

Using InfoSector to Audit PCI-DSS Compliance

Payment Card Industry Data Security Standard (PCI-DSS) addresses controls that are needed to protect card holder data. PCI-DSS has twelve top level requirements. Requirement 1 addresses network security implemented by firewalls. InfoSector's constraint analysis can be an important tool in verifying compliance with Requirement 1.

Example PCI Constraint

Consider Requirement 1.3.1 “Implement a DMZ to limit inbound and outbound traffic to only services necessary for the cardholder data environment (CDE)”. For a firewall separating the DMZ and the inside networks from the Internet, this requirement indicates that only necessary services should be allowed to pass in and out of the DMZ. All other traffic should be denied. Given a list of necessary services, this could be expressed in conditional logic as:

```
If inbound interface = eth0
  if destination address is WebServer and
    service is web
    ok
  else if destination address is DNSServer
    and service is DNS
    ok
  ...
  otherwise
    Action contains Deny
```

The outer condition tests whether the traffic is coming from the outside interface, i.e. testing for traffic entering the organization. The cases test for necessary servers and services. The requirement doesn't fail if these services aren't allowed, so the action is just ok. The last case is the “otherwise” case. If the packet hasn't met any of the previous conditions, this is the action that should occur. In this case, any traffic that doesn't meet the previous conditions should be denied.

This can be expressed in a direct expression. We add the otherwise operator as * in addition to the standard and (&), or (|), and not (!).

```
(Scope = $InternetIncoming &
  ((Dest Addr ^ $WebServer & Dest Svc ^ TCP:80) |
  (Dest Addr ^ $DNSServer & Dest Svc ^ $DnsSvc) |
```

```
(Dest Addr ^ $MailServer & Dest Svc ^ $MailServices))
* (Action = Deny))
```

Figure 1 shows this expression in InfoSector's graphical expression editor. Notice that instead of referring to addresses and ports directly, the editor shows names, e.g., \$DnsSvc. InfoSector provides macros for use in expression. In this way, you can set up general expressions and apply the constraints in different situations by changing the addresses and ports that the macros map to. This means that general constraints like those for PCI-DSS can be expressed once, and then applied in multiple organizations just by defining the specific network and port values for the target organization.

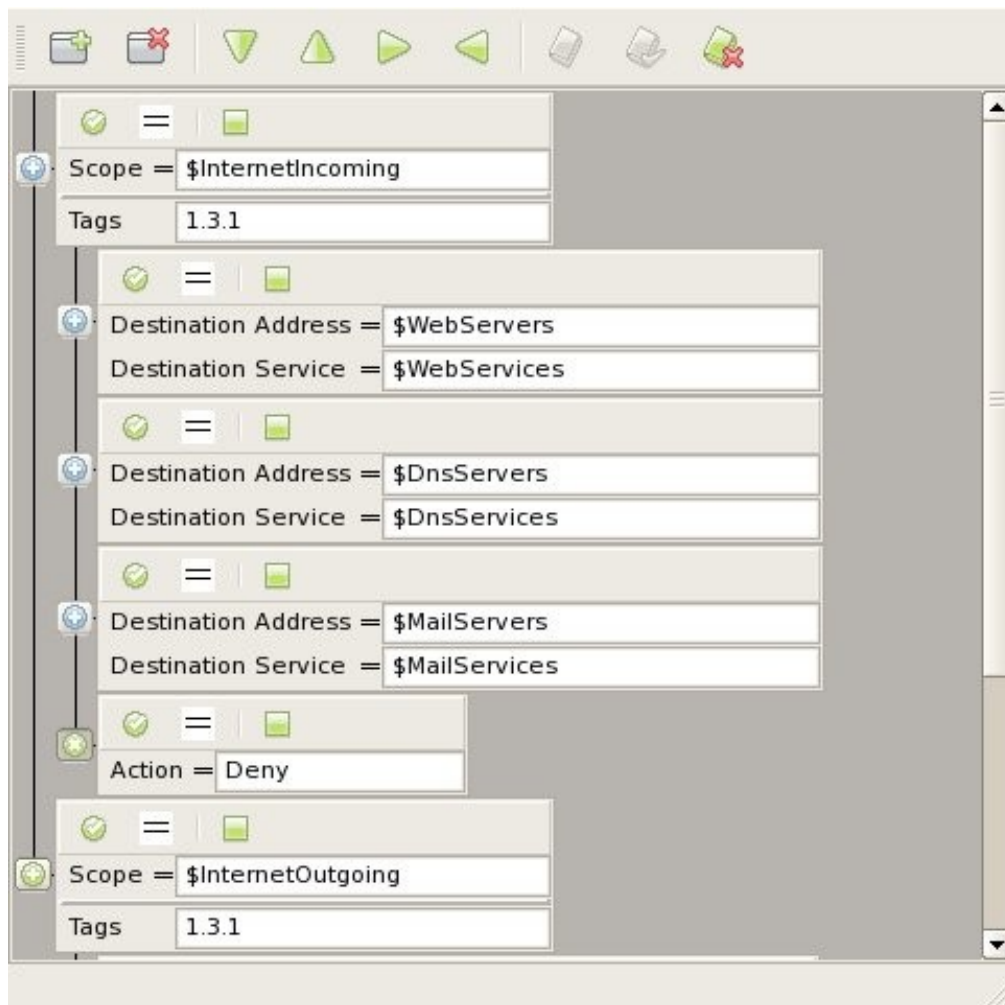


Figure 1: Graphical representation of requirement 1.3.1 for PCI-DSS.

PCI Constraint Summary

Quite a few of the points in PCI-DSS Requirement 1 can be verified with the help of InfoSector. The

table below reviews the subpoints of Requirement 1 and discusses whether and how InfoSector can address compliance.

Requirement	Covered by InfoSector	Comments
1.1.1 - A formal process for approving and testing all network connections and changes to the firewall and router configurations	Indirectly	A process requirement. Must be verified by reviewing the organization's change control process. However, use of a configuration analysis tool like InfoSector can provide evidence of a formal change control process for the network configuration.
1.1.2 - Current network diagram with all connections to cardholder data, including any wireless networks	Indirectly	Auditor must manually review the diagram. Could use InfoSector in dissection mode to verify the correctness of the diagram.
1.1.3 - Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	No	Must review the network diagram and perhaps the machine room wiring to verify that a firewall is present to enforce specified restrictions.
1.1.4 - Description of groups, roles, and responsibilities for logical management of network components	No	This addresses how the administration of the device configuration is divided between IT staff. Again a process-oriented requirement.
1.1.5 - Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure	Yes	This can be divided into two constraints. One that verifies that only services with a business case justification can possibly transit the firewall. The other constraint identifies insecure protocols such as ftp and telnet. While these services may be allowable, the customer must provide evidence that they are necessary and they must identify additional controls that are in place to address the inherent protocol insecurity.
1.1.6 - Requirement to review firewall and router rule sets at least every six months	Indirectly	If InfoSector reports are part of the organization's change process, the dated reports can be used to show the frequency of rule set review.
1.2.1 - Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment	Yes	A constraint can be built from the necessary services. If the service is not listed, an otherwise clause can be used to indicate that all other traffic must be denied.
1.2.2 - Secure and synchronize router configuration files.	No	Another process requirement that the auditor must verify. The start up and the running configurations should be the same.

Requirement	Covered by InfoSector	Comments
1.2.3 - Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.	Yes	Create a constraint that enumerates the business-necessary traffic. The otherwise clause indicates that all other traffic should be denied.
1.3.1 - Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.	Yes	Described in detail in the example section.
1.3.2 - Limit inbound Internet traffic to IP addresses within the DMZ.	Yes	Build a constraint that tests that only inbound traffic to DMZ addresses is allowed.
1.3.3 - Do not allow any direct routes inbound or outbound for traffic between the Internet and the cardholder data environment.	Yes	Create a constraint that ensures that traffic flows direct from the Internet to the cardholder data environment are not allowed.
1.3.4 - Do not allow internal addresses to pass from the Internet into the DMZ.	Yes	Ensure that internal address spoofing is prohibited. Build a constraint to ensure that inbound traffic with an internal source address is prohibited.
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.	Yes	Build a constraint to ensure that traffic leaving the card holder data environment can only reach DMZ addresses.
1.3.6 - Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)	Yes	Verify that the inspection action is performed on all traffic that is allowed to traverse the firewall.
1.3.7 - Place the database in an internal network zone, segregated from the DMZ.	No	This requires a review of the network diagram and/or physical wiring.
1.3.8 - Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet, using RFC 1918 address space. Use	Yes	Build a constraint that ensures that all traffic from internal address to the Internet also has address translation performed.

Requirement	Covered by InfoSector	Comments
network address translation (NAT) technologies—for example, port address translation (PAT).		
1.4 - Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.	No	Requires review of programs installed on firewalls and desktops.