

Usage guide

Firesectm

Firewall Rule base Analysis Tool
For PCI DSS Compliance

Comprehensive rule base analysis for medium to large enterprise environments

The large picture – Automation of rule base analysis

- Simplified analysis of large rule sets
- Groups common rules
- Removes redundancy
- Searches for vulnerable rule patterns
- Compares rule sets
- Analyses security

Supported Firewalls in Full Version

Netscreen
Cyberguard , Cyberguard Knight Star
Cisco PIX
Generic rule sets

Supported Firewalls in Trial Version

Only default configuration & logs provided with the setup



Introduction

The Payment Card Industry Data Security Standard (PCI DSS) is built to ensure that merchants who allow for credit card transactions adhere to a formalized set of controls to protect card holder data. The Standard is divided into 12 requirements grouped together into 6 control objectives.

The first of these 12 requirements deals exclusively with firewall configuration. This requirement addresses the need to segregate those systems, which hold card holder data and to ensure that they are well-protected from external and internal threats. It lists out restrictions that must be imposed in terms of ports to be allowed and blocked and traffic to be allowed or blocked between the Internet, DMZ and internal IP addresses.

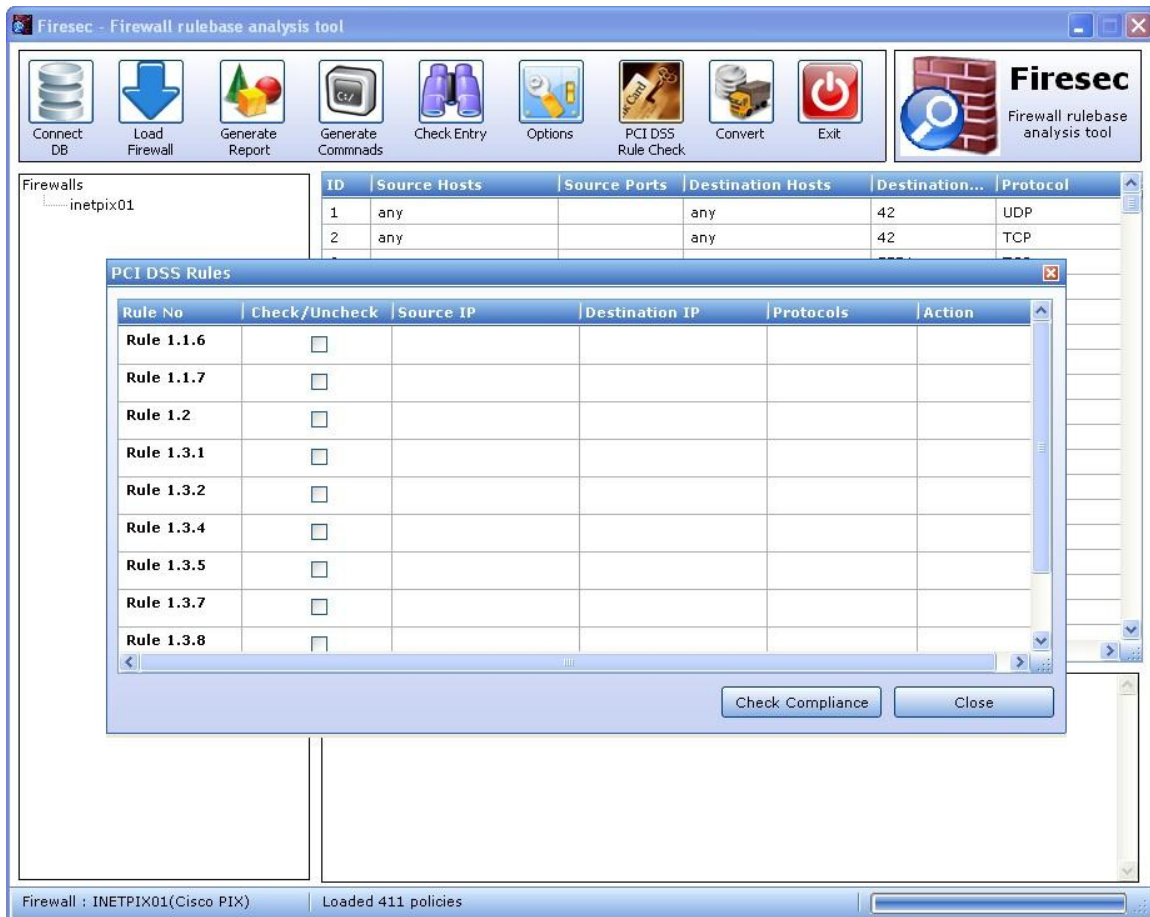
In cases, where a firewall has more than a few dozen rules, manual evaluation of the configuration becomes almost impossible. This is where Firesec™ comes in.

Firesec™ is an advanced firewall configuration analysis tool, which helps you answer the following questions:

1. What traffic is allowed on to my card holder database?
2. Are there any rules that permit traffic from my internal IP addresses to the Internet?
3. Have I opened up risky ports such as Telnet (TCP 23), FTP (TCP 21), RDP (TCP 3389) to any of my servers?
4. What traffic is allowed between my internal IP addresses and my DMZ?
5. Do I have any rules which contradict each other (Shadow rules)?
6. Do I have rules, which are no longer in use (Unused Rules)?
7. Do I have rules, which are subsets of each other (Redundant Rules)?

How Firesec™ checks for PCI DSS Compliance

The following sections look at specific requirements of PCI DSS and illustrate how Firesec can easily help you ensure for compliance against each of these requirements. Launch the PCI DSS compliance checker by clicking on the button “PCI DSS Rule Check”¹



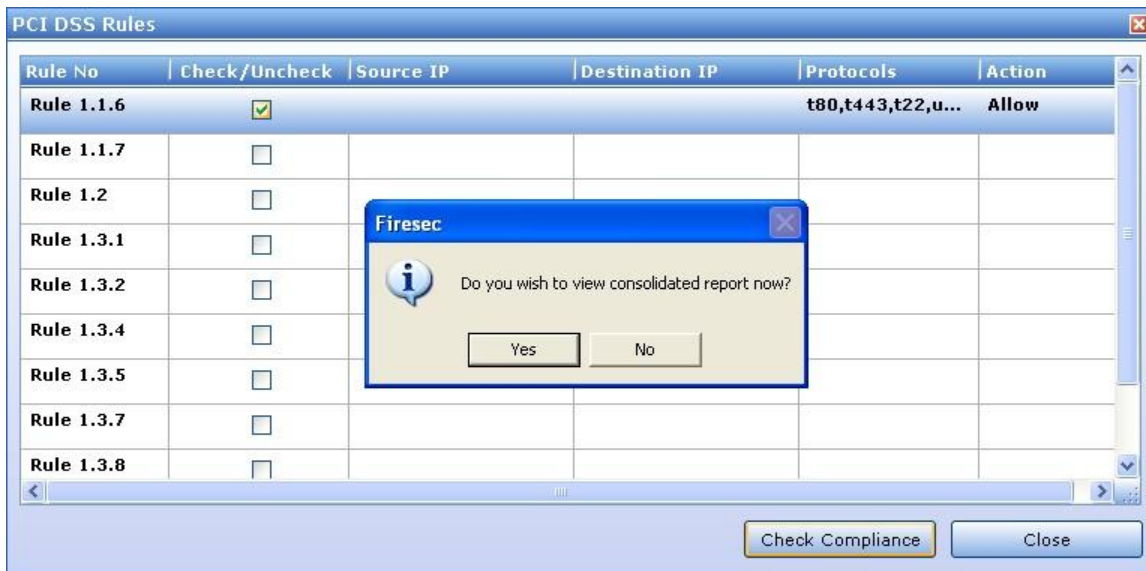
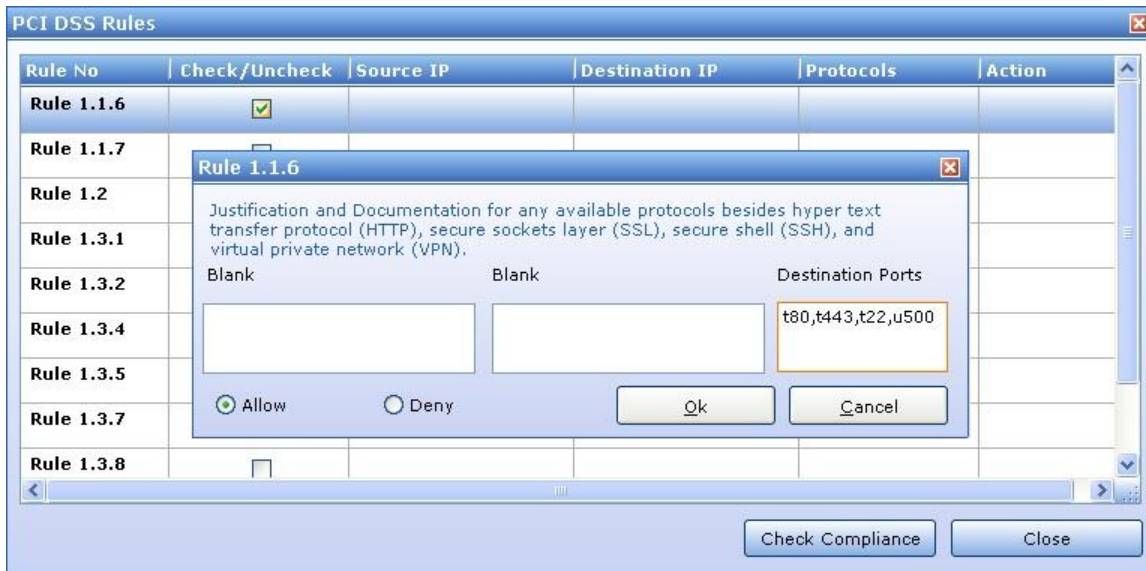
¹ Please note that the PCI DSS checking module is not available as part of the Firesec Standard Edition.

1.1 - Establish firewall configuration standards that include the following

Rule 1.1.6

Justification and documentation for any available protocols besides hypertext transfer protocol (HTTP), and secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN)

Click on the item Rule 1.1.6



Firesec Inputs Required²

Source IPs – keep it blank

Destination IPs – keep it blank

Destination Ports – t80, t443, t22, u500. These represent the HTTP, HTTPS, SSH and VPN ports respectively.

What Firesec does?

Firesec will now check for all rules that allow for ports *other than* the ones given in the list. The ports given in the list are considered as safe, and necessary for business use. The results are as shown below:

Statistics on the analysis:

Rules category	Compliant / Non-Compliant
Rule 1.1.6	317

Results of PCI DSS Compliance

Rule 1.1.6
Justification and Documentation for any available protocols besides hyper text transfer protocol (HTTP), secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN).
The following policies can be dropped based on Rule 1.1.6 to protect card holder data.

Input :

Source IPs	Destination IPs	Destination Ports	Action
		t80,t443,t22,u500	Allow

Output :

ID	Source Hosts	Destination Hosts	Services	Action
9	22.118.128.0/32	22.118.128.0/32	iany	permit
13	any	22.118.128.135/32	t25	permit
14	any	22.118.128.141/32	t25	permit
15	any	22.118.128.154/32	t25	permit
35	22.118.128.0/32	22.118.128.77/32	u53	permit
36	22.118.128.0/32	22.118.128.72/32	u162	permit
37	22.118.128.225/32, 22.118.128.226/32	symantec3 symantec4	t1645:1646	permit
38	22.118.128.225/32, 22.118.128.226/32	symantec4	uradius:radius-acct	permit
39	22.118.128.225/32	22.118.128.80/32	u1646	permit
32	22.118.128.0/32	22.118.128.78/32	t53	permit
44	any	22.118.128.19/32	iecho	permit
45	any	22.118.128.21/32	iecho	permit
46	any	22.118.128.19/32	iany	permit
47	any	22.118.128.21/32	iany	permit
52	22.118.133.49/32	22.118.128.150/32	t8080	permit
55	22.118.128.225/32	22.118.128.67/32	uradius	permit
57	any	22.118.128.74/32	t25	permit

How can you fix this?

You will have to ensure that there is adequate justification and documentation for all rules, which allow for traffic to ports other than those, which are specifically permitted under this rule.

² Firesec inputs can be entered in a number of ways.

IP Address: Here you can enter a single IP address, a range of IP addresses using CIDR format, or a comma-separated list of IP addresses and/or IP address ranges

Ports: Ports can be entered either as single ports with a 't' or a 'u' appended to the port number to specific TCP or UDP protocol respectively. Additionally, port ranges can be entered using the -, such as t1024-65535 to specify ports between 1024 and 65535. Combinations of ports and port ranges can be entered separated by commas.

Rule 1.1.7

Justification and documentation for any risky protocols allowed (for example, file transfer protocol (FTP), which includes reason for use of protocol and security features implemented

Click on Rule 1.1.7

Firesec inputs required

Source IPs - blank

Destination IP – blank

Destination ports – risky ports such as FTP (TCP 21), telnet (FTP 23), or even an entire range such as t1024-65535 (all ports above 1024).

What Firesec does?

Firesec will scan the entire ruleset looking for rules which allow traffic to these risky ports, and will then highlight them in the compliance report.

How can you fix this?

Check whether you really need these rules or not. Determine the justification for these rules, if none can be found, drop them. If there is valid justification, then document this justification for each of the rules. You may evaluate a network redesign or a relook at your firewall configuration standards if the violations are too many.

Rule 1.1.8

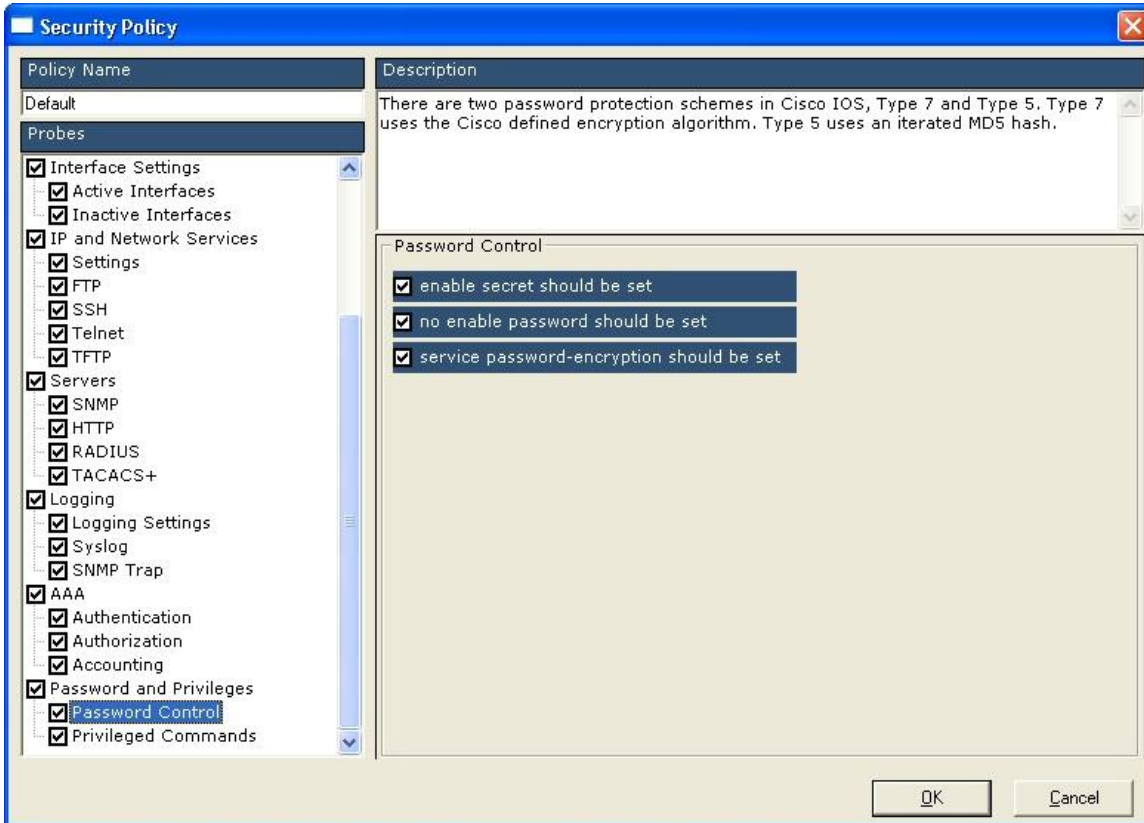
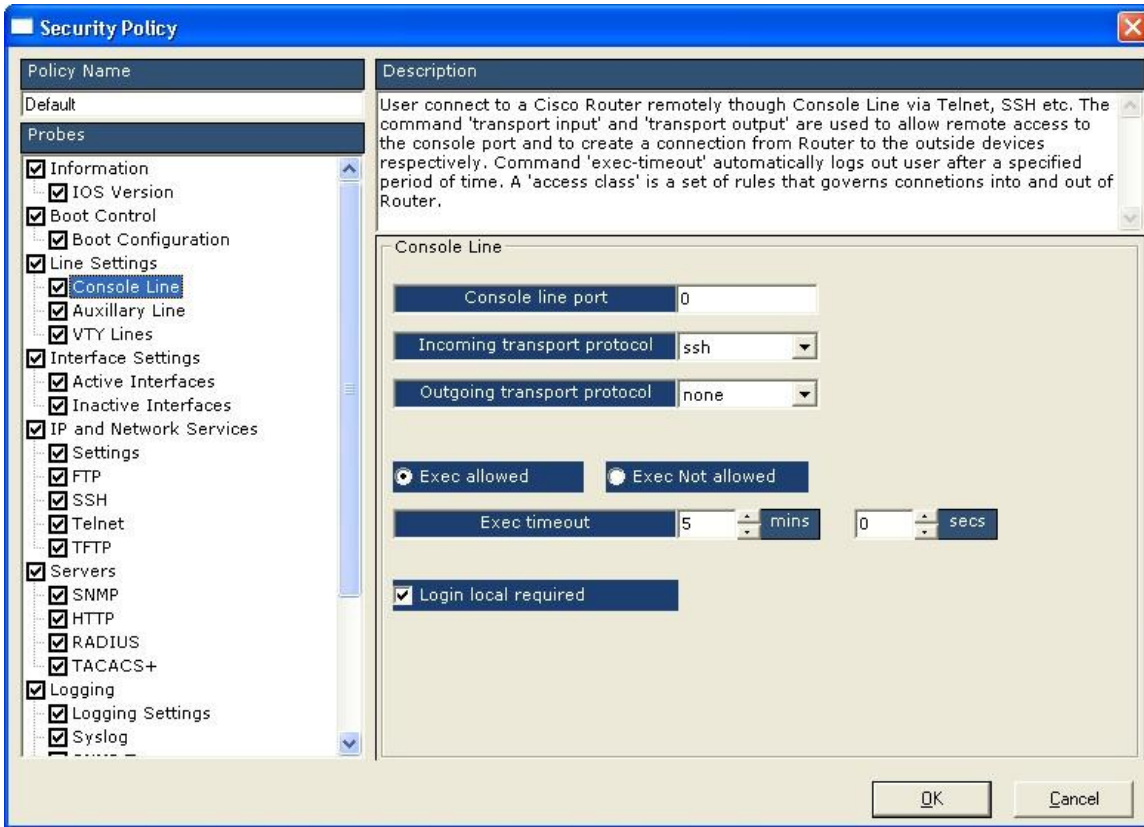
Quarterly review of firewall and router rule sets

Simply run Firesec on a regular basis – at least once a quarter, and do a completely analysis of the firewall and router rule sets.

Rule 1.1.9

Configuration standards for routers.

Click on the Router Configuration check from Firesec. It shows up a policy documentation screen, where you can enter the values to be allowed/disallowed for various router configuration options such as IOS version, Boot Control, Line Settings, Interface Settings, IP and Network Services, Servers, Logging, AAA, and Password and Privileges. The following screen illustrates some of the settings that you can do.



Once you have configured these settings, simply load your router configuration and it will be analyzed for compliance against these settings. A report is generated showing areas of non-compliance as shown below:

1.2 - Build a firewall configuration that denies all traffic from “untrusted” networks and hosts, except for protocols necessary for the cardholder data environment.

Firesec inputs required

Source IPs – enter a list of *trusted* IP addresses, such as your internal network and any partner or remote office network ranges

Destination IPs – you may keep this blank

Destination Ports – either enter the list of trusted protocols, or keep it blank

What Firesec does?

Firesec will analyze all rules, where the source IP address belongs to a range, which is *not* in the list of source IP addresses provided by you. Since, we can easily define a trusted range, it is preferable to do so, and then look for IP addresses that fall outside this range or ranges.

If you have supplied a list of destination ports, then these rules will be checked for destination ports, which are outside of the given list of trusted ports. Thus, here we follow the principle of white-listing of IP addresses and ports, and look for rules, which fall outside the whitelist.

How can you fix this?

Take each rule shown in the report for this section, and evaluate whether it can be removed completely or restricted further in terms of the IP addresses and ports.

1.3 - Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks. This firewall configuration should include the following:

Rule 1.3.1

Restricting inbound Internet traffic to Internet protocol (IP) addresses within the DMZ (ingress filters)

[Click on Rule 1.3.1](#)

Firesec inputs required

Source IPs – enter a list of *internal* IP addresses, or rather those IP address ranges, which are not to be considered as *external*. This would be your internal LAN IP address range, the DMZ range, any partner or trusted IP address range.

Destination IPs – enter the range of your DMZ IP addresses

Destination ports – blank

What Firesec does?

Firesec scans your ruleset for all rules, which allow traffic from any IP address *other than* those listed in the source IP address range. It then checks these rules further to see which of these have the destination IP address *other than* the DMZ IP address range. Essentially, we are looking for any rule, which allows inbound traffic to an IP address not belonging to the DMZ range.

How can you fix this?

In the compliance report for this section you will find rules, which allow inbound Internet traffic to an IP address other than the DMZ. Check each of these rules, and wherever possible remove those, which may not be necessary. You may consider moving servers from your internal LAN to the DMZ or an Extranet segment if it is absolutely necessary for outsiders or trusted parties to access these servers. As a matter of principle they should not be on the internal trusted segment.

Rule 1.3.2

Not allowing internal addresses to pass from the Internet into the DMZ**Click on Rule 1.3.2****Firesec inputs required**

Source IPs – the IP address or addresses of internal LAN

Destination IPs – the IP address or range of your DMZ

What Firesec does?

Firesec checks whether the IP addresses of the internal LAN are accessing the un-trusted network and from that un-trusted network whether it is accessing the DMZ. If a violation is found this is shown in the compliance report.

How can you fix this?

Remove all rules which are highlighted as allowing traffic from internal IP addresses to pass through to the DMZ via the Internet.

Rule 1.3.4

Placing the database in an internal network zone, segregated from the DMZ**Click on Rule 1.3.4****Firesec inputs required**

Source IPs – the IP address or addresses of your database

Destination IPs – the IP address or range of your DMZ

What Firesec does?

Firesec checks whether the IP addresses of the database are part of the DMZ range or not. If a violation is found this is shown in the compliance report.

How can you fix this?

Move the database from the DMZ into your internal LAN. Modify your applications to talk to the relocated database. Modify your firewall rules to allow this specific traffic to pass through from the DMZ to the database on the internal LAN.

Rule 1.3.5

Restricting inbound and outbound traffic to that which is necessary for the cardholder data environment**Click on Rule 1.3.5****Firesec inputs required**

Source IPs – IP addresses that relate to the cardholder data environment. Typically, the segment which contains systems that constitutes the cardholder data environment.

Destination IPs – same as the source IPs

Destination ports –

What Firesec does?

Firesec will scan the entire ruleset and look for rules which relate to the cardholder data environment in either the source IPs or destination IPs.

How can you fix this?

Analyze these rules, and ensure they only allow necessary inbound and outbound traffic for the cardholder data environment.

Rule 1.3.7

Denying all other inbound and outbound traffic not specifically allowed**Click on Rule 1.3.7****Firesec inputs required**

No inputs are required for this rule.

What Firesec does?

Firesec checks for the presence of the “deny any any” rule at the end of the firewall ruleset.

How can you fix this?

If Firesec does not find such a rule, it reports it as a non-compliance. Ensure that the firewall contains a “deny all” rule at the end of each access list.

Rule 1.3.8

Installing perimeter firewalls between any wireless networks and the cardholder data environment, and configuring these firewalls to deny any traffic from the wireless environment or from controlling any traffic (if such traffic is necessary for business purposes)

[Click on Rule 1.3.8](#)

Firesec inputs required

Source IPs – IP addresses of the wireless networks
Destination IPs – IP addresses of the cardholder data
Destination ports – blank

What Firesec does?

Firesec checks for all rules where the source IP addresses are those of the wireless network and the destination IP addresses belong to the cardholder data environment.

How can you fix this?

Ensure that the output reflects a restricted set of traffic between these environments; or rather no traffic is permitted between the wireless networks and the cardholder data environment.

1.4 - Prohibit direct public access between external networks and any system component that stores cardholder data (for example, databases, logs, trace files).

[Click on Rule 1.4](#)

Firesec inputs required

Source IPs – IP address ranges of *internal* networks.
Destination IPs – IP addresses of system components that store cardholder data
Destination ports – blank

What Firesec does?

Firesec checks for rules, where the source IP address *does not* belong to the range provided. It then checks whether the destination IP address belongs to the list of systems specified as holding cardholder data.

How can you fix this?

Check all the rules that are shown as being non-compliant with this requirement, i.e. these are rules, which allow traffic between external networks and any system component storing cardholder data. Remove these rules, or modify them to severely restrict such traffic. You may need to modify your network design.

Rule 1.4.1

Implement a DMZ to filter and screen all traffic and to prohibit direct routes for inbound and outbound Internet traffic

Click on Rule 1.4.1

Firesec inputs required

Source IPs – Trusted IP range
Destination IPs – Internal LAN range
Destination ports –

What Firesec does ?

First it will check for all rules, where source IP intersects internal LAN range & Destination IP is NOT a subset of Trusted IP range. Second it will check for all rules, where source IP is NOT a subset of Trusted IP range and Destination IP intersects internal LAN range.

How can you fix this?

Ensure that there is no rule, which permits traffic to flow directly between the internal LAN and the Internet.

Rule 1.4.2

Restrict outbound traffic from payment card applications to IP addresses within the DMZ.

Click on Rule 1.4.2

Firesec inputs required

Source IPs – IP addresses of systems that host payment card applications
Destination IPs – IP address ranges of the DMZ
Destination ports – blank

What Firesec does?

Firesec will check for all rules where traffic from payment card systems is allowed to IP addresses other than the DMZ.

How can you fix this?

Determine whether this traffic is really necessary to be permitted. To comply with this requirement, you will have to allow traffic from payment card applications only to the DMZ.

1.5 - Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet. Use technologies that implement RFC 1918 address space, such as port address translation (PAT) or network address translation (NAT).

Click on Rule 1.5

Firesec inputs required

No inputs required

What Firesec does?

Firesec finds out IP addresses that are translated using PAT or NAT

How can you fix this?

Ensure that there is no direct route from the internal network to the Internet, which might bypass the firewall.