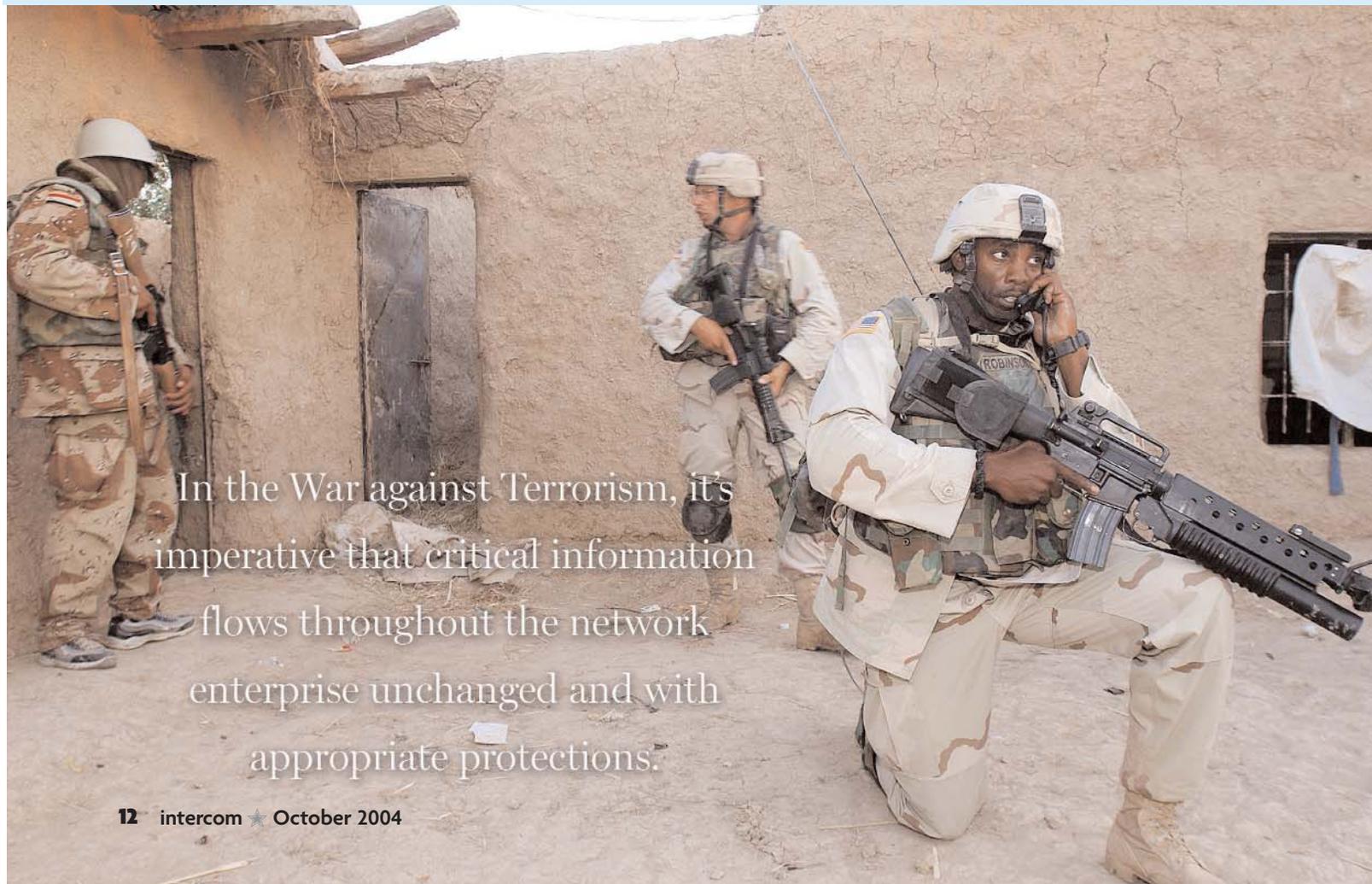
LANGLEY AFB, Va. — During Desert Storm, the deployed communications infrastructure provided the warfighter with secure and non-secure voice services and minimal data services. Ten years later, during Operation Iraqi Freedom, the deployed communications infrastructure provided the warfighter with a host of services, including information assurance tools that protected critical data throughout the spectrum of the war.

IA is the corner stone for

data transfer that ensures the data is delivered intact, protected, and unchanged.

In the deployed environment, base-level IA tools are provided by the Theater Deployable Communications program.

These tools consist of boundary protection, intrusion and misuse detection, and internal system controls, all of which are modeled after the Combat Information Transport System architecture used at the fixed bases. Maximizing the use of tools common to the CITS baseline not only ensures interoperability and improves integration, but also eases the training burden, enforces standards, and streamlines operations.



In the War against Terrorism, it's imperative that critical information flows throughout the network enterprise unchanged and with appropriate protections.

# warfighter

## BOUNDARY PROTECTION

The main boundary protection features protect the network perimeter by providing a means to control the information that crosses the network boundary.

The primary equipment used to enforce this protection includes an external router and the firewall. A Web Proxy Server and a Split Domain Name System Server also support the boundary protection role.

**As the first line of defense, the external router protects the screened subnet as well as the interior network from the external Internet.** It performs this function primarily through IP level packet filtering based on source and destination address and protocol.

In doing so, it resists IP spoofing attacks. In addition, the external router “screens” the firewall from direct attack. This is important since routers typically offer fewer services than host machines, such as firewalls, and hence are less vulnerable to a direct attack.

**The Sidewinder firewall furnishes the bulk of the boundary protection services.** The TDC design uses a “dual dual-homed proxy” firewall, which has two network connections — one to the internal network and one to the exter-

nal network. By not allowing direct connections between the internal and external networks, the firewall protects internal users from the rest of the Internet.

## INTRUSION AND MISUSE DETECTION

At the network perimeter, intrusion detection functionality is provided at the firewall.

Because the architecture contains a consolidated access point, the firewall is able to provide intrusion/misuse detection for all non-web base traffic.

**The intrusion/misuse function performed by the firewall is to detect and report unauthorized base network access and to attempt identification of potential attackers.**

The host-based solution is Symantec Host IDS software. The HIDS software is hosted on the Network Management Server running Microsoft Windows 2003.

## INTERNAL SYSTEM CONTROLS

The internal system controls are capable of assessing security issues such as proper password length, server configurations, access control rules, and user account administration. It also assists in the enforcement of network and security policies. The TDC

program provides two software packages to provide internal system controls: Symantec Enterprise Security Manager and Internet Security Scanner.

ESM is hosted on the Network Management Server while agent software is installed on all network control servers (except for the external primary DNS server) and most network servers.

**It checks for vulnerabilities and potential security holes in account integrity, login parameters, password strength, file systems and directories, network and server settings, system queues, and startup scripts.**

ISS is a protection mechanism offering integrity and security management. It is hosted on the “security” workstation to “learn” network vulnerabilities by performing a series of tests for well-known vulnerabilities.

Password Policy is enforced by Windows 2003.

