SOLUTION NOTE

INFOBLOX AND SERVICENOW INTEGRATION ORCHESTRATES AND ACCELERATES THREAT RESPONSE

SUMMARY

With Infoblox and ServiceNow integration, your network and security teams can resolve security issues faster and more collaboratively with enhanced visibility, agility and automation.

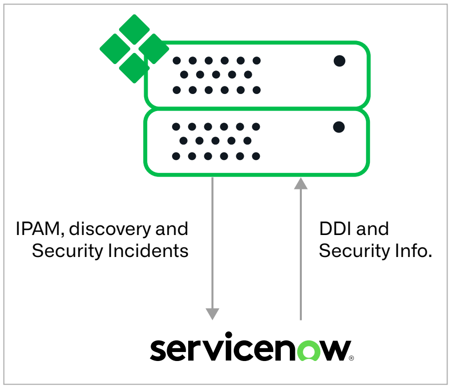
The joint solution combines industry-leading Infoblox DNS, DHCP, and IP address management (DDI) and the advanced Configuration Management and Database (CMDB) and incident management capabilities from ServiceNow. It empowers your network and security practitioners to respond faster to network changes and security events by enabling them to automatically receive information on new devices as well as infected or compromised hosts and automate repetitive tasks through intuitive workflows.

CHALLENGES

Today's enterprise network consists of a large number of network and security devices, each of which generates data about incidents and events. Yet, that data is often not shared across different tools or devices. The inability to easily share data and the lack of interoperability creates solution silos and limits vital context that could speed response. According to the SANS 2023 SOC Survey, keeping up with the volume of security alerts and integrating different security tools are among the challenges related to security operations. According to the same survey, investing in technologies like Security Orchestration Automation Response(SOAR) to automate security automation and threat detection remains a priority for security teams today.

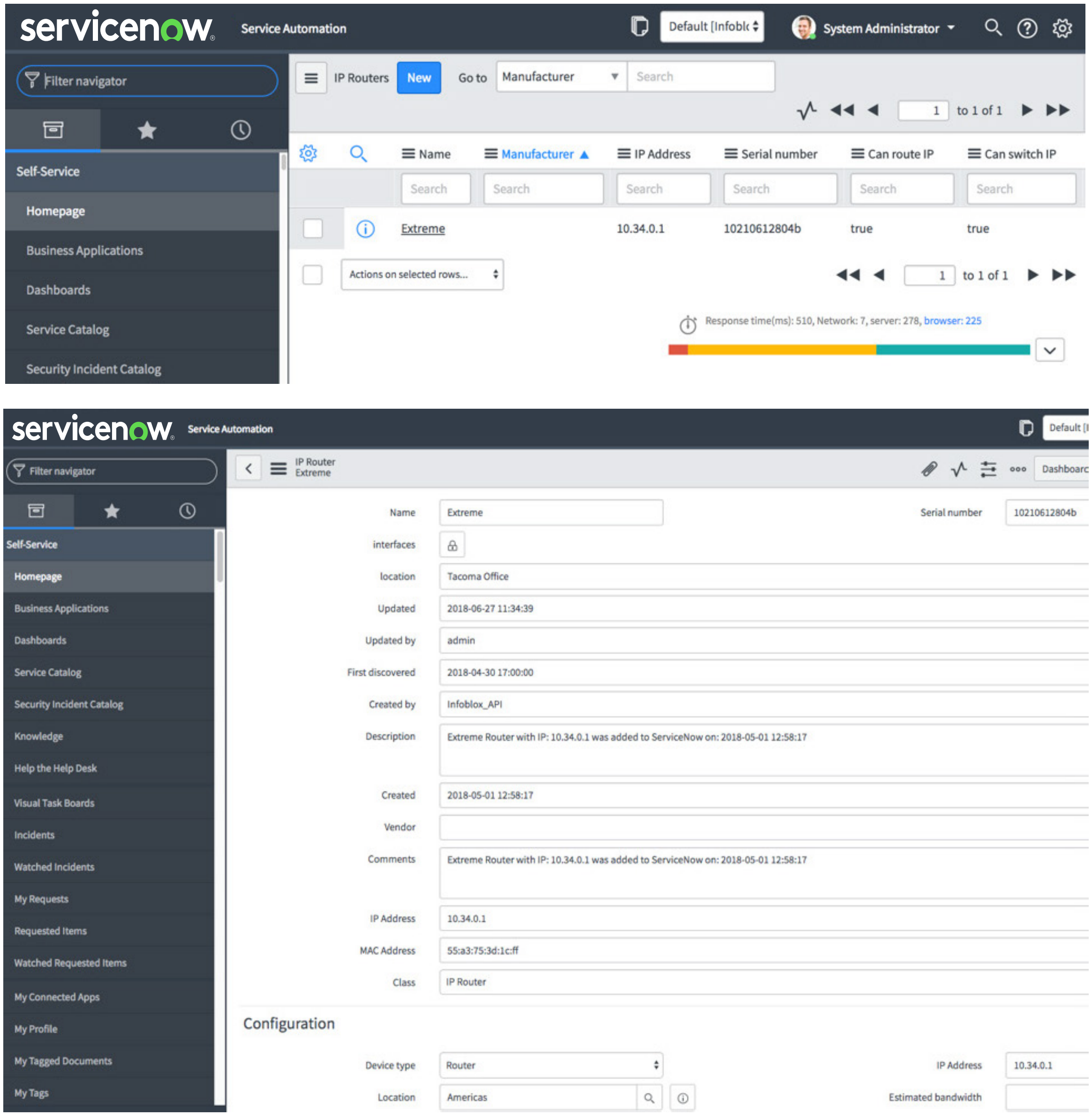
JOINT SOLUTION

The Infoblox component of the joint solution incorporates advanced DDI capabilities and the industry's most extensive threat intelligence and third-party security vendor API integrations. The ServiceNow components include leading CMDB and incident management capabilities, which are widely used by organizations and provide a 360-degree, consolidated view across all IT assets and security incidents, greatly improving the speed and efficiency of response.



ENABLING CONSOLIDATED VISIBILITY

Infoblox synchronizes information on new devices, networks and IP addresses with the ServiceNow CMDB to create incident notifications, which are then pushed to recipients. The combined solution gives your network and security personnel the ability to see new devices, incidents, and indicators of compromise (IoCs) discovered by Infoblox all in one place from within the ServiceNow portal interface (Fig. 1).



Name	Manufacturer ▲	IP Address	Serial number	Can route IP	Can switch IP
Extreme		10.34.0.1	10210612804b	true	true

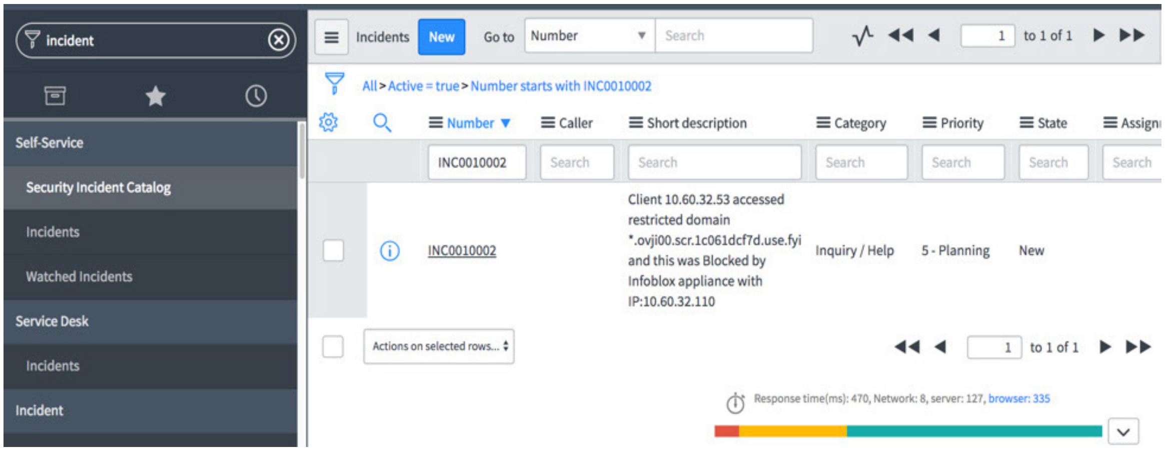
Response time(ms): 510, Network: 7, server: 278, browser: 225

Name	Extreme
Serial number	10210612804b
interfaces	
location	Tacoma Office
Updated	2018-06-27 11:34:39
Updated by	admin
First discovered	2018-04-30 17:00:00
Created by	Infoblox_API
Description	Extreme Router with IP: 10.34.0.1 was added to ServiceNow on: 2018-05-01 12:58:17
Created	2018-05-01 12:58:17
Vendor	
Comments	Extreme Router with IP: 10.34.0.1 was added to ServiceNow on: 2018-05-01 12:58:17
IP Address	10.34.0.1
MAC Address	55:a3:75:3d:1c:ff
Class	IP Router

Configuration

Device type	Router
IP Address	10.34.0.1
Location	Americas
Estimated bandwidth	

Figure 1



All > Active = true > Number starts with INC0010002

Number ▼	Caller	Short description	Category	Priority	State	Assign
INC0010002		Client 10.60.32.53 accessed restricted domain *.ovji00.scr.1c061dcf7d.use.fyi and this was Blocked by Infoblox appliance with IP:10.60.32.110	Inquiry / Help	5 - Planning	New	

Response time(ms): 470, Network: 8, server: 127, browser: 335

Figure 2: The integrated solution also displays details of DNS security events detected by Infoblox within the ServiceNow UI

INFOBLOX & SERVICENOW DISCOVERY

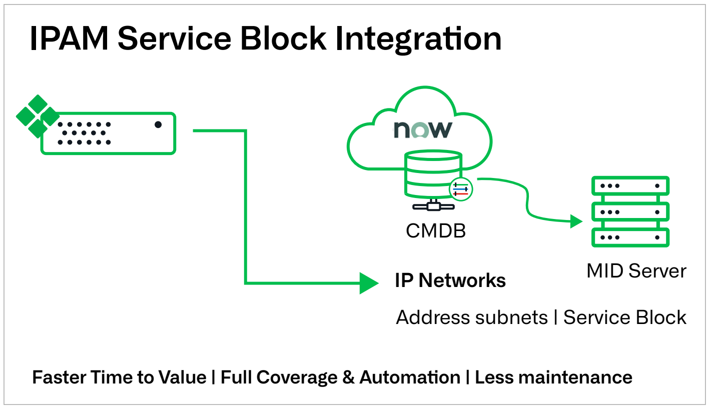

IPAM Service Block Integration
now
CMDB
MID Server
IP Networks
Address subnets | Service Block
Faster Time to Value | Full Coverage & Automation | Less maintenance

Figure 3

With the Discovery component of the ServiceNow solution your teams can get consolidated dashboard views into your onprem and cloud resources. The ServiceNow Discovery service uses IP subnet information to trigger discovery using agentless protocols. Infoblox integration helps bootstrap ServiceNow Discovery by pulling all the IP subnet information from your IPAM solution to the ServiceNow IP network table (Fig. 3).

Infoblox & ServiceNow Discovery

To take advantage of the integration between ServiceNow Discovery and Infoblox, you will need an Infoblox Security Ecosystem license. Additional Infoblox licenses are required to receive network DDI information, threat information through Infoblox Response Policy Zones (RPZ), and threat intelligence. The ServiceNow Discovery and Infoblox integration was built by Infoblox and is supported by the Infoblox community.

Getting Started

You can download Infoblox's DDI application (Infoblox activity pack) from the ServiceNow store to get started. It comes loaded with over twenty valuable activations (e.g., RPZ, ADP, TI rule and DNS records management). These activations enable you to customize specific workflows on ServiceNow to interoperate with the Infoblox Grid. It also contains two sample workflows for creating and deleting RPZ rules as shown (Fig. 4).

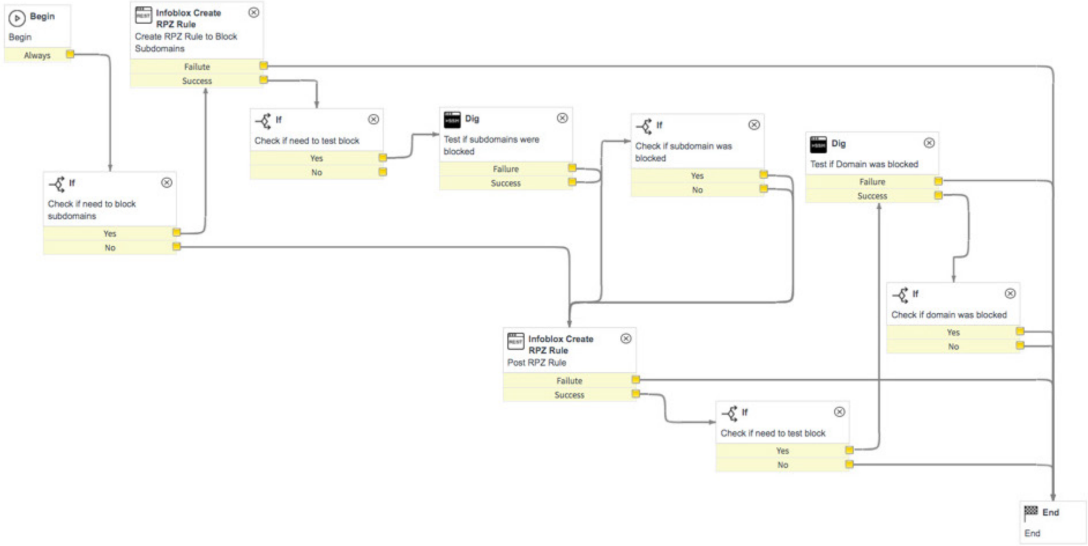

Begin
Begin
Always
Infoblox Create RPZ Rule
Create RPZ Rule to Block Subdomains
Failute
Success
If
Check if need to block subdomains
Yes
No
If
Check if need to test block
Yes
No
Dig
Test if subdomains were blocked
Failure
Success
If
Check if subdomain was blocked
Yes
No
Dig
Test if Domain was blocked
Failure
Success
If
Check if domain was blocked
Yes
No
Infoblox Create RPZ Rule
Post RPZ Rule
Failute
Success
If
Check if need to test block
Yes
No
End
End

Figure 4

INFOBLOX & SERVICENOW DISCOVERY

The Infoblox and ServiceNow joint solution provides your organization with the following benefits:

Consolidated dashboard views into network changes:

Integration between Infoblox and ServiceNow provides visibility into devices and endpoints joining and leaving the network, which helps security and network admins to take appropriate actions sooner.

Visibility and faster response to DNS threats:

Whenever Infoblox detects DNS threats, it automatically notifies ServiceNow, enabling security personnel to respond faster.

Elimination of network service outages:

Enable proactive identification of network and security issues to ensure quick response to network changes and security events.

Rapid resolution of network issues at light speed:

Eliminate network issues before they cause service outages by proactively assessing product or service health in real time and engaging the right resources to fix the issues fast.

To learn more about this integration and demo, please visit https://community.infoblox.com/t5/servicenow/gp-p/SERVICENOW

Infoblox & ServiceNow Discovery

ServiceNow was started in 2004 with the belief that getting simple stuff done at work can be easy and getting complex multi-step tasks completed can be painless. From the beginning, ServiceNow envisioned a world where anyone could create powerful workflows to get enterprise work done. Today, ServiceNow's cloud-based platform simplifies the way we work through a structured security response engine. ServiceNow Security Operations automates, predicts, digitizes, and optimizes security and vulnerability response to resolve threats quickly based on business impact. Reduce manual processes and increase efficiency across security and IT teams. ServiceNow is how work gets done.

To find out how, visit: http://www.servicenow.com/

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054

+1.408.986.4000
www.infoblox.com

Version: 20240221v1