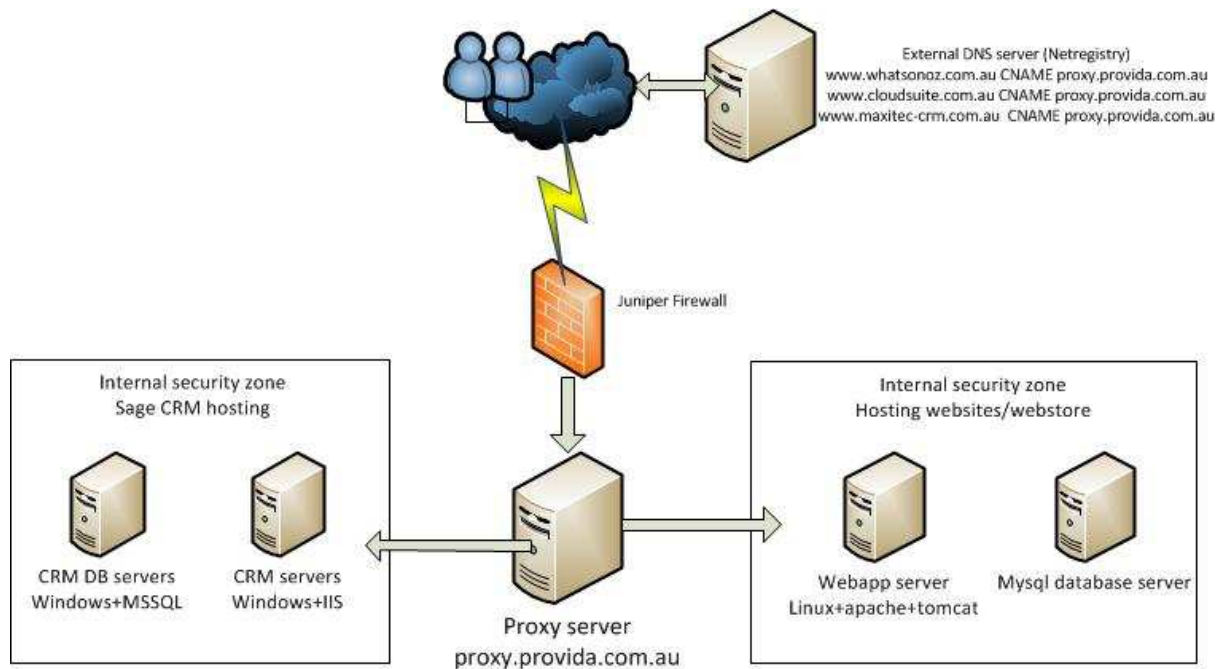

CRM/Web Store/Web Site

Hosting Security White Paper

Version 1.04

14 November 2011

1. Structure



2. Data flow

To access the hosting server, all users from the internet will go through the flow as per below:

- 1) Internet connection -- 10 MB dedicated symmetrical link via Internode
- 2) Juniper firewall – hardware firewall
- 3) Proxy server – Iptables firewall and mod_security
- 4) Web application server -- Iptables firewall
- 5) Mysql Database -- Iptables firewall

3. Juniper firewall

This is robust and popular firewall hardware in the network security area. Provida uses the SSG Series which is a purpose-built, high performance platform that delivers WAN connectivity and security, plus the muscle to protect the high-speed LAN against internal network and application-level attacks while simultaneously stopping content-based attacks.

The SSG Series firewall provides a comprehensive set of Unified Threat Management (UTM) security features including stateful firewall, IPSec VPN, IPS, antivirus (anti-spyware, anti-phishing, anti-adware), anti-spam, and Web filtering.

The Juniper firewall protects the network at the first instance. It limits certain services/ports which can be accessible from outside the Provida hosting framework.

4. IPTABLES firewall

This is a software firewall running on most of the linux servers and giving the basic host/OS level protection.

5. Proxy server

RHEL (Red Hat) 6 Linux server + iptables firewall + apache + proxy module + security module.

The proxy server is the reverse proxy for all the websites, CRM web applications and web store applications. With the apache security module, the http server can detect any external attacks on the network.

6. Webapp server

RHEL 6 Linux server + iptables firewall + apache + tomcat

7. Database server

RHEL 6 Linux server + iptables firewall + MYSQL server

8. Backup

All servers are backed up using VEEAM software, according the schedule. This is Operating System (OS) and file level backup which will allow recovery of the OS or file in the event that disaster recovery is required.

The MYSQL database is backed up by script according to the schedule. This will allow database level recovery which will not affect the OS and other databases running on the same database host.

The MSSQL database is backed up according to the MSSQL backup plan schedule.

9. Security of data transfer between Nimbus Web Store and Sage database

The web store is integrated with the Sage software database which means the web store will exchange data to and from the Sage database. Data includes customer, order, pricing and product information.

Provida uses "sData" with HTTPS and Digest with Linux server hosting to achieve data transfer securely. "sData" is developed and owned by Sage Software PLC, a UK based publicly listed company. It is a REST-style web services protocol which will ensure efficient and secure data exchange over HTTPS.

As such the following security protocols apply to the Nimbus web store:

1) Data transfer with HTTPS

All data will be encrypted by the CA (Certificate Authority) certificate which is issued by a Trusted and Endorsed CA association. This will secure the communication over the internet. At present all the web style applications rely on HTTPS for secure communication such as, online banking. The cost of the security certificate will be built into monthly web store fee, but if clients prefer they can arrange their own security certificate.

Provida currently uses Security certificates from GoDaddy (US) and Crazy Domains (AU). The web store and its data are secured with a 128/256 bit encryption that will ensure safe and secure e-commerce transactions over the internet. The SSL certificate is trusted by all major browsers including IE, Opera, Chrome, Safari and FireFox. Provida offers SSL certificates for shopping cart and credit card transactions as well as the sData transfer layer between Sage software and the web store. The SSL certificate issuer offers up to \$10,000 warranty insurance for any security breach.

2) Authentication with Digest

Digest access authentication is one of the agreed upon methods a web server can use to negotiate credentials with a user's web browser. It uses encryption to send the password over the network which is safer than basic access authentication that sends plain text.

Basically, the client starts by making an un-authenticated request to the server, and the server responds with a 401 response indicating that it supports Digest authentication. The server also sends a *nonce*, which can be thought of as an opaque token. The client then re-requests the resource, sending up the username, and a cryptographic hash of the password combined with the nonce value. The server then generates the hash itself, and if it matches the request's hash, the request is allowed.

The authentication has to be finished before any further communication between back end ERP system and the web store can be processed. It is not necessary to apply Digest since all data has been encrypted by HTTPS, but this can still enhance the security when doing authentication at the first step. It is extremely difficult to hack the password after it has been hashed using Digest.

3) Hosted Linux Server

All Provida web stores are hosted on a Linux (Red Hat) Enterprise grade server. Since Linux does not rely heavily on Remote Procedure Calls (RPC) like Windows

and was built from the ground up with a multi-user Unix architecture, it is more secure from hacking and virus attack.

Hosted clients have some other options regarding data transfer:

- 1) VPN, Site to Site VPN need to be setup and all data will be encrypted. So all traffic between web store site and Sage database site will be protected. **THIS WILL NOT BE AS SECURE AS SDATA WITH HTTPS.**
- 2) Hosting both the Sage database and the Nimbus web store at the Provida hosting centre. Since all traffic occurs at our data centre internally, no additional security is required.

(END OF DOCUMENT)