Network Requirements for Internet & POS

Version 1.60 10/07/2010

Introduction

KWI requires a firewall, which can filter (block) both incoming and outgoing services by IP address/Protocol/Port and also by URL and (not just specific IP address, protocol, port number combinations). All firewalls can block incoming services, but not all firewalls can block outgoing traffic by URL address.

It is important to filter outgoing traffic by URL to limit the applications which the POS is allowed to connect to externally, and to stop any Trojans or viruses which do make it inside the security perimeter from phoning home (remote control). Outgoing traffic filtering helps to prevent your site from being used as a spam relay or to spread infections to others.

You should treat the requirements detailed in this document as a baseline security policy for traffic entering and leaving the store. If your business requires an "Intranet" between your store and corporate locations you should enhance this policy to prevent rogue traffic between sites within your own internal network.

Standardized Store/Internet Configurations

In order to provide standardized services, KWI needs to connect to stores using IP over the public Internet. KWI can not provision individual VPNs to each store.

KWI also requires simultaneous access from its Help Desk to all clients' stores. KWI can not utilize a PC Anywhere gateway where effectively only a single connection is granted from KWI to be shared across all stores. A "single session gateway" prevents KWI from having multiple Help Desk technicians working on stores simultaneously creating a bottleneck where only one technician can access a single store at a time.

Standardized Store/Internet Configuration Goals

The only TCP/IP access that should be allowed are the addresses & services listed below (in addition to any access that is needed for the Client's day to day business). This policy is designed to limit Spyware and Virus programs from the Internet.

1. Outbound SSH (secure shell) allows access to KWI's SFTP polling. SSH/SFTP requires TCP port 22 outbound to kligerweiss.net, ftp1.kligerweiss.net, ftp2.kligerweiss.net , ftp3.kligerweiss.net, ftp4.kligerweiss.net, ftp5.kligerweiss.net, ftp6.kligerweiss.net, ftp7.kligerweiss.net, ftp8.kligerweiss.net, ftp9.kligerweiss.net, ftp10.kligerweiss.net.
2. Inbound PC Anywhere for KWI help desk support. PC Anywhere requires UDP & TCP ports 5631-5632 inbound from 65.206.45.0 /26, 204.249.103.0/26, 65.51.69.64/26, and 65.51.37.192/28
3. Microsoft's File sharing (CIFS/SMB shared drives) from the POS terminals to external locations must be blocked. KWI does use shared drives within the store for application & support purposes (selected files & directories are shared between registers within a store). This requirement can be met by blocking UDP ports 137 & 138 and TCP ports 139 & 445 (both in and out) at the firewall.

4. Websites for Symantec NAV Live Updates:
   http://liveupdate.symanteclivеupdate.com (Primary)
   http://liveupdate.symantec.com (Secondary)
   ftp://update.symantec.com (Last)
5. KWI Website for Java Merchandising Application: http://www.kligerweiss.net/, https://www.kligerweiss.net/, 65.206.45.0/26, 65.51.69.64/26 and 65.51.37.192/28 for access to KWI's Back Office Java application servers on ports 80, 8080, 8443 and 443 TCP and UDP for access in and out at the firewall. For security reasons this access should be restricted to http://www.kligerweiss.net/, https://www.kligerweiss.net/.
6. For Internet credit card processing on the First Data North and South platforms using Datawire IPN, KWI requires the following DNS addresses are accessible:

URL	IP Address	Port
https://vxn.datawire.net	216.220.36.75	443
https://vxn1.datawire.net	129.33.160.116	443
https://vxn2.datawire.net	64.243.142.36	443
https://vxn3.datawire.net	206.112.91.167	443
https://support.datawire.net	66.241.131.100 69.46.100.78	443

   To access the First Data "test" systems using Datawire IPN, KWI requires the following DNS addresses are accessible:

URL	IP Address	Port
https://staging1.datawire.net	65.110.169.83	443
https:// staging2.datawire.net	69.46.100.76	443
https://stagingsupport.datawire.net	66.241.131.101 69.46.100.81	443

7. KWI needs the Static IP address info with unique subnets for the stores. Every location will need to have a public NAT (or have a range of publics) for KWI help desk to be able to access the terminals for support.
8. DNS must be enabled on the POS devices. The POS must be able to gain access to a DNS server to allow address resolution. KWI will not support manually created static host table entries at POS where specific DNS filtering is not available. This will allow easy access to your desired Internet resources using traditional "www.kligerweiss.net" type names and/or migration once specific rotating IP change.
9. To sync the time IP address 192.5.41.209 UDP port 123 needs to be available and open to SNTP traffic.
10. POS health monitoring software for Fujitsu Team POS 3000 hardware will use SMTP (port 25) to relay hardware issues detected back to KWI via **smtp.com**.

11. For Internet gift card processing to Profit Point, KWI requires the following sites are accessible:

URL	Port
https://www.wa.rewardforloyalty.com:8417/NetConnect/controller2	80
http://crl.verisign.net	80

For Internet gift card processing to Profit Point, KWI requires the following services are accessible:

SNAP External Services			
Service	**Host**	**IP address**	**Ports**
Raw IP Transactions	ipgw.profitpointinc.com	68.234.43.47	443
Web site	snap.profitpointinc.com	68.234.43.48	443
Web site	merchants.profitpointinc.com	68.234.43.49	443
Web site	admin.profitpointinc.com	68.234.43.50	443
API Interfaces	api.profitpointinc.com	68.234.43.51	443
Balance Checker	checkbalance.rewardforloyalty.com	68.234.43.39	80, 443
User Registration	register.rewardforloyalty.com	68.234.43.36	80, 443

To connect to the Profit Point "test" system, KWI requires the sites are accessible:

URL	Port
https://www.wa.rewardforloyalty.com:8417/NetConnect/controller	80
http://crl.verisign.net	80

12. For clients utilizing AJB credit/debit/check/gift card engine, the router at store level needs to have Internet dial backup capabilities as AJB uses strictly IP connections to all processors. The store router needs to automatically failover to dial backup immediately when it senses there is no connectivity to the Internet.
13. Versions of the Java run time plug-in for Internet Explorer will need to be upgraded from time to time to compliment new functionality being added to the back office system. For this: http://java.sun.com should also be left open.
14. E-mail from KWI to customers may come from two domains: kwi.com and kligerweiss.net. Generally, human e-mail will come from the kwi.com domain, while automated e-mail (reports, etc.) will come from one of two addresses: DoNotReply@kwi.com (display name "KWI") or files@kligerweiss.net. Both domains should be trusted and excluded from spam filtering to prevent reports and general correspondence from failing to be received by the intended user base.

Client Review and Sign Off

We acknowledge that we have reviewed the above documentation and agree to meet the requirements and specifications as outlined.

Name (Print)

Signature

Date

Change History

Version	Date	Item	Change
1.60	10-7-2010	5. KWI Website…	Retired IP range: 204.249.103.0/26
1.60	10-7-2010	6. For Internet credit…	Corrected IP Address typo: https://vxn2.datawire.net (64.243.142.36)
1.60	10-7-2010	11. For Internet gift…	Added Production URL: http://crl.verisign.net Added "test" system URLs