GHEM Secure Access Control

White Paper

Table of Contents

Contents

Executive Summary

Companies spend an enormous amount of money and time monitoring and securing access to critical network elements across the enterprise. If not judiciously managed, security holes creep into the network. The result from security breaches creates a financial toll and loss of trust in the company. In addition to security holes, improperly trained administrators can take down critical parts of the network or inadvertently introduce new security holes. **GHEM Secure Access Control is a secure remote access application that provides strict access and real-time monitoring to disparate network elements across the enterprise**. All administrative traffic to a network element is routed through a GHEM server making it an administrative gateway to all critical network elements. GHEM Secure Access Control controls access and can limit commands to a network element by user or group, enforcing 'zero trust'. The system classifies ports giving automated systems or select users' priority access to specific ports. In addition, GHEM Secure Access Control supports aliases so network elements can be searched by other names such as CLLI codes. Authentication protocols such as LDAP and Active Directory are integrated into the system to make user administration a snap. With a user-friendly, web front-end, GHEM Secure Access Control makes it easy for administrators to globally view all port and monitor user activity across the enterprise. In addition, GHEM Secure Access Control provides a web terminal so end-users do not have to install or maintain additional emulators. Having implemented the application at small, medium and large telecommunications customers across the globe, GHEM Secure Access Control is the manageable secure solution for your telecommunications network.

Background

Telecommunication companies have a large quantity and variety of critical network elements to support their telecommunications infrastructure. The variety of equipment requires multiple communication protocols and custom logon scripts to maintain the equipment. This equipment is normally dispersed over a large geographical footprint making it uneconomical to maintain equipment locally.

Companies managing telecommunication networks require efficient, standard, and secure means to remotely administer all of their equipment. Companies prefer a solution that uses commodity hardware, leverages existing authentication systems, that doesn't require additional software dependencies or technical expertise to operate.

Price of a Security Breach

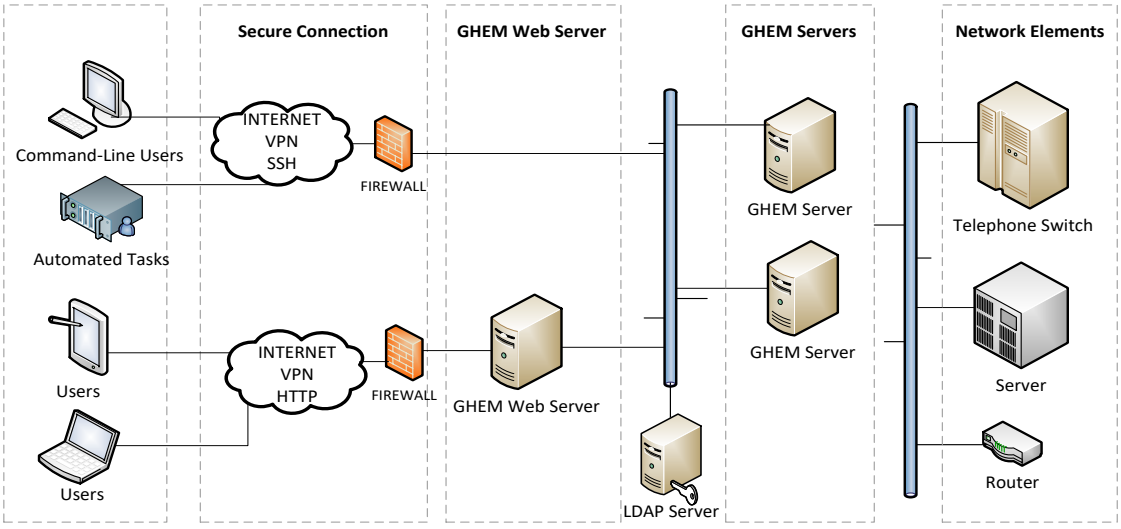
Access to the network gives unauthorized users ability to perform malicious attacks and steal proprietary information. **The average cost to a company for a security breach in 2020 was over 8.6 million dollars**. Therefore, the liability for a telecommunication company handling thousands of organizations is in the billions of dollars.

Cost of Neglect

In addition, today's economy puts demands on fewer resources to maintain the constantly changing network infrastructure. Fewer resources with additional work and/or relying on improperly trained resources turn into neglect. According to the Ponemon Institute, ***thirty nine percent of organizations say that negligence was the root cause of the data breaches***.

Solution

With decades of experience in the software, security, and telecommunications industry, Valbrea teamed with partners to deliver an economical, yet very robust security application called GHEM Secure Access Control. GHEM Web provides a user-friendly, web front-end to GHEM. GHEM, Global Host Element Manager, is a command-line based system that manages all of the security features of the network application. The diagram below shows how GHEM Secure Access Control is configured within a network.



All administration traffic is routed through GHEM Servers by statically connecting ports (or nailing-up ports) from the network elements to the GHEM servers. This prevents other devices from attaching to the network elements. (*An option is provided for dynamically connecting ports but is not recommended.*)

The system highlights are as follows:

Manage Access to Network Elements

- Restrict User Access by Individual or Group
- Limit User Commands by individual or Group
- Optimize Access (one side-effect of static ports if waiting on a port to become available. GHEM Secure Access Control allows users to log them in as soon as the port becomes available)
- Automatic Port Timeouts to Clear Inactive Sessions
- Single Sign On (SSO) for all Network Elements (Supports LDAP and Active Directory)

- Designate Priority Access to Ports using Port Classification (for automated tasks or super users)

Monitor Network Elements

- Monitor and Control Any User's Session in Real-Time.
- Ability to Override User Commands or Disconnect User in Real-Time.
- Real-Time View of Every Port (administrator can see all activity across the enterprise)

Audit Features

- Logs connections and all user commands to a host
- Creates Session Files that allow administrators to replay a user's entire session.

Connectivity

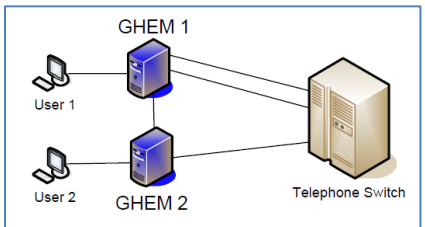
- Supports the following methods of connectivity for network devices: telnet, SSH, Modem Ports, and X.25.
- Manages ports to throughput. Therefore, since many central office port cards are set to different baud rates for input and output port speeds, GHEM will manage this appropriately. GHEM natively supports legacy IBM X.25 cards (AIX). X.25 is port dependent on the TP4 (i.e. 64 port/128 port connections); therefore, utilizing existing or same type port master cards would provide the smoothest transition.

Scalability and Failover

To successfully secure a large telecommunications network, the solution had to scale and be fault tolerant. The simplicity of GHEM Secure Access Control makes it easy to scale by adding additional hardware. For small to medium-sized customers, adding memory and disk space handles most scalability issues. Larger customers would add additional servers.

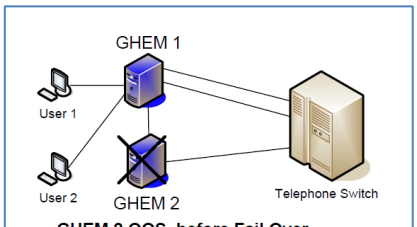
Failover requires additional servers. Below is a sequence of diagrams to illustrate how GHEM handles failover.

1



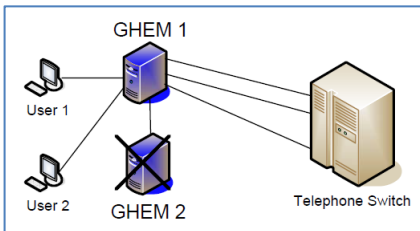
Normal Operation
User 1 can use all 3 switch connections
User 2 can use all 3 switch connections

2



GHEM 2 OOS, before Fail Over
User 1 can use 2 switch connections
User 2 can use 2 switch connections (must manually connect to GHEM 1

3

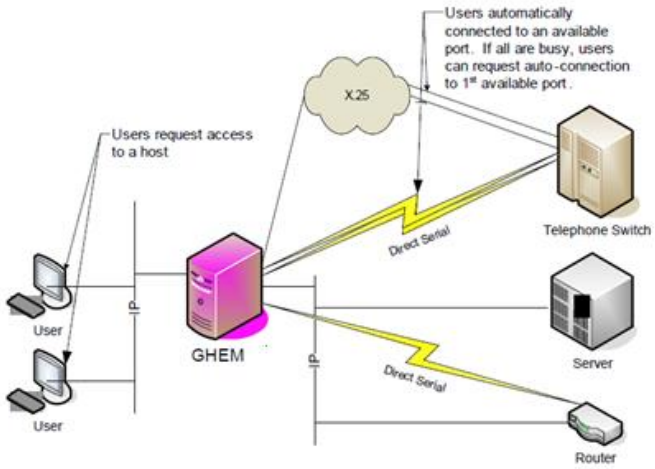


GHEM 2 Failed Over to GHEM 1
User 1 can use 3 switch connections
User 2 can use 3 switch connections
GHEM Admin must manually activate connections on GHEM 1

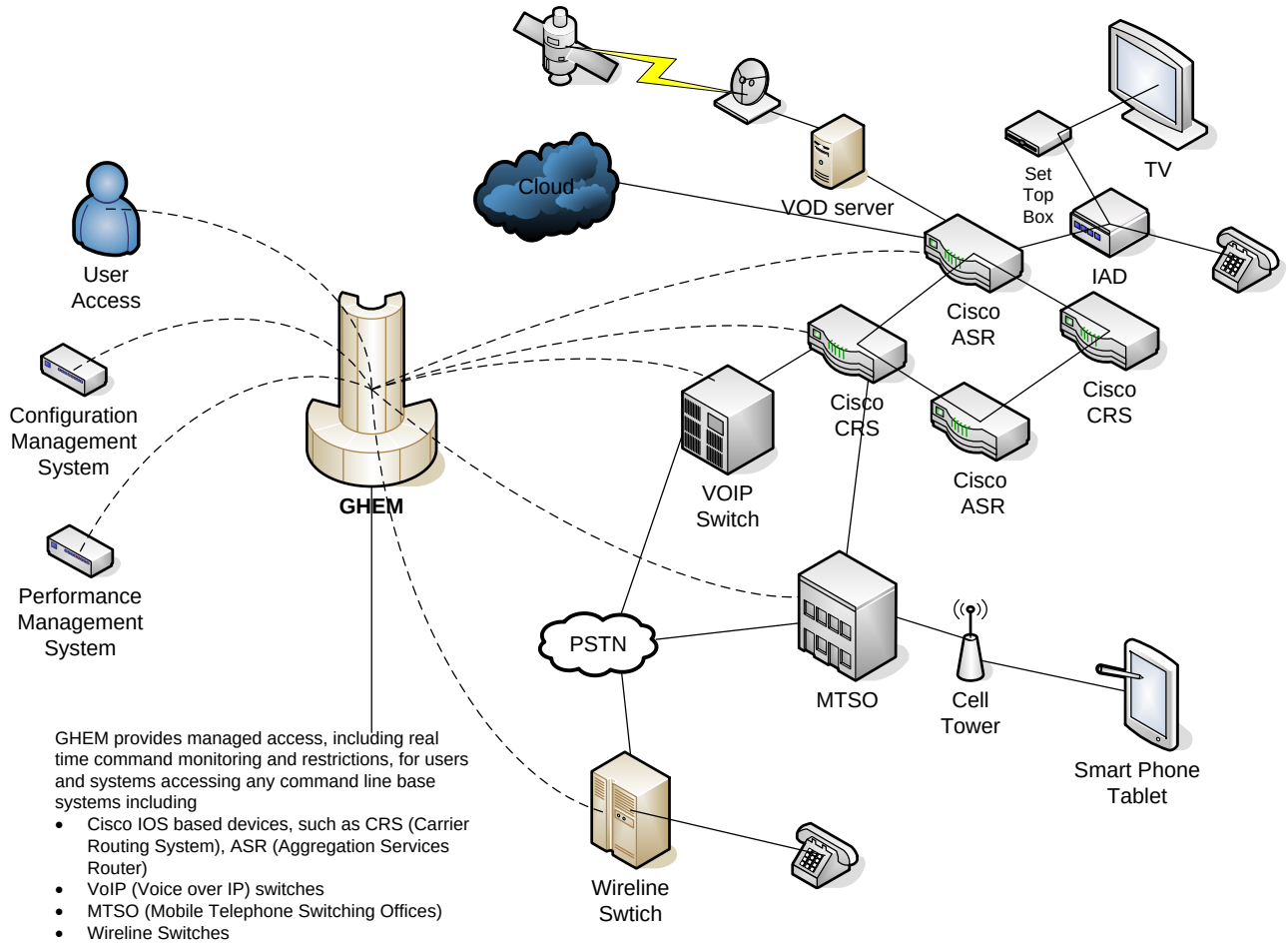
Implementation Scenarios

GHEM Secure Access Control can be implemented in any size telecommunications environment using a variety of configurations. Typical implementation scenarios are within the telecom industry and are shown below:

Traditional Telco



CLEC – Competitive Local Exchange Carrier

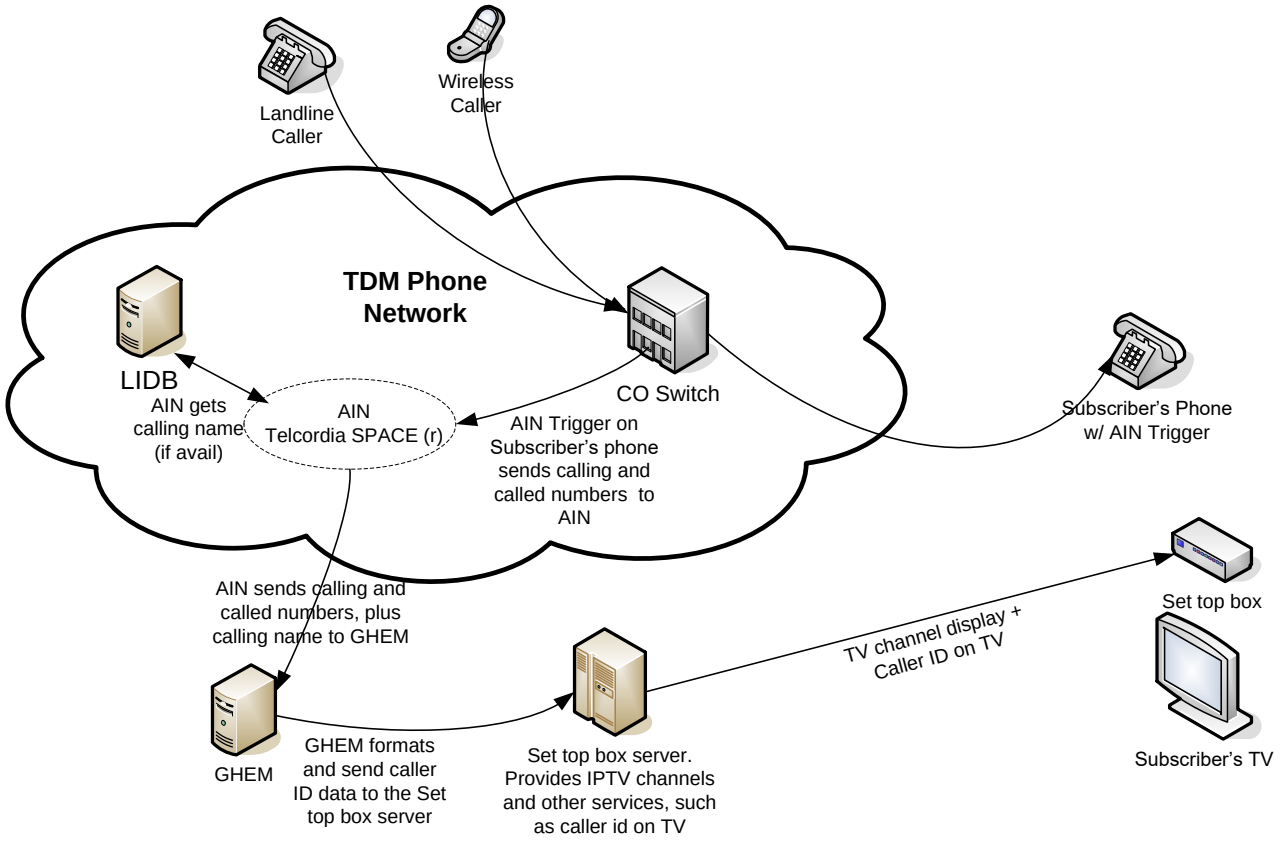


Additional Features

Since GHEM already contains technology to communicate within the telecom network, GHEM can be customized to perform additional tasks.

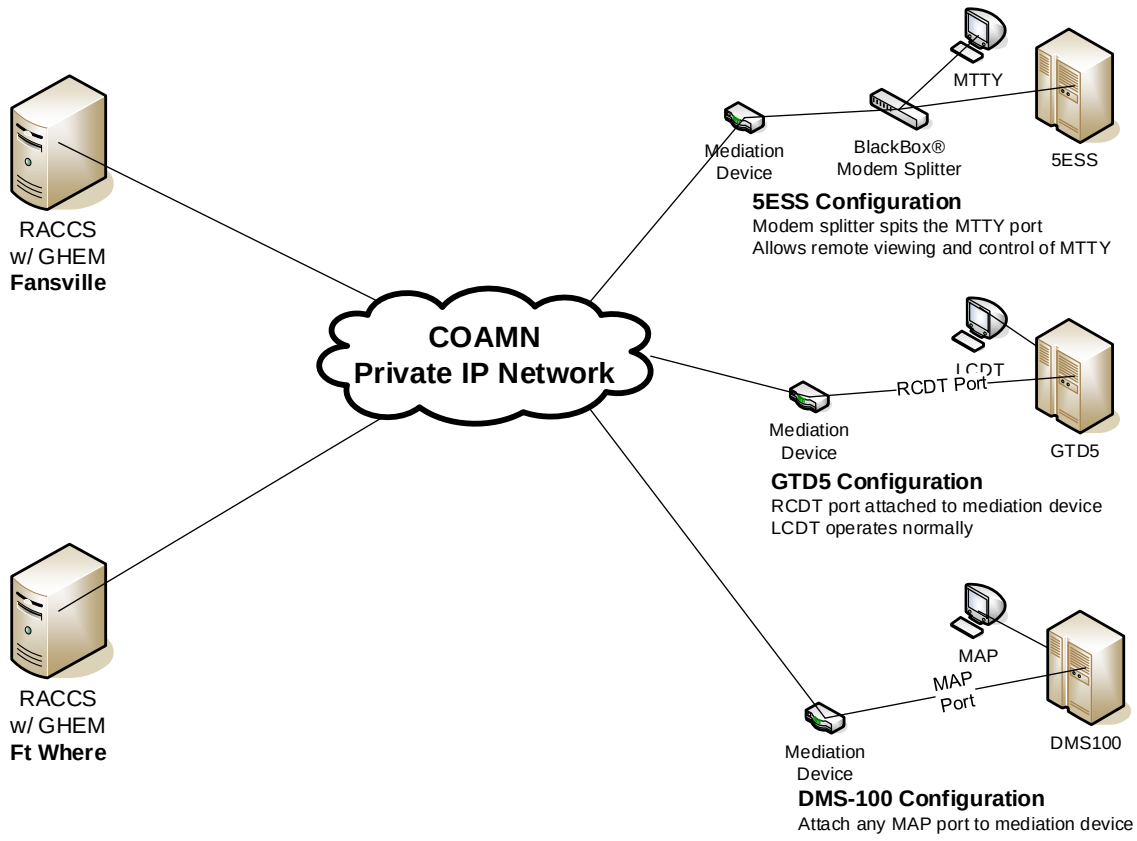
Caller ID on TV Module

In this scenario, GHEM is used to display caller id information on a subscriber's television.



Remote Alerting and Console Control System (RACCS)

RACCS provides authorized users remote access capabilities to the master console port of certain network elements, visibility into and a log of recent alarms filtered by priority which have occurred and are available only through the master console port for alerting and critical system recovery via the master console port of the individual network elements. Examples of network element types are the GTD5, DMS100, and 5ESS.



Benefits

GHEM Secure Access Control has been successfully implemented in small, medium and large telecommunication companies in several countries. The system's design and functionality deliver results that include:

- Proven Technology
- Ease of Implementation
- Requires Minimal Training
- Runs on Standard, Commodity Hardware
- Leverages existing user authentication systems such as LDAP or Active Directory
- Does not require the expense of a database or database administrator

Specifications

Below is a list of current specifications required for GHEM Secure Access Control:

- Currently supported on AIX or Linux 32-bit platforms.
- Other Unix variants are possible providing that variant supports the GNU C compiler.
- GHEM currently relies on hardware solutions for application failover and redundancy.
- Server sizing must be determined based on the user load, data storage, and number of X.25 ports required for a particular server. Since X.25 is a required technology, we recommend the use of IBM servers which support the built-in X.25 card. GHEM currently supports this card up to AIX version 5.2. Later versions of AIX are possible, but further testing would be required to certify the drivers for the X.25 card.
- GHEM also supports, although testing for specific devices would be required, external IP-to-X.25 mediation devices should the customer prefer this hardware option. In this case either AIX or Linux would be supported.
- GHEM stores all data in flat files locally on the application server; therefore, the system has no database or storage provider requirements.