Network and Security

EXECUTIVE SUMMARY

SUMMARY

ClubHouse Online E3 provides an industry leading Web Site solution, fully integrated with your Club Management System using industry best practices in network and security infrastructure.

FLEXIBILITY

The Web solution itself provides unsurpassed flexibility and should meet or exceed even the most security conscious IT requirements in areas such as: Authorization, Authentication, Encryption and Network Infrastructure.

DATA SECURITY

All data travelling between ClubHouse Online E3 is fully encrypted using a customized X.509 Certificate and TripleDES encryption algorithm *(used by the Electronic Payment industry).* We explicitly ensure that data is only sent from the Club Management Server to ClubHouse Online E3 and only to the ClubHouse Online E3 server.

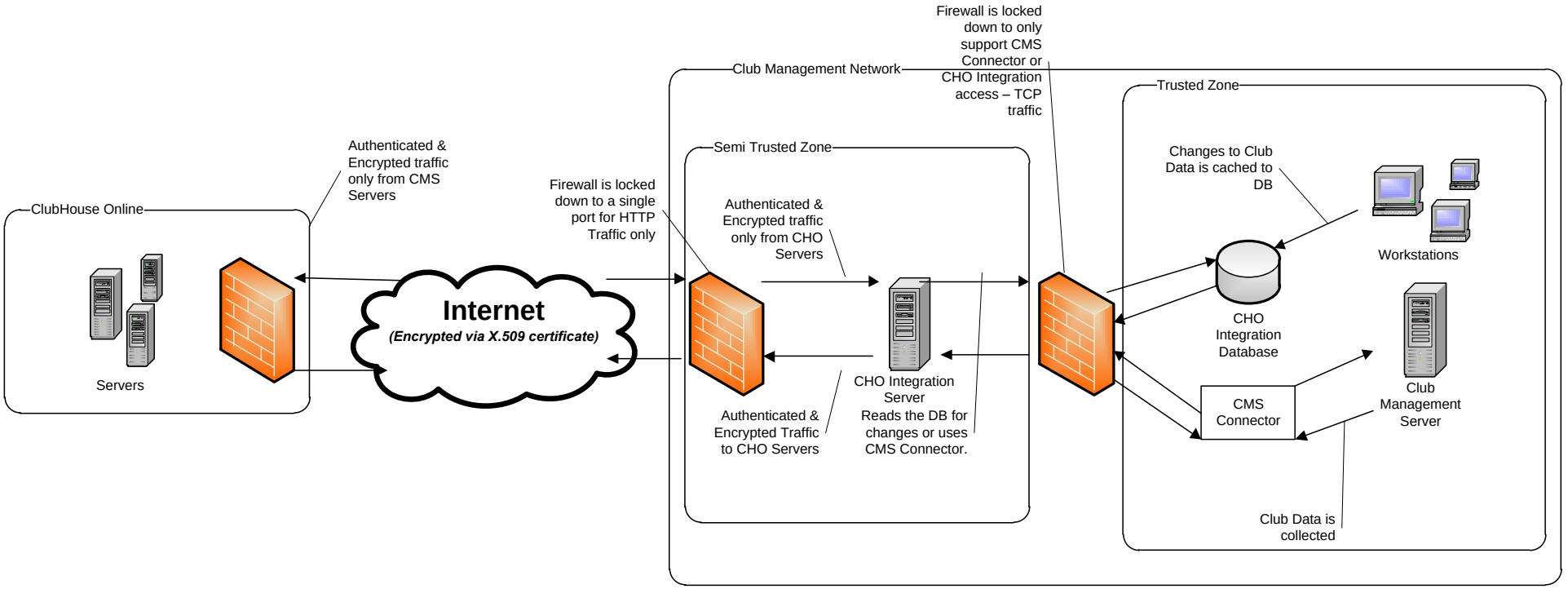
NETWORK SECURITY

ClubHouse Online E3 architecture fully supports a DMZ network utilizing Semi-Trusted and Trusted Zones. All traffic can travel over a single port (configurable by the club) and servers can be hardened to ensure best practices for Network and Security.

CONTENTS

NETWORK ARCHITECTURE

ARCHITECTURE DIAGRAM



OVERVIEW

CLUBHOUSE ONLINE E3

ClubHouse Online E3 is the centralized Web Server farm that houses the Web Solution. It consists of a firewall, load balancer and multiple servers to process requests that come from Club Management Software to ensure maximum uptime. All data that is passed to ClubHouse Online E3 uses 2 X.509 Certificates to validate the request coming in. The first is the central ClubHouse Online X.509 server certificate; a club will not send data to any server that does not contain this certificate. The second is the club's personal X.509 client certificate; the data from the club is decrypted using the club's certificate information – if that does not match the information that ClubHouse Online E3 has for that client, the request will fail. Without access to the club's client certificate it is not possible to decrypt the data.

These two security measures ensure that:

- No data is sent to any system other than ClubHouse Online E3.
- No one other than ClubHouse Online E3 can read the club's data.

CLUB MANAGEMENT NETWORK

The club's servers are stored within the club's own network which should be protected by a firewall for all incoming connections. We recommend that club's setup a ***Semi-Trusted Zone*** that contains the CHO Integration server and is protected by a firewall from connecting to the Club Management System. This provides a buffer zone that separates the club's internal network from the often untrusted (and possibly hostile) zone of the Internet. The Club's ***Trusted Zone*** is the protected internal network that should be kept as secure as possible.

SEMI-TRUSTED ZONE

This zone part of the Club Management Network and is owned / maintained by the Club. It separates the Internet and potential hackers from your Club Management system. What does having a Semi-Trusted Zone accomplish? It allows the club to open up their network to the internet (which is required for ClubHouse Online E3 to work), without exposing their entire network to the internet. It is easier to hack any computer that is exposed to the Internet therefore any computer that does not need to be exposed to the internet – should not be and should not be directly exposed to a computer that is exposed to the internet.

Best Practices for the Semi-Trusted Zone:

- It should have a different domain from the internal domain. It should be separated from both the Internet and the internal network by a firewall
- Only the specific ports required for the application to run should be open and available on either firewall
    - We recommend only opening a single port for HTTP traffic from the Internet
    - We recommend only opening 2 ports for the CHO Integration server into your Trusted Zone
        - One for the CMS Connector
        - One for the CHO Integration Database

TRUSTED ZONE

The internal network is the trusted zone. This is the isolated network which your club runs on. In the unlikely case that the CHO Integration Server is hacked, the rest of your network will not be compromised because it's on a completely separate, isolated network.

The key aspect of this architecture is that your club servers and data are not, at any point, exposed directly to the internet; nor are they on any computer that is directly exposed to the internet.

CHO INTEGRATION SERVER

The CHO Integration server runs within the Semi-Trusted Zone. It provides connectivity to ClubHouse Online E3 via IIS Web Services using X.509 certificates over HTTP. All traffic sent by the CHO Integration server to ClubHouse Online E3 is fully encrypted using TripleDES[1] and all connections to and from the ClubHouse Online E3 server are validated with X.509 Certificates. The CHO Integration Server will not connect to any web service that does not present the ClubHouse Online E3 Server Certificate.

Connecting to the Trusted Zone is only done over 2 ports – one for data connectivity to the SQL Database and the other is TCP access to the Club Management Server.

[1] TripleDES is considered to be one of the best public encryption algorithms. It is the standard algorithm used by the electronic payment industry.

CLUB MANAGEMENT SYSTEM

OVERVIEW

This section provides an overview of the servers and components required for ClubHouse Online E3 for the Club Management System and Servers. As described above, there are two main servers for the Club Management System architecture: the CHO Integration Server and the Club Management Server.

The CHO Integration server is the server that connects your Club Management System to the internet and represents the Semi-Trusted zone.

The Club Management Server is the server that houses your Jonas or CSG system and represents the Trusted zone.

CHO INTEGRATION SERVER

The CHO Integration server is responsible for all connectivity and security between the Club Management Server and ClubHouse Online E3. A specific set of services are deployed to manage that connectivity and security and to ensure reliability of all messaging.

On the CHO Integration server we deploy:

- Data Integration Web Service
- Club Photo Integration Web Service
- Reliable Message Queuing (RMQ) Service
- Club Management Polling Service
- Remote Update Service

DATA INTEGRATION WEB SERVICE

This Web Service is the main integration point between ClubHouse Online E3 and the CHO Integration server. This server receives all requests from ClubHouse Online E3 and processes them to send data back via RMQ. Very little data is ever sent back to ClubHouse Online E3 via the Web Service itself.

CLUB PHOTO INTEGRATION WEB SERVICE

This Web Service is a REST Web Service, optionally deployed, designed for displaying the Club Management System's photo on ClubHouse Online E3.

RELIABLE MESSAGE QUEUING (RMQ) SERVICE

This Windows service is designed to reliably send messages from the Club Management System to ClubHouse Online E3. It uses a queuing process to ensure that all messages are delivered successfully and in the sequence that they arrived in.

CLUB MANAGEMENT POLLING SERVICE

This Windows service is designed to poll your Club Management System for changes and to send those changes back to ClubHouse Online E3 via RMQ.

REMOTE UPDATE SERVICE

This Windows service is designed to poll the ClubHouse Online E3 Webservice to determine if there is an update required for any of the above services. If required – it will download and install those updates.

CLUB MANAGEMENT SERVER

The Club Management Server is your main Jonas or CSG server.

On the Club Management Server we deploy:

- Club Management System (CMS) Connector
- CHO Integration Database
- Remote Update Service

CLUB MANAGEMENT SYSTEM (CMS) CONNECTOR

The CMS Connector is a TCP listening component which awaits commands from the Data Integration Web Service, Club Photo Integration Web Service or the Club Management Polling Service. It's responsible for all connections to the Club Management System itself.

CHO INTEGRATION DATABASE

This database holds all of the clubs messages and updates to be picked up by the various services before they are sent to ClubHouse Online E3.

REMOTE UPDATE SERVICE

This Windows service is designed to poll the Integration Server's Remote Update Service to determine if there is an update required for any of the above services. If required – it will copy and install those updates.

CLUBHOUSE ONLINE E3 SERVER

OVERVIEW

ClubHouse Online E3 is a centralized Web Server farm secured online by Rackspace (www.rackspace.com), one of the world's leading hosting providers. They facilitate and manage the network and security infrastructure – ensuring that ClubHouse Online E3 is up to date with the latest firewalls, software, patches, anti-virus, anti-spyware, intrusion detection services.

WEB FARM

The web servers are managed within a Web Farm ensuring that there is always a server to meet requests and there is minimal downtime. Even for most application upgrades there does not need to be any service outage – since half of the servers in the Web Farm continue to handle requests while we upgrade the other servers with the latest application. Once the application has been upgraded on the first half of the servers, we upgrade the other set of servers; while continuing to process requests on the first half.

SECURITY

Security is one of the key features of ClubHouse Online E3. It uses its own security system that is based on the standard .NET security features.

AUTHENTICATION

Usernames and passwords are chosen by the member themselves are passwords and never available within the system. Passwords, once stored in the database, are never retrieved from it or passed externally. It is not possible for anyone to determine what an existing user's password is. The club gets to determine the complexity of the passwords including complex and high security passwords. Additionally we have other precautions such as locking users out of the system when too many invalid attempts occur.

AUTHORIZATION

ClubHouse Online E3 allows users to easily grant permissions for particular modules or particular pages or site sections. You can assign permissions to a particular user or set of users quickly and easily.

CONTENT PERSONALIZATION

ClubHouse Online E3 allows users to control the access rights of site visitors. They can create secured sections of the site that are only accessible by registered visitors. Club's members can have personalized navigation and content based on their permissions, so clubs can display different content to members, board members, employees or any other segment within a ClubHouse Online E3 site.

ENCRYPTION

All of our sites work under SSL to encrypt all data travelling between the website and the member's browser. Additionally, all data between a Club Management System's server and ClubHouse Online E3 is encrypted and signed using X.509 Certificates ensuring that the data is only sent to ClubHouse Online E3 and is only readable by ClubHouse Online E3.

CREDIT CARDS

ClubHouse Online E3 does not directly process or store Credit Card information. Any processing or storage of credit card information is done by a 3rd party provider and is not part of the ClubHouse Online E3 solution.

FAQ

PCI COMPLIANCE

IS CLUBHOUSE ONLINE E3 PCI COMPLIANT?

ClubHouse Online E3 is not in scope from a PA-DSS standpoint because it doesn't store, process, or transmit cards. However, from an overall PCI standpoint web sites and how they communicate is something that needs to be considered when the club is reviewing their PCI compliance efforts. ClubHouse Online E3 does require a port to be open in the firewall in order to be able to communicate with the Club Management back office system. With this being said, the ClubHouse Online E3 solution has been architected so that the programs required to communicate with the Club Management back office system can run on a single server (i.e. same server that is hosting the Club Management back office core applications) or from an integration server that sits in a DMZ. The choice of how they want to setup E3 to communicate with their Club Management back office system is really up to the client. In the event that a client is running a credit card processor that uses token based technology for handling credit cards (e.g. ETS Transvault or CreditLine Secure) then it would be less of a security risk if E3 and the Club Management back office system were running on a single server since only tokens would be stored on the server.

For clubs that are concerned about PCI compliance - our recommendation is that E3 is installed with an integration server (stored in a DMZ); this solution should cater to the club's PCI effort.

If a club chooses to not use the integration server this configuration may not cater to the club's PCI effort. It's very unlikely that any club server with IIS installed that directly connects to the internet will be PCI compliant.

In the end we strongly recommend that you follow up with your PCI Qualified Security Assessor.

INTEGRATION SERVER

WHY SHOULD I USE AN INTEGRATION SERVER?

Any computer within your network that is connected to the Internet, directly or indirectly, is a potential risk for an attack from viruses or external attackers. As a security best practice; any computer that does not need to be exposed to the Internet should not be – nor should it be directly exposed to a computer that is exposed to the internet.

An integration server in a semi-trusted zone allows the club to open up their network to the internet (which is required for ClubHouse Online E3 to work), without exposing their club server or other parts of their network to the internet. This provides better security to their vital club data.

DO I NEED AN INTEGRATION SERVER?

No, ClubHouse Online E3 does not require an integration server; but it's strongly recommended for security purposes. If you choose not to use an Integration Server – ClubHouse Online E3 will use your club server directly and your club server will be directly exposed to the Internet. This will increase the potential risk for an attack on your club server.

DO I NEED TWO PHYSICAL SERVERS? (CAN I USE A VIRTUAL SERVER)?

The integration server does not need to be a separate physical server – we have tested a large number of implementations of the integration server as a virtual server using various virtualization environments (including Microsoft Hyper V, Citrix XenServer and Sun xVM). We fully support the integration server (or the club server) as a virtual server.

DO I NEED AN INTEGRATION SERVER TO BE PCI COMPLIANT?

If the club is concerned about PCI compliance - our recommendation is that E3 is installed with an integration server; this solution should cater to the club's PCI effort.

If the club chooses to not use the integration server this configuration will not cater to the club's PCI effort. It's very unlikely that any club server with IIS installed that directly connects to the internet will be PCI compliant.

Either way, we recommend that you follow up with your PCI Qualified Security Assessor.

HOW DOES CLUBHOUSE ONLINE E3 PROTECT MY DATA?

We install secure web services on the server which can only be accessed if you have our private X.509 certificate.

All of the data sent / received on the web service is encrypted via Triple DES Encryption (http://en.wikipedia.org/wiki/Triple_DES). This is the same standard used by the electronic payment industry. Each club is provided their own unique private key via an X.509 Certificate.

All data on the ClubHouse Online E3 servers are secured with the latest firewalls, software, patches, anti-virus, anti-spyware, intrusion detection services.

IS THE REMOTE UPDATE SERVICE REQUIRED?

No, you do not have to install the Remote Update Service. It is a recommended service as it will improve the ability of our support team to assist you and ensure that you always have the latest code installed on your servers.