

PCI DSS Compliance Report for acmecorp-pix

Completed on Thu Jul 15 11:28:07 CDT 2010

Firewall Name: acmecorp-pix
Device Model: Cisco PIX

This assessment is based on the PCI Data Security Standard, Version 1.2, and covers all control items that address Firewall policy issues. The report lists control items by their number and provides a description identical to that in the PCI Data Security Standard (DSS) document URL:
(https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml).

To validate a control item, a set of automated security checks are run. The control item is deemed to be compliant if all checks are passed. The results are presented in summary form in a table with hyperlinks to detail. If there is a need to perform manual validation, additional data relevant to the control item is also provided in a separate table. Some control items do not need security checks and can be complied with by using FirePAC reports, and these are explained in the control item assessment detail.

Four additional reports regarding networks in the PCI zone can also be generated.

The [PCI Zone Detail Policy Findings](#) report provides a description of sources, destinations, and services to and from networks in the PCI zone. This report is a comprehensive listing of all traffic to and from the PCI zone from other locations, including remote locations that are not part of the network.

The [PCI Zone Failed Policy Checks Detail](#) report shows details of policy check failures identified in this report. This information identifies acl and NAT rules that caused the failures, and can be used to make changes in the configuration.

The [PCI Zone Dangerous Rules](#) report looks at firewall configuration rules and identifies those that cause the most number of policy checks to fail.

The [Firewall Configuration](#) report is the firewall configuration and is used to view the individual rules via hyperlinks from other reports.

Use Alt-left arrow to return to the source of the hyperlink.

Statistics

Number of networks in PCI zone: 1
IPSec VPNs: 0
Number of policy checks performed: 112

PCI Compliance Summary

Control Item	Description	Pass/Fail
1.1.5b	Identify insecure services, protocols, and ports allowed; and verify they are necessary and that security features are documented and implemented by examining firewall and router configuration standards and settings for each service. An example of an insecure service, protocol, or port is FTP, which passes user credentials in clear-text.	FAIL
1.2.1a	Verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment, and that the restrictions are documented.	FAIL
1.2.1b	Verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit "deny all" or an implicit deny after allow statement.	PASS
1.3.1	Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.	FAIL
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.	FAIL
1.3.3	Do not allow any direct routes inbound or outbound for traffic between the Internet and the cardholder data environment	FAIL
1.3.4	Do not allow internal addresses to pass from the Internet into the DMZ.	FAIL
1.3.5	Restrict outbound traffic from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ.	FAIL
1.3.6	Implement stateful inspection, also known as dynamic packet filtering. (That is, only 'established' connections are allowed into the network.)	FAIL
1.3.7	Place the database in an internal network zone, segregated from the DMZ.	PASS
1.3.8	Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet, using RFC 1918 address space. Use network address translation (NAT) technologies, for example, port address translation (PAT).	PASS
2.2.1	For a sample of system components, verify that only one primary function is implemented per server. For example, web servers, database servers, and DNS should be implemented on separate servers.	PASS
2.3	Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	FAIL

Networks Reachable in the PCI Zone

The following networks are reachable from each network interface in the PCI Zone.

PCI Zone Interface	Reachable Networks
testweb (192.168.50.1/24)	192.168.50.0/24

IPSec VPN Tunnels

The following remote networks are reachable through IPSec VPN tunnels. These networks may represent remote sites, partner networks or datafeeds.

No remote networks are reachable through IPSec VPN tunnels.

PCI Control Item Assessment Detail

For each PCI DSS control item, all the security policy checks that were performed to check for compliance are listed. The policy checks that passed, and those that failed are shown, along with a severity indicator (Red High, Orange Medium, Yellow Low) for each failed policy check. A hyperlink from the failed policy check description leads to the PCI Zone Failed Policy Checks Detail report that provides a detailed explanation of the policy check as well as the multiple ways that it may have failed.

1.1.5b

FAIL

Identify insecure services, protocols, and ports allowed; and verify they are necessary and that security features are documented and implemented by examining firewall and router configuration standards and settings for each service. An example of an insecure service, protocol, or port is FTP, which passes user credentials in clear-text.

Security policy checks that passed

- C1028 FTP services are not allowed from External zone to PCI zone.
- C1029 TFTP services are not allowed from External zone to PCI zone.
- C1030 DNS services are not allowed from External zone to PCI zone.
- C1031 Mail services are not allowed from External zone to PCI zone.
- C1032 HTTP services are not allowed from DMZ zone to PCI zone.
- C1033 FTP services are not allowed from DMZ zone to PCI zone.
- C1034 TFTP services are not allowed from DMZ zone to PCI zone.
- C1036 Mail services are not allowed from DMZ zone to PCI zone.
- C1040 Netbios services are not allowed from External zone to PCI zone.
- C1041 Microsoft RPC services are not allowed from External zone to PCI zone.
- C1042 Microsoft directory services are not allowed from External zone to PCI zone.
- C1043 Netbios services are not allowed from DMZ zone to PCI zone.
- C1044 Microsoft RPC services are not allowed from DMZ zone to PCI zone.
- C1045 Microsoft directory services are not allowed from DMZ zone to PCI zone.
- C1049 Netbios services are not allowed from PCI zone to External zone.
- C1050 Microsoft RPC services are not allowed from PCI zone to External zone.
- C1051 Microsoft directory services are not allowed from PCI zone to External zone.
- C1052 Netbios services are not allowed from PCI zone to DMZ zone.

- C1053 Microsoft RPC services are not allowed from PCI zone to DMZ zone.
- C1054 Microsoft directory services are not allowed from PCI zone to DMZ zone.
- C1055 Traceroute is not allowed to enter the PCI zone from the External zone.
- C1056 Traceroute is not allowed to enter the PCI zone from DMZ zone.
- C1060 Packets with TCP/UDP high ports are not allowed to enter the PCI zone from DMZ zone.
- C1064 NFS services are not allowed from External zone to PCI zone.
- C1065 X11 services are not allowed from External zone to PCI zone.
- C1069 Telnet services are not allowed from External zone to PCI zone.
- C1070 MSSQL services are not allowed from External zone to PCI zone.
- C1071 R services are not allowed from External zone to PCI zone.
- C1072 Fingers service are not allowed from External zone to PCI zone.
- C1084 NFS services are not allowed from DMZ zone to PCI zone.
- C1085 X11 services are not allowed from DMZ zone to PCI zone.
- C1086 P2P file-sharing services are not allowed from DMZ zone to PCI zone.
- C1088 Instant message services are not allowed from DMZ zone to PCI zone.
- C1089 Telnet services are not allowed from DMZ zone to PCI zone.
- C1090 MSSQL services are not allowed from DMZ zone to PCI zone.
- C1091 R services are not allowed from DMZ zone to PCI zone.
- C1092 Finger service is not allowed from DMZ zone to PCI zone.
- C1101 FTP services are not allowed from PCI zone to External zone.
- C1102 TFTP services are not allowed from PCI zone to External zone.
- C1103 Telnet services are not allowed from PCI zone to External zone.
- C1104 Instant message services are not allowed from PCI zone to External zone.
- C1105 R services are not allowed from PCI zone to External zone.
- C1106 NFS services are not allowed from PCI zone to External zone.
- C1107 X11 services are not allowed from PCI zone to External zone.
- C1117 Database services are not allowed from DMZ zone to PCI zone.

Security policy checks that failed

- C1027 ■ [HTTP services allowed from the External zone to PCI zone](#)
- C1035 ■ [DNS services allowed from DMZ zone to PCI zone](#)
- C1058 ■ [TCP/UDP high ports allowed from External zone to PCI zone](#)

Services allowed to and from the PCI zone

Services To PCI Network*
icmp
tcp/7618 (7618)
tcp/9895 (9895)
tcp/aimpp-port-req (2847) tcp/amt-blc-port (2848)
tcp/cbt (7777)
tcp/ftp (21) tcp/ssh (22) tcp/telnet (23)
tcp/h323 (1742)
tcp/http (80) tcp/hosts2-ns (81)
tcp/http-alt (8080)
tcp/https (443)
tcp/netsupport (5405)
tcp/nntp (119)
tcp/smtp (25)
tcp/vnc-server (5900) tcp/5901 (5901)
udp/any

Services From PCI Network*
icmp
tcp/http (80)
tcp/https (443)
tcp/smtp (25)
tcp/ssh (22)
udp/dnsix (90)
udp/domain (53)

*NOTE: Services may be repeated in several rows due to policies that have different sources and destinations.

1.2.1a

FAIL

Verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment, and that the restrictions are documented.

Security policy checks that passed

- C1014 ACL rule(s) that allow "any" TCP service entering PCI zone from External zone not found.
- C1015 ACL rule(s) that allow "any" UDP service entering PCI zone from External zone not found.
- C1017 ACL rule(s) that allow "any" service entering PCI zone from DMZ zone not found.
- C1018 ACL rule(s) that allow "any" TCP service entering PCI zone from DMZ zone not found.
- C1016 ACL rule(s) that allow "any" destination address entering PCI zone from External zone not found.
- C1021 ACL rule(s) that allow "any" source address entering PCI zone from DMZ zone not found.
- C1028 FTP services are not allowed from External zone to PCI zone.
- C1029 TFTP services are not allowed from External zone to PCI zone.
- C1030 DNS services are not allowed from External zone to PCI zone.
- C1031 Mail services are not allowed from External zone to PCI zone.
- C1032 HTTP services are not allowed from DMZ zone to PCI zone.
- C1033 FTP services are not allowed from DMZ zone to PCI zone.
- C1034 TFTP services are not allowed from DMZ zone to PCI zone.
- C1036 Mail services are not allowed from DMZ zone to PCI zone.
- C1040 Netbios services are not allowed from External zone to PCI zone.
- C1041 Microsoft RPC services are not allowed from External zone to PCI zone.
- C1042 Microsoft directory services are not allowed from External zone to PCI zone.
- C1043 Netbios services are not allowed from DMZ zone to PCI zone.
- C1044 Microsoft RPC services are not allowed from DMZ zone to PCI zone.
- C1045 Microsoft directory services are not allowed from DMZ zone to PCI zone.
- C1049 Netbios services are not allowed from PCI zone to External zone.
- C1050 Microsoft RPC services are not allowed from PCI zone to External zone.
- C1051 Microsoft directory services are not allowed from PCI zone to External zone.
- C1052 Netbios services are not allowed from PCI zone to DMZ zone.
- C1053 Microsoft RPC services are not allowed from PCI zone to DMZ zone.
- C1054 Microsoft directory services are not allowed from PCI zone to DMZ zone.
- C1060 Packets with TCP/UDP high ports are not allowed to enter the PCI zone from DMZ zone.
- C1061 SNMP services are not allowed from External zone to PCI zone.
- C1063 LDAP services are not allowed from External zone to PCI zone.
- C1064 NFS services are not allowed from External zone to PCI zone.
- C1065 X11 services are not allowed from External zone to PCI zone.
- C1066 P2P file-sharing services are not allowed from External zone to PCI zone.
- C1067 SunRPC services are not allowed from External zone to PCI zone.

- C1068 Instant message services are not allowed from External zone to PCI zone.
- C1069 Telnet services are not allowed from External zone to PCI zone.
- C1070 MSSQL services are not allowed from External zone to PCI zone.
- C1071 R services are not allowed from External zone to PCI zone.
- C1072 Fingers service are not allowed from External zone to PCI zone.
- C1073 ACL rule(s) that allow "any" TCP service entering PCI zone from Internal zone not found.
- C1076 ACL rule(s) that allow "any" TCP service entering Internal zone from PCI zone not found.
- C1077 ACL rule(s) that allow "any" UDP service entering Internal zone from PCI zone not found.
- C1078 ACL rule(s) that allow "any" source address entering Internal zone from PCI zone not found.
- C1083 LDAP service are not allowed from DMZ zone to PCI zone.
- C1084 NFS services are not allowed from DMZ zone to PCI zone.
- C1085 X11 services are not allowed from DMZ zone to PCI zone.
- C1086 P2P file-sharing services are not allowed from DMZ zone to PCI zone.
- C1087 SunRPC services are not allowed from DMZ zone to PCI zone.
- C1088 Instant message services are not allowed from DMZ zone to PCI zone.
- C1089 Telnet services are not allowed from DMZ zone to PCI zone.
- C1090 MSSQL services are not allowed from DMZ zone to PCI zone.
- C1091 R services are not allowed from DMZ zone to PCI zone.
- C1092 Finger service is not allowed from DMZ zone to PCI zone.
- C1097 ACL rule(s) that allow "any" service entering DMZ zone from PCI zone not found.
- C1101 FTP services are not allowed from PCI zone to External zone.
- C1102 TFTP services are not allowed from PCI zone to External zone.
- C1103 Telnet services are not allowed from PCI zone to External zone.
- C1104 Instant message services are not allowed from PCI zone to External zone.
- C1105 R services are not allowed from PCI zone to External zone.
- C1106 NFS services are not allowed from PCI zone to External zone.
- C1107 X11 services are not allowed from PCI zone to External zone.
- C1117 Database services are not allowed from DMZ zone to PCI zone.
- C1118 ACL rule(s) that allow "any" destination and "any" services entering from External zone to PCI zone not found.
- C1123 ACL rule(s) that allow "any" service entering PCI zone from External zone not found.
- C1126 Packets with TCP/UDP high ports are not allowed to enter the External zone from PCI zone.
- C1127 Packets with TCP/UDP high ports are not allowed to enter the DMZ zone from PCI zone.

Security policy checks that failed

- C1020 ■ [Rule\(s\) with "any" destination address allow access from DMZ zone to PCI zone](#)
- C1027 ■ [HTTP services allowed from the External zone to PCI zone](#)
- C1035 ■ [DNS services allowed from DMZ zone to PCI zone](#)
- C1074 ■ [Rule\(s\) allow "any" UDP service from Internal zone to PCI zone](#)
- C1075 ■ [Rule\(s\) with "any" destination address allow access from Internal zone to PCI zone](#)
- C1058 ■ [TCP/UDP high ports allowed from External zone to PCI zone](#)

Inbound traffic from External Networks to PCI zone

External Network	Allowed Service	To PCI Zone Network*
0.0.0.0 to 9.255.255.255	tcp/http (80)	62.59.14.171
	tcp/https (443)	62.59.14.171
	tcp/ssh (22)	62.59.14.171
11.0.0.0 to 172.15.255.255	tcp/http (80)	62.59.14.171
	tcp/https (443)	62.59.14.171
	tcp/ssh (22)	62.59.14.171
172.18.0.0 to 192.168.0.255	tcp/http (80)	62.59.14.171
	tcp/https (443)	62.59.14.171
	tcp/ssh (22)	62.59.14.171
192.168.10.0 to 192.168.49.255	tcp/http (80)	62.59.14.171
	tcp/https (443)	62.59.14.171
	tcp/ssh (22)	62.59.14.171
192.168.51.0 to 255.255.255.255	tcp/http (80)	62.59.14.171
	tcp/https (443)	62.59.14.171
	tcp/ssh (22)	62.59.14.171
192.168.6.0 to 192.168.8.255	tcp/http (80)	62.59.14.171
	tcp/https (443)	62.59.14.171
	tcp/ssh (22)	62.59.14.171
69.237.83.3	tcp/cbt (7777)	62.59.14.171

Inbound traffic from DMZ Networks to PCI Zone

DMZ Network	Allowed Service	To PCI Zone Network*
192.168.1.2	udp/domain (53)	192.168.50.0/24

Outbound traffic from PCI zone to External Networks

PCI Zone Network*	Allowed Service	To External Network
192.168.50.0/24	icmp	0.0.0.0 to 9.255.255.255
		11.0.0.0 to 172.15.255.255
		172.18.0.0 to 192.168.0.255
		192.168.10.0 to 192.168.49.255
		192.168.51.0 to 255.255.255.255
		192.168.6.0 to 192.168.8.255
	tcp/http (80)	0.0.0.0 to 9.255.255.255
		11.0.0.0 to 172.15.255.255
		172.18.0.0 to 192.168.0.255
		192.168.10.0 to 192.168.49.255
		192.168.51.0 to 255.255.255.255
		192.168.6.0 to 192.168.8.255
	tcp/https (443)	0.0.0.0 to 9.255.255.255
		11.0.0.0 to 172.15.255.255
		172.18.0.0 to 192.168.0.255
		192.168.10.0 to 192.168.49.255
		192.168.51.0 to 255.255.255.255
		192.168.6.0 to 192.168.8.255
	tcp/smtp (25)	0.0.0.0 to 9.255.255.255
		11.0.0.0 to 172.15.255.255
		172.18.0.0 to 192.168.0.255
		192.168.10.0 to 192.168.49.255
		192.168.51.0 to 255.255.255.255
		192.168.6.0 to 192.168.8.255
tcp/ssh (22)	0.0.0.0 to 9.255.255.255	
	11.0.0.0 to 172.15.255.255	
	172.18.0.0 to 192.168.0.255	
	192.168.10.0 to 192.168.49.255	
	192.168.51.0 to 255.255.255.255	
	192.168.6.0 to 192.168.8.255	

PCI Zone Network*	Allowed Service	To External Network
192.168.50.0/24	udp/dnsix (90)	0.0.0.0 to 9.255.255.255
		11.0.0.0 to 172.15.255.255
		172.18.0.0 to 192.168.0.255
		192.168.10.0 to 192.168.49.255
		192.168.51.0 to 255.255.255.255
		192.168.6.0 to 192.168.8.255
	udp/domain (53)	0.0.0.0 to 9.255.255.255
		11.0.0.0 to 172.15.255.255
		172.18.0.0 to 192.168.0.255
		192.168.10.0 to 192.168.49.255
		192.168.51.0 to 255.255.255.255
		192.168.6.0 to 192.168.8.255

Outbound traffic from PCI Zone to DMZ networks

PCI Zone Network*	Allowed Service	To DMZ Network
192.168.1.2	udp/domain (53)	192.168.50.0/24

*NOTE: This may be a NATed address of a network in the PCI Zone

1.2.1b

PASS

Verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit "deny all" or an implicit deny after allow statement.

Security policy checks that passed

- C1013 Rule(s) that allow "any" service from "any" source to "any" destination not found.
- C1025 Found rule(s) that deny all traffic using deny all or implicit deny

Security policy checks that failed

No failed checks found

Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.

Security policy checks that passed

- C1014 ACL rule(s) that allow "any" TCP service entering PCI zone from External zone not found.
- C1015 ACL rule(s) that allow "any" UDP service entering PCI zone from External zone not found.
- C1017 ACL rule(s) that allow "any" service entering PCI zone from DMZ zone not found.
- C1018 ACL rule(s) that allow "any" TCP service entering PCI zone from DMZ zone not found.
- C1021 ACL rule(s) that allow "any" source address entering PCI zone from DMZ zone not found.
- C1028 FTP services are not allowed from External zone to PCI zone.
- C1029 TFTP services are not allowed from External zone to PCI zone.
- C1030 DNS services are not allowed from External zone to PCI zone.
- C1031 Mail services are not allowed from External zone to PCI zone.
- C1032 HTTP services are not allowed from DMZ zone to PCI zone.
- C1033 FTP services are not allowed from DMZ zone to PCI zone.
- C1034 TFTP services are not allowed from DMZ zone to PCI zone.
- C1036 Mail services are not allowed from DMZ zone to PCI zone.
- C1040 Netbios services are not allowed from External zone to PCI zone.
- C1041 Microsoft RPC services are not allowed from External zone to PCI zone.
- C1042 Microsoft directory services are not allowed from External zone to PCI zone.
- C1043 Netbios services are not allowed from DMZ zone to PCI zone.
- C1044 Microsoft RPC services are not allowed from DMZ zone to PCI zone.
- C1045 Microsoft directory services are not allowed from DMZ zone to PCI zone.
- C1049 Netbios services are not allowed from PCI zone to External zone.
- C1050 Microsoft RPC services are not allowed from PCI zone to External zone.
- C1051 Microsoft directory services are not allowed from PCI zone to External zone.
- C1052 Netbios services are not allowed from PCI zone to DMZ zone.
- C1053 Microsoft RPC services are not allowed from PCI zone to DMZ zone.
- C1054 Microsoft directory services are not allowed from PCI zone to DMZ zone.
- C1055 Traceroute is not allowed to enter the PCI zone from the External zone.
- C1056 Traceroute is not allowed to enter the PCI zone from DMZ zone.
- C1060 Packets with TCP/UDP high ports are not allowed to enter the PCI zone from DMZ zone.
- C1061 SNMP services are not allowed from External zone to PCI zone.
- C1063 LDAP services are not allowed from External zone to PCI zone.

C1064 NFS services are not allowed from External zone to PCI zone.

C1065 X11 services are not allowed from External zone to PCI zone.

C1066 P2P file-sharing services are not allowed from External zone to PCI zone.

C1067 SunRPC services are not allowed from External zone to PCI zone.

C1068 Instant message services are not allowed from External zone to PCI zone.

C1069 Telnet services are not allowed from External zone to PCI zone.

C1070 MSSQL services are not allowed from External zone to PCI zone.

C1071 R services are not allowed from External zone to PCI zone.

C1072 Fingers service are not allowed from External zone to PCI zone.

C1073 ACL rule(s) that allow "any" TCP service entering PCI zone from Internal zone not found.

C1076 ACL rule(s) that allow "any" TCP service entering Internal zone from PCI zone not found.

C1077 ACL rule(s) that allow "any" UDP service entering Internal zone from PCI zone not found.

C1078 ACL rule(s) that allow "any" source address entering Internal zone from PCI zone not found.

C1083 LDAP service are not allowed from DMZ zone to PCI zone.

C1084 NFS services are not allowed from DMZ zone to PCI zone.

C1085 X11 services are not allowed from DMZ zone to PCI zone.

C1086 P2P file-sharing services are not allowed from DMZ zone to PCI zone.

C1087 SunRPC services are not allowed from DMZ zone to PCI zone.

C1088 Instant message services are not allowed from DMZ zone to PCI zone.

C1089 Telnet services are not allowed from DMZ zone to PCI zone.

C1090 MSSQL services are not allowed from DMZ zone to PCI zone.

C1091 R services are not allowed from DMZ zone to PCI zone.

C1092 Finger service is not allowed from DMZ zone to PCI zone.

C1097 ACL rule(s) that allow "any" service entering DMZ zone from PCI zone not found.

C1098 ACL rule(s) that allow "any" TCP service entering DMZ zone from PCI zone not found.

C1099 ACL rule(s) that allow "any" UDP service entering DMZ zone from PCI zone not found

C1101 FTP services are not allowed from PCI zone to External zone.

C1102 TFTP services are not allowed from PCI zone to External zone.

C1103 Telnet services are not allowed from PCI zone to External zone.

C1104 Instant message services are not allowed from PCI zone to External zone.

C1105 R services are not allowed from PCI zone to External zone.

C1106 NFS services are not allowed from PCI zone to External zone.

C1107 X11 services are not allowed from PCI zone to External zone.

C1120 ACL rule(s) that allow "any" destination and "any" services entering from DMZ zone to PCI zone not found.

- C1121 ACL rule(s) that allow "any" source and "any" services entering from DMZ zone to PCI zone not found.
- C1126 Packets with TCP/UDP high ports are not allowed to enter the External zone from PCI zone.
- C1127 Packets with TCP/UDP high ports are not allowed to enter the DMZ zone from PCI zone.

Security policy checks that failed

- C1020 ■ [Rule\(s\) with "any" destination address allow access from DMZ zone to PCI zone](#)
- C1027 ■ [HTTP services allowed from the External zone to PCI zone](#)
- C1035 ■ [DNS services allowed from DMZ zone to PCI zone](#)
- C1074 ■ [Rule\(s\) allow "any" UDP service from Internal zone to PCI zone](#)
- C1075 ■ [Rule\(s\) with "any" destination address allow access from Internal zone to PCI zone](#)

Services allowed between the DMZ and PCI zones

Service	From Zone	To Zone
udp/domain (53)	DMZ	PCI
	PCI	DMZ

1.3.2 **FAIL**

Limit inbound Internet traffic to IP addresses within the DMZ.

Security policy checks that passed

- C1011 ICMP echo requests from the External zone are blocked from entering the PCI zone
- C1014 ACL rule(s) that allow "any" TCP service entering PCI zone from External zone not found.
- C1015 ACL rule(s) that allow "any" UDP service entering PCI zone from External zone not found.
- C1016 ACL rule(s) that allow "any" destination address entering PCI zone from External zone not found.
- C1028 FTP services are not allowed from External zone to PCI zone.
- C1029 TFTP services are not allowed from External zone to PCI zone.
- C1030 DNS services are not allowed from External zone to PCI zone.
- C1031 Mail services are not allowed from External zone to PCI zone.
- C1040 Netbios services are not allowed from External zone to PCI zone.
- C1041 Microsoft RPC services are not allowed from External zone to PCI zone.
- C1042 Microsoft directory services are not allowed from External zone to PCI zone.
- C1061 SNMP services are not allowed from External zone to PCI zone.
- C1063 LDAP services are not allowed from External zone to PCI zone.
- C1064 NFS services are not allowed from External zone to PCI zone.

- C1065 X11 services are not allowed from External zone to PCI zone.
- C1066 P2P file-sharing services are not allowed from External zone to PCI zone.
- C1067 SunRPC services are not allowed from External zone to PCI zone.
- C1068 Instant message services are not allowed from External zone to PCI zone.
- C1069 Telnet services are not allowed from External zone to PCI zone.
- C1070 MSSQL services are not allowed from External zone to PCI zone.
- C1071 R services are not allowed from External zone to PCI zone.
- C1072 Fingers service are not allowed from External zone to PCI zone.
- C1073 ACL rule(s) that allow "any" TCP service entering PCI zone from Internal zone not found.
- C1115 Database services are not allowed from External zone to PCI zone.
- C1118 ACL rule(s) that allow "any" destination and "any" services entering from External zone to PCI zone not found.

Security policy checks that failed

- C1027 ■ [HTTP services allowed from the External zone to PCI zone](#)
- C1074 ■ [Rule\(s\) allow "any" UDP service from Internal zone to PCI zone](#)
- C1075 ■ [Rule\(s\) with "any" destination address allow access from Internal zone to PCI zone](#)
- C1058 ■ [TCP/UDP high ports allowed from External zone to PCI zone](#)

PCI destinations of inbound Internet traffic

External Network	Inbound Service	Network in PCI Zone*
0.0.0.0 to 9.255.255.255	tcp/http (80)	62.59.14.171
	tcp/https (443)	62.59.14.171
	tcp/ssh (22)	62.59.14.171
11.0.0.0 to 172.15.255.255	tcp/http (80)	62.59.14.171
	tcp/https (443)	62.59.14.171
	tcp/ssh (22)	62.59.14.171
172.18.0.0 to 192.168.0.255	tcp/http (80)	62.59.14.171
	tcp/https (443)	62.59.14.171
	tcp/ssh (22)	62.59.14.171
192.168.10.0 to 192.168.49.255	tcp/http (80)	62.59.14.171
	tcp/https (443)	62.59.14.171
	tcp/ssh (22)	62.59.14.171
192.168.51.0 to 255.255.255.255	tcp/http (80)	62.59.14.171

External Network	Inbound Service	Network in PCI Zone*
192.168.51.0 to 255.255.255.255	tcp/https (443)	62.59.14.171
	tcp/ssh (22)	62.59.14.171
192.168.6.0 to 192.168.8.255	tcp/http (80)	62.59.14.171
	tcp/https (443)	62.59.14.171
	tcp/ssh (22)	62.59.14.171
69.237.83.3	tcp/cbt (7777)	62.59.14.171

*NOTE: The addresses in the "Network in PCI Zone" column may be NATed address of a network in the PCI Zone

1.3.3

FAIL

Do not allow any direct routes inbound or outbound for traffic between the Internet and the cardholder data environment

Security policy checks that passed

- C1011 ICMP echo requests from the External zone are blocked from entering the PCI zone
- C1016 ACL rule(s) that allow "any" destination address entering PCI zone from External zone not found.
- C1028 FTP services are not allowed from External zone to PCI zone.
- C1029 TFTP services are not allowed from External zone to PCI zone.
- C1030 DNS services are not allowed from External zone to PCI zone.
- C1031 Mail services are not allowed from External zone to PCI zone.
- C1040 Netbios services are not allowed from External zone to PCI zone.
- C1041 Microsoft RPC services are not allowed from External zone to PCI zone.
- C1042 Microsoft directory services are not allowed from External zone to PCI zone.
- C1061 SNMP services are not allowed from External zone to PCI zone.
- C1063 LDAP services are not allowed from External zone to PCI zone.
- C1064 NFS services are not allowed from External zone to PCI zone.
- C1065 X11 services are not allowed from External zone to PCI zone.
- C1066 P2P file-sharing services are not allowed from External zone to PCI zone.
- C1067 SunRPC services are not allowed from External zone to PCI zone.
- C1068 Instant message services are not allowed from External zone to PCI zone.
- C1069 Telnet services are not allowed from External zone to PCI zone.
- C1070 MSSQL services are not allowed from External zone to PCI zone.
- C1071 R services are not allowed from External zone to PCI zone.
- C1072 Fingers service are not allowed from External zone to PCI zone.
- C1115 Database services are not allowed from External zone to PCI zone.

- C1118 ACL rule(s) that allow "any" destination and "any" services entering from External zone to PCI zone not found.
- C1126 Packets with TCP/UDP high ports are not allowed to enter the External zone from PCI zone.
- C1129 FTP services are not allowed from PCI zone to External zone.
- C1130 TFTP services are not allowed from PCI zone to External zone.
- C1133 Netbios services are not allowed from PCI zone to External zone.
- C1134 Microsoft RPC services are not allowed from PCI zone to External zone.
- C1135 Microsoft directory services are not allowed from PCI zone to External zone.
- C1136 SNMP services are not allowed from PCI zone to External zone.
- C1137 LDAP services are not allowed from External zone to PCI zone.
- C1138 NFS services are not allowed from PCI zone to External zone.
- C1139 X11 services are not allowed from PCI zone to External zone.
- C1140 P2P file-sharing services are not allowed from PCI zone to External zone.
- C1141 SunRPC services are not allowed from PCI zone to External zone.
- C1142 Instant message services are not allowed from PCI zone to External zone.
- C1143 Telnet services are not allowed from PCI zone to External zone.
- C1144 MSSQL services are not allowed from PCI zone to External zone.
- C1145 R services are not allowed from PCI zone to External zone.
- C1146 Fingers service are not allowed from PCI zone to External zone.
- C1147 Database services are not allowed from PCI zone to External zone.

Security policy checks that failed

- C1027 ■ [HTTP services allowed from the External zone to PCI zone](#)
- C1128 ■ [HTTP services allowed from the PCI zone to External zone](#)
- C1131 ■ [DNS services allowed from PCI zone to External zone](#)
- C1132 ■ [Mail services allowed from PCI zone to External zone](#)
- C1012 ■ [ICMP reply services are allowed from PCI zone to External zone](#)
- C1058 ■ [TCP/UDP high ports allowed from External zone to PCI zone](#)

PCI networks traffic with Internet

PCI Network*	External Network	Service
192.168.50.0/24	0.0.0.0 to 9.255.255.255	icmp
		tcp/http (80)
		tcp/https (443)

PCI Network*	External Network	Service
192.168.50.0/24	0.0.0.0 to 9.255.255.255	tcp/smtp (25)
		tcp/ssh (22)
		udp/dnsix (90)
		udp/domain (53)
	11.0.0.0 to 172.15.255.255	icmp
		tcp/http (80)
		tcp/https (443)
		tcp/smtp (25)
		tcp/ssh (22)
		udp/dnsix (90)
		udp/domain (53)
	172.18.0.0 to 192.168.0.255	icmp
		tcp/http (80)
		tcp/https (443)
		tcp/smtp (25)
		tcp/ssh (22)
		udp/dnsix (90)
		udp/domain (53)
	192.168.10.0 to 192.168.49.255	icmp
		tcp/http (80)
		tcp/https (443)
		tcp/smtp (25)
		tcp/ssh (22)
		udp/dnsix (90)
		udp/domain (53)
	192.168.51.0 to 255.255.255.255	icmp
		tcp/http (80)
		tcp/https (443)
tcp/smtp (25)		
tcp/ssh (22)		
udp/dnsix (90)		
udp/domain (53)		
192.168.6.0 to 192.168.8.255	icmp	
	tcp/http (80)	
	tcp/https (443)	

PCI Network*	External Network	Service	
192.168.50.0/24	192.168.6.0 to 192.168.8.255	tcp/smtp (25)	
		tcp/ssh (22)	
		udp/dnsix (90)	
		udp/domain (53)	
62.59.14.171	0.0.0.0 to 9.255.255.255	tcp/http (80)	
		tcp/https (443)	
		tcp/ssh (22)	
	11.0.0.0 to 172.15.255.255	tcp/http (80)	
		tcp/https (443)	
		tcp/ssh (22)	
	172.18.0.0 to 192.168.0.255	tcp/http (80)	
		tcp/https (443)	
		tcp/ssh (22)	
	192.168.10.0 to 192.168.49.255	tcp/http (80)	
		tcp/https (443)	
		tcp/ssh (22)	
	192.168.51.0 to 255.255.255.255	tcp/http (80)	
		tcp/https (443)	
		tcp/ssh (22)	
	192.168.6.0 to 192.168.8.255	tcp/http (80)	
		tcp/https (443)	
		tcp/ssh (22)	
	69.237.83.3		tcp/cbt (7777)

*NOTE: This may be a NATed address of a network in the PCI Zone

1.3.4

FAIL

Do not allow internal addresses to pass from the Internet into the DMZ.

Security policy checks that passed

No passed checks found

Security policy checks that failed

- C1022 ■ [Reserved source IP addresses \(non RFC-1918\) allowed access from External zone to DMZ zone.](#)
- C1024 ■ [RFC-1918 private IP Source addresses allowed access from External zone to DMZ zone.](#)

Interfaces that do not have anti spoofing turned on

Interface Name	IP Address*	Zone
outside	62.59.14.189	External

*NOTE: Publicly routable internal addresses need to be manually checked for spoofing.

1.3.5

FAIL

Restrict outbound traffic from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ.

Security policy checks that passed

- C1049 Netbios services are not allowed from PCI zone to External zone.
- C1050 Microsoft RPC services are not allowed from PCI zone to External zone.
- C1051 Microsoft directory services are not allowed from PCI zone to External zone.
- C1076 ACL rule(s) that allow "any" TCP service entering Internal zone from PCI zone not found.
- C1077 ACL rule(s) that allow "any" UDP service entering Internal zone from PCI zone not found.
- C1078 ACL rule(s) that allow "any" source address entering Internal zone from PCI zone not found.
- C1101 FTP services are not allowed from PCI zone to External zone.
- C1102 TFTP services are not allowed from PCI zone to External zone.
- C1103 Telnet services are not allowed from PCI zone to External zone.
- C1104 Instant message services are not allowed from PCI zone to External zone.
- C1105 R services are not allowed from PCI zone to External zone.
- C1106 NFS services are not allowed from PCI zone to External zone.
- C1107 X11 services are not allowed from PCI zone to External zone.
- C1126 Packets with TCP/UDP high ports are not allowed to enter the External zone from PCI zone.

Security policy checks that failed

- C1012 ■ [ICMP reply services are allowed from PCI zone to External zone](#)

IP addresses accessible from the PCI zone

IP Address	Zone
0.0.0.0 to 9.255.255.255	External
11.0.0.0 to 172.15.255.255	External
172.18.0.0 to 192.168.0.255	External
192.168.10.0 to 192.168.49.255	External
192.168.50.0/24	DMZ
192.168.51.0 to 255.255.255.255	External
192.168.6.0 to 192.168.8.255	External

1.3.6

FAIL

Implement stateful inspection, also known as dynamic packet filtering. (That is, only 'established' connections are allowed into the network.)

Security policy checks that passed

- C1037 Denial of Service (Land Attack) protection is enabled in the firewall.

Security policy checks that failed

- C1038 ■ [Protection against SYN Flood attack](#)

1.3.7

PASS

Place the database in an internal network zone, segregated from the DMZ.

Security policy checks that passed

- C1115 Database services are not allowed from External zone to PCI zone.
- C1117 Database services are not allowed from DMZ zone to PCI zone.
- C1125 Database services are not allowed from External zone to DMZ zone.

Security policy checks that failed

No failed checks found

*NOTE: Manually confirm that there is no DB server in the DMZ if the Control item passes.

1.3.8

PASS

Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet, using RFC 1918 address space. Use network address translation (NAT) technologies, for example, port address translation (PAT).

Addresses in the PCI zone that are not NATed and which access the external network

All addresses in the PCI zone which access the external network are NATed.

2.2.1

PASS

For a sample of system components, verify that only one primary function is implemented per server. For example, web servers, database servers, and DNS should be implemented on separate servers.

Multiple services from the same network*

No data found for Multiple services from the same network.

*NOTE: Our automated security policy checks cannot resolve the case of a single host having virtual ip addresses or being NATed to multiple external addresses. A manual check may be necessary to confirm compliance if it reported as a PASS

2.3

FAIL

Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.

Security policy checks that passed

C1009 Firewall does not allow insecure services(telnet, ftp, http and tftp) from External zones to the firewall for the management of the firewall.

Security policy checks that failed

C1010 ■ [Insecure Internal/DMZ access to firewall](#)