UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549

FORM SD

SPECIALIZED DISCLOSURE REPORT

FORTINET, INC.
(Exact Name of Registrant as Specified in its Charter)

Delaware	**001-34511**	**77-0560389**
(State or other jurisdiction of incorporation or organization)	**(Commission File Number)**	**(IRS Employer Identification No.)**

899 Kifer Road, Sunnyvale, California	**94086**
(Address of Principal Executive Offices)	**(Zip Code)**

John Whittle
(408) 235-7700
(Name and telephone number, including area code, of the person to contact in connection with this report.)

Not Applicable
(Former Name or Former Address, if Changed Since Last Report)

Check the appropriate box below to indicate the rule pursuant to which this form is being filed, and provide the period to which the information in this form applies:

☒ Rule 13p-1 under the Securities Exchange Act (17 CFR 240.13p-1) for the reporting period January 1 to December 31, 2013

Item 1.01. Conflict Minerals Disclosure and Report.

Conflict Minerals Disclosure

A copy of the Conflict Minerals Report of Fortinet, Inc. ("Fortinet") for the reporting period January 1 to December 31, 2013 is filed as Exhibit 1.02 to this specialized disclosure report on Form SD and is also available at Fortinet's website at http://investor.fortinet.com/sec.cfm.

Item 1.02. Exhibit.

Fortinet has filed, as an exhibit to this Form SD, a Conflict Minerals Report as required by Item 1.01 of this Form.

Item 2.01. Exhibit.

Exhibit Number	Description of Document
1.02	Fortinet, Inc. Conflict Minerals Report for the reporting period January 1 to December 31, 2013.

SIGNATURES

Pursuant to the requirements of the Securities Exchange Act of 1934, the registrant has duly caused this report to be signed on its behalf by the duly authorized undersigned.

FORTINET, INC.

Dated: May 30, 2014

By: /s/ John Whittle
Name: John Whittle
Title: Vice President of Corporate Development and Strategic Alliances, General Counsel

EXHIBIT INDEX

Exhibit Number	Description of Document
1.02	Fortinet, Inc. Conflict Minerals Report for the reporting period January 1 to December 31, 2013.

Fortinet, Inc.
Conflict Minerals Report
For The Reporting Period January 1 to December 31, 2013

This Conflict Minerals Report ("CMR") has been prepared by Fortinet, Inc. (herein referred to, alternatively, as "Fortinet," "we" and "our"). This CMR for the reporting period January 1 to December 31, 2013 is presented to comply with the final conflict minerals implementing rules ("Final Rules") promulgated by the Securities and Exchange Commission ("SEC"), as modified by SEC guidance issued on April 29, 2014 and the SEC order issued on May 2, 2014. The Final Rules were adopted by the SEC to implement reporting and disclosure requirements related to conflict minerals as directed by the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 as codified in Section 13(p) of the Securities Exchange Act of 1934. The Final Rules impose certain reporting obligations on SEC registrants whose manufactured products contain conflict minerals that are necessary to the functionality or production of their products. "Conflict minerals" are currently defined by the SEC as cassiterite, columbite-tantalite (coltan), gold, wolframite, or their derivatives, which the SEC has currently limited to tin, tantalum, tungsten and gold.

To comply with the Final Rules, we conducted due diligence on the origin, source and chain of custody of the conflict minerals that were necessary to the functionality or production of the products that we manufactured or contracted to manufacture to ascertain whether these conflict minerals originated in the Democratic Republic of Congo or an adjoining country (collectively, "Covered Countries") and financed or benefited armed groups (as defined in Section 1, Item 1.01(d)(2) of Form SD) in any of these countries.

Pursuant to SEC guidance issued April 29, 2014 and the SEC order issued May 2, 2014, Fortinet is not required to describe any of its products as "DRC conflict free" (as defined in Section 1, Item 1.01(d)(4) of Form SD), "DRC conflict undeterminable" (as defined in Section 1, Item 1.01(d)(5) of Form SD) or "having not been found to be 'DRC conflict free,'" and therefore makes no conclusion in this regard in the report presented herein. Furthermore, given that Fortinet has not voluntarily elected to describe any of its products as "DRC conflict free," an independent private sector audit of the report presented herein has not been conducted.

I. Company Overview

Fortinet provides high performance network security solutions that are designed to address the fundamental problems of an increasingly bandwidth-intensive network environment and a more sophisticated information technology threat landscape.

II. Product Overview

Fortinet provides high performance network security solutions, which enable broad, integrated and high performance protection against advanced security threats while simplifying the IT security infrastructure for enterprises, service providers and governmental entities worldwide. Since inception through March 31, 2014, Fortinet had shipped over1,500,000 appliances via more than 20,000 channel partners to more than 190,000 end-customers worldwide, including a majority of the 2013 Fortune Global 100.

Fortinet's core product line, comprised of FortiGate physical and virtual appliances, ships with a set of broad security and networking capabilities, including firewall, virtual private network (VPN), application control, antivirus, intrusion prevention, Web filtering, vulnerability management, anti-spam, wireless controller, wide area network (WAN) acceleration and native internet protocol version 6 (IPv6) support functionality. Customers select the functions or combination of functions that best meet their specific security requirements — whether that be a high-speed data center firewall (DCFW) at the network core, a next-generation firewall (NGFW) at the edge, or a broad unified threat management (UTM) solution at branch sites. Fortinet derives a substantial majority of product sales from our FortiGate appliances, which range from the FortiGate-20 to -100 series, designed for small

businesses, FortiGate-200 to -800 series for mid-sized enterprises, to the FortiGate-1000 to -5000 series for large enterprises, telecommunications carriers, and service providers. Fortinet's network security platform also includes our FortiGuard security subscription services, which end-customers can subscribe to in order to obtain access to dynamic updates to intrusion prevention, application control, anti-malware, Web filtering, and anti-spam functionality. End-customers can also choose to purchase FortiCare technical support services for our products. End-customers also often use FortiManager and FortiAnalyzer products in conjunction with a FortiGate deployment to provide centralized management, analysis and reporting capabilities. Fortinet complements our core FortiGate product line with other appliances and software that offer additional protection from security threats to other critical areas of the enterprise, such as protection from advanced persistent threats (APTs), messaging, Web application firewalls, databases, protection against distributed denial of service attacks (DDoS) and endpoint security for employee computers and mobile devices. Sales of these complementary products and related services represent less than 10% of our total revenue.

III. Supply Chain Overview

Fortinet outsources the manufacture of its security hardware appliance products to a variety of contract manufacturers and original design manufacturers. Fortinet submits purchase orders to its contract manufacturers that describe the type and quantities of products to be manufactured, the delivery date and other delivery terms. Fortinet's proprietary FortiASICs, which are incorporated in certain of Fortinet's hardware appliance products, are fabricated by contract manufacturers. The components included in Fortinet's products are sourced from various suppliers by Fortinet or more frequently by Fortinet's contract manufacturers. Some of the components important to Fortinet's business, including specific types of central processing units, network chips, and solid-state drives (silicon-based storage device), are available from a limited or sole source of supply. For purposes of this CMR, references to our "products" refer to our hardware appliance products, and references to our "suppliers" refer to our product suppliers.

IV. Conflict Minerals Analysis and Reasonable Country of Origin Inquiry

Based upon a review of our products and our reasonable country of origin inquiry ("RCOI"), we have concluded that:

- our products contain conflict minerals that are necessary to the production or functionality of such products; and
- we are unable to determine whether the conflict minerals present in our products originate in the Covered Countries.

V. Design of Due Diligence Measures

Fortinet designed its due diligence with respect to the source and chain of custody of the conflict minerals contained in its products based on the five-step framework set forth in the Second Edition of the Organisation for Economic Co-operation and Development's Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas and the supplements thereto (the "OECD Guidance").

VI. Due Diligence Measures Performed by Fortinet

Fortinet performed the following due diligence measures in accordance with the OECD Guidance and the Final Rules:

OECD Guidance Step #1: Establish Strong Company Management Systems

- In May 2014, Fortinet adopted a Conflict Minerals Policy (the "Conflict Minerals Policy") that sets forth (i) its commitment to complying with the Final Rules, (ii) its expectations of its suppliers regarding supporting Fortinet's compliance activities, and (iii) its policies and practices with respect to the engagement of suppliers and the implementation of risk mitigation measures. The Conflict Minerals Policy can be found on our website at www.fortinet.com/aboutus/environmental_relations.html.

- The implementation of Fortinet's RCOI and the conducting of due diligence on the source and chain of custody of Fortinet's necessary conflict minerals are managed by Fortinet's legal and operations departments. The Audit Committee (the "Audit Committee") of Fortinet's Board of Directors provides oversight and review with respect to these processes.
- The legal and operations staff responsible for conflict minerals compliance (i) have received training regarding conflict minerals compliance and (ii) are required to be familiar with Fortinet's Conflict Minerals Policy and with Fortinet's conflict minerals-related processes.
- Material conflict minerals-related records, including completed CMRTs (as defined below), will be maintained by Fortinet for a period of five (5) years from the date of creation.
- Fortinet's Conflict Minerals Policy will be made available to existing suppliers, and Fortinet intends to make available the Conflict Minerals Policy to new suppliers. In addition, in August 2013, a conflict minerals compliance provision (the "Conflict Minerals Contractual Provision") was added to Fortinet's form manufacturing purchase agreement requiring suppliers to comply with the Conflict Minerals Policy, and Fortinet intends to request that the Conflict Minerals Contractual Provision be incorporated into new manufacturing purchase agreements.
- Interested parties can report improper activities in violation of the Conflict Minerals Policy via email at environmental_relations@fortinet.com. This email address is published on Fortinet's website at www.fortinet.com/aboutus/environmental_relations.html.

OECD Guidance Step #2: Identify and Assess Risk in the Supply Chain

- Fortinet has requested that its suppliers complete in full the Electronic Industry Citizenship Coalition/Global e-Sustainability Initiative Conflict Minerals Reporting Template (the "CMRT"). The CMRT is designed to request from suppliers sufficient information regarding its suppliers' practices with respect to the sourcing of conflict minerals to enable it to comply with its requirements under the Final Rules.
- Fortinet's legal and operations departments manage the collection of information reported on the CMRT by Fortinet's suppliers.

OECD Guidance Step #3: Design and Implement a Strategy to Respond to Identified Risks

- If, on the basis of areas of concern that are identified as a result of either (i) the supplier data acquisition or engagement processes or (ii) the receipt of information from other sources, Fortinet determines that a supplier is sourcing conflict minerals that are directly or indirectly financing or benefiting armed groups, Fortinet intends to enforce the Conflict Minerals Policy by means of a series of escalations.
- Such escalations may range from prompt engagement with the supplier to resolve the sourcing issue, to requiring such supplier to implement a risk management plan (which plan may involve, as appropriate, remedial action up to and including disengagement from upstream suppliers), to disengagement by Fortinet from the applicable supplier.

OECD Guidance Step #4: Carry Out Independent Third-Party Audit of Supply Chain Due Diligence at Identified Points in the Supply Chain

Given that we do not have a direct relationship with the smelters and refiners that process the conflict minerals that are present in our products, we rely on the Conflict-Free Sourcing Initiative (the "CFSI") to conduct third-party audits of smelters and refineries.

OECD Guidance Step #5: Report on Supply Chain Due Diligence

As required by the Final Rules, we have filed a Form SD and this Conflict Minerals Report as an exhibit thereto for the 2013 calendar year reporting period. The Form SD and Conflict Minerals Report are also available on our website at http://investor.fortinet.com/sec.cfm.

VII. Smelters or Refineries Identified

As a result of Fortinet's reasonable country of origin inquiry, 48 suppliers, representing approximately 93% of our suppliers, provided completed CMRTs to Fortinet. Fortinet's suppliers identified the names of approximately 757 smelters and refineries from which they source conflict minerals (including country locations of each smelter or refinery). Of those smelters and refineries, approximately 73 smelters and refineries, or approximately 9.6%, have been certified by the CFSI's Conflict-Free Smelter Program (the "CFSP"). The remainder of the smelters and refineries are not, at this time, certified by the CFSP. With respect to these smelters and refineries, although we were not able to determine the mines of origin of the conflict minerals sourced from such smelters and refineries, we were able to determine their country locations. Attached as Addendum A to this CMR is a list of such country locations, grouped according to the specific conflict mineral processed by such smelters or refineries.

VIII. Steps to Mitigate Risk

Fortinet intends to take the following steps to mitigate the risk that conflict minerals benefit armed groups:

- Continue to engage with suppliers to obtain complete CMRTs; and
- Encourage the development of supplier capabilities to perform conflict-minerals related due diligence by the implementation of risk mitigation measures, as appropriate.

FORWARD LOOKING STATEMENTS

Statements relating to due diligence improvements, Fortinet's intentions, and other statements herein are forward-looking in nature and are based on Fortinet's management's current expectations or beliefs. These forward-looking statements are not a guarantee of performance and are subject to a number of uncertainties and other factors that may be outside of Fortinet's control and which could cause actual events to differ materially from those expressed or implied by the statements made herein, and Fortinet reserves the right to change its processes and policies related to conflict minerals.

DOCUMENTS INCORPORATED BY REFERENCE

Unless otherwise expressly stated herein, any documents, third party materials or references to websites (including Fortinet's) are not incorporated by reference in, or considered to be a part of this CMR, unless expressly incorporated by reference herein.

Addendum A

Non-CFSP-Certified Smelter and Refinery Country Locations by Mineral

Mineral	Country Locations
Tin	ARGENTINA
	BELGIUM
	BOLIVIA
	BRAZIL
	CANADA
	CHINA
	CZECH REPUBLIC
	EGYPT
	ETHIOPIA
	FRANCE
	GERMANY
	HONG KONG
	INDONESIA
	ITALY
	JAPAN
	KOREA
	MALAYSIA
	MEXICO
	PERU
	PHILIPPINES
	POLAND
	RUSSIAN FEDERATION
	SINGAPORE
	SLOVAKIA (SLOVAK REPUBLIC)
	SWITZERLAND
	TAIWAN
	THAILAND
	UNITED KINGDOM
	UNITED STATES
	VIETNAM
	VIRGIN ISLANDS (U.S.)
Tantalum	AUSTRIA
	BRAZIL
	CANADA
	CHINA
	ETHIOPIA
	GERMANY
	INDIA

	INDONESIA
	JAPAN
	KAZAKHSTAN
	KOREA
	MEXICO
	RUSSIAN FEDERATION
	SOUTH AFRICA
	SWITZERLAND
	THAILAND
	UNITED KINGDOM
	UNITED STATES
Tungsten	AMERICAN SAMOA
	AUSTRIA
	BELGIUM
	BRAZIL
	CANADA
	CHINA
	COLOMBIA
	GERMANY
	HONG KONG
	ISRAEL
	JAPAN
	KOREA
	NETHERLANDS
	RUSSIAN FEDERATION
	SWEDEN
	TAIWAN
	UNITED STATES
	VIETNAM
Gold	ALGERIA
	AUSTRALIA
	BELGIUM
	BOLIVIA
	BRAZIL
	CANADA
	CHILE
	CHINA
	FRANCE
	GERMANY
	HONG KONG
	INDIA

INDONESIA
ITALY
JAPAN
KAZAKHSTAN
KOREA
KYRGYZSTAN
MALAYSIA
MEXICO
NETHERLANDS
PERU
PHILIPPINES
RUSSIAN FEDERATION
SAUDI ARABIA
SINGAPORE
SOUTH AFRICA
SPAIN
SWEDEN
SWITZERLAND
TAIWAN
THAILAND
TURKEY
UNITED KINGDOM
UNITED STATES
UZBEKISTAN