NS1 Labs

Using DNS to Minimize Cyber Threat Exposure

CISA and the FBI recommend monitoring DNS traffic for connections to malicious domains. Orb, a free open source observability tool, makes it easy.

Posted by
Shannon Weyrick on
March 11, 2022

Using DNS to Reduce Exposure to Russian Cyber Threats

On February 26, the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) issued a **joint Cybersecurity Advisory** outlining malware threats associated with Russian cyber operations in Ukraine. In a detailed **technical overview** of threat vectors, the agencies recommended a series of actions network administrators can take to minimize exposure.

One category of recommended measures includes monitoring Domain Name System (DNS) traffic to known sites associated with malware distribution. In addition to keeping tabs on sites with Russian or Ukrainian top level domains (TLDs), a sudden spike in traffic to certain proxy sites could also be an indicator of compromise.

There are plenty of observability tools out there which monitor DNS traffic, block malicious domains, and take other measures to prevent DDoS attacks. Yet most of these provide only a surface-level view into the underlying DNS data. Many network and security teams would like the option to go one level deeper, to identify the cause of abnormal DNS activity.

Spikes in DNS traffic could indicate a malware or DDoS attack. Or they could be associated with more mundane technical issues - a misconfiguration, or a simple missing DNS entry. Getting a quick handle on the health of your DNS activity is the first step in taking meaningful action - or assessing whether further action is required.

Orb: Easy, Free, Open Source DNS Monitoring

For admins concerned with DNS as a threat vector, **NS1 Labs** created **Orb** - a free, open source platform which gives any network administrator the ability to dig deeper into patterns of DNS activity. Orb, available as both self-hosted software or a free SaaS offering through **Orb.live** - orchestrates a fleet of agents to gather deep, distributed visibility across your infrastructure. Analysis happens **right on the network edge** with “small data” metric output, increasing reaction time and minimizing bloated data stores so you can focus on what matters most.

Orb offers a quick, easy (and free!) way to track malicious traffic associated with cybersecurity threats with connections to Russia, Ukraine, Belarus, or other current sources of malicious activity. With a few simple configuration steps, network administrators can deploy lightweight agents anywhere on the network. Those agents then push data to a **Prometheus database and Grafana dashboard**, or other standard observability tools you may already be using.

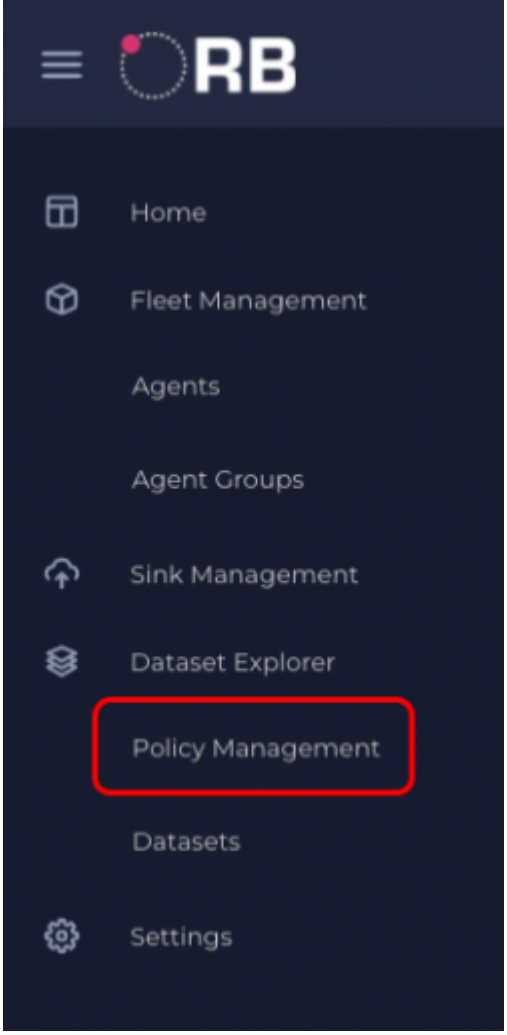
Orb is just a piece of NS1’s larger commitment to open source technology as the starting point for innovation. We’re also committed to **pktvisor**, the edge analyzer that powers Orb; **flamethrower**, a DNS performance and testing tool; as well as several **NetBox**-related projects. It all adds up to a unique quiver of tools that we’re making available for free through **NS1 Labs**.

Getting Started with Orb

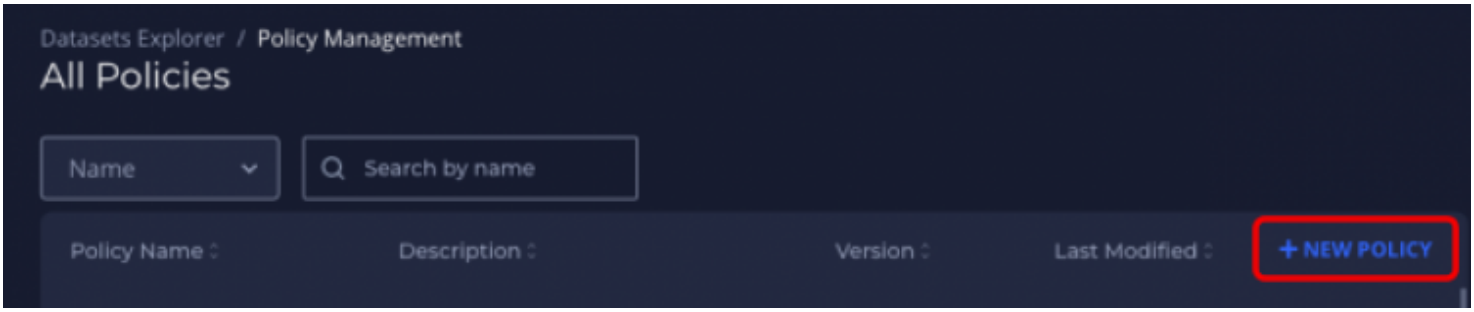
You can set up Orb in ten minutes or less. All of the details can be found in the **Orb documentation**.

Once you have an account set up, follow the instructions below to create a policy for generating metrics matching a domain suffix.

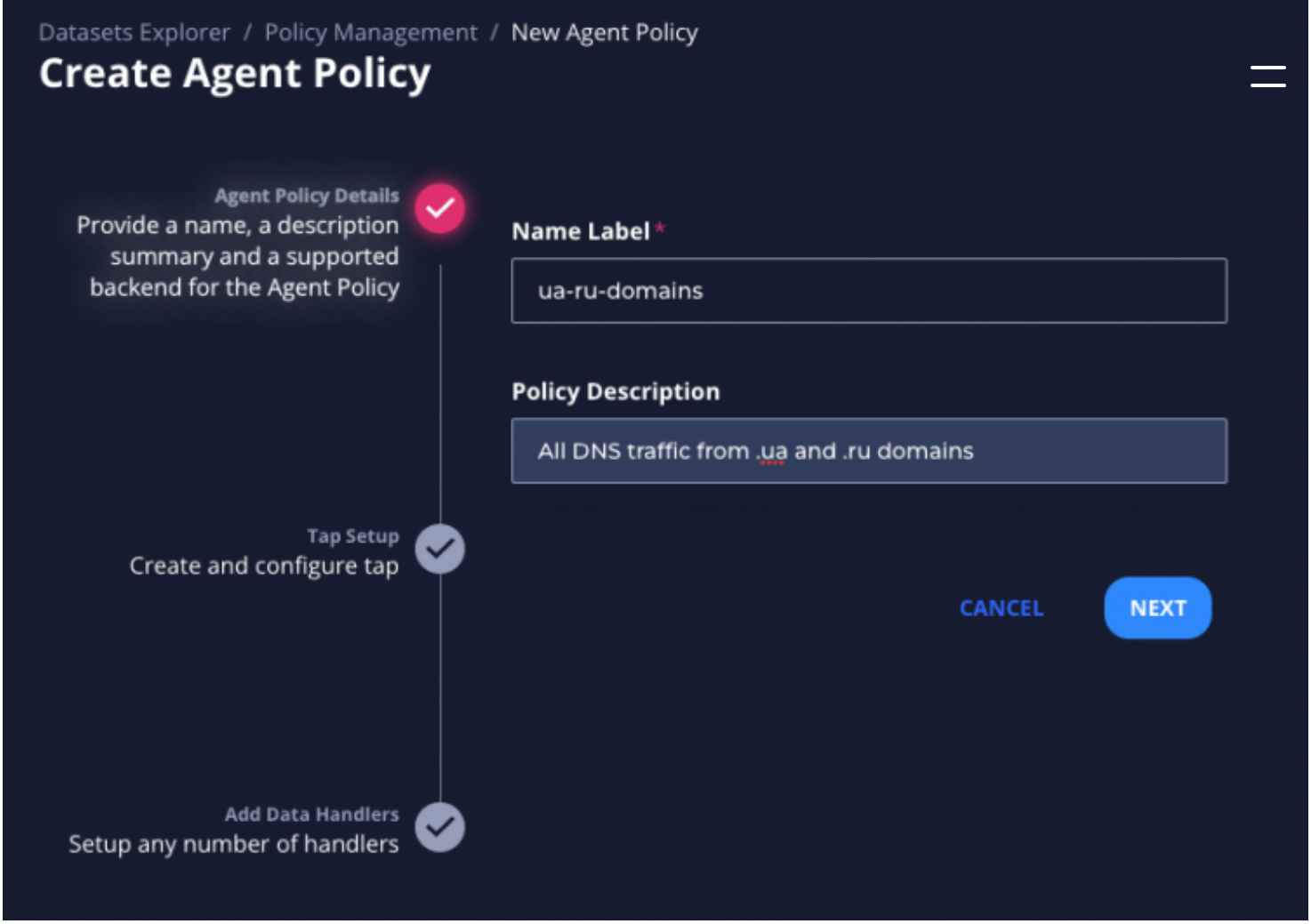
First, select Policy Management in the menu on the left.



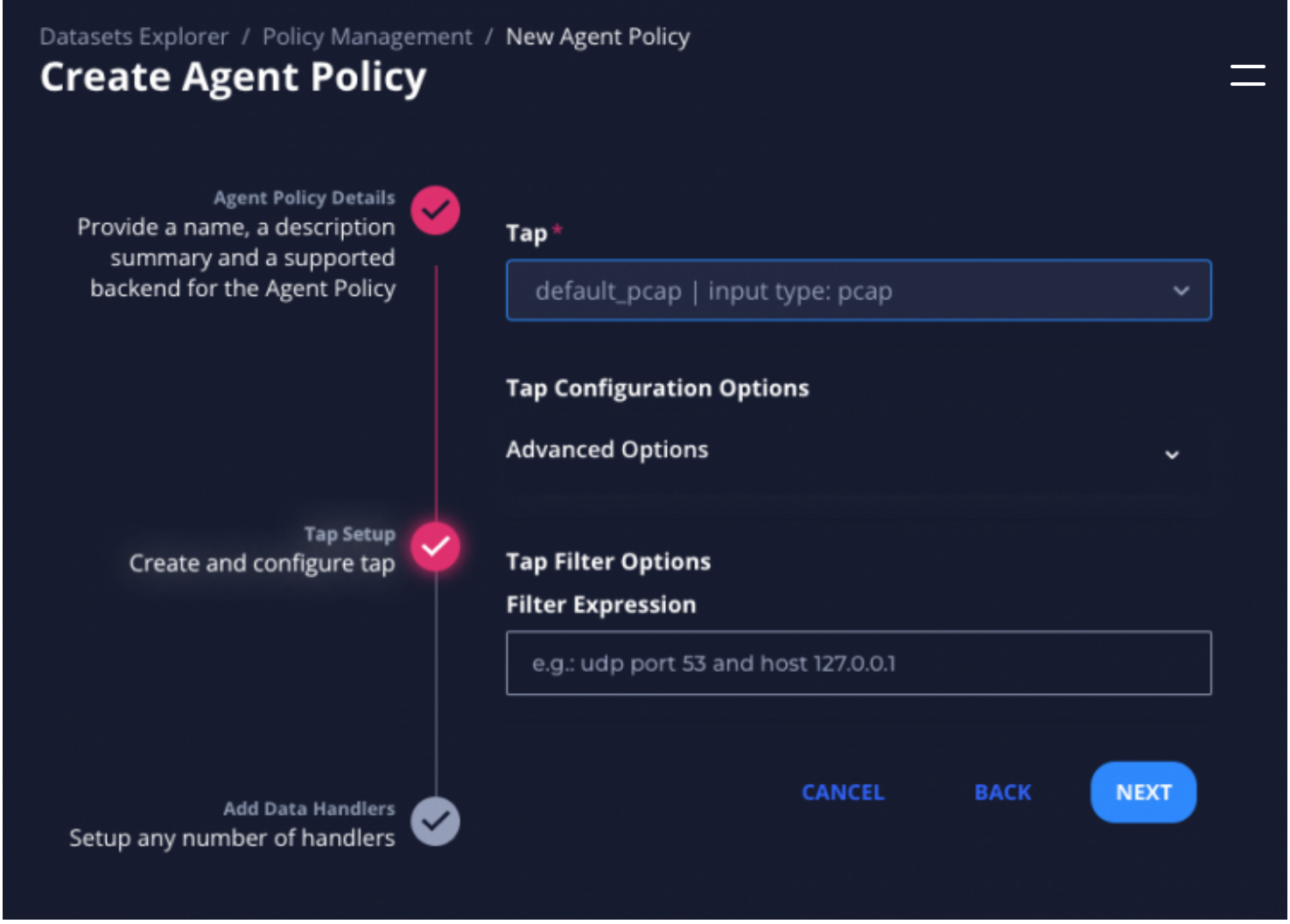
Next, click New Policy on the top right of the table:



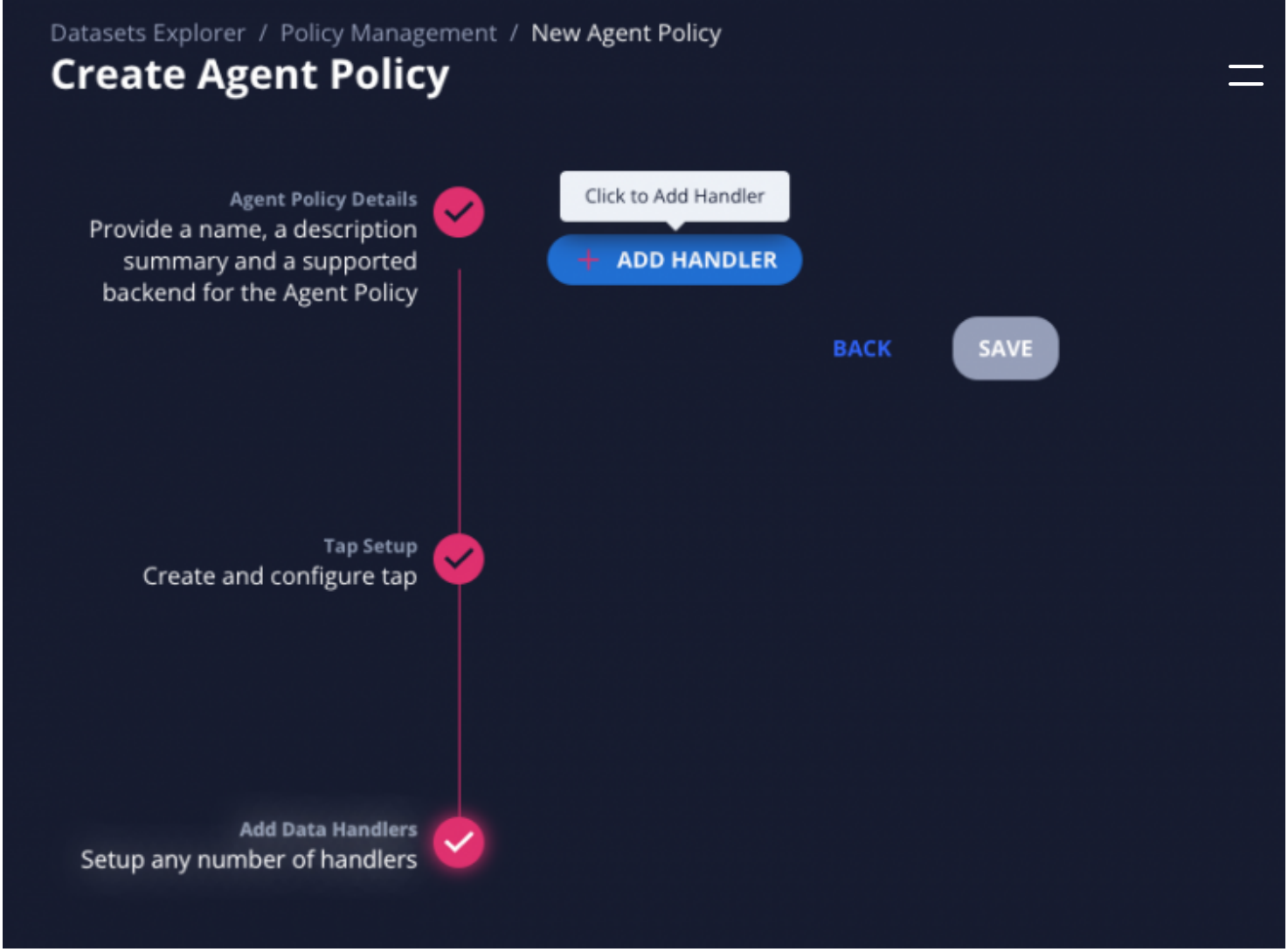
Next, give your new policy a name. It needs to be unique, and can't contain spaces (use underscores or dashes instead). You may add an optional description, then click Next.



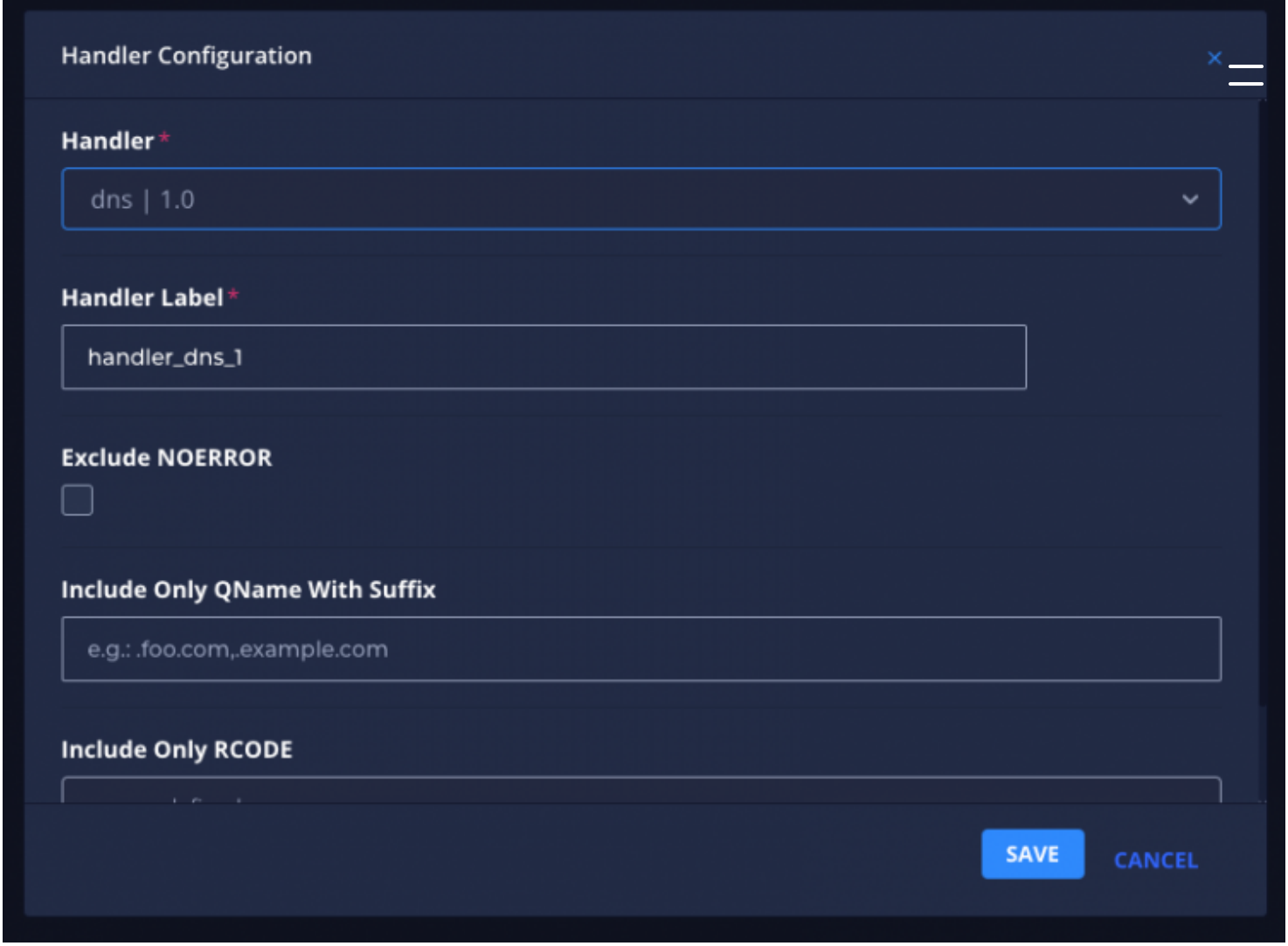
Next, select the Tap (input stream) to analyze - in this example, we'll use "default_pcap" which is the default for Packet Capture. All of the other options are advanced and may be left as is, so click Next.



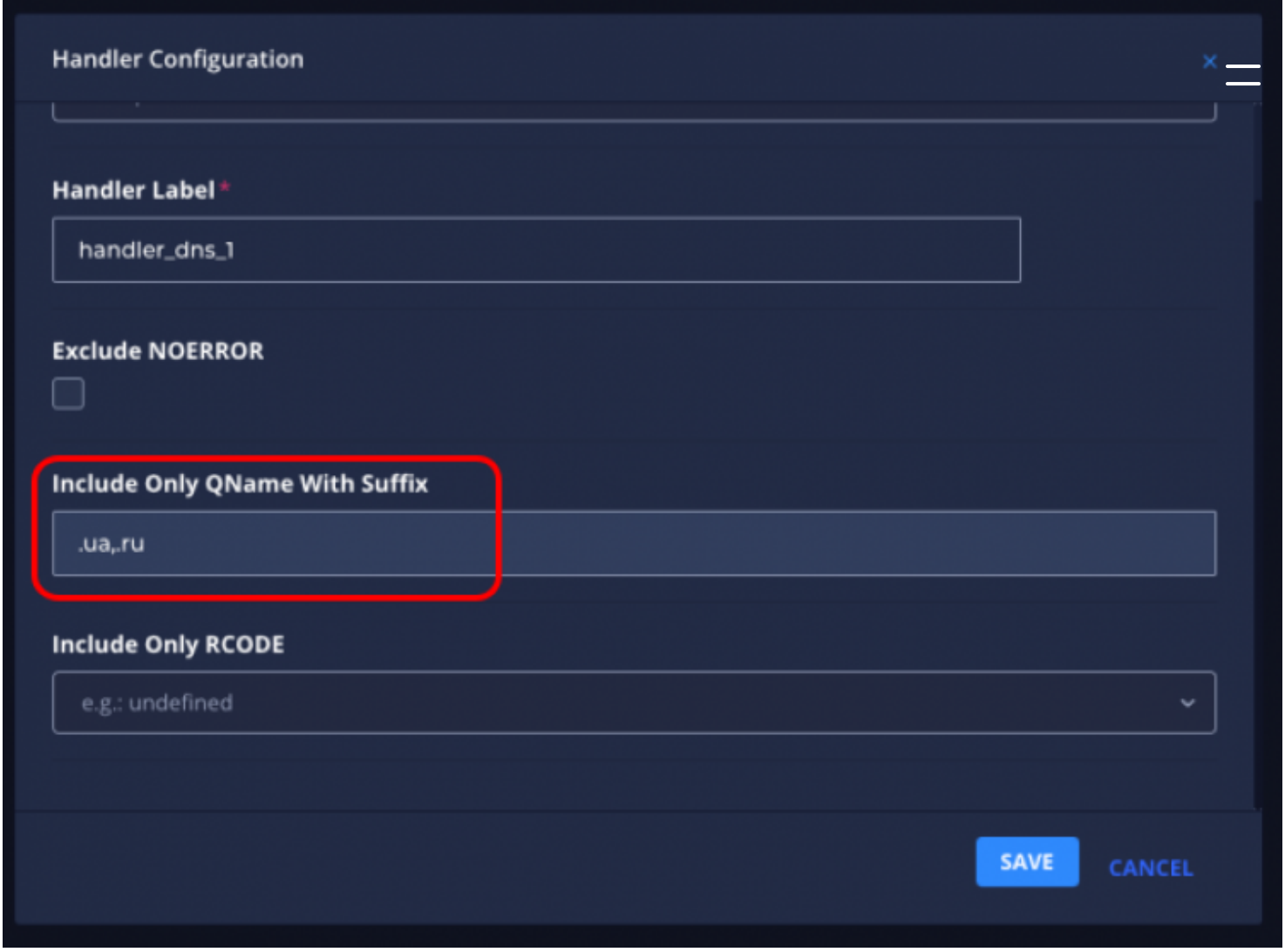
Next, you need to add a Stream Handler to the policy, which tells it how to analyze the input stream selected in the previous step. Click Add Handler.



Because we want to analyze DNS traffic, select the “dns” handler. The only required field here is the Handler Label, which is automatically generated for you (handler_dns_1 in this case). But we want to customize the analysis by only analyzing domain names ending in “.ua” or “.ru”. This is done with the filter labeled “Include Only QNames With Suffix”.



In this box we can input a comma delimited list of suffixes, so enter “.ua,.ru”, then click Save to save this Handler.



Finally, click Save to save the policy.

You can now create a **Dataset** to send this policy to your agents.

Further Reading

FEATURED

Orb - A New Paradigm for Dynamic Edge Observability

Last week we announced the launch of NS1 Labs - learn more about Orb and pktvisor, two open source technologies developed by NS1 Labs that align with our vision for the future of application and audience connectivity.

Read the Article ⊙

A Wave of Open Source Innovation at NS1 Labs

Read the Ebook ⊙

✳ View all Resources

NS1.
an IBM Company

ABOUT

Blog

News

Careers

Diversity & Inclusion

SUPPORT

Help Center

NS1 Status

Documentation

Contact Support

SUBSCRIBE

Email Address

Subscribe

Partner Portal

Terms of Service

Privacy Policy

Responsible Disclosure Policy