



Ivanti Neurons for Service Mapping

Security Overview

Table of Contents

| | |
|---|----|
| 1. Introduction | 3 |
| 1.1 Shared Security Model | 3 |
| 2. Ivanti Neurons for Service Mapping Architecture | 3 |
| 3. Ivanti Neurons for Service Mapping Internal Components | 4 |
| 3.1 Core Application | 4 |
| 3.2 Discovery Server | 4 |
| 3.3 Discovery Application | 4 |
| 4. Ivanti Neurons for Service Mapping AWS Components | 5 |
| 4.1 Load Balancing | 5 |
| 4.2 AWS CloudWatch | 6 |
| 4.3 AWS Virtual Private Cloud | 6 |
| 4.4 AWS Security Groups | 8 |
| 5. End Point Security | 9 |
| 5.1 Network Firewall | 9 |
| 5.2 Antivirus System | 10 |
| 5.3 Nagios Monitoring System | 11 |
| 6. Application Safeguards | 11 |
| 6.1 Single Sign On (SSO) | 11 |
| 6.2 Two Factor Authentication | 11 |
| 6.3 External Authentication | 11 |
| 6.4 Configurable Data Privacy | 11 |
| 6.5 RACI Matrix Authorization | 11 |
| 6.6 Role Based Access Levels | 11 |
| 6.7 Audit Controls | 11 |
| 6.8 Rule Based Escalations and Notifications | 11 |
| 7. Summary | 11 |
| Support and Contact | 12 |

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

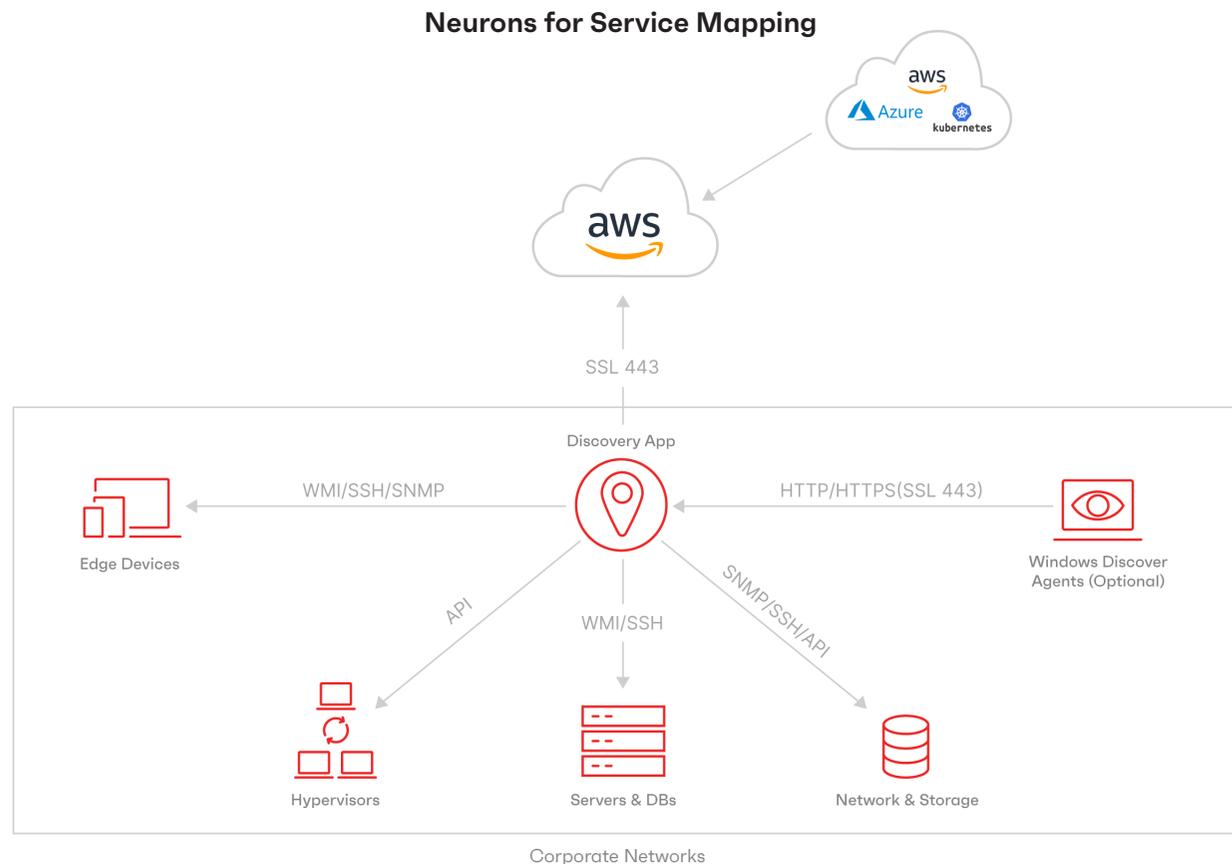
Any application hosted on AWS falls under Amazon's shared security model, broken into four parts:

- 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

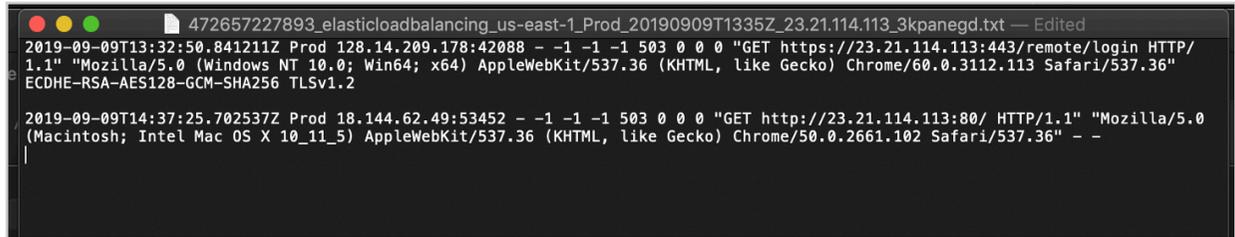
Ivanti Neurons for Service Mapping employs various components of AWS in the production environment, ensuring the security of all services and data.

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.



```
472657227893_elasticloadbalancing_us-east-1_Prod_20190909T1335Z_23.21.114.113_3kpanegd.txt -- Edited
2019-09-09T13:32:50.841211Z Prod 128.14.209.178:42088 - -1 -1 -1 503 0 0 0 "GET https://23.21.114.113:443/remote/login HTTP/1.1" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.113 Safari/537.36" ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2
2019-09-09T14:37:25.702537Z Prod 18.144.62.49:53452 - -1 -1 -1 503 0 0 0 "GET http://23.21.114.113:80/ HTTP/1.1" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.102 Safari/537.36" - -
```

4.2 AWS CloudWatch

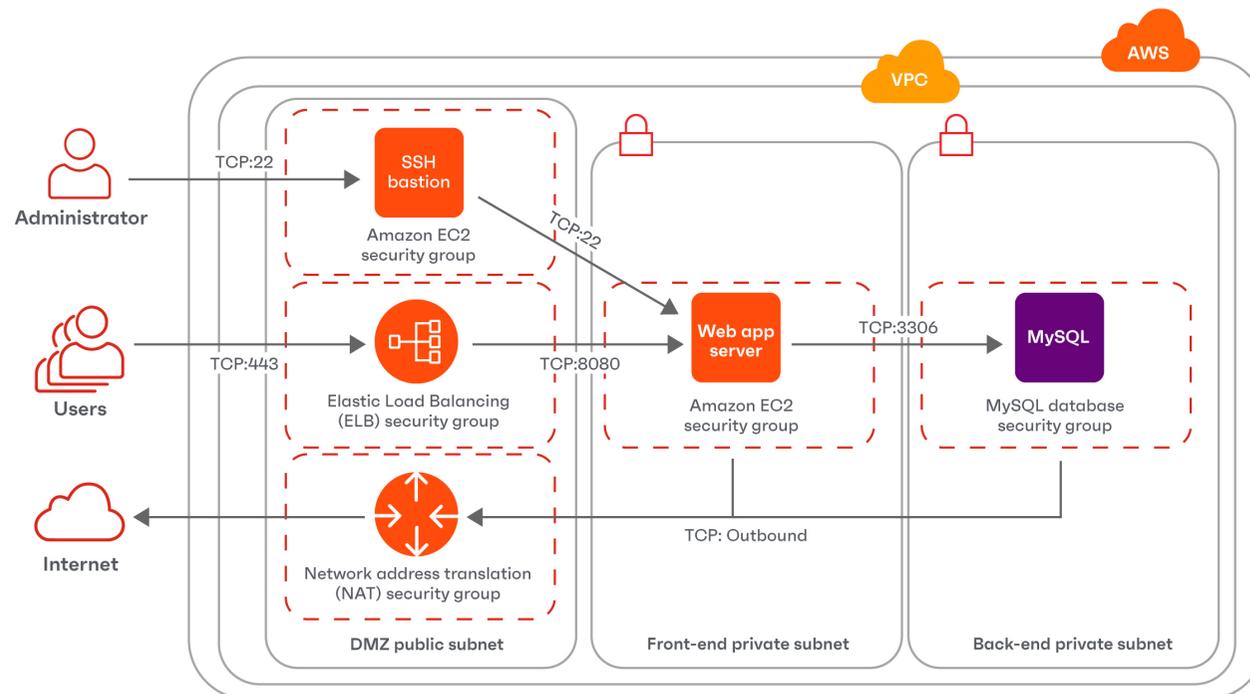
Ivanti Neurons for Service Mapping uses Amazon's CloudWatch service to monitor its EC2 instances. Amazon CloudWatch is a web service that provides monitoring for AWS cloud resources, starting with Amazon EC2. It provides visibility into resource utilization, operational performance and overall demand 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:

Create VPC
Actions

1 to 5 of 5

| Name | VPC ID | State | IPv4 CIDR | IPv6 CIDR | DHCP options set | Main Route table |
|---|-----------------------|-----------|--------------|-----------|-----------------------------|---------------------------------------|
| Virima Domain | vpc-00955321a66629ed4 | available | 10.0.0.0/16 | - | dopt-568e9e34 POC,EM5,Int | rtb-01a038676078a2633 Virima Domain |
| <input checked="" type="checkbox"/> EM5 | vpc-44aa4720 | available | 10.0.0.0/24 | - | dopt-568e9e34 POC,EM5,Int | rtb-fbfb2e9f EM5 |
| Int | vpc-b2327dc9 | available | 10.0.0.0/24 | - | dopt-568e9e34 POC,EM5,Int | rtb-f89d083 Int |
| Not In Use | vpc-e5ee5a82 | available | 192.168.0... | - | - | rtb-21556946 AWS Internal |
| POC | vpc-f0b23b96 | available | 10.0.0.0/16 | - | dopt-568e9e34 POC,EM5,Int | rtb-6f69a716 POC |

VPC: vpc-44aa4720

Description
CIDR Blocks
Flow Logs
Tags

| | |
|--|--|
| <p>VPC ID vpc-44aa4720</p> <p>State available</p> <p>IPv4 CIDR 10.0.0.0/24</p> <p>IPv6 CIDR -</p> <p>Network ACL aci-00e60864 EM5</p> <p>DHCP options set dopt-568e9e34 POC,EM5,Int</p> <p>Route table rtb-fbfb2e9f EM5</p> | <p>Tenancy default</p> <p>Default VPC No</p> <p>Classic link Disabled</p> <p>DNS resolution Enabled</p> <p>DNS hostnames Enabled</p> <p>ClassicLink DNS Support Disabled</p> <p>Owner 472657227893</p> |
|--|--|

```

116 2 472657227893 eni-e2316835 10.0.0.101 10.0.0.6 3306 59950 6 2 548 1568013887 1568013903 ACCEPT OK
117 2 472657227893 eni-e2316835 10.0.0.6 10.0.0.101 59918 3306 6 5 323 1568013887 1568013903 ACCEPT OK
118 2 472657227893 eni-e2316835 10.0.0.101 10.0.0.59 3306 56274 6 2 548 1568013887 1568013903 ACCEPT OK
119 2 472657227893 eni-e2316835 10.0.0.6 10.0.0.101 59930 3306 6 4 330 1568013887 1568013903 ACCEPT OK
120 2 472657227893 eni-e2316835 10.0.0.101 10.0.0.6 3306 59934 6 2 556 1568013887 1568013903 ACCEPT OK
121 2 472657227893 eni-e2316835 10.0.0.101 10.0.0.59 51856 22 6 8 2021 1568013887 1568013903 ACCEPT OK
122 2 472657227893 eni-e2316835 10.0.0.101 10.0.0.5 3306 37964 6 1 52 1568013887 1568013903 ACCEPT OK
123 2 472657227893 eni-e2316835 10.0.0.59 10.0.0.101 22 51856 6 6 2197 1568013887 1568013903 ACCEPT OK
124 2 472657227893 eni-e2316835 10.0.0.101 10.0.0.5 3306 38000 6 2 556 1568013887 1568013903 ACCEPT OK
125 2 472657227893 eni-e2316835 10.0.0.6 10.0.0.101 40294 9300 6 12 696 1568013887 1568013903 ACCEPT OK
126 2 472657227893 eni-e2316835 10.0.0.6 10.0.0.101 40484 9300 6 12 696 1568013887 1568013903 ACCEPT OK
127 2 472657227893 eni-e2316835 10.0.0.246 10.0.0.101 22 53066 6 7 912 1568013887 1568013903 ACCEPT OK
128 2 472657227893 eni-e2316835 10.0.0.6 10.0.0.101 59904 3306 6 3 161 1568013887 1568013903 ACCEPT OK
129 2 472657227893 eni-e2316835 10.0.0.101 10.0.0.6 3306 59904 6 1 52 1568013887 1568013903 ACCEPT OK
130 2 472657227893 eni-e2316835 10.0.0.59 10.0.0.101 56273 3306 6 4 330 1568013887 1568013903 ACCEPT OK
131 2 472657227893 eni-e2316835 10.0.0.101 10.0.0.5 3306 38012 6 2 548 1568013887 1568013903 ACCEPT OK
132 2 472657227893 eni-e2316835 10.0.0.101 10.0.0.5 9300 46108 6 12 624 1568013887 1568013903 ACCEPT OK
133 2 472657227893 eni-e2316835 10.0.0.101 10.0.0.6 3306 59978 6 19 4078 1568013887 1568013903 ACCEPT OK
134 2 472657227893 eni-e2316835 10.0.0.101 10.0.0.6 3306 59918 6 2 323 1568013887 1568013903 ACCEPT OK
135 2 472657227893 eni-e2316835 10.0.0.101 10.0.0.6 3306 59948 6 2 542 1568013887 1568013903 ACCEPT OK
136 2 472657227893 eni-e2316835 10.0.0.6 10.0.0.101 59934 3306 6 4 338 1568013887 1568013903 ACCEPT OK
137 2 472657227893 eni-e2316835 10.0.0.101 10.0.0.5 9300 45850 6 12 624 1568013887 1568013903 ACCEPT OK
138 2 472657227893 eni-e2316835 10.0.0.101 10.0.0.5 3306 38072 6 76 34589 1568013887 1568013903 ACCEPT OK
139 2 472657227893 eni-e2316835 10.0.0.101 10.0.0.6 3306 43436 6 95 107935 1568013887 1568013903 ACCEPT OK
140 2 472657227893 eni-0128e35adb66ca8ef 10.0.0.139 66,172,10,184 60809 123 17 1 76 1568013892 1568013908 ACCEPT OK
141 2 472657227893 eni-0128e35adb66ca8ef 10.0.0.139 10.0.0.101 3306 41038 6 20 5133 1568013892 1568013908 ACCEPT OK
142 2 472657227893 eni-0128e35adb66ca8ef 10.0.0.139 10.0.0.6 3306 43014 6 150 982978 1568013892 1568013908 ACCEPT OK
143 2 472657227893 eni-0128e35adb66ca8ef 10.0.0.101 10.0.0.139 41038 3306 6 25 2318 1568013892 1568013908 ACCEPT OK
144 2 472657227893 eni-0128e35adb66ca8ef 68,183,226,230 10.0.0.139 43581 8088 6 1 40 1568013892 1568013908 REJECT OK
145 2 472657227893 eni-0128e35adb66ca8ef 10.0.0.6 10.0.0.139 43014 3306 6 95 47520 1568013892 1568013908 ACCEPT OK
146 2 472657227893 eni-0128e35adb66ca8ef 66,172,10,184 10.0.0.139 123 60809 17 1 76 1568013892 1568013908 ACCEPT OK
147 2 472657227893 eni-627e27b5 10.0.0.117 10.0.0.6 9300 40474 6 12 624 1568013895 1568013911 ACCEPT OK
148 2 472657227893 eni-627e27b5 10.0.0.222 10.0.0.6 10804 8080 6 12 10874 1568013895 1568013911 ACCEPT OK

```

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.

The screenshot displays the AWS IAM console interface for a Security Group. At the top, there is a 'Create Security Group' button and an 'Actions' dropdown menu. Below this is a search bar with the text 'Group ID : sg-cf8f27b3' and an 'Add filter' button. A table lists the security group details:

| Name | Group ID | Group Name | VPC ID | Owner | Description |
|---------|-------------|------------|--------------|--------------|-------------|
| POC DB1 | sg-cf8f27b3 | POC DB | vpc-f0b23b96 | 472657227893 | POC DB |

Below the table, there are tabs for 'Description', 'Inbound', 'Outbound', and 'Tags'. The 'Inbound' tab is selected. An 'Edit' button is visible above the rule list. The rule list table is as follows:

| Type | Protocol | Port Range | Source | Description |
|-----------------|----------|------------|-------------------|----------------|
| All traffic | All | All | 10.0.0.0/16 | POC VPC Subnet |
| All traffic | All | All | 23.21.163.41/32 | Monitoring |
| SSH | TCP | 22 | 203.109.116.50/32 | Virima Office |
| SSH | TCP | 22 | 18.233.51.0/32 | Windows POC |
| SSH | TCP | 22 | 104.188.180.97/32 | SRam Home |
| SSH | TCP | 22 | 115.99.75.243/32 | Balaji Home |
| SSH | TCP | 22 | 106.208.49.243/32 | Balaji Chennai |
| Custom TCP Rule | TCP | 6379 | 54.83.57.117/32 | Vbuild |
| MYSQL/Aurora | TCP | 3306 | 54.83.57.117/32 | Vbuild |
| MYSQL/Aurora | TCP | 3306 | 34.198.59.129/32 | POC EM2 |
| MYSQL/Aurora | TCP | 3306 | 34.194.28.162/32 | POC EM1 |
| MYSQL/Aurora | TCP | 3306 | 104.188.180.97/32 | SreeRam Home |
| MYSQL/Aurora | TCP | 3306 | 203.109.116.50/32 | Virima Office |
| MYSQL/Aurora | TCP | 3306 | 115.99.75.243/32 | Balaji Home |

At the bottom of the console, there is a footer with '(US)', '© 2008 - 2019, Amazon Web Services, Inc. or its affiliates. All rights reserved.', 'Privacy Policy', and 'Terms of Use'.

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.

The screenshot shows the Sophos Central Admin dashboard. The left sidebar contains navigation options: Overview, Dashboard, Alerts, Threat Analysis Center, Logs & Reports, People, Devices, Global Settings, Protect Devices, MY PRODUCTS (Endpoint Protection, Server Protection, Firewall Management), and MORE PRODUCTS (New: Sophos Cloud Optix, Free Trials). The main content area is titled 'Sophos Central Dashboard' and includes a 'Most Recent Alerts' table, 'Devices and users: summary' with an 'Endpoint Computer Activity Status' chart, 'Endpoint and server web control' metrics, and 'Global Security News'.

| Alert Icon | Time | Alert Message | User | Device ID |
|------------|-----------------------|---|----------------------|-----------|
| Warning | Sep 9, 2019 4:20 AM | Policy non-compliance: Network Threat Protection | BLRDC\Akash | VTL003 |
| Error | Aug 16, 2019 11:55 PM | Manual malware cleanup required: 'Mal/Generic-R' at 'G:\images.scr' | BLRDC\binu | VTL098 |
| Error | Jul 12, 2019 6:49 AM | Real time protection disabled | VTL012\Administrator | VTL012 |

Endpoint Computer Activity Status

- 24 Active
- 3 Inactive 2+ Weeks
- 0 Inactive 2+ Months
- 0 Not Protected

Endpoint and server web control

- 0 Web Threats Blocked
- 1827 Policy Violations Blocked
- 0 Policy Warnings Issued
- 0 Policy Warnings Proceeded

Global Security News

- WordPress 5.2.3 fixes new clutch of security vulnerabilities (9 hours ago)

The screenshot shows the 'Tamper Protection' settings page in the Sophos Central Admin interface. The page title is 'Tamper Protection' with a breadcrumb 'Global Settings / Tamper Protection'. A 'Require users to enter a password in order to change their protection settings in the Sophos Central Endpoint agent on all computers and servers.' checkbox is checked. The 'Tamper Protection' toggle switch is turned on, with the text 'Tamper protection enabled for your computers and servers'. A note states: 'Note: You can enable/disable tamper protection for a specific device from its details page.' There are 'Save' and 'Cancel' buttons at the top right.

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 trail 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, please 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.

The Ivanti logo consists of the word "ivanti" in a bold, lowercase, sans-serif font. The letter "i" is red, while the remaining letters "vanti" are black. A small registered trademark symbol (®) is located at the top right of the letter "i".

[ivanti.com](https://www.ivanti.com)

1 800 982 2130

sales@ivanti.com