StoreNext

Technical Bulletin

Protecting POS Lanes with Internet Connections for Connected Payments

CP-TECH-08:08
June 11, 2008

Most dealers have set up their customers' stores so that Internet access is not available to POS lanes. While this is a good practice, the standard Connected Payments setup requires that each lane has Internet access.

Internet access will not put the lanes in jeopardy if basic security is installed. Reasonable protection is neither expensive nor difficult to implement. And since the standard Internet security setup recommended for Connected Payments is fundamentally mandated by the PCI Data Security Standards anyway, stores may as well gain the advantages of lane-by-lane replication and POS independence that Connected Payments offers.

There are three typical and straightforward security recommendations for POS lanes when they are connected to the Internet:

1. ***Install Solidcore*** — this is plug-and-play with ISS45 and ScanMaster, and PCI requires A-V on the lanes anyway (see Reference Bulletin 1215).
2. ***Get a firewall*** — this can be as simple as installing a freeware software firewall on each lane.
3. ***Both***

CONTROLLING INBOUND TRAFFIC

Breaking down "internet connectivity to the lanes," the first step is to understand that the security of ***incoming*** TCP/IP traffic is pretty simple to set up and won't be affected by the Windows default route setup or firewall defaults. Firewall defaults are always set to prohibit any inbound-initiated traffic – and you don't want to change these settings. No ports from a firewall should be forwarded to any other machines inside the network.

CONTROLLING OUTBOUND TRAFFIC

Once the inbound settings are understood and confirmed, the real task is to limit the ***outbound*** TCP/IP traffic: for example, it's important to make sure that no one can go to a POS lane and launch a Web browser to the Internet.

One simple way to control the outbound traffic is to limit the applications that can be launched at a lane. Of course, Solidcore can prohibit browsers such as Internet Explorer, FTP, and other processes from running. This is a great start, but you can also control outbound traffic through a firewall configuration.

You can see that these requirements can even be met with a very inexpensive solution. Even a $59.99 consumer-grade router has firewall settings that lock down the lane very well, and for

another $100 a business-class router provides controls that are even better. Another option can be a software firewall running on the XP box such as ZoneAlarm, and of course there are more powerful solutions from companies like Cisco or SonicWall. Most solutions have the advantage of enabling and controlling network security from a centrally based hardware firewall device. So there are many ways to implement a firewall and they don't have to be expensive, sophisticated or complicated.

To use a basic example, you can get a Linksys consumer-grade router/firewall model BEFSX41 nationwide for less than $60. This isn't to endorse this specific router but it provides a good example of how the necessary features are provided standard in even a low-cost home-version model like this one.

In the example of the BEFSX41, Linksys offers a feature called the "Restrict Access Tab." Using this option, you can configure a policy for a group of PCs on your network and control exactly what those PCs can access on the Internet. In this example, you would create one policy that covers all the lanes by only allowing port 443 and port 6260 outbound from these lanes.

If you were to stop here, keep in mind that these settings would still allow traffic from the lanes to go out ports 443 and 6260 to any destination. However, limiting access to those two ports prohibits obvious issues that could come from browsing the Web or doing e-mail. In conjunction with Solidcore, even this basic setting locks down activity very well.

To do even better, step up to a business-grade firewall offering additional features and configuration details. It doesn't have to be an all-powerful Cisco enterprise machine, just something more in the $100 - $200 range likely targeted for small business or secure home requirements. For example, some Netgear routers in this price range have stronger and more configurable outbound filters, and any router designed for home-office use would have these features.

Using one of these enables you to create a stronger policy for the lanes. As above, you would first restrict outbound IP outbound traffic to ports 443 and 6260. But now strengthen the policy by also limiting that traffic to specific IP addresses. Which ones? The Connected Payments DNS names below, of course.

This setup will prohibit any application running on the POS lane from sending IP traffic anywhere but Connected Payments — and then only through the two ports identified below. These outbound traffic restrictions lock down the POSTs very tightly.

The following table provides all the information on the outbound IP traffic the lanes would need to send:

Outbound POS Lane Traffic Requirements for Connected Payments			
IP Address	**Port**	**DNS**	**Purpose Description**
4.79.143.164	443	trn1.servereps.com	Default/primary processing for transactions (Data Center #1)
4.79.143.168	443	svc1.servereps.com	Default/primary services (Data Center #1)
208.80.28.164	443	trn2.servereps.com	Alternate/secondary processing for transactions (Data Center #2)
208.80.28.168	443	svc2.servereps.com	Alternate/secondary (Data Center #2)
4.79.143.165	6260	bin1.servereps.com	BIN File Service Note: future enhancements will enable BIN File Service via port 443, further limiting port requirements.

When you implement these settings, make sure the restrictions are set up using the DNS names, not the IP addresses. This ensures that even if the IP addresses in the Connected Payments data centers change (although there no immediate plans for this) no firewall reconfiguration will be required .

But what about the Connected Payments network user interface ("GUI") for settlement, reporting and analysis? Of course, this would never be accessed from the POS lanes, but at least one workstation in a store will normally need this access through Microsoft Internet Explorer. Although many stores want general Internet access on at least one machine, the firewall can lock down the manager/bookkeeper machine for single-purpose connections too.

Port 443 is the only port required, so by creating a similar policy to the lane policy above, general Internet access can be restricted. And although Solidcore on that machine will prohibit viruses and malware, these settings can prevent staffers from browsing the Internet, downloading funware, running e-mail or any other activity that might lead to unintended malware ending up on the box.

One word of caution: if you allow only port 443 outbound from the bookkeepers workstation, you should create a properly configured shortcut or bookmark to Connected Payments. This is because Microsoft Internet Explorer defaults to port 80 when a user types in "www.servereps.com."[1] Although a user entering "**https://**www.servereps.com" will cause the web browser to automatically use port 443, most people never type in the "https://" part — so it's better if they have a pre-configured shortcut.

The following table shows the IP and ports required by the Connected Payments Web User Interface:

[1] Don't worry if you have kept port 80 available since the Connected Payments data center will automatically switch the communications to port 443 upon connection.

Outbound Workstation Traffic Requirements for Connected Payments			
IP Address	**Port**	**DNS**	**Purpose Description**
4.79.143.167	443	www.servereps.com	Connected Payments Reporting and Analysis (Web GUI) Note: port 80 can also be used, but will be changed to port 443 (https) once connection is made to the Data Center

As should be evident by now, simple firewall configuration can lock down the store to prevent risks once the Windows default route is set. Since most merchants (and dealers) will find it easier and feel more comfortable implementing centralized control of the store network, this can be accomplished in other ways too.

For example, instead of a centralized or router-based firewall, there are many software-based freeware firewalls available that, as above, control and filter network traffic but control it on a lane-by-lane basis. Since the controls we need are basic and nothing fancy is required for this purpose, almost any freeware software firewall will get the job done.

However, one tool you unfortunately cannot use is Windows XP's built-in firewall — this is because it only controls inbound traffic and doesn't provide the necessary outbound traffic control.