FortiScan v5.0 MR1

PCI DSS Jump Start

FortiScan v5.0 MR1 PCI DSS Jump Start

September 26, 2013

17-511-219078-20130926

Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Technical Documentation	http://docs.fortinet.com
Knowledge Base	http://kb.fortinet.com
Forums	https://support.fortinet.com/forum
Customer Service & Support	https://support.fortinet.com
Training Services	http://training.fortinet.com
FortiGuard Threat Research & Response	http://www.fortiguard.com
Document Feedback	Email: techdocs@fortinet.com

eCommerce thrives because customers trust that vendors will keep their financial data safe. Points of sale (POS) have become increasingly intelligent and mobile.

If you are required to comply with PCI DSS standards for credit card data, and you manage many POS, a data center, or a colocation center that must be compliant, FortiScan can help.

Simply follow the instructions here, from start to finish!

PCI DSS requirements

Payment Card Industry Data Security Standard (PCI DSS), defined by the PCI Security Standards Council, is a set of data security requirements to which banks, online merchants, and Member Service Providers (MSPs) must adhere, enforcing the safe handling of card holder information.

To comply with the requirements, merchants and MSPs must:

- Annually conduct an on-site audit or complete the PCI Self-Assessment Questionnaire.
- Quarterly conduct vulnerability scans on all Internet-facing networks and systems. These scans must be performed by an approved scanning vendor. Vulnerability scans detect security threats associated with electronic commerce, and provide the bank, merchant, or MSP with a report demonstrating compliance status. Threats must be remediated.

To meet the second requirement, FortiScan can generate PCI technical and executive compliance reports that shows the pass or failure status for each host on your network.

Download FortiScan

You might already have a physical FortiScan appliance.

But if you need the flexibility and resilience of a virtual machine, or if you are not ready to commit to a physical appliance, you can download a 64-bit virtual machine version of FortiScan, called FortiScan VM:

http://www.fortinet.com/resource_center/product_downloads.html

You can try FortiScan VM for 15 days, worry-free. Stackable vCPU expansion licenses are available to grow with you.

Be sure to enable 64-bit addressing and hardware-assisted virtualization technology (VT) in your BIOS, map the vNICs, and size your vCPU and storage repository before powering on FortiScan-VM. Details are in the *FortiScan VM Install Guide*.

Once you have a virtual or physical FortiScan, you are ready to begin.

Prepare your hosts to be scanned

Adjust your network topology and settings so that the PCI scan can reach its targets.

Hosts must be:

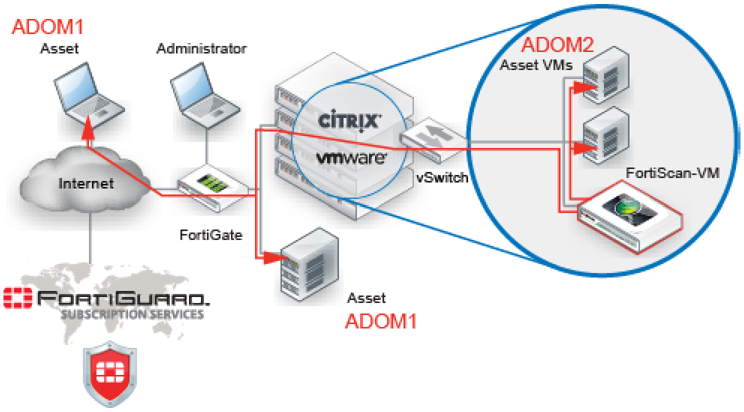
- Powered on
- Running their usual services
- Have a static IP address / permanent DHCP reservation

To reduce the time required to discover live hosts, hosts should also be responsive to ARP or ICMP `ECHO_REQUEST` (ping) from FortiScan's IP address.

FortiScan should be placed on:

- The Internet
- With POS and other clients on your private network and any other network whose hosts access the computer whose PCI DSS compliance you are testing.

Figure 1: FortiScan architecture



Adjust firewall policies, add VPN, add virtual IPs, and/or configure port forwarding if necessary for the scan to reach the target computer. But keep in mind that if you modify security policies for the scan to reach the target, some vulnerabilities and non-compliances might be false positives.

Define your domains

First, define at least one administrative domain (ADOM). If you are an MSSP, you may want to define a few: one for each customer, or one for each division of a large enterprise.

ADOMs:

- ***Restrict*** your compliance scans to your domain
- ***Define*** which assets each FortiScan administrator can see and/or govern
- ***Distinguish*** computers on different parts of your network that use the same IP address

If you do not want to put computers with identical IP addresses into separate ADOMs, you can achieve a similar affect via a VPN.

Connect your FortiScan to a FortiGate. Next, establish a VPN between the FortiGate and the ADOM's computers. Finally, add each computer's remote IP from the VPN (not their identical ones) to the ADOM.

To define an ADOM:

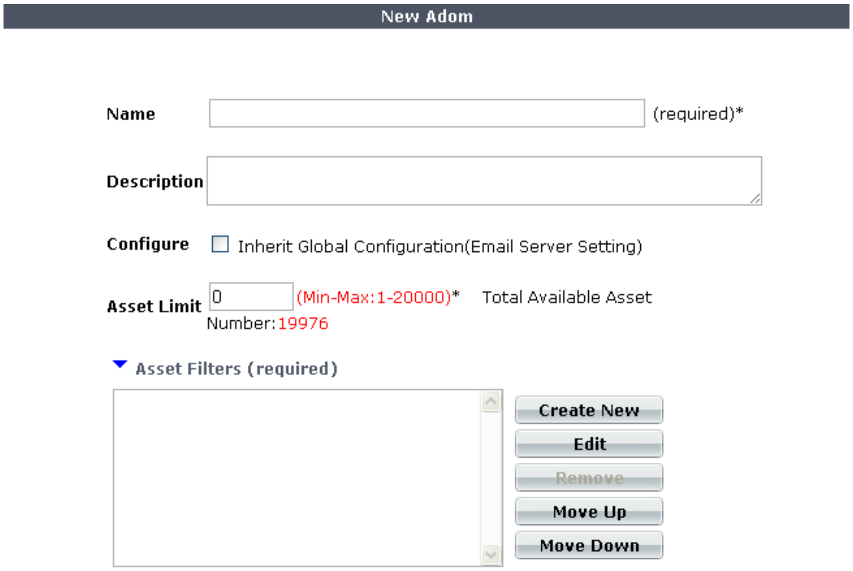
1. Connect to FortiScan's web UI. If you are connecting directly to port1 and using its default IP address, the URL is https://192.168.1.1/.
2. Log in to the web UI as `admin`.

   Other FortiScan administrator accounts cannot create new ADOMs.
3. From *Current ADOM*, select *Global*.

   Other ADOMs cannot configure new ADOMs.
4. Go to *System* > *ADOM* > *ADOM*.
5. Select *Create New*.

   The *New ADOM* window opens.

Figure 2: New ADOM window



New Adom

Name (required)*

Description

Configure □ Inherit Global Configuration(Email Server Setting)

Asset Limit 0 (Min-Max:1-20000)* Total Available Asset Number:19976

Asset Filters (required)

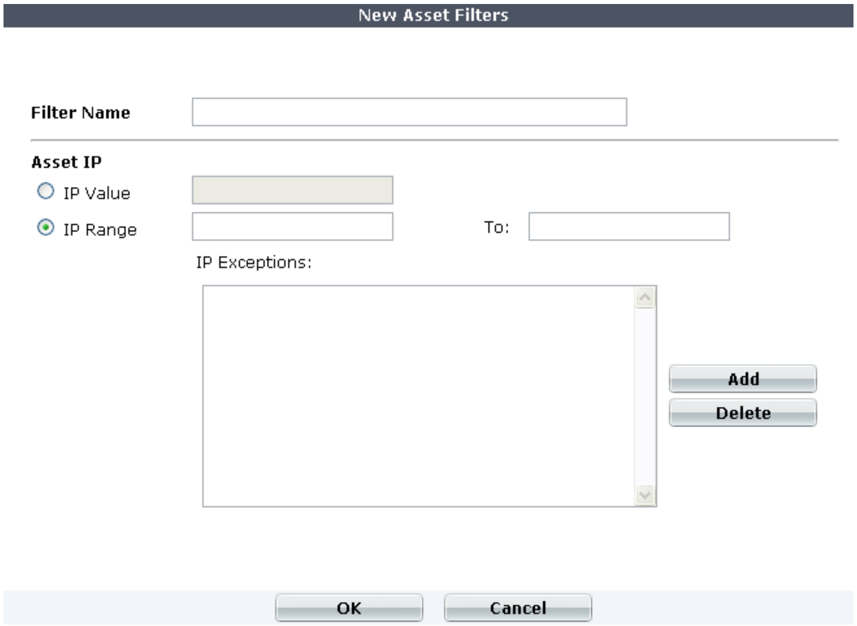
6. Configure the following settings:

Name	Type a unique name for the administrative domain, such as `www.example.com`. The name cannot be longer than 11 characters, and cannot contain special characters, except underscores (_), hyphens (-), periods (.), and “at” symbols (@).
Asset Limit	Type the maximum number of assets that can belong to this ADOM. The total number of assets that can be supported by a FortiScan appliance varies by model. To prevent an ADOM from consuming this hardware limit and starving other ADOMs for resources, restrict the ADOM to a proportionate amount of the total. For details on the limits of each model, see the *FortiScan Administration Guide*.

7. Next to the *Asset Filters* area, select *Create New*.

   A dialog should appear where you can define the IP address space that belongs to the ADOM. The *New Asset Filters* window opens.

Figure 3: New asset filters window



New Asset Filters

Filter Name

Asset IP

○ IP Value

● IP Range　To:

IP Exceptions:

8. Configure the following settings:

Filter Name	Type a unique name for the asset filter, such as `server_farm1` or `pos1`.
Asset IP	Define the IP address space that belongs to the ADOM. Select either: • **IP Value:** In the text field to the right of this option, type an IP address that you want to include in the ADOM. • **IP Range:** In the two text fields to the right of this option, type the first and last IP addresses in a range of IP addresses that you want to include in the ADOM. If you need to exclude one or more of the IP addresses from the IP range, select *Add* to configure *IP Exceptions*. **Note:** Computers do not need to be present at every IP address in the range. Live computers in this space will be detected later, during a discovery scan.

9. Select *OK* to return to the New ADOM window.
10. Repeat the previous two steps for each set of IP addresses that you want to include in the ADOM.
11. Select the *Move Up* or *Move Down* buttons to change the order of IP address sets.

    Entries are evaluated for a match from top to bottom. Position filter entries so that the first matching entry matching will include or exclude the IP address from the ADOM, whichever you intend.
12. Select *OK*.

    The new ADOM is added to the list on *System* > *ADOM* > *ADOM*, and the drop-down list in *Current ADOM*. Administrator accounts can now be assigned to the new ADOM.

Discover your domain's live targets

What if some IP addresses in your domain are unused? You don't want to waste time scanning for computers that aren't there.

To determine live IP addresses, run a discovery scan. This adds a list of your computers to your ADOM's asset inventory.

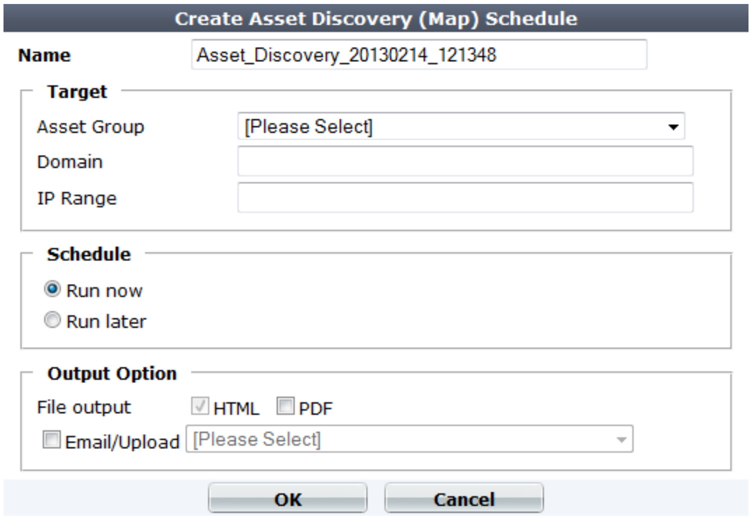
To schedule a discovery scan

1. From *Current ADOM*, select an ADOM that is not *Global*.

   The discovery scan will add new assets to that specific ADOM's asset inventory.
2. Go to *Asset* > *Discovery* > *Schedule*.
3. Select *Create New*.

   The *Create Asset Discovery (Map) Schedule* window opens.

Figure 4: Create asset discovery (map) schedule window



Create Asset Discovery (Map) Schedule

Name: Asset_Discovery_20130214_121348

Target

- Asset Group: [Please Select]
- Domain:
- IP Range:

Schedule

- ● Run now
- ○ Run later

Output Option

- File output: ☑ HTML □ PDF
- □ Email/Upload: [Please Select]

4. Configure the following settings:

Name	The name of the profile.
Target	
IP Range	Enter an IP range that will be the network scan target. The IP range must be within the same subnet. The FortiScan appliance will attempt to contact live hosts. Reported host numbers may vary at different scan times if some hosts, such as laptops, are sometimes unreachable.
Schedule	Select when to start the network scan, either: • **Run Now:** Generate a report when the profile is saved, and any time that you select *Run Now* for this profile in the list of scan profiles. No scheduled reports will be generated. • **Run Later**: Generate a report at scheduled intervals. You must configure the *Start Date* and *Time*, and select the recurrence pattern (either *Daily*, *Weekly*, or *Monthly*). Also configure the schedule expiration date.

5. Select *OK*.

When a scheduled network discovery scan job completes, discovered hosts are automatically imported into *Asset* > *Inventory* > *Asset Inventory*, where they appear in the *All Assets* and the *Unprotected* asset groups.

The name *Unprotected* indicates only that they do not have a FortiScan agent installed. This is okay if you only require quarterly PCI DSS compliance checks.

If you want continuous monitoring or patch and configuration deployment that an agent-based solution can provide, see the *FortiScan Administration Guide*.

Group hosts to be scanned

Do you want to scan all of your computers at once, or do you want to scan them in batches. If you do not want to scan them all at once, group your hosts into sets.

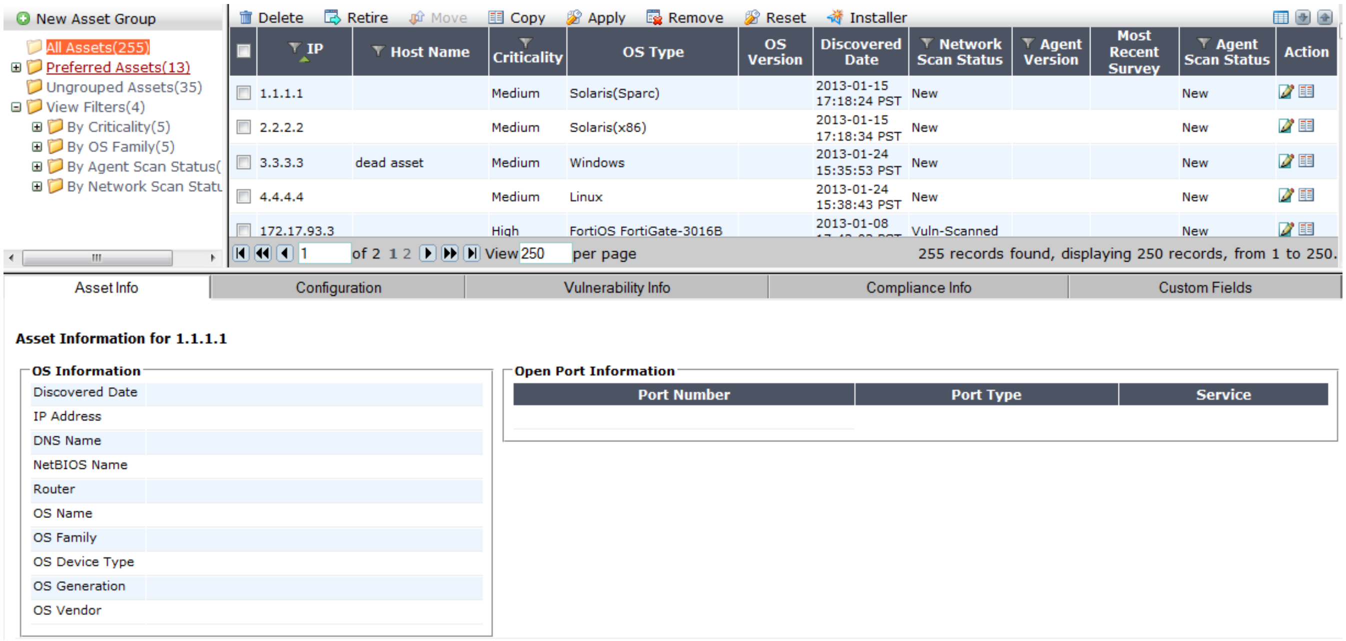
To create an asset group:

1. From *Current ADOM*, select an ADOM that is not *Global*.

   (Assets belong to specific ADOMs.)

2. Go to *Asset* > *Inventory* > *Asset Inventory*.

Figure 5: Asset inventory page



□	IP	Host Name	Criticality	OS Type	OS Version	Discovered Date	Network Scan Status	Agent Version	Most Recent Survey	Agent Scan Status	Action
□	1.1.1.1		Medium	Solaris(Sparc)		2013-01-15 17:18:24 PST	New			New	
□	2.2.2.2		Medium	Solaris(x86)		2013-01-15 17:18:34 PST	New			New	
□	3.3.3.3	dead asset	Medium	Windows		2013-01-24 15:35:53 PST	New			New	
□	4.4.4.4		Medium	Linux		2013-01-24 15:38:43 PST	New			New	
□	172.17.93.3		High	FortiOS FortiGate-3016B		2013-01-08	Vuln-Scanned			New	

1 of 2 1 2 View 250 per page 255 records found, displaying 250 records, from 1 to 250.

Asset Information for 1.1.1.1

OS Information

- Discovered Date
- IP Address
- DNS Name
- NetBIOS Name
- Router
- OS Name
- OS Family
- OS Device Type
- OS Generation
- OS Vendor

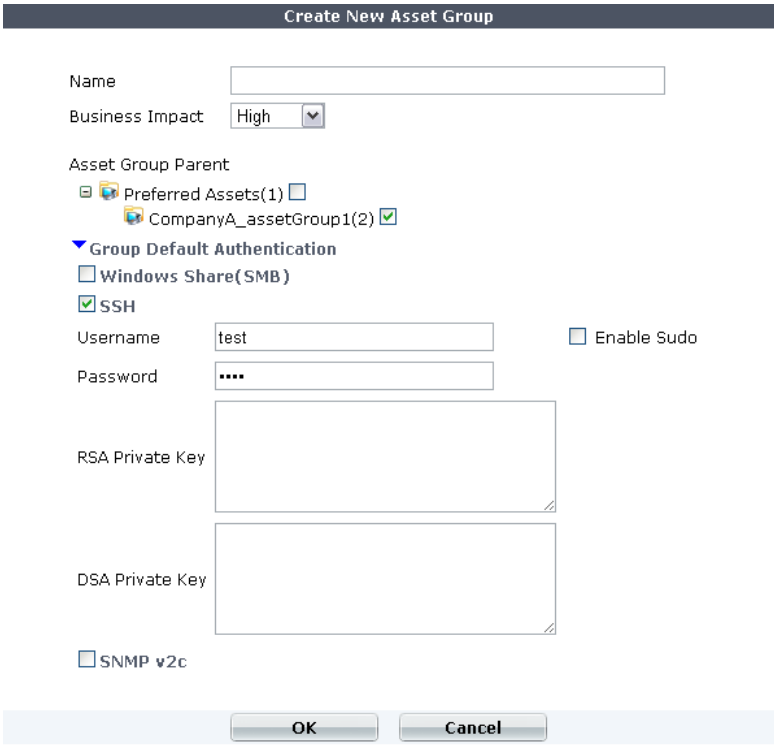
Open Port Information

Port Number	Port Type	Service

3. In the asset selection tree, select the *New Asset Group* button.

   The *Create New Asset Group* window opens.

Figure 6: Create new asset group window



Create New Asset Group

Name

Business Impact: High

Asset Group Parent

⊟ Preferred Assets(1) □

CompanyA_assetGroup1(2) ☑

Group Default Authentication

□ Windows Share(SMB)

☑ SSH

Username: test

□ Enable Sudo

Password: ••••

RSA Private Key

DSA Private Key

□ SNMP v2c

4. Configure the following settings:

Name	Enter the name for the new asset group
Asset Group Parent	Select the parent group in which to include the new asset group. To create a top level group, select the *Preferred Assets* group as the parent. **Note:** Asset groups that are automatically created by the FortiScan appliance, such as *All Assets*, cannot be a group parent.

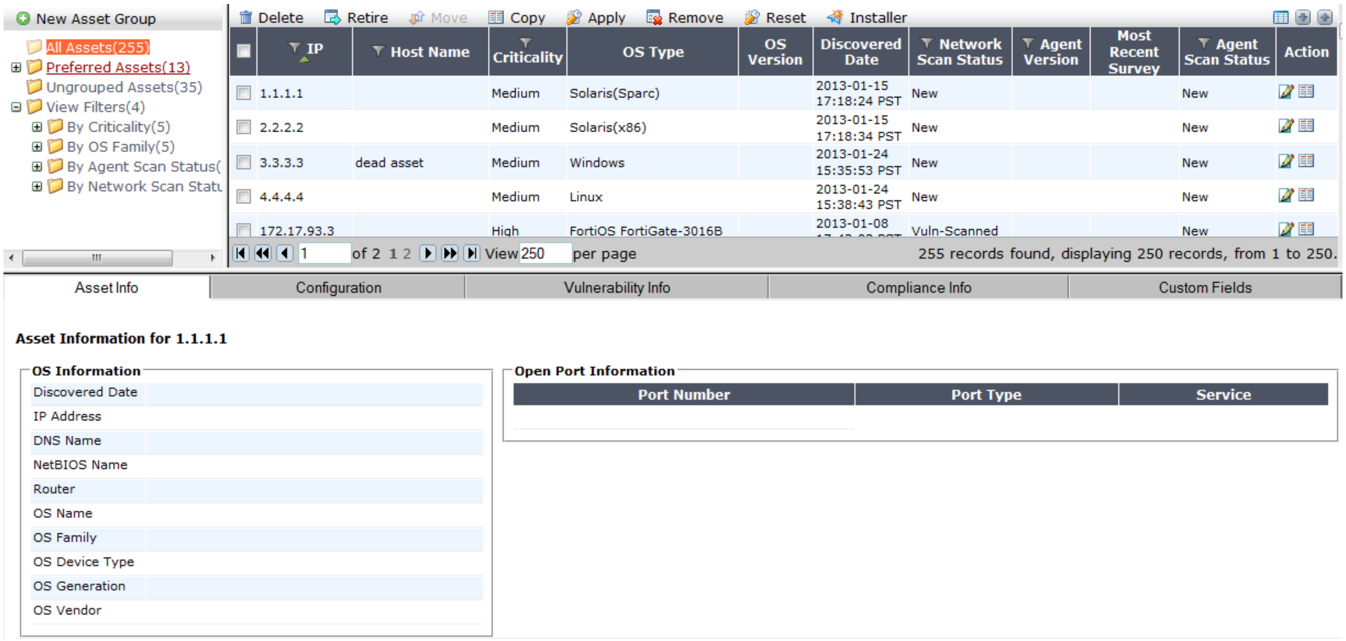
5. Select *OK*.

   The empty new group appears in the asset selection tree under its parent group. Continue by adding assets to the group. (See "To add an asset to an asset group".)

To add an asset to an asset group

1. From *Current ADOM*, select an ADOM that is not *Global*.
2. Go to *Asset* > *Inventory* > *Asset Inventory*.

Figure 7: Asset inventory page



☐	IP	Host Name	Criticality	OS Type	OS Version	Discovered Date	Network Scan Status	Agent Version	Most Recent Survey	Agent Scan Status	Action
☐	1.1.1.1		Medium	Solaris(Sparc)		2013-01-15 17:18:24 PST	New			New	
☐	2.2.2.2		Medium	Solaris(x86)		2013-01-15 17:18:34 PST	New			New	
☐	3.3.3.3	dead asset	Medium	Windows		2013-01-24 15:35:53 PST	New			New	
☐	4.4.4.4		Medium	Linux		2013-01-24 15:38:43 PST	New			New	
☐	172.17.93.3		High	FortiOS FortiGate-3016B		2013-01-08	Vuln-Scanned			New	

1 of 2 1 2 View 250 per page 255 records found, displaying 250 records, from 1 to 250.

Asset Information for 1.1.1.1

OS Information

Discovered Date	
IP Address	
DNS Name	
NetBIOS Name	
Router	
OS Name	
OS Family	
OS Device Type	
OS Generation	
OS Vendor	

Open Port Information

Port Number	Port Type	Service

3. In the asset selection tree, select *All Assets*, *Ungrouped Assets*, or another group that already contains the asset.

   The contents of the group appear in the asset inventory pane, in the top right quadrant.

4. In the asset inventory window, either:

   - Add a single asset, in the row of the asset that you want to add, select the *Copy* icon.
   - Add multiple assets, mark the check boxes for each asset that you want to add, then on the toolbar, select *Copy*.

   The *Copy Asset* dialog appears in the asset editor pane.

5. In the dialog's *Asset Group Parent* tree, select the group to which you want to add the asset(s), and then select *OK*.

Schedule your PCI DSS scan

FortiScan can generate PCI reports according to whatever schedule you specify. You do not need to manually initiate them.

Time required to complete a remote vulnerability scan varies by:

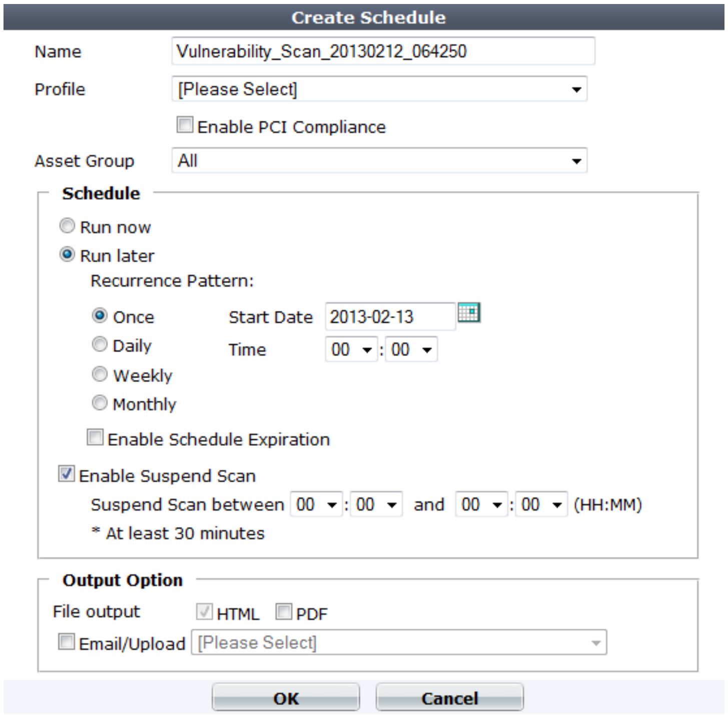
- The number of target hosts
- The number of ports that you are scanning on each host
- Whether the host responds quickly on those ports

For example, for a very comprehensive scan of many hosts that are not always responsive, the scan could take a couple of days to complete. For best results, wait for previous remote vulnerability scans to complete, and do not schedule scans concurrently.

1. Go to *Network Scan > Vulnerability Scan > Schedule*.
2. Select *Create New*.

   The *Create Schedule* dialog box opens.

Figure 8: Create schedule dialog box



Create Schedule

Name: Vulnerability_Scan_20130212_064250

Profile: [Please Select]

□ Enable PCI Compliance

Asset Group: All

Schedule

○ Run now

● Run later

Recurrence Pattern:

● Once — Start Date: 2013-02-13 — Time: 00 : 00

○ Daily

○ Weekly

○ Monthly

□ Enable Schedule Expiration

☑ Enable Suspend Scan

Suspend Scan between 00 : 00 and 00 : 00 (HH:MM)

* At least 30 minutes

Output Option

File output: ☑ HTML □ PDF

□ Email/Upload: [Please Select]

3. Configure the following settings:

Name	Type a name for the vulnerability scan report.
Enable PCI Compliance	Enable to use the pre-defined PCI DSS compliance scan profile. Enabling this option automatically selects the predefined PCI DSS scan profile (*vcm_pci_profile*) the *Profile* drop-down list. *Profile* then becomes read-only. Predefined scan profiles such as *vcm_pci_profile* are included with the firmware, and are updated by FortiGuard Vulnerability and Compliance Management service if you have subscribed.
Asset Group	Select which asset group to scan (see "Group hosts to be scanned" on page 9).
Schedule	Select either: • **Run Now:** Select to specify an on-demand scan and report. A scan will run and a report will be generated immediately after the schedule is saved, and also whenever the *Run Now* icon is manually selected thereafter. (Reports will not be automatically periodically generated.) This is the default. • **Run Later**: Select to have scan reports automatically generated at regular intervals and configure the times and dates of the recurring schedule. Also configure the schedule expiration date.

Output Option	
File output	Mark the check boxes of the PCI DSS report file formats that you want. HTML is the format available as part of the Web-based Manager, and cannot be disabled.
Email/Upload	To have the report delivered to an e-mail address or FTP server, enable this option and enter the appropriate information.

4. Select *OK*.

   FortiScan will begin the scan now if you configured that. Otherwise, it will begin at the scheduled time. When the scan is complete, results will appear in *Network Scan* > *Vulnerability Scan* > *Report*. FortiScan can generate two compliance reports, a *PCI Executive Report* and a *PCI Technical Report*, based on severity levels predefined by Fortinet.

Generate your PCI DSS reports

Compliance report templates are pre-defined report formats designed to conform to PCI DSS requirements. If you subscribe to the FortiGuard Vulnerability and Compliance Management service, predefined templates are automatically updated.

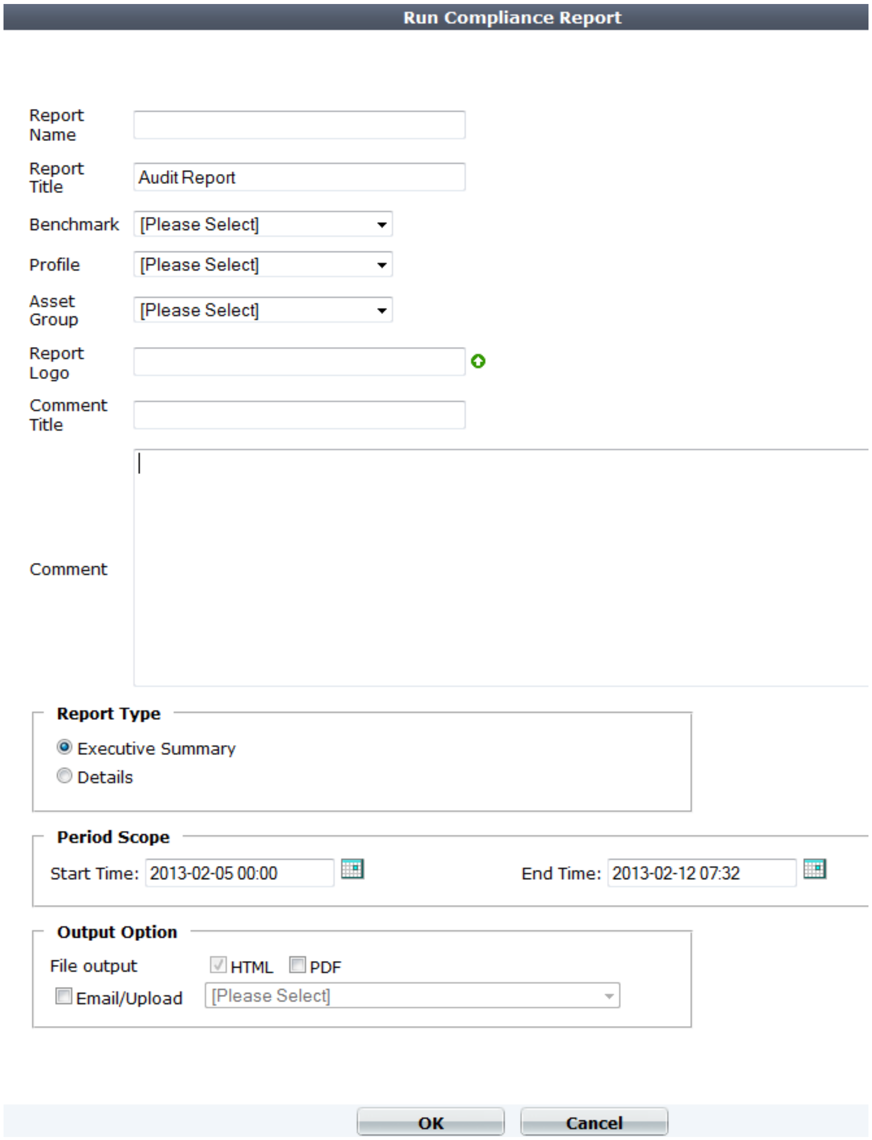
After your scan has completed, FortiScan has the data that it needs to be able to generate your report.

To generate a PCI DSS compliance report

1. From *Current ADOM*, select the name of an ADOM that is not *Global*.
2. Go to *Report* > *Network Scan* > *Compliance Report* > *Template*.
3. In the row corresponding to the report that you want to generate, mark its check box, then select *Run now*.

   The *Run Compliance Report* page opens.

Figure 9: Run compliance report page



Run Compliance Report

Report Name	
Report Title	Audit Report
Benchmark	[Please Select]
Profile	[Please Select]
Asset Group	[Please Select]
Report Logo	
Comment Title	
Comment	

Report Type

● Executive Summary
○ Details

Period Scope

Start Time: 2013-02-05 00:00 End Time: 2013-02-12 07:32

Output Option

File output ☑ HTML ☐ PDF
☐ Email/Upload [Please Select]

4. Configure the following settings:

Report Name	Enter the report name the FortiScan appliance will display in the compliance report list. The date and time will be appended to the end of the name each time a compliance report is generated.
Report Title	Enter a title that will appear in the report. This field is automatically populated depending on the type of template you choose.
Benchmark	Select a benchmark.
Profile	Select a scan profile.
Asset Group	Select an asset group. The compliance report results will be limited to the hosts defined in the specified asset group.
Report Logo	Upload a logo for the report.

Comment Title	Enter a title for any comments you have for the report.
Comment	Enter the comment content.
Report Type	Select the type of report. If you select *Details*, choose the rules to be reported and report columns of rules.
Period Scope	Select a start and end time. The compliance report results will be limited to the time period you specify.
Output Option	
File Output	Select the formats in which the report will be generated. HTML is the default format. Any or all other available formats may be selected.
Email/ Upload	To have the report delivered to an e-mail address or FTP server, select this option and select the output template or create a new one.

5. Select *OK*.

   The list of report templates appears again. To determine whether the report is in progress or complete, refresh the page and update the *Status* column by selecting the *Template* submenu. The scan is complete when the *Status* column is blank.

Use your PCI DSS reports

Once you have generated your PCI DSS reports, review them for non-compliances.

To view the list of non-compliant hosts

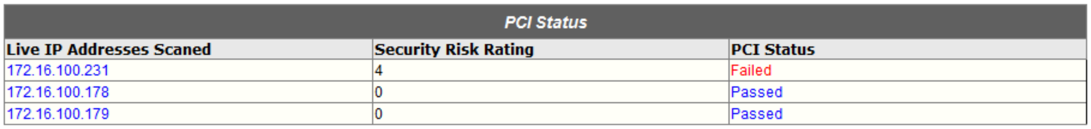
1. From *Current ADOM*, select the name of an ADOM that is ***not*** *Global*.

   (This is the ADOM whose report you will be viewing.)

2. Go to *Network Scan* > *Compliance Report* > *Report*.
3. Select the report's name to view the HTML version of the report. (If you generated the report in any additional file formats, you can select the link in the *Format* column to view one of those formats.)
4. In the *PCI Status* section, if any host's *Last Scan* is *Failed*, correct that computer to be compliant.

   Figure 10:{PCI status

   PCI Status



PCI Status

Live IP Addresses Scaned	Security Risk Rating	PCI Status
172.16.100.231	4	Failed
172.16.100.178	0	Passed
172.16.100.179	0	Passed

5. This page displays the following information:

Report Summary	
Created	The date and time network map report was generated.
Total Hosts	The IP addresses or IP range of the computers that were live and responding during the scan.

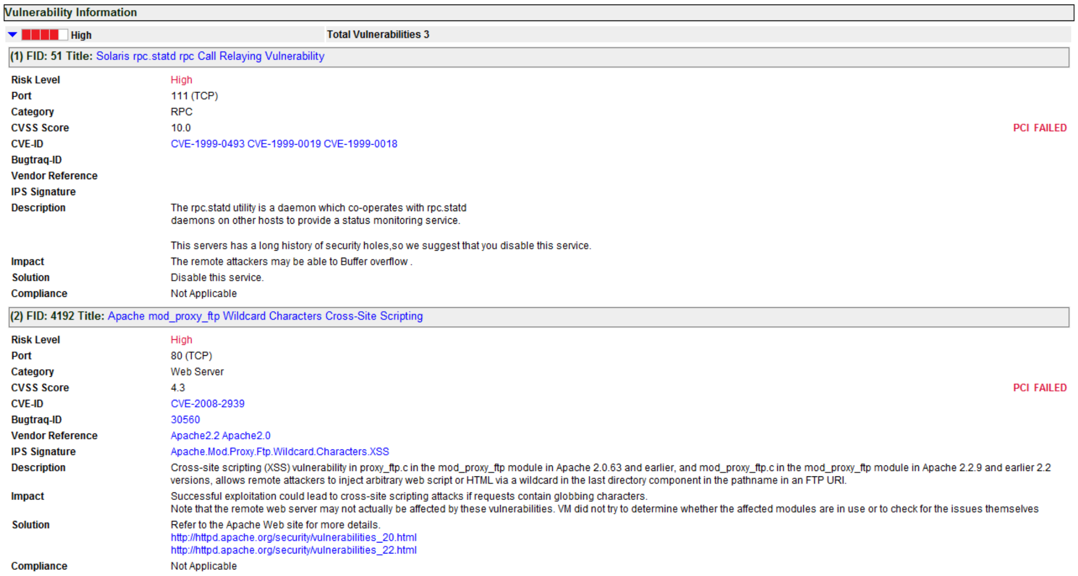
Summary From Date	The starting date and time of the report data.
Summary To Date	The ending date and time of the report data.
VM Engine Version	The FortiGuard Vulnerability and Compliance Management engine version number and date of last update. This is updated via the FortiGuard Distribution Network if you are a FortiGuard Vulnerability Management service subscriber.
VM Plugins Version	The FortiGuard Vulnerability and Compliance Management module version number and date of last update. This is updated via the FortiGuard Distribution Network if you are a FortiGuard Vulnerability and Compliance Management service subscriber.
PCI Status	
IP Addresses	The IP address of the host scanned.
Failed Times	The number of times the host failed the PCI compliance scan.
Passed Times	The number of times the host passed the PCI compliance scan.
PCI Disabled	The number of times the host was scanned with the PCI option disabled in the scan schedule.
Total Scanned Times	The total number of scans on the host.
Last Scan	The PCI DSS compliance status of the host according to the latest scan. • **Passed:** No vulnerabilities or potential vulnerabilities, as defined by the PCI Security Standards Council's PCI DSS compliance standards, were detected on the host. If there are any security vulnerabilities that are not violations, you should still address them, usually in order of severity. • **Failed:** At least one PCI DSS violation was detected on the host. All actual or potential vulnerabilties with this status must be remediated in order to be compliant.
Host Details	The top 10 vulnerable hosts by vulnerabilities and by times.
Vulnerability Detail	The total number of vulnerabilities detected are presented by severity, category, and date. The top 20 vulnerabilities are also listed.
Host	All services and vulnerabilities found for each host. The vulnerabilities that cause the host to fail compliance are highlighted. This section is omitted from PCI Executive Reports.
Appendix	Information about the Payment Card Industry (PCI) status and vulnerability levels.

To resolve a host's non-compliance:

1. In the *Hosts* section of the report, select the blue disclosure arrow next to the host's IP address. This will reveal a list of vulnerability scans of that host.

2. Select the blue arrow next to a vulnerability scan date to reveal the list of discovered problems.
3. After the list of open ports, severity level and category summary, and OS fingerprint, in the *Vulnerability Information* subsection, select the blue arrow next to each severity level (*High*, *Medium*, *Low*, or *Information*) to expand the list of vulnerabilities at each level.
4. Resolve each problem by doing one of the suggested solutions for each vulnerability.

Figure 11: Vulnerability information page



Vulnerability Information

▼ 🟥🟥🟥🟥 High — Total Vulnerabilities 3

(1) FID: 51 Title: Solaris rpc.statd rpc Call Relaying Vulnerability

Risk Level	High	
Port	111 (TCP)	
Category	RPC	
CVSS Score	10.0	PCI FAILED
CVE-ID	CVE-1999-0493 CVE-1999-0019 CVE-1999-0018	
Bugtraq-ID		
Vendor Reference		
IPS Signature		
Description	The rpc.statd utility is a daemon which co-operates with rpc.statd daemons on other hosts to provide a status monitoring service. This servers has a long history of security holes,so we suggest that you disable this service.	
Impact	The remote attackers may be able to Buffer overflow .	
Solution	Disable this service.	
Compliance	Not Applicable	

(2) FID: 4192 Title: Apache mod_proxy_ftp Wildcard Characters Cross-Site Scripting

Risk Level	High	
Port	80 (TCP)	
Category	Web Server	
CVSS Score	4.3	PCI FAILED
CVE-ID	CVE-2008-2939	
Bugtraq-ID	30560	
Vendor Reference	Apache2.2 Apache2.0	
IPS Signature	Apache.Mod.Proxy.Ftp.Wildcard.Characters.XSS	
Description	Cross-site scripting (XSS) vulnerability in proxy_ftp.c in the mod_proxy_ftp module in Apache 2.0.63 and earlier, and mod_proxy_ftp.c in the mod_proxy_ftp module in Apache 2.2.9 and earlier 2.2 versions, allows remote attackers to inject arbitrary web script or HTML via a wildcard in the last directory component in the pathname in an FTP URI.	
Impact	Successful exploitation could lead to cross-site scripting attacks if requests contain globbing characters. Note that the remote web server may not actually be affected by these vulnerabilities. VM did not try to determine whether the affected modules are in use or to check for the issues themselves	
Solution	Refer to the Apache Web site for more details. http://httpd.apache.org/security/vulnerabilities_20.html http://httpd.apache.org/security/vulnerabilities_22.html	
Compliance	Not Applicable	

FortiScan can automatically fix many of the vulnerabilities it can detect, significantly shortening your response time. For details, see the *FortiScan Administration Guide*.

Your compliance "to do" list

Your PCI DSS reports contain the information that you need to resolve issues to bring your organization into compliance.

What if you want to divide the work among multiple people?

FortiScan can automatically assign tickets and track completion of your compliance work. It can even resolve some issues automatically. For details, see the *FortiScan Administration Guide*.