





PCI Compliance Report

Fri Jul 17 14:38:26 CDT 2009
YahooCMA (192.168.20.192)
created by FireMon

This report is based on the [PCI Data Security Standard version 1.2](#), and covers control items related to Firewall policies.

8 of 15 checks pass for the YahooCMA device.

Summary

Section	Pass/Fail	Description
1.1.1		<p>Verify that there is a formal process for testing and approval of all network connections and changes to firewall and router configurations.</p> <p>Results <i>FireMon has detected 0 changes to this firewall over the past 30 days.</i></p>
1.1.5a		<p>Verify that firewall and router configuration standards include a documented list of services, protocols and ports necessary for business-for example, hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols.</p> <p>Results <i>All of the services permitted by the firewall from the <u>External</u> zone to the <u>DMZ</u> zone are allowed.</i></p>
1.1.5b		<p>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.</p> <p>Results <i>All of the services permitted by the firewall from the <u>External</u> zone to the <u>DMZ</u> zone are allowed.</i></p>
1.2.1b		<p>Verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit "deny all" or an implicit</p> <p>Results <i>All policies on this firewall include a drop rule as the final rule.</i></p>
1.2.3		<p>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.</p> <p>Results <i>All of the services permitted by the firewall from the <u>External</u> zone to the <u>DMZ</u> zone are allowed.</i></p>
1.3.1		<p>Verify that a DMZ is implemented to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.</p> <p>Results <i>All of the services permitted by the firewall from the <u>External</u> zone to the <u>DMZ</u> zone are allowed.</i></p>
1.3.2		<p>Verify that inbound Internet traffic is limited to IP addresses within the DMZ.</p> <p>Results <i>All of the services permitted by the firewall from the <u>External</u> zone to the <u>DMZ</u> zone are allowed.</i></p>
1.3.3		<p>Verify there is no direct route inbound or outbound for traffic between the Internet and the cardholder data environment.</p> <p>Results <i>11 services that are not defined as allowed are permitted from the <u>External</u> zone to the <u>PCI</u> zone.</i></p>
1.3.4		<p>Verify that internal addresses cannot pass from the Internet into the DMZ.</p> <p>Results</p>
1.3.5		<p>Verify that outbound traffic from the cardholder data environment to the Internet can only access IP addresses within the DMZ.</p> <p>Results <i>9 services that are not defined as allowed are permitted from the <u>External</u> zone to the <u>PCI</u> zone.</i></p>
1.3.6		<p>Verify that the firewall performs stateful inspection (dynamic packet filtering). [Only established connections should be allowed in, and only if they are associated with a previously established session (run a port scanner on all TCP ports with "syn reset" or "syn ack" bits set - a response means packets are allowed through even if they are not part of a previously established session).]</p> <p>Results <i>Stateful inspection is enabled on the firewall.</i></p>
1.3.7		<p>Verify that the database is on an internal network</p> <p>Results <i>All of the services permitted by the firewall from the <u>DMZ</u> zone to the <u>PCI</u> zone are allowed.</i></p>
2.2.2		<p>For a sample of system components, inspect enabled system services, daemons, and protocols. Verify that unnecessary or insecure services or protocols are not enabled, or are justified and documented as to appropriate use of the service. For example, FTP is not used, or is encrypted via SSH or other technology.</p> <p>Results <i>9 services that are not defined as allowed are permitted from the <u>*</u> zone to the <u>PCI</u> zone.</i></p>
2.3.0		<p>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.</p> <p>Results <i>9 services that are not defined as allowed are permitted from the <u>External</u> zone to the <u>PCI</u> zone.</i></p>
6.1.0		<p>Verify all system components and software have latest vendor-supplied security patches installed.</p> <p>Results <i>The device is missing the " file.</i></p>

Detail

1.1 Establish firewall and router configuration standards that include the following

Section 1.1.1 - (Fail)

Verify that there is a formal process for testing and approval of all network connections and changes to firewall and router configurations.

Summary

FireMon has detected 0 changes to this firewall over the past 30 days.

Recommendations

To meet this requirement, make sure that you continuously run FireMon. FireMon will detect and collect firewall changes immediately after they occur.

Details

No changes were detected.

Section 1.1.5a - (Pass)

Verify that firewall and router configuration standards include a documented list of services, protocols and ports necessary for business—for example, hypertext transfer protocol (HTTP) and Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols.

Summary

All of the services permitted by the firewall from the External zone to the DMZ zone are allowed.

Recommendations

The number of services permitted to the DMZ zone should be limited. To ensure continuous compliance with this requirement, please periodically review the list of services allowed to the DMZ zone. Make sure that each service is fully documented.

Details

Evaluated

All rules that allow traffic between External and DMZ, in either direction.

Allowed Services (1)

The PCI service group includes PCI.

Disallowed Services (0)

The following services are not explicitly allowed, services include no services.

Section 1.1.5b - (Pass)

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.

Summary

All of the services permitted by the firewall from the External zone to the DMZ zone are allowed.

Recommendations

The number of services permitted to the DMZ zone should be limited. To ensure continuous compliance with this requirement, please periodically review the list of services allowed to the DMZ zone. Make sure that each service is fully documented.

Details

Evaluated

All rules that allow traffic between External and DMZ, in either direction.

Allowed Services (1)

The PCI service group includes PCI.

Disallowed Services (0)

The following services are not explicitly allowed, services include no services.

1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.

Section 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

Summary



All policies on this firewall include a drop rule as the final rule.

Recommendations

All traffic, unless explicitly permitted, must be denied. You can ensure continuous compliance with this requirement by maintaining a drop rule at the end of every firewall policy.

Details

Policy: SPLAT-Policy

Security Rule							^Top
Rule	Name	Source	Destination	Service	Action	Log	Comments
72	Global Drop	* Any	* Any	* Any	 Drop	 Log	

Section 1.2.3 - (Pass)

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.

Summary

All of the services permitted by the firewall from the External zone to the DMZ zone are allowed.

Recommendations

Wireless networks are inherently risky, so access from a wireless network to a PCI network should be limited. To ensure continuous compliance with this requirement, please periodically review your list of allowed wireless services for accuracy.

Details

Evaluated

All rules that allow traffic from External to DMZ.

Allowed Services (1)

The PCI Services service group includes PCI Services.

Disallowed Services (0)

The following services are not explicitly allowed, services include no services.

1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.

Section 1.3.1 - (Pass)

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

Summary

All of the services permitted by the firewall from the External zone to the DMZ zone are allowed.

Recommendations

The DMZ should limit traffic to the PCI zone. To ensure continuous compliance with this requirement, please periodically review your list of services defined as acceptable between the PCI zone and the DMZ.

Details

Evaluated

All rules that allow traffic between External and DMZ, in either direction.

Allowed Services (1)

The PCI service group includes PCI.

Disallowed Services (0)

The following services are not explicitly allowed, services include no services.

Section 1.3.2 - (Pass)

Verify that inbound Internet traffic is limited to IP addresses within the DMZ.

Summary

All of the services permitted by the firewall from the External zone to the DMZ zone are allowed.

Recommendations

To ensure ongoing compliance with this requirement, please continue to force all external communication with a destination in the PCI zone to terminate in the DMZ.

Details

Evaluated

All rules that allow traffic from External to DMZ.

Allowed Services (1)

The PCI service group includes PCI.

Disallowed Services (0)

The following services are not explicitly allowed, services include no services.

Section 1.3.3 - (Fail)

Verify there is no direct route inbound or outbound for traffic between the Internet and the cardholder data environment.

Summary

11 services that are not defined as allowed are permitted from the External zone to the PCI zone.

Recommendations

To meet this requirement, remove any rules that permit direct traffic between the External zone to the PCI zone.

Details

Evaluated

All rules that allow traffic between External and PCI, in either direction.

Allowed Services (0)

The service group includes no services.

Disallowed Services (11)

The following services are not explicitly allowed, services include AOL, AOL_Messenger, Citrix_ICA, Citrix_ICA_Browsing, Citrix_metaFrame, ESP, FM_GUI_Access, ICQ_locator, RDP, domain-tcp, tcp_service_test.

Policy: SPLAT-Policy

Security Rule							^Top
Rule	Name	Source	Destination	Service	Action	Log	Comments
33		* Any	mdean_group AddrTransHostHidelP	TCP domain-tcp	Accept	None	CCM#670
38		F-199.158 .104.0-21- Renamed	L-FSAKC-165.221.017 .0	Citrix_meta Frame AOL_Messenger	Accept	Log	Insert new rule
45	jira 373 take 23	temp-group@ BackEnd_Net	AddrTransNet this_is_a_really_long _host_name_to_test_T T1457	TCP tcp_service_test	Authenticate	Log	CCN: DEV-563 another test
53	Secure Access	AddrTransNet	CoreDev_Serv Build_Server spswitch sprouter	UDP RDP TCP FM_GUI_Access	Accept	Log	Req from Steve D . - test 23;Req from Jody B. - test 902;Req from Matt D. - test late

Section 1.3.4 - (Fail)

Verify that internal addresses cannot pass from the Internet into the DMZ.

Unable to generate this report

Section 1.3.5 - (Fail)

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

Summary

9 services that are not defined as allowed are permitted from the External zone to the PCI zone.

Recommendations

No direct traffic should be permitted from the PCI zone to any zone other than the DMZ. To meet this requirement, you should permit traffic from the PCI zone to only the DMZ.

Details

Evaluated

All rules that allow traffic from External to PCI.

Allowed Services (1)

The PCI service group includes PCI.

Disallowed Services (9)

The following services are not explicitly allowed, services include AOL, AOL_Messenger, Citrix_ICA, Citrix_ICA_Browsing, Citrix_metaFrame, ESP, ICQ_locator, domain-tcp, tcp_service_test.

Section 1.3.6 - (Pass)

Verify that the firewall performs stateful inspection (dynamic packet filtering). [Only established connections should be allowed in, and only if they are associated with a previously established session (run a port scanner on all TCP ports with "syn reset" or "syn ack" bits set - a response means packets are allowed through even if they are not part of a previously established session).]

Summary

Stateful inspection is enabled on the firewall.

Recommendations

Stateful inspection, or dynamic packet filtering, is a firewall architecture that tracks the network connections travelling across the firewall and inspects the communication packets down to the application layer. To ensure ongoing compliance with this requirement, continue to maintain stateful inspection on the firewall.

Details

Stateful Packet Inspection is enabled.

Section 1.3.7 - (Pass)

Verify that the database is on an internal network

Summary

All of the services permitted by the firewall from the DMZ zone to the PCI zone are allowed.

Recommendations

To ensure ongoing compliance with this requirement, continue to segregate the database from the DMZ.

Details

Evaluated

All rules that allow traffic from DMZ to PCI.

Allowed Services (1)

The Database Services service group includes Database Services.

Disallowed Services (0)

The following services are not explicitly allowed, services include no services.

2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.

Section 2.2.2 - (Fail)

For a sample of system components, inspect enabled system services, daemons, and protocols. Verify that unnecessary or insecure services or protocols are not enabled, or are justified and documented as to appropriate use of the service. For example, FTP is not used, or is encrypted via SSH or other technology.

Summary

9 services that are not defined as allowed are permitted from the * zone to the PCI zone.

Recommendations

Component management should be restricted to those services that are encrypted or justified. To meet this requirement, please review the list of allowed services as well as a list of services not allowed. Be sure to fully document the justification for each allowed service.

Details

Evaluated

All rules that allow traffic from * to PCI.

Allowed Services (1)

The PCI service group includes PCI.

Disallowed Services (9)

The following services are not explicitly allowed, services include AOL, AOL_Messenger, Citrix_ICA, Citrix_ICA_Browsing, Citrix_metaFrame, ESP, ICQ_locator, domain-tcp, tcp_service_test.

Policy: SPLAT-Policy

Security Rule							^Top
Rule	Name	Source	Destination	Service	Action	Log	Comments
33		* Any	mdean_group AddrTransHostHideIP	TCP domain-tcp	Accept	- None	CCM#670
38		F-199.158.104 .0-21-Renamed	L-FSAKC-165.221.017.0	Citrix_meta Frame AOL_Messenger	Accept	Log	Insert new rule
45	jira 373 take 23	temp-group@ BackEnd_Net	AddrTransNet this_is_a_really_long_host _name_to_test_TT1457	TCP tcp_service_test	Authenticate	Log	CCN: DEV -563 another test

Section 2.3.0 - (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.

Summary

9 services that are not defined as allowed are permitted from the External zone to the PCI zone.

Recommendations

Management console access should be restricted to those services that are encrypted or justified. To meet this requirement, please review the list of allowed services as well as a list of services not allowed. Be sure to fully document the justification for each allowed service.

Details

Evaluated

All rules that allow traffic from External to PCI.

Allowed Services (1)

The PCI service group includes PCI.

Disallowed Services (9)

The following services are not explicitly allowed, services include AOL, AOL_Messenger, Citrix_ICA, Citrix_ICA_Browsing, Citrix_metaFrame, ESP, ICQ_locator, domain-tcp, tcp_service_test.

Policy: SPLAT-Policy

Security Rule							^Top
Rule	Name	Source	Destination	Service	Action	Log	Comments
33		* Any	mdean_group AddrTransHostHideIP	TCP domain-tcp	Accept	- None	CCM#670
38		F-199.158.104 .0-21-Renamed	L-FSAKC-165.221.017.0	Citrix_meta Frame AOL_Messenger	Accept	Log	Insert new rule
45	jira 373 take 23	temp-group@ BackEnd_Net	AddrTransNet this_is_a_really_long_host _name_to_test_TT1457	TCP tcp_service_test	Authenticate	Log	CCN: DEV -563 another test

6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release.

Section 6.1.0 - (Fail)

Verify all system components and software have latest vendor-supplied security patches installed.

Summary

The device is missing the " file.

Recommendations

Check the setup of the device in FireMon, or contact technical support.

Details

The device is not currently supported.

