UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
15/790,303	10/23/2017	**Laxmikant Gunda**	N422	4869

152691 7590 04/10/2020

Setter Roche LLP
1860 Blake Street
Suite 100
Denver, CO 80202

EXAMINER
POPHAM, JEFFREY D

ART UNIT	PAPER NUMBER
2432	

NOTIFICATION DATE	DELIVERY MODE
04/10/2020	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ipadmin@vmware.com
uspto@setterroche.com

Office Action Summary	Application No. 15/790,303	Applicant(s) Gunda et al.	
	Examiner Jeffrey D Popham	Art Unit 2432	AIA (FITF) Status Yes

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTHS FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☑ Responsive to communication(s) filed on 2/4/2020.

☐ A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.

2a)☐ This action is **FINAL.** 2b) ☑ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims*

5) ☑ Claim(s) 1-20 is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6) ☐ Claim(s) _____ is/are allowed.

7) ☑ Claim(s) 1-20 is/are rejected.

8) ☐ Claim(s) _____ is/are objected to.

9) ☐ Claim(s) _____ are subject to restriction and/or election requirement

* If any claims have been determined allowable, you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to **PPHfeedback@uspto.gov.**

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☑ The drawing(s) filed on 10/23/2017 is/are: a)☑ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

a)☐ All b)☐ Some** c)☐ None of the:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

** See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Information Disclosure Statement(s) (PTO/SB/08a and/or PTO/SB/08b) Paper No(s)/Mail Date _____.

3) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date _____.

4) ☐ Other: _____.

Remarks

Claims 1-20 are pending.

Notice of Pre-AIA or AIA Status

The present application, filed on or after March 16, 2013, is being examined under the first inventor to file provisions of the AIA.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 2/4/2020 has been entered.

Response to Arguments

Applicant's arguments filed 2/4/2020 have been fully considered but they are not persuasive.

Applicant alleges "Mohanty discloses that 'identification module 104 may identify the data center application in a variety of ways' and then lists examples of how identification module 104 may identify the data center application (see Mohanty, ¶ 0036). None of the examples provided in Mohanty describe querying virtual machines to identify first applications thereon and determining that the virtual machines implement

the data center application. Instead, Mohanty may query a data center platform to identify a set of systems that include the data center application or may query the data center application itself to identify those systems (see Mohanty, ¶¶ 0004, 0045). Even if the systems were virtual machines, Mohanty fails to disclose that the systems themselves are ever queried to identify first applications executing thereon, as is required by claim 1." Mohanty does disclose that the data center may be made up of multiple virtual machines, for example, in paragraph 31 ("The term 'data center,' as used herein, may refer to any collection of computing systems, real or virtual, for example, a data center may include a software-defined data center composed of virtual machines and/or a virtual network"). When viewing this in combination with Mohanty's disclosure of querying the data center to determine applications executing thereon, one will readily find querying of the virtual machines that make up the data center in order to determine which are running which applications. Therefore, Mohanty discloses the querying and determining being argued by Applicant.

Applicant continues by alleging "Moreover, in both of the examples above, Mohanty would need to know of the existence of the data center application prior to querying the data center platform or the data center application itself for information about the data center application (i.e., for information identifying the systems that include the data center application). In contrast, querying virtual machines to identify first applications executing thereon does not require the existence of a multi-tier application be known prior to the query, which further differentiates the querying step of claim 1 from the queries performed by Mohanty." This is not actually claimed. The claims do not prohibit knowledge of a multi-tier application prior to the querying step. In

response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-20 are rejected under 35 U.S.C. 101 because the claimed invention is directed to an abstract idea without significantly more. The claim(s) recite(s) computing element administration steps that comprise a mental process. This judicial exception is not integrated into a practical application because all of the steps could be performed by a human. The claim(s) does/do not include additional elements that are sufficient to amount to significantly more than the judicial exception because the claims at best include generic computer components that perform well understood, routine, and conventional processing.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103 which forms the basis for all obviousness rejections set forth in this Office action:

> A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have

> been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 6-11, and 16-20 are rejected under 35 U.S.C. 103 as being unpatentable over Mohanty (U.S. Patent Application Publication 2016/0191463) in view of Yin (U.S. Patent Application Publication 2015/0372977).

Regarding Claim 1,

Mohanty discloses a method of micro-segmenting virtual computing elements based on applications running thereon, the method comprising:

Querying a plurality of virtual machines to identify first applications executing thereon (Exemplary Citations: for example, Abstract, Paragraphs 4, 24, 26, 29, 31, 34, 36, 37, 45, 50 and associated figures; identifying applications by querying data center, which is comprised of virtual machines, for example);

Based on the first applications, determining that the plurality of virtual machines implement one or more multi-tier applications, wherein each of the multi-tier applications comprises two or more of the first applications (Exemplary Citations: for example, Abstract, Paragraphs 24, 26, 29, 31, 34-52 and associated figures; tiered applications, for example);

Maintaining information about the one or more multi-tier applications, wherein the information at least indicates a security group for each virtual machine of the plurality of virtual machines and an application tier for each of the first applications (Exemplary Citations: for example, Abstract, Paragraphs 24, 26, 29, 31, 34-52 and associated figures; tiers, groups, categories, sub-categories, metadata, tags, etc., as examples);

Identifying communication traffic flows between virtual machines of the plurality of virtual machines (Exemplary Citations: for example, Abstract, Paragraphs 35, 39-46, 48, 50, 51, 64-68 and associated figures; communication paths, traffic between VMs, traffic between physical machines, internal traffic, external traffic, cluster traffic, etc., as examples);

Identifying with which multi-tier application of the one or more multi-tier applications each of the first applications is associated based on the communication traffic flows and the information (Exemplary Citations: for example, Abstract, Paragraphs 24, 26, 29, 31, 34-52, 64-68 and associated figures; determining applications and tiers that flows are associated with, for example);

Identifying one or more removable traffic flows of the communication traffic flows based, at least in part, on the information, wherein each of the removable traffic flows comprises one of the communication traffic flows that the information indicates should not be allowed to occur (Exemplary Citations: for example, Abstract, Paragraphs 35, 39-46, 48, 50, 51, 64-68 and associated figures; firewall monitors, intercepts, inspects traffic to determine whether traffic is good or suspicious, for example); and

Blocking the one or more removable traffic flows (Exemplary Citations: for example, Abstract, Paragraphs 35, 39-46, 48, 50, 51, 64-68 and associated figures; blocking certain paths, such as suspicious traffic

from one group to another group that may contain a virus, blocking network traffic between systems in the same network, etc., as examples);

But does not appear to explicitly disclose that the communications traffic flows are communication traffic flows that occur, and are allowed to occur, during an amount of time.

Yin, however, discloses that the communications traffic flows are communication traffic flows that occur, and are allowed to occur, during an amount of time (Exemplary Citations: for example, Abstract, Paragraphs 31, 48-52, 55-60, 63, 64, 67, 68, 72-76, and associated figures; traffic flows that occur could be, for example, applications sending traffic for a certain user, which are allowed to occur, but then could have their action modified (e.g., to block or limit access for an application for a certain user, group, department, or the like) after an administrator views a report regarding such traffic flows, for example). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention, which is before any effective filing date of the claimed invention, to incorporate the firewall policy management techniques of Yin into the network security system of Mohanty in order to allow the system to block or limit access for certain users/applications/devices/groups/etc. after it is determined that their current communication abilities should be modified, provide an efficient and user-friendly mechanism for firewall policy creation and modification, and/or allow users to more easily modify firewall policies.

Regarding Claim 11,

Claim 11 is a system claim that corresponds to method claim 1 and is rejected for the same reasons.

Regarding Claim 6,

Mohanty as modified by Yin discloses the method of claim 1, in addition, Mohanty discloses that blocking the one or more removable traffic flows comprises implementing one or more firewall rules that block the one or more removable traffic flows (Exemplary Citations: for example, Abstract, Paragraphs 35, 39-46, 48, 50, 51, 64-68 and associated figures).

Regarding Claim 16,

Claim 16 is a system claim that corresponds to method claim 6 and is rejected for the same reasons.

Regarding Claim 7,

Mohanty as modified by Yin discloses the method of claim 1, in addition, Mohanty discloses that each of multi-tier applications comprises three tiers, wherein the three tiers include a web tier, application tier, and database tier (Exemplary Citations: for example, Abstract, Paragraphs 45, 60 and associated figures).

Regarding Claim 17,

Claim 17 is a system claim that corresponds to method claim 7 and is rejected for the same reasons.

Regarding Claim 8,

Mohanty as modified by Yin discloses the method of claim 7, in addition, Mohanty discloses that the one or more removable traffic flows

comprise traffic flows other than those between the web tier and the application tier, the application tier and the database tier, and an external system and the web tier (Exemplary Citations: for example, Abstract, Paragraphs 35, 39-46, 48, 50, 51, 64-68 and associated figures).

Regarding Claim 18,

Claim 18 is a system claim that corresponds to method claim 8 and is rejected for the same reasons.

Regarding Claim 9,

Mohanty as modified by Yin discloses the method of claim 1, in addition, Mohanty discloses that the communication traffic flows are identified from network traffic monitored by one or more hypervisors hosting the plurality of virtual machines (Exemplary Citations: for example, Paragraphs 27-31, 35, 90, 94, and associated figures; any identifying of flows, where all portions of the system may be on virtual machines, where a virtual machine is abstracted from hardware by a hypervisor, for example).

Regarding Claim 19,

Claim 19 is a system claim that corresponds to method claim 9 and is rejected for the same reasons.

Regarding Claim 10,

Mohanty as modified by Yin discloses the method of claim 1, in addition, Mohanty discloses that the information further includes an identifier for each of the one or more multi-tier applications (Exemplary

Citations: for example, Abstract, Paragraphs 24, 26, 29, 31, 34-52 and associated figures).

Regarding Claim 20,

Claim 20 is a system claim that corresponds to method claim 10 and is rejected for the same reasons.

Claims 2-5 and 12-15 are rejected under 35 U.S.C. 103 as being unpatentable over Mohanty in view of Yin and Brooks (U.S. Patent Application Publication 2005/0262554).

Regarding Claim 2,

Mohanty as modified by Yin discloses the method of claim 1, in addition, Mohanty discloses presenting the one or more removable traffic flows to a user (Exemplary Citations: for example, Abstract, Paragraphs 35, 39-46, 48, 50, 51, 64-68 and associated figures; presenting the above to a server, program, system, network, etc., as examples);

Receiving confirmation from the user that the removable traffic should be removed (Exemplary Citations: for example, Abstract, Paragraphs 35, 39-46, 48, 50, 51, 64-68 and associated figures; any confirmation from the above that the traffic should be removed (e.g., if traffic is suspicious), for example); and

Wherein blocking the removable traffic flows occurs in response to the confirmation (Exemplary Citations: for example, Abstract, Paragraphs 35, 39-46, 48, 50, 51, 64-68 and associated figures).

Brooks also discloses presenting the one or more removable traffic flows to a user (Exemplary Citations: for example, Abstract, Paragraphs 41-47, 68-71, and associated figures; displaying a graphical representation of a network with devices, connections/communications, rules, etc., as examples);

Receiving confirmation from the user that the removable traffic should be removed (Exemplary Citations: for example, Abstract, Paragraphs 41-47, 68-71, and associated figures; user requested change and/or final request after various changes, for example); and

Wherein blocking the removable traffic flows occurs in response to the confirmation (Exemplary Citations: for example, Abstract, Paragraphs 41-47, 68-71, and associated figures). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention, which is before any effective filing date of the claimed invention, to incorporate the network visualization techniques of Brooks into the network security system of Mohanty as modified by Yin in order to allow users to easily view the network with all of its devices, connections, rules, and the like, make it easier for a user to understand what is within the network when making manual updates/decisions, and/or to increase security in the system.

Regarding Claim 12,

Claim 12 is a system claim that corresponds to method claim 2 and is rejected for the same reasons.

Regarding Claim 3,

Mohanty as modified by Yin and Brooks discloses the method of claim 2, in addition, Brooks discloses that presenting the removable traffic flow comprises:

Presenting a graphical display that visually groups virtual machines of the plurality of virtual machines into respective application tiers and respective security groups (Exemplary Citations: for example, Abstract, Paragraphs 41-47, 68-71, and associated figures; the network visual display will display all systems, VMs, rules, tiers, and the like, of the combination, for example); and

Displaying the communication traffic flows between the virtual machines (Exemplary Citations: for example, Abstract, Paragraphs 41-47, 68-71, and associated figures).

Regarding Claim 13,

Claim 13 is a system claim that corresponds to method claim 3 and is rejected for the same reasons.

Regarding Claim 4,

Mohanty as modified by Yin and Brooks discloses the method of claim 3, in addition, Mohanty discloses labelling the application tiers and the security groups (Exemplary Citations: for example, Abstract, Paragraphs 24, 26, 29, 31, 34-52 and associated figures; tiers and groups have labels, for example); and

Brooks discloses that the graphical display labels the application tiers and the security groups (Exemplary Citations: for example, Abstract, Paragraphs 24, 26, 29, 31, 34-52 and associated figures; everything is labeled in the graphics, for example).

Regarding Claim 14,

Claim 14 is a system claim that corresponds to method claim 4 and is rejected for the same reasons.

Regarding Claim 5,

Mohanty as modified by Yin and Brooks discloses the method of claim 3, in addition, Mohanty discloses that presenting the one or more removable traffic flows further comprises highlighting the removable traffic flows of the communication traffic flows (Exemplary Citations: for example, Abstract, Paragraphs 35, 39-46, 48, 50, 51, 64-68 and associated figures; removable traffic flows are suspicious, for example); and

Brooks discloses that presenting the one or more removable traffic flows further comprises highlighting the removable traffic flows of the displayed communication traffic flows (Exemplary Citations: for example, Abstract, Paragraphs 24, 26, 29, 31, 34-52 and associated figures; flows are shown in the display and new flows will show anew, for example).

Regarding Claim 15,

Claim 15 is a system claim that corresponds to method claim 5 and is rejected for the same reasons.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey D Popham whose telephone number is (571)272-7215. The examiner can normally be reached on Monday through Friday 9:00-5:30.

Examiner interviews are available via telephone, in-person, and video conferencing using a USPTO supplied web-based collaboration tool. To schedule an interview, applicant is encouraged to use the USPTO Automated Interview Request (AIR) at http://www.uspto.gov/interviewpractice.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey Nickerson can be reached on (469) 295-9235. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Jeffrey D. Popham/
Primary Examiner, Art Unit 2432

REMARKS

Claims 1-20 are pending in the application. Claims 1-20 stand rejected. Claims 1, 2, 6, 11, 12, and 16 are amended herein. No new matter has been added. The Applicant respectfully requests consideration of the following remarks and allowance of the claims.

Telephone Interview Summary

The Applicant submits this telephone interview summary to meet the requirements of 37 C.F.R. § 1.133(b), and according to the requirements listed in MPEP § 713.04. A telephone interview was conducted on June 25, 2020. The parties involved were Examiner Jeffrey Popham and the Applicant's Attorney Brian Arment. No exhibits were discussed. The parties discussed adding computing components to the claims to overcome the § 101 rejections thereof. The parties also discussed how the intended scope claim 1 differs from the Mohanty reference. No agreement was reached and no other pertinent matters were discussed.

35 U.S.C. § 101 Rejections

Claims 1-20 stand rejected under 35 U.S.C. § 101 as directed to non-statutory subject matter. Claims 1 and 11 have been amended to overcome the rejections.

In particular, consistent with the discussion during the interview, claims 1 and 11 now recite physical computing systems/processors on which the virtual machines execute. Moreover, claims 1 and 11 describe hypervisors that host the virtual machines and describe how elements within those hypervisors (i.e., the firewall and the traffic monitor) are used to affect a high-level network traffic policy by blocking removable traffic flows that run afoul of that policy. The PTO's October 2019 update to its subject matter eligibility guidance indicates that, even if claims 1 and 11 were otherwise considered abstract, a practical application of the claimed limitations is enough to avoid triggering a judicial exception. Since the limitations of claim 1 and 11 result in the blocking of removable traffic flows that were otherwise allowed to occur, the limitations clearly have a practical application with respect to the network communications between the recited virtual machines.

Based on the preceding remarks, the Applicant respectfully requests withdrawal of the § 101 rejections at the Examiner's earliest convenience.

35 U.S.C. § 103 Rejections

Claims 1, 6-11, and 16-20 stand rejected under 35 U.S.C. § 103 as unpatentable over U.S. Patent Application Publication No. 2016/0191463 to Mohanty in view of U.S. Patent Application Publication No. 2015/0372977 to Yin. The Applicant respectfully traverses the rejection for at least the following reasons.

Claim 1 now recites that removable traffic flows, which are identified and then blocked, comprise one of the communication traffic flows that a high-level network traffic policy indicates should not be allowed to occur. The high-level network traffic policy defines, based on security groups, which of the two or more tiers communications should be allowed to flow between and which of the two or more multi-tier applications communications should be allowed to flow between.

Before the removable traffic flows can be identified, claim 1 requires that other steps occur that, essentially, determine whether the high-level traffic policy of claim 1 applies to the virtual machines. That is, the steps determine whether the communications between the virtual machines are communications between first applications that operate at tiers of one or more multi-tier applications and which particular multi-tier application each of the first application operates. Without such prior determinations, it would be unknown whether the high-level policy even applies to a traffic flow between any two of the virtual machines, much less whether the traffic flow is allowed by the high-level policy. Mohanty does not perform steps in the order required by claim 1 to identify removable traffic flows.

Specifically, claim 1 requires querying a plurality of virtual machines to identify first applications executing thereon. After the first application are identified, claim 1 determines that the virtual machines implement one or more multi-tier applications that include the first applications. Then, tiers for each of the first applications are identified and, after the tier identification, claim 1 determines with which of the multi-tier applications each of the first applications is associated based on the traffic flows and the tier for each application.

Mohanty does not follow the above sequence of steps to determine information about its data center application. Instead, Mohanty queries a data center platform to obtain information about data center applications and the systems upon which those applications are executing (see Mohanty, ¶ 0045). Even if the data center application was a multi-tier application, Mohanty would merely be informed by the data center platform about which systems make up the multi-

tier application (see *Id.*). There is also no teaching in Mohanty that the data center platform performs the sequence of steps from claim 1 to determine the provided information about the data center application.

Yin was merely used by the final Office action to disclose communication traffic flows that occur and are allowed to occur. Yin fails to overcome Mohanty's above-discussed deficiencies.

In view of the above remarks, the Applicant respectfully submits that Mohanty and Yin, alone and in combination, fail to teach or suggest all the limitations of claim 1. Claim 1 is, therefore, allowable over the art of record and such indication is requested at the Examiner's earliest convenience.

Independent claim 11 recites limitations similar to those of claim 1 and is, therefore, allowable over the art of record for at least the same reasons.

The Applicant refrains from discussing the remaining dependent claims in view of their dependence upon otherwise allowable independent claims.

CONCLUSION

Based upon the above remarks, the Applicant submits that the claims in their present form are allowable.

The Applicant believes no fees are due with respect to this filing. However, should the Office determine additional fees are necessary, the Office is hereby requested to contact the undersigned to arrange for payment of the applicable fees.

Respectfully submitted,

/Brian L. Arment/

SIGNATURE OF PRACTITIONER
Brian L. Arment, Reg. No. 64,134
Setter Roche LLP
Telephone: (720) 432-2031
E-mail: brian@setterroche.com

Correspondence address:

CUSTOMER NO. 152691

Setter Roche LLP
14694 Orchard Parkway
Building A, Suite 200
Westminster, CO 80023

APPENDIX A

Claims as amended but without markup for clarity:

1. (CURRENTLY AMENDED) A method of micro-segmenting virtual computing elements based on applications running thereon, the method comprising:

in a micro-segmentation system implemented using one or more physical processors:

querying a plurality of virtual machines to identify first applications executing thereon;

after the first applications are identified, determining that the plurality of virtual machines implement one or more multi-tier applications based on the first applications, wherein each of the multi-tier applications comprises two or more of the first applications;

after determining that the plurality of virtual machines implement the one or more multi-tier applications, determining in which tier of two or more tiers each of the first applications operate for the one or more multi-tier applications;

identifying communication traffic flows that occur, and are allowed to occur, during an amount of time between virtual machines of the plurality of virtual machines through one or more hypervisors executing on physical computing systems to host the plurality of virtual machines, wherein a communication traffic monitor in the one or more hypervisors is employed by the micro-segmentation system to perform the identifying of the communication traffic flows;

after determining the tier in which each of the first applications operate, identifying with which multi-tier application of the one or more multi-tier applications each of the first applications is associated based on the communication traffic flows and the tier in which each of the first applications operates;

after identifying with which multi-tier application of the one or more multi-tier applications each of the first applications is associated, identifying one or more removable traffic flows of the communication traffic flows, wherein each of the removable traffic flows comprises one of the communication traffic flows that a high-level network traffic policy indicates should not be allowed to occur, wherein the high-level network traffic policy defines, based on security groups, which of the two or more tiers communications should be allowed to flow between and which of the two or more multi-tier applications communications should be allowed to flow between; and

directing a firewall in the one or more hypervisors to block the one or more removable traffic flows.

2. (CURRENTLY AMENDED) The method of claim 1, further comprising:

presenting the one or more removable traffic flows to a user;

receiving confirmation from the user that the removable traffic flows should be removed; and

wherein ~~blocking~~ directing the firewall to block the one or more removable traffic flows occurs in response to the confirmation.

3. (ORIGINAL) The method of claim 2, wherein presenting the removable traffic flows comprises:

presenting a graphical display that visually groups virtual machines of the plurality of virtual machines into respective application tiers and respective security groups; and

displaying the communication traffic flows between the virtual machines.

4. (ORIGINAL) The method of claim 3, wherein the graphical display labels the application tiers and the security groups.

5. (PREVIOUSLY PRESENTED) The method of claim 3, wherein presenting the one or more removable traffic flows further comprises:

highlighting the removable traffic flows of the displayed communication traffic flows.

6. (CURRENTLY AMENDED) The method of claim 1, wherein ~~blocking~~ directing the firewall to block the one or more removable traffic flows comprises implementing one or more firewall rules that block the one or more removable traffic flows.

7. (ORIGINAL) The method of claim 1 wherein each of multi-tier applications comprises three tiers, wherein the three tiers include a web tier, application tier, and database tier.

8. (ORIGINAL) The method of claim 7, wherein the one or more removable traffic flows

comprise traffic flows other than those between the web tier and the application tier, the application tier and the database tier, and an external system and the web tier.

9. (PREVIOUSLY PRESENTED) The method of claim 1, wherein the communication traffic flows are identified from network traffic monitored by one or more hypervisors hosting the plurality of virtual machines.

10. (CANCELED)

11. (CURRENTLY AMENDED) A system for micro-segmenting virtual computing elements based on applications running thereon, the system comprising:

one or more computer readable storage media;

a processing system, comprising one or more central processing unit cores, operatively coupled with the one or more computer readable storage media; and

program instructions stored on the one or more computer readable storage media that, when read and executed by the processing system, direct the processing system to:

query a plurality of virtual machines to identify first applications executing thereon;

after the first applications are identified, determine that the plurality of virtual machines implement one or more multi-tier applications based on the first applications, wherein each of the multi-tier applications comprises two or more of the first applications;

after the plurality of virtual machines are determined to implement the one or more multi-tier applications, determine in which tier of two or more tiers each of the first applications operate for the one or more multi-tier applications;

identify communication traffic flows that occur, and are allowed to occur, during an amount of time between virtual machines of the plurality of virtual machines through one or more hypervisors executing on physical computing systems to host the plurality of virtual machines, wherein a communication traffic monitor in the one or more hypervisors is employed by the micro-segmentation system to perform the identifying of the communication traffic flows;

after the tier in which each of the first applications operate is determined, identify with which multi-tier application of the one or more multi-tier applications each of the first applications is associated based on the communication traffic flows and the tier in which each of the first applications operates;

after with which multi-tier application of the one or more multi-tier applications each of the first applications is associated are identified, identify one or more removable traffic flows of the communication traffic flows, wherein each of the removable traffic flows comprises one of the communication traffic flows that a high-level network traffic policy indicates should not be allowed to occur, wherein the high-level network traffic

policy defines, based on security groups, which of the two or more tiers communications should be allowed to flow between and which of the two or more multi-tier applications communications should be allowed to flow between; and

direct a firewall in the one or more hypervisors to block the one or more removable traffic flows.

12. (CURRENTLY AMENDED) The system of claim 11, wherein the program instructions further direct the processing system to:

present the one or more removable traffic flows to a user;

receive confirmation from the user that the removable traffic flows should be removed; and

wherein the program instructions direct the processing system to direct the firewall to block the one or more removable traffic flows in response to the confirmation.

13. (ORIGINAL) The system of claim 12, wherein to present the removable traffic flows the program instructions direct the processing system to at least:

present a graphical display that visually groups virtual machines of the plurality of virtual machines into respective application tiers and respective security groups; and

display the communication traffic flows between the virtual machines.

14. (ORIGINAL) The system of claim 13, wherein the graphical display labels the application tiers and the security groups.

15. (PREVIOUSLY PRESENTED) The system of claim 13, wherein to present the one or more removable traffic flows the program instructions further direct the processing system to at least:

highlight the removable traffic flows of the displayed communication traffic flows.

16. (CURRENTLY AMENDED) The system of claim 11, wherein to direct the firewall to block the one or more removable traffic flows the program instructions direct the processing system to at least:

implement one or more firewall rules that block the one or more removable traffic flows.

17. (ORIGINAL) The system of claim 11 wherein each of multi-tier applications comprises three tiers, wherein the three tiers include a web tier, application tier, and database tier.

18. (ORIGINAL) The system of claim 17, wherein the one or more removable traffic flows comprise traffic flows other than those between the web tier and the application tier, the application tier and the database tier, and an external system and the web tier.

19. (PREVIOUSLY PRESENTED) The system of claim 11, wherein the communication traffic flows are identified from network traffic monitored by one or more hypervisors hosting the plurality of virtual machines.

20. (CANCELED)

In the Claims:

1. (CURRENTLY AMENDED) A method of micro-segmenting virtual computing elements based on applications running thereon, the method comprising:

in a micro-segmentation system implemented using one or more physical processors:

querying a plurality of virtual machines to identify first applications executing thereon;

~~based on the~~ after the first applications are identified, determining that the plurality of virtual machines implement one or more multi-tier applications based on the first applications, wherein each of the multi-tier applications comprises two or more of the first applications;

after determining that the plurality of virtual machines implement the one or more multi-tier applications, determining in which tier of two or more tiers each of the first applications operate for the one or more multi-tier applications;

~~maintaining information about the one or more multi-tier applications, wherein the information at least indicates a security group for each virtual machine of the plurality of virtual machines and an application tier for each of the first applications;~~

identifying communication traffic flows that occur, and are allowed to occur, during an amount of time between virtual machines of the plurality of virtual machines through one or more hypervisors executing on physical computing systems to host the plurality of virtual machines, wherein a communication traffic monitor in the one or more hypervisors is employed by the micro-segmentation system to perform the identifying of the communication traffic flows;

after determining the tier in which each of the first applications operate, identifying with which multi-tier application of the one or more multi-tier applications each of the first applications is associated based on the communication traffic flows and the tier in which each of the first applications operates ~~and information~~;

after identifying with which multi-tier application of the one or more multi-tier applications each of the first applications is associated, identifying one or more removable traffic flows of the communication traffic flows ~~based, at least in part, on the information~~, wherein each of the removable traffic flows comprises one of the communication traffic flows that ~~the information~~ a high-level network traffic policy indicates should not be allowed to occur, wherein the high-level network traffic policy defines, based on security groups, which of the two or more tiers communications should be allowed to flow between and which of the two or more multi-tier

applications communications should be allowed to flow between; and

~~blocking~~ directing a firewall in the one or more hypervisors to block the one or more removable traffic flows.

2. (CURRENTLY AMENDED) The method of claim 1, further comprising:

presenting the one or more removable traffic flows to a user;

receiving confirmation from the user that the removable traffic flows should be removed; and

wherein ~~blocking~~ directing the firewall to block the one or more removable traffic flows occurs in response to the confirmation.

3. (ORIGINAL) The method of claim 2, wherein presenting the removable traffic flows comprises:

presenting a graphical display that visually groups virtual machines of the plurality of virtual machines into respective application tiers and respective security groups; and

displaying the communication traffic flows between the virtual machines.

4. (ORIGINAL) The method of claim 3, wherein the graphical display labels the application tiers and the security groups.

5. (PREVIOUSLY PRESENTED) The method of claim 3, wherein presenting the one or more removable traffic flows further comprises:

highlighting the removable traffic flows of the displayed communication traffic flows.

6. (CURRENTLY AMENDED) The method of claim 1, wherein ~~blocking~~ directing the firewall to block the one or more removable traffic flows comprises implementing one or more firewall rules that block the one or more removable traffic flows.

7. (ORIGINAL) The method of claim 1 wherein each of multi-tier applications comprises three tiers, wherein the three tiers include a web tier, application tier, and database tier.

8. (ORIGINAL) The method of claim 7, wherein the one or more removable traffic flows comprise traffic flows other than those between the web tier and the application tier, the application tier and the database tier, and an external system and the web tier.

9. (PREVIOUSLY PRESENTED) The method of claim 1, wherein the communication traffic flows are identified from network traffic monitored by one or more hypervisors hosting the plurality of virtual machines.

10. (CANCELED)

11. (CURRENTLY AMENDED) A system for micro-segmenting virtual computing elements based on applications running thereon, the system comprising:

one or more computer readable storage media;

a processing system, comprising one or more central processing unit cores, operatively coupled with the one or more computer readable storage media; and

program instructions stored on the one or more computer readable storage media that, when read and executed by the processing system, direct the processing system to:

query a plurality of virtual machines to identify first applications executing thereon;

~~based on the~~ after the first applications are identified, determine that the plurality of virtual machines implement one or more multi-tier applications based on the first applications, wherein each of the multi-tier applications comprises two or more of the first applications;

after the plurality of virtual machines are determined to implement the one or more multi-tier applications, determine in which tier of two or more tiers each of the first applications operate for the one or more multi-tier applications;

~~maintain information about the one or more multi-tier applications, wherein the information at least indicates a security group for each virtual machine of the plurality of virtual machines and an application tier for each of the first applications;~~

identify communication traffic flows that occur, and are allowed to occur, during an amount of time between virtual machines of the plurality of virtual machines through one or more hypervisors executing on physical computing systems to host the plurality of virtual machines, wherein a communication traffic monitor in the one or more hypervisors is employed by the micro-segmentation system to perform the identifying of the communication traffic flows;

after the tier in which each of the first applications operate is determined, identify with which multi-tier application of the one or more multi-tier applications each of the first applications is associated based on the communication traffic flows and the tier in which each of the first applications operates ~~and information~~;

after with which multi-tier application of the one or more multi-tier applications each of the first applications is associated are identified, identify one or more removable

traffic flows of the communication traffic flows ~~based, at least in part, on the information~~, wherein each of the removable traffic flows comprises one of the communication traffic flows that ~~the information~~ a high-level network traffic policy indicates should not be allowed to occur, wherein the high-level network traffic policy defines, based on security groups, which of the two or more tiers communications should be allowed to flow between and which of the two or more multi-tier applications communications should be allowed to flow between; and

direct a firewall in the one or more hypervisors to block the one or more removable traffic flows.

12. (CURRENTLY AMENDED) The system of claim 11, wherein the program instructions further direct the processing system to:

present the one or more removable traffic flows to a user;

receive confirmation from the user that the removable traffic flows should be removed; and

wherein the program instructions direct the processing system to direct the firewall to block the one or more removable traffic flows in response to the confirmation.

13. (ORIGINAL) The system of claim 12, wherein to present the removable traffic flows the program instructions direct the processing system to at least:

present a graphical display that visually groups virtual machines of the plurality of virtual machines into respective application tiers and respective security groups; and

display the communication traffic flows between the virtual machines.

14. (ORIGINAL) The system of claim 13, wherein the graphical display labels the application tiers and the security groups.

15. (PREVIOUSLY PRESENTED) The system of claim 13, wherein to present the one or more removable traffic flows the program instructions further direct the processing system to at least:

highlight the removable traffic flows of the displayed communication traffic flows.

16. (CURRENTLY AMENDED) The system of claim 11, wherein to direct the firewall to block the one or more removable traffic flows the program instructions direct the processing system to at least:

implement one or more firewall rules that block the one or more removable traffic flows.

17. (ORIGINAL) The system of claim 11 wherein each of multi-tier applications comprises three tiers, wherein the three tiers include a web tier, application tier, and database tier.

18. (ORIGINAL) The system of claim 17, wherein the one or more removable traffic flows comprise traffic flows other than those between the web tier and the application tier, the application tier and the database tier, and an external system and the web tier.

19. (PREVIOUSLY PRESENTED) The system of claim 11, wherein the communication traffic flows are identified from network traffic monitored by one or more hypervisors hosting the plurality of virtual machines.

20. (CANCELED)