Guide to Simple Network Design

PCATS Recommendation, April 14, 2011

Abstract

This document provides guidance on simple network design for typical C-Store environments. In addition, this document provides discussion points for consulting with a network or data security professional.

Contributors

The PCATS Data Security Committee developed the content for this guide.

Revision History

Revision Date	Revision Number	Revision Author	Revision Changes
04/08/2011	Draft 0.1	Data Security Committee	Initial Draft
04/14/2011	Draft 0.2	Linda Toth, PCATS	Standardize format

Copyright Statement

Disclaimers

The National Association of Convenience Stores (NACS), Petroleum Convenience Alliance for Technology Standards (PCATS), participating vendors and retailers make no warranty, express or implied, nor do they assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product, or process described in these materials.

Table of Contents

1 Introduction 5
1.1 Overview 5
1.2 Audience 5
1.3 Complex Network Design 5
2 Simple Configuration 1 6
No direct internet access to point-of-sale environment. 6
2.1 Assumptions 6
2.2 Minimum criteria for security and compliance 6
3 Simple Configuration 2 7
No internet access to point-of-sale, other computers on separate network 7
3.1 Assumptions 7
3.2 Minimum criteria for security and compliance 7
4 Simple Configuration 3 8
Point-of-sale segmented from other computer systems on same network 8
4.1 Assumptions 8
4.2 Minimum criteria for security and compliance 9

Appendices

A. References 10
B. Glossary 11

1 Introduction

1.1 Overview

C-Store operators are typically non-technical people and network design can be very confusing. To that end, PCATS is offering some very simple designs that locations can use when talking with third-parties about network attached systems, configuration of those systems within the store, and the ability to meet the criteria set for security for a level 4 merchant under the PCI Data Security Standards (PCI-DSS).

1.2 Audience

The target audience for this document is the C-Store owner who has no or limited Information Technology (IT) network and security resources. While we expect that C-Store owners are level 4 merchants, this guidance is applicable for all C-Store owners, regardless of actual merchant level.

1.3 Complex Network Design

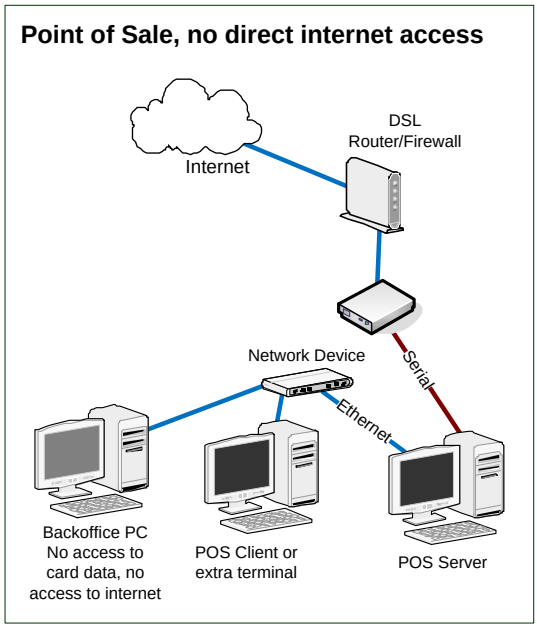
If a C-Store's environment does not fit within these simple configurations, PCATS recommends hiring a Data Security or PCI subject matter expert to design a store network that meets the security needs, compliance needs and business needs appropriate for the location.

2 Simple Configuration 1

No direct internet access to point-of-sale environment.

2.1 Assumptions

1. Point-of-sale has no direct connection to the internet.
2. No other systems are connected to the point-of-sale system with a connection to the internet.
3. Credit cards are processed over a phone line or using an intermediary network attached device that has a non-IP based (typically serial) connection to the point-of-sale.
4. Intermediary credit card processing devices may include Datawire Micronode, Secure Payment Gateway (EchoSat), or some other serial to IP converter that allows encrypted credit card traffic to pass to the processor.



2.2 Minimum criteria for security and compliance

1. Point-of-sale PA-DSS certified and installed by qualified point-of-sale reseller according to the point of sale vendor's PA-DSS Implementation Guide.
    a. Anti-virus or white-listing software installed on point-of-sale at time of installation with updates done on a quarterly basis.
    b. All default passwords changed at installation.
2. Back-office computer optional, but no direct internet access including email and web surfing. If present, back-office computer has anti-virus or white-listing software.
3. Remote access to back-office PC allowed using dial-out, but must be disconnected when not in use.
4. No wireless allowed.
5. DSL Router/Firewall considered outside of cardholder environment, but change default username and password on device.
6. Physical documents with cardholder data secured (paper receipts, paper reports, etc.).
7. No backup of point-of-sale system in place.
8. Network device(s) reviewed quarterly to ensure no other devices added to the network.

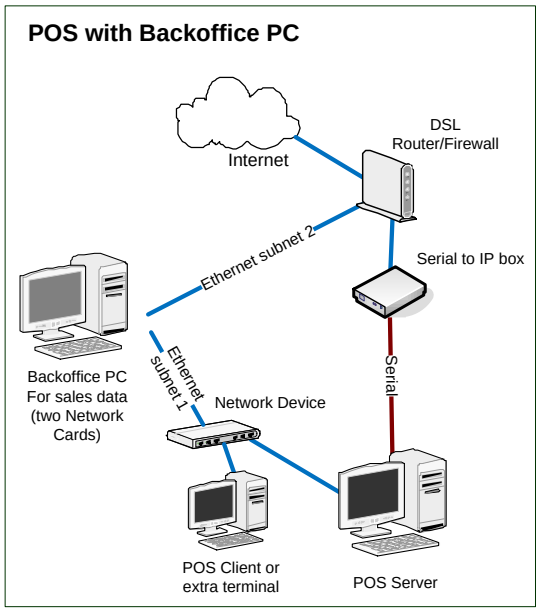
9. NACS provided Best Practices Security Policies in place.
10. Logging capabilities are turned on at the Point of Sale
11. Removable media access such as USB ports, CD-ROM and other access to the system, if applicable, is only allowed at time of installation or during upgrades.

3 Simple Configuration 2

No internet access to point-of-sale, other computers on separate network

3.1 Assumptions

1. Point-of-sale has no connection to the internet.
2. Other systems with internet access are in a different network subnet segmented physically, with a firewall or with a secondary network card.
3. Credit cards are processed over a phone line or using a intermediary device that has a non-IP based connection to the point-of-sale.



3.2 Minimum criteria for security and compliance

1. Point-of-sale PA-DSS certified and installed by qualified point-of-sale reseller according to the point of sale vendor's PA-DSS Implementation Guide.
    a. Anti-virus or white-listing software installed on point-of-sale at time of installation with updates done on a quarterly basis.
    b. All default passwords changed at installation.
2. Remote access only allowed to back-office PC and must be disabled when not in use.
3. No direct internet access allowed to point-of-sale system.

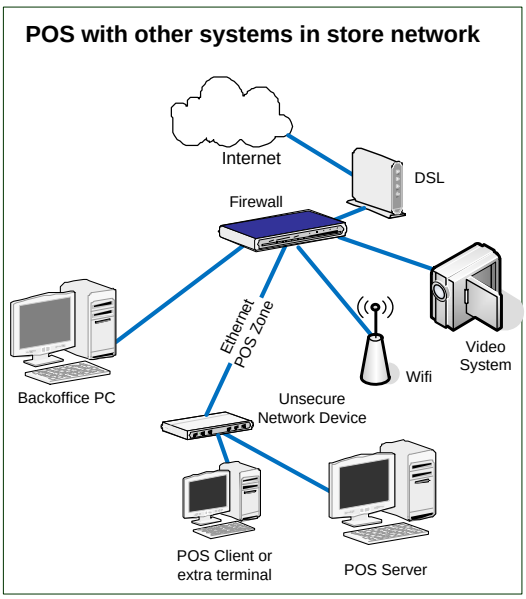
4. Back-office computer's internet connection on separate network segment from point-of-sale system (either a) serial connection to point-of-sale server, b) two network cards used or c) segmented network through router/firewall).
5. Back-office computer has limited connectivity to point-of-sale system, ie software firewall like Windows Firewall turned on.
6. No wireless allowed on either back-office or point-of-sale network segment.
7. Router/firewall has a) default username and password changed, b) upgraded to latest software and c) has highest firewall settings in place.
8. Physical documents with cardholder data secured (paper receipts, paper reports, etc.).
9. No backup of point-of-sale system in place.
10. Network device(s) reviewed quarterly to ensure no other devices added to the network.
11. NACS provided Best Practices Security Policies in place.
12. Logging capabilities are turned on at the Point of Sale
13. Removable media access such as USB ports, CD-ROM and other access to the system, if applicable, is only allowed at time of installation or during upgrades.
14. If point-of-sale is on a public facing network, vulnerability scanning must be done according to PCI-DSS.

4 Simple Configuration 3

Point-of-sale segmented from other computer systems on same network

4.1 Assumptions

1. Point-of-sale has no direct connection to the internet or internet access is used for credit card processing and remote support only and is behind a firewall.
2. Other systems with internet access are segmented with the firewall.



4.2 Minimum criteria for security and compliance

1. Point of Sale PA-DSS certified and installed by qualified point-of-sale reseller according to the point of sale vendor's PA-DSS Implementation Guide.
    a. Anti-virus or white-listing software installed on point-of-sale at time of installation with updates done on a quarterly basis.
    b. All default passwords changed at installation.
2. Firewall installed and managed by third-party vendor contractually obligated to meet PCI requirements.
    a. Point-of-sale on separate secure network segment from other computer systems, controlled by a stateful firewall that allows for true network segmentation.
    b. Outbound traffic from point-of-sale network segment explicitly authorized in the firewall.
    c. Remote access only allowed through strong security protocols.
3. No wireless allowed in point-of-sale network zone.
4. Physical documents with cardholder data secured (paper receipts, paper reports, etc.).
5. Backup of point-of-sale system either not in place or physically secured.
6. Network device(s) reviewed quarterly to ensure no other devices added to the network.
7. NACS provided Best Practices Security Policies in place.
8. Logging capabilities are turned on at the Point of Sale
9. Removable media access such as USB ports, CD-ROM and other access to the system, if applicable, is only allowed at time of installation or during upgrades.
10. If point-of-sale is on a public facing network, vulnerability scanning must be done according to PCI-DSS.

.

A. References

A.1 Normative References

A.2 Non-Normative References

B. Glossary

Term	Definition
DSC	Data Security Committee
NACS	National Association of Convenience Stores
PCATS	Petroleum Convenience Alliance for Technology Standards
PCI DSS	Payment Card Industry Data Security Standard
PCI	Alternate abbreviation for Payment Card Industry Data Security Standard