**ANRC/CSG Research Proposal**

**Exchange Parkway Plaza**
**5309 Wurzbach Rd.**
**Suite 101**
**San Antonio, Texas 78238**
**www.anrc-services.com/csg**
**Phone: 1-800-742-7931 (toll free)**
**Fax: 1-866-611-7047 (toll free)**

# Battling Intruder Initiated Secure Communications:

***A network defender's perspective and proposed solution to properly analyze unauthorized secure sessions.***

**7/13/2010**

## Introduction

A wealth of technologies have been created around the premise of intrusion detection. Most approaches provide the network defender with tools they need to properly administer their infrastructure and protect it from unauthorized access using a reactive posture. Hackers have adapted to these technologies by masking their communication sessions with strong encryption schemes rendering traditional automated defense (detection/prevention) systems useless.

Network intruders route their malicious activities with encrypted sessions hurdling right over these defense systems, and operating with complete impunity. The very technologies which have been created to secure our data transmissions are now being used to the advantage of the network intruder for concealment.

We propose a solution which will provide the network administrator with a technology that can decrypt adversarial encrypted communications and route the traffic through traditional Intrusion Detection Systems for detection and mitigation. This solution will be transparent to both the Operating System in use (Windows, Linux, MacOS, etc.) and can be tailored to perform on any enterprise network configuration.

## Problem Statement

Figure 1 below graphically represents a typical corporate LAN with Intrusion Detection Systems (IDS) and firewall in place. The secure (encrypted) communications originating from the LAN cannot be interrogated by the IDS's, and therefore are assumed to be benign and forwarded outside of the corporate network to the Internet. A network intruder realizes this vulnerability and employs encryption to their advantage to mask their malicious activities.

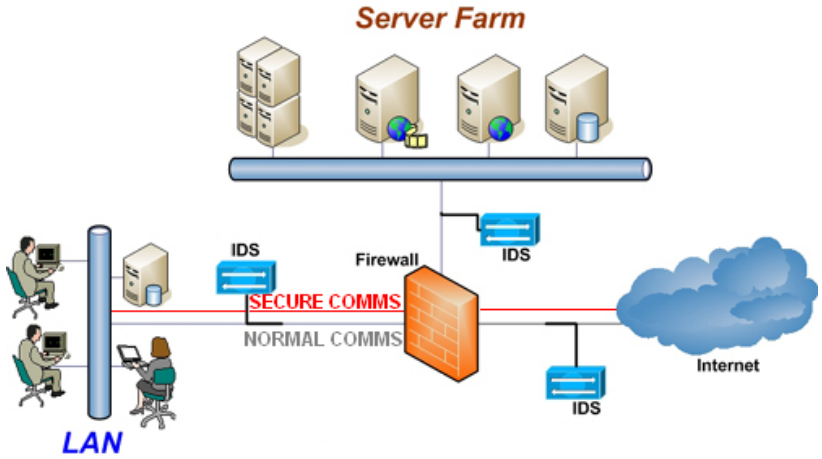


**Figure 1.** Typical Corporate LAN with IDS and Firewall

There are several popular ways network attackers encrypt their traffic to and from a compromised network:

1. Masquerading as a "browser" using SSL traffic and communicating over port 443.
2. Bridging the network through a software-based VPN solution and routing selected traffic from a compromised computer through an Internet forwarded port (i.e. 80, 443).
3. Obfuscating their traffic through static key encryption schemes such as:
    a. DES/3DES
    b. XOR'ing with a static key

Methods 1 and 2 rely on client-server Public Key Encryption (PKE) schemes and are the most difficult to deter. Though method 3a and 3b is trivial to decipher, there are an infinitesimal number of permutations and combinations that an attacker can use and is specific to the actual tunneling software they have developed. This method is beyond the scope of this solution and can be combated easily once the static key is found (usually by reverse engineering the software). Instead our solution focuses on methods 1 and 2.

Our solution aims to decrypt this traffic once it arrives at the IDS and provide the network defense systems an opportunity to scrutinize and interrogate the session and if invalid (through rule/signature/anomaly based sets) denying the transmission from proceeding beyond the local LAN to the Internet. At a minimum the IDS can alert the security administrator of the unauthorized tunneling attempt for further investigation.

For design and technical specifications please contact us directly.

## CSG Solution

We propose to develop enterprise scalable *CryptoSensors* that can preprocess PKE communications and forward decrypted traffic to IDS engines for traditional rule/signature/anomaly based analysis. Figure 2 below graphically demonstrates the CSG Solution.

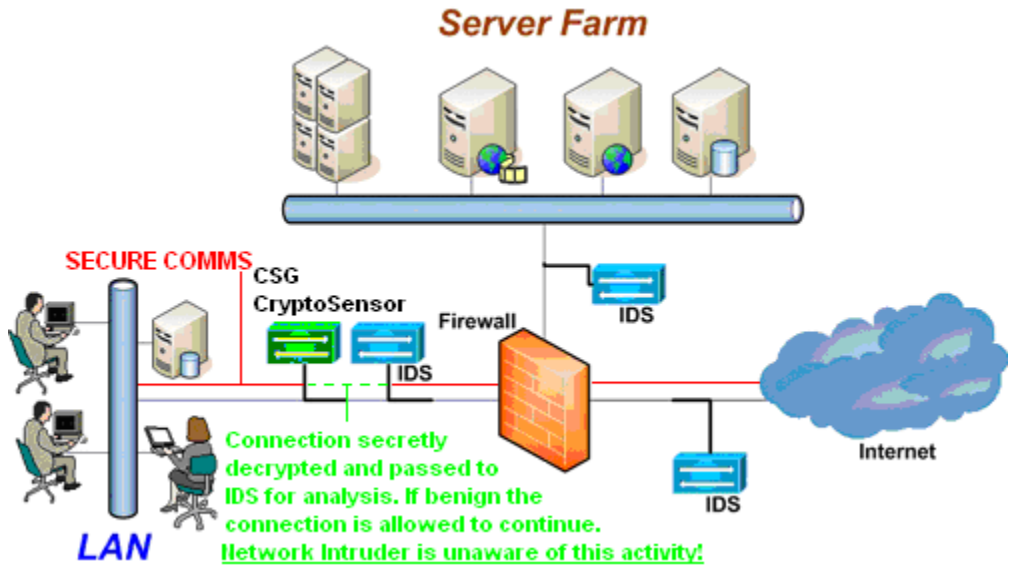


**Figure 3.** CSG Solution restores the network defense systems abilities.

### *Benefit 1*

The CSG *CryptoSensor* will be transparent to the network.

### *Benefit 2*

The solution is enterprise scalable and can be tailored to unique client network configurations.

### *Benefit 3*

The solution restores the network defender's IDS software/hardware effectiveness and allows the system administrator to see all encrypted communications passing through the device.

### *Benefit 4*

The CSG *CryptoSensor* is transparent to the client PKE applications; they are unaware the traffic will be interrogated prior forward beyond the corporate LAN.

### *Benefit 5*

Non-malicious encrypted communications will be re-encrypted after automated detection to ensure security so that regular legitimate traffic will not be affected by the *CryptoSensor*.

## Implementation

Contact us for details on implementing this solution for your corporate environment.

## Summary

CSG has years of experience in the Network Security field and highly qualified technical professionals ready to complete this extremely challenging and unique project, furthermore this project is ready to commence at the client's discretion and scheduling needs. The added awareness and value to using a CSG *CryptoSensor* is immeasurable. *The need for decrypting unauthorized network transmissions has never been greater and this project stands at the forefront of any/all research efforts currently being explored*. We thank you for taking the time to explore our project proposal and look forward to hearing from you.

*- Nathan Swaim*

President/CEO Computer Security Group

PAGE INTENTIONALLY LEFT BLANK