ivanti

Ivanti Neurons for Service Mapping

Security Overview

Table of Contents

Information in this document is for information purposes only and is not a commitment, promise, or legal obligation to deliver any material, code, or functionality and should not be relied upon in making a purchasing decision.

1. Introduction

The Ivanti Neurons for Service Mapping solution is built on top of a secure and robust application platform, hosted on Amazon Web Services (AWS) cloud. AWS delivers a scalable cloud computing platform with high availability and dependability. AWS' physical and operational security processes are well defined and are designed to meet any compliance requirements. Along with AWS security, Ivanti Neurons for Service Mapping has its own application security measures to protect data in transit and at rest.

1.1 Shared Security Model

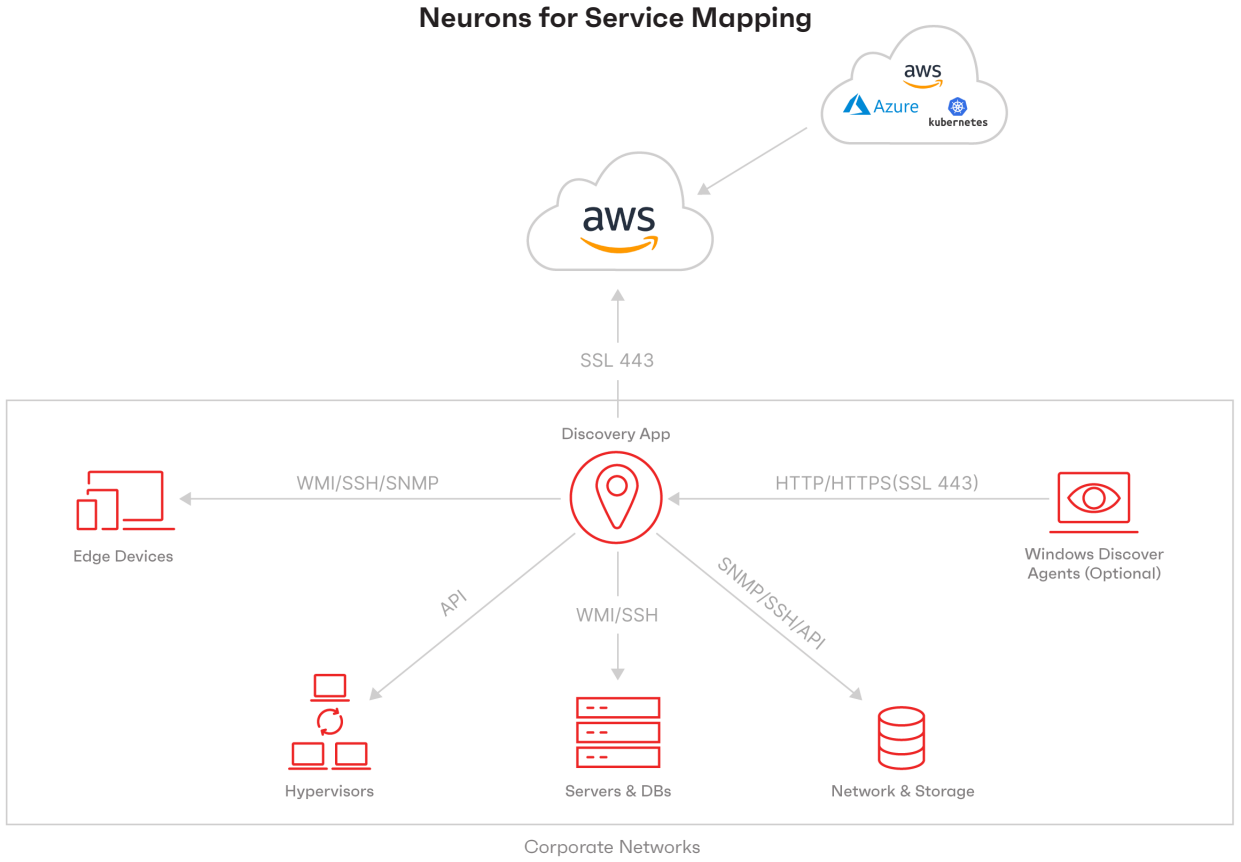
Any application hosted on AWS falls under Amazon's shared security model, broken into four parts:

- Physical security
- Network security
- Platform security
- People and procedures

Under the shared security model, AWS operates, manages and controls components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate. Ivanti Neurons for Service Mapping assumes responsibility and management of the operating system hosting the Ivanti Neurons for Service Mapping services (including updates and security patches), other associated application software as well as the configuration of the AWS-provided security group firewall.

2. Ivanti Neurons for Service Mapping Architecture

The following diagram outlines the standard architecture, security protocols and encryption methods used for Ivanti Neurons for Service Mapping. Discovery is at the core of Ivanti Neurons for Service Mapping, offering automatic and seamless population of CMDB through agentless and agent-based discovery methodologies.



3. Ivanti Neurons for Service Mapping Internal Components

As outlined in the architecture diagram, there are multiple components that make up Ivanti Neurons for Service Mapping.

3.1 Core Application

The core application for Ivanti Neurons for Service Mapping runs on a separate EC2 instance and carries out all the backend functionality of Discovery and ITSM processes.

3.2 Discovery Server

The Discovery server runs on its own EC2 instance and is responsible for secure transmission of data with the Discovery Applications and the EM core application. Discovery Server listens on port 8081 for all communication from the Discovery Application and on port 8080 for all communication from the core application.

3.3 Discovery Application

Discovery Application is the only on-premises component of Ivanti Neurons for Service Mapping and is responsible for carrying out the scans across the network. It can be installed on any standalone Windows server or a Virtual Machine. The Discovery App also encrypts the credentials entered using AES encryption and stores them locally on its host system. It uses SHA256 hashing algorithm to encrypt and SSL protocol to transmit the scanned data back to the discovery server. The following table lists communication ports and authentication methods used for scanning the hosts:

Device Type	Port	Authentication
Unix, Linux, Mac and Solaris	22 (SSH)	SSH Username, Password and Private Keys
Windows	135, 137, 138, 139 (WMI) and 445 (File and Printer Sharing)	Windows
Network Device, Router, Switches	161 (SNMP)	Community String (v1, v2), User ID/Password (v3)

4. Ivanti Neurons for Service Mapping AWS Components

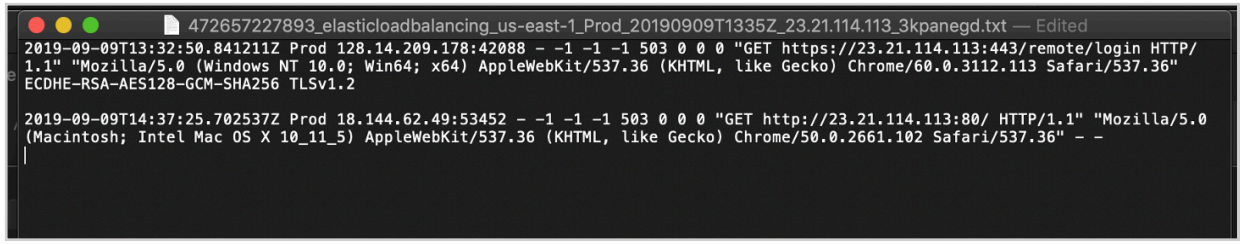
Ivanti Neurons for Service Mapping employs various components of AWS in the production environment, ensuring the security of all services and data.

4.1 Load Balancing

Ivanti Neurons for Service Mapping utilizes both application and network load balancing to manage traffic on a fleet of Amazon EC2 instances, distributing traffic to instances across all availability zones within a region.

Load balancing has all the advantages of an on-premises load balancer, plus several security benefits, which include:

- Taking over the encryption and decryption work from the Amazon EC2 instances and manages it centrally on the load balancer.
- Offering clients a single point of contact, and can also serve as the first line of defense against attacks on the network.
- Supporting the creation and management of security groups associated with Load Balancing to provide additional networking and security options.
- Supporting end-to-end traffic encryption using TLS (previously SSL) on those networks that use secure HTTP (HTTPS) connections.
- With monitoring enabled, AWS Load Balancers can produce detailed logs on access patterns and the traffic that was kept out.



4.2 AWS CloudWatch

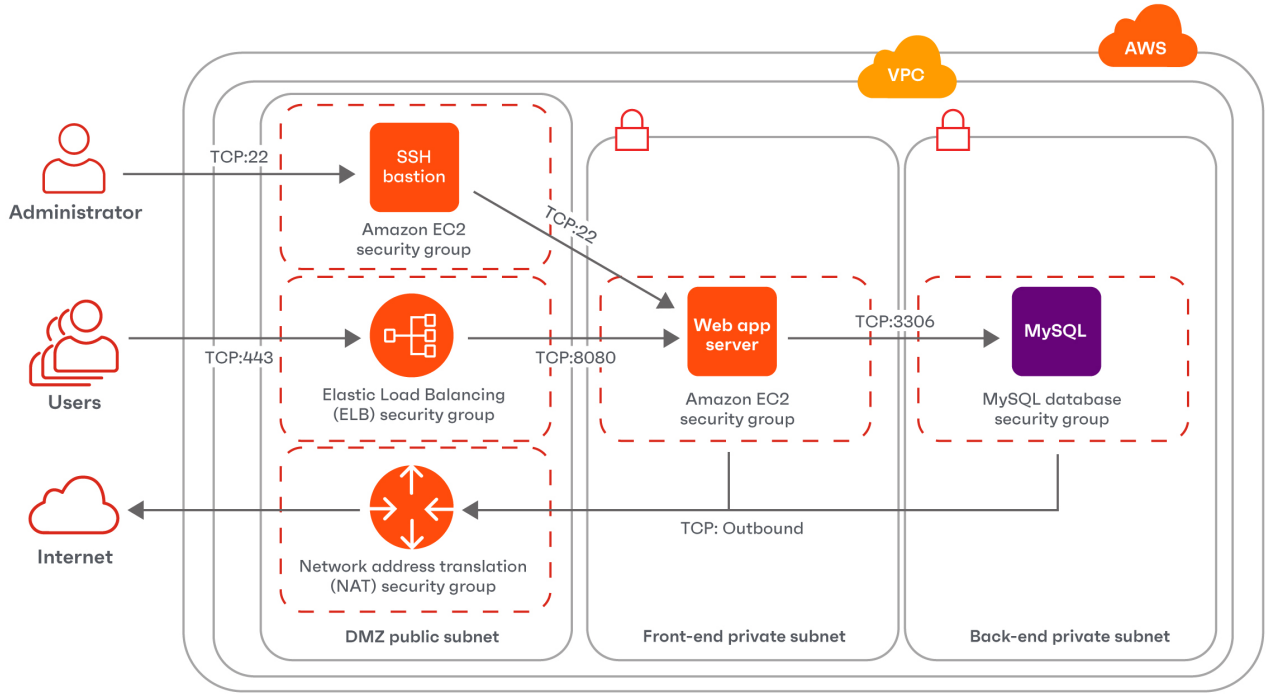
Ivanti Neurons for Service Mapping uses Amazon's CloudWatch service to monitor its EC2 instances. Amazon CloudWatch is a web service that provides monitoring for AWS cloud resources, starting with Amazon EC2. It provides visibility into resource utilization, operational performance and overall demand patterns, including metrics such as CPU utilization, disk reads and writes and network traffic. CloudWatch alarms and notifies if certain thresholds are crossed, such as disk space and memory utilization.

4.3 AWS Virtual Private Cloud (VPC)

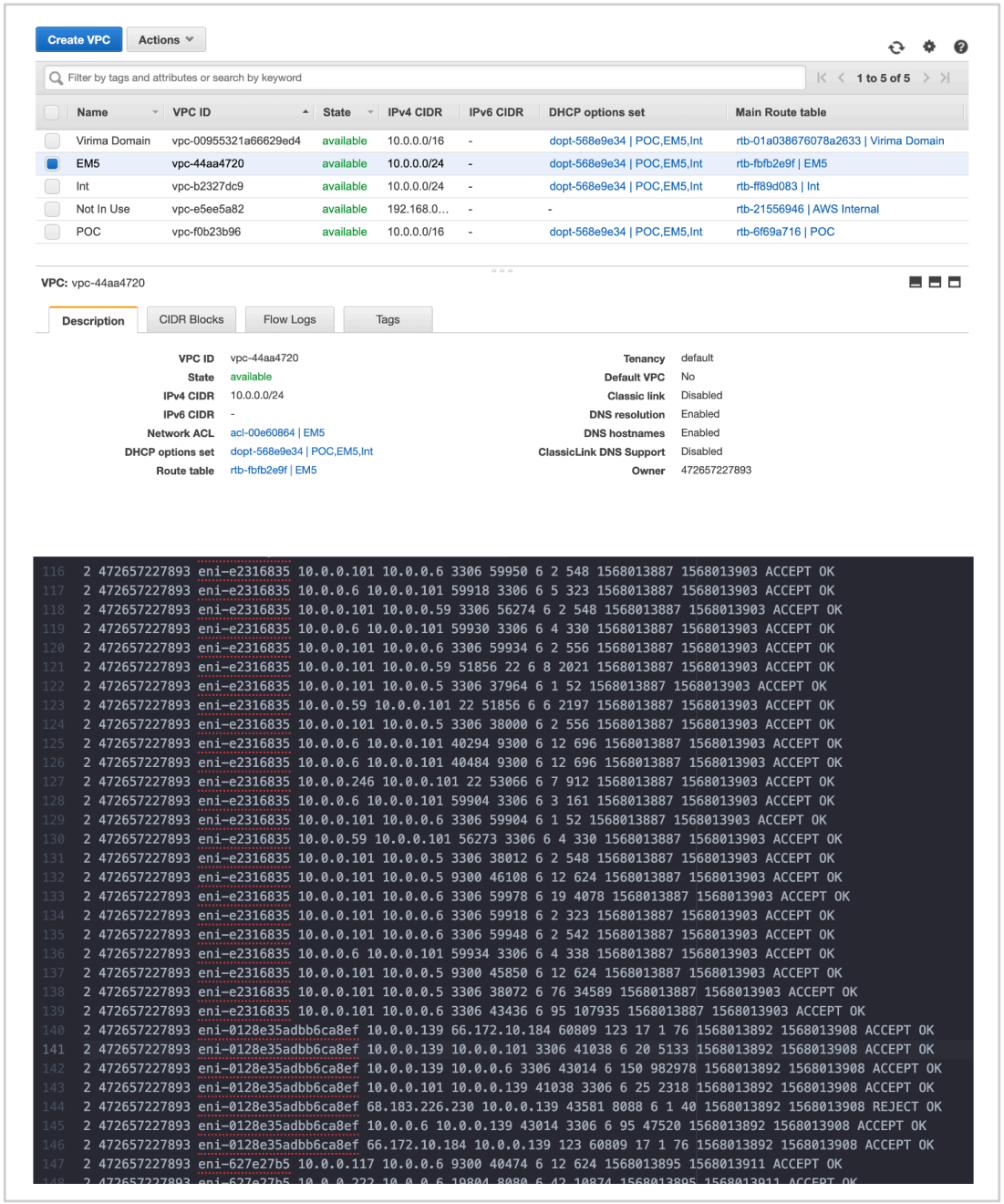
Ivanti Neurons for Service Mapping leverages Amazon VPC to create an isolated portion of the AWS cloud and launch Amazon EC2 instances that have private (RFC 1918) addresses and ensures that the EC2 instances don't have any public IPs. The main EC2 instance hosting Ivanti Neurons for Service Mapping core application within the VPC is accessible only from the elastic load balancer. Ivanti Neurons for Service Mapping VPC is a distinct, isolated network within the cloud; network traffic within the VPC is isolated from all other Amazon VPCs and subject to the following controls:

- API Access
- Subnets and Route Tables
- Firewall (Security Groups)

Ivanti Neurons for Service Mapping VPC is depicted in the following diagram, detailing various access types and how the user interaction happens with the deployed application:

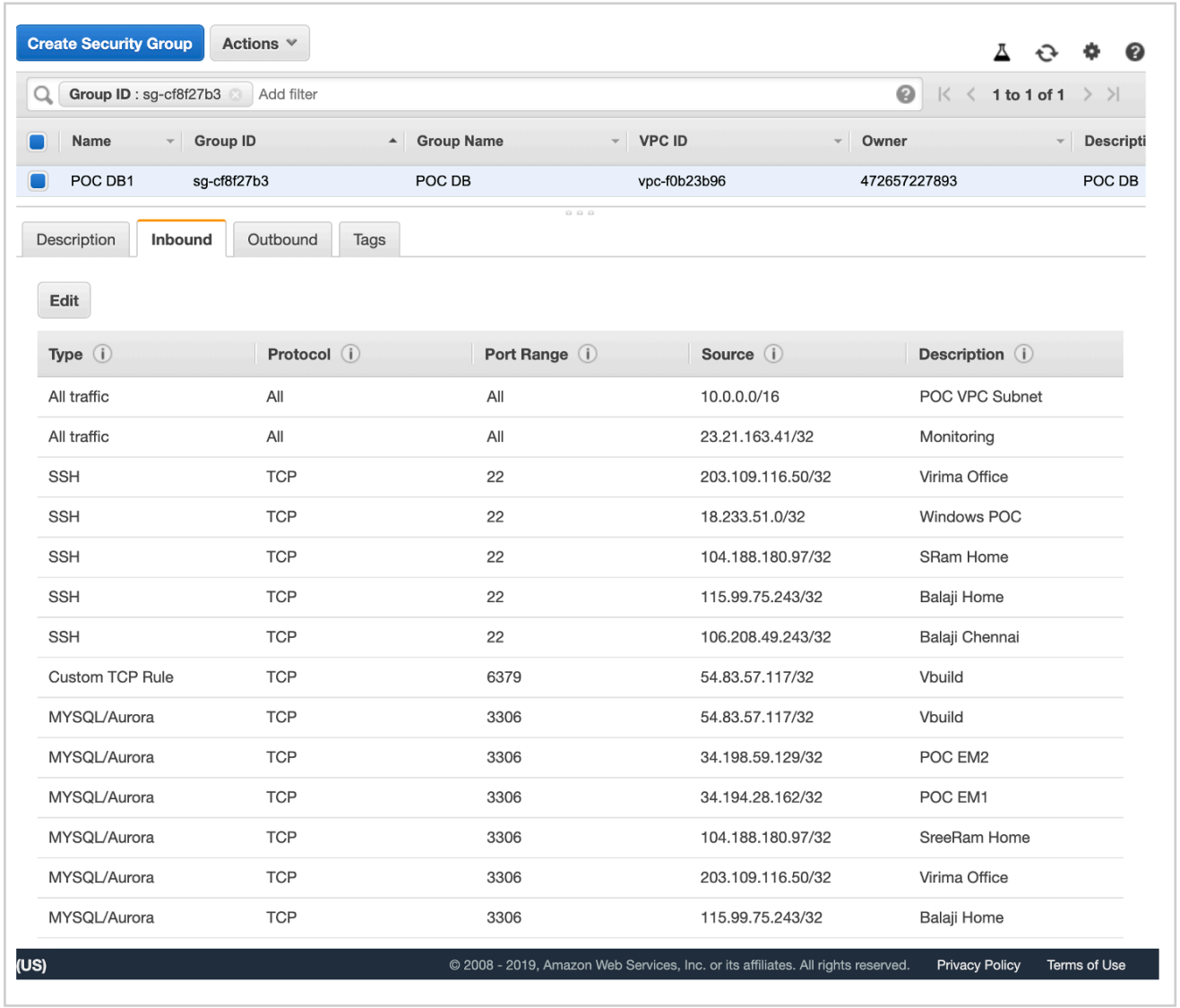


AWS Virtual Private Cloud not only secures the environment from public access, it also acts as a firewall to keep away unwanted traffic. Ivanti Neurons for Service Mapping maintains and monitors the Virtual Private Cloud very closely. Some of the configured VPCs and their access logs produced are shown to the right:



4.4 AWS Security Groups

Along with AWS CloudWatch, Elastic Load Balance and Virtual Private Cloud, Ivanti Neurons for Service Mapping also leverages AWS Security groups that let us identify and enforce all the access rules for each layer of infrastructure. Currently, Ivanti Neurons for Service Mapping has different security groups configured for different environments.



5. End Point Security

Along with cloud security measures, Ivanti Neurons for Service Mapping also ensures the security of end points in developer environments.

5.1 Network Firewall

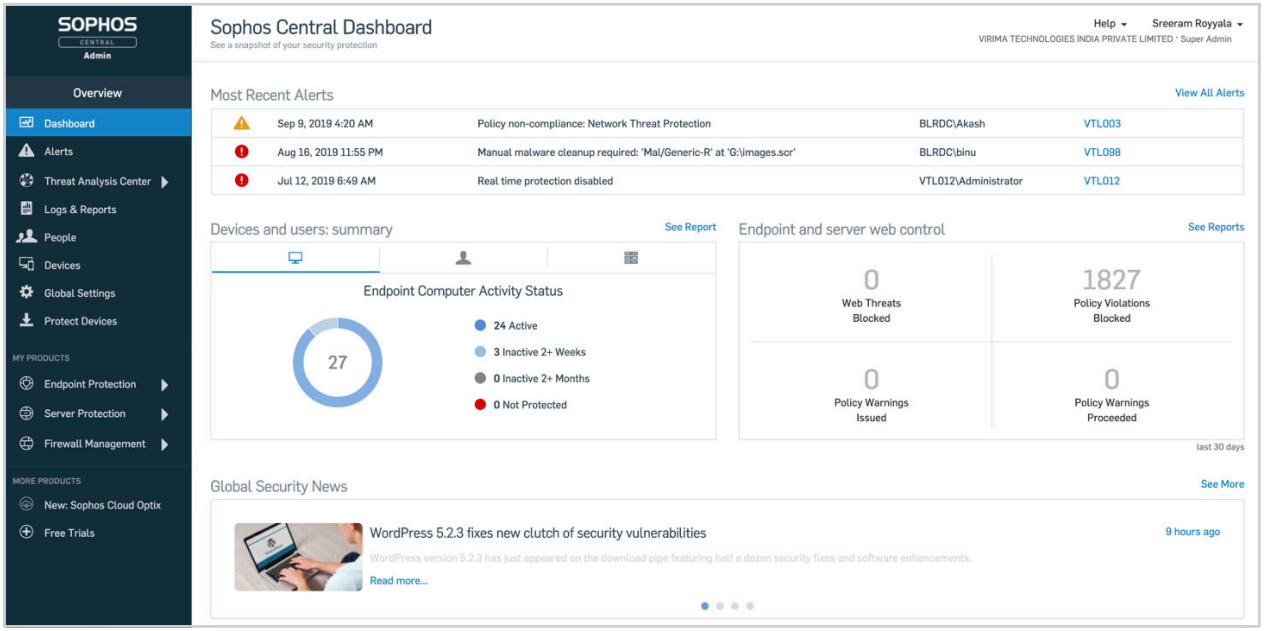
Network firewall is configured to keep malicious traffic away from office environment and keep developers workstations and Ivanti Neurons for Service Mapping lab environment safe. Ivanti Neurons for Service Mapping leverages pfsense virtual firewall for office protection. A sample of Current Firewall rules are outlined to the right:

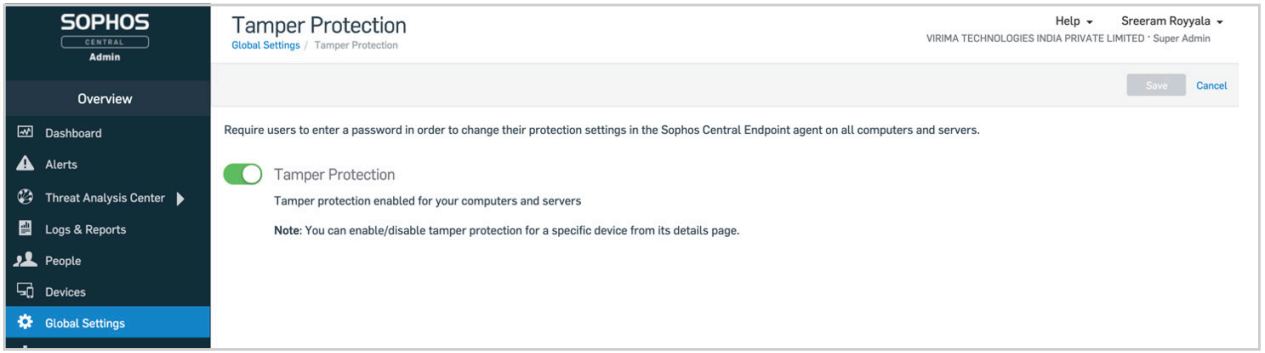
```
<filter>
        <rule>
                <id></id>
                <tracker>1516772506</tracker>
                <type>pass</type>
                <interface>wan</interface>
                <ipprotocol>inet</ipprotocol>
                <tag></tag>
                <tagged></tagged>
                <max></max>
                <max-src-nodes></max-src-nodes>
                <max-src-conn></max-src-conn>
                <max-src-states></max-src-states>
                <statetimeout></statetimeout>
                <statetype><![CDATA[keep state]]></statetype>
                <os></os>
                <protocol>tcp</protocol>
                <source>
                        <any></any>
                </source>
                <destination>
                        <address>192.168.201.1</address>
                        <port>443</port>
                </destination>
                <descr></descr>
                <updated>
                        <time>1516772506</time>
                        <username>admin@156.100.193.6</username>
                </updated>
                <created>
                        <time>1516772506</time>
                        <username>admin@125.120.193.6</username>
                </created>
        </rule>


        <separator>
                <opt1></opt1>
                <lan></lan>
                <wan></wan>
                <opt2></opt2>
                <openvpn></openvpn>
        </separator>
</filter>
```

5.2 Antivirus System

Ivanti Neurons for Service Mapping requires all developer workstations and laptops to be secured by an industry-standard antivirus system that's centrally managed and monitored. Ivanti Neurons for Service Mapping leverages Sophos endpoint security that can provide metrics on each of the protected devices and overall status on how effectively malware or policy violations are blocked. A screen capture of the dashboard is shown to the right:

Users of the system won't be able to install any unauthorized software without proper authentication as Tamper protection is turned on in Sophos.





5.3 Nagios Monitoring System

Ivanti Neurons for Service Mapping is very proactive in keeping the production environment and all its cloud infrastructure under control in terms of capacity and availability monitoring. We leverage Nagios monitoring to generate alerts in case of any systems crossing capacity thresholds.

6. Application Safeguards

Ivanti Neurons for Service Mapping has various built-in safeguards within the application to protect data from unauthorized users and users without proper privileges.

6.1 Single Sign On (SSO)

User access can be configured to utilize Single Sign On using any of the industry standard SSO providers utilizing SAML 2.0.

6.2 Two factor authentication

User access can be configured to be authenticated using a CAPTCHA or email along with the regular userID/password login.

6.3 External Authentication

User access can be configured to be authenticated against Active Directory or LDAP behind the scenes, along with the default Ivanti Neurons for Service Mapping user authentication.

6.4 Configurable Data Privacy

Asset/CI field data can be encrypted and stored based on administrator preferences. Also, admins can also select who can view the encrypted data based on user roles and responsibilities.

6.5 RACI Matrix Authorization

User authorization within the Ivanti Neurons for Service Mapping application is driven through a RACI matrix that defines users based on their role and addresses the following access levels:

- Responsible
- Accountable
- Consulted
- Informed

6.6 Role Based Access Levels

The role of the user drives the RACI matrix authorization. There are various standard ITSM roles that are already defined within the system. Depending on organizational preferences, new roles can be added and access levels can be set based on the type of the role.

6.7 Audit Controls

Ivanti Neurons for Service Mapping stores the complete audit trial of all the records in the system. Whenever an ITSM or asset record is added or updated, the information on the changes, the time of the change and the user responsible for the change are automatically stored in the system.

6.8 Rule Based Escalations and Notifications

Depending on the criticality of the data or the process, automatic escalations and notifications can be setup to alert stakeholders whenever certain updates occur to the record data.

Summary

Ivanti Neurons for Service Mapping takes security and availability of our clients' data very seriously. We also recognize that individual security and compliance needs may exceed those of standard industry practices. These needs can be addressed on a case-by-case basis.

Support and Contact

If you would like to call us directly via phone, pleaes use one of the options below:

Americas Support
Monday - Friday
8:00 am – 8:00 pm (GMT -5)
(except for public holidays)

1-801-308-8047

Europe, Middle East, and Africa (EMEA) Support
Monday - Friday
7:00 am – 6:00 pm (GMT +0)
(except for public holidays)

United Kingdom
+44 1925358112

Germany
+49 6996758625

France
+33 176400193

United Kingdom
+31 738080114

Asia Pacific (APAC) Support
Monday - Friday
6:00 am – 7:30 pm (China Std Time Zone UTC +8)
(except for public holidays)

Australia
+61 286078037

China
108001402489 (South)
108007142471 (North)

India
+914071279231

Singapore
+6531652833

*Customers can enter their case number and have the system route their call to the case owner (if available). This will reduce or eliminate the need to repeat the reported problem to a new support engineer.

ivanti.com
1 800 982 2130
sales@ivanti.com

Copyright © 2023, Ivanti. All rights reserved. IVI-2771 6/23 MM