# FortiOS 6.4 and FortiGate NGFW Appliances

## NDcPP Common Criteria Logging Addendum

**FORTINET DOCUMENT LIBRARY**

https://docs.fortinet.com

**FORTINET VIDEO GUIDE**

https://video.fortinet.com

**FORTINET KNOWLEDGE BASE**

http://kb.fortinet.com

**FORTINET BLOG**

https://blog.fortinet.com

**CUSTOMER SERVICE & SUPPORT**

https://www.fortinet.com/support/contact.html

**FORTINET NSE INSTITUTE (TRAINING)**

https://training.fortinet.com/

**FORTIGUARD CENTER**

https://fortiguard.com

**FORTICAST**

http://forticast.fortinet.com

**END USER LICENSE AGREEMENT AND PRIVACY POLICY**

https://www.fortinet.com/doc/legal/EULA.pdf

https://www.fortinet.com/corporate/about-us/privacy.html

**FEEDBACK**

Email: techdoc@fortinet.com

Monday, February 27, 2023

NDcPP Logging Addendum for FortiOS 6.4 and FortiGate NGFW Appliances

01-649-887811-20230227

# TABLE OF CONTENTS

**Introduction** ..... **4**
References ..... 4
**Log Message Examples** ..... **5**

# Introduction

Fortinet performs FIPS 140-2 and NDcPP Common Criteria certifications on specific FortiOS versions in combination with specific FortiGate family hardware models. At the publication date of this document, the latest NDcPP CC certified version of FortiOS is 6.4.

The documentation set for FortiGate units operated in FIPS-CC mode consists of this document and the standard FortiOS 6.4 documentation set. This document provides examples of NDcPP Common Criteria specific log messages. The standard documentation is available from the Fortinet Technical Documentation web site (http://docs.fortinet.com).

For detailed information on the FortiOS 6.4 NDcPP Common Criteria certification, including the certified hardware models, refer to the FortiOS 6.4 NDcPP Security Target. The Security Target can be found on the Fortinet Support web site in the FortiOS 6.4 FIPS-CC certified firmware download directory (http://support.fortinet.com).

## References

| |
|---|
| Security Target: FortiGate/FortiOS 6.4 |
| FortiOS 6.4 and FortiGate NGFW Appliances FIPS 140-2 and NDcPP Common Criteria Technote |
| FortiOS 6.4.9 Administration Guide |
| FortiOS 6.4.9 CLI Reference |
| FortiOS 6.4.9 Log Message Reference |
| Model specific Hardware Information Supplements |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| FAU_GEN.1[1] | Start-up of the audit functions | None. | date=2023-02-22 time=12:21:59 logver=604099148 timestamp=1677086519 devname="FortiGate-61F" devid="FGT61FTK19006185" vd="root" itime=1677086519 logver=0604099148 time=17:47:57 eventtime=1677086519324798321 tz="-0800" logid="0100032009" type="event" subtype="system" level="information" logdesc="FortiGate started" msg="FortiGate started in FIPS-CC mode" |
| | Shut-down of the audit functions | None. | logver=604099148 timestamp=1676769063 devname="FortiGate-61F" devid="FGT61FTK19007193" vd="root" date=2023-02-19 time=01:11:03 eventtime=1676769063324798321 tz="-0800" logid="0100032138" type="event" subtype="system" level="critical" logdesc="Device rebooted" user="admin" ui="console" action="reboot" msg="User admin rebooted the device from console." |
| | Administrative login | Name of user account shall be logged if individual user accounts are required for administrators | *Please refer to FIA_UIA_EXT.1.* |
| | Administrative logout | Name of user account shall be logged if individual user accounts are required for administrators | *Please refer to FTA_SSL.4.* |
| | Changes to TSF data related to configuration changes | In addition to the information that a change occurred it shall be logged what has been changed. | *Configuring the log disk settings:*<br><br>logver=604099148 timestamp=1676819648 devname="FortiGate-61F" devid="FGT61FTK20001997" vd="root" date=2023-02-19 time=15:14:08 eventtime=1676819648324798321 tz="-0800" logid="0100044546" type="event" |

[1] While Table 2 in the NDcPP claims “None” for FAU_GEN.1, these items have been extracted from the FAU_GEN.1.1 element for cross-reference.

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | subtype="system" level="information" logdesc="Attribute configured" user="admin" ui="ssh(192.168.158.10)" action="Edit" cfgtid=16146641 cfgpath="log.disk.setting" cfgattr="status[disable->enable]max-log-file-size[1->99]log-quota[599->15635]" msg="Edit log.disk.setting "<br><br>*Configuring the password policy settings:*<br><br>logver=604099335 timestamp=1676895443 devname="FortiGate-40F" devid="FGT40FTK20010928" vd="root" date=2023-02-20 time=12:17:23 eventtime=1676895443324798321 tz="-0800" logid="0100044546" type="event" subtype="system" level="information" logdesc="Attribute configured" user="admin" ui="GUI(192.168.144.144)" action="Edit" cfgtid=16181855 cfgpath="system.password-policy" cfgattr="status[disable->enable]" msg="Edit system.password-policy "<br><br>*Configuring the settings for the remote logging FortiAnalyzer (note there are multiple FortiAnalyzer connections that can be configured; log.fortianalyzer.setting is the first):*<br><br>logver=604099148 timestamp=1676899546 devname="FAZ-200D" devid="FL200D3A13002601" vd="root" date=2023-02-20 time=13:25:46 eventtime=1676899546324798321 tz="-0800" logid="0100044546" type="event" subtype="system" level="information" logdesc="Attribute configured" user="admin" ui="ssh(192.168.187.210)" action="Edit" cfgtid=16177528 cfgpath="log.fortianalyzer.setting" cfgattr="status[disable->enable] server[172.25.176.57->172.25.176.112]certificate[1->5]" msg="Edit log.fortianalyzer.setting "<br><br>*Configuring a new CRL with automatic scheduled process:*<br><br>logver=604099335 timestamp=1677058791 devname="FortiGate-101F" devid="FGT101FTK19001804" vd="root" date=2023-02-22 time=09:39:51 eventtime=1677058791324798321 tz="-0800" logid="0100044547" type="event" |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | subtype="system" level="information" logdesc="Object attribute configured" user="admin" ui="ssh(192.168.126.134)" action="Add" cfgtid=16173190 cfgpath="vpn.certificate.crl" cfgobj="Crl_name" cfgattr="http-url[->http://www.acme.com/int1.crl.pem]update-interval[0->20]" msg="Add vpn.certificate.crl Local_cert_name"<br><br>*Updating the CRL fetch scheduling interval:*<br><br>logver=604099335 timestamp=1676854961 devname="FortiGate-61F" devid="FGT61FTK96789764" vd="root" date=2023-02-20 time=01:02:41 eventtime=1676854961324798321 tz="-0800" logid="0100044547" type="event" subtype="system" level="information" logdesc="Object attribute configured" user="admin" ui="ssh(192.168.42.176)" action="Edit" cfgtid=16169987 cfgpath="vpn.certificate.crl" cfgobj="Crl_name" cfgattr="update-interval[20070211->211207]" msg="Edit vpn.certificate.crl Local_cert_name"<br><br>*Updating a CRL via HTTP using the automatic scheduled process:*<br><br>logver=604099335 timestamp=1676751031 devname="FortiGate-61F" devid="FGT61FTK96789764" vd="root" date=2023-02-18 time=20:10:31 eventtime=1676751031324798321 tz="-0800" logid="0101041987" type="event" subtype="vpn" level="information" logdesc="Certificate updated" action="info" cert-type="CRL" status="success" name="Crl_name" method="HTTP" reason="N/A" msg="A certificate is updated"<br><br>*Removing a CRL:*<br><br>logver=604099335 timestamp=1677103967 devname="FortiGate-61F" devid="FGT61FTK97689764" vd="root" date=2023-02-22 time=22:12:47 eventtime=1677103967324798321 tz="-0800" logid="0101041985" type="event" subtype="vpn" level="information" logdesc="Certificate removed" action="info" |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | user="admin" ui="ssh(192.168.64.65)" name="Crl_name" msg="A certificate is removed" cert-type="CRL" status="success"<br><br>*Additional TSF data is audited as a result of management functions defined in FMT_SMF.1 and FMT_SMF.1/FFW.* |
| | Generating/import of cryptographic keys (CSR)<br><br>Generating of cryptographic keys (SSH HostKey) | In addition to the action itself a unique key name or key reference shall be logged. | *The action is provided in the "action" field (e.g. 'Add'). The key reference is provided in the "cfgobj" field and is the unique friendly name given by the administrator for the specific key.*<br><br>*For SSH host key generation, there is only one SSH key and therefore the key reference is implicitly satisfied.*<br><br>*Creating a new CSR (generating a private key):*<br><br>logver=604099335 timestamp=1676786013 devname="FortiGate-81F" devid="FGT81FTK27080709" vd="root" date=2023-02-19 time=05:53:33 eventtime=1676786013324798321 tz="-0800" logid="0100044547" type="event" subtype="system" level="information" logdesc="Object attribute configured" user="admin" ui="GUI(192.168.238.215)" action="Add" cfgtid=16179610 cfgpath="vpn.certificate.local" cfgobj="Local_cert_name" cfgattr="password[ENC(string)]private-key[]certificate[]csr[]state[]range[]ike-localid-type[]" msg="Add vpn.certificate.local Local_cert_name""<br><br>*Generating SSH host public/private key pair:*<br><br>logver=604099335 timestamp=1677002095 devname="FortiGate-81F" devid="FGT81FTK27080709" vd="root" date=2023-02-21 time=17:54:55 eventtime=1677002095324798321 tz="-0800" logid="0100032025" type="event" subtype="system" level="warning" logdesc="SSH server re-key" user="admin" ui="ssh(192.168.94.147)" msg="User admin regenerated SSH server keys" |

Log Message Examples

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | Changing of cryptographic keys | In addition to the action itself a unique key name or key reference shall be logged. | *Please refer to audit messages for generation/import above.* |
| | Deleting of cryptographic keys (Managing TOE and CA certificates) | In addition to the action itself a unique key name or key reference shall be logged. | *Please refer to audit messages for FIA_X509_EXT.1/Rev.* |
| | Resetting passwords | Name of related user account shall be logged. | logver=604099335 timestamp=1676983007 devname="FortiGate-40F" devid="FGT40FTK20060909" vd="root" date=2023-02-21 time=12:36:47 eventtime=1676983007324798321 tz="-0800" logid="0100044547" type="event" subtype="system" level="information" logdesc="Object attribute configured" user="admin" ui="GUI(192.168.33.115)" action="Edit" cfgtid=16183974 cfgpath="system.admin" cfgobj="admin" cfgattr="password[ENC(string)]" msg="Edit system.admin admin" |
| | [Starting and stopping services]; (SSH/HTTPS) | Starting and stopping services should be logged. | *The specific service for SSH/HTTPS can be found by examining the "cfgattr" field which shows the changes in enabled/disabled services.*<br><br>*Disabling, for example, ssh:*<br><br>logver=604099148 timestamp=1676754542 devname="FortiGate-61F" devid="FGT61FTK19940211" vd="root" date=2023-02-18 time=21:09:02 eventtime=1676754542324798321 tz="-0800" logid="0100044547" type="event" subtype="system" level="information" logdesc="Object attribute configured" user="admin" ui="console" action="Edit" cfgtid=16179604 cfgpath="system.interface" cfgobj=" mgmt1" cfgattr="allowaccess[ping https ssh->ping https]" msg="Edit system.interface mgmt1"<br><br>*Enabling, for example, ssh and https:* |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | logver=604099335 timestamp=1677067480 devname="FortiGate-61F" devid="FGT61FTK20092411" vd="root" date=2023-02-22 time=12:04:40 eventtime=1677067480324798321 tz="-0800" logid="0100044547" type="event" subtype="system" level="information" logdesc="Object attribute configured" user="admin" ui="console" action="Edit" cfgtid=16140399 cfgpath="system.interface" cfgobj="mgmt1" cfgattr="allowaccess[ping->ping https ssh]" msg="Edit system.interface mgmt1" |
| | [Starting and stopping services]; (IPsec) | | *The specific service is given by the named tunnel in the "vpntunnel" field.*<br><br>*Starting IPsec:*<br><br>logver=604099392 timestamp=1676906183 devname="FortiGate-101F" devid="FGT101FTK16001895" vd="root" date=2023-02-20 time=15:16:23 eventtime=1676906183324798321 tz="-0800" logid="0101037138" type="event" subtype="vpn" level="notice" logdesc="IPsec connection status changed" msg="IPsec connection status change" action="tunnel-up" remip=11.101.1.1 locip=173.1.1.1 remport=26759 locport=1017 outintf="port1" cookies="4abcd0c097600c8b/f176da79bcb9589c" user="N/A" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="vpn_example_tunnel" tunnelip=N/A tunnelid=7627932783 tunneltype="ipsec" duration=0 sentbyte=0 rcvdbyte=0 nextstat=0<br><br>*Stopping IPsec:*<br><br>logver=604099392 timestamp=1676739381 devname="FortiGate-101F" devid="FGT101FTK16001895" vd="root" date=2023-02-18 time=16:56:21 eventtime=1676739381324798321 tz="-0800" logid="0101037138" type="event" subtype="vpn" level="notice" logdesc="IPsec connection status changed" msg="IPsec connection status change" action="tunnel-down" remip=11.101.1.1 locip=173.1.1.1 remport=17505 locport=15432 outintf="port1" |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | cookies="dced31cb3757c18e/420616ea9a70bfa0" user="C = CA, S = Ontario, L = Ottawa, CN = ..." group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="vpn_example_tunnel" tunnelip=N/A tunnelid=7627932783 tunneltype="ipsec" duration=37243 sentbyte=3096 rcvdbyte=3665 nextstat=0 |
| FIA_AFL.1 | Unsuccessful login attempts limit is met or exceeded. | Origin of the attempt (e.g., IP address). | *The "origin of the attempt" is found using the "ui" field as well as in the "msg" itself.*<br><br>logver=604099148 timestamp=1677023525 devname="FortiGate-81F" devid="FGT81FTK36350909" vd="root" date=2023-02-21 time=23:52:05 eventtime=1677023525324798321 tz="-0800" logid="0100032021" type="event" subtype="system" level="alert" logdesc="Admin login disabled" ui="192.168.1.56" action="login" status="failed" reason="exceed_limit" msg="Login disabled from IP 192.168.1.56 for 300 seconds because of 6 bad attempts" |
| FIA_UIA_EXT.1 | All use of identification and authentication mechanism. | Origin of the attempt (e.g., IP address). | *The "origin of the attempt" is found using the "ui" field. For "console", that is the origin of the attempt. For remote administration interfaces, the "ui" field contains the IP address of the remote endpoint.*<br><br>*Console:*<br><br>logver=604099148 timestamp=1676809962 devname="FortiGate-81F" devid="FGT81FTK36350909" vd="root" date=2023-02-19 time=12:32:42 eventtime=1676809962324798321 tz="-0800" logid="0100032001" type="event" subtype="system" level="information" logdesc="Admin login successful" sn="1676809962" user="admin" ui="console" method="console" srcip=192.168.221.24 dstip=192.168.182.121 action="login" status="success" reason="none" profile="super_admin" msg="Administrator admin logged in successfully from console"<br><br>*HTTPS:*<br><br>logver=604099148 timestamp=1676706239 devname="FortiGate-81F" devid="FGT81FTK20081847" vd="root" date=2023-02-18 time=07:43:59 |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | eventtime=1676706239324798321 tz="-0800" logid="0100032001" type="event" subtype="system" level="information" logdesc="Admin login successful" sn="1676706239" user="admin" ui="https(192.168.138.193)" method="https" srcip= 192.168.138.193 dstip=192.168.188.174 action="login" status="success" reason="none" profile="super_admin" msg="Administrator admin logged in successfully from https(192.168.138.193)"<br><br>*SSH:*<br><br>logver=604099148 timestamp=1676961764 devname="FortiGate-81F" devid="FGT81FTK20081847" vd="root" date=2023-02-21 time=06:42:44 eventtime=1676961764324798321 tz="-0800" logid="0100032001" type="event" subtype="system" level="information" logdesc="Admin login successful" sn="1676961764" user="admin" ui="ssh(192.168.118.100)" method="ssh" srcip= 192.168.118.100 dstip=192.168.91.194 action="login" status="success" reason="none" profile="N/A" msg="Administrator admin logged in successfully from ssh(192.168.118.100)"<br><br>*Example of a failed login:*<br><br>logver=604099335 timestamp=1676758260 devname="FortiGate-81F" devid="FGT81FTK36350909" vd="root" date=2023-02-18 time=17:11:00 eventtime=1676758260324798321 tz="-0800" logid="0100032002" type="event" subtype="system" level="alert" logdesc="Admin login failed" sn="0" user="admin" ui="https(192.168.129.18)" method="https" srcip= 192.168.129.18 dstip=192.168.30.37 action="login" status="failed" reason="passwd_invalid" msg="Administrator admin login failed from https(192.168.129.18) because of invalid password" |
| FIA_UAU_EXT.2 | All use of identification and authentication mechanism. | Origin of the attempt (e.g., IP address). | *Please refer to FIA_UIA_EXT.1* |

Log Message Examples

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| FMT_MOF.1/ManualUpdate | Any attempt to initiate a manual update | None | *Updates when performed by a valid Security Administrator can either succeed or fail and therefore refer to log messages for FPT_TUD_EXT.1.*<br><br>*When invalid users attempt to initiate an update, the command itself fails to be executed:*<br><br>logver=604099148 timestamp=1676885962 devname="FortiGate-61F" devid="FGT61FTK20043642" vd="root" date=2023-02-20 time=09:39:22 eventtime=1676885962324798321 tz="-0800" logid="0100032149" type="event" subtype="system" level="notice" logdesc="Command failed" user="user1" ui="ssh(192.168.162.115)" msg="Command failed:'execute restore image ftp /srv/ftp/image.bin 52.7.23.11 ' Return code -28: " |
| FMT_SMF.1 | All management activities of TSF data. | None | *Ability to configure the access banner:*<br><br>logver=604099148 timestamp=1676850487 devname="FortiGate-81F " devid="FGT81FTK20071964" vd="root" date=2023-02-19 time=23:48:07 eventtime=1676850487324798321 tz="-0800" logid="0100044547" type="event" subtype="system" level="information" logdesc="Object attribute configured" user="admin" ui="ssh(192.168.6.231)" action="Edit" cfgtid=16158790 cfgpath="system.replacemsg.admin" cfgobj="pre_admin-disclaimer-text" cfgattr="buffer[Admin Disclaimer Notice-> Admin Disclaimer Update]" msg="Edit system.replacemsg.admin pre_admin-disclaimer-text"<br><br>*Ability to configure the session inactivity time before session termination or locking (console):*<br><br>logver=604099148 timestamp=1676739099 devname="FortiGate-81F" devid="FGT81FTK20071964" vd="root" date=2023-02-18 time=16:51:39 eventtime=1676739099324798321 tz="-0800" logid="0100044546" type="event" subtype="system" level="information" logdesc="Attribute configured" user="admin" |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | ui="ssh(192.168.186.86)" action="Edit" cfgtid=16167946 cfgpath="system.global" cfgattr="admin-console-timeout[0->30]" msg="Edit system.global"<br><br>*Ability to configure the session inactivity time before session termination or locking (SSH/HTTPS):*<br><br>logver=604099148 timestamp=1677092213 devname="FortiGate-81F" devid="FGT81FTK20071964" vd="root" date=2023-02-22 time=18:56:53 eventtime=1677092213324798321 tz="-0800" logid="0100044546" type="event" subtype="system" level="information" logdesc="Attribute configured" user="admin" ui="console" action="Edit" cfgtid=16181583 cfgpath="system.global" cfgattr="admintimeout[300->120]" msg="Edit system.global"<br><br>*Ability to update the TOE, and to verify the updates using digital signature capability prior to installing those updates: Please refer to audit messages for FPT_TUD_EXT.1.*<br><br>*Ability to configure the authentication failure parameters for FIA_AFL.1:*<br><br>*Configuring the authentication lock-out settings:*<br><br>logver=604099148 timestamp=1677045543 devname="FortiGate-81F" devid="FGT81FTK20071964" vd="root" date=2023-02-22 time=05:59:03 eventtime=1677045543324798321 tz="-0800" logid="0100044546" type="event" subtype="system" level="information" logdesc="Attribute configured" user="admin" ui="console" action="Edit" cfgtid=16135062 cfgpath="system.global" cfgattr="admin-lockout-threshold[1->3]admin-lockout-duration[0->60]" msg="Edit system.global "<br><br>*Ability to start and stop services: Please refer to audit messages for FAU_GEN.1 above.*<br><br>*Ability to manage the cryptographic keys: Please refer to audit messages for FAU_GEN.1 above as well as audit messages for FMT_MTD.1/CryptoKeys.* |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | *Ability to configure the cryptographic functionality:*<br><br>*Configuring the IPsec IKE cryptographic algorithm proposal:*<br><br>logver=604099335 timestamp=1676966888 devname="FortiGate-81F" devid="FGT81FTK20071964" vd="root" date=2023-02-21 time=08:08:08 eventtime=1676966888324798321 tz="-0800" logid="0100044547" type="event" subtype="system" level="information" logdesc="Object attribute configured" user="admin" ui="ssh(192.168.160.149)" action="Edit" cfgtid=16134645 cfgpath="vpn.ipsec.phase1-interface" cfgobj="vpn_example_tunnel" cfgattr="proposal[aes-md5->aes-sha512]" msg="Edit vpn.ipsec.phase1-interface vpn_example_tunnel"<br><br>*Configuring the IPsec IKE DH group:*<br><br>logver=604099148 timestamp=1676887495 devname="FortiGate-81F" devid="FGT81FTK20071964" vd="root" date=2023-02-20 time=10:04:55 eventtime=1676887495324798321 tz="-0800" logid="0100044547" type="event" subtype="system" level="information" logdesc="Object attribute configured" user="admin" ui="ssh(192.168.156.182)" action="Edit" cfgtid=16168241 cfgpath="vpn.ipsec.phase1-interface" cfgobj="vpn_example_tunnel" cfgattr="dhgrp[14->20]" msg="Edit vpn.ipsec.phase1-interface vpn_example_tunnel"<br><br>*Configuring the IPsec ESP cryptographic algorithm proposal:*<br><br>logver=604099335 timestamp=1677045671 devname="FortiGate-81F" devid="FGT81FTK20071964" vd="root" date=2023-02-22 time=06:01:11 eventtime=1677045671324798321 tz="-0800" logid="0100044547" type="event" subtype="system" level="information" logdesc="Object attribute configured" user="admin" ui="ssh(192.168.25.35)" action="Edit" cfgtid=16166449 cfgpath="vpn.ipsec.phase2-interface" cfgobj="vpn_example_tunnel" |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | cfgattr="proposal[aes-sha256->aes-sha512]" msg="Edit vpn.ipsec.phase2-interface vpn_example_tunnel"<br><br>*Configuring the IPsec phase 2 DH algorithm:*<br><br>logver=604099148 timestamp=1676905301 devname="FortiGate-81F" devid="FGT81FTK20071964" vd="root" date=2023-02-20 time=15:01:41 eventtime=1676905301324798321 tz="-0800" logid="0100044547" type="event" subtype="system" level="information" logdesc="Object attribute configured" user="admin" ui="ssh(192.168.12.72)" action="Edit" cfgtid=16174616 cfgpath="vpn.ipsec.phase2-interface" cfgobj="vpn_example_tunnel" cfgattr="dhgrp[14->20]" msg="Edit vpn.ipsec.phase2-interface vpn_example_tunnel"<br><br>*Ability to configure the lifetime for IPsec SAs:*<br><br>*Rekey time for phase 1:*<br><br>logver=604099148 timestamp=1677007456 devname="FortiGate-61F" devid="FGT61FTK20068719" vd="root" date=2023-02-21 time=19:24:16 eventtime=1677007456324798321 tz="-0800" logid="0100044547" type="event" subtype="system" level="information" logdesc="Object attribute configured" user="admin" ui="ssh(192.168.186.59)" action="Edit" cfgtid=16169346 cfgpath="vpn.ipsec.phase1-interface" cfgobj="vpn_example_tunnel" cfgattr="keylife[86400->3600]" msg="Edit vpn.ipsec.phase1-interface vpn_example_tunnel"<br><br>*Rekey time for phase 2:*<br><br>logver=604099148 timestamp=1677018215 devname="FortiGate-61F" devid="FGT61FTK20068719" vd="root" date=2023-02-21 time=22:23:35 eventtime=1677018215324798321 tz="-0800" logid="0100044547" type="event" subtype="system" level="information" logdesc="Object attribute configured" |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | user="admin" ui="ssh(192.168.217.242)" action="Edit" cfgtid=16167503 cfgpath="vpn.ipsec.phase2-interface" cfgobj="vpn_example_tunnel" cfgattr="keylife-type[seconds->seconds]keylifeseconds[43200->2990]" msg="Edit vpn.ipsec.phase2-interface vpn_example_tunnel"<br><br>*Rekey volume for phase 2:*<br><br>logver=604099148 timestamp=1676897456 devname="FortiGate-61F" devid="FGT61FTK20068719" vd="root" date=2023-02-20 time=12:50:56 eventtime=1676897456324798321 tz="-0800" logid="0100044547" type="event" subtype="system" level="information" logdesc="Object attribute configured" user="admin" ui="ssh(192.168.231.6)" action="Edit" cfgtid=16183197 cfgpath="vpn.ipsec.phase2-interface" cfgobj="vpn_example_tunnel" cfgattr="keylife-type[seconds->seconds]keylifekbs[5120->5120]" msg="Edit vpn.ipsec.phase2-interface vpn_example_tunnel"<br><br>*Ability to import X.509v3 certificates to the TOE's trust store: Please refer to audit messages in FAU_GEN.1 and FIA_X509_EXT.1/Rev.*<br><br>*Ability to configure the reference identifier for the peer:*<br><br>logver=604099148 timestamp=1677004391 devname="FortiGate-61F" devid="FGT61FTK20068719" vd="root" date=2023-02-21 time=18:33:11 eventtime=1677004391324798321 tz="-0800" logid="0100044547" type="event" subtype="system" level="information" logdesc="Object attribute configured" user="admin" ui="ssh(192.168.105.141)" action="Add" cfgtid=16138554 cfgpath="user.peer" cfgobj="PeerName" cfgattr="ca[ CA_Cert_2 ]subject C=US, ST=AZ, L=Phoenix, O=ACME, OU=Finance, CN=WAN VM ]" msg="Add user.peer PeerName" |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | *Ability to set the time which is used for time-stamps: Please refer to audit messages for FPT_STM_EXT.1.*<br><br>*Ability to manage the trusted public keys database:*<br><br>logver=604099335 timestamp=1676794442 devname="FortiGate-61F" devid="FGT61FTK20068719" vd="root" date=2023-02-19 time=08:14:02 eventtime=1676794442324798321 tz="-0800" logid="0100044547" type="event" subtype="system" level="information" logdesc="Object attribute configured" user="admin" ui="ssh(192.168.48.104)" action="Edit" cfgtid=16178254 cfgpath="system.admin" cfgobj="admin" cfgattr="ssh-public-key1[->]" msg="Edit system.admin admin" |
| FPT_TUD_EXT.1 | Initiation of update; | None | *Updates when performed by a valid Security Administrator can either succeed or fail; therefore see next line.* |
| | Result of the update attempt (success or failure) | None | *Successful update:*<br><br>logver=604099148 timestamp=1676876940 devname="FGT-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-20 time=07:09:00 eventtime=1676876940324798321 tz="-0800" logid="0100032201" type="event" subtype="system" level="critical" logdesc="Image loaded successfully" user="admin" ui="GUI(192.168.200.42)" action="loaded-image" status="success" msg="User admin loaded an image from GUI(192.168.200.42). The new image does have a valid RSA signature."<br><br>*Examples of errors (e.g. due to invalid signatures or file corruption):*<br><br>logver=604078573 timestamp=1677103224 devname="FGT-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-22 time=22:00:24 eventtime=1677103224324798321 tz="-0800" logid="0100032226" type="event" subtype="system" level="critical" logdesc="Image failed to load" user="admin" |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | ui="ssh(192.168.201.43)" action="loaded-image" status="failure" msg="User admin loaded a wrong image from ssh(192.168.201.43)."<br><br>logver=604099335 timestamp=1677016593 devname="FGT-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-21 time=21:56:33 eventtime=1677016593324798321 tz="-0800" logid="0100032201" type="event" subtype="system" level="critical" logdesc="Image loaded successfully" user="admin" ui="GUI(192.168.202.45)" action="loaded-image" status="success" msg="User admin loaded an image from GUI(192.168.202.45). The new image does not have a valid RSA signature." |
| FPT_STM_EXT.1 | Discontinuous changes to time – either Administrator actuated or changed via an automated process.<br><br>(Note that no continuous changes to time need to be logged. See also application note on FPT_STM_EXT.1) | For discontinuous changes to time:<br><br>**(i)** The old and new values for the time.<br><br>**(ii)** Origin of the attempt to change time for success and failure (e.g., IP address). | *The "msg" field contains the old and new date/time information. The origin of the attempt is found using a combination of the named user in the "userid" field (and also in the "msg" field) and the "ui" field (who and from where, respectively).*<br><br>logver=604099148 timestamp=1676680394 devname="FGT-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-18 time=00:33:14 eventtime=1676680394324798321 tz="-0800" logid="0100032140" type="event" subtype="system" level="notice" logdesc="Global time setting changed by user" user="admin" ui="GUI(192.168.190.183)" srcip=192.168.190.183 action="time_change" field="date-time" msg="User admin changed time from Sat Feb 18 00:33:14 2023 to Mon Feb 20 21:45:12 2023" |
| FTA_SSL_EXT.1 (if "terminate the session" is selected) | The termination of a local session by the session locking mechanism. (Console) | None | logver=604099148 timestamp=1676775359 devname="FGT-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-19 time=02:55:59 eventtime=1676775359324798321 tz="-0800" logid="0100032003" type="event" subtype="system" level="information" logdesc="Admin logout successful" sn="1676775359" user="admin" ui="console" method="console" srcip=192.168.47.7 dstip=192.168.52.112 action="logout" status="success" duration=301 reason="timeout" msg="Administrator admin timed out on console" |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| FTA_SSL.3 | The termination of a remote session by the session locking mechanism. (Web UI) | None | logver=604099148 timestamp=1676982268 devname="FGT-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-21 time=12:24:28 eventtime=1676982268324798321 tz="-0800" logid="0100032003" type="event" subtype="system" level="information" logdesc="Admin logout successful" sn="1676982268" user="admin" ui="https(192.168.78.250)" method="https" srcip=192.168.78.250 dstip=192.168.17.227 action="logout" status="success" duration=184 reason="timeout" msg="Administrator admin timed out on https(192.168.78.250)" |
| | The termination of a remote session by the session locking mechanism. (SSH) | None | logver=604099148 timestamp=1677025206 devname="FGT-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-22 time=00:20:06 eventtime=1677025206324798321 tz="-0800" logid="0100032003" type="event" subtype="system" level="information" logdesc="Admin logout successful" sn="1677025206" user="admin" ui="ssh(192.168.78.250)" method="ssh" srcip=192.168.78.250 dstip=192.168.188.238 action="logout" status="success" duration=381 reason="timeout" msg="Administrator admin timed out on ssh(192.168.78.250)" |
| FTA_SSL.4 | The termination of an interactive session. (Console) | None | logver=604099148 timestamp=1677101355 devname="FGT-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-22 time=21:29:15 eventtime=1677101355324798321 tz="-0800" logid="0100032003" type="event" subtype="system" level="information" logdesc="Admin logout successful" sn="1677101355" user="admin" ui="console" method="console" srcip=192.168.54.69 dstip=192.168.128.223 action="logout" status="success" duration=3 reason="exit" msg="Administrator admin logged out from console" |
| | The termination of an interactive session. (Web UI) | None | logver=604099148 timestamp=1676828065 devname="FGT-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-19 time=17:34:25 eventtime=1676828065324798321 tz="-0800" logid="0100032003" type="event" subtype="system" level="information" logdesc="Admin logout successful" |

Log Message Examples

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | sn="1676828065" user="admin" ui="https(192.168.48.234)" method="https" srcip=192.168.48.234 dstip=192.168.34.60 action="logout" status="success" duration=62 reason="exit" msg="Administrator admin logged out from https(192.168.48.234)" |
| | The termination of an interactive session. (SSH) | None | logver=604099335 timestamp=1676972384 devname="FGT-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-21 time=09:39:44 eventtime=1676972384324798321 tz="-0800" logid="0100032003" type="event" subtype="system" level="information" logdesc="Admin logout successful" sn="1676972384" user="admin" ui="ssh(192.168.218.82)" method="ssh" srcip=192.168.218.82 dstip=192.168.204.27 action="logout" status="success" duration=22 reason="exit" msg="Administrator admin logged out from ssh(192.168.218.82)" |
| FTP_ITC.1 | Initiation of the trusted channel. (TLS Client) | None | logver=604099335 timestamp=1677068091 devname="FGT-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-22 time=12:14:51 eventtime=1677068091324798321 tz="-0800" logid="0100038408" type="event" subtype="system" level="information" logdesc="SSL connection established" dstip=192.168.57.21 dstport=514 action="connect" status="success" msg="SSL connection to 192.168.57.21 is successfully established." |
| | Termination of the trusted channel. (TLS Client) | None. | logver=604099335 timestamp=1676797712 devname="FGT-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-19 time=09:08:32 eventtime=1676797712324798321 tz="-0800" logid="0100038409" type="event" subtype="system" level="information" logdesc="SSL connection closed" dstip=192.168.115.20 dstport=514 action="disconnect" status="success" msg="SSL connection to 192.168.115.20 is successfully closed." |
| | Failure of the trusted channel functions. (TLS Client) | Identification of the initiator and target of **failed** trusted | *The initiator is the TOE (found in "devname" and "devid"). The target is the IP or DNS name found in the "dstip" field and also found in the "msg" field.* |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | channels establishment attempt. | logver=604099148 timestamp=1676702479 devname="FGT-2601F" devid=" F2K61FTK21900118" vd="root" date=2023-02-18 time=06:41:19 eventtime=1676702479324798321 tz="-0800" logid="0100038410" type="event" subtype="system" level="information" logdesc="SSL connection failed" dstip=192.168.180.22 dstport=514 reason="connect() failed: 111" action="connect" status="failure" msg="SSL connect to 192.168.180.22 has failed."<br>*For more in-depth reasons for the nature of the failure, please refer to audit messages for FCS_TLSC_EXT.1.* |
| FTP_TRP.1/Admin | Initiation of the trusted path. (Web UI) | None | *Please refer to FIA_UIA_EXT.1 for login attempts against the HTTPS interface.* |
| | Termination of the trusted path. (Web UI) | None | *Please refer to FTA_SSL.4 for logout against the HTTPS interface.* |
| | Failure of the trusted path functions. (Web UI) | None | *Please refer to FIA_UIA_EXT.1 for failure attempts against the HTTPS interface.* |
| | Initiation of the trusted path. (SSH) | None | *Please refer to FIA_UIA_EXT.1 for login attempts against the SSH interface.* |
| | Termination of the trusted path. (SSH) | None | *Please refer to FTA_SSL.4 for logout against the SSH interface.* |
| | Failure of the trusted path functions. (SSH) | None | *Please refer to FIA_UIA_EXT.1 for failure attempts against the SSH interface.* |

Log Message Examples

Optional Auditable Events

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| FCS_TLSC_EXT.2 | Failure to establish a TLS Session | Reason for failure | *Please refer to FCS_TLSC_EXT.1.* |

Selection-Based Auditable Events

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| FCS_HTTPS_EXT.1 | Failure to establish a HTTPS Session. | Reason for failure | *Please refer to FCS_TLSS_EXT.1.* |
| FCS_IPSEC_EXT.1 | Failure to establish an IPsec SA. | Reason for failure | *The "reason for failure" is found in either in the "logdesc", "msg" or the "reason" fields.*<br><br>*Policy mismatch:*<br><br>logver=604099335 timestamp=1677098507 devname="FGT-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-22 time=20:41:47 eventtime=1677098507324798321 tz="-0800" logid="0101037124" type="event" subtype="vpn" level="error" logdesc="IPsec phase 1 error" msg="IPsec phase 1 error" action="negotiate" remip=192.168.223.108 locip=192.168.10.47 remport=500 locport=500 outintf="port1" cookies="3ccd0e68774ff798/8906ac1e24f101f2" user="N/A" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="vpn_example_tunnel" status="negotiate_error" reason="peer SA proposal not match local policy" peer_notif="NOT-APPLICABLE"<br><br>*Invalid certificates:*<br><br>logver=604099148 timestamp=1676935023 devname="FGT-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-20 time=23:17:03 eventtime=1676935023324798321 tz="-0800" logid="0101037124" type="event" subtype="vpn" level="error" logdesc="IPsec phase 1 error" msg="IPsec phase 1 error" |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | action="negotiate" remip=192.168.105.13 locip=192.168.248.156 remport=500 locport=500 outintf="port1" cookies="ef7dfcf02365818e/2f302a2974969205" user="C = CA, S = Ontario, L = Ottawa, CN = ..." group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="vpn_example_tunnel" status="negotiate_error" reason="invalid certificate"<br><br>*Unable to negotiate IKEv1 aggressive mode with peer:*<br><br>logver=604099148 timestamp=1677018731 devname="FGT-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-21 time=22:32:11 eventtime=1677018731324798321 tz="-0800" logid="0101037128" type="event" subtype="vpn" level="error" logdesc="Progress IPsec phase 1" msg="progress IPsec phase 1" action="negotiate" remip=192.168.213.218 locip=192.168.95.125 remport=500 locport=500 outintf="port1" cookies="b9b794077bfd6980/9b56cc1e80380d9f" user="N/A" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="vpn_example_tunnel" status="failure" init="remote" mode="aggressive" dir="inbound" stage=1 role="responder" result="ERROR"<br><br>*Unable to start IKEv1:*<br><br>logver=604099392 timestamp=1676728068 devname="FGT-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-18 time=13:47:48 eventtime=1676728068324798321 tz="-0800" logid="0101037128" type="event" subtype="vpn" level="error" logdesc="Progress IPsec phase 1" msg="progress IPsec phase 1" action="negotiate" remip=192.168.230.177 locip=192.168.34.52 remport=500 locport=500 outintf="port1" cookies="425a0d133ddea9df/bbcd86f2f2c04d65" user="N/A" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="vpn_example_tunnel" status="failure" init="remote" mode="main" dir="inbound" stage=1 role="responder" result="ERROR" |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | *Unable to start IKEv2:*<br><br>logver=604099335 timestamp=1676724234 devname="FGT-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-18 time=12:43:54 eventtime=1676724234324798321 tz="-0800" logid="0101037128" type="event" subtype="vpn" level="error" logdesc="Progress IPsec phase 1" msg="progress IPsec phase 1" action="negotiate" remip=192.168.51.153 locip=192.168.207.201 remport=500 locport=500 outintf="port1" cookies="6fe8c72538d8ffbf/e54bc469294c1604" user="N/A" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="vpn_example_tunnel" status="failure" init="local" exch="SA_INIT" dir="inbound" role="initiator" result="ERROR" version="IKEv2"<br><br>*Unable to start IKEv2 CHILD_SA:*<br><br>logver=604099148 timestamp=1676869927 devname="FGT-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-20 time=05:12:07 eventtime=1676869927324798321 tz="-0800" logid="0101037130" type="event" subtype="vpn" level="error" logdesc="Progress IPsec phase 2" msg="progress IPsec phase 2" action="negotiate" remip=192.168.228.126 locip=192.168.237.35 remport=500 locport=500 outintf="port1" cookies="96f7e4ced7336dfe/e610770922867e38" user="N/A" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="vpn_example_tunnel" status="failure" init="local" exch="CREATE_CHILD" dir="inbound" role="initiator" result="ERROR" version="IKEv2" |
| FCS_SSHS_EXT.1 | Failure to establish an SSH session | Reason for failure | *The “reason for failure” is found in either in the “logdesc”, “msg” or the “reason” fields.*<br><br>*Bad public key:*<br><br>logver=604099335 timestamp=1676770587 devname="FGT-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-19 time=01:36:27 eventtime=1676770587324798321 tz="-0800" logid="0100032002" type="event" |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | subtype="system" level="alert" logdesc="Admin login failed" sn="0" user="admin" ui="ssh(192.168.78.36)" method="ssh" srcip=192.168.78.36 dstip=192.168.254.178 action="login" status="failed" reason="ssh_key_invalid" msg="Administrator admin login failed from ssh(192.168.78.36) because of invalid ssh key"<br><br>*Bad packet size:*<br><br>logver=604099335 timestamp=1676728937 devname="FGT-2601F" devid=" F2K61FTK21900118" vd="root" date=2023-02-18 time=14:02:17 eventtime=1676728937324798321 tz="-0800" logid="0100032026" type="event" subtype="system" level="warning" logdesc="SSH server received bad length packet" ui="sshv2" msg="Bad packet length:262160"<br><br>*Bad host key algorithm negotiation:*<br><br>logver=604099335 timestamp=1676718664 devname="FGT-2601F" devid=" F2K61FTK21900118" vd="root" date=2023-02-18 time=11:11:04 eventtime=1676718664324798321 tz="-0800" logid="0100032247" type="event" subtype="system" level="error" logdesc="SSH protocol cannot be negotiated" addr="192.168.22.16" port=0 msg="Negotiation failed: no matching host key type found. Their offer: ssh-dss."<br><br>*Bad HMAC algorithm negotiation:*<br><br>logver=604099335 timestamp=1676803764 devname="FGT-2601F" devid=" F2K61FTK21900118" vd="root" date=2023-02-19 time=10:49:24 eventtime=1676803764324798321 tz="-0800" logid="0100032247" type="event" subtype="system" level="error" logdesc="SSH protocol cannot be negotiated" addr="192.168.33.49" port=0 msg="Negotiation failed: no matching MAC found. Their offer: hmac-md5." |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | *Bad diffie-hellman key exchange algorithm negotiation:*<br><br>logver=604099335 timestamp=1677008151 devname="FGT-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-21 time=19:35:51 eventtime=1677008151324798321 tz="-0800" logid="0100032247" type="event" subtype="system" level="error" logdesc="SSH protocol cannot be negotiated" addr="192.168.19.77" port=0 msg="Negotiation failed: no matching key exchange method found. Their offer: diffie-hellman-group1-sha1." |
| FCS_TLSC_EXT.1 | Failure to establish a TLS Session | Reason for failure | *The "reason for failure" is found in either in the "logdesc", "msg" or the "reason" fields.*<br><br>*Unsupported protocol:*<br><br>logver=604099148 timestamp=1676830538 devname="FGT-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-19 time=18:15:38 eventtime=1676830538324798321 tz="-0800" logid="0100038410" type="event" subtype="system" level="information" logdesc="SSL connection failed" dstip=192.168.27.14 dstport=514 reason="ssl_connect() failed: 338030850 (error:1425F102:SSL routines:ssl_choose_client_version:unsupported protocol)" action="connect" status="failure" msg="SSL connect to 192.168.27.14 has failed."<br><br>*Various types of invalid certificate subject/SAN:*<br><br>logver=604099335 timestamp=1676907014 devname="FGT-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-20 time=15:30:14 eventtime=1676907014324798321 tz="-0800" logid="0100038410" type="event" subtype="system" level="error" logdesc="SSL connection failed" dstip=N/A dstport=N/A reason="IP address mismatch" action="info" status="failure" msg="Certificate is invalid, subject: C = CA, S = Ontario, L = Ottawa, CN = ..."<br><br>*Invalid certificate purpose:* |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | logver=604099335 timestamp=1677100371 devname="FGT-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-22 time=21:12:51 eventtime=1677100371324798321 tz="-0800" logid="0100038410" type="event" subtype="system" level="error" logdesc="SSL connection failed" dstip=N/A dstport=N/A reason="unsupported certificate purpose" action="info" status="failure" msg="Certificate is invalid, subject: C = CA, S = Ontario, L = Ottawa, CN = ..."<br><br>*Invalid certificate verification:*<br><br>logver=604099335 timestamp=1676684088 devname="FGT-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-18 time=01:34:48 eventtime=1676684088324798321 tz="-0800" logid="0100038410" type="event" subtype="system" level="information" logdesc="SSL connection failed" dstip=192.168.155.22 dstport=514 reason="ssl_connect() failed: 337047686 (error:1416F086:SSL routines:tls_process_server_certificate:certificate verify failed)" action="connect" status="failure" msg="SSL connect to 192.168.155.22 has failed."<br><br>*Invalid certificate type:*<br><br>logver=604099335 timestamp=1676961533 devname="FortiGate-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-21 time=06:38:53 eventtime=1676961533324798321 tz="-0800" logid="0100038410" type="event" subtype="system" level="information" logdesc="SSL connection failed" dstip=192.168.149.254 dstport=13897 reason="ssl_connect() failed: 337047935 (error:1416F17F:SSL routines:tls_process_server_certificate:wrong certificate type)" action="connect" status="failure" msg="SSL connect to 192.168.149.254 has failed."<br><br>*Various types of bad ciphersuites:*<br><br>logver=604099335 timestamp=1676748497 devname="FortiGate-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-18 time=19:28:17 |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | eventtime=1676748497324798321 tz="-0800" logid="0100038410" type="event" subtype="system" level="information" logdesc="SSL connection failed" dstip= 192.168.31.229 dstport=7403 reason="ssl_connect() failed: 337756408 (error:1421C0F8:SSL routines:set_client_ciphersuite:unknown cipher returned)" action="connect" status="failure" msg="SSL connect to 192.168.31.229 has failed."<br><br>logver=604099335 timestamp=1676926947 devname="FortiGate-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-20 time=21:02:27 eventtime=1676926947324798321 tz="-0800" logid="0100038410" type="event" subtype="system" level="information" logdesc="SSL connection failed" dstip= 192.168.16.112 dstport=2434 reason="ssl_connect() failed: 337756421 (error:1421C105:SSL routines:set_client_ciphersuite:wrong cipher returned)" action="connect" status="failure" msg="SSL connect to 192.168.16.112 has failed."<br><br>*Invalid ECDHE curve parameters:*<br><br>logver=604099335 timestamp=1676876990 devname="FortiGate-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-20 time=07:09:50 eventtime=1676876990324798321 tz="-0800" logid="0100038410" type="event" subtype="system" level="information" logdesc="SSL connection failed" dstip= 192.168.75.147 dstport=13745 reason="ssl_connect() failed: 337265018 (error:141A417A:SSL routines:tls_process_ske_ecdhe:wrong curve)" action="connect" status="failure" msg="SSL connect to 192.168.75.147 has failed."<br><br>*Various forms of invalid certificate signature errors:*<br><br>logver=604099335 timestamp=1676936891 devname="FortiGate-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-20 time=23:48:11 eventtime=1676936891324798321 tz="-0800" logid="0100038410" type="event" subtype="system" level="information" logdesc="SSL connection failed" dstip= 192.168.148.123 dstport=22759 reason="ssl_connect() failed: 67567754 |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | (error:0407008A:rsa routines:RSA_padding_check_PKCS1_type_1:invalid padding)" action="connect" status="failure" msg="SSL connect to 192.168.148.123 has failed."<br><br>logver=604099335 timestamp=1676710259 devname="FortiGate-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-18 time=08:50:59 eventtime=1676710259324798321 tz="-0800" logid="0100038410" type="event" subtype="system" level="information" logdesc="SSL connection failed" dstip= 192.168.175.104 dstport=21028 reason="ssl_connect() failed: 67702888 (error:04091068:rsa routines:int_rsa_verify:bad signature)" action="connect" status="failure" msg="SSL connect to 192.168.175.104 has failed."<br><br>*Invalid handshake or bad application data:*<br><br>logver=604099335 timestamp=1676845971 devname="FortiGate-2601F" devid="F2K61FTK21900118" vd="root" date=2023-02-19 time=22:32:51 eventtime=1676845971324798321 tz="-0800" logid="0100038410" type="event" subtype="system" level="information" logdesc="SSL connection failed" dstip= 192.168.120.154 dstport=15407 reason="ssl_connect() failed: 336130329 (error:1408F119:SSL routines:ssl3_get_record:decryption failed or bad record mac)" action="connect" status="failure" msg="SSL connect to 192.168.120.154 has failed." |
| FCS_TLSS_EXT.1 | Failure to establish a TLS Session | Reason for failure | *The "reason for failure" is found in either in the "logdesc", "msg" or the "reason" fields.*<br><br>logver=604099335 timestamp=1677095471 devname="FGT-301E" devid="FG3H1E5818901639 " vd="root" date=2023-02-22 time=19:51:11 eventtime=1677095471324798321 tz="-0800" logid="0100038420" type="event" subtype="system" level="information" logdesc="HTTPS connection" remote=192.168.10.99 action="connect" status="failure" reason="SSL accept failed" msg="SSL library error 1 in handshake (server FortiGate:443)" |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| FIA_X509_EXT.1/Rev | Unsuccessful attempt to validate a certificate (TLS Client to FortiAnalyzer) | Reason for failure | *The "reason for failure" is found in either in the "logdesc", "msg" or the "reason" fields.*<br><br>*General certificate validation error:*<br><br>logver=604099148 timestamp=1676685958 devname="FGT-1500D" devid="FG1K5D3I15802490" vd="root" date=2023-02-18 time=02:05:58 eventtime=1676685958324798321 tz="-0800" logid="0100038410" type="event" subtype="system" level="information" logdesc="SSL connection failed" dstip=192.168.69.158 dstport=11769 reason="ssl_connect() failed: 337047686 (error:1416F086:SSL routines:tls_process_server_certificate:certificate verify failed)" action="connect" status="failure" msg="SSL connect to 192.168.69.158 has failed."<br><br>*Expired certificate:*<br><br>logver=604099335 timestamp=1676978891 devname="FGT-1101E" devid="FG10E1TB199002362" vd="root" date=2023-02-21 time=11:28:11 eventtime=1676978891324798321 tz="-0800" logid="0100038410" type="event" subtype="system" level="error" logdesc="SSL connection failed" dstip=N/A dstport=16373 reason="certificate has expired" action="info" status="failure" msg="Certificate is invalid, subject: C = CA, S = Ontario, L = Ottawa, CN = ..."<br><br>*Revoked certificate:*<br><br>logver=604099335 timestamp=1676749765 devname devname="FGT-1101E" devid="FG10E1TB199002362" vd="root" date=2023-02-18 time=19:49:25 eventtime=1676749765324798321 tz="-0800" logid="0100038410" type="event" subtype="system" level="information" logdesc="SSL connection failed" dstip=192.168.77.37 dstport=4510 reason="ssl_connect() failed: 218529960 (error:0D0680A8:asn1 encoding routines:asn1_check_tlen:wrong tag)" action="connect" status="failure" msg="SSL connect to 192.168.232.108 has failed." |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | *Invalid EC parameters:*<br><br>logver=604099335 timestamp=1676873655 devname devname="FGT-1101E" devid="FG10E1TB199002362" vd="root" date=2023-02-20 time=06:14:15 eventtime=1676873655324798321 tz="-0800" logid="0100038410" type="event" subtype="system" level="error" logdesc="SSL connection failed" dstip=N/A dstport=24608 reason="certificate use explicit EC parameter" action="info" status="failure" msg="Certificate is invalid, subject: C = CA, S = Ontario, L = Ottawa, CN = ..."<br><br>*In addition, various other specific failures associated with TLS certificate validation are found in audit messages for FCS_TLSC_EXT.1.* |
| | Unsuccessful attempt to validate a certificate (IPsec peer) | Reason for failure | *The "reason for failure" is found in either in the "logdesc", "msg" or the "reason" fields.*<br><br>*Invalid certificate:*<br><br>logver=604099335 timestamp=1676917898 devname="FGT-3301E" devid="FG33E1T919900081" vd="root" date=2023-02-20 time=18:31:38 eventtime=1676917898324798321 tz="-0800" logid="0101037124" type="event" subtype="vpn" level="error" logdesc="IPsec phase 1 error" msg="IPsec phase 1 error" action="negotiate" remip=192.168.108.134 locip=192.168.181.18 remport=19661 locport=23103 outintf="port1" cookies="1fb9189bc91653d1/1ac3960cf472c53b" user="N/A" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="vpn_example_tunnel" status="negotiate_error" reason="invalid certificate" peer_notif="NOT-APPLICABLE"<br><br>*Expired certificate:* |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | logver=604099392 timestamp=1677043026 devname="FGT-3301E" devid="FG33E1T919900081" vd="root" date=2023-02-22 time=05:17:06 eventtime=1677043026324798321 tz="-0800" logid="0101037124" type="event" subtype="vpn" level="error" logdesc="IPsec phase 1 error" msg="IPsec phase 1 error" action="negotiate" remip=192.168.224.61 locip=192.168.73.17 remport=2016 locport=17556 outintf="port1" cookies="6631ed3b8b6617b6/a56264945cc3fa72" user="C = CA, S = Ontario, L = Ottawa, CN = ..." group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="vpn_example_tunnel" status="negotiate_error" reason="invalid certificate (expired)"<br><br>*Revoked certificate:*<br><br>logver=604099392 timestamp=1676752719 devname="FGT-3301E" devid="FG33E1T919900081" vd="root" date=2023-02-18 time=20:38:39 eventtime=1676752719324798321 tz="-0800" logid="0101037124" type="event" subtype="vpn" level="error" logdesc="IPsec phase 1 error" msg="IPsec phase 1 error" action="negotiate" remip=192.168.236.85 locip=192.168.16.74 remport=18705 locport=2243 outintf="port1" cookies="cb1b12b7035ac183/90be167a0fdf71a6" user="C = CA, S = Ontario, L = Ottawa, CN = ..." group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="vpn_example_tunnel" status="negotiate_error" reason="invalid certificate (revoked)"<br><br>*Invalid signature:*<br><br>logver=604099335 timestamp=1676764921 devname="FGT-3601E" devid="FG36E1TB18900045" vd="root" date=2023-02-19 time=00:02:01 eventtime=1676764921324798321 tz="-0800" logid="0101037124" type="event" subtype="vpn" level="error" logdesc="IPsec phase 1 error" msg="IPsec phase 1 error" action="negotiate" remip=192.168.217.105 locip=192.168.76.209 remport=32142 locport=15417 outintf="port1" cookies="6c7ecbf7d194ccf2/720dc6b209844eaf" user="C = CA, S = Ontario, L = Ottawa, CN = ..." group="N/A" useralt="N/A" xauthuser="N/A" |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | xauthgroup="N/A" assignip=N/A vpntunnel="vpn_example_tunnel" status="negotiate_error" reason="invalid certificate signature"<br><br>*Invalid EC parameters:*<br><br>logver=604099335 timestamp=1676740501 devname="FGT-3601E" devid="FG36E1TB18900045" vd="root" date=2023-02-18 time=17:15:01 eventtime=1676740501324798321 tz="-0800" logid="0101037124" type="event" subtype="vpn" level="error" logdesc="IPsec phase 1 error" msg="IPsec phase 1 error" action="negotiate" remip=192.168.75.26 locip=192.168.75.9 remport=15294 locport=13464 outintf="port1" cookies="9b62382e4ccd1d89/5477af1fcf13a727" user="C = CA, S = Ontario, L = Ottawa, CN = ..." group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="vpn_example_tunnel" status="negotiate_error" reason="invalid certificate EC param(s)" |
| | Any addition of trust anchors in the TOE's trust store | Identification of certificates added as trust anchor in the TOE's trust store | *The "reason for failure" is found in either in the "logdesc", "msg" or the "reason" fields.*<br><br>*Successfully adding a trust anchor:*<br><br>logver=604099148 timestamp=1676874413 devname="FGT-101F" devid="FG101FTK19004320" vd="root" date=2023-02-20 time=06:26:53 eventtime=1676874413324798321 tz="-0800" logid="0100044547" type="event" subtype="system" level="information" logdesc="Object attribute configured" user="admin" ui="ssh(192.168.174.183)" action="Add" cfgtid=16174250 cfgpath="vpn.certificate.ca" cfgobj="Local_cert_name" cfgattr="CA_Cert_Name" msg="Add vpn.certificate.ca CA_Cert_Name"<br><br>*Invalid basic constraints on load:*<br><br>logver=604099335 timestamp=1676995703 devname="FGT-101F" devid="FG101FTK19004320" vd="root" date=2023-02-21 time=16:08:23 eventtime=1676995703324798321 tz="-0800" logid="0101041989" type="event" |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | subtype="vpn" level="information" logdesc="Certificate error" action="info" cert-type="CA" status="error" name="N/A" method="N/A" msg="Certificate is invalid. no basic constraints"<br><br>*Various forms of invalid CA certificate on load:*<br><br>logver=604099335 timestamp=1676701992 devname="FGT-101F" devid="FG101FTK19004320" vd="root" date=2023-02-18 time=06:33:12 eventtime=1676701992324798321 tz="-0800" logid="0100038410" type="event" subtype="system" level="error" logdesc="SSL connection failed" dstip=N/A dstport=14827 reason="invalid CA certificate" action="info" status="failure" msg="Certificate is invalid, subject: C = CA, S = Ontario, L = Ottawa, CN = ..."<br><br>logver=604099335 timestamp=1677006553 devname="FGT-101F" devid="FG101FTK19004320" vd="root" date=2023-02-21 time=19:09:13 eventtime=1677006553324798321 tz="-0800" logid="0101041989" type="event" subtype="vpn" level="information" logdesc="Certificate error" action="info" cert-type="CA" status="error" name="N/A" method="N/A" msg="Certificate is invalid. not a CA cert" |
| | Any replacement of trust anchors in the TOE's trust store (if applicable) | Identification of certificates replaced as trust anchor in the TOE's trust store (if applicable) | *Trust anchors can only be added or removed.* |
| | Any removal of trust anchors in the TOE's trust store | Identification of certificates removed as trust anchor in the TOE's trust store | logver=604099148 timestamp=1676812507 devname="FGT-201E" devid="FG201E4Q16901982" vd="root" date=2023-02-19 time=13:15:07 eventtime=1676812507324798321 tz="-0800" logid="0100044545" type="event" subtype="system" level="information" logdesc="Object configured" user="admin" ui="GUI(192.168.94.129)" action="Delete" cfgtid=16162998 cfgpath="vpn.certificate.ca" cfgobj=" CA_Cert_Name" msg="Delete vpn.certificate.ca CA_Cert_Name" |

Firewall Audit Messages

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| FFW_RUL_EXT.1 | Application of rules configured with the 'log' operation | Source and destination addresses<br>Source and destination ports<br>Transport Layer Protocol<br>TOE Interface | *The source address is the "srcip" and the destination is the "dstip" except where clarified in the Common Criteria TechNote.*<br>*The source port is the "srcport" and the destination is the "dstport" for port-based protocols except where clarified in the Common Criteria TechNote.*<br>*The transport layer protocol is the "proto" field.*<br>*The TOE interface will be contained in the "srcintf", "dstintf" or "intf" except where clarified in the Common Criteria TechNote.*<br>*Accepted traffic – note in this case, the "policyid" and the action="accept" indicates the policy was hit and subsequently permitted.*<br>logver=604099392 timestamp=1676782278 devname="FGT-3980E" devid="FG39E8T018901869" vd="root" date=2023-02-19 time=04:51:18 eventtime=1676782278324798321 tz="-0800" logid="0000000013" type="traffic" subtype="forward" level="notice" srcip=192.168.96.13 identifier=12962 srcintf="port1" srcintfrole="undefined" dstip=192.168.131.214 dstintf="port3" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved" sessionid=5228 proto=6 action="accept" policyid=48 policytype="policy" poluuid="74102305-2ea8-7cb2-4c98-88963f486149" service="Service_Name" trandisp="noop" duration=60 sentbyte=3932 rcvdbyte=2627 sentpkt=53 rcvdpkt=17 appcat="unscanned"<br>*Deny due to invalid flags in the TCP state machine:* |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | logver=604099335 timestamp=1676919509 devname="FGT-3980E" devid="FG39E8T018901869" vd="root" date=2023-02-20 time=18:58:29 eventtime=1676919509324798321 tz="-0800" logid="0000000007" type="traffic" subtype="forward" level="warning" srcip=192.168.32.33 srcport=13200 srcintf="port1" srcintfrole="undefined" dstip=192.168.233.77 dstport=12289 dstintf="port3" dstintfrole="undefined" srcuuid="086cc073-20e0-1ea8-bd5f-f8cf90838c1a" dstuuid="f4ac620d-a600-0ec2-a144-123fc49a0e38" srccountry="Reserved" dstcountry="Reserved" sessionid=6319 proto=6 action="deny" policyid=98 policytype="policy" poluuid="f68d5860-f54a-9969-096e-c6eeed6500d9" service="Service_Name" trandisp="noop" duration=1 sentbyte=0 rcvdbyte=0 sentpkt=1 rcvdpkt=0 msg="psh or urg in state syn_recv, suspicious"<br><br>*Invalid session match:*<br><br>logver=604099335 timestamp=1677100633 devname="FGT-3980E" devid="FG39E8T018901869" vd="root" date=2023-02-22 time=21:17:13 eventtime=1677100633324798321 tz="-0800" logid="0000000007" type="traffic" subtype="forward" level="warning" srcip=192.168.177.148 srcport=1228 srcintf="port1" srcintfrole="undefined" dstip=192.168.116.112 dstport=4464 dstintf="port3" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved" proto=6 action="deny" policyid=0 policytype="policy" service="Service_Name" trandisp="noop" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=1 rcvdpkt=0 msg="no session matched"<br><br>*TCP syn flooding:*<br><br>logver=604099392 timestamp= devname="FGT-3980E" devid="FG39E8T018901869" vd="root" date=2023-02-19 time=02:08:50 eventtime=1676772530324798321 tz="-0800" logid="0720018432" type="utm" subtype="anomaly" eventtype="anomaly" level="alert" severity="critical" srcip=192.168.30.127 srccountry="Reserved" dstip=192.168.198.78 srcintf="port1" srcintfrole="undefined" sessionid=4411 action="clear_session" proto=6 service="Service_Name" count=35 attack="tcp_syn_flood" srcport=12415 dstport=6779 attackid=100663396 policyid=58 |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | policytype="DoS-policy" ref="http://www.fortinet.com/ids/VID100663396" msg="anomaly: tcp_syn_flood, 35 > 100" crscore=50 craction=4096 crlevel="critical"<br><br>*Deny due to specific policy – note in this case, the "policyid" and the action="deny" indicates the policy was hit and subsequently denied. The "default" deny rule is policy 0:*<br><br>logver=604099148 timestamp=1676713409 devname="FortiGate-3980E" devid="FG39E8T018901869" vd="root" date=2023-02-18 time=09:43:29 eventtime=1676713409324798321 tz="-0800" logid="0000000013" type="traffic" subtype="forward" level="notice" srcip=192.168.25.11 identifier=13206 srcintf="port1" srcintfrole="undefined" dstip=192.168.67.31 dstintf="port3" dstintfrole="undefined" srcuuid="ece91a31-9086-d336-3b11-4167440bef33" dstuuid="29b21ddc-fc81-7d4b-a271-64305fa9b1da" srccountry="Reserved" dstcountry="Reserved" sessionid=8654 proto=6 action="deny" policyid=45 policytype="policy" poluuid="60580ede-e3be-8942-5f13-e0e1ca5807cd" service="Service_Name" trandisp="noop" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0 appcat="unscanned" crscore=30 craction=131072 crlevel="high"<br><br>*Various denials due to invalid fragments:*<br><br>logver=604099148 timestamp=1676952426 devname="FortiGate-3980E" devid="FG39E8T018901869" vd="root" date=2023-02-21 time=04:07:06 eventtime=1676952426324798321 tz="-0800" logid="0000000007" type="traffic" subtype="forward" level="warning" srcip=192.168.112.30 srcport=23596 srcintf="port1" srcintfrole="undefined" dstip=192.168.15.229 dstport=9282 dstintf="port3" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved" proto=6 action="deny" policyid=0 policytype="policy" service="Service_Name" trandisp="noop" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0 msg="fragment check error, drop"<br><br>logver=604099148 timestamp=1677105369 devname="FortiGate-3980E" devid="FG39E8T018901869" vd="root" date=2023-02-22 time=22:36:09 |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | eventtime=1677105369324798321 tz="-0800" logid="0000000007" type="traffic" subtype="forward" level="warning" srcip=2001::3086:542d:9723:4cef srcport=31918 srcintf="port1" srcintfrole="undefined" dstip=2001::7e61:4843:0ccc:19a3 dstport=8825 dstintf="port3" dstintfrole="undefined" proto=6 action="deny" policyid=0 policytype="policy" service="Service_Name" dstcountry="Reserved" srccountry="Reserved" trandisp="noop" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0 msg="fragment is too long, drop"<br><br>logver=604099148 timestamp=1676918023 devname="FortiGate-3980E" devid="FG39E8T018901869" vd="root" date=2023-02-20 time=18:33:43 eventtime=1676918023324798321 tz="-0800" logid="0000000007" type="traffic" subtype="forward" level="warning" srcip=192.168.142.237 srcport=26786 srcintf="port1" srcintfrole="undefined" dstip=192.168.51.93 dstport=12217 dstintf="port3" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved" proto=6 action="deny" policyid=0 policytype="policy" service="Service_Name" trandisp="noop" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0 msg="fragments expired, drop"<br><br>*Various denials due to invalid general and specific addresses:*<br><br>logver=604099148 timestamp=1676974686 devname="FortiGate-3980E" devid="FG39E8T018901869" vd="root" date=2023-02-21 time=10:18:06 eventtime=1676974686324798321 tz="-0800" logid="0000000007" type="traffic" subtype="forward" level="warning" srcip=2001::620a:80e9:13f8:a810 srcport=1798 srcintf="port1" srcintfrole="undefined" dstport=17129 dstintf="port3" dstintfrole="undefined" proto=6 action="deny" policyid=0 policytype="policy" service="Service_Name" srccountry="Reserved" trandisp="noop" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0 msg="invalid dest address, drop"<br><br>logver=604099148 timestamp=1676843959 devname="FortiGate-3980E" devid="FG39E8T018901869" vd="root" date=2023-02-19 time=21:59:19 eventtime=1676843959324798321 tz="-0800" logid="0000000007" type="traffic" |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | subtype="forward" level="warning" srcport=27730 srcintf="port1" srcintfrole="undefined" dstip=2001::1b62:84af:b5a7:e24e dstport=6650 dstintf="port3" dstintfrole="undefined" proto=6 action="deny" policyid=0 policytype="policy" service="Service_Name" dstcountry="Reserved" trandisp="noop" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0 msg="invalid source address, drop"<br><br>logver=604099148 timestamp=1676980177 devname="FortiGate-3980E" devid="FG39E8T018901869" vd="root" date=2023-02-21 time=11:49:37 eventtime=1676980177324798321 tz="-0800" logid="0000000007" type="traffic" subtype="forward" level="warning" srcip=2001::024c:83eb:f9d6:bf24 srcport=27373 srcintf="port1" srcintfrole="undefined" dstip=2001::3613:c7b8:f289:ec54 dstport=5878 dstintf="port3" dstintfrole="undefined" proto=6 action="deny" policyid=0 policytype="policy" service="Service_Name" dstcountry="Reserved" trandisp="noop" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0 msg="src address 2001::024c:83eb:f9d6:bf24 is multicast address, drop"<br><br>*Various denials due to path-check and reverse-path-check failures:*<br><br>logver=604099148 timestamp=1677047040 devname="FortiGate-3980E" devid="FG39E8T018901869" vd="root" date=2023-02-22 time=06:24:00 eventtime=1677047040324798321 tz="-0800" logid="0000000007" type="traffic" subtype="forward" level="warning" srcip=192.168.221.233 srcport=7231 srcintf="port1" srcintfrole="undefined" dstip=192.168.251.228 dstport=29968 dstintf="port3" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved" sessionid=8889 proto=6 action="deny" policyid=0 policytype="policy" service="Service_Name" trandisp="noop" duration=103 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0 msg="blocked by forwarding policy (port1->port3), drop"<br><br>logver=604099148 timestamp=1677052111 devname="FortiGate-3980E" devid="FG39E8T018901869" vd="root" date=2023-02-22 time=07:48:31 eventtime=1677052111324798321 tz="-0800" logid="0000000007" type="traffic" subtype="forward" level="warning" srcip=192.168.251.44 srcport=11906 srcintf="port1" |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | srcintfrole="undefined" dstip=192.168.237.43 dstport=4390 dstintf="port3" dstintfrole="undefined" srcuuid="06b3636e-7431-2d56-f770-c3fba930d584" dstuuid="f281f13f-41fb-b8c3-925d-c38945379ef9" srccountry="Reserved" dstcountry="Reserved" sessionid=5881 proto=6 action="deny" policyid=23 policytype="policy" poluuid="943e9b85-0008-2417-828c-d53b9e54a1e3" service="Service_Name" trandisp="noop" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0 msg="Denied by forward policy check (policy 23)"<br><br>logver=604099148 timestamp=1676883501 devname="FortiGate-3980E " devid="FG39E8T018901869" vd="root" date=2023-02-20 time=08:58:21 eventtime=1676883501324798321 tz="-0800" logid="0000000007" type="traffic" subtype="forward" level="warning" srcip=192.168.210.111 srcport=113 srcintf="port1" srcintfrole="undefined" dstip=192.168.248.249 dstport=27179 dstintf="port3" dstintfrole="undefined" srccountry="Reserved" sessionid=9763 proto=6 action="deny" policyid=0 policytype="policy" service="Service_Name" trandisp="noop" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0 msg="path check fail(bad dst),drop"<br><br>logver=604099148 timestamp=1676683603 devname="FortiGate-3980E" devid="FG39E8T018901869" vd="root" date=2023-02-18 time=01:26:43 eventtime=1676683603324798321 tz="-0800" logid="0000000007" type="traffic" subtype="forward" level="warning" srcip=192.168.222.158 srcport=7257 srcintf="port1" srcintfrole="undefined" dstip=192.168.172.47 dstport=15666 dstintf="port3" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved" sessionid=36 proto=6 action="deny" policyid=0 policytype="policy" service="Service_Name" trandisp="noop" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0 msg="reverse path check fail(bad src),drop"<br><br>*Various denials due to invalid IP options:*<br><br>logver=604099148 timestamp=1676928697 devname="FortiGate-3980E" devid="FG39E8T018901869" vd="root" date=2023-02-20 time=21:31:37 eventtime=1676928697324798321 tz="-0800" logid="0000000007" type="traffic" |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | subtype="forward" level="warning" srcip=192.168.6.65 srcport=25564 srcintf="port1" srcintfrole="undefined" dstip=192.168.135.219 dstport=30754 dstintf="port3" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved" sessionid=68 proto=6 action="deny" policyid=0 policytype="policy" service="Service_Name" trandisp="noop" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0 msg="record route ip option, drop"<br><br>logver=604099148 timestamp=1676948935 devname="FortiGate-3980E" devid="FG39E8T018901869" vd="root" date=2023-02-21 time=03:08:55 eventtime=1676948935324798321 tz="-0800" logid="0000000007" type="traffic" subtype="forward" level="warning" srcip=192.168.238.213 srcport=20807 srcintf="port1" srcintfrole="undefined" dstip=192.168.99.44 dstport=22737 dstintf="port3" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved" sessionid=860 proto=6 action="deny" policyid=0 policytype="policy" service="Service_Name" trandisp="noop" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 rcvdpkt=0 msg="source route ip option, drop" |
| FMT_SMF.1/FFW | All management activities of TSF data (including creation, modification and deletion of firewall rules). | None. | *Creating firewall rules:*<br><br>logver=604099148 timestamp=1676711055 devname=" FortiGate-61F" devid="FGT61FTK19006185" vd="root" date=2023-02-18 time=09:04:15 eventtime=1676711055324798321 tz="-0800" logid="0100044547" type="event" subtype="system" level="information" logdesc="Object attribute configured" user="admin" ui="console" action="Add" cfgtid=16134853 cfgpath="firewall.policy" cfgobj="2" cfgattr="status[disable srcintf[port1]dstintf[port2]srcaddr[all dstaddr[all srcaddr6[]dstaddr6[]action[accept]schedule[always]service[all]" msg="Add firewall.policy 2"<br><br>*Deleting firewall rules:*<br><br>logver=604099148 timestamp=1676687714 devname="FortiGate-61F" devid="FGT61FTK20060302" vd="root" date=2023-02-18 time=02:35:14 |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | eventtime=1676687714324798321 tz="-0800" logid="0100044545" type="event" subtype="system" level="information" logdesc="Object configured" user="admin" ui="ssh(192.168.84.242)" action="Delete" cfgtid=16175140 cfgpath="firewall.policy" cfgobj="89" msg="Delete firewall.policy 89"<br><br>*Editing firewall rules:*<br><br>logver=604099148 timestamp=1676950632 devname="FortiGate-61F" devid="FGT61FTK20060302" vd="root" date=2023-02-21 time=03:37:12 eventtime=1676950632324798321 tz="-0800" logid="0100044547" type="event" subtype="system" level="information" logdesc="Object attribute configured" user="admin" ui="ssh(192.168.94.171)" action="Edit" cfgtid=16153339 cfgpath="firewall.policy" cfgobj="97" cfgattr="action[deny->accept]" msg="Edit firewall.policy 97"<br><br>*Changing the priority of policy rules:*<br><br>logver=604099148 timestamp=1676794983 devname="FortiGate-61F" devid="FGT61FTK20060302" vd="root" date=2023-02-19 time=08:23:03 eventtime=1676794983324798321 tz="-0800" logid="0100044545" type="event" subtype="system" level="information" logdesc="Object configured" user="admin" ui="ssh(192.168.72.6)" action="Move" cfgtid=16146312 cfgpath="firewall.policy" cfgobj="16" msg="Move firewall.policy 123 to 124"<br><br>*Creating custom firewall objects (services, IP address groups, etc.) – the actual object will be denoted by the "cfgpath" and the modification data will be found in the "cfgattr".*<br><br>logver=604099148 timestamp=1676964324 devname="FortiGate-61F" devid="FGT61FTK20060302" vd="root" date=2023-02-21 time=07:25:24 eventtime=1676964324324798321 tz="-0800" logid="0100044547" type="event" subtype="system" level="information" logdesc="Object attribute configured" user="admin" ui="ssh(192.168.165.123)" action="Edit" cfgtid=16151981 |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | cfgpath="firewall.service.custom" cfgobj="Service_name" cfgattr="icmpcode[0->255]" msg="Edit firewall.service.custom Service_name"<br><br>logver=604099148 timestamp=1676732848 devname="FortiGate-61F" devid="FGT61FTK20060302" vd="root" date=2023-02-18 time=15:07:28 eventtime=1676732848324798321 tz="-0800" logid="0100044547" type="event" subtype="system" level="information" logdesc="Object attribute configured" user="admin" ui="ssh(192.168.163.244)" action="Add" cfgtid=16165989 cfgpath="firewall.address6" cfgobj="src_addr_allow" cfgattr="type[ipprefix]ip6[2345:425:2CA1:0000:0000:567:5673:23b5]" msg="Add firewall.address6 Address_Object"<br><br>logver=604099392 timestamp=1676922583 devname="FortiGate-61F" devid="FGT61FTK19006185" vd="root" date=2023-02-20 time=19:49:43 eventtime=1676922583324798321 tz="-0800" logid="0100044547" type="event" subtype="system" level="information" logdesc="Object attribute configured" user="admin" ui="ssh(192.168.16.155)" action="Add" cfgtid=16156269 cfgpath="firewall.DoS-policy6" cfgobj="35"cfgattr="name[DOS]interface[wan1]srcaddr[all]dstaddr[all]service[ALL]anomaly:sctp_dst_session[log[disable->enable]threshold[5000->5000]]anomaly:sctp_src_session[log[disable->enable]threshold[5000->5000]]anomaly:sctp_scan[log[disable->enable]threshold[1000->1000]]anomaly:sctp_flood[log[disable->enable]threshold[2000->2000]]anomaly:ip_dst_session[log[disable->enable]threshold[5000->5000]]anomaly:ip_src_session[log[disable->enable]threshold[5000->5000]]anomaly:icmp_dst_session[log[disable->enable]threshold[1000->1000]]anomaly:icmp_src_session[log[disable->enable]threshold[300->300]]anomaly:icmp_sweep[log[disable->enable]threshold[100->100]]anomaly:icmp_flood[log[disable->enable]threshold[250->250]]anomaly:udp_dst_session[log[disable->enable]threshold[5000->5000]]anomaly:udp_src_session[log[disable->enable]threshold[5000->5000]]anomaly:udp_scan[log[disable->enable]threshold[2000- |

Log Message Examples

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | >2000]]anomaly:udp_flood[log[disable->enable]threshold[2000->2000]]anomaly:tcp_dst_session[log[disable->enable]threshold[5000->5000]]" msg="Add firewall.DoS-policy6 35" |

VPN Gateway PP-Module Audit Messages

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| FCS_IPSEC_EXT.1 | Session Establishment with peer | Entire packet contents of packets transmitted/received during session establishment | *Session establishment occurs during IKEv1 phase 1/phase 2 and IKEv2 INIT_SA and CHILD_SA.*<br><br>*Negotiating phase 1/INIT_SA:*<br><br>logver=604099148 timestamp=1676878969 devname="FortiGate-81F" devid="FGT81FTK20091997" vd="root" date=2023-02-20 time=07:42:49 eventtime=1676878969324798321 tz="-0800" logid="0101037120" type="event" subtype="vpn" level="notice" logdesc="Negotiate IPsec phase 1" msg="negotiate IPsec phase 1" action="negotiate" remip=192.168.252.99 locip=192.168.233.28 remport=8098 locport=22956 outintf="port1" cookies="7dc4a7cc86cafcf3/84146237a817675b" user="N/A" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="vpn_example_tunnel" status="success" result="N/A" peer_notif="N/A"<br><br>*Completed phase 1/INIT_SA:*<br><br>logver=604099148 timestamp=1676776434 devname="FortiGate-81F" devid="FGT81FTK20091997" vd="root" date=2023-02-19 time=03:13:54 eventtime=1676776434324798321 tz="-0800" logid="0101037127" type="event" subtype="vpn" level="notice" logdesc="Progress IPsec phase 1" msg="progress IPsec phase 1" action="negotiate" remip=192.168.50.96 locip=192.168.36.201 remport=29485 locport=18148 outintf="port1" cookies="5b61e0f87ed73348/3f29b6e0b3b21852" |

| Requirement | Auditable Events | Additional Audit Record Contents | Example |
|---|---|---|---|
| | | | user="N/A" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="vpn_example_tunnel" status="success" init="local" exch="AUTH" dir="inbound" role="initiator" result="DONE" version="IKEv2"<br><br>*Negotiating phase 2/CHILD_SA:*<br><br>logver=604099148 timestamp=1677067318 devname="FortiGate-81F" devid="FGT81FTK20091997" vd="root" date=2023-02-22 time=12:01:58 eventtime=1677067318324798321 tz="-0800" logid="0101037122" type="event" subtype="vpn" level="notice" logdesc="Negotiate IPsec phase 2" msg="negotiate IPsec phase 2" action="negotiate" remip=192.168.100.215 locip=192.168.74.10 remport=293 locport=1109 outintf="port1" cookies="de8cf7f27a3cb6b7/952a311522a81e90" user="N/A" group="N/A" useralt="N/A" xauthuser="N/A" xauthgroup="N/A" assignip=N/A vpntunnel="vpn_example_tunnel" status="success" role="initiator" esptransform="ESP_AES" espauth="N/A"<br><br>*Complete packet contents of packets transmitted/received during session establishment can be viewed by creating a packet capture of the traffic. Refer to the Common Criteria Technote for more information.* |
| FPF_RUL_EXT.1 | Application of rules configured with the 'log' operation | Source and destination addresses<br><br>Source and destination ports<br><br>Transport Layer Protocol | *Please refer to FWF_RUL_EXT.1* |

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results 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 certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. 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.