



## PCI Zone Firewall Checks Detail Report for acmecorp-pix

### Completed on Thu Jul 15 11:27:57 CDT 2010

The PCI Zone Failed Policy Check Details report shows a list of failed policy checks, their severity and the rule-trail that caused them to fail. A rule-trail is a sequence of configuration rules (acl and NAT) that execute in sequence in the firewall to cause the policy check failure. This information can be used to correct risky rules and harden the firewall against exposures.

Each failed check is associated with a severity (high,medium, low) that provides a way for prioritizing fixes to the firewall configuration rules. Red represents High, Orange Medium and Yellow Low severity.

A policy check rule is evaluated against multiple targets, and may pass on some and fail on others. Each such failure is represented by a row in a table, and is organized by firewall entering and exiting interfaces.

The rule-trail in each row (the entries under columns: acl rule and NAT rule) of the table is a set of rule numbers. These refer to rule numbers in the firewall's configuration. Hyperlinks are provided that when clicked will highlight the text of the rule in the configuration report.

### Security Audit Summary

Number of policy checks performed: 112

Number of failed policy checks: 8 high risks, 3 medium risks, 3 low risks items

- High Risk
- Medium Risk
- Low Risk

#### Risk   Description

C1020	■ Rule(s) with "any" destination address allow access from DMZ zone to PCI zone	<a href="#">Details</a>
C1027	■ HTTP services allowed from the External zone to PCI zone	<a href="#">Details</a>
C1035	■ DNS services allowed from DMZ zone to PCI zone	<a href="#">Details</a>
C1074	■ Rule(s) allow "any" UDP service from Internal zone to PCI zone	<a href="#">Details</a>
C1075	■ Rule(s) with "any" destination address allow access from Internal zone to PCI zone	<a href="#">Details</a>
C1128	■ HTTP services allowed from the PCI zone to External zone	<a href="#">Details</a>
C1131	■ DNS services allowed from PCI zone to External zone	<a href="#">Details</a>
C1132	■ Mail services allowed from PCI zone to External zone	<a href="#">Details</a>
C1010	■ Insecure Internal/DMZ access to firewall	<a href="#">Details</a>
C1012	■ ICMP reply services are allowed from PCI zone to External zone	<a href="#">Details</a>

- C1058 ■ TCP/UDP high ports allowed from External zone to PCI zone [Details](#)
- C1022 ■ Reserved source IP addresses (non RFC-1918) allowed access from External zone to DMZ zone. [Details](#)
- C1024 ■ RFC-1918 private IP Source addresses allowed access from External zone to DMZ zone. [Details](#)
- C1038 ■ Protection against SYN Flood attack [Details](#)

## Security Audit Details

### C1020 Rule(s) with "any" destination address allow access from DMZ zone to PCI zone

Found ACL rule(s) that allow "any" destination address entering PCI zone from DMZ zone

Firewall should only allow the access to the designated hosts that provide business services. Allowing access from DMZ zone to all destinations in PCI zones can inadvertently expose hosts that are running the same services as the designated hosts.

The following rules matched this check.

Entering/Exiting interfaces	ACL rule	NAT rule
mail1 to testweb	<a href="#">82</a>	<a href="#">No NATs</a>

### C1027 HTTP services allowed from the External zone to PCI zone

HTTP services allowed from External zone to PCI zone.

Http services in PCI zone can be accessed from External zone. Servers providing Internet services should be isolated in DMZ networks.

The following rules matched this check.

Entering/Exiting interfaces	ACL rule	NAT rule
outside to testweb	<a href="#">64</a> , <a href="#">65</a>	<a href="#">217</a>

### C1035 DNS services allowed from DMZ zone to PCI zone

DNS services are allowed from DMZ zone to PCI zone.

DNS service in PCI zone can be accessed from DMZ zone. DNS is one of the most attacked of the Internet services. This service should be restricted from the DMZ networks.

The following rules matched this check.

Entering/Exiting interfaces	ACL rule	NAT rule
mail1 to testweb	<a href="#">82</a>	<a href="#">198</a>

### **C1074 Rule(s) allow "any" UDP service from Internal zone to PCI zone**

Found ACL rule(s) that allow "any" UDP service entering PCI zone from Internal zone.

Firewalls should not allow unrestricted UDP service access from internal hosts to PCI zone. This would allow access to many vulnerable and unprotected services on the PCI zones. Only required services should be allowed from Internal zone.

The following rules matched this check.

Entering/Exiting interfaces	ACL rule	NAT rule
inside to testweb	<a href="#">108</a>	<a href="#">No NATs</a>

### **C1075 Rule(s) with "any" destination address allow access from Internal zone to PCI zone**

Found ACL rule(s) that allow "any" destination address entering PCI zone from Internal zone

Firewall should only allow the access to the designated hosts that provide business services. Allowing access from Internal zone to all destinations in PCI zones can inadvertently expose hosts that are running the same services as the designated hosts.

The following rules matched this check.

Entering/Exiting interfaces	ACL rule	NAT rule
inside to testweb	<a href="#">86</a>	<a href="#">No NATs</a>

### **C1128 HTTP services allowed from the PCI zone to External zone**

HTTP services allowed from PCI zone to External zone.

Http services in External zone can be accessed from PCI zone.

The following rules matched this check.

Entering/Exiting interfaces	ACL rule	NAT rule
testweb to outside	<a href="#">132</a> , <a href="#">133</a>	<a href="#">196</a> , <a href="#">217</a>

### **C1131 DNS services allowed from PCI zone to External zone**

DNS services are allowed from PCI zone to External zone.

DNS service in External zone can be accessed from PCI zone.

The following rules matched this check.

Entering/Exiting interfaces	ACL rule	NAT rule
testweb to outside	<a href="#">138</a>	<a href="#">196</a> , <a href="#">217</a>

### **C1132 Mail services allowed from PCI zone to External zone**

Mail services are allowed from PCI zone to External zone.

Mail service in External zone can be accessed from PCI zone.

The following rules matched this check.

Entering/Exiting interfaces	ACL rule	NAT rule
testweb to outside	<a href="#">135</a>	<a href="#">196</a> , <a href="#">217</a>

### **C1010 Insecure Internal/DMZ access to firewall**

Firewall can be accessed from internal/DMZ zones through insecure services.

It is recommended that only the secure management protocols should be used to manage the firewall.

The following rules matched this check.

Entering/Exiting interfaces	ACL rule	NAT rule
inside to device [acmecorp-pix]	<a href="#">246</a> , <a href="#">272</a> , <a href="#">273</a>	<a href="#">No NATs</a>

### **C1012 ICMP reply services are allowed from PCI zone to External zone**

ICMP reply services are allowed from PCI zone to External zone

Certain ICMP reply services (including echo replies, time exceeded, and destination unreachable) can be used by attacker to scan the PCI zone and propagate worms.

The following rules matched this check.

Entering/Exiting interfaces	ACL rule	NAT rule
testweb to outside	<a href="#">137</a>	<a href="#">196</a> , <a href="#">217</a>

### **C1058 TCP/UDP high ports allowed from External zone to PCI zone**

Packets with TCP/UDP high ports are allowed to enter the PCI zone from External zone.

Packets with TCP/UDP high ports is allowed from External zone to PCI zone. Deny all TCP and UDP ports above 1023 to provide reasonable assurance that the application ports are being used as intended.

The following rules matched this check.

Entering/Exiting interfaces	ACL rule	NAT rule
outside to testweb	<a href="#">67</a>	<a href="#">217</a>

### **C1022 Reserved source IP addresses (non RFC-1918) allowed access from External zone to DMZ zone.**

Packets with reserved source addresses (RFC-1700, RFC-2544, etc.), can enter the DMZ zone from External zone.

Inbound traffic from a system using source addresses that are reserved by RFC-1700, RFC-2544, RFC-3068, RFC-3171, Link Local, and TEST-NET should not be allowed from External zone(s) which has public routable IP addresses. The following addresses are checked : 0.0.0.0-0.255.255.255, 127.0.0.0-127.255.255.255, 169.254.0.0-169.254.255.255, 192.0.2.0-192.0.2.255, 198.18.0.0-198.19.255.255, and 224.0.0.0-239.255.255.255

The following rules matched this check.

Entering/Exiting interfaces	ACL rule	NAT rule
outside to mail1	<a href="#">77</a> , <a href="#">78</a>	<a href="#">213</a>
outside to proxymail	<a href="#">58</a> , <a href="#">59</a> , <a href="#">73</a> , <a href="#">74</a> <a href="#">75</a> , <a href="#">76</a>	<a href="#">218</a> , <a href="#">219</a>
outside to testweb	<a href="#">64</a> , <a href="#">65</a> , <a href="#">66</a>	<a href="#">217</a>

### **C1024 RFC-1918 private IP Source addresses allowed access from External zone to DMZ zone.**

Packets with source addresses that are reserved for private networks (RFC1918) can enter the DMZ zone from the External zone.

Inbound traffic from a system using source addresses that are reserved for private networks should not allowed from External zone(s) which has public routable IP addresses. The following addresses are analyzed: 10.0.0.0-10.255.255.255, 172.16.0.0-172.31.255.255, and 192.168.0.0-192.168.255.255

The following rules matched this check.

Entering/Exiting interfaces	ACL rule	NAT rule
outside to mail1	<a href="#">77</a> , <a href="#">78</a>	<a href="#">213</a>
outside to proxymail	<a href="#">58</a> , <a href="#">59</a> , <a href="#">73</a> , <a href="#">74</a> <a href="#">75</a> , <a href="#">76</a>	<a href="#">218</a> , <a href="#">219</a>
outside to testweb	<a href="#">64</a> , <a href="#">65</a> , <a href="#">66</a>	<a href="#">217</a>

### **C1038 Protection against SYN Flood attack**

SYN Flood attack protection is not enabled in the firewall.

The SYN attack causes a denial of service by sending to the target a high volume of packets which initiate a TCP connection. This connection is then never completed and the target host is left overwhelmed by half open connections, thus preventing legitimate connections from being made.