



## Firewall Security Audit

Host name:acmecorp-pix

### Completed on Thu Jul 15 11:27:47 CDT 2010

The Firewall 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

Policy checks profile: Standard

Number of policy checks performed: 124

Number of failed policy checks: 6 high risks, 5 medium risks, 11 low risks items

- High Risk
- Medium Risk
- Low Risk

#### Risk Description

C20	■ Rule(s) with "any" destination address allow access from DMZ zone to internal zone	<a href="#">Details</a>
C21	■ Rule(s) with "any" source address allow access from DMZ zone to internal zone	<a href="#">Details</a>
C31	■ Mail services allowed from external zone to internal zone	<a href="#">Details</a>
C35	■ DNS services allowed from DMZ zone to internal zone	<a href="#">Details</a>
C39	■ IP Address Spoofing	<a href="#">Details</a>
C100	■ Rule(s) with "any" source address allow access from DMZ zone to external zone	<a href="#">Details</a>
C10	■ Insecure Internal access to firewall	<a href="#">Details</a>
C12	■ ICMP reply services are allowed from internal zone to external zone	<a href="#">Details</a>
C49	■ Netbios services allowed from internal zone to external zone	<a href="#">Details</a>

C52	■ Netbios services allowed from internal zone to DMZ zone	<a href="#">Details</a>
C106	■ NFS services allowed from internal zone to external zone	<a href="#">Details</a>
C23	■ Reserved source IP addresses (non RFC-1918) allowed access from external zone to DMZ zone.	<a href="#">Details</a>
C25	■ RFC-1918 private IP Source addresses allowed access from external zone to DMZ zone.	<a href="#">Details</a>
C26	■ IP addresses 0.0.0.0, 127.0.0.1 are allowed as destination	<a href="#">Details</a>
C36	■ Mail services allowed from DMZ zone to internal zone	<a href="#">Details</a>
C38	■ Protection against SYN Flood attack	<a href="#">Details</a>
C57	■ Traceroute traffic allowed from external zone to DMZ zone	<a href="#">Details</a>
C59	■ TCP or UDP high ports allowed from external zone to DMZ zone	<a href="#">Details</a>
C99	■ Rule(s) allow "any" UDP service from internal zone to DMZ zone	<a href="#">Details</a>
C101	■ FTP services allowed from internal zone to external zone	<a href="#">Details</a>
C102	■ TFTP services allowed from internal zone to external zone	<a href="#">Details</a>
C103	■ Telnet services allowed from internal zone to external zone	<a href="#">Details</a>

## Dangerous Rules

*This is a listing of access-control lists that allow dangerous services from outside to inside or from inside to outside, based on a predefined list of checks. These checks not only examine a specific rule, but also consider the cumulative impact of all the preceding rules on the dangerous service. Hence, this list is an accurate indication of serious security gaps in firewall defenses. The list of checks that are used for determining a dangerous rule are also listed along with the dangerous rule.*

82	access-list acl_mail1 permit udp host 192.168.1.2 any eq domain Total: 2 High: 2
	C20 ■ <a href="#">Rule(s) with "any" destination address allow access from DMZ zone to internal zone</a>
	C35 ■ <a href="#">DNS services allowed from DMZ zone to internal zone</a>
108	access-list acl_inside permit udp any any Total: 3 Medium: 3
	C49 ■ <a href="#">Netbios services allowed from internal zone to external zone</a>
	C52 ■ <a href="#">Netbios services allowed from internal zone to DMZ zone</a>
	C106 ■ <a href="#">NFS services allowed from internal zone to external zone</a>

## Security Audit Details

### C20 Rule(s) with "any" destination address allow access from DMZ zone to internal zone

Found ACL rule(s) which allows "any" destination address entering internal 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 Internal zones can inadvertently expose hosts that are running the same services as the designated hosts.

The following rules matched this check.

Entering/Exiting interfaces	Security Rules	Address Translation Rules
mail1 to inside	<a href="#">82</a>	<a href="#">No NATs</a>

### C21 Rule(s) with "any" source address allow access from DMZ zone to internal zone

Found ACL rule(s) which allows "any" source address entering internal zone from DMZ zone

Access from DMZ hosts to internal networks should be restricted to specific hosts that need to communicate to internal hosts.

The following rules matched this check.

Entering/Exiting interfaces	Security Rules	Address Translation Rules
mail1 to inside	<a href="#">79</a>	<a href="#">No NATs</a>

### C31 Mail services allowed from external zone to internal zone

Mail services allowed from external zone to internal zone.

Mail service in internal zone can be accessed from external zone. Servers providing mail services should be isolated in DMZ networks. NIST Publication 800-41 (page 61) recommends to block mail services unless external mail relays.

The following rules matched this check.

Entering/Exiting interfaces	Security Rules	Address Translation Rules
outside to inside	<a href="#">60</a> , <a href="#">62</a> , <a href="#">68</a> , <a href="#">69</a> <a href="#">70</a> , <a href="#">71</a> , <a href="#">72</a>	<a href="#">212</a>

### C35 DNS services allowed from DMZ zone to internal zone

DNS services allowed from DMZ zone to internal zone.

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

The following rules matched this check.

Entering/Exiting interfaces	Security Rules	Address Translation Rules
mail1 to inside	<a href="#">82</a>	<a href="#">214</a>

### C39 IP Address Spoofing

IP Address Spoofing protection is not enabled in your firewall.

IP spoofing is commonly used by denial-of-service attacks which usually flood the victim with overwhelming amounts of packets. Static filtering policy might not apply to spoofed packets since the spoofed packets can have any source address. However, some anti-spoofing mechanisms have been implemented in firewall devices, e.g. ingress filtering at interface level or the firewall "anti-spoof" settings.

### C100 Rule(s) with "any" source address allow access from DMZ zone to external zone

Found ACL rule(s) which allows "any" source address entering external zone from DMZ zone

Access from DMZ hosts to external networks should be restricted to specific hosts that need to communicate to external hosts.

The following rules matched this check.

Entering/Exiting interfaces	Security Rules	Address Translation Rules
proxymail to outside	<a href="#">139</a>	<a href="#">No NATs</a>
testweb to outside	<a href="#">132</a>	<a href="#">No NATs</a>

### C10 Insecure Internal access to firewall

Your firewall can be accessed from internal 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	Security Rules	Address Translation Rules
inside to device [acmecorp-pix]	<a href="#">272</a> , <a href="#">273</a>	<a href="#">No NATs</a>

### C12 ICMP reply services are allowed from internal zone to external zone

ICMP reply services are allowed from internal zone to external zone

Certain ICMP reply services (including echo replies, time exceeded, and destination unreachable) can be used by attacker to scan your internal networks and propagate worms. NIST Publication 800-41 (page 61) recommends to block those icmp services in outbound traffic.

The following rules matched this check.

Entering/Exiting interfaces	Security Rules	Address Translation Rules
inside to outside	<a href="#">106</a>	<a href="#">191</a> , <a href="#">192</a> , <a href="#">193</a> , <a href="#">194</a> <a href="#">195</a> , <a href="#">196</a> , <a href="#">202</a> , <a href="#">212</a>

### C49 Netbios services allowed from internal zone to external zone

Netbios services allowed from internal zone to external zone.

Netbios services in external zone can be accessed from internal zone. Any Netbios access should be restricted in internal zones.

The following rules matched this check.

Entering/Exiting interfaces	Security Rules	Address Translation Rules
inside to outside	<a href="#">108</a>	<a href="#">191</a> , <a href="#">192</a> , <a href="#">193</a> , <a href="#">194</a> <a href="#">195</a> , <a href="#">196</a> , <a href="#">202</a> , <a href="#">212</a>

### C52 Netbios services allowed from internal zone to DMZ zone

Netbios services allowed from internal zone to DMZ zone.

Netbios services in DMZ zone can be accessed from internal zone. Any Netbios access should be restricted in internal zones.

The following rules matched this check.

Entering/Exiting interfaces	Security Rules	Address Translation Rules
inside to mail1	<a href="#">108</a>	<a href="#">197</a> , <a href="#">214</a>
inside to testweb	<a href="#">108</a>	<a href="#">198</a> , <a href="#">199</a> , <a href="#">200</a> , <a href="#">201</a>

### C106 NFS services allowed from internal zone to external zone

NFS services allowed from internal zone to external zone.

External NFS services can be accessed from internal hosts. NFS services might not provide strong authentication and encryption mechanism. NFS packets might be sniffed when they are across the open Internet.

The following rules matched this check.

Entering/Exiting interfaces	Security Rules	Address Translation Rules
inside to outside	<a href="#">108</a>	<a href="#">191</a> , <a href="#">192</a> , <a href="#">193</a> , <a href="#">194</a> <a href="#">195</a> , <a href="#">196</a> , <a href="#">202</a> , <a href="#">212</a>

### C23 Reserved source IP addresses (non RFC-1918) allowed access from external zone to DMZ zone.

Packets with source addresses that are reserved by RFC-1700, RFC-2544, etc. can enter your DMZ networks from external zone.

Inbound traffic from a system using a source address source addresses that are reserved by RFC-1700, RFC-2544, RFC-3068, RFC-3171, Link Local, and TEST-NET should not be coming from external zone(s) which has public routable IP addresses. The following addresses are analyzed: 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, 192.18.0.0-192.19.255.255, and 224.0.0.0-239.255.255.255

The following rules matched this check.

Entering/Exiting interfaces	Security Rules	Address Translation Rules
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>

## C25 RFC-1918 private IP Source addresses allowed access from external zone to DMZ zone.

Packets with source addresses that are reserved for private networks (refer to RFC1918) can enter your DMZ networks from external zone.

Inbound traffic from a system using a source address source addresses that are reserved for private networks should not coming 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	Security Rules	Address Translation Rules
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>

## C26 IP addresses 0.0.0.0, 127.0.0.1 are allowed as destination

Packets to IP addresses 0.0.0.0, 127.0.0.1 are allowed through the firewall.

127.0.0.1 is the IPv4 loopback address; 0.0.0.0 is the unspecified IPv4 address. Inbound or outbound network traffic for any given zone should not contain a destination address of 127.0.0.1 and 0.0.0.0. NIST Publication 800-41 recommends to block these two IP addresses as source and destination in both inbound and outbound traffic.

The following rules matched this check.

Entering/Exiting interfaces	Security Rules	Address Translation Rules
inside to outside	<a href="#">86</a> , <a href="#">87</a> , <a href="#">88</a> , <a href="#">89</a> <a href="#">90</a> , <a href="#">91</a> , <a href="#">92</a> , <a href="#">93</a> <a href="#">94</a> , <a href="#">95</a> , <a href="#">96</a> , <a href="#">97</a> <a href="#">98</a> , <a href="#">99</a> , <a href="#">100</a> , <a href="#">101</a> <a href="#">102</a> , <a href="#">103</a> , <a href="#">106</a> , <a href="#">107</a> <a href="#">108</a> , <a href="#">110</a> , <a href="#">113</a> , <a href="#">119</a>	<a href="#">191</a> , <a href="#">192</a> , <a href="#">193</a> , <a href="#">194</a> <a href="#">195</a> , <a href="#">196</a> , <a href="#">212</a>
mail1 to outside	<a href="#">82</a>	<a href="#">196</a>
proxymail to outside	<a href="#">139</a> , <a href="#">140</a> , <a href="#">141</a> , <a href="#">142</a>	<a href="#">218</a>
testweb to outside	<a href="#">132</a> , <a href="#">133</a> , <a href="#">134</a> , <a href="#">135</a> <a href="#">136</a> , <a href="#">137</a> , <a href="#">138</a>	<a href="#">196</a> , <a href="#">217</a>

## C36 Mail services allowed from DMZ zone to internal zone

Mail services allowed from DMZ zone to internal zone.

Hosts on the DMZ can access the internal mail servers. if these hosts are compromised, attacker can compromise the internal mail servers and propagate worms or virus through internal mail servers.

The following rules matched this check.

Entering/Exiting interfaces	Security Rules	Address Translation Rules
mail1 to inside	<a href="#">79</a>	<a href="#">214</a>

### C38 Protection against SYN Flood attack

SYN Flood attack protection is not enabled in your 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.

### C57 Traceroute traffic allowed from external zone to DMZ zone

Traceroute traffic can enter your DMZ networks from external zone.

Traceroute traffic is allowed from external zone to DMZ zone. Traceroute is used for mapping networks. It is not appropriate to allowed traceroute traffic into the DMZ networks.

The following rules matched this check.

Entering/Exiting interfaces	Security Rules	Address Translation Rules
outside to proxymail	<a href="#">73</a>	<a href="#">218</a>

### C59 TCP or UDP high ports allowed from external zone to DMZ zone

Packets with TCP/UDP high ports can enter your DMZ networks from external zone.

Packets with TCP/UDP high ports are allowed from external zone to DMZ 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	Security Rules	Address Translation Rules
outside to proxymail	<a href="#">61</a> , <a href="#">75</a>	<a href="#">218</a>
outside to testweb	<a href="#">67</a>	<a href="#">217</a>

## C99 Rule(s) allow "any" UDP service from internal zone to DMZ zone

Found ACL rule(s) which allow "any" UDP service entering DMZ zone from internal zone.

Access from internal zone to DMZ zone should be restricted to only required services. This prevents and allows detection of use of such typically undesirable services such as P2P filesharing, instant messaging, and network games. Compromised hosts will also send spam or viruses over non-standard ports.

The following rules matched this check.

Entering/Exiting interfaces	Security Rules	Address Translation Rules
inside to mail1	<a href="#">108</a>	<a href="#">No NATs</a>
inside to testweb	<a href="#">108</a>	<a href="#">No NATs</a>

## C101 FTP services allowed from internal zone to external zone

FTP services allowed from internal zone to external zone.

External FTP services can be accessed from internal hosts. Due to its inherently insecure data transferring, FTP service can be easily sniffed. It is recommended to use other secure file transfer services, e.g. SFTP and FTPS.

The following rules matched this check.

Entering/Exiting interfaces	Security Rules	Address Translation Rules
inside to outside	<a href="#">89</a> , <a href="#">91</a>	<a href="#">191</a> , <a href="#">192</a> , <a href="#">193</a> , <a href="#">194</a> <a href="#">195</a> , <a href="#">196</a> , <a href="#">202</a> , <a href="#">212</a>

## C102 TFTP services allowed from internal zone to external zone

TFTP services allowed from internal zone to external zone.

External TFTP service can be accessed from internal hosts. Due to the lack of security, TFTP is generally only used within private and local networks

The following rules matched this check.

Entering/Exiting interfaces	Security Rules	Address Translation Rules
inside to outside	<a href="#">108</a>	<a href="#">191</a> , <a href="#">192</a> , <a href="#">193</a> , <a href="#">194</a> <a href="#">195</a> , <a href="#">196</a> , <a href="#">202</a> , <a href="#">212</a>

## C103 Telnet services allowed from internal zone to external zone

Telnet services allowed from internal zone to external zone.

External Telnet services can be accessed from internal hosts. Telnet services might not provide strong authentication and encryption mechanism. Telnet packets might be sniffed when they are across the open Internet. It is recommended to use other alternative services with strong authentication and encryption, e.g. SSH.

The following rules matched this check.

Entering/Exiting interfaces	Security Rules	Address Translation Rules
inside to outside	<a href="#">94</a>	<a href="#">191</a> , <a href="#">192</a> , <a href="#">193</a> , <a href="#">194</a> <a href="#">195</a> , <a href="#">196</a> , <a href="#">202</a> , <a href="#">212</a>